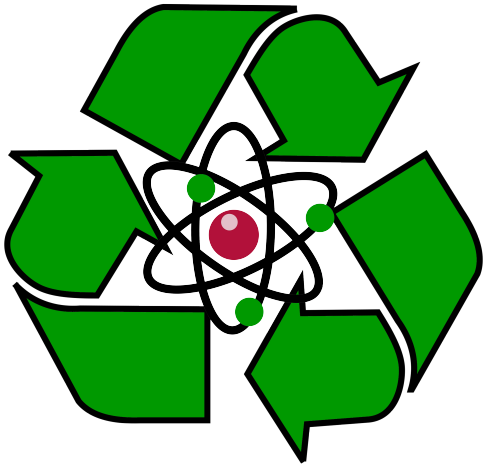
Quantum Key Recycling with noise

Daan Leermakers and Boris Škorić
TU Eindhoven

W.I.C. Symposium
May 31, 2018



TU/e Technische Universiteit Eindhoven University of Technology

Outline

- Quantum Key Distribution (noiseless/noisy)
- Quantum Key Recycling (noiseless/noisy)
- 8-state encoding
- Security proof
- Communication rate

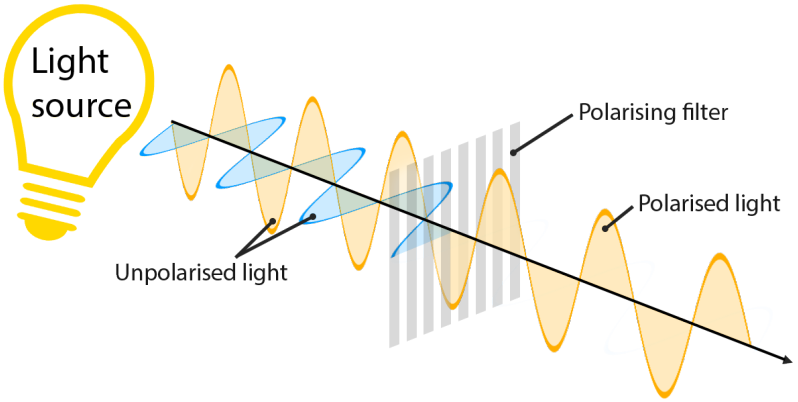
Cryptography using Quantum Mechanics

- Relies on two properties
  - Destructive measurements
  - No cloning theorem
- Exploited famously in 1984 with Quantum Key Distribution (BB84).
- Even before BB84, the idea of Quantum Key Recycling was introduced.

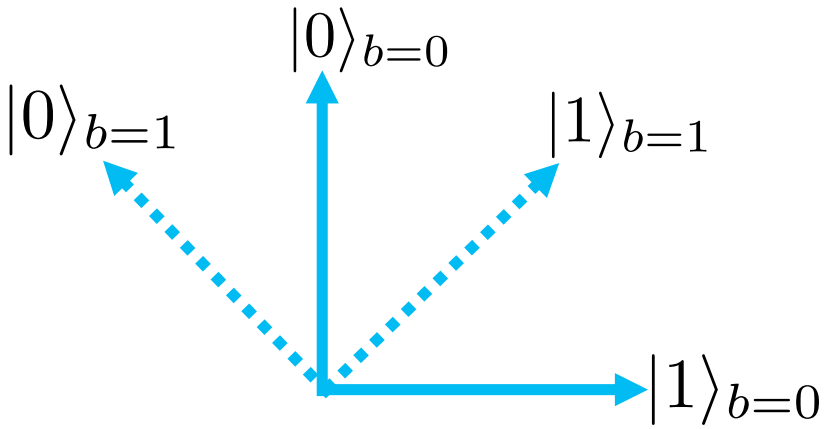
NO CLONING!

Encoding bits into quantum states

- Classical information can be encoded into the polarization of a photon



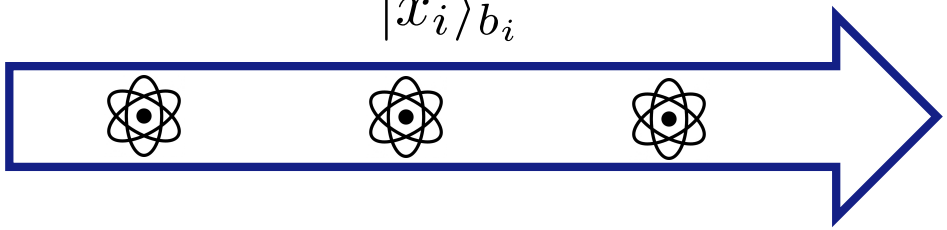
- Alice encodes the bit in one of the two bases choses randomly.
- Bob measures in a random bases.
- Information is sent when they choose the same basis.
- An attacker doesn't know which basis to measure in.



Quantum Key Distribution (noiseless)

1. Alice generates two random bit strings $x, b \in \{0,1\}^n$.
2. Alice prepares the qubit states by encoding x_i in basis b_i and sends it to Bob.

$|x_i\rangle_{b_i}$



3. Bob measures the qubits in a random basis $b' \in \{0,1\}^n$ resulting in $x' \in \{0,1\}^n$.
4. Over a classical channel Alice and Bob compare b_i and b_i'. Where $b_i \neq b_i'$ the information is discarded. where $b_i = b_i'$ they now share a secret bit.
5. To ensure nobody is eavesdropping they compare a small fraction of their bits. If there is a discrepancy they abort.

$b',\ y' \subset x'$

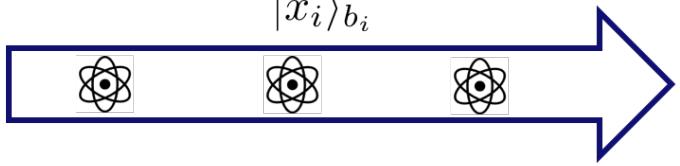
$b,\ y \subset x$

6. Alice and Bob use this secret key as a one-time pad to communicate a message.

Quantum key distribution (with noise)

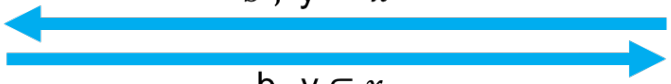
1. Alice generates two random bit strings $x, b \in \{0,1\}^n$.
2. Alice prepares the qubit states by encoding x_i in basis b_i and sends it to Bob.

$|x_i\rangle_{b_i}$



3. Bob measures the qubits in a random basis $b' \in \{0,1\}^n$ resulting in $x' \in \{0,1\}^n$.
4. Over a classical channel Alice and Bob compare b_i and b_i'. Where $b_i \neq b_i'$ the information is discarded. where $b_i = b_i'$ they now share a secret bit.
5. To ensure nobody is eavesdropping they compare a small fraction of their bits. If there is a discrepancy they abort.

$b',\ y' \subset x'$



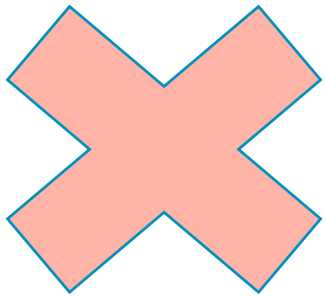
$b,\ y \subset x$

6. Alice and Bob use this secret key as a one time pad to communicate a message.

- In the case of a noisy quantum channel two additional steps are needed.
- An Error Correction Code that deals with the amount of noise they are willing to accept.
- A Privacy Amplification step where they shorten there string such that all potentially leaked information is removed.
- Both steps are operations on the classical bit string.

Quantum Key Recycling

- Alice and Bob start with a shared key $b \in \{0,1\}^n$ and use this key as their basis to encode and measure.
- This removes the need to throw away part of the measured string.



4. Over a classical channel Alice and Bob compare b_i and b_i'. Where $b_i \neq b_i'$ the information is discarded. where $b_i = b_i'$ they now share a secret bit.

b', y' $\subset x'$

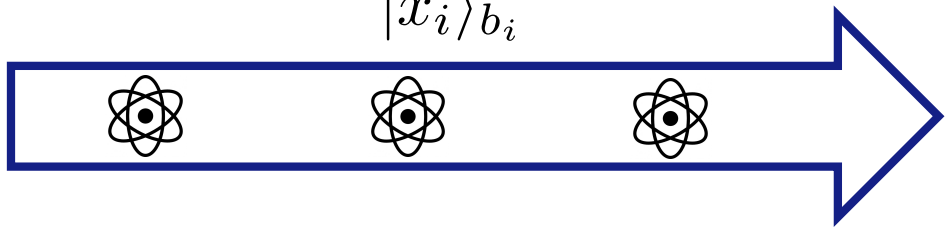
b, y $\subset x$

- Quantum Key Recycling is more efficient than the original BB84 scheme and removes the need for 2-way communication (except for 1 accept/reject bit)
- To deal with noisy channels Error Correction and Privacy Amplification need to be done as a first step. For privacy amplification and additional key u is

Quantum Key Recycling (noiseless)

1. Alice generates a random bit strings $x \in \{0,1\}^n$.
2. Alice prepares the qubit states by encoding x_i in basis b_i and sends it to Bob.

$$|x_i\rangle_{b_i}$$



3. In addition Alice sends a ciphertext $c = \mu \oplus x$ and an authentication tag t.

c, t $\qquad\qquad$ c', t'

4. Bob measures the qubits in the correct basis b resulting in $x' \in \{0,1\}^n$.
5. Bob computes the message $\mu = c' \oplus x'$
   Bob accepts when $t' = Mac(K_{mac}, x'||c')$.
6. Bob communicates accept/reject to Alice.

Acc/rej

- In the next round, Alice and Bob can reuse their secret key b!

Quantum Key Recycling (with noise)

1. Alice generates a random bit strings $x \in \{0,1\}^n$.
2. Alice prepares the qubit states by encoding x_i in basis b_i and sends it to Bob.

$$|x_i\rangle_{b_i}$$

3. For Error Correction Alice computes a syndrome and one-time pads it with a short key $s = K_{SS} \oplus S(x)$.
For Privacy Amplification she computes $z = Ext(u, x)$.
Alice sends a ciphertext $c = \mu \oplus z$, s and an authentication tag $t = M(K_{MAC}, x||c||s)$.

$$c, t, s$$

4. Bob measures the qubits in the correct basis b resulting in $x' \in \{0,1\}^n$.
5. Bob accepts when reconstruct x'' from x' is successful and $t = M(K_{MAC}, x''||c'||s')$. He computes $z'' = Ext(u, x'')$ and the message $\mu = c' \oplus z''$.
6. Bob communicates accept/reject to Alice.

Acc/rej

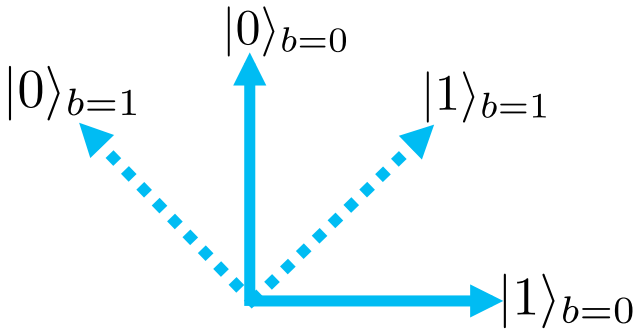
Privacy Amplification

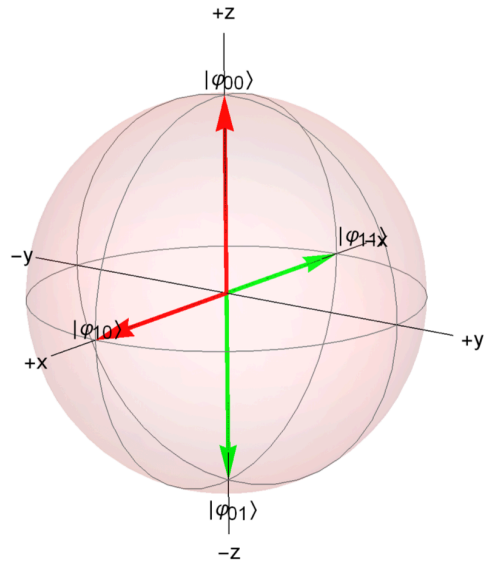
- Question: How much Privacy amplification is needed?

- In Quantum Key Distribution: How much does an attacker (Eve) know about the string x.
- In Quantum Key Recycling: How much does Eve know about the string x and the keys b, u.
- When not revealing the basis choice b, is advantageous to switch to 8-state qubit encoding.

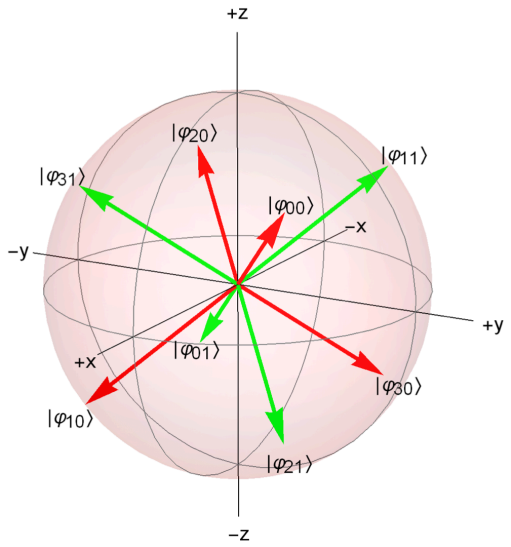
Qubit encodings

- 4-state encoding:





- 8-state encoding:
- Tetrahedron shape → bit vectors add up to zero
- Eve learns nothing about the message from a direct measurement on the qubit.



Security proof

- Since the message is perfectly secure, we only have to worry about the security of the key material.
- If Eve does not know the basis b, the 8-state encoding protect the message perfectly.
- How much privacy amplification is needed to ensure the protocol is arbitrarily close to ideal?

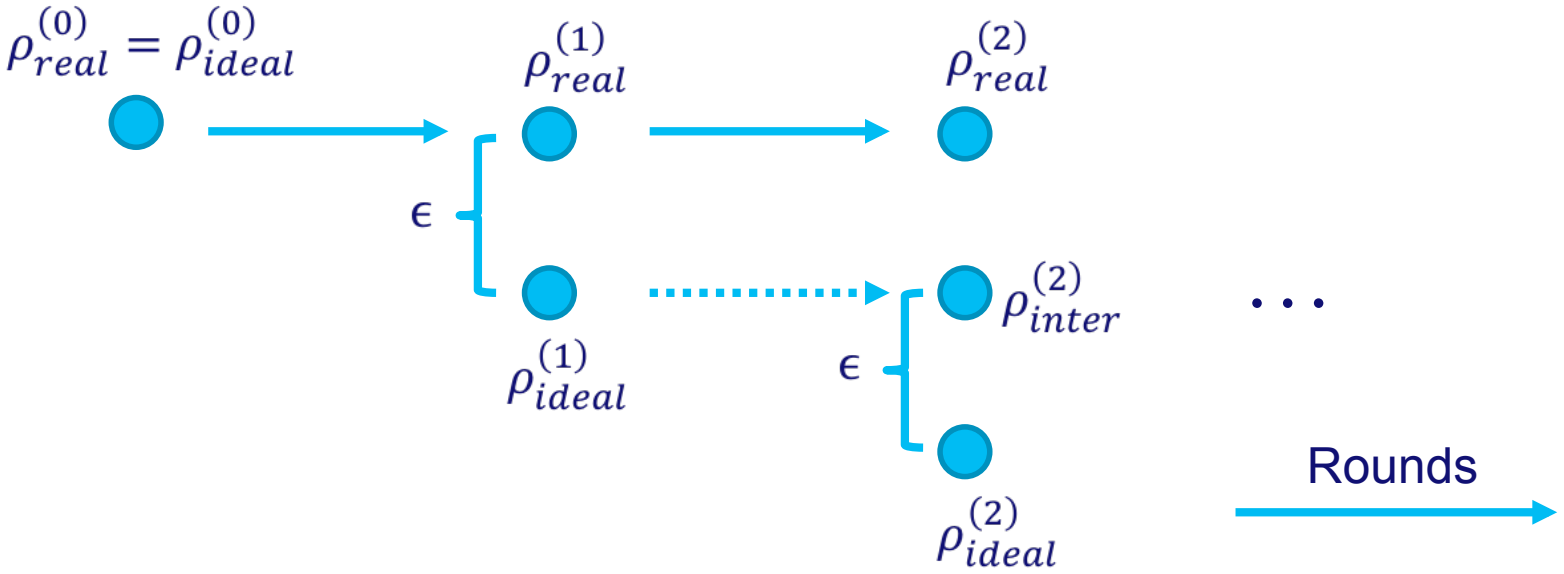
$$\| \underbrace{\rho_z^{\mathrm{UBE}}}_{\text{Eve's real state}} - \underbrace{\rho^{\mathrm{UB}} \otimes \rho_z}_{\substack{\text{Eve's state completely separated from U,B} \\ \text{"Ideal state"}}} \|_1 \leq \varepsilon$$

Induction argument

- If one round of Quantum Key recycling is secure, multiple are as well.
- $||\rho_{real}^{(1)} - \rho_{ideal}^{(1)}||_1 \leq \epsilon \implies ||\rho_{real}^{(N)} - \rho_{ideal}^{(N)}||_1 \leq N\epsilon$

- $||\rho_{real}^{(1)} - \rho_{ideal}^{(1)}||_1 = ||\rho_{inter}^{(2)} - \rho_{ideal}^{(2)}||_1$
- $||\rho_{real}^{(1)} - \rho_{ideal}^{(1)}||_1 \geq ||\rho_{real}^{(2)} - \rho_{inter}^{(2)}||_1$

$\implies ||\rho_{real}^{(2)} - \rho_{ideal}^{(2)}||_1 \leq 2\epsilon$



Rate

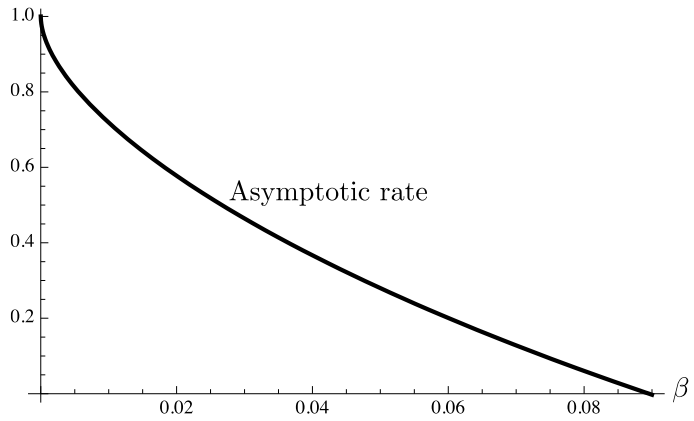
- 'Rate'= the data sent minus the key spent per round per qubit.
- Allowed noise expressed in Bit Error Rate (β)

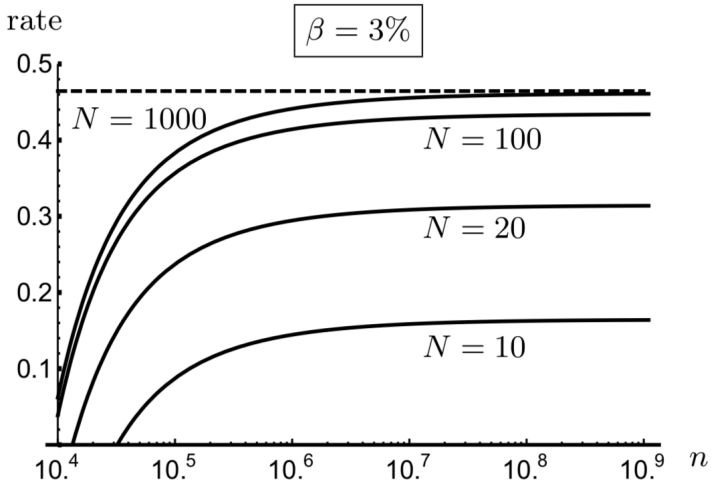
$$Rate = 1 - h(\beta) - 2\log f(\beta) - \mathcal{O}(\frac{1}{\sqrt{n}})$$

Error correction

Privacy amplification:

$$f(\beta) = \sqrt{(1-\beta)\left(1-\frac{3}{2}\beta\right)} + \sqrt{\frac{1}{2}\beta(1-\beta) + \beta\sqrt{2}}$$





Conclusion

- The laws of quantum physics can be used to construct secure cryptographic protocols.
- 8-state encoding improves the security of Quantum Key Recycling compared to 4-state encoding.
- Quantum Key Recycling allows the secure re-use of encryption keys up to noise levels of around 9%.