The BB84 cryptologic protocol
of quantum key distribution

Dimitri Petritis

Institut de recherche mathématique de Rennes
Université de Rennes 1 et CNRS (UMR 6625)

Santiago, November 2013
Principles of coding and cryptography

- **Message** = $m \in \mathbb{A}^*$ (monoidal closure of finite alphabet $\mathbb{A}$).
- **Length** of message $|m|$.
- **Coding** $C : \mathbb{A}^* \to \mathbb{A}^*$ (or more generally $\mathbb{B}^*$).
- **Decoding** $D : \mathbb{B}^* \to \mathbb{A}^*$, with $\text{Dom} D = \text{im} C = C(\text{Dom} C)$, such that
  \[ D \circ C|_{\text{Dom} C} = 1. \]

Vigenère’s\(^1\) coding: **key** $k \in \mathbb{A}^*$ with $|k| = |m|$; $c_i = m_i + k_i \mod \mathbb{A}$, $i = 1, \ldots, |m|$; $m_i = c_i - k_i \mod \mathbb{A}$, $i = 1, \ldots, |m|$.

- $\mathbb{A} = \{a, \ldots, z\} \simeq \{0, \ldots, 25\}$; $m =$hello, $k =$chile, $c =$jluws.
- For **cryptography**: $D$ easy to compute, very difficult to guess.

\(^1\)Blaise de Vigenère (1523–1596): diplomat, cryptograph, translator, alchemist, and astrologue.
Vernam’s ciphering (1917)

- Vernam (1917) proposed **US Patent 1310719**.
- \((k_i)_{i=1,\ldots,|m|}\) independent random variables uniformly distributed on \(\mathbb{A}\).
- Key used **only once** (one time pad).
- All keys equiprobable, hence all messages \(m\) corresponding to given ciphering \(c\) equiprobable.
- If we receive a ciphered message of length 39, all \(26^{39} = 1.53 \times 10^{55}\) words can be possible messages. Most of them have no meaning. But even if some have meaning, we don’t know which is the correct one.
- \(m =\) overwhelminglyvictoriousovertheevilaxis and \(m' =\) wewonthebattlebutwedefinitelylostthewar are potential source messages (equiprobable)!
Shannon’s theorem on cryptography

Theorem (Shannon (1949))

- \(|m|\) is large,
- \(|k| = |m|, \) and
- the key is used only once,

imply\(^a\) that Vernam’s ciphering is ideal (inviolable for all practical purposes).


- BUT: How to communicate the key?
- Vernam’s ciphering abandoned.
- Rivest, Shamir, Adleman (1978), or more generally “discrete logarithm protocols” used instead.
Is RSA secure?

If \( p, q \) large primes and \( N = pq \) then hard to factor \( N \). Denote \( n = \log N \).

- Beginnings of RSA protocol (1978), \( \tau = O(\exp(n)) \).
- Lenstra-Lenstra (1997), \( \tau = O(\exp(n^{1/3}\log n^{2/3})) \).
- Shor (1994), if a quantum computer existed \( \tau = O(n^3) \).

Very rough estimation: 1 operation per nanosecond, \( n = 1000 \)

<table>
<thead>
<tr>
<th>( O(\exp(n)) )</th>
<th>( O(\exp(n^{1/3}\log n^{2/3})) )</th>
<th>( O(n^3) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 10^{417} ) yr (^2)</td>
<td>0.2 yr</td>
<td>1 s</td>
</tr>
</tbody>
</table>

\(^2\)For comparison: age of the universe \( 1.5 \times 10^{10} \) yr
Non-cloning theorem

**Theorem (Non-cloning)**

Let $|\phi\rangle$ and $|\psi\rangle$ unit vectors of $\mathbb{H}$ such that

$$\langle \phi | \psi \rangle \neq 0 \text{ and } |\phi\rangle \neq \exp(i\theta)|\psi\rangle.$$

Then, no physical procedure can duplicate them.

- Must show non-existence of unitary $U : \mathbb{H} \otimes 2 \to \mathbb{H} \otimes 2$ s.t.
  $$U|\phi\alpha\rangle = |\phi\phi\rangle, \quad U|\psi\alpha\rangle = |\psi\psi\rangle,$$
  for $\alpha$ ancillary\(^3\) pure state.

- Shall show $\forall n \geq 0, \exists U : \mathbb{H} \otimes (n+2) \to \mathbb{H} \otimes (n+2)$ s.t.
  $$U|\phi\alpha_0 \ldots \alpha_n\rangle = |\phi\beta_1 \ldots \beta_n\rangle \text{ and}$$
  $$U|\psi\alpha_0 \ldots \alpha_n\rangle = |\psi\gamma_1 \ldots \gamma_n\rangle,$$
  with $\alpha_i, \beta_i$, and $\gamma_i$ pure states.

\(^3\)adj. from Latin *ancillaris*, from *ancilla* ‘maidservant’.
Proof of non-cloning theorem

Proof.

• Suppose possible:

\[ \langle \phi | \psi \rangle = \langle \phi \alpha_0 \ldots \alpha_n | U^* U \psi \alpha_0 \ldots \alpha_n \rangle \]

\[ = \langle \phi | \psi \rangle^2 \prod_{i=1}^{n} \langle \beta_i | \gamma_i \rangle. \]

• By hypothesis, \( \langle \phi | \psi \rangle \neq 0 \Rightarrow \langle \phi | \psi \rangle \prod_{i=1}^{n} \langle \beta_i | \gamma_i \rangle = 1. \)

• Cauchy-Schwarz: \(|\langle \phi | \psi \rangle| \leq \|\phi\| \|\psi\| \leq 1. \) But by hypothesis \( \phi \neq e^{i\theta} \psi \Rightarrow \langle \phi | \psi \rangle \neq 1 \Rightarrow |\langle \phi | \psi \rangle| < 1. \)

• \( \prod_{i=1}^{n} |\langle \beta_i | \gamma_i \rangle| > 1. \)

• Impossible because \( \forall i, |\langle \beta_i | \gamma_i \rangle| \leq \|\beta_i\| \|\gamma_i\| \leq 1. \)
**Setup of Bennett-Brassard 1984 (BB84) protocol**

![Diagram of quantum channel between Alicia and Bernardo]

- **Classical channel**: public and vulnerable but authenticated, e.g. internet with electronic signature.
- **Quantum channel**: vulnerable, e.g. optical fibre or light beam in free air, can be under complete control of an intruder.
- **Use of qubits**\(^4\), i.e. pure states of \(\mathbb{C}^2\).

---

\(^4\)Experimental use of qudits, with \(d > 2\), for this protocol are now being tested in Concepción.
BB84: ressources

Alicia and Bernardo agree publicly

- to use two onb of $\mathbb{H} = \mathbb{C}^2$.

$$\mathbb{B}^+ = \left\{ \epsilon_0^+ = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \epsilon_1^+ = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\},$$

$$\mathbb{B}^\times = \left\{ \epsilon_0^\times = \frac{\epsilon_0^+ + \epsilon_1^+}{\sqrt{2}}, \epsilon_1^\times = \frac{\epsilon_0^+ - \epsilon_1^+}{\sqrt{2}} \right\}.$$  

First element of each basis associated with bit 0, second element with bit 1;

- integer $n = (4 + \delta)N$, ($N =$ length of key they wish to use in fine).

Alicia possesses apparatus implementing operation $T : \{0, 1\}^2 \rightarrow \mathbb{H}$.

$$T(x, y) = \begin{cases} 
\epsilon_0^+ & \text{if } (x, y) = (0, 0), \\
\epsilon_1^+ & \text{if } (x, y) = (1, 0), \\
\epsilon_0^\times & \text{if } (x, y) = (0, 1), \\
\epsilon_1^\times & \text{if } (x, y) = (1, 1); 
\end{cases}$$

(notice $\| T(x, y) \| = 1$).
Generation of the key (Alicia’s side)

**AliciasKeyGeneration**

**Require:** `UnifRandomGenerator(\{0, 1\}), T, n`

**Ensure:** Strings $\mathbf{a}, \mathbf{b} \in \{0, 1\}^n$ and sequence $(|\psi_i\rangle)_{i=1,\ldots,n}$

- Generate randomly $a_1, \ldots, a_n$
  - $\mathbf{a} \leftarrow (a_1, \ldots, a_n) \in \{0, 1\}^n$

- Generate randomly $b_1, \ldots, b_n$
  - $\mathbf{b} \leftarrow (b_1, \ldots, b_n) \in \{0, 1\}^n$

- Store $\mathbf{a}, \mathbf{b}$ locally
  - $i \leftarrow 1$

- Repeat
  - $|\psi_i\rangle \leftarrow T(a_i, b_i)$
  - Transmit $|\psi_i\rangle$ to Bernardo via public quantum channel
  - $i \leftarrow i + 1$

- Until $i > n$
BernardosKeyGeneration

Require: UnifRanGen({0, 1}), $M^\# = |\epsilon_1^\#\rangle\langle\epsilon_1^\#|$, for $\# \in \{+, \times\}$, $n$,
sequence $|\psi_i\rangle$, for $i = 1, \ldots, n$,
Ensure: Two strings of $n$ bits $a', b' \in \{0, 1\}^n$

Generate randomly $b'_1, \ldots, b'_n$
$b' \leftarrow (b'_1, \ldots, b'_n) \in \{0, 1\}^n$
i $\leftarrow 1$
repeat
  if $b'_i = 0$ then
    ask whether $M^+$ takes value 1 in state $|\psi_i\rangle$
  else
    ask whether $M^\times$ takes value 1 in state $|\psi_i\rangle$
  end if
  if counter triggered then
    $a'_i \leftarrow 1$
  else
    $a'_i \leftarrow 0$
  end if
i $\leftarrow i + 1$
until $i > n$
$a' \leftarrow (a'_1, \ldots, a'_n) \in \{0, 1\}^n$
transmit string $b' \in \{0, 1\}^n$ to Alicia via public classical channel
store locally $a', b'$
Conciliation algorithm (at Alicia’s side)

**Conciliation**

**Require:** Strings $b, b' \in \{0, 1\}$

**Ensure:** Sequence $(k_1, \ldots, k_L)$ (with $L \leq n$) of positions of coinciding bits

$c \leftarrow b \oplus b'$

$i \leftarrow 1$

$k \leftarrow 1$

repeat

$k \leftarrow \min\{j : k \leq j \leq n \text{ such that } c_j = 0\}$

if $k \leq n$ then

$k_i \leftarrow k$

$i \leftarrow i + 1$

end if

until $k > n$

$L \leftarrow i - 1$

transmit\(^5\) $(k_1, \ldots, k_L)$ to Bernardo via public classical channel

---

\(^5\) Notice that $L := L_n$. 

Santiago, November 2013

QCCC
Proof of possibility of key distillation

**Theorem**

*If no eavesdropping on quantum channel*

\[
\mathbb{P}\left( (a'_{k_1}, \ldots, a'_{k_L}) = (a_{k_1}, \ldots, a_{k_L}) \right) = 1.
\]

**Proof.**

<table>
<thead>
<tr>
<th>(a_i)</th>
<th>(b_i)</th>
<th>(\psi_i)</th>
<th>(b_i')</th>
<th>(\langle \psi_i \mid M_{+} \psi_i \rangle)</th>
<th>(a_i')</th>
<th>(b_i')</th>
<th>(\langle \psi_i \mid M_{\times} \psi_i \rangle)</th>
<th>(a_i')</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>(\epsilon_0^+)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1/2</td>
<td>0 or 1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>(\epsilon_1^+)</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1/2</td>
<td>0 or 1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>(\epsilon_0^\times)</td>
<td>0</td>
<td>1/2</td>
<td>0 or 1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>(\epsilon_1^\times)</td>
<td>0</td>
<td>1/2</td>
<td>0 or 1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

If \(b_i' = b_i\) then \(\mathbb{P}(a_i' = a_i) = 1\). Certainty on coincidences although \(a\)’s never exchanged.
Reconciliation

If no intrusion, Alicia and Bernardo can use $a$ — sampled at places of coincidence — as key because $(a_{k_1}, \ldots, a_{k_L}) = (a'_{k_1}, \ldots, a'_{k_L})$ a.s.

Lemma

If no intrusion, for large $n$, $L_n = \mathcal{O}(n/2) = \mathcal{O}(2N)$.

Proof.

Simple use law of large numbers.
Eavesdropping

- Encarnación (...del mal) — a malevolent third party — eavesdrops but cannot copy quantum states.

  Encarnación can use procedure similar to Alicia’s and Bernardo’s to produce sequence $\tilde{\psi}_i$ according to her own sequences $(a''_i, b''_i)$.

- Since $b''$ independent of $b$ and $b'$, $b$ and $b'$ will coincide on $O(n/4)$ positions instead of $O(n/2)$. 
Eavesdropping detection and reconciliation

- After Alicia and Bernardo have passed by previous steps,
  - they share positions \( l = (k_1, \ldots, k_L) \) where \( b \) and \( b' \) coincide;
  - they know that \( a, a' \) — if sampled according to \( l \) — must coincide.

- Bernardo randomly extracts subsequence of \( l' = (r_1, \ldots, r_{L/2}) \) (of size \( L/2 \)) of \( l \) and samples his \( a' \) sequence on this positions getting \( \tilde{a} = (a'_{r_1}, \ldots, a'_{r_{L/2}}) \).

- He sends \( l' \) and \( \tilde{a} \) to Alicia.

- Alicia checks whether \( (a_{r_1}, \ldots, a_{r_{L/2}}) = (a'_{r_1}, \ldots, a'_{r_{L/2}}) \). If yes, she announces so to Bernardo and they use the complementary sequence that has never been exchanged as key.

- Else, intrusion is detected.
Topics not touched up to now

- Need really random numbers. But can buy true RNG USB key.

- Classical channel authentication can be solved with better protocols than classical\(^6\).
- Have supposed perfect transmission, but noise always present. Can be solved with quantum error correcting codes\(^7\).
- Encarnación can be more subtle: get partial information from unsharp measurement\(^8\).

---

\(^6\)See, eg. Kanamori et al., IEEE Globecom 2005 for a review.
\(^8\)Next lecture.