Security and Privacy Protection for Intelligent Infrastructures in the Post-Quantum Era

Lukas Malina*, Petr Dzurenda*, Sara Ricci*, Jan Hajny*, Gautam Srivastava†, Raimundas Matulevičius‡,
Abasi-Amefon O. Affia‡, Maryline Laurent§, Nazatul Haque Sultan§, Qiang Tang¶
* Department of Telecommunications, Brno University of Technology, Brno, Czech Republic
† Department of Mathematics and Computer Science, Brandon University, Brandon, Canada
‡ Institute of Computer Science, University of Tartu, Tartu, Estonia
§ SAMOVAR, Telecom SudParis, Institut Polytechnique de Paris, France
¶ 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

Abstract—As we move into a new decade, the global realm of Intelligent Infrastructure (II) services integrated in the Internet of Things (IoT) at the forefront. With billions of connected devices spanning continents through interconnected networks, security and privacy protection techniques for the emerging Intelligent Infrastructure (II) services integrated in the Internet of Things (IoT) environments become a paramount concern. In this paper, an up-to-date privacy method mapping along with their current use case survey is provided for II/IoT services. Moreover, we present a focus on post-quantum cryptography techniques that maybe used in the future through concrete products, pilots and projects and including the latest developments. The topics presented in this paper are of utmost importance as (1) several recent regulations such as GDPR have given privacy a significant place in the digital society, and (2) the increase of II/IoT applications and digital services with growing data collection are introducing new threats and risks on privacy leakages. This in-depth survey begins with an overview of security and privacy threats in II/IoT. Next, we introduce some Privacy-Enhancing Technologies (PETs) suitable for the II/IoT services having certain privacy requirements, and map recent PETs schemes based on post-quantum cryptography constructions that can withstand quantum computing attacks. This paper also overviews how PETs can be deployed in practical use cases integrated in IIs and maps some current projects, pilots and products that deal with PETs. Finally, a practical case study on Internet of Vehicles is presented to demonstrate how PETs can enhance security and privacy. The purpose of the survey is to shed some light on current state of PETs with an emphasis on their implementation in II/IoT even in post quantum era.

Index Terms—Authentication, Cryptography, Internet of Things, Intelligent Infrastructures, Post-Quantum Cryptography, Privacy, Privacy-Enhancing Technologies, Security, Threats.

1 Introduction

Intelligent Infrastructures (IIs) interconnect various Internet of Things (IoT) applications and services in order to capture and analyse data as well as invoke autonomic responses. IIs based on IoT bring new benefits to society, customers and to the environment. Nonetheless, highly-connected electronic objects and digital systems around people's lives form a large intelligent network that can cause personal data leakages.

In theory, incoming IIs and IoT 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 [1] proposed eight privacy design strategies that are defined as follows:

1) **Minimize**: processed personal data should be confined to the minimal amount.
2) **Hide**: personal data and their interrelationships (linkability) should be protected or not public.
3) **Separate**: personal data should be processed in a distributed way.
4) **Aggregate**: limit as much as possible the detail in which personal data is processed, aggregating data in the highest level.
5) **Inform**: data subjects should be notified whenever their personal data are processed.
6) **Control**: data subjects should have control over the processing of their personal data.
7) **Enforce**: processing personal data should be committed in a privacy-friendly way, and should be adequately enforced.
8) **Demonstrate**: the system should be able to demonstrate compliance with the privacy policy and any applicable legal requirements.

Privacy protection techniques better known as Privacy-Enhancing Technologies (PETs) can implement these PbD 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 well known ENISA report [2], 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, the general data protection regulation (GDPR) replaced the Data Protection Directive 95/46/EC in 2018 [3]. The GDPR is comprised of the most basic data security and privacy principles by Article 5 that include lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity/confidentiality, and accountability. Moreover, the GDPR enhances various privacy aspects such as consent, right to be forgotten and privacy (data protection) by design that is mentioned in Article 25. Thus, privacy-preserving protection for IIs and IoT services are in the scope of the aforementioned regulations. In this paper, a map of the current PETs and their practical deployment in II/IoT is presented in an in-depth and well organized manner to assist the article's readership to navigate this complex and ever-evolving area of research.

Many PETs are based on traditional cryptographic primitives such as Public-Key Cryptography (PKC) algorithms. Nonetheless, most of current PKC schemes are theoretically vulnerable to potential attacks run by quantum computers. Post-Quantum Cryptography (PQC) offers the solutions against those attacks. Hence, privacy-enhancing technologies based on post-quantum cryptographic primitives are the natural next step evolution of PETs. As such, preparation for the future should begin now and the design of some IoT/II services to be resistant to potential future threats should commence - such as attacks run by quantum computers. This paper also maps the current state of the art of PETs that are already designed as for quantum resistance.

1.1 Privacy in Intelligent Infrastructures Applications

The use cases in both IoT and IIs are plentiful. Since both types of systems rely on mobile connectivity and data sharing, privacy issues are common. Added to the fact that these devices are often constrained, leads to a deadly mix for security and privacy.

The goal of both IoT and IIs is higher convenience for mankind. But with those promises have come security and privacy concerns. Since many of these IoT and II systems are built on the backbone of low power consuming computationally constrained devices, these devices lack the ability to run high powered security algorithms and methodologies. Hence, we see definitive vulnerabilities present that can easily be exposed by malicious minds. In this section, we explore a collection of use cases over the past few years that are specific to IoTs and IIs where users have been shown to experience security and privacy related issues.

In 2015, researchers at the University of Arizona shows that more than $70,000$ medical devices had been exposed online. Moreover, of that number 20% belonged to a singular health organization. [4]. It is evident in today's IoT world that still many devices connect to the Internet through dated Operating Systems which is the main concern to privacy breaches as these Operating systems often lack the needed security for today's advanced attacks. This study alone showed that a majority of the exposed devices ran Windows XP, an OS that has not been serviced in almost a decade with any sort of security patches and built on a 32-bit word size. Nevertheless, Windows XP still finds itself at the backbone of many legacy systems across the globe adding to the potential future privacy breaches that may occur as time passes on. Devices are easily found online through services like Shodan, a service that promotes itself as the "world's first search engine for devices"[2]. Devices as those found on Shodan running Windows XP with dated security are often easy to crack using Brute Force attacks that modern chipsets can easily manage. During the research at the University of Arizona, the researchers found that pacemakers, anesthesia equipment, infusion systems, cardiology devices, nuclear medical systems, magnetic resonance imaging (MRI) scanners can all be easily found using simple Shodan searches. Although it has never been actually reported, as many hackers motivations lie outside of medical equipment hacks, changing settings of medical equipment can prove detrimental to any patient connecting to devices such as the ones mentioned earlier.

In the realm of Smart Home IoT, a very hot commercial area in today's society with many household appliances gaining accessibility to the Internet, a well-known attack was the FATS attack, short for Fingerprint and Timing based Snooping (FATS) which was first presented in [5] by Srinivasan. FATS involved 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 through adversaries located somewhere in a WAN (Wide Area Network). The attack itself shows that simple WiFi packet sniffing techniques that have been successful for over a decade now can still give malicious entities an advantage in modern Smart Homes to aid in privacy breaches.

In a recent article featured in Forbes magazine, the research of Rotem *et al.* who work for vpnMentor, showed how easily an IoT management platform run by an Asian company Orvibo was easily accessible over an HTTP connection. Through a simple Internet Protocol connection

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

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

to the database they were able to gain access to over 3 billion records which included a slew of personal private information such as usernames, account codes for reset, payment information, and user passwords. Moreover, for some accounts, even some digital camera recordings from “smart cameras" were available The following data was available through this now well-known breach:

- Passwords
- Email addresses
- IP Address
- Account reset codes
- Family name
- Precise Geolocation
- Usernames

This breach of Orvibo highlights the different types of data that may be accessible once a system is compromised in an unsecured IoT or II network. Moreover, it also highlights the damage that can be easily caused over well known everyday use protocols like HTTP and IP.

Assisted living is defined as a living situation where senior citizens (elderly) who still enjoy living alone take the aid of IoT/II devices to ease some of their daily tasks as well as using devices with Internet connectivity to monitor their movements to ensure their safety. In [6], Henze *et al.* showed that unobtrusive sensors used to monitor senior citizens vital signs may be an area of concern for privacy breaches. These sensors will read vitals from patients and the upload this information to the cloud 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 persona private data may be vulnerable during transmission to the cloud. Since sensor devices are often constrained and unable to run high complexity security protocols, they can easily compromise an entire system. The main issue raised by the authors was how to properly integrate high computational services like cloud storage with constrained devices like sensors. This is an ongoing issue and an extremely hot research topic for our current decade.

Social challenges come from the need to mould Smart City service as delivered to the specific profiles of every person [7]. As such, a given service that is available in a Smart city may in fact have a slew of configurable options. The more customizable a service is usually dictates how successful that service may become. However, these custom user profiles within deployed applications may pose a security and privacy concern for the specific user the profile is connected to. So the main societal challenge becomes ensuring the privacy and security of the user’s that use specific services. The vital integration of privacy and security mechanisms within Smart City applications is an important direction of current and future research. The priority is and will continue to be ensuring user confidence in new technologies, as without user confidence services are not used and investments and infrastructure are wasted.

Autonomous vehicle technology is a hot area of research and will become a commonplace service in the future [8], [9]. Currently, IoV, short for the Internet of Vehicles is an ongoing service connecting a large set of sensors, controllers, and devices that are attached to either vehicles or vehicle infrastructure to allow for ease of autonomous control. It is quite an undertaking to be able to design effective privacy mechanisms which in turn can make sure collection of the IoV Big Data is both trusted as well as not tampered with. There is massive risk involved with the injection of malicious or fraudulent message into IoV by malicious vehicles. This process can endanger the entire traffic system(s). Moreover, an entire network once compromised may endanger the lives of any persons involved in the network.

Solanas present the ideas of S-Health (Smart Health) as a synergistic effort connection smart cities and mobile health [10]. Even though S-Health as an entity may be able to prevent many health issues, it in turn gathers large amounts of information directly related to citizens, their personal private information, as well as their medical information. From information that is gathers, many personal traits can be inferred since the data points towards habits, religion, as well as possibly social status. The result of combining health information with personal information as a privacy concern is a ticking time bomb. S-Health sheds light as well on smart systems used as protective equipment (glasses, helmets, hazmat suits) that are constantly being traced and monitored.

Listed areas of IoT and II are summarized giving privacy concerns as well as some applications being used in Table 1. In [11], Finn *et al.* suggest 7 privacy concerns given 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 your private 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 t keep thoughts and feelings private.
- **Privacy of location and space**: right to move freely in public without being identified (keep location private).
- **Privacy of association**: right to associate with others freely without monitoring.

1.2 Related Work

There are several interesting studies and survey papers focusing on security and privacy in IoT [12], [13], [14], [15], [16], [17]. Furthermore, there are surveys and research papers that focus solely on privacy in IoT and in IIs. Some examples are given in [18], [19], [20], [21], [22], [23], [24], [25], [26].

For instance, Porambage *et al.* [18] provide a holistic view of the privacy challenges in IoT. The authors discuss topics in IoT privacy, solutions and future research directions. Next, Dwork [19] outlines 5 scientific challenges regarding privacy in intelligent infrastructures, as follows:

1) privacy for streaming IoT-data

TABLE 1
IoT Areas with Application Example and Privacy Concerns [11]

IoT Area	Privacy Concerns	Application
Internet of Vehicles	Action, Image	RideLogic
Healthcare IoT	Data, Person	Geniatech, Cycore
IoT Blockchain Implementations	Personal, Data	Helium
Smart Home	Data, Location	Orvibo
Internet of Underwater Things	Communication	WFS Tech
Smart Cities	Communication, Location Data	Cisco

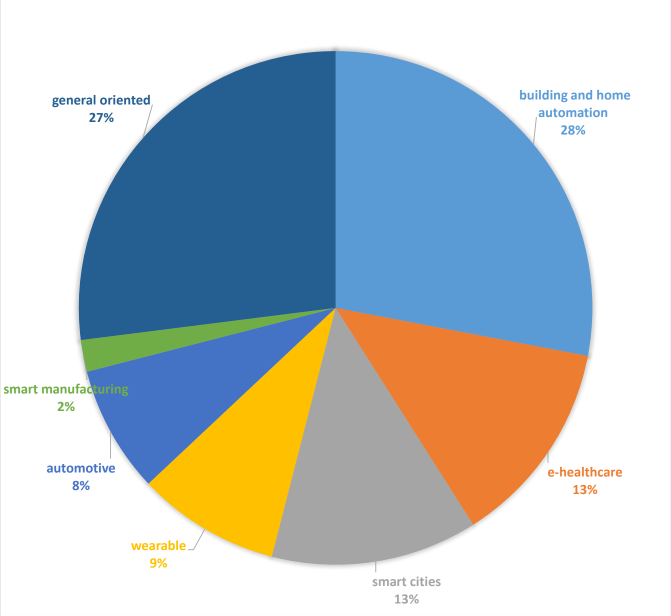


Fig. 1. The focus of research papers in various IoT applications [21].

2) privacy at the IoT-edge
3) decentralized Private Computation
4) Variable privacy
5) Event-based privacy

Cha *et al.* [21] aim to identify the current state of development of the PETs in various fields of IoT applications. The paper also examines whether the existing PETs comply with the latest legal principles and privacy standards. The survey explores 120 papers focusing on the solutions of PETs in IoT. Authors categorize PETs in IoT into 7 research domains:

- Control Over Data
- Enforcement
- Anonymization or Pseudonymization
- Personal Data Protection
- Anonymous Authorization
- Partial Data Disclosure
- Holistic Privacy Preservation

The authors work conducts 15 privacy principles from GDPR and ISO/IEC 29100:2011. Furthermore, their work links the principles with PETs papers and presents some future directions of advanced technologies. Figure 1 depicts the focus of 120 privacy-oriented IoT papers in various fields.

Seliem *et al.* review existing research and propose solutions to rising privacy concerns from multiple viewpoints to identify the risks and mitigation in [22]. 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.* deal with differences between privacy and security in [23]. The authors present 11 general approaches and techniques that are being used to fulfill privacy requirements. Nevertheless, their analysis and classification models are not overly deep. Curzon *et al.* [25] aim to show how privacy of individuals could be exposed in various Smart City applications and how this exposure could be mitigated using multiple privacy enhancing technologies. This survey also shortly presents various PETs. Recently, Hassan *et al.* [26] survey differential privacy techniques for cyber physical systems including industrial Internet of things. The authors present open issues, challenges, and future research direction for differential privacy techniques in cyber physical systems. Nevertheless, their study do not explore other PETs and their quantum resistant variants.

There are several review papers focusing on post-quantum cryptography such as [27], [28], [29], [30], [31], [32], [33], [34]. Bernstein and Lange [31] explain the damage of classic cryptography done by quantum computing and describe some candidates for post-quantum cryptography. Tan and Zhou [32] review post-quantum (PQ) digital signature algorithms and analyze the suitability of PQ signatures in various general applications such as TLS, Bitcoin, GSM eSIM and so on. Nejatollahi *et al.* [33] provide a comprehensive survey focused 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 [35] surveys 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. Furthermore, the implementation aspects of PQC on constrained devices are also studied in other papers such as [36], [37].

To the best of our knowledge, there is a lack of studies that connect essential topics in both privacy protection and post-quantum cryptography as well as those that review quantum-based privacy-enhancing schemes and its adoption for IoT/IIs services. In our study, we categorize and present concrete privacy-enhancing technologies based on traditional cryptography as well as on emerging post-quantum cryptography constructions. Furthermore, we also map privacy-required IoT applications, privacy threats in

IoT, and PETs deployed in concrete projects/products. In Table 2 we present all acronyms and notations that are used throughout the paper.

TABLE 2
List of Acronyms and Notations

AA	Anonymous Authentication
ABC	Attribute-Based Credentials
ABE	Attribute-Based Encryption
APEA	Anonymous and Pseudonymous Entity Authentication
BS	Blind Signatures
CBC	Code-Based Cryptography
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
DP	Differential Privacy algorithms
DS	Data Splitting
DTLS	Datagram Transport Layer Security
FHE	Fully Homomorphic Encryption
GPS	Global Positioning System
GS	Group Signatures
HBC	Hash-Based Cryptography
HE	Homomorphic Encryption
IBC	Isogeny-Based Cryptography
II(s)	Intelligent Infrastructure(s)
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
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
RS	Ring Signatures
SR	Searchable Encryption
SMC	Secure Multi-party Computations
SDC	Statistical Disclosure Control
U	User
TLS	Transport Layer Security
TTP	Trusted Third Party
V	Vehicle
ZKP	Zero-Knowledge Proof

1.3 Contribution

This paper addresses the privacy issues related to intelligent infrastructures and the IoT environment. It maps the recent technical-based PETs, and surveys the post-quantum resistant PETs. The readiness of PQ PETs in IoT and IIs is also discussed. The contribution of this review paper can be summarized as follows:

- Identification of privacy threats and leakages in IIs, even for post-quantum era.
- Description of current PETs and some recent quantum resistant PET schemes.
- An inventory of practical deployments of PETs in ICT including list of current projects and products and various IoT/II use cases where PETs can be deployed.
- An illustrative case study for demonstrating a privacy-preserving II service useful for the Internet of Vehicle (IoV) and smart city and for presenting some options for a secure design in post-quantum era.

1.4 Paper Organization

The rest of the paper is organized as follows. Section 2 presents the privacy issues relative to IoT/IIs. Section 3 deals with the categorization and assessment of PETs in IoT/IIs. Section 4 surveys emerging security and privacy solutions and technologies that are suitable in IoT/IIs for post-quantum era. Section 5 shows practical deployment of PETs in ICT and IoT/IIs, and Section 6 presents a chosen case study of PETs deployed in the selected II service of IoV.

Lastly, some concluding remarks are given in Section 7.

2 Security Threats and Privacy Leakages in Intelligent Infrastructures

2.1 Basic Privacy and Security Threats

An intelligent infrastructure, based on the Internet of things paradigm, utilizes cooperative sensing and networking capabilities. Most IoT systems consist of (*i*) systems that collect data about the state of the scenarios, (*ii*) systems which transmit collected data and (*iii*) systems which provide the data to end-users following a predefined process [38]. The vehicular subsystem considers the interaction of systems within the Intelligent Transportation System (ITS) as it concerns vehicles and its agents (e.g., vehicle, infrastructure and users such as drivers, passengers, pedestrians). II is a type of the IoT system as it encompasses cooperative interactions with a variety of things or objects, to reach a common goal [39]. IoT systems consist of three architectural layers [40], [41], [42], [43], [44], [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 is defined as an event where the *vulnerability* of a system asset is exploited by an attacker (*threat*) leading to some *impact* – a negation of the criteria of the business asset in a system [46], [47]. Table 3 summarizes the threats at the different architectural layers. The threats are categorized following the **STRIDE** threat model based on the first impact experienced [48].

Perception layer threats attack the sensing, vision, positioning and actuating components. Following [48] Table 3 includes 24 threats. *Network layer threats* affect the system assets' ability to transmit the necessary data for an IoT function. Data is typically transmitted through local/internal network, device-to-device, and device-to-infrastructure communication technologies. To illustrate the network layer threats, Table 3 assembles 47 threats [48].

Application layer threats involve attacks to disrupt or corrupt high level IoT processes and services. To illustrate them, Table 3 includes 12 threats.

2.2 Privacy Threats in Intelligent Infrastructures

Privacy, in the era of IoT, can be affected by activities including personal information collection, processing, sharing, and invasion/leakage [49]. Information collection, processing, and sharing activities are fundamental in running these cooperative IoT/II systems. Personal information is collected including:

1) user identity in general
2) geolocation in transportation
3) health conditions in healthcare
4) lifestyle habits inferred from intelligent surveillance, smart energy, and home

Service providers process the provided as well as the disseminated data to query required functions and data using cloud servers to provide personalised or group/crowd-sourced services. As data in IoT/II systems becomes abundant for its use in intelligent applications (i.e., assisted or autonomous driving [50], healthcare services in Smart Cities [51], Smart Homes), the implication of privacy invasion/leakage is increasingly becoming a major concern.

The following privacy threats and attacks that 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 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 their 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 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 behavior in certain time and place.
- **Tracking attack**: An attacker is able to trace and record person's movement through time and space (based on localization or behavioral leakages and user identification).
- **Profiling attack**: An attacker is able to create profiles in order to analyze information about users and infer their personal interests by correlation with their profiles and data.
- **Inventory attack**: An attacker is able to send certain query requests to the object and analyze the related responses to determine 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 user's reputation.

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

2.2.1 Privacy Leakages through 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 [52]. 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 with background knowledge of common appliances' consumption rates, estimate what devices are possibly switched ON, to infer a higher probability 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) [53].

Intelligent surveillance, although designed for monitoring criminal behaviors, may also capture smart city residents' daily life habits and behaviors, and such data, even being unconsciously disclosed to un-trusted entities, may become prejudicial to the residents' privacy [54].

In vehicular IIs where integrating mobile Inertial Measurement Unit (IMU) sensors with the vehicle can, on the one hand, lead to the development of numerous beneficial applocations. Still, on the other hand, collection of IMU data, which is available on various devices such as smartphones, Original Equipment Manufacturer (OEM)-authorized OBD-II dongles, and wearables, can leak driver privacy [50]. 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 [50]. It can also reflect the driver's risk level [55] 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 [55], [50], [56].

Research has suggested the application of off-the-shelf privacy and security techniques, such as encryption, anonymity, and access control, to preserve privacy leakage during data sensing [54].

2.2.2 Privacy Leakages through 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,

TABLE 3
Summary of Security Threats, adapted from [48]

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, Unauthorised 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, Unauthorised 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

and acceleration [57], [58]. Risk impact includes the loss of confidentiality of sensitive information contained in the beacons following an eavesdropping attack to trace the vehicle which is acheived by linking the location data together [57], [58]. 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 on the occupants by the pre-processing, classification, and matching of traffic data [59]. Wireless communication technologies when used, are prone to privacy leakages, so, an attacker can monitor encrypted network traffic of smart home devices to infer sensitive information of occupants without using any advanced technique [60].

Besides encryption, research has suggested the injection of noisy data flows in communication among smart devices and the Internet [59], as well as the application of straightforward solutions such as VPN or Tor-like Tools, signal attenuation, and traffic shaping to preserve privacy leakage during data communication [60].

2.2.3 Privacy Leakages through 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 increases the risk of sensitive data leaks through correlation [61].

The vehicular II application layer collects all data from fog nodes, environmental sensors, and vehicular GPS sensors over a long period of time. 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 [62]. The frequency of the sent health status information can determine the type of health issue a driver is facing 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 period of time, this information can describe any ongoing disease the driver may suffer from [62]. Collected location data can be used to track a vehicle even when the vehicle is not sharing its location information. With the recording of the vehicles' 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 [62].

In smart home applications, where the application is permitted to collect the events of the occupant, this application can learn behavioral patterns in a variety of ways that are not readily noticeable [52]. Research has suggested [63], [64] the use of trusted remote data stores, and broker for access control to centralized storage, as well as a combination of different cryptographic techniques, to preserve privacy leakages in the application layer.

2.3 Threats in Intelligent Infrastructures in Post-Quantum Era

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

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

- **QC-based threat using the Shor's algorithm**: The Shor's algorithm running on a functional quantum computer with a sufficient number of qubits is able to 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 [65]. To be noted that current quantum computers (QCs) are capable to run Shor's algorithm and already have about tens of logical qubits and physical qubits. To prevent the attack by Shor's algorithm, vulnerable asymmetric cryptography schemes should be substituted by PQC schemes.

- **QC-based threat using the Grover's algorithm**: Grover's algorithm 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 cryptography schemes should increase the sizes of keys and other essential parameters.

Future quantum computers may retroactively affect current ICT systems, their 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 deployment of PQC solutions.

- *Long term digital signatures*: To prevent threats, Post-quantum (PQ) resistant digital signatures should be employed. Current documents digitally signed with conventional cryptographic algorithms, such as RSA, ECDSA, etc., will be in the post-quantum era considered as un-trusted. In the context of electronic documents, it causes signing information pertaining to signed documents to come into question. It can have significant impact for authenticity of current official and legislative documents, contracts, certificates, etc.
- *Long term data security*: To prevent threats, the PQ resistant 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 death of a patient or client. It can cause problem to some confidential data archives which have usually lifetimes longer than the time it takes for new computer paradigms to threaten conventional cryptographic algorithms.

3 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), as well as applied in any of the folliwing:

- networks
- data storage
- cloud
- backend servers.

TABLE 4
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

PETs often provide some or all of the following basic privacy features:

- **anonymity**: a user cannot be recognized as the source of data.
- *data privacy*: stored data do not leak undesired properties, e.g. identities, user's vital data etc.
- **pseudonymity**: a user can be identified only to certain system parties (issuers). There is balance between anonymity and accountability.
- **unlinkability**: the same user's actions cannot be linked together (sessions are mutually unlinkable).
- **untraceability**: user's credentials, identities or actions cannot be tracked by unauthorized parties (e.g. verifiers).

In addition, PETs usually combine privacy features with common security features that can be defined as follows:

- **accountability**: a user has specific responsibilities and access to services.
- **authentication**: a user can validly prove his/her possession, claim, access or identity.
- **availability**: the connectivity of smart thing or service/application persists.
- **data confidentiality**: data are secured against exposing by encryption methods.
- **data authenticity and integrity**: data are secured against their tampering or removing by the unauthorized parties.
- **non-repudiation**: a user (a signer) cannot deny his/her signature.
- **revocation**: a trusted system entity is able to remove/revoke a chosen user (his/her credential) from a system.

PETs and security technologies are usually combined together in order to reach most of the above privacy and security features.

Table 4 categorizes the most essential PETs, which are described in the following subsections. Note that the provided examples are limited and do not cover all privacy-preserving schemes.

3.1 Privacy-enhancing Digital Signatures

3.1.1 Group Signatures

A Group signature (GS) is a digital signature providing group-based authentication. GS provides privacy for signers against verifiers. GS schemes allow any group member (a user) to anonymously sign a message on behalf of the group. 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 signature on the message is created by using a group member secret key. The signed message is verified by one group public key that is spread in the group of users. The basic principle of group signatures is depicted in Figure 2.

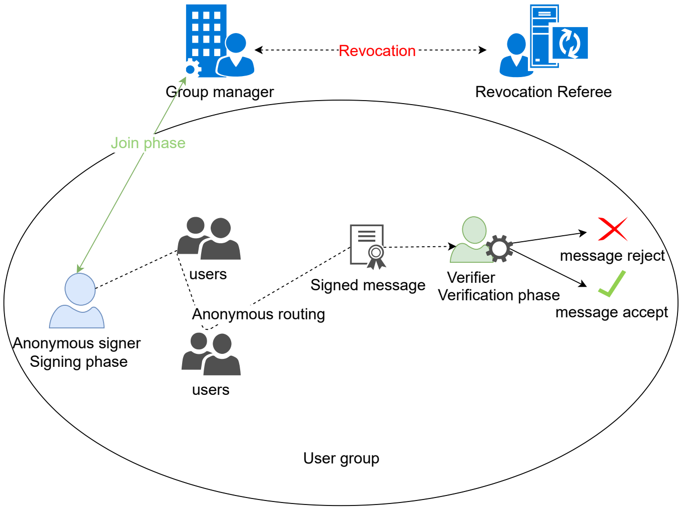


Fig. 2. The basic principle of GS schemes.

In the two past decades, extensive research has focused on group signature schemes (> 5.4K papers in Scopus).

There are many variants of GS schemes providing various 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 a data on behalf of the group. Moreover, several group signature schemes are included in the standard ISO/IEC 20008-2:2013 [66] and several public libraries including GS schemes are released in public repositories. There are many well established group signature schemes, e.g. [67], [68], [69], [70], [71], [72], [73] and several schemes, e.g. [74] and [75] are also orientated on computational efficiency in order to be applicable on constrained devices. Several papers focusing on group signatures in IoT have been published recently, e.g. [76], [77], [78].

Nevertheless, there is still ongoing work on the design of efficient group signatures with immediate revocation features appropriate for constrained devices and on the design of new GS schemes based on quantum-resistant assumptions.

3.1.2 Ring Signatures

A ring signature (RS) is a digital signature providing group-based authentication in order to achieve privacy of users against verifiers. Any user (member) of a group (ring) can sign a message on behalf of a group (ring). The user signs a message with his/her private key and then he/she publishes a set of public keys merged with his/her public key, i.e., multiple public keys. RS schemes are similar to GS schemes and some studies call them as ad-hoc group signatures. Nevertheless, RS schemes remove the central point of a group manager and RS do not need 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 a perfect privacy (untraceability) because there is no authority that can revoke the anonymity of signers. The basic principle of ring signatures is depicted in Figure 3.

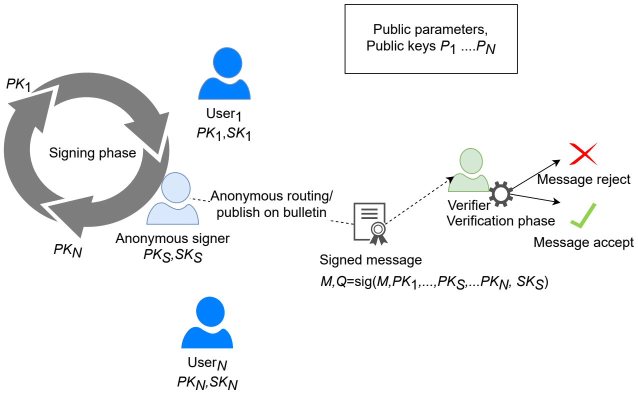


Fig. 3. The basic principle of RS schemes.

Ring signature schemes have been studied since 2001 (> 1.2K papers in Scopus). There are several variants of RS schemes providing various features. 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 ring signature schemes such as [79], [80], [81]. Nowadays, RS are employed in several cryptocurrencies and altcoins such as Monero, CryptoNote, TokenPay, etc. Nevertheless, RS produce 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, but the performances of phases and the size of ring signature are more challenging for memory, bandwidth, and computational resources than with 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. [82], [83], [84], [85], [86], [87]. Nevertheless, there is still ongoing work on the design of efficient and logarithmic-sized ring signatures appropriate for constrained devices and on the design of new RS schemes based on quantum-resistant assumptions.

3.1.3 Blind Signatures

Blind signatures (BS) are a form of digital signatures which 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 signature, anonymous credentials and in 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 Figure 4.

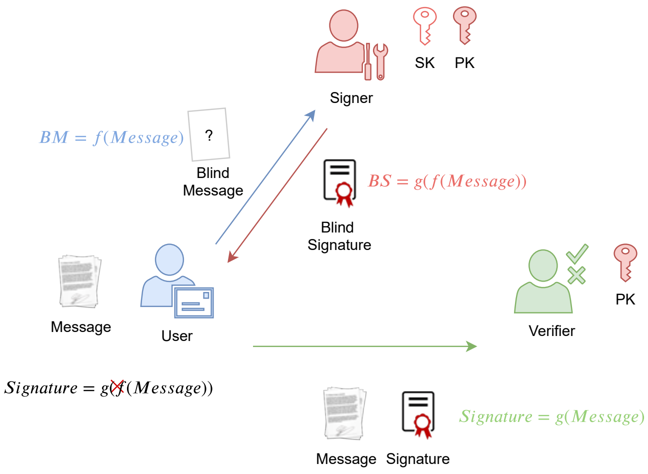


Fig. 4. The basic principle of BS schemes.

Generally, we can consider BS mature and ready to be used in digital systems, Scopus records > 1.6K papers. Many BS, e.g. [88], [89], [90], [91] are based on standard signature schemes which 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 are mostly used in payment systems such as PayCash. Officially there is no standard which deals with BS, however, BS are based on standard digital signatures, hence we can consider their standardization. The main goal of the current proposals is to build efficient and post-quantum resistant schemes, e.g. [92], [93].

3.2 Privacy-enhancing User Authentication

3.2.1 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), which is widely used in current systems. In ABC context, the digital identity is considered to be a set of characteristics (personal attributes) that describe certain person. 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. Actually, credentials are very similar to traditional digital certificates. Both structures can contain attributes such as age, citizenship, gender, social security number, credit card number, etc. The fundamental difference between credentials and certificates is that credentials are never shown to other parties. A user is able to 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 user or steal his identity, profile users and track their movement and behaviour. The basic principle of ABC authentication approach is depicted in Figure 5.

Many research articles focused on ABC technology are published, e.g., [94], [95], [96], [97], [98], [99], [100] (> 0.6K papers in Scopus). This technology can be considered mature and ready to use in current ICT systems. In fact, there is already a running IRMA (I Reveal My Attributes) pilot project with the IRMA card and mobile application product for privacy-friendly authentication. Furthermore, current ABC schemes are efficient enough to run, even on IoT constrained devices. For example, the article [101] presents an anonymous scheme that runs the show protocol in less than 500 ms (in case of 3 stored attributes) on current smart cards. The necessity of this technology in authentication/identification systems have also been demanded by the U.S. and E.U. institutions. The main known drawback of the technology remains the revocation, which has been solved in recent years, for example in the paper [102]. Nevertheless, there is still ongoing work on the design of new ABC schemes. Other directions in future research are to provide decentralized ABC system in order to increase privacy and security and/or to transform ABC schemes to quantum resistant forms.

3.2.2 Anonymous and Pseudonymous Entity Authentication

Anonymous Authentication (AA) preserves user privacy. In an AA system, a user can get an access to a service without disclosing his/her identifier. This method prevents a verifier to track and profile them. However, the verifier can still reliably determine whenever the user is authentic or not. The authenticated user only provides a proof of knowledge of the secret for some chosen claims, e.g. a user belongs to the group with specific privileges. Basic AA systems are based on zero-knowledge proof (ZKP) protocols as in [103]. More advanced schemes enable trusted third parties (TTPs), called openers, to open the proofs and learn the user's identity. The TTP is able to disclose user identity, revoke session unlinkability or revoke a user from a system. If such TTP exists, the system is called partially anonymous or partially unlinkable, see ISO/IEC 29191:2012 [104]. The most of the current AA and PA schemes are formed by group signatures (ISO/IEC 20009-2 [105]), blind signatures (ISO/IEC 20009-3 [106]) or identity escrow schemes, see [107] 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. The basic principle of anonymous and pseudonymous entity authentication mechanisms is depicted in Figure 6. Scopus records more than 2.2K papers focused on AA and PA schemes.

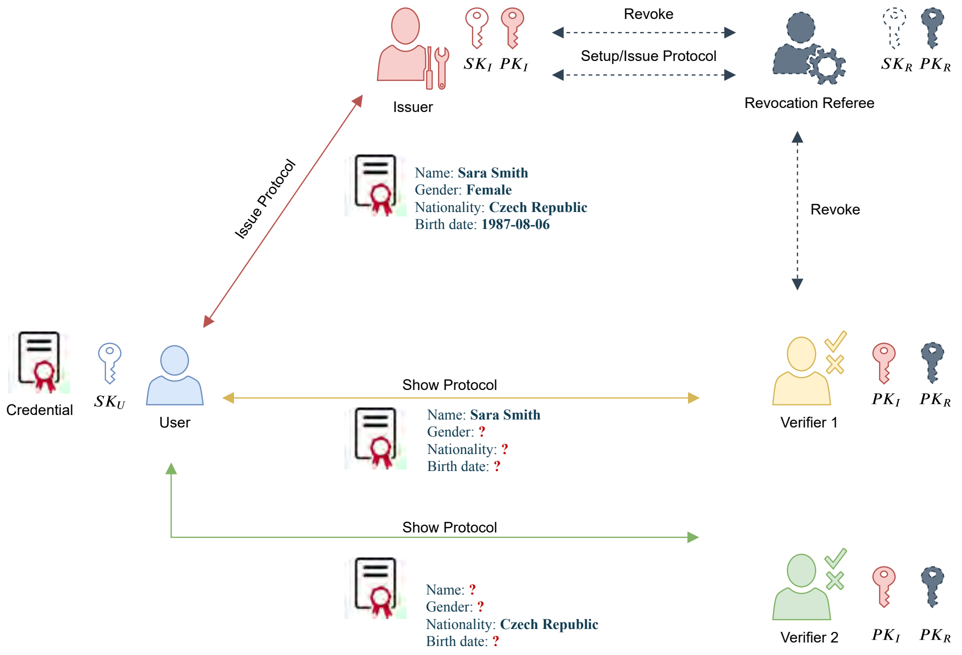


Fig. 5. The basic principle of ABC schemes.

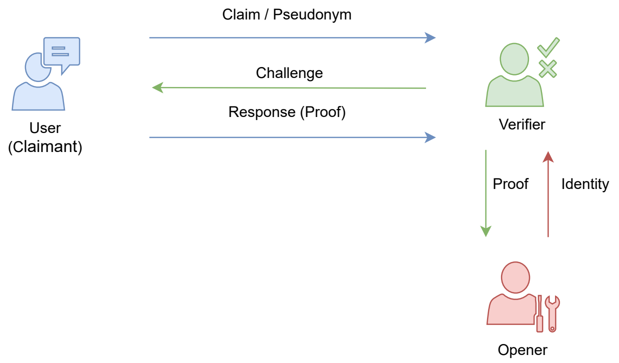


Fig. 6. The basic principle of anonymous and pseudonymous schemes.

3.3 Privacy-enhancing Communication Systems

3.3.1 *Mix-networks and Proxies*

Mix networks (Mixnets) represent a basic privacy technology that is 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 in order to disrupt the relation between incoming and ongoing 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). Some schemes add dummy messages to make tracing more difficult. Mixnets can employ simple one-tier architecture (one proxy) or a chain of proxies (mixes shuffle messages and resent them to other mixes via multi-tiered architecture). Using only one central proxy server could be weak against various attacks (denial of service, local eavesdroppers, the maliciousness of the central node, compulsion), therefore, robust Mixnets protocols and schemes usually employ more servers in a chain (a cascade) or in multi-path topologies. The equal-size messages with the address of an addressee (or a bulletin) are usually encrypted by public key cryptography (e.g. by public keys of proxy servers). Mixnets protocols usually employ re-randomizable encryption schemes such as the ElGamal encryption scheme. The basic principle of mix networks is depicted in Figure 7 (E denotes an encryption function using various public keys).

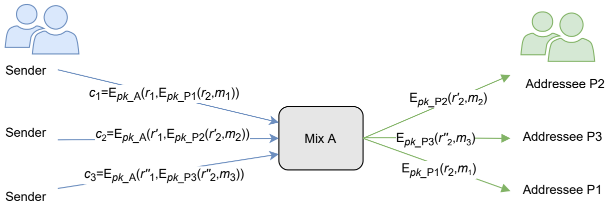

Sender
Sender
Sender
c_1=E$_{pk\_A}$(r_1,E$_{pk\_P1}$(r_2,m_1))
c_2=E$_{pk\_A}$(r'_1,E$_{pk\_P2}$(r'_2,m_2))
c_3=E$_{pk\_A}$(r''_1,E$_{pk\_P3}$(r''_2,m_3))
Mix A
E$_{pk\_P2}$(r'_2,m_2)
E$_{pk\_P3}$(r''_2,m_3)
E$_{pk\_P1}$(r_2,m_1)
Addressee P2
Addressee P3
Addressee P1

Fig. 7. The basic principle of mix networks.

Mixnets, that were frist introduced in 1981, have been actively studied since the year 2000 (> 1.7K papers in Scopus). There are several variants and strategies of Mixnets protocols. The pioneer and most established schemes are [108], [109], [110], [111], [112], [113], [114], [115], [116].

In general, Mixnets provide anonymous communication which could be used as 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, which might hurt privacy. Mixnets usually rely on public key cryptography in order to protect messages against traffic analysis.

Mixnets technology has been studied primarily for classic networks, nevertheless, there are few papers focusing on the implementation of Mixnets solutions on constrained devices (and IoT), e.g., [117], [118]. For example, Chaum *et al*. [117] presented cMix: Mixing with minimal real-time asymmetric cryptographic operations in 2017. 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.

3.3.2 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 path, which is called an onion router. The data are encapsulated by the sender 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 reach the destination (e.g. web server). The basic principle of onion encryption in onion routing is depicted in Fig. 8.

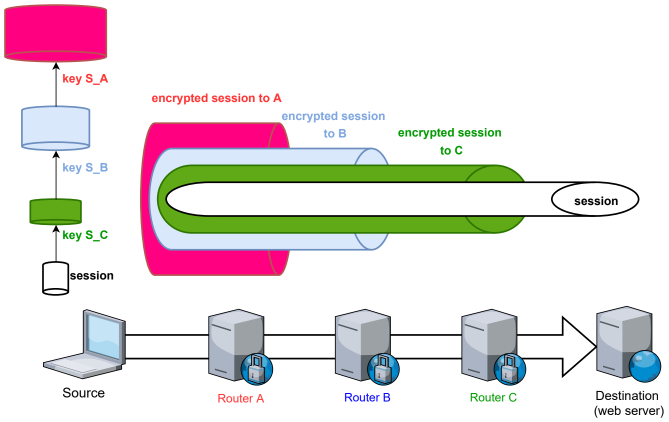


Fig. 8. The basic principle of onion encryption in onion routing.

Onion routing was developed in the mid-1990s at the U.S. Naval Research Laboratory by employees Syverson, Reed and Goldschlag. Their papers [119], [120] describe anonymous connections and their implementation using onion routing. These papers also describe several application proxies for onion routing, as well as configurations of onion routing networks. The most mature project is Tor (The onion router). Tor [121] is based on a circuit-based low-latency anonymous communication service and onion routing. Further information about Tor is available at the ToR website[3].

Other applications and projects employ the onion routing principle or are inspired by Tor (> 0.3K papers in Scopus). Tribler [122] is an open source decentralized BitTorrent client which provides anonymous peer-to-peer communication by onion routing. In 2014, with the release of version 6.3.1, a custom built-in onion routing network was introduced as part of Tribler[4]. Tox[5] is a peer-to-peer instant-messaging and video-calling protocol that offers end-to-end encryption. As some metadata leaks were raised in Tox, developers then introduced the Onion routing implementation for the friend-finding process. Works such as [123], [124] deal with the deployment of DTLS (Datagram Transport Layer Security) in onion routing and its efficiency. The paper [124] employs DTLS in order to tailor onion routing to IoT and presents the practical evaluation of the tailored solution in IoT.

3.3.3 Privacy-enhancing Communication Systems for Wireless Access Network

In general, 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 [125], [126], [127], [128]: 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 which the device 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 are able to infer social links between users. Furthermore, 802.11 frames use the device 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. The feasibility of tracking wireless access network devices in the wild has been identified by several research works (> 0.03K papers in Scopus), namely [127], [128], [**?**], [126]. Research has demonstrated these technologies are the source of several privacy leaks. Informed of such problems, the manufacturers and the standards developing organizations have improved the practices (e.g., by banishing SSID disclosure in Wi-Fi access point active search mechanisms) and have designed privacy extensions, in particular the use of randomized MAC addresses during several modes of operation. However research has shown that this is not sufficient to fully prevent privacy risks (e.g., re-identifying an equipment that uses MAC address randomization is often possible). And application protocols relying on those technologies, in wide use, are also creating additional problems that make several attacks (e.g., inventory attacks) feasible. To conclude, if PETs do exist in the domain of wireless access networks, a lot remains to be done to reduce the privacy risks, the main complexity lying in the implementation and usage details.

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

[4] https://www.tribler.org/

[5] https://tox.chat/

3.4 Privacy-enhancing Encryption Technologies

3.4.1 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 result remain encrypted and inaccessible to the evaluator throughout the whole process. Only the data owner, who holds a decryption key (a secret key), is able to access data and reveal the result through ciphertext decryption. Similarly to traditional encryption, also HE offers symmetric and asymmetric scheme variants. Furthermore, HE can be of three main types:

1) partially homomorphic encryption (PHE)
2) somewhat homomorphic encryption (SHE)
3) fully homomorphic encryption (FHE)

PHE schemes support only one operation (addition "+" or multiplication "×") to be applied on encrypted data. This operation can be performed an unlimited number of times. Examples of PHE are Paillier cryptosystem [129] (additive scheme), RSA [130] and ElGamal [131] (multiplicative schemes) schemes. SHE schemes are limited by the number of homomorphic operations that can be performed on ciphertext, however they can use both operations ("+", "×") on encrypted data. FHE schemes, e.g. [132], [133], [134], [135], support an unbounded number of homomorphic operations and therefore they allow to compute any function on encrypted data. The applications of HE found place especially in privacy-friendly outsourced computations in a cloud. In fact, cloud providers can process users' data without knowing their content and the result of computations. This approach is impossible with traditional encryption methods, as cloud providers must first get access to unencrypted data before performing operations on it. The basic principle of homomorphic encryption is depicted in Figure 9.

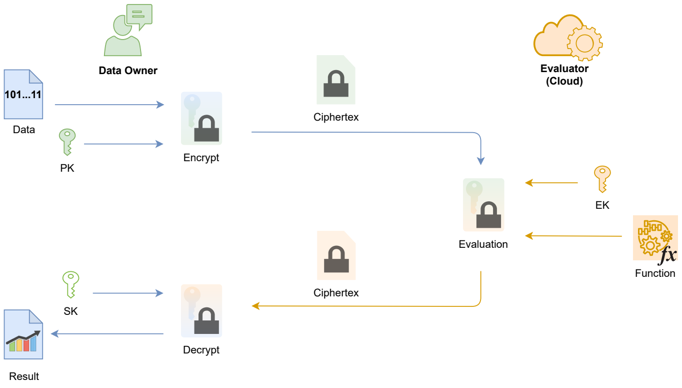


Fig. 9. The basic principle of HE schemes.

Especially FHE technology has become more interesting research area in the last decade. This increase is caused mostly by the growing of cloud services and outsourced computations. Currently, there are around 1K papers dealing with FHE technology and around 3k papers focused on HE technology. There are several proposed FHE schemes targeting shortcomings of existing solutions. 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 [136] created by the consortium of international industries, government and academia sectors. Furthermore, several public FHE libraries are released in public repositories. We did not find any papers which deal with FHE on IoT devices since the technology is too complex to be implementable on constrained devices. The main goal of current proposals is to reduce schemes' complexity to minimum and to make schemes as fast as possible.

3.4.2 Searchable Encryption

When outsourcing sensitive data to some remote cloud storage servers, data owners first need to encrypt the data so that any unauthorized entity including the cloud service provider cannot gain knowledge of any information about the actual data. However, data encryption removes the data search capability from the users including the owner of the data. To enable the owner to search the desired data over the encrypted data, a trivial approach is to download the whole encrypted database, decrypt it locally, and then search for the desired plaintext data. Clearly, this is not a practical approach. Another solution is to let the cloud service provider decrypt the encrypted database to perform a search query over the decrypted database, and sends only the desired result back to the user. However, this approach violates data privacy and confidentiality.

Searchable Encryption (SE) is a cryptographic technique which enables performing search operations using some keywords over encrypted data without disclosing any useful information about the actual content of the encrypted data and the searched keywords [137]. Using SE, any user, having proper credentials, can delegate the search capabilities to the cloud service provider without disclosing any useful information. The basic architecture of SE is shown in Figure 10.

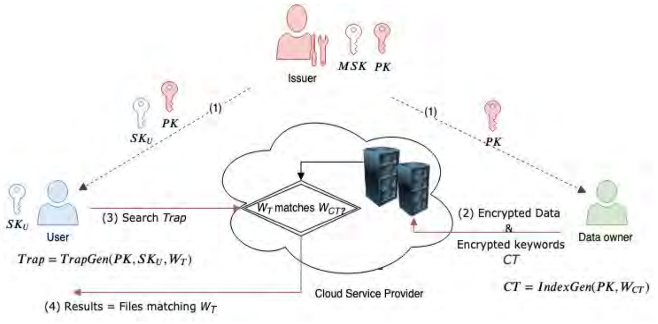


Fig. 10. Basic Architecture of an asymmetric SE Scheme.

SE has already become a promising privacy-preserving technology. In the last two decades, many schemes (> 1.4K papers in Scopus) have been proposed to address various security issues and to provide different functionalities. The pioneer and established schemes, e.g., [138], [139], [140], [141] are usually based on either symmetric key encryption or asymmetric key encryption. There are also several novel schemes that deal with the application of SE in IoT applications, e.g., [142], [143], [144].

In SE, it is very important to find and retrieve the requested data as quickly as possible. It still remains as a challenge to design a computationally inexpensive SE mechanism. There is still much work to do to improve its efficiency while keeping strong security to adopt SE widely in IoT based applications.

3.4.3 Attribute-Based Encryption

Attribute-Based Encryption (ABE), introduced in [145], is a one-to-many public encryption mechanism, i.e., the same data can be shared with several users. ABE is categorized into two groups, namely, Key-Policy ABE (KP-ABE) [146] and Ciphertext-Policy ABE (CP-ABE) [147]. In KP-ABE, attributes are used to encrypt data and access policies, which are defined on some attributes, are used to compute the decryption keys for the users. As such, a user can decrypt encrypted data if and only if attributes associated with the encrypted data satisfy the access policy of the decryption key. On the other hand, in CP-ABE, data are encrypted using access policies and decryption keys are computed using attributes. That is, a user can decrypt if and only if attributes associated with the decryption key satisfy the access policy associated with the encrypted data. The basic principles of both KP-ABE and CP-ABE are shown in Figure 11 and Figure 12 respectively.

ABE has already emerged as a promising cryptographic technology ($>$ 2.7K papers in Scopus). It has been used in a wide variety of environments such as cloud computing [148], [149], [150], mobile cloud computing [151], [152], [153], [144] and in other prominent ways as well. However, ABE has several practical challenges that are hindering its wide adaptation in practical applications.

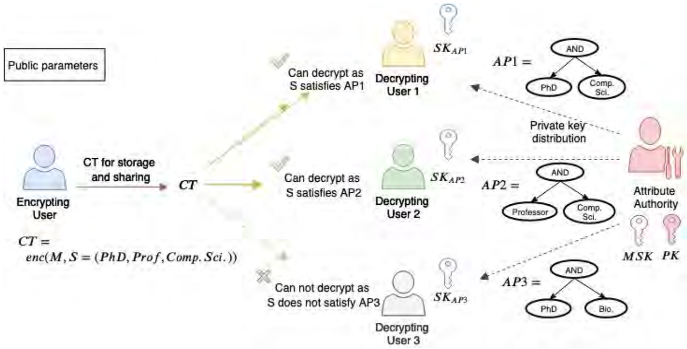


Fig. 11. The basic principle of KP-ABE schemes.

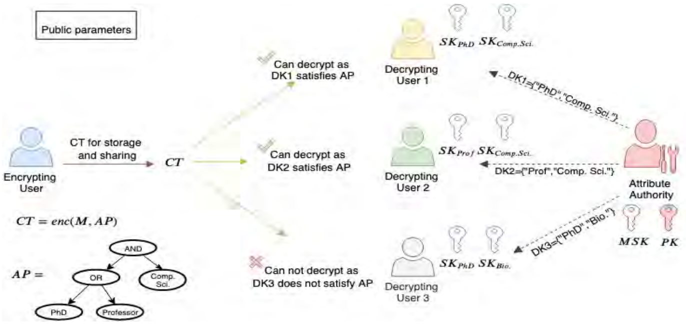


Fig. 12. The basic principle of CP-ABE schemes.

First, revocation is a challenge in ABE systems. Each user may share the same set of attribute types. As such, revocation of a user may affect other non-revoked users who share their attributes with the revoked user. Second, ABE systems need costly cryptographic operations, e.g., pairing, elliptic curve multiplication and exponentiation operations to perform encryption and decryption. As such, ABE may not be suitable for the environments where devices have less resources in terms of computing and storage power unless computationally expensive operations are outsourced. Third, ABE systems suffer from the key-escrow problem, as the AA knows all the master secrets. Hence, they can decrypt any ciphertexts of their choice. There are several recent proposals that try to be lightweight or address mentioned challenges. For instance, Tan *et al.* [154] propose an enhanced lightweight key-policy attribute-based encryption (KP-ABE) scheme for the Internet of Things (IoT). Cheng *et al.* [155] propose a scheme to control traffic light in IoV while preserving privacy of the users such as location and direction. Xiong *et al.* [156] present an efficient ciphertext-policy attribute-based encryption (CP-ABE) scheme that for the first time simultaneously achieves partially hidden policy, direct revocation, and verifiable outsourced decryption.

3.5 Privacy-enhancing Computations and Data Storing

3.5.1 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 to others [157]. The first example of SMC was presented by Yao in 1982 [158], 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 to identify which of them is richer without revealing their actual wealth. Formally, SMC is defined as follows: for a number of parties $P_1, P_2 \dots P_n$ each having initial secret input $x_1, x_2, \dots x_n$, SMC securely computes function f using the secret inputs, where $f(x_1, x_2, \dots x_n) = (y_1, y_2, \dots y_n)$. 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 Figure 13. 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 13) and intermediate values (message (2) shown in Figure 13) to the other users. Finally, each user can compute a common value of $S = X_1 + X_2 + X_3$ without knowing the actual secrets of the other users.

Currently, there are many papers dealing with SMC ($>$ 1.9K papers in Scopus) and the schemes [159], [160], [161] can be considered pioneereering and as the most established. Secure Multi-party Computations (SMCs) has already emerged as a promising and well-established privacy-enhancing technology. This can be observed from the available research projects and products. SMC can be suitable for various IoT/IIoTs use cases where privacy-preserving computation is needed, e.g., smart metering, voting, auctions,

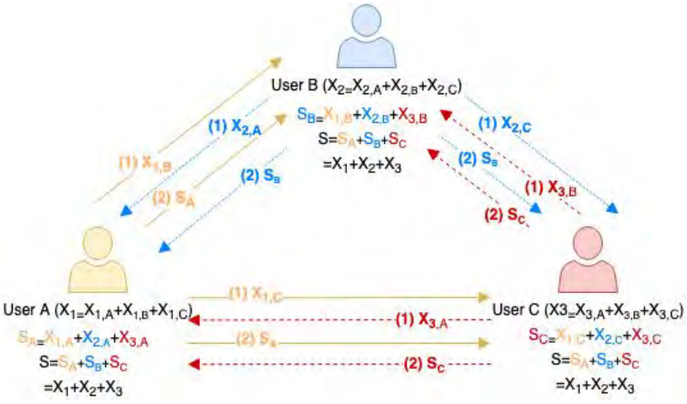


Fig. 13. A sample illustration of SMC.

etc. Although many works have been published for the use of SMC in practical applications in IoT/IIs [162], [163], [164], [165], there is still much work to do in terms of reducing computation and communication overhead for wider use of SMC.

3.5.2 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 for outsourcing user sensitive data as alternative to fully homomorphic encryption which is currently considered to be 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 usually to efficiently compute on 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, there are various DS schemes 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.* [166], Yang *et al*. [167], Domingo *et al.* [168]. The technology was used for example in the European research project CLARUS[6].

3.6 General Anonymisation Techniques

To support research and policymaking, there is an increasing demand for microdata, which is 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. In order to preserve the privacy of individuals as well as 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 show 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, then it can infer that this patient has cancer.
- **Inferential Disclosure**: In this case, the attacker is able to 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 both academia and the organizations which need to deal with microdata data publication. In academia, researchers have been active in examining the limitations and improvements with respect to existing notions, e.g. [169], [170], [171]. Many new notions have been proposed, e.g. the p-sensitive k-anonymity [170]. SDC methods are typically vulnerable when the attacker gains unexpected background knowledge and access to auxiliary data.

Differential privacy [172] is a formal mathematical concept for guaranteeing privacy protection when analyzing or releasing statistical data. In a book by Dwork and Roth [173], an example application is illustrated for social science research: in order to collect statistical information about embarrassing or illegal behavior (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, the SDC methods have received more criticisms, due to the fact that 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 [174] gave a good comparison study to SDC methods and differential privacy. Recently, researchers have attempted to combine these concepts. For example, Li *et al.* [175] showed how to achieve differential privacy and k-anonymity in the same data release. Holohan *et al*. [176] proposed the concept of (k, ϵ)-anonymity. Domingo-Ferrer and Soria-Comas [177] 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.

When applying differential privacy into real-world applications, one concern is about the privacy budget, namely ϵ. It is often hard to set this value and it is also difficult

[6] http://www.clarussecure.eu/

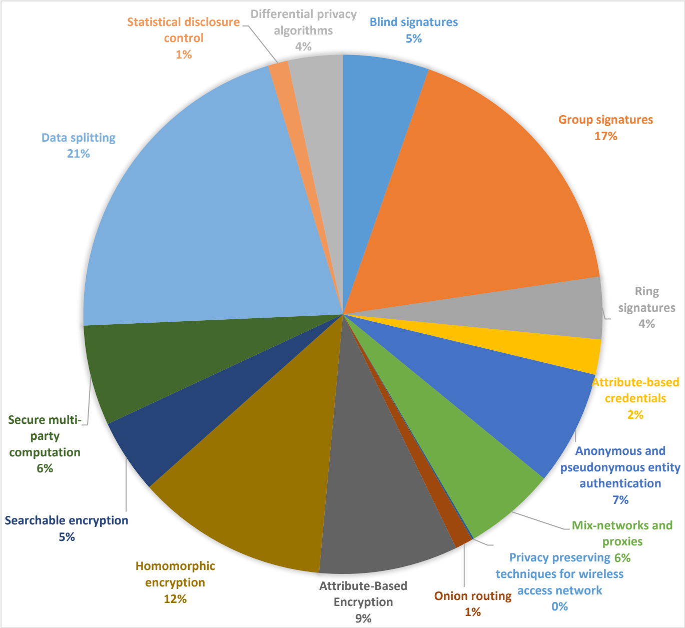


Fig. 14. The ratio of privacy-enhancing technologies on Scopus (in # of documents).

to explain the guarantees to non-experts. Besides, another concern is that adding noise to existing processes or data is not appealing and can even cause problem in some application scenarios, e.g. medical research [178], [179]. A lot of efforts are needed to solve these concerns.

3.7 Summary

In this section, we overview 15 privacy-enhancing technologies that are divided into 6 privacy-enhancing categories: digital signatures, user authentication, communication systems, encryption technologies, computations and data storing, and general anonymization technologies.

3.7.1 PETs in Literature

PETs have been studied in many research papers and have reached different maturity levels in different fields of application. The ratio of Scopus papers focused on mentioned PETs is depicted in Fig. 14, according to the following query syntax example on Scopus for searchable encryption:

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

3.7.2 PETs Position in Intelligent Infrastructures

Several technologies such as attribute-based credentials, group signatures, mixnets have already been considered in II/IoT. Figure 15 shows the indicative positions of analyzed privacy-enhancing technologies in the intelligent infrastructure 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. Nevertheless, only the appropriate combination of PETs that cover various properties can protect privacy in more complex systems such as Intelligent Infrastructures.

4 Privacy-Enhancing Technologies in Post-Quantum Era

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

4.1 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 [180], NTRU [181], New Hope [182], Kyber [183].
- **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 [184] such as the Unbalanced Oil and Vinegar Cryptosystems (UOV) [185] which provide digital signatures. Other MVC examples are the Rainbow signature scheme [186] and Tame Transformation Signatures [187].
- **Hash**-based cryptography (HBC) is based on the security of one-way hash functions. In 1989, Merkle [188] presented the Merkle Signature Scheme (MSS) based on one-time signatures such as the Lamport signature scheme [189]) 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 [190] uses binary Goppa codes with high error correction capability grouped in matrices. Further, the Niederreiter cryptosystem [191] as a McEliece variant offers both encryption and signing. The versions of McEliece schemes use usually large public keys.
- **Isogeny**-based cryptography (IBC) is based on super-singular 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 KEM protocols such as Supersingular Isogeny Diffie-Hellman (SIDH) [192] and Supersingular Isogeny Key Exchange (SIKE) [193].
- **Symmetric** quantum resistant cryptography (SQRC) presents current secure symmetric cryptosystems that use doubling the key size in order to be robust against PQ attack by the Grover algorithm.

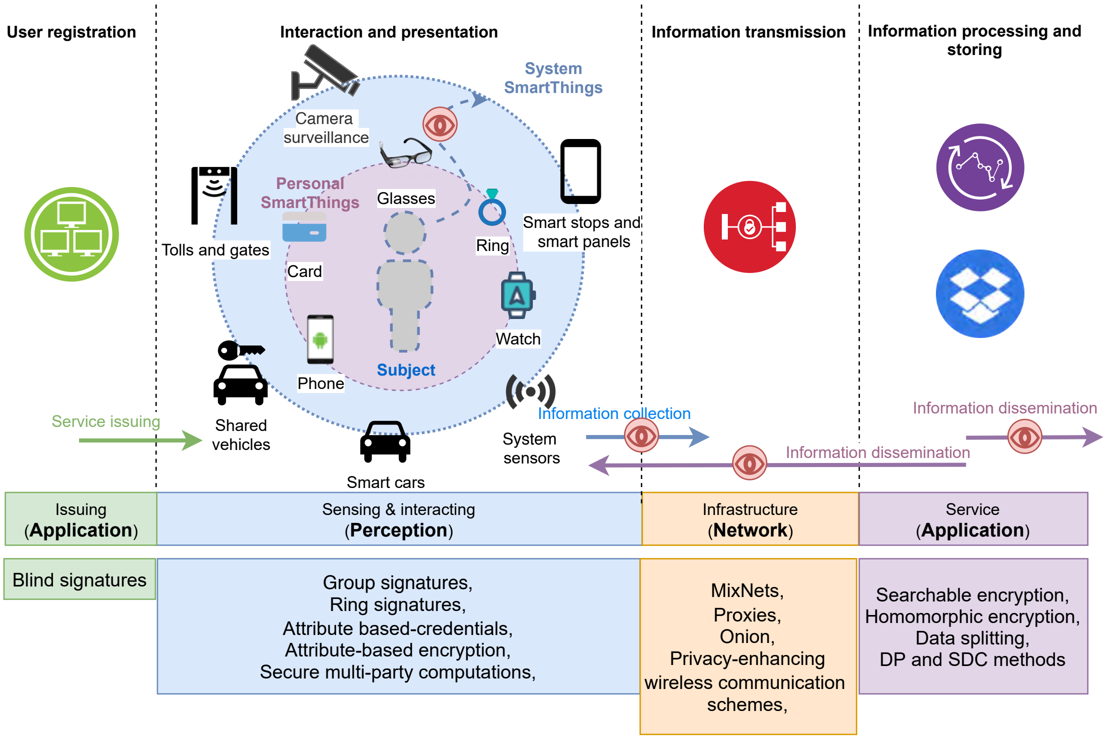

User registration
Interaction and presentation
Information transmission
Information processing and storing
System SmartThings
Camera surveillance
Personal SmartThings
Glasses
Tolls and gates
Card
Ring
Smart stops and smart panels
Watch
Phone
Subject
Shared vehicles
Smart cars
System sensors
Service issuing
Information collection
Information dissemination
Information dissemination
Issuing (Application)
Sensing & interacting (Perception)
Infrastructure (Network)
Service (Application)
Blind signatures
Group signatures, Ring signatures, Attribute based-credentials, Attribute-based encryption, Secure multi-party computations,
MixNets, Proxies, Onion, Privacy-enhancing wireless communication schemes,
Searchable encryption, Homomorphic encryption, Data splitting, DP and SDC methods

Fig. 15. The position of PETs in II/IoT communication model.

Quantum-resistant schemes have been around for more than 40 years (e.g. the McEliece public key encryption scheme [190]), and, since the first PQC conference in KU Leuven in 2006, PQC schemes have been intensively studied in many papers, e.g., [194], [195], [196], [197]. Moreover, current quantum computing's rise (e.g. Google's 53-qubit Sycamore processor [198]) causes that PQC is even more popular these days. Recently, several practical projects and implementations have been realized, e.g., notable H2020 projects PQCRYPTO[7] and SAFEcrypto[8] were completed in 2018. In addition, the Open Quantum Safe (OQS) project releases an open source C library for quantum-safe cryptographic algorithms called LIBOQS[9] which offers more than 60 key encapsulation mechanisms and 63 signature schemes. LIBOQS has been recently integrated with OpenSSH and OpenSSL libraries as separated forks.

4.1.1 *Post-quantum Cryptography Standardization*

In 2016, NIST started a process to solicit, evaluate, and standardize PQC schemes. Recently, NIST (NISTIR 8240)[10] announced 26 second-round candidates (semifinalists), 17 schemes for quantum resistant KEM and 9 schemes for quantum resistant digital signatures. These semifinalists are listed in Fig. 16. The results of the NIST competition (standardization) will be published between 2022 and 2024. Nevertheless, it is assumed that NIST will announce a set of recommended schemes.

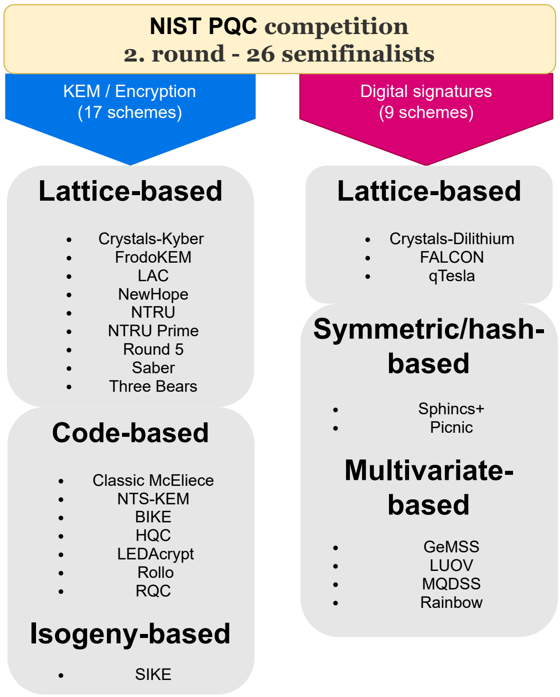


Fig. 16. PQC NIST competition - 26 semifinalists.

4.1.2 *Post-quantum Cryptography in IoT/II environment*

PQC schemes can be easily implemented in current IT infrastructures unlike quantum cryptography and quantum key distribution schemes which require specific and expensive equipment and focus only on key establishment. PQC schemes are usually more memory and computation-

[7] http://pqcrypto.eu.org/
[8] https://www.safecrypto.eu/
[9] https://github.com/open-quantum-safe/liboqs
[10] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

ally demanding than traditional cryptography solutions. Constrained IoT end nodes, i.e. low performance-microcontrollers 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 benchmarking and testing framework for these microcontrollers. Kannwischer *et al.* [199] presents this framework and the results of 15 schemes from NIST PQC competition.

There are many studies that dealt with the performance assessment of PQC on various platforms from smartcards and constrained devices, e.g., [200], [201], [37], [202], [203]. For example, Nejatollahi *et al.* in [204] and [33] provide a survey of various software and hardware implementations of lattice-based cryptography schemes.

More works focused on the implementations of PQC schemes on constrained devices and/or in IoT/II services are presented next.

4.2 Lattice-based cryptography in IoT/II

Poppelmann *et al.* [205] compare 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 [206] presents the compression technique of Ring-LWE ciphertexts in order to implement these PQC schemes on constrained devices in IoT, Smart Cards, and RFID applications. The ciphertext size can be reduced by more than 40% at 128-bit security level. Albrecht *et al.* [207] use RSA co-processors on standard smart cards in order to accelerate lattice-based cryptography. Converted polynomials to big integers can be processed on a RSA co-processor and obtained results are then converted back to the polynomials. Furthermore, there are more papers focused on the implementation of concrete schemes, for example, the lattice-based Kyber on Cortex-M4 [208], NewHope on ARM Cortex-M[209], NTRUEncrypt for 8-bit AVR microcontrollers [210]. The intensive research and implementations prove that lattice-based PQC schemes can be deployed in various constrained devices in IoT. 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.

4.3 Multivariate cryptography in IoT/II

Yang *et al.* [211] provide the enTTS (20,28) scheme implementation, i.e., the protocol instance has less than 64-bit level of security, on 16-bit MSP430 chip. The signing phase takes 71 ms and verification phase about 726 ms. Czypek *et al.* [212] present C implementations of UOV, Rainbow and enTTS schemes for embedded devices. They also provide benchmark tests on 8-bit ATxMega128a1 microcontroller for all schemes with 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 signature. The Rainbow scheme provides time of 257 ms for signing and 288 ms for verifying. Shim *et al.* [213] propose their own MQ-signature scheme called HiMQ-3. The HiMQ-3 (128-bit security level instance) was run on 8-bit ATxmega384C3 microprocessor and required about 53 ms for signing and 166 ms for verifying signature. Moya Riera *et al.* [214] provide performance analysis of the Rainbow scheme on ARM Cortex-M4. The best results are produced by 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 signature verification.

4.4 Isogeny-based cryptography in IoT/II

Seo *et al.* [215] present high-speed implementations of SIDH and SIKE schemes for 32-bit ARMv7-A processor family. Their full key-exchange execution of SIDHp503 takes about 88 ms on a ARM Cortex-A15 and about 45 ms on an ARM Cortex-A72 (64-bit ARMv8-A). Joppe *et al.* [215] present an efficient Montgomery reduction algorithm for IBC on 32-bit embedded devices. They provide 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 [216], [217], [218], [219]. Koppermann *et al.* [220] provide implementations of SIDH, where ephemeral key exchange requires more than 18 s on a 32-bit Cortex-M4 and more than 11 mins on a 16-bit MSP430. In 2019, Hwajeong *et al.* [221] presented the first practical software implementation of SIKE on 32-bit ARM Cortex-M4 microcontrollers. Their key encapsulation of SIKEp434 takes about 1.94 s and only about 2.73 s for SIKEp503. Furthermore, authors also compare their work with SIDH implementation of Costello *et al.* [217] which is significantly slower. Costello's SIDHp503 implementation running on ARM Cortex-M4 microcontroller required about 28.55 s in total.

4.5 Hash-based cryptography in IoT/II

Rohde *et al.* [222] introduce the 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 s for signing and is more efficient than RSA-1024 signing operation. The size of the signature is 2350 B and the size of the private key is 848 B (RSA needs only 128 B for both parameters). Pereira *et al.* [223] present the implementation of Merkle with W-OTS scheme which consumes up to 3000 B (for height H=16) in RAM on the ATmega128l (@7.37MHz, 4KiB SRAM, 128KiB ROM). The signing phase requires 0.6 s. Kannwischer *et al.* [199] present the results of the SPHINCS+ implementation for 36 variants. The measured signing times are from 22 seconds to 88 minutes on 32-bit ARM Cortex-M4 microcontroller (24 MHz), thus, the SPHINCS+ scheme is not suitable for these constrained platforms.

4.6 Code-based cryptography in IoT/II

Strenzke and Falko [224] implement the McEliece scheme (100-bits security level) on a microcontroller. Nevertheless, the key generation algorithm could not be implemented on the microprocessor for exceeding card's RAM size. Heyse *et al.* [225] deal 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 [226] presents the implementation of code-based BIKE on a Cortex-M4 microcontroller. The implementation employs reduced data representation and adequate decoding algorithms in order 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.

The overview of the 6 PQC families is depicted in Fig. 17. The presented examples for each PQC family include the performance and memory requirements taken from recent implementations. The green values indicate a potential suitability for an implementation on constrained devices. The red parameters indicate potential obstacles in case of the deployment on constrained devices. Table 5 and Table 6 show state-of-the-art implementations of PQC schemes on embedded devices using ARM Cortex-M and AVR microcontroller architectures. This comparison indicates that IBC and HBC schemes usually require significant amount of clock cycles per the operation. Furthermore, code-based and hash-based schemes often use large parameters, large public keys, large signatures (e.g. > tens kiB), hence, there are only few practical implementations on embedded devices with constrained memory, e.g., BIKE and Sphincs+.

4.7 Quantum Resistant Privacy-Enhancing Technologies

PET schemes are usually based on traditional security assumptions that are not resist to quantum computing attacks. Nevertheless, there are already several proposals of PETs that are quantum-resistant.

4.7.1 Quantum Resistant Group Signatures

The one of the first quantum resistant group signatures was introduced by Gordon *et al.* [231] in 2010. The authors presented a group signature scheme from lattice assumptions. Quantum resistant group signatures are usually based on lattice-based constructions but there are also schemes using code-based, hash-based constructions, chosen examples are listed as follows:

- **Better zero-knowledge proofs for lattice encryption and their application to group signatures. F. Benhamouda, J. Camenisch, S. Krenn, V. Lyubashevsky and G. Neven. 2014.** [232]: This group signature scheme is a "hybrid" in the sense that privacy features hold under a lattice-based assumption and security features are secured under discrete logarithm problem. To be noted that it is not a pure lattice-based group signature.
- **Simpler Efficient Group Signatures from Lattices. P. Q. Nguyen, J. Zhang and Z. Zhang. 2015.** [233]: A new lattice-based group signature is provably based on the hardness of the Small Integer Solutions (SIS) and Learning with Errors (LWE) problems in the random oracle model.
- **Provably Secure Group Signature Schemes from Code-Based Assumptions. M.F. Ezerman, H.T. Lee, S. Ling, K. Nguyen and H. Wang. 2015.** [234]: The paper introduces two provably secure group signature schemes from code-based assumptions, i.e., the hardness of the McEliece problem, the Learning Parity with 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 and 540 times smaller than the lattice-based scheme [233] for group of 256 users.
- **Post-quantum EPID signatures from symmetric primitives. D. Boneh, S. Eskandarian, B. Fisch. 2019.**[235]: This work deals with Enhanced Privacy ID signature schemes (group signatures) built only from symmetric primitives, such as hash functions and pseudo random functions. The scheme produces the post-quantum signature of size 6.74 MB for groups of size up to 2^{20}.

4.7.2 Quantum Resistant Ring Signatures

The first quantum resistant ring signatures schemes were proposed in 2007 by Zheng, Li and Chen who proposed the code-based ring signature scheme producing a signature size 144 + $126N$ bits where N is the size of the ring. Further, Cayrel *et al.* [236] presents one of the first lattice-based threshold ring signature scheme in 2010. Besides lattice-based and code-based RS schemes, there are several multivariate-based constructions, e.g. [237]. Chosen examples are listed as follows:

- **Zero-knowledge arguments for lattice-based accumulators: logarithmic-size ring signatures and group signatures without trapdoors, B. Libert, S. Ling, K. Nguyen, H. Wang, 2016.** [238]: The paper presents lattice-based logarithmic-size ring signatures based on RST scheme [239].
- **Towards practical lattice-based one-time linkable ring signatures. C. Baum, H. Lin, S. Oechsner, 2018.** [240]: The paper presents a linkable ring signature scheme constructed from a lattice-based collision-resistant hash function. The signature size is linear with the size of a ring.
- **A multivariate based threshold ring signature scheme. A. Petzoldt, S. Bulygin, J. Buchmann. 2013.** [237]: This work introduces a threshold ring identification and signature scheme that is based on the MQ-Problem. The scheme produces signatures of sizes cca 300 or 600 kB.
- **Efficient Multivariate Ring Signature Schemes. M.S.E. Mohamed, A. Petzoldt. 2017.** [241]: The work extends multivariate signature Rainbow scheme to ring signature scheme and presents public key reduction technique. The 6.8 kB public key for 50 users can be reduced by ca 68% to 2.1 kB and the signature size is ca 31 kB.

TABLE 5
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 [227]	LBC	C + ASM	ATxmega128A1 (32 MHz)	8-bit AVR	-	0.671	0.275
NewHope-256bit [209]	LBC	C + ASM	ARM Cortex M0 (32 MHz)	32-bit ARM	1.168	1.738	0.298
NewHope-1024cpa [199]	LBC	ASM	ARM Cortex-M4F (24 MHz)	32-bit ARM	1.034	1.495	0.206
NTRUEnc-256bit [210]	LBC	C + ASM	ATmega1281 (16 MHz)	8-bit AVR	-	1.539	2.103
NTRUEnc-256bit [228]	LBC	C	ARM Cortex M0 (32 MHz)	32-bit ARM	71.186	1.411	2.377
Kyber-1024 [199]	LBC	ASM	ARM Cortex-M4F (24 MHz)	32-bit ARM	1.575	1.779	1.709
Frodo-640AES [199]	LBC	ASM	ARM Cortex-M4F (24 MHz)	32-bit ARM	47.050	45.883	45.366
BIKE-1 [226]	CBC	C	ARM Cortex-M4 (168 MHz)	32-bit ARM	6.437	6.867	89.131
SIKEp751 [221]	IBC	ASM	ARM Cortex-M4 (168 MHz)	32-bit ARM	282	455	491
SIKEp751 [221], [217]	IBC	C	ARM Cortex-M4 (168 MHz)	32-bit ARM	3,651	5,918	6,359
SIDHp751 [221]	IBC	ASM	ARM Cortex-M4 (168 MHz)	32-bit ARM	-	457	520
SIDHp751 [221], [217]	IBC	C	ARM Cortex-M4 (168 MHz)	32-bit ARM	-	5,915	6,763
SIDHp751 [221], [220]	IBC	ASM	ARM Cortex-M4 (168 MHz)	32-bit ARM	-	1,992	2,260

TABLE 6
Comparison of Chosen Quantum Resistant Dig. 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 [205]	LBC	C + ASM	ATxmega128A1 (32 MHz)	8-bit AVR	10.537	2.814
BLISS-I [229]	LBC	C + ASM	ARM Cortex-M4F (168 MHz)	32-bit ARM	4.648	0.539
Dilithium-III [229]	LBC	C + ASM	ARM Cortex-M4F (168 MHz)	32-bit ARM	8.348	2.342
FALCON-I [230]	LBC	C	ARM Cortex-M4F (24 MHz)	32-bit ARM	80.503	0.530
qTesla-I [199]	LBC	C	ARM Cortex-M4F (24 MHz)	32-bit ARM	5.830	0.787
Sphincs-sha256-128f [199]	HBC	C	ARM Cortex-M4F (24 MHz)	32-bit ARM	952.977	42.386
UOV [212]	MVC	C	ATxMega128a1 (32 MHz)	8-bit AVR	13.314	14.134
Rainbow [212]	MVC	C	ATxMega128a1 (32 MHz)	8-bit AVR	8.227	9.216
enTTS [212]	MVC	C	ATxMega128a1 (32 MHz)	8-bit AVR	2.142	30.789
HiMQ-3big [213]	MVC	C	ATxmega384C3 (32 MHz)	8-bit AVR	0.959	2.219
HiMQ-3small [213]	MVC	C	ATxmega384C3 (32 MHz)	8-bit AVR	1.247	5.328
Rainbow [212]	MVC	C	ARM Cortex-M4 (16 MHz)	32-bit ARM	2.930	1.321

4.7.3 Quantum Resistant Blind Signatures

The first quantum resistant blind signature scheme was presented by Rückert [242] in 2010. 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 [243], code-based [93] or isogeny-based [244]. Chosen examples are listed as follows:

- **Isogeny-based Quantum-resistant Undeniable Blind Signature Scheme. M.S. Srinath, V. Chandrasekaran. 2016.** [244]: The work presents an Undeniable Blind Signature scheme (UBSS) based on isogenies between supersingular elliptic curves.
- **A round-optimal lattice-based blind signature scheme for cloud services. H. Zhu *et al.* 2017.** [92]: The paper presents a round-optimal lattice-based blind signature scheme based on the closest vector problem using infinity norm.
- **A practical multivariate blind signature scheme. A. Petzoldt, A. Szepieniec, M.S.E. Mohamed. 2017.** [243]: The paper proposes a generic technique to transform the Rainbow multivariate signature scheme into a blind signature schemes. The proposed scheme produces 28.5 kB blind signatures with using 70.2 kB private key and 106.8 kB public key for 128-bit security level.
- **A code-based blind signature. O. Blazy, P. Gaborit, J. Schrek, N. Sendrier. 2017.** [93]: This paper introduces the first blind signature protocol that employs code-based cryptography and provides quantum resistance.

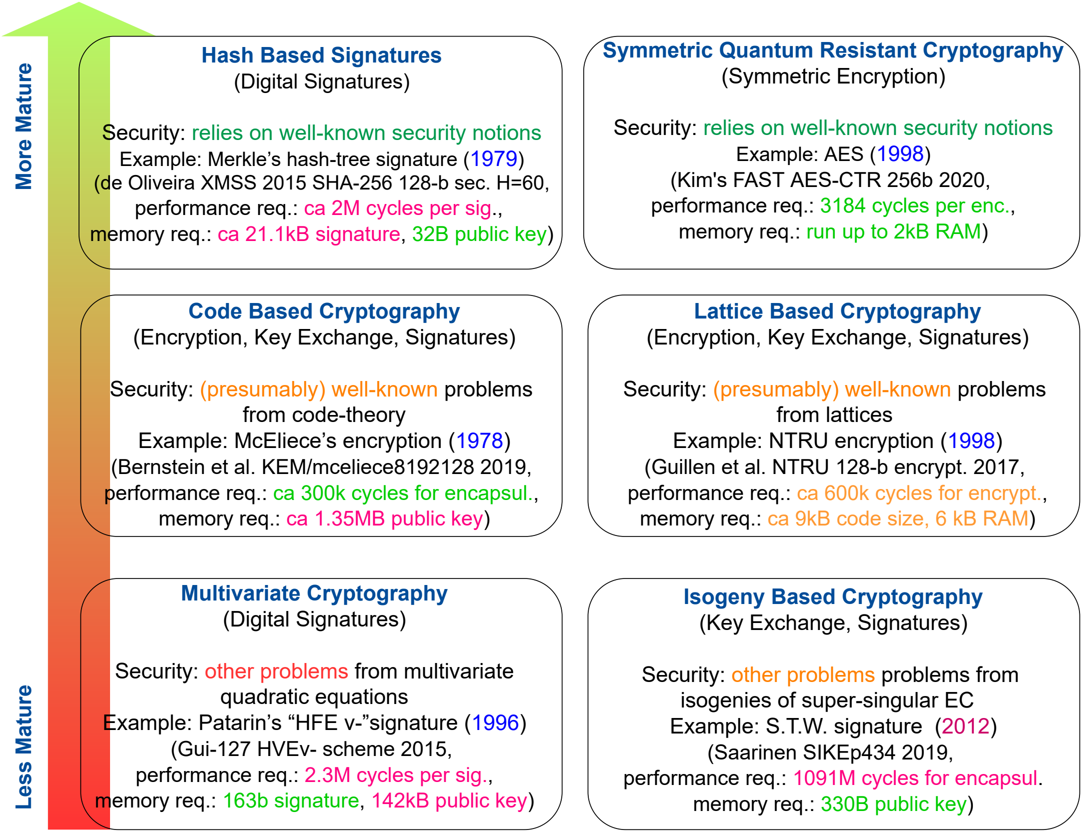
4.7.4 Quantum Resistant Attribute-Based Credentials

ABC schemes are usually based on group signature primitives and/or attribute based signatures schemes (ABS). Quantum resistant ABC have been developed from QR GS schemes. Chosen examples of QR ABC are listed as follows:

- **Fully anonymous attribute tokens from lattices. Camenisch, Neven and Ruckert, 2012.** [245]: The paper presents the lattice-based constructions for anonymous attribute tokens where users use issued attribute-containing credentials that revealing only a subset of their attributes.
- **Relaxed lattice-based signatures with short zero-knowledge proofs. Boschini, Camenisch and Neven, 2018.** [246]: This research presents a lattice-based anonymous attribute token scheme that offers the post-quantum security. The size of AA token from lattices is 17.77 MB.
- **Efficient lattice-based zero-knowledge arguments with standard soundness: construction and applications. R. Yang *et al.* 2019.** [247]: The paper presents an argument system and the designs of privacy-preserving methods based on lattices.

4.7.5 Quantum Resistant Mixnets

Recently, several mixnets solutions using post-quantum cryptography primitives have been proposed. Quantum re-



Hash Based Signatures
(Digital Signatures)

Security: relies on well-known security notions
Example: Merkle's hash-tree signature (1979)
(de Oliveira XMSS 2015 SHA-256 128-b sec. H=60,
performance req.: ca 2M cycles per sig.,
memory req.: ca 21.1kB signature, 32B public key)

Symmetric Quantum Resistant Cryptography
(Symmetric Encryption)

Security: relies on well-known security notions
Example: AES (1998)
(Kim's FAST AES-CTR 256b 2020,
performance req.: 3184 cycles per enc.,
memory req.: run up to 2kB RAM)

Code Based Cryptography
(Encryption, Key Exchange, Signatures)

Security: (presumably) well-known problems
from code-theory
Example: McEliece's encryption (1978)
(Bernstein et al. KEM/mceliece8192128 2019,
performance req.: ca 300k cycles for encapsul.,
memory req.: ca 1.35MB public key)

Lattice Based Cryptography
(Encryption, Key Exchange, Signatures)

Security: (presumably) well-known problems
from lattices
Example: NTRU encryption (1998)
(Guillen et al. NTRU 128-b encrypt. 2017,
performance req.: ca 600k cycles for encrypt.,
memory req.: ca 9kB code size, 6 kB RAM)

Multivariate Cryptography
(Digital Signatures)

Security: other problems from multivariate
quadratic equations
Example: Patarin's "HFE v-"signature (1996)
(Gui-127 HVEv- scheme 2015,
performance req.: 2.3M cycles per sig.,
memory req.: 163b signature, 142kB public key)

Isogeny Based Cryptography
(Key Exchange, Signatures)

Security: other problems problems from
isogenies of super-singular EC
Example: S.T.W. signature (2012)
(Saarinen SIKEp434 2019,
performance req.: 1091M cycles for encapsul.
memory req.: 330B public key)

Fig. 17. Overview of PQC families with examples.

sistant Mixnets usually substitute public key cryptography used for key establishment by PQC alternatives. Some examples of proposed QR mixnet systems are listed as follows:

- **Proof of a shuffle for lattice-based cryptography. N. Costa, R. Martinez, P. Morillo. 2019.** [248]: This paper presents the first proof of a shuffle based on lattice-based cryptography. The paper shows how to create a universally verifiable mix-net for mixing votes that are encrypted by a RLWE encryption scheme.
- **A verifiable and practical lattice-based decryption mix net with external auditing. X. Boyen, T. Haines, J. Muller. 2020.** [249]: The paper presents a verifiable decryption mixnet that employs practical lattice-based primitives with the identification of 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 public key is 93 kB.

4.7.6 Quantum Resistant Homomorphic Encryption

Lattices provide both additive and multiplicative homomorphisms and can serve as an ideal mathematical object to build fully homomorphic encryption. Hence, there are many proposals of lattice-based FHE schemes e.g. Gentry's FHE scheme [133] proposed in 2009. Besides lattice-based HE schemes, Bogdanov and Lee [250] proposed homomorphic encryption from codes in 2011. Few examples of quantum resistant HE schemes are as follows:

- **Fully homomorphic encryption using ideal lattices. Gentry. 2009.** [133]: The first proposal of fully homomorphic encryption scheme. The scheme uses ideal lattices and is almost bootstrappable. More details are described in Gentry's Ph.D. thesis [251].
- **(Leveled) fully homomorphic encryption without bootstrapping. Brakerski, Gentry and Vaikuntanathan. 2014.** [252]: The scheme is based on LWE problem. They use batching to parallel computations on messages and modulus switching technique to manage noise.
- **Efficient fully homomorphic encryption from (standard) LWE. Brakerski and Vaikuntanathan. 2014.** [253]: The article presents leveled FHE scheme based on the (standard) learning with errors (LWE) assumption. The scheme generates very short ciphertexts thanks to new proposal of dimension-modulus reduction technique. This is the first time where key and modulus switching techniques are introduced.
- **Dynamic fully homomorphic encryption-based merkle tree for lightweight streaming authenticated data structures. Xu *et al.* 2018.** [254]: The authors present fully homomorphic encryption-based Merkle Tree (FHMT) as a novel technique for streaming authenticated data structures for streaming verifiable computation.
- **Tfhe: Fast fully homomorphic encryption over the**

torus. Chillotti, Gama, Georgieva, Izabachene. 2018. [255]: This work describes a fast FHE scheme over the torus (TFHE), and revisits, generalizes and enhances the FHE based on GSW and its ring versions.

4.7.7 Quantum Resistant Searchable Encryption

Many searchable encryption schemes are based on the 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. Zhang *et al.*'s lattice based searchable encryption scheme [256] in 2012. Some examples are listed as follows:

- **Semantic searchable encryption scheme based on lattice in quantum-era. Y. Yang , M. MA. 2016.** [257]: The work describes a public key encryption with semantic keyword search using the LBC construction based on learning with errors (LWE) problem.
- **Lattice-based public key searchable encryption from experimental perspectives. R. Behnia, M.O. Ozmen, A.A. Yavuz, 2018.** [258]: The paper presents lattice-based Public key Encryption with Keyword Search (PEKS) that uses NTRU.

4.7.8 Quantum Resistant Attribute-Based Encryption

Many ABE schemes are based on bilinear map over elliptic curves but these schemes do not provide post-quantum security. Nevertheless, few ABE schemes based on lattice have been proposed in order to be quantum resistant. The first lattice ABE scheme was introduced by Boyen [259] in 2012. Chosen QR ABE examples are presented as follows:

- **Functional encryption for threshold functions (or fuzzy IBE) from lattices. S. Agrawal *et al.* 2012.** [260]: The work introduces a fuzzy identity-based encryption (fuzzy IBE) scheme based on lattices that is among the first realization of quantum resistant ABE.
- **Attribute-based functional encryption on lattices. X. Boyen. 2013.** [259]: The paper presents an efficient key-policy ABE proposal using LWE problem that is secured in the standard model.
- **Efficient attribute-based encryption from R-LWE. W. Zhu *et al.* 2014.** [261]: The work proposes an efficient ABE scheme based on the learning with errors over rings (R-LWE).

4.7.9 Quantum Resistant Secure Multi-Party Computation

Quantum resistant secure multi-party computation has been studied in several papers such as [262], [263], [264]. QC SMC are usually based on quantum resistant encryption techniques such as QR homomorphic encryption. For example, the paper [262] proposes a new notion of secure multiparty computation based on FHE from NTRU encryption. Recently, Kim *et al.* [264] focus on round-efficient and secure MPC protocols based on LWE assumption. The combination of secure multi-party and PQC is still ongoing research.

4.7.10 Other PETs

Only cryptography-based PET solutions (named in the previous subsections) have concerns in the post-quantum era and should be promoted to post-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.

4.7.11 Summary

Since 2010, there are many proposals of quantum-resistant PETs. The most promising PQC family is lattice-based cryptography that is employed in the most of cryptography-based PETs. Fig. 18 depicts the deployment of PQC families in PETs that is mainly based on mapped QR PETs in this survey. To be noted that more quantum resistant PETs schemes may exist.

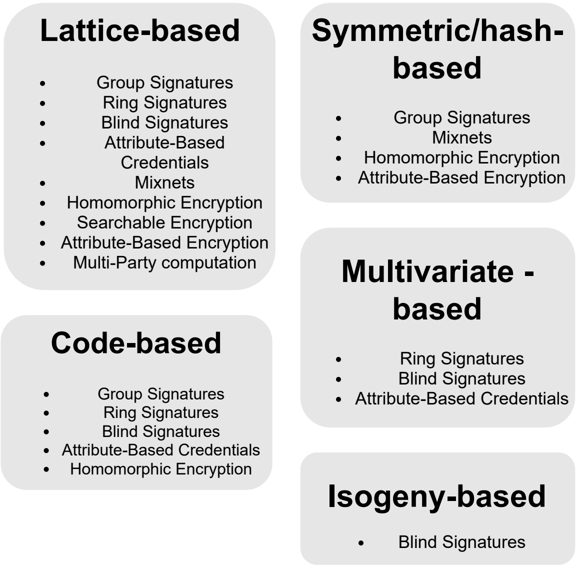


Fig. 18. Deployment of PQC in PETs.

5 Deployment of Privacy-enhancing Technologies in Intelligent Infrastructures

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

5.1 Practical Deployment of PETs

This section contains the identification of 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 EU. Table 7 maps the PETs in current or past research projects. PETs as concrete products or pilots are listed and shortly described in Tables 8, 9.

5.2 Use Cases of PETs

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

TABLE 7
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.
	PERCY	The FP7 project focused on cryptographic primitives and protocols that let human users deal with cryptographic keys and encrypted personal data and also dealt with group signatures based on lattice problems.
	HIPERLATCRYP	The FP7 project deals also with the development of a special type of multiuser anonymous digital signatures.
Ring Signatures	PRISMACLOUD	This project partly did research in constructing the logarithmic sized ring signatures.
	Scalable & Private Voting through Bilinear Pairings	This a proposal of ZK Labs Research's project (submitted to Aragon Nest) that should enable private and scalable voting and authentication system based on Ethereum and linkable ring signatures.
Attribute-Based Credential	ABC4Trust	The goal of ABC4Trust FP7 project is to address the federation and interchangeability of technologies that support trustworthy yet privacy-preserving Attribute-based Credentials (ABC).
Mix-networks and Proxies	Privacy and Accountability in Networks via Optimized Randomized Mix-nets (PANORAMIX)	This H2020 project focuses on the development of 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. The project aims at creating a European mix-network open-source codebase and infrastructure.
Homomorphic Encryption	Towards Practical Fully Homomorphic Encryption	Research deals with investigation on algorithmic optimizations to speed up LWE-based schemes, software implementations on CPUs and GPUs and building a LWE-FHE based homomorphic instruction set.
	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.
	PROgramming Computation on EncryptEd Data (PROCEED)	U.S. Department of Defense program that seeks to make computation on encrypted data practical.
Searchable Encryption	Project 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.
	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.
	Tredisec Trust-aware, REliable and Distributed Information SEcurity in the Cloud	The main goal of this project is to provide data confidentiality, integrity and availability guarantees in cloud by leveraging the cryptographic techniques.
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.
	Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare	The goal of this project is to ensure security and privacy of the sensitive personal data and also to ensure the trust of the users on healthcare services in a cloud environment.
	Secure Computation on Encrypted Data	The project focuses on (i) to design pairing and lattice-based encryption that is more efficient and usable in practice; and (ii) to get a better understanding of expressive functional encryption schemes and to push the boundaries from encrypting data to encrypting software.
Secure Multi-party Comp.	Better MPC Protocols in Theory and in Practice	The project proposes the state of the art for SMC protocols.
	Implementing Multi-Party Computation Technology	The goals of this project include the design of methodologies for coping with the asynchronicity of networks, for realistically measuring and modeling SMC protocols performance, for utilizing low round complexity protocols in practice, for dealing with problems with large input sizes, and many more.
Data Splitting	CLARUS	The CLARUS H2020 project aims to enhance trust in cloud computing by creating a secure framework for the storage and processing of data outsourced to the cloud. Data splitting is included in the solution.
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 use of the core statistical products. The algorithms under development will be used for the 2020 Census in US.

5.2.1 *Use Cases of Group Signatures*

- **Public transport**: if a user has a valid pre-payed ticket then 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 a winner can be securely traced by the authority.
- **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 in Internet of Vehicles**: a user driving vehicles can anonymously share traffic/car status messages (to road infrastructure/tolls/to other vehicles) that are signed by a GS scheme. Malicious users/cars sending bogus messages could be revoked.
- **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. Malicious users/cars sending bogus messages could be revoked.

TABLE 8
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 [87]) 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 which 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 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 primarily protection against spam and DoS attacks. Furthermore, the technology promises more privacy-preserving properties compare with 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 [265], SW release 2007). The system is based on Camenisch-Lysyanskaya signature [266] that allows the issuer to sign user's attributes to create a cryptographic credential. By using the zero-knowledge protocol, the user randomizes and sends the credential to a verifier in order to anonymously prove his/her possession of attributes. The specification of the Identity Mixer Cryptographic Library was released in 2010 [267].. WWW: https://github.com/IBM-Cloud/idemix-issuer-verifier
	U-Prove	U-Prove is a user-centric cryptographic technology based on Brands techniques [95] 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 [268]. More about U-Prove technology can be found in [269]. 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/irmacard
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 privacy 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 that 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

- **Privacy-preserving e-voting**: users should be able to cast votes anonymously, where votes are signed by GS.
- **Privacy-preserving e-cash**: GS are used for protecting the privacy of users transactions that are signed by GS.

5.2.2 Use Cases of Ring Signatures

- **Privacy-preserving auctions/tenders**: users as buyers submit bids/tenders (i.e. signed messages by a 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 claimability features.
- **Privacy-preserving e-voting**: users should be able to cast votes anonymously where votes are signed by RS scheme. All double-votes or multiple-votes can be detected.
- **Privacy-preserving e-cash**: RS schemes protect the privacy of users who perform and sign transactions. Double spending can be detected.

5.2.3 Use Cases of Blind Signatures

- **Parking**: BS can be used to blind 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 they funds are transferred.
- **e-voting**: BS can be used to guarantee voter's privacy for confidentiality and voter's digital signature for voter's authentication.

TABLE 9
PETs in Products and Pilots (II.)

PETs	Pilot/Product	Description
Onion Routing	Tor	Tor [121] 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 making 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 which 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 visualisations, dashboards or reports. The 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, which contains a query analysis and a rewriting engine to enforce DP for general-purpose SQL queries. The rewriting engine is able to 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 on 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) [270], 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 in practice. Now, RAPPOR has been made an open source project. WWW: https://github.com/google/rappor.

5.2.4 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 ask for a car-sharing service.
- **Office access**: a user can request access to her office or lab as being an employee/student/professor.
- **Club membership**: a user can prove his membership and his valid payment for a membership fee.
- **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 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.

5.2.5 Use Cases of Mixnets and Onion routing

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

5.2.6 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 to 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.
- **HealthCare**: HE enables a clinic analysis over sensitive data of patients.
- **e-voting**: HE protects the privacy of voters 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.

5.2.7 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.
- **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.

5.2.8 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 for retrieving their desired data from an untrusted service provider without disclosing sensitive information about the actual data.
- **Traffic Control Management in Internet of Vehicles**: ABE can be used to share sensitive traffic information among the drivers or vehicle sensors [155].

TABLE 10
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					✓	✓	✓	✓	

5.2.9 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.
- **Smart grid networks**: computation over fine-grained smart metering data without revealing any individuals energy consumption to support energy services.

5.3 Summary

Table 10 summaries the practical deployment of PETs in various use cases based on current state of the art. Group signatures are the basic cryptography primitives that can be applied in the most use cases. Further, ABC and HE approaches are widely used. To be noted that there may exist more PET-based systems that can be employed in various use cases.

6 Selected Case Study of Privacy-Enhancing Technologies

In order to demonstrate how PETs can improve security and privacy in practical scenarios, we focus on a Privacy-Enhancing Vehicle Parking Service (PE-VPS) that is a part of Internet of Vehicle environment.

6.1 Privacy-Preserving Vehicle Parking Service

Let us consider a case where a vehicular 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 associated parking device. Automating this scenario would benefit with the quicker and reliable parking service, however it also brings 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 on by intended scenario actors.

6.1.1 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 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 an access of the vehicles to a parking lot, and controls and releases parking permits.
- **Parking Service Provider** (PSP): a main system entity that provides an interface between users and parking lot terminals that are integrated in the system. PSP registers/removes users and cooperates on checking the parking availability based on a user location and his/her preferences. We assume that PSP is honest but can be curious.
- **Trusted Third Party** (TTP): a 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 firstly must be registered in TTP and PSP in order to use PE-VPS and to find available parking space.

6.1.2 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 during using the system by external parties or other users.
- **unlinkability**: parking actions of the same user (vehicle) should not be linked together by PSP or other users.
- **untraceability**: user's credentials and/or parking actions cannot be traced by PSP.

The system security requirements are as follows:

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

6.1.3 Phases of Privacy-Preserving Vehicle Parking Service

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

- **Registration phase**: Fig. 19 depicts the basic principle of the Registration phase with steps (1) and (2). In step (1), a user makes a registration with TTP in order to check his identity and his personal information such as name, phone, email, vehicle plate number, vehicle plate number. The user obtains the signed TTP credential, e.g. Attribute-based Credential (ABC) with user's attributes that are issued by TTP. In step (2), the user makes a registration with PSP when he/she shows/proves only necessary attributes, e.g. email, VPN by 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) which is then used by the user for pseudonymous access to a parking service. In this step, the anonymous payment can be deployed in order to prepaid a balance/credit for parking permits on the certain time period.
- **Request phase**: Fig. 19 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) in order to anonymously access user into the service and create a secure channel which prevents eavesdropping. Then, the user 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, that PSP is not able to recognize user's VPN and track his/her behaviour in the system.
- **Parking phase**: Fig. 20 depicts the parking phase with steps (5) and (6). In step (5), the user device transfers to the vehicle (an on board unit) PLT name and target location in order to navigate to PLT. In step (6), the user device asks to enter the PLT with the parking permit (PLT name, target location and the signature of unblinded VPN) in order to activate automatic parking. The access is allowed to the vehicle with the valid parking permit and with valid VPN

that is taken by a camera and checked as the input of the unblinded VPN signature (by BS verification).
- **Revocation** phase - in case that a user breaks rules or simply leaves the PSP service, his/her PSP credential is revoked (e.g. added in Blacklist, removed from Whitelist etc.).

6.1.4 Deployment of PETs in Vehicle Parking Service

In privacy-friendly scenario of Vehicle Parking Service (VPS) and its related IoV subsystems (e.g. payment, communication), the following PETs can be applied in order 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 during 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 in order 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 uses RS. User transactions are then hidden to 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 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.

6.2 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 II/IoT 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 in order to resist quantum attacks as follows:

- **Quantum-resistant Communication Security Protocols**: used secure communication channels such as TLS sessions should choose suitable ciphersuites 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 been already analyzed and tested on real devices (ARMs, FPGAs, PCs). Nevertheless, the concrete recommended PQC schemes will be announced by NIST in 2022 - 2024.
- **Quantum-resistant Attribute-based Credentials**: employing lattice-based anonymous attribute tokens, e.g. [245], [246], may prevent quantum computer attacks but 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 delay 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 [243] with 28.5 kB signatures, can be practical from communication header perspective. In addition, classic multivariate schemes have been already 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 [235]. These sizes are not very practical for IoV environment with constrained devices and limited communication overhead. Future research should be oriented on 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 [241]. The implementations of multivariate schemes into cryptocurrencies for secure payments can be 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 in order to be secure in post quantum era.

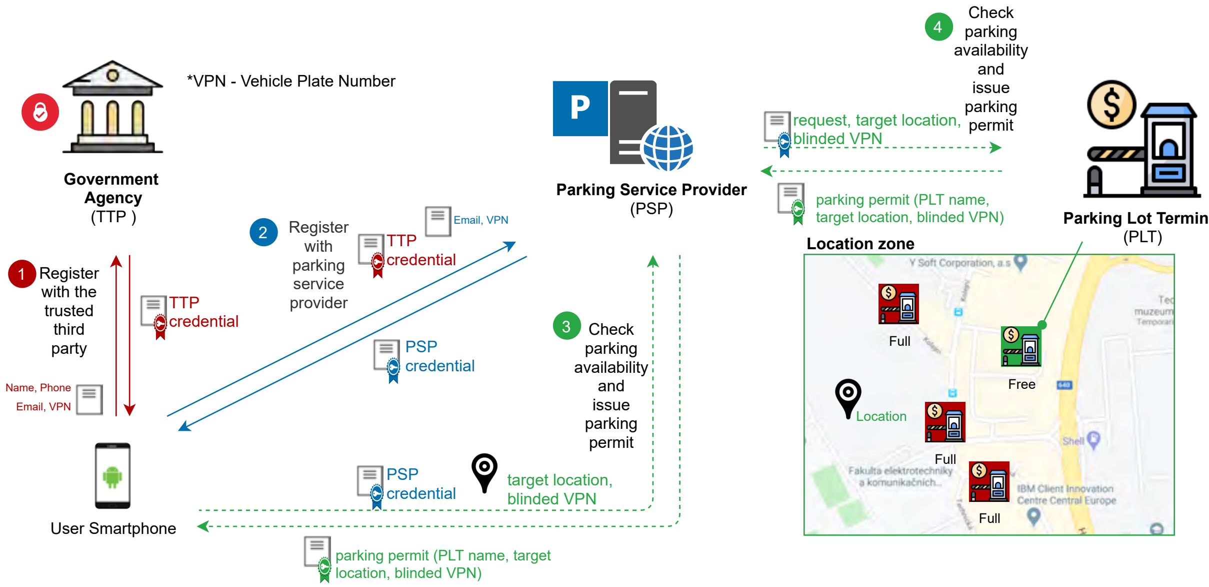

*VPN - Vehicle Plate Number
Government Agency (TTP)
1 Register with the trusted third party
Name, Phone Email, VPN
TTP credential
2 Register with parking service provider
TTP credential
Email, VPN
PSP credential
Parking Service Provider (PSP)
3 Check parking availability and issue parking permit
PSP credential
target location, blinded VPN
parking permit (PLT name, target location, blinded VPN)
User Smartphone
4 Check parking availability and issue parking permit
request, target location, blinded VPN
parking permit (PLT name, target location, blinded VPN)
Parking Lot Terminal (PLT)
Location zone
Full
Free
Location
Full
Full

Fig. 19. Registration and Request phases in PE-VPS.

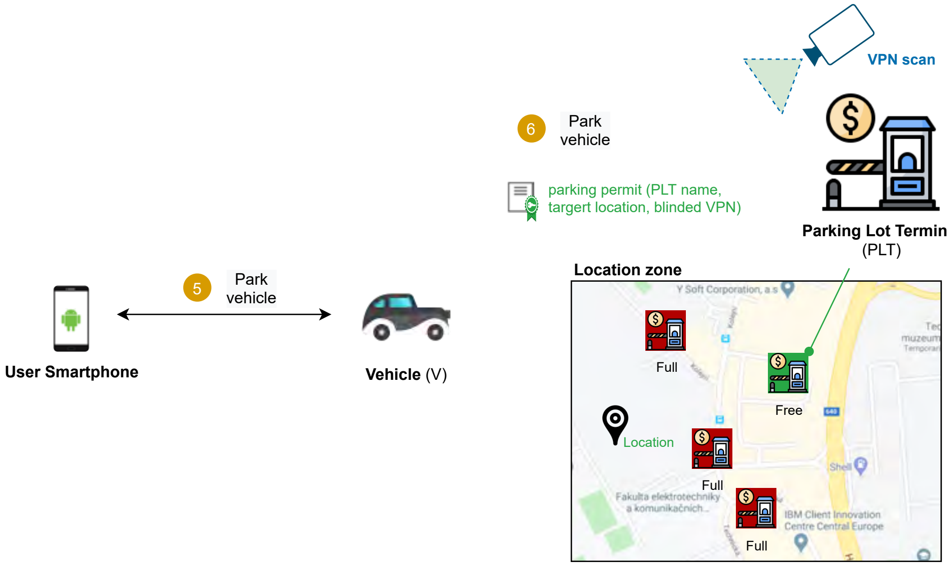


Fig. 20. Parking phase in PE-VPS.

7 Conclusion

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

ACKNOWLEDGMENTS

This paper is supported in part by European Union's Horizon 2020 research and innovation program under grant agreement No 830892, project SPARTA. The National Sustainability Program under Grant no. LO1401 and the Technology Agency of the Czech Republic under "Legal and technical tools for privacy protection in cyberspace" project (TL02000398) financed the research described in this article. For the research, the infrastructure of the SIX Center was used.

REFERENCES

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

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[8] W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, and X. Shen, "Internet of vehicles in big data era," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 19–35, 2017.

[9] Q. Kong, R. Lu, M. Ma, and H. Bao, "A privacy-preserving sensory data sharing scheme in internet of vehicles," *Future Generation Computer Systems*, vol. 92, pp. 644–655, 2019.

[10] A. Solanas, C. Patsakis, M. Conti, I. S. Vlachos, V. Ramos, F. Falcone, O. Postolache, P. A. Pérez-Martínez, R. Di Pietro, D. N. Perrea *et al.*, "Smart health: a context-aware health paradigm within smart cities," *IEEE Communications Magazine*, vol. 52, no. 8, pp. 74–81, 2014.

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

[12] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 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] 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.

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

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

[30] 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.

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

[32] T. G. Tan and J. Zhou, "A survey of digital signing in the post quantum era."

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

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

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

[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] 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.

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

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

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] 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.

[57] 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.

[58] 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.

[59] 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.

[60] 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.

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

[62] 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.

[63] 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.

[64] 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.

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

[66] 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.

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

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

[69] 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.

[70] 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.

[71] 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.

[72] 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.

[73] 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.

[74] 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.

[75] 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.

[76] 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.

[77] 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.

[78] 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.

[79] 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.

[80] 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.

[81] 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.

[82] 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.

[83] 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.

[84] 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.

[85] 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.

[86] 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.

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

[88] 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.

[89] 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.

[90] 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.

[91] 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.

[92] 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.

[93] 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.

[94] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Communications of the ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.

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

[96] 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.

[97] 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.

[98] 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.

[99] 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.

[100] 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.

[101] 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.

[102] 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.

[103] 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.

[104] 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.

[105] ——, "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.

[106] ——, "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.

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

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

[109] D. Kesdogan, J. Egner, and R. Büschkes, "Stop-and-go-mixes providing probabilistic anonymity in an open system," in *International Workshop on Information Hiding*. Springer, 1998, pp. 83–98.

[110] C. Gulcu and G. Tsudik, "Mixing e-mail with babel," in *Proceedings of Internet Society Symposium on Network and Distributed Systems Security*. IEEE, 1996, pp. 2–16.

[111] O. Berthold, H. Federrath, and S. Köpsell, "Web mixes: A system for anonymous and unobservable internet access," in *Designing privacy enhancing technologies*. Springer, 2001, pp. 115–129.

[112] 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.

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

[114] 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.

[115] P. Golle and A. Juels, "Parallel mixing," in *Proceedings of the 11th ACM conference on Computer and communications security*. ACM, 2004, pp. 220–226.

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

[117] 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.

[118] 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.

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

[120] 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.

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

[122] J. A. Pouwelse, P. Garbacki, J. Wang, A. Bakker, J. Yang, A. Iosup, D. H. Epema, M. Reinders, M. R. Van Steen, and H. J. Sips, "Tribler: a social-based peer-to-peer system," *Concurrency and computation: Practice and experience*, vol. 20, no. 2, pp. 127–138, 2008.

[123] 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.

[124] 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.

[125] 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.

[126] 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.

[127] 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.

[128] 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.

[129] 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.

[130] 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.

[131] 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.

[132] 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.

[133] C. Gentry *et al.*, "Fully homomorphic encryption using ideal lattices." in *Stoc*, vol. 9, no. 2009, 2009, pp. 169–178.

[134] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2010, pp. 24–43.

[135] 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.

[136] 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.

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

[138] 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.

[139] 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.

[140] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in *Proceeding Sof the International Conference on Computational Science and Its Applications, Part I*, ser. ICCSA '08, 2008, pp. 1249–1259.

[141] Q. Chai and G. Gong, "Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers," in *2012 IEEE International Conference on Communications (ICC)*, June 2012, pp. 917–922.

[142] M. Shen, B. Ma, L. Zhu, X. Du, and K. Xu, "Secure Phrase Search for Intelligent Processing of Encrypted Data in Cloud-Based IoT," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1998–2008, April 2019.

[143] C. Guo, R. Zhuang, Y. Jie, K. R. Choo, and X. Tang, "Secure Range Search Over Encrypted Uncertain IoT Outsourced Data," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1520–1529, April 2019.

[144] 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.

[145] 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.

[146] 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.

[147] 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.

[148] C. Yang, R. Harkreader, and G. Gu, "Empirical evaluation and new design for fighting evolving Twitter spammers," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1280–1293, 2013.

[149] 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.

[150] H. Ma, R. Zhang, S. Sun, Z. Song, and G. Tan, "Server-aided fine-grained access control mechanism with robust revocation in cloud computing," *IEEE Transactions on Services Computing*, pp. 1–1, 2019.

[151] 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.

[152] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," *Future Generation Computer Systems*, vol. 49, pp. 104 – 112, 2015.

[153] N. Oualha and K. T. Nguyen, "Lightweight Attribute-Based Encryption for the Internet of Things," in *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, Aug 2016, pp. 1–6.

[154] 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.

[155] 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.

[156] 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.

[157] 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.

[158] 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.

[159] 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.

[160] 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.

[161] 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.

[162] A. B. Alexandru and G. J. Pappas, "Secure Multi-party Computation for Cloud-based Control," *arXiv e-prints*, p. arXiv:1906.09652, Jun 2019.

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

[164] 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.

[165] M. von Maltitz and G. Carle, "Leveraging Secure Multiparty Computation in the Internet of Things," in *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '18, 2018, pp. 508–510.

[166] 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.

[167] 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.

[168] 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.

[169] 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.

[170] 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.

[171] 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.

[172] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography Conference*. Springer, 2006.

[173] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, pp. 211–407, 2014.

[174] C. Clifton and T. Tassa, "On syntactic anonymity and differential privacy," *Trans. Data Privacy*, vol. 6, no. 2, pp. 161–183, 2013.

[175] 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.

[176] 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.

[177] 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.

[178] 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.

[179] 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.

[180] 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.

[181] 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.

[182] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange-a new hope." in *USENIX Security Symposium*, vol. 2016, 2016.

[183] 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.

[184] 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.

[185] 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.

[186] 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.

[187] 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.

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

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

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

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

[192] 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.

[193] 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.

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

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

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

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

[198] 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.

[199] M. J. Kannwischer, J. Rijneveld, P. Schwabe, and K. Stoffelen, "pqm4: Testing and benchmarking nist pqc on arm cortex-m4," 2019.

[200] 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.

[201] 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.

[202] 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.

[203] 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.

[204] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Software and hardware implementation of lattice-cased cryptography schemes," 2017.

[205] 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.

[206] 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.

[207] 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.

[208] 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.

[209] 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.

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

[211] 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.

[212] 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.

[213] 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.

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

[215] 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.

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

[217] 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,2016âĂŞ2018

[218] 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.

[219] 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.

[220] 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.

[221] 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.

[222] 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.

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

[224] 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.

[225] 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.

[226] 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.

[227] 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.

[228] 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.

[229] 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.

[230] 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.

[231] 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.

[232] 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.

[233] 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.

[234] 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.

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

[236] 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.

[237] 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.

[238] 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.

[239] 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.

[240] 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.

[241] M. S. E. Mohamed, A. Petzoldt, and C. RingRainbow, "Efficient multivariate ring signature schemes." *IACR Cryptology ePrint Archive*, vol. 2017, p. 247, 2017.

[242] M. Rückert, "Lattice-based blind signatures," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2010, pp. 413–430.

[243] 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.

[244] M. S. Srinath and V. Chandrasekaran, "Isogeny-based quantum-resistant undeniable blind signature scheme." *IACR Cryptology ePrint Archive*, vol. 2016, p. 148, 2016.

[245] 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.

[246] 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.

[247] 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.

[248] N. Costa, R. Martínez, and P. Morillo, "Lattice-based proof of a shuffle." *IACR Cryptology ePrint Archive*, vol. 2019, p. 357, 2019.

[249] X. Boyen, T. Haines, and J. Müller, "A verifiable and practical lattice-based decryption mix net with external auditing," 2020.

[250] A. Bogdanov and C. H. Lee, "Homomorphic encryption from codes," *arXiv preprint arXiv:1111.4301*, 2011.

[251] C. Gentry and D. Boneh, *A fully homomorphic encryption scheme*. Stanford University Stanford, 2009, vol. 20, no. 09.

[252] 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.

[253] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) lwe," *SIAM Journal on Computing*, vol. 43, no. 2, pp. 831–871, 2014.

[254] 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.

[255] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène, "Tfhe: Fast fully homomorphic encryption over the torus," *Journal of Cryptology*, pp. 1–58, 2018.

[256] 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.

[257] Y. Yang and M. Ma, "Semantic searchable encryption scheme based on lattice in quantum-era," 2016.

[258] 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.

[259] X. Boyen, "Attribute-based functional encryption on lattices," in *Theory of Cryptography Conference*. Springer, 2013, pp. 122–142.

[260] 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.

[261] 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.

[262] 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.

[263] 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.

[264] 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.

[265] 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.

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

[267] J. Camenisch *et al.*, "Specification of the identity mixer cryptographic library," Tech. rep, Tech. Rep., 2010.

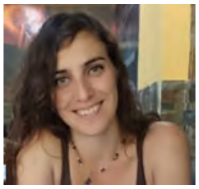
[268] C. Paquin and G. Zaverucha, "U-prove cryptographic specification v1.1 (revision 3)," *Technical Report, Microsoft Corporation*, 2013.

[269] C. Paquin, "U-prove technology overview v1.1 (revision 2)," *Microsoft Corporation Draft Revision*, vol. 1, 2013.

[270] 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*, 2014, pp. 1054–1067.

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 90 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 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 2018, she has been codirecting 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).