Quantum cryptography

Quantum communication

G. Chênevert

October 23, 2020

Quantum cryptography

A quick overview of cryptography

BB84

E91

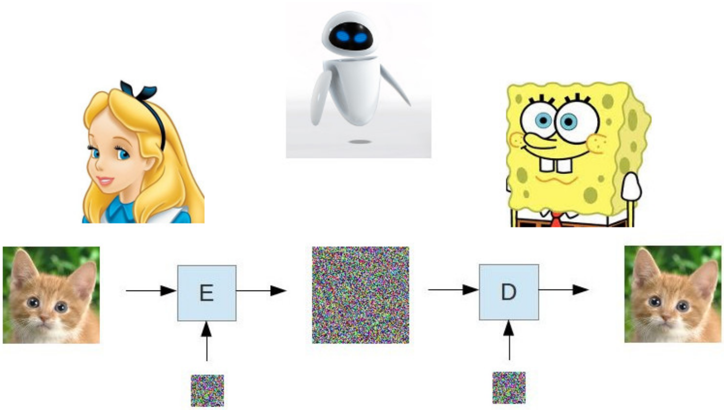
What is cryptography?

Cryptography is a set of techniques that allows *secure* communication between two or more parties, even in the presence of rational adversaries.

Desirable properties for secure communication include:

- confidentiality
- message integrity
- sender authentication

Confidentiality



Symmetric encryption

The bulk of today's digital information transiting on communication is encrypted using **secret-key encryption algorithms** such as the

Advanced Encryption Standard (AES)

Standardized by the US NIST in 2001 following an international competition

Uses 128-bit random keys

Exercise: Eve could always try to *guess* what the key is to recover the message...

How long in your estimate would it take her? (hint: much too long)

The key distribution problem

How do Alice and Bob end up with the secret keys to begin with??

Classical solutions to the key distribution problem

- previous access to a secure channel (!)
- trusted third party (*e.g.* Kerberos)
- public-key encryption (*e.g.* RSA)
- key agreement protocol (Diffie-Hellman)

This is the standard method used today for example in SSL/TLS ("https")

Based on the assumed hardness of the *discrete logarithm problem*

Diffie-Hellman key agreement protocol (1976)

- Alice and Bob agree on a set of (safe) parameters n and g
- Alice chooses a random α and computes $a \underset{n}{\equiv} g^{\alpha}$
- Bob chooses a random β and computes $b \underset{n}{\equiv} g^{\beta}$
- Alice sends a to Bob; Bob sends b to Alice
- Alice computes $k_A \underset{n}{\equiv} b^{\alpha}$; Bob computes $k_B \underset{n}{\equiv} a^{\beta}$

Since $k_A = k_B$, Alice and Bob end up with a shared secret k.

Some problems remain

Used properly, this allows secure channels with perfect forward secrecy to be set up.

Main vulnerability is the **man-in-the-middle** attack in which an active adversary hijacks the key agreement and sets up a pair of secure channels with Alice and Bob.

$\Longrightarrow$ authentication is needed on top of that, quite complex systems result

(Moreover: most asymmetric algorithms in use today would be broken by a large-scale quantum computer...)

Quantum key distribution (QKD)

often referred to as *Quantum cryptography*

Allows Alice and Bob to agree on a secret key without relying on hardness assumptions on certain computational problems

Two main protocols:

- **BB84** – Bennett & Brassard (1984)

  based on quantum superposition

- **E91** – Ekert (1991)

  based on entanglement

Quantum cryptography

A quick overview of cryptography

BB84

E91

BB84: Idea

Prepare and measure qubits (photons) in two conjugate orthogonal bases,

e.g. **rectilinear**:

$$|+\rangle_0 = |H\rangle, \qquad |+\rangle_1 = |V\rangle$$

and **diagonal**:

$$|\times\rangle_0 = |D\rangle, \qquad |\times\rangle_1 = |A\rangle$$

and make random base choices.

BB84: Basic step

- Alice randomly chooses a preparation basis $\mathcal{A} \in \{+, \times\}$ and a bit $a \in \{0, 1\}$.
- Alice prepares a qubit in state $|\mathcal{A}\rangle_a$ and sends it to Bob on a quantum channel.

- Bob randomly chooses a measurement basis $\mathcal{B} \in \{+, \times\}$ and measures the qubit :

$$b = \mathcal{M}_{\mathcal{B}}|\mathcal{A}\rangle_a.$$

BB84: Basic step

- Alice and Bob tell each other (over a classical channel) which bases $\mathcal{A}$ and $\mathcal{B}$ they chose.
- If $\mathcal{A} = \mathcal{B}$: they now share the common, secret value of $a = b$
- If $\mathcal{A} \neq \mathcal{B}$: they throw a and b away and start again.

On average, a new shared secret bit is obtained every 2 such exchanges.

BB84: Example

Alice randomly picks $\mathcal{A} = \times$ and $a = 0$.

She thus sends a $|\times\rangle_0 = |D\rangle$ photon to Bob.

- First case: Bob by chance chooses the same basis $\mathcal{B} = \times$. Measuring the received $|D\rangle$ in the diagonal basis, he gets (with probability 1) $|D\rangle = |\times\rangle_0$ thus finds $b = 0$.
- Second case: Bob unfortunately chooses the "wrong" basis $\mathcal{B} = +$. Measuring the received $|D\rangle$ in the rectilinear basis, he gets $|+\rangle_0 = |H\rangle$ or $|+\rangle_1 = |V\rangle$ with 50% probability each: the information about Alice's bit a is lost.

BB84: Security

No such thing as a passive attacker on a quantum channel! Necessarily "ActEve"

If she wants to learn something from the qubit in transit, she will:

- choose a measurement basis $\mathcal{E} \in \{+, \times\}$
- get $e = \mathcal{M}_{\mathcal{E}}|\mathcal{A}\rangle_a$ **leaving the qubit in state** $|\mathcal{E}\rangle_e$
- and Bob will in reality get $b = \mathcal{M}_{\mathcal{B}}|\mathcal{E}\rangle_e$.

BB84: Security

If Eve guesses correctly ($\mathbb{P} = \frac{1}{2}$): Alice and Bob have no way to know!

But when she picks the wrong basis: there is 50 % chance that $a \neq b$

So if Alice and Bob tell a and b to each other, they have $\frac{1}{4}$ chance of detecting Eve.

...but they just made their secret bits public

BB84: Security

Solution: exchange more bits than needed.

If Alice and Bob disclose the results of m successful exchanges, the probability that Eve goes undetected is $\left(\frac{3}{4}\right)^m \longrightarrow 0$ as $m \to \infty$.

With enough security bits, Eve will be detected with high probability.

Exercise

How many photons would Alice and Bob need to exchange on average if they want to establish a private 128-bit key with negligible ($\leq \frac{1}{2^{128}}$) probability that an eavesdropper goes undetected?

Answer: 874

Quantum cryptography

A quick overview of cryptography

BB84

E91

E91: Basic idea

Alice and Bob share an entangled pair of qubits in Bell state

$$|\Phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Both measure their qubit, yielding random values a and b with $a = b$.

But how can Eve be detected? She destroys entanglement by measuring one of the qubits, but it's not noticeable in this setup.

E91: Protocol

The problem can be solved by rotating the measurement basis:

$$\mathcal{B}_\theta : \begin{cases} |0\rangle_\theta = \quad \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \\ |1\rangle_\theta = -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle \end{cases}$$

- Alice chooses randomly $\alpha \in \{0, \frac{\pi}{8}, \frac{\pi}{4}\}$ and measures her qubit in basis $\mathcal{B}_\alpha$
  $\rightsquigarrow$ value $|a\rangle_\alpha$.
- Bob chooses randomly $\beta \in \{0, \frac{\pi}{8}, -\frac{\pi}{8}\}$ and measures his qubit in basis $\mathcal{B}_\beta$
  $\rightsquigarrow$ value $|b\rangle_\beta$.

E91: Security

If Alice and Bob selected the same basis ($\mathbb{P} = \frac{2}{9}$): they now share a common random bit $a = b$.

The remaining bits can be used to compute the Bell-CHSH parameter S:

- if the pairs are entangled we get $S = 2\sqrt{2}$
- if Eve destroyed entanglement we have the classical behavior $|S| \leq 2$.

Exercise:

How many entangled pairs need to be transmitted on average in order for Alice and Bob to obtain 128 shared secret bits this way?

Answer: 576