Security Proofs for (Post-)Quantum Cryptography

Céline Chevalier

Université Panthéon-Assas Paris II

UNIVERSITÉ PARIS II
PANTHÉON-ASSAS

February, 6th 2020

Based on joint discussions with Elham Kashefi, Marc Kaplan,
Tanguy Roumain de la Touche, Luka Music, Quoc Huy Vu and Ehsan Ebrahimi
(ANR Project CryptiQ)

Roadmap

Roadmap

Secure Communication

Security Goals

- confidentiality: nothing revealed on the message
- integrity: no modification of the message
- authentication: the sender's identity is guaranteed

$\xrightarrow{m_A}$

$\xleftarrow{m_B}$

Alice

Bob

Secure Communication

Security Goals (communication controlled by the adversary)

- confidentiality: nothing revealed on the message
- integrity: no modification of the message
- authentication: the sender's identity is guaranteed

Secure Communication

Security Goals (create a secure shared secret key: AKE)

- confidentiality: nothing revealed on the message (encryption)
- integrity: no modification of the message (signature, MAC)
- authentication: the sender's identity is guaranteed (signature)

Secure communication on the Internet via SSL/TLS protocol

Secure Communication

Goal of the Adversary

obtain "some information": recover a message, a key...

Behaviour of the Adversary

- passive: eavesdropping (against confidentiality)
- active:
  - impersonation (against authentication)
  - action on the transmitted message (against integrity)
    modification, delay, destruction, replay...

Means of the Adversary

- access to an attack algorithm
- (classical) computing capacities: $< 2^{128}$ (minimum $< 2^{80}$)

Symmetric Cryptography
Private-Key Cryptography

Same (private) key for both users (similar to a safe)

m

Alice (K)

$C = Encrypt_K(m)$ →

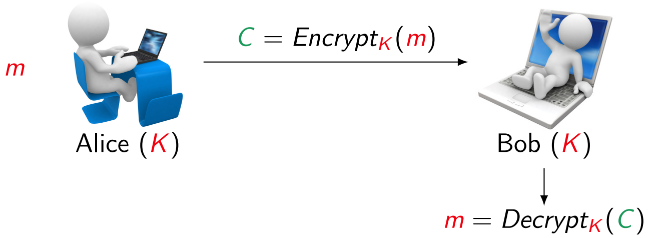
Bob (K)

↓

$m = Decrypt_K(C)$

Security: impossible to recover m from C without knowing K

Same (private) key for both users (similar to a safe)



Security: impossible to recover m from C without knowing K

- ✔ efficiency: small parameters (128-bit key for security in 2^{128} operations)
- ✘ need for a pre-shared key
- ✘ storage of keys: $n(n-1)/2$ for n people
- ✘ no security proof
  (constructions based on heuristics: permutations and substitutions)

Asymmetric Cryptography

Public-Key Cryptography

Pair of (private, public) keys for each user (similar to a mailbox and its key)

m  $C = Encrypt_{pk_B}(m)$ → 

Alice (pk_B)

Bob ((pk_B, sk_B))

↓

$m = Decrypt_{sk_B}(C)$

Security: impossible to recover m from C without knowing sk_B

Pair of (private, public) keys for each user (similar to a mailbox and its key)

m

Alice (pk_B)

$C = Encrypt_{pk_B}(m)$ →

Bob ((pk_B, sk_B))

↓

$m = Decrypt_{sk_B}(C)$

Security: impossible to recover m from C without knowing sk_B

- ✘ efficiency: big parameters (2048-bit key for RSA for security in 2^{128} op.)
- ✔ no previous interaction
- ✘ confidence in the key (certificates)
- ✔ security proof
- ✔✘ computational assumption (factoring, discrete log. ...)

Symmetric or Asymmetric Cryptography?

Symmetric Cryptography:
private key pre-shared between two users

- ✔ efficiency: small parameters (128-bit key for security in 2^{128} operations)
- ✘ need for a pre-shared key
- ✘ storage of keys: $n(n-1)/2$ for n people
- ✘ no security proof

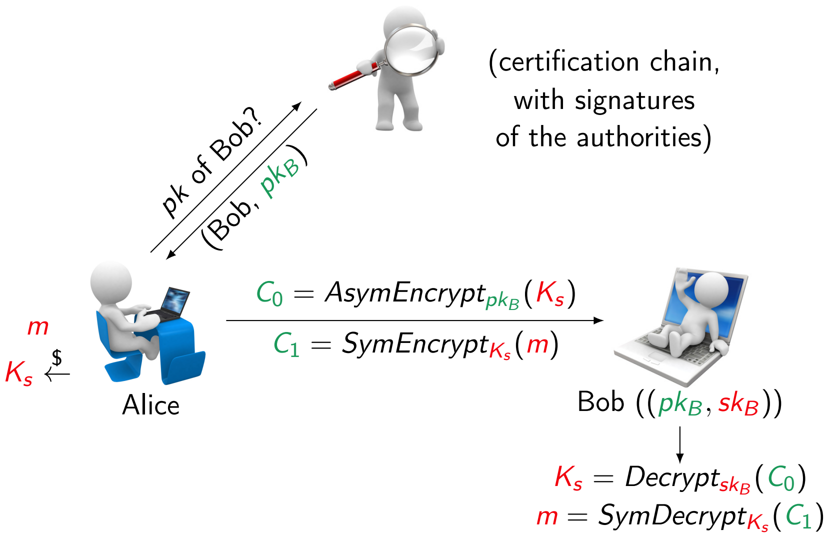
Asymmetric Cryptography:
Pair of (public, private) keys for each user

- ✘ efficiency: big parameters (2048-bit key for RSA for security in 2^{128} operations)
- ✔ no previous interaction
- ✘ confidence in the key (certificates)
- ✔ security proof
- ✔✘ computational assumption (factoring, discrete log. ...)

Solution: asymmetric key exchange + symmetric encryption (SSL/TLS)

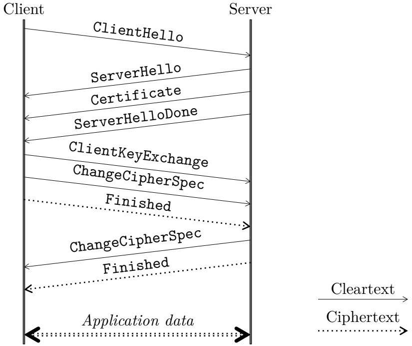
Transport Layer Security (TLS) – Using RSA

Combining Symmetric and Asymmetric Cryptography using Certificates



Transport Layer Security (TLS) – Using RSA

Overview of the Protocol



SSL/TLS: a security protocol providing

- server authentication
- data confidentiality and integrity

Two phases

- Handshake protocol
  - algorithm negotiation
  - server authentication
  - key exchange
- Record protocol
  - application data exchanges

(slide courtesy of O. Levillain)

Transport Layer Security (TLS) – Using DHE/RSA

Combining Symmetric and Asymmetric Cryptography using Certificates

(certification chain, with signatures of the authorities)

vk of Bob?

(Bob, vk_B)

m

Alice

$DHE(Alice, Bob)$

$C_1 = SymEncrypt_{K_s}(m)$

Bob $((vk_B, sk_B))$

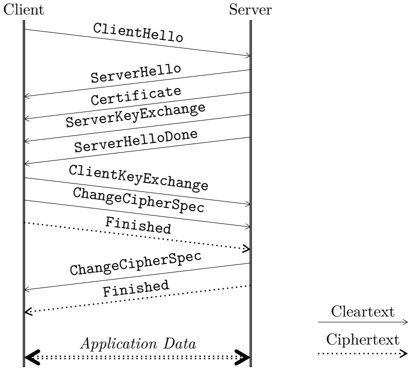
$K_s = DHE(Alice, Bob)$

$K_s = DHE(Alice, Bob)$

$m = SymDecrypt_{K_s}(C_1)$

Transport Layer Security (TLS) – Using DHE/RSA

Overview of the Protocol



SSL/TLS: a security protocol providing

- server authentication
- data confidentiality and integrity

Two phases

- Handshake protocol
  - algorithm negotiation
  - server authentication
  - key exchange
- Record protocol
  - application data exchanges

(slide courtesy of O. Levillain)

RSA Encryption Scheme [RivestShamirAdleman'78]

Algorithm

p, q prime numbers
$n = pq$

e such that $e \wedge \varphi(n) = 1$ (with $\varphi(n) = (p-1)(q-1)$)
$d = e^{-1} \mod \varphi(n)$

public key: $pk = (n, e)$
private key: $sk = (n, d)$

$Encrypt_{pk}(m) = m^e \bmod n$
$Decrypt_{sk}(c) = c^d \bmod n$

Correctness

Fermat's little theorem: $a^{\varphi(n)} = 1 \bmod n$
$de = 1 + k\ \varphi(n)$
$c^d \bmod n = m^{de} \bmod n = m \times m^{k\ \varphi(n)} \bmod n = m \bmod n$

Diffie-Hellman Key Exchange [DiffieHellman'76]

Algorithm

G a cyclic group of order q, g a generator of G

a

Alice

$A = g^a \bmod q$ →

← $B = g^b \bmod q$

Bob

b

Alice: ↓ $K_s = B^a$

Bob: ↓ $K_s = A^b$

Signed Diffie-Hellman (DHE/RSA)

to avoid man-in-the-middle attack (server authentication)
signature/verification keys for Bob: (sk_B, vk_B)
Bob adds a signature $\sigma = Sign_{sk_B}(B)$
Alice checks the signature $Verify_{vk_B}(B, \sigma)$

Roadmap

m

Alice

$C = Encrypt_{pk_B}(m)$ $\longrightarrow$

Bob $((pk_B, sk_B))$

$\downarrow$

$m = Decrypt_{sk_B}(C)$

Encrypt/Decrypt: trapdoor one-way function

- Encrypt: easy operation
- Decrypt: difficult operation... — one-wayness
- ... unless sk_B is known — trapdoor

$\longrightarrow$ computational assumptions

Factoring

$n = pq$, with p and q secret

Problem: Find p and q

Records:

- 768 bits (232 decimal digits), Number Field Sieve, December 2009 (2000 years of computing on a single core 2.2 GHz AMD Opteron)
- 795 bits (240 decimal digits), Number Field Sieve, November 2019 (900 core-years on a 2.1 GHz Intel Xeon Gold 6130 CPU)

Factoring

$n = pq$, with p and q secret

Problem: Find p and q

RSA Problem [RivestShamirAdleman'78]

$n = pq$, with p et q secret, $e, y \in \mathbb{Z}[n]^*$

Problem: Find x such that $y = x^e \bmod n$

Comparison

Factoring $\Longrightarrow$ Solving RSA problem:
$\varphi(n) = (p-1)(q-1)$ and $d = e^{-1} \bmod \varphi(n)$
Trapdoor: prime factors of n

Discrete Logarithm

$G = \langle g \rangle$ cyclic group of order q, $X \in G$

Problem: Find x such that $X = g^x$

Records:

- 768 bits (232 decimal digits), June 2016
- 795 bits (240 decimal digits), Number Field Sieve, November 2019 (3100 core-years on a 2.1 GHz Intel Xeon Gold 6130 CPU)

Discrete Logarithm

$G = \langle g \rangle$ cyclic group of order q, $X \in G$

Problem: Find x such that $X = g^x$

Computational Diffie-Hellman Probem [DiffieHellman'76]

$G = \langle g \rangle$ cyclic group of order q, $X = g^x \in G$, $Y = g^y \in G$

Problem: Compute g^{xy}

Comparison

Solving DL $\Longrightarrow$ Solving CDH
DL: Weakest (thus preferred) assumption

Discrete Logarithm

$G = \langle g \rangle$ cyclic group of order q, $X \in G$

Problem: Find x such that $X = g^x$

Decisional Diffie-Hellman Probem [DiffieHellman'76]

$G = \langle g \rangle$ cyclic group of order q, $X = g^x \in G$, $Y = g^y \in G$, $Z \in G$

Problem: Decide whether $Z = g^{xy}$

Comparison

Solving DL $\Longrightarrow$ Solving CDH $\Longrightarrow$ Solving DDH
DL: Weakest
DDH: Strongest

Security Proofs for Asymmetric Cryptography

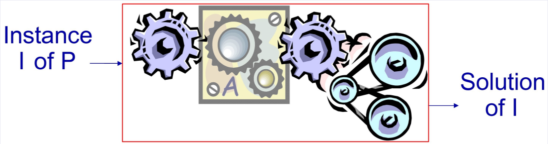
By reduction to a Computational Assumption

Principle

Security Proof:
guarantee that an assumption is sufficient to ensure the required notion
If an adversary can break the protocol,
Then one can build an adversary breaking the assumption

Proof by reduction

Let $\mathcal{A}$ be an adversary against the protocol.
One constructs an adversary $\mathcal{B}$ that breaks a problem P.



Conclusion: P intractable $\Longrightarrow$ $\mathcal{A}$ cannot exist $\Longrightarrow$ secure protocol

(slide courtesy of D. Pointcheval)

Security Proofs for Asymmetric Cryptography

By reduction to a Computational Assumption

Security Proof for a Protocol

- Computational Assumption (factoring, DH...)
- Security Notion (depending on the type of protocol)
- Reduction (construction of an adversary against the assumption using the adversary against the protocol)

Which Consequences for Broken Assumptions?

- Imagine a protocol is proven secure under the factoring assumption...
- and a quantum computer breaks this assumption,
- then the security proof remains sound...
- but does not give any guarantee anymore on the security of the protocol!

Roadmap

Quantum Attack Algorithms

Against Asymmetric Cryptography

Shor's Algorithm [Shor'99]

Algorithm for factoring an integer N (and computing discrete logarithms)

Complexity of number field sieve: $\exp(O(n^{1/3}(\log n)^{2/3}))$
Complexity of Shor's algorithm: $O(n^2 \log n \log \log n)$
with $n = \log_2 N$

Need for more than 10000 qubits for factoring 2048-bit RSA modulus

Post-Quantum RSA Encryption Scheme

To guarantee the same security than 2048-bit keys:

- needed size of keys: 2^{42} bits $=$ 1TB
- duration of key generation: 2 days for 3.166TB RAM

Need for new computational assumptions...

Steps of the Algorithm

1. Choose $m \in \mathbb{N}^*$ at random.
   If $\mathrm{pgcd}\,(m, N) \neq 1$, halt ($m$ is a non-trivial factor of N).
2. Apply the quantum period finding protocol to determine the unknown period P of the function:

$$f_N : \begin{cases} \mathbb{N} \longrightarrow \mathbb{N} \\ a \longmapsto m^a \bmod N \end{cases}$$

3. If P is odd, go back to step 1
   (with probability $1/2^k$, where k is the number of distinct factors of N).

Steps of the Algorithm

4. Since P is even,

$$(m^{P/2} - 1)(m^{P/2} + 1) = m^P - 1 \equiv 0 \bmod N$$

   If $m^{P/2} + 1 \equiv 0 \bmod N$, go back to step 1
   (with probability less than $(1/2)^{k-1}$).
5. Use the euclidean algorithm to compute $d = \mathrm{pgcd}\,(m^{P/2} - 1, N)$, which is a non-trivial factor of N.

High-Level Idea of Shor's Algorithm

Quantum Period Finding Algorithm

Substeps of the Quantum Algorithm (Step 2)

a. Choose $Q = 2^L$ with $N^2 \leqslant Q < 2N^2$.
Initialize two registers (input and output):

$$|\Psi_0\rangle = |0\ldots0\rangle|0\ldots0\rangle$$

b. Apply the quantum Fourier transform to the first register:

$$|\Psi_0\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|0\rangle$$

It contains all the integers $0, 1, \ldots, Q-1$ in superposition.

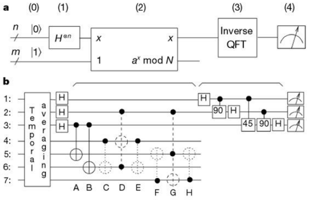
c. Apply the unitary transformation $|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$:

$$|\Psi_1\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|f(x)\rangle$$

The two registers are now entangled.

Substeps of the Quantum Algorithm (Step 2)

- d Apply the quantum Fourier transform to the first register.
  It creates a stochastic source which outputs a symbol $y \in \{0, \ldots, Q-1\}$ with a probability linked with f.
- e Measure register 1: $y/N = k/r$ with r being a candidate for the period (otherwise, start again).



(Shor's algorithm, from Nature 414883)

Quantum Attack Algorithms

Against Symmetric Cryptography

Grover's Algorithm [Grover'96]

Unstructured search algorithm

Quadratic speedup for exhaustive search of the secret key of a symmetric encryption scheme

A little less for collision search on hash functions

Complexities of Attacks

Encryption scheme	Cl. adversary	Q. adversary	Post-quantum secure?
AES128	2^{128}	2^{64}	✘
AES256	2^{256}	2^{128}	✔
sha256	2^{128}	2^{85}	?
sha512	2^{256}	2^{170}	✔

Without new attacks, doubling the size of keys is sufficient.

High-Level Idea of Grover's Algorithm

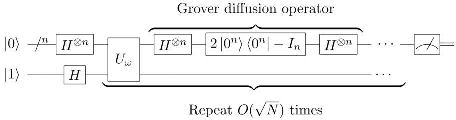
Goal of the algorithm: unstructured search

Given $X = \{x_1, \ldots, x_N\}$ and $f \colon X \longrightarrow \{0, 1\}$,
find $x^\star \in X$ such that $f(x^\star) = 1$

Classical search: $O(N)$ queries

Quantum search : $O(\sqrt{N})$ queries
with high probability of success
optimal complexity

High-Level Idea of Grover's Algorithm



(Grover's algorithm, from Wikipedia)

Steps of the Algorithm

- Preparation of a state in superposition ($n = \log_2(N)$:

$$|\Psi_0\rangle = \frac{1}{2^n} \sum_{x=0}^{2^N-1} |x\rangle$$

- Application of two operators (Grover iteration) several times, to check whether a quantum state fulfills a certain property
- Amplitude amplification
- Measurement

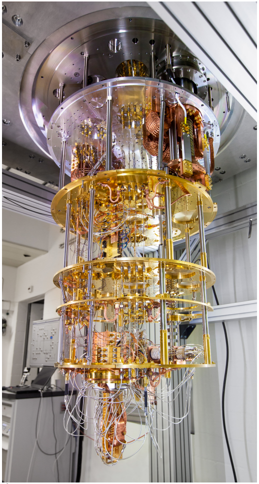
Industrial Context

Quantum Adversary?

[Shor'99] and [Grover'96] algorithms for factoring and search

➤ asymetric cryptography potentially threatened
(risk of attack against the computational assumptions)

➤ emergence of so-called post-quantum cryptography
(computational assumption resistant to quantum computer)



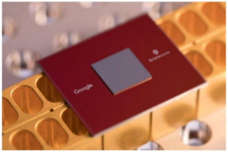
(IBM's quantum computer based on superconducting qubits, from Wikipedia)

Industrial Context

Quantum Adversary?

The quantum computer, a concrete problem? Not clear yet...

- ✘ still a lot of technical challenges
- ✔ but some recent progress:
  - 2006: feasability announcement by IBM
  - 2016: IBM 16 qubits
  - 2018: Google, Bristlecone 72 qubits
  - 2019: quantum supremacy announcement

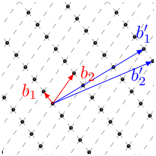


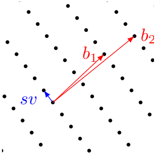
“Only a rash person would declare that there will be no useful quantum computers by the year 2050, but only a rash person would predict that there will be.‘” (N. Mermin)

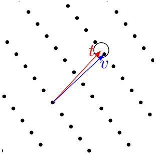
- ✔ but standardisation competition of the NIST (encryption and signature)

“NSA will initiate a transition to quantum resistant algorithms in the not too distant future.‘” (source *NSA*)

- lattices
- error-correcting codes
- supersingular isogenies
- multivariate equations
- hash functions







Computational Problems

- find a good basis (SIVP)
- find a short vector (SVP)
- find a vector close to another one (CVP)
- solve a noisy linear system (LWE)

Learning with Errors (LWE)

LWE Assumptions [Regev'05]

$q \geqslant 2$ prime
$a_i \in \mathbb{Z}_q^n$ public
$s \in \mathbb{Z}_q^n$ secret
many noisy inner products $b_i = \langle a_i, s \rangle + e_i \in \mathbb{Z}_q$

- Computational: Given (a_i) and (b_i), compute s
- Decisional: Given $A = (a_i)$,
  distinguish $(A, {}^tA\,s + e)$ from uniform (A, b)

For a good choice of parameters, at least as hard as solving SIVP for polynomial approximation factors [Regev'05]

Standardisation Competition of the NIST

Agenda

- 2012 : creation of PQC project
- 2015 : beginning of the competition
- 2017 : 69 submissions accepted to round 1
- 2019 : 26 submissions accepted to round 2
- ... : round 3?

Goal: obtain **several** secure post-quantum algorithms for encryption and signature

Application Conditions

- strong theoretical foundations
- no requirement for a security proof
- portable implementation

Standardisation Competition of the NIST

Overview of the Competition (Round 2)

- 17 candidates for encryption (lattices, codes, isogenies)
- 9 candidates for signature (lattice, multivariate equations, hash functions)
- quite difficult to follow, huge domain
- several monitoring projects, partial comparison tools
- no concise documentation
- requirements not well specified
  - API defined by Dan J. Bernstein
  - only external interface naming conventions:
    - crypto_kem_mceliece348864f_ref_keypair
    - r5_cca_kem_keygen
  - variable comment quality
  - code with or without crypto library, with hard links to .so or .a files...

Roadmap

Quantum Cryptographic Algorithms

New Laws of Physics and Hope for Unconditional Security

irreversibility of measurement, no-cloning theorem, entanglement...

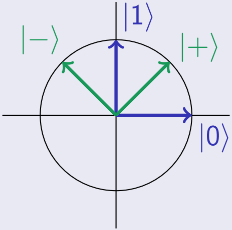
History of Quantum Cryptographic Algorithms

- [Wiesner'70] quantum money, first link between secrecy and quantum physics (bills with photons polarized by the bank in random directions)
- [BennettBrassard'84] quantum key distribution
- [HilleryBuzekBerthiaume'99, CleveGottesmanLo'99] quantum secret sharing
- [GottesmanChuang'01] quantum digital signature (similar to the classical case, based on one-way quantum function)
- [Broadbent, FitzsimonsKashefi'09] blind quantum computing

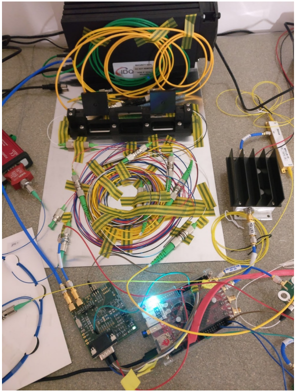
BB84 Quantum Key Distribution Algorithm

High-Level Idea

Encoding of the bits



$+$ basis: $|0\rangle$ for 0, $|1\rangle$ for 1
$\times$ basis: $|+\rangle$ for 0, $|-\rangle$ for 1



(Implementation of QKD at VeriQloud)

Alice: chooses a bit (0 or 1) and chooses a basis ($+$ or $\times$)
sends the corresponding polarized photon

Main Steps of the Algorithm

Quantum Communication	Random bits chosen by Alice	0	1	1	0	1	0	0	0	1	0
	Random basis chosen by Alice	×	+	+	×	+	×	+	+	×	+
	Sent photons	↗	↑	↑	↗	↑	↗	→	→	↖	→
	Random basis chosen by Bob	+	×	+	×	×	×	+	×	+	+
	Bits received by Bob	1		1		0	0	0		1	0
Authenticated public communication	Failures revealed by Bob		✘		✘				✘		
	Raw key of Alice	0		1		1	0	0		1	0
	Raw key of Bob	1		1		0	0	0		1	0
	Basis revealed by Bob	+		+		×	×	+		+	+
	Alice's answer			✓			✓	✓			✓
	A priori shared bits (sifted key)			1			0	0			0

BB84 Quantum Key Distribution Algorithm

High-Level Idea

Idea of the Security

Correctness: properties of the measurement
Security: irreversibility of the measurement, no-cloning theorem

Types of Attacks

- individual attacks: interaction of Eve with each qubit separately and independently
  only attacks feasible with current technology
- collective attacks: interaction of Eve with each qubit independently, but joint measurement
- coherent attacks: preparation of an arbitrary entangled state, interaction with all the qubits and joint measurement

BB84 Quantum Key Distribution Algorithm

High-Level Idea

One Possible Eavesdropping Attack: Intercept-resend

- situations halted in the sifting phase:

Alice	Eve	Bob
$+$	$+$	$\times$
$+$	$\times$	$\times$

Alice	Eve	Bob
$\times$	$+$	$+$
$\times$	$\times$	$+$

- situations leading to an abnormal error for Bob (with half probability):

Alice	Eve	Bob
$+$	$\times$	$+$
$\times$	$+$	$\times$

- situations leading to no error for Bob:

Alice	Eve	Bob
$+$	$+$	$+$
$\times$	$\times$	$\times$

- consequence: 25% errors due to eavesdropping, 75% bits learnt by Eve

BB84 Quantum Key Distribution Algorithm

High-Level Idea

Last Steps of the Protocol (from sifted key to secret key)

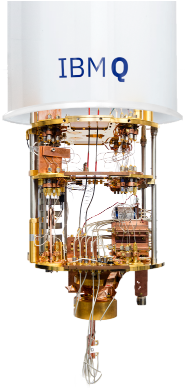
- Reconciliation
  Alice and Bob discard a certain amount of bits to check the error rate. Above $\approx 11\%$, they abort the protocol.
- Error correction
- Privacy amplification

Example: sifted key (b_1, b_2, b_3, b_4)
estimation of information known by Eve: $\leqslant 1$ bit

secret key: $(b_1 \oplus b_2, b_3 \oplus b_4)$
information known by Eve: 0 bit

Industrial Context

Maybe a quantum adversary to fear,
but also positive aspects...



Quantum user?

Several proofs of existence
of quantum communication:

- 2000 km of quantum network in China,
  China-Austria satellite communication...
- access to IBM-Q platform
- concrete deployment of protocols:
  first implementations of QKD
  by IDQuantique in the years 2000

➤ need to consider and model
both quantum adversaries and users

Quantum-Enhanced Cryptography

Quantum-Enhanced Cryptography

- classical user, quantum adversary
- quantum communication allowed
- classical cryptography, post-quantum assumptions
- promising improvements in terms of security, efficiency...

Classical multiparty computation using quantum resources [Clementi et al'17]

- classical users with linear classical processing (classical XOR gates)
- quantum communication (single qubit gates on quantum states)
- joint computation of a non-linear multivariable function
- proof of concept: 4 users, pairwise AND, implementation using photonic bits

Roadmap

Different Flavors of Cryptography

Post-Quantum Cryptography

- classical user, quantum adversary
- classical cryptography, post-quantum assumptions

Different Flavors of Cryptography

Post-Quantum Cryptography

- classical user, quantum adversary
- classical cryptography, post-quantum assumptions

Quantum Cryptography

- quantum user, quantum adversary
- quantum cryptography, post-quantum assumptions

Different Flavors of Cryptography

Post-Quantum Cryptography

- classical user, quantum adversary
- classical cryptography, post-quantum assumptions

Quantum-Enhanced Cryptography

- classical user, quantum adversary, quantum communication
- hybrid cryptography, post-quantum assumptions

Quantum Cryptography

- quantum user, quantum adversary
- quantum cryptography, post-quantum assumptions

Search for Unconditional Security

New Laws of Physics and Hope for Unconditional Security

No more computational assumptions? Not quite...

History of Impossibilities

- [LoChau'97, Mayers'97] impossibility of unconditionally secure bit commitment and oblivious transfer
- [Damgaard et al'07, WehnerSchaffnerTerhal'07] bounded storage models
  possibility of unconditionally secure bit commitment and oblivious transfer
  (honest parties need no quantum memory and adversary needs to store at least $n/2$ qubits to break the protocol)
- [ChaillouxKerenidis'09] 2-party coin flipping
  (impossibility of perfect security, bounds)

Search for Unconditional Security

New Laws of Physics and Hope for Unconditional Security

No more computational assumptions? Not quite...

The Case of QKD

- need for authenticated channels
- [Unruh'10] everlasting security
  adversary classical during the execution, quantum afterwards
  possibility of everlastingly secure QKD using signature cards
- impossibility of everlasting PAKE with reasonable setup assumptions

New Models and Security Proofs

Adapting Usual Simulating Tricks

- Rewinding the adversary [Watrous'09, Unruh'12]
- Observing or programming random oracles [Boneh et al'10]
- Superposition access to oracles, protocols...
- Modeling "evident actions": store queries, test an equality, compare values...

Adapting Communication and Security Models

- Coexistence of classical and quantum channels
- Superposition attacks