

Quantum Cryptography

TechReport

Physics-based encryption, the shift to post-quantum standards, and what the transition means for digital trust in Latin America and the Caribbean.



Copyright © 2026 Inter-American Development Bank (IDB). This work is subject to a Creative Commons Attribution 4.0 International Public License CC BY 4.0 (<https://creativecommons.org/licenses/by/4.0/legalcode>). The terms and conditions indicated in the URL link must be met and the respective recognition must be granted to the IDB.

Any and all disputes arising under this license that cannot be settled amicably shall be resolved in accordance with the following procedure. Pursuant to a notice of mediation communicated by reasonable means by either you or the licensor to the other, the dispute shall be submitted to non-binding mediation conducted in accordance with the World Intellectual Property Organization (WIPO) Mediation Rules. Any dispute that cannot be settled amicably shall be submitted to arbitration pursuant to the United Nations Commission on International Trade Law (UNCITRAL) rules. The use of the IDB name for any purpose other than the respective recognition and the use of the IDB logo are not authorized by this license and require an additional license agreement.

Note that the URL link includes terms and conditions that are an integral part of this license.

The opinions expressed in the work are those of its authors and do not necessarily reflect the views of the IDB, its Board of Executive Directors, or the countries they represent.



AUTHORS AND COLLABORATORS

TechReports are an initiative of Techlab, the Emerging Technologies Laboratory of the Inter-American Development Bank's (IDB) Technology and Transformation Department. TechLab is responsible for exploring, experimenting with, and disseminating information on new technologies to understand their impact on the IDB Group and the Latin American and Caribbean region.

AUTHORS

Belén Girardo

Fernando Puerto Mendoza

COLLABORATORS

Ignacio Cerrato

Daniel Gammell Ibañez

SUPERVISOR

Mariana Gutiérrez

CONTENTS

1. Executive Summary	7
2. Introduction: Why Cryptography Matters Now More Than Ever	10
2.1 The Role of Cryptography in Global Digital Infrastructure.....	10
2.2 Quantum Computing as a Turning Point	11
2.3 Urgency for the Region: Vulnerabilities and Opportunities for Latin America and the Caribbean.....	11
3. Conceptual Framework: One Field, Two Responses.....	14
3.1 Classical Cryptography.....	14
3.2 Quantum Cryptography	14
3.3 Post-Quantum Cryptography.....	15
3.4 Glossary of Key Terms.....	16
4. Quantum Cryptography: Foundations and Protocols.....	19
4.1 Basic Physical Principles: Superposition, Entanglement, and the "No-Cloning Theorem"	19
4.2 Quantum Key Distribution (QKD).....	20
4.3 Quantum Random Number Generation (QRNG)	21
4.4 Quantum Position Verification (QPV) and Authentication	22
4.5 Homomorphic Encryption and the Blind Quantum Protocol	22
4.6 Current State of Technological Maturity.....	24
5. The Quantum Threat to Existing Digital Security	27
5.1 Why Quantum Computers Break RSA and Public-Key Encryption.....	27
5.2 Shor's Algorithm: The Mechanics of the Threat	27
5.3 "Store Now, Decrypt Later": The Threat That Is Already Active	28
5.4 Time Horizon: When Does the Risk Become Real?	30
6. Sectoral Applications.....	32
6.1 Financial Sector and Central Banking	32
6.2 Government and Public Administration	32
6.3 Health	32
6.4 Critical Infrastructure and Energy	33

6.5 Supply Chains and Foreign Trade	33
7. Recommendations	36
7.1 The Mosca Theorem	36
7.2 Recommendations for Governments and Institutions in the Region	37
7.3 Multilateral Actors and the IDB's Institutional Position	38
7.3.1 <i>Corporate Technology at the IDB</i>	39
8. Conclusion	42
9. References	44

CHAPTER

1

Executive Summary

1. Executive Summary

Cryptography underpins much of the infrastructure that every digital system in the world - including countries in Latin America and the Caribbean - depends on today: bank transfers, government communications, electronic health records, and global supply chains, among others. Each of these processes rely on public-key encryption schemes that have protected digital trust for more than four decades.

That balance is about to be challenged; the advance of quantum computing threatens to render those same schemes vulnerable. According to available estimates, that scenario could materialize within five to twenty years (Veritasium, 2023).

The risk, however, is not only in the future. Various actors, with sufficient technical capacity and resources, are already intercepting and storing encrypted information; betting on being able to decrypt it once a sufficiently powerful quantum computer exists. Every year that passes without a migration toward resistant encryption schemes widens the volume of information that is protected today but will be exposed once that threat materializes.

This report presents quantum cryptography, which uses principles of physics such as superposition, entanglement, and the no-cloning theorem to protect information and detect any interception attempt through protocols such as quantum key distribution (QKD). It also introduces the notion of post-quantum cryptography as the roadmap to follow.

The report then applies this conceptual framework to the sectors where migration to quantum cryptography is most urgent and examines its ethical and governance implications: the irreversibility of data already exposed under the logic of *Store Now, Decrypt Later* (SNDL), the risks of state surveillance empowered by quantum decryption capabilities, and the dilemmas raised by a technological transition whose development is today concentrated in a small number of countries.

For Latin America and the Caribbean, this report's message is twofold. On one hand, the region faces a structural risk: it does not lead the development of quantum hardware or the definition of the new post-quantum standards, which exposes it to external dependence on decisions that will affect the security of its most sensitive information. On the other, the early stage of the global standardization and migration process represents a concrete opportunity for influence: to actively participate in the cryptographic agility and data governance processes that are being defined today, rather than passively adopting their outcomes.



5–20 YEARS

estimated horizon until a
quantum computer can
break RSA



OVER 20×

fewer qubits now needed to
break RSA-2048 than
estimated in 2019



2030 / 2035

NSA deadlines to migrate to
quantum-resistant
algorithms



26 > 12

Mosca theorem, regional
example — the risk is
already present

CHAPTER

2

Introduction

2. Introduction: Why Cryptography Matters Now More Than Ever

2.1 The Role of Cryptography in Global Digital Infrastructure

Cryptography constitutes, to a large extent, the invisible infrastructure on which the contemporary digital economy rests. Every bank transfer, every official communication between government agencies, every clinical record stored on a server, and every transaction within a global supply chain depends on mathematical mechanisms that ensure information travels and is stored without being intercepted, read, or altered by unauthorized third parties. This dependence is not a recent phenomenon. For much of the twentieth century, protecting a message required the sender and receiver to have previously shared, in person, the same secret key (a scheme known as symmetric cryptography), which proved impracticable at the scale and speed demanded by information exchange in an interconnected world.

The solution arrived in 1977, when researchers Ronald Rivest, Adi Shamir, and Leonard Adleman proposed a scheme bearing their last name initials: RSA. Their innovation consisted of separating the key used to encrypt from the key used to decrypt – an approach known as asymmetric or public-key cryptography – so that anyone could send an encrypted message to a recipient without having to previously agree on a shared key.

The scheme relies on computational asymmetry: it is simple to multiply two very large prime numbers to obtain a public key, but it is extraordinarily difficult, for any classical computer, to reverse that operation and discover the two original primes. In the case of RSA-2048, the current security standard, the resulting number has around 617 digits, and factoring it using the best known classical algorithm would require, according to estimates, hundreds of trillions of years. The digital trust of the last four decades was built on that seemingly unbreakable asymmetry (Veritasium, 2023).

617 digits

the length of an RSA-2048 modulus
— factoring it classically would take
hundreds of trillions of years

2.2 Quantum Computing as a Turning Point

That balance, however, was not designed to withstand a fundamentally different kind of computer. While a classical bit can only represent one value (zero or one) at a given moment, a qubit can exist in a superposition of both states simultaneously. This property has a considerable practical consequence: a system of just a few qubits can already represent and operate on multiple values at once, and that number of states grows exponentially with each additional qubit. Twenty qubits alone are enough to represent more than a million simultaneous states.

That parallel-computing capacity does not make quantum computers superior for every task — in fact, extracting useful information from a superposition remains, in general, extraordinarily difficult. But in 1994 researcher Peter Shor identified that one of the few problems where this quantum parallelism offers a decisive advantage is the factoring of large numbers: the very mathematical problem on which RSA's security rests. Since then, the challenge has stopped being purely theoretical.

Estimates of the quantum resources needed to break RSA-2048 have fallen drastically as algorithms and error-correction techniques have advanced. In 2019, factoring an RSA-2048 key was estimated to require around 20 million noisy physical qubits. Six years later, a revision by Craig Gidney, a researcher at Google Quantum AI, cut that figure to under a million qubits — a reduction of more than twenty-fold relative to the previous estimate (Gidney, 2025). Although today's quantum computers are still far from reaching that scale, the speed at which the required resources keep shrinking reinforces the urgency of moving toward cryptographic systems resistant to quantum computing.

That urgency already translates into concrete timelines. The U.S. National Institute of Standards and Technology (NIST) recommends beginning the transition before vulnerable algorithms are withdrawn from its standards around 2035. For its part, the U.S. National Security Agency (NSA), set 2030 as a milestone for migrating national security systems to quantum-resistant algorithms through its Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) standard. These timelines show that the transition is no longer conceived as a response to a distant threat, but as a technological and regulatory process that is already underway and that will also affect countries and organizations that depend on the standards, vendors, and infrastructure of their main international partners.

2.3 Urgency for the Region: Vulnerabilities and Opportunities for Latin America and the Caribbean

Given this outlook, the question for Latin America and the Caribbean (LAC) is not only technical, but one of timing and priorities. The region faces a finite window to migrate the critical systems of the financial, government, health, and infrastructure sectors toward quantum-resistant schemes, before quantum computing reaches the maturity needed to break the public-key encryption that protects those same infrastructures today. That window is further narrowed by an already active

phenomenon: the practice of intercepting and storing encrypted information today in the expectation of decrypting it in the future, once sufficiently powerful quantum hardware exists.

Simultaneously, that same early stage — in which cryptographic agility processes and data governance frameworks are only just beginning to be defined globally — represents a concrete opportunity for the region's countries to participate, insofar as it is still possible, and influence how those processes are designed and implemented, rather than simply adopting them once they are settled.

CHAPTER

3

Conceptual Framework

3. Conceptual Framework: One Field, Two Responses

3.1 Classical Cryptography

To understand why quantum computing generates so much concern, it is useful to draw a precise distinction between the two paradigms that today compete to become the response to that threat, and to first contrast them with the paradigm they seek to replace: classical cryptography.

As described in the previous section, public-key cryptography (the dominant standard since the late 1970s) does not hide the key used to encrypt a message but rather makes it public and bases its security on the practical difficulty of solving a specific mathematical problem, such as the factoring of large prime numbers in the case of RSA.

The difficulty is not absolute: it is a computational difficulty, meaning it depends on the computing power available to attempt to solve it by brute force or through more sophisticated algorithms. As long as that power was limited to classical computers, the security margin — 16 million years to factor a typical key — proved more than sufficient. The underlying limitation of classical cryptography is not conceptual but temporal: its security is only as solid as the gap between the difficulty of the underlying mathematical problem and the computing capacity available to attack it. It is that gap which quantum computing threatens to close.

3.2 Quantum Cryptography

The first paradigm, quantum cryptography, does not seek to replace classical cryptography's mathematical problem with a harder one, but rather to change the foundation of security entirely: instead of relying on assumptions about computational difficulty, it relies on the laws of quantum physics.

It uses devices capable of generating, transmitting, and registering individual particles (typically photons) to encode information, drawing on two central properties of quantum mechanics: *superposition*, which allows a particle to exist in more than one state at a time until the moment it is measured, and *entanglement*, which links the state of two particles such that measuring one instantly determines the state of the other, regardless of the distance separating them (NIST, 2025).

Among the practical applications of these principles, the most established is quantum key distribution (QKD), examined in detail in Chapter 4, in QKD, the encryption key is transmitted not through classical bits but through photons, while the very act of measuring a photon to intercept it irreversibly alters its state, revealing the intrusion to both sender and receiver. This property, known as the *no-cloning theorem*, is what distinguishes quantum cryptography from any classical

scheme: a classical attacker can copy bits without being detected, whereas a quantum attacker, in attempting to copy or measure a qubit, necessarily alters it and leaves evidence of the attempt.

3.3 Post-Quantum Cryptography

The second paradigm, post-quantum cryptography (PQC), starts from a different premise: it does not require quantum hardware or specialized photonic infrastructure, but instead consists of designing new mathematical algorithms that run on conventional classical computers, whose security does not depend on problems that a quantum algorithm can solve efficiently.

Most of these algorithms are based on lattice mathematics: geometric structures formed by integer combinations of a set of vectors, in which finding the lattice point closest to an arbitrary point is a manageable problem in a few dimensions, but becomes extraordinarily difficult to solve — even for the most powerful computers — when the lattice is defined on the order of a thousand dimensions, as is the case in the proposed encryption schemes.

Aware of the urgency of having validated alternatives before the quantum threat becomes operational, NIST structured a formal, multi-stage evaluation process. After several years of scrutiny, during which a significant number of the initial proposals were broken, NIST announced in July 2022 the selection of four algorithms as its new post-quantum model, constituting the new global standard and marking the formal starting point of the global migration toward this security paradigm (NIST, 2025).

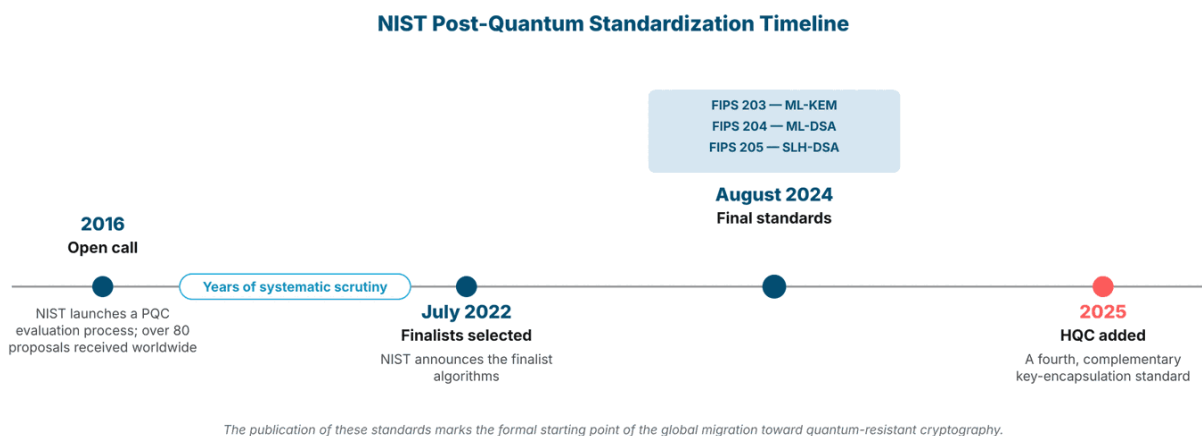


Figure 1. Timeline of NIST's post-quantum cryptography standardization process: from the 2016 open call for proposals to the 2025 addition of HQC as a fourth post-quantum standard.

The publication of this set of standards is not just a technical milestone: it represents the formal starting point of the global migration of cryptographic infrastructure toward schemes designed to withstand quantum computing (NIST, 2025).

3.4 Glossary of Key Terms

To facilitate reading the rest of this report, the central technical terms introduced so far are summarized below.

Term	Definition
Qubit	the basic unit of quantum information. Unlike a classical bit, which can only take the value 0 or 1, a qubit can exist in a superposition of both values simultaneously.
Superposition	the property by which a quantum particle (a photon, an atom, an electron) can be in two or more states at once, until it is measured or observed, at which point the state "collapses" into a single one of the possible values.
Entanglement	the phenomenon by which two or more quantum particles become linked such that measuring the state of one instantly determines the state of the other, even if they are physically far apart.
No-cloning theorem	the principle that it is impossible to copy the state of a qubit without altering it, which makes it possible to detect any interception attempt on a quantum communication channel.
Quantum Key Distribution (QKD)	a protocol that uses quantum particles, generally photons, to transmit an encryption key between two parties, such that any interception attempt is detectable.
Lattice	a mathematical structure made up of all points reachable through integer combinations of a set of vectors; its high-dimensional version forms the basis of the post-quantum algorithms now standardized by NIST.
Shor's algorithm	a quantum algorithm developed in 1994 by Peter Shor and Don Coppersmith, capable of factoring large numbers exponentially faster than the best known classical algorithms, which represents the principal quantum threat to RSA encryption.

**Store now, decrypt later
(SNDL)**

the practice by which state or non-state actors intercept and store encrypted information today, betting on being able to decrypt it in the future once a sufficiently powerful quantum computer exists.

CHAPTER

4

Foundations and Protocols

4. Quantum Cryptography: Foundations and Protocols

4.1 Basic Physical Principles: Superposition, Entanglement, and the "No-Cloning Theorem"

Before detailing the quantum protocols applied to information security, it is worth clarifying how the two phenomena mentioned in the previous chapter operate in practice. Superposition can be observed, for example, in a photon passing through a polarizing filter: before striking the filter, the photon exists in a simultaneous combination of horizontal and vertical polarization, and only upon interacting with the material does it "decide" on one of the two states. That collision with the filter — whether physical, or, in a communication channel, triggered by an interception attempt — collapses the superposition and makes it difficult for an intruder to reconstruct the original state without being detected (NIST, 2025).

That same principle helps illustrate the difference between the quantum world and everyday intuition. In the thought experiment of Schrödinger's cat, a cat sealed in a box is, in a strictly quantum sense, simultaneously alive and dead until the box is opened and someone observes it: it is the act of observation that forces the system to "decide" on one of the two possible states. Entanglement takes that same logic one step further, as illustrated in Box 4.1, and it is this, together with the no-cloning theorem, that makes it possible to build communication channels in which any attempt at copying or interception leaves a detectable trace.

Box 4.1 — The Glove Analogy

To understand entanglement without resorting to quantum mathematics, a simple example is useful. If a person has two gloves, one black and one white, kept in a box, and pulls one out, it is unsurprising that, upon finding it is white, the one remaining in the box must be black: the information was already fixed beforehand.

The difference from the classical case is not one of degree: there, the outcome was already determined before opening the box; in the quantum case, neither glove had a defined color until the instant of measurement. The value of entanglement for cryptography, then, does not lie in the possibility of communicating faster, but in the existence of correlations that cannot be reproduced or copied without disturbing the system. Any attempt by a third party to intercept or measure the particles alters those correlations and can reveal the intrusion.

4.2 Quantum Key Distribution (QKD)

As noted in Chapter 3, the most established protocol built on these principles is quantum key distribution. In its simplest form, two parties exchange a sequence of photons whose polarization encodes the bits of an encryption key; since any attempt to measure those photons alters their state, a third party attempting to intercept the transmission introduces detectable errors, allowing the compromised key to be discarded before it is used.

The protocol's most cited use case, documented since 2004, was its use to secure a funds transfer between an Austrian bank and the city government of Vienna (NIST, 2025). Its main practical limitation is distance: photon absorption in optical fiber reduces the key-generation rate as the distance grows, and that loss cannot be compensated by copying and amplifying the signal, because the no-cloning theorem prevents it. To overcome this, researchers are investigating "quantum repeaters," devices that distribute and exchange entanglement across short fiber segments to build a longer-range secure connection.

The most advanced alternative approach to date sidesteps the fiber problem by moving the channel into space. Unlike the terrestrial medium, the free atmosphere above its dense layer attenuates photons much more gently, making it possible to maintain viable transmission rates over distances that would be inaccessible to any cable. China has led this path since 2016, when it launched *Micius*, the world's first quantum communications satellite. In 2021, scientists at the University of Science and Technology of China published the results of the first integrated intercontinental-scale quantum communication network in *Nature* magazine: an infrastructure combining more than 700 terrestrial optical fibers with two links to the Micius satellite, covering 4,600 kilometers in total and serving more than 150 institutional users, including state banks, municipal power grids, and government agencies.

It is worth noting that in this architecture the satellite operates as a trusted node — that is, it manages the keys in transit — which shifts part of the security requirement onto the integrity of the satellite itself; ongoing research aims to replace this model with direct entanglement distribution, which would eliminate that dependency (Chen et al., 2021).



4,600 km

span of the first integrated
intercontinental quantum
communication network, serving
150+ institutions

The practical application of these principles, however, faces limitations that are far from trivial. No instrument is perfect: there are no detectors capable of registering absolutely every photon that reaches them, nor light sources that, without exception, emit a single photon per pulse, which introduces false negatives and false positives that must be kept to a minimum for the resulting key to be reliable. Standards developing organizations such as NIST have concentrated much of their research on building single-photon detectors capable of operating at temperatures near absolute zero, minimizing noise and improving detection accuracy.

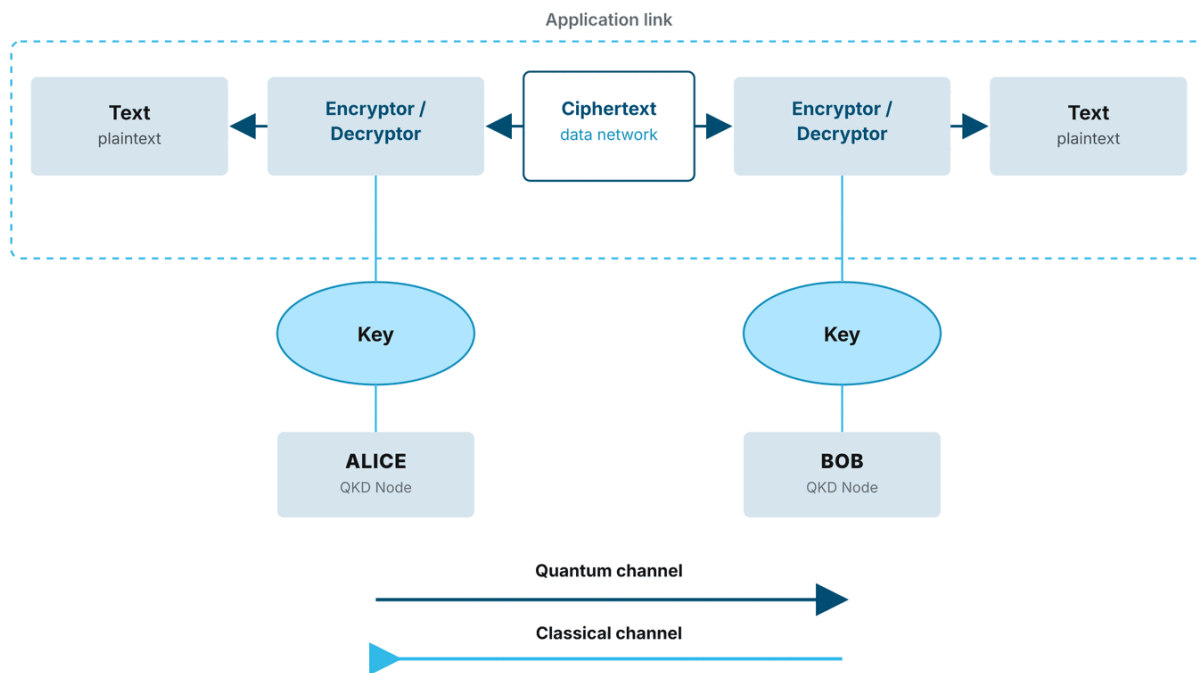


Figure 2. How quantum key distribution (QKD) works: the exchange between Alice and Bob, the role of the photon, the no-cloning theorem as an intrusion-detection mechanism, and the generation of the secure key.

These imperfections also open up a specific avenue of attack. Because manufacturing tolerances generate small variations in each instrument detection window, an attacker can intercept a photon, measure it, and resend the receiver a "fake state" calibrated to exploit those variations, avoiding detection. Fully closing this class of vulnerabilities requires more sophisticated protocols, known as "device-independent," whose security does not depend on the physical properties of the particular hardware running them, but on the correlations observed in the results (Durr-E-Shahwar et al., 2024).

4.3 Quantum Random Number Generation (QRNG)

A second relevant protocol is quantum random number generation (QRNG), which addresses a not-very-visible weakness in digital security: a large share of encryption keys are built from

numbers presumed to be random, in an operation repeated hundreds of billions of times a day, but which is rarely random in an absolute sense.

A coin toss, for example, may seem unpredictable, even though in theory its outcome could be anticipated if its physical trajectory were known with precision; similarly, software-based random number generators typically start from a seed value that, although difficult to deduce, is not entirely unpredictable.

Quantum physics, by contrast, offers a source of genuine randomness: the exact instant a radioactive atom decays, or the path a photon takes through a system of lenses and optical components, are phenomena that no physical model can predict. NIST researchers have built generators that translate this behavior into reliable sequences of zeros and ones, now used to feed public randomness mechanisms employed in secure multi-party computing applications.

4.4 Quantum Position Verification (QPV) and Authentication

A third, still experimental development is quantum position verification, which seeks to solve a different problem: not protecting the content of a message but confirming that its sender or recipient is actually located where they claim to be, by requiring the recipient to manipulate qubits in a way that is only possible from that physical position.

An illustrative case helps size the problem: if a diplomat needs to send a confidential message to her home country, she will want certainty that the server she is communicating with is actually located in the territory it claims to represent, and not at a spoofed location. Researchers at the Joint Center for Quantum Information and Computer Science are currently studying how to bring this type of verification into real-world applications, although the protocol has not yet been deployed outside an experimental setting.

QPV, however, only verifies where a party is, not who they are; for full identity authentication, the literature proposes combining this mechanism with conventional digital certificates, so that quantum cryptography complements, rather than replaces, the existing public-key infrastructure.

4.5 Homomorphic Encryption and the Blind Quantum Protocol

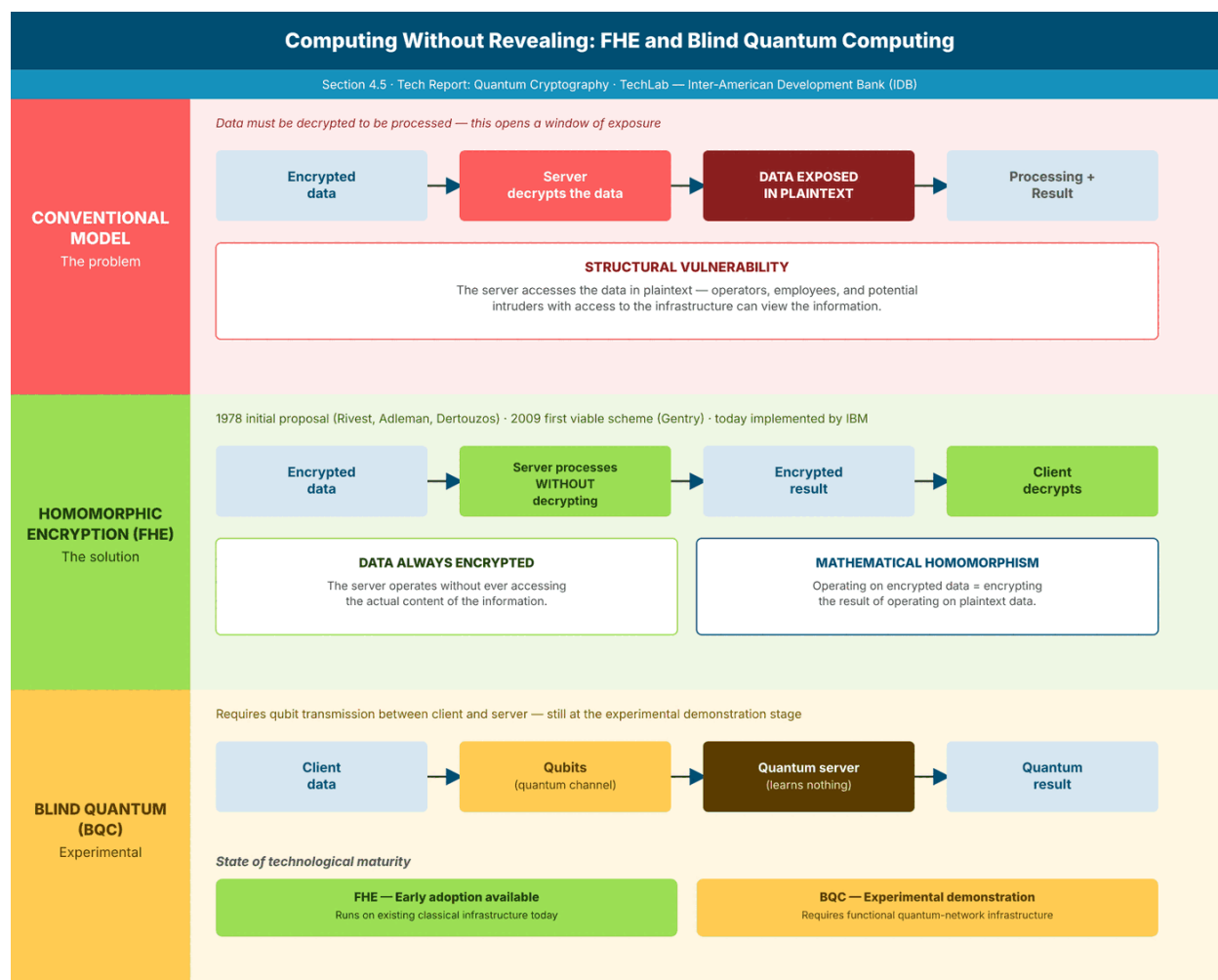
A fourth development in the field of cryptography addresses a different problem from that of communication: protecting data while it is being processed. The typical situation is that of an organization that needs to process large volumes of sensitive information on external infrastructure, whether for computing capacity or cloud economies of scale. Encryption protects that data in transit and at rest, but most current systems require it to be decrypted at the moment of computation, creating a window of exposure that affects both the confidentiality and the integrity of the information. It is in that interval that a structural vulnerability lies, one that the conventional cloud model has not yet resolved.

The most mature response to that challenge is *fully homomorphic encryption* (FHE): a scheme that allows mathematical operations to be performed directly on encrypted data, without ever decrypting it and without the party running the computation accessing the content of the information. The result returned by the external server is, in turn, an encrypted value that only the key holder can interpret. The logic that makes this possible rests on the concept of mathematical homomorphism: if a function F transforms elements of one set into another while preserving its algebraic structure, then operating on the transformed data produces the same result as operating first and transforming afterward. In concrete terms: adding two homomorphically encrypted numbers produces the same encrypted result as adding the plaintext numbers and then encrypting the sum. That property allows a third party to operate on information it never actually knew.

The idea was first formulated in 1978 by Ronald Rivest, Leonard Adleman, and Michael Dertouzos — the same Rivest and Adleman who, a year earlier, had published the RSA algorithm — but its feasibility remained unproven for three decades. It was Craig Gentry who, in 2009, established the mathematical foundations for building an FHE scheme that was simultaneously secure and computationally realizable. FHE is now a real, deployed technology: companies such as IBM have incorporated it into zero-trust architectures, where data remains encrypted throughout the entire processing cycle, including operations in untrusted cloud environments. Its main limitation remains computational cost, since homomorphic operations are orders of magnitude more resource-intensive than their equivalent on plaintext data, which restricts its adoption to use cases where the protection of the data justifies that overhead.

This is where the intersection with quantum computing arises, although it must be stated precisely: there is no consolidated evidence today that available or medium-term quantum computers offer a clear practical advantage in accelerating the algorithms underlying FHE. Some researchers are exploring whether certain mathematical operations on lattices, the basis of modern FHE schemes, could benefit from quantum algorithms, but that line of inquiry remains an open research question. What has been demonstrated is the reverse direction: because FHE is grounded in problems such as Learning With Errors, considered resistant to quantum computer attacks, this technology is itself part of the family of post-quantum solutions and does not need to be replaced in the face of the threat that quantum computing poses to classical encryption.

Running parallel to FHE and conceptually related, the quantum field has developed the *blind quantum computing* (BQC) protocol, in which a client delegates processing to a quantum server without the server learning anything about the task or the data it handles. Unlike FHE, which operates on classical data over conventional infrastructure, BQC requires the transmission of qubits between parties and is directly tied to the development of functional quantum networks. Both protocols share the same goal — computing on what cannot be seen — but from radically different architectures and stages of maturity: FHE is a technology in early adoption, while BQC is a protocol still at the experimental demonstration stage.



Source: TechLab — Inter-American Development Bank (IDB) · Tech Report: Quantum Cryptography

Figure 3. Fully homomorphic encryption (FHE) and blind quantum computing (BQC): two protocols for computing on data without exposing it, compared by architecture and stage of maturity.

4.6 Current State of Technological Maturity

Ranked by their degree of maturity, the protocols described in this chapter occupy different positions: QKD is the most advanced, with pilot implementations documented since 2004; QRNG is at a more consolidated stage of adoption, already integrated into public randomness mechanisms; while QPV and BQC remain, for now, in predominantly experimental or academic-research phases. The specialized literature describes quantum cryptography as a whole as a technology "under development" that must overcome systematically identified obstacles — such as unintended polarization drift, limited transmission distances, and constraints on key-generation rates as the distance traveled increases — before achieving adoption comparable to that of classical cryptography (Durr-E-Shahwar et al., 2024).

On the general pace of progress in quantum computing, the perspective of Aram Harrow is illustrative — an MIT researcher with 25 years in the field and co-developer of the HHL algorithm in 2008, one of the first demonstrations of an exponential advantage of quantum computers over classical ones. Harrow acknowledges having been, in his own words, "too pessimistic" in systematically estimating ten-to-fifteen-year horizons, and now argues that it is worth preparing for the emergence, on a shorter timeline, of thousand-qubit quantum computers capable of performing tasks impossible for today's computers — which he considers the true starting point of useful quantum computing (El País, 2026).

CHAPTER

5

The Quantum Threat

5. The Quantum Threat to Existing Digital Security

5.1 Why Quantum Computers Break RSA and Public-Key Encryption

The reason a sufficiently powerful quantum computer would put RSA encryption, and public-key cryptography in general, at risk lies in how it processes information. A classical computer with two bits can only represent, at a given instant, one of four possible values; a quantum computer with two qubits can represent all four simultaneously, and that number of states doubles with each additional qubit. That property alone does not turn a quantum computer into a universally faster tool: reading a superposition requires measuring it, and every measurement collapses the result to a single value chosen essentially at random, destroying the rest of the information contained in the other states (Veritasium, 2023).

Exploiting that advantage therefore requires algorithms capable of manipulating the superposition in such a way that, upon measurement, precisely the sought-after information is obtained, and so far only a small number of problems have been identified where this is possible. Factoring large numbers is one of them. Box 5.1 illustrates this logic with a simplified example of parallel computation.

Box 5.1 — Why More Qubits Multiply Computing Power

With two classical bits, it is possible to represent only one of four values at a given time (00, 01, 10, or 11), interpretable as the numbers 0, 1, 2, and 3. To calculate, for example, the result of raising the number 7 to each of those values, a classical computer must repeat the operation four times, once per state.

With two qubits, by contrast, the system can represent all four values simultaneously, so that a single quantum operation produces, in superposition, all four results at once: 7 raised to 0, 1, 2, and 3 — that is, 1, 7, 49, and 343. Each additional qubit doubles the number of representable states: twenty qubits alone are enough for more than a million simultaneous states, and three hundred would, in theory, suffice to represent more states than there are particles in the observable universe.

The catch is that this information can only be extracted through algorithms specifically designed to exploit it; otherwise, measuring the superposition simply yields a random result, and the rest of the information is lost.

5.2 Shor's Algorithm: The Mechanics of the Threat

In 1994, Peter Shor and Don Coppersmith showed how to exploit that advantage through the *quantum Fourier transform*, an operation capable of extracting the frequency of a periodic signal.

Their central idea is to transform the problem of factoring a number n (the product of two primes p and q) into that of finding the period of a sequence: a number g with no common factors with n is chosen, raised to successive powers, and the remainder of dividing each result by n is recorded; those remainders repeat with a periodicity r that, once found via the Fourier transform, makes it possible — if r turns out to be even — to construct two new numbers that share factors with n , which the Euclidean algorithm can then quickly identify as p and q (Veritasium, 2023).

Running this procedure on classical computers offers no speed advantage; what a quantum computer decisively accelerates is, specifically, the step of finding that period r . Box 5.2 reproduces, in simplified form, the arithmetic logic behind this procedure.

Box 5.2 — How Shor's Algorithm Factors a Number: An Example with $n = 77$

Take a number n , the product of two unknown primes, and set $n = 77$ purely to illustrate the method (in a real case, the primes would have hundreds of digits). A number g smaller than n and sharing no common factors with it is chosen — for example, $g = 8$ — and its successive powers are calculated, dividing each result by n and recording only the remainder: 8^1 leaves a remainder of 8; 8^2 leaves 64; 8^3 leaves 50; and so on, until 8^{10} leaves a remainder of exactly 1.

That exponent, 10, is the “period” r that Shor's algorithm can find efficiently via the quantum Fourier transform. Since r is even, it can be used to construct two new numbers: $8^5 + 1 = 32,769$ and $8^5 - 1 = 32,767$, which very likely share factors with n .

Applying the Euclidean algorithm (dividing the larger number by the smaller and repeating the process with the remainder until reaching zero) yields a greatest common divisor of 32,769 and 77 equal to 11, one of the two prime factors of 77; dividing 77 by 11 gives the second, 7. On a classical computer, finding the period r offers no speed advantage; it is precisely that step which a quantum computer solves exponentially faster, and that is where the threat to RSA encryption lies.

Estimates of the physical qubits needed to run the algorithm against real RSA keys have fallen steadily: from one billion in 2012, to 230 million in 2017, and to 20 million in 2019 — illustrating how quickly the gap between theory and an operational threat is closing.

5.3 "Store Now, Decrypt Later": The Threat That Is Already Active

The quantum threat to public-key cryptography is not, however, an entirely future risk. Under the logic known as “store now, decrypt later” (SNDL), state and non-state actors are already intercepting and storing large volumes of encrypted information today, unable to read it in the present but betting on being able to do so once a sufficiently powerful quantum computer exists. The strategy is rational because much of that information will retain its value a decade from now.

The list of typical targets for this practice includes both public and private actors: central banks, intelligence agencies, pharmaceutical companies, and critical-infrastructure operators all handle

information whose sensitivity does not expire in the short term, making them natural targets of SNDL even in the continued absence of a quantum computer capable of exploiting it.

The U.S. National Security Agency has publicly noted that a sufficiently large quantum computer, should one ever be built, would be capable of compromising all the public-key algorithms widely deployed today — which makes SNDL an active threat even while the hardware needed to exploit it does not yet exist (Veritasium, 2023).



Figure 4. The “Store Now, Decrypt Later” (SNDL) attack flow: intercepting and storing encrypted data today to decrypt it once a sufficiently powerful quantum computer exists.

Data whose sensitivity persists ten years or more: typical SNDL targets.

Category	Assets with persistent sensitivity	Typical horizon
Defense and security	Military bases and defense installations; intelligence agents and classified communications	Operational positions valid for decades
Critical infrastructure	Power grids, nuclear and water plants; emergency protocols and key facilities	Infrastructure active for 20 to 50 years
Financial sector	Sovereign debt strategies and reserves; sovereign fund contracts and positions	Valid for the entire contract duration
Personal data	Genetic and biometric information; complete medical history	Biometrics and DNA are permanent and irrevocable
Intellectual property	Pharmaceutical formulas and trade secrets; unpublished scientific research, strategic R&D	Patents valid for 15 to 20 years

5.4 Time Horizon: When Does the Risk Become Real?

Pinpointing exactly when this risk will materialize is difficult, in part because the estimates themselves have changed quickly. Available projections place the emergence of a quantum computer capable of breaking RSA encryption within a horizon of five to twenty years, depending on the source and the year the estimate was made, and the observed trend suggests that horizon tends to shorten rather than lengthen.

Comparing the quantum computing capacity available today with that required to run Shor's algorithm against real keys illustrates the nature of this horizon: looking at the current state of commercially available quantum processors, the distance from the millions of qubits needed remains wide, but the growth trajectory has been consistently exponential. That same dynamic explains why researchers who for years held to ten-to-fifteen-year horizons, such as Harrow, have revised their own projections toward shorter timeframes.

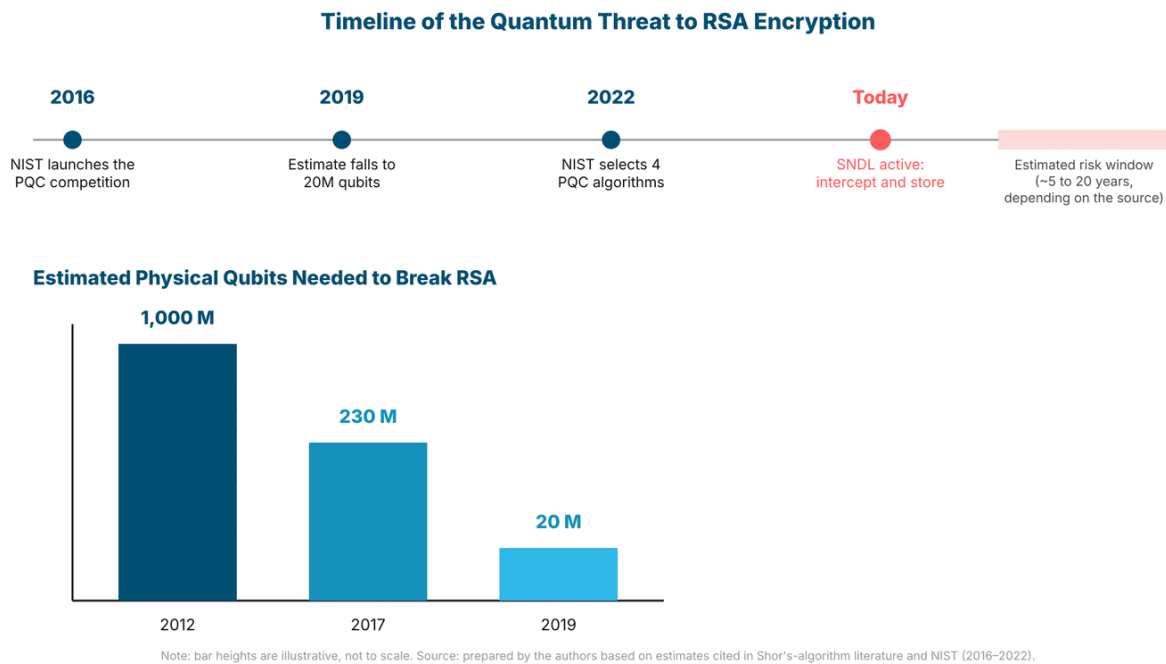


Figure 5. Timeline of the quantum threat: regulatory and technological milestones (NIST 2016–2022), the decline in estimated qubits needed to break RSA (2012–2019), and the critical SNDL window.

CHAPTER

6

Sectoral Applications

6. Sectoral Applications

The preceding chapters established why public-key cryptography is vulnerable to quantum computing, how that threat operates, and what alternatives exist to respond to it. This chapter applies that discussion to the sectors where migration toward resistant schemes is most urgent, already identified in this report's executive summary: finance, government, health, critical infrastructure, and foreign trade.

6.1 Financial Sector and Central Banking

The financial system is probably the sector whose dependence on public-key cryptography is most direct: bank transfers, electronic payment systems, online banking, and securities-trading platforms ultimately depend on the public keys used to authenticate transactions being neither forgeable nor decryptable.

The SNDL logic described in Chapter 5 is particularly relevant in this sector: customer data and transaction records intercepted today would retain much of their value — as well as their potential for reputational and financial harm — even if decrypted several years after being captured. Central banks, in their role as supervisors of the financial system, also face the additional task of coordinating migration timelines across multiple regulated entities, a sector-wide cryptographic-agility challenge that exceeds the capacity of any single institution.

6.2 Government and Public Administration

Official communications between government agencies, digital identity systems, and administrative records share the same structural exposure as the financial sector: they depend on public-key cryptography to ensure that only authorized recipients can read a message or validate an identity. The difference, in this case, lies in the nature of the information at stake: much of diplomatic and government intelligence communication retains its sensitivity for far longer periods than a financial transaction, making it one of the most frequently cited targets of the practice of intercepting and storing information today to decrypt it in the future.

Quantum position verification and digital certificates thus foreshadow one of the most direct applications of quantum cryptography in government: confirming that an official communication actually originates from the server and jurisdiction it claims to.

6.3 Health

Clinical records and electronic health records present a particular combination of sensitivity and persistence: unlike a password, which can be changed once compromised, a medical diagnosis or a genetic history does not lose its sensitive character over time, which makes it especially vulnerable to SNDL logic.

The growing digitalization of health systems through electronic health records, telemedicine, and data exchange between providers and insurers, among other channels, further multiplies the points at which information travels encrypted across networks that will eventually need to migrate to post-quantum schemes, although the available evidence does not allow for precise timelines or a clear picture of current adoption status in the health sector of Latin America and the Caribbean.

6.4 Critical Infrastructure and Energy

Power grids, water distribution systems, and telecommunications networks increasingly rely on remote control systems and encrypted communications between sensors, operations centers, and vendors, which extends much of the digital security risks discussed in this report into the physical operation of these services.

Unlike a financial or clinical record, where a breach compromises the confidentiality of the information, a successful attack on the encrypted communications of a power or water grid could also compromise the operational continuity of the service, adding a physical-security dimension to the discussion of cryptographic agility. The literature consulted offers no further detail on the state of the region's critical infrastructure in the face of this threat: this is, accordingly, an area where a sectoral diagnostic is particularly needed.

6.5 Supply Chains and Foreign Trade

Global supply chains depend on traceability systems, customs documentation, and communication between multiple actors that today rely on digital signatures and encrypted channels to guarantee the authenticity of trade documentation and prevent fraud.

The distributed nature of these chains, which involve actors with varying technological capacities and diverse regulatory jurisdictions, means that migration toward post-quantum schemes requires, in this sector, a considerable degree of multilateral coordination. Foreign trade in Latin America and the Caribbean, highly dependent on international markets and logistics chains, is therefore exposed to the migration timelines set by its main trading partners — an additional factor that reinforces the value of early regional participation in standardization processes.

In the United States, for example, the National Security Agency (NSA) established, through the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), a phased timeline for incorporating quantum-resistant algorithms: it calls for certain systems, such as traditional networking equipment, to adopt these algorithms exclusively by 2030, while the general transition of national security systems must be completed by 2035 (National Security Agency, 2022).

These timelines anticipate changes in technological, interoperability, and security requirements that may extend beyond U.S. borders and affect businesses and institutions in the region. In this context, early participation by Latin America and the Caribbean in standardization processes and advance planning of the migration are essential to reduce costs, avoid new technological dependencies, and preserve integration with international markets.

Sector	What public-key cryptography protects today	Why SNDL matters
Financial and central banking	Transfers, online banking and payment authentication	Customer and transaction data retain value for years
Government and public administration	Digital identity and official communications	Diplomatic and intelligence communications with long sensitivity
Health	Electronic health records and telemedicine	The sensitivity of a diagnosis or genetic history does not expire
Critical infrastructure and energy	Communication between sensors, networks and control centers	Compromises operational continuity, not only confidentiality
Supply chains and foreign trade	Digital signatures in customs documentation	Requires multilateral coordination among actors and jurisdictions

Synthesis prepared from the exposure logic described in Chapters 2, 5, and 7 of this report; it does not substitute for a sector-specific diagnostic for Latin America and the Caribbean.

Figure 6. Sectoral exposure to the quantum threat: a qualitative synthesis based on the conceptual framework developed in Chapters 2 through 6.



Recommendations

7. Recommendations

The analysis developed in the preceding chapters leaves a clear diagnosis: the threat that quantum computing poses to today's cryptographic infrastructure is neither speculative nor distant, and it is already active with the "store now, decrypt later" scheme. The question that remains to be answered is how to act.

This chapter proposes a structured framework to answer that question, organized around four pillars: a tool for calibrating the urgency of action, practical recommendations for governments and institutions in the region, the role multilateral organizations can play in supporting the transition, and the IDB's institutional vision.

7.1 The Mosca Theorem

Before formulating specific recommendations, it is worth establishing the analytical framework that answers a question many organizations put off: exactly when is it necessary to act? The Mosca theorem, formulated by quantum computing researcher Michele Mosca, offers an answer through a simple inequality with first-order operational implications.

The theorem proposes defining three variables: X , the number of years the data to be protected must remain confidential; Y , the number of years it will take to migrate systems to quantum-resistant cryptographic schemes; and Z , the number of years remaining until a cryptographically relevant quantum computer exists at scale. The central conclusion is that an organization faces present risk whenever $X + Y > Z$, even if the quantum computer does not yet exist. The reason is structural: if migration takes longer than the time remaining before the threat materializes, any data that must remain secure beyond that point is already exposed through SNDL attacks.

Applied to a Latin American or Caribbean government managing infrastructure data with a twenty-year validity period ($X = 20$), whose complex systems require between five and seven years to migrate ($Y = 6$), and where conservative estimates place a relevant quantum computer within a horizon of ten to fifteen years ($Z = 12$): the sum yields 26 against 12. The risk is present, even before the quantum computer exists.

The theorem's usefulness does not depend on certainty about Z , and that is precisely its greatest strength: even amid the uncertainty that characterizes quantum-computing projections, the sum of X and Y is frequently large enough to generate present risk regardless of which estimate of Z turns out to be correct. Under these conditions, the appropriate response is not to wait for certainty about Z , but to reduce X and Y through a planned migration. For the region, the theorem also carries a direct prioritization implication: sectors that manage long-lived data — defense, health, justice, financial infrastructure — top the agenda not necessarily because the threat is more imminent in their case, but because their X value is larger, which brings forward the threshold at which the inequality is violated.

7.2 Recommendations for Governments and Institutions in the Region

The recommendations that follow are ordered by operational logic: the first lay the institutional groundwork without which the rest cannot be executed; the next define the technical priorities of the migration; and the last address the long-term enabling conditions. All of them share a common starting point: the transition to post-quantum cryptography is not a narrowly scoped technology project, but an infrastructure transformation with dimensions spanning governance, human resources, the vendor supply chain, and regional cooperation.

- Define institutional responsibilities and governance. No cryptographic transition at scale is possible without an institutional framework to sustain it. At a minimum, this means designating a lead with sufficient authority to drive cross-cutting decisions, establishing a roadmap with verifiable milestones, and securing executive sponsorship that guarantees continuity beyond political cycles. In contexts where that capacity does not yet exist or is still incipient, the priority is to build it before advancing on the technical dimension: a migration without clear governance tends to fragment into isolated initiatives that fail to deliver systemic protection.
- Build and maintain a cryptographic inventory. It is not possible to migrate what is not known. The first operational step of any transition is a discovery process that maps where public-key cryptography is used, with which algorithms, in which systems, and what type of information it protects. That inventory is not a one-off exercise but a living asset: systems change, vendors update their components, and an institution's cryptographic surface evolves. Investing in tools and processes that keep that inventory current is a structural condition of the transition, not a stage that is completed and closed.
- Prioritize by data longevity and SNDL exposure. Migration cannot – and should not – happen simultaneously across all infrastructure. The most robust prioritization criterion combines two dimensions: the sensitivity and useful life of the protected data, and its actual exposure to SNDL attacks. Systems that protect information requiring confidentiality that must hold for decades, and that are already potentially being intercepted and stored by actors with long-term capacity, should top the roadmap. In practice, this usually includes diplomatic communications, critical-infrastructure records, citizens' biometric data, and financial systems with long-term liabilities.
- Adopt cryptographic agility as a design principle. Uncertainty over the pace of quantum development, and the possibility that future advances could affect even the post-quantum algorithms considered solid today, mean that long-term resilience depends not solely on the algorithms chosen, but on the ability to replace them without a full re-engineering effort. Designing systems with cryptographic agility — that is, the ability to swap out the underlying algorithm in a modular way — turns the transition into a manageable process rather than a disruptive event. This principle applies both to new systems and to those undergoing renewal: building in cryptographic agility at the design stage costs a small fraction of what retrofitting it would cost once systems are already operational.

- Migrate to the standards already finalized and follow the reference timelines. The publication of the NIST standards in August 2024 (FIPS 203, FIPS 204, and FIPS 205), together with the addition of HQC in 2025, removes uncertainty over which algorithms to adopt. Governments and institutions in the region should establish migration plans aligned with the timelines that leading international partners have begun to set, which aim to complete the transition of the most critical systems between 2030-35. Waiting for those timelines to become mandatory amounts, in many cases, to violating the Mosca inequality for data that is already being stored today.
- Engage vendors and set requirements in public procurement. A significant share of governments' cryptographic infrastructure is not developed in-house but purchased from software, hardware, and cloud service providers. Post-quantum migration therefore requires passing these requirements on to the vendor ecosystem: building NIST-standard compatibility requirements into tender specifications, requiring transition roadmaps from current vendors, and favoring solutions with built-in cryptographic agility in procurement processes. Institutions with the capacity to articulate these requirements can, in addition, generate a spillover effect across the regional technology market.
- Build capacity and promote regional cooperation. Post-quantum migration requires technical profiles that are currently scarce in the region: specialists in applied cryptography, cryptographic-inventory auditing, and the integration of post-quantum algorithms into existing system architectures. Building this capacity cannot rely solely on each institution's internal training: regional cooperation, the exchange of methodologies, and the construction of joint training programs are more efficient mechanisms for generating critical mass. South-South cooperation mechanisms and technical exchange platforms among countries in the region have a specific and irreplaceable role in this process.
- Coordinate across sectors. A country's cryptographic infrastructure does not belong to a single institutional actor: central banks, telecommunications, health, defense, and identity systems share protocols, vendors, and, in many cases, infrastructure. An uncoordinated sector-by-sector migration can create breaking points at the interfaces between systems that have already migrated and those that have not. Cross-sector coordination, with formal channels for alignment and shared prioritization criteria, is a condition for the integrity of the transition at the national scale.

7.3 Multilateral Actors and the IDB's Institutional Position

The transition to post-quantum cryptography raises challenges that no country in the region can address entirely on its own: a shortage of specialized technical capacity, resource asymmetries between large and small economies, regulatory fragmentation, and dependence on global technology vendors. In this context, multilateral organizations have an enabling role that goes beyond financing and extends to the production of regional public goods: standards, methodologies, regulatory frameworks, and knowledge-exchange platforms.

At the global level, United Nations system agencies offer particularly relevant spaces for regulatory and technical coordination. The International Telecommunication Union (ITU) has incorporated post-quantum preparedness into its digital-infrastructure standards agenda, and its maturity-assessment frameworks can serve as a starting point for national diagnostics in the region. UNESCO, drawing on its mandate on the ethics of emerging technologies, contributes the conceptual framework for addressing governance and equity-of-access dimensions. The Organisation for Economic Co-operation and Development (OECD), for its part, has published guidelines on responsible innovation in security technologies that are relevant to the design of national regulatory frameworks.

At the regional level, The Caribbean Community (CARICOM) faces a situation that warrants differentiated attention. Its member economies, most of them small island states, combine high dependence on digital infrastructure for public services and tourism with limited technical and budgetary capacity to manage a complex cryptographic transition. The risk that the post-quantum gap will deepen between the region's larger economies and the Caribbean states is real, and it calls for specific technical and financial cooperation mechanisms, including shared inventory and migration platforms that reduce the per-unit cost of the transition for these countries.

Organizations like The World Bank can mobilize resources for the more capital-intensive investment stage, with technical assistance instruments especially relevant for designing regulatory frameworks and building capacity in countries with lower relative development. The International Monetary Fund (IMF) has a specific channel of influence in the financial sector: incorporating post-quantum risk into Financial Sector Assessment Programs (FSAPs) and prudential supervision frameworks can accelerate action by central banks and financial institutions more effectively than any standalone technical recommendation. The Organization of American States (OAS), through the Inter-American Committee against Terrorism (CICTE) and its cybersecurity program, has channels of coordination with member countries' security agencies and computer security incident response teams (CSIRTs) that can help institutionalize the post-quantum dimension within national agendas.

7.3.1 Corporate Technology at the IDB

The IDB occupies a unique position in this process: it is simultaneously an institution that must manage its own cryptographic transition and an actor capable of supporting member countries in theirs. These two dimensions reinforce one another: the Bank's credibility as a partner in the region's transition depends, in part, on its ability to travel that path rigorously within its own infrastructure.

The greatest opportunity for advancing toward quantum-resistant schemes lies in managing two factors: data that requires its confidentiality to be maintained for more than a decade, and which is therefore exposed to SNDL attacks, and systems with planned renewal cycles, where building in cryptographic agility costs only a fraction of what a later re-engineering effort would cost.

The cybersecurity team within the IDB's Technology and Transformation Department (TTD) is applying this approach. The discovery and cryptographic-inventory phase for corporate systems has already begun, to identify where public-key cryptography is used, with which algorithms, and what information it protects. The process requires meeting three conditions: executive sponsorship with clear governance and a designated lead; visibility through an up-to-date inventory of cryptographic systems; and clear reference standards — currently those published by NIST in 2024 — aligned with the timelines set by leading international partners, which aim to complete the migration of critical systems between 2030-35.

The first concrete step is the inventory, prioritized by data longevity: not everything needs to migrate at once, but it is essential to know what to migrate first. The Bank's role begins by leading by example, walking that path itself, and sharing methodology and lessons learned with institutions across the region through joint initiatives such as this report.

CHAPTER

8

Conclusion

8. Conclusion

This report began from a simple premise with profound implications: public-key cryptography, which for more than four decades has sustained global digital trust, faces in quantum computing a structural threat whose horizon of materialization keeps drawing closer. That threat is neither hypothetical nor exclusively in the future: under the logic of "store now, decrypt later," the exposure of sensitive information is, in practice, already underway, even before a quantum computer exists that can fully exploit it.

In response to that threat, the report addressed the concept of quantum cryptography, which uses principles of physics such as superposition, entanglement, and the no-cloning theorem to protect information and detect any interception attempt. It also introduced the notion of post-quantum cryptography, which replaces vulnerable mathematical problems with other security schemes, such as those based on lattices, that neither classical nor quantum computers can solve efficiently. Of the two, the latter today offers the more viable adoption path in the short and medium term, precisely because it does not require the specialized physical infrastructure that the former does.

The selection, in 2022, of the first four algorithms of NIST's post-quantum standard marked the formal beginning of a migration that, nevertheless, is far from complete: as discussed throughout this report, replacing an encryption algorithm requires identifying where public-key cryptography is used across financial, government, health, critical-infrastructure, and foreign-trade systems, and coordinating that transition among a multiplicity of actors that do not always share timelines or capabilities.

Latin America and the Caribbean do not yet play a leading role in the development of quantum hardware or in the definition of the new standards — a gap that could deepen the region's external dependence on decisions key to the security of its most sensitive information. But that same early stage of the global process, in which governance frameworks, migration strategies, and cryptographic-agility practices are still being defined, represents a concrete opportunity for influence, provided the region acts with the urgency demanded by a risk horizon estimated at five to twenty years.

This transition involves far more than equations and protocols: it engages the protection of data that, once exposed, cannot be protected retroactively; it calls into question the balance between state surveillance capabilities and privacy rights; and it raises equity questions about who has the institutional capacity to migrate in time and who does not. Addressing these dimensions will be just as decisive for the ultimate outcome of this transition as the strength of the algorithms that underpin it.



References

9. References

- Chen, Y.-A. et al. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589, 214–219. <https://www.nature.com/articles/s41586-020-03093-8>
- Gidney, C. (2025). How to factor 2048-bit RSA integers in less than a week using less than a million noisy qubits. *arXiv*. <https://doi.org/10.48550/arXiv.2505.15917>
- IBM. (n.d.). What is homomorphic encryption? *IBM Think*. <https://www.ibm.com/es-es/think/topics/homomorphic-encryption>
- El País. (2026, June 5). Aram Harrow, quantum researcher: "We don't have 10 years left for these computers, they will arrive sooner." *El País Tecnología*. <https://elpais.com/tecnologia/2026-06-05/aram-harrow-investigador-cuantico-no-quedan-10-anos-para-estos-ordenadores-llegaran-antes.html>
- Mosca, M., & Piani, M. (2015). Quantum threat timeline. *Cryptology ePrint Archive*, Paper 2015/1075. <https://eprint.iacr.org/2015/1075>
- National Institute of Standards and Technology (NIST). (2025). What is quantum cryptography? *NIST Cybersecurity*. <https://www.nist.gov/cybersecurity-and-privacy/what-quantum-cryptography>
- National Security Agency. (2022, September). Commercial National Security Algorithm Suite 2.0. *U.S. Department of Defense*. https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF
- Veritasium. (2023). How quantum computers break the internet... starting now [video]. *YouTube*. <https://www.youtube.com/watch?v=-UrdExQW0cs>
- WeLiveSecurity by ESET. (2019, September 4). Homomorphic encryption: the closest encryption paradigm. *WeLiveSecurity*. <https://www.welivesecurity.com/la-es/2019/09/04/criptografia-homomorfica-paradigma-cifrado-cercano/>