Quantum key distribution: how to distill unconditionally secure keys

Matteo Canale

Ph.D. student @ UniPD
Intern @ ID Quantique SA

matteo.canale@dei.unipd.it

BunnyTN3 - March 12th, 2012

Outline

Outline

Quantum tools for Information-Theoretic security

- Information-Theoretic security

Quantum tools for Information-Theoretic security

- Information-Theoretic security
  - strongest notion of security, as it makes no assumptions on the attacker's computing power

Quantum tools for Information-Theoretic security

- Information-Theoretic security
  - strongest notion of security, as it makes no assumptions on the attacker's computing power
  - only relies on information theory

Quantum tools for Information-Theoretic security

- Information-Theoretic security
  - strongest notion of security, as it makes no assumptions on the attacker's computing power
  - only relies on information theory
- Physical laws of Quantum Mechanics can be exploited while looking for I-T security

Quantum tools for Information-Theoretic security

- Information-Theoretic security
  - strongest notion of security, as it makes no assumptions on the attacker's computing power
  - only relies on information theory
- Physical laws of Quantum Mechanics can be exploited while looking for I-T security
  1. Eavesdropping detection

     "In quantum systems, one cannot take a measurement without perturbing the system itself."

Quantum tools for Information-Theoretic security

- Information-Theoretic security
  - strongest notion of security, as it makes no assumptions on the attacker's computing power
  - only relies on information theory
- Physical laws of Quantum Mechanics can be exploited while looking for I-T security
  1. Eavesdropping detection

     "In quantum systems, one cannot take a measurement without perturbing the system itself."
     - passive attacks can be detected

Quantum tools for Information-Theoretic security

- Information-Theoretic security
  - strongest notion of security, as it makes no assumptions on the attacker's computing power
  - only relies on information theory
- Physical laws of Quantum Mechanics can be exploited while looking for I-T security

1. Eavesdropping detection

   "In quantum systems, one cannot take a measurement without perturbing the system itself."
   - passive attacks can be detected
   - no perturbation $\Rightarrow$ no measurement $\Rightarrow$ no eavesdropping

Quantum tools for Information-Theoretic security

- Information-Theoretic security
  - strongest notion of security, as it makes no assumptions on the attacker's computing power
  - only relies on information theory
- Physical laws of Quantum Mechanics can be exploited while looking for I-T security

1. Eavesdropping detection

   "In quantum systems, one cannot take a measurement without perturbing the system itself."
   - passive attacks can be detected
   - no perturbation $\Rightarrow$ no measurement $\Rightarrow$ no eavesdropping
2. No-cloning theorem

   "Perfect copying is impossible in the quantum domain."

Quantum tools for Information-Theoretic security

- Information-Theoretic security
  - strongest notion of security, as it makes no assumptions on the attacker's computing power
  - only relies on information theory
- Physical laws of Quantum Mechanics can be exploited while looking for I-T security

  1. Eavesdropping detection

     "In quantum systems, one cannot take a measurement without perturbing the system itself."
     - passive attacks can be detected
     - no perturbation $\Rightarrow$ no measurement $\Rightarrow$ no eavesdropping

  2. No-cloning theorem

     "Perfect copying is impossible in the quantum domain."
     - replay and man-in-the-middle attacks are more difficult to deploy

Quantum Key Distribution

- Eavesdropping detection + no-cloning theorem
  - do not provide a complete solution for all cryptographic purposes, but offer an advantage over classical systems
  - they allow to know a posteriori if the information sent over a quantum channel and shared by two parties is actually secret

Quantum Key Distribution

- Eavesdropping detection + no-cloning theorem
  - do not provide a complete solution for all cryptographic purposes, but offer an advantage over classical systems
  - they allow to know a posteriori if the information sent over a quantum channel and shared by two parties is actually secret

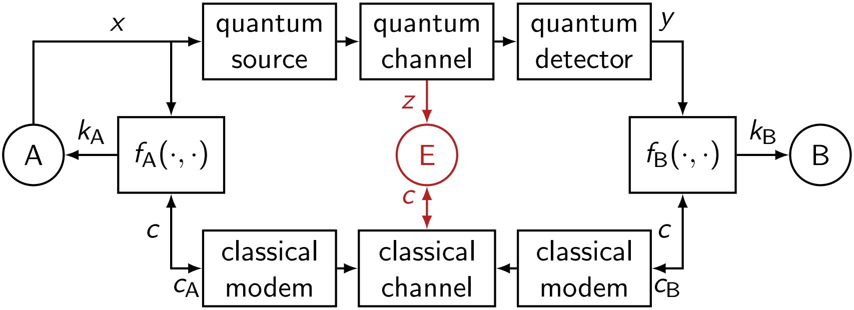
- What if we use these tools in order to deploy a secret key agreement protocol?

$$\Downarrow$$

Quantum Key Distribution
(QKD)

Outline

QKD system model



Channel characteristics

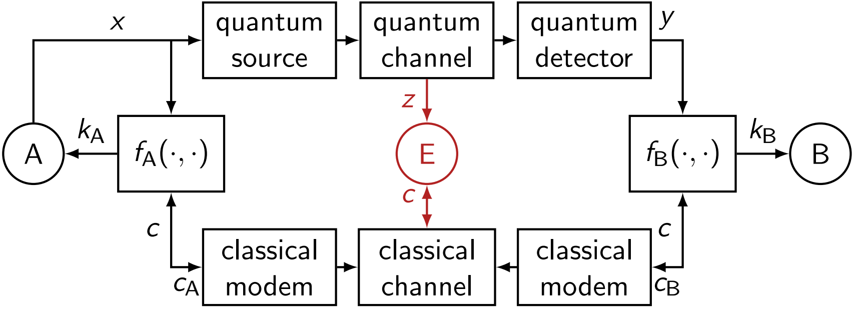
Quantum Ch.	Classical Ch.
private	public, auth.
low rate	high rate
unreliable	reliable

Objectives

$$\max_{f_a, f_B, x} H(k_A) \quad \text{subject to:}$$

- (Correctness) $P[k_A \neq k_B] < \varepsilon$
- (Secrecy) $I(k_A, k_B; z, c) < \varepsilon'$
- (Uniformity) $L(K_A) - H(K_A) < \varepsilon''$

QKD system model



Legend

x/y	prepared/measured random bit sequence
z	information on x leaked to E
$c = [c_A, c_B]$	public communications
f_A, f_B	key distillation functions
k_A, k_B	final keys

Key distillation: a practical scheme

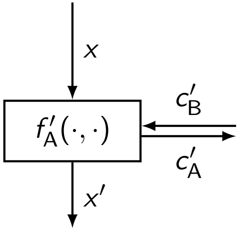
3-phase protocol [Maurer,1993]:

Key distillation: a practical scheme

3-phase protocol [Maurer,1993]:

1. Sifting → advantage over E

so that $I(x';y') > I(x';z,c')$



Key distillation: a practical scheme

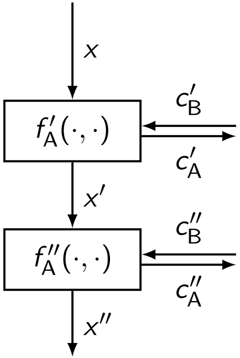
3-phase protocol [Maurer,1993]:

1. Sifting $\rightarrow$ advantage over E

$$\text{so that} \quad I(x';y') > I(x';z,c')$$

2. Information reconciliation $\rightarrow$ correctness

$$\text{so that} \quad P[x'' \neq y''] < \varepsilon'$$



Key distillation: a practical scheme

3-phase protocol [Maurer,1993]:

1. Sifting → advantage over E

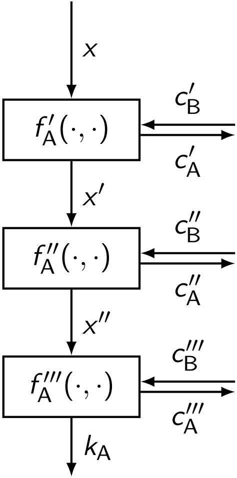
   so that $I(x';y') > I(x';z,c')$

2. Information reconciliation → correctness

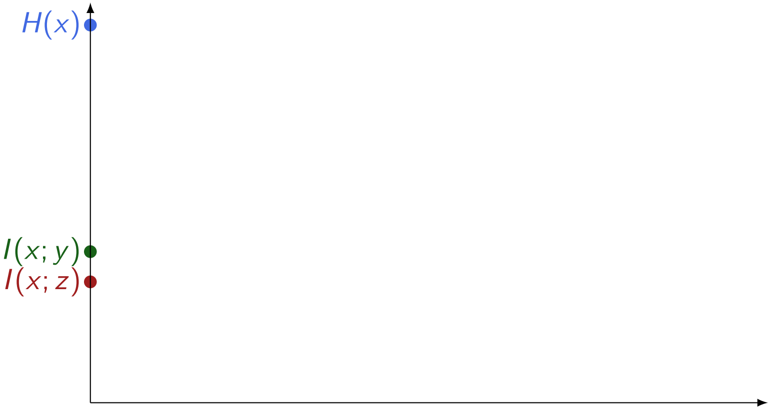
   so that $P[x'' \neq y''] < \varepsilon'$

3. Privacy amplification → secrecy

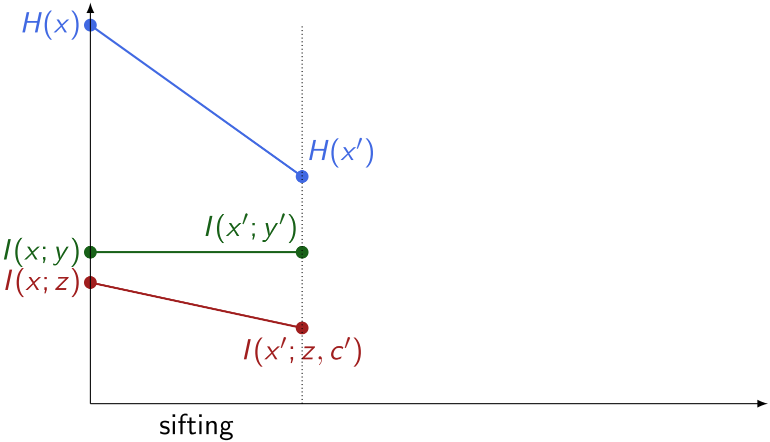
   so that $I(k_A, k_B; z, c) < \varepsilon''$



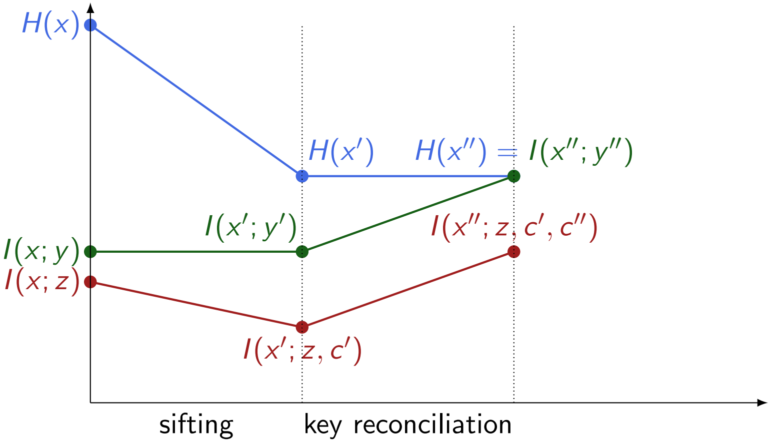
A practical scheme



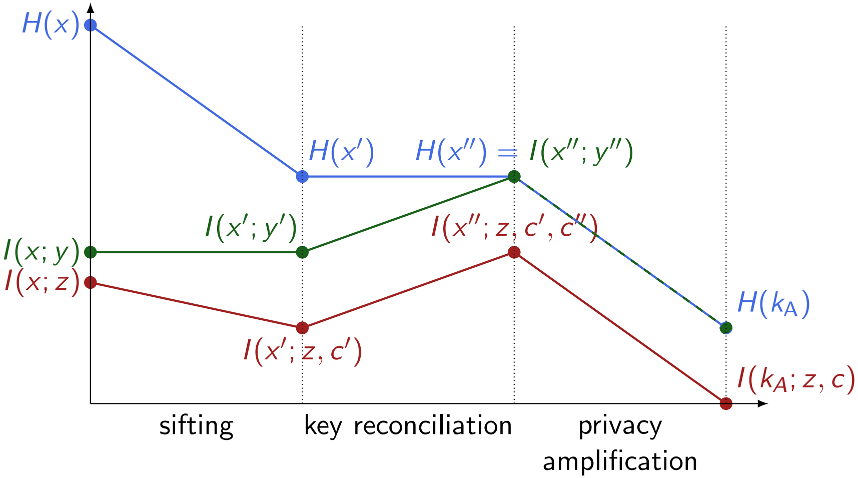
A practical scheme



A practical scheme



A practical scheme



Outline

Sifting (BB84 protocol [Bennett-Brassard,1984])

Map Bit → Qubit		
Bit	Qubit (✣)	Qubit (⤧)
0	$\leftrightarrow$	$\nwarrow\!\!\searrow$
1	$\updownarrow$	$\swarrow\!\!\nearrow$

Sifting (BB84 protocol [Bennett-Brassard,1984])

1. Alice randomly generates

Map Bit → Qubit		
Bit	Qubit ($+$)	Qubit ($\times$)
0	$\leftrightarrow$	$\nwarrow\!\!\searrow$
1	$\updownarrow$	$\swarrow\!\!\nearrow$

Sifting (BB84 protocol [Bennett-Brassard,1984])

Map Bit → Qubit		
Bit	Qubit (✥)	Qubit (⊠)
0	↔	⤡
1	↕	⤢

1. Alice randomly generates
   - bits $\{x_n\}$ i.i.d. in $\{0, 1\}$

x_n	0	1	1	0	0	1	1	1

Sifting (BB84 protocol [Bennett-Brassard,1984])

Map Bit → Qubit		
Bit	Qubit ($+$)	Qubit ($\times$)
0	$\leftrightarrow$	$\searrow$ (↖↘)
1	$\updownarrow$	$\nearrow$ (↙↗)

1. Alice randomly generates
   - bits $\{x_n\}$ i.i.d. in $\{0, 1\}$
   - bases $\{\psi_n\}$ i.i.d. in $\{+, \times\}$

x_n	0	1	1	0	0	1	1	1
ψ_n	$+$	$\times$	$\times$	$+$	$\times$	$+$	$+$	$\times$

Sifting (BB84 protocol [Bennett-Brassard,1984])

Map Bit → Qubit		
Bit	Qubit (✥)	Qubit (⊠)
0	↔	⤡
1	↕	⤢

1. Alice randomly generates
   - bits $\{x_n\}$ i.i.d. in $\{0, 1\}$
   - bases $\{\psi_n\}$ i.i.d. in {✥, ⊠}
2. $\{a_n\} = \text{modulate}_{\{\psi_n\}}(\{x_n\})$

x_n	0	1	1	0	0	1	1	1
ψ_n	✥	⊠	⊠	✥	⊠	✥	✥	⊠
a_n	↔	⤢	⤢	↔	⤡	↕	↕	⤢

Sifting (BB84 protocol [Bennett-Brassard,1984])

Map Bit → Qubit		
Bit	Qubit (✛)	Qubit (⊠)
0	↔	⤡
1	↕	⤢

1. Alice randomly generates
   - bits $\{x_n\}$ i.i.d. in $\{0, 1\}$
   - bases $\{\psi_n\}$ i.i.d. in {✛, ⊠}
2. $\{a_n\} = \text{modulate}_{\{\psi_n\}}(\{x_n\})$
3. Bob randomly generates $\{\xi_n\}$ i.i.d. in {✛, ⊠}

x_n	0	1	1	0	0	1	1	1
ψ_n	✛	⊠	⊠	✛	⊠	✛	✛	⊠
a_n	↔	⤢	⤢	↔	⤡	↕	↕	⤢
ξ_n	⊠	⊠	✛	✛	✛	⊠	✛	⊠

Sifting (BB84 protocol [Bennett-Brassard,1984])

Map Bit → Qubit		
Bit	Qubit (✛)	Qubit (⊠)
0	↔	⤡
1	↕	⤢

1. Alice randomly generates
   - bits $\{x_n\}$ i.i.d. in $\{0,1\}$
   - bases $\{\psi_n\}$ i.i.d. in {✛, ⊠}
2. $\{a_n\} = \text{modulate}_{\{\psi_n\}}(\{x_n\})$
3. Bob randomly generates $\{\xi_n\}$ i.i.d. in {✛, ⊠}
4. $\{b_n\} = \text{measure}_{\{\xi_n\}}(\{a_n\})$

x_n	0	1	1	0	0	1	1	1
ψ_n	✛	⊠	⊠	✛	⊠	✛	✛	⊠
a_n	↔	⤢	⤢	↔	⤡	↕	↕	⤢
ξ_n	⊠	⊠	✛	✛	✛	⊠	✛	⊠
b_n	⤢	⤢	↔	↔	↕	⤢	↕	⤢

Sifting (BB84 protocol [Bennett-Brassard,1984])

Map Bit → Qubit		
Bit	Qubit (+)	Qubit (×)
0	↔	⤡
1	↕	⤢

1. Alice randomly generates
   - bits $\{x_n\}$ i.i.d. in $\{0,1\}$
   - bases $\{\psi_n\}$ i.i.d. in {+, ×}
2. $\{a_n\} = \text{modulate}_{\{\psi_n\}}(\{x_n\})$
3. Bob randomly generates $\{\xi_n\}$ i.i.d. in {+, ×}
4. $\{b_n\} = \text{measure}_{\{\xi_n\}}(\{a_n\})$
5. $\{y_n\} = \text{demod}(\{b_n\})$

x_n	0	1	1	0	0	1	1	1
ψ_n	+	×	×	+	×	+	+	×
a_n	↔	⤢	⤢	↔	⤡	↕	↕	⤢
ξ_n	×	×	+	+	+	×	+	×
b_n	⤢	⤢	↔	↔	↕	⤢	↕	⤢
y_n	**1**	1	**0**	0	**1**	**1**	1	1

Sifting (BB84 protocol [Bennett-Brassard,1984])

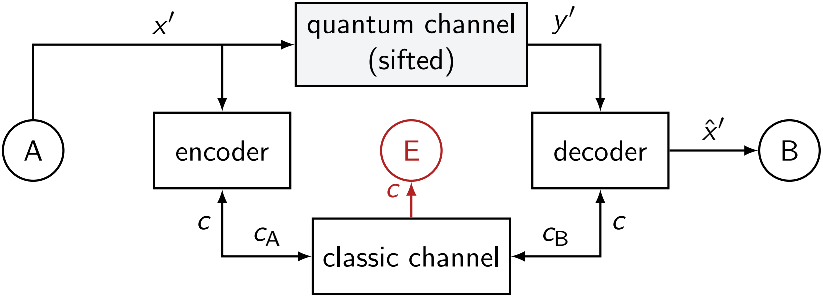
Map Bit $\to$ Qubit		
Bit	Qubit ($+$)	Qubit ($\times$)
0	$\leftrightarrow$	$\nwarrow\!\!\!\searrow$
1	$\updownarrow$	$\swarrow\!\!\!\nearrow$

1. Alice randomly generates
   - bits $\{x_n\}$ i.i.d. in $\{0,1\}$
   - bases $\{\psi_n\}$ i.i.d. in $\{+,\times\}$
2. $\{a_n\} = \text{modulate}_{\{\psi_n\}}(\{x_n\})$
3. Bob randomly generates $\{\xi_n\}$ i.i.d. in $\{+,\times\}$
4. $\{b_n\} = \text{measure}_{\{\xi_n\}}(\{a_n\})$
5. $\{y_n\} = \text{demod}(\{b_n\})$

x_n	0	1	1	0	0	1	1	1
ψ_n	$+$	$\times$	$\times$	$+$	$\times$	$+$	$+$	$\times$
a_n	$\leftrightarrow$	$\swarrow\!\!\!\nearrow$	$\swarrow\!\!\!\nearrow$	$\leftrightarrow$	$\nwarrow\!\!\!\searrow$	$\updownarrow$	$\updownarrow$	$\swarrow\!\!\!\nearrow$
ξ_n	$\times$	$\times$	$+$	$+$	$+$	$\times$	$+$	$\times$
b_n	$\swarrow\!\!\!\nearrow$	$\swarrow\!\!\!\nearrow$	$\leftrightarrow$	$\leftrightarrow$	$\updownarrow$	$\swarrow\!\!\!\nearrow$	$\updownarrow$	$\swarrow\!\!\!\nearrow$
y_n	**1**	1	**0**	0	**1**	**1**	1	1

SIFTING - keep $(x_i, y_i) \iff \psi_i = \xi_i$

Key reconciliation



Channel characteristics

Quantum Ch.	Classical Ch.
private	public, auth.
low rate	high rate
unreliable	reliable

Objectives

1. Correctness: $P[x' = \hat{x}'] \approx 1$
2. Secrecy: $I(x'; c) < \delta$

Key reconciliation

1. Interactive
   - Keys are interactively reconciled by means of a binary error search based on multiple, subsequent public communications [Brassard-Salvail,93].

Key reconciliation

1. Interactive
   - Keys are interactively reconciled by means of a binary error search based on multiple, subsequent public communications [Brassard-Salvail,93].
2. Systematic
   - Given a $(n+r,n)$ generating matrix $\mathbf{G} = \begin{bmatrix} \mathbf{I}_n \\ \mathbf{A} \end{bmatrix}$:
     1. Alice transmits the redundancy $\mathbf{c} = \mathbf{A}\mathbf{x}'$
     2. Bob chooses $\hat{\mathbf{x}}' = \arg\min_{\mathbf{a}\in\mathcal{C}} d(\mathbf{a},[\mathbf{y},\mathbf{c}])$
   - Examples: LDPC [Mondin et al.,2010]
     BCH [Traisilanun et al.,2007]

Key reconciliation

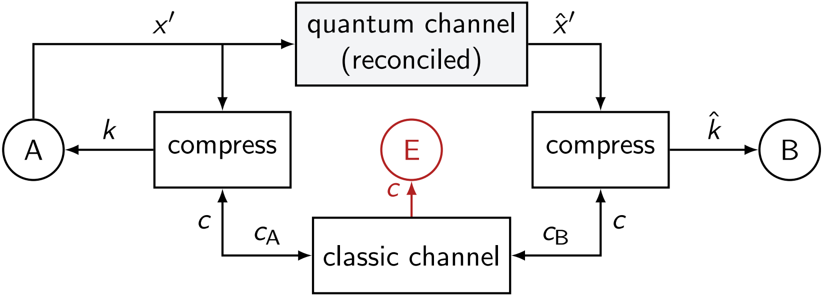
1. Interactive
   - Keys are interactively reconciled by means of a binary error search based on multiple, subsequent public communications [Brassard-Salvail,93].
2. Systematic
   - Given a $(n+r, n)$ generating matrix $\mathbf{G} = \begin{bmatrix} \mathbf{I}_n \\ \mathbf{A} \end{bmatrix}$:
     1. Alice transmits the redundancy $\mathbf{c} = \mathbf{A}\mathbf{x}'$
     2. Bob chooses $\hat{\mathbf{x}}' = \arg\min_{\mathbf{a}\in\mathcal{C}} d(\mathbf{a}, [\mathbf{y}, \mathbf{c}])$
   - Examples: LDPC [Mondin et al.,2010]
     BCH [Traisilanun et al.,2007]
3. Hashing
   - Given a $(n, n-r)$ parity check matrix $\mathbf{H}$:
     1. Alice transmits the syndrome $\mathbf{c} = \mathbf{H}\mathbf{x}'$
     2. Bob chooses $\hat{\mathbf{x}}' = \arg\min_{\mathbf{a}:\mathbf{Ha}=\mathbf{c}} d(\mathbf{a}, \mathbf{y})$
   - Examples: Winnow [Buttler et al.,2003]
     LDPC [Elkouss et al.,2009]

Key reconciliation

The choice of the coding technique for reconciliation depends on the model for the classical channel

Layer	Ch. type	Condition	Delays	Codes used
Physical	AWGN	high SNR	none	systematic (soft)
Data link	binary	low BER	low	systematic (hard)
Net & up	packet	error free	long	interactive, hashing

Privacy amplification



Channel characteristics

Quantum Ch.	Classical Ch.
private low rate	public, auth. high rate

Goals

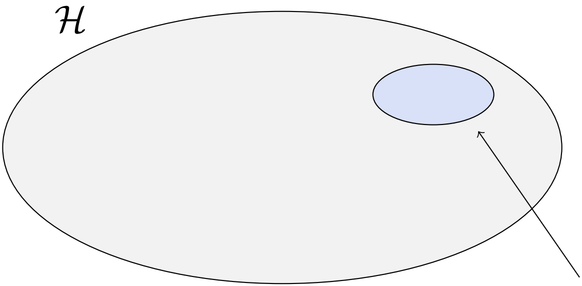
1. Maximum privacy: $I(\mathbf{k};\mathbf{z},\mathbf{c}) < \varepsilon''$
2. Minimum compression: $\max H(\mathbf{k})$

Choosing a compression function

Definition (2-universal hash functions [Wegman-Carter,1979])

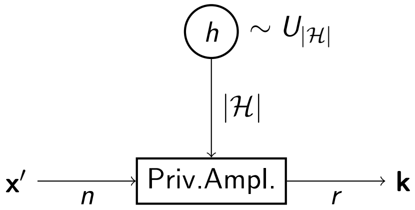
A class $\mathcal{H}$ of hash functions from $\{0,1\}^n$ to $\{0,1\}^m$ is 2-universal if

$$\forall\ x, y \in \{0,1\}^n,\ x \neq y, \quad h \in \mathcal{H} : P[h(x) = h(y)] \leq \frac{1}{2^m}$$



$$|\{h \in \mathcal{H} : h(x) = h(y)\}| \leq \frac{1}{2^m}|\mathcal{H}|$$

Choosing a compression function



- $n = H(\mathbf{x}')$
- $t = I(\mathbf{x}'; \mathbf{z}, \mathbf{c})$
- $s =$ security margin

$$\Rightarrow r = H(\mathbf{k}) = n - t - s$$

Theorem ([Bennett et al.,1995])

If the compressing function h is chosen uniformly from a class of 2-UHFs, then on average (over $\mathbf{z}$ and h)

$$I(\mathbf{k}; \mathbf{z}, h) \leq \frac{2^{-s}}{\ln 2}$$

Choosing a compression function

- Families of 2-universal hash functions
  - ...
  - Random matrices
    - ...
    - Toeplitz random matrices
      Randomly choose an $(n+m-1)$-bit seed which defines a random $m \times n$ Toeplitz matrix

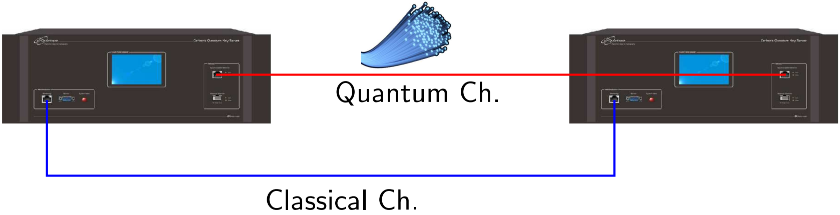
$$\begin{bmatrix} z_1 \\ \vdots \\ z_m \end{bmatrix} = \begin{bmatrix} s_4 & s_5 & \dots & \dots & \dots & \dots & s_{n+m-1} \\ s_3 & s_4 & \ddots & \ddots & \ddots & \ddots & s_{n+m-2} \\ s_2 & s_3 & \ddots & \ddots & \ddots & \ddots & \vdots \\ s_1 & s_2 & s_3 & s_4 & s_5 & \dots & s_{n-1} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

    - ...
  - ...

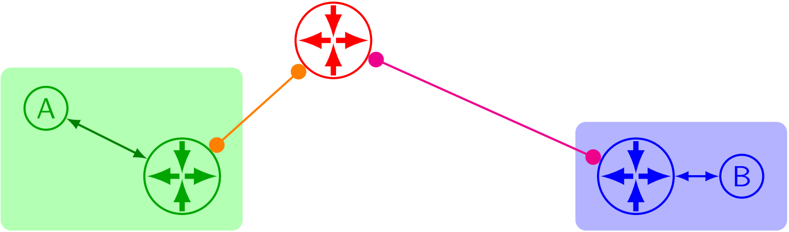
Outline

Quantum and classical channels

- Quantum channel
  - Fiber optics (commercial solutions: id Quantique, MagiQ, ...)
  - Free-space (prototypes: UniPD, LMU, ...)
- Classical channel
  - Ethernet
  - 802.11
  - ...



QKD Networks



- SECOQC (2004-2008)
  `http://www.secoqc.net`
- SwissQuantum (2009-2011)
  `http://swissquantum.idquantique.com`
- Tokyo QKD Network (2010)
  `http://www.uqcc2010.org`
- ...

QKD at UniPD: the QuantumFuture project

QuantumFuture

- 4-year research project at UniPD
- 1.4 M€, funded by the University of Padova
- 4 RUs: Telecom, Controls, Optics, Astronomy
- Main focus on free-space QKD

More information available at:
http://quantumfuture.dei.unipd.it

QKD at id Quantique

- Network encryption
  - plug-&-play commercial QKD devices
  - QKD devices for research and development applications
- Quantum Random Number Generators
- Single Photon Detectors for Quantum Applications

More information available at:
http://www.idquantique.com

Essential references

- [Maurer,1993] U. Maurer, "Secret key agreement by public discussion from common information", IEEE Transactions on Information Theory, vol. 39, no. 3, pp. 733-742, 1993.
- [Bennett-Brassard,1984] C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing", in IEEE International Conference on Computers, Systems and Signal Processing, 1984, pp. 175-179.
- [Brassard-Salvail,1993] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion", International Conference on the Theory and Applications of Cryptographic Techniques, Advances in Cryptology, EUROCRYPT, pp. 410-423, 1993.
- [Mondin et al.,2010] M. Mondin, M. Delgado, F. Mesiti, and F. Daneshgaran, "Soft-processing for Information Reconciliation in QKD Applications", International Journal of Quantum Information, 2010.

Essential references

- [Traisilanun et al.,2007] W. Traisilanun, K. Sripimanwat, and O. Sangaroon, "Secret key reconciliation using BCH code in quantum key distribution", in International Symposium on Communications and Information Technologies, ISCIT, 2007, pp. 1482-1485.
- [Buttler et al.,2003] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography", Physical Review A, vol. 67, no. 5, p. 052303, May 2003.
- [Elkouss et al.,2009] D. Elkouss, A. Leverrier, R. Allaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution", in IEEE International Symposium on Information Theory, ISIT, 2009, pp. 1879-1883.

Essential references

- [Bennett et al.,1995] C. H. Bennett, G. Brassard, C. Crepeau, and U. Maurer, "Generalized privacy amplification", IEEE Transactions on Information Theory, vol. 41, no. 6, pp. 1915-1923, 1995.
- [Canale,2011] Canale, M. On Information-Theoretic Secret Key Agreement for Quantum Key Distribution. Tech. report, 2011.
- [Canale et al.,2011] M. Canale, D. Bacco, S. Calimani, F. Renna, N. Laurenti, G. Vallone, P. Villoresi , "A prototype of a free-space QKD scheme based on the B92 protocol", in International Symposium on Applied Sciences in Biomedical and Communication Technologies, ISABEL, 2011.