



# Ch13: Quantum-Safe Security



### Random numbers

Applications:

- Cryptography
- Numerical simulations
- Statistical sampling

Critical that these values be:

- Uniformly distributed
- Independent

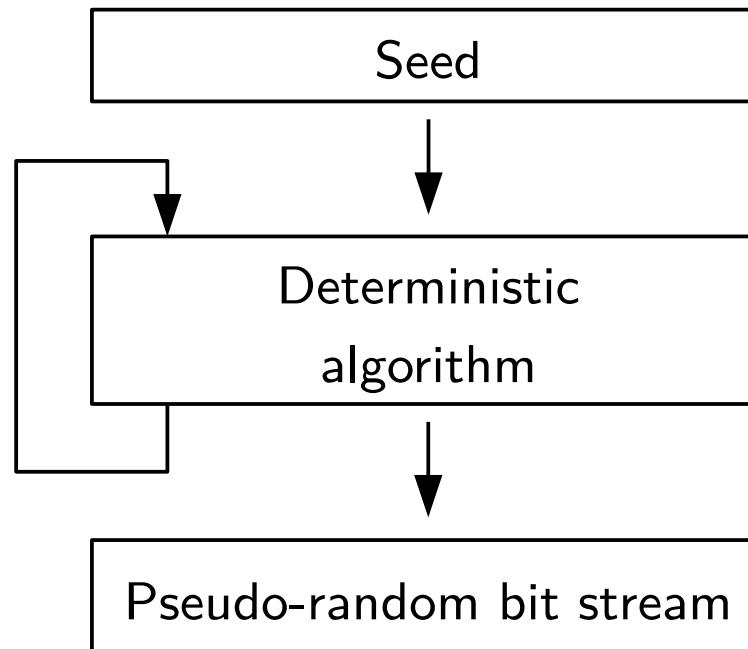


There are two main classes of generators: software and physical.



## Pseudo random number generators (PRNG)

They consist of an algorithm into which some initial value – called the seed – is fed, and which produces by iteration a sequence of pseudo-random numbers:





### Pseudo random number generators (PRNG)

In a well-designed algorithm, this sequence may have most of the properties of a random sequence, and thus pass statistical randomness tests.

However, it is important to note that computers are deterministic systems: given a certain input, a program will always produce the same output.

Because of this very fundamental property, it is impossible for a program to produce a sequence of truly random numbers

By knowing the seed, it is always possible to reproduce the sequence.



## Pseudo random number generators (PRNG)

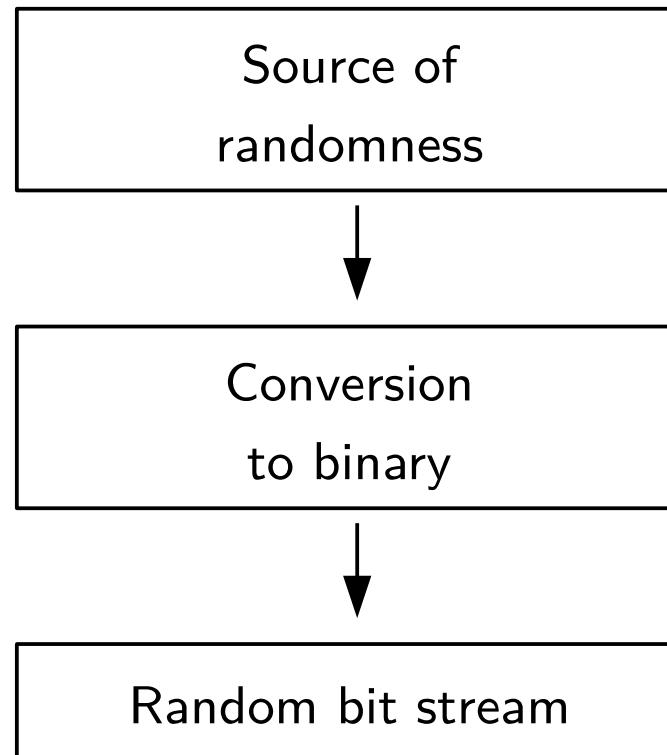
PRNG is a single point of failure for many real-world cryptosystems. If random numbers are insecure – likely to be predictable – then the entire application is insecure.

Topic	Summary	Additional Information
Dual_EC_DRBG	This algorithm was officially recommended by NIST, until it was discovered that it may contain a backdoor, potentially implanted by NSA.	<a href="http://www.wired.com/2013/09/nsa-backdoor/">http://www.wired.com/2013/09/nsa-backdoor/</a>
Low entropy in Linux servers	Initially reported in a Black-Hat conference in 2015.	<a href="http://www.bbc.com/news/technology-33839925">http://www.bbc.com/news/technology-33839925</a>
Untrusted physical RNGs	FreeBSD developers recommend against using the physical RNGs in the processors manufactured by Intel and Via for fear of a backdoor.	<a href="http://arstechnica.com/security/2013/12/we-cannot-trust-intel-and-vias-chip-based-crypto-freebsd-developers-say/">http://arstechnica.com/security/2013/12/we-cannot-trust-intel-and-vias-chip-based-crypto-freebsd-developers-say/</a>
Weak keys	There are now well-documented examples, showing how badly chosen or re-used keys damage encryption systems.	<a href="https://freedom-to-tinker.com/blog/haldermanheninger/how-is-nsa-breaking-so-much-crypto/">https://freedom-to-tinker.com/blog/haldermanheninger/how-is-nsa-breaking-so-much-crypto/</a> <a href="https://factorable.net/weakkeys12.conference.pdf">https://factorable.net/weakkeys12.conference.pdf</a>



### Hardware random number generators (HRNG)

For security or other applications where high quality randomness is needed, physical approaches are taken to generate random bits.





### Hardware random number generators (HRNG)

A HRNG typically consists of:

- A transducer to convert some aspect of the physical phenomena to an electrical signal;
- An amplifier and other electronic circuitry to increase the amplitude of the random fluctuations to a measurable level;
- Some type of analog to digital converter to convert the output into a digital number, often a simple binary digit 0 or 1.

By repeatedly sampling the randomly varying signal, a series of random numbers is attained.



### Hardware random number generators (HRNG)

While processes described by classical physics such as clock jitter, chaotic behaviour, etc can be used to deliver entropy, classical physics is fundamentally deterministic, i.e. predictable for a given set of conditions.

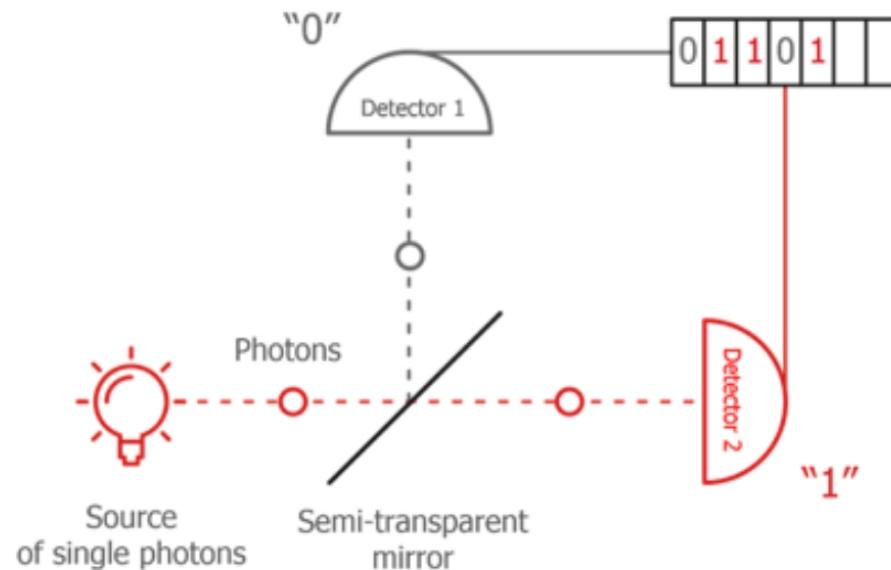
In addition, although random numbers generated by classical physical processes are likely to pass randomness tests, it can be impossible to verify that they are not influenced by their environment, reducing the output quality.



### Quantum random number generators (QRNG)

Generators based on quantum physical processes deliver the highest quality random data.  
Contrary to classical physics, quantum physics is fundamentally random.

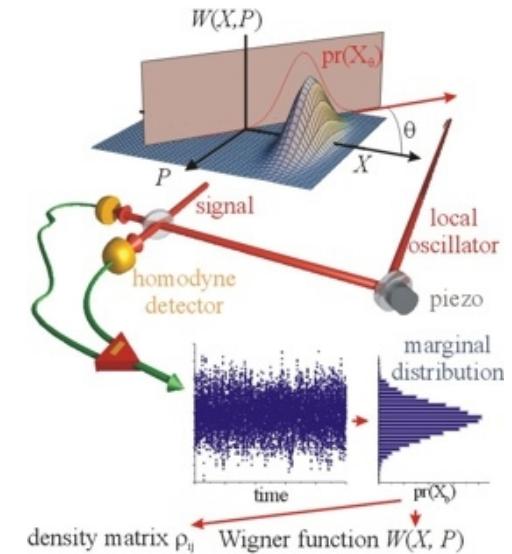
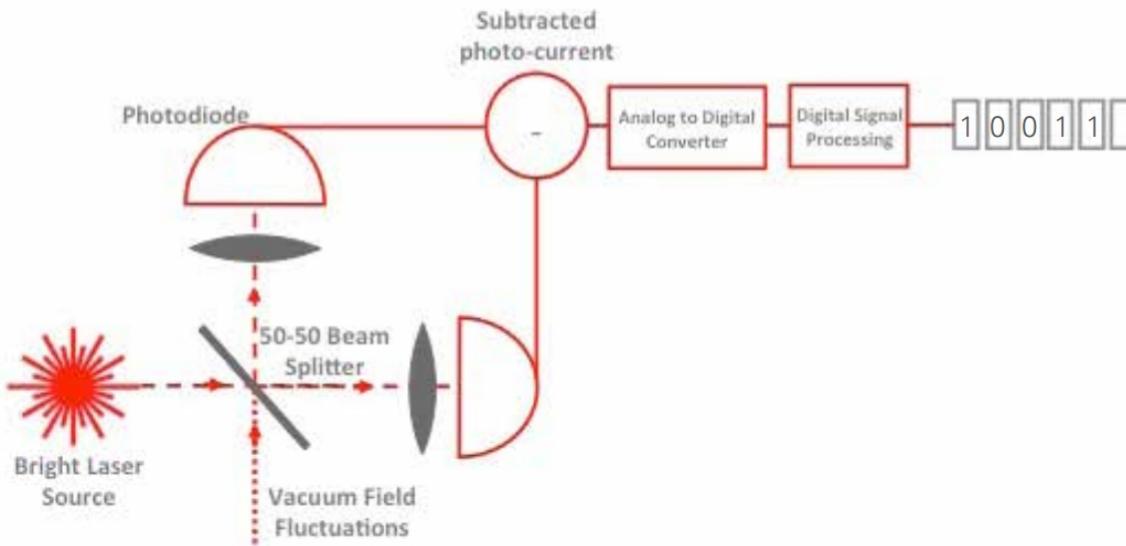
- QRNG based on single-photon splitting:



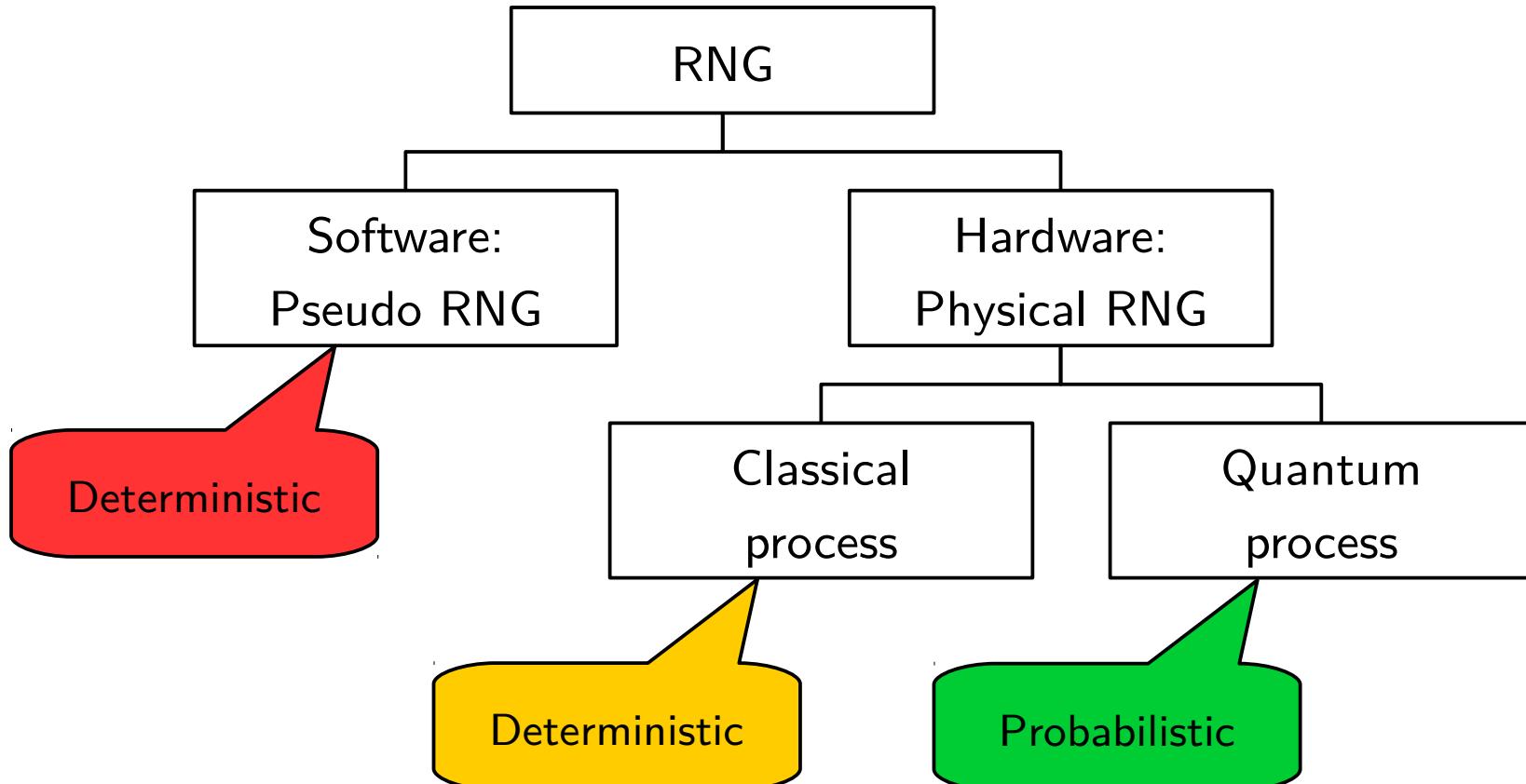
## Quantum random number generators (QRNG)

Generators based on quantum physical processes deliver the highest quality random data.  
Contrary to classical physics, quantum physics is fundamentally random.

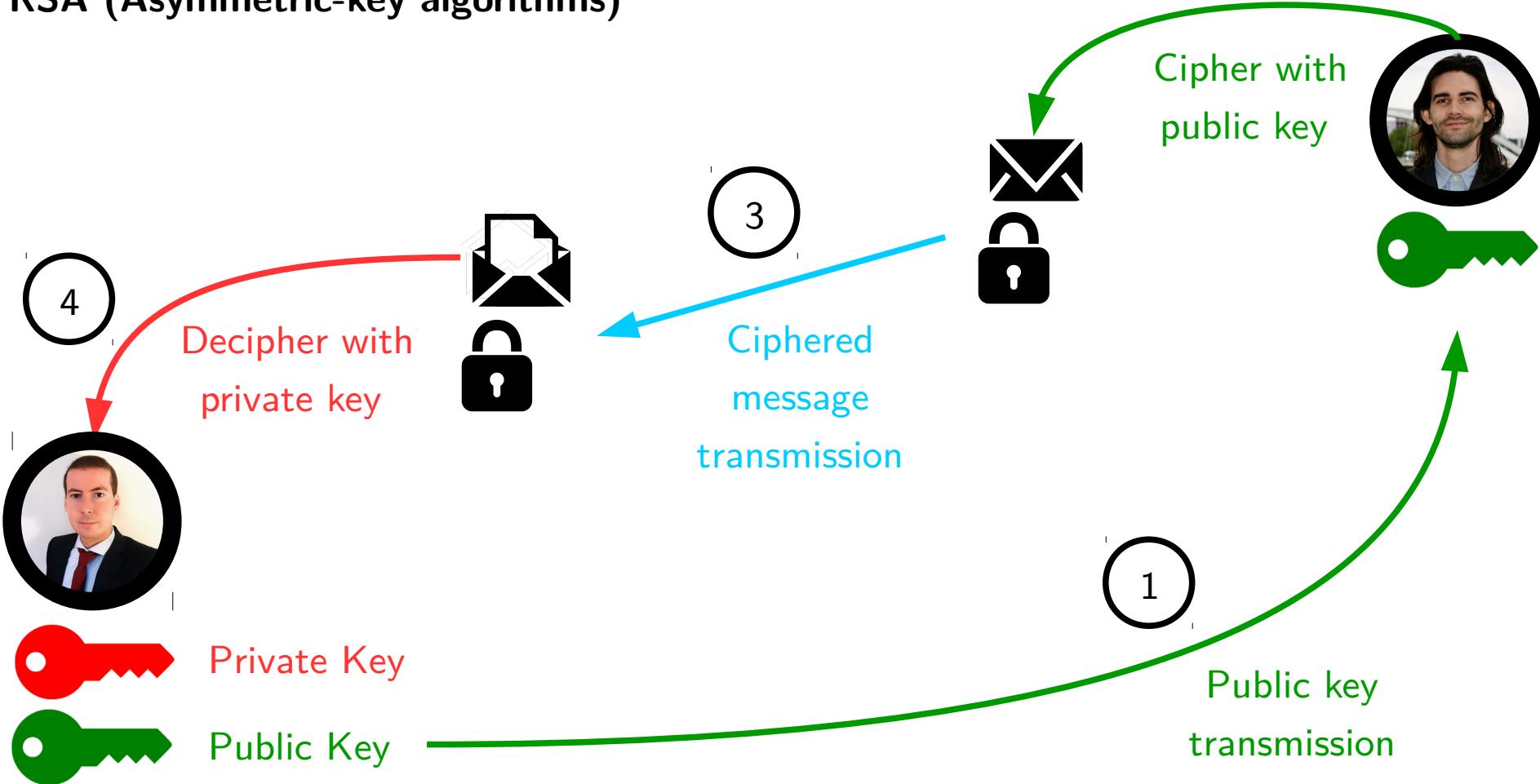
- QRNG based on quantum vacuum noise measurements:



### Summary



## RSA (Asymmetric-key algorithms)



## RSA (Asymmetric-key algorithm)



Practicality



Computational security



Decipher with  
private key



Ciphered  
message  
transmission



Private Key



Public Key

Cipher with  
public key



Public key  
transmission



## Shor's quantum factoring algorithm

## Shor's Integer Factorization Algorithm Circuit

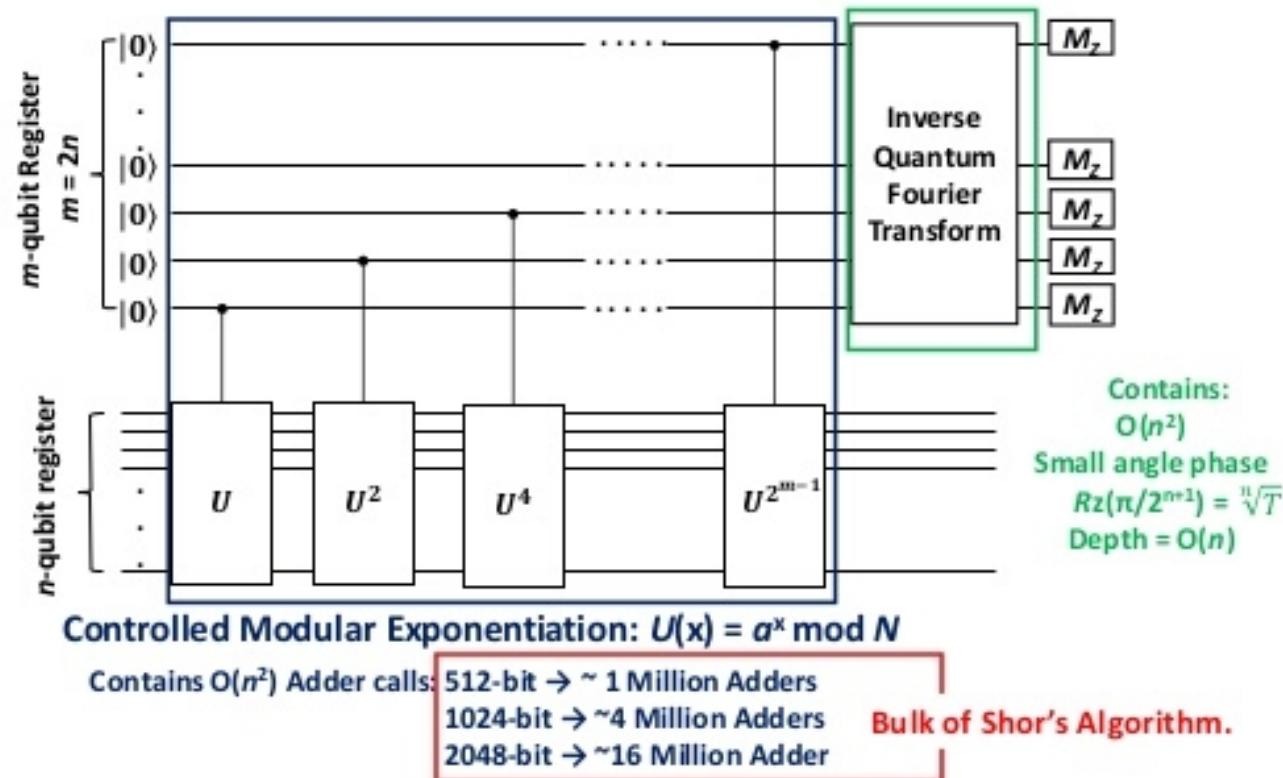
For  $n$ -bit integer  $N$   
 $\text{GCD}(a, N) = 1, a < N$

$$N = (a^{r/2}-1)(a^{r/2}+1)$$

Period  $r$  is hidden in  
Eigenvalues of  
 $U(x) = a^x \bmod N$

Classical Complexity:  
Exponential in  $n$

Quantum Complexity:  
Polynomial  $O(n^3)$





## 13.2 Post-quantum cryptography

### Shor's quantum factoring algorithm

Cornell University

We gratefully acknowledge support from the Simons Foundation and member institutions.

arXiv.org > quant-ph > arXiv:1905.09749

Search... All fields Search Help | Advanced Search

**Quantum Physics**

[Submitted on 23 May 2019 ([v1](#)), last revised 5 Dec 2019 (this version, v2)]

## How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney, Martin Ekerå

We significantly reduce the cost of factoring integers and computing discrete logarithms in finite fields on a quantum computer by combining techniques from Shor 1994, Griffiths-Niu 1996, Zalka 2006, Fowler 2012, Ekerå-Håstad 2017, Ekerå 2017, Ekerå 2018, Gidney-Fowler 2019, Gidney 2019. We estimate the approximate cost of our construction using plausible physical assumptions for large-scale superconducting qubit platforms: a planar grid of qubits with nearest-neighbor connectivity, a characteristic physical gate error rate of  $10^{-3}$ , a surface code cycle time of 1 microsecond, and a reaction time of 10 microseconds. We account for factors that are normally ignored such as noise, the need to make repeated attempts, and the spacetime layout of the computation. When factoring 2048 bit RSA integers, our construction's spacetime volume is a hundredfold less than comparable estimates from earlier works (Fowler et al. 2012, Gheorghiu et al. 2019). In the abstract circuit model (which ignores overheads from distillation, routing, and error correction) our construction uses  $3n + 0.002n \lg n$  logical qubits,  $0.3n^3 + 0.0005n^3 \lg n$  Toffolis, and  $500n^2 + n^2 \lg n$  measurement depth to factor  $n$ -bit RSA integers. We quantify the cryptographic implications of our work, both for RSA and for schemes based on the DLP in finite fields.

Comments: 26 pages, 10 figures, 5 tables  
Subjects: Quantum Physics (quant-ph)

**Download:**

- PDF
- Other formats

(CC BY)

**Ancillary files (details):**

- [estimate\\_costs.py](#)
- [estimate\\_costs\\_test.py](#)
- [fill-in-table.py](#)

Current browse context:  
[quant-ph](#)  
[< prev](#) | [next >](#)  
[new](#) | [recent](#) | [1905](#)

**References & Citations**

- [INSPIRE HEP](#)  
(refers to | cited by)
- [NASA ADS](#)
- [Google Scholar](#)
- [Semantic Scholar](#)

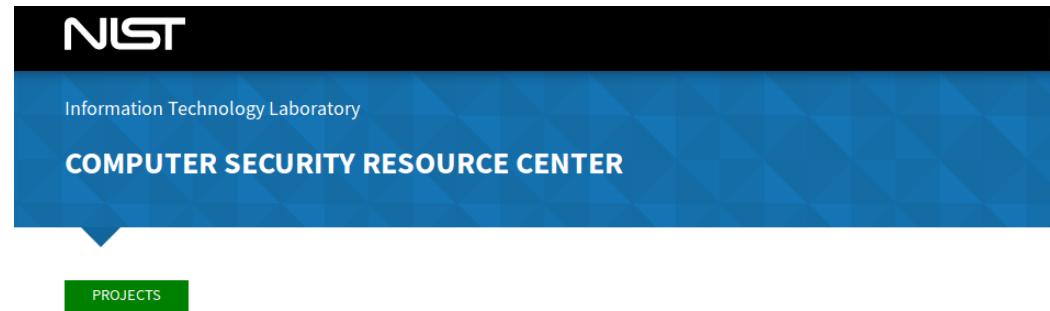
**2 blog links** ([what is this?](#))



## 13.2 Post-quantum cryptography

### Post-quantum algorithms

TYPES OF CRYPTOGRAPHY	
QUANTUM-BREAKABLE	QUANTUM-SECURE
 RSA encryption	 Lattice-based cryptography
A message is encrypted using the intended recipient's public key, which the recipient then decrypts with a private key. The difficulty of computing the private key from the public key is connected to the hardness of prime factorization.	Security is related to the difficulty of finding the nearest point in a lattice with hundreds of spatial dimensions (where the lattice point is associated with the private key), given an arbitrary location in space (associated with the public key).
 Diffie-Hellman key exchange	 Code-based cryptography
Two parties jointly establish a shared secret key over an insecure channel that they can then use for encrypted communication. The security of the secret key relies on the hardness of the discrete logarithm problem.	The private key is associated with an error-correcting code and the public key with a scrambled and erroneous version of the code. Security is based on the hardness of decoding a general linear code.
 Elliptic curve cryptography	 Multivariate cryptography
Mathematical properties of elliptic curves are used to generate public and private keys. The difficulty of recovering the private key from the public key is related to the hardness of the elliptic-curve discrete logarithm problem.	These schemes rely on the hardness of solving systems of multivariate polynomial equations.



The NIST Computer Security Resource Center logo features the NIST logo at the top, followed by "Information Technology Laboratory" and "COMPUTER SECURITY RESOURCE CENTER". Below this is a green button labeled "PROJECTS".

### Post-Quantum Cryptography

f G+ t

#### Project Overview

NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. [Full details can be found in the Post-Quantum Cryptography Standardization page.](#)

*The [Round 2 candidates](#) were announced January 30, 2019. [NISTIR 8240, Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process](#) is now available.*

#### Background

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of *post-quantum cryptography* (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.



## 13.2 Post-quantum cryptography

### Post-quantum algorithms

Cornell University

We gratefully acknowledge support from the Simons Foundation and member institutions.

arXiv.org > quant-ph > arXiv:1710.10377

Search... All fields  Help | Advanced Search

**Quantum Physics**

[Submitted on 28 Oct 2017]

## Quantum attacks on Bitcoin, and how to protect against them

Divesh Aggarwal, Gavin K. Brennen, Troy Lee, Miklos Santha, Marco Tomamichel

The key cryptographic protocols used to secure the internet and financial transactions of today are all susceptible to attack by the development of a sufficiently large quantum computer. One particular area at risk are cryptocurrencies, a market currently worth over 150 billion USD. We investigate the risk of Bitcoin, and other cryptocurrencies, to attacks by quantum computers. We find that the proof-of-work used by Bitcoin is relatively resistant to substantial speedup by quantum computers in the next 10 years, mainly because specialized ASIC miners are extremely fast compared to the estimated clock speed of near-term quantum computers. On the other hand, the elliptic curve signature scheme used by Bitcoin is much more at risk, and could be completely broken by a quantum computer as early as 2027, by the most optimistic estimates. We analyze an alternative proof-of-work called Momentum, based on finding collisions in a hash function, that is even more resistant to speedup by a quantum computer. We also review the available post-quantum signature schemes to see which one would best meet the security and efficiency requirements of blockchain applications.

Comments: 21 pages, 6 figures

Subjects: **Quantum Physics (quant-ph)**; General Finance (q-fin.GN)

Journal reference: Ledger, [S.I.], v. 3, oct. 2018

DOI: [10.5195/ledger.2018.127](https://doi.org/10.5195/ledger.2018.127)

Cite as: [arXiv:1710.10377 \[quant-ph\]](https://arxiv.org/abs/1710.10377)

**Download:**

- [PDF](#)
- [Other formats](#)

(license)

Current browse context:  
**quant-ph**

[< prev](#) | [next >](#)  
[new](#) | [recent](#) | [1710](#)

Change to browse by:  
[q-fin](#)  
[q-fin.GN](#)

**References & Citations**

- [INSPIRE HEP](#)  
(refers to | cited by)
- [NASA ADS](#)
- [Google Scholar](#)
- [Semantic Scholar](#)

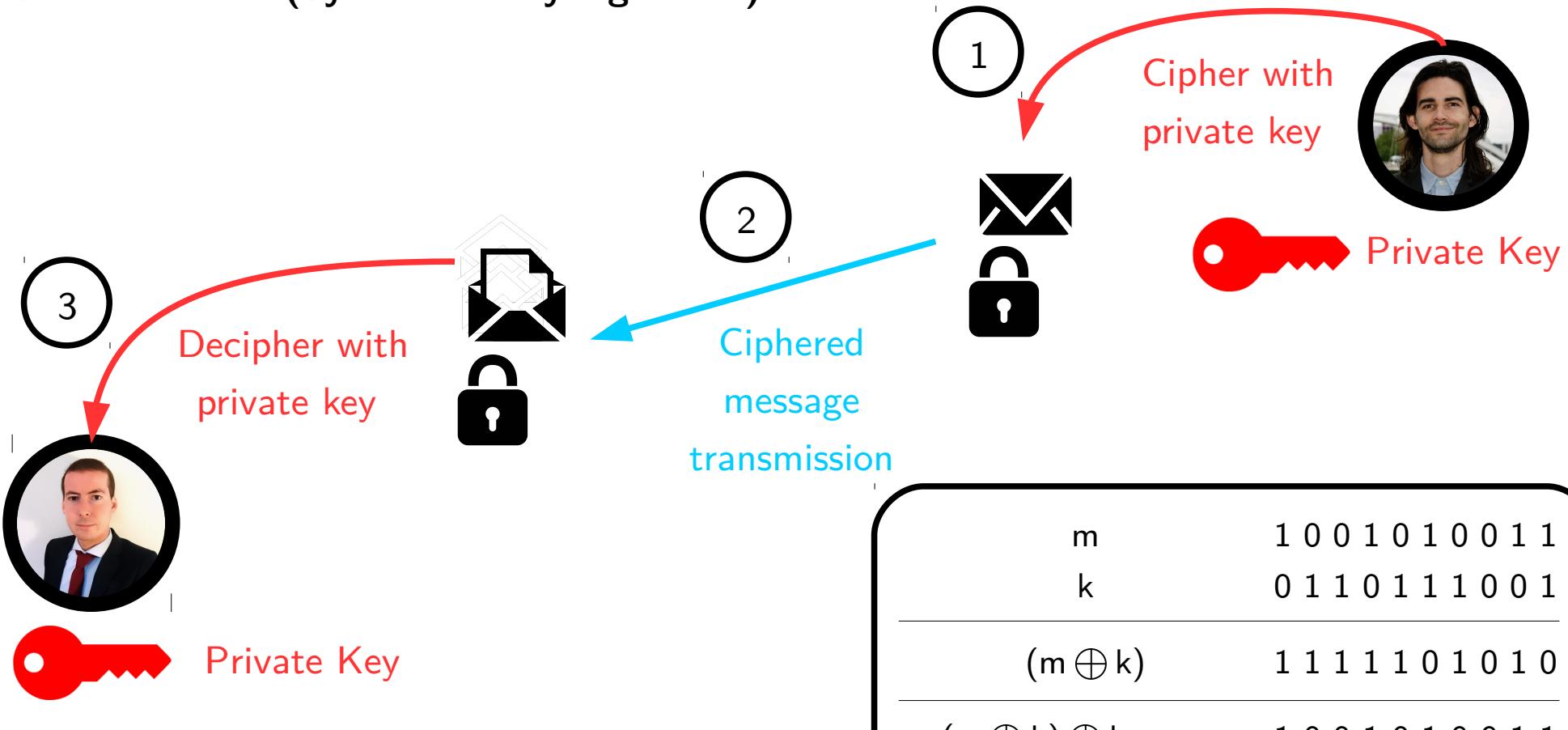
**3 blog links** ([what is this?](#))

[Export citation](#)



## 13.3 Quantum Key Distribution

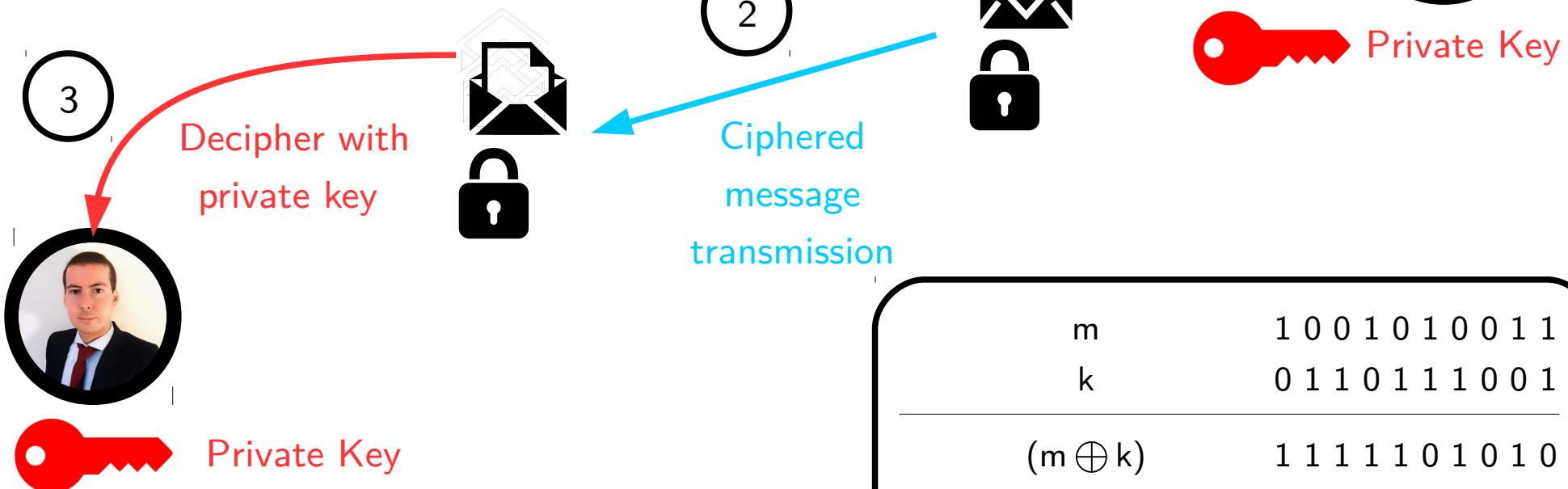
### One-Time Pad (Symmetric-key algorithm)



## One-Time Pad (Symmetric-key algorithm)

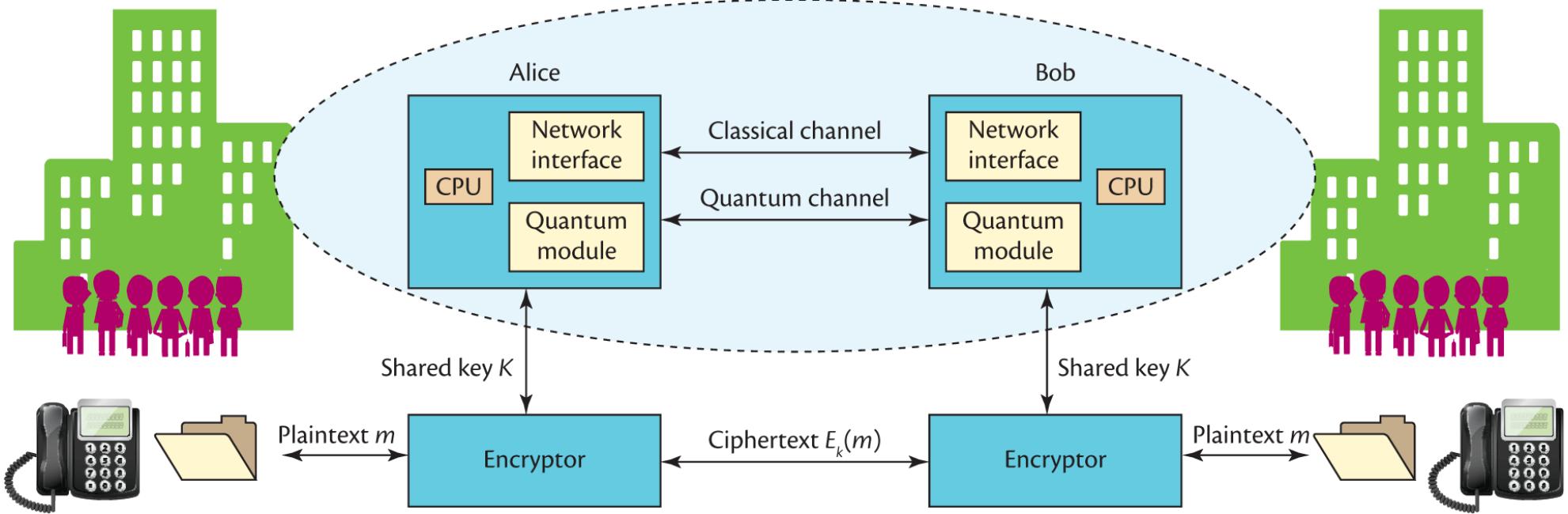
 Information-theoretic security

 Impractical

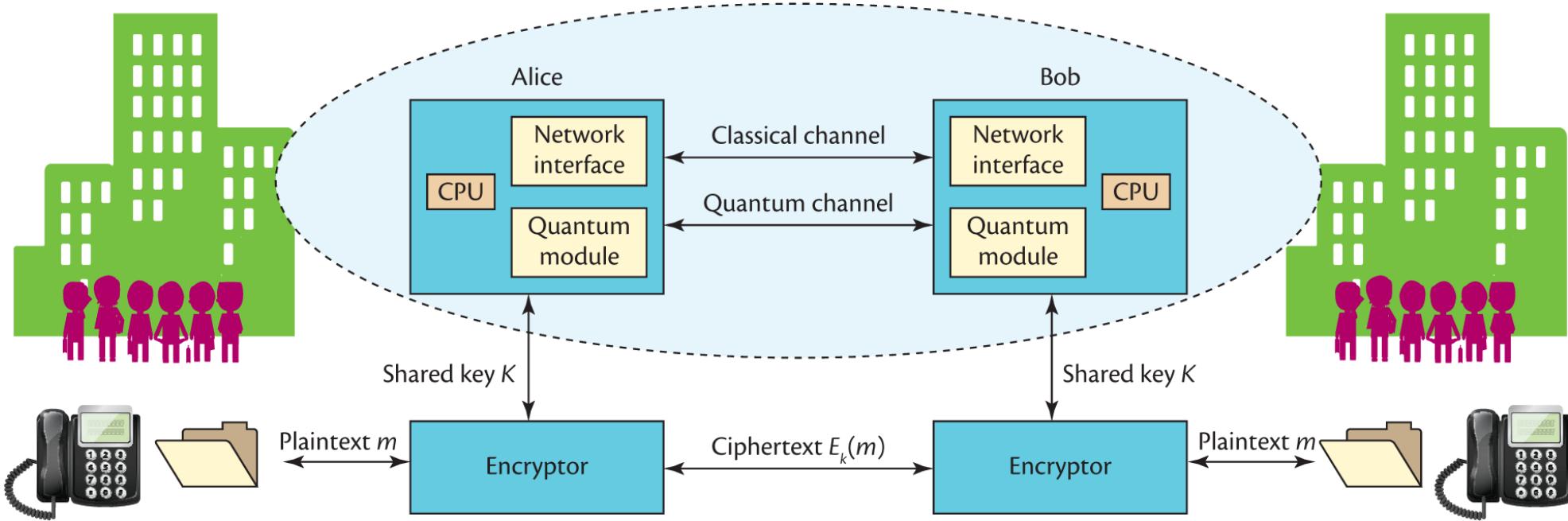


 Private Key

## QKD + One Time Pad



## QKD + One Time Pad

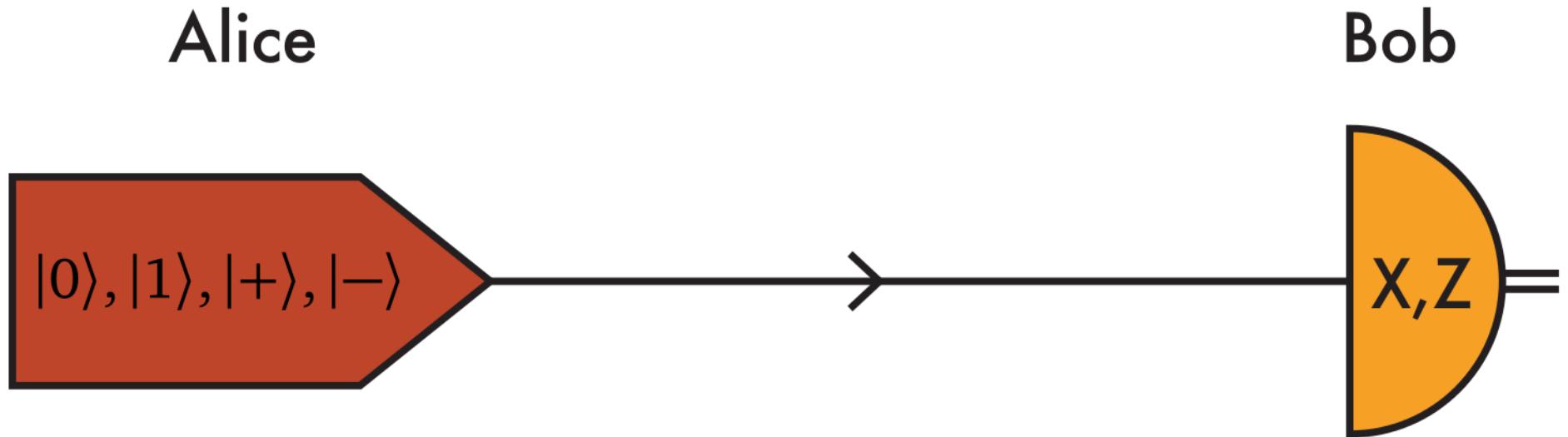


Information-theoretic security



Practicality

## BB84 QKD protocol



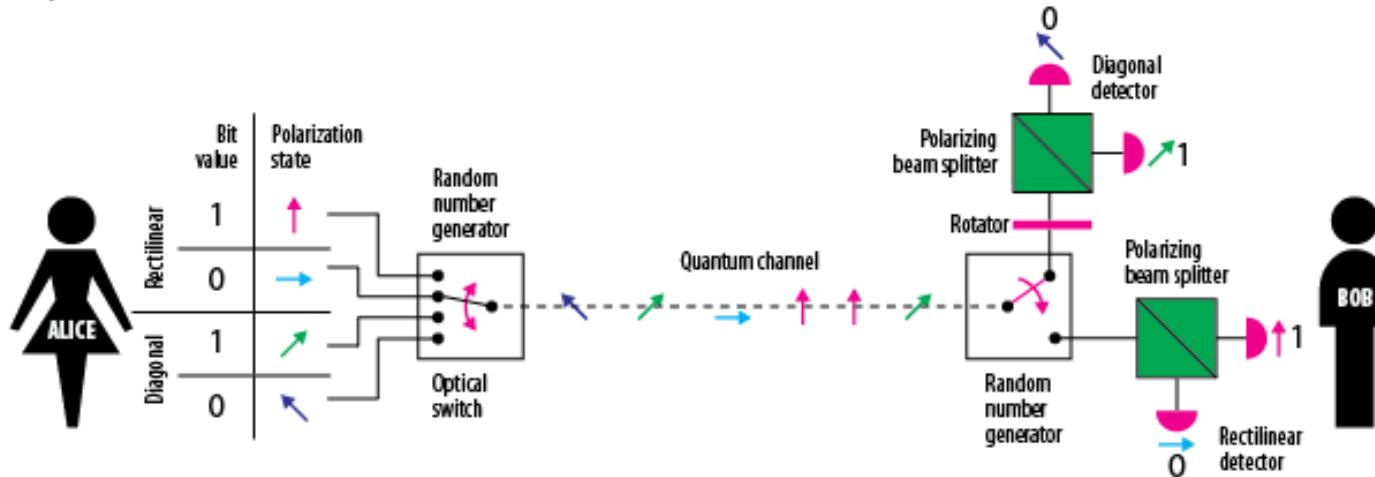
The Hello World of quantum key distribution

Security is provided by:

- Heisenberg uncertainty principle (no commuting operators)
- No cloning theorem

# 13.2 Quantum Key Distribution

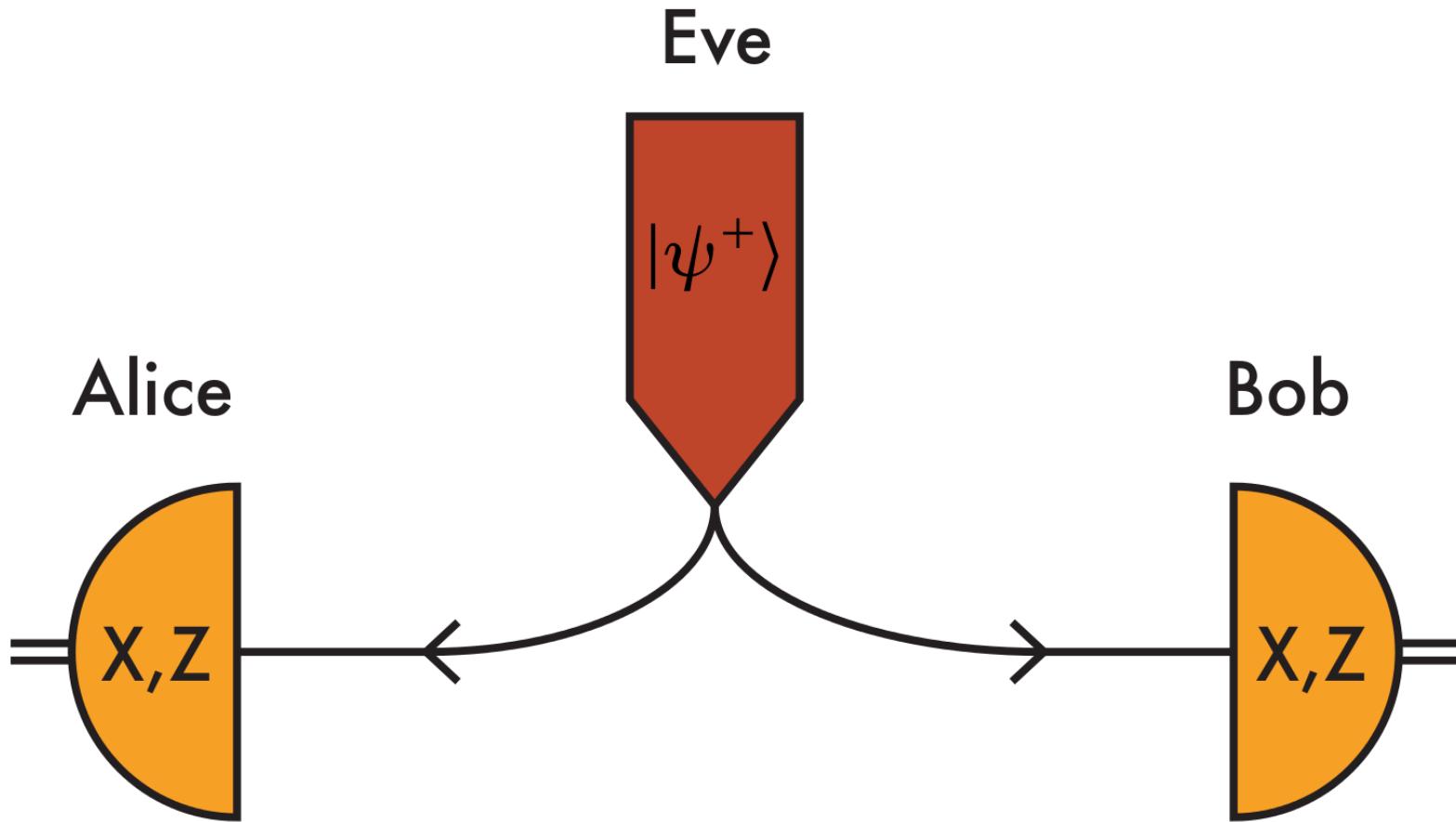
## BB84 QKD protocol



	Quantum transmission & detection							
	Public discussion (i.e., sifting)							
ALICE sends photons	←	→	↑	↑	↑	←	↑	↑
ALICE's random bits	0	1	0	1	1	1	0	1
BOB's detection events	↑	→	←	↑	↑	→	←	↑
BOB's detected bit values	1	1	0	1	1	1	0	0
BOB tells ALICE the basis choices he made	↑←	↗	↖	↑←	↗	↖	↗	↖
ALICE tells BOB which bits to keep	✓	✓	✓	✓	✓	✓	✓	✓
ALICE and BOB's shared sifted key	-	1	-	1	-	1	0	-

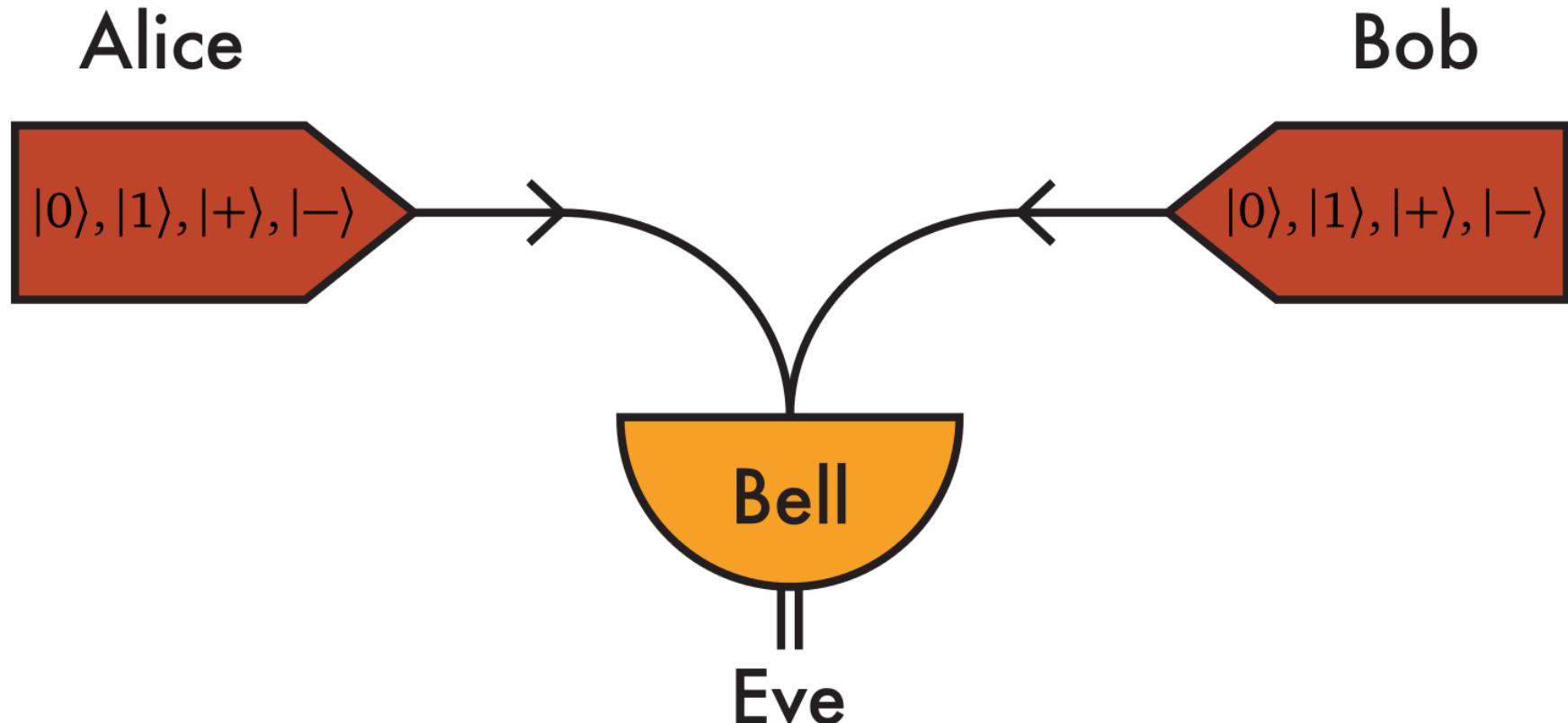


## E91 QKD protocol





## MDI QKD protocol

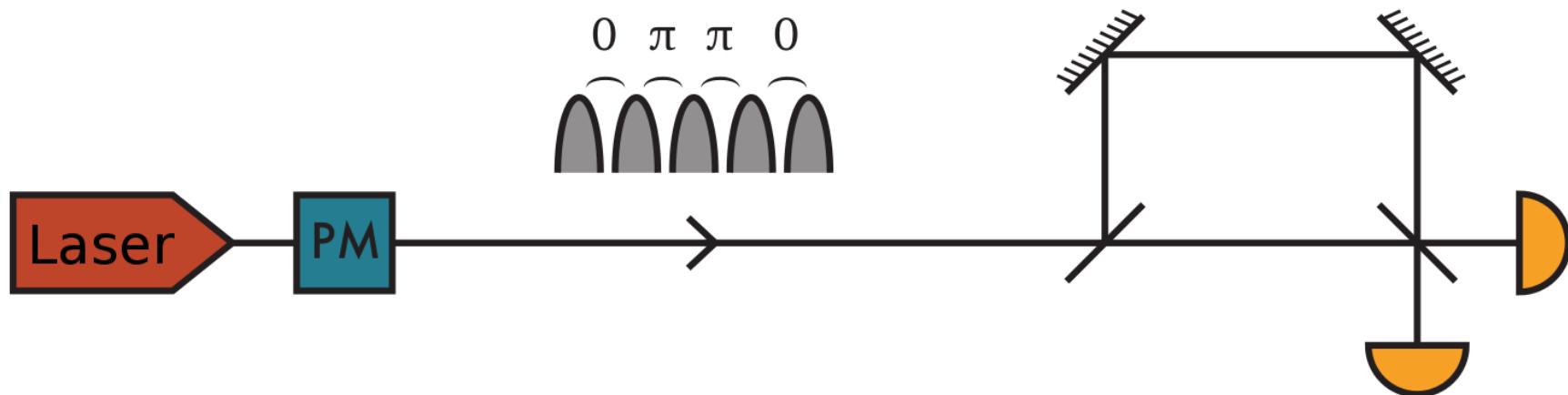




## DPS QKD protocol

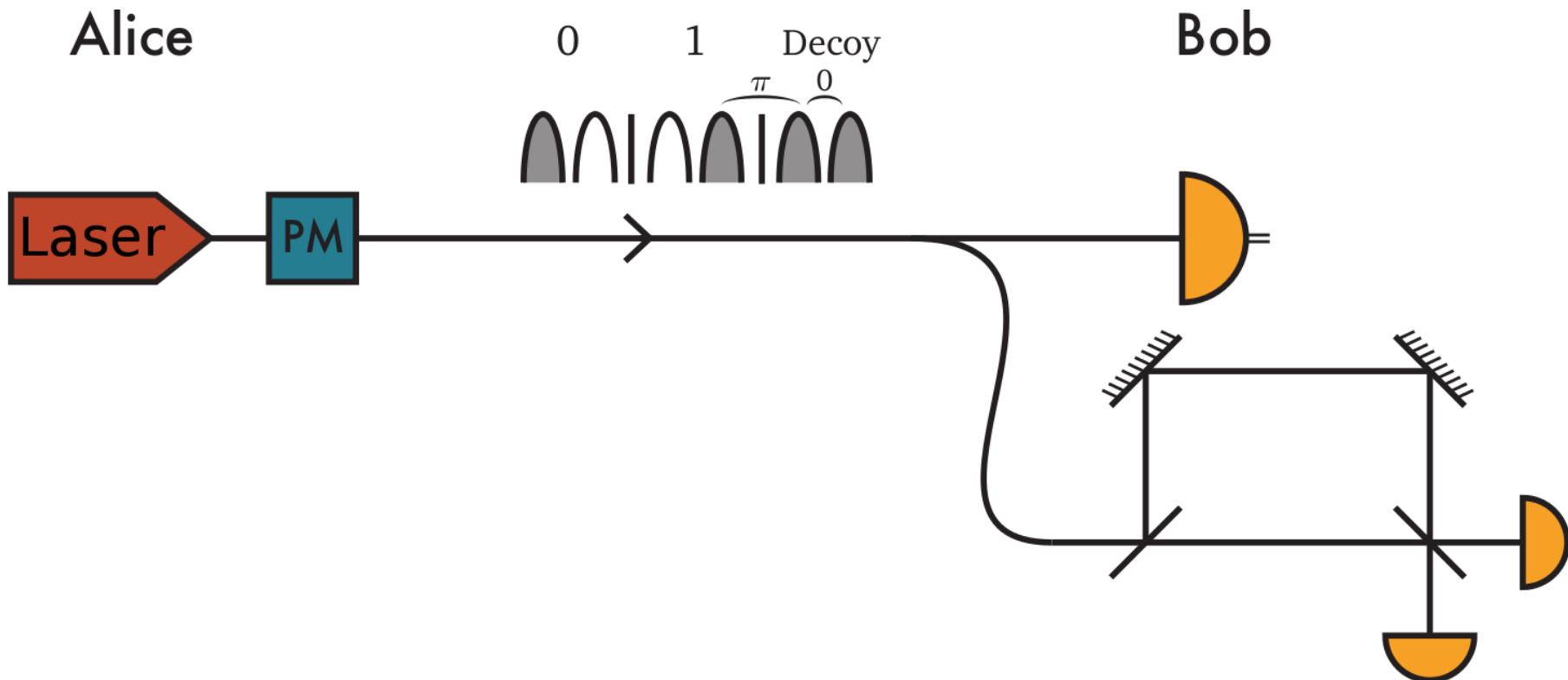
Alice

Bob

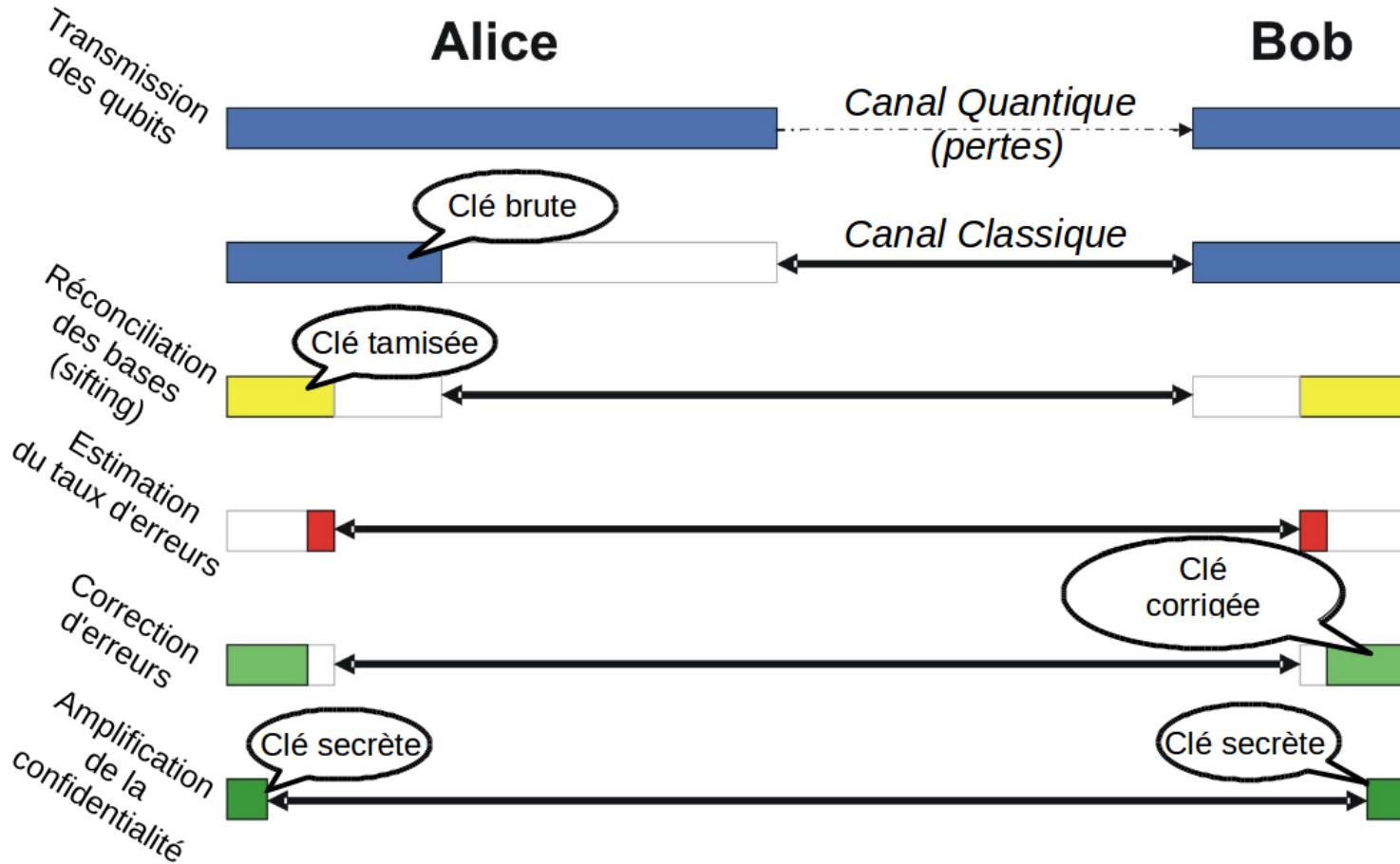




## COW QKD protocol



## Post-processing steps





## 13.3 Quantum Key Distribution

### Field implementations

The screenshot shows the homepage of ID Quantique's website. At the top left is the IDQ logo. To the right are a search bar, a "Partner Portal" button, and a "Shop Online" button with a shopping cart icon. Below the header is a navigation menu with links: Random Number Generation, Quantum-Safe Security, Single-Photon Systems, News & Events, Resource Library, and About IDQ. The main content area features a dark blue background with a network graph of nodes and connections. On the left, there are social media sharing icons for Twitter, LinkedIn, and Email, followed by a news headline: "ID Quantique, SK Telecom & Nokia Secure Optical Transport System Using Quantum Key Distribution (QKD)". A "Learn More" link is located below the headline. On the right, there is a red "Contact Us" button and the "SWISS QUANTUM" logo. At the bottom of the page, there is a short paragraph about ID Quantique's mission and a note about their quantum random number generator.

ID Quantique (IDQ) is the world leader in quantum-safe crypto solutions, designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and quantum key distribution solutions and services to the financial industry, enterprises and government organisations globally.

IDQ also commercializes a quantum random number generator, which is the reference in the security, simulation and gaming industries.



# 13.3 Quantum Key Distribution

## Field implementations

 European Commission | CORDIS  
EU research results

English EN  Search

HOME RESULTS PACKS RESEARCH&EU MAGAZINES NEWS & EVENTS PROJECTS & RESULTS ABOUT US  Sign in

**HORIZON 2020** Open European Quantum Key Distribution Testbed

**Fact Sheet**

**Objective**

OPENQKD brings together a multidisciplinary team of the leading European telecommunication equipment manufacturers, end-users and critical infrastructure providers, network operators, QKD equipment providers, digital security professionals and scientists from 13 countries to reinforce Europe's position at the forefront of quantum communication capabilities globally.

The project will create an open QKD testbed to promote network functionality and use-cases to potential end-users and relevant stakeholders from research and industry. Over 25 use-case trials have already been determined and will be complimented by open calls for funding third parties. OPENQKD will develop an innovation ecosystem and training ground as well as helping to grow the technology and solution supply chains for quantum communication technologies and services.

In preparation for not only managing a central QKD testbed in Geneva (CH), but as precursor to managing a pan-European network, we will incorporate testbeds in Cambridge (UK), Madrid (ES) and Poznan (PL), along with specific use-case-driven test sites, and develop a virtual network of these islands of security as an interim substitute for a QKD backbone, bringing these distant networks together. OPENQKD will deploy 40 QKD systems with standardized hardware and software interfaces for network devices and protocols over 1000km of fiber links, as well as testing compatibility with satellite-based schemes.

The OPENQKD network will be used to demonstrate the transparent integration of quantum-safe technologies and solutions broadly across the European digital landscape as well as advancing initiatives for the standardization and certification of QKD-enabled technologies. The work in the OPENQKD testbed should lay the foundations for rolling out a pan-European quantum-safe digital infrastructure, with a solid basis to educate and lead a quantum-aware workforce and with European industry leaders already engaged.

**Field of Science**

/natural sciences/computer and information sciences/software  
/social sciences/sociology/governance/public services

**Programme(s)**

H2020-EU.2.1.1. - INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies (ICT)

**Project Information**

**OPENQKD**

Grant agreement ID: 857156

Status: Ongoing project

Start date: 2 September 2019 End date: 1 September 2022

Funded under: H2020-EU.2.1.1.

Overall budget: € 17 974 246,25

EU contribution: € 14 999 989,89



Coordinated by:  
**AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH**  
Austria

## Field implementations

