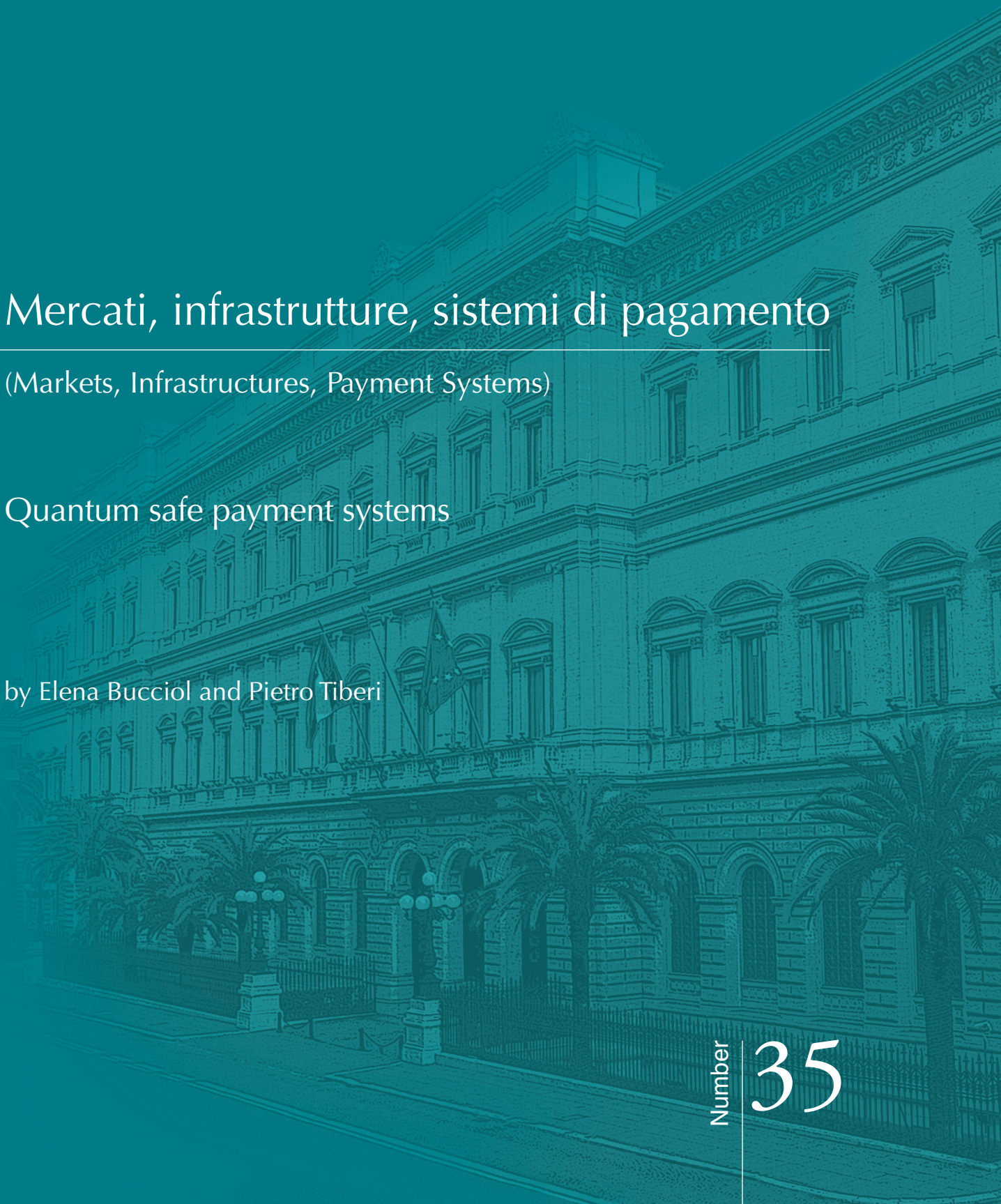
BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

Quantum safe payment systems

by Elena Bucciol and Pietro Tiberi



June 2023

Number 35

BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento
(Markets, Infrastructures, Payment Systems)

Quantum safe payment systems

by Elena Bucciol and Pietro Tiberi

Number 35 – June 2023

The papers published in the 'Markets, Infrastructures, Payment Systems' series provide information and analysis on aspects regarding the institutional duties of the Bank of Italy in relation to the monitoring of financial markets and payment systems and the development and management of the corresponding infrastructures in order to foster a better understanding of these issues and stimulate discussion among institutions, economic actors and citizens.

The views expressed in the papers are those of the authors and do not necessarily reflect those of the Bank of Italy.

The series is available online at www.bancaditalia.it.

Printed copies can be requested from the Paolo Baffi Library: richieste.pubblicazioni@bancaditalia.it.

ISSN 2724-6418 (online)
ISSN 2724-640X (print)

Banca d'Italia
Via Nazionale, 91 - 00184 Rome - Italy
+39 06 47921

Designed and printing by the Printing and Publishing Division of the Bank of Italy

Quantum safe payment systems

by Elena Bucciol* and Pietro Tiberi*

Abstract

European payment system infrastructures such as T2, T2 Securities and TIPS rely on advanced cryptographic systems for a significant part of their security. In the near future, advances in quantum technologies and algorithms could make today's security systems vulnerable. Quantum technologies, however, can also be used to devise cryptographic schemes that are able to achieve unconditional security and are therefore resistant to attacks by adversaries with unlimited processing capabilities.

Random number sequence generation and protocols for the secure exchange of cryptographic keys between two parties are the pillars of any cryptographic system. In this paper, which takes European payment systems as a point of reference, we analyze some of the solutions currently available for quantum random number generation (QRNG) and quantum key distribution (QKD) infrastructures.

Making payment systems quantum-safe also requires the development of applications so as to make it quick and easy to replace potentially compromised cryptographic algorithms.

Keywords: Quantum computing, Quantum security, QKD, QRNG, Target Services.

Sintesi

Le infrastrutture del sistema dei pagamenti europeo come T2, T2 Securities e TIPS affidano una parte importante della loro sicurezza all'utilizzo di sistemi crittografici evoluti. Nel prossimo futuro, gli sviluppi delle tecnologie quantistiche e la conseguente invenzione di nuovi algoritmi quantistici potrebbero mettere a rischio la sicurezza dei sistemi di sicurezza oggi in uso. Le tecnologie quantistiche, tuttavia, possono essere anche utilizzate per mettere a punto schemi crittografici in grado di raggiungere un livello di sicurezza incondizionata e pertanto resistenti ad attacchi portati da avversari dotati di capacità elaborative illimitate.

La generazione di sequenze di numeri casuali e i protocolli di scambio sicuro delle chiavi crittografiche tra due soggetti sono due pilastri di qualsiasi sistema crittografico. In questo lavoro, prendendo come riferimento i sistemi di pagamento europei, si analizzano alcune delle soluzioni attualmente disponibili per la realizzazione di sistemi di generazione di numeri casuali quantistici (QRNG) e per la realizzazione di infrastrutture di distribuzione quantistica delle chiavi (QKD).

Per rendere i sistemi di pagamento *quantum safe* è inoltre necessario sviluppare applicazioni che rendano semplice e veloce la sostituzione di algoritmi crittografici eventualmente compromessi.

* Bank of Italy, IT Operations Directorate.

CONTENTS

1 Introduction

The security of payment systems and, on the whole, of every ICT infrastructure, relies heavily on cryptographic systems. The business continuity model adopted by the Eurosystem,[1] with reference to all the settlement systems managed, is based on the replication of data across multiple datacentres, whose integrity and confidentiality (i.e. data in transit) is guaranteed by appropriate encryption systems. Encryption protects communications between processing systems even within the same datacentre, and the sensitive data stored into the individual systems are encrypted as well. These safeguards are implemented by taking advantage of the best cryptographic systems available on the market.

The cryptographic schemes currently used are based on two building blocks: the generation of random sequences of bits with maximum entropy (Wang, Pan and Wu 2019) and the existence of mathematical problems that are intractable,[2] such as prime number factorization[3] and the discrete logarithm problem.[4] These are the basis of all systems of authentication, authorization, digital signature, and distribution of encryption keys.

The development of quantum computing was one of the major scientific revolutions of the last century; however, for decades, the ability to control quantum systems as desired was limited, thus restricting the class of technological applications that can be envisioned. In recent years, something unexpected happened (Dowling and Milburn 2003) that has made the control of quantum systems advance considerably; further progress appears very plausible in the near future due to increased interest and investments and scientific breakthroughs. Moreover, many countries around the globe have launched national quantum technologies programmes (Wallden and Kashefi 2019).

In 1982, the physicist Richard Feynman theorized the possibility of building a computer based on the laws of quantum physics (Feynman 1982); however, it is only thanks to the recent technological and engineering developments, that an actual quantum computer could be built, which, in some fields and applications, has proven to be better than traditional computers (Google 2018). Moreover, the special algorithms designed to run on a quantum computer (Shor 1994) (Grover 1996) are in the offing to exploit quantum computation and attack the current cryptographic schemes still based on computational complexity.

According to the National Institute of Standards and Technology (NIST)[5] (L. Chen *et al.* 2016), the main cryptographic algorithms based on asymmetric keys are vulnerable to quantum computing based attacks. In particular, a recent study has shown that it is possible to derive the prime factors of a 2048-bit RSA[6] key in about 8 hours using 20 million noisy qubits (Gidney and Ekerå 2021).

Quantum technologies, if seen from the point of view of malicious users, can be considered a

1. Trans-European Automated Real-Time Gross Settlement Express Transfer System (T2) (Bramini *et al.* 2021), Target Instant Payment System (TIPS) (Renzetti *et al.* 2021) and Target2 Securities (T2S) (Mastropasqua *et al.* 2021).

2. A problem that could be solved in theory (e.g. given large but finite resources, especially time), but for which, in practice, any solution takes too many resources to be feasible, is known as an intractable problem.

3. In number theory, integer factorization is the decomposition of a composite number into a product of smaller integers. If these factors are further restricted to prime numbers, the process is called prime factorization. In terms of computational complexity, the problem is clearly in class NP, but it is generally suspected that it is not NP-complete, though this has not been proven (Buhler, Lenstra and Pomerance 1993).

4. In mathematics, for given real numbers a and b, the logarithm $\log_b a$ is a number x such that $b^x = a$. Analogously, in any group G, powers b^k can be defined for all integers k, and the discrete logarithm $\log_b a$ is an integer k such that $b^k = a$. Discrete logarithms are quickly computable in a few special cases. However, no efficient method is known for computing them in general. A number of important algorithms in public-key cryptography base their security on the assumption that the discrete logarithm problem over carefully chosen groups has no efficient solution (McKurley 1990).

5. The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is very active in the field of cyber security and is the promoter of the NIST Cybersecurity Framework which provides guidance on how both internal and external stakeholders of organizations can manage and reduce cybersecurity risk.

6. In cryptography, the acronym RSA indicates an asymmetric encryption algorithm, invented in 1977 by Ronald Rivest, Adi Shamir, and Leonard Adleman, which can be used to encrypt or sign information. The encryption system is based on the existence of two distinct keys, used to encrypt and decrypt. If the first key is used for encryption, the second must necessarily be used for decryption and vice versa.

risk for ICT security, but they can actually provide many advantages if used for honest purposes. In fact, they can be adopted to improve some existing protocols.

The best known example is Quantum Key Distribution (QKD) (Xu *et al.* 2020) (Lo, Curty and Tamaki 2014) (Diamanti *et al.* 2016).

In QKD, it is possible to establish a shared secret key, with information-theoretic security, between two spatially separated entities, using untrusted quantum channels. This could not be achieved by relying only on classical communication without pre-shared keys.[7] Importantly, having a protocol with information-theoretic security means that security is not based on any computational assumptions and the information will remain secure even if the attacker uses a quantum computer (Wallden and Kashefi 2019).

Devices based on the laws of quantum mechanics play a substantial role also in the field of random number generation: a quantum random generator (QRNG) can obtain random sequences of bits with uniform distribution at maximum entropy, thus making it possible to overcome the security performances (Markowsky 2014) of current random number generators (PRNG[8] and TRNG[9]).

With the advent of quantum computers, there is an imminent need to incorporate quantum tools into current computer systems to strengthen their security and expedite the replacement of cryptographic mechanisms that are vulnerable to newly developed quantum algorithms.

This is a general concern for any type of vulnerability of cryptographic algorithms and not only for those deriving from quantum computation (Horvath and Mahdi 2017). All computer systems should therefore be designed to ensure so-called crypto-agility (Sullivan 2009). Crypto-agility, or cryptographic agility, is the ability of an information security system to adopt an alternative to the original encryption method or cryptographic primitive without significant changes in system infrastructure.

In this paper, we will describe how, by using quantum tools such as QRNG and QKD and by achieving crypto-agility, the current European payment system infrastructures can be improved and made more resistant to cyberattacks carried out by enemies who can exploit the computational capabilities offered by quantum computers.

2 Methods

2.1 Quantum random number generators

The use of random bit sequences is essential in cryptography. Their best-known use is the One-time pad, which is a key that can be used only once. For example: Alice and Bob share a secret key k, a long binary string whose bits are selected uniformly and independently. When Alice wants to send a message m to Bob, she sends the ciphertext $c = m \oplus k$, where $\oplus$ is the bitwise exclusive OR operator. On receiving c, Bob computes $m = c \oplus k$ by applying the bitwise exclusive OR operator to both the ciphertext and the key. This simple cryptographic scheme has the property of perfect secrecy as long as you use perfectly random bitstrings for the key k and do not reuse the same encryption key several times (Shannon 1949).

This example describes the most important use of randomness in cryptography: the generation of keys; the secret piece of information that allows legitimate keyholders to communicate securely.

If the cipher selects the key uniformly at random, then a brute-force attack[10] will take 2^N steps

7. Indeed, with pre-shared keys (PSKs) information-theoretic security can be achieved by paying the logistic cost of shipping key material around.

8. A Pseudo Random Number Generator (PRNG) is an algorithm that takes as input a random sequence of length k (seed) and generates an output sequence with a lenght of $l >> k$ and that appears random.

9. A True Random Number Generator (TRNG) is a device that generates random numbers from a physical process, rather than using an algorithm. Such devices are often based on microscopic phenomena that generate low-level, statistically random 'noise' signals, such as thermal noise.

10. In cryptography, an attack that involves trying all possible combinations to find a match (see https://csrc.nist.gov/

to guess the key, where N is the key's length. In the case of AES-128,[11] this will take 2^{128} attempts which is way beyond the ability of the fastest known computer. But, again, the assumption that the key is random, plays a fundamental role in limiting the cost of a brute-force attack. Adversaries can discover a non-random key much faster if they know that the key's bits are biased towards zero; they will not bother testing keys containing a lot of ones (Gennaro 2006).

Another important use of randomness is the generation of unique values, or nonces. Unique strings are important in cryptographic protocols to prevent replay attacks (Singh and Misra 2012), in which an adversary tries to reuse correct values from previous executions of the protocol, hoping that they will appear correct in the current attempt. Randomness is the easiest way to create nonces.

To generate truly random sequences of bits, a truly random process is needed. The canonical example of a random process is the tossing of a coin where there is equal probability (50/50) that the coin will land with either side up. Repeated coin tosses are independent, meaning that the outcome of one toss does not affect the outcome of the others. If we associate the bit 0 with the event that the coin lands on heads, then by repeatedly flipping a coin N times, we obtain a uniformly distributed N-bit string: each possible string has the same probability of being produced (2^{-N}).

The probability that a secret is guessed correctly on the first attempt is related to the entropy sources. Entropy is defined in relation to one's knowledge of an experiment's output before observation and reflects the uncertainty associated with predicting its value – the larger the amount of entropy, the lower the probability in predicting the value of an observation. There are many possible measures for entropy; according, to NIST (Turan *et al.* 2018) we use a very conservative measure known as min-entropy, which measures the effectiveness of the strategy used to guess the most likely output of the entropy source.

Entropy definition

The min-entropy (S) of an independent discrete random variable X that takes values from the set $A = \{x_1, x_2, ..., x_k\}$ with probability $Pr(X = x_i) = p_i$ for $i = 1, \ldots, k$ is defined as

$$S = \min_{1 \le i \le k} \left(-\log_2(p_i) \right) = -\log_2 \left(\max_{1 \le i \le k} (p_i) \right) \tag{1}$$

If X has min-entropy S, then the probability of observing any particular value for X is no greater than 2^{-S}.

The maximum possible value for the min-entropy of a random variable with N distinct values is $-\log_2 2^{-N} = N$, which is attained when the random variable has a uniform probability distribution as in the coin toss example.

The entropy source is one of the main components of modern TRNGs (True Random Number Generators), which are the basis of many modern cryptographic systems. The true random number generation method generates random bits from a physical phenomenon that is expected to be random and then compensates for possible biases and correlations existing between the bits by post-processing mechanism. The physical phenomenon includes measuring atmospheric noise, thermal noise, and other external electromagnetic phenomena (Sreekumar and Ramesh 2016).

The basic blocks of a TRNG include:

- **Entropy source (ES)**: includes thermal noise, clock jitter, metastability, and chaos. One of the concerns of the analogue source is it should be independent of external disturbances, which may

glossary).

11. AES (Advanced Encryption Standard) is a powerful encryption algorithm selected by the U.S. government to safeguard classified information. AES uses different key lengths (128, 192, and 256 bit) to encode and decode data in a block-by-block manner.

adversely affect the reliability of the randomness generation. Therefore, the selection of random source has a great importance in the amount of randomness.

- **The post-processing section (PP)**: is used to improve the quality of TRNG. This is for balancing the bias between the bits '1' and '0'. Bias removal usually involves bit compression techniques. So this additional post-processing stage reduces the amount of available output bits obtained from the entropy source. The simplest solution for bias reduction is the use of a subsequent XOR corrector.

The cryptographic system guarantees its security only under the assumption that a sufficient amount of entropy is available from a RNG to generate its cryptographic keys. Nowadays, security standards such as the NIST SP 800-90B (Turan *et al.* 2018) or the German BSI's[12] stringent AIS31 test standard (Killmann and Schindler 2011), emphasize the importance of the quality of ES. To obtain a certification, vendors must provide not only statistical tests, but also a theoretical background and stochastic modelling providing the quality and reliability of the ES.

TRNGs with a weak ES rely heavily on strong post-processing, usually through a hash-based Deterministic Random Bit Generator,[13] which will remove the effect of imperfections in the physical ES but, in some cases, may merely hide a flaw (inherent vulnerability). Therefore, entropy analysis always requires direct access to raw entropy data, rather than to post-processing data. Unfortunately, users cannot access the entropy data of TRNG: there is often no way for users to detect a failure of attacks on the ES of a TRNG.

The laws of quantum physics can help to overcome the limitations of current entropy sources used in TRNGs. Quantum physics is the sole theory that contains intrinsic randomness (Bronner *et al.* 2009). Contrary to classical physics, quantum physics does not predict what will happen when individual measurements are performed, it only determines the probabilities for all possible measurement outcomes.

12. BSI as the Federal Cyber Security Authority shapes information security in digitalization through prevention, detection, and response for government, business, and society.

13. A DRBG is an algorithm that produces a sequence of bits that are uniquely determined from an initial value called a seed. The output of the DRBG appears to be random, i.e., the output is statistically indistinguishable from random values. A cryptographic DRBG has the additional property that the output is unpredictable, given that the seed is not known. Hash-based DRBG makes use of crypto hash functions like SHA-256.

Quantum randomness

Quantum randomness occurs in the measurement of a physical state[a] $|\Psi\rangle$ which is in a quantum superposition[b] of basis states:

$$|\psi\rangle = \sum_{i=1}^{z} a_i |x_i\rangle \tag{2}$$

The coefficients a_i, z being the number of basis vectors, are the probability amplitudes of measuring the system along the i-base and $\sum_{i=1}^{z} |a_i|^2 = 1$. The elementary quantum superposition state is a linear superposition of two single states ($z = 2$):

$$|\psi\rangle = a_1 |x_1\rangle + a_2 |x_2\rangle \tag{3}$$

A quantum superposition of a two-state system is called a quantum bit (*qubit*) (Schumacher 1995). In contrast to a classical bit, a qubit can be found not only in one of the two basis states but also in a superposition of both. Measurements of qubits yield a projection on one basis state with the probability given by the coefficients. In physical experiments, qubits can be realized easily, e.g. using photons. Using a single-photon source, it is possible to emit single particles and let them propagate towards a semi-transparent mirror with a $1/2$ probability to be transmitted or reflected (Figure 1). A photonic qubit arises from a distinguishable path by transmission T or reflection R:

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|T\rangle + |R\rangle) \tag{4}$$

For a random number generator, the basis states of the qubit are associated with the binary values 0 and 1, respectively.

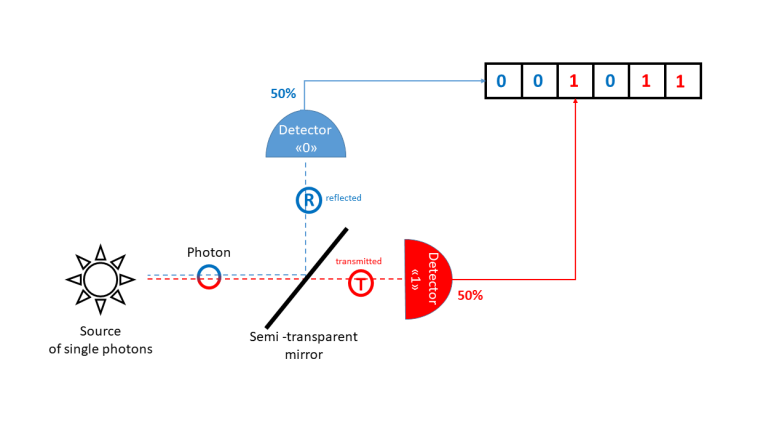


Figure 1. Basic diagram of an Optical QRNG based on single photon detectors after a beam-splitter (semi-transparent mirror)

a. The 'state' of a system (or particle) is a complete description of its current behaviour (e.g. where it is, how fast it is moving, etc.). Usually the Ψ state is denoted by $|\Psi\rangle$ using the bra-ket notation introduced by P.A.M. Dirac (Dirac 1939) to simplify the complex calculations required when combining different quantum states together. From a purely mathematical point of view, *ket* $|\Psi\rangle$ can be considered a column vector while the corresponding *bra* $\langle\Psi|$ is a row vector whose components are the complex conjugates of the ket

b. Quantum superposition is a fundamental principle of quantum mechanics. It states that, much like waves in classical physics, any two (or more) quantum states can be added together ('superposed') and the result will be another valid quantum state. Mathematically, it refers to a property of solutions to the Schrödinger equation; since the Schrödinger equation is linear, any linear combination of solutions will also be a solution.

The first quantum random number generator used the superposition (see the box 'Quantum randomness') of a single photon state on a beam splitter and was demonstrated in 2000 (Jennewein *et al.* 2000) and 2004 (Hai-Qiang *et al.* 2004).

Although sufficient for a proof-of-concept, the limitations of this approach were immediately evident. The bit-generation rate was limited by the dead time[14] of the detectors and the bit-bias was influenced by both the beam splitter transmission ratio and the varying detection efficiencies. When published as a standalone system in Jennewein *et al.* 2000, bit-generation rates of 1 Mbit/s were shown, and commercial products were able to achieve $\simeq$ 10 Mbit/s. However, as long as the random 'choice' remains binary, only one bit per photon can be generated at most (Wayne 2017). Recently, popular QRNG realizations have been based mainly on photon-counting detection (Hadfield 2009), and phase or vacuum fluctuations due to their higher speed, which can reach even a few Gb/s (Xu *et al.* 2012).

Although entropy sources based on photon counting or phase fluctuations are faster, they suffer from a bias linked to photon production or fluctuations statistics that are not uniform,[15] as is the case of single-photon detectors.

In order to compensate for these effects and for the inevitable disturbances linked to classical noise, thus generating a random sequence that can pass the security tests, a post-processing (PP) action must be performed on the raw data generated by the ES.

Therefore, to extract perfect-random bits and improve the randomness quality of raw data, a randomness extractor is implemented in the PP stage. Roughly speaking, a randomness extractor is a function as:

$$\{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m \tag{5}$$

which means that for a raw and non-perfect-random sequence X on $\{0,1\}^n$ with min-entropy $S(X) \geq m$, the extracted output sequence Y is a nearly uniform distribution on $\{0,1\}^m$. In other words, a randomness extractor takes a small random seed (d bits) and a raw random source (n bits) and outputs a near-perfect-random bit-string (m bits). Similarly to the TRNGs, the hash-based DRBGs using SHA-256 are the most used random extractors in the PP stage.

So far, we have described the functioning of a single quantum random number. Following, we will illustrate how to improve cyber resilience by including these objects in an ICT infrastructure. At the time of writing, there are multiple commercial QRNG solutions available on the market: from single quantum chips to expansion cards (USB or PCI-E) to be installed in a server, up to standalone systems to be installed inside datacentre racks.

14. For detection systems that record discrete events, such as particle and nuclear detectors, the dead time is the time after each event during which the system is not able to record another event (Lucke 1976). An everyday life example of this is what happens when someone takes a photo using a flash - another picture cannot be taken immediately afterwards because the flash needs a few seconds to recharge.

15. In a photon counting ES, the detected photons follow a Poisson statistics: $P(k \text{ events in the interval } t) = \frac{(rt)^k e^{-rt}}{k!}$ where r is the number of events per unit of time. In phase or vacuum fluctuating ES, the events follow a normal statistic distribution.

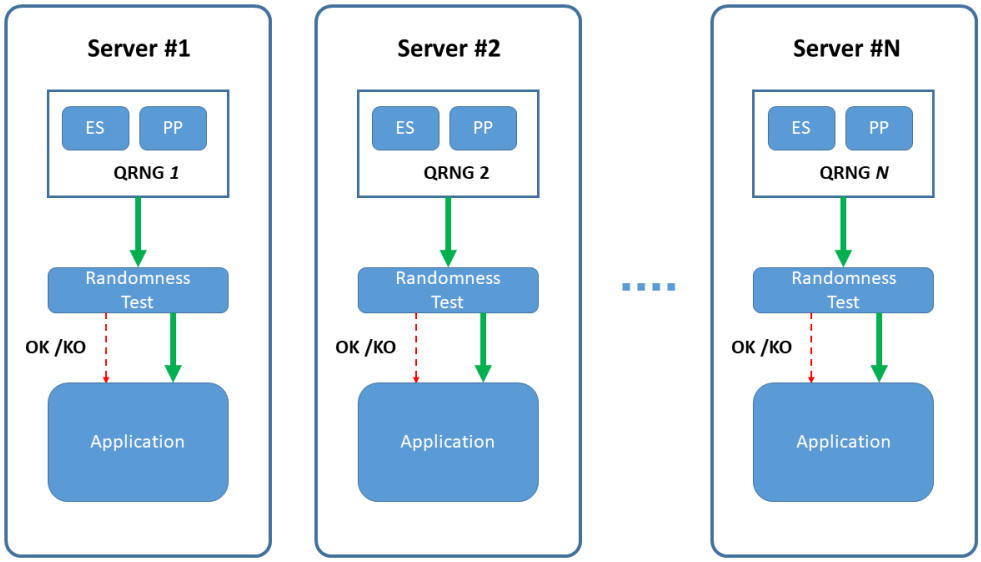


Figure 2. One QRNG per Server. Solid green lines are for the real random bitflow while dashed red lines are for quality control signalling (i.e. min entropy value of the stream)

The simplest solution to integrate the QRNG capabilities within the ICT infrastructure could be to insert QRNG expansion cards in each of the servers that need to use cryptographically secure random bit sequences. This approach, shown in Figure 2, has some drawbacks:

- huge number of servers using crypto functions, the amount of the new objects to be managed (i.e. QRNG cards) would increase the complexity of the overall ICT infrastructure;
- not very reliable, a single QRNG card failure would make the server unavailable;
- in order to receive the random data stream and monitor its quality in terms of minimum acceptance entropy (i.e. NIST SP800-22 and BSI AIS31 standard) each application must interface with specific card APIs.

A centralized service for the generation of random numbers can be a viable alternative, as it can satisfy all the requests of the various servers that use random sequences of bits to provide their cryptographic services (Figure 3). This approach, suggested by Huang *et al.* 2021, can be used even within the Eurosystem infrastructure.

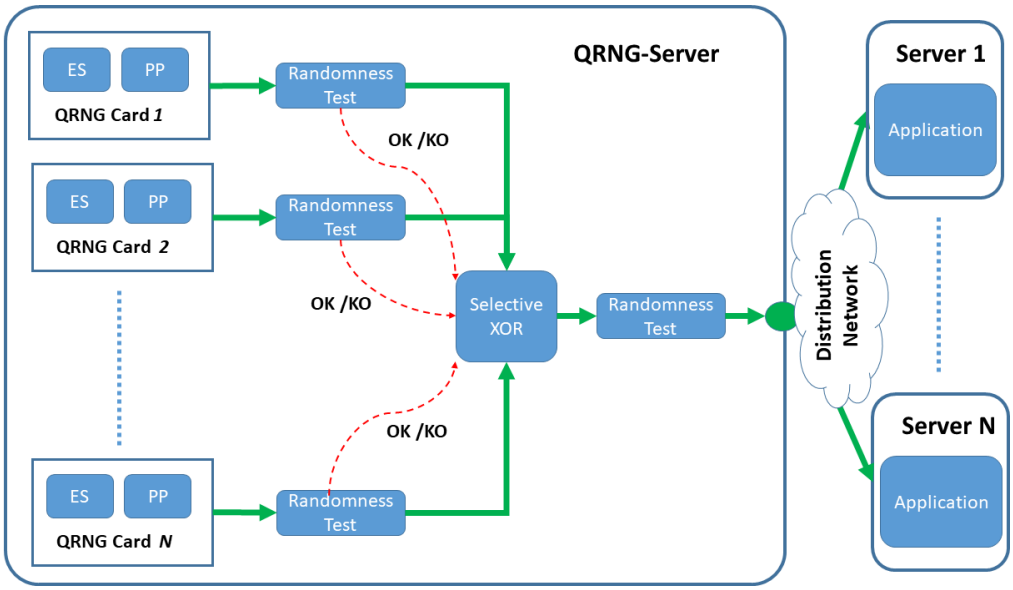


Figure 3. Basic block diagram of a single centralized Quantum Random Number Generation server (QRNG-Server)

The main component of the centralized random number generation system is the QRNG server. It reliably generates random sequences of bits and makes them available to cryptographic servers through a secure distribution network.

The QRNG Server contains multiple hardware cards dedicated to the random number generation (QRNG Card). Every single random bit stream generated by the QRNG cards, which can be modelled as a random variable $X_i(n)$, is subjected to a randomness test according to NIST SP800-22 and AIS31 standards. All the random flows $X_i(n)$ and the corresponding results of the randomness tests ($T[X_i(n)] = OK$ or KO) are then sent to a single central component called 'Selective XOR' to perform the following action:

$$Y(n) = X_1(n) \oplus X_2(n) \oplus \ldots \oplus X_M(n) \tag{6}$$

which combines the single $X_i(n)$ streams into a single random stream $Y(n)$ using simple bitwise XOR[16] operations ($\bigoplus$). In (6) only the M random streams $X_i(n)$ that are available and that have passed the randomness test (i.e. $T_i[X_i(n)] = OK$) are used. Using the Selective XOR function has the following advantages:

- the operation of XOR on a set of independent variables $X_i(n)$ considerably increases the minimum entropy S of the output sequence $Y(n)$ as defined in (1) (Jessa 2015);
- it increases overall resilience, as at least one QRNG source out of N must be available to output $Y(n)$;
- it increases overall security, as only sequences $X_i(n)$ that have passed the randomness test are selected as part of the output $Y(n)$.

To certify the quality of the data, a final randomness test is performed out on $Y(n)$ before delivering it to the requesting servers.

An important aspect of the overall security of the system is ensuring that the certified random sequence reaches the target servers without any alteration. For this reason, the Delivery Network

16. The XOR operator is a logical operator (boolean operator) of exclusive disjunction between two logical propositions. Given two logical propositions A and B, the exclusive disjunction between the two propositions is true only if one of the two propositions is true.

must guarantee the encryption of its transmission through secure and quantum-safe encryption technologies,[17] such as symmetric AES encryption by means of encryption keys of suitable length (ETSI 2017). The encryption keys can be pre-shared with the servers (Huang *et al.* 2021), but it would be advisable for this distribution to take place dynamically and securely through a Delivery Network based on quantum key distribution (QKD).

The main assets of the Eurosystem infrastructure are T2 (Bramini *et al.* 2021), T2S (Mastropasqua *et al.* 2021), and TIPS (Renzetti *et al.* 2021) (Arcese, Di Giulio and Lasorella 2021). These systems are deployed over different datacentres across multiple geographic regions. The centralized system for managing random numbers, such as the one described above, appears quite simple to implement: being the shared-nothing system, only a limited number of QRNG servers must be deployed in each of the datacentres that host the payment services, with no need for complex geographic data replication architectures (see Figure 4).

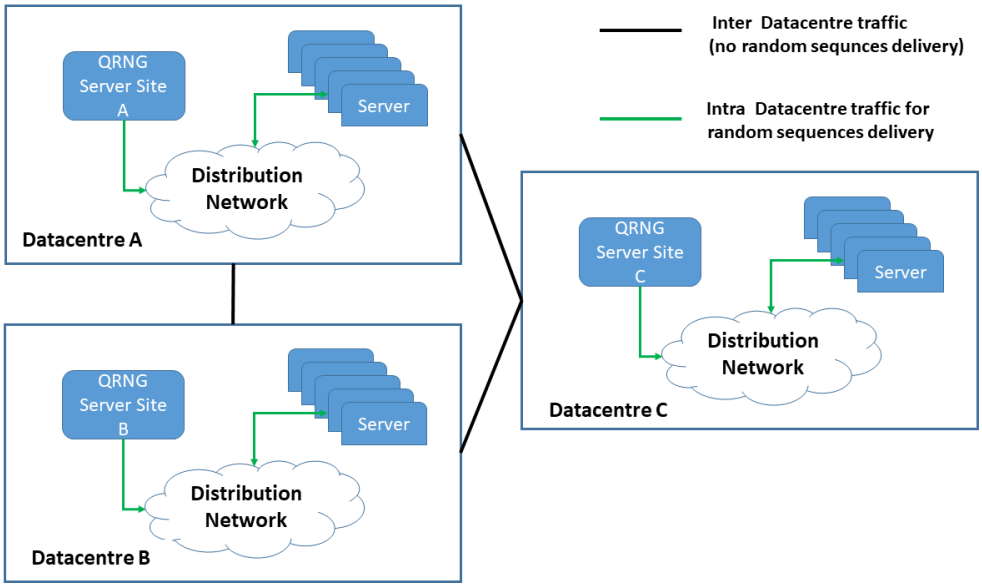


Figure 4. Example of QRNG server-based centralized service on a 3-datacentre footprint. A single QRNG server will be used inside each datacentre without inter-datacentre communications of random sequences

The main parameter to consider in the sizing of the QRNG server is the number of encryption keys generated per second. The encryption keys are mainly used to protect user connections and connections among servers using TLS protocol.[18] Considering the average number of users connected to the Target Services[19] and the number of servers that use TLS, the estimated number of keys per second is about 1,000, with 256 being the average length of the single key. This is only a rough estimate, as demand for encryption keys is constantly on the rise. For this reason, a rule of thumb is to double the capacity considered at the beginning of the process.

The QRNGs available on the market already far exceed these requirements and are constantly evolving.[20] So, a single QRNG card can generate a random stream of bits (at the output of the post-

17. See https://www.etsi.org/deliver/etsi_gr/QSC/001_099/006/01.01.01_60/gr_QSC006v010101p.pdf
18. The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. It runs in the application layer of the Internet and is composed of two layers: the TLS record and the TLS handshake protocols.
19. T2, T2S, and TIPS.
20. An intersting example is the QRANGE project founded by the European Commission (https://cordis.europa.eu/project/id/820405) under the coordination of Université de Genève with the participation of Università degli Studi di Trento, Katholieke Universiteit Leuven, Fondazione Bruno Kessler, Université Libre de Bruxelles, Robert Bosch GmbH, Fundacio Institut de Ciencies Fotoniques, ID Quantique SA, Quside Technologies S.L which aims at developing a fast, compact and self-testing

processing section) sufficient to generate at least 2,000 encryption keys per second with a length of 256 bits. The capacity of the single card, due to the presence of the selective XOR component described by (6), also constitutes the total capacity of the single QRNG server; therefore, more servers need to be added in order to scale up the system.

Availability definition

Availability measures the ability of an entity or system to perform a required function under certain conditions at a given instant or during a given time interval. It can be defined as the ratio of current operating time to total time (therefore less than or equal to 1). Therefore, we can calculate the steady state availability using the following formula:

$$A = \frac{MTTF}{MTTF + MTTR} \tag{7}$$

where MTTF is the Mean Time To Failure and MTTR is the Mean Time To Recovery. For a serial system composed by N, each element of the system must function correctly for the whole system to function correctly. The corresponding availability is:

$$A_{series} = \prod_{i=1}^{N} A_i \tag{8}$$

where A_i is the steady state availability of the single element.
For a parallel system composed by N, only one of multiple elements needs to be operational for the whole system to be operational. The corresponding availability is:

$$A_{parallel} = 1 - \prod_{i=1}^{N} (1 - A_i) \tag{9}$$

where A_i is the steady state availability of the single element.

The QRNG server is a critical component of the datacentre infrastructure and should therefore be designed properly to fulfil the high availability constraints.

At single server level, according to (9) the solution proposed based on the presence of the 'selective XOR' component (6) means that:

$$A_{QRNG} = 1 - (1 - A_i)^N \tag{10}$$

where A_i is the availability of each single QRNG card, N is the number of installed cards, and A_{QRNG} is the total availability of the QRNG subsystem. This number should be multiplied by the availability of the server where the cards are installed (A_{Server}) to obtain the total availability of a single QRNG server ($A_{QRNG_{Server}}$). To further increase the total availability of the random number generation system of a single datacentre, it is possible to insert more QRNG servers working in parallel.

(Rusca *et al.* 2019) QRNG system.

2.2 Quantum Key Distribution systems

As discussed in the previous chapter, it is already possible to generate a random sequence of bits as a genuinely stochastic key for cryptographic purposes. In this section we will illustrate how to share the key among parties and use it to improve security.

Currently, there are two approaches to the key-based encryption algorithms: symmetric (or secret key), which uses the same key to encrypt and decrypt, and asymmetric (or public key) which uses a pair of mathematically related keys where the public key is known to everyone. Public key cryptosystem security is based on algorithmic complexity (i.e. it is hard to deduce the secret key from the public key in a reasonable amount of time). Hybrid strategies are commonly employed for optimal performance, where asymmetric cryptography is used to exchange keys between parties and symmetric encryption is applied to secure the bulk of information. The advancement in the processing capacity of quantum-enhanced computing systems poses a significant threat to the security of current encryption scheme. To mitigate these risks and build a quantum safe system, in recent years, two distinct yet complementary approaches have been developed: post-quantum cryptography (development of quantum resistant conventional cryptographic algorithms) and Quantum Key Distribution (a key distribution method based on quantum mechanics laws).

Quantum-resistant algorithms (Perlner and Cooper 2009) can be implemented on existing classical platforms and their security is based on mathematical complexity.[21] NIST has been leading a public competition to standardize one or more quantum-resistant public-key cryptographic algorithms: four algorithms have been identified, and the standards are expected to be finalized in approximately two years. However, these algorithms rely on unproven computational hardness assumptions: if proven wrong,[22] the encryption may become insecure. Additionally, encrypted messages and public keys could be intercepted and stored by an eavesdropper waiting for future technological or mathematical advancements (download now, decrypt later) breaking the so-called long term security (Xu *et al.* 2020).

A different perspective is offered by combining quantum mechanics principles with symmetrical key algorithms. As mentioned in the previous chapter, the algorithms used in symmetric cryptography are inherently more resistant to quantum attacks as they are only vulnerable to brute force attacks. An opponent, with quantum computing capabilities, can only use the Grover algorithm (Grover 1996), which only provides a quadratic time improvement.[23] The choice of longer keys could adequately mitigate risks and achieve the so-called unconditional security (Mayers 1998). Key distribution, among the entities involved in the communication, represents the most critical challenge to symmetric key encryption. Quantum Key Distribution (QKD) theory offers a way to generate and distribute cipher keys through unsecured channels, in a provably (Shannon 1949) secure way by exploiting the power of the laws of quantum physics. This method is based on unique quantum physics properties (Gisin *et al.* 2002): the bits are encoded in particle quantum properties (qubits) such as single-photon polarization[24] and transmitted in a way that any potential eavesdropping can be detected.[25] Hence, a random sequence of bits can be obtained as a cipher key that can be used to encrypt classical data using traditional symmetric algorithms.[26]

21. Researchers are working on a wide range of approaches such as lattice-based cryptography (based on the computational difficulty of some mathematical theory of discrete lattices problems).

22. Most of cryptosystems currently in use (RSA, Diffie-Hellman, and Elliptic Curve Cryptography) are considered vulnerable by Shor's algorithm while those recently proposed have not been broken yet but may never be proven to be definitively quantum-safe due to possible unknown algorithms. See for example https://eprint.iacr.org/2022/214.pdf

23. This algorithm solves the problem of searching in an unsorted database.

24. Qubits can be related to the quantum state of photons, electrons, atoms, or any other system with quantum properties. However, manipulating photons' properties to encode qubits is easier and, thanks to optical fibres (i.e. the media on which modern telecommunication networks are based), photons could be sent over long distances with relatively little loss.

25. Quantum theory prevents eavesdroppers both from measuring a well prepared signal without altering it and from making a copy of it thanks to to the no-cloning theorem (see the box 'Photon information encoding').

26. The one-time pad (OTP), theoretically proven secure, is not suitable for high data encryption (the key length has to be

Photon information encoding

A light beam is made of single particles (photons), each of which has a particular quantum property that affects its behaviour when it goes through a polarizing filter. This property (polarization) represents one of the preferred ways to encode quantum information and realize qubits. For example, choosing a rectilinear basis, the bit value 0 could be associated with the state $|0\rangle$ (a photon that passes through a horizontally polarized filter) and the bit 1 with $|90\rangle$. Similarly, another basis (for example diagonal) could be used and the polarization state $|45\rangle$ could be associated with the bit value 0 and the bit value 1 with $|135\rangle$.

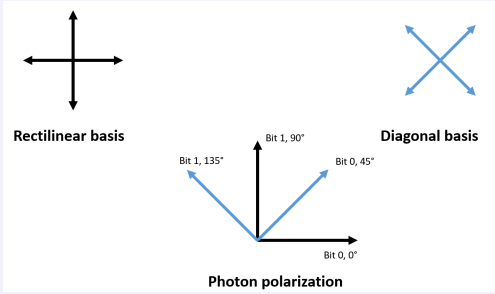


Figure 5. Bit coding using photon polarization (figure adapted from Haitjema 2007)

Quantum mechanics predicts that a photon polarized horizontally $|0\rangle$ (the same for $|90\rangle$), has a $1/2$ probability of passing through a polarizer with a polarization angle of 45°, given that the state could be expressed as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|45\rangle + |135\rangle\right) \tag{11}$$

When this happens, this sort of measurement operation also causes the so-called system collapse into the corresponding value function ($|45\rangle$ or $|135\rangle$) and destroys the initial superposition for this basis. For example:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|45\rangle + |135\rangle\right) \Rrightarrow |\psi\rangle = |45\rangle \tag{12}$$

Thus, during signal transmission, any interference inevitably alters qubit information and allows the detection of eavesdropping. Unlike the behaviour of classical systems, the duplication of an unknown quantum state is forbidden by the theory due to the no-cloning theorem (Wootters and Zurek 2009). Therefore, no one can make copies of a transmitted signal.

A QKD system consists of some devices emitting photons and detecting their polarization, a quantum channel to exchange quantum-enhanced keys between the nodes (Alice and Bob), a classical authenticated channel to transmit the encrypted messages, and a protocol to communicate. QKD protocols are based on two approaches (Xu *et al.* 2020) (Lo, Curty and Tamaki 2014) (Diamanti *et al.* 2016): the entanglement-based scheme (like Ekert-91 or BBM92)[27] and the prepare and measure scheme (for more details, see the box 'BB84 protocol')[28] the latter being more

at least as long as the data to be secured) and more efficient 'block ciphers' algorithms could be used, such as AES, which is also considered secure if it uses sufficiently large key sizes (ETSI 2015).

27. In the entanglement-based scheme a source emits entangled photons (see the box) and Alice and Bob both detect them to generate the key. Eavesdropping is detected also by verifying if the correlations are violating a particular inequality (Bell) as demonstrated by the recently Nobel-prize awarded scientists Aspect (Aspect, Grangier and Roger 1981), Clauser (Clauser *et al.* 1969), and Zeilinger (Giustina *et al.* 2015).

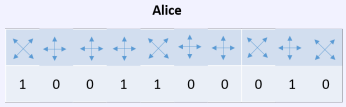
28. In the prepare and measure scheme, quantum states prepared by Alice are sent and measured by Bob.

mature.[29]

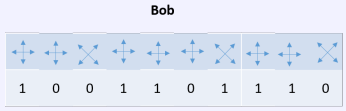
BB84 protocol

The best-known and widely used QKD protocol was proposed in 1984 by Bennett and Brassard (Bennett and Brassard 1984). Alice and Bob want to exchange a secret key. They agree to use polarized photons for communication, two bases for measurements (in this example rectilinear and diagonal), and the bit value assigned to the measurement results.

Alice prepares a random sequence of N polarized photons (bits are encoded in the polarization state of a photon) changing the two bases and sends it to Bob.

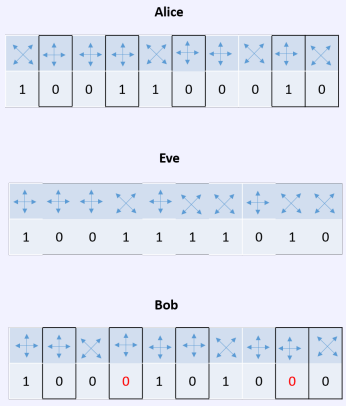


Bob, independently of Alice, selects bases for emitted photons measurement. He obtains the same value transmitted by Alice when he uses the same basis to detect them (about 50% of the cases). After the transmission, both Alice and Bob have a classical N bit string (*raw key*).



Alice and Bob publicly exchange information in a classical way to obtain their shared secret key: for each bit (without revealing the value obtained) Bob declares the basis he used and Alice tells him when she used the same. Bits detected in different bases are rejected. The key length is halved, but it is random and the same for both.

They publicly check for interference by comparing a random part of the key they have just obtained.
If an eavesdropper Eve has intercepted the photons polarization using a random basis (and has resent them by the same basis), Bob adopts the same Alice basis in about half of the cases but Eve's resent basis changes the polarization. It causes an error rate of about 25% during key comparison. In this case the procedure must be repeated.
Finally, the remaining key (bits used for the check are discarded) can be used to encrypt messages and send them via a public communication channel.



QKD secure communication requires specialized hardware, such as single photon sources and

29. Protocols are also distinguished by using discrete variables (DV-QKD, information is encoded in a discrete quantum state, such as single photon polarization) or continuous variables (CV-QKD, information is codified in a continuous variable such as electromagnetic field physical properties). Both approaches being investigated and present different advantages (Pirandola *et al.* 2020).

detectors. The real life implementations are necessarily imperfect (Pacher *et al.* 2015) (sometimes signals are doubled, detectors cannot have full efficiency and have dead time, basis alignment could be defective).[30] In order to overcome these imperfections, a number of QKD protocols have been proposed[31] and various quantum devices are already available on the market (Cao *et al.* 2022).

In QKD, two logical communication channels are foreseen: a quantum channel to send encoded photons between two parties and a classical channel, to manage post-processing procedures and send encrypted data using the secure keys thus obtained. Neither of those channels needs to be private.

There are mainly two ways to transport photons along the quantum channel: optical fibres or free space media. Optical fibres, which are now widely used in telecommunications, have low photon loss and high stability if the point-to-point distance is limited to a few hundred kilometres.[32] Most of the QKD settings have been set up on dedicated dark fibre scenarios due to implementation constraints.[33] However, from a practical and economical perspective, the coexistence of quantum and classical signals in the same media would be a desirable approach (Alléaume *et al.* 2020).[34]

On the other hand, free-space optical links provide better performance and flexibility when covering longer distances: in August 2016 the first quantum satellite, Micius (Liao *et al.* 2017), was launched in China and a QKD link of over 1000 Km was established using a satellite-based entanglement distribution protocol on low-Earth-orbit satellites.

The next step will be to connect multiple QKD point-to-point systems to set up large-scale quantum networks based on the existing communication infrastructures (Cao *et al.* 2022). The single QKD links could be integrated, for instance, with quantum repeaters or with trusted relays. Quantum information cannot be copied (due to the no-cloning theorem), therefore it is impossible to use conventional repeaters based on the amplification mechanism. This problem could be bypassed (Sangouard *et al.* 2011) by using quantum repeater protocols based on intermediate nodes that rely on long-distance entanglement between emitter and receiver via entanglement swapping.[35]

30. A well-known attack for example is the Photon Number Splitting (PNS) attack: in real life, photons are produced in multi-bunches, so an eavesdropper could take one of them and leave the others to be detected by Bob. The SARG04 protocol(Scarani *et al.* 2004) was introduced to mitigate this risk. Another well-known attack is the DoS (Denial of Service) attack, which can also always be carried out by interrupting the channel and can be prevented only by setting up alternative channels as in classical communications.

31. Decoy-state QKD (Lo, Ma and Chen 2005), Device-Independent (Acín *et al.* 2007), Measurement Device Independent (Lo, Curty and Qi 2012): the goal is to provide security also with corrupted devices and find efficient methods to discard the least amount of bits transmitted.

32. The current state-of-the-art experiments make it possibile to reach distances over 500Km (J.-P. Chen *et al.* 2020), but a realistic implementation should consider a maximum of 100 Km (Diamanti *et al.* 2016).

33. Quantum signals are weak (few photons per pulse) compared to classical signals (millions of photons): coexistence is a challenging task since any interaction could compromise quantum states coherence.

34. Some multiplexing techniques based on wavelength or time division have been recently introduced to share the optical bandwidth available; data and quantum signals could be transmitted via a single optical fibre of up to 90 km in length with a good bit rate(Patel *et al.* 2012).

35. Such a promising protocol foresees the creation of chains of entangled photons (for an overview see (Manzalini and Amoretti 2022)). Entanglement swapping (Horodecki *et al.* 2009) enable the realization of entangled states of photons that have never interacted before, obtaining them from independent entangled states.

Entanglement

One of the least non intuitive features of quantum mechanical theory (quoting Schröedinger *the one which enforces its entire departure from classical lines of thought*) linked to linearity and, therefore, to the superposition principle is entanglement. This phenomenon occurs when two or more physical systems interact in such a way that some of their physical properties cannot be described independently of each other, regardless of the distance between them.

Suppose having two photons (1 and 2) emitted in two opposite directions with the same polarization, for example the horizontal polarization $|0\rangle_1$ and $|0\rangle_2$. Quantum mechanics describes a physical system by the tensor product:

$$|\psi\rangle = |0\rangle_1 \otimes |0\rangle_2 \tag{13}$$

Each photon is independent and will pass the respective test if the filter is aligned with its polarization. Moreover, the system $|\psi\rangle = |90\rangle_1 \otimes |90\rangle_2$ is allowed, as well as each normalized linear superposition of two physical systems (that is also experimentally easy to prepare), such as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |0\rangle_2 + |90\rangle_1 \otimes |90\rangle_2) \tag{14}$$

Suppose doing a measurement process (i.e. inserting a vertical filter) on photon 1 described by (14): the physical system will collapse on one of the possible states, for instance:

$$|\psi\rangle = |90\rangle_1 \otimes |90\rangle_2 \tag{15}$$

This means that photon 2, which could also be very distant from photon 1, immediately acquires a physical property (in this example the vertical polarization) without being measured.
There are many methods (Edamatsu 2007) for generating entangled photon pairs that are currently under evaluation because their properties could be used in a large number of applications in quantum communication and information technology.

In a trusted relay based QKD network, instead, the keys are generated for each QKD connection and stored in the node memories at QKD endpoints, then they are combined and forwarded from a node to another concatenating QKD links.[36]

Introducing a standard for QKD plays a crucial role also in allowing integration and interoperability among different networks and commercial devices. Several standardization initiatives are underway from the most important organizations[37] such as ITU, ETSI, ISO/IEC, and IEEE (Loeffler *et al.* 2020).

Among other countries, the EU's key funding programme for research and innovation has funded a long-term research and innovation initiative (The Quantum Technologies Flagship)[38] that aims to

36. A more robust option is realized using untrusted relay models that guarantee security also if the node is controlled by an eavesdropper. Moreover, there are some promising approaches to next-generation long-distance communication such as TF-QKD (Lucamarini *et al.* 2018).
37. See, for example, https://www.etsi.org/technologies/quantum-safe-cryptography.
38. https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship

'put Europe at the forefront of the quantum revolution'. The EuroQCI initiative,[39] in particular, is expected to contribute to the creation of 'a secure quantum communication infrastructure spanning the whole EU'.

The payment system infrastructure is among the most critical ones to protect. The EMIP[40] architecture 'provides a valid answer to the technical challenges of a European-wide settlement system offering a fully scalable central processing system, a storage sub-system with synchronous and asynchronous mirroring and a dedicated network connecting the processing sites (4CBNet)'.[41]

Securing mission-critical Storage Area Network (Figure 6) through a QKD link between the disaster recovery site and the main site[42] by a point-to-point implementation could be a significant improvement.

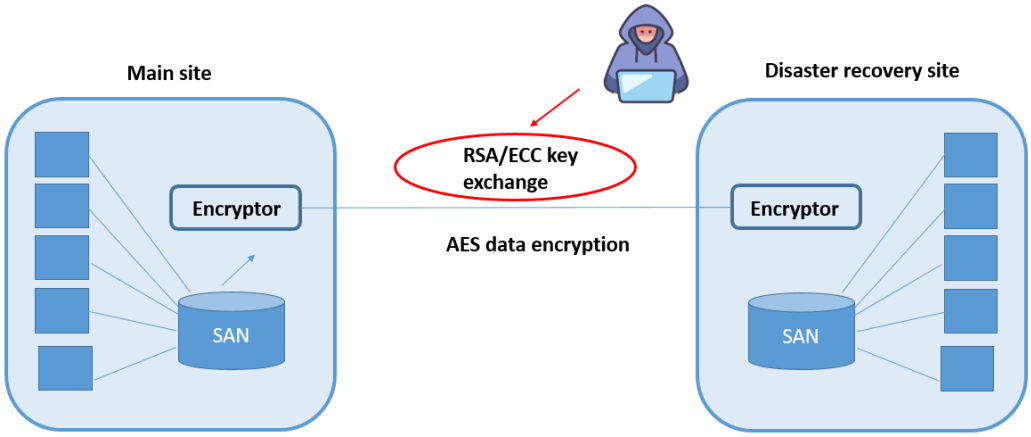


Figure 6. Current classical datacentre cryptography

For simple point-to-point implementations, various QKD solutions are already available on the market. Device implementation can vary across vendors but the basic functions of a QKD system are universal: an optical subsystem with components for the preparations and measurement of quantum information and a digital data conversion module.[43] The system consists of two units, usually compatible with a rack installation, connected by a quantum fibre channel.[44]

This means that a possible way to create a secure and quantum-resistant communication link between two sites is to install a QKD device in each site (Figure 7), and connect them by an optical fibre link dedicated to key exchange. The shared secret keys generated by the QKD devices are then passed on to link encryptors to secure the data transmitted over a classical channel (Figure 8).[45]

39. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci
40. Eurosystem Market Infrastructure Platform
41. https://www.ecb.europa.eu/paym/target/t2s/profuse/shared/pdf/general_technical_design_spotlight.pdf
42. Datacentres are usually organized at a 'primary' site and a 'backup' is equipped as 'disaster recovery' site via SAN (Storage Area Network) mirroring technology for business continuity purposes. These sites are normally a few Km apart.
43. See https://www.etsi.org/deliver/etsi_gs/qkd/001_099/002/01.01.01_60/gs_qkd002v010101p.pdf.
44. These devices are already mature to be used in a production environment. The necessary monitoring and administration functions are usually included.
45. Some commercial devices are already supporting the ETSI standard ETSI GS QKD 014 interface for the quantum key exchange.

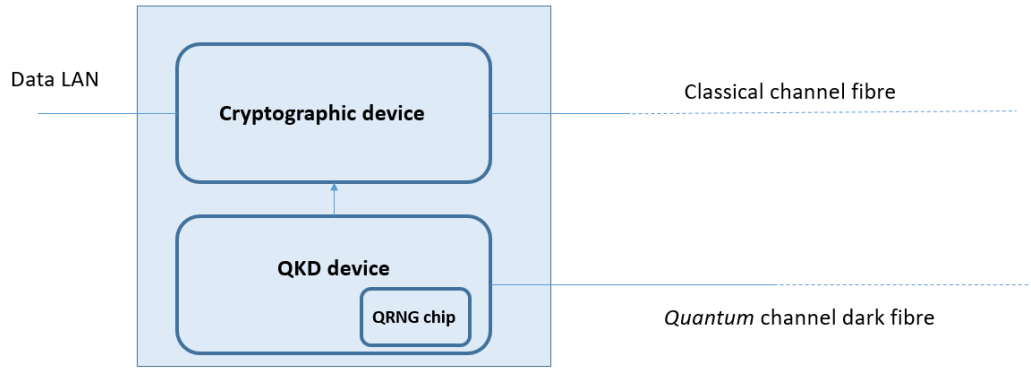


Figure 7. QKD encryptors logical model.

To further improve security, a QRNG chip (or a system call, as suggested earlier) embedded in the QKD system can guarantee that keys are produced randomly. Due to the possibile limited key rate generation, a key storage is installed at both endpoints of the QKD links (Mehic *et al.* 2020).

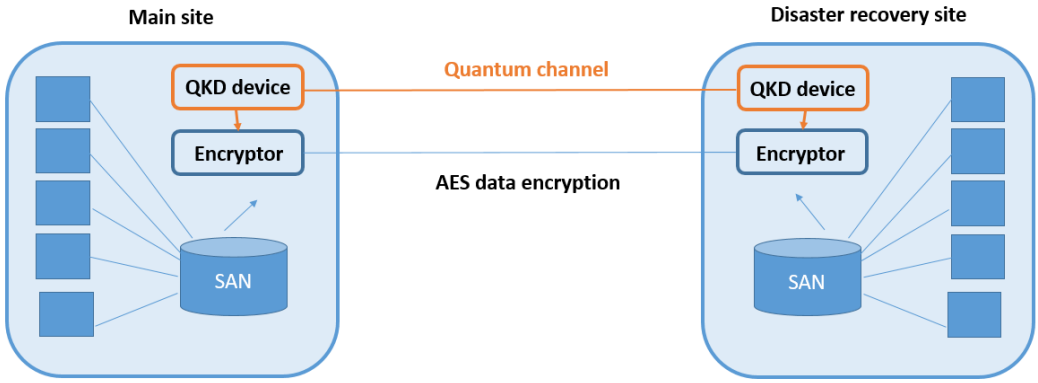


Figure 8. Quantum safe datacentres cryptography

Implementing this quantum security scheme between inter-regional datacentres represents a more challenging scenario. Quantum commercial devices can be deployed in any network configurations, including relay for longer distances. However, establishing a secure connection between datacentres in Europe, for instance via trusted repeaters, would require multiple stations to cover the current distances. In the next future, it would be desirable to adopt quantum-safe networks (Cao *et al.* 2022) taking advantage of heterogeneous QKD systems offered by QKD providers, as is currently the case for traditional network providers.

2.3 Cryptographic agility

The discovery of new cryptographic weaknesses or advances in the technologies supporting cryptoanalysis often leads to the need to replace a legacy cryptographic algorithm. The advent of quantum computing technology will compromise many of the current cryptographic algorithms (L. Chen *et al.* 2016), especially public-key cryptography, which is widely used to protect digital information.[46] A multitude of public key-based protocols, including TLS, IPSEC,[47] digital signing and code signing, will become vulnerable to eavesdropping and public disclosure as they are not strong enough to resist a quantum attack.

Mosca's theorem

People naturally ask if they can continue to delay taking action since there are many other urgent and serious matters at hand. Whether one can continue to procrastinate roughly depends on three questions.

- Firstly, how long do you need your cryptographic keys to remain secure? Denote this number by **x**, the security shelf-life. We may have x = 0 years for applications requiring only real-time security. Or maybe x = 10, 20, or 100 years when protecting your personal health data, trade secrets, or national security information. The value of x is in general a personal or business or policy decision.
- Next, how long will it take to deploy a set of tools that are quantum-safe? Denote this number by **y**, the migration time. For example, we may have y = 0 years if this is simply a matter of deploying an auto-update that replaces AES-128 with AES-256 within a system fully controlled by a single vendor. However, we may have y $\geq$ 15 years if it involves a relatively untested public-key encryption method that has to be adapted for a constrained environment with many players who must agree on a standard.
- Lastly, how long will it be before a quantum computer, or some other method, breaks the currently deployed public-key cryptography tools? Let **z** denote this number, the collapse time.

If **x + y > z**, we have a serious problem today, since information protected by quantum vulnerable tools at the end of the next **y** years can be broken by quantum attacks in less than **x** years from then (Mosca 2018).

The arrival date of quantum threats is unknown at this time (i.e. the *z* variable of Mosca's theorem). The National Academy of Science in the United States affirms that they expect a quantum computer to reach a useful scale in less than 20 years' time (2038). Some academics working in the field report that we have a 50-50 shot of seeing a quantum computer strong enough to obliterate conventional cryptography in the next 10 years (2028) (Macaulay and Henderson 2021).

It is essential for the payment industry, which has a great interest in keeping secret information safe from adversaries, to be forward-thinking in its approach to information security. This involves considering more than merely how soon a quantum computer may be built. It also means thinking about how long information needs to stay secure and how long it will take to update the existing IT infrastructure so that it is quantum-safe (i.e the x+y elapsed time of Mosca's theorem).

NIST started a post-quantum cryptography competition in 2016, in order to identify cryptographic algorithms capable of withstanding quantum computer attacks and make them available

46. See https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/pqc-migration-project-description-final.pdf

47. Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).

by 2024.[48] A recent study by the European Union Agency for Cybersecurity (ENISA)[49] has highlighted how we should start planning to replace the current cryptographic algorithms, especially those used for digital signature (e.g. RSA, ECDSA[50]) with post-quantum variants (Beullens *et al.* 2021).

Rolling out new cryptographic algorithms takes a lot of time and effort because apps and cryptography are often tied together by the specific API used in that implementation and sometimes changes in cryptography require complete changes in apps and new versions of both apps and cryptography may no longer be compatible with legacy versions (Figure 9).

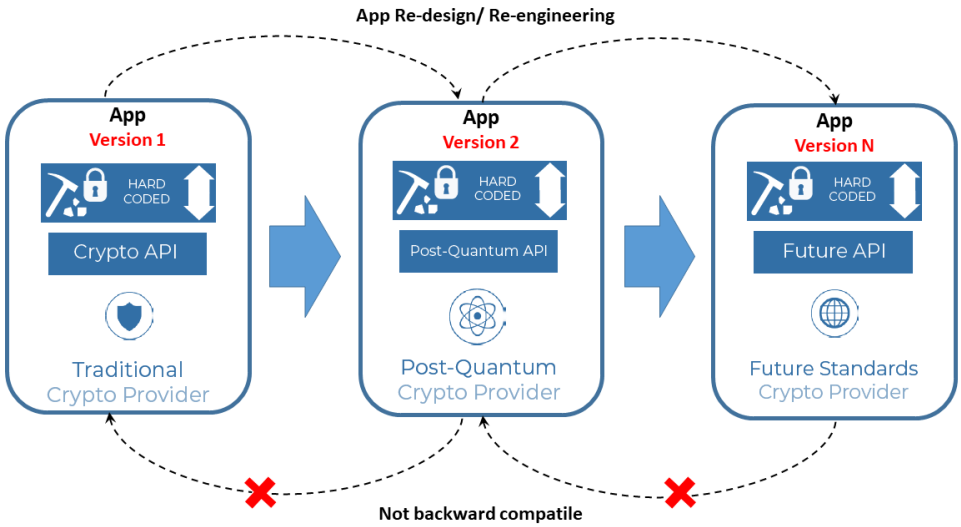


Figure 9. Current Development Architecture: cryptography and apps integration is usually hardcoded (Macaulay and Henderson 2021)

Such a structure (Figure 9) requires extensive time and costs to be updated, which means that variable y of Mosca's theorem will be significantly increased. To reduce this time, it is therefore necessary to radically change how cryptographic primitives are integrated into ICT systems to reduce the time required to replace a cryptographic algorithm that is no longer secure.

This goal can be achieved through crypto-agility i.e. the ability to implement, update, change, and remove cryptographic functions from systems and applications on demand, without changing the systems or applications themselves.

Cypto-agility can be achieved by creating one or more layers of abstraction between applications and cryptographic functions (Aciobanitei, Urian and Pura 2018). Thus, there is a need to identify the crypto provider, which implements a specific cryptographic algorithm and therefore offers services to applications through an abstract API (Abstract Crypto API). In this way, applications are agnostic with regard to the specific underlying cryptographic scheme in use.

48. On July 5, 2022, NIST announced the selected algorithms for the final round (https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022).
49. See https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation
50. The Elliptic Curve Digital Signature Algorithm (ECDSA) offers a variant of the Digital Signature Algorithm (DSA) which uses elliptic curve cryptography.

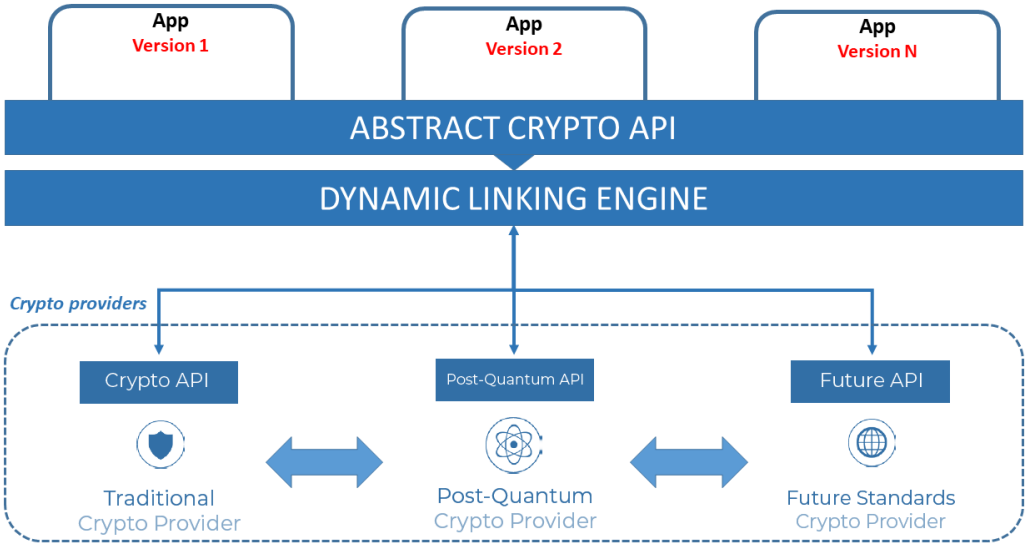


Figure 10. Cryptographic agile architecture: crypto migration becomes independent from app lifecycle. (Macaulay and Henderson 2021)

The Abstract Crypto API should provide some fundamental primitives related to random numbers generation and encryption keys distribution. These primitives can easily be created using the QRNG and QKD services described in the two previous chapters and must be integrated with further primitives dedicated to data encryption/decryption, digital signature, and verification. Crypto providers are linked at runtime with apps without requiring source code modifications. This task is performed by the dynamic linking engine (Figure 10).

The transition from the model illustrated in Figure 9 to the one proposed in Figure 10 is a complex process that requires time and effort. However, cryptography is widely used in the Eurosystem payment system to safeguard information, ensure data confidentiality and protect data integrity. Therefore, it would be useful to timely consider the proposed framework to achieve cryptographic agility.

Managing the replacement of cryptographic primitives through crypto-agility, as described above, may not be very effective for payment systems based on blockchain technology. Blockchain systems are unlike other cryptosystems, in that they are not *just* meant to protect an information asset. A blockchain is a ledger and as such it *is* the asset (Kearney and Perez-Delgado 2021).

In Bitcoin, for example, replacing the ECDSA digital signature scheme with a post-quantum scheme would almost certainly involve making hard forks[51] in the transaction chain (Tessler and Byrnes 2018).

3 Conclusions

Security plays a key role in payment infrastructures; which is why it must be guaranteed at all times, even vis-à-vis new technologies that constantly introduce new threats. Recent technological advances in quantum computing are breaking new ground in many fields but, at the same time, have opened up new possibilities of attack against cryptographic technologies, which are the foundations of the current security payment systems.

51. A hard fork (or hard-fork), as it relates to blockchain technology, is a radical change to a network's protocol that makes previously invalid blocks and transactions valid, or vice-versa. A hard fork requires all nodes or users to upgrade to the latest version of the protocol software.

On the other hand, quantum physics also provides the means for current cryptographic systems to evolve into new architectures capable of guaranteeing high levels of security even when quantum computers will be widely used.

In this paper, we have proposed three lines of intervention to improve the current cryptographic system used in payment systems and make it resistant to attacks carried out with quantum processing capabilities. The basis of all cryptographic systems is the effective generation of random numbers, hence this work introduces a reference architecture for the generation and distribution of random numbers. The second contribution relates to the use of quantum systems for the secure distribution of encryption keys (QKD). The quantum devices necessary to create the systems were launched on the market a long time ago and have reached a level of maturity and performance that justifies their use in payment systems.

Finally, we proposed a methodological contribution to start designing agile cryptographic application (i.e. crypto-agility). This will make it possible to easily replace a cryptographic scheme that has become insecure with a new and currently secure scheme, thus minimizing the impact on the application.

The global technological landscape is rapidly changing, thus calling for an evolution of the technological foundations on which the security of current payment systems are based. This paper outlines a possible evolutionary path to achieve this goal.

References

Acín, A., N. Brunner, N. Gisin, S. Massar, S. Pironio and V. Scarani. 2007. "Device-Independent Security of Quantum Cryptography against Collective Attacks". *Physical Review Letters* 98, no. 23 (June). ISSN: 1079-7114. https://doi.org/10.1103/physrevlett.98.230501. http://dx.doi.org/10.1103/PhysRevLett.98.230501.

Aciobanitei, I., P. D. Urian and M. Pura. 2018. "A Cryptography API: Next Generation Key Storage Provider for Cryptography in the Cloud". In *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI),* 1–4. https://doi.org/10.1109/ECAI.2018.8679042.

Alléaume, R., R. Aymeric, C. Ware and Y. Jaouën. 2020. "Technology Trends for Mixed QKD/WDM Transmission up to 80 km". *Optical Fiber Communication Conference (OFC) 2020,* https://doi.org/10.1364/ofc.2020.m4a.1. http://dx.doi.org/10.1364/OFC.2020.M4A.1.

Arcese, Di Giulio and Lasorella. 2021. "Real-Time Gross Settlement systems: breaking the wall of scalability and high availability". *Markets, Infrastructures, Payment Systems,* nos. 2021-2, https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/approfondimenti/2021-002/N.2-MISP.pdf.

Aspect, A., P. Grangier and G. Roger. 1981. "Experimental Tests of Realistic Local Theories via Bell's Theorem". *Phys. Rev. Lett.* 47 (7): 460–463. https://doi.org/10.1103/PhysRevLett.47.460. https://link.aps.org/doi/10.1103/PhysRevLett.47.460.

Bennett, C. H., and G. Brassard. 1984. "Quantum cryptography: Public key distribution and coin tossing". *Theoretical Computer Science* 560 (December): 7–11. ISSN: 0304-3975. https://doi.org/10.1016/j.tcs.2014.05.025. http://dx.doi.org/10.1016/j.tcs.2014.05.025.

Beullens, W., J.-P. D'Anvers, A. Hülsing, T. Lange, L. Panny, C. de Saint Guilhem and N. P. Smart. 2021. "Post-Quantum Cryptography: Current state and quantum mitigation". *European Union Agency for Cybersecurity* (March). https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation.

Bramini, P., M. Coletti, F. D. Stasio, P. Molina, V. Schina and M. Valentini. 2021. "Il sistema europeo per il regolamento dei pagamenti di importo rilevante". *Markets, Infrastructures, Payment Systems,* nos. 2021-09, https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/questioni-istituzionali/2021-009/N.9-MISP.pdf.

Bronner, P., A. Strunz, C. Silberhorn and J.-P. Meyn. 2009. "Demonstrating quantum random with single photons". *European Journal of Physics* 30, no. 5 (August): 1189–1200. https://doi.org/10.1088/0143-0807/30/5/026. https://doi.org/10.1088/0143-0807/30/5/026.

Buhler, J. P., H. W. Lenstra and C. Pomerance. 1993. "Factoring integers with the number field sieve". In *The development of the number field sieve,* edited by A. K. Lenstra and H. W. Lenstra, 50–94. Berlin, Heidelberg: Springer Berlin Heidelberg.

Cao, Y., Y. Zhao, Q. Wang, J. Zhang, S. Ng and L. Hanzo. 2022. "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet". *IEEE Communications Surveys Tutorials* PP (January). https://doi.org/10.1109/COMST.2022.3144219.

Chen, J.-P., C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan *et al.* 2020. "Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km". *Phys. Rev. Lett.* 124 (7). https://doi.org/10.1103/PhysRevLett.124.070501. https://link.aps.org/doi/10.1103/PhysRevLett.124.070501.

Chen, L., S. Jordan, Y. Liu, D. Moody, R. Peralta, R. Perlner and D. Smith-Tone. 2016. "Report on Post-Quantum Cryptography". *NIST* (April). http://dx.doi.org/10.6028/NIST.IR.8105.

Clauser, J. F., M. A. Horne, A. Shimony and R. A. Holt. 1969. "Proposed Experiment to Test Local Hidden-Variable Theories". *Phys. Rev. Lett.* 23 (15): 880–884. https://doi.org/10.1103/PhysRevLett.23.880. https://link.aps.org/doi/10.1103/PhysRevLett.23.880.

Diamanti, E., H.-K. Lo, B. Qi and Z. Yuan. 2016. “Practical challenges in quantum key distribution”. *npj Quantum Information* 2, no. 1 (November): 16025. ISSN: 2056-6387. https://doi.org/10.1038/npjqi.2016.25. https://doi.org/10.1038/npjqi.2016.25.

Dirac, P. A. M. 1939. “A new notation for quantum mechanics”. *Mathematical Proceedings of the Cambridge Philosophical Society* 35 (3): 416–418. https://doi.org/10.1017/S0305004100021162.

Dowling, J., and G. Milburn. 2003. “Quantum technology: The second quantum revolution”. *Philosophical Transactions of the Royal Society of London.*

Edamatsu, K. 2007. “Entangled Photons: Generation, Observation, and Characterization”. *Japanese Journal of Applied Physics* 46, no. 11R (November). https://doi.org/10.1143/JJAP.46.7175. https://dx.doi.org/10.1143/JJAP.46.7175.

ETSI. 2015. “Quantum Safe Cryptography and Security”. *ETSI White Paper No. 8* (June). https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

———. 2017. “ETSI GR QSC 006”. *ETSI,* no. 2, https://www.etsi.org/deliver/etsi_gr/QSC/001_099/006/01.01.01_60/gr_QSC006v010101p.pdf.

Feynman, R. 1982. “Simulating physics with computers”. *Int J Theor Phys* 21 (4). https://doi.org/10.1007/BF02650179. https://doi.org/10.1007/BF02650179.

Gennaro, R. 2006. “Randomness in cryptography”. *IEEE Security Privacy* 4 (2): 64–67. https://doi.org/10.1109/MSP.2006.49.

Gidney, C., and M. Ekerå. 2021. “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits”. *Quantum* 5 (April): 433. ISSN: 2521-327X. https://doi.org/10.22331/q-2021-04-15-433. http://dx.doi.org/10.22331/q-2021-04-15-433.

Gisin, N., G. Ribordy, W. Tittel and H. Zbinden. 2002. “Quantum cryptography”. *Rev. Mod. Phys.* 74 (1): 145–195. https://doi.org/10.1103/RevModPhys.74.145. https://link.aps.org/doi/10.1103/RevModPhys.74.145.

Giustina, M., M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner *et al.* 2015. “Significant-Loophole-Free Test of Bell’s Theorem with Entangled Photons”. *Phys. Rev. Lett.* 115 (25). https://doi.org/10.1103/PhysRevLett.115.250401. https://link.aps.org/doi/10.1103/PhysRevLett.115.250401.

Google. 2018. “Google aims for quantum supremacy”. *www.google.com,* https://physicsworld.com/a/google-aims-for-quantum-supremacy/.

Grover, L. 1996. “A fast quantum mechanical algorithm for database search Share on”. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing,* 212–219. https://doi.org/10.1145/237814.237866. https://doi.org/10.1145/237814.237866.

Hadfield, R. 2009. “Single-photon detectors for optical quantum information applications”. *Nature Photonics* 3 (December). https://doi.org/10.1038/nphoton.2009.230.

Hai-Qiang, M., W. Su-Mei, Z. Da, C. Jun-Tao, J. Ling-Ling, H. Yan-Xue and W. Ling-An. 2004. “A Random Number Generator Based on Quantum Entangled Photon Pairs”. *Chinese Physics Letters* 21, no. 10 (October): 1961–1964. https://doi.org/10.1088/0256-307x/21/10/027. https://doi.org/10.1088/0256-307x/21/10/027.

Haitjema, M. 2007. “A Survey of the Prominent Quantum Key Distribution Protocols.”, http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/.

Horodecki, R., P. Horodecki, M. Horodecki and K. Horodecki. 2009. “Quantum entanglement”. *Reviews of Modern Physics* 81, no. 2 (June): 865–942. https://doi.org/10.1103/revmodphys.81.865. https://doi.org/10.1103%2Frevmodphys.81.865.

Horvath, M., and D. Mahdi. 2017. “Better Safe Than Sorry: Preparing for Crypto-Agility”. *Gartner* (March). https://www.gartner.com/en/documents/3645384.

Huang, L., H. Zhou, K. Feng and C. Xie. 2021. “Quantum random number cloud platform”. *npj Quantum Information* 7 (July): 107. https://doi.org/10.1038/s41534-021-00442-x.

Jennewein, T., U. Achleitner, G. Weihs, H. Weinfurter and A. Zeilinger. 2000. “A fast and compact quantum random number generator”. *Review of Scientific Instruments* 71, no. 4 (April): 1675–1680. ISSN: 1089-7623. https://doi.org/10.1063/1.1150518. http://dx.doi.org/10.1063/1.1150518.

Jessa, M. 2015. “A Novel Method for Increasing the Entropy of a Sequence of Independent, Discrete Random Variables”. *Entropy* 17 (10): 7118–7132. ISSN: 1099-4300. https://doi.org/10.3390/e17107118. https://www.mdpi.com/1099-4300/17/10/7118.

Kearney, J. J., and C. A. Perez-Delgado. 2021. “Vulnerability of blockchain technologies to quantum attacks”. *Array* 10. ISSN: 2590-0056. https://doi.org/10.1016/j.array.2021.100065. https://www.sciencedirect.com/science/article/pii/S2590005621000138.

Killmann, W., and W. Schindler. 2011. “A proposal for: Functionality classes for random number generators”. *Federal Office of Information Security (BSI),* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf;jsessionid=5531F070D1976A95664EEB634D92EE1C.internet481?__blob=publicationFile&v=1.

Liao, S.-K., W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin *et al.* 2017. “Satellite-to-ground quantum key distribution”. *Nature* 549, no. 7670 (August): 43–47. ISSN: 1476-4687. https://doi.org/10.1038/nature23655. http://dx.doi.org/10.1038/nature23655.

Lo, H.-K., M. Curty and B. Qi. 2012. “Measurement-Device-Independent Quantum Key Distribution”. *Phys. Rev. Lett.* 108 (13). https://doi.org/10.1103/PhysRevLett.108.130503. https://link.aps.org/doi/10.1103/PhysRevLett.108.130503.

Lo, H.-K., M. Curty and K. Tamaki. 2014. “Secure quantum key distribution”. *Nature Photonics* 8, no. 8 (August): 595–604. ISSN: 1749-4893. https://doi.org/10.1038/nphoton.2014.149. https://doi.org/10.1038/nphoton.2014.149.

Lo, H.-K., X. Ma and K. Chen. 2005. “Decoy State Quantum Key Distribution”. *Phys. Rev. Lett.* 94 (23). https://doi.org/10.1103/PhysRevLett.94.230504. https://link.aps.org/doi/10.1103/PhysRevLett.94.230504.

Loeffler, M., C. Goroncy, T. Länger, A. Poppe, A. Neumann, M. Legré, I. Khan *et al.* 2020. “Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution”. *Online* (December). https://doi.org/https://openqkd.eu/wp-content/uploads/2021/03/OPENQKD_CurrentStandardisationLandscapeAndExistingGapsInTheAreaOfQuantumKeyDistribution.pdf.

Lucamarini, M., Z. L. Yuan, J. F. Dynes and A. J. Shields. 2018. “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters”. *Nature* 557, no. 7705 (May): 400–403. ISSN: 1476-4687. https://doi.org/10.1038/s41586-018-0066-6. http://dx.doi.org/10.1038/s41586-018-0066-6.

Lucke, R. L. 1976. “Counting statistics for nonnegligible dead time corrections”. *Review of Scientific Instruments* 47 (6): 766–767. https://doi.org/10.1063/1.1134733. eprint: https://doi.org/10.1063/1.1134733. https://doi.org/10.1063/1.1134733.

Macaulay, T., and R. Henderson. 2021. “Cryptographic agility in practice: emerging use cases”. *INFOSEC Global,* https://assets.website-files.com/5bd73d456f7b3f2db2bbbb95/5c76a740dcc2cc4646a06805_ISG_AgilityUseCases_Whitepaper-FINAL.pdf.

Manzalini, A., and M. Amoretti. 2022. “End-to-End Entanglement Generation Strategies: Capacity Bounds and Impact on Quantum Key Distribution”. *Quantum Reports* 4 (3): 251–263. ISSN: 2624-960X. https://doi.org/10.3390/quantum4030017. https://www.mdpi.com/2624-960X/4/3/17.

Markowsky, G. 2014. “The Sad History of Random Bits”. *Journal of Cyber Security and Mobility* 3 (January): 1–24. https://doi.org/10.13052/jcsm2245-1439.311.

Mastropasqua, C., A. Intonti, M. Jennings, C. Mandolini, M. Maniero, S. Vespucci and D. Toma. 2021. “T2S - TARGET2-Securities”. *Mercati, infrastrutture, sistemi di pagamento (Markets, Infrastructures, Payment Systems),* nos. 2021-04, https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/questioni-istituzionali/2021-004/N.4-MISP.pdf.

Mayers, D. 1998. “Unconditional security in Quantum Cryptography”, https://doi.org/10.48550/ARXIV.QUANT-PH/9802025. https://arxiv.org/abs/quant-ph/9802025.

McKurley, K. S. 1990. “The Discrete Logarithm Problem”. In *Proceedings of Symposia in Applied Mathematics,* 49–73. American Mathematical Society.

Mehic, M., M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin *et al.* 2020. “Quantum Key Distribution: A Networking Perspective”. *ACM Comput. Surv.* (New York, NY, USA) 53, no. 5 (September). ISSN: 0360-0300. https://doi.org/10.1145/3402192. https://doi.org/10.1145/3402192.

Mosca, M. 2018. “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?” *IEEE Security Privacy* 16 (5): 38–41. https://doi.org/10.1109/MSP.2018.3761723.

Pacher, C., A. Abidin, T. Lorünser, M. Peev, R. Ursin, A. Zeilinger and J.-Å. Larsson. 2015. “Attacks on quantum key distribution protocols that employ non-ITS authentication”. *Quantum Information Processing* 15, no. 1 (November): 327–362. https://doi.org/10.1007/s11128-015-1160-4. https://doi.org/10.1007%5C%2Fs11128-015-1160-4.

Patel, K. A., J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty and A. J. Shields. 2012. “Co-existence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber”. *Phys. Rev. X* 2 (4). https://doi.org/10.1103/PhysRevX.2.041010. https://link.aps.org/doi/10.1103/PhysRevX.2.041010.

Perlner, R., and D. Cooper. 2009. “Quantum Resistant Public Key Cryptography: A Survey”. IDtrust 2009, Gaithersburg, MD, 2009-04-14. https://doi.org/https://doi.org/10.1145/1527017.1527028.

Pirandola, S., U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund *et al.* 2020. “Advances in quantum cryptography”. *Advances in Optics and Photonics* 12, no. 4 (December). ISSN: 1943-8206. https://doi.org/10.1364/aop.361502. http://dx.doi.org/10.1364/AOP.361502.

Renzetti, Bernardini, Marino, Mibelli, Ricciardi and Sabell. 2021. “TIPS - TARGET Instant Payment Settlement Il sistema europeo per il regolamento dei pagamenti istantanei”. *Markets, Infrastructures, Payment Systems,* nos. 2021-01, https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/questioni-istituzionali/2021-001/MIS-20210129.pdf.

Rusca, D., T. van Himbeeck, A. Martin, J. B. Brask, W. Shi, S. Pironio, N. Brunner and H. Zbinden. 2019. “Self-testing quantum random-number generator based on an energy bound”. *Phys. Rev. A* 100 (6). https://doi.org/10.1103/PhysRevA.100.062338. https://link.aps.org/doi/10.1103/PhysRevA.100.062338.

Sangouard, N., C. Simon, H. de Riedmatten and N. Gisin. 2011. “Quantum repeaters based on atomic ensembles and linear optics”. *Rev. Mod. Phys.* 83 (1): 33–80. https://doi.org/10.1103/RevModPhys.83.33. https://link.aps.org/doi/10.1103/RevModPhys.83.33.

Scarani, V., A. Acín, G. Ribordy and N. Gisin. 2004. “Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations”. *Physical Review Letters* 92, no. 5 (February). ISSN: 1079-7114. https://doi.org/10.1103/physrevlett.92.057901. http://dx.doi.org/10.1103/PhysRevLett.92.057901.

Schumacher, B. 1995. “Quantum coding”. *Phys. Rev. A* 51 (4): 2738–2747. https://doi.org/10.1103/PhysRevA.51.2738. https://link.aps.org/doi/10.1103/PhysRevA.51.2738.

Shannon, C. E. 1949. “Communication theory of secrecy systems”. *The Bell System Technical Journal* 28 (4): 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.

Shor, P. 1994. “Algorithms for quantum computation: discrete logarithms and factoring”. In *Proceedings 35th Annual Symposium on Foundations of Computer Science,* 124–134. https://doi.org/10.1109/SFCS.1994.365700.

Singh, A. K., and A. K. Misra. 2012. “Analysis of Cryptographically Replay Attacks and Its Mitigation Mechanism”. In *Proceedings of the International Conference on Information Systems Design and Intelligent Applications 2012 (INDIA 2012) held in Visakhapatnam, India, January 2012,* edited by S. C. Satapathy, P. S. Avadhani and A. Abraham, 787–794. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-27443-5.

Sreekumar, L., and P. Ramesh. 2016. “Selection of an Optimum Entropy Source Design for a True Random Number Generator”. *Procedia Technology* 25 (December): 598–605. https://doi.org/10.1016/j.protcy.2016.08.150.

Sullivan, B. 2009. “Cryptographic Agility”. *Security Briefs - Microsoft* (August). https://docs.microsoft.com/en-us/archive/msdn-magazine/2009/august/cryptographic-agility.

Tessler, L., and T. Byrnes. 2018. *Bitcoin and quantum computing.* arXiv: 1711.04235 [quant-ph].

Turan, M. S., E. Barker, J. Kelsey, K. A. McKay, M. L.Baish and M. Boyle. 2018. “Recommendation for the Entropy Sources Used for Random Bit Generation”. *NIST Special Publication 800-90B* (January). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf.

Wallden, P., and E. Kashefi. 2019. “Cyber Security in the Quantum Era”. *Commun. ACM* (New York, NY, USA) 62, no. 4 (March): 120. ISSN: 0001-0782. https://doi.org/10.1145/3241037. https://doi.org/10.1145/3241037.

Wang, J., J. Pan and X. Wu. 2019. “The entropy source of pseudo random number generators: from low entropy to high entropy”. In *2019 IEEE International Conference on Intelligence and Security Informatics (ISI),* 161–163. https://doi.org/10.1109/ISI.2019.8823457.

Wayne, M. A. 2017. “Optical quantum random number generation: applications of single-photon event timing”. 71. http://hdl.handle.net/2142/97316.

Wootters, W. K., and W. H. Zurek. 2009. “The no-cloning theorem”. *Physics Today* 62 (2): 76–77.

Xu, F., X. Ma, Q. Zhang, H.-K. Lo and J.-W. Pan. 2020. “Secure quantum key distribution with realistic devices”. *Rev. Mod. Phys.* 92 (2). https://doi.org/10.1103/RevModPhys.92.025002. https://link.aps.org/doi/10.1103/RevModPhys.92.025002.

Xu, F., B. Qi, X. Ma, H. Xu, H. Zheng and H.-K. Lo. 2012. “Ultrafast quantum random number generation based on quantum phase fluctuations”. *Opt. Express* 20, no. 11 (May). https://doi.org/10.1364/OE.20.012366. http://www.opticsexpress.org/abstract.cfm?URI=oe-20-11-12366.

Papers published in the 'Markets, Infrastructures, Payment Systems' series

n. 1 TIPS - TARGET Instant Payment Settlement – The Pan-European Infrastructure for the Settlement of Instant Paymentsi, *by Massimiliano Renzetti, Serena Bernardini, Giuseppe Marino, Luca Mibelli, Laura Ricciardi and Giovanni M. Sabelli* (Institutional Issues)

n. 2 Real-Time Gross Settlement systems: breaking the wall of scalability and high availability, *by Mauro Arcese, Domenico Di Giulio and Vitangelo Lasorella* (Research Papers)

n. 3 Green Bonds: the Sovereign Issuers' Perspective, *by Raffaele Doronzo, Vittorio Siracusa and Stefano Antonelli* (Research Papers)

n. 4 T2S - TARGET2-Securities – The pan-European platform for the settlement of securities in central bank money, *by Cristina Mastropasqua, Alessandro Intonti, Michael Jennings, Clara Mandolini, Massimo Maniero, Stefano Vespucci and Diego Toma* (Institutional Issues)

n. 5 The carbon footprint of the Target Instant Payment Settlement (TIPS) system: a comparative analysis with Bitcoin and other infrastructures, *by Pietro Tiberi* (Research Papers)

n. 6 Proposal for a common categorisation of IT incidents, *by Autorité de Contrôle Prudentiel et de Résolution, Banca d'Italia, Commissione Nazionale per le Società e la Borsa, Deutsche Bundesbank, European Central Bank, Federal Reserve Board, Financial Conduct Authority, Ministero dell'Economia e delle Finanze, Prudential Regulation Authority, U.S. Treasury* (Institutional Issues)

n. 7 Inside the black box: tools for understanding cash circulation, *by Luca Baldo, Elisa Bonifacio, Marco Brandi, Michelina Lo Russo, Gianluca Maddaloni, Andrea Nobili, Giorgia Rocco, Gabriele Sene and Massimo Valentini* (Research Papers)

n. 8 The impact of the pandemic on the use of payment instruments in Italy, *by Guerino Ardizzi, Alessandro Gambini, Andrea Nobili, Emanuele Pimpini and Giorgia Rocco* (Research Papers) (in Italian)

n. 9 TARGET2 – The European system for large-value payments settlement, *by Paolo Bramini, Matteo Coletti, Francesco Di Stasio, Pierfrancesco Molina, Vittorio Schina and Massimo Valentini* (Institutional Issues) (in Italian)

n. 10 A digital euro: a contribution to the discussion on technical design choices, *by Emanuele Urbinati, Alessia Belsito, Daniele Cani, Angela Caporrini, Marco Capotosto, Simone Folino, Giuseppe Galano, Giancarlo Goretti, Gabriele Marcelli, Pietro Tiberi and Alessia Vita* (Institutional Issues)

n. 11 From SMP to PEPP: a further look at the risk endogeneity of the Central Bank, *by Marco Fruzzetti, Giulio Gariano, Gerardo Palazzo and Antonio Scalia* (Research Papers)

n. 12 TLTROs and collateral availability in Italy, *by Annino Agnes, Paola Antilici and Gianluca Mosconi* (Research Papers) (in Italian)

n. 13 Overview of central banks' in-house credit assessment systems in the euro area, *by* L*aura Auria, Markus Bingmer, Carlos Mateo Caicedo Graciano, Clémence Charavel, Sergio Gavilá, Alessandra Iannamorelli, Aviram Levy, Alfredo Maldonado, Florian Resch, Anna Maria Rossi and Stephan Sauer* (Institutional Issues)

n. 14 The strategic allocation and sustainability of central banks' investment, *by Davide Di Zio, Marco Fanari, Simone Letta, Tommaso Perez and Giovanni Secondin* (Research Papers) (in Italian)

n. 15 Climate and environmental risks: measuring the exposure of investments, *by Ivan Faiella*, *Enrico Bernardini*, *Johnny Di Giampaolo*, *Marco Fruzzetti*, *Simone Letta, Raffaele Loffredo and Davide Nasti* (Research Papers)

n. 16 Cross-Currency Settlement of Instant Payments in a Multi-Currency Clearing and Settlement Mechanism, *by Massimiliano Renzetti*, *Fabrizio Dinacci and Ann Börestam* (Research Papers)

n. 17 What's ahead for euro money market benchmarks?, *by Daniela Della Gatta* (Institutional Issues) (in Italian)

n. 18 Cyber resilience per la continuità di servizio del sistema finanziario, *by Boris Giannetto and Antonino Fazio* (Institutional Issues) (in Italian)

n. 19 Cross-Currency Settlement of Instant Payments in a Cross-Platform Context: a Proof of Concept, *by Massimiliano Renzetti, Andrea Dimartina, Riccardo Mancini, Giovanni Sabelli, Francesco Di Stasio, Carlo Palmers, Faisal Alhijawi, Erol Kaya, Christophe Piccarelle, Stuart Butler, Jwallant Vasani, Giancarlo Esposito, Alberto Tiberino and Manfredi Caracausi* (Research Papers)

n. 20 Flash crashes on sovereign bond markets – EU evidence, *by Antoine Bouveret, Martin Haferkorn, Gaetano Marseglia and Onofrio Panzarino* (Research Papers)

n. 21 Report on the payment attitudes of consumers in Italy: results from ECB surveys, *by Gabriele Coletti, Alberto Di Iorio, Emanuele Pimpini and Giorgia Rocco* (Institutional Issues)

n. 22 When financial innovation and sustainable finance meet: Sustainability-Linked Bonds, *by Paola Antilici, Gianluca Mosconi and Luigi Russo* (Institutional Issues) (in Italian)

n. 23 Business models and pricing strategies in the market for ATM withdrawals, *by Guerino Ardizzi and Massimiliano Cologgi* (Research Papers)

n. 24 Press news and social media in credit risk assessment: the experience of Banca d'Italia's In-house Credit Assessment System, *by Giulio Gariano and Gianluca Viggiano* (Research Papers)

n. 25 The bonfire of banknotes, *by Michele Manna* (Research Papers)

n. 26 Integrating DLTs with market infrastructures: analysis and proof-of-concept for secure DvP between TIPS and DLT platforms, *by Rosario La Rocca, Riccardo Mancini, Marco Benedetti, Matteo Caruso, Stefano Cossu, Giuseppe Galano, Simone Mancini, Gabriele Marcelli, Piero Martella, Matteo Nardelli and Ciro Oliviero* (Research Papers)

n. 27 Statistical and forecasting use of electronic payment transactions: collaboration between Bank of Italy and Istat, *by* Guerino Ardizzi and Alessandra Righi (Institutional Issues) (in Italian)

n. 28 TIPS: a zero-downtime platform powered *by* automation, by *Gianluca Caricato, Marco Capotosto, Silvio Orsini and Pietro Tiberi* (Research Papers)

n. 29 TARGET2 analytical tools for regulatory compliance, *by Marc Glowka, Alexander Müller, Livia Polo Friz, Sara Testi, Massimo Valentini and Stefano Vespucci* (Institutional Issues)

n. 30 The security of retail payment instruments: evidence from supervisory data, *by Massimiliano Cologgi* (Research Papers)

n. 31 Open Banking in the payment system: infrastructural evolution, innovation and security, supervisory and oversight practices, *by Roberto Pellitteri, Ravenio Parrini, Carlo Cafarotti and Benedetto Andrea De Vendictis* (Institutional Issues) (in Italian)

n. 32 Banks' liquidity transformation rate: determinants and impact on lending, *by Raffaele Lenzi, Stefano Nobili, Filippo Perazzoli and Rosario Romeo* (Research Papers)

n. 33 Investor behavior under market stress: evidence from the Italian sovereign bond market, *by Onofrio Panzarino* (Research Papers)

n. 34 Siamese neural networks for detecting banknote printing defects, *by Katia Boria, Andrea Luciani, Sabina Marchetti and Marco Viticoli* (Research Papers) (in Italian)