ITUPublications

International Telecommunication Union

Standardization Sector

ITU-T Technical Report

(06/2026)

XSTR.ac-pqc

Guidance on use of post-quantum cryptography (PQC)-based advanced cryptography

Technical Report ITU-T XSTR.ac-pqc

Guidance on use of post-quantum cryptography (PQC)-based advanced cryptography

Summary

Technical Report ITU-T XSTR.ac-pqc introduces advanced cryptographic mechanisms based on post-quantum cryptography (PQC) and provides technical guidance for their future use in environments such as IMT-2020/IMT-2030, cyber-physical systems, and large-scale IoT deployments. It focuses on advanced cryptographic techniques that can be constructed from PQC-related assumptions and primitives, including lattice-based assumptions. This guidance is intended to assist service designers and developers in selecting and applying PQC-based advanced cryptography in future advanced communication and application environments.

Keywords

Advanced cryptography, post quantum cryptography.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Table of Contents

Technical Report ITU-T XSTR.ac-pqc

Guidance on use of post-quantum cryptography (PQC)-based advanced cryptography

1 Scope

This Technical Report introduces advanced cryptographic mechanisms based on post quantum cryptography (PQC) and provides technical guidance for their future use in environments such as IMT-2020/IMT-2030, cyber-physical systems, and large-scale IoT deployments. It focuses on advanced cryptographic techniques that can be constructed from PQC-related assumptions and primitives, including lattice-based assumptions. This guidance is intended to assist service designers and developers in selecting and applying PQC-based advanced cryptography in future advanced communication and application environments.

2 References

None.

3 Definitions

3.1 Term defined elsewhere

This Technical Report uses the following term defined elsewhere:

3.1.1 authentication [b-ITU-T Y.2014]: A property by which the correct identity of an entity or party is established with a required assurance. The party being authenticated could be a user, subscriber, home environment or serving network.

3.2 Terms defined in this Technical Report

This Technical Report defines the following terms:

3.2.1 advanced cryptography: Advanced cryptography refers to cryptographic techniques that have more advanced functions (such as the ability to perform calculations and searches while encrypted) compared to conventional cryptography.

3.2.2 post-quantum cryptography: Cryptography that is designed to be secure against attacks by both quantum and classical computers and to interoperate with existing communications protocols and networks.

NOTE – Synonyms include quantum resistant cryptography and quantum secure cryptography.

3.2.3 primitive: A fundamental component of a cryptographic system that serves as a building block for constructing more complex cryptographic algorithms.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

GKA Group Key Agreement

KDC Key Distribution Centre

NIZK Non-Interactive Zero-Knowledge

PQC Post Quantum Cryptography

5 Conventions

None.

6 Introduction of PQC-based advanced cryptography

6.1 General

This Technical Report (TR) focuses on advanced cryptographic techniques based on PQC primitives selected through the NIST competition and by ISO/IEC JTC1/SC27. In other words, this TR does not cover advanced cryptographic techniques that employ structures or assumptions that differ significantly from those used in the PQC primitives of the NIST competition or ISO/IEC SC27 standards. Furthermore, traditional RSA- and DLP-based schemes are not PQC and are therefore also outside the scope of this TR.

This Technical Report covers advanced cryptographic techniques that provide features different from those of conventional cryptographic techniques, including:

– The ability to use a well-known email address or person's name as the encryption key, rather than a random encryption key.

– The ability to control access to files and documents by specifying attributes, e.g., employees with a position of section chief or higher.

– Logical and arithmetic operations can be performed while encrypted.

– Membership of a certain group can be authenticated while keeping personal information confidential.

– The ability to conceal access patterns to the DB.

These features can provide security functions that are not available in conventional cryptographic techniques. Because advanced cryptographic techniques have different characteristics and implementation constraints, and because their advantages can be used in a variety of applications and services, guidance is needed on how to select and implement an advanced cryptographic technique that is appropriate for a given purpose and use case.

Many conventional constructions of advanced cryptography have been greatly developed by utilizing pairings on elliptic curves and related computationally difficult problems. However, for advanced cryptography in the era of quantum computing, it is not possible to use the computational problem associated with pairing, and it is necessary to use the NP-hard problem or the related computational problem, as is also used in the basic cryptographic techniques (encryption, signature, etc.) of quantum computer-resistant cryptography (PQC). Currently, many advanced cryptosystems are constructed using lattice problems such as computational problems.

The following sub-clauses describe the advanced cryptographic technology based on PQC.

6.2 PQC-based advanced cryptography related to encryption

6.2.1 ID-based encryption

ID-based encryption is a type of public-key cryptography in which an arbitrary string of characters, including the user's ID, can be used as the public key. Since it is possible to use as the public key the name, e-mail address, ID, company name, department signature, or other information that the recipient of the ciphertext knows well and can recognize at a glance, it is more convenient than conventional cryptographic schemes that use public keys that have nothing to do with the recipient.

Specifically, in a mail service that encrypts mail bodies and attached files, the public key is the email address, which is the public information of each user, and the private key is generated by the service provider, who sends the private key to each user to keep. The sender of the e-mail encrypts the body of the e-mail using the e-mail address of the recipient as the public key (encryption key). The recipient

of the e-mail has the private key (decryption key) for the e-mail address and can decrypt and read this e-mail. Since the private key is information that only the recipient of the e-mail address has, the confidentiality of the e-mail is maintained. In this method, because the sender only needs the recipient's email address to create ciphertext that only the recipient can decrypt, there is no need to obtain the recipient's public key through communication or other means as in conventional public key cryptography.

For PQC-based identity-based encryption, the first lattice-based identity-based encryption scheme was proposed in 2008 [b-Gentry]. In 2014, an efficient scheme using a lattice structure called NTRU was proposed [b-Ducas]. In 2018, a scheme achieving strong security with reasonable parameters was proposed [b-Katsumata]. More recently, efficient lattice-based schemes have been proposed [b-Tomita], [b-Tomita, T].

6.2.2 Attribute-based encryption

Attribute-based encryption is a type of public-key cryptography that allows the decryption authority to be changed according to attributes such as the title, company name, or region name of the recipient of the ciphertext when decrypting the ciphertext. More precisely, by having an access structure corresponding to the attributes in the ciphertext or decryption key (secret key), the decryption authority for the ciphertext can be controlled collectively. If the access structure is created for each attribute in the conventional public key cryptosystem, the ciphertext is created according to the number of users using the public key of the user with the same attribute.

In contrast, attribute-based cryptography can provide an access structure with a single ciphertext, and is superior to conventional public-key cryptography in terms of efficiency. As an example of the use of attribute-based cryptography, a solution that uses attribute-based cryptography to realize a secure and efficient access control mechanism for encrypted files in a file exchange service via a cloud environment is provided.

For PQC-based attribute-based encryption, the first lattice-based attribute-based encryption scheme [b-Agrawal] was proposed in 2011, but it was shown in 2014 that the scheme works only under a restricted access policy [b-Boneh]. A scheme with strong security was proposed in 2019 [b-Tsabary], and further improvements were proposed in 2020 [b-Katsumata, S]. [b-ETSI TS 104 015], published in February 2025, specifies efficient quantum-safe hybrid key exchanges with hidden access policies, and should be referenced carefully as a related access-policy-based quantum-safe key establishment mechanism rather than as a general attribute-based encryption standard [b-ETSI TS 104 015].

6.2.3 Broadcast encryption

Broadcast encryption is a method that enables multiple authorized users to decrypt content encrypted for a designated receiver set by transmitting a ciphertext through a broadcast channel. In public-key broadcast encryption, the encryption key and the decryption keys are different: the sender uses public information for encryption, while each authorized receiver uses an individual secret key for decryption. In private-key broadcast encryption, the encryption key and decryption keys are secret. Public-key broadcast encryption is attractive because the sender can encrypt using public information.

Public-key broadcast encryption allows the sender to encrypt a message with a public key, and each of the authorized receivers can decrypt a ciphertext with an individual secret key. Although there are efficient pairing-based broadcast encryption schemes, PQC-based broadcast encryption requires a strong assumption (e.g., [b-Wee]) and no efficient PQC-based broadcast encryption scheme with a reasonable assumption is known at present.

6.2.4 Homomorphic encryption

Homomorphic encryption is a cryptographic technique that allows arithmetic operations (such as four arithmetic operations) to be performed while data is encrypted. The operations that can be performed differ depending on the encryption scheme, including addition only, multiplication only, and both addition and multiplication. Since the operations are performed in encrypted form, even if the data is

leaked during the operation, the raw data cannot be deciphered, and applications such as analysis in which the data is deposited in a computer with high processing speed are embodied. There are examples such as demonstration experiments aimed at improving the accuracy of fraudulent transaction detection by using transaction data from multiple financial institutions, or the analysis of IC cards of companies to secure the use of IC card usage history, boarding and alighting history, purchase history, and so on. In the field of machine learning there is research and development on a method for generating machine learning models while ensuring the privacy of the learning data by utilizing homomorphic cryptography.

As for homomorphic cryptography based on PQC, the first fully homomorphic cryptography based on PQC [b-Gentry, C] was proposed in 2009 on a lattice structure basis. Subsequently, BGV [b-Brakerski], FV [b-Fan], FHEW [b-Ducas, L], TFHE [b-Chillotti], and CKKS [b-Cheon] have been proposed, including practical fully homomorphic cryptography. Open-source fully homomorphic cryptography libraries such as the homomorphic encryption library (HElib) and the simple encrypted arithmetic library (SEAL) are also available.

6.2.5 Functional encryption (FE)

Functional encryption enables the generation of secret keys that allow computations on the encrypted data and subsequently decrypting the output. This provides fine-grained access control, allowing users to learn specific information about the encrypted data without revealing the entire plaintext. [b-Waters], [b-Wang].

In functional encryption, a key generation centre generates a public key and a secret key sk_F depending on a function F with the domain of plaintexts. A sender generates and sends a ciphertext of a plaintext m by using the public key. A receiver having the secret key sk_F can obtain $F(m)$ by decryption.

6.2.6 Predicate encryption (PE)

In predicate encryption, decryption capability is determined by a predicate rather than by possession of a conventional recipient-specific decryption key. Ciphertexts are associated with attributes, and secret keys are associated with predicates, which are Boolean functions defined over those attributes [b-Zhang], [b-Gorbunov].

A user holding a secret key for a predicate f can decrypt a ciphertext only if the predicate evaluates to true for the ciphertext attribute; that is, decryption is possible if and only if $f(x) = 1$. Otherwise, the ciphertext reveals no information about the plaintext beyond what is intentionally disclosed by the scheme.

6.2.7 Searchable encryption (SE)

Searchable encryption enables users to search encrypted data while preserving data privacy by using encrypted search queries. It is particularly relevant to cloud storage and other scenarios in which data confidentiality is required while search functionality must still be supported.

The data owner encrypts their data and creates a searchable index for the encrypted data. The encrypted data and the searchable index are stored on a server, such as a cloud server. When a user wants to search, they generate a "trapdoor" (a special encrypted query) based on the keyword they want to search for, after that the server uses the trapdoor to search the encrypted index without decrypting the data. It returns the identifiers of the documents that match the query. The user can then decrypt the matching documents using the appropriate key [b-Yang].

Technically, the scheme of public key encryption with keyword search (PEKS) is known to be equivalent to anonymous ID-based encryption [b-Abdalla].

6.2.8 Proxy re-encryption

Proxy re-encryption is an encryption scheme in which an entity different from the creator of the ciphertext (proxy) converts one ciphertext into another ciphertext whose plaintext is the same, without decrypting it. It is common for the secret key to be different between the input ciphertext and the output ciphertext. For this reason, it can be used in applications where the secret key needs to be updated or the owner has changed.

As an example of its use, it is particularly useful in cloud storage, where access privileges are expected to be changed dynamically, because it allows the recipient to be changed dynamically without decryption. In addition, by utilizing proxy re-encryption, it is also expected to be used in situations where devices with individual decryption keys are used separately, or where ciphertext stored on a server is converted into ciphertext that can be decrypted using the decryption key of the device being used. Other applications include encrypted email forwarding, key escrow, secure distributed file systems, and secure publish-subscribe systems.

For PQC-based proxy re-encryption, lattice-based schemes such as a concise scheme [b-Chandran] and an efficiency-oriented scheme [b-Polyakov] have been proposed. Schemes by [b-Davidson], [b-Fuchsbauer], and [b-Sato] have also been proposed to improve these schemes and achieve the desired security properties.

6.3 PQC-based advanced cryptography related to digital signature

6.3.1 Identity-based signature

ID-based signature is a digital signature that can generate signatures with a signature key associated with an ID, and a trusted third party called a key generation centre is used to generate the signature key. As PQC-based ID-based signatures, an efficient lattice-based construction was proposed with practical and appropriate parameter selection [b-Pan].

In general, it is known that an ID-based signature scheme can be constructed by combining two digital signatures [b-Bellare], [b-Kiltz], [b-Lee].

6.3.2 Attribute-based signature

Attribute-based signature is a digital signature in which the authority to generate signatures can be controlled. In particular, key-policy attribute-based signature schemes allow access policies and attributes to be bound to a signature key and a signature, respectively, so that signatures are accepted for verification only when the attributes satisfy the access policy. A scheme based on a lattice problem that satisfies adaptive security using the strong cryptographic primitive NIZK (non-interactive zero-knowledge) proof has been proposed [b-Kaafarani]. An efficient scheme without NIZK has also been proposed, but its security is considered relatively weaker [b-Luo].

6.3.3 Aggregate signature and multi-signature

An aggregate signature is a digital signature mechanism that can compress several distinct signatures into one compact signature [b-Boneh, D]. This type of signature is useful for reducing the total size of many signatures transmitted over a channel. For PQC-based aggregate signatures, several lattice-based schemes have been proposed [b-Sato, S], [b-Tomita 1], [b-Aardal].

On the other hand, multiple signature (multi-signature) is a digital signature scheme in which multiple signers generate compact signatures for the same message. Based on PQC, a scheme based on the lattice problem has been proposed in which the number of rounds of exchanges between signers after receiving a message to be signed (the number of rounds in the online phase) is two rounds [b-Damgard]. Another scheme with a one-round online phase and key aggregation has also been proposed [b-Boschini].

6.3.4 Threshold signature

Threshold signatures can generate valid signatures for the same message if a certain number of shares of the signature's partial information (shares) are gathered. This feature is useful for decentralizing the authority to generate signatures and has recently been applied in applications related to cryptographic assets.

As for PQC-based threshold signatures, a scheme based on the lattice problem has been proposed [b-Agrawal, S].

6.3.5 Group signature

Group signature allows members of a group to generate signatures that are acceptable for verification using the group's public key and have the anonymity of not allowing verifiers or third parties to identify which member of the group generated the signature. However, the group administrator can identify the group member who generated the signature.

As a group signature based on PQC, a scheme based on the lattice problem was first proposed [b-Gordon]. Further, the scheme is proposed based on the standard lattice assumption and has desirable properties and security such as the ability to dynamically add and remove group members and strong anonymity [b-Beullens].

6.3.6 Ring signature

A ring signature is an anonymous digital signature in which it can be verified that a signature was generated by one person in a group connected in the shape of a ring, and it is not possible to identify who generated the signature in the group. In a group signature, there is a group manager who can identify the signer who generated the signature, but in a ring signature, there is no such manager. Recently, ring signatures have been studied extensively in terms of applications to cryptographic assets.

One of the PQC-based ring signature schemes is based on the lattice problem [b-Esgin], which has the smallest signature size when the ring size is relatively small. On the other hand, when the ring size is large (e.g., 1 000 or more), the method [b-Beullens, W] is effective in reducing the signature size, which is also characterized by a small signature size.

6.3.7 Broadcast authentication

Broadcast authentication, where a central entity (e.g., a sender) wants to remotely and simultaneously control many arbitrary target entities (i.e., IoT devices) using one-to-many communications is considered, not individual communication between the sender and each IoT device. In the system, a sender broadcasts a command to all IoT devices so that only the designated devices can verify the validity of it. Each IoT device checks the validity of the command and executes the command if it is regarded as valid. A PQC-based broadcast authentication was proposed in [b-Aono]. An anonymous broadcast authentication, which is a broadcast authentication with anonymity, conceals information on designated entities against any device except for the information that the device itself is designated or not, as proposed in [b-Aono].

6.3.8 Batch verification

Batch verification techniques enhance efficiency by allowing multiple digital signatures based on the PQC to be verified simultaneously. This capability is particularly advantageous in group settings where numerous nodes need to verify each other's signatures efficiently.

6.4 Key agreement-based advanced cryptography

6.4.1 Group key agreement

Group key agreement (GKA) is a cryptographic protocol that enables a group of parties to establish a shared secret key over an insecure network. This key can then be used to secure communications

among the group members. The process ensures that the key is influenced by all participating parties and is not predetermined by any single party, which is crucial for maintaining the confidentiality and integrity of the group's communications.

6.4.2 Group key distribution

Group key distribution protocols are essential for secure communication within a group, ensuring that a shared secret key is distributed among all group members. These protocols are designed to handle dynamic group membership, allowing new members to join and existing members to leave without compromising the group's security. One common approach is the logical key hierarchy (LKH), which uses a hierarchical structure to efficiently manage keys and minimize the number of rekeying operations required when membership changes. Another method is the use of a key distribution centre (KDC), which acts as a trusted authority to distribute session keys to group members. These protocols play a crucial role in maintaining the confidentiality and integrity of group communications.

7 Guidance on use of advanced cryptography based on PQC

7.1 General

In the following sub-clauses, regarding typical advanced cryptographies, cryptographic construction methods and their practical usages, etc. are provided with corresponding usage scenarios (use cases) for future emerging environments such as IMT-2020/IMT-2030 and CPS (cyber physical system).

7.2 Use cases

7.2.1 Use case: Large-capacity audience stadiums

Considering the application of IMT-2020/IMT-2030 from the viewpoint of mMTC (massive machine type communication), a case can be envisioned where a stadium accommodates a large capacity of audience, such as a sports stadium, where multi-view video distribution or distribution of video from another venue can be provided. Specifically, when providing services such as large-capacity scrambled video distribution only to an authorized audience, the number of spectators to be served is large, and it is important for security to be able to efficiently authenticate and authorize service users (audience) and distribute key information required for scrambled video distribution to service users. The key information required for scrambled video distribution is important for security.

Here, we consider the use of high-performance cryptography to ensure important security. In order to efficiently authenticate and authorize a large number of service users (audience), it is effective to use broadcast authentication (see clause 6.3.7).

Furthermore, in order to efficiently distribute the key information required for scrambled video delivery to service users, it is effective to use broadcast encryption or broadcast-type KEM to deliver the keys required for scrambled video delivery (see clause 6.2.3).

The structure of this use case is shown in the Figure 1 below.

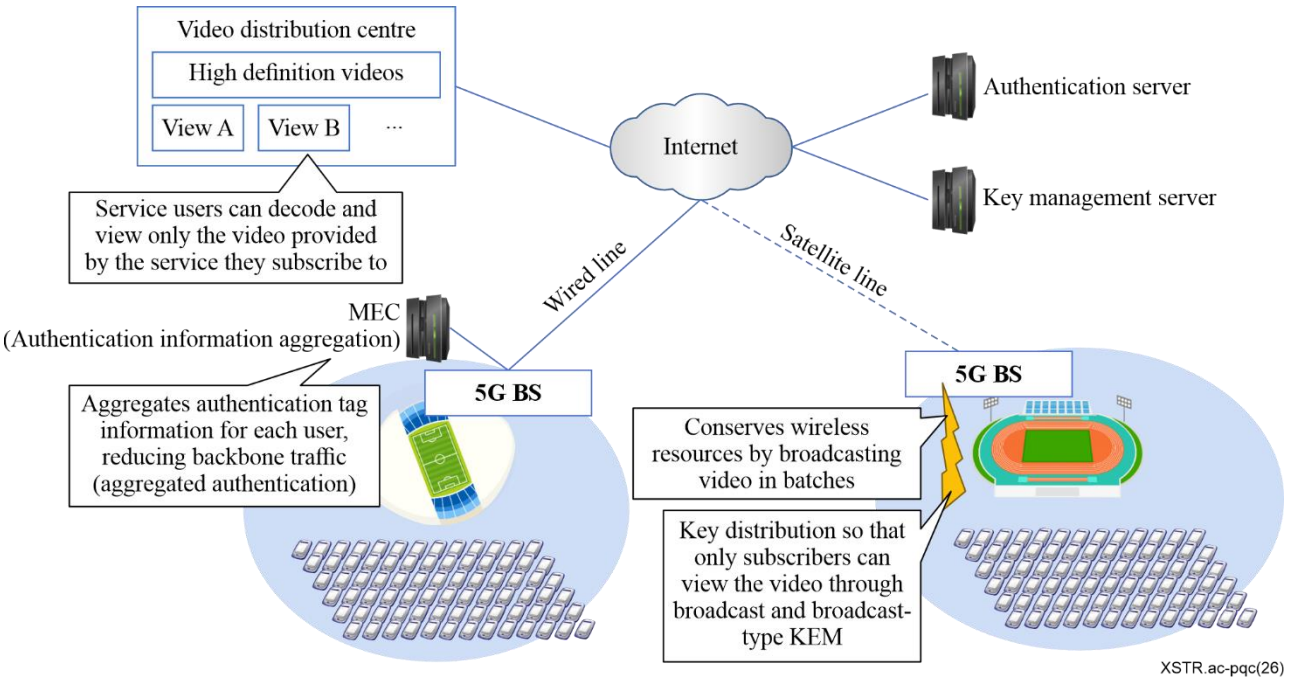

Figure 1 – Structure of use case (Large-capacity audience stadiums)

In Figure 1 above, two sports stadiums are assumed, with a large audience in them, and video distribution services are provided to an authorized audience (service users) from the video distribution centre. It is assumed that the authorization process necessary for secure video distribution and the scrambling key for distribution are configured by an advanced cryptographic system based on PQC.

As implementation of PQC-based (anonymous) broadcast authentication, the scheme based on LWE in [b-Aono] can be used. It should be noted that there has not yet been a proposal for an efficient method for broadcast encryption scheme algorithms based on standard assumptions, for instance module-LWE (such as computational assumptions equivalent to those used in primitives by NIST).

7.2.2 Use case: Sensor network

Considering the application of IMT-2020/IMT-2030 from the viewpoint of mMTC (massive machine type communication), a case can be envisioned in which a large number of sensor devices are deployed over a public wireless network such as IMT-2020/IMT-2030, and the data collected from them is centrally aggregated and comprehensively analysed. In such an environment, it is important for security and reliability to efficiently verify the legitimacy of sensor devices and to analyse the collected data while preserving privacy.

Specifically, when a large number of sensor devices continuously transmit data, it becomes essential to efficiently authenticate the devices and verify the validity of the transmitted data. To achieve this, aggregate signatures (see clause 6.3.3) can be utilized so that multiple signatures generated by individual sensor devices can be compressed into a single compact signature. This allows the edge node to verify the validity of data from many devices with reduced computational overhead, and to forward the aggregated data and signatures to a central server for large-scale analysis.

Furthermore, in order to analyse the collected data without exposing raw sensor information, it is effective to use homomorphic cryptography (see clause 6.2.4). By encrypting sensor data in a manner that still allows computation on ciphertexts, the central server can perform high-speed analysis and obtain meaningful results without accessing the underlying plaintext data, thereby enhancing privacy protection.

The structure of this use case can be shown in Figure 2 below.

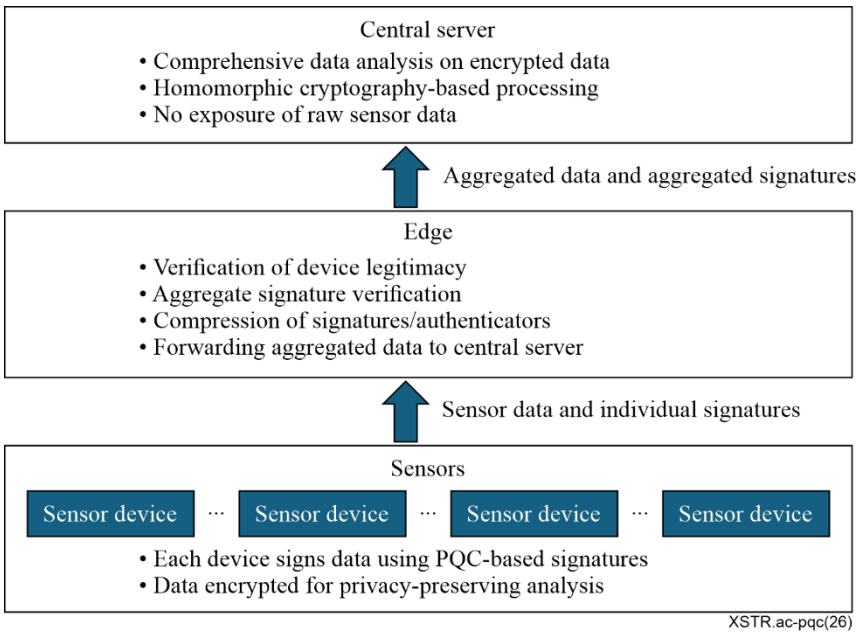

Figure 2 – Structure of use case (Sensor network)

In Figure 2, a large number of sensor devices are assumed to be deployed across a wide area, transmitting data to edge nodes over an IMT-2020/IMT-2030 network. The edge nodes verify the legitimacy of the devices and the validity of the transmitted data using aggregate signatures, compress the signatures or authenticators, and forward the aggregated data to a central server. The central server then performs comprehensive analysis on the encrypted data using homomorphic cryptography, enabling privacy-preserving data processing.

For the implementation of PQC-based aggregate signatures, the schemes proposed in [b-Tomita 1] and [b-Aardal] can be used, because those schemes are constructed under assumptions equivalent to those used in primitives by NIST. These PQC-based aggregate signature schemes enable efficient verification of large-scale sensor networks while maintaining strong security against quantum-capable adversaries.

7.2.3 Use case: Smart city

Smart cities rely on the massive interconnection of IoT devices, sensors, environmental monitors, public transportation systems, energy grids and cloud systems. These systems exchange sensitive data and often have long operational lifetimes. Data that is considered secure today could be exposed in the future if quantum-capable adversaries become practical. Therefore, organizations should consider post-quantum cryptography and PQC-based advanced cryptography as part of long-term security planning, preferably through software and protocol updates where feasible.

In this context, advanced cryptographic mechanisms based on PQC – such as PQC-based key encapsulation mechanisms (KEM), digital signatures, homomorphic cryptography, predicate encryption, and attribute-based access control – play a critical role in securing the diverse subsystems that constitute a smart city. These mechanisms enable future-proof protection of communication channels, privacy-preserving data analysis, and fine-grained access control across various domains.

The structure of this use case can be shown in Figure 3 below.

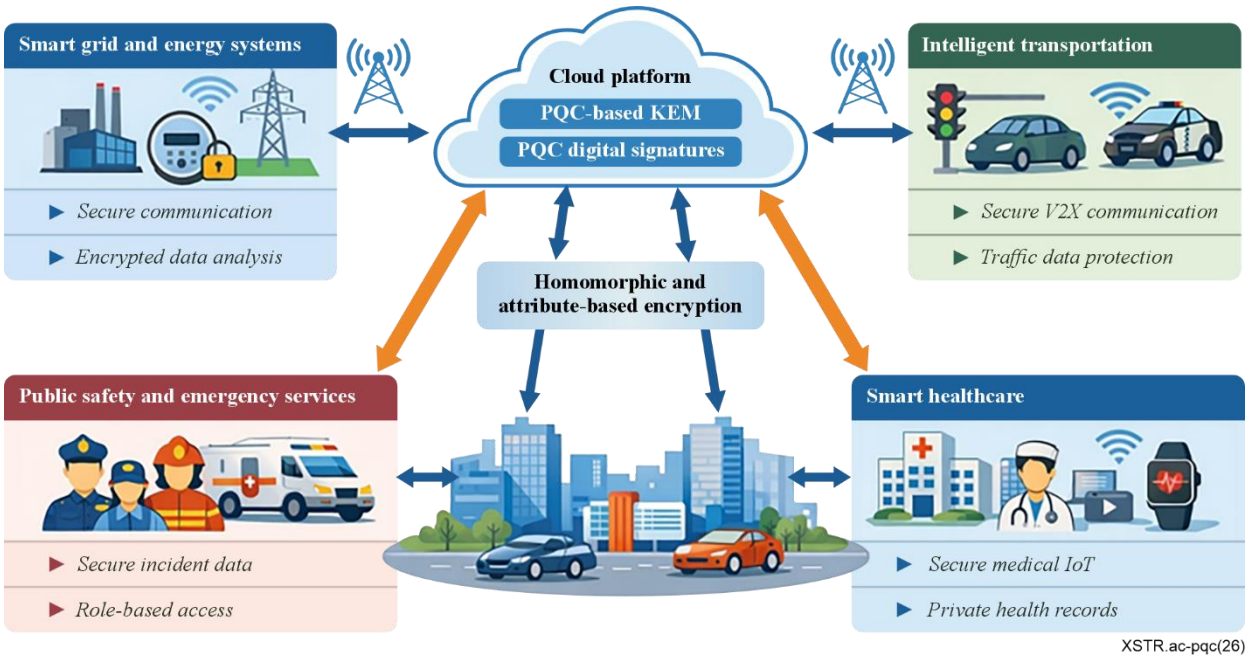

Figure 3 – Structure of use case (Smart city)

In Figure 3, multiple smart city subsystems such as energy systems, transportation networks, public safety platforms, and healthcare infrastructures – are interconnected through public wireless networks and cloud services. PQC-based digital signatures authenticate devices and services, PQC-based KEM protects communication channels, and homomorphic and attribute-based cryptographic techniques enable privacy-preserving data processing and controlled access to sensitive information.

Smart grid and energy systems

In smart grid environments, smart meters, substations, and control centres continuously exchange operational data. Ensuring the authenticity of devices and the confidentiality of consumption data is essential for preventing quantum-enabled attacks that could disrupt power distribution or falsify usage information.

- PQC-based KEM protects meter-to-grid communication, ensuring long-term confidentiality of consumption data and control commands.
- PQC-based digital signatures authenticate firmware updates and device identities, preventing impersonation or malicious device injection.
- Homomorphic cryptography enables utility companies to analyse encrypted consumption patterns to predict peak usage and optimize energy distribution without decrypting individual user data.
- Attribute-based encryption (ABE) allows utility workers to access only region-specific or device-specific data according to their roles.
- A city's energy management system can query encrypted data to detect anomalies or fraud while preserving user privacy.

Intelligent transportation systems (ITS)

Vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication requires strong authentication and confidentiality to ensure safe and efficient transportation services in a post-quantum environment.

- PQC-based digital signatures authenticate traffic signals, autonomous vehicles, and toll systems, ensuring message integrity even against quantum-capable adversaries.

- Homomorphic cryptography allows traffic control systems to analyse encrypted sensor data to optimize signal timings and reduce congestion without revealing vehicle identities.
- Predicate encryption (PE) enables fine-grained access control, granting real-time tracking data only to authorized law enforcement or traffic authorities.
- Searchable encryption allows emergency responders to search encrypted accident logs without exposing sensitive details to unauthorized parties.

Public safety and emergency services

Police, fire, and medical units should securely share sensitive information during emergencies. Ensuring the authenticity of responders and the confidentiality of incident data is essential for maintaining public safety.

- PQC-based identity management ensures that only authenticated responders can access critical communication channels.
- PQC-secured key exchange protects inter-agency communication from quantum-enabled interception.
- Homomorphic cryptography enables paramedics and hospital systems to process encrypted patient data without revealing private health information until necessary.
- Attribute-based access control ensures that responders receive only the information relevant to their role or incident involvement.
- Searchable encryption allows responders to search encrypted historical incident records to support rapid decision-making.

Smart healthcare infrastructure

Medical IoT devices and cloud-based healthcare systems generate and store highly sensitive patient data that should remain protected over long periods.

- PQC-based KEM and digital signatures secure medical IoT telemetry and prevent tampering with device data.
- Homomorphic cryptography enables cloud services to analyse encrypted health data (e.g., smartwatch heart rate trends) while preserving patient privacy.
- Predicate encryption or ABE allows hospitals to grant access to encrypted medical histories based on doctor specialty or patient condition.
- Searchable encryption enables authorized researchers to search encrypted patient records for disease patterns or treatment outcomes without exposing personal information. For information regarding privacy protection related to this matter, please refer to [b-DIN SPEC 4997].

7.2.4 Use case: Securing wireless body area networks in next-generation 5G/6G environments

In the landscape of healthcare augmented by 5G/beyond 5G technology, wireless body area networks (WBANs) deliver an array of enhanced services that significantly bolster both patient care and medical research. These services encompass continuous vital sign monitoring, remote diagnostics, and telemedicine consultations. Together, they enable uninterrupted and extensive patient surveillance, reducing the dependency on repeated hospitalisation. Leveraging 5G technology's rapid transmission and substantial capacity, WBANs can swiftly relay substantial health data to medical professionals, guaranteeing expedited and precise evaluations. Considering the extensive number of smart medical devices and users involved, security protocols should efficiently validate and grant access to legitimate users, including patients and healthcare professionals. Moreover, the secure distribution of key information for communicating encrypted medical data is vital for maintaining confidentiality and integrity.

Digital signatures are useful for efficiently authenticating and authorising a large number of medical devices and users involved in WBANs.

In this context, advanced cryptographic mechanisms based on PQC – such as PQC-based signatures, KEM, homomorphic encryption, and attribute-based access control – play a critical role in ensuring long-term protection of sensitive medical information.

The following advanced cryptographic techniques based on PQC can be applied:

PQC-based authentication and authorization

Digital signatures are useful for efficiently authenticating and authorising a large number of medical devices and users involved in WBANs. To ensure long-term resistance against quantum adversaries:

- **PQC-based digital signatures** authenticate wearable sensors, implantable devices, and medical gateways.
- These signatures also secure firmware updates and device enrolment, preventing malicious device impersonation.
- Healthcare professionals can be authenticated using **role-based PQC signature credentials**, ensuring that only authorized personnel can access WBAN data streams.

PQC-secured key establishment for encrypted medical data

PQC-based key establishment mechanisms can provide a robust method for generating encryption keys. These keys protect sensitive medical information during transmission between:

- Body-worn sensors
- Smartphones or medical hubs
- Hospital servers or cloud-based analytics systems

As described in clauses 6.4.1 and 6.4.2, PQC-based group key agreement or group key distribution mechanisms can support secure communication among multiple WBAN components and associated healthcare systems.

Privacy-preserving medical data processing

To further enhance confidentiality while enabling real-time analytics:

- **Homomorphic encryption (HE)** allows medical hubs or cloud systems to process encrypted physiological data (e.g., ECG, glucose levels) without decrypting it.
- This enables anomaly detection, trend analysis, and emergency alerts while preserving patient privacy.
- **Searchable encryption** allows authorized clinicians to query encrypted medical logs (e.g., "find abnormal heart rate events") without exposing raw data.

Fine-grained access control for medical roles

Given the sensitivity of WBAN data, access should be strictly controlled:

- **Attribute-based encryption (ABE)** or **predicate encryption (PE)** ensures that decryption rights are tied to medical roles, patient consent, or emergency conditions.
- For example, paramedics can access only time-critical emergency data, while specialists can access long-term diagnostic records.
- This prevents unauthorized access even if communication channels or storage systems are compromised.

Secure aggregation and multi-device coordination

WBANs often involve multiple sensors operating simultaneously:

- **PQC-based aggregate signatures** can compress multiple device signatures into a single compact authenticator, reducing bandwidth and verification overhead.
- This is particularly effective in 5G/6G environments where numerous sensors continuously transmit data.

A visual representation of the use case architecture is depicted in Figure 4 below.

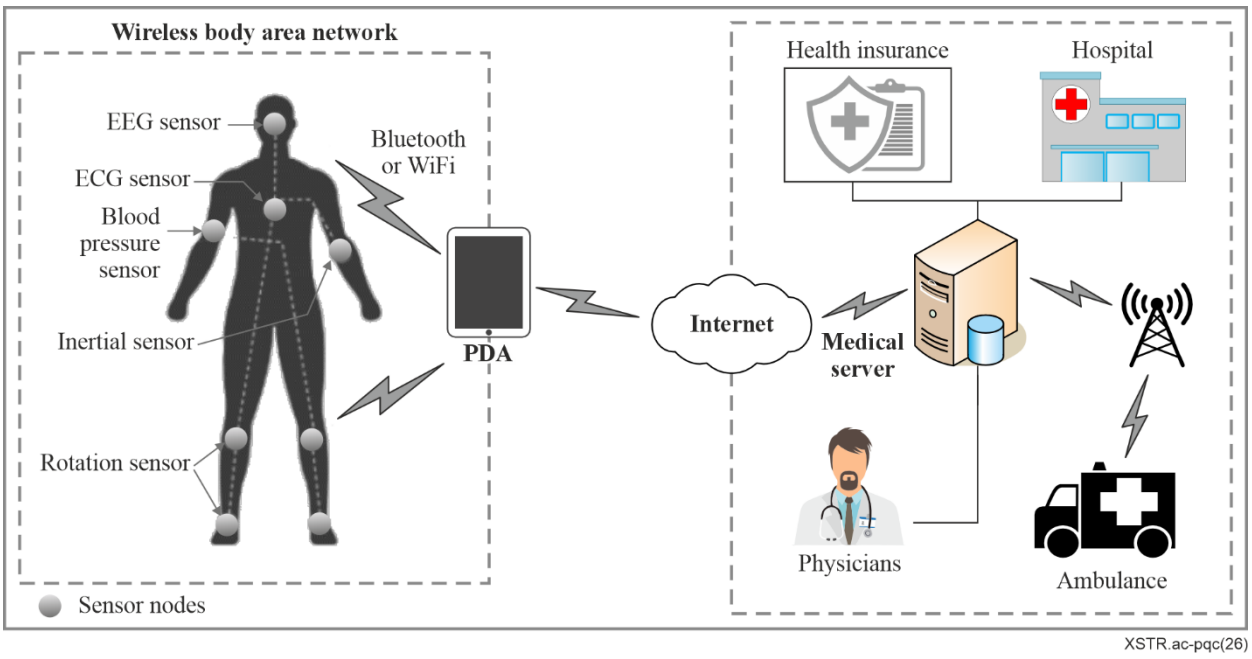

Figure 4 – Structure of wireless body area network

7.2.5 Use case: Autonomous vehicular communication systems

Considering the application of IMT-2020/IMT-2030 from the viewpoint of URLLC and mMTC, a case can be envisioned in which a large number of vehicles and roadside units (RSUs) communicate over a public wireless network to support autonomous driving, traffic safety, and efficient mobility management. In such an environment, it is essential for security and reliability to efficiently authenticate vehicular entities, verify the integrity of exchanged messages, and preserve the privacy of drivers and passengers.

Specifically, when vehicles continuously transmit safety-critical information – such as position, speed, and hazard notifications – it becomes necessary to ensure both strong authenticity and anonymity. To achieve this, group signatures and group key distribution (see clauses 6.3.5 and 6.4.2) can be utilized so that vehicles can authenticate themselves as legitimate members of the transportation system without revealing their individual identities. This enables privacy-preserving authentication while still allowing a trusted authority to trace misbehaving vehicles when required.

Furthermore, in high-density traffic scenarios, roadside units and control centres should verify a large number of signatures within strict latency constraints. For this purpose, batch verification (see clause 6.3.8) or aggregate signature (see clause 6.3.3) is effective, as it enables multiple signatures or credentials to be validated simultaneously with reduced computational overhead. This is particularly important in IMT-2020/IMT-2030-enabled vehicular networks, where numerous vehicles can broadcast messages at short intervals.

The combination of these advanced cryptographic mechanisms enhances the scalability and robustness of autonomous vehicular communication systems. PQC-based group signatures and batch-verifiable signature schemes constructed under assumptions equivalent to those used in NIST-standardized primitives can provide long-term security against quantum-capable adversaries while supporting the real-time requirements of vehicular environments.

The structure of this use case can be shown in Figure 5 below.

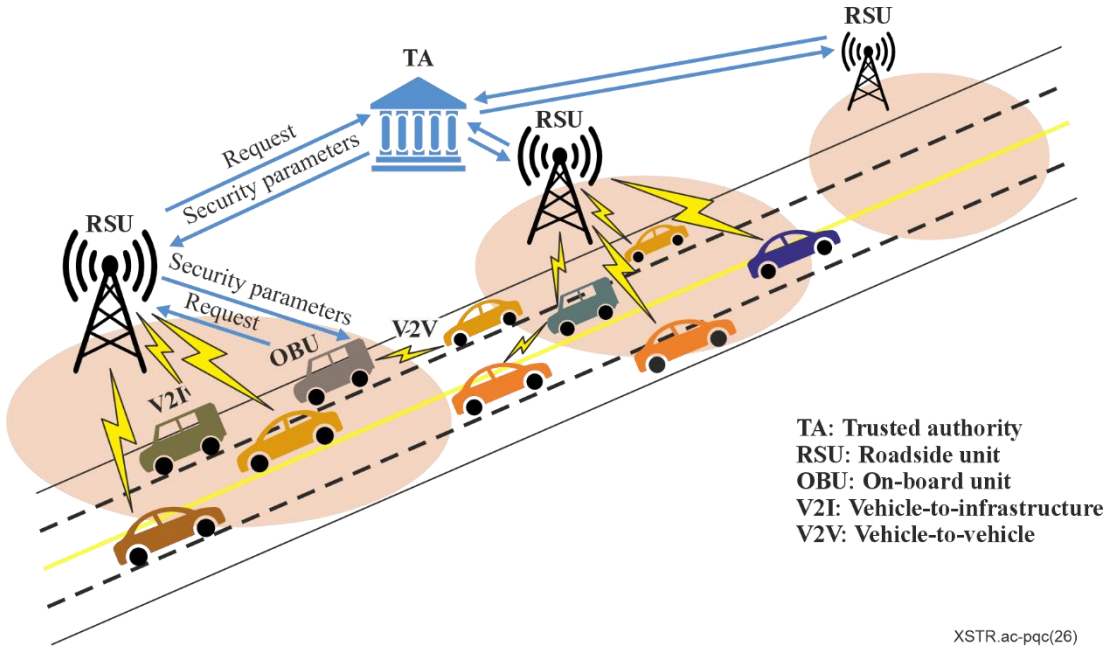

Figure 5 – Structure of use case (Autonomous vehicular communication systems)

Bibliography

[b-ITU-T Y.2014] Recommendation ITU-T Y.2014 (2010), *Network attachment control functions in next generation networks*.

[b-ETSI TS 104 015] ETSI TS 104 015 v1.1.1. (2025), Cyber security (CYBER); Quantum-safe cryptography (QSC); *Efficient quantum-safe hybrid key exchange with hidden access policies*.
<https://www.etsi.org/deliver/etsi_ts/104000_104099/104015/01.01.01_60/ts_104015v010101p.pdf>

[b-Agrawal] Agrawal, S., Freeman, D.M., and Vaikuntanathan, V. (2011), *Functional encryption for inner product predicates from learning with errors*. ASIACRYPT 2011. Lect. Notes in Comput. Sci. pp. 21-40, Springer.
<https://link.springer.com/chapter/10.1007/978-3-642-25385-0_2>

[b-Abdalla] Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P., and Shi, H. (2005), *Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions*. Advances in Cryptology – CRYPTO 2005.
<https://link.springer.com/chapter/10.1007/11535218_13>

[b-Agrawal, S] Agrawal, S., Stehle, D., and Yadav, A. (2022), *Round-optimal lattice-based threshold signatures, revisited.* Cryptology ePrint Archive. Paper 2022/634.
<https://eprint.iacr.org/2022/634>

[b-Aono] Aono, Y., and Shikata, J. (2023), *Anonymous Broadcast Authentication with Logarithmic-order Ciphertexts from LWE*. Cryptology and Network Security. CANS 2023. Lecture Notes in Computer Science, vol. 14342, pp. 28-50, Springer.
<https://link.springer.com/chapter/10.1007/978-981-99-7563-1_2>

[b-Aardal] Aardal, M.A., Aranha, D.F., Boudgoust, K., Kolby, S., Takahashi, A. (2024), *Aggregating Falcon Signatures with LaBRADOR*. Advances in Cryptology – CRYPTO 2024. Lecture Notes in Computer Science, vol. 14920, pp. 71-106. Springer.
<https://link.springer.com/chapter/10.1007/978-3-031-68376-3_3>

[b-Beullens, W] Beullens, W., Katsumata, S., and Pintore, F. (2020), *Calamari and falafl: Logarithmic [linkable] ring signatures from isogenies and lattices*. Cryptology ePrint Archive. Paper 2020/646.
<https://eprint.iacr.org/2020/646>

[b-Boneh] Boneh, D., Gentry, C., Gorbunov, S., Halevi, S., Nikolaenko, V., Segev, G., Vaikuntanathan, V., and Vinayagamurthy, D. (2014), *Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits*. EUROCRYPT 2014, Lect. Notes in Comput. Sci., vol. 8441, pp. 533-556, Springer.
<https://link.springer.com/chapter/10.1007/978-3-642-55220-5_30#citeas>

[b-Brakerski] Brakerski, Z., Gentry, C., and Vaikuntanathan, V. (2014), *(Leveled) fully homomorphic encryption without bootstrapping*, ACM Transactions on Computation Theory, vol. 6, no. 3, pp. 1-36.
<https://dl.acm.org/doi/10.1145/2633600>

[b-Bellare] Bellare, M., Namprempre, C., Neven, G. (2009), *Security proofs for identity-based identification and signature schemes*. Journal of Cryptology. Volume 22, pp. 1-61.
<https://link.springer.com/article/10.1007/s00145-008-9028-8>

[b-Boneh, D] Boneh, D., and S. Kim, (2020), *One-time and interactive aggregate signatures from lattices.*
<https://crypto.stanford.edu/~skim13/agg_ots.pdf>

[b-Beullens] Beullens, W., Dobson, S., Katsumata, S., Lai, Y-F., and Pintore, F. (2021), *Group signatures and more from isogenies and lattices: Generic, simple, and efficient*. Cryptology ePrint Archive. Paper 2021/1366
<https://eprint.iacr.org/2021/1366>

[b-Boschini] Boschini, C., Takahashi, A., and Tibouchi, M. (2022), *MuSig-L: Lattice-based multi-signature with single-round online phase*. Cryptology ePrint Archive. Paper 2022/1036.
<https://eprint.iacr.org/2022/1036>

[b-Chillotti] Chillotti, I., Gama, N., Georgieva, M., and Izabachène, M. (2019), *TFHE: Fast fully homomorphic encryption over the torus*. Journal of Cryptology, vol. 33, pp. 34-91.
<https://link.springer.com/article/10.1007/s00145-019-09319-x>

[b-Cheon] Cheon, J.H., Kim, A., Kim, M., and Song, Y.S. (2016), *Homomorphic encryption for arithmetic of approximate numbers*. Advances in Cryptology - ASIACRYPT 2017. Lect. Notes in Comput, Sci., vol. 10624, pp. 409-437, Springer.
<https://link.springer.com/chapter/10.1007/978-3-319-70694-8_15>

[b-Chandran] Chandran, N., Chase, M., Liu, F-H., Nishimaki, R., and Xagawa, K. (2014), *Re-encryption, functional re-encryption, and multi-hop re-encryption: A framework for achieving obfuscation-based security and instantiations from lattices*. PKC 2014, Lect. Notes in Comput. Sci., vol. 8383, pp. 95-112, Springer.
<https://link.springer.com/chapter/10.1007/978-3-642-54631-0_6>

[b-Ducas, L] Ducas, L., and Micciancio, D. (2015), *FHEW: Bootstrapping homomorphic encryption in less than a second*. Advances in Cryptology -- EUROCRYPT 2015, Lect. Notes in Comput. Sci., vol. 9056, pp. 617-640, Springer.
<https://link.springer.com/chapter/10.1007/978-3-662-46800-5_24>

[b-Davidson] Davidson, A., Deo, A., Lee, E., and Martin, K. (2019), *Strong post-compromise secure proxy re-encryption*. Cryptology ePrint Archive. Paper 2019/368.
<https://eprint.iacr.org/2019/368>

[b-Ducas] Ducas, L., Lyubashevsky, V., and Prest, T. (2014), *Efficient identity-based encryption over NTRU lattices*. Springer, Advances in Cryptology ASIACRYPT 2014, Lect. Notes in Comput. Sci., vol. 8874, pp. 22-41.
<https://link.springer.com/chapter/10.1007/978-3-662-45608-8_2>

[b-Damgard] Damgard, I., Orlandi, C., Takahashi, A., and Tibouchi, M. (2021), *Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices*. Public-Key-Cryptography – PKC 2021, Lect. Notes in Comput. Sci. vol. 12710, pp. 99-130 Springer.
<https://link.springer.com/chapter/10.1007/978-3-030-75245-3_5>

[b-DIN SPEC 4997] DIN SPEC 4997:2020, *Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology*.
<https://webstore.ansi.org/standards/din/dinspec49972020>

[b-Esgin] Esgin, M.F., Steinfeld, R., Liu, J.K., and Liu, D. (2019), *Lattice-based zero-knowledge proofs: New techniques for shorter and faster constructions and applications*. Cryptology ePrint Archive. Paper 2019/445.
<https://eprint.iacr.org/2019/445>

[b-Fan] Fan, J., and Vercauteren, F. (2012), *Somewhat practical fully homomorphic encryption*. Cryptology ePrint Archive. Paper 2012/144.
<https://eprint.iacr.org/2012/144>

[b-Fuchsbauer] Fuchsbauer, G., Kamath, C., Klein, K., and Pietrzak, K. (2018), *Adaptively secure proxy re-encryption*. Cryptology ePrint Archive. Paper 2018/426.
<https://eprint.iacr.org/2018/426>

[b-Gentry] Gentry, C., Peikert, C., and Vaikuntanathan, V. (2008), *Trapdoors for hard lattices and new cryptographic constructions*.
<https://eprint.iacr.org/2007/432.pdf>

[b-Gentry, C] Gentry, C. (2009), *Fully homomorphic encryption using ideal lattices*. STOC 2009: ACM, pp. 169-178.
<https://dl.acm.org/doi/10.1145/1536414.1536440>

[b-Gorbunov] Gorbunov, S., Vaikuntanathan, V., and Wee, H. (2015), *Predicate Encryption for Circuits from LWE*. Cryptology ePrint Archive. Paper 2015/029.
<https://eprint.iacr.org/2015/029>

[b-Gordon] Gordon, S.D., Katz, K., and Vaikuntanathan, V. (2010), *A group signature scheme from lattice assumptions*. ASIACRYPT 2010, Lect. Notes IN Comput. Sci., vol. 6477, pp. 395-412, Springer.
<https://link.springer.com/chapter/10.1007/978-3-642-17373-8_23>

[b-Katsumata] Katsumata, S., Yamada, S., and Yamakawa, T. (2018), *Tighter security proofs for GPV-IBE in the quantum random oracle model*. Springer Link. Advances in Cryptology. pp. 253-282.
<https://link.springer.com/chapter/10.1007/978-3-030-03329-3_9>

[b-Katsumata, S] Katsumata, S., Nishimaki, R., Yamada, S., and Yamakawa, T. (2020), *Adaptively secure inner product encryption from LWE*. Cryptology ePrint Archive. Paper 2020/1135.
<https://eprint.iacr.org/2020/1135>

[b-Kiltz] Kiltz, E., and G. Neven. (2009), *Identity-based signatures.* Identity-Based Cryptography.
<http://www.neven.org/papers/ibschapter.pdf>

[b-Kaafarani] Kaafarani, A.E., and Katsumata, S. (2018), *Attribute-based signatures for unbounded circuits in the ROM and efficient instantiations from lattices*. Cryptology ePrint Archive. Paper 2018/022.
<https://eprint.iacr.org/2018/022>

[b-Luo] Luo, F., and Al-Kuwari, S. (2022), *Attribute-based signatures from lattices: Unbounded attributes and semi-adaptive security*.
<https://elmi.hbku.edu.qa/en/publications/attribute-based-signatures-from-lattices-unbounded-attributes-and/>

[b-Lee] Lee, Y., Park, J.H., Lee, K., Lee, D.H. (2020), *Tight security for the generic construction of identity-based signature (in the multi-instance setting)*. Theoretical Computer Science, Volume 847, pp. 122-133. <https://www.sciencedirect.com/science/article/pii/S0304397520305557?via%3Dihub>

[b-Polyakov] Polyakov, Y., Rohloff, K., Sahu, G., and Vaikuntanathan, V. (2017), *Fast proxy re-encryption for publish/subscribe systems*. Cryptology ePrint Archive. Paper 2017/410. <https://eprint.iacr.org/2017/410>

[b-Pan] Pan, J., and Wagner, B. (2021), *Short identity-based signatures with tight security from lattices*. Cryptology ePrint Archive. Paper 2021/970. <https://eprint.iacr.org/2021/970>

[b-Sato] Sato, S., and Shikata, J. (2025), *Bounded CCA2-secure Proxy Re-encryption from Lattices*. <https://sacworkshop.org/SAC25/slides/Sato.pdf>

[b-Sato, S] Sato, S., and Shikata, J. (2022), *Identity-based interactive aggregate signatures from lattices*. ICISC 2022, Lect. Notes in Comput. Sci., vol. 13849, pp. 408-432, Springer. <https://link.springer.com/chapter/10.1007/978-3-031-29371-9_20>

[b-Tomita] Tomita, T., and Shikata, S. (2024), *Efficient Identity-Based Encryption with Tight Adaptive Anonymity from RLWE*. Post-Quantum Cryptography. Springer Nature. <https://www.springerprofessional.de/en/efficient-identity-based-encryption-with-tight-adaptive-anonymit/27199988>

[b-Tomita, T] Tomita, T., and Shikata, J. (2024), *Compact and Tightly Secure (Anonymous) IBE from Module LWE in the QROM*. Cryptography ePrint Archive, 2024/1765. <https://eprint.iacr.org/2024/1765>

[b-Tomita 1] Tomita, T., and Shikata, J. (2023), *Compact Aggregate Signature from Module-lattices*. Cryptology ePrint Archive. Paper 2023/471. <https://eprint.iacr.org/2023/471>

[b-Tsabary] Tsabary, R. (2019), *Fully secure attribute-based encryption for t-CNF from LWE*. CRYPTO 2019. Lect. Notes in Comput. Sci., vol. 11692, pp. 62-85, Springer. <https://link.springer.com/chapter/10.1007/978-3-030-26948-7_3>

[b-Wee] Wee, H. (2022), *Optimal broadcast encryption and CP-ABE from evasive lattice assumptions*. EUROCRYPT 2022, Lect. Notes in Comput. Sci., vol. 13276, pp. 217-241, Springer. <https://link.springer.com/chapter/10.1007/978-3-031-07085-3_8>

[b-Waters] Waters, B. (2013), *Functional encryption: Origins and recent developments*. Public-Key cryptography-PKC 2013. <https://link.springer.com/chapter/10.1007/978-3-642-36362-7_4>

[b-Wang] Wang, J., Huang, C., Yang, K., Wang, J., Wang, X., and Chen, X. (2015), *MAVP-FE: Multi-Authority Vector Policy Functional Encryption with Efficient Encryption and Decryption*. IEEE. <https://ieeexplore.ieee.org/document/7122471>

[b-Yang] Yang, J., Liu, Z., Li, J., Jia, C., and Cui, B. (2015), *Multi-Key Searchable Encryption Without Random Oracle*. IEEE.
<https://ieeexplore.ieee.org/document/7057073>

[b-Zhang] Zhang, M., Wang, X.A., Yang, X., and Cai, W. (2013), *Efficient Predicate Encryption Supporting Construction of Fine-Grained Searchable Encryption*. 2013 5th International Conference on Intelligent Networking and Collaborative Systems, IEEE.
<https://ieeexplore.ieee.org/document/6630453>