Voice of Experts

Blockchain & Cryptography

Sylvain CARRIOU, Mourad FAHER, Alban FERAUD,
Christine HENNEBERT

EUROSMART, OCTOBER 2018

Table of contents

Foreword

Stéfane Mouille

President of Eurosmart

stefane.mouille@eurosmart.com

The digital world is now hyper-connected and it is gradually changing daily life of the European Citizens and consumers.

This transformation of our society imposes to revise also our legal framework to make sure that the European Values are included into this “new digital ocean”.

This digital world is not virtual! It is composed of hardware, software, applications, connectivity and human know-how.

This expertise derives from technology experts which play a part in modernizing the traditional institutional scheme and finally innovating the world.

Eurosmart is proud to count the most renowned technologies experts from the cryptography community, digital identity technologies, biometric technologies and digital security.

These critical technologies are deployed in the hands of several billions of users to secure their digital identities, transactions, business and personal data… Sometimes simply their privacy.

Eurosmart is the ‘spokesperson’ of this European excellence in the world and our experts are actively contributing to the European and International standardization process.

We are proud of our European roots but we can boast an open-mindedness at the same time, thanks to our global presence.

In view of this, we would like to share biannually the “Opinion of experts” from our community.

The first edition is dedicated to the cryptography technology with a strong focus on the blockchain in the digital identity and the personal data protection, the future of the post quantum crypto.

We hope you will enjoy reading the first article.

A Hello World business model for ID in Blockchain context

Mourad FAHER

Standardization Experts, Standards & Technology, Gemalto

mourad.faher@gemalto.com

The context

With the outlook of sketching a use case featuring IDentity and Blockchain, one will first consider the current context, and make a general observation: nowadays social network platforms and operators (and not only them) have identity information almost at will, since it is delivered by the careless users the protection of their personal data through social networks or other streams. But from May 2018, things will have to change because the entry into force of the GDPR (2016/679) will entail very careful management of personal data. As a result, all internet operators will no longer be able to handle/exploit the data of their subscribers without privacy protection measures. Gradually, other ways of managing the flow of personal data will have to emerge, since the exploitation and the usefulness of personal data will not stop because of the GDPR, it will simply have to be done in a frame more regulated to protect data controllers and data processors from lawsuits and fines.

Example of Requirements

Now, in order to derive roughly an economic model for Identity over blockchain, let's assume the IDentity is carried on blockchain in a way or another; **it will have** to remain consistent with the context evoked above, and **to allow for**:

The user/citizen to give their consent for their personal data to be posted on the blockchain

2) The user to give its consent for its personal data to be consulted by a third party (e.g. service provider, supplier of ID attributes, actuarial / statistical companies, merchandising companies, etc.)

3) The operator of said blockchain to ensure that the personal data are recorded in a format such as each ID attribute represents a "unitary transaction" (such transactions are then added to a block and validated for

the blockchain to grow). And this so that the user whose data is in play, can:

> **3a**. identify individually each attribute of their identity (e.g. surname, first name, age group, birth data, marital status, address, municipality of residence, place of birth, qualification (s), professional experience, etc.)
>
> **3b**. decide whether or not, when requested, to disclose all or part of their data so as to preserve anonymity in certain cases and vis-à-vis certain third parties (e.g. if I disclose to you my current municipality of residence, and my place of birth, you can derive statistics but not directly know who I am unambiguously).
>
> **3c**. be assured that their transferred data are not physically on the blockchain, but rather on repositories pointed from the blockchain.

4) The blockchain operator to notify the user each time a query to explore its data is addressed to the blockchain

5) The blockchain operator to deliver the required data only if the user consents (digitally)

6) The user to revoke (right-to-be-forgotten) all or part of its personal data, even if the user had previously consented to make them accessible from the blockchain i.e. if the user makes a justified request, these data should no longer be accessible to any third party

7) The operator of the blockchain to give the user the means to update their personal data (e.g. address, qualification, marital status etc.)

Without seeking here to be exhaustive, one has already covered with the above requirements much of the GDPR.

Towards a business model tentative

Now, let's put into practice the requirement points (from **(1)** to **(7)**) enumerated in the previous section, and try to derive from it an economic model (a more in-depth study is necessary of course):

(1) For the consent to be factual, effective and non repudiatable, it must be executed digitally and willingly by the user out of a personal support of personal data from which the data will be transferred to the blockchain. This would allow the users to see and consider tangibly the data they want to transfer, and to be associated with the supply operation to the blockchain. Considering that for the use case of "ID and blockchain" to work, it should be attractive not only to users acquainted with blockchain concepts and capable to proceeding to the data transfer operation, but as well to more conservative ones. Therefore it would be irrelevant to make this choice unbalanced to the detriment of the non-blockchain-minded user, and both users should be enabled to access and enjoy digital services. To this aim, they should have their ID data initial resource available from the same versatile form-factor (e.g. smart card, eSIM, eUICC, embedded SE on mobile, TEE or connected wearable object, etc.) To encourage every user, one can introduce an incentive by rewarding them (with **cryptocurrency**) during the operation **(2)**.

Operation **(2)** is a promise to clear the transaction **(1)**: "*If you pay an amount to obtain your individual digital identity token, you can use it to carry personal data of your choice on a blockchain and withdraw from their use a remuneration in cryptocurrency; and with an amount of X cryptocurrency, you can get e.g. discounts for XYZ, benefits of XYZ etc.*" (Advantages to be assessed with service providers and various providers). As an additional incentive, and to divest itself of the exclusively governmental side of the use of the ID data, the operator of the blockchain can propose to the user, in addition to the certified data transferred from its individual support of data, to be able to indicate additional data in response to question panels focused on specific areas. And this is where the operator of the blockchain can charge third parties who want their panel is part of the choice offered to the user. Therefore, in this model, the operator of the blockchain is remunerated in at least two ways: the delivery of the secure token bearing the certified ID, and the subscription paid by third parties (merchandising companies etc.) Interested in having their panel appear among the choices offered to the user. Why would the user be interested in answering a panel? Because it increases its chances of seeing its data requested/read/collected/processed and thus increase its earnings in **cryptocurrency**.

Operation **(3)** is part of the project management and could therefore be achieved by adopting a common blockchain data format (yet to be normalized, just starting e.g. in ISO TC307). Accordingly, each ID attribute can stand for a **transaction** serving to populate the blocks of a blockchain.

(3a) is part of the project management. How in practice would (3b) be achieved? The user with an individual ID token (smart card, eSE on mobile, etc.) connects to a public site and loads and installs the signed client software that allows him to transfer his authorization (consent) to port personal data to the blockchain. The software communicates with the ID token and exposes an interface (GUI) through which the user can choose from the certified data he wants to transfer, and which also exposes the panels to choose from. The technology

to achieve this is proven and should not be a problem. Several client devices can be supported (PC, smartphone equipped with NFC, mobile directly embedding a secure element, and even later connected personal objects, etc.). It will of course be taken into account that future users will be able to perform the transfer operation from their NFC-enabled mobile once paired with their individual ID card as an example.

Point **(4)** is part of project management, and can typically be achieved by the implementation of a "**smart contract**". The **notification** can be done via the mobile of the user who receives a message warning about the read request event. When a user "transfers" his data, he receives cryptocurrency, and when a third party requires this data, it pays cryptocurrency in turn. So one has an additional revenue for the operator of the blockchain ID: a third party who wants to explore **certified** and/or **uncertified ID data**, will have to pay a cryptocurrency amount, and he will have to buy it from the operator of the blockchain ID: "X euros against Y in cryptocurrency". So let's recap: the blockchain operator has revenues as follows: **the delivery of the secure document bearing the certified ID** + **the subscription paid by the third parties wanting to publish their panels** + **the cryptocurrency bought by third parties to access the data**. It is understood that the smart contract orchestrating the crypto-currency remittance and handling the events requires an asynchronous operation management to cater to a high volume of transactions (**scalability**).

Point **(5)** is realized in **(4)** through the **smart contract**. The point **(6)** is regulated by the point **(3c)**: it suffices to delete the pointed data without modifying the blockchain.

The point **(7)** is regulated by the point **(1)**: it suffices the user to redo, as described in step **(1)**, a transfer of the certified data or/and to re-enter fresh data on question panels.

Conclusion

In the previous model one implicitly considered that when the user publishes (transfer) his certified and non-certified data, it acts as a simple user while the blockchain **validator** (**minor**) collects, checks, hashes and signs the transaction to issue **blocks** to be appended to the growing blockchain. When minors are not relying on a **PoW** (Proof of Work) to validate the blocks, a properly designed **PoS** (Proof of Stake) shall take a **consensus** management algorithm for miners' role, including for their reward in cryptocurrency.

With this tentative business model, one went step by step through some topics relating to blockchain governance and concepts, and one saw how a jurisdictional context sets the requirements and complexity and can be the opportunity for a new European innovative digital approach, provided the requirements are met.

A Secure Hardware for GDPR compliance on blockchain

Christine HENNEBERT

Expert on Blockchain & Secure Systems and Connected Objects, CEA-LETI Grenoble

christine.hennebert@cea.fr

Blockchains / DLT systems are secure distributed systems that lead to a reconsideration of ecosystems and business models by considerably changing the role of today's trusted third parties. While centralized systems are "**data-centric**", blockchains enable to build "**user-centric**" systems and to give to the users the control of the use made of their personal data.

The personal data is digital data issued from communicating objects. They carry information about the life, behavior or habits of the owner of the objects. The General Data Protection Regulation (GDPR) obliges companies from May 2018 to protect these data and prohibits their exploitation without their owner's knowledge and consent.

With a blockchain, it becomes possible to ensure by design the security and the privacy of complete Internet of Things (IoT) systems and to deliver from end-to-end data while ensuring their security and protecting the privacy of their owner.

The owner of the data is not necessarily the owner of the communicating object from which the data is generated and issued. We are interested in the use-case of the collective self-consumption of energy. In a co-ownership, the energy (and the data indicating its quantity) issued from sources of production belongs to the community while the equipment that products the energy (solar panels, geothermal apparatus ...) results of the investment of a third party. Similarly, the data that indicates the energy consumption issued from the connected sensor and located in a housing, is the property of the occupant of the housing, while the energy smart meter is fixed, linked to the housing and managed by a third party.

In this context, it is necessary to associate, in a flexible and scalable manner, the identifier of the connected objects with the identity of the owners of the data they generate and transmit. In the case of housing, the communicating objects that generate the personal data are fixed. The identifier of the energy consumption smart meter must be associated with the identity of the occupant of the

housing at the time of the signing of the lease, then dissociate at his departure. A technical solution consists of using attributes for this purpose. The identifier of the communicating objects is completed by various attributes describing characteristics of the object, such as, for example, its type, its data transmission rate, its update version, the number of the housing where it is located. Similarly, the digital identity of the person occupying the housing is completed by attributes such as the date of signing the lease or the housing number. Thus, it is conceivable to protect and keep independently the identifiers of the communicating objects and the identities of people, which prevents an outside observer to make the connection between the two. When transferring and exploiting digital data, based on a common attribute such as housing number, the system will be able to find both the source of the data and its owner while respecting the "privacy" in accordance with GDPR regulations.

Personal data must be protected in accordance with GDPR regulations and must also be accurate and certified. To guarantee privacy, data must be transmitted and stored confidentially. They must also be authenticated, which involves checking the identifier of the source even the identity of the owner. The integrity is an exigence ensured by cryptography.

The blockchain offers an elegant solution to all these security needs because it avoids or greatly simplifies key management, which is a complex problem that lacks of a satisfactory solution in centralized systems. The blockchain intrinsically guarantees the **traceability**, **timestamping** and **non-repudiation** of the data. It provides traceability by consulting the shared register for greater transparency, trust and democracy. It authenticates, without any possible denial, the wallet from which the transactions are issued. Thus, it allows each occupant to manage by himself the access to his personal data and the use that is made of it, without resorting to any trusted third party.

To orchestrate the exchanges between the actors of the system (people, sensors and machines), **Smart Contracts** are developed with a Turing-complete language (with clear syntax and machine-independent semantics) and deployed in the blockchain. Executed in a blockchain, Smart Contracts enable the distribution and the automation of the tasks in a safe and traceable way.

Thanks to the properties of the blockchain, it is possible to store the encrypted data off-chain without explicit mention to their source nor to their owner, and to be retrieved with their owner's consent. The **right to be forgotten** can be satisfied by removing any possible access to personal data, which can be done and traced by a blockchain.

Ensuring to the users of the system that their personal data are protected in the sense of "privacy", means being able to manage their digital identity. The identity should be masked to certain actors, revealed to others, for the billing of energy consumption for example, associated or dissociated with connected objects in a contextual way, included in a group, and revoked if necessary. The use of a self-sovereign digital identity provides an appropriate response to this problem that still needs to be deepened and tested in concrete use cases. This also raises the question of interoperability between Smart Contracts and between blockchains with different parameters. In particular, the way to authenticate the actors and to access to the ledger of the blockchain needs to be standardized to deploy complex and communicating interoperable systems.

The security and privacy functions are realized thanks to cryptography and secret keys embedded in the physical objects. While deployment in real environment in society, the communicating objects that generates the data are physically accessible. Their **embedded secret keys and cryptographic functions** must be robust to physical attacks, especially side-channel attacks and fault injections. To scale, it is mandatory to design and produce communicating objects that embed **secure hardware elements**.

The combination of the blockchain with devices secured by hardware will offer a new generation of products and systems centered on the interest of users and cyber-robust.

How can we ensure that the information entered in the blockchain matches with a physical reality?

Sylvain CARRIOU

President of Christalchain

scariou@crystalchain.io

The promise of the blockchain is summed up in 4 key points: the **immutability** of data over time, the **timestamp** of their integration in the blockchain, their permanent **auditability** and the public or anonymous **authentication** of their issuer.

These different sources of security make it much easier to identify and locate a fraud and thus deter the fraudster.

However, this technology does not evaluate the relevance and veracity of the recorded data. This question often comes up in our discussions with our customers and partners. It seems therefore appropriate to share here the different methods that we have experimented with and identified in order to provide additional security regarding the **correspondence between physical realities and digital data** integrated into the blockchain. Depending on the use case, we can identify several ways to proceed. These methods are not incompatible with each other; on the contrary, combining them enables blockchain users to add security.

The first method is **physical control**. The observation of an impartial third party through auditing and controls allow to certify the processes and the information linked to the processes. This applies for example to an independent certifier who audits an enterprise's inventory, the quality of a product sample or the processes used.

These audits are ad hoc, usually done once a year. To ensure the reliability of this method, **it is important for the audited samples to be representative** of the production batches and that the audited processes are not modified between two audits.

The second method is the automatic **analysis of the consistency** of the data entered in the blockchain. Checking the consistency of the data can be done in several ways.

We can verify whether or not a data is consistent by **comparing it with a history or a predefined standard**. Imagine a factory that orders each month a different

component from a supplier. During an order, if the quantity of one of the ordered components seems abnormally high, a program can create an alert to check if an error has been made. This can be done through comparing the current ordered quantities to the history.

In the context where several data relating to the same event or to the same product are integrated, the **consistency between data can be checked**, in particular when several actors of the same sector are involved in the blockchain.

Take the example of a processing plant that deals with two types of food, organic products and non-organic products, whose flows are recorded in the blockchain. If the plant decides to sell some of the non-organic products as organic ones, there will be an inconsistency with the amount of organic product that will have been delivered to the company upstream. This analysis can incorporate business-specific parameters such as the rate of return or loss between upstream and downstream.

The consistency analysis still **requires a common ground for comparing the data or a causal link** between the data.

The third method is the **automation of data integration** by using connected objects. The use of connected objects makes it possible, with sensors and actuators, to interact reciprocally between the physical and digital worlds.

The use of sensors makes it possible to **remove the human intervention** during the integration of the data. It is however necessary to ensure the integrity of the equipment used throughout its design, installation and use.

This solution seems to fully meet the issues discussed in this article. Indeed, connected objects have the advantage of being able to collect information **continuously**, and in a completely independent and therefore **impartial way**.

As part of the integration of **information triggering smart-contracts**, we can resort to the use of "**Oracles**". "*Oracles are trusted entities that sign (and attest to) claims about the state of the world"* [1]. These Oracles can be software or hardware.

Some software oracles can retrieve relevant information from trusted resources such as certified institutions and certify through cryptographic processes the authenticity of the source. This model still requires for the source not to be corrupted and that the Oracle software does not transform the information.

Other software Oracles use **voting mechanisms with tokens** within a community whose interest in telling the truth matches financial incentives for each member of the community. These mechanisms are particularly used in **predictive market** such as sports betting, in order to testify to the outcome of the event that led to speculation.

This type of Oracle seems promising but does not allow dealing with private or more specific information such as the geolocation of an object or the temperature in a room.

Hardware Oracles simply connect objects such as the sensors mentioned above, which have been secured with a **cryptographic certificate** and a system of **disconnection of the sensor** in case of piracy.

These Oracles seem appropriate to link the physical world to the digital world because they can benefit from or they complement the connected objects solution (which removes the human bias) by offering a greater **computer security**.

The search for secure solutions to ensure the durability of the convergence between the physical world and the digital world is one of the major issues of our time. This article aims to provide a brief overview of existing and emerging solutions. Of course, for each sector, we must ask ourselves the issues, the risks and the feasibility of each available control or guarantee system.

1 Rabesandratana, Vanessa, et Nicolas Bacca. « L'Oracle hardware : la couche de confiance entre les blockchains et le monde physique », Annales des Mines - Réalités industrielles, vol. août 2017, no. 3, 2017, pp. 91-93.

Quantum information science: a new horizon for cryptography

Alban FERAUD

Regulatory affairs, market & business development - Strategy & Market Offer Citizen Identity - IDEMIA

alban.feraud@idemia.com

Preamble

This document would give an overview on quantum physic principles, quantum key distribution and quantum information science and would reflect a deeper mode the cryptography aspects, also named as Post Quantum Cryptography, included the expected impact on cyber security and on the security market.

What it the quantum information science?

Quantum information science (QIS) results from the two main advents of the 20th century: (1) the information theory, and (2) the quantum physics.

Information theory was created by Claude Shannon and has allowed moving from an analogous representation of information (where the information is directly represented by a physical quantity such as an electric current in a circuit) to a digital representation where the information is encoded into binary units (bits) where each of them is encoded as a physical quantity. This theory has paved the way to the digitalization that is at the heart of the main innovations of the 20th century: the internet, mobile communication …

Quantum physics describes the behavior of infinitely small particles. Each and any experiment that has been realized have demonstrated that it is accurate. It is at the basis of major breakthroughs of the 20th century such as nuclear energy, climax models, chemical processes, laser technology, or medical imaging (e.g. scanner MRI), medicine and health services…

The combination of both sciences allows harnessing on the properties of matter described by quantum physics to obtain, process and transfer information. The quantum properties of the matter promises significant benefits in term of speed, capacity and security for information

processing compared to what is realizable in the digital world.

Over the last decades, academic and industrial interest for QIS' technologies has significantly risen. The number of patents (published) increased by 430% between 2014 and 2017 while it doubled between 2004 and 2013.

Even though there are still many breakthroughs to come, there are today many companies proposing innovating goods and solutions relying on QIS's technologies. These companies are mainly located in US, Europe and China.

The main industrial applications of QIS's technologies span from the **quantum metrology and sensor**– e.g. atomic clocks, magnetometer, gravimeters, and inertial motion units -, **to quantum computation and simulation** – for precise simulation of quantum phenomenon and implementation of innovative simulation algorithms regular computer can't execute - and the **quantum communication** mainly encompassing the quantum key distribution.

In the near future, QIS's technologies will impact cryptography as we currently know in several respects:

1. **Quantum communication** offer (1) an alternative method to secure a communication channel that does not (solely) rely on cryptography means and (2) new methods for generating random number based on quantum phenomenon;
2. **Quantum computation and simulation** will in the future allow implementation of new algorithms that may put at risk the asymmetric cryptosystems we use today.

Random Number Generator

Random number: what for?

Random number are instrumental for cryptography as they are used for (1) key generation, (2) cryptographic algorithms and (3) authentication protocols.

In the key generation process, random number ensures that the resulting key can't be found more quickly than by trying to guess its value. It shall not be possible in any manner to predict or have any piece of knowledge about a single bit of the generated key. Should this occur, it would weaken and even ruin the security of cryptographic operations performed using the said key.

Some cryptographic algorithms such as EC-DSA use challenge to compute a digital signature or an encrypted block. The strength of the cryptographic operation and the confidentiality of the private key requires to also ensure the complete secrecy of the challenge. The knowledge of as less as a single bit of the challenge may lead to the disclosure of the private key. It implies to ensure the challenge is not predictable so that it can't be guessed by an attacker. Random number can achieve this requirement.

Random number are also used for authentication protocols. In a challenge/response process, usually a challenge is generated and sent by an accepter (requiring an authentication) to the prover (that will prove it is genuine). Upon reception the prover signs it with its authentication creation key to generate an authentication token it returns to the accepter. The latter checks the authentication token using the corresponding authentication verification key to make sure the prover possesses the authentication creation key. To ensure a strong authentication protocol, the challenge generated by the acceptor shall not be predictable to avoid attacks in which someone tries to impersonate the legitimate prover by intercepting their communications and presenting to the acceptor a correct authentication token. Two cases may occur : (1) the attacker can predict a future challenge leaving him time to compute in advance the corresponding authentication token, or (2) the acceptor generates a challenge that has already been generated and used in a previous authentication protocol and whose corresponding authentication token is known by the attacker (that recorded it), that just has to replay (replay attack). A random number used as challenge can totally eliminate these risks.

True random number

In order to be secure, a random number shall be truly random. This is far from being simple. Software based random number generator creates a stream of bits from a deterministic process (internal clock, counter…). Despite it may look random, it is not as the very nature of the underlying source is deterministic. Deep statistical analysis of the stream of bits or the knowledge of the generation methods may lead to predict future values. As the stream of bits is predictable, this kind of generator is not suitable.

Usually true random numbers are generated from a physical phenomenon whose very nature is known to be governed by randomness and is not deterministic, such as thermal noise (noise in a resistance resulting from the jitter of electrical carrier - electrons - due to the temperature) or avalanche breakdown within a diode junction (noise resulting from random avalanche breakdown when the applied voltage is near the avalanche voltage).

Limitation of current true random number generator technology

Designing a true random generator requires several steps. First of all, the source of randomness resulting from the physical phenomenon shall be modelled to assess its properties. It includes (1) statistical properties such as the entropy (amount of randomness) as well as (2) the mode of failure and their characterization (what are the behaviour of the generated random when a failure occurs), and (3) dependencies to environmental factors (temperature, electromagnetic field…). Modelling is instrumental to design a post-treatment to apply on the output of the source of randomness to (1) correct its statistical bias that have been identified and (2) implement tests for the detection of failure of the source of randomness.

Modelling a source of randomness is very complex and requires deep technical knowledge. The model of the source of randomness shall first be made a posteriori, in accordance with the real design of the source of randomness and then be validated by checking the expected statistical behaviour predicted by the model matches the one observed.

Added value of quantum physics

The very nature of quantum physics is random. When measuring a physical quantity of a quantum particle, such as for instance the spin of an electron[1] or the polarization of photon[2], the output takes indeed a discrete set of values, but the distribution is governed by probabilistic laws. So much so that it is possible to leverage on this core property of quantum physics to obtain pure randomness.

This new approach allows generating true random number whose very nature is provable as governed by the basic laws of quantum physics. Compared to the former approach, quantum physics brings here (1) a provable source of randomness and (2) a modelling of the source of randomness a priori.

It is a totally different approach from generating true random numbers based on physical phenomenon. While in the first approach, the modelling of the source of randomness is made a posteriori and results from the analysis of the physical phenomenon at stake, quantum random number generator results from proven quantum laws. As a matter of fact it brings both (1) a higher level of confidence in the source of randomness as it is provably random and (2) facilitation of its design.

Today's implementation of quantum random generator relies for instance on (1) the transmission of a photon upon a semitransparent mirror or (2) the decay event of a radioactive source.

Technology readiness

This technology is mature and there are several offers on the market of device generating quantum random number (QRNG). However it has not yet been accepted by the main markets requiring true random number, such as the financial market.

The benefits of quantum random number are not sufficient for the time being to allow this market to grow.

Quantum Key distribution

The promises of Quantum Key distribution

Quantum key distribution promises to (1) allow secure distribution or sharing of secret key between two parties, (2) in a manner ensuring confidentiality, integrity and authenticity of the key, (3) detection of interception, and (4) in an untrusted environment. Unlike protocols for key distribution relying on cryptography (such as Diffie Hellmann), quantum key distribution – in theory – allows distributing key without possessing a priori any secret.

Two different types of quantum key distribution methods shall be sorted out as their very nature is fundamentally different:

- **Regular quantum key distribution** methods where an entity sends to a receiver a secret key value;
- **Quantum key distribution based on quantum entanglement** where both entities get a secret key value from the same source;

1. Regular quantum key distribution:

Several modes of implementation have been proposed such as:

- BB84 (Bennett and Brassard - 1984) ;
- B92 (Bennett – 1992);
- SARG (V. Scarani, A. Acin, G. Ribordy, and N. Gisin - 2004);
- 4+2 protocols (B. Huttner, N. Imoto, N. Gisin, and T. Mor – 1995);
- 6 state protocols (D. Bruß & H. Bechmann-Pasquinucci and N. Gisin – 1998);

1 An electron is an elementary components of atoms. It gravitates around the centre made up with protons and neutrons.
2 The photon is the basic constituent of light.

The protocol BB84 is currently mostly used. Furthermore most implementations have been made using polarized photons sent within optical fibres or the air.

Underlying quantum physic principle

The security of this method mainly relies on one of the key principle of quantum physics. A quantum attribute remains undetermined and is in a superposition of quantum state until it is measured. Once a measurement is made, the quantum attribute takes a defined value and is not anymore in a superposition of state. This leads to an irreversible change of the state of the object (wave function collapse). It could be compared to a flower bud in the dark. When being exposed to the light, in order human eye to appraise it, each and any photon alter the surface and the color of the bud, so much so that what our eye do see is not the real flower bud. Furthermore, these photons irreversibly change the very nature of the flower bud as it causes color to fade. With quantum physics it is the same. Any attempt to measure an attribute causes an irreversible modification of its internal state.

Mode of operation

The method consists in transmitting a stream of bits to a receiver through an insecure channel, each bit being encoded over a quantum attribute of a quantum carrier called a qubit (quantum bit). Usually the qubit is the polarization state (|↑> or |→>) of a photon sent (1) within an optical fiber or (2) through the atmosphere.

The general principle is always the same. First, the sender encodes a stream of random bits as qubits using a randomly selected base (e.g. for photons carrier, a random polarization filter × or + is used before sending photons), and sends the qubits to the receiver. The receiver randomly chooses a base (e.g. for photons carrier, a random polarization filter × or +) to measure the qubit, converts it into bit value and records the result.

In a second step the key sifting is performed. Both the sender and receiver dialogue over a trusted channel to declare the bases they used (e.g. polarization filter × or + used to send/receive photons). They only keep the bits corresponding to the case when their bases were correlated (sender and receivers used the same bases for sending and receiving the same qubit), all the other bits are withdrawn.

In the case of (1) a perfect quantum channel (no alteration of the information by the transmission medium) and (2) without attacker intercepting the information, the remaining stream of bits shall be identical for both the sender and the receiver. However it is never the case at least because the quantum channel alter the transmission of information (loss of quantum particles, parasite...). Therefore it is necessary to measure the quantum bit error rate (QBER) reflecting indistinctly the effects of these two factors. In some way, this rate reflects the maximum amount of information an attacker may have intercepted during the key distribution. The receiver discloses to the sender a portion of the sifted key through a trusted channel so that it can assess the QBER. If this rate is too high (typically above 10%), the key distribution is halted and resumed as the risk an attacker intercepted substantial part of the information is too high.

If the QBER remains below a security threshold, both entities carry on the protocol. The bits that have been disclosed over the trusted channel to assess the QBER are withdrawn by both entities from the sifted key and a key distillation is performed. During this step the sifted key is processed by the receiver to correct the transmission errors. It allows reconstructing an error free sifted key thanks to error correcting code technology.

Next a privacy amplification is performed. It aims at reducing the impact of the information known to the attacker (previously estimated thanks to the QBER). It consists in compressing the stream of remaining bits obtained following key distillation to increase the entropy and decrease the rate of information in the hands of the attacker. The outcome of this step then can be used as a cryptographic key.

Finally a key confirmation stage takes place. Each entity (sender and receiver) confirms to the other entity that it has the right key. Each entity sends a proof of possession (data signed with the said key) to the other one. However it shall also be combined with a proof of authenticity of each stakeholder (sender and receiver) to avoid a man in the middle attack. This step is crucial so that each entity can identify and authenticate the other one claiming and proving the possession of the key, to avoid a man in the middle.

Security by design

The protection against interception of information follows from quantum physics properties. Should an attacker eavesdrops the information, the qubit carrying the information would be measured. It would lead to (1) either the disappearance of the quantum particle, or (2) the alteration of the qubit that will cause an increase of the quantum bits error rate (QBER).

The attacker could also try to copy the qubit before reading it while sending the other one to the receiver in an attempt not to be detected. Again quantum physics brings native security as it ensures it is not possible to clone a qubit. Cloning a qubit would imply to read the

value of the qubit and copy its quantum state to another quantum particle. But it is not possible as reading the value of the qubit means measuring the quantum state which leads to its irreversible modification and a loss of information (wave function collapse).

Here we see that quantum physics brings strong answer to many security concerns related to the secrecy of a plain text information sent in an untrusted environment.

Limitations

As surprising as this method may appear it has several limitations. First it still requires both entities (sender and receiver) to possess cryptographic keys to authenticate each other when completing the key distribution. Even though previously distributed key may be reused for this purpose, it does not prevent from setting up a key distribution mechanisms between both entities to manage the initiation of the protocol (first time) and also in case of recovery (previous key is erased).

Furthermore this protocol also requires a trusted channel to be available between the sender and receiver to transfer sensitive information such as the bases and a portion of sifted key used to evaluate the quantum bit error rate. Even though confidentiality is not required, integrity and authenticity are required. This channel may be (1) a dedicated secured link or (2) secured using classical cryptographic protocol relying on previously distributed key.

Current implementations of quantum key distribution mainly use polarization of photons to convey information through optical fibre or the air. However a photon can't be conveyed beyond 100 km within an optical fibre due to the glass absorption. It requires to set up repeaters at most every 100 kms to re-emit a photon holding the information. Unfortunately as of today the technology for quantum repeaters is not mature, therefore the information shall be repeated by converting it in the non-quantum domain and re-emit it in the quantum domain. Thus the sensitive information is handled unprotected into the repeater: each repeater becomes a weakest link.

When sending the photon throughout the air, such limitation does not apply as the absorption rate is much lower allowing more important transmission distance (>1000kms). However it also has drawbacks. The transmission shall take place during the night to avoid interferences from the sun's photons and take place far from artificial sources of light (cities). So far current implementations made use of reception stations located in mountains, limiting the absorption impact of atmosphere (lower density of the air) and pollution.

The security of these protocols assumes that each bit is encoded over one single qubit. However, this is not the case. On average a laser pulse contains 0,1 photon, most pulses don't contain any photon, 10% contain 1 photon and 1% of pulses contain more than one photon. Therefore there is a probability that several qubits are sent for a given bit, giving the ability to an attacker to read one corresponding qubit without being detected through the quantum bit error rate.

Technology readiness

Quantum key distribution has been used or is currently being used in several optical fiber networks in the world:

Switzerland	Quantum key distribution was used in 2007 to secure the transmission of the vote results to the governmental central data repository;
China	A national optical fiber network of more than 2000 kms between Shanghai and Beijing and also connecting the other surrounding towns has been deployed. It contains more than 32 repeaters distant of 70 km each. This network is secured thanks to quantum key distribution and is used for commercial and national communication;
Austria	In 2008, SECOQC (Secure Communication based on Quantum Cryptography) was the first computer network secured by quantum key distribution. It was launched in Vienna. This project was funded by EC.

2. Quantum key distribution based on quantum entanglement

The Ekert scheme (A. Ekert – 2001) is the main mode of implementation.

Underlying quantum physic principle

Here the bits of information are not distributed from one entity to another one using qubits but they are simultaneously obtained by the two entities (sender and receiver) from a qubit each of them own. Furthermore each qubit is made up with a quantum particle having its quantum state entangled with the other quantum particle's quantum state.

When two qubits are entangled, quantum states of each quantum particle are bound meaning that their values are linked : the quantum state of one quantum particle defines the quantum state of the second quantum particle. This property maintains even if the qubits are not physically located at the same place.

More precisely, any measurement made on a quantum state of a quantum particle (reading the value of a qubit) will determine the value of the quantum state of the other quantum particle (value of the other qubit). Let's consider a pair of entangled quantum states of quantum particles (qubits), one of them is given to A, and the second one to B. If A reads the value of its qubit and gets a, B will get ā with a probability of 100% when reading the value of its qubit. The outcome of the measure of the qubit of A remains governed by probalistic and may give different values (e.g. a or ā), but once the qubit value has been read (and thus measured) the value is fixed and consequently the value of the qubit of B also, having 100% of chance to be ā.

This property is called quantum entanglement. Two or more qubits (quantum particles holding entangled quantum state) may be entangled, and furthermore this property may be maintained even if the qubits are separated from thousands of km.

Mode of operation

Both entities shall both have a qubit, both qubits being entangled. Therefore it requires a previous step of creation of quantum particles having entangled state (qubits) and their distribution to each recipient.

Each entity (sender and receiver) measures the value of its qubit according to a base randomly chosen from two possible ones, each measurement giving a bit of information. This procedure is carried out until a sufficient amount of bits has been obtained. Each entity keeps its measurement base secret until all the stream of bits has been generated.

In a second step, both entities exchange their measurement bases through a trusted channel. When both entities used the same measurement base for the same bit of information, the bit is kept to form the sifted key. Statically the sifted key is around one third of the size of the input bit stream.

The output of the other measurements are used to compute a statistic indicator reflecting the correlation of measurements made by each entity when using non compatible bases. This statistic indicator is instrumental as it allows confirming to each entity that both qubits are entangled. When both qubits are entangled, the statistic indicator shall be above 2 (strictly).

As in previous quantum key distribution, the sifted key go through a key distillation. Even though both qubits are entangled, the values of sifted key obtained by each party may be different resulting from imperfections of the environment and measurements. A dialogue takes place between both entities over a trusted channel to (1) measure the quantum bit error rate (QBER) over the sifted key and (2) correct errors. This stage ends up with a corrected sifted key value which is the same for both entities.

Next a privacy amplification and key confirmation stages take place as in regular quantum key distribution protocol.

Security by design

The design of the protocol ensures protection against eavesdropping attempts. The verification of the statistic indicator ensures that both qubits used for the generation of the key are entangled together. It excludes any eavesdropper to have access to the source of information.

Limitations

This different flavor of quantum key distribution also has the same limitation as the regular one.

It still requires both entities to possess cryptographic keys used to authenticate each other when completing the key distribution and to set up a trusted channel to secure transmission of sensitive information in the course of the protocol (such as the bases, the information needed to compute the statistic indicator and correct the value of sifted key). This channel may be (1) a dedicated secured link or (2) secured using classical cryptographic protocol relying on previously distributed key.

The same limitations in optical fibre and through atmosphere also apply.

Furthermore it also requires (1) a source able to create quantum particles having entangled quantum states (entangled qubits), and (2) a way to distribute these quantum particles to the end entities. So far the best mode of implementation is to use entangled photons created thanks to a laser located in a satellite which are sent to ground station on Earth.

Technology readiness

This method of quantum key distribution has been achieved in June 2017. The chinese satellite MICIUS generated entangled photons and sent pairs of entangled photon to ground stations on Earth : one in Austria (Graz) and one in China. These entangled photons were used to

generate secret keys to encrypt a video conference of 75 minutes between both countries.

Quantum Key distribution and classical cryptography

As of today, it seems not possible to implement a quantum key distribution protocol without classical cryptography. Classical cryptography remains necessary so that each entity can authenticate each other at the end of the key distribution. It is also of great interest to establish and communicate sensitive information (bases…) through the trusted channel. Therefore quantum key distribution should not be seen as an alternative to classical cryptography but rather as being complimentary.

Quantum safe cryptography

The promises of Quantum computer

While classical computer handles bits that can only take one value amongst two ('0' or '1'), the quantum computer would handle qubits that can take two values at the same time (|0> and |1>) thanks to the property of quantum superposition. Here lies the main difference.

With a classical computer using a register of n bits it is only possible to store one value amongst 2n at the time. With a quantum computer using a register of n qubits, it is possible to encode up to 2n values at the same time. It is a total shift of paradigm. While a classical computer can only handle a single value stored in its register in one operation, the promise of the quantum computer is to handle 2n values stored within qubits in its register in one operation. This is the concept of quantum parallelism, which allow paralleling basic operations on data.

Roughly, it means that a quantum operation would allow in one operation making what takes 2n operations with a classical computer. In the same way as the classical computer uses logical gates performing basic operations on bits such AND and XOR, it requires to design quantum gates allowing performing basic operations on qubits.

The challenge to design a real quantum computer (or calculator) is threefold. It shall be possible to create and maintain qubits in a register for a time long enough to allow the computation to be made, to design quantum gates and make them handle the qubits.

Despite communications made by companies, it is not even sure if the quantum computer will ever exist. If it is to ever exist, it is not expected before the next 20 years.

Which consequences on classical cryptography?

Asymmetric cryptography - unlike symmetric cryptography - does not use the same key when transforming a message on one way and the other way around. It brings considerable benefits as it allows sorting out entities allowed to transform information in one way from the ones allowed to invert the transformation. Namely users having the right key – called private key – can perform the private operations over data (such as computing signature or decrypting) while the ones having the other key – called the public key – can perform public operations (such as signature verification or encryption). Each key only give access to one type of operation. In particular the public key (1) does not allow to perform sensitive operations, and (2) does not allow to retrieve the private key. Thus public key can't be used by their holder for forgery purposes.

Asymmetric cryptography allowed new use cases to appear : (1) authentication where only the holder of the private key can authenticate itself by generating an authentication token that anyone having the public key can verify or (2) digital signature where only the holder of the private key can materialize its consent by creating a digital signature that anyone can verify using the corresponding public key.

Asymmetric cryptography is a cornerstone of (1) the PKI and authentication protocol over the Internet, and (2) intrinsic to digital signature concept which are instrumental for IT security.

Indeed the private and public key are bound as what has been created with a given private key can only be inverted with the corresponding public key. As the public key contains all the information about the private key value, it implies that theoretically it is possible to revert back to the private key from the public key. Even though it is theoretically possible, asymmetric algorithms are designed in such a way that it is not achievable within a timeframe commensurate with human life. They are design so that reverting back to the private key from the public key relies on a so called "hard mathematical problem", namely a problem whose computational complexity can't be handled by today's and tomorrow's computational power and would take decades to be solved.

Today's asymmetric algorithms rely on two types of hard mathematical problem: (1) factorization in prime factors of a large number for RSA, and (2) computation of discrete logarithm for cryptography over elliptic curves, DSA and DH.

These mathematical problems have been studied for decades and are well known. In particular the optimal algorithms solving these problems have been identified and analyzed. It allows estimating the cost and time needed for solving any of these mathematical problems on today's computer and thus size the key length of an asymmetric algorithm to ensure security over a defined timeframe.

Should a quantum computer ever exist, other types of optimal algorithms for solving these problems would become possible, algorithms that can't be executed on today's computer but that would be possible on a quantum computer. Shor algorithm is currently the best solving algorithm known. As everything related to quantum physics, it only provides the solution with a high probability. However, the probability of failure may be decreased by executing it several times.

Shor algorithm (executed on a quantum computer) would be much more efficient than the most efficient algorithm that could be executed on classical computer. While the latter has a complexity of O((log N)3) – in time - and O(log N)) – in memory when factorizing a number N, the classical algorithm has a larger complexity which is exponential with N.

Should Shor algorithm ever be implemented, the hypothesis on which today's asymmetric algorithms (including RSA and elliptic curve cryptography) security is based would collapse. A public key could be inverted in a very short time to get the private key, ruining the security of PKI (that heavily relies on asymmetric cryptography) and thus annihilate all IT security. However, this risk only applies to asymmetric algorithms, symmetric algorithms (such as AES) and hashing function are not impacted.

The horizon when a quantum computer able to break today's and tomorrow's asymmetric algorithms will be available may seem to be far away (20 years). However the deployment and widespread use of applications of classical asymmetric algorithms – such as PKI – took more than 20 years. Therefore, considering the inertness required to introduce asymmetric algorithms, it is urgent to anticipate as of today such risk in order to design a new family of asymmetric algorithms whose strength will not be affected by a quantum computer. It requires to build asymmetric algorithms on a new hard mathematical problem that can't be easily solved by quantum computer.

Designing a new generation of asymmetric algorithms

Candidates for new generation of mathematical problems are already known for many years : (1) Lattice based, (2) multivariate, (3) hash based, (4) code based, and (5) supersingular elliptic curve isogeny based. These new types of mathematical problems define new generation of asymmetric algorithms. Those are named quantum safe cryptography (QSC) as it is designed to be resistant to the quantum computer capacity (quantum safe).

Technology readiness

Currently there are no post quantum asymmetric algorithm that are recognized by the community and the national security agencies as secure.

The research community throughout the world is deeply working on defining, assessing and reviewing post quantum asymmetric algorithms to identify the best one(s). In order to foster the emergence of secure and optimal post quantum asymmetric algorithms, NIST in the US has launched at the beginning of 2017 an international contest aiming at standardizing post quantum asymmetric algorithms with a deadline fur submission of proposals in Nov. 2017. This context will ensure each candidate algorithms is reviewed by peers to assess its quality and security.

For the time being, no deadline for the completion of this contest has been communicated by NIST.

In Jul. 2018 China has launched a PQC competition silimar to NIST, with a deadline in Feb. 2019.

Several national IT security agencies consider quantum safe algorithms are not mature enough to envision using them. They consider that at least five years of hindsight are required before considering them as trustable and starting using them to replace classical asymmetric algorithms.

Outlook

It is expected that the future "quantum world" will probably have more cryptographic standards, different schems for encryption, signatures and key exchange and longer keys, signatures and ciphertext. These are major challangers for the security world, that we have today for the smart card market as well well as for the embedded security market. Smart cards have typical lifetime between 3 years (e.g. Banking Cards) and 15 years (e.g. electronic Driving License Cards), in the embedded world the lifetime can cross the 20 years line, for example in industrial internet area, were we have cyberphysical production systems (CPPS) in use. This means CPPS, which would be sold today would be used were the quantum world would be started.

Glossary

EC	European Commission
NIST	National Institute for Standardization and Technology
PKI	Public Key Infrastructure
PQC	Post Quantum Cryptography
QBER	Quantum Bit Error Rate

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

EUROSMART members are companies (**BCA**, **Fingerprint Cards**, **Gemalto**, **Giesecke+Devrient**, **GS TAG**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Internet of Trust**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **STMicroelectronics**, **Toshiba**, **Trusted Objects**, **WISekey**, **Winbond**), testing, inspection and certification (TIC) companies (**SGS**), laboratories (**CEA-LETI**, **Keolabs**, **SERMA**), research organisations (**Fraunhofer AISEC**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **Mobismart**, **Danish Biometrics**).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART

The Voice of the Digital Security Industry

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 35 | www.eurosmart.com