Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2021.DOI

Post-Quantum Era Privacy Protection for Intelligent Infrastructures

Lukas Malina[1], Petr Dzurenda[1], Sara Ricci[1], Jan Hajny[1], Gautam Srivastava[2,3], Raimundas Matulevičius[4], Abasi-amefon O. Affia[4], Maryline Laurent[5], Nazatul Haque Sultan[5], Qiang Tang[6]

[1]Department of Telecommunications, Brno University of Technology, Brno, Czech Republic
[2]Department of Mathematics and Computer Science, Brandon University, Brandon, MB R7A 6A9, Canada (e-mail: srivastavag@brandonu.ca)
[3]Research Center for Interneural Computing, China Medical University, Taichung 40402, Taiwan, Republic of China
[4]Institute of Computer Science, University of Tartu, Tartu, Estonia
[5]SAMOVAR, Telecom SudParis, Institut Polytechnique de Paris, France
[6]Luxembourg Institute of Science and Technology, Luxembourg
E-mail: {malina, dzurenda, ricci, hajny }@feec.vutbr.cz, srivastavag@brandonu.ca, {raimundas.matulevicius, amefon.affia}@ut.ee, maryline.laurent@telecom-sudparis.eu, qiang.tang@list.lu

Corresponding author: Lukas Malina (e-mail: malina@feec.vutbr.cz)

ABSTRACT As we move into a new decade, the global world of Intelligent Infrastructure (II) services integrated into the Internet of Things (IoT) are at the forefront of technological advancements. With billions of connected devices spanning continents through interconnected networks, security and privacy protection techniques for the emerging II services become a paramount concern. In this paper, an up-to-date privacy method mapping and relevant use cases are surveyed for II services. Particularly, we emphasize on post-quantum cryptography techniques that may (or must when quantum computers become a reality) be used in the future through concrete products, pilots, and projects. The topics presented in this paper are of utmost importance as (1) several recent regulations such as Europe's General Data Protection Regulation (GDPR) have given privacy a significant place in digital society, and (2) the increase of IoT/II applications and digital services with growing data collection capabilities are introducing new threats and risks on citizens' privacy. This in-depth survey begins with an overview of security and privacy threats in IoT/IIs. Next, we summarize some selected Privacy-Enhancing Technologies (PETs) suitable for privacy-concerned II services, and then map recent PET schemes based on post-quantum cryptographic primitives which are capable of withstanding quantum computing attacks. This paper also overviews how PETs can be deployed in practical use cases in the scope of IoT/IIs, and maps some current projects, pilots, and products that deal with PETs. A practical case study on the Internet of Vehicles (IoV) is presented to demonstrate how PETs can be applied in reality. Finally, we discuss the main challenges with respect to current PETs and highlight some future directions for developing their post-quantum counterparts.

INDEX TERMS Authentication; Cryptography; Internet of Things; Intelligent Infrastructures; Post-Quantum Cryptography; Privacy; Privacy-Enhancing Technologies; Security; Threats.

I. INTRODUCTION

INTELLIGENT Infrastructures (IIs) are known to interconnect a variety of Internet of Things (IoT) applications and services to capture and analyze data as well as invoke autonomic responses. II is a type of IoT system as it encompasses cooperative interactions with various things or objects to reach a common goal [1]. IIs based on IoT utilize cooperative sensing and networking capabilities and bring new benefits to society, customers, and the environment. However, highly connected electronic objects and digital systems around people's lives form a large intelligent network that may cause personal data leakages.

In theory, incoming IoT/II applications should already include privacy protection during the design and application stages. Security engineers and practitioners may use various privacy protection principles, technologies, or Privacy by Design (PbD) strategies. PbD involves various technological and organizational components,

implementing privacy as well as data protection principles. Hoepman [2] proposed eight privacy design strategies, i.e., Minimize, Hide, Separate, Aggregate, Inform, Control, Enforce, Demonstrate. Privacy protection techniques, better known as Privacy-Enhancing Technologies (PETs), can implement most of these privacy strategies. PETs are usually based on the principles of data minimization, anonymization, pseudonymization, and data protection that allow users to protect their Personally Identifiable Information (PII). The European Union Agency for Network and Information Security (ENISA) defines PETs as the broader range of technologies that are designed for supporting privacy and data protection. In the recent ENISA report [3], a fundamental inventory of the existing approaches and privacy design strategies were provided. The report distinguishes the privacy enabling techniques such as authentication, attribute-based credentials, secure private communications, communications anonymity/pseudonymity, privacy in databases, storage privacy, privacy-preserving computations, transparency enhancing techniques, and intervenability enhancing techniques.

Privacy protection is already an important part of many regulations and international standards. In 2011, the ISO organization released the ISO/IEC 29100:2011 Privacy Framework Standard[1] which aimed at protecting PII based on 11 distinct principles, from data collection, data usage, data storage to data destruction. Furthermore, Europe's general data protection regulation (GDPR) replaced the Data Protection Directive 95/46/EC in 2018 [4]. The GDPR comprises the most basic data security and privacy principles in Article 5 that includes lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity/confidentiality, and accountability. Moreover, the GDPR enhances various privacy aspects such as consent, the right to be forgotten, and privacy (data protection) by design mentioned in Article 25. Thus, privacy-preserving protection for II services are in the scope of the aforementioned regulations.

In this paper, a map of the current PETs and their practical deployment in IoT/IIs is presented in an in-depth and well-organized manner to assist the article's reader in navigating this complex and ever-evolving area of research. In Table 1, we present all basic acronyms and notations that are used throughout the paper.

Many PETs are based on traditional cryptographic primitives such as Public-Key Cryptography (PKC) algorithms. Nonetheless, most of the current PKC schemes are theoretically vulnerable to potential attacks run by quantum computers. Post-Quantum Cryptography (PQC) offers solutions against those attacks. Hence, PETs based on "post-quantum" cryptographic primitives are the natural evolution of PETs in the future. As such, preparation for the future should begin now, and the design of some II services to be resistant to potential future threats should commence. By design, the post-quantum PETs promise to preserve data privacy in II services in the long term. This will encourage

[1] https://www.iso.org/standard/45123.html

TABLE 1
LIST OF ABBREVIATIONS, ACRONYMS AND NOTATIONS

AA	Anonymous Authentication
ABC	Attribute-Based Credentials
ABE	Attribute-Based Encryption
AES	Advanced Encryption Standard
APEA	Anonymous and Pseudonymous Entity Authentication
ARM	Advanced RISC Machine
BIKE	Bit Flipping Key Encapsulation
BLISS	Bimodal Lattice Signature Scheme
BS	Blind Signatures
CBC	Code-Based Cryptography
CCA	Chosen-Ciphertext Attack
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
DP	Differential Privacy algorithms
DoS	Denial of Service
DS	Data Splitting
DTLS	Datagram Transport Layer Security
ECDSA	Elliptic Curve Digital Signature Algorithm
FHE	Fully Homomorphic Encryption
FPGA	Field Programmable Gate Array
GPS	Global Positioning System
GS	Group Signatures
HBC	Hash-Based Cryptography
HE	Homomorphic Encryption
HFE	Hidden Field Equations
IBC	Isogeny-Based Cryptography
II(s)	Intelligent Infrastructure(s)
IMU	Inertial Measurement Unit
IoT	Internet of Things
IoV	Internet of Vehicles
ITS	Intelligent Transportation System
KEM	Key Encapsulation Mechanism
KP-ABE	Key-Policy Attribute-Based Encryption
LBC	Lattice-Based Cryptography
LWE	Learning With Errors
MAC	Media Access Control address
MCU	MicroController Unit
Mixnet	Mix Network
MSS	Multi-message Signature Scheme
MVC	Multivariate-Based Cryptography
PET(s)	Privacy-Enhancing Technology(ies)
PHE	Partially Homomorphic Encryption
PLT(s)	Parking Lot Terminal (s)
PSP	Parking Service Provider
PQ	Post-Quantum
PQC	Post-Quantum Cryptography
QC	Quantum Computer
QR	Quantum-Resistant
RFID	Radio-Frequency IDentification
RLWE	Ring Learning With Errors
RS	Ring Signatures
SDC	Statistical Disclosure Control
SE	Searchable Encryption
SIDH	Supersingular Isogeny Diffie Hellman
SIKE	Supersingular Isogeny Key Encapsulation
SMC	Secure Multi-party Computations
SSID	Service Set IDentifier
U	User
TLS	Transport Layer Security
ToR	The onion Router
TTP	Trusted Third Party
UOV	Unbalanced Oil and Vinegar Cryptosystem
V	Vehicle
VPN	Virtual Private Network
WPA	Wi-Fi Protected Access
ZKP	Zero-Knowledge Proof

the deployment of use cases in smart city and industrial sensors, smart healthcare applications, defence systems [5]. The downside is that post-quantum PETs may introduce computational and memory constraints on some IoT nodes as classic PKC schemes have done in the past.

In general, this survey paper centres on answering the following two questions: "Which current Privacy-Enhancing Technologies (PETs) are suitable for Intelligent Infrastructures (IIs) which involve IoT devices", and "Which PETs are also secure in a post-quantum era? "

A. PRIVACY CONCERNS IN IOT/II

There are plenty of privacy and security issues in current IoT/II systems since they typically rely on mobile connectivity and resource-constrained devices. In a recent article featured in Forbes magazine, Rotem *et al.* showed how an IoT management platform run by an Asian company Orvibo was easily accessible over an HTTP connection[2]. Through a simple Internet Protocol connection to the database, they gained access to over 3 billion records, including a slew of private information such as usernames, account codes for reset, payment information, and user passwords. This breach of Orvibo highlights the different types of data accessible once a system is compromised in an unsecured IoT/II system in the reality.

Next, we describe some application domains in IoT/IIs and provide some example privacy issues to motivate the following-up discussions.

Internet of Vehicles: Autonomous vehicle technology is a hot area of research and will become quite common in the years to come. The Internet of Vehicles (IoV) is an ongoing service connecting a large set of sensors, controllers, and devices attached to vehicles or vehicle infrastructure to ease autonomous control. It is quite a challenge to design effective privacy mechanisms that, in turn, can make sure a collection of IoV Big Data is both trusted and not tampered with. For example, there is a massive risk involved with injecting a malicious or fraudulent message into IoV by malicious vehicles. This process can endanger the entire traffic system(s). Moreover, once compromised, an entire network may endanger the lives of any persons involved in the network. In a specific use case, smart vehicle parking services could also encounter several privacy issues, e.g., privacy-preserving access to parking lots, payments and making statistics. Section VII focuses on this scenario and presents more details.

Healthcare IoT/II: In 2015, researchers at the University of Arizona show that more than $70,000$ medical devices had been exposed online, among which 20% belonged to a single health organization [6]. It is evident that many IoT devices still connect to the Internet through dated Operating Systems which do not possess modern security infrastructure. This study showed that most exposed devices ran Windows XP, an OS that has not been serviced in almost a decade. Nevertheless, Windows XP still finds itself at the backbone of many legacy systems worldwide, adding to the potential future privacy breaches that may occur as time passes on in Healthcare IoT. Other known privacy concerns in Healthcare were brought to light through Shodan, a service that promotes itself as the "world's first search engine for devices"[3]. Devices found on Shodan running Windows XP with dated security are often easy to crack using Brute Force attacks alone.

Smart Homes: In Smart Home IoT/II, a sought-after commercial area allows household appliances to gain accessibility to the Internet. A well-known attack on these systems is the FATS attack, short for Fingerprint and Timing based Snooping (FATS), which was first presented in [7]. FATS involves room classification, activity recognition, and activity detection by analyzing WiFi traffic from a given sensor network that has been deployed in a Smart Home. The attack itself relies heavily on packet sniffing techniques of WiFi activity instead of through last-mile ISP (Internet Service Provider) or adversaries located somewhere in a WAN (Wide Area Network). The attack itself shows that simple WiFi packet sniffing techniques that have been available for over a decade now can still give malicious entities an advantage in breaching privacy in modern Smart Homes.

Smart Cities: Assisted living is defined as a living situation where senior citizens (elderly) take the aid of IoT devices to ease some of their daily tasks and use devices with Internet connectivity to monitor their movements to ensure their safety. In [8], Henze *et al.* showed that unobtrusive sensors used to monitor senior citizens' vital signs might be an area of concern for privacy breaches. These sensors will read vitals from patients and upload this information to the cloud for giving medical practitioners fast access to the information as needed. The authors pinpointed two levels of privacy issues, one with personal data and the other focusing on medical information. The medical information of patients and other private data may be vulnerable during transmission to the cloud. Since sensor devices are often constrained and unable to run complex security protocols, they are often the single point of failure. It is an open issue to securely integrate computation-expensive services like cloud storage with constrained IoT devices like sensors.

TABLE 2
IoT Areas with Application Example and Privacy Concerns [9]

IoT Area	Privacy Concerns	Application
Internet of Vehicles	Action, Image	RideLogic
Healthcare IoT/II	Data, Person	Geniatech, Cycore
Smart Home	Data, Location	Orvibo
Smart Cities	Communication, Location Data	Cisco

[2] https://www.forbes.com/sites/daveywinder/2019/09/16/personal-data-from-entire-166m-population-of-ecuador-leaked-online/?sh=7c6a1f6a3705

[3] https://www.shodan.io/

Table 2 summarizes the privacy issues in the aforementioned application domains. Referring to the 7 privacy concerns proposed by Finn *et al.* [9], we elaborate the summarized privacy concerns from Table 2 as follows:

- **Privacy of person**: right to keep both body characteristics and functions private.
- **Privacy of behaviour and action**: right to keep personal sensitive issues (sexual, political, religions) private.
- **Privacy of communication**: right to keep personal sensitive communication (e-mails, telephone, cell phone, wireless communication, etc.) private.
- **Privacy of data and image**: right to keep personal data, including images, private.
- **Privacy of thoughts and feelings**. right to keep personal thoughts and feelings private.
- **Privacy of location and space**: right to move freely in public without being identified (keep the location private).
- **Privacy of association**: right to associate with others freely without being monitored.

A detailed description of privacy threats and leakages in IIs is provided in Section III. More examples of privacy-preserving use cases and practical deployment (pilots, products) are discussed in Section VI.

B. CONTRIBUTION

Taking aim at a comprehensive analysis of privacy protection for IoT/IIs, this paper maps the recent technical-based PETs and surveys the post-quantum resistant PETs. The readiness of PQ PETs in IoT/IIs is also discussed. In more detail, the contribution can be summarized as follows:

- Identification of privacy threats and leakages in IoT/IIs, even for the post-quantum era (Section III).
- Description of current PETs and some recent quantum-resistant PET schemes (Sections IV and V).
- An inventory of practical deployments of PETs in IoT/IIs, including a list of current projects and products and various use cases where PETs can be deployed (Section VI).
- An illustrative case study for demonstrating a privacy-preserving II service, e.g. the Internet of Vehicle (IoV), and presenting some options for a secure design in the post-quantum era (Section VII).
- Discussion of main challenges and future research directions for quantum-resistant privacy-enhancing technologies (Section VIII).

C. PAPER ORGANIZATION

The outline of the paper is depicted in Figure 1. In Section II, we give an overview of the literature. Next in Section III, we focus on privacy threats in Intelligent Infrastructures. Section IV focuses primarily on PETs and presents relevant solutions for IoT/IIs. Section V surveys emerging security and privacy solutions and technologies suitable in IoT/IIs for the post-quantum era. Section VI maps the practical deployment of PETs in IoT/IIs, and Section VII presents a chosen case study of PETs deployed in the selected II service of IoV. Section VIII discusses the main challenges and future research directions of PETs in IoT/IIs. Lastly, some concluding remarks are given in Section IX.

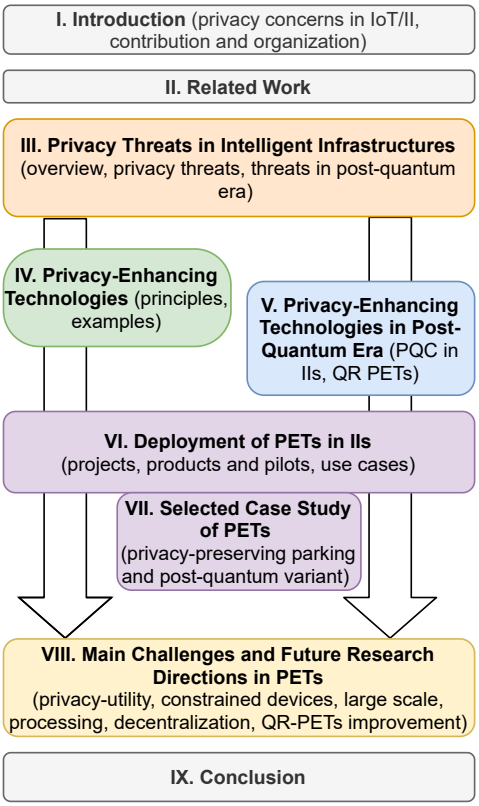


FIGURE 1. The outline of the survey paper

II. RELATED WORK

Several interesting studies and survey papers focus on security and privacy in IoT and intelligent infrastructures [10]–[17]. Furthermore, there are surveys and research papers that focus solely on privacy in IoT and IIs. Some examples are given in [18]–[26]. Representative surveys from the literature are illustrated in Table 3, where the last four columns (e.g. privacy threats analysis, PETs analysis, quantum-resistant PETs, and practical use cases/projects) define the objectives and privacy coverage. From Table 3, it is clear that our survey is more systematic and comprehensive as it is the only survey to our knowledge that covers all four columns together. In the rest of this section, we describe the detailed contribution of some papers from Table 3 as well as other relevant ones.

Porambage *et al.* [18] provided a holistic view of the privacy challenges in IoT. The authors discuss topics in IoT privacy solutions, and future research directions.

TABLE 3
COMPARISON WITH OTHER SURVEYS FOCUSED ON PRIVACY IN IOT/IIS AND RELATED AREAS

Paper reference	Year	Area	Objective and main coverage	Privacy threats analysis	PETs analysis	Quantum resistance	Practical projects / use cases
Porambage *et al.* [18]	2016	IoT	Overview of privacy issues and challenges	LD	ND	ND	LD
Shim [11]	2016	WSN	Survey on public key cryptographic primitives	ND	ND	LD	ND
Kumar *et al.* [15]	2016	Smart Grid	Survey on security and privacy issues in smart metering	✓	LD	ND	ND
Lopez *et al.* [20]	2017	WSN	Survey on privacy problems in IoT and WSN	✓	LD	ND	LD
Lin *et al.* [13]	2017	IoT	Survey on IoT technologies and its security and privacy issues	LD	LD	ND	✓
Sen *et al.* [13]	2018	IoT	Survey on privacy solutions in IoT	✓	✓	ND	LD
Seliem *et al.* [22]	2018	IoT	Survey on privacy issues and concerns in IoT systems	✓	LD	ND	✓
Cha *et al.* [21]	2018	IoT	Survey on PETs solutions in IoT	LD	✓	ND	✓
Curzon *et al.* [25]	2019	Smart cities	Survey on PETs solutions in smart cities	LD	✓	ND	LD
Butun *et al.* [14]	2019	IoT	Survey on attacks and security solutions in WSN and IoT	LD	LD	ND	✓
Li and Palanisamy [24]	2019	IoT	Survey on privacy laws, IoT architectures and PETs	LD	✓	ND	✓
Roy and Kalita [27]	2019	Constr. devices	Survey on post-quantum cryptography on constrained devices	ND	ND	✓	ND
Fernandez-Carames [5]	2019	IoT	Survey on quantum-resistant cryptosystems	ND	ND	✓	✓
Nejatollahi *et al.* [28]	2019	General	Survey on trends in lattice-based cryptographic schemes	ND	ND	✓	LD
Hassan *et al.* [26]	2020	CPS	Survey on differential privacy techniques for CPSs	✓	LD	ND	✓
Hamad *et al.* [17]	2020	IoT	Survey on general security and privacy issues in IoT	LD	✓	ND	✓
Lohachab *et al.* [29]	2020	IoT	Survey on post-quantum cryptographic techniques for securing IoT network	ND	ND	✓	LD
Yang *et al.* [30]	2020	Cloud Storage	Survey on data security and privacy protection for cloud storage	LD	✓	LD	LD
This work	2020	IoT and IIs	Survey on current PETs, privacy projects and quantum resistant PETs	✓	✓	✓	✓

✓ - Detailed Discussion; LD - Limited Discussion; ND - No Discussion.

Next, Dwork [19] outlined 5 scientific challenges regarding privacy in intelligent infrastructures, as follows:

1) Privacy for streaming IoT-data
2) Privacy at the IoT-edge
3) Decentralized private computation
4) Variable privacy
5) Event-based privacy

Cha *et al.* [21] aimed at identifying the current state of development of PETs in various fields of IoT applications. The paper also examines whether existing PETs comply with the latest legal principles and privacy standards. The survey explores 120 papers focusing on the solutions of PETs in IoT, where 28% of papers are dedicated to building and home automation, 13% to e-healthcare, 13% to smart cities, 9% to wearable, 8% to automotive, 2% to smart manufacturing and 27% are general cases. In this work, PETs in IoT have been categorized into 7 research domains:

- Control over data
- Enforcement
- Anonymization or pseudonymization
- Personal data protection
- Anonymous authorization
- Partial data disclosure
- Holistic privacy preservation

In this work, Cha *et al.* extracted 15 privacy principles from GDPR and ISO/IEC 29100:2011, and linked them with PETs papers and presented some future directions of advanced technologies.

Seliem *et al.* [22] reviewed existing research and propose solutions to rising privacy concerns from multiple viewpoints to identify both risks and the mitigation of those risks. The paper provides an evaluation of privacy issues and concerns in IoT systems due to resource constraints. The authors also describe IoT solutions that embrace a variety of privacy concerns such as identification, tracking, monitoring, and profiling. Sen *et al.* [23] dealt with differences between privacy and security. They present 11 general approaches and techniques that are being used to fulfil privacy requirements. Nevertheless, their analysis and classification models are not overly deep. Curzon *et al.* [25]

aimed to show how individuals' privacy could be exposed in various Smart City applications and how the exposure could be mitigated using multiple privacy-enhancing technologies. This survey also briefly presents some PETs. Recently, Hassan *et al.* [26] surveyed differential privacy techniques for cyber-physical systems, including the industrial Internet of Things. The authors present open issues, challenges, and future research directions for differential privacy techniques in cyber-physical systems. Nevertheless, their study does not explore other PETs and their quantum-resistant variants.

Several review papers have focused on post-quantum cryptography, such as [28]–[37]. Bernstein and Lange [35] explained the damage of classic cryptography done by quantum computing and describe some candidates for post-quantum cryptography. Tan and Zhou [36] reviewed post-quantum (PQ) digital signature algorithms and analyzed PQ signatures' suitability in various general applications such as TLS and Bitcoin, GSM eSIM, and so on. Nejatollahi *et al.* [28] provided a comprehensive survey by focusing on lattice-based cryptography (LBC) and its use in computer security, including implementation challenges in software and hardware. The authors solely focus on LBC schemes and do not consider post-quantum privacy-enhancing cryptography schemes. Recently, Fernandez-Carames [5] surveyed quantum-resistant cryptosystems and schemes for IoT. The author maps post-quantum security projects and results of post-quantum schemes applied on various devices from resource-constrained microcontrollers, FPGA cards to cloud servers. Lohachab *et al.* [29] provided a general survey on post-quantum techniques for securing IoT networks but without a detailed discussion of PETs. Furthermore, the implementation aspects of PQC on constrained devices are also studied in other papers such as [27], [38]. Finally, Yang *et al.* [30] surveyed several PETs that are suitable for cloud storage, but their discussion about the quantum resistance of PETs is limited to one subsection dedicated to Post-Quantum Encryption.

To the best of our knowledge, there is a lack of comprehensive studies that connect essential topics in both privacy protection and post-quantum cryptography with their adoption in IoT/II services. Our study categorizes and presents concrete privacy-enhancing technologies based on traditional cryptography and emerging post-quantum cryptography constructions. We also map privacy-required IoT/II applications, privacy threats in IoT/II, and PETs deployed in concrete projects/products.

III. PRIVACY THREATS IN INTELLIGENT INFRASTRUCTURES

A. HIGH-LEVEL OVERVIEW

Most IoT systems consist of (*i*) systems that collect data about the state of scenarios, (*ii*) systems that transmit collected data, and (*iii*) systems that provide the data to end-users following a predefined process [39]. The vehicular subsystem considers the interaction of systems within the Intelligent Transportation System (ITS) as it concerns vehicles and their agents (e.g., vehicle, infrastructure, and users such as drivers, passengers, pedestrians). IoT/II systems consist of three architectural layers [40]–[45]:

- **Perception**: The perception layer contains software components and hardware devices (sensors, actuators, visioning, and positioning devices), carrying out basic functions of collection, controlling, and storing data.
- **Network**: The network layer facilitates wired or wireless transmission (in-vehicle, vehicle to vehicle, and vehicle to infrastructure) of collected data from the perception layer.
- **Application**: In the application layer, the network layer meets the end-user, services, processes, computing, and storage, allowing high-level intelligent processing of the sensed, generated, and transmitted data.

A risk can be defined as an event where the vulnerability of an asset in a system is exploited by an attacker (*threat*), leading to some *impact* – negating the asset's criteria for security in a system [46], [47]. Table 4 summarizes the threats at the different architectural layers. The threats are categorized following the STRIDE[4] threat model [50] based on the first impact experienced [51].

Perception layer threats attack sensing, vision, positioning and actuating components. Following the work in [51], Table 4 includes 24 threats. *Network layer threats* affect the system assets' ability to transmit the necessary data for an IoT/II function. Data is typically transmitted through local/internal network, device-to-device, and device-to-infrastructure communication technologies. Table 4 assembles 47 threats [51]. *Application layer threats* that involve attacks to disrupt or corrupt high-level IoT/II processes and services to illustrate the network layer threats. To illustrate them, Table 4 includes 12 threats.

B. PRIVACY THREATS CATEGORIZATION

In the IoT era, privacy can be affected by personal information collection, processing, sharing, and invasion/leakage [52]. Information collection, processing, and sharing activities are fundamental in running these cooperative IoT/II systems. Personal information is collected, which may include:

1) user identity in general
2) geolocation in transportation
3) health conditions in healthcare

[4]Several threat classification models exist. For example, CAPEC (Common Attack Pattern Enumeration and Classification) provides a taxonomy of the security attacks to exploit known vulnerabilities [48]. Elsewhere in [49], the MITRE ATT&CK model presents a knowledge base of adversary techniques highlighted after the observation of the real-world cases. In our study we select the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of privilege) model, which suggests a straightforward way to elicit and categorize security threats by explaining critical protected assets that have been impacted.

TABLE 4
SUMMARY OF SECURITY THREATS, ADAPTED FROM [51]

System Asset	Threats					
	S	**T**	**R**	**I**	**D**	**E**
Perception layer	Spoofing, Node Impersonation, Illusion, Replay, Sending deceptive messages, Masquerading	Forgery, Data manipulation, Tampering, Falsification of readings, Message Injection	Bogus message	Stored attacks, Eavesdropping	Message saturation, Jamming, DoS, Disruption of system	Backdoor, Unauthorized access, Malware, Elevation of privilege, Remote update of ECU
Network layer	Sybil, Spoofing (GPS), Replay attack, Masquerading, RF Fingerprinting, Wormhole, Camouflage attack, Impersonation attack, Illusion attack, Key/Certificate Replication, Tunneling, Position Faking	Timing attacks, Injection (message, command, code, packet), Manipulation/Alteration/ Fabrication/Modification, Routing modification/manipulation, Tampering (broadcast, message transaction, hardware), Forgery, Malicious update (software/firmware)	Bogus messages, Rogue Repudiation, Loss of event trace-ability	Eavesdropping, Man-in-the-middle, ID disclosure, Location tracking, Data sniffing, Message interception, Information disclosure, Traffic analysis, Information gathering, TPMS tracking, Secrecy attacks	DoS/DDoS, Spam, Jamming, Flooding, Message suppression, Channel interference, Black hole.	Malware, Brute Force, Gaining control, Social engineering, Logical attacks, Unauthorized access, Session Hijack
Application layer	Spoofing, Sybil, Illusion attack	Malicious Update		Eavesdropping, Location tracking, Privacy leakage	DoS	Jail-breaking OS, Social engineering, Rogue Data-center, Malware

4) lifestyle habits inferred from intelligent surveillance, smart energy, and home

Service providers process the provided and disseminated data to query required functions and use cloud servers to provide personalized or group/crowd-sourced services. As data in IoT/II systems become abundant for its use in intelligent applications (i.e., assisted or autonomous driving [53], healthcare services in Smart Cities [54], Smart Homes), the implication of privacy invasion/leakage is increasingly becoming a major concern.

The following privacy threats and attacks can be observed in IoT/II environments:

- **Data over-collection threat**: Unaware and/or superabundant collection of personal data.
- **Linkage threat**: Creating some unforeseen data results by different systems can lead to the linkage of personal data by data correlation.
- **Identification threat**: Associating personal data, e.g., name, address, gender, physical signatures (voice, face) with a concrete user identity.
- **Lifecycle transitions leakage**: Obtaining personal information from devices in a certain stage of their lifecycle when the devices are not under owner (user) control.
- **Privacy-violating interactions and presentation leakage**: Unwanted presenting user's data through a medium component (voice, video screens) placed in public. This can lead to the disclosure of user sensitive information.
- **Localization leakage**: Undesirable leakage of a user's location by Global Positioning System (GPS) coordinates, IP addresses, latency, or cell phone location.
- **Behavioral leakage**: Unwanted determining and recording a user's behaviour in a certain time and place.
- **Tracking attack**: An attacker can trace and record a person's movement through time and space (based on localization or behavioural leakages and user identification).
- **Profiling attack**: An attacker can create profiles to analyze information about users and infer their interests by correlation with their profiles and data.
- **Inventory attack**: An attacker can send certain query requests to the object and analyze the related responses to determine the interests of users, e.g., unauthorized detection of health issues, industrial espionage.
- **Identity-theft attack**: An attacker can steal user identity (credentials) to misuse his/her services or harm a given user's reputation.

Privacy leakages can occur due to the characteristics of perception, network, and application architecture layers. In the following subsections, we illustrate a few key examples.

1) Privacy Leakages through IoT/IIs Perception Devices

Privacy leakages in the perception layer can occur during data sensing and storage. IoT/II devices are especially vulnerable to privacy leakage and information inference by attackers.

Privacy leakages can occur in Smart Home applications by analyzing the physical characteristics of smart devices [55]. Close monitoring and inference of smart meter "appliances' ON/OFF status at different times" can reflect the usage patterns of energy consumers. Adversaries can obtain meter readings and background knowledge of common appliances' consumption rates, estimate what devices are possibly switched ON, and infer a higher probability of looking at the reading time (i.e., microwave at 6:30 pm or TV at 8:00 pm). Besides the consumption

rate/time, an inference can be made by appliances' unique signatures on the length of usage (i.e., washer running continuously for at least 30 minutes in general) [56].

Intelligent surveillance, although designed for monitoring criminal behaviours, may also capture smart city residents' daily life habits and behaviours, and such data, even being unconsciously disclosed to untrusted entities, may become prejudicial to the residents' privacy [57].

In vehicular IIs where integrating mobile Inertial Measurement Unit (IMU) sensors with the vehicle can lead to the development of numerous beneficial applications on the one hand. On the other hand, the collection of IMU data, available on various devices such as smartphones, Original Equipment Manufacturer (OEM)-authorized OBD-II dongles, and wearable devices can leak driver privacy [53]. As an example, in usage-based automotive insurance plans to have restrictions enforced using the insurance company's application may provide evidence against insurance claims [53]. It can also reflect the driver's risk level [58] with driving IMU data gathered from the application as an Event Data Recorder. Although the purpose of the application was not for driver fingerprinting, this can be used to do just that [53], [58], [59]. Research has suggested applying off-the-shelf privacy and security techniques, such as encryption, anonymity, and access control, to preserve privacy leakage during data sensing [57].

2) Privacy Leakages through IoT/IIs Network

Privacy leakages in the network layer can occur during data transmission. In vehicular IIs, privacy leakage attacks happen as vehicles periodically broadcast *beacons* that contain information about the vehicle. This information can include speed, vehicle identity, current vehicle location, position, and acceleration [60], [61]. Risk impact includes the loss of confidentiality of sensitive information contained in the beacons following an eavesdropping attack to trace the vehicle which is achieved by linking the location data together [60], [61]. The *infotainment* system in vehicular IIs, which is an amalgamation of in-vehicle entertainment and information, can be connected to various external networks which may lead to leakage of personal information such as user location and private call recordings stored directly on the infotainment system. In Smart Home network infrastructures, privacy leakages can be leveraged to infer sensitive information about the occupants by the pre-processing, classification, and traffic data matching [62]. Wireless communication technologies are prone to privacy leakages, so an attacker can monitor encrypted network traffic of smart home devices to infer sensitive information without using any advanced technique [63].

Besides encryption, research has suggested the injection of noisy data flows in communication between smart devices and the Internet [62]. Other techniques, such as VPN, Tor-like Tools, signal attenuation, and/or traffic shaping could also be used to avoid privacy leakage during data communication [63].

3) Privacy Leakages through IoT/IIs Applications

Privacy leakages in the application layer can occur during data processing and storage. Combining multiple data sources from different data holders, perception devices, and applications increase the risk of sensitive data leaks through correlation [64].

The vehicular II application layer collects all data from fog nodes, environmental sensors, and vehicular GPS sensors over a long period. Data can be leaked by exposing the raw pre-processed data about a given person, such as health status by a vehicle safety application, etc., to undeclared/unwanted entities [65]. The frequency of the sent health status information can determine the type of health issue a driver faces by detecting a pattern in the received data. For instance, if a driver is a smoker and his/her blood pressure and sugar level readings are being uploaded to the application for some time, this information can describe any ongoing disease the driver may suffer from [65]. Collected location data can track a vehicle even when the vehicle is not sharing its location information. With the recording of a given vehicle's most visited places, it is possible to predict where the user will be on a specific day and time by employing machine learning techniques on available big data [65].

In smart home applications, where the application is permitted to collect the occupant's events, this application can learn behavioural patterns in various ways that are not readily noticeable [55]. Research has suggested [66], [67] using trusted remote data stores and a broker for access control to centralized storage and a combination of different cryptographic techniques to preserve privacy leakages in the application layer.

C. THREATS IN THE POST-QUANTUM ERA

Many current solutions providing information security and user privacy use asymmetric cryptographic schemes based on the integer factorization problem, the discrete logarithm problem, and other versions of these security problems. In the post-quantum era, Quantum Computer (QC)-based attacks can jeopardize these security assumptions.

The quantum computer-based threats can be divided as follows:

- **QC-based threat using Shor's algorithm**: The Shor's algorithm running on a functional quantum computer with a sufficient number of qubits can solve the current security assumptions of **asymmetric cryptosystems** (i.e. discrete logarithm problem and factorization problem, and other versions of these problems). For example, Shor's algorithm running on functional QC needs about 4000 logical qubits to break 2048-bit RSA keys [68]. To be noted, current quantum computers (QCs) can run Shor's algorithm and already have about tens of logical qubits and physical qubits. To prevent Shor's algorithm's attack, vulnerable asymmetric cryptography schemes should be substituted by PQC schemes.

- **QC-based threat using Grover's algorithm**: Grover's algorithm [69] streamlines the collision or symmetric key brute force search on $\mathcal{O}(\sqrt{N})$, where N is the domain size of the function. This threat mainly jeopardizes **symmetric cryptography with short parameters**, i.e., ciphers with short key sizes, hash functions producing short hashes, and MAC functions with short parameters. To prevent the attack by Grover's algorithm, symmetric cryptographic schemes should increase the sizes of keys and other essential parameters.

Future quantum computers may retroactively affect current ICT systems and the security and privacy of their users. These threats are crucial, especially from long-term security and privacy perspectives, and therefore, they should be averted, already nowadays, by the deployment of PQC solutions.

- *Long term secure digital signatures*: To prevent threats, Post-quantum (PQ) secure digital signatures should be employed. Current documents digitally signed with conventional cryptographic algorithms, such as RSA, ECDSA, etc., will be considered un-trusted in the post-quantum era. In the context of electronic documents, it causes signing information about signed documents to come into question. It can significantly impact the authenticity of the current official and legislative documents, contracts, certificates, etc.
- *Long term data security*: To prevent threats, the PQ secure encryption algorithms should be employed. Long-term data security can be required by legislation and national or international law. In some countries, like Germany, it is stipulated that medical and legal data must remain confidential from third parties even after a patient or client's death. It can cause a problem to some confidential data archives that usually lifetimes longer than the time it takes for new computing paradigms to threaten conventional cryptographic algorithms.

D. CONCLUDING REMARKS

In summary, security threats, privacy leakages, and attacks exist at different IoT/II layers, including perception, network, and application layers. This will remain the case in the post-quantum systems as well. Thus, to mitigate these threats, the countermeasures, in terms of the PQC solutions, will have to be developed and implemented at the IoT/II's different layers.

IV. PRIVACY-ENHANCING TECHNOLOGIES

This section presents our analysis of privacy-enhancing technologies and their readiness as well as suitability for IoT/IIs. We mainly focus on PETs that can be implemented in end-devices, used as applications (user-side), and applied in networks, data storage, cloud, and/or backend servers. PETs often provide some or all of the following basic privacy features: anonymity, data privacy, pseudonymity, unlinkability, and untraceability. Also, PETs usually combine privacy features with common security features as accountability, authentication, availability, data confidentiality, data authenticity, data integrity, non-repudiation, and revocation. PETs and security technologies are usually combined to reach most of the above privacy and security features.

TABLE 5
CATEGORIES OF PRIVACY-ENHANCING (PE) TECHNOLOGIES

Privacy-Enhancing (PE) category	Technology name
PE digital signatures	Blind signatures Group signatures Ring signatures
PE user authentication	Attribute-based credentials Anonymous and pseudonymous entity authentication
PE communication systems	Mix-networks and proxies Privacy-preserving techniques for wireless access network Onion routing
PE encryption technologies	Attribute-based encryption Homomorphic encryption Searchable encryption
PE computations and data storing	Secure multi-party computations Data splitting
General anonymization technologies	Statistical disclosure control Differential privacy algorithms

Fig. 2 shows the indicative positions of PETs in the IoT/II environment and potential privacy breaches that are marked with eye icons. The human interaction with proximity and vicinity IoT smart things (sensors, interfaces) may lead to several privacy threats and leakages that have to be mitigated. Hence, only the appropriate combination of PETs with various properties can protect privacy in more complex systems such as Intelligent Infrastructures. Furthermore, Table 5 presents the essential PETs grouped into 6 categories. The following subsections then introduce these PETs, their basic principles, and examples. Note that the provided examples are limited and do not cover all privacy-preserving schemes.

PETs have been studied in many research papers and have reached different maturity levels in different applicable fields. Fig. 3 presents the number of papers indexed in Scopus for each PET and their ratio. Data was taken from January 2021, according to the following query syntax example on Scopus for searchable encryption:

```
TITLE-ABS-KEY ("searchable encryption") AND ( LIMIT-TO
( SUBJAREA , "COMP" ) OR LIMIT-TO ( SUBJAREA , "ENGI" ) OR
LIMIT-TO ( SUBJAREA , "MATH" ) ).
```

Using similar query syntax, we have obtained results for each PET. Some papers and surveys may focus on several PETs simultaneously or only mention some concrete PETs in their abstract without detailed elaboration. The results indicate that Homomorphic Encryption appeared in 4012 results and is currently the most popular PET.

A. PRIVACY-ENHANCING DIGITAL SIGNATURES

1) Group Signatures

A Group signature (GS) is a digital signature providing group-based authentication. GS provides privacy for signers

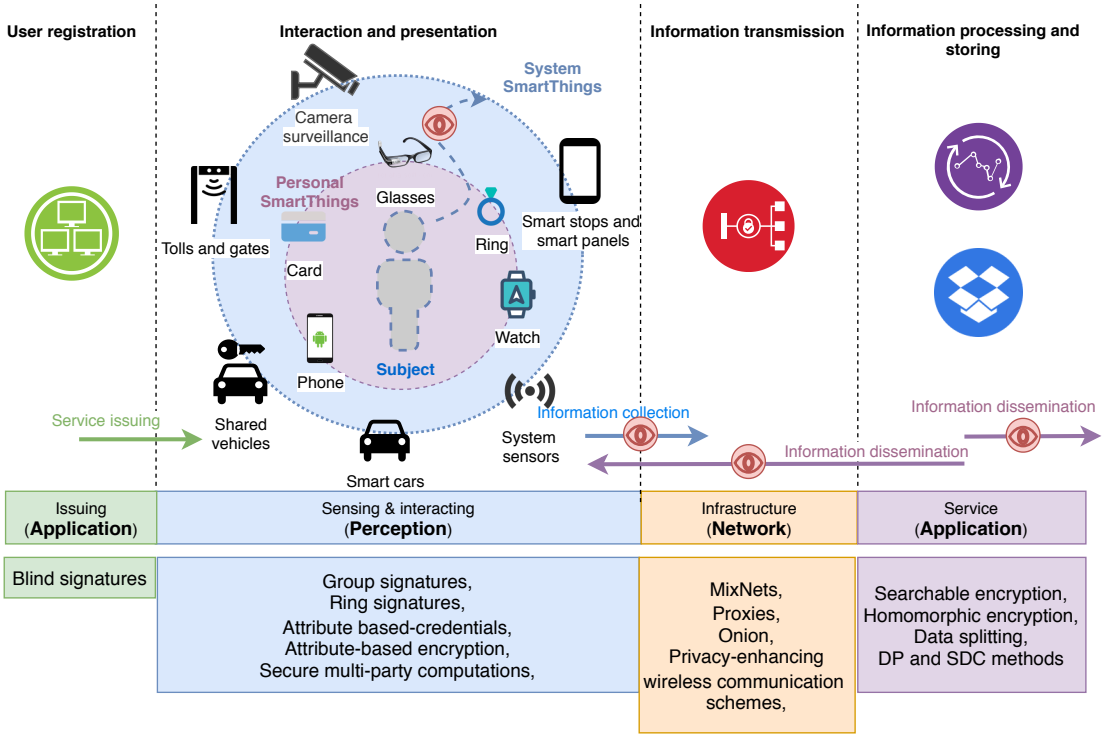


FIGURE 2. The position of PETs in the IoT/II environment

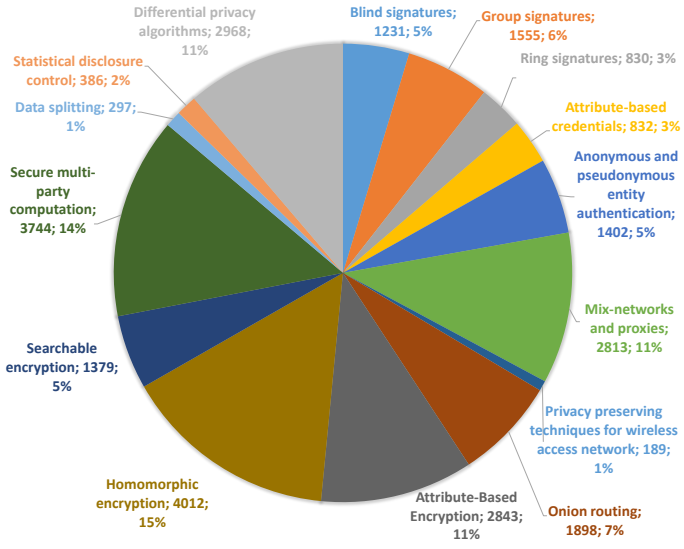


FIGURE 3. The ratio of privacy-enhancing technologies on Scopus (in numbers of documents)

against verifiers. GS schemes allow any group member (a user) to sign a message on behalf of the group anonymously. Users can also authenticate themselves on behalf of the group without using standard digital certificates (used in current public key infrastructures (PKI)) or user identities. The basic principle of group signatures is depicted in Fig. 4. The signature on the message is created by using a group member's secret key. The signed message is verified by a verifier who, using one group public key that is spread in the group of users.

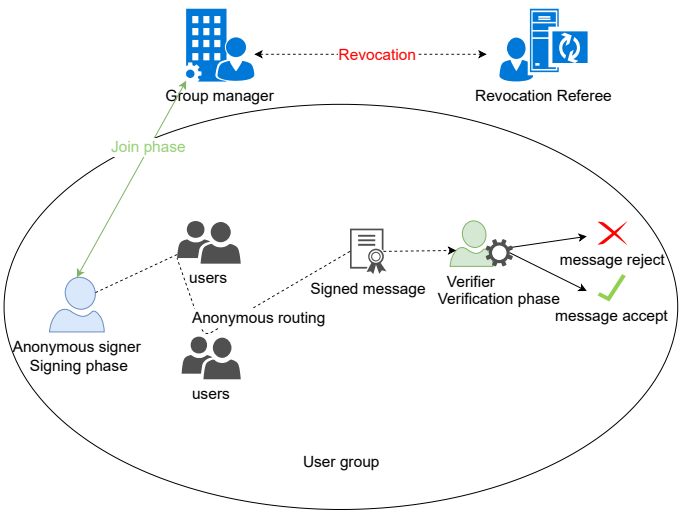


FIGURE 4. The basic principle of GS schemes

There are many variants of GS schemes which provide slightly different features. In general, GS can be used as a basic layer/cryptographic primitive in privacy-preserving ICT services, mainly for proving membership in a group and/or within signing data on behalf of the group. Moreover, several GS schemes have been included in the standard ISO/IEC 20008-2:2013 [70] and several public libraries

containing GS schemes have been released in public repositories. There are many well-established GS schemes, e.g., [71]–[77]. Several schemes have been proposed with a focus on the application to resource-constrained devices such as IoT, e.g. [78]–[82].

2) Ring Signatures

A ring signature (RS) is a digital signature providing group-based authentication to protect users' privacy against verifiers. Any user (member) of a group (ring) can sign a message on behalf of a group (ring). Fig. 5 illustrates the basic principle of RS. The user signs a message with his/her private key (SK_S), and then he/she publishes a set of public keys merged with his/her public key, i.e., multiple public keys (PK_1,PK_S...PK_N). RS schemes are similar to GS schemes, and some studies call them ad-hoc group signatures. Nevertheless, RS schemes remove the central point of a group manager, and RS does not need a centralized initial setup (i.e. a join phase between a user and a manager). Users easily adhere to ring signatures by using prescribed cryptographic parameters and create non-closed groups. RS schemes usually provide perfect privacy (untraceability) because no authority can revoke the anonymity of signers.

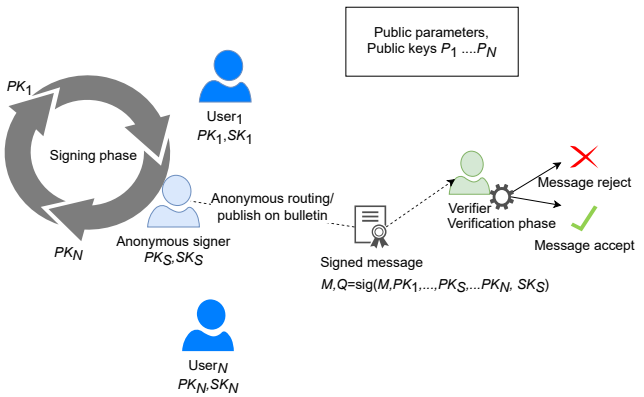


FIGURE 5. The basic principle of RS schemes

In general, RS can be used as a basic layer/cryptographic primitive in ICT services with strong privacy-preserving requirements, e.g. e-voting and e-cash. There are several well-established RS schemes, such as [83]–[85]. Nowadays, RS is employed in several cryptocurrencies and altcoins such as Monero, CryptoNote, TokenPay, etc. Nevertheless, RS produces sized signatures by adding multiple public keys and requires several expensive asymmetric cryptographic operations depending on the ring size. Overall, RS offer stronger privacy features than group signatures with a manager. Still, the performance of phases and the RS size are more challenging for memory, bandwidth, and computational resources than using GS schemes. Therefore, RS schemes are more appropriate for desktop applications and web services that run on non-constrained nodes. Several papers focusing on the implementation of RS in IoT have been published recently, e.g. [86]–[91].

3) Blind Signatures

Blind signatures (BS) are a form of digital signatures that hide (blind) the content of a message to signers. However, the resulting blind signature can be publicly verifiable against the original (un-blinded) message in the manner of a standard digital signature. The technology is used especially in privacy-enhanced protocols where the message owner and signer are different entities. Blind signatures are often used in other cryptographic constructions such as group signatures, anonymous credentials, and use cases such as e-cash schemes and e-voting systems. The general construction of BS is usually based on standard digital signature algorithms such as RSA, Schnorr, or DSA algorithms. The basic principle of blind signatures is depicted in Fig. 6.

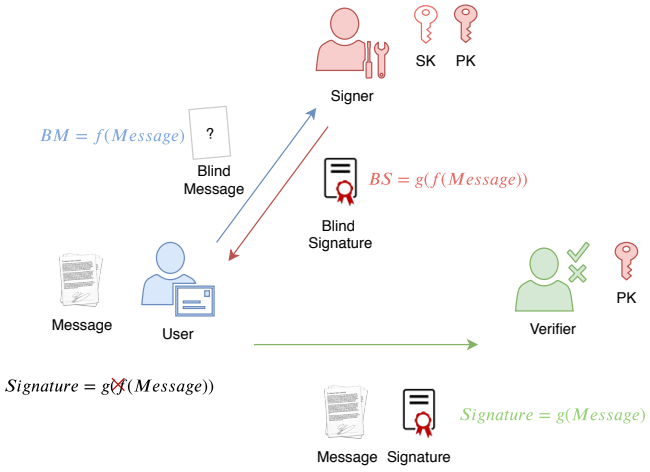


FIGURE 6. The basic principle of BS schemes

Many BS schemes, for example as in [92]–[95], are based on standard signature schemes and are widely applied in many security systems. These standard digital signatures have hardware support also on many constrained IoT devices such as smart cards. BS is mostly used in payment systems such as PayCash. Officially there is no standard which deals with BS. However, BS is based on standard digital signatures; hence we can consider their standardization. The main goal of the current proposals is to build efficient and quantum-resistant schemes.

B. PRIVACY-ENHANCING USER AUTHENTICATION

1) Attribute-Based Credentials

Attribute-Based Credential (ABC), sometimes called **anonymous credential** or **private certificate**, is a core technology used in privacy-friendly authentication systems. The authentication is based on personal characteristics instead of user identity (i.e. full name, unique identifier, digital certificate X.509), widely used in current systems. In

the ABC context, digital identity is considered to be a set of characteristics (personal attributes) that describe a certain person, e.g., age, citizenship, gender, etc. The attributes are grouped into credentials (cryptographic containers) and can be shown selectively, anonymously, and without anyone's ability to trace or link the showing transactions.

A user can select only a subset of the attributes included in the credential to be disclosed (shown) while others remain hidden. Furthermore, each showing transaction is randomized, i.e. all proofs are anonymous and mutually unlinkable. This approach prevents the verifier from impersonating users and/or stealing their identity, profiling users, or tracking their movement and behaviour. An example of the ABC authentication approach is depicted in Figure 7 where the User shows his name and nationality and proves these attributes using her secret key and signed credential list. Verifiers 1 and 2 only check disclosed attributes (name and nationality).

Many research articles focused on ABC technology have been published, e.g., [96]–[101]. ABC can be considered mature and ready to use in current ICT systems. There is already a running IRMA (I Reveal My Attributes) pilot project with the IRMA card and mobile application products for privacy-friendly authentication. Furthermore, current ABC schemes are efficient enough to run, even on IoT devices. For example, the article [102] presents an anonymous scheme that runs the shown protocol in less than 500 ms (in the case of 3 stored attributes) on current smart cards. The necessity of this technology in authentication/identification systems has also been demanded by the U.S. and E.U. institutions. The main known drawback of the technology remains revocation, which has been solved in recent years, for example, in the article [103].

2) Anonymous and Pseudonymous Entity Authentication

Anonymous Authentication (AA) preserves user privacy. In an AA system, a user can access a service without disclosing his/her identifier. This method prevents a verifier from tracking and profiling them. However, the verifier can still reliably determine whenever the user is authentic or not. The authenticated user only provides proof of knowledge of the secret for some chosen claims, e.g. a user belongs to the group with specific privileges. The basic principle of anonymous and pseudonymous entity authentication mechanisms is depicted in Figure 8. A user sends proof parameters as the response to the challenge message from a verifier. Basic AA systems are based on zero-knowledge proof (ZKP) protocols as in [104]. More advanced schemes enable trusted third parties (TTP), called openers, to open the proofs and learn the user's identity. The TTP can disclose user identity, revoke session unlinkability, or revoke a user from a given system. If such TTP exists, the system is called partially anonymous or partially unlinkable, see ISO/IEC 29191:2012 [105]. Most of the current AA and PA schemes are formed by group signatures (ISO/IEC 20009-2 [106]), blind signatures (ISO/IEC 20009-3 [107]) or identity escrow schemes, see [108] for more details. AA or PA can be applied in a range of applications and use cases including electronic voting, electronic identities, social networks, or mobile payments.

C. PRIVACY-ENHANCING COMMUNICATION SYSTEMS

1) Mix-networks and Proxies

Mix networks (Mixnets) represent a basic privacy technology used for privacy-preserving communication via public networks, the most common being the Internet. Mixnets enable users to create an anonymous communication network that is protected against traffic analysis. Users (senders) can communicate with destinations without revealing their identity or location. Mixnets usually employ mix nodes (proxy servers, mixes, relays) that gather messages from multiple transmitters to disrupt the relation between incoming and outgoing traffic. Messages are collected (up to threshold - batch), mixed (reordered), and resent (flushed) with a certain delay from a mix node to the next node (a mix, a recipient). The basic principle of mix networks is depicted in Figure 9 (E denotes an encryption function using various public keys). Some schemes add dummy messages to make tracing more difficult. Mixnets can use a simple one-tier architecture (one proxy) or a multi-tiered architecture (a proxy chain). Using only one central proxy server could be weak against various attacks (denial of service, local eavesdroppers, the central node's maliciousness, compulsion). Therefore, robust Mixnets protocols and schemes usually employ more servers in a chain (a cascade) or multi-path typologies. Equal size messages with the address of an addressee (or a bulletin) are usually encrypted by public-key cryptography (e.g., public keys of proxy servers). Mixnets protocols usually employ re-randomizable encryption schemes such as the ElGamal encryption scheme.

In general, Mixnets, e.g. [109]–[113], provide anonymous communication, which could be used as a basic primitive for many use cases, e.g. anonymous email services, web browsing, message exchange, and e-voting. Nowadays, Mixnets are offered to users via several open-source tools and web projects. Mixnets support user privacy but at the price of some service delays and are based on the strong assumption that mixes nodes/servers and service providers are trusted, hurting privacy.

Mixnets technology has been studied primarily for classic networks. Nevertheless, only a few papers focus on implementing Mixnets solutions on constrained devices (and IoT/IIs), e.g., [114], [115]. For example, Chaum *et al*. [114] presented cMix: Mixing with minimal real-time asymmetric cryptographic operations. The cMix protocol uses a pre-computation to eliminate all expensive real-time public-key operations at the senders, recipients, and mixnodes. The real-time phase needs only a few fast modular multiplications. cMix is considered to be the first mixing suitable for low latency chat for lightweight devices.

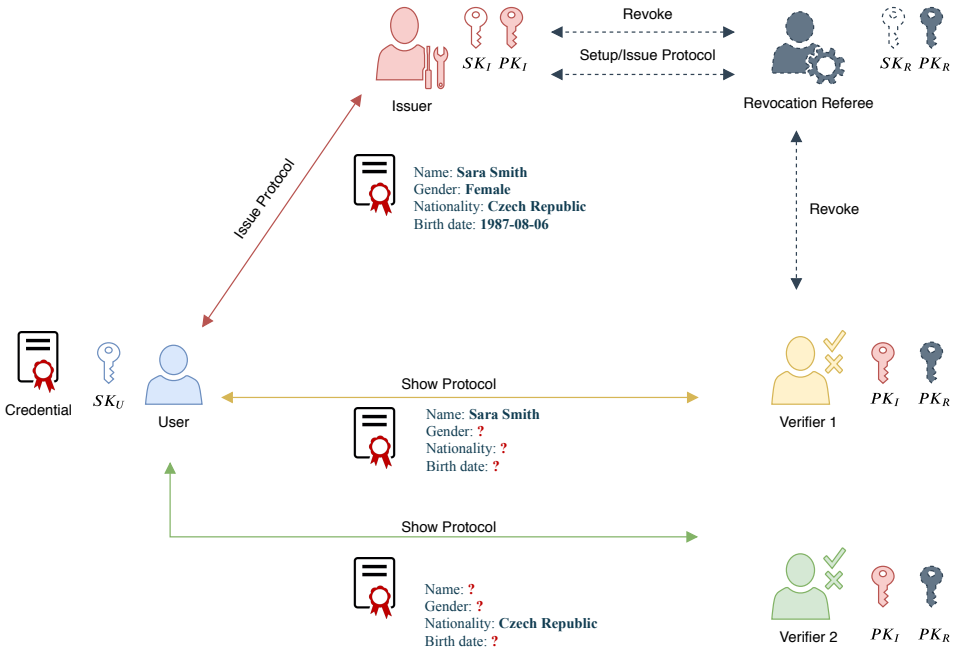


FIGURE 7. The basic principle of ABC schemes

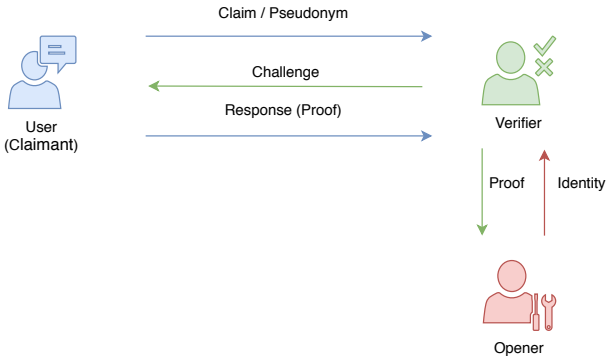


FIGURE 8. The basic principle of anonymous and pseudonymous schemes

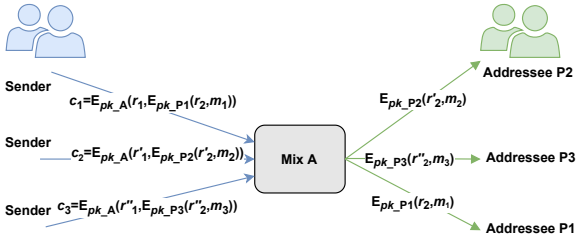


FIGURE 9. The basic principle of mix networks

path called an onion router. The sender encapsulates the data in several layers of encryption, analogous to onion layers. Each onion router decrypts its onion layer and relays data to the next onion router. When the final layer is decrypted, the data reaches the destination (e.g. webserver). The basic principle of onion encryption in onion routing is depicted in Figure 10. In this example, 3 routers create 3 encryption layers between them and the sender who communicates with a web server.

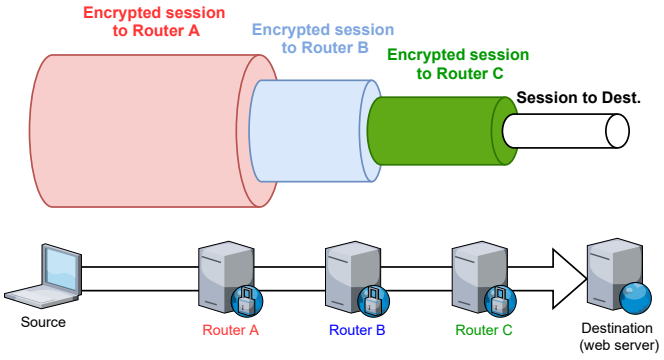


FIGURE 10. The basic principle of onion encryption in onion routing

2) Onion Routing

Onion routing is an anonymous communication technique used in computer networks. Onion networks employ an onion encryption approach where a sender establishes a single encryption layer with each network node along the

Onion routing was developed in the mid-1990s at the U.S. Naval Research Laboratory by employees Syverson, Reed, and Goldschlag. Their papers [116], [117] describe anonymous connections and their implementation using onion routing. These papers also describe several application proxies for onion routing and configurations of onion

routing networks. The most mature project is ToR (the onion router). ToR [118] is based on a circuit-based low-latency anonymous communication service and onion routing. More information is available on the ToR website[5].

There are also Other applications and projects the employ the onion routing principle or are inspired by ToR. Works such as [119], [120] deal with the deployment of DTLS (Datagram Transport Layer Security) in onion routing and its efficiency. The paper [120] employs DTLS to tailor onion routing to IoT and presents the practical evaluation of the tailored solution in IoT.

3) Privacy-Enhancing Communication Systems for Wireless Access Network

Data transferred over wireless access networks are usually encrypted, e.g., by WPA in IEEE 802.11 Wi-Fi networks. Nonetheless, the management frames (headers and data) are not protected and can be exposed to eavesdroppers, which can cause serious privacy issues. Moreover, the current massive adoption of portable devices and wireless networks may raise those privacy and security threats. Historically, two types of problems have been identified [121]–[124]: The first problem concerns the scan for nearby Wi-Fi access points actively sending probe requests. The probe requests may include the name (SSID) of the network used in the previous connections. Those SSIDs emitted by devices may reveal a lot of personal data, e.g., travel history and identity. Based on these data, the eavesdroppers can infer social links between users. Furthermore, 802.11 frames use device's MAC address that are globally unique identifiers tied to devices. Using such identifiers, one can detect the presence of people and trace them.

The use of wireless access technologies, e.g. Wi-Fi, BlueTooth, in mobile equipment raises privacy concerns. Several research works, namely [122]–[124] have identified the feasibility of tracking wireless access network devices. Research has demonstrated these technologies are the source of several privacy leaks. Informed of such problems, manufacturers and standards developing organizations have improved their practices (e.g., disabling SSID disclosure in Wi-Fi access point active search mechanisms) and have designed privacy extensions, particularly using randomized MAC addresses during several modes of operation. However, research has shown that this is not sufficient to prevent privacy risks fully (e.g., re-identifying equipment that uses MAC address randomization is often possible). In conclusion, if PETs exist in wireless access networks, a lot remains to be done to reduce privacy risks. The main complexity lies in the implementation and usage details.

D. PRIVACY-ENHANCING ENCRYPTION TECHNOLOGIES

1) Homomorphic Encryption

Homomorphic encryption (HE) is a special form of encryption technique providing data security. In contrast to standard encryption methods, HE allows an evaluator (third party) to apply specific functions (computations) on encrypted data. However, both data and results remain encrypted and inaccessible to the evaluator throughout the whole process. Only the data owner, who holds a decryption key (i.e., a secret key), can access data and reveal the result through ciphertext decryption. Similar to traditional encryption, HE also offers symmetric and asymmetric scheme variants. Furthermore, HE can be of three main types, *partially homomorphic encryption* (PHE), which supports only addition or multiplication operation [125], [126], [127]; *somewhat homomorphic encryption* (SHE), which supports a limited number of homomorphic operations [128], [129]; and *fully homomorphic encryption* (FHE), which supports an unbounded number of homomorphic operations [130], [131].

The applications of HE are common in privacy-friendly outsourced computations in a cloud. The basic principle of homomorphic encryption in the context of the cloud is depicted in Figure 11, where a Data Owner encrypts plaintext data using a key PK and uploads the ciphertexts to the Evaluator (i.e., cloud) to perform a specific function, say $f()$. The Evaluator then performs homomorphic operations over the ciphertext, and the final result can be recovered from the ciphertext after decryption using the key SK.

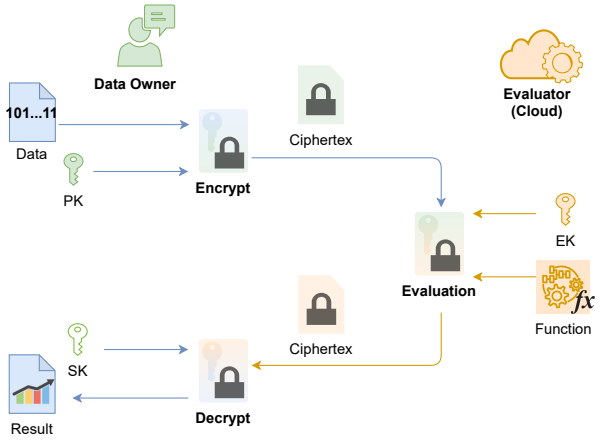


FIGURE 11. The basic principle of HE schemes

FHE technology has gained considerable interest from the research community in the last decade. This increase is caused mostly by the growth of cloud services and outsourced computations. HE can be used wherever the computations on encrypted data are required. Nowadays, there is no official standardization of this technology. The pioneer standardization document is the document [132] created by the consortium of international industries, government, and academic sectors. Furthermore, several

[5]https://www.torproject.org/

public FHE libraries have been released in public repositories. We did not find any papers which deal with FHE on IoT/II devices since the technology is too complex to be implemented on constrained devices. The main goal of current proposals is to reduce the schemes' complexity to a minimum and make them as fast as possible.

2) Searchable Encryption

Searchable Encryption (SE) is used to perform keyword search operations over encrypted data. SE enables the users or data owners to delegate search capabilities using some keywords over encrypted data to an untrusted service provider without disclosing any sensitive information about the searched keywords and the actual plaintext data [133]. In SE, the data owner generates an index of keywords associated with a data file and encrypts the data file and the index before storing it into storage servers, which are maintained by a service provider. Whenever a user wants to retrieve the ciphertexts, the user generates a search query in the form of a trapdoor using a key and the desired keywords and sends that trapdoor to the service provider. Afterward, the service provider performs a search operation over the encrypted indexes using the trapdoor and returns the data files associated with the indexes if the keyword associated with the trapdoor matches with the keywords associated with the indexes.

SE is divided into two categories: *Searchable Symmetric Encryption* (SSE) [134], [135], based on symmetric-key cryptography, and *Searchable Asymmetric Encryption* (SAE) [136]–[138], which is based on public-key cryptography. Several SE-based keyword search schemes have been proposed for IoT/IIs to achieve various functionalities such as dynamic data collection [139], forward privacy [140], file-centric keyword search [141], multi-recipient keyword search [142], and so on.

3) Attribute-Based Encryption

Attribute-Based Encryption (ABE) is a public-key encryption technique. ABE uses attributes to encrypt data, and any user can decrypt the data using a decryption key if the user possesses a certain set of matching attributes with the encrypted data. First introduced in [143], ABE has two main variants, namely, *Key-Policy ABE* (KP-ABE) [144] and *Ciphertext-Policy ABE* (CP-ABE) [145]. The KP-ABE technique uses attributes to encrypt data and access policy, that are defined over some attributes, to generate decryption key. A user can decrypt any encrypted data if and only if the attributes associated with the encrypted data satisfy the access policy of the decryption key. Figure 12 shows the basic principles of KP-ABE, where a data owner encrypts plaintext message `M` using the attribute set `S`. Users such as user 1 and user 2 can decrypt the ciphertext `CT`, as their access policies $\texttt{AP}_1$ and $\texttt{AP}_2$ associated with their respective decryption keys are satisfied by the attribute set `S`; while user 3 cannot. The CP-ABE technique is the reverse of the KP-ABE technique. It encrypts data using access policy and attributes to generate decryption keys. Any user having a decryption key that satisfies the access policy can decrypt. The basic principle of CP-ABE is shown in Figure 13.

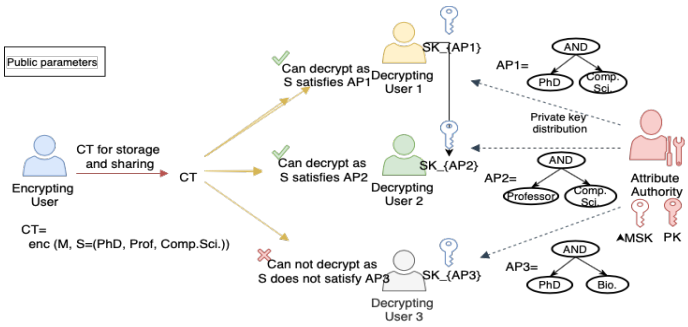


FIGURE 12. The basic principle of KP-ABE schemes

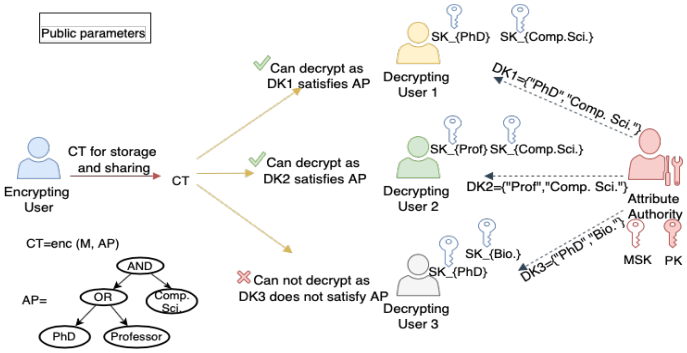


FIGURE 13. The basic principle of CP-ABE schemes

ABE has been used in various environments, such as cloud computing [146], [147], mobile cloud computing [148], [149] and other prominent ways. Some of the challenges in ABE in context to IoT/II environments are privilege revocation [150], Key-Escrow problem [151], requirement of expensive cryptographic operations such as pairing, elliptic curve multiplication, and exponentiation operations. Recently several works such as [152], [153], [154] have been proposed to address the challenges in ABE for IoT/II environments.

E. PRIVACY-ENHANCING COMPUTATIONS AND DATA STORING

1) Secure Multi-party Computations

Secure Multi-party Computation (SMC) is a cryptographic problem in which n parties collaborate to compute a common value with their private information without disclosing it to others [155]. In 1982, Yao presented the first example of SMC [156], which is referred to as the millionaire problem. Suppose Alice and Bob are two millionaires willing to know who has more wealth than the other. SMC enables them to identify which of them is richer without revealing their actual wealth. Formally, SMC is defined as follows: for a number of parties $P_1, P_2 \ldots P_n$ each having initial secret input $x_1, x_2, \ldots x_n$,

SMC securely computes function f using the secret inputs, where $f(x_1, x_2, \ldots x_n) = (y_1, y_2, \ldots y_n)$. Each party P_i only receives the output y_i. During the computation process, no party discloses its secret input to anyone. The process can be illustrated in Fig. 14. User A, User B, and User C are the three parties wishing to compute a common value S using their secret information X_1, X_2, and X_3 respectively. Each user first divides its secret into three components. For example, User A divides its secret X_1 as follows: $X_1 = X_{1,A} + X_{1,B} + X_{1,C}$. Each user sends a share of its secret (message (1) shown in Figure 14) and intermediate values (message (2) shown in Figure 14) to the other users. Finally, each user can compute a common value of $S = X_1 + X_2 + X_3$ without knowing the other users' actual secrets.

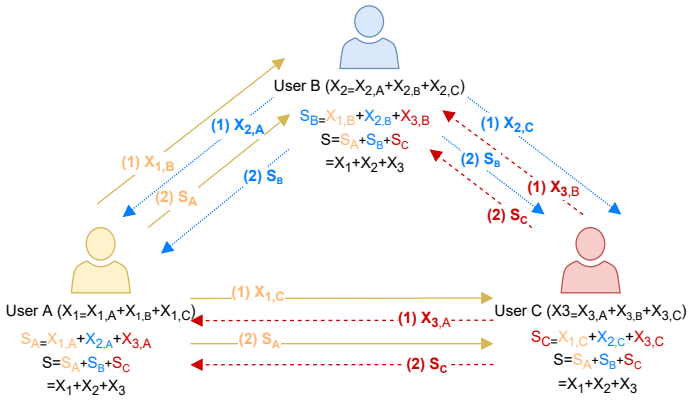


FIGURE 14. A sample illustration of SMC

Currently, SMC schemes such as [157]–[159] can be considered pioneering and well established. SMC can be suitable for various IoT/II use cases where privacy-preserving computation is needed, e.g., smart metering, voting, auctions, etc. Many works have been published in recent years to use SMC in practical applications in IoT/IIs [160], [161]. We observe that there is still much work to do to reduce computation and communication overhead for wider SMC use.

2) Data Splitting

Data splitting (DS), data partitioning, or fragmentation means dividing an original sensitive data set into fragments and storing each fragment in a different site in such a way that the fragment in any site considered in isolation is no longer sensitive. Data splitting is used mainly in privacy-friendly cloud computation services to outsource user-sensitive data as an alternative to fully homomorphic encryption, which is currently considered computationally inefficient. Queries on split data can often be answered much more efficiently than queries on encrypted data. In data splitting, the most challenging step is to efficiently compute the fragmented data when the computations involve more than one fragment. Specifically, challenging tasks in computing on split/distributed data are data mining and data correlation.

Currently, various DS schemes are using different methods and processing different types of data, such as numerical (data being only numerical values), categorical (data being represented with string values) or files, e.g., Li *et al.* [162], Yang *et al.* [163], Domingo *et al.* [164].

F. GENERAL ANONYMIZATION TECHNIQUES

There is an increasing demand for microdata to support research and policymaking, often collected from individuals. For service providers, microdata dissemination increases returns on data collection and helps improve data quality and credibility. However, publishing the microdata raises the challenge of ensuring individuals' confidentiality/privacy while making microdata files more accessible. To preserve individuals' privacy and the utility of the data, statistical disclosure control (SDC) methods need to be applied before releasing data. Otherwise, an attacker having access to some released microdata might attempt to identify or find out more information about a particular individual. A disclosure attack (aka. re-identification attack) occurs when the attacker reveals previously unknown information about an individual based on the released data. There are three levels of information disclosure, with degraded seriousness:

- **Identity Disclosure**: In this case, the attacker associates a known individual with a released data record.
- **Attribute Disclosure**: In this case, the attacker determines some new characteristics of an individual based on the information available in the released data. Suppose that a hospital publishes some microdata that shows all female patients aged 60 to 70 have cancer. If the attacker knows that a female patient of age 65 is included in the microdata, it can infer that this patient has cancer.
- **Inferential Disclosure**: In this case, the attacker can determine the value of some attributes of an individual more accurately with the released data than otherwise would have been possible. For example, regarding the previous knowledge that an individual's salary is between 3000 to 6000 euros, the attacker may infer that this individual's salary falls into $[5500, 6000]$ based on the released microdata.

SDC methods have received a lot of attention from academia and organizations that need to deal with microdata data publication. In academia, researchers have been active in examining the limitations and improvements concerning existing notions, e.g. [165]–[167]. Many new notions have been proposed, e.g. the p-sensitive k-anonymity [166].

Differential privacy [168] is a formal mathematical concept for guaranteeing privacy protection when analyzing or releasing statistical data. In the book by Dwork and Roth [169], an example application is illustrated for social science research: to collect statistical information

about embarrassing or illegal behaviour (captured by having a property P), a randomized process can be implemented and produce some randomized responses. After the concept of differential privacy was proposed, SDC methods have received more criticism, because these methods are vulnerable to background knowledge of the attacker while differential privacy methods normally enable the attacker to have unlimited background knowledge. Clifton and Tassa [170] gave a good comparison study to SDC methods and differential privacy. Recently, researchers have attempted to combine these concepts. For example, Li *et al.* [171] showed how to achieve differential privacy and k-anonymity in the same data release. Holohan *et al.* [172] proposed the concept of (k, ϵ)-anonymity. Domingo-Ferrer and Soria-Comas [173] compared the privacy guarantees provided by k-anonymity and ϵ-differential privacy. They also provided a mechanism to approximate the equivalent ϵ parameter of a t-closeness setting and vice-versa.

G. CONCLUDING REMARKS

Privacy breaches are prevalent in many IoT/II systems, causing massive privacy concerns and demanding comprehensive privacy protection solutions. This section overviews 15 PETs divided into 6 privacy-enhancing categories: digital signatures, user authentication, communication systems, encryption technologies, computations and data storing, and general anonymization technologies. The discussed PETs can be applied at different (perception, network, and application) layers of the IoT/II environment to provide adequate protection against potential privacy breaches. However, many of these technologies are based on traditional cryptographic primitives, presenting a critical problem in the post-quantum era.

V. PRIVACY-ENHANCING TECHNOLOGIES IN POST-QUANTUM ERA

This section presents the current state of Post-Quantum Cryptography (PQC) and its deployment in the IoT/II environment. Furthermore, it maps and briefly presents quantum-resistant alternatives for cryptography-based PETs.

A. POST-QUANTUM CRYPTOGRAPHY

Post-quantum Cryptography represents a secure alternative to traditional cryptography. PQC uses hard problems that cannot be efficiently solved by a quantum computer that can employ Shor's and/or Grover's algorithms. PQC mainly deals with quantum-resistant asymmetric cryptography providing secure Key Encapsulation Mechanisms (KEM) and digital signatures. PQC is divided into 6 families:

- **Lattice**-Based Cryptography (LBC) is based on lattice-related computational problems, i.e., the Shortest Vector Problem (SVP) or the Ring Learning With Errors (RLWE) problem. LBC is very flexible and provides public-key encryption, KEM, and digital signatures. Notable examples: the Frodo scheme [174], NTRU [175], New Hope [176], Kyber [177].
- **Multivariate** Cryptography (MVC) is based on systems of multivariate polynomial equations over a finite field $\mathbb{F}$. MVC uses on Hidden Field Equations (HFE) trapdoor functions [178] such as the Unbalanced Oil and Vinegar Cryptosystems (UOV) [179] which provides digital signatures. Other MVC examples are the Rainbow signature scheme [180] and Tame Transformation Signatures [181].
- **Hash**-Based Cryptography (HBC) is based on the security of one-way hash functions. In 1989, Merkle [182] presented the Merkle Signature Scheme (MSS) based on one-time signatures such as the Lamport signature scheme [183] and a binary hash tree (called Merkle tree).
- **Code**-Based Cryptography (CBC) is based on using error-correcting codes for creating one-way functions. CBC schemes are based on the hardness of decoding a message that contains random errors and recovering the code structure. For instance, the McEliece public-key encryption scheme [184] uses binary Goppa codes with high error correction capability grouped in matrices. Further, the Niederreiter cryptosystem [185] as a McEliece variant offers both encryption and signing functionalities. McEliece and its variants usually use large public keys.
- **Isogeny**-Based Cryptography (IBC) is based on supersingular elliptic curve isogenies that protect against quantum adversaries. IBC schemes employ the problem of constructing an isogeny between two supersingular curves with the same number of points. IBC schemes are usually key exchange protocols such as Supersingular Isogeny Diffie-Hellman (SIDH) [186] and Supersingular Isogeny Key Exchange (SIKE) [187].
- **Symmetric** Quantum-Resistant Cryptography (SQRC) is based on current secure symmetric cryptosystems that use doubling the key size to be robust against PQ attack by the Grover algorithm.

Quantum-resistant schemes have been around for more than 40 years (e.g. the McEliece public-key encryption scheme [184]), and, since the first PQC conference in KU Leuven in 2006, PQC schemes have been intensively studied in many papers, e.g., [188]–[191]. Moreover, current advances in quantum computing (e.g. Google's 53-qubit Sycamore processor [192]) makes PQC more and more popular. Recently, several practical projects and implementations have been realized, e.g., notable H2020 projects PQCRYPTO[6] and SAFEcrypto[7] were completed in 2018. Besides, the Open Quantum Safe (OQS) project released an open-source C library for quantum-safe cryptographic algorithms called LIBOQS[8] which offers more than 60 key encapsulation mechanisms and 63

[6] http://pqcrypto.eu.org/
[7] https://www.safecrypto.eu/
[8] https://github.com/open-quantum-safe/liboqs

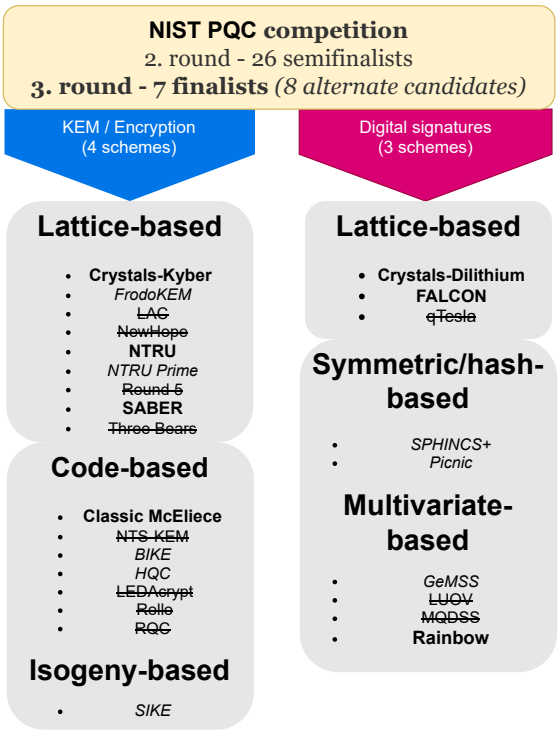


FIGURE 15. PQC NIST competition - 7 finalists chosen from 26 semifinalists

signature schemes. LIBOQS has been recently integrated with OpenSSH and OpenSSL libraries as separated forks.

In 2016, NIST started a process to solicit, evaluate, and standardize PQC schemes. Recently, NIST has announced 7 third-round finalists chosen from 26 second-round candidates (semifinalists), 4 schemes for quantum-resistant KEM (Classic McEliece, CRYSTALS-KYBER, NTRU, SABER) and 3 schemes for quantum-resistant digital signatures (CRYSTALS-DILITHIUM, FALCON, Rainbow) [193]. Furthermore, NIST has chosen 8 alternate candidates for the third round, i.e., FrodoKEM, NTRU Prime, BIKE, HQC, SIKE as KEM schemes, and SPHINCS+, Picnic, GeMSS as signature schemes. The finalists and semifinalists are listed in Figure 15. The final results of the NIST competition (standardization) will be published between 2022 and 2024.

B. POST-QUANTUM CRYPTOGRAPHY IN IOT/IIS

PQC schemes can be easily implemented in current IoT/IT infrastructures, unlike quantum cryptography and quantum key distribution schemes, which require specific and expensive equipment and focus only on the key establishment. PQC schemes are usually more memory and computationally demanding than traditional cryptography solutions. Constrained IoT end nodes, i.e., low-performance-micro-controllers with small memory, may have implementation obstacles even with traditional asymmetric cryptography such as RSA with 2K bits keys.

Nonetheless, optimized and lightweight-designed PQC schemes can be implemented in IoT/II environments. For example, the pqm4 library developed by H2020 PQCRYPTO is a practical library for the ARM Cortex-M4 family of microcontrollers. The library contains several implementations of post-quantum key-encapsulation mechanisms and post-quantum signature schemes and serves as a benchmarking and testing framework for these microcontrollers. Kannwischer *et al.* [194] presented this framework and the results of 15 schemes from the NIST PQC competition.

Many studies deal with the performance assessment of PQC on various platforms from smartcards and constrained devices, e.g., [38], [195]–[198]. For example, Nejatollahi *et al.* in [199] and [28] provided a survey of various software and hardware implementations of lattice-based cryptography schemes. More works focused on implementing PQC schemes on constrained devices and/or in IoT/II services are presented next.

1) Lattice-Based Cryptography in IoT/II

Poppelmann *et al.* [200] compared the implementations of Ring-LWE encryption and the Bimodal Lattice Signature Scheme (BLISS) on an 8-bit Atmel ATxmega128 microcontroller. The implemented Ring-LWE encryption takes 27 ms for encryption, and 6.7 ms for decryption and the implemented BLISS signature takes 329 ms and 88 ms for verification. Saarinen [201] presented the compression technique of Ring-LWE ciphertexts to implement these PQC schemes on constrained devices in IoT/II, Smart Cards, and RFID applications. The ciphertext size can be reduced by more than 40% at the 128-bit security level. Albrecht *et al.* [202] used RSA co-processors on standard smart cards to accelerate lattice-based cryptography. Converted polynomials into big integers can be processed on an RSA co-processor, and obtained results are then converted back to polynomials. Furthermore, more papers focused on implementing concrete schemes, for example, the lattice-based Kyber on Cortex-M4 [203], NewHope on ARM Cortex-M [204], and NTRUEncrypt for 8-bit AVR microcontrollers [205]. Intensive research and implementations prove that lattice-based PQC schemes can be deployed in various constrained devices in IoT/II. Nevertheless, LBC signature schemes require more memory (e.g. Dilithium signature size is 2.701 kB) than classic signatures, e.g. ECDSA signature size is only 64 B.

2) Multivariate Cryptography in IoT/II

Yang *et al.* [206] provided the implementation of enTTS (20,28) working with 20-byte hashes and 28-byte signatures, i.e., the protocol instance has less than 64-bit level of security on a 16-bit MSP430 chip. The signing phase takes 71 ms, and the verification phase about 726 ms. Czypek *et al.* [207] presented C implementations of Unbalanced Oil-Vinegar (UOV), Rainbow and enTTS schemes for embedded devices. They provided benchmark tests on

an 8-bit ATxMega128a1 microcontroller for all schemes with a 128-bit level of security. The implementation of UOV requires about 399 ms for signing and 424 ms for signature verification. The enTTS implementation requires only 66 ms for signing but about 962 ms to verify the signature. The Rainbow scheme provides a time of 257 ms for signing and 288 ms for verifying. Shim *et al.* [208] proposed their own MQ-signature scheme called HiMQ-3. The HiMQ-3 (128-bit security level instance) was run on an 8-bit ATxmega384C3 microprocessor and required about 53 ms for signing and 166 ms for verifying a signature. Moya Riera *et al.* [209] provided a performance analysis of the Rainbow scheme on ARM Cortex-M4. The best results are produced by the optimized Rainbow scheme in the `Ia_Classic` parameter set. The time for signing takes about 0.015 ms and only about 0.013 ms for the verification.

3) **Isogeny**-Based Cryptography in IoT/II

Seo *et al.* [210] presented high-speed implementations of SIDH and SIKE schemes for the 32-bit ARMv7-A processor family. Their full key-exchange execution of SIDHp503 takes about 88 ms on an ARM Cortex-A15 and about 45 ms on an ARM Cortex-A72 (64-bit ARMv8-A). Joppe *et al.* [210] presented an efficient Montgomery reduction algorithm for IBC on 32-bit embedded devices. They provide an implementation of the modular reduction that is 1.5 times faster on ARM Cortex-A8. There are actually several publications that focus on efficient implementation on embedded devices running ARM Cortex-A family, see [211]–[214]. Koppermann *et al.* [215] provided implementations of SIDH, where ephemeral key exchange requires more than 18 sec on a 32-bit Cortex-M4 and more than 11 minutes on a 16-bit MSP430. In 2019, Hwajeong *et al.* [216] introduced the first practical software implementation of SIKE on 32-bit ARM Cortex-M4 microcontrollers. Their key encapsulation of SIKEp434 takes about 1.94 sec and only about 2.73 sec for SIKEp503. Furthermore, the authors also compare their work with the SIDH implementation of Costello *et al.* [212] which is significantly slower. Costello's SIDHp503 implementation running on ARM Cortex-M4 microcontroller required about 28.55 sec in total.

4) **Hash**-Based Cryptography in IoT/II

Rohde *et al.* [217] introduced an implementation of the Merkle signature scheme on an 8-bit smart card microprocessor. Their MSS-128 with H=16 (allowing cca 65k signatures) needs cca 1.2 sec for signing and is more efficient than the RSA-1024 signing operation. The signature size is 2350 B, and the size of the private key is 848 B (RSA needs only 128 B for both parameters). Pereira *et al.* [218] presented Merkle's implementation with the W-OTS scheme, which consumes up to 3000 B (for height H=16) in RAM on the ATmega128l (@7.37 MHz, 4 KB SRAM, 128 KB ROM). The signing phase requires 0.6 sec. Kannwischer *et al.* [194] presented the results of the SPHINCS+ implementation for 36 variants. The measured signing times are from 22 sec to 88 minutes on a 32-bit ARM Cortex-M4 microcontroller (24 MHz). Thus, the SPHINCS+ scheme is not suitable for these constrained platforms.

5) **Code**-Based Cryptography in IoT/II

Strenzke and Falko [219] implemented the McEliece scheme (100-bits security level) on a microcontroller. Nevertheless, the key generation algorithm could not be implemented on the microprocessor for exceeding the card's RAM size. Heyse *et al.* [220] dealt with QC-MDPC McEliece implementations on embedded devices (8-bit AVR microcontroller). They present a compact implementation on the microcontroller using only 4800 and 9600 bits for the public and secret key (80-bits security level). Recently, the paper [221] presents the implementation of code-based BIKE on a Cortex-M4 microcontroller. The implementation employs reduced data representation and adequate decoding algorithms to achieve 6 million cycles for key generation, 7 million cycles for encapsulation, and 89 million cycles for decapsulation for BIKE-1. The upper limit of the presented memory consumption is 66.83 kB (encapsulation) for the BIKE-1 version.

C. QUANTUM-RESISTANT PRIVACY-ENHANCING TECHNOLOGIES

PET schemes are usually based on traditional security assumptions that are not resistant to quantum computing attacks. Nevertheless, there are already several proposals of PETs that are quantum-resistant. In the following, we present pioneer and chosen promising QR-PETs examples.

1) Quantum-Resistant Group Signatures

In 2010, one of the first quantum-resistant group signatures was introduced by Gordon *et al.* [226]. The authors presented a group signature scheme from lattice assumptions. Quantum-resistant group signatures are usually based on lattice-based constructions, but few schemes are using code-based and hash-based constructions. In 2014, Benhamouda *et al.* [227] presented zero-knowledge proofs for lattice encryption and their application to group signatures. This group signature scheme is a "hybrid" because privacy features hold under a lattice-based assumption, and security features are secured under discrete logarithm problem. We note here that it is not a pure lattice-based group signature. In 2015, Nguyen *et al.* [228] introduced a new lattice-based group signature that is probably based on the hardness of the Small Integer Solutions (SIS) and Learning with Errors (LWE) problems in the random oracle model. In 2015, Ezerman *et al.* [229] proposed two provably secure group signature schemes from code-based assumptions, i.e., the hardness of the McEliece problem, the Learning Parity with the Noise problem, and a variant of the Syndrome Decoding problem. The public key (642 kB) and signature size (1.07 MB) are 2,300 times

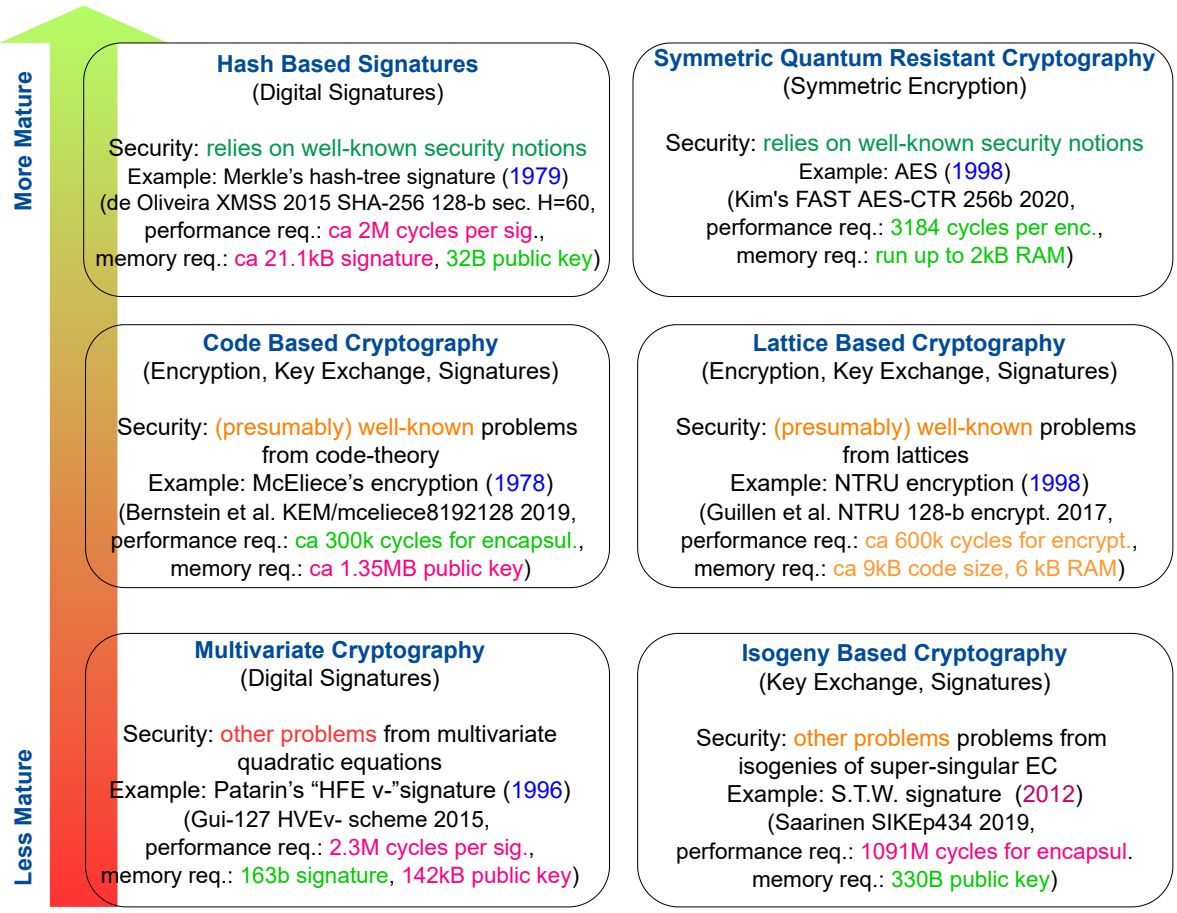


FIGURE 16. Overview of PQC families with examples

TABLE 6
COMPARISON OF CHOSEN QUANTUM-RESISTANT KEM IMPLEMENTATIONS FOR EMBEDDED DEVICES (TIMINGS ARE REPORTED IN TERMS OF CLOCK CYCLES)

Scheme	PQ family	Language	Hardware		Timings (cc $\times 10^6$)		
			MCU	Architecture	KeyGen	Encaps	Decaps
Ring-LWE [222]	LBC	C + ASM	ATxmega128A1 (32 MHz)	8-bit AVR	-	0.671	0.275
NewHope-256bit [204]	LBC	C + ASM	ARM Cortex M0 (32 MHz)	32-bit ARM	1.168	1.738	0.298
NewHope-1024cpa [194]	LBC	ASM	ARM Cortex-M4F (24 MHz)	32-bit ARM	1.034	1.495	0.206
NTRUEnc-256bit [205]	LBC	C + ASM	ATmega1281 (16 MHz)	8-bit AVR	-	1.539	2.103
NTRUEnc-256bit [223]	LBC	C	ARM Cortex M0 (32 MHz)	32-bit ARM	71.186	1.411	2.377
Kyber-1024 [194]	LBC	ASM	ARM Cortex-M4F (24 MHz)	32-bit ARM	1.575	1.779	1.709
Frodo-640AES [194]	LBC	ASM	ARM Cortex-M4F (24 MHz)	32-bit ARM	47.050	45.883	45.366
BIKE-1 [221]	CBC	C	ARM Cortex-M4 (168 MHz)	32-bit ARM	6.437	6.867	89.131
SIKEp751 [216]	IBC	ASM	ARM Cortex-M4 (168 MHz)	32-bit ARM	282	455	491
SIKEp751 [216], [212]	IBC	C	ARM Cortex-M4 (168 MHz)	32-bit ARM	3,651	5,918	6,359
SIDHp751 [216]	IBC	ASM	ARM Cortex-M4 (168 MHz)	32-bit ARM	-	457	520
SIDHp751 [216], [212]	IBC	C	ARM Cortex-M4 (168 MHz)	32-bit ARM	-	5,915	6,763
SIDHp751 [216], [215]	IBC	ASM	ARM Cortex-M4 (168 MHz)	32-bit ARM	-	1,992	2,260

and 540 times smaller than the lattice-based scheme [228] for the group of 256 users. In 2019, Boneh *et al.* dealt with Enhanced Privacy ID signature schemes (group signatures) built only from symmetric primitives, such as hash functions and pseudo-random functions. Their scheme produces the post-quantum signature of size 6.74 MB for groups of size up to 2^{20}.

2) Quantum-Resistant Ring Signatures

The first quantum-resistant ring signature schemes were introduced in 2007 by Zheng, Li, and Chen [230], who proposed the code-based ring signature scheme producing a signature size $144 + 126N$ bits where N is the size of the ring. Furthermore, in 2010, Cayrel *et al.* [231] presented one of the first lattice-based threshold ring

TABLE 7
COMPARISON OF CHOSEN QUANTUM-RESISTANT DIGITAL SIGNATURE IMPLEMENTATIONS FOR EMBEDDED DEVICES (TIMINGS ARE REPORTED IN TERMS OF CLOCK CYCLES)

Scheme	PQ family	Language	Hardware		Timings (cc $\times 10^6$)	
			MCU	Architecture	Sign	Verify
BLISS-I [200]	LBC	C + ASM	ATxmega128A1 (32 MHz)	8-bit AVR	10.537	2.814
BLISS-I [224]	LBC	C + ASM	ARM Cortex-M4F (168 MHz)	32-bit ARM	4.648	0.539
Dilithium-III [224]	LBC	C + ASM	ARM Cortex-M4F (168 MHz)	32-bit ARM	8.348	2.342
FALCON-I [225]	LBC	C	ARM Cortex-M4F (24 MHz)	32-bit ARM	80.503	0.530
qTesla-I [194]	LBC	C	ARM Cortex-M4F (24 MHz)	32-bit ARM	5.830	0.787
Sphincs-sha256-128f [194]	HBC	C	ARM Cortex-M4F (24 MHz)	32-bit ARM	952.977	42.386
UOV [207]	MVC	C	ATxMega128a1 (32 MHz)	8-bit AVR	13.314	14.134
Rainbow [207]	MVC	C	ATxMega128a1 (32 MHz)	8-bit AVR	8.227	9.216
enTTS [207]	MVC	C	ATxMega128a1 (32 MHz)	8-bit AVR	2.142	30.789
HiMQ-3big [208]	MVC	C	ATxmega384C3 (32 MHz)	8-bit AVR	0.959	2.219
HiMQ-3small [208]	MVC	C	ATxmega384C3 (32 MHz)	8-bit AVR	1.247	5.328
Rainbow [207]	MVC	C	ARM Cortex-M4 (16 MHz)	32-bit ARM	2.930	1.321

signature schemes. In 2016, Libert *et al.* [232] introduced zero-knowledge arguments for lattice-based accumulators. They created lattice-based logarithmic-size ring signatures based on the RST scheme [233]. In 2018, Baum *et al.* [234] presented a linkable one-time ring signature scheme constructed from a lattice-based collision-resistant hash function. The signature size is linear with the size of a ring. Besides lattice-based and code-based RS schemes, there are several multivariate-based constructions, e.g. [235], [236]. In 2013, Petzoldt *et al.* [235] introduced a threshold ring identification and signature scheme that is based on the MQ-Problem. The scheme produces signatures of sizes ca 300 or 600 kB. Later in 2017, Mohamed and Petzoldt [236] extended the multivariate-based Rainbow signature scheme to the ring signature scheme and presented a public key reduction technique. The 6.8 kB public key for 50 users can be reduced by 68% to 2.1 kB, and the signature size is ca 31 kB.

3) Quantum-Resistant Blind Signatures

In 2010, the first quantum-resistant blind signature scheme was presented by Rückert [237]. Since this first lattice-based blind signature scheme, quantum-resistant blind signatures have been constructed by using various post-quantum approaches, e.g. multivariate-based [238], code-based [239] or isogeny-based [240]. In 2016, Srinath and Chandrasekaran [240] presented an Undeniable Blind Signature scheme (UBSS) based on isogenies between supersingular elliptic curves. In 2017, Zhu *et al.* [241] designed a round-optimal lattice-based blind signature scheme based on the closest vector problem using infinity norm. The scheme can be appropriate for cloud services. In 2017, Petzoldt *et al.* [238] proposed a generic technique to transform the Rainbow multivariate signature scheme into blind signature schemes. The proposed scheme produces 28.5 kB blind signatures using 70.2 kB private key and 106.8 kB public key for 128-bit security level. Finally, in 2017, Blazy *et al.* [239] proposed a code-based blind signature scheme.

4) Quantum-Resistant Attribute-Based Credentials

ABC schemes are usually based on group signature primitives and/or attribute-based signatures schemes (ABS). Quantum-resistant ABC schemes have been mainly developed from QR GS schemes. In 2012, Camenisch *et al.* [242] presented the lattice-based constructions for anonymous attribute tokens where users use issued attribute-containing credentials that revealing only a subset of their attributes. In 2018, Boschini [243] introduced a lattice-based anonymous attribute token scheme with short zero-knowledge proofs. The size of AA tokens from lattices is 17.77 MB. In 2019, Yang *et al.* [244] presented lattice-based zero-knowledge arguments with standard soundness and the designs of privacy-preserving methods based on lattices.

5) Quantum-Resistant Mixnets

Recently, several Mixnets solutions using post-quantum cryptography primitives have been proposed. Quantum-resistant Mixnets usually substitute public key cryptography used for the key establishment by PQC alternatives. In 2019, Costa *et al.* [245] presented the first proof of a shuffle based on lattice-based cryptography. Their paper showed how to create a universally verifiable Mixnet for mixing votes encrypted by an RLWE encryption scheme. In 2020, Boyen *et al.* [246] introduced a verifiable decryption Mixnet that employs practical lattice-based primitives to identify misbehaving mix servers. The scheme can be used for post-quantum-secure e-voting. The scheme uses hybrid encryption that consists of a lattice-based CCA2-secure public-key KEM and an AES-256; the size of the public key is 93 kB.

6) Quantum-Resistant Homomorphic Encryption

Lattices can provide both additive and multiplicative homomorphisms and serve as an ideal mathematical object to build fully homomorphic encryption (FHE). Hence, there are many lattice-based FHE schemes proposed, e.g., Gentry's FHE scheme [247] was proposed in 2009 as the first proposal of the FHE scheme. The scheme is

based on ideal lattices and is almost bootstrap able. More details are described in Gentry's Ph.D. thesis [248]. In 2014, Brakerski *et al.* [249] presented the FHE scheme based on learning with errors (LWE) problem. They use batching for parallel computations on messages and modulus switching techniques to manage noise. In 2014, Brakerski and Vaikuntanathan [250] presented a levelled FHE scheme based on the (standard) LWE assumption. The scheme generates very short ciphertexts thanks to a new proposal of a dimension-modulus reduction technique. This is the first time where key and modulus switching techniques are introduced. Besides lattice-based HE schemes, In 2011, Bogdanov and Lee [251] proposed homomorphic encryption from codes in 2011. In 2018, Xu *et al.* [252] presented fully homomorphic encryption based on Merkle Tree (FHMT) as a novel technique for streaming authenticated data structures for streaming verifiable computation. In 2018, Chillotti *et al.* [253] described a fast FHE scheme over the torus (TFHE) and revisited, generalized, and enhanced the FHE based on GSW and its ring versions.

7) Quantum-Resistant Searchable Encryption

Many searchable encryption schemes are based on bilinear maps that may not be secure in the post-quantum era. Hence, post-quantum secure variants of SE schemes have been proposed, e.g., in 2012 Zhang *et al.*'s lattice based searchable encryption scheme [254]. In 2016, Yang and Ma [255] described public-key encryption with a semantic keyword search using the LBC construction based on learning with errors (LWE) problem. In 2018, Behnia *et al.* [256] presented lattice-based Public-key Encryption with Keyword Search (PEKS) that uses NTRU.

8) Quantum-Resistant Attribute-Based Encryption

Many ABE schemes are based on a bilinear map over elliptic curves, but these schemes do not provide post-quantum security. Nevertheless, a few ABE schemes based on lattice have been proposed to be quantum-resistant. In 2012, Boyen introduced the first lattice ABE scheme [257] . In 2012 as well, Agrawal *et al.* [258] introduced a fuzzy identity-based encryption (fuzzy IBE) scheme based on lattices among the first realizations of quantum-resistant ABE. In 2014, Zhu *et al.* [259] proposed an efficient ABE scheme based on the learning with errors over rings (R-LWE).

9) Quantum-Resistant Secure Multi-Party Computation

Quantum-resistant secure multi-party computation has been studied in several papers, such as [260]–[262]. QC SMC is usually based on quantum-resistant encryption techniques such as QR homomorphic encryption. For example, the paper [260] proposes a new notion of secure multiparty computation based on FHE from NTRU encryption. Recently, Kim *et al.* [262] focused on round-efficient and secure MPC protocols based on LWE assumptions. The combination of secure multi-party and PQC is still ongoing research.

10) Other PETs

Only cryptography-based PET solutions (named in the previous subsections) have concerns in the post-quantum era and should be promoted as quantum-resistant. Other privacy-enhancing technologies such as privacy-preserving techniques for wireless access networks, proxies, data splitting, statistical disclosure control, differential privacy algorithms, and general anonymization techniques are not based on mathematical hardness assumptions, so these techniques do not have the concerns in the post-quantum era.

D. CONCLUDING REMARKS

In this section, the overview of the 6 PQC families is depicted in Figure 16. The presented examples for each PQC family include the performance and memory requirements taken from recent implementations. The green values indicate potential suitability for implementation on constrained devices. The red parameters indicate potential obstacles in the case of deployment on constrained devices. Tables 6 and 7 show state-of-the-art implementations of PQC schemes on embedded devices using ARM Cortex-M and AVR microcontroller architectures. Timings were gathered from referred papers in the Scheme column in both tables. This comparison indicates that IBC and HBC schemes usually require a significant amount of clock cycles per operation. Furthermore, code-based and hash-based schemes often use large parameters, large public keys, large signatures (e.g. $>$ tens kB). Hence, only a few practical implementations on embedded devices with constrained memory, e.g., BIKE and Sphincs+.

Since 2010, there have been many proposals for quantum-resistant PETs. The most promising PQC family is lattice-based cryptography that is employed in most cryptography-based PETs. Figure 17 depicts the deployment of PQC families in PETs that is mainly based on mapped QR PETs in this survey.

VI. DEPLOYMENT OF PRIVACY-ENHANCING TECHNOLOGIES IN INTELLIGENT INFRASTRUCTURES

This section deals with the practical deployment of PETs in IoT/IIs. Furthermore, the use case and potential usage of PETs in line with IoT/II services are presented.

A. PRACTICAL DEPLOYMENT OF PETS

This section identifies the current state, technology readiness, and the presentation of existing significant pilots, products, and projects. The CORDIS search engine is used for the detection of significant research projects in the EU. Table 8 maps the PETs in current or past research projects. Some PETs are directly implemented as privacy-preserving products and pilots. For example, onion routing is already widely used by privacy-preserving communication applications such as

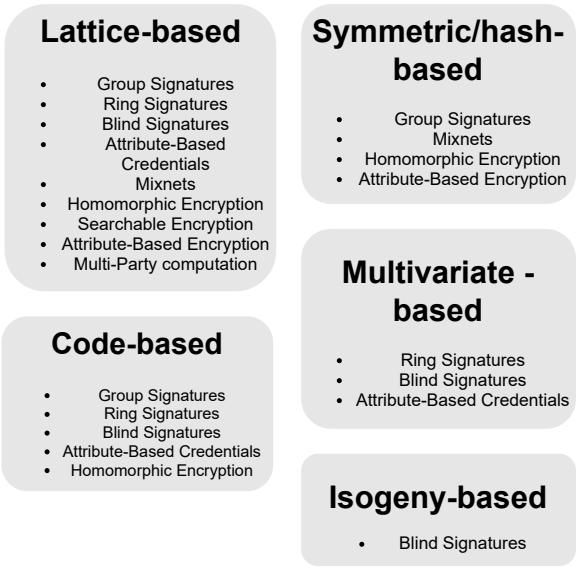


FIGURE 17. Deployment of PQC in PETs

ToR [118], Tribler[9] and Tox[10]. Attribute-Based Credential schemes are implemented in Idemix [263], U-Prove [264], and IRMA[11] systems. Further, ring signatures are practically deployed in several cryptocurrencies, e.g., Monero [91], Cryptonote[12]. On the other hand, some PETs serve mainly for experimental purposes as software libraries, e.g. homomorphic encryption (HElib[13], Microsoft SEAL[14]) or group signatures (group-signature-scheme-eval[15]). The full list of PETs as products and pilots with brief descriptions and links can be found in Tables 10, 11 in the Appendix.

B. USE CASES OF PETS

PETs have various use cases and scenarios that are already used in current ICT or integrated into IoT/II services. The most popular use cases of each privacy-enhancing technology are listed in the following text.

1) Use Cases of Group Signatures

- **Public transport**: if a user has a valid pre-paid ticket, he/she can prove it by signing a challenge from a verifier.
- **Privacy-preserving auctions/tenders**: users as buyers submit bids/tenders (i.e., signed messages by a GS scheme), and if preferred tender or highest bid is selected, then the authority can securely trace a winner [265].
- **Office access**: a user has access to his/her office or lab since he/she is in a group of valid employees (by signing a challenge from a verifier).
- **Club membership**: a user can prove his/her membership in a group of members (by signing a challenge from a verifier).
- **Traffic Control Management on Internet of Vehicles**: a user driving vehicles can anonymously share traffic/car status messages (to road infrastructure/to other vehicles) that are signed by a GS scheme. Malicious users/cars sending bogus messages could be revoked [266].
- **Parking**: a user can enter a city zone and park his/her car since he/she has the membership in the zone (by a signing challenge from a verifier).
- **Privacy-preserving data collection** (e.g., power consumption from smart meters): a system/operator/service can collect signed data from users being members of a group [80]. Malicious users/cars sending bogus messages could be revoked.
- **Privacy-preserving e-voting**: users should be able to cast votes anonymously, where GS signs votes.
- **Privacy-preserving e-cash**: GS are used to protect the privacy of users' transactions signed by GS.

2) Use Cases of Ring Signatures

- **Privacy-preserving auctions/tenders**: users as buyers submit bids/tenders (i.e., signed messages by an RS scheme), and if preferred tender or highest bid is selected, then a winner can prove his/her signed bid by the second signature, thus ensuring support of linkability and claim ability features.
- **Privacy-preserving e-voting**: users should be able to cast votes anonymously where the RS scheme signs votes [267]. All double-votes or multiple-votes can be detected.
- **Privacy-preserving e-cash**: RS schemes protect users' privacy who perform and sign transactions [267]. Double spending can be detected.

3) Use Cases of Blind Signatures

- **Parking**: BS can be used to blind a user's vehicular plate number in parking services.
- **Payment systems**: users can use a payment system without revealing the full banking information about what, where, when, and to whom their funds are transferred [268].
- **e-voting**: BS can be used to guarantee voter's privacy for confidentiality and voter's digital signature for voter's authentication [269].

4) Use Cases of Attribute-Based Credentials

- **Public transport**: a user has a valid ticket and applies for a discount since she is a child/student/senior.
- **Driving/renting/sharing a car**: a user having a valid driving license of category B can rent/drive a car or

[9] https://www.tribler.org/
[10] https://tox.chat/
[11] https://github.com/credentials/irma_card
[12] https://cryptonote.org/
[13] https://github.com/homenc/helib
[14] https://www.microsoft.com/en-us/research/project/homomorphic-encryption/
[15] https://github.com/klapm/group-signature-scheme-eval

TABLE 8
PETs IN RESEARCH PROJECTS

PETs	Project name and/or acronym	Description
Group Signatures	PRISMACLOUD	In this H2020 project, group signatures without encryption have been constructed and integrated into tools providing privacy-preserving cryptography for the cloud. Link: https://prismacloud.eu/.
	PERCY	The FP7 project focused on cryptographic primitives dealt with group signatures based on lattice problems. Link : https://cordis.europa.eu/project/id/321310
	HIPERLATCRYP	The FP7 project also deals with developing a special type of multiuser anonymous digital signatures. Link: https://cordis.europa.eu/project/id/268469
Ring Signatures	PRISMACLOUD	This project partly researched constructing the logarithmic sized ring signatures. Link: https://prismacloud.eu/
	Scalable & Private Voting through Bilinear Pairings	This is a proposal of ZK Labs Research's project (to Aragon Nest) that should enable private and scalable voting and authentication based on Ethereum and ring signatures. Link: https://github.com/aragon/nest/issues/40
Attribute-Based Credential	ABC4Trust	The goal of the ABC4Trust FP7 project is to address the federation and interchangeability of technologies that support trustworthy yet privacy-preserving Attribute-based Credentials (ABC). Link: https://www.abc4trust.eu/
Mix-networks and Proxies	Privacy and Accountability in Networks via Optimized Randomized Mix-nets (PANORAMIX)	This H2020 project focuses on developing a multipurpose infrastructure for privacy-preserving communications based on mix-networks (mix-nets) and its integration into high-value applications exploited by European businesses, such as e-voting. Link: https://panoramix-project.eu/
Homomorphic Encryption	Towards Practical Fully Homomorphic Encryption	Research deals with an investigation on algorithmic optimizations to speed up LWE-based schemes, implementations on CPUs (GPUs), and building an LWE-FHE based homomorphic instruction set. Link: http://vernam.wpi.edu/research/homomorphic-encryption/
	Homomorphic Encryption for Cloud Privacy	The project centers on three modules: instruction set development for homomorphic computing, processor-specific optimizations for homomorphic schemes, and the investigation of new homomorphic schemes. Link: http://vernam.wpi.edu/research/homomorphic-encryption/
	PROgramming Computation on EncryptEd Data (PROCEED)	This U.S. Department of Defense program seeks to make a computation on encrypted data practical. Link: https://www.darpa.mil/program/programming-computation-on-encrypted-data
Searchable Encryption	CloudUTrust - Symmetric Searchable Encryption and Attribute-Based Encryption for cloud security and privacy	The goal of this project is to ensure data confidentiality and privacy in a cloud environment by combining the concepts of Attribute-Based Encryption and symmetric key encryption SE. Link: https://www.ri.se/en?refdom=sics.se
	Practical Searchable Encryption Design through Computation Delegation	This project deals with the research issues of allowing third-party service providers to search in encrypted data. Link: https://www.fnr.lu/projects/practical-searchable-encryption-design-through-computation-delegation/
	Tredisec Trust-aware, REliable and Distributed Information SEcurity in the Cloud	The main goal of this project are to provide data confidentiality, integrity, and availability guarantees in the cloud by leveraging the cryptographic techniques. Link: http://www.tredisec.eu/
Attribute-Based Encryption	Security In trusted SCADA and smart-grids (SCISSOR)	This project aims to design a new generation SCADA security monitoring framework with attribute-based encryption. Link: https://cordis.europa.eu/project/id/644425
	Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare	The project focuses on the security and privacy of sensitive personal data and tries to ensure the users' trust in healthcare services in a cloud environment. Link: https://cordis.europa.eu/project/rcn/219333/factsheet/en
	Secure Computation on Encrypted Data	The project focuses on (i) designing pairing and lattice-based encryption that is more efficient and usable in practice; and (ii) getting a better understanding of expressive functional encryption schemes and pushing the boundaries from encrypting data to encrypting software. Link: https://cordis.europa.eu/project/id/639554
Secure Multi-party Comp.	Better MPC Protocols in Theory and Practice	The project proposes state of the art for SMC protocols. Link: https://cordis.europa.eu/project/id/669255
	Implementing Multi-Party Computation Technology	The project focuses on designing methodologies for coping with the asynchronicity of networks, realistically measuring and modelling SMC protocols performance, and utilizing low round complexity protocols in practice for dealing with large input sizes, etc. Link: https://cordis.europa.eu/project/rcn/204773/factsheet/en
Data Splitting	CLARUS	The CLARUS H2020 project aims to enhance trust in cloud computing by creating a secure framework for storing and processing data outsourced to the cloud. Link: https://cordis.europa.eu/project/id/644024
Differential Privacy	U.S. Census Bureau	Census Bureau with the help of academic researchers is designing a differentially private publication system that can directly address these vulnerabilities while preserving the fitness for the use of the core statistical products. Link: https://www.census.gov/newsroom/blogs/random-samplings/2019/02/census_bureau_adopts.html

ask for a car-sharing service.

- **Office access**: a user can request access to her office or lab as an employee/student/professor [270].
- **Club membership**: a user can prove his membership and valid payment for a membership fee [271].
- **Low emission zones**: a user is authorized to enter a city zone as she is driving a diesel car with the Euro 6 emission standard.
- **Parking**: a user, proving his membership in the parking zone and the valid payment for the parking, is allowed to enter his car into the parking zone.
- **Legal restrictions**: a user can prove that he is older than 18/21 without disclosing his birth date.
- **Electronic identification**: a user holding his/her electronic identity card issued by a competent state institution can prove she is provided with a set of attributes (i.e., age range, EU citizenship, etc.) to any EU officer [272].

5) Use Cases of Mixnets and Onion routing

- **Privacy-preserving high-latency remailer systems**: these systems provide an anonymous e-mail delivery service or message exchange [110].
- **Privacy-preserving low-latency web applications**: these systems are providing anonymous web browsing

[118].

- **Privacy-preserving file exchange**: Mixnets can provide general anonymous communication channels for data and file exchange.
- **e-voting**: Mixnets can be used for constructing a secure electronic voting system by ensuring one bulletin per recipient.

6) Use Cases of Homomorphic Encryption

- **Genomics**: FHE can help human DNA and RNA sequences - two powerful tools in the study of biology, medicine, and human history - to find genome sequences in a privacy-friendly way.
- **Network security**: FHE can help analyze some network traffic of critical infrastructure being outsourced in a cloud to detect anomalies and intrusions while hiding the traffic content.
- **Smart grid networks**: smart building can send encrypted energy consumption data without revealing any information about the true value [273].
- **HealthCare**: HE enables a clinic analysis over sensitive data of patients [274].
- **e-voting**: HE protects voters' privacy during an election event and their decision as well.
- **Payment systems**: HE enables to provide financial services to commercial and retail customers while their profits and expenses remain secret.
- **Search engines**: users can search for information without revealing the true query and the received data to a search engine provider.

7) Use Cases of Searchable Encryption

- **Data Retrieval from untrusted Servers**: Users can retrieve data based on some keywords without disclosing any sensitive information to unintended entities, including the service provider [275].
- **Energy Auction**: Energy sellers can privately inquire about acceptable bids.
- **Secure Email Routing**: Emails can be transmitted to the receiver based on some keywords through some mail gateways without leaking any sensitive information.

8) Use Cases of Attribute-Based Encryption

- **Content-Based Access Control in Cloud**: ABE is suitable for providing fine-grained access control to data in an untrusted cloud storage environment.
- **Privacy-aware Data Retrieval**: ABE can be used to enable the users having resource-constrained devices such as IoT/II for retrieving their desired data from an untrusted service provider without disclosing sensitive information about the actual data.
- **Traffic Control Management on Internet of Vehicles**: ABE can be used to share sensitive traffic information among the drivers or vehicle sensors [153].

TABLE 9
PETs IN USE CASES

PETs/Use case	GS	RS	BS	ABC	Mix / OR	HE	SE	ABE	MPC
Public transport	✓			✓					
Auctions	✓	✓					✓		✓
Access control	✓			✓					
Membership	✓			✓					
IoV communication	✓			✓				✓	
Parking	✓		✓	✓					
e-identification				✓					
e-voting	✓	✓	✓		✓	✓			✓
Payment systems	✓	✓	✓			✓			
Healthcare networks						✓		✓	✓
Smart grid networks	✓					✓			✓
Network security					✓	✓	✓	✓	

9) Use Cases of Secure Multi-Party Computation

- **e-voting**: computing the final result of an election without disclosing any information about the individuals voting details.
- **Electronic Auction**: computing the winning bid without disclosing any information about the other bidders [276].
- **Smart grid networks**: computation over fine-grained smart metering data without revealing any individual's energy consumption to support energy services.
- **HealthCare**: computing statistic analysis on patient data without compromising the patient data privacy [277].

10) Use Cases of Differential Privacy

- **Federated learning**: an organization like Google can leverage differential privacy to learn a machine learning model based on its users' data without collecting the data [278].
- **Database queries**: an organization like Uber can leverage differential privacy to grant SQL queries to its database (which contains data collected from its customers) without worrying about privacy breaches [279].

C. CONCLUDING REMARKS

Table 9 summarizes the practical deployment of PETs in various use cases based on the current state-of-the-art. We developed Table 9 from analyzed use cases and references presented above. The basic cryptographic primitives applied in most use cases are group signatures. Furthermore, in the analyzed references, ABC and HE approaches are also widely used. We note here that the discussed PETs may apply to more use cases than listed as its function within a particular use case can be employed within other use-cases.

VII. SELECTED CASE STUDY OF PRIVACY-ENHANCING TECHNOLOGIES

To demonstrate how PETs can improve security and privacy in practical scenarios, we focus on a Privacy-Enhancing Vehicle Parking Service (PE-VPS), a part of the Internet of Vehicles (IoV) environment.

A. PRIVACY-PRESERVING VEHICLE PARKING SERVICE

Let us consider a case where a given user wants to park his/her vehicle in the parking terminal lot. Firstly, he/she needs to register with the parking service provider, receive the parking permit, and then initiate the parking procedure using an associated parking device. Automating this scenario would benefit from the quicker and reliable parking service; however, it also brings a few challenges regarding ensuring the user's privacy. In the *honest-but-curious* case, the user's name, vehicle plate number, current location, and similar properties should be kept private and processed by intended scenario actors.

1) System Model of Vehicle Parking Service

The privacy-preserving vehicle parking service consists of the following entities:

- **Vehicle** (V): a vehicle with a user parking device (e.g., smartphone, car multimedia system, navigation device) that is actively used in the system. In the case of employing autonomous vehicles, it is assumed that user parking devices are usually integrated as vehicle electronic systems and controlled via multimedia system panels.
- **Parking Lot Terminal** (PLT): an entity that manages access of the vehicles to a parking lot and controls and releases parking permits.
- **Parking Service Provider** (PSP): the main system entity that provides an interface between users and parking lot terminals integrated into the system. PSP registers/removes users and cooperates on checking the parking availability based on a user's location and his/her preferences. We assume that PSP is honest but can be curious.
- **Trusted Third Party** (TTP): an honest entity (e.g., government agency, municipality) that manages and releases users' TTP credentials and may assist in case of the revocation of user privacy.
- **User** (U): A user who uses the vehicle (V) and the user parking device with a system application. The user must first be registered in TTP and PSP to use PE-VPS and find available parking space.

2) Privacy and Security Requirements

The system has these privacy requirements:

- **data privacy**: stored and exchanged information do not expose undesired properties, e.g., user's vehicle plate, user parking history, etc.
- **pseudonymity**: a user is pseudonymous and can be identified only by certain parties (TTP). The user is not identifiable while using the system by external parties or other users.
- **unlinkability**: PSP or other users should not be able to link together parking actions of the same user (vehicle).
- **untraceability**: PSP cannot trace user's credentials and/or parking actions.

System security requirements are as follows:

- **accountability**: a user has specific responsibilities, e.g., payment per service use.
- **authentication**: parking permits are granted only to authenticated users. Access to the parking lot is then granted only to the user with a valid parking permit.
- **availability**: the connectivity of vehicle, user device, and service/application persist.
- **data confidentiality**: sensitive and personal data (e.g. Vehicle Plate Number - VPN) are secured. Data eavesdropping and exposure are prevented by encryption and/or blind signatures.
- **data authenticity and integrity**: data (e.g., parking permits, information about locations, and free parking slots) are secured against their tampering by unauthorized parties.
- **non-repudiation**: a proof that data are signed by a certain entity who cannot repudiate it.
- **revocation**: the cooperation of TTP and PSP enables the identification and removal of a user or its parking permission from the system.

3) Phases of Privacy-Preserving Vehicle Parking Service

The high-level description of PE-VPS phases is as follows:

- **Registration phase**: Figure 18 depicts the basic principle of the Registration phase with steps (1) and (2). In step (1), a user registers with TTP to check his identity and personal information such as name, phone, email, vehicle plate number, and vehicle plate number. The user obtains the signed TTP credential, e.g., Attribute-based Credential (ABC), with the user's attributes issued by TTP. In step (2), the user registers with PSP when he/she shows/proves only necessary attributes, e.g., email, VPN, using the ABC technique. PSP checks TTP-signed attribute-based credentials and returns to the user the signed PSP credential (e.g., a parking-service-access attribute, capability-based token) used by the user for pseudonymous access to a parking service. In this step, the anonymous payment can be deployed to prepaid a balance/credit for parking permits for a certain period.
- **Request phase**: Figure 18 shows the basic principle of the Request phase with steps (3) and (4) where the user asks PSP for checking the available parking space and issuing the parking permit. In step (3), the user firstly logins to PSP and proves his/her PSP credential, e.g., by using the parking-service-access attribute or capability-based token. PSP checks this user credential (by ABC) to anonymously access the

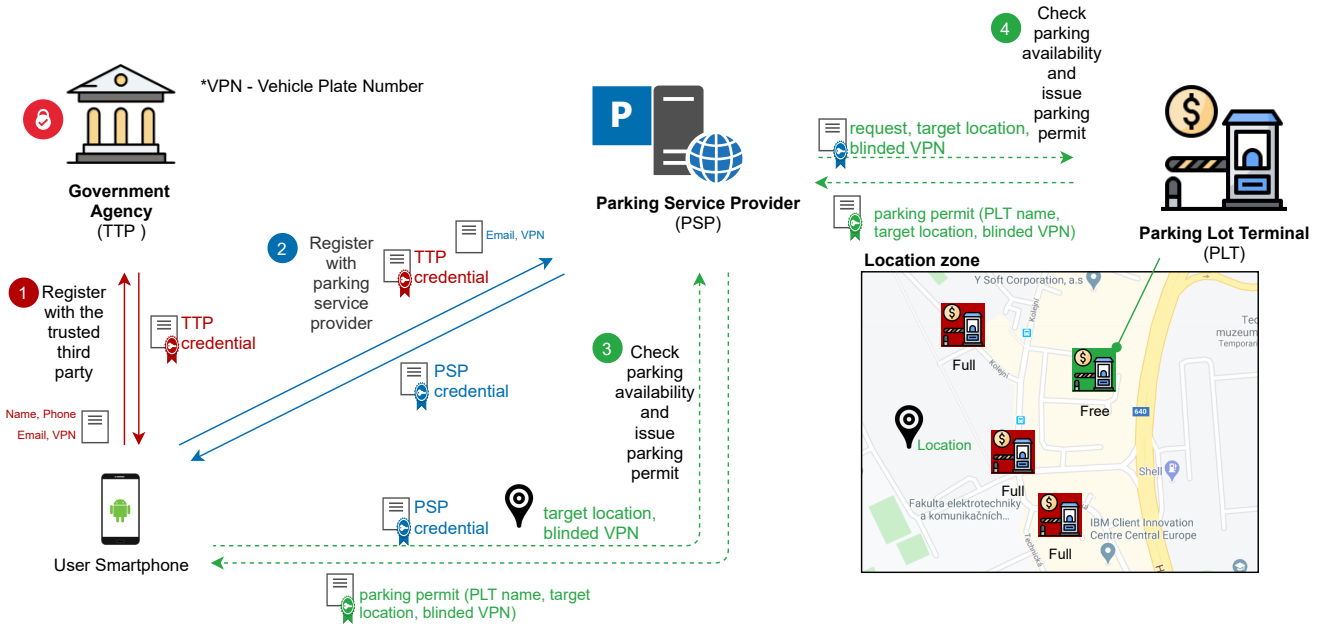


FIGURE 18. Registration and Request phases in PE-VPS

user into the service and create a secure channel that prevents eavesdropping. The user then sends a request with his/her target location and blinded VPN by using a Blind Signature (BS) technique. In step (4), PSP cooperating with PLTs checks an available parking space and prepares the parking permit. The parking permit that consists of PLT name, target location, and the signature of blinded VPN (signed by PLT) is then forwarded to the user via PSP. To be noted, PSP cannot recognize a user's VPN and track his/her behaviour in the system.

- **Parking phase**: Figure 19 depicts the parking phase with steps (5) and (6). In step (5), the user device transfers to the vehicle (an onboard unit) PLT name and target location to navigate to PLT. In step (6), the user device asks to enter the PLT with the parking permit (PLT name, target location, and an unblinded VPN signature) to activate automatic parking. The access is allowed to the vehicle with the valid parking permit and with a valid VPN taken by a camera and checked as the input of the unblinded VPN signature (by BS verification).
- **Revocation** phase - If a user breaks the rules or leaves the PSP service, his/her PSP credential is revoked (e.g., added in Blacklist, removed from Whitelist, etc.).

4) Deployment of PETs in Vehicle Parking Service

In a privacy-friendly scenario of Vehicle Parking Service (VPS) and its related IoV subsystems (e.g., payment, communication), the following PETs can be applied to preserve user privacy:

- **Attribute-based Credentials**: ABC can be deployed for pseudonymous and selected user authentication to PSP. The user can show and prove his/her selected attributes such as (email, vehicular plate number, or prepaid parking service access attribute).
- **Blind Signatures**: BS can be deployed while creating the parking permit. The user can hide (blind) the content of a message (e.g., vehicular plate number) to the signer (PLT) who signs parking permits and to other observers (PSP, other users). Then, PSP cannot track users by their VPNs. Blinded VPN are unlikable to each other.
- **Group Signatures**: GS can be deployed for increasing privacy during broadcasting notifications from user devices/vehicles. In IoV, Vehicles may broadcast or send to infrastructure the notifications (e.g., leaving parking lot/area) that can be signed by group signatures to preserve authenticity, integration, non-repudiation, and anonymity. The signed messages are verified by one public key. Only TTP can open then some malicious signatures and track and revoke signers.
- **Ring Signatures**: RS can be deployed in privacy-preserving payment. Some cryptocurrencies such as Monero already use RS. User transactions are then hidden from observers.
- **Searchable Encryption**: SE can be deployed for the own sake of the driver for him to get private statistics, e.g., frequency of the parking service use during the past month. The transaction history can be privately parsed to retrieve useful information relative to the user.
- **Homomorphic encryption**: HE can be deployed for the PSP to get general statistics about the

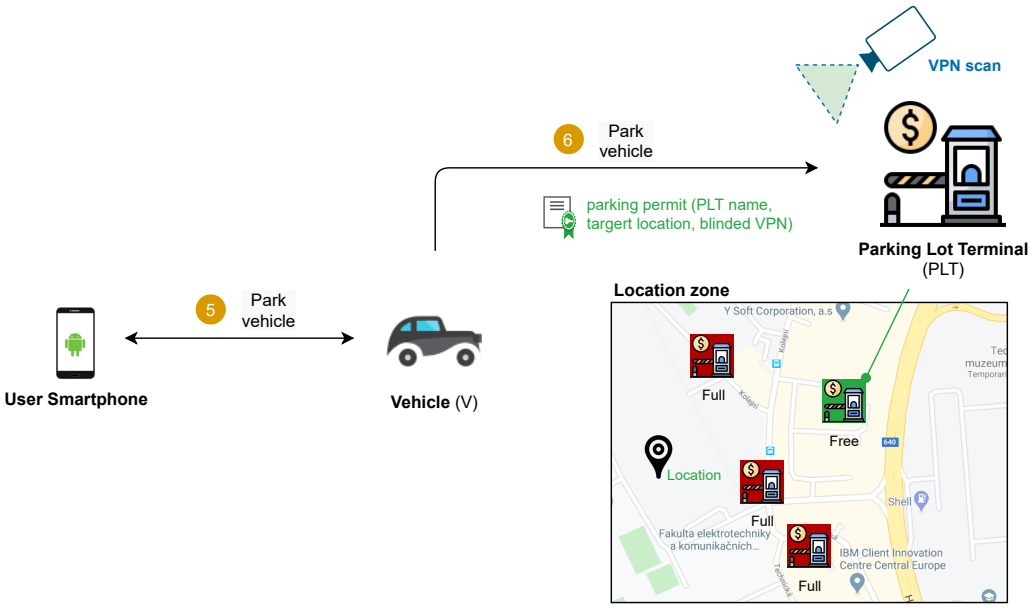


FIGURE 19. Parking phase in PE-VPS

parking service usage, e.g., frequency per PLT, or to get per-user statistics, e.g., frequency of use, number of paid parking hours, for instance, for affording prices/offers to the biggest customers. Simple operations could be managed over encrypted content for the PSP to get the computation results.

- **Attribute-based encryption**: ABE can be deployed for a user to share the computed usage statistics with the employer - the staff resources, the accountancy service - to get reimbursed for the parking costs.

B. TOWARDS QUANTUM-RESISTANT PRIVACY-ENHANCING VEHICLE PARKING SERVICES

There are already several quantum-resistant cryptography schemes and privacy-enhancing technologies that can be used in an IoT/II environment. This subsection deals with the deployment of PQC and QR-PETs in IoV with the parking scenario. Besides benefits and/or disadvantages, some future research problems are presented. The privacy-friendly vehicular parking scenario can be extended and/or modified to resist quantum attacks as follows:

- **Quantum-resistant Communication Security Protocols**: used secure communication channels such as TLS sessions should choose suitable cipher suites that consist of PQC primitives, e.g., NewHope for KEM, Dilithium for data signing, and double-sized symmetric encryption such as AES-GCM-256. Many PQC primitives for encryption, KEM, and signing have already been analyzed and tested on real devices (ARMs, FPGAs, PCs). Nevertheless, NIST will announce the recommended PQC schemes in 2022 - 2024.
- **Quantum-resistant Attribute-based Credentials**: employing lattice-based anonymous attribute tokens, e.g., [242], [243], may prevent quantum computer attacks. Still, the sizes of tokens/signed attributes will be quite large, e.g., units-tens MB. Those sizeable tokens will require more memory space in user devices and may cause delays during the authentication phases. Future research should be oriented on reasonable-sized signed attributes with efficient revocation approaches.
- **Quantum-resistant Blind Signatures**: employing multivariate blind signature schemes, e.g., Petzoldt *et al.*'s scheme [238] with 28.5 kB signatures, can be practical from a communication header perspective. Besides, classic multivariate schemes have already been tested on various embedded devices; thus, these schemes can be deployed on user devices and PLTs.
- **Quantum-resistant Group Signatures**: current quantum-resistant group signatures produce still quite sizeable signatures, e.g., 6.74 MB in [280]. These sizes are not very practical for IoV environments with constrained devices and limited communication overhead. Future research should be oriented to reasonable-sized and constant group signatures.
- **Quantum-resistant Ring Signatures**: employing an efficient quantum-resistant ring signature scheme such as multivariate ring signature based on Rainbow scheme [236]. The implementations of multivariate schemes into cryptocurrencies for secure payments can be an interesting research problem.
- **Quantum-resistant Encryption Techniques**: several HE, SE, and ABE encryption schemes with privacy properties already use lattice-based constructions.

These schemes can be deployed into the scenario to be secure in the post-quantum era.

C. CONCLUDING REMARKS

The Privacy-Enhancing Vehicle Parking Service (PE-VPS) use case presents a unique scenario where multiple PETs (e.g. the digital signatures, user authentication, and privacy-enhancing encryption primitives) are incorporated in an IoV system to ensure privacy protection. Post-quantum-resistant cryptography schemes and quantum-resistant adaptations of proposed PETs can also be applied to the vehicle parking scenario.

VIII. MAIN CHALLENGES AND FUTURE RESEARCH DIRECTIONS IN PRIVACY-ENHANCING TECHNOLOGIES

There are currently many issues and challenges in the area of PETs that should be solved when heading into the Post Quantum era. This section focuses on open problems, the potential improvements of PETs, and future trends. The following subsections discuss chosen aspects of PETs and their deployment in various parts of IoT/IIs.

A. PRIVACY-UTILITY TRADE-OFF

Regarding general anonymization techniques introduced in Section IV-F, SDC methods are typically vulnerable when the attacker gains unexpected background knowledge and access to auxiliary data. In contrast, differential privacy avoids such drawbacks and can provide information-theoretic privacy guarantees. However, when applying this concept to real-world applications, a general concern is the privacy-utility trade-off, which is often problematic to define in reality [281]. Another consideration is about the privacy budget, namely ϵ. It is often hard to set this value, and it is also difficult to explain the guarantees to non-experts. Another concern is that adding noise to existing processes or data is not appealing and can even cause a problem in some application scenarios, e.g., medical research [282], [283]. Much effort is needed to solve these concerns, and the effectiveness of solutions can only be evaluated on a case-by-case basis.

Furthermore, the privacy-utility trade-off is a concern in ring signatures. In many RS schemes, the ring signature's length is usually linear with the ring's size. On the one hand, larger ring signatures with larger anonymity set parameters typically provide a higher privacy level. On the other hand, these schemes are usually memory and computationally expensive. Some size-optimal ring signatures have been recently proposed [284], [285]. Nevertheless, designing well-balanced efficient, privacy-preserving, and constant-sized or logarithmic-sized ring signature schemes is still ongoing.

B. UTILIZATION OF PETS ON CONSTRAINED DEVICES

Our IoT/II world is filled with billions of constrained devices. Constrained devices often assist with and/or apply security and privacy-preserving countermeasures, e.g., GS, RS, ABC, ABE, SMC, in the perception layer of IoT/IIs. There is still ongoing work on efficient group signatures with immediate revocation features or ring signatures appropriate for constrained devices, and some first proposals are [80]–[82], [88], [89]. We can also expect that future schemes will be preferred to be based on quantum-resistant GS/RS constructions, namely, lattice-based problems [286]. Nevertheless, these constructions often work with cryptographic parameters (matrixes, public keys, signatures) with sizes from tens of kilobits to a few megabits and may cause problems for memory-constrained devices. Moreover, due diligence needs to be taken when assigning heavy computational tasks to resource-constrained devices; this is an active research area. As another example, it remains an open challenge to design a computationally inexpensive (which takes minimal data retrieval time) searchable encryption mechanism with strong security to adopt them widely in IoT. Also, HE schemes are currently computationally expensive for most sensors due to numerous heavy asymmetric cryptographic operations. Hence, HE schemes are used more in back-end services at servers.

C. PETS IN LARGE SCALE APPLICATIONS

When applying the differential privacy concept to IoT/II applications with large-scale distributed system structure, one potential concern is to find a trustworthy curator for everybody in the system. To this end, the concept of local differential privacy has been proposed [287]. Yet, local differential privacy introduces a new problem, i.e., the general concerns of differential privacy need to be addressed in a distributed manner.

Furthermore, revocable attribute-based credential schemes, which achieve practical running times on constrained devices, are still under development and in a proof-of-concept stage. In future work, we can expect more practical implementations of ABC systems in large scale applications such as privacy-preserving access control in modern services such as smart parking, sharing cars, access to low-emission zones, digital elections, etc.

Role-Based Encryption (RBE) is a promising cryptographic encryption primitive. The main idea of RBE is to integrate the properties of the RBAC model and the public-key encryption method. The first concept of RBE was proposed in [288] by Zhou *et al.* for securing cloud data. Afterward, a few schemes [289]–[291] have been designed for the cloud to achieve various functionalities and increase efficiency. RBE uses RBAC access policies to encrypt data, and any user, who possesses qualified roles, can access the data after decryption using their decryption key. One of the crucial features of RBE is the inheritance property, where one role can inherit access rights of the other roles. It is a suitable encryption technique for an environment where the access rights are organized in a hierarchical form. It is observed that RBE has not been explored in the IoT/II environment. It will be interesting to see RBE's application in IoT/II

environment in terms of performance, despite having some challenges like privilege revocation, dynamic change in an access policy, etc., and how it is comparable to other techniques such as ABE.

In some large scale IoT/II applications, emerging fog computing reduces centrality and provides local computing processing for faster data analysis. Recently, Mukherjee *et al.* [292] have discussed primary privacy issues and privacy preservation challenges in fog computing, e.g., access control with heterogeneous requirements.

D. PRIVACY-PRESERVING DATA MINING AND PROCESSING

Data splitting and data processing in cloud-based environments at the moment are mostly working on clear (non-encrypted) data due to the infeasibility of processing encrypted ones. Searchable encryption (SE) and homomorphic encryption (HE) are limited to pre-defined queries/computations. Moreover, SE starts to leak information on the stored data after a certain number of queries. On the other hand, processing unencrypted data requires a certain level of trust and can result in privacy leakage. Hybrid solutions where parts of the data are encrypted (e.g., HE) and another left in the clear can be a good trade-off between privacy and fast-processing. However, where the data are fully encrypted, solutions will lead to perfect privacy and security. Recently, Alabdulatif *et al.* [293] introduced a novel privacy-preserving distributed big data analytics framework for cloud-based applications using fully homomorphic encryption proposed by Brakerski *et al.* [249]. They improve encrypted analysis tasks by splitting large datasets into small subsets and processed them in a distributed manner.

One of the promising applications of HE is in machine learning, especially in deep learning. Research has been conducted so far and addressed neural network operations [294], [295], pre-trained neural networks [296]–[298], and high parallelizable machine learning operations [299], [300]. However, some challenges are yet to be addressed, such as performance-boosting by efficiently switching to GPUs, doing the full training over encrypted data, and making the processing highly parallelizable.

E. BLOCKCHAIN-BASED AND DECENTRALIZED PETS

Future research directions will provide a decentralized ABC system to increase security, privacy, and trust. There is a need for more user-centric systems that allow users to have power over their data and selectively disclose only what is necessary for having the service. Anonymous attribute-based credentials make users become the real owners of their data. Unfortunately, current solutions are usually based on a centralized approach. There are several proposals of ABC schemes based on a public ledger [301], [302] that provide protocols for decentralized issuance. However, these schemes lack important algorithms (particularly for revocation and inspection), are too complex (both computationally and memory-wise) for the implementation on constrained devices, and have limited compatibility with existing major schemes. Recently, Singh *et al.* [303] presented a privacy-preserving credential scheme that uses the blockchain. The proposal allows users to self-blind their attributes, and their credentials are still verifiable by a service provider on the blockchain. Besides the aforementioned proposals, more proposals for decentralized ABC systems are currently missing.

In SE, most of the existing schemes have been designed for centralized environments, where a central authority (i.e., service provider) performs the keyword search operations over the encrypted data. Recently, IDC reported [304] that 80% of the organizations and enterprises are now moving towards multi-cloud services such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, due to many reasons including enabling agile business innovation, reaching global markets, satisfying compliance and regulatory concerns, and ensuring appropriate application performance and cost management. As such, a decentralized SE mechanism has become an essential requirement nowadays. This research issue has yet to be well explored. Another interesting area is SE systems' design supporting properties of the traditional Role-Based Access Control (RBAC) model [305].

Another area of future research involving blockchain technology is its combination with federated learning to offload some computational tasks to the edge (local updates) while maintaining an overall picture centrally (global update) [306], [307]. Within federated learning, there will be an overall need to maintain the data's security and privacy shared through such networks while ensuring that these networks' devices are trusted. This research topic is expected to be extremely active in the coming years, as shown in [306], a very recent survey focusing on this very topic specifically.

Finally, Ferrag *et al.* [308] survey existing blockchain protocols designed for IoT/II networks and discuss anonymity and privacy in various Bitcoin and Blockchain systems. They also mentioned several potential future work directions, e.g., design blockchain-based protocols for preserving transaction privacy in vehicular cloud advertisement dissemination, etc.

F. IMPROVEMENT AND SECURITY OF QUANTUM RESISTANT PETS

Current proposals of QR PETs such as [229], [236], [238], [243], [256], [262] are mostly orientated on classic computer nodes with more powerful hardware. Quantum-resistant constructions when compared with traditional constructions based on elliptic curves, DH problems, RSA problems are still more memory and computationally expensive. Nevertheless, lattice-based constructions offering a good memory-performance trade-off seem very attractive in designing new QR PETs schemes. Future research should focus on new QR PETs schemes designed as energy-efficient

and tailored for IoT services. Moreover, new theoretical insights are still needed for the security analysis of QR PETs.

Another interesting future direction is the privacy aspects of physics-based Quantum-Key Distribution (QKD) approaches. For example, efficient privacy amplification in the post-processing of QKD has started to gain attention recently [309], [310].

G. STANDARDIZATION OF QUANTUM RESISTANT PETS

As shown in Figure 15, 7 third round finalists (Classic McEliece, CRYSTALS-Kyber, NTRU, SABER, CRYSTALS- Dilithium, Falcon, Rainbow) have been announced by NIST in the PQC Standardization Process [193]. However, a similar standardization process with novel quantum-resistant PETs is still future work. Moreover, only a few standards are already available for classic PETs schemes, e.g., ISO/IEC 20008-2:2013 [70].

H. CONCLUDING REMARKS

In this section, we summarized our research work by listing seven challenges worth further investigation. This includes the challenges on the trade-offs of the privacy utility, utilization of PETs on constrained devices, PETs in large scale application, privacy-preserving data mining and processing, blockchain-based and decentralized PETS, improvement and security of quantum resistant PETs, and standardization of quantum resistant PETs. All challenges are important and highlight the future research directions, potentially leading to the secure systems in the post-quantum era.

IX. CONCLUSION

The need for security and privacy in our current IoT/II world can be stated with no hesitation. However, finding strong solutions that can provide secure environments has been a challenge due to computational as well as energy constraints and a lack of uniformity across networks. This paper gives an in-depth look at privacy protection approaches and highlights their current deployment in ICT products, pilots, projects, and IoT/II use cases. There is a myriad of classical privacy threats that are faced daily in IoT/II environments. Furthermore, we present 15 privacy-enhancing technologies to help categorize these threats and solutions. As a detailed use case, a parking service with respect to the Internet of Vehicles is presented as an illustrative case to demonstrate how several categories of PETs can be employed for satisfying security and privacy requirements in various parking service functions and phases. Additionally, this paper analyzes the state-of-the-art in post-quantum cryptography with an emphasis on privacy-preserving schemes. It is shown that lattice-based schemes for key establishment and digital signatures are more suitable for various constrained IoT/II platforms than other PQC families. This is a direct consequence of the trade-off between memory and computation requirements advocated by lattice-based schemes. Furthermore, this paper maps recent quantum-resistant privacy-preserving schemes and show that lattice-based constructions can be used in most PETs as presented.

Focusing on the next steps in PET-based research, we have highlighted several directions, including reaching the privacy-utility trade-off, optimizing PETs schemes for constrained IoT devices, practical implementation of PETs in large scale systems and cloud services, designing decentralized PETs, increasing efficiency and security of quantum-resistant PETs, and finally the process of beginning QR PETs standardization. We foresee that advancement in these directions will certainly make PETs more appealing to the practitioners in IoT/IIs and beyond. Moreover, such advancements will also give birth to more versatile applications in the emerging decentralized and distributed computing paradigms enabled by technologies such as 5G and Blockchain Distributed Ledger Technology (DLT).

ACKNOWLEDGEMENTS

This paper is supported in part by European Union's Horizon 2020 research and innovation program under grant agreement No 830892, project SPARTA, and in part by the Ministry of the Interior of the Czech Republic under grant VJ01030002.

APPENDIX: TABLES

TABLE 10
PETs IN PRODUCTS AND PILOTS (I.)

PETs	Pilot/Product	Description
Group Signatures	group-signature-scheme-eval	This is a partial ISO20008-2.2 implementation of group signature schemes in order to evaluate it on mobile devices. Authors: Klaus Potzmader Johannes Winter Daniel Hein Christian Hanser Peter Teu, Liqun Chen. WWW: https://github.com/klapm/group-signature-scheme-eval
	libgroupsig	The libgroupsig library is an experimental library with 4 group signature schemes. WWW: https://bitbucket.org/jdiazvico/libgroupsig/wiki/Architecture
Ring Signatures	Monero	Since 2014, Monero is a cryptocurrency technology with a focus on private and censorship-resistant transactions. Monero employs ring signatures (MLSAG signatures [91]) in order to provide private transactions. WWW: https://web.getmonero.org/resources/about/
	Cryptonote (cryptonotecoin)	The website Cryptonote presents the features and description of Cryptonote cryptocurrency uses one-time ring signatures. The repository contains a CryptoNote protocol implementation and instructions for starting a new CryptoNote currency. WWW: https://cryptonote.org/
	TokenPay	TokenPay is the altcoin and payment platform based on the Proof of Stake algorithm. TokenPay combines ring signatures, dual-key stealth address, and Zero-Knowledge Proof, making the transactions on TokenPay Blockchain completely anonymous and untraceable. The code is available on GitHub, WWW: https://github.com/tokenpay/tokenpay.
Blind Signature	PayCash	The Russian electronic payment platform for anonymous payments on the Internet. WWW: http://www.paycash.com.mx/
	Hashcash	Hashcash is a proof-of-work algorithm that provides primary protection against spam and DoS attacks. Furthermore, the technology promises more privacy-preserving properties than other blockchain-based systems such as Bitcoin, Ethereum, etc. WWW: http://www.hashcash.com
Attribute-Based Credential	Identity Mixer (Idemix)	Identity Mixer (Idemix) is an anonymous credential system developed at IBM Research (description in [311], SW release 2007). The system is based on Camenisch-Lysyanskaya signature [312] that allows the issuer to sign the user's attributes to create a cryptographic credential. Using the zero-knowledge protocol, the user randomizes and sends the credential to a verifier to anonymously prove his/her possession of attributes. The specification of the Identity Mixer Cryptographic Library was released in 2010 [263].. WWW: https://github.com/IBM-Cloud/idemix-issuer-verifier
	U-Prove	U-Prove is a user-centric cryptographic technology based on Brands techniques [96] that enables the issuance and presentation of cryptographically protected statements. U-Prove tokens that encoded user attributes may be on-demand (one time) or long-lived (reusable with an expiration time). U-Prove cryptographic specification can be found in [313]. More about U-Prove technology can be found in [264]. Microsoft releases two implementations: U-Prove C# SDK and U-Prove Extensions SDK that implements extensions to the U-Prove Cryptographic Specification, 2014. WWW: https://www.microsoft.com/en-us/research/project/u-prove/
	IRMA	IRMA (I Reveal My Attributes) empowers persons to disclose online, via mobile phones, certain attributes of them (e.g. over 18), but at the same time hide other attributes (like your name or phone number). IRMA is based on Idemix and provides Issuer unlinkability and Multi-show unlinkability. The IRMA app is available for Android (Google) and for iOS (Apple). The smart card version was released for MultOS cards in 2014. WWW: https://github.com/credentials/irma_card
Mix-networks and Proxies	Mixmaster	The website Mixmaster presents the type II remailer protocol and the most popular implementation of it. WWW: https://sourceforge.net/projects/mixmaster/files/
	Mixminion: A Type III Anonymous Remailer	Mixminion is the reference implementation of the Type III Anonymous Remailer protocol. This project is not under active development. Github code: https://github.com/mixminion/mixminion/
	JonDoNym	JonDonym (Java Anon Proxy or JAP) is a proxy system based on several mix cascades for private browsing. The project was developed originally by the Technische Universitat Dresden, the Universitat Regensburg and Privacy Commissioner of Schleswig-Holstein. JonDo is a proxy client (SW) that forwards the traffic of internet applications encrypted via the mix cascade. The website also offers a web browser JonDoFox is based on Tor Browser. WWW: https://anonymous-proxy-servers.net
	Open Verificatum	Verificatum is a mix-based based e-voting system. The code is available on GitHub: https://github.com/verificatum

TABLE 11
PETs IN PRODUCTS AND PILOTS (II.)

PETs	Pilot/Product	Description
Onion Routing	Tor	Tor [118] based on onion routing provides users the privacy-enhancing web browser application. WWW: https://www.torproject.org/.
	Tribler	Tribler is an open source decentralized BitTorrent client which provides anonymous peer-to-peer communication by onion routing, WWW: https://www.tribler.org/
	Tox	Tox is a peer-to-peer instant-messaging and video-calling protocol that offers end-to-end encryption . WWW: https://tox.chat/
Homomorphic Encryption	HEAT: Homomorphic Encryption Applications and Technology	An open source software library that supports applications that wish to use homomorphic cryptography. WWW: https://heat-project.eu/.
	Microsoft SEAL	The Microsoft open-source library with implementations of BFV and CKKS schemes. The goal of the library is to make homomorphic encryption available in an easy-to-use form both to experts and to non-experts. WWW: https://www.microsoft.com/en-us/research/project/homomorphic-encryption/.
	PALISADE	PALISADE provides efficient implementations of lattice-based cryptography building blocks and leading homomorphic encryption schemes to the open-source library from a consortium of DARPA. WWW: https://palisade-crypto.org/.
	HElib	HElib is an open-source (AL v2.0) software library that implements homomorphic encryption (HE) schemes, i.e., the Brakerski-Gentry-Vaikuntanathan (BGV) scheme with bootstrapping and the Approximate Number scheme of Cheon-Kim-Kim-Song (CKKS), WWW: https://github.com/homenc/helib.
Searchable Encryption	Search Encrypt	The Search Encrypt encrypts users' search terms between the users' computer and service searchencrypt.com. It forces an advanced SSL encryption utilizing perfect forward security to keep the user protected while searching and also encrypts the users' search term locally before being sent to the servers. WWW: https://www.searchencrypt.com/.
	PaaSword - A Holistic Data Privacy and Security by Design Platform-as-a-Service Framework	PaaSword provides a privacy-preserving framework for enterprise cloud computing. WWW: https://paasword.io/.
Attribute-Based Encryption	Zeutro LLC: Encryption & Data Security	Zeutro is a software company that produces the OpenABE library - open-source cryptographic library with attribute-based encryption implementations in C/C++. WWW> https://github.com/zeutro/openabe.
	Entrance jTR-ABE repository	The implementation of a Ciphertext Policy Attribute-Based Encryption (CP-ABE) scheme by Liu and Wong named: Practical Attribute-Based Encryption: Traitor Tracing, Revocation, and Large Universe. https://entrance.snet.tu-berlin.de/entrance_github/.
Secure Multi-party Comp.	Jana: Private-Data-as-a-Service	Jana (funded by DARPA's Brandis program) aims to provide practical private data as a service to protect subject privacy while retaining data utility to analysts. WWW: https://galois.com/project/jana-private-data-as-a-service/.
	Unbound	Unbound uses Secure Multi-party Computation (SMC) to protect secrets such as cryptographic keys by ensuring they never exist in complete form. WWW: https://www.unboundtech.com/.
Differential Privacy	Privitar Lens	Privitar Lens is a solution that sits between data providers and applications, providing a privacy-preserving API to statistical insights that can power a range of data products such as interactive visualizations, dashboards or reports. Privacy protection is based on the differential privacy concepts and works for high-dimensional datasets such as location or transaction records. WWW: https://www.privitar.com/lens.
	Uber	Uber has released an open-source project containing a query analysis and a rewriting engine to enforce DP for general-purpose SQL queries. The rewriting engine can transform an input query into an intrinsically private query that embeds a DP mechanism in the query directly. The transformed query enforces differential privacy on its results and can be applied to any standard SQL database. Many current differential privacy mechanisms are used in the approach. At now, the code includes rewriters based on Elastic Sensitivity and Sample and Aggregate. WWW: https://github.com/uber/sql-differential-privacy.
	RAPPOR Google	In 2014, three Google researchers proposed a new technology, named Randomized Aggregatable Privacy-Preserving Ordinal Response (RAPPOR) [278], which allows for privacy-preserving crowdsourcing statistics from end-user client software by applying differential privacy mechanisms. It allows the forest of client data to be studied without permitting the possibility of looking at individual trees. It considered the trade-off between differential-privacy and utility guarantees and discussed the properties when facing different attack models. Now, RAPPOR has been made an open-source project. WWW: https://github.com/google/rappor.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] J.-H. Hoepman, "Privacy design strategies," in IFIP International Information Security Conference. Springer, 2014, pp. 446–459.

[3] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Metayer, R. Tirtea, and S. Schiffner, "Privacy and data protection by design-from policy to engineering," arXiv preprint arXiv:1501.03726, 2015.

[4] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," A Practical Guide, 1st Ed., Cham: Springer International Publishing, 2017.

[5] T. M. Fernández-Caramés, "From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things," IEEE Internet of Things Journal, 2019.

[6] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker, and H. Chen, "Uninvited connections: a study of vulnerable devices on the internet of things (iot)," in 2014 IEEE Joint Intelligence and Security Informatics Conference. IEEE, 2014, pp. 232–235.

[7] V. Srinivasan, J. Stankovic, and K. Whitehouse, "Protecting your daily in-home activity information from a wireless snooping attack," in Proceedings of the 10th international conference on Ubiquitous computing. ACM, 2008, pp. 202–211.

[8] M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, and K. Wehrle, "User-driven privacy enforcement for cloud-based services in the internet of things," in 2014 International Conference on Future Internet of Things and Cloud. IEEE, 2014, pp. 191–196.

[9] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," in European data protection: coming of age. Springer, 2013, pp. 3–32.

[10] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," Computer networks, vol. 76, pp. 146–164, 2015.

[11] K.-A. Shim, "A survey of public-key cryptographic primitives in wireless sensor networks," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 577–601, 2015.

[12] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, "On perspective of security and privacy-preserving solutions in the internet of things," Computer Networks, vol. 102, pp. 83–95, 2016.

[13] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017.

[14] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616–644, 2019.

[15] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2886–2927, 2019.

[16] L. Malina, G. Srivastava, P. Dzurenda, J. Hajny, and S. Ricci, "A privacy-enhancing framework for internet of things services," in International Conference on Network and System Security. Springer, 2019, pp. 77–97.

[17] S. A. Hamad, Q. Z. Sheng, W. E. Zhang, and S. Nepal, "Realizing an internet of secure things: A survey on issues and enabling technologies," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1372–1391, 2020.

[18] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, and A. V. Vasilakos, "The quest for privacy in the internet of things," IEEE Cloud Computing, vol. 3, no. 2, pp. 36–45, 2016.

[19] C. Dwork and G. J. Pappas, "Privacy in information-rich intelligent infrastructure," arXiv preprint arXiv:1706.01985, 2017.

[20] J. Lopez, R. Rios, F. Bao, and G. Wang, "Evolving privacy: From sensors to the internet of things," Future Generation Computer Systems, vol. 75, pp. 46–57, 2017.

[21] S.-C. Cha, T.-Y. Hsu, Y. Xiang, and K.-H. Yeh, "Privacy enhancing technologies in the internet of things: Perspectives and challenges," IEEE Internet of Things Journal, 2018.

[22] M. Seliem, K. Elgazzar, and K. Khalil, "Towards privacy preserving iot environments: A survey," Wireless Communications and Mobile Computing, vol. 2018, 2018.

[23] A. A. A. Sen, F. A. Eassa, K. Jambi, and M. Yamin, "Preserving privacy in internet of things: a survey," International Journal of Information Technology, vol. 10, no. 2, pp. 189–200, 2018.

[24] C. Li and B. Palanisamy, "Privacy in internet of things: From principles to technologies," IEEE Internet of Things Journal, vol. 6, no. 1, pp. 488–505, Feb 2019.

[25] J. Curzon, A. Almehmadi, and K. El-Khatib, "A survey of privacy enhancing technologies for smart cities," Pervasive and Mobile Computing, 2019.

[26] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 746–789, 2020.

[27] K. S. Roy and H. K. Kalita, "A survey on post-quantum cryptography for constrained devices," International Journal of Applied Engineering Research, vol. 14, no. 11, pp. 2608–2615, 2019.

[28] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Post-quantum lattice-based cryptography implementations: A survey," ACM Computing Surveys (CSUR), vol. 51, no. 6, pp. 1–41, 2019.

[29] A. Lohachab, A. Lohachab, and A. Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum iot networks," Internet of Things, vol. 9, p. 100174, 2020.

[30] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: A survey," IEEE Access, vol. 8, pp. 131 723–131 740, 2020.

[31] R. A. Perlner and D. A. Cooper, "Quantum resistant public key cryptography: a survey," in Proceedings of the 8th Symposium on Identity and Trust on the Internet, 2009, pp. 85–93.

[32] J. Buchmann, R. Lindner, M. Rückert, and M. Schneider, "Post-quantum cryptography: lattice signatures," Computing, vol. 85, no. 1-2, pp. 105–125, 2009.

[33] D. Micciancio and O. Regev, "Lattice-based cryptography," in Post-quantum cryptography. Springer, 2009, pp. 147–191.

[34] J. A. Buchmann, D. Butin, F. Göpfert, and A. Petzoldt, "Post-quantum cryptography: state of the art," in The New Codebreakers. Springer, 2016, pp. 88–108.

[35] D. J. Bernstein and T. Lange, "Post-quantum cryptography," Nature, vol. 549, no. 7671, pp. 188–194, 2017.

[36] T. G. Tan and J. Zhou, "A survey of digital signing in the post quantum era." IACR Cryptol. ePrint Arch., vol. 2019, p. 1374, 2019.

[37] K. Basu, D. Soni, M. Nabeel, and R. Karri, "Nist post-quantum cryptography-a hardware evaluation study." IACR Cryptology ePrint Archive, vol. 2019, p. 47, 2019.

[38] L. Malina, L. Popelova, P. Dzurenda, J. Hajny, and Z. Martinasek, "On feasibility of post-quantum cryptography on small devices," IFAC-PapersOnLine, vol. 51, no. 6, pp. 462–467, 2018.

[39] A. Perallos, U. Hernandez-Jayo, I. J. G. Zuazola, and E. Onieva, Intelligent Transport Systems: Technologies and Applications. John Wiley & Sons, 2015.

[40] X. Yang, Z. Li, Z. Geng, and H. Zhang, "A Multi-layer Security Model for Internet of Things," in Internet of Things, Y. Wang and X. Zhang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 388–393.

[41] O. Yousuf and R. N. Mir, "A Survey on the Internet of Things Security: State-of-Art, Architecture, Issues and Countermeasures," Information & Computer Security, vol. 27, no. 2, pp. 292–323, 2019.

[42] L. Li, "Study on Security Architecture in the Internet of Things," in Proceedings of 2012 International Conference on Measurement, Information and Control, vol. 1. IEEE, 2012, pp. 374–377.

[43] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, "Study and Application on the Architecture and Key Technologies for IoT," in 2011 International Conference on Multimedia Technology. IEEE, 2011, pp. 747–751.

[44] Z. Zhang, M. C. Y. Cho, C. Wang, C. Hsu, C. Chen, and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," in 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, Nov 2014, pp. 230–234.

[45] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," in 2013 Ninth international conference on computational intelligence and security. IEEE, 2013, pp. 663–667.

[46] É. Dubois, P. Heymans, N. Mayer, and R. Matulevičius, "A systematic approach to define the domain of information system security risk management," in Intentional Perspectives on Information Systems Engineering. Springer, 2010, pp. 289–306.

[47] R. Matulevičius, Fundamentals of Secure System Modelling. Springer, 2017.

[48] "CAPEC - Common Attack Pattern Enumeration and Classification," https://capec.mitre.org/, last accessed 8-Oct-2020.

[49] "MITRE ATT&CK," https://attack.mitre.org/, last accessed 8-Oct-2020.

[50] A. Shostack, Threat Modeling: Designing for Security. John Wiley & Sons, 2014.

[51] O. A.-a. Affia, R. Matulevičius, and A. Nolte, "Security risk management in cooperative intelligent transportation systems: A systematic literature review," in Proceedings of CoopIS 2019. Springer, 2019.

[52] D. J. Solove, "A taxonomy of privacy," U. Pa. L. Rev., vol. 154, p. 477, 2005.

[53] D. Chen, K.-T. Cho, and K. G. Shin, "Mobile imus reveal driver's identity from vehicle turns," arXiv preprint arXiv:1710.04578, 2017.

[54] A. A. Alghanim, S. M. M. Rahman, and M. A. Hossain, "Privacy analysis of smart city healthcare services," in 2017 IEEE International Symposium on Multimedia (ISM). IEEE, 2017, pp. 394–398.

[55] R. Xu, Q. Zeng, L. Zhu, H. Chi, X. Du, and M. Guizani, "Privacy leakage in smart homes and its mitigation: Ifttt as a case study," IEEE Access, vol. 7, pp. 63 457–63 471, 2019.

[56] Y. Hong, W. M. Liu, and L. Wang, "Privacy preserving smart meter streaming against information leakage of appliance status," IEEE transactions on information forensics and security, vol. 12, no. 9, pp. 2227–2241, 2017.

[57] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," IEEE Communications Magazine, vol. 55, no. 1, pp. 122–129, 2017.

[58] L. Zhou, Q. Chen, Z. Luo, H. Zhu, and C. Chen, "Speed-based location tracking in usage-based automotive insurance," in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2017, pp. 2252–2257.

[59] X. Gao, B. Firner, S. Sugrim, V. Kaiser-Pendergrast, Y. Yang, and J. Lindqvist, "Elastic pathing: Your speed is enough to track you," in Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2014, pp. 975–986.

[60] N. Kaibalina and A. M. Rizvi, "Security and privacy in vanets," in 2018 IEEE 12th International Conference on Application of Information and Communication Technologies (AICT). IEEE, 2018, pp. 1–6.

[61] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," IEEE Communications Magazine, vol. 53, no. 6, pp. 126–132, 2015.

[62] I. Sanchez, R. Satta, I. N. Fovino, G. Baldini, G. Steri, D. Shaw, and A. Ciardulli, "Privacy leakages in smart home wireless technologies," in 2014 International Carnahan Conference on Security Technology (ICCST). IEEE, 2014, pp. 1–6.

[63] A. Acar, H. Fereidooni, T. Abera, A. K. Sikder, M. Miettinen, H. Aksu, M. Conti, A.-R. Sadeghi, and A. S. Uluagac, "Peek-a-boo: I see your smart home activities, even encrypted!" arXiv preprint arXiv:1808.02741, 2018.

[64] D. Eckhoff and I. Wagner, "Privacy in the smart city-applications, technologies, challenges, and solutions," IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 489–516, 2017.

[65] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy management in social internet of vehicles: Review, challenges and blockchain based solutions," IEEE Access, vol. 7, pp. 79 694–79 713, 2019.

[66] H. Choi, S. Chakraborty, Z. M. Charbiwala, and M. B. Srivastava, "Sensorsafe: a framework for privacy-preserving management of personal sensory information," in Workshop on Secure Data Management. Springer, 2011, pp. 85–100.

[67] M. Layouni, K. Verslype, M. T. Sandıkkaya, B. De Decker, and H. Vangheluwe, "Privacy-preserving telemonitoring for ehealth," in IFIP Annual Conference on Data and Applications Security and Privacy. Springer, 2009, pp. 95–110.

[68] T. Moses, "Quantum computing and cryptography," Entrust Inc. January, 2009.

[69] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996, pp. 212–219.

[70] I. O. for Standardization, "Iso/iec 20008-2: Information technology - security techniques - anonymous digital signatures - part 2: Mechanisms using a group public key. stage 60.60," International Organization for Standardization. Geneva, Switzerland, pp. 0–86, 2013.

[71] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Annual International Cryptology Conference. Springer, 2004, pp. 41–55.

[72] C. Delerablée and D. Pointcheval, "Dynamic fully anonymous short group signatures," in Progress in Cryptology-VIETCRYPT 2006. Springer, 2006, pp. 193–210.

[73] J. Camenisch and J. Groth, "Group signatures: Better efficiency and new theoretical aspects," in International Conference on Security in Communication Networks. Springer, 2004, pp. 120–133.

[74] T. Isshiki, K. Mori, K. Sako, I. Teranishi, and S. Yonezawa, "Using group signatures for identity management and its implementation," in Proceedings of the second ACM workshop on Digital identity management. ACM, 2006, pp. 73–78.

[75] J. Groth, "Fully anonymous group signatures without random oracles," in International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2007, pp. 164–180.

[76] J. Y. Hwang, S. Lee, B.-H. Chung, H. S. Cho, and D. Nyang, "Short group signatures with controllable linkability," in Lightweight Security & Privacy: Devices, Protocols and Applications (LightSec), 2011 Workshop on. IEEE, 2011, pp. 44–52.

[77] B. Libert, T. Peters, and M. Yung, "Scalable group signatures with revocation," in Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2012, pp. 609–627.

[78] K. Emura and T. Hayashi, "A light-weight group signature scheme with time-token dependent linking," in Lightweight Cryptography for Security and Privacy. Springer, 2015, pp. 37–57.

[79] D. Derler and D. Slamanig, "Highly-efficient fully-anonymous dynamic group signatures," in Proceedings of the 2018 on Asia Conference on Computer and Communications Security. ACM, 2018, pp. 551–565.

[80] C. Esposito, A. Castiglione, F. Palmieri, and A. De Santis, "Integrity for an event notification within the industrial internet of things by using group signatures," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3669–3678, 2018.

[81] R. Xie, C. He, C. Xu, and C. Gao, "Lattice-based dynamic group signature for anonymous authentication in iot," Annals of Telecommunications, pp. 1–12, 2019.

[82] S. Eom and J.-H. Huh, "Group signature with restrictive linkability: minimizing privacy exposure in ubiquitous environment," Journal of Ambient Intelligence and Humanized Computing, pp. 1–11, 2018.

[83] J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups," in Australasian Conference on Information Security and Privacy. Springer, 2004, pp. 325–335.

[84] Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup, "Anonymous identification in ad hoc groups," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2004, pp. 609–626.

[85] Q. Wu, W. Susilo, Y. Mu, and F. Zhang, "Ad hoc group signatures," in Advances in Information and Computer Security, H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, and S. Kawamura, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 120–135.

[86] A. Debnath, P. Singaravelu, and S. Verma, "Privacy in wireless sensor networks using ring signature," Journal of King Saud University-Computer and Information Sciences, vol. 26, no. 2, pp. 228–236, 2014.

[87] N. Vance, D. Y. Zhang, Y. Zhang, and D. Wang, "Privacy-aware edge computing in social sensing applications using ring signatures," in 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). IEEE, 2018, pp. 755–762.

[88] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for iot," Sensors, vol. 19, no. 2, p. 326, 2019.

[89] J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Online/offline ring signature scheme," in International Conference on Information and Communications Security. Springer, 2009, pp. 80–90.

[90] X. Yang, W. Wu, J. K. Liu, and X. Chen, "Lightweight anonymous authentication for ad hoc group: A ring signature approach," in International Conference on Provable Security. Springer, 2015, pp. 215–226.

[91] S. Noether, A. Mackenzie et al., "Ring confidential transactions," Ledger, vol. 1, pp. 1–18, 2016.

[92] J. L. Camenisch, J.-M. Piveteau, and M. A. Stadler, "Blind signatures based on the discrete logarithm problem," in Workshop on the Theory and Application of of Cryptographic Techniques. Springer, 1994, pp. 428–432.

[93] M. Stadler, J.-M. Piveteau, and J. Camenisch, "Fair blind signatures," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1995, pp. 209–219.

[94] M. Abe and E. Fujisaki, "How to date blind signatures," in International Conference on the Theory and Application of Cryptology and Information Security. Springer, 1996, pp. 244–251.

[95] F. Zhang and K. Kim, "Id-based blind signature and ring signature from pairings," in International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2002, pp. 533–547.

[96] S. Brands, Rethinking public key infrastructures and digital certificates: building in privacy. Mit Press, 2000.

[97] E. R. Verheul, "Self-blindable credential certificates from the weil pairing," in International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2001, pp. 533–551.

[98] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2001, pp. 93–118.

[99] M. Chase, S. Meiklejohn, and G. Zaverucha, "Algebraic macs and keyed-verification anonymous credentials," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014, pp. 1205–1216.

[100] J. Hajny, P. Dzurenda, and L. Malina, "Attribute-based credentials with cryptographic collusion prevention," Security and Communication Networks, vol. 8, no. 18, pp. 3836–3846, 2015.

[101] S. Ringers, E. Verheul, and J.-H. Hoepman, "An efficient self-blindable attribute-based credential scheme," in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp. 3–20.

[102] J. Camenisch, M. Drijvers, P. Dzurenda, and J. Hajny, "Fast keyed-verification anonymous credentials on standard smart cards," in IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, 2019, pp. 286–298.

[103] J. Camenisch, M. Drijvers, and J. Hajny, "Scalable revocation scheme for anonymous credentials based on n-times unlinkable proofs," in Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society. ACM, 2016, pp. 123–133.

[104] I. Chatzigiannakis, A. Vitaletti, and A. Pyrgelis, "A privacy-preserving smart parking system using an iot elliptic curve based security platform," Computer Communications, vol. 89, pp. 165–177, 2016.

[105] I. O. for Standardization, "Iso/iec 29191:2012 information technology - security techniques - requirements for partially anonymous, partially unlinkable authentication. stage 90.93," International Organization for Standardization. Geneva, Switzerland.

[106] ——, "Iso/iec 20009-2:2013 information technology - security techniques - anonymous entity authentication - part 2: Mechanisms based on signatures using a group public key. stage 90.93," International Organization for Standardization. Geneva, Switzerland, pp. 0–51, 2013.

[107] ——, "Iso/iec cd 20009-3 information security - anonymous entity authentication - part 3: Mechanisms based on blind signatures. stage 30.60," International Organization for Standardization. Geneva, Switzerland, now under development.

[108] J. Kilian and E. Petrank, "Identity escrow," in Annual International Cryptology Conference. Springer, 1998, pp. 169–185.

[109] D. Chaum, "Untraceable electronic mail, return addresses and digital pseudonyms," in Secure electronic voting. Springer, 2003, pp. 211–219.

[110] G. Danezis, R. Dingledine, and N. Mathewson, "Mixminion: Design of a type iii anonymous remailer protocol," in 2003 Symposium on Security and Privacy, 2003. IEEE, 2003, pp. 2–15.

[111] U. Möller, L. Cottrell, P. Palfrader, and L. Sassaman, "Mixmaster protocolâĂŤversion 2," Draft, July, vol. 154, p. 28, 2003.

[112] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second. IEEE, 2004, pp. 127–131.

[113] O. Pereira and R. L. Rivest, "Marked mix-nets," in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp. 353–369.

[114] D. Chaum, D. Das, F. Javani, A. Kate, A. Krasnova, J. De Ruiter, and A. T. Sherman, "cmix: Mixing with minimal real-time asymmetric cryptographic operations," in International Conference on Applied Cryptography and Network Security. Springer, 2017, pp. 557–578.

[115] U. Sarfraz, M. Alam, S. Zeadally, and A. Khan, "Privacy aware iota ledger: Decentralized mixing and unlinkable iota transactions," Computer Networks, vol. 148, pp. 361–372, 2019.

[116] D. M. Goldschlag, M. G. Reed, and P. F. Syverson, "Hiding routing information," in International workshop on information hiding. Springer, 1996, pp. 137–150.

[117] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous connections and onion routing," IEEE Journal on Selected areas in Communications, vol. 16, no. 4, pp. 482–494, 1998.

[118] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," Naval Research Lab Washington DC, Tech. Rep., 2004.

[119] J. Reardon and I. Goldberg, "Improving tor using a tcp-over-dtls tunnel," in Proceedings of the 18th conference on USENIX security symposium. USENIX Association, 2009, pp. 119–134.

[120] J. Hiller, J. Pennekamp, M. Dahlmanns, M. Henze, A. Panchenko, and K. Wehrle, "Tailoring onion routing to the internet of things: Security and privacy in untrusted environments," in IEEE ICNP, 2019.

[121] M. Cunche, "I know your MAC address: targeted tracking of individual using Wi-Fi," Journal of Computer Virology and Hacking Techniques, 10(4): 219âĂŞ227, Dec. 2013.

[122] M. Cunche, M. A. Kaafar, and R. Boreli, "Linking wireless devices using information contained in Wi-Fi probe requests," Pervasive and Mobile Computing, pp. 56–69, 2013.

[123] B. Greenstein, R. Gummadi, J. Pang, M. Y. Chen, T. Kohno, S. Seshan, and D. Wetherall, "Can ferris bueller still have his day off? protecting privacy in the wireless era," in 11th USENIX Workshop on Hot Topics in Operating Systems (HOTOS'07). USENIX Association, 2007.

[124] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless lan through disposable interface identifiers: a quantitative analysis," Mobile Networks and Applications, vol. 10, no. 3, pp. 315–325, 2005.

[125] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1999, pp. 223–238.

[126] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[127] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE transactions on information theory, vol. 31, no. 4, pp. 469–472, 1985.

[128] I. Damgård, V. Pastro, N. Smart, and S. Zakarias, "Multiparty Computation from Somewhat Homomorphic Encryption," in Advances in Cryptology – CRYPTO 2012, 2012, pp. 643–662.

[129] D. Boneh, C. Gentry, S. Halevi, F. Wang, and D. J. Wu, "Private Database Queries Using Somewhat Homomorphic Encryption," in Applied Cryptography and Network Security, 2013, pp. 102–118.

[130] R. L. Rivest, L. Adleman, M. L. Dertouzos et al., "On data banks and privacy homomorphisms," Foundations of secure computation, vol. 4, no. 11, pp. 169–180, 1978.

[131] N. P. Smart and F. Vercauteren, "Fully homomorphic encryption with relatively small key and ciphertext sizes," in International Workshop on Public Key Cryptography. Springer, 2010, pp. 420–443.

[132] M. Albrecht, M. Chase, H. Chen, J. Ding, S. Goldwasser, S. Gorbunov, S. Halevi, J. Hoffstein, K. Laine, K. Lauter, S. Lokam, D. Micciancio, D. Moody, T. Morrison, A. Sahai, and V. Vaikuntanathan, "Homomorphic encryption security standard," HomomorphicEncryption.org, Toronto, Canada, Tech. Rep., November 2018.

[133] F. Han, J. Qin, and J. Hu, ""secure searches in the cloud: A survey"," Future Generation Computer Systems, vol. 62, pp. 66 – 75, 2016.

[134] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proceeding 2000 IEEE Symposium on Security and Privacy. S P 2000, May 2000, pp. 44–55.

[135] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS '06, 2006, p. 79âĂŞ88.

[136] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption with Keyword Search," in Advances in Cryptology - EUROCRYPT 2004, 2004, pp. 506–522.

[137] T. Fuhr and P. Paillier, "Decryptable searchable encryption," in Provable Security, 2007, pp. 228–236.

[138] N. H. Sultan, N. Kaaniche, M. Laurent, and F. A. Barbhuiya, "Authorized Keyword Search over Outsourced Encrypted Data in Cloud Environment," IEEE Transactions on Cloud Computing, pp. 1–1, 2019.

[139] J. Fu, Y. Liu, H. Chao, B. K. Bhargava, and Z. Zhang, "Secure data storage and searching for industrial iot by integrating fog computing and

cloud computing," IEEE Transactions on Industrial Informatics, vol. 14, no. 10, pp. 4519–4528, 2018.
[140] B. Chen, L. Wu, N. Kumar, K. R. Choo, and D. He, "Lightweight searchable public-key encryption with forward privacy over iiot outsourced data," IEEE Transactions on Emerging Topics in Computing, pp. 1–1, 2019.
[141] R. Zhou, X. Zhang, X. Du, X. Wang, G. Yang, and M. Guizani, "File-centric multi-key aggregate keyword searchable encryption for industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3648–3658, 2018.
[142] Y. Lu, J. Li, and Y. Zhang, "Privacy-preserving and pairing-free multirecipient certificateless encryption with keyword search for cloud-assisted iiot," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 2553–2562, 2020.
[143] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques, 2005, pp. 457–473.
[144] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS '06, 2006, pp. 89–98.
[145] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in 2007 IEEE Symposium on Security and Privacy (SP '07), May 2007, pp. 321–334.
[146] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7, pp. 1735–1744, July 2014.
[147] N. H. Sultan, F. A. Barbhuiya, and M. Laurent, "Icauth: A secure and scalable owner delegated inter-cloud authorization," Future Generation Computer Systems, vol. 88, pp. 319 – 332, 2018.
[148] Y. Jin, C. Tian, H. He, and F. Wang, "A secure and lightweight data access control scheme for mobile cloud computing," in 2015 IEEE Fifth International Conference on Big Data and Cloud Computing, Aug 2015, pp. 172–179.
[149] J. Long, K. Zhang, X. Wang, and H.-N. Dai, "Lightweight Distributed Attribute Based Keyword Search System for Internet of Things," in Security, Privacy, and Anonymity in Computation, Communication, and Storage, 2019, pp. 253–264.
[150] N. H. Sultan, F. A. Barbhuiya, and N. Sarma, "Scauth: Selective cloud user authorization for ciphertext-policy attribute-based access control," in 2017 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 2017, pp. 93–98.
[151] N. H. Sultan, F. A. Barbhuiya, and N. Sarma, "A Universal Cloud User Revocation Scheme with Key-escrow Resistance for Ciphertext-policy Attribute-based Access Control," in Proceedings of the 10th International Conference on Security of Information and Networks, ser. SIN '17, 2017, pp. 11–18.
[152] S. Tan, K. Yeow, and S. O. Hwang, "Enhancement of a Lightweight Attribute-Based Encryption Scheme for the Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6384–6395, Aug 2019.
[153] L. Cheng, J. Liu, G. Xu, Z. Zhang, H. Wang, H. Dai, Y. Wu, and W. Wang, "Sctsc: A semicentralized traffic signal control mode with attribute-based blockchain in iovs," IEEE Transactions on Computational Social Systems, pp. 1–10, 2019.
[154] H. Xiong, Y. Zhao, L. Peng, H. Zhang, and K.-H. Yeh, "Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing," Future Generation Computer Systems, vol. 97, pp. 453 – 461, 2019.
[155] W. Du and M. J. Atallah, "Secure Multi-party Computation Problems and Their Applications: A Review and Open Problems," in Proceedings of the 2001 Workshop on New Security Paradigms, ser. NSPW '01, 2001, pp. 13–22.
[156] A. C. Yao, "Protocols for Secure Computations," in Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, ser. SFCS '82, 1982, pp. 160–164.
[157] D. Chaum, C. Crépeau, and I. Damgard, "Multiparty Unconditionally Secure Protocols," in Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, ser. STOC '88, 1988, pp. 11–19.
[158] T. Rabin and M. Ben-Or, "Verifiable Secret Sharing and Multiparty Protocols with Honest Majority," in Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing, ser. STOC '89, 1989, pp. 73–85.
[159] A. Ben-David, N. Nisan, and B. Pinkas, "FairplayMP: A System for Secure Multi-party Computation," in Proceedings of the 15th ACM Conference on Computer and Communications Security, ser. CCS '08, 2008, pp. 257–266.
[160] A. B. Alexandru and G. J. Pappas, "Secure Multi-party Computation for Cloud-based Control," arXiv e-prints, p. arXiv:1906.09652, Jun 2019.
[161] M. A. Mustafa, S. Cleemput, A. Aly, and A. Abidin, "A Secure and Privacy-preserving Protocol for Smart Metering Operational Data Collection," IEEE Transactions on Smart Grid, pp. 1–1, 2019.
[162] L. Li, R. Lu, K.-K. R. Choo, A. Datta, and J. Shao, "Privacy-preserving-outsourced association rule mining on vertically partitioned databases," IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1847–1861, 2016.
[163] J.-J. Yang, J.-Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Future Generation Computer Systems, vol. 43, pp. 74–86, 2015.
[164] J. Domingo-Ferrer, S. Ricci, and C. Domingo-Enrich, "Outsourcing scalar products and matrix products on privacy-protected unencrypted data stored in untrusted clouds," Information Sciences, vol. 436, pp. 320–342, 2018.
[165] J. Domingo-Ferrer and V. Torra, "A critique of k-anonymity and some of its enhancements," in 2008 Third International Conference on Availability, Reliability and Security, 2008, pp. 990–993.
[166] A. Campan, T. M. Truta, and N. Cooper, "P-sensitive k-anonymity with generalization constraints," Trans. Data Privacy, vol. 3, no. 2, pp. 65–89, 2010.
[167] J. Domingo-Ferrer, S. Ricci, and J. Soria-Comas, "A methodology to compare anonymization methods regarding their risk-utility trade-off," in Modeling Decisions for Artificial Intelligence - 14th International Conference, 2017, pp. 132–143.
[168] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in Theory of Cryptography Conference. Springer, 2006.
[169] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," Found. Trends Theor. Comput. Sci., vol. 9, pp. 211–407, 2014.
[170] C. Clifton and T. Tassa, "On syntactic anonymity and differential privacy," Trans. Data Privacy, vol. 6, no. 2, pp. 161–183, 2013.
[171] N. Li, W. H. Qardaji, and D. Su, "On sampling, anonymization, and differential privacy or, k-anonymization meets differential privacy," in 7th ACM Symposium on Information, Compuer and Communications Security, 2012, pp. 32–33.
[172] N. Holohan, S. Antonatos, S. Braghin, and P. M. Aonghusa, "(k, ϵ)-anonymity: k-anonymity with ϵ-differential privacy," http://arxiv.org/abs/1710.01615, 2017.
[173] J. Domingo-Ferrer and J. Soria-Comas, "From t-closeness to differential privacy and vice versa in data anonymization," Knowledge-Based Systems, vol. 74, pp. 151–158, 2015.
[174] J. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila, "Frodo: Take off the ring! practical, quantum-secure key exchange from lwe," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016, pp. 1006–1018.
[175] J. Hoffstein, J. Pipher, and J. H. Silverman, "Ntru: A ring-based public key cryptosystem," in International Algorithmic Number Theory Symposium. Springer, 1998, pp. 267–288.
[176] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange-a new hope." in USENIX Security Symposium, vol. 2016, 2016.
[177] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-kyber: a cca-secure module-lattice-based kem," in 2018 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2018.
[178] J. Patarin, "Hidden fields equations (hfe) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1996, pp. 33–48.
[179] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1999, pp. 206–222.
[180] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," in International Conference on Applied Cryptography and Network Security. Springer, 2005, pp. 164–175.
[181] J.-M. Chen and B.-Y. Yang, "A more secure and efficacious tts signature scheme," in International Conference on Information Security and Cryptology. Springer, 2003, pp. 320–338.

[182] R. C. Merkle, "A certified digital signature," in Conference on the Theory and Application of Cryptology. Springer, 1989, pp. 218–238.

[183] L. Lamport, "Constructing digital signatures from a one-way function," Technical Report CSL-98, SRI International Palo Alto, Tech. Rep., 1979.

[184] R. J. Mceliece, "A public-key cryptosystem based on algebraic," Coding Thv, vol. 4244, pp. 114–116, 1978.

[185] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory," Prob. Control and Inf. Theory, vol. 15, no. 2, pp. 159–166, 1986.

[186] D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," in International Workshop on Post-Quantum Cryptography. Springer, 2011, pp. 19–34.

[187] R. Azarderakhsh, M. Campagna, C. Costello, L. Feo, B. Hess, A. Jalali, D. Jao, B. Koziel, B. LaMacchia, P. Longa et al., "Supersingular isogeny key encapsulation," Submission to the NIST Post-Quantum Standardization project, 2017.

[188] D. J. Bernstein, "Introduction to post-quantum cryptography," in Post-quantum cryptography. Springer, 2009, pp. 1–14.

[189] ——, "Post-quantum cryptography," Encyclopedia of Cryptography and Security, pp. 949–950, 2011.

[190] N. Sendrier, "Code-based cryptography: State of the art and perspectives," IEEE Security & Privacy, vol. 15, no. 4, pp. 44–50, 2017.

[191] D. Butin, "Hash-based signatures: State of play," IEEE Security & Privacy, vol. 15, no. 4, pp. 37–43, 2017.

[192] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, no. 7779, pp. 505–510, 2019.

[193] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y.-K. Liu, C. Miller, D. Moody, R. Peralta et al., "Status report on the second round of the nist post-quantum cryptography standardization process," NIST, Tech. Rep., July, 2020.

[194] M. J. Kannwischer, J. Rijneveld, P. Schwabe, and K. Stoffelen, pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4. [Sl]: CSRC, 2019.

[195] A. Boorghany and R. Jalili, "Implementation and comparison of lattice-based identification protocols on smart cards and microcontrollers." IACR Cryptology ePrint Archive, vol. 2014, p. 78, 2014.

[196] O. M. Guillen, T. Pöppelmann, J. M. B. Mera, E. F. Bongenaar, G. Sigl, and J. Sepulveda, "Towards post-quantum security for iot endpoints with ntru," in Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017. IEEE, 2017, pp. 698–703.

[197] R. Xu, C. Cheng, Y. Qin, and T. Jiang, "Lighting the way to a smart world: Lattice-based cryptography for internet of things," arXiv preprint arXiv:1805.04880, 2018.

[198] L. Malina, S. Ricci, P. Dzurenda, D. Smekal, J. Hajny, and T. Gerlich, "Towards practical deployment of post-quantum cryptography on constrained platforms and hardware-accelerated platforms," in International Conference on Information Technology and Communications Security. Springer, 2019, pp. 109–124.

[199] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Software and hardware implementation of lattice-cased cryptography schemes," University of California Irvine, CECS TR 17, vol. 4, 2017.

[200] T. Pöppelmann, T. Oder, and T. Güneysu, "High-performance ideal lattice-based cryptography on 8-bit atxmega microcontrollers," in International Conference on Cryptology and Information Security in Latin America. Springer, 2015, pp. 346–365.

[201] M.-J. O. Saarinen, "Ring-lwe ciphertext compression and error correction: Tools for lightweight post-quantum cryptography," in Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security. Acm, 2017, pp. 15–22.

[202] M. R. Albrecht, C. Hanser, A. Hoeller, T. Pöppelmann, F. Virdia, and A. Wallner, "Implementing rlwe-based schemes using an rsa co-processor," IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 169–208, 2019.

[203] L. Botros, M. J. Kannwischer, and P. Schwabe, "Memory-efficient high-speed implementation of kyber on cortex-m4," in International Conference on Cryptology in Africa. Springer, 2019, pp. 209–228.

[204] E. Alkim, P. Jakubeit, and P. Schwabe, "Newhope on arm cortex-m," in International Conference on Security, Privacy, and Applied Cryptography Engineering. Springer, 2016, pp. 332–349.

[205] H. Cheng, J. Groszschädl, P. Roenne, and P. Ryan, "A lightweight implementation of ntruencrypt for 8-bit avr microcontrollers," 2019.

[206] B.-Y. Yang, C.-M. Cheng, B.-R. Chen, and J.-M. Chen, "Implementing minimized multivariate pkc on low-resource embedded systems," in International Conference on Security in Pervasive Computing. Springer, 2006, pp. 73–88.

[207] P. Czypek, S. Heyse, and E. Thomae, "Efficient implementations of mqpks on constrained devices," in International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2012, pp. 374–389.

[208] K.-A. Shim, C.-M. Park, N. Koo, and H. Seo, "A high-speed public-key signature scheme for 8-bit iot constrained devices," IEEE Internet of Things Journal, 2020.

[209] J. Moya Riera, "Performance analysis of rainbow on arm cortex-m4," B.S. thesis, Universitat Politècnica de Catalunya, 2019.

[210] H. Seo, Z. Liu, P. Longa, and Z. Hu, "Sidh on arm: faster modular multiplications for faster post-quantum supersingular isogeny key exchange," IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 1–20, 2018.

[211] R. Azarderakhsh, D. Fishbein, and D. Jao, "Efficient implementations of a quantum-resistant key-exchange protocol on embedded systems," Citeseer, 2014.

[212] C. Costello, P. Longa, and M. Naehrig, "Sike round 2 speed record on arm cortex-m4," in SIDH Library. [Online]. Available: https://github.com/Microsoft/PQCrypto-SIDH,2016-2018

[213] B. Koziel, A. Jalali, R. Azarderakhsh, D. Jao, and M. Mozaffari-Kermani, "Neon-sidh: efficient implementation of supersingular isogeny diffie-hellman key exchange protocol on arm," in International Conference on Cryptology and Network Security. Springer, 2016, pp. 88–103.

[214] A. Jalali, R. Azarderakhsh, M. M. Kermani, and D. Jao, "Supersingular isogeny diffie-hellman key exchange on 64-bit arm," IEEE Transactions on Dependable and Secure Computing, 2017.

[215] P. Koppermann, E. Pop, J. Heyszl, and G. Sigl, "18 seconds to key exchange: Limitations of supersingular isogeny diffie-hellman on embedded devices," Cryptology ePrint Archive, Report 2018/932, 2018, https://eprint.iacr.org/2018/932.

[216] H. Seo, A. Jalali, and R. Azarderakhsh, "Sike round 2 speed record on arm cortex-m4," in International Conference on Cryptology and Network Security. Springer, 2019, pp. 39–60.

[217] S. Rohde, T. Eisenbarth, E. Dahmen, J. Buchmann, and C. Paar, "Fast hash-based signatures on constrained devices," in International Conference on Smart Card Research and Advanced Applications. Springer, 2008, pp. 104–117.

[218] G. C. Pereira, C. Puodzius, and P. S. Barreto, "Shorter hash-based signatures," Journal of Systems and Software, vol. 116, pp. 95–100, 2016.

[219] F. Strenzke, "A smart card implementation of the mceliece pkc," in IFIP International Workshop on Information Security Theory and Practices. Springer, 2010, pp. 47–59.

[220] S. Heyse, I. Von Maurich, and T. Güneysu, "Smaller keys for code-based cryptography: Qc-mdpc mceliece implementations on embedded devices," in International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2013, pp. 273–292.

[221] M. Bischof, T. Oder, and T. Güneysu, "Efficient microcontroller implementation of bike," in International Conference on Information Technology and Communications Security. Springer, 2019, pp. 34–49.

[222] Z. Liu, H. Seo, S. S. Roy, J. Großschädl, H. Kim, and I. Verbauwhede, "Efficient ring-lwe encryption on 8-bit avr processors," in International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2015, pp. 663–682.

[223] O. M. Guillen, T. Pöppelmann, J. M. B. Mera, E. F. Bongenaar, G. Sigl, and J. Sepulveda, "Towards post-quantum security for iot endpoints with ntru," in Proceedings of the Conference on Design, Automation & Test in Europe, ser. DATE '17. 3001 Leuven, Belgium, Belgium: European Design and Automation Association, 2017, pp. 698–703.

[224] T. Güneysu, M. Krausz, T. Oder, and J. Speith, "Evaluation of lattice-based signature schemes in embedded systems," in 2018 25th IEEE International Conference on Electronics, Circuits and Systems (ICECS). IEEE, 2018, pp. 385–388.

[225] T. Oder, J. Speith, K. Höltgen, and T. Güneysu, "Towards practical microcontroller implementation of the signature scheme falcon," in International Conference on Post-Quantum Cryptography. Springer, 2019, pp. 65–80.

[226] S. D. Gordon, J. Katz, and V. Vaikuntanathan, "A group signature scheme from lattice assumptions," in International Conference on the Theory and

Application of Cryptology and Information Security. Springer, 2010, pp. 395–412.
[227] F. Benhamouda, J. Camenisch, S. Krenn, V. Lyubashevsky, and G. Neven, "Better zero-knowledge proofs for lattice encryption and their application to group signatures," in International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2014, pp. 551–572.
[228] P. Q. Nguyen, J. Zhang, and Z. Zhang, "Simpler efficient group signatures from lattices," in IACR International Workshop on Public Key Cryptography. Springer, 2015, pp. 401–426.
[229] M. F. Ezerman, H. T. Lee, S. Ling, K. Nguyen, and H. Wang, "Provably secure group signature schemes from code-based assumptions," IEEE Transactions on Information Theory, 2020.
[230] D. Zheng, X. Li, and K. Chen, "Code-based ring signature scheme." IJ Network Security, vol. 5, no. 2, pp. 154–157, 2007.
[231] P.-L. Cayrel, R. Lindner, M. Rückert, and R. Silva, "A lattice-based threshold ring signature scheme," in International Conference on Cryptology and Information Security in Latin America. Springer, 2010, pp. 255–272.
[232] B. Libert, S. Ling, K. Nguyen, and H. Wang, "Zero-knowledge arguments for lattice-based accumulators: logarithmic-size ring signatures and group signatures without trapdoors," in Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2016, pp. 1–31.
[233] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in Advances in Cryptology — ASIACRYPT 2001, C. Boyd, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 552–565.
[234] C. Baum, H. Lin, and S. Oechsner, "Towards practical lattice-based one-time linkable ring signatures," in International Conference on Information and Communications Security. Springer, 2018, pp. 303–322.
[235] A. Petzoldt, S. Bulygin, and J. Buchmann, "A multivariate based threshold ring signature scheme," Applicable Algebra in Engineering, Communication and Computing, vol. 24, no. 3-4, pp. 255–275, 2013.
[236] M. S. E. Mohamed, A. Petzoldt, and C. RingRainbow, "Efficient multivariate ring signature schemes." IACR Cryptology ePrint Archive, vol. 2017, p. 247, 2017.
[237] M. Rückert, "Lattice-based blind signatures," in International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2010, pp. 413–430.
[238] A. Petzoldt, A. Szepieniec, and M. S. E. Mohamed, "A practical multivariate blind signature scheme," in International conference on financial cryptography and data security. Springer, 2017, pp. 437–454.
[239] O. Blazy, P. Gaborit, J. Schrek, and N. Sendrier, "A code-based blind signature," in 2017 IEEE International Symposium on Information Theory (ISIT). IEEE, 2017, pp. 2718–2722.
[240] M. S. Srinath and V. Chandrasekaran, "Isogeny-based quantum-resistant undeniable blind signature scheme." IACR Cryptology ePrint Archive, vol. 2016, p. 148, 2016.
[241] H. Zhu, Y.-a. Tan, X. Zhang, L. Zhu, C. Zhang, and J. Zheng, "A round-optimal lattice-based blind signature scheme for cloud services," Future Generation Computer Systems, vol. 73, pp. 106–114, 2017.
[242] J. Camenisch, G. Neven, and M. Rückert, "Fully anonymous attribute tokens from lattices," in International Conference on Security and Cryptography for Networks. Springer, 2012, pp. 57–75.
[243] C. Boschini, J. Camenisch, and G. Neven, "Relaxed lattice-based signatures with short zero-knowledge proofs," in International Conference on Information Security. Springer, 2018, pp. 3–22.
[244] R. Yang, M. H. Au, Z. Zhang, Q. Xu, Z. Yu, and W. Whyte, "Efficient lattice-based zero-knowledge arguments with standard soundness: construction and applications," in Annual International Cryptology Conference. Springer, 2019, pp. 147–175.
[245] N. Costa, R. Martínez, and P. Morillo, "Lattice-based proof of a shuffle." IACR Cryptology ePrint Archive, vol. 2019, p. 357, 2019.
[246] X. Boyen, T. Haines, and J. Müller, "A verifiable and practical lattice-based decryption mix net with external auditing," 2020.
[247] C. Gentry et al., "Fully homomorphic encryption using ideal lattices." in Stoc, vol. 9, no. 2009, 2009, pp. 169–178.
[248] C. Gentry and D. Boneh, A fully homomorphic encryption scheme. Stanford University Stanford, 2009, vol. 20, no. 09.
[249] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(leveled) fully homomorphic encryption without bootstrapping," ACM Transactions on Computation Theory (TOCT), vol. 6, no. 3, p. 13, 2014.
[250] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) lwe," SIAM Journal on Computing, vol. 43, no. 2, pp. 831–871, 2014.
[251] A. Bogdanov and C. H. Lee, "Homomorphic encryption from codes," arXiv preprint arXiv:1111.4301, 2011.
[252] J. Xu, L. Wei, Y. Zhang, A. Wang, F. Zhou, and C.-z. Gao, "Dynamic fully homomorphic encryption-based merkle tree for lightweight streaming authenticated data structures," Journal of Network and Computer Applications, vol. 107, pp. 113–124, 2018.
[253] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène, "Tfhe: Fast fully homomorphic encryption over the torus," Journal of Cryptology, pp. 1–58, 2018.
[254] J. Zhang, B. Deng, and X. Li, "Learning with error based searchable encryption scheme," Journal of Electronics (China), vol. 29, no. 5, pp. 473–476, 2012.
[255] Y. Yang and M. Ma, "Semantic searchable encryption scheme based on lattice in quantum-era," 2016. [Online]. Available: http://jise.iis.sinica.edu.tw/JISESearch/pages/View/PaperSearch.jsf?searchBy=TITLE&title=Semantic+Searchable+Encryption+Scheme+based+on+Lattice+in+Quantum-era
[256] R. Behnia, M. O. Ozmen, and A. A. Yavuz, "Lattice-based public key searchable encryption from experimental perspectives," IEEE Transactions on Dependable and Secure Computing, 2018.
[257] X. Boyen, "Attribute-based functional encryption on lattices," in Theory of Cryptography Conference. Springer, 2013, pp. 122–142.
[258] S. Agrawal, X. Boyen, V. Vaikuntanathan, P. Voulgaris, and H. Wee, "Functional encryption for threshold functions (or fuzzy ibe) from lattices," in International Workshop on Public Key Cryptography. Springer, 2012, pp. 280–297.
[259] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, "Efficient attribute-based encryption from r-lwe," Chin. J. Electron, vol. 23, no. 4, pp. 778–782, 2014.
[260] A. López-Alt, E. Tromer, and V. Vaikuntanathan, "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption," in Proceedings of the forty-fourth annual ACM symposium on Theory of computing, 2012, pp. 1219–1234.
[261] J. Buchmann, N. Büscher, F. Göpfert, S. Katzenbeisser, J. Krämer, D. Micciancio, S. Siim, C. van Vredendaal, and M. Walter, "Creating cryptographic challenges using multi-party computation: The lwe challenge," in Proceedings of the 3rd ACM International Workshop on ASIA Public-Key Cryptography, 2016, pp. 11–20.
[262] E. Kim, H.-S. Lee, and J. Park, "Towards round-optimal secure multiparty computations: Multikey fhe without a crs," International Journal of Foundations of Computer Science, vol. 31, no. 02, pp. 157–174, 2020.
[263] J. Camenisch et al., "Specification of the identity mixer cryptographic library," Tech. rep, Tech. Rep., 2010.
[264] C. Paquin, "U-prove technology overview v1.1 (revision 2)," Microsoft Corporation Draft Revision, vol. 1, 2013.
[265] C.-C. Lee, P.-F. Ho, and M.-S. Hwang, "A secure e-auction scheme based on group signatures," Information Systems Frontiers, vol. 11, no. 3, pp. 335–343, 2009.
[266] L. Malina, A. Vives-Guasch, J. Castellà-Roca, A. Viejo, and J. Hajny, "Efficient group signatures for privacy-preserving vehicular networks," Telecommunication Systems, vol. 58, no. 4, pp. 293–311, 2015.
[267] P. P. Tsang and V. K. Wei, "Short linkable ring signatures for e-voting, e-cash and attestation," in International Conference on Information Security Practice and Experience. Springer, 2005, pp. 48–60.
[268] W.-J. Tsaur, J.-H. Tsao, and Y.-H. Tsao, "An efficient and secure ecc-based partially blind signature scheme with multiple banks issuing e-cash payment applications," in Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE). The Steering Committee of The World Congress in Computer Science, Computer âĂę, 2018, pp. 94–100.
[269] S. Ibrahim, M. Kamat, M. Salleh, and S. R. A. Aziz, "Secure e-voting with blind signature," in 4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings. IEEE, 2003, pp. 193–197.
[270] J. Hajny, P. Dzurenda, and L. Malina, "Attribute-based credentials with cryptographic collusion prevention," Security and Communication Networks, vol. 8, no. 18, pp. 3836–3846, 2015.
[271] J. Camenisch and E. Van Herreweghen, "Design and implementation of the idemix anonymous credential system," in Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002, pp. 21–30.

[272] G. Alpár, F. van den Broek, B. Hampiholi, B. Jacobs, W. Lueks, and S. Ringers, "Irma: practical, decentralized and privacy-friendly identity management using smartphones," in 10th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2017), 2017.

[273] V. Mai and I. Khalil, "Design and implementation of a secure cloud-based billing model for smart meters as an internet of things using homomorphic cryptography," Future Generation Computer Systems, vol. 72, pp. 327–338, 2017.

[274] O. Kocabas and T. Soyata, "Towards privacy-preserving medical cloud computing using homomorphic encryption," in Virtual and Mobile Healthcare: Breakthroughs in Research and Practice. IGI Global, 2020, pp. 93–125.

[275] T. Hoang, A. A. Yavuz, and J. Guajardo Merchan, "A secure searchable encryption framework for privacy-critical cloud storage services," IEEE Transactions on Services Computing, pp. 1–1, 2019.

[276] D. W. Archer, D. Bogdanov, Y. Lindell, L. Kamm, K. Nielsen, J. I. Pagter, N. P. Smart, and R. N. Wright, "From Keys to Databases-Real-World Applications of Secure Multi-Party Computation," The Computer Journal, vol. 61, no. 12, pp. 1749–1771, 09 2018.

[277] R. Tso, A. Alelaiwi, S. M. M. Rahman, M.-E. Wu, and M. S. Hossain, "Privacy-preserving data communication through secure multi-party computation in healthcare sensor cloud," Journal of Signal Processing Systems, vol. 89, no. 1, pp. 51–59, 2017.

[278] Ú. Erlingsson, V. Pihur, and A. Korolova, "RAPPOR: randomized aggregatable privacy-preserving ordinal response," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014, G. Ahn, M. Yung, and N. Li, Eds. ACM, 2014, pp. 1054–1067.

[279] N. M. Johnson, J. P. Near, and D. Song, "Towards practical differential privacy for SQL queries," Proc. VLDB Endow., vol. 11, no. 5, pp. 526–539, 2018.

[280] D. Boneh, S. Eskandarian, and B. Fisch, "Post-quantum epid signatures from symmetric primitives," in Cryptographers' Track at the RSA Conference. Springer, 2019, pp. 251–271.

[281] M. Diaz, H. Wang, F. du Pin Calmon, and L. Sankar, "On the robustness of information-theoretic privacy measures and mechanisms," IEEE Trans. Inf. Theory, vol. 66, no. 4, pp. 1949–1978, 2020.

[282] F. K. Dankar and K. E. Emam, "Practicing differential privacy in health care: A review," Trans. Data Privacy, vol. 6, no. 1, pp. 35–67, 2013.

[283] M. Fredrikson, E. Lantz, S. Jha, S. Lin, D. Page, and T. Ristenpart, "Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing," in Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20-22, 2014., 2014, pp. 17–32.

[284] M. Backes, N. Döttling, L. Hanzlik, K. Kluczniak, and J. Schneider, "Ring signatures: Logarithmic-size, no setup-from standard assumptions," in Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2019, pp. 281–311.

[285] J. Zhang, W. Bai, and Z. Jiang, "On the security of a practical constant-size ring signature scheme." IJ Network Security, vol. 22, no. 3, pp. 392–396, 2020.

[286] D. Dharminder and D. Mishra, "Lcppa: Lattice-based conditional privacy preserving authentication in vehicular communication," Transactions on Emerging Telecommunications Technologies, vol. 31, no. 2, p. e3810, 2020, e3810 ett.3810. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3810

[287] G. Cormode, S. Jha, T. Kulkarni, N. Li, D. Srivastava, and T. Wang, "Privacy at scale: Local differential privacy in practice," in Proceedings of the 2018 International Conference on Management of Data, SIGMOD Conference 2018, Houston, TX, USA, June 10-15, 2018, G. Das, C. M. Jermaine, and P. A. Bernstein, Eds. ACM, 2018, pp. 1655–1658.

[288] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," IEEE Trans. Info. For. and Sec., vol. 8, no. 12, pp. 1947–1960, Dec 2013.

[289] Y. Zhu, G. Ahn, H. Hu, D. Ma, and S. Wang, "Role-based cryptosystem: A new cryptographic RBAC system based on role-key hierarchy," IEEE Trans. Info. For. and Sec., vol. 8, no. 12, pp. 2138–2153, Dec 2013.

[290] J. M. M. PÃl'rez, G. M. PÃl'rez, and A. F. S. Gomez, "SecRBAC: Secure data in the Clouds," IEEE Trans. on Serv. Comp., vol. 10, no. 5, pp. 726–740, Sept 2017.

[291] N. H. Sultan, V. Varadharajan, L. Zhou, and F. A. Barbhuiya, "A role-based encryption scheme for securing outsourced cloud data in a multi-organization context," 2020, 2004.05419, arXiv, cs.CR.

[292] M. Mukherjee, M. A. Ferrag, L. Maglaras, A. Derhab, and M. Aazam, "Security and privacy issues and solutions for fog," Fog and Fogonomics: Challenges and Practices of Fog Computing, Communication, Networking, Strategy, and Economics, pp. 353–374, 2020.

[293] A. Alabdulatif, I. Khalil, and X. Yi, "Towards secure big data analytic for cloud-enabled applications with fully homomorphic encryption," Journal of Parallel and Distributed Computing, vol. 137, pp. 192–204, 2020.

[294] F. Bourse, M. Minelli, M. Minihold, and P. Paillier, "Fast homomorphic evaluation of deep discretized neural networks," in Advances in Cryptology – CRYPTO 2018, 2018, pp. 483–512.

[295] N. J. Hernandez Marcano, M. Moller, S. Hansen, and R. H. Jacobsen, "On fully homomorphic encryption for privacy-preserving deep learning," in 2019 IEEE Globecom Workshops (GC Wkshps), 2019, pp. 1–6.

[296] Q. Zhang, L. T. Yang, and Z. Chen, "Privacy preserving deep computation model on cloud for big data feature learning," IEEE Transactions on Computers, vol. 65, no. 5, pp. 1351–1362, 2016.

[297] L. T. Phong, Y. Aono, T. Hayashi, L. Wang, and S. Moriai, "Privacy-preserving deep learning via additively homomorphic encryption," IEEE Transactions on Information Forensics and Security, vol. 13, no. 5, pp. 1333–1345, 2018.

[298] P. Li, J. Li, Z. Huang, T. Li, C.-Z. Gao, S.-M. Yiu, and K. Chen, "Multi-key privacy-preserving deep learning in cloud computing," Future Generation Computer Systems, vol. 74, pp. 76 – 85, 2017.

[299] J. Li, X. Kuang, S. Lin, X. Ma, and Y. Tang, "Privacy preservation for machine learning training and classification based on homomorphic encryption schemes," Information Sciences, vol. 526, pp. 166 – 179, 2020.

[300] J. Jeony, D. Kimz, and J. Kim, "Cyclic parameter sharing for privacy-preserving distributed deep learning platforms," in 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2019, pp. 435–437.

[301] C. Garman, M. Green, and I. Miers, "Decentralized anonymous credentials." in NDSS. Citeseer, 2014.

[302] R. Yang, M. H. Au, Q. Xu, and Z. Yu, "Decentralized blacklistable anonymous credentials with reputation," Computers & Security, vol. 85, pp. 353–371, 2019.

[303] K. Singh, O. Dib, C. Huyart, and K. Toumi, "A novel credential protocol for protecting personal attributes in blockchain," Computers & Electrical Engineering, vol. 83, p. 106586, 2020.

[304] International Data Corporation (IDC), "Automation, Analytics, and Governance Power Enterprise Multicloud Management Strategies", White Paper, 2019.

[305] N. H. Sultan, M. Laurent, and V. Varadharajan, "Securing organization's data: A role-based authorized keyword search scheme with efficient decryption," 2020, 2004.10952, arXiv, cs.CR.

[306] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," IEEE Communications Surveys & Tutorials, 2020.

[307] D. Połap, G. Srivastava, A. Jolfaei, and R. M. Parizi, "Blockchain technology and neural networks for the internet of medical things," in IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2020, pp. 508–513.

[308] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188–2204, 2018.

[309] M. Hayashi and T. Tsurumaru, "More efficient privacy amplification with less random seeds via dual universal hash function," IEEE Transactions on Information Theory, vol. 62, no. 4, pp. 2213–2232, 2016.

[310] B.-Y. Tang, B. Liu, Y.-P. Zhai, C.-Q. Wu, and W.-R. Yu, "High-speed and large-scale privacy amplification scheme for quantum key distribution," Scientific reports, vol. 9, no. 1, pp. 1–8, 2019.

[311] J. Camenisch and E. Van Herreweghen, "Design and implementation of the idemix anonymous credential system," in Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002, pp. 21–30.

[312] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in International Conference on Security in Communication Networks. Springer, 2002, pp. 268–289.

[313] C. Paquin and G. Zaverucha, "U-prove cryptographic specification v1.1 (revision 3)," Technical Report, Microsoft Corporation, 2013.

LUKAS MALINA is a senior researcher at the Department of Telecommunications at Brno University of Technology (BUT), Czech Republic. He accomplished his MSc. degree with honors and obtains the Dean prize for masters thesis at BUT in 2010. He received his Ph.D. degree from BUT in 2014. His research activities focus on applied cryptography, privacy-preserving protocols and authentication systems. He has published more than 70 papers in international journals and conferences, and he has provided several invited research and teaching lectures abroad, e.g., in Finland (University of Tampere, 2013), Spain (URV Tarragona, 2015), Russia (St. Petersburg ITMO, 2017), Belgium (KU Leuven, 2017). Assoc. prof. Malina is currently involved as a taskleader in the SPARTA H2020 project (task: Privacy-by-Design) and as a senior researcher in several Czech scientific projects focused on cybersecurity.

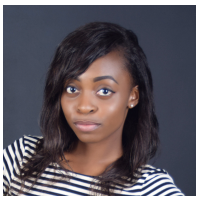
PETR DZURENDA is a postdoctoral researcher at Department of Telecommunications of the Faculty of Electrical Engineering and Communication at Brno University of Technology, Czech Republic. He received his Ph.D. degree at Brno University of Technology in 2019. His research is focused on privacy-enhancing technologies, cryptographic protocol design and protocol implementation on constrained devices in IoT area. He is author and co-author of several new privacy-friendly solutions and cryptographic schemes, such as group signatures and anonymous credentials, which are practically implementable on current smart cards. Currently, Dr. Dzurenda is involved in the SPARTA H2020 project (task: Privacy-by-Design).

SARA RICCI is a postdoctoral researcher at the Department of Telecommunications of the Faculty of Electrical Engineering and Communication at Brno University of Technology, Czech Republic. She accomplished her M.Sc. degree in Mathematics at University of Pisa in 2015, Italy and her PhD studies in Computer Engineering and Mathematics Security at Universitat Rovira i Virgili, Spain in 2018. Her research interest are theoretical cryptography, in particular lattice-based and elliptic curve cryptography, and data privacy and security. She is also focused on the design of new privacy-preserving cryptographic protocols and their security analyses. Currently, Dr. Ricci is involved in the SPARTA H2020 project.

JAN HAJNY works as an associate professor at the Faculty of Electrical Engineering and Communication at Brno University of Technology, Czech Republic. He received his Ph.D. degree at Brno University of Technology in 2012. Currently, he deals with the research into cryptographic protocols for the privacy and digital identity protection. Assoc. prof. Hajny is the co-founder and lead of the Cryptology Research Group (http://crypto.utko.feec.vutbr.cz) and is responsible for managing the Information Security study program at the university. He is the author of more than 80 scientific publications and cooperates with renowned laboratories abroad.

GAUTAM SRIVASTAVA was awarded his B.Sc. degree from Briar Cliff University in U.S.A. in the year 2004, followed by his M.Sc. and Ph.D. degrees from the University of Victoria in Victoria, British Columbia, Canada in the years 2006 and 2011, respectively. He then taught for 3 years at the University of Victoria in the Department of Computer Science, where he was regarded as one of the top undergraduate professors in the Computer Science Course Instruction at the University. From there in the year 2014, he joined a tenure-track position at Brandon University in Brandon, Manitoba, Canada, where he currently is active in various professional and scholarly activities. He was promoted to the rank Associate Professor in January 2018. Dr. G, as he is popularly known, is active in research in the field of Data Mining and Big Data. In his 8-year academic career, he has published a total of 100 papers in high-impact conferences in many countries and in high-status journals (SCI, SCIE). Dr. G currently sits as an Associate Editor for IEEE Transactions on Fuzzy Systems, IEEE Transactions on Industrial Informatics, as well as IEEE Access.

RAIMUNDAS MATULEVIČIUS received his Ph.D. diploma from the Norwegian University of Science and Technology in the computer and information science. Currently, he holds a Professor of Information Security position at the University of Tartu (Estonia). His research interests include security and privacy of information, security risk management and model-driven security. His publication record includes more than 100 articles published in the peer-reviewed journals, conference and workshops. Prof. Matulevičius has been a program committee member at international conferences (e.g., NordSec, PoEM, REFSQ, and CAiSE). He is an author of a book on "Fundamentals of Secure System Modelling" (Springer, 2017). Currently, he is involved in the SPARTA H2020 project (task: Privacy-by-Design) and is a principal researcher in few other international and national projects.



ABASI-AMEFON O. AFFIA is a junior research fellow and a doctoral student of Computer Science at the University of Tartu, Estonia. She received her Master's degree in Cyber-security from Tallinn University of Technology and the University of Tartu, Estonia. Her research interests include the security of information systems and intelligent infrastructure systems, socio-technical security and privacy analysis, and security risk management in intelligent infrastructure systems.

MARYLINE LAURENT is Full Professor with Telecom SudParis since 2004. After entering in Institut Mines-Telecom as an assistant professor in 2000, in 2013, she took the leadership of the research team R3S (Networks, Systems, Services, Security) of the SAMOVAR laboratory of Telecom SudParis, and she cofounded the multidisciplinary research chair Values and Policies of Personal Information. Since 2020, she has been directing the RST (Networks, Services, Telecommunications) department of Telecom SudParis. Her research topics are related to network security and privacy mechanisms, including protocols and functions, applied to clouds, Internet of Things and identity management. She is author of more than 100 publications in high-ranked conferences and journals, and of several books.

NAZATUL HAQUE SULTAN is a Research Associate working with CSIRO Data61, Australia and Advanced Cyber Security Engineering Research Centre (ACSRC), University of Newcastle, Australia. Prior to that, he was working as a Research and Development Engineer in the RST Department at Telecom SudParis, Institute Polytechnique de Paris, France. He also worked as a Senior Research Fellow in Govt. of India sponsored R&D projects. Nazatul received his Ph.D. from the Indian Institute of Information Technology Guwahati in November 2019. He also completed Master of Technology in Information Technology and Bachelor of Engineering in Computer Science and Engineering. His research interests include Privacy-Enhancing Technologies (PETs) and Applied Cryptography for distributed systems and decentralized architectures, i.e., IoT, Fog, Cloud, Named Data Networking (NDN), Searchable Encryption, Role-Based Encryption; and Access Control.

QIANG TANG is currently a senior research scientist from Luxembourg Institute of Science and Technology (LIST). His research interests lie in applied cryptography, DLT/blockchain-enabled security design, and the privacy issues in machine learning. Dr. Tang received his Ph.D. degree from Royal Holloway, University of London, UK. Qiang is affiliated with ILNAS (Institut Luxembourgeois de la Normalisation, de l'Accrditation, de la Sécurité et qualité des produits et services) by serving in the subcommittee ISO/IEC JTC 1/SC 27 (security and privacy) and SC 38 (cloud computing and distributed platforms), SC42 (artificial intelligence), as well as TC307 (Blockchain). He is a member of the DLT/Blockchain working group of the Luxembourg financial regulator Commission de Surveillance du Secteur Financier (CSSF).