# Information-Theoretic Security and Quantum Key Distribution: when security comes from uncertainty

Nicola Laurenti

Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione

Ph.D. Summer School in Information Engineering
Bressanone/Brixen, 4–8 July 2011



## Acknowledgements

This presentation, and the related work is the product of my collaboration with

Matteo Canale and Francesco Renna

and the contributions from

H. Vincent Poor (Princeton), Matthieu Bloch (Georgia Tech), Paolo Villoresi, Pino Vallone, Simon Calimani, Davide Girardi, Davide Bacco and all the QuantumFuture staff (DEI, U. Padua)

QuantumFuture
The shift in the communication paradigm
Università degli Studi di Padova





## Outline





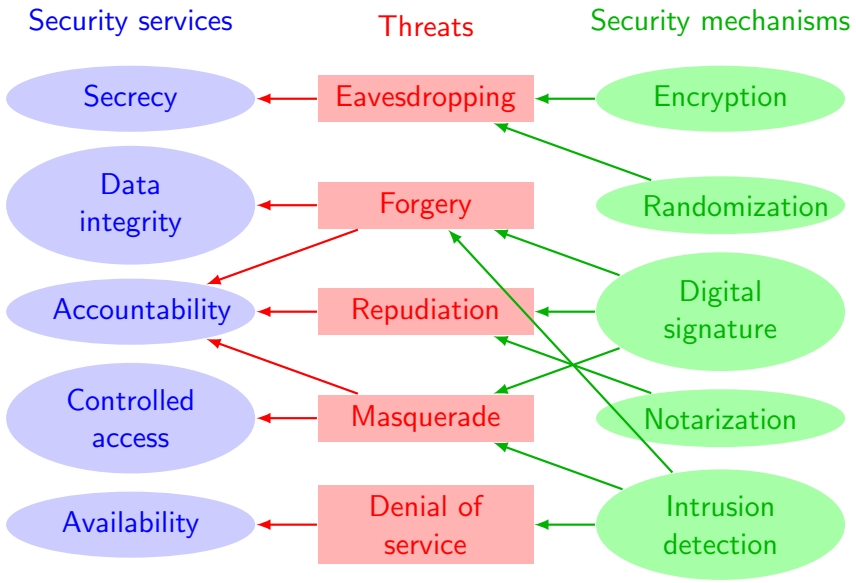
Motivations for QKD | Information-theoretic security | Quantum key distillation | QKD and higher layers

## Outline

1. **Motivations for Quantum Key Distribution**
   - What do we need keys for?
   - The key distribution problem
2. **Information-theoretic security**
   - The wiretap channel
   - Information-theoretic secret key agreement
3. **Quantum key distillation**
   - Protocols for the Quantum physical layer
   - Key reconciliation
   - Privacy amplification
4. **QKD and higher layers**
   - Creation of QKD networks
   - Integration with higher layers security protocols

Information-Theoretic Security and Quantum Key Distribution N. Laurenti

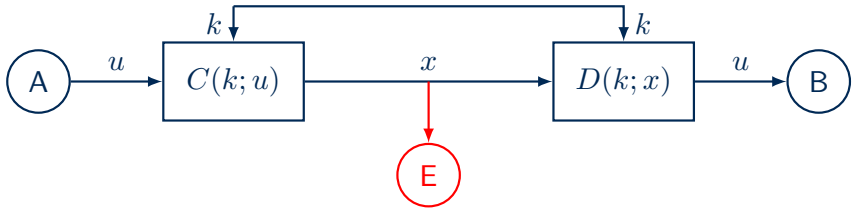
## What is security?








## A system for secret communication [Shannon, '49]




**Kerchoff's Assumption**

E knows:

- the functions $C(\cdot;\cdot)$, $D(\cdot;\cdot)$
- the distributions $p_u(\cdot)$, $p_k(\cdot)$

Secrecy of $u$ is only based on hiding the key $k$

**Perfect secrecy**

$u$ statistically independent of $x$

$$p_u(\alpha) = p_{u|x}(\alpha|\beta) \quad , \quad I(u;x) = 0$$

**Theorem**

*Perfect secrecy requires*

$$H(k) \geq H(u)$$





## A vicious circle?

In order to transmit a perfectly secret message $u$, we need to transmit a perfectly secret key $k$ of the same length. Is this a frustrating impasse?

1. We can settle for "less than perfect" secrecy of the message (computational security)
2. We can settle for "less than perfect" secrecy of the key (public key cryptography)
3. The secret key can be shared in advance (key predistribution)
4. We can obtain perfect secrecy with the help of the channel (physical layer secrecy)
5. The secret key need not be known a priori by A nor B (key agreement)

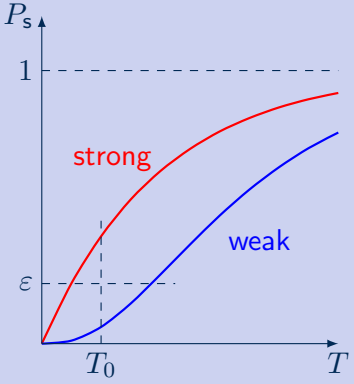




## Computational security

**The complexity vs. success probability tradeoff**

For a (probabilistic) attack




**Concrete security $(T_0, \varepsilon)$**

For any probabilistic attack with complexity $T < T_0$, the success probability is $P_s < \varepsilon$

**Asymptotic security in key length $n$**

For any probabilistic attack with polynomial complexity as $n \to \infty$

$$T = O(P(n))$$

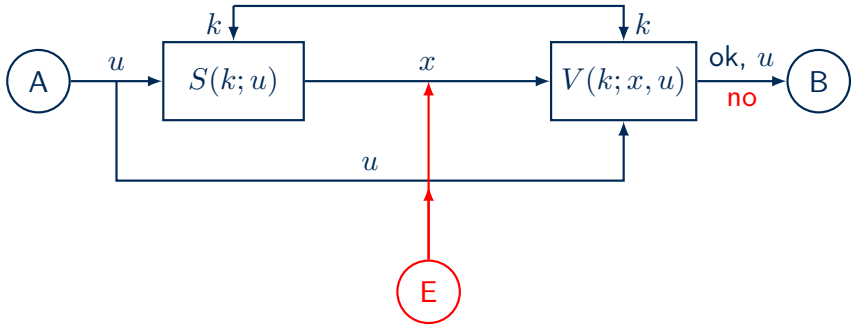
the success probability vanishes

$$P_s = o(1/Q(n))$$

for any polynomials $P(n), Q(n)$.

Ex.: "brute force" attack with $N$ trials: $T \propto N$ , $P_s = N/2^n$

## Message authentication / integrity protection




### Kerchoff's-like Assumption

E knows:

- the functions $S(\cdot;\cdot)$, $V(\cdot;\cdot)$
- the distributions $p_u(\cdot)$, $p_k(\cdot)$

Non forgeability of $x$ is only based on hiding the key $k$

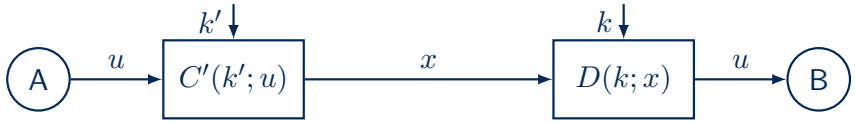




## Public key cryptography [Rivest-Shamir-Adleman, '78]

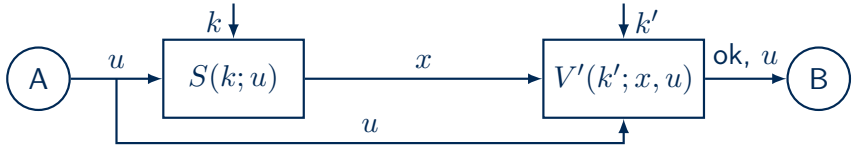
### Secrecy / confidentiality

- $C(k;u) = C'(k';u)$ for all $u$
- $k'$ can be easily derived from $k$ and is public for A to use
- $k$ can not be recovered from $k'$ and is kept secret by B




### Authentication / integrity protection

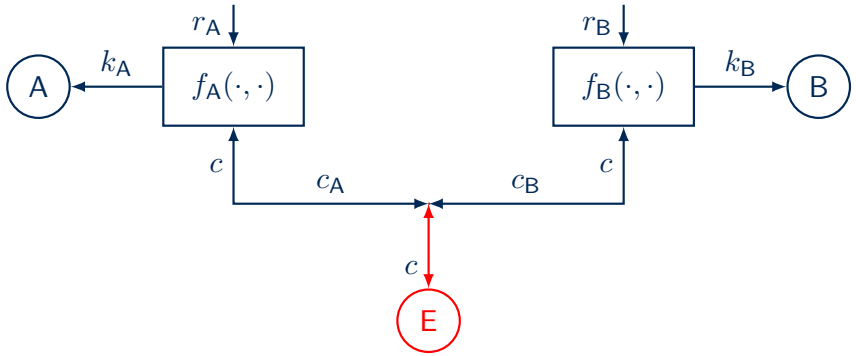
$V(k;x,u) = V'(k';x,u)$ for all $x, u$, and $k$ is kept secret by A








## Cryptographic key agreement [Diffie-Hellman, '76]




### Objective

$$\max L(k_A) \quad \text{subject to:}$$

correctness: $k_A = k_B$

secrecy: infeasible to derive $k$ from $c$

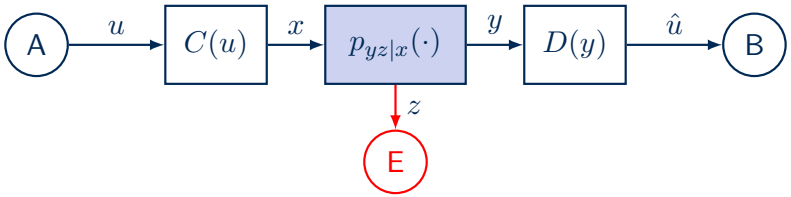
uniformity: $p_{k_A}(a) \approx 1/2^{L(k_A)}$





## Outline

## The wiretap channel [Wyner, '75]




We aim for reliable transmissions to B, i.e. $\lim_{n\to\infty} P\left[\boldsymbol{u} \neq \hat{\boldsymbol{u}}\right] = 0$, under the constraint of secrecy with respect to E

### Secrecy constraints

- Perfect secrecy, [Shannon, '49]: $I(\boldsymbol{u}, \boldsymbol{z}) = 0$
- Asymptotic perfect secrecy: $\lim_{n\to\infty} I(\boldsymbol{u}, \boldsymbol{z}) = 0$
- Vanishing information rate, [Wyner, '75]: $\lim_{n\to\infty} \frac{1}{n} I(\boldsymbol{u}, \boldsymbol{z}) = 0$





## Random encoding & channel resolvability

- The basic idea is to use a probabilistic encoder $u \to x$
- Consider a subset $\mathcal{X}_n' \subset \mathcal{X}^n$ that allows to simulate the channel, that is $p_{z|x\in\mathcal{X}_n'}(\cdot) = p_{z|x\in\mathcal{X}^n}(\cdot) = p_z(\cdot)$
- Map each possible message $u$ to a disjoint $\mathcal{X}_n'(u)$
- Choose the codeword $x$ randomly from $\mathcal{X}_n'(u)$

### Channel resolvability [Han-Verdù, '93]

The minimum number of typical codewords in $\mathcal{X}_n'$ is $|\mathcal{X}_n'| \geq 2^{nI(x;z)}$

### Secrecy rates and secrecy capacity

Transmission rates for which we can satisfy the secrecy constraint and guarantee reliability are called achievable secrecy rates. The secrecy capacity is the supremum of all achievable secrecy rates.





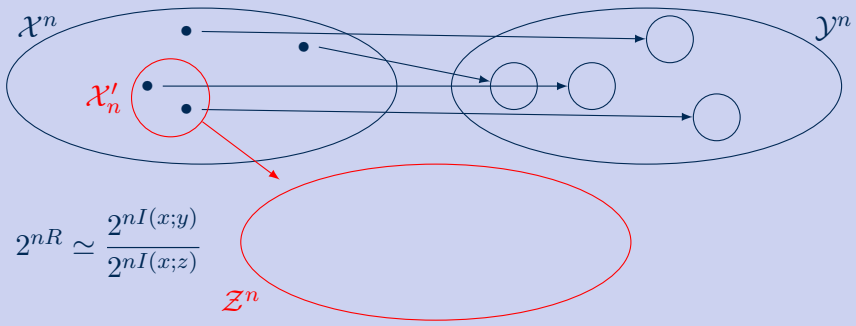
## Secrecy capacity

### Theorem

*The secrecy capacity of the wiretap channel in bit/channel use is*

$$C_{\mathsf{s}} = \max_{u}[I(u;y) - I(u;z)]^+ \geq \max_{x}[I(x;y) - I(x;z)]^+$$

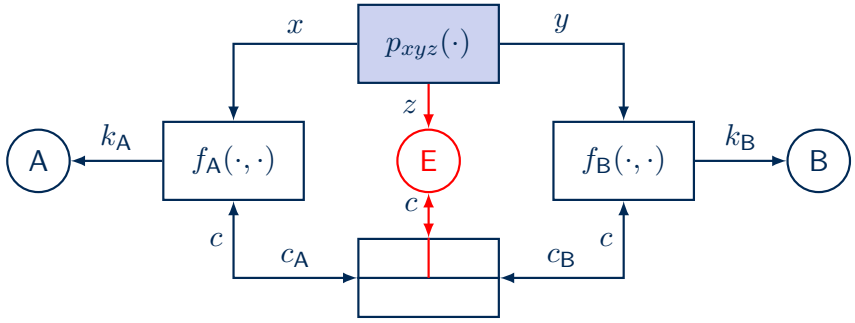
### Visualization of the proof








## Info-theoretic key agreement [Ahlswede-Csiszar, '93]




### Objective

$$\max_{f_{\mathsf{A}}, f_{\mathsf{B}}} H(k_{\mathsf{A}}) \quad \text{subject to:}$$

correctness: $\mathrm{P}\left[k_{\mathsf{A}} \neq k_{\mathsf{B}}\right] < \varepsilon$

secrecy: $I(k_{\mathsf{A}}, k_{\mathsf{B}}; z, c) < \varepsilon'$

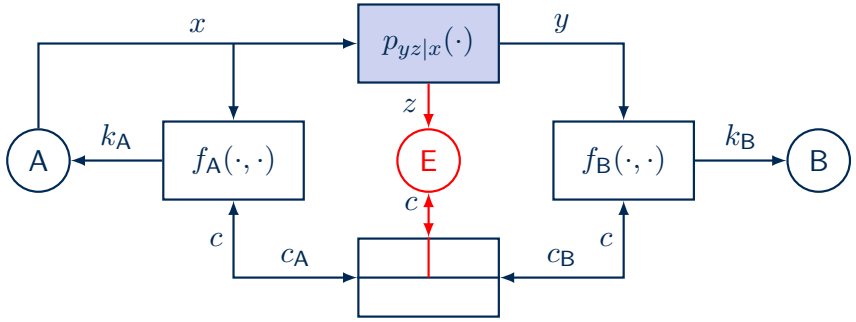
uniformity: $L - H(k_{\mathsf{A}}) < \varepsilon''$

### Upper bound

For $\varepsilon, \varepsilon', \varepsilon'' \to 0$

$$\max_{f_{\mathsf{A}}, f_{\mathsf{B}}} H(k_{\mathsf{A}}) \leq I(x;y|z)$$

## Information-theoretic key agreement [Maurer, '93]




**Objective**

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

correctness: $\mathrm{P}\left[k_A \neq k_B\right] < \varepsilon$

secrecy: $I(k_A, k_B; z, c) < \varepsilon'$

uniformity: $L - H(k_A) < \varepsilon''$

**Upper and lower bounds**

For $\varepsilon, \varepsilon', \varepsilon'' \to 0$

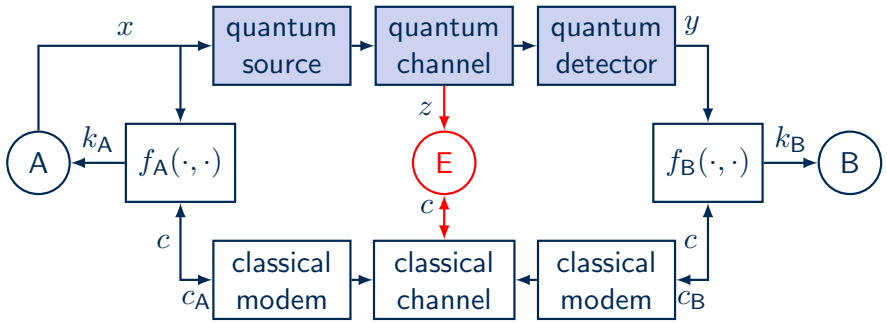
$$\max_{f_A,f_B,x} H(k_A) \leq \max_x I(x; y|z)$$

$$\max_{f_A,f_B,x} H(k_A) \geq \max_x I(x; y) - I(x; z)$$





## Quantum key agreement [Bennett-Brassard, '84]




**Objective**

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

correctness: $\mathrm{P}\left[k_A \neq k_B\right] < \varepsilon$

secrecy: $I(k_A, k_B; z, c) < \varepsilon'$

uniformity: $L - H(k_A) < \varepsilon''$

**Upper bound**

For $\varepsilon, \varepsilon', \varepsilon'' \to 0$

$$\max_{f_A,f_B,x} H(k_A) \leq \max_x I(x; y|z)$$





## Outline







## A practical scheme (I)

Based on a divide and conquer approach
3-phase protocol:

1. Sifting → advantage over E

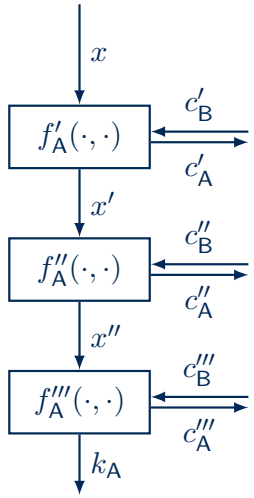
   so that $I(x'; y') > I(x'; z, c')$

2. Information reconciliation → correctness

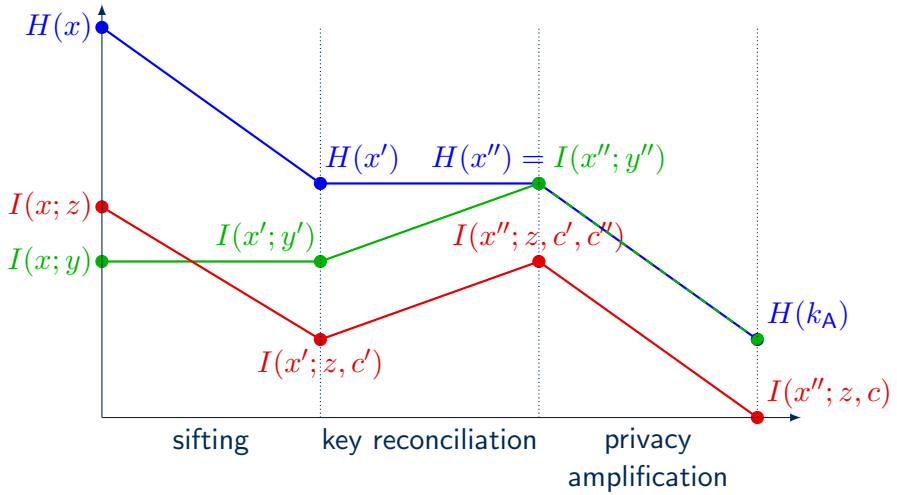
   so that $\mathrm{P}\left[x'' \neq y''\right] < \varepsilon$

3. Privacy amplification → secrecy

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



## A practical scheme (II)

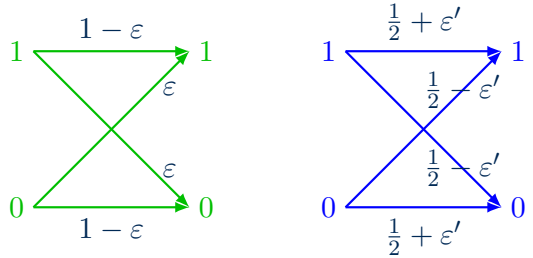







## The BB84 protocol

| $x_n$ | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|
| $A_n$ | ↕ | ⤡ | ⤡ | ↕ | ⤡ | ↕ | ↕ | ⤡ |
| $a_n$ | ↔ | ⤢ | ⤢ | ↔ | ⤡ | ↕ | ↕ | ⤢ |
| $B_n$ | ⤡ | ⤡ | ✛ | ✛ | ✛ | ⤡ | ✛ | ⤡ |
| $b_n$ | ⤢ | ⤢ | ↔ | ↔ | ↕ | ⤢ | ↕ | ⤢ |
| $y_n$ | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 |

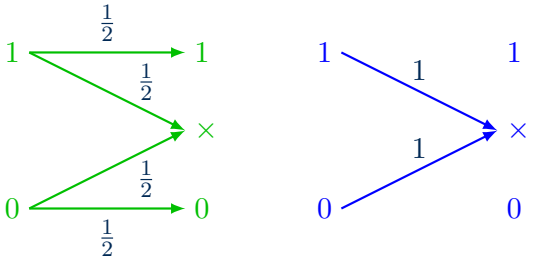







## The B92 protocol

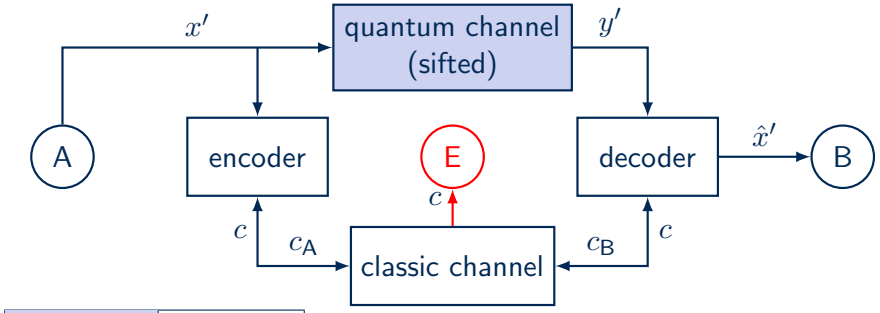
| $x_n$ | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|
| $a_n$ | ↔ | ⤢ | ⤢ | ↔ | ↔ | ⤢ | ⤢ | ⤢ |
| $B_n$ | ↕ | ↕ | ⤡ | ⤡ | ↕ | ⤡ | ↕ | ↕ |
| th | no | no | no | yes | no | no | yes | no |
| $y_n$ | × | × | × | 0 | × | × | 1 | × |








## Reconciliation of sifted keys




| quantum channel | classic channel |
|---|---|
| private | public |
| low rate | high rate |
| unreliable | reliable |

**Aim**

To allow B to reliably reconstruct $\hat{x}' = x'$, by transmitting $c = (c_A, c_B)$ publicly, with the minimum leakage of information $I(x'; c)$ to E.

## Existing models and solutions

Coding techniques for reconciliation fall into 1 of 3 categories:

**cascade** iteratively (and interactively) split the keys to locate single errors and correct them [Brassard-Salvail, '93]

**hashing** given a $(n, n-r)$ parity check matrix $\boldsymbol{H}$
Alice transmits $\boldsymbol{c} = \boldsymbol{H}\boldsymbol{x}'$.
Bob chooses $\hat{\boldsymbol{x}}' = \arg\min_{\boldsymbol{a}:\boldsymbol{H}\boldsymbol{a}=\boldsymbol{c}} d(\boldsymbol{a}, \boldsymbol{y})$
Examples: Winnow [Buttler *et al.*, '03]
LDPC [Elkouss *et al.*, '09]

**systematic** pick a $(n+r, n)$ generating matrix $\boldsymbol{G} = \begin{bmatrix} \boldsymbol{I}_n \\ \boldsymbol{A} \end{bmatrix}$
Alice transmits $\boldsymbol{c} = \boldsymbol{A}\boldsymbol{x}'$.
Bob chooses $\hat{\boldsymbol{x}}' = \arg\min_{\boldsymbol{a}\in\mathcal{C}} d(\boldsymbol{a}, \boldsymbol{y})$
Examples: LDPC [Mondin *et al.*, '10]
BCH [Traisilanun *et al.*, '07]





## Existing models and solutions

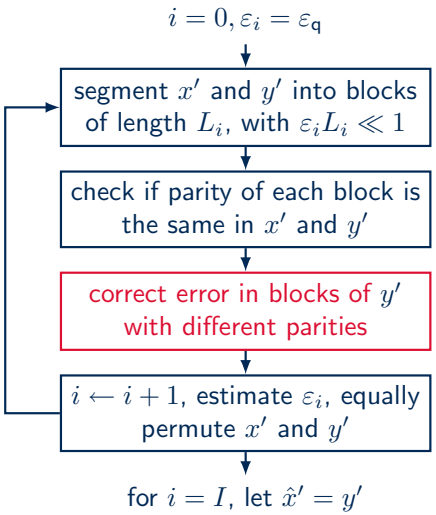
The choice of the coding technique for reconciliation depends on the model for the classical channel

| 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 | cascade, hashing |





## Cascade and Winnow: common structure




- the condition $\varepsilon_i L_i \ll 1$ ensures that multiple errors in a block are unlikely
- the block parities need to be exchanged $(c_A, c_B)$
- both algorithms can correct a single error per block

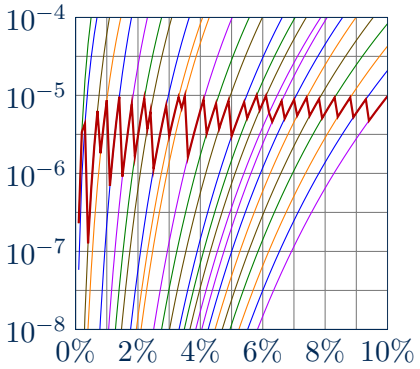




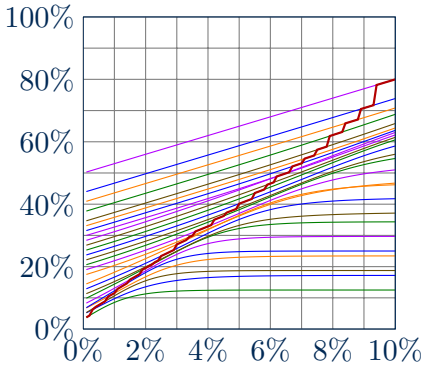
## Analysis and parameter optimization (Winnow)

Key BER target $\leq 10^{-5}$

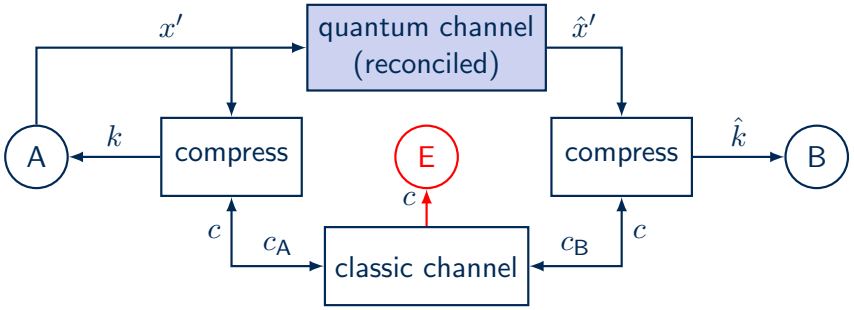
Reconciled Key BER




Average revealed bits



## Privacy amplification




| quantum channel | classic channel |
|---|---|
| private low rate | public high rate |

**Aim**

To allow A and B to remove any information E might have from $\hat{k} = k$, by publicly agreeing on the compressing function, and with the minimum amount of compression.





## Choosing a compression function

- Must be chosen randomly, after transmission
- Must be compactly representable

Assume we know that Eve has observed some $t$-bit linear function of the reconciled key

$$\boldsymbol{z} = \boldsymbol{M}\boldsymbol{x}' \quad , \quad \text{with } \boldsymbol{M} \in \{0,1\}^{t\times n}$$

(include $\boldsymbol{c}$ observed during reconciliation)

**Theorem (Universal hashing functions [Bennett *et al.*, '95])**

*If the compressing function $\boldsymbol{A}$ is chosen uniformly from a class of universal hashing $s \times n$ matrices, then on average (over $\boldsymbol{M}$ and $\boldsymbol{A}$)*

$$I(\boldsymbol{k}; \boldsymbol{z}, \boldsymbol{A}) \leq \frac{1}{\ln 2} 2^{s+t-n}$$





## Choosing a compression function

Once we choose a hashing matrix $\boldsymbol{A}$, we would like to obtain

1. $H(\boldsymbol{k}) = s$ (perfect uniformity)
2. $I(\boldsymbol{k}; \boldsymbol{z}) = 0$ (perfect secrecy)

**Lemma 1**

If $\operatorname{rank}(\boldsymbol{A}) = s$ and $\boldsymbol{x}'$ is uniform over $\{0,1\}^n$, then $\boldsymbol{k}$ is uniform over $\{0,1\}^s$

**Example: binary Toeplitz matrices**

- $\boldsymbol{A}$ is uniquely specified by $n+s-1$ bits $\boldsymbol{a} = [a_{-r+1}, \ldots, a_{n-1}]$
- If $\boldsymbol{a}$ is uniform in $\{0,1\}^{n+s-1}$, $\mathrm{P}\left[\operatorname{rank}(\boldsymbol{A}) < s\right] = 1/2^{n-s+1}$

**Lemma 2**

If $\dim \mathcal{N}(\boldsymbol{M}) - \dim\left(\mathcal{N}(\boldsymbol{M}) \cap \mathcal{N}(\boldsymbol{A})\right) = \operatorname{rank}(\boldsymbol{A})$ and $\boldsymbol{x}'$ is uniform over $\{0,1\}^n$, then $I(\boldsymbol{k}; \boldsymbol{z}) = 0$



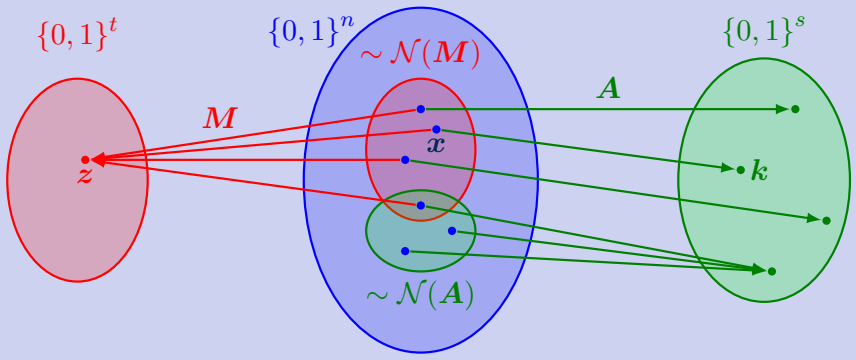


## Choosing a compression function

**Theorem**

*If $\dim \mathcal{N}(\boldsymbol{M}) - \dim\left(\mathcal{N}(\boldsymbol{M}) \cap \mathcal{N}(\boldsymbol{A})\right) = s$ and $\boldsymbol{x}'$ is uniform over $\{0,1\}^n$, then $\boldsymbol{k}$ is uniform and perfectly secret.*

**Illustration**



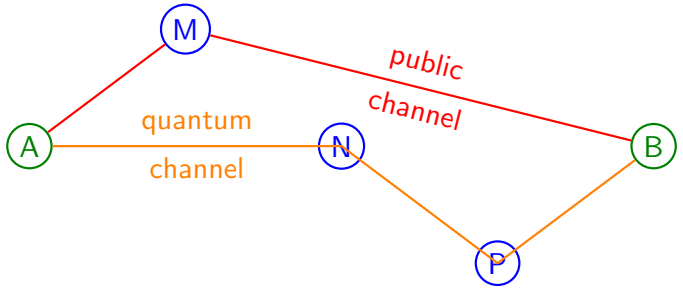
# Outline







# QKD networks with photonic switches

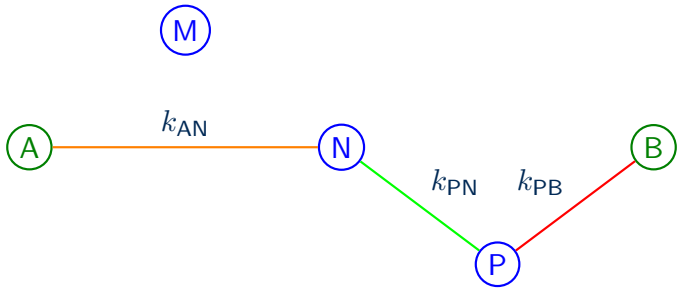



- the public channel can follow a different route
- N, P do not observe qubits directed from A to B
- switches in N, P introduce further losses in the lightpath A-B
  $\rightarrow$ reducing the achievable key rates





# QKD networks with trusted repeaters [Elliott, '02]

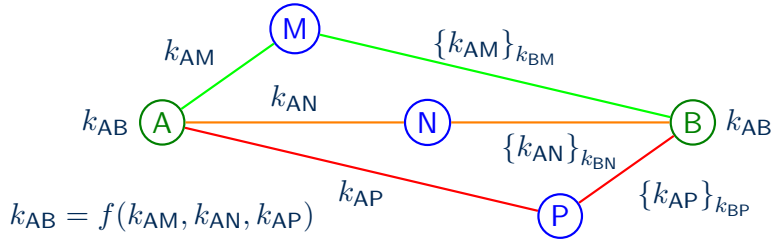



- On each link there is a different Quantum Key shared between the terminals
- A secret message (or a key $k_{AB}$) is decrypted and re-encrypted at nodes N, P
- Allows to geographically extend the network





# Reti QKD con ripetitori non sicuri [Salvail, '10]

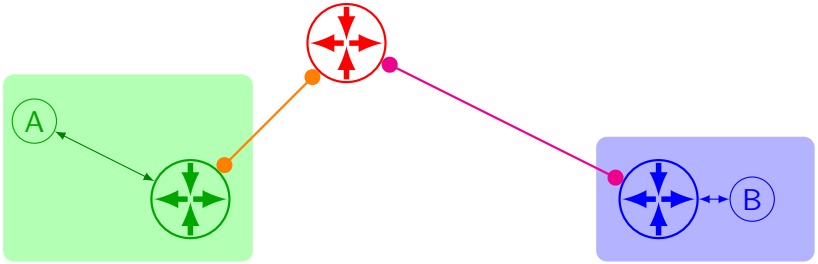



Use a secret sharing scheme $(n, t, d)$:

- $n$ intermediate nodes take part in transmitting the key from A to B
- any $t$ nodes, nodes behaving honestly allow reconstruction of the key $k_{AB}$ in A and B
- up to $d$ malicious and colluding nodes con not obtain any information on $k_{AB}$

Can be generalized to arbitrary access structures $(N, \mathcal{T}, \mathcal{D})$

## Integration with IPSec Tunnel mode

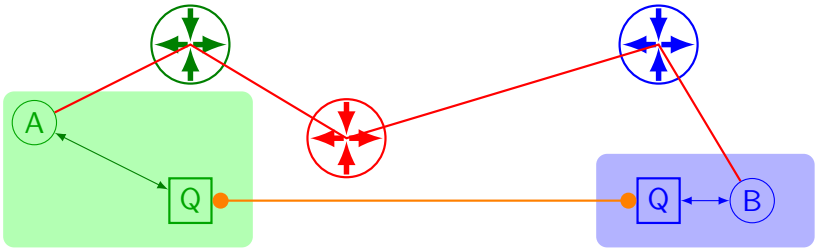



- QKD can provide master secrets, replacing Diffie-Hellman in IKE and ISAKMP
- Only cryptographic gateways need to be linked by quantum channels and equipped with QKD terminals
- Terminal to gateway path must be secured otherwise
- Authenticated channel between gateways?





## Integration with TLS?

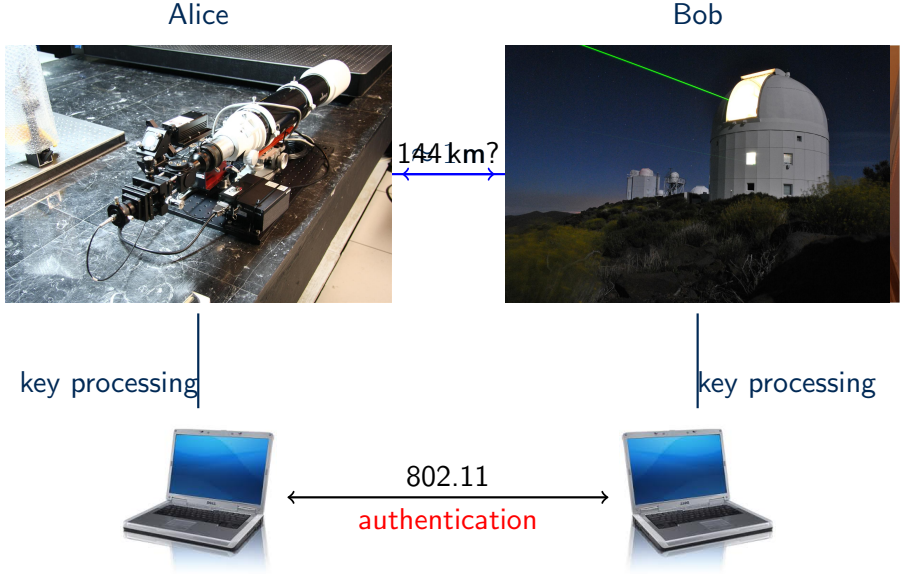



- QKD can provide shared master secrets, replacing D-H/RSA in TLS handshake protocol
- Every subnetwork pair must share a quantum channel
- In-subnetwork paths must be otherwise secured
- Authenticated channel between subnetworks





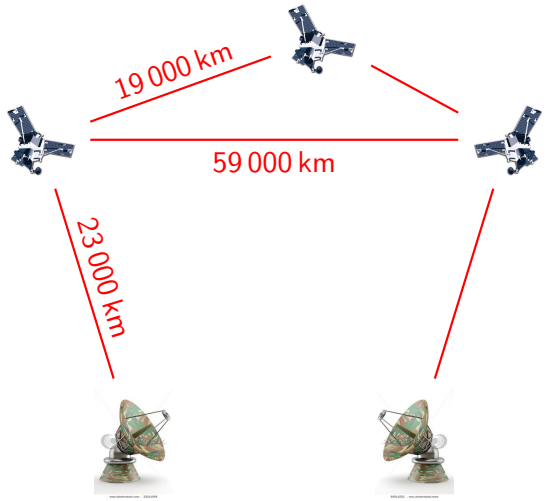
## QKD implementation in Quantum Future








## Ideas for a QKD intersatellite network




- Key reconciliation based on LDPC codes
- QKD network with (partially) trusted repeaters
- Resilient to node capture
- Use QKD in *end-to-end* protocols at all layers

## References: Cryptography


C. E. Shannon
"Communication Theory of Secrecy Systems"
*Bell System Technical Journal*, 28(4): 656–715, 1949.

W. Diffie and M. E. Hellman
"New Directions in Cryptography"
*IEEE Trans. Inf. Th.*, 22(6): 644–654, 1976.

R. L. Rivest, A. Shamir, and L. Adleman
"A method for obtaining digital signatures and public-key cryptosystems"
*Communications of the ACM*, 21(2): 120–126, 1978.






## References: Information Theoretic Security


A. D. Wyner
"The wire-tap channel"
*Bell System Technical Journal*, 54(4): 1355–1387, 1975.

I. Csiszar and J. Korner
"Broadcast Channels with Confidential Messages"
*IEEE Trans. Inf. Th.*, 24(3): 339–348, 1978.

J. Barros and M. R. D. Rodrigues
"Secrecy Capacity of Wireless Channels"
*ISIT '06*, 356–360.

M. Bloch and J. N. Laneman
"On the Secrecy Capacity of Arbitrary Wiretap Channels"
*Allerton Conference*, 2008.






## References: Information Theoretic Key Agreement


R. Ahlswede and I. Csiszar
"Common randomness in information theory and cryptography — Part I: Secret sharing"
*IEEE Trans. Inf. Th.*, 39(4): 1121–1132, 1993.

U. M. Maurer
"Secret key agreement by public discussion from common information"
*IEEE Trans. Inf. Th.*, 39(3): 733–742, 1993.

C. H. Bennett, G. Brassard, C. Crepeau, U. M. Maurer
"Generalized privacy amplification"
*IEEE Trans. Inf. Th.*, 41(6): 1915–1923, 1995.






## References: Quantum Key Distribution


C. H. Bennett
"Quantum cryptography using any two nonorthogonal states"
*Phys. Rev. Lett.*, 68(21): 3121–3124, 1992.

N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden
"Quantum cryptography"
*Rev. Mod. Phys.*, 74(1): 145–195, 2002.

D. Gottesman
"Proof of security of quantum key distribution with two-way classical communications"
*IEEE Trans. Inf. Th.*, 49(2): 457–475, 2003.

## References: Information Reconciliation


- G. Brassard, L. Salvail
  "Secret-Key Reconciliation by Public Discussion"
  *EUROCRYPT 1993*, 410–423.
- 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"
  *Phys. Rev. A*, 67(5): 052303/1–8, 2003..
- D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros
  "Efficient reconciliation protocol for discrete-variable quantum key distribution"
  *ISIT '09*, 1879–1883.






## References: QKD networks


- C. Elliott
  "Building the quantum network"
  *New J. Phys.*, 4(1): 1–12, 2002.
- C. Elliott, D. Pearson, and G. Troxel
  "Quantum cryptography in practice"
  *ACM SIGCOMM '03*, 227–238.
- L. Salvail, M. Peev, E. Diamanti, and R. Alléaume
  "Security of trusted repeater quantum key distribution"
  *J. of Computer Security*, 18(1): 61–87, 2010.






## References: QKD and network protocols


- M. A. Sfaxi, S. Ghernaouti-Hélie, G. Ribordy, and O. Gay
  "Using Quantum Key Distribution within IPSEC to secure MAN communications"
  *IFIP MAN conference*, 2005.
- S. Ghernaouti-Hélie and M. A. Sfaxi
  "Upgrading PPP security by Quantum Key Distribution"
  *IFIP International Conference on Network Control and Engineering for QoS, Security and Mobility*, 2007.
- M. Elboukhari, M. Azizi, and A. Azizi
  "Improving TLS Security By Quantum Cryptography"
  *Int. J. Netw. Secur. & Appl.*, 2(1): 87–100, 2010.






## References: Some of our works


- 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"
  *ISABEL*, 2011.
- M. Canale, F. Renna, and N. Laurenti
  "QKD secrecy for privacy amplification matrices with selective individual attacks"
  *QCRYPT*, vol. 12318: 52304–52304, 2011.
- F. Renna, M. Bloch, and N. Laurenti
  "Semi-Blind Key-Agreement over MIMO Fading Channels"
  *IEEE ICC*, 1–6, 2011.