SC27 Journal Vol 1 Issue 3

<table>
<thead>
<tr>
<th>Document type</th>
<th>Related content</th>
<th>Document date</th>
<th>Expected action</th>
</tr>
</thead>
<tbody>
<tr>
<td>General document</td>
<td></td>
<td>2022-03-04</td>
<td>INFO</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ISSUE 3

CRYPTOGRAPHY AND SECURITY MECHANISMS

Feb 2022
The views and opinions expressed in the articles in this Journal are those of the author(s) and do not necessarily reflect the views or opinions of ISO, IEC, JTC 1, SC 27 or the editor of this publication.

ISO, IEC, SC 27, the editor and the authors shall not be liable regarding the use, interpretation or implementation of the material contained in any of the articles contained in this publication.

© ISO 2021
CONTENTS

Prologue 7
Words from the SC 27 Chair 9
Paving the Runway for Standardization of Post-Quantum Cryptography 11
Achieving privacy and authenticity through advanced digital signature mechanisms 20
Encryption algorithms 28
Reducing Data Security Risk Using Standardized Key Establishment Mechanisms 32
How to choose and use block ciphers - Introduction to ISO/IEC 18033-3 39
About SC 27/WG 2 44
Welcome to Issue 3 of the ISO/IEC JTC 1/SC 27 Journal. The purpose of Journal is to present articles from SC 27 experts involved in the development of standards covering information security, cybersecurity and privacy protection.

Cryptography plays an important role in the digital world we live, work in and conduct business in. Cryptographic mechanisms are in cryptocurrencies, digital passports, financial transactions, online purchasing, IoT applications, smartphone apps, and many more uses.

The first standard committee in ISO to consider IT security was established in the early 80s. This committee was TC 97 and they had three projects: ISO standardisation of DES (DEA), the standard modes of operation for DES and an extended set of modes of operation. As interest grew in the standardisation of cryptographic mechanisms the work in TC 97 was transferred into a new committee SC 20, which had three working groups dealing with standards for: symmetric-key algorithms, asymmetric-key algorithms and crypto applied to data communications. By 1990 a new committee SC 27 was established and the work of SC 20 on symmetric-key algorithms and asymmetric-key algorithms was transferred into this new committee. The topic of cryptography standardisation has grown in SC 27 to embrace many new areas as well as still maintaining some of the traditional standards developed in SC 20.

Thus, cryptographic standards in ISO has a history of over 40 years during which time there have been many technological changes and SC 27 has carried on the legacy of ISO crypto-
standards, and is today the international centre of cryptographic standards.

This third issue of the SC 27 Journal focuses on the work of SC 27/WG 2 whose scope of work covers cryptography and security mechanisms.

Any questions or feedback relating to the content of this Journal can be directed to editor (sc27.wg1.edwardjh@gmail.com)

Dr Edward Humphreys
SC 27 Journal Editor
Just a few years ago, cryptography was something for nerds. When I was studying mathematics, only a few students attended number theory classes. Even in the perception of a typical math student, logic and set theory were, at best, drier subjects than number theory. Maybe that has changed since then.

Today it is difficult to find a more complex object that does not contain cryptographic components. You don't even have to think about industrial applications, it's enough to stay in our daily life. It's pretty common these days to send encrypted email, and almost everyone uses a messenger with end-to-end encryption (although most people probably don't know exactly what that is). Working remotely from home wouldn't be possible without a VPN (i.e., without cryptography) and working remotely has been essential to keeping the global economy afloat during the COVID-19 pandemic. The solar power plant on the roof of my house communicates with my heating system, with my car and with the electricity grid; this communication is (hopefully) secured by suitable cryptographic means. This networking on a small scale continues on large scale. The energy transition ahead of us towards renewable energies will lead to much more complex energy networks than before. This growing complexity will be reflected in more complex control structures connecting many more stakeholders cryptographically secure while helping to blur the border between IT and OT.

I would like to point out one more example. Once our society recovers from the pandemic, travel will come back. Passports
and ID cards are required for travel. Such machine-readable travel documents are only possible based on a global public key infrastructure. Given the long lifespan of travel documents, it is essential to ensure the authenticity of electronically signed data over a long period of time. This makes it necessary to make reliable statements about the properties of future technologies. In this particular case, the reliability of current cryptography needs to be analysed in view of the potentially impending quantum computing age. In addition, new cryptographic methods need to be developed which, due to their complexity properties, still have sufficient functional strength when powerful quantum computers are available.

One could fill this whole magazine with more examples. The experts who contribute to SC 27 projects deal with many important and interesting cryptography-related topics. This issue of the SC 27 Journal gives the reader a brief overview on some of these topics and is definitely worth reading.
PAVING THE RUNWAY FOR STANDARDIZATION OF POST-QUANTUM CRYPTOGRAPHY

Lily CHEN (SC 27 expert, USA)

The cryptography and security mechanisms standardized by SC27 have become the cornerstone for today’s global cybersecurity. The mechanisms have been deployed to provide network security, enable e-commerce, establish virtual private networks (VPN) for business and enterprise applications, and block malware invasion of IT devices.

When people consider quantum supremacy, a question appears: will the cryptographic mechanisms being standardized and deployed still be secure when quantum computers become available? This article will discuss quantum impact on the current widely deployed cryptographic mechanisms and introduce approaches being taken by SC27 to prepare for the quantum era.

**Cryptography**

Quantum computers will accelerate information processing and solve previously infeasible problems thus offering life-changing scientific breakthroughs. However, full scale quantum computers, once available, will impact cybersecurity in a catastrophic way.

The cryptographic primitives standardized by ISO/IEC JTC1 SC27 can be categorized as public-key (a.k.a. asymmetric-key) cryptography and symmetric-key cryptography. For example, “ISO/IEC 18033 Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers” specifies...
public-key cryptography primitives, while “ISO/IEC 18033 Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers” specifies symmetric-key cryptography primitives.

At a high level, public-key cryptography is used to provide authenticity of an entity or data and to securely establish symmetric keys. Symmetric-key cryptography, using the established keys, protects the confidentiality and integrity of information. For example, the transport layer security (TLS) protocol uses public-key cryptography to establish keys and to conduct mutual authentication between a client and a server. Then, the actual information being exchanged is protected by symmetric-key cryptographic algorithms using the keys established by public-key processes. Another application of public-key cryptography is using digital signatures for code signing to prevent undetected insertion of malware.

The security of public key cryptography is based on the “hardness” of certain computational problems. For well-known RSA schemes, their security depends on the difficulty of factoring large integers. That is, given a large integer $n$, find primes $p$ and $q$ such that $n = pq$. This is a hard problem because, as the size of the integer $n$ increases, the complexity of factorization increases exponentially. When $n$ is an appropriately chosen integer of 2048 bits or larger, it requires at least $2^{112}$ operations to factor $n$. For classical computers, such complexity means it is practically infeasible to factor.

Quantum Impact
Currently, most of the public-key cryptographic mechanisms standardized in ISO/IEC are either factorization-based, such as signatures specified in “ISO/IEC 14888-2 Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms” or discrete-logarithm-based, such as signatures specified in “ISO/IEC 14888-3 IT Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms.” Both problems have been considered hard for classical computers to solve within a practical time frame. Therefore, the public-key cryptography mechanisms that are based on these problems currently provide sufficient protection from cryptanalysis.

However, in 1994, Peter Shor, an MIT professor, showed how quantum computers can be used to solve both the factorization and discrete logarithm problems in polynomial time. That is, the complexity of factorization increases as a polynomial function of the size of the integer $n$. As a result, the arrival of quantum computers large enough to run Shor’s algorithm efficiently will eventually render the security of all widely implemented public-key cryptographic schemes ineffective.

Quantum computers will also impact the security of symmetric-key cryptography. By Grover’s algorithm, for a block cipher with 128-bit key, using exhaustive search, the complexity of finding the key will be reduced from $2^{128}$ to $2^{64}$, that is, the square root of $2^{128}$. Here $2^{128}$ is the classical complexity, while $2^{64}$ is the quantum complexity. Even though we do not have a practical estimate of the quantum computing cost, we can mitigate the quantum attacks on symmetric-key cryptography by increasing its key size.
In summary, the quantum impact to public-key cryptography is catastrophic, while the impact to symmetric-key cryptography can be managed by increasing key sizes. Considering that most symmetric-key cryptography primitives have provided options to use higher key sizes, addressing quantum resistant public-key cryptography is more urgent.

Post-Quantum Cryptography

The cryptographic research community has been looking for quantum resistant cryptographic mechanisms since the beginning of this century. As noted above, some problems are hard for classical computers but not for quantum computers. The challenge is finding problems that are hard for both classical and quantum computers. Fortunately, researchers have identified sets of problems which seem to be hard even for quantum computers (e.g., finding shortest vectors for lattices). Public-key cryptography mechanisms can be designed that rely on these problems. Such mechanisms are referred to as post-quantum cryptography (PQC) or quantum-resistant cryptography.

Post-quantum cryptography has been a very active research area in the past decade. Many PQC algorithms have been published in the research literature. The National Institute of Standards and Technology (NIST) in the USA has been conducting a PQC standardization effort since 2016. In the past five years, many submitted candidate algorithms have been analyzed and evaluated by the research community. After considering security, performance, and many other aspects, NIST has narrowed down the candidate pool twice. NIST is now in the third round of this process, with seven finalists and eight alternate candidates. NIST
is expected to complete its third round selection in 2022 and release draft PQC standards in the 2022-2023 timeframe.

Together with the NIST standardization effort, international standards organizations have undertaken initiatives to prepare for PQC standardization. Industry is also actively exploring a transition path.

SC27 has more than 30 years history in developing cryptographic standards. Many cryptographic experts from different national bodies have consistently contributed to different standards. The contributors are resourceful and knowledgeable. But considering that post-quantum cryptography is relatively new even for many experts and many algorithms are still under evaluation, it is critical to create opportunities for the experts to get familiar with post-quantum cryptography and be ready to make decisions on standardization.

**Standing Document (SD8)**

SC27 WG2 started a study period on post-quantum cryptography in October 2015. The study period lasted 24 months with multiple calls for contributions soliciting input from the SC27 experts. As a decision from the study period, WG2 decided to develop a standing document to introduce some basic primitives to be used as a reference for the experts. The standing document should focus on several well-researched categories of post-quantum cryptography.

It is agreed that the standing document must focus on basic concepts and security assumptions in each of the categories of post-quantum cryptography. It needs to introduce the major
applicable cryptographic classes. Specific algorithms should be used as examples to illustrate the principles and operations for the experts to understand each category.

SD8 consists of six parts and introduces five categories of the most researched post-quantum cryptographic mechanisms. Here is a high-level description for each part:

- Part 1 provides a general introduction on post-quantum cryptography, including security definitions and performance considerations;
- Part 2 focuses on hash-based signatures. Hash-based signatures are different from other categories in post-quantum cryptography. It is not based on number theory assumptions but on the security of hash functions. It was introduced in the 1970s. Stateful hash-based signatures are essentially one-time signatures. It requires state management to guarantee that each private-key can only be used to sign one message. But on the other hand, it relies on minimal security assumptions. The security properties are better understood;
- Part 3 introduces lattice-based mechanisms. Lattice-based cryptography is an attractive post-quantum cryptography family. Part 3 provides descriptions of the major approaches in building lattice-based mechanisms together with twelve example algorithms for public-key encryption, key exchange, and digital signatures;
- Part 4 introduces code-based cryptography. Like hash-based signatures, code-based cryptosystems have been developed since 1978 using error-correcting codes to build public-key
cryptography. This part describes the main structure of code-based encryption algorithms and the security analysis methods;

- Part 5 introduces multivariate cryptosystems. Multivariate cryptography refers to public-key cryptography whose public keys represent a multivariate and nonlinear (usually quadratic) polynomial map. The main computational problem underlying multivariate cryptography is to find preimages for these multivariate polynomial maps. This part described the major variants of multivariate cryptosystems and highlighted attack methods applying to each variant;

- Part 6 introduces a relatively new category, isogeny-based cryptography. The idea of using maps between elliptic curves to build public-key cryptography traces back to 1997, while the first concrete design was proposed about ten years ago. This part introduces the background of isogeny-based cryptography and gives details of an early design of the isogeny-based CRS system and recent supersingular-isogeny Diffie-Hellman (SIDH) protocol. It also discusses security assumptions and attacks on isogeny-based cryptosystems.

Each part of SD8 is authored by well recognized researchers on the topic. More than eight experts from multiple national bodies and liaison organizations, Belgium, China, Japan, Netherland, USA, PQCrypto, etc., all contributed to SD8. The effort lasted about two years. Since 2020, SD8 has been publicly available at https://www.din.de/en/meta/jtc1sc27/downloads.

During the development of SD8, SC27 WG2 also held tutorial sessions at each working group meeting. The experts who authored SD8 gave tutorial presentations on the different topics.
corresponding to each part of SD8. The tutorials gave opportunities for the experts to ask questions and helped to make SD8 accessible.

SD8 has played an effective role in preparing SC27 for post-quantum cryptography standardization. It has been shared with liaison organizations such as ETSI TC CYBER WG QSC, ITU-T SG 17, ISO/IEC JTC 1 SC6, and ISO TC 68/SC 2. As a preparation effort, SC27 also established liaison relationships with post-quantum cryptography research projects such as PQCRYPTO, SAFEcrypto, PRISMACLOUD, FutureTPM, etc. in sharing information on development and practice of post-quantum cryptography.

**Moving forward**

Through the SD8 effort, SC27 experts have been well-prepared to move forward with standardization of post-quantum cryptography. As a matter of fact, the project for specifying stateful hash-based signatures in “ISO/IEC 14888-4 Information technology — Security techniques — Digital signatures with appendix — Part 4: Stateful hash-based mechanisms” is in the first committee draft stage. Stateful hash-based signatures can be used for code signing as an example of early adoption of post-quantum cryptography.

Standardization of post-quantum cryptography poses challenges to SC27. As a standards subcommittee with a long history of constantly adapting to rapidly advanced technology and applications, SC27 has made great progress in preparing to
develop the next generation of cryptographic standards for quantum era.
Achieving privacy and authenticity through advanced digital signature mechanisms


INTRODUCTION AND MOTIVATION

Digital signature schemes, as specified in the ISO/IEC 9796 and ISO/IEC 14888 series, are of utmost importance in a digital world, as they allow for verifying the authenticity of digital messages and documents. More precisely, a valid digital signature guarantees the following properties:

- **Authenticity or data origin authentication**: The received message was created by a known sender. This also means that, without access to the secret signing key, it is computationally infeasible to compute a valid signature on a previously unsigned message for a given verification key;
- **Integrity**: The received message has not been modified during transmission. In particular, a digital signature scheme ensures that a signature on a message already becomes invalid when flipping a single bit of the protected message.
- **Non-repudiation**: Digital signature schemes create transferable proofs that disallow a signer of a message to later deny having signed it.

While digital signatures enable a wide range of online services and applications, it turns out that their security requirements are sometimes overly restrictive when aiming for privacy-preserving solutions following a privacy-by-design principle, as mandated by...
different legal regulations, including, but not limited to, the European Union’s General Data Protection Regulation (GDPR) or Brazil’s General Personal Data Protection Law (LGPD).

The following sections provide a brief overview of more advanced digital signature mechanisms that introduce different types of controlled flexibility to the aforementioned security requirements, thereby enabling the design of privacy-preserving applications without giving up on the required authenticity and integrity guarantees. **Privacy in this context** can be seen as confidentiality of personally identifiable information by enabling the user to withhold that information completely. Thus, the mechanisms achieve integrity and authenticity guarantees without ever making certain personally identifiable information, such as users’ name, available to any individual, entity, or process. Confidentiality, as property that information is not made available or disclosed to unauthorized individuals, entities, or processes has been defined in many SC 27 WG 2 standards. Hereby the mechanisms follow the privacy principle of data minimization as described in the SC 27 standard ISO/IEC 29100.

**AUTHENTICITY-PRESERVING REDACTION OF SIGNED DOCUMENTS**

Standard digital signatures do not allow for the subsequent modification of signed data. However, in certain scenarios such modifications would be required to achieve privacy. As a motivating example, consider the case of signed medical records: A user wishes to share the records with a research organization, but without revealing full name or social insurance number. The research organization on the other hand has authenticity requirements to ensure the correctness and
trustworthiness of the data in order to achieve a high data quality. Using traditional digital signatures would require the health authority to re-sign the health record to create a partial medical record of the user for each specific study containing only those specific parts of the records that the user wishes to release.

Redactable attestation schemes overcome the obstacle of requiring an active involvement of a trusted signer to issue signed excerpts from already signed information. Such schemes allow the attestor (the entity which signs the document) to label specific message blocks such that they can later be redacted by the holder of the attested document without invalidating the attestation, while guaranteeing that no other modifications (e.g., insertions, or deletions of unlabelled message parts) of the document can be performed. Allowed redactions can be carried out without requiring access to the secret key of the attestor, thus the original signer is not involved. Upon receipt of a redacted signed message the verifier will use the public verification key of the attestor to establish integrity, origin authentication and non-repudiation also on a correctly redacted message, just like in traditional digital signatures. Most importantly, privacy is preserved, thus any message part which was removed by redaction cannot be reconstructed from only knowing the redacted message and attestation. Depending on the specific scheme, additional properties can be achieved, e.g., to hide whether a redaction has been performed at all, or to ensure that two redacted documents cannot be linked to each other, even if derived from the same attested message.

In the example, the health authority could now define parts of the patient record (e.g., name, insurance number, dates, etc.) as
redactable, and a patient could decide which parts of the report to share, and which parts to keep confidential.

While established as an active research domain with 20 years of research, and enabling many novel privacy-preserving applications, redactable attestation schemes yet await a widespread application. On the one hand, this is due to a lack of awareness of these more recent cryptographic mechanisms, and on the other hand also a lack of standardization makes it difficult to use such advanced schemes without risking incompatibilities and legal uncertainty. In a state of legal uncertainty, it remains for each individual user of a scheme to claim that the needed properties of authenticity, non-repudiation and integrity are matching legal requirements. Meeting legal requirements often is one strong reason why digital signature schemes are employed in the first place.

The issue of not being standardized is now being addressed by SC 27 with the new ISO/IEC 23264 series, focusing on the standardization of redactable attestation schemes. While the already published ISO/IEC 23264-1 defines the framework and security requirements, ISO/IEC 23264-2 is currently under development, and will specify a variety of schemes with different security properties. These ongoing activities complement the already existing ISO/IEC 27038, which specifies the redaction of digital documents but does not consider how to uphold a valid signature after redaction of signed data.
SIGNING DOCUMENTS ON BEHALF OF A GROUP

Another caveat of standard digital signatures is that they uniquely identify the signer, which may not be necessary in many application scenarios. Staying within the health domain, a motivating example could be the following: when visiting a doctor, a patient gets a digitally signed time confirmation to present to her employer. However, while the document itself does not reveal any information about potential diseases, the employer could infer some information by checking the signer of the time confirmation, as it reveals the doctor’s identity, and thus also possible specializations of the doctor. Straightforward countermeasures such as, e.g., sharing the same signing key among all doctors in a given region, are not satisfactory, as they would be susceptible to key leakage and more.

One solution is offered by anonymous digital signature schemes using a group public key, as defined in ISO/IEC 20008-2. In such schemes, a group manager can issue signing keys to members of a group, who can then use their assigned keys for issuing digital signatures. However, in order to verify a signature, only the public key of the group manager is needed, and it is not possible to tell which member of a group is responsible for a given signature, i.e., group members can sign messages on behalf of the entire group. Yet, for many such schemes, a dedicated entity called opener may revoke the anonymity of a user in case of misuse, which may then lead, e.g., to the revocation of signing rights of a specific group member.

In the given example, a local health authority could take the role of the group manager, and distribute individual signing keys to all doctors, who may then sign such a confirmation for the time a
patient visited the doctor. The patient’s employer would receive strong cryptographic guarantees that the document was signed by an authorized doctor, while the patient’s privacy - which doctor was visited - would be fully maintained.

This type of signatures has found many applications already in the real world, including, e.g., Direct Anonymous Attestation as standardized in ISO/IEC 11889, which is implemented as part of the Trusted Platform Module (TPM) shipped with most modern laptops.

Within SC 27, WG 2 is active in keeping ISO/IEC 20008-2 up to date by extending the standard with new schemes offering increased efficiency. Furthermore, ISO/IEC 20008-3, which is currently under development, will specify a variant of the above approach, which does not require a group manager, but allows for ad hoc definitions of the set of public keys among which the signer may stay anonymous. These so-called ring signatures are already being used, e.g., in cryptocurrencies.

**PRIVACY-PRESERVING AUTHENTICATION**

Authentication is a crucial step to enforce legitimate access to sensitive or otherwise protected resources. However, in many applications, it is sufficient to ensure that a user is authorized to access certain resources, but there is no need to identify the individual user for protection of the user’s privacy.

A possible example is a scenario where a user wishes to access some age-restricted online service. While it is not necessary to reveal the user’s full identity, the service provider requires strong guarantees that the user is old enough to be granted access. The
use of plain digital signatures is overly complicated here, as in general a user would need to receive, e.g., from a public authority, a digital signature for every possible policy, e.g., age limit.

This problem can be overcome by anonymous entity authentication mechanisms, where a prover (the entity that claiming to be in the possession of a certain attribute) receives a digital certificate on personal data, and can then selectively decide which information to reveal to a relying party (the entity that is verifying the claimed possession of the attribute).

In the given scenario, a user could now receive a digital certificate on a data set containing name, address, birth date and more. Subsequently the user then only releases, e.g., her birth date to a relying party, without leaking any further information. Depending on the selected scheme, also unlinkability of different actions by the same user can be achieved. ISO/IEC 27551 provides an overview of the different privacy levels of unlinkable entity authentication mechanisms.

Such privacy-preserving authentication schemes can be built from various building blocks, including digital signatures using a group public key as defined in ISO/IEC 20008-2, or redactable attestation schemes as defined in ISO/IEC 23264-1. Furthermore, so-called blind signatures as standardized in the ISO/IEC 18370 series, where parts of the message to be signed can be disguised from the signer, can serve as a starting point for anonymous entity authentication mechanisms, as well as many other applications, including e-cash and privacy-preserving electronic voting protocols.
In the ISO/IEC 20009 series, SC 27 is standardizing a variety of mechanisms for anonymous user authentication from different building blocks, with the newest member of the family being ISO/IEC 20009-3 based on blind signatures, whose publication as an International Standard is expected soon. The specified mechanism is already available as free and open-source software release by major software companies, and its standardization will further contribute to the dissemination of privacy-preserving authentication mechanisms into large-scale applications.

**CONCLUSION**

In this article, we provided an overview of WG 2’s recent and ongoing standardization activities related to advanced digital signature schemes. These schemes can be used to maintain the high authenticity and integrity requirements of digital signatures where needed, while at the same time giving sufficient flexibility and functionality to support the design of various novel applications and business models which are in full compliance with legal regulations, in particular, related to privacy and data protection.

By actively pushing forward the development of standards related to privacy-preserving technologies, WG 2 offers their customers recommendations and guidelines for the selection and implementation of advanced schemes, supporting them in achieving high and formal security and privacy guarantees, adhering to legal regulations, and increasing trust into their digital services and products.
Encryption is one of the most foundational technique in cryptography and communication security in general. Encryption is a process that transforms a plaintext, i.e. a human-comprehensible text, into a ciphertext using a key. The ciphertext is a random-like text that is not understandable unless one possesses the key to decrypt it.

This cryptographic primitive is extensively used in communication security protocols, as for example rendering a conversation confidential or exchanging securely secrets.

The ISO/IEC 18033 series defines various encryption systems in 8 parts:

ISO/IEC 18033 Parts 2 and 5 focus on asymmetric encryption systems which use related but different keys in order to encrypt and decrypt plaintexts. More specifically, Part 2 defines algorithms that use a key pair for data confidentiality: one of the keys (public key) is used for encryption, the other (private key) is used for decryption. Part 5 specifies identity-based encryption systems, similar to the ones presented in Part 2 but the public key is a string that enables the identification of the owner.

ISO/IEC 18033 Parts 3 and 4 define two types of symmetric encryption systems, i.e. encryption systems that use the same key for encryption and decryption. Both parts define block ciphers and stream ciphers, respectively. The former is a type of algorithm that encrypts data blocks of fixed lengths. The latter use keystreams to encrypt plaintexts bitwise or blockwise.

ISO/IEC Part 6 defines a particular type of encryption, homomorphic encryption, which allows some computations on encrypted data without decrypting it.

Two others parts are currently under development, namely ISO/IEC 18033 Parts 7 and 8. The first defines tweakable block ciphers. They are block ciphers which take an additional input, the tweak, for encryption and decryption. The second is about fully homomorphic encryption schemes, which allow arbitrary computations on encrypted data without decrypting it.
The first part has had its fourth edition been published this year 2021, and is the general part of the ISO/IEC 18033 series. It defines terms and explains what encryption is, what are its nature and properties, and what are the requirements that are necessary for the subsequent parts of this series. Moreover, it presents in details the criteria for inclusion and deletion of encryption systems within ISO standards, along with possible attacks again such systems. Its role it to set up the necessary framework for all types of encryption systems.

The range of the application of such encryption techniques is very large and is actually involve in any form of data protection. Encryption is perhaps the most important cryptographic building block built in secure communication protocols. Indeed, depending on its design and configuration, an encryption system can bring any of the properties that a stakeholder would want for a communication product or service: confidentiality, privacy, data integrity, authenticity, non-repudiation, and so on and so forth. This ranges from IoT devices, autonomous vehicles or smart meters to complete infrastructures such as data centers until satellite navigation systems even entire smart cities.

As per confidentiality, the most obvious example of its application is the confidentiality of the communication between a client (a standard user on the Web) and a server (hosting a particular website). It is at the basis of the Transport Layer Security (TLS) protocol, used by billions of users every day on the Web.

Authenticity is of paramount importance on the Web, and one way to attain this property is the use of a Public Key Infrastructure (PKI). In PKIs, a centralised trusted authority Certification
Authority (CA) binds a public key (from an asymmetric key pair) with an individual, usually the owner of the corresponding private key. By doing so, encrypted or signed data using this key pair is trusted to be from that individual. This is done through the use of a public key certificate, containing the public key and public information of the individual. A way to avoid the use of public key certificate is identity-based encryption, as the public key is an easily identifiable string.

On a different note, (fully) homomorphic encryption is a technique that enables privacy-preserving mechanisms. Due to its ciphertext-computability property, the most investigated use case is cloud computing. Indeed, as one of the biggest impediments for outsourcing computation is the sensitivity of the data to be shared with the cloud computing provider, homomorphic encryption offers an appealing solution that would allow a data owner to outsource all its computations without compromising the privacy of its data. This is exactly why this is well use in electronic voting: it enables the exact counting of the votes without ever “opening the ballot papers”.

CRYPTOGRAPHY AND ITS UBIQUITOUSNESS IN THE DIGITAL SOCIETY

Cryptography, as indicated by its Greek origin "hiding" and "writing," is a method of hiding information by using a code or cipher. Only the intended recipient can decipher and read the hidden message.

Cryptography has a long history, which may trace back to ancient Egypt. Around 100 BC, Julius Caesar developed the famous "Caesar Cipher" to send secret messages to his generals in the field. Caesar Cipher is simple and easy to break. In World War II, the Enigma machine, a more advanced cipher device, was used by Germany to transmit intelligence information and commands secretly. The device has a rotor mechanism controlling the keyboard input and light board output. One inputs the message letter from the keyboard, and the corresponding ciphertext lights up on the light board. To decipher a code, one just needs to type in the ciphertext on the keyboard and read the light-up letter on the light board. The rotor settings on the machine had to be changed regularly to ensure security. The sending and receiving stations had to know and use the same settings to transmit a message successfully. This paradigm is the so-called symmetric cipher because both stations use the same key. In the 1970s, Whitfield Diffie and Martin Hellman introduced to the public
domain a new paradigm, the so-called public key cryptography or asymmetric cryptography. In this setting, a party has two cryptographic keys, one is publicly known, and the other is held privately. The sender uses the public key to encrypt data, and the recipient uses the corresponding private key to decrypt the ciphertext.

After about 50 years of development, modern cryptography has become a fundamental technology of securing the Internet, financial business, corporate data, personal private information, and many others in the digital society. Following are a few examples.

In the COVID-19 pandemic, many governments released the so-called contact-tracing apps to help public health officials to track infected people's close contact. However, location data is a type of sensitive data and should be closely protected. Advanced cryptography technology enables such contact-tracing systems to notify potentially exposed users without massive central surveillance. With so many people admitted to hospitals during the pandemic, the electronic health record system is vital for speedy processing and exchanging patients' medical information to save lives. An electronic health record includes a patient's demographics, vital signs, past medical history, immunizations, laboratory data, medications, etc. Regulations require proper measures to secure protected health information in electronic health records. Cryptography is the fundamental technology to provide data confidentiality and flexible access control to protected health information.

The financial sector heavily relies on cryptography to protect data security. The traditional banking system had used cryptographic mechanisms such as Data Encryption Standard
(DES) to protect monetary transactions since the 1970s. DES was later replaced by the new Advanced Encryption Standard (AES) algorithm. In the 21st century, billions of chip-based payment cards, also known as smart cards, are used worldwide. The smart cards contain an embedded microprocessor. The microprocessor chip stores cryptographic keys and are programmed to execute cryptographic algorithms to guarantee that transactions are from the right customers and not modified. In recent years, the rise of financial technology put even higher demands on using cryptology. With the booming of the mobile Internet, consumers have increasingly demanded easy digital access to their bank accounts, primarily through mobile devices. Completing transactions over the Internet faces much higher risks than traditional banking servicing through in-person contact. Safeguard systems use cryptography to encrypt accounting information and protect systems from faked transactions.

In the pandemic, working at home becomes the norm. Employees used to work in the corporate internal network protected by network security facilities like firewalls. The cooperate documents are transferred to and stored in the designated computers and devices. Now, employees access corporate information systems through the Internet and download sensitive documents to personal computers or mobile devices. The cooperate data been transferred over the Internet and stored on personal devices must be encrypted to prevent data leakage.

**NEED FOR SECURE KEY MANAGEMENT**

Both symmetric cipher and asymmetric cipher require cryptographic keys. Key management plays a central role in using cryptographic mechanisms for securing electrometric
communications. The fundamental problem of key management is to establish keying material securely between or among users, just like sharing Enigma machine rotor settings between stations. The established keying material can be further used with different cryptographic mechanisms to secure data communication between users.

The key establishment procedure, defined as a key establishment protocol, should guarantee that the established key comes from the purported user and is up to date and not modified during the process. If the key is used as a secret, the protocol should also make sure that the key is not exposed to unintended parties.

A typical example of a key establishment protocol would be the Transport Layer Security (TLS) protocol. According to statistics, over 70% of Alexa Top 100,000 websites nowadays adopt the TLS protocol to secure data flow over the Internet. The TLS protocol enables the browser clients to establish secret keys with the accessing website server. These secret keys are further used to protect communication data between the clients and the server.

Secure key establishment protocols are notoriously difficult to design, and many proposed or even some widely deployed key establishment protocols were later found to have serious vulnerabilities. Hence, it is essential to deploy well-scrutinized protocols for security purposes. Otherwise, any cryptographic mechanisms will be ineffective if the used key is weak or comprised.
ISO/IEC KEY MANAGEMENT STANDARDS

ISO/IEC publishes a serial of key management standard documents: ISO/IEC 11770: Information security — Key management. The serial of standard comprises seven parts:

- ISO/IEC 11770-1:2010 defines a general key management model including the key life-cycle model, required key management services, and conceptual models for key distribution.
- ISO/IEC 11770-4:2017 defines a series of key establishment mechanisms based on weak secrets such as passwords that a human can readily memorize.
- ISO/IEC 11770-5:2017 defines a series of key establishment mechanisms based on symmetric cryptographic techniques to establish shared secret keys between groups of users.
- ISO/IEC 11770-6:2016 specifies key derivation functions that take secret information, such as those established using mechanisms defined in other parts, and other parameters as input, and output one or more "derived" secret keys.
- ISO/IEC 11770-7:2021 specifies mechanisms for cross-domain password-based key establishment. Each user shares a login password with its domain authentication server. The key establishment mechanisms enable two users from different domains to establish a shared secret.
The relation among the seven parts is shown in figure below.

As an example, ISO/IEC 11770-3:2021 is briefly introduced here. ISO/IEC 11770-3 defines key management mechanisms based on asymmetric cryptographic techniques. The mechanisms in the document are in three categories. Fifteen mechanisms in Category 1 are specified to enable two parties to establish a shared secret key. The shared secret key results from exchanging messages between two parties in these mechanisms, and none of the parties can predetermined the value of the shared secret key. Six mechanisms in Category 2 are specified to enable one part to choose a secret key and securely transport it to the peer party. Three mechanisms in Category 3 are defined to transfer one party's public key to others in an authenticated way. As shown above, the document provides a broad range of mechanisms with different security attributes and efficiency.
CONCLUDING REMARK

In the digital era, massive data is accumulated daily. Sensitive data such as personal data, corporate data, government data, etc., is collected, transferred, processed, and stored in open or restricted environments. Sensitive information faces increasing risks from unauthorized access. Cryptography plays a vital role in preventing the data from falling into the wrong hands without the knowledge of the user or owner. A cryptographic mechanism relies on a secure key management method to distribute required cryptographic keys safely. Designing secure key establishment mechanisms is elusive, and the subtleness of such mechanisms often causes severe vulnerabilities. It is recommended to use carefully-designed and well-scrutinized mechanisms. ISO/IEC 11770 provides a broad range of such choices from symmetric-based to asymmetric-based mechanisms. ISO/IEC 11770 also defines password-based mechanisms and a few to establish shared secrets among a group of users.
INTRODUCTION

A block cipher transforms a block of plaintext bits to a block of ciphertext bits of same size, under control of a secret key. As a popular component in symmetric cryptographic schemes, block cipher is widely used in all kinds information systems for data protection. The first publication of block cipher in human history, i.e. the Data Encryption Standard (DES), dating back to 1970s, lays an initial foundation for the public understanding of modern cryptography and standardization.

ISO/IEC 18033-3 specifies a set of classical block ciphers. It is a part of ISO/IEC 18033 series, which aim to promote the application of encryption systems and reflect the state of the art in current encryption systems, including asymmetric ciphers (18033-2), block ciphers (18033-3), stream ciphers (18033-4), the identity-based asymmetric encryption system (18033-5), homomorphic encryption (18033-6), tweakable block ciphers (18033-7, under development), and fully homomorphic encryption (18033-8, under development).

This paper discusses how to choose and use block ciphers in ISO/IEC 18033-3.
To choose a proper block cipher, security is the most important thing to consider. The security strength of a well-designed block cipher depends on two parameters: key length and block length. The key is top secret for a block cipher. One of DES's weak points is the valid key length of 56 bits. Trying every possible key in turn was possible even in 1970s using some dedicated cracking machines. The key length of algorithms in ISO/IEC 18033-3 is at least 128 bits, except that the 128-bit key of TDEA has 112 valid bits, the rest may be used for error detection. It is impossible to do exhaustive search for a 112-bit key.

The block length restricts the security of applications above block ciphers. Even the key is unknown, all plaintext-ciphertext pairs are enough to break the above security, if the block length is too small.

Eight block ciphers are contained in ISO/IEC 18033-3:2010 and AMD1:2021. They are listed in the following table.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Key length</th>
<th>Block length</th>
</tr>
</thead>
<tbody>
<tr>
<td>TDEA</td>
<td>128 or 192 bits</td>
<td>64 bits</td>
</tr>
<tr>
<td>MISTY1</td>
<td>128 bits</td>
<td>64 bits</td>
</tr>
<tr>
<td>CAST-128</td>
<td>128 bits</td>
<td>64 bits</td>
</tr>
<tr>
<td>HIGHT</td>
<td>128, 192 or 256 bits</td>
<td>128 bits</td>
</tr>
<tr>
<td>AES</td>
<td>128 bits</td>
<td></td>
</tr>
<tr>
<td>Camellia</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEED</td>
<td>128 bits</td>
<td></td>
</tr>
<tr>
<td>SM4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• TDEA (Triple Data Encryption Algorithm), which is commonly known as Triple DES, provides a simple way to increase the key size of DES, but the cost is three calls to DES.

• MISTY1 was one of the final algorithms in the European NESSIE project, and selected by the CRYPTREC project for Japanese government use in 2003.

• CAST-128 as a famous default block cipher in some earlier versions of GPG and PGP, is a Canadian e-government approved block cipher.

• HIGHT is a Korean industry standard, and is suitable for lightweight applications.

• AES (Advanced Encryption Standard) was chosen by an open and transparent process lasting from 1997 to 2000 in order to replace DES, and written in U.S. FIPS PUB 197 in 2001.

• Camellia is a NESSIE selected algorithm and Japanese e-government algorithm.

• SEED is a Korean industry standard and Korean e-government algorithm.

**SM4 BLOCK CIPHER IN AMD1:2021**

SM4 (formerly SMS4) was first used in a Chinese National Standard for Wireless LANs (GB 15629.11-2003), then publicly released independently in 2006, officially renamed to "SM4" in Chinese industry standard GM/T 0002-2012, and finally standardized in 2016 as a Chinese National Standard (GB/T 32907-2016).

SM4 adopts a unique unbalanced Feistel structure unlike the other algorithms in 18033-3. Its S-box is linear equivalent to that of AES, having good differential and non-linear properties. Its
succinct linear transformation is optimal among the same types. SM4 strikes a good balance between efficiency and security.

After the release of SM4 algorithm, a lot of literature shows that SM4 has no security weakness, and is secure against classic cryptanalysis methods including differential attack, related-key differential attack, impossible differential attack, linear attack, zero-correlation linear attack, rectangle attack, square attack, and algebraic attack etc.

SM4 algorithm is widely used in Chinese commercial cipher products. At least more than 700 different products use SM4 including security chips, terminals, equipment, and application systems. The products are widely used in multiple essential fields in China, covering smart grid, financial system, commercial applications, and transposition and so on.

**HOW TO USE BLOCK CIPHERS**

It is dangerous to directly encrypt plaintext blocks using block ciphers. The block cipher is not a secure encryption scheme, but only an important component in symmetric cryptographic schemes, such as encryption scheme, message authentication code (MAC) scheme, authenticated encryption scheme. We call these schemes block cipher modes of operation, or modes in short. All schemes have corresponding ISO/IEC standard documents:

- **SEED** is a Korean industry standard and Korean e-government algorithm.
- **For encryption modes providing confidentiality**, refer to ISO/IEC 10116:2017 Information technology — Security techniques — Modes of operation for an n-bit block cipher
- For MAC modes providing authenticity, refer to ISO/IEC 9797-1:2011 Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher
- For Authenticated encryption modes providing both confidentiality and authenticity, refer to ISO/IEC 19772:2020 Information security — Authenticated encryption

For block ciphers of n-bit block length, the modes have typically only n/2-bit security. If n is 64, that usually means only $2^{32}$ blocks of data can be processed for a key, therefore Key lifecycle management is important for small-block mode applications.

**CONCLUSIONS**

ISO/IEC 18033-3 provides a set of classic block ciphers, which must be in modes of operation to implement confidentiality or authenticity features. Choose it well and use it securely according to ISO/IEC 18033-3, 10116, 9797-1, 19772 and 10118-2 etc. documents.
ABOUT SC 27/WG 2

The work of WG 2 attracts experts from a diverse range of business organizations, government bodies and agencies, consumer and industry groups, and academia.

WG 2 SCOPE

The scope of WG 2 covers cryptographic (and non-cryptographic) techniques and mechanisms specifying several options regarding symmetric cryptographic techniques and asymmetric cryptographic, which includes:

- confidentiality;
- entity authentication;
- non-repudiation;
- key management, including random number generation and prime number generation;
- data integrity such as message authentication, hash-functions, and digital signatures.

WG 2 PORTFOLIO

WG 2 has developed many cryptographic standards to address the need for ensuring security of IT systems and applications. The following is a high-level view of the WG 2 portfolio:

- ISO/IEC 4922 Secure multiparty computation
  - Part 1: General (Under development)
  - Part 2: Mechanisms based on secret sharing (Under development)
- ISO/IEC 7064 Check character systems
- ISO/IEC 9796 Digital signature schemes giving message recovery
  - Part 2: Integer factorization based mechanisms
  - Part 3: Discrete logarithm based mechanisms
- ISO/IEC 9797 Message authentication codes (MACs)
  - Part 1: Mechanisms using a block cipher
  - Part 2: Mechanisms using a dedicated hash-function
  - Part 3: Mechanisms using a universal hash-function
- ISO/IEC 9798 Entity authentication
  - Part 1: General
  - Part 2: Mechanisms using symmetric encipherment algorithms
  - Part 3: Mechanisms using digital signature techniques
  - Part 4: Mechanisms using cryptographic check function
  - Part 5: Mechanisms using zero knowledge techniques
  - Part 6: Mechanisms using manual data transfer
- ISO/IEC 10116 Modes of operation for an n-bit block cipher algorithm
- ISO/IEC 10118 Hash-functions
  - Part 1: General
  - Part 2: Hash-functions using an n-bit block cipher
  - Part 3: Dedicated hash-functions
  - Part 4: Hash-functions using modular arithmetic
- ISO/IEC 11770 Key management
  - Part 1: framework
  - Part 2: Mechanisms using symmetric techniques
  - Part 3: Mechanisms using asymmetric techniques
  - Part 4: Mechanisms based on weak secrets
  - Part 5: Group key management
• Part 6: Key derivation
• Part 7: Cross-domain password-based authenticated key exchange

• ISO/IEC 13888 Non-repudiation
  • Part 1: General
  • Part 2: Mechanisms using symmetric techniques
  • Part 3: Mechanisms using asymmetric techniques

• ISO/IEC 14888 Digital signatures with appendix
  • Part 1: General
  • Part 2: Integer factorization based mechanisms
  • Part 3: Discrete logarithm based mechanisms
  • Part 4: Stateful hash-based mechanisms (Under development)

• ISO/IEC 15946 Cryptographic techniques based on elliptic curves
  • Part 1: General
  • Part 5: Elliptic curve generation (Under revision)

• ISO/IEC 18014 Time-stamping services
  • Part 1: Framework
  • Part 2: Mechanisms producing independent tokens
  • Part 3: Mechanisms producing linked tokens
  • Part 4: Traceability of time sources

• ISO/IEC 18031 Random bit generation (Under revision)
• ISO/IEC 18032 Prime number generation
• ISO/IEC 18033 Encryption algorithms
  • Part 1: General
  • Part 2: Asymmetric ciphers
  • Part 3: Block ciphers
  • Part 4: Stream ciphers
  • Part 5: Identity-based ciphers
- Part 6: Homomorphic encryption
- Part 7: Tweakable block ciphers (Under development)
- Part 8: Fully homomorphic encryption (Under development)
- ISO/IEC 18370 Blind digital signatures
  - Part 1: General
  - Part 2: Discrete logarithm based mechanism
- ISO/IEC 19592 Secret sharing
  - Part 1: General
  - Part 2: Fundamental mechanisms
- ISO/IEC 19772 Authenticated encryption
- ISO/IEC 20008 Anonymous digital signatures
  - Part 1: General
  - Part 2: Mechanisms using a group public key
  - Part 3: Mechanisms using a group public key (Under development)
- ISO/IEC 20009 Anonymous entity authentication
  - Part 1: General
  - Part 2: Mechanisms based on signatures using a group public key
  - Part 3: Mechanisms based on blind signatures (Under development)
  - Part 4: Mechanisms based on weak secrets
- ISO/IEC 23264 Redaction of authentic data
  - Part 1: General
  - Part 2: Redactable signature schemes based on asymmetric mechanisms (Under development)
- ISO/IEC 29150 Signcryption
- ISO/IEC 29192 Lightweight cryptography
  - Part 1: General
• Part 2: Block ciphers
• Part 3: Stream ciphers
• Part 4: Mechanisms using asymmetric techniques
• Part 5: Hash-functions
• Part 6: Message authentication codes (MACs)
• Part 7: Broadcast authentication protocols
• Part 8: Authenticated encryption (Under development)

Takeshi CHIKAZAWA (WG 2 Convenor)
Hirotaka YOSHIDA (WG 2 Convenor-Support),