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

- Vigenère's[1] coding: **key** $\mathbf{k} \in \mathbb{A}^*$ with $|\mathbf{k}| = |\mathbf{m}|$; $c_i = m_i + k_i \mod \mathbb{A}, i = 1, \ldots, |\mathbf{m}|$; $m_i = c_i - k_i \mod \mathbb{A}, i = 1, \ldots, |\mathbf{m}|$.
- $\mathbb{A} = \{a, \ldots, z\} \simeq \{0, \ldots, 25\}$; $\mathbf{m}$ =hello, $\mathbf{k}$ =chile, $\mathbf{c}$ =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.
- $(k_i)_{i=1,\ldots,|\mathbf{m}|}$ independent random variables uniformly distributed on $\mathbb{A}$.
- Key used only once (one time pad).
- All keys equiprobable, hence all messages $\mathbf{m}$ corresponding to given ciphering $\mathbf{c}$ 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.
- $\mathbf{m} =$ overwheliminglyvictoriousovertheevilaxis and
  $\mathbf{m}' =$ wewonthebattlebutwedefinitelylostthewar
  are potential source messages (equiprobable)!

UNIVERSITÉ DE RENNES 1

Shannon's theorem on cryptography

Theorem (Shannon (1949))

- $|\mathbf{m}|$ *is large,*
- $|k| = |\mathbf{m}|$*, and*
- *the key is used only once,*

imply[a] *that Vernam's ciphering is ideal (inviolable for all practical purposes).*

[a] C Shannon, Communication theory of secrecy systems, Bell System Tech. J., 1949, 28, 656-715.

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

Very rough estimation: 1 operation par nanosecond, $n = 1000$

$\mathcal{O}(\exp(n))$	$\mathcal{O}(\exp(n^{1/3}(\log n)^{2/3}))$	$\mathcal{O}(n^3)$
10^{417} yr [2]	0.2 yr	1 s

[2] For comparison: age of the universe 1.5×10^{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 $U : \mathbb{H}^{\otimes 2} \rightarrow \mathbb{H}^{\otimes 2}$ s.t. $U|\,\phi\alpha\,\rangle = |\,\phi\phi\,\rangle$, $U|\,\psi\alpha\,\rangle = |\,\psi\psi\,\rangle$, for α ancillary[3] pure state.
- Shall show $\forall n \geq 0$, $\nexists U : \mathbb{H}^{\otimes(n+2)} \rightarrow \mathbb{H}^{\otimes(n+2)}$ s.t. $U|\,\phi\alpha_0 \ldots \alpha_n\,\rangle = |\,\phi\phi\beta_1 \ldots \beta_n\,\rangle$ and $U|\,\psi\alpha_0 \ldots \alpha_n\,\rangle = |\,\psi\psi\gamma_1 \ldots \gamma_n\,\rangle$, with α_i, β_i, and γ_i pure states.

[3] adj. from Latin **ancillaris**, from **ancilla 'maidservant'.**

Proof of non-cloning theorem

Proof.

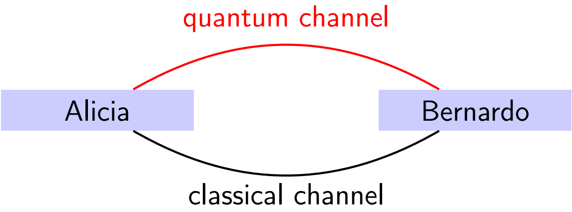
- Suppose possible:

$$\begin{aligned} \langle \phi \,|\, \psi \rangle &= \langle \phi\alpha_0 \ldots \alpha_n \,|\, U^* U \psi \alpha_0 \ldots \alpha_n \rangle \\ &= \langle \phi \,|\, \psi \rangle^2 \prod_{i=1}^{n} \langle \beta_i \,|\, \gamma_i \rangle. \end{aligned}$$

- 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 $\forall i, |\langle \beta_i \,|\, \gamma_i \rangle| \leq \|\beta_i\|\|\gamma_i\| \leq 1$.

$\square$

Setup of Bennett-Brassard 1984 (BB84) protocol



- 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 $T : \{0,1\}^2 \to \mathbb{H}$.

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

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 $i > n$

Generation of the key (Bernardo's side)

BernardosKeyGeneration

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

```
Generate randomly b'_1, ..., b'_n
b' ← (b'_1, ..., b'_n) ∈ {0,1}^n
i ← 1
repeat
   if b'_i = 0 then
      ask whether M^+ takes value 1 in state |ψ_i⟩
   else
      ask whether M^× takes value 1 in state |ψ_i⟩
   end if
   if counter triggered then
      a'_i ← 1
   else
      a'_i ← 0
   end if
   i ← i + 1
until i > n
a' ← (a'_1, ..., a'_n) ∈ {0,1}^n
transmit string b' ∈ {0,1}^n to Alicia via public classical channel
store locally a', b'
```

Conciliation algorithm (at Alicia's side)

Conciliation

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

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

$\mathbf{c} \leftarrow \mathbf{b} \oplus \mathbf{b}'$
$i \leftarrow 1$
$k \leftarrow 1$
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 $L := L_n$.

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.

a_i	b_i	ψ_i	b'_i	$\langle \psi_i \mid M_+ \psi_i \rangle$	a'_i	b'_i	$\langle \psi_i \mid M_\times \psi_i \rangle$	a'_i
0	0	ϵ_0^+	0	0	0	1	1/2	0 or 1
1	0	ϵ_1^+	0	1	1	1	1/2	0 or 1
0	1	$\epsilon_0^\times$	0	1/2	0 or 1	1	0	0
1	1	$\epsilon_1^\times$	0	1/2	0 or 1	1	1	1

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

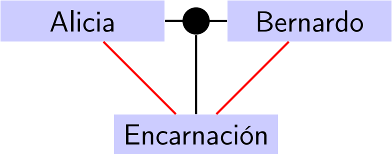
If no intrusion, for large n, $L_n = \mathcal{O}(n/2) = \mathcal{O}(2N)$.

Proof.

Simple use law of large numbers. □

Eavesdropping

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



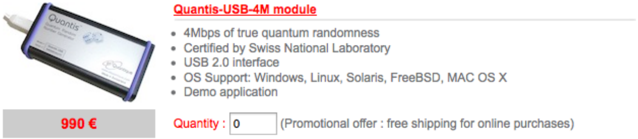
- Encarnación can use procedure similar to Alicia's and Bernardo's to produce sequence $\tilde{\psi}_i$ according to her own sequences (a_i'', b_i'').
- Since $\mathbf{b}''$ independent of $\mathbf{b}$ and $\mathbf{b}'$, $\mathbf{b}$ and $\mathbf{b}'$ will coincide on $\mathcal{O}(n/4)$ positions instead of $\mathcal{O}(n/2)$.

Eavesdropping detection and reconciliation

- After Alicia and Bernardo have passed by previous steps,
  - they share positions $\mathbf{l} = (k_1, \ldots, k_L)$ where $\mathbf{b}$ and $\mathbf{b}'$ coincide;
  - they know that $\mathbf{a}$, $\mathbf{a}'$ — if sampled according to $\mathbf{l}$ — must coincide.
- Bernardo randomly extracts subsequence of $\mathbf{l}' = (r_1, \ldots, r_{L/2})$ (of size $L/2$) of $\mathbf{l}$ and samples his $\mathbf{a}'$ sequence on this positions getting $\tilde{\mathbf{a}} = (a'_{r_1}, \ldots, a'_{r_{L/2}})$.
- He sends $\mathbf{l}'$ and $\tilde{\mathbf{a}}$ 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.
[7] See, eg. Gottesman, Proc. Symp. Appl. Math. 68, 13–58, AMS (2010).
[8] Next lecture.