Practical schemes for Secret Key Agreement as applied to QKD

Matteo Canale, Nicola Laurenti
{canalema,nil}@dei.unipd.it

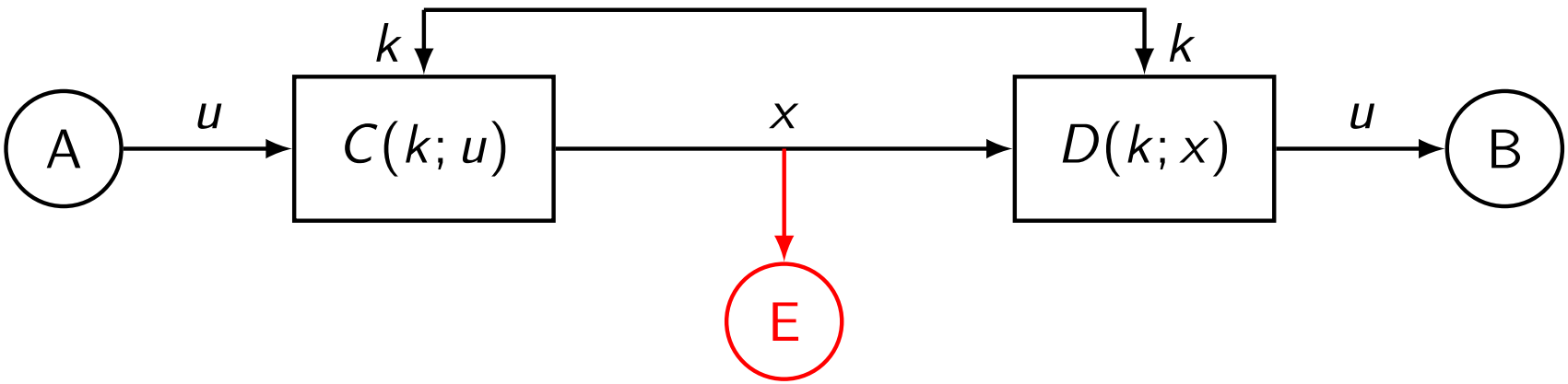
July 5th, 2011

Outline

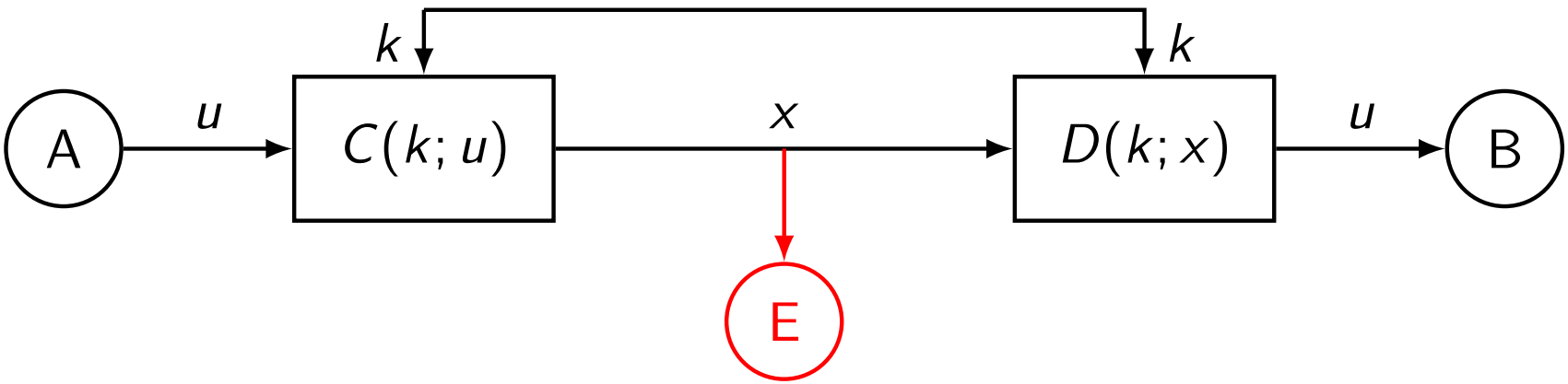
Outline

Outline

Security in a communication system



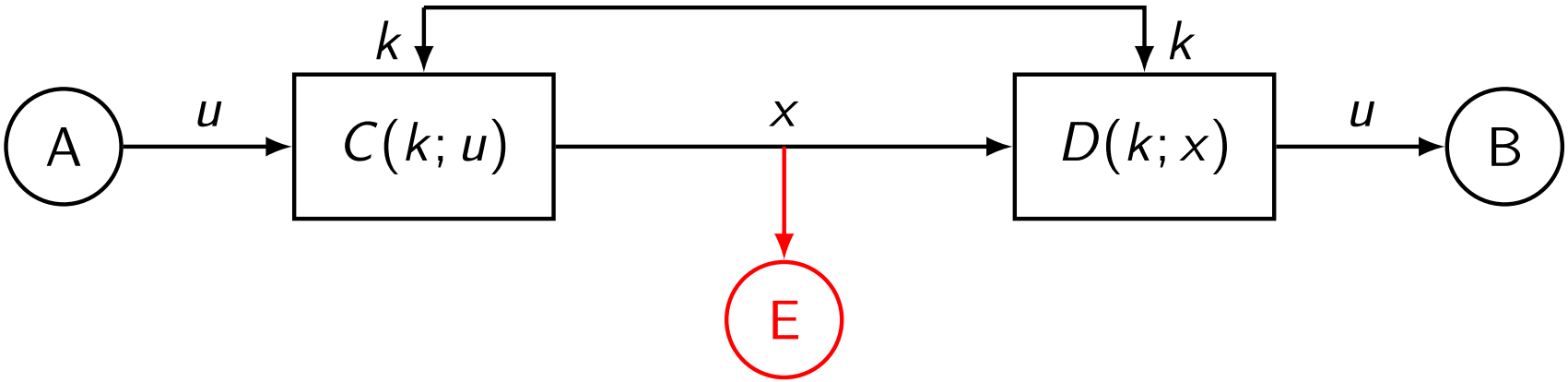
Security in a communication system



Kerchoffs's Principle

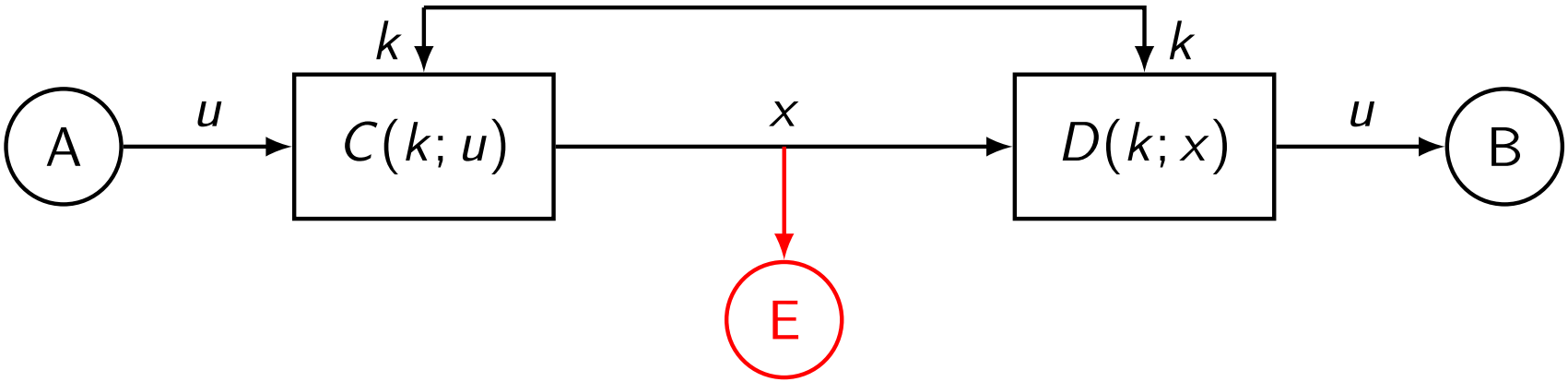
A cryptosystem should be secure even if everything about the system, *except the key*, is public knowledge.

Computational Vs. Information-Theoretic Security



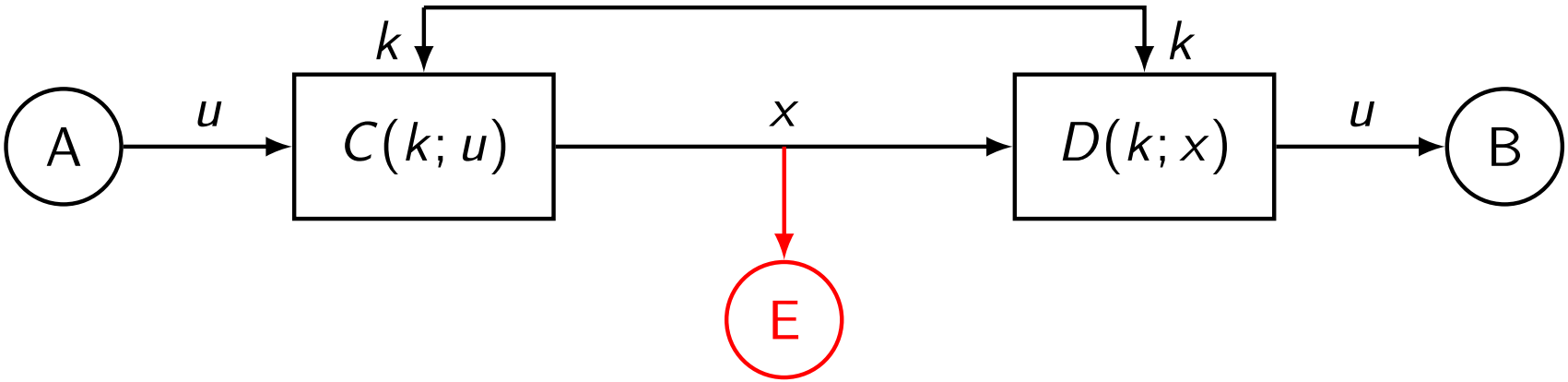
- *Computational security*

Computational Vs. Information-Theoretic Security



- *Computational security*
  - computing u is *computationally infeasible* given x but not k
  - based on the assumed, yet unproven, hardness of a certain problem (e.g., factoring large integers)

Computational Vs. Information-Theoretic Security



- *Computational security*
  - computing u is *computationally infeasible* given x but not k
  - based on the assumed, yet unproven, hardness of a certain problem (e.g., factoring large integers)
- Information-Theoretic Security
  - $I(u; x) \to 0$
  - based on information theory, it is the strongest notion of security, no assumptions on the attacker's computing power

Quantum tools for I-T security

- Physical laws of quantum mechanics can be exploited while looking for I-T security

Quantum tools for I-T security

- 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 I-T security

- 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

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

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

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 shared information is actually secret

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

$$\Downarrow$$

Quantum Key Distribution
(QKD)

QKD at UNIPD: the QuantumFuture project

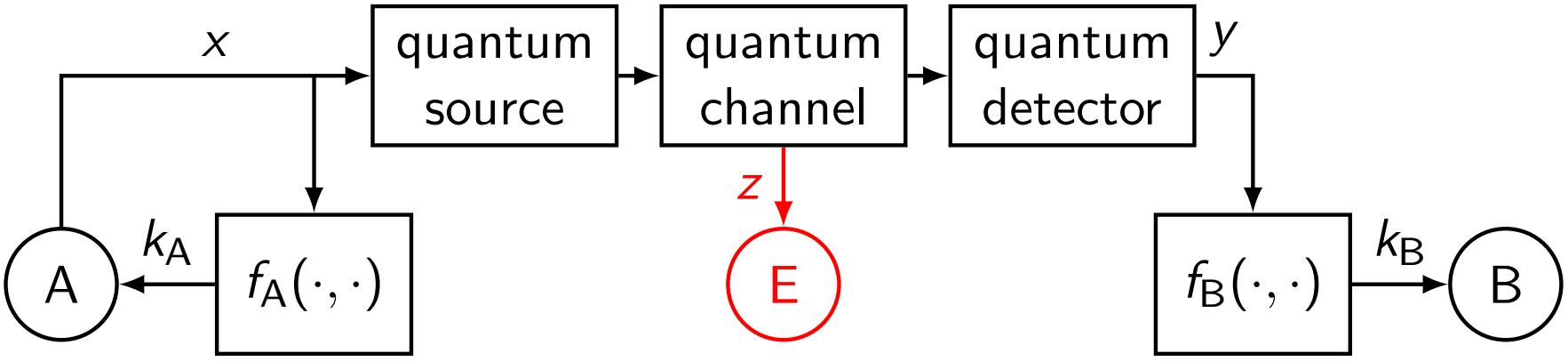
QuantumFuture

- 3-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

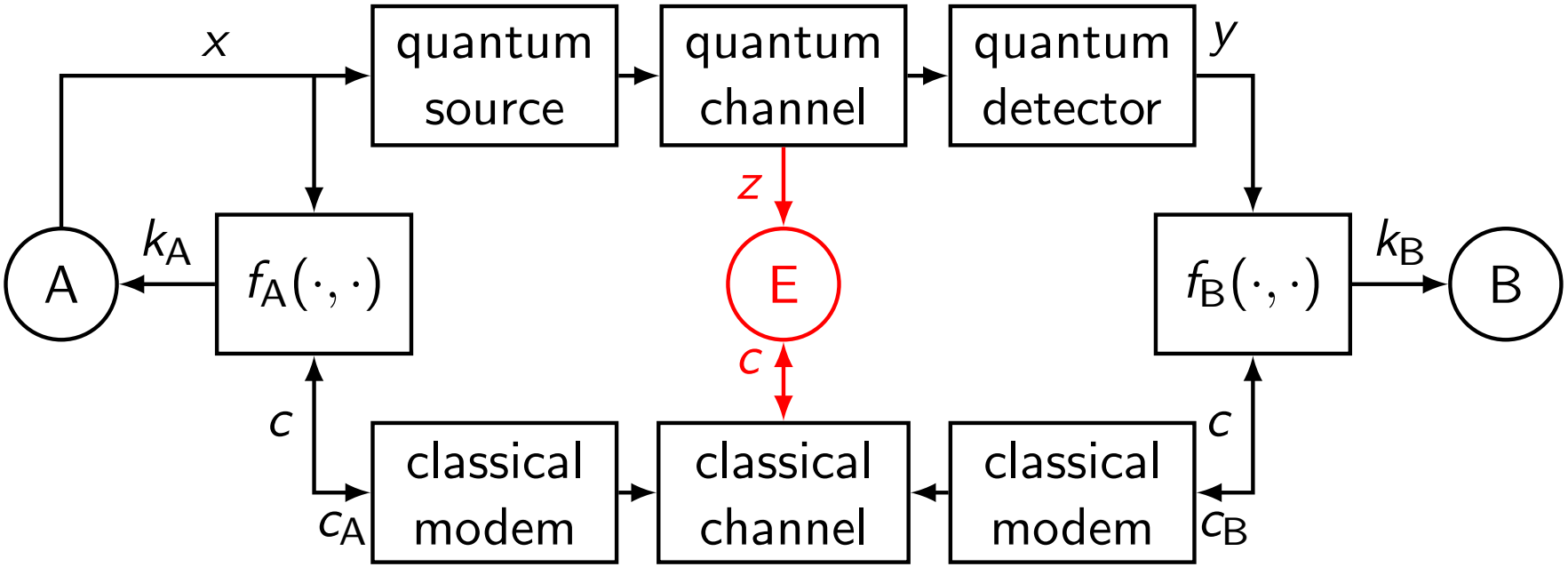
More information available at:
http://quantumfuture.dei.unipd.it

Outline

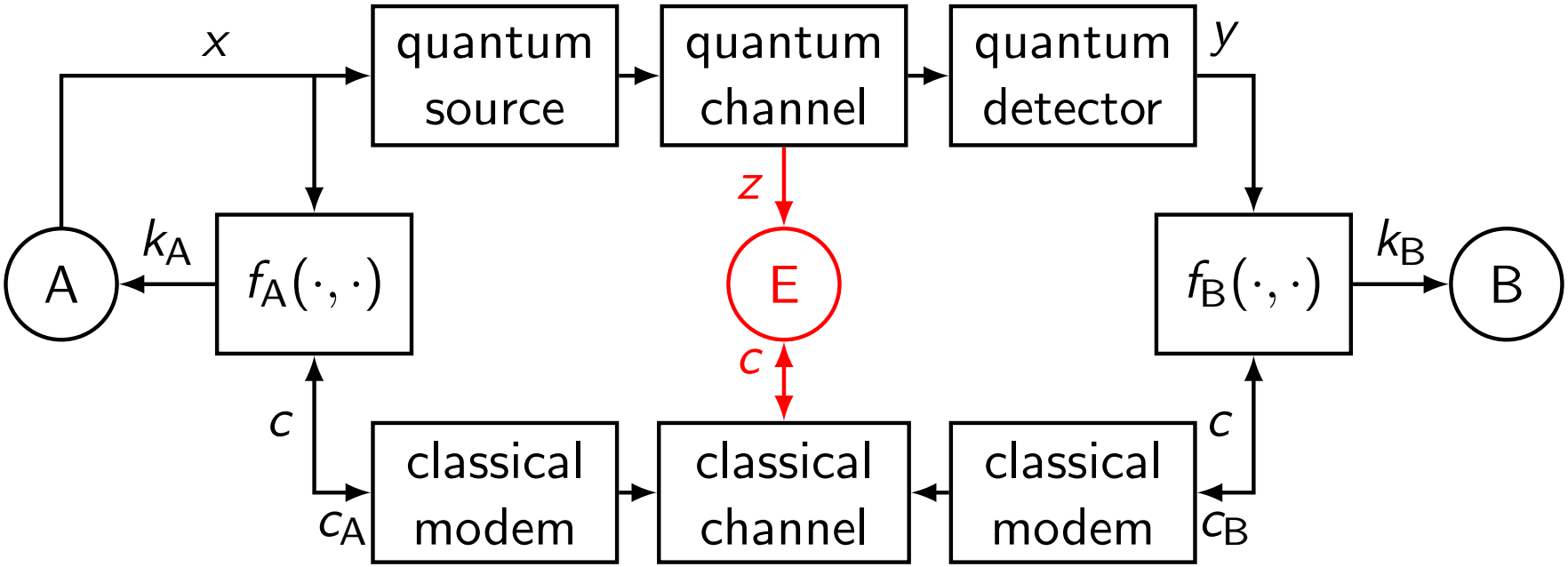
QKD system model (I)



QKD system model (I)



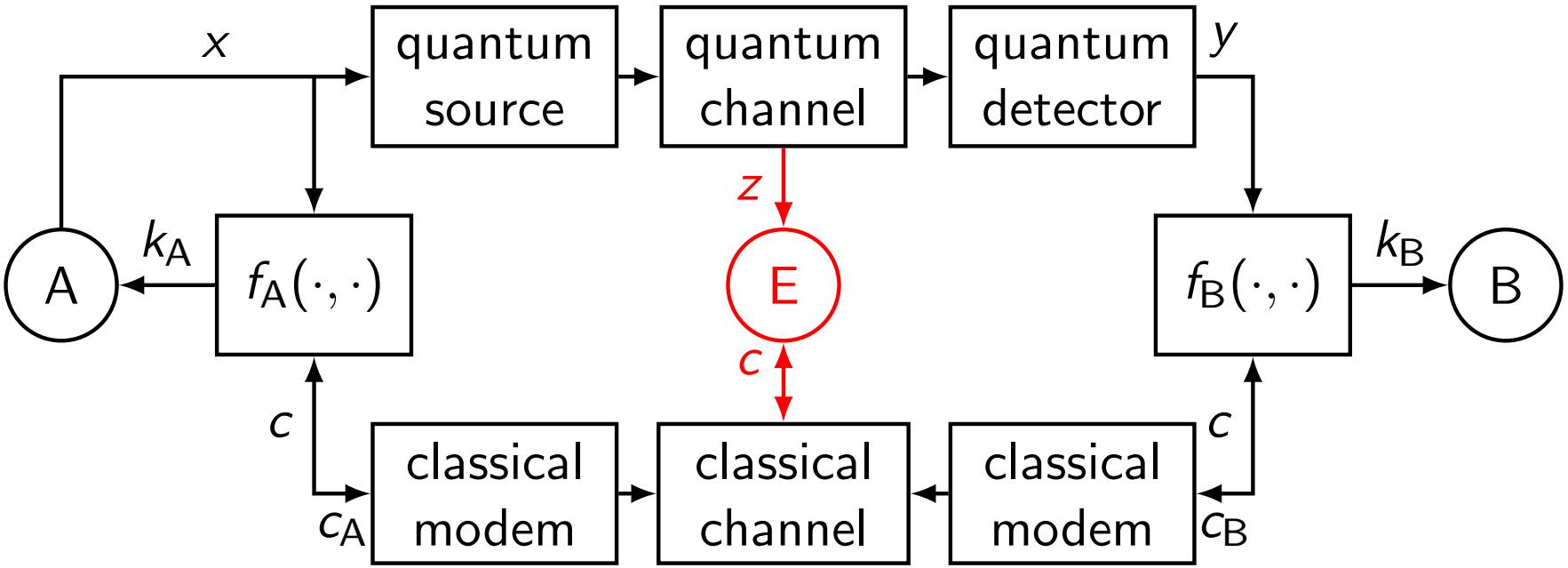
QKD system model (I)



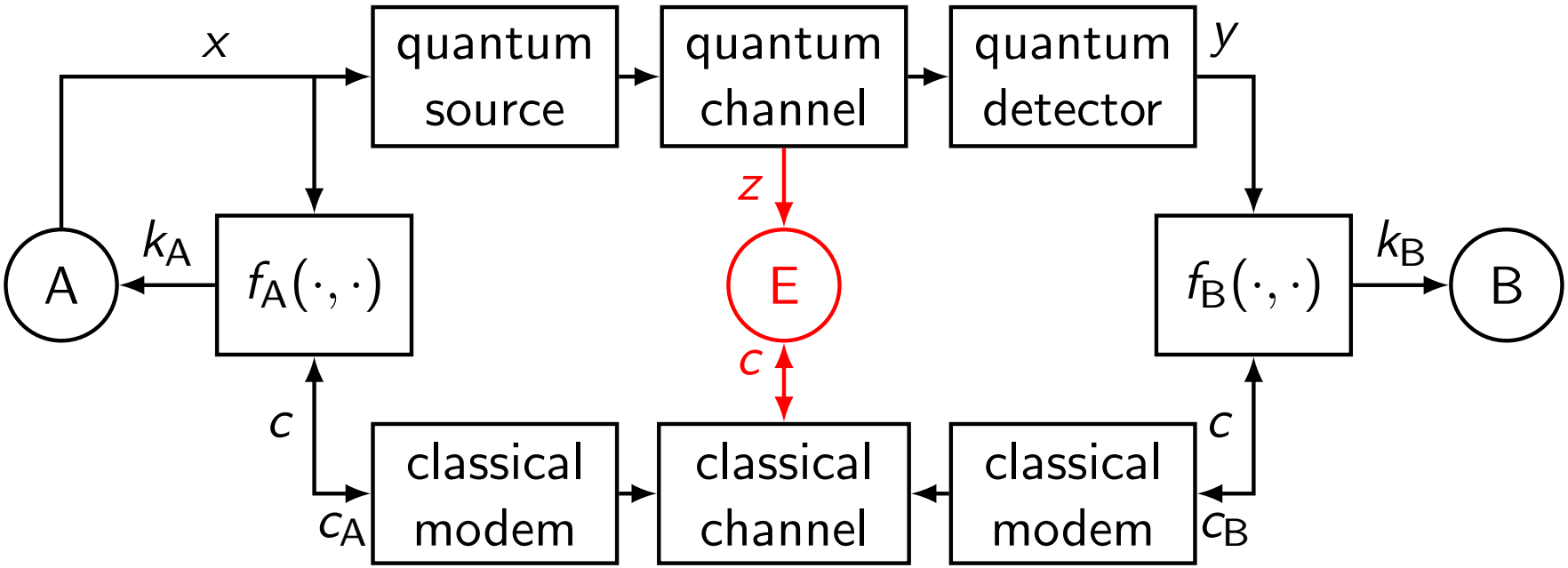
Channel characteristics

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

QKD system model (II)



QKD system model (II)



Objective

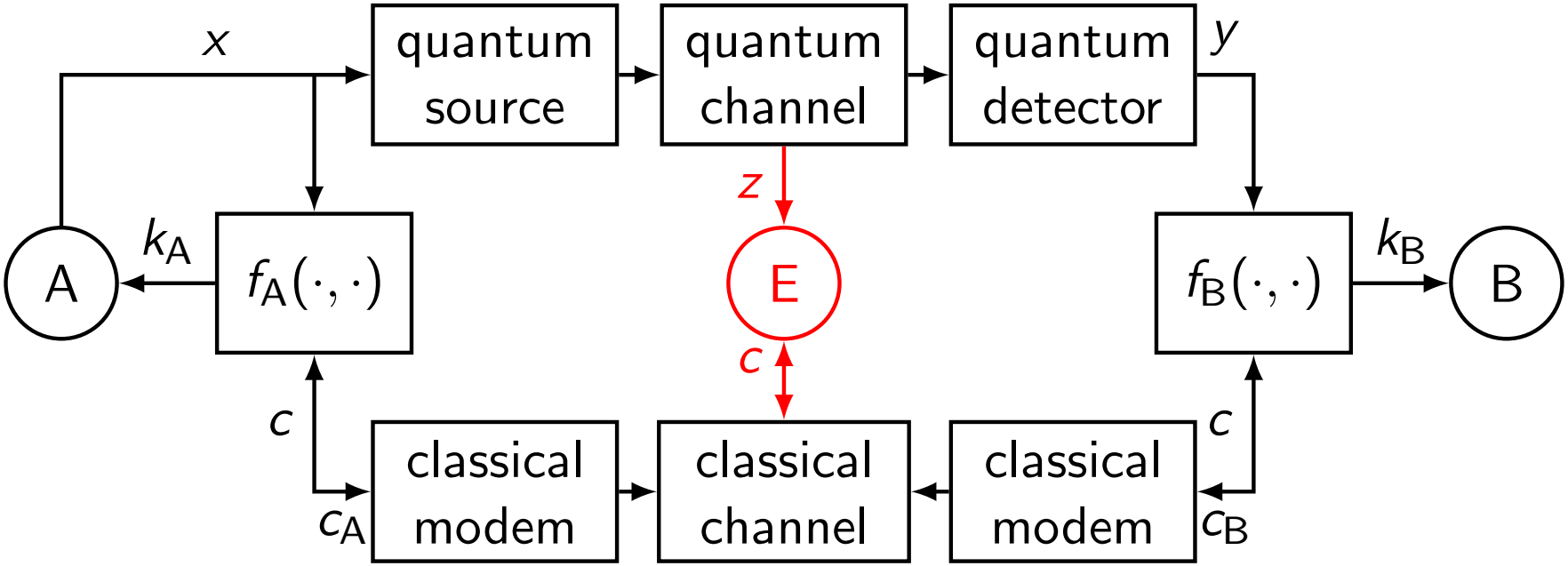
$$\max_{f_a, f_B, x} H(k_A) \quad \text{subject to:}$$

correctness: $P[k_A = k_B] < \varepsilon$

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

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

QKD system model (II)



Objective

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

correctness: $P[k_A = k_B] < \varepsilon$

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

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

Upper bound

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

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

A practical scheme (I)

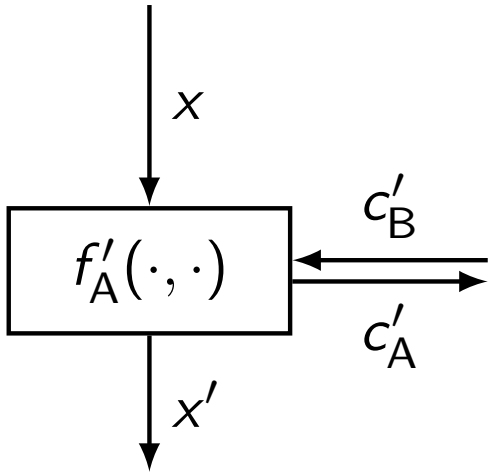
Based on a divide and conquer approach
3-phase protocol [Maurer, '93]:

A practical scheme (I)

Based on a divide and conquer approach
3-phase protocol [Maurer, '93]:

1. Sifting $\rightarrow$ advantage over E

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



A practical scheme (I)

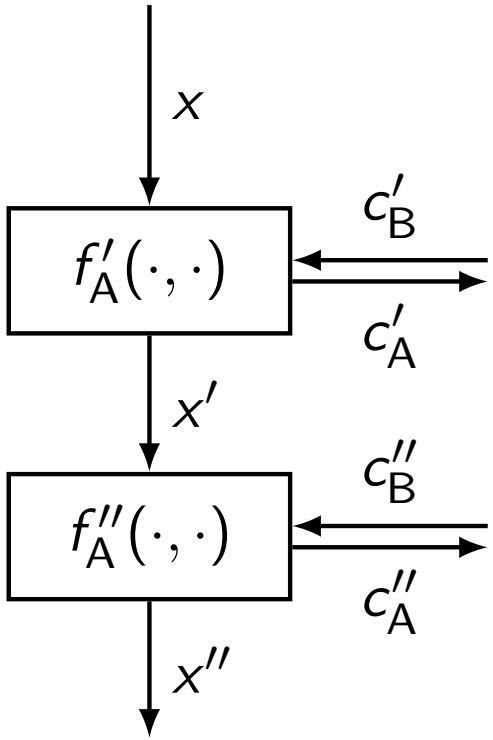
Based on a divide and conquer approach
3-phase protocol [Maurer, '93]:

1. Sifting $\rightarrow$ advantage over E

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

2. Information reconciliation $\rightarrow$ correctness

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



A practical scheme (I)

Based on a divide and conquer approach
3-phase protocol [Maurer, '93]:

1. Sifting $\rightarrow$ advantage over E

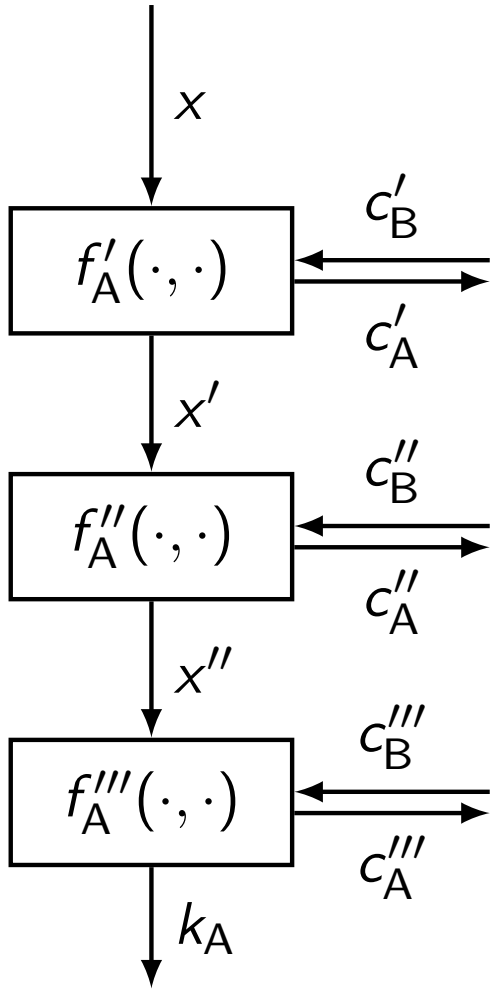
$$\text{so that} \quad I(x';y') > I(x';z,c')$$

2. Information reconciliation $\rightarrow$ correctness

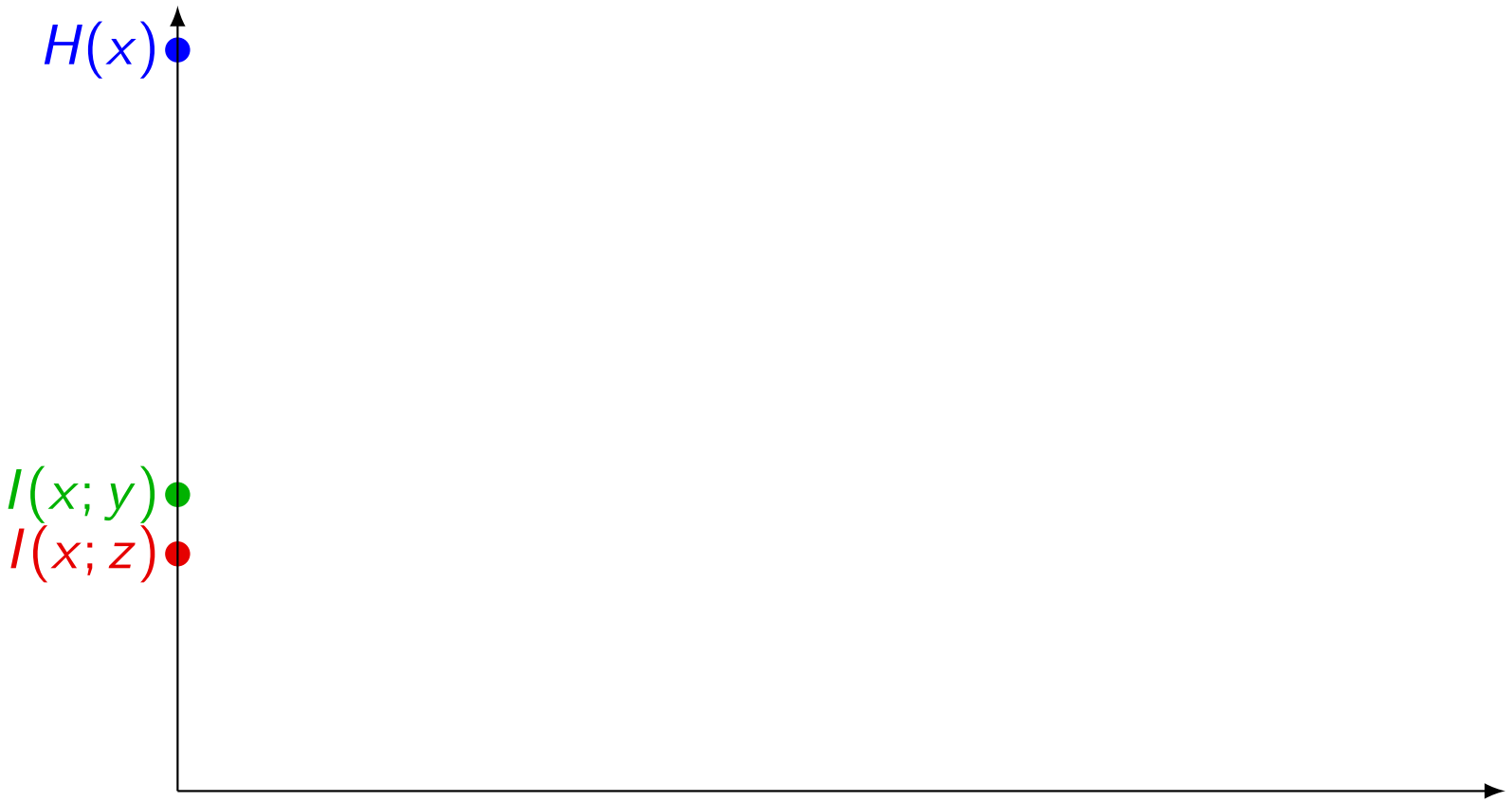
$$\text{so that} \quad \mathrm{P}\left[x'' \neq y''\right] < \varepsilon'$$

3. Privacy amplification $\rightarrow$ secrecy

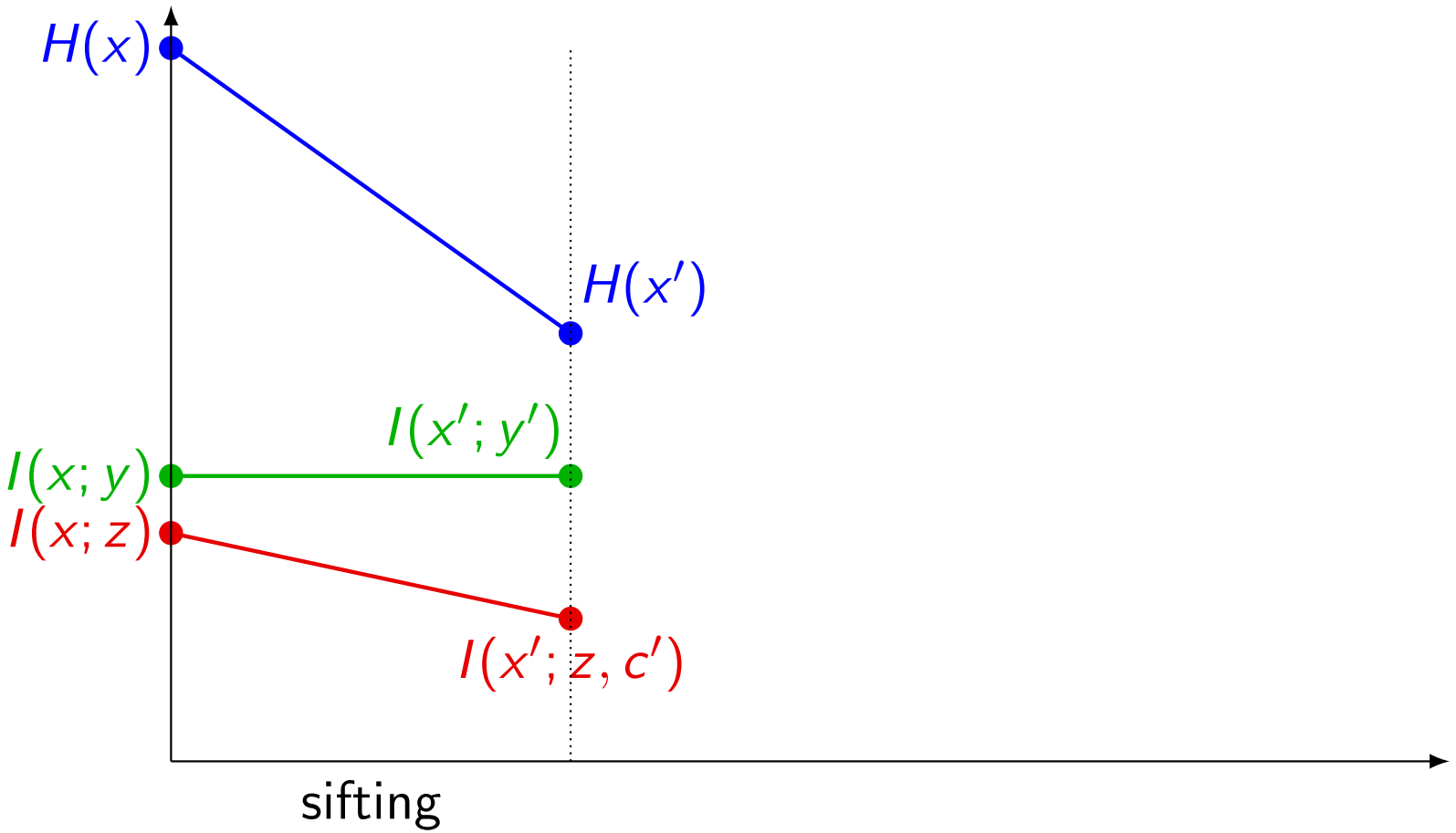
$$\text{so that} \quad I(k_A,k_B;z,c) < \varepsilon''$$



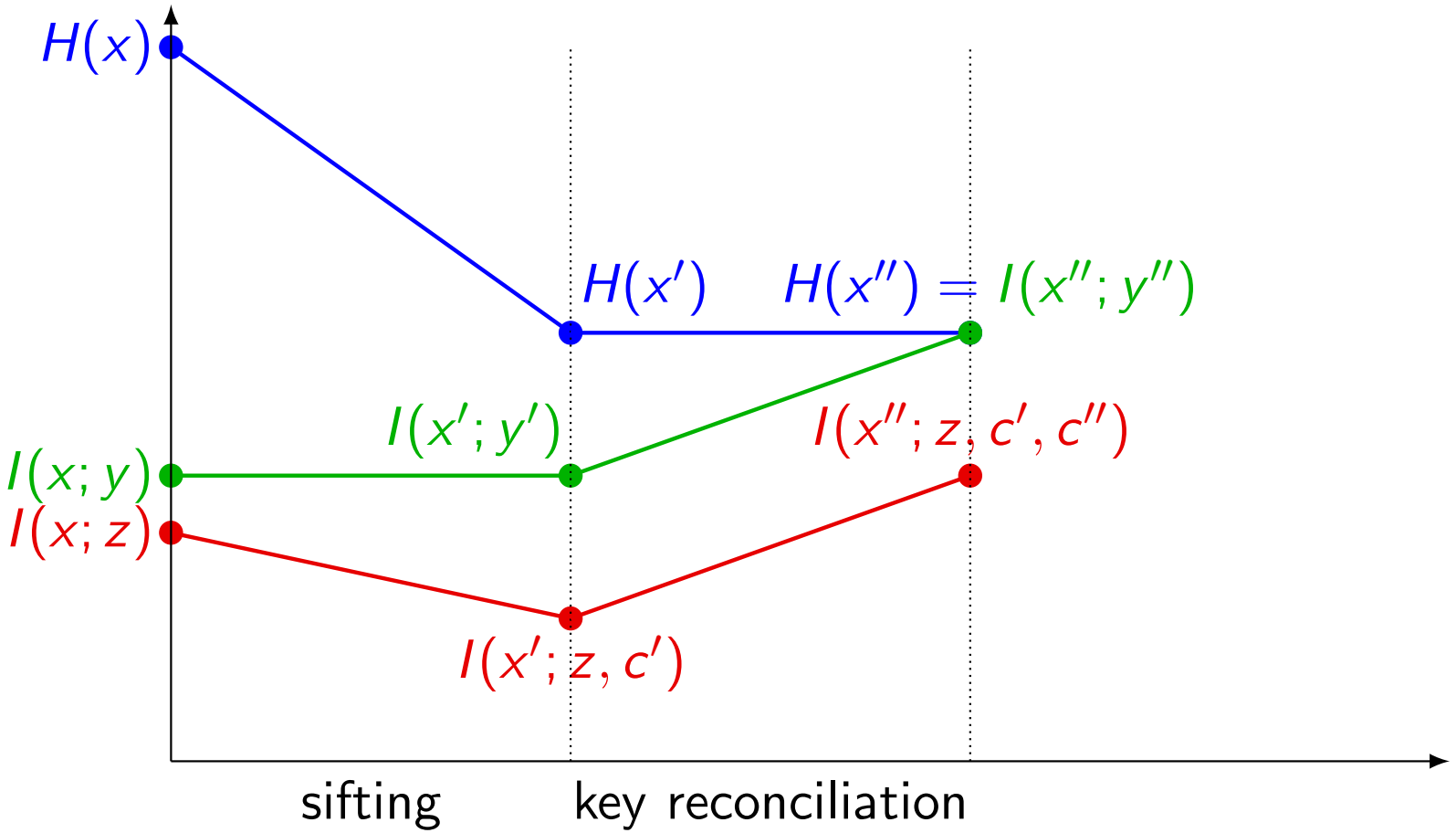
A practical scheme (II)



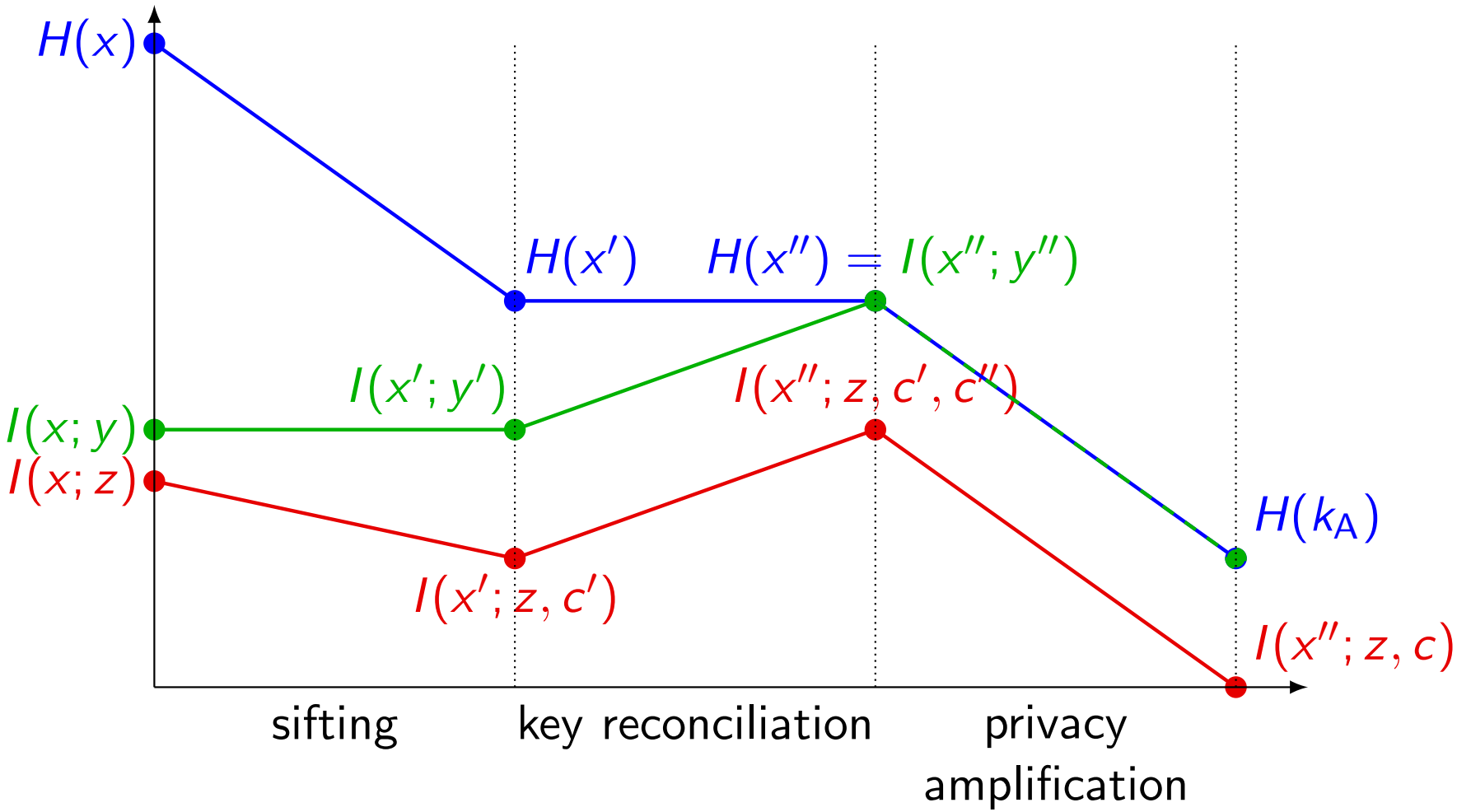
A practical scheme (II)



A practical scheme (II)

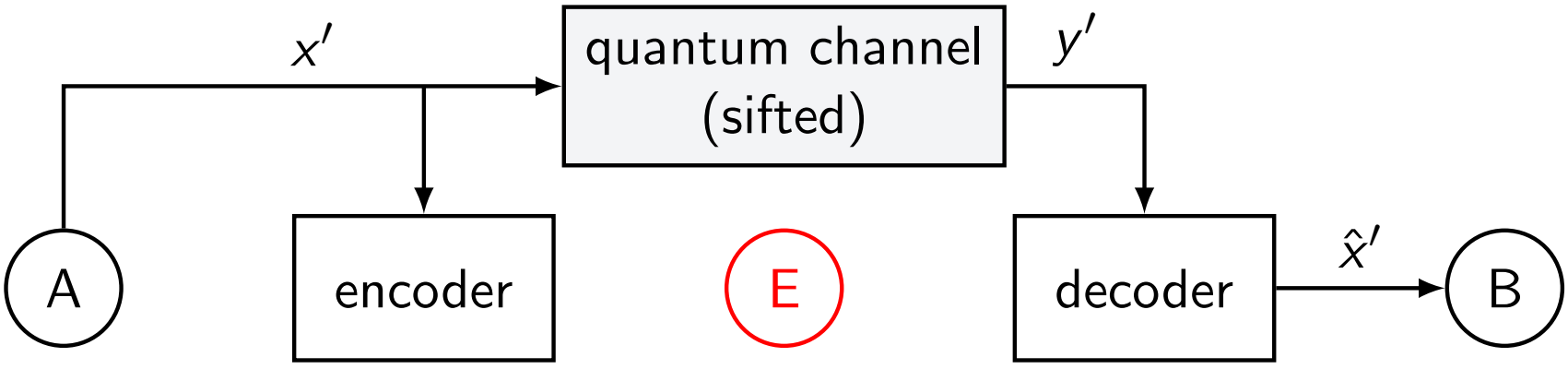


A practical scheme (II)

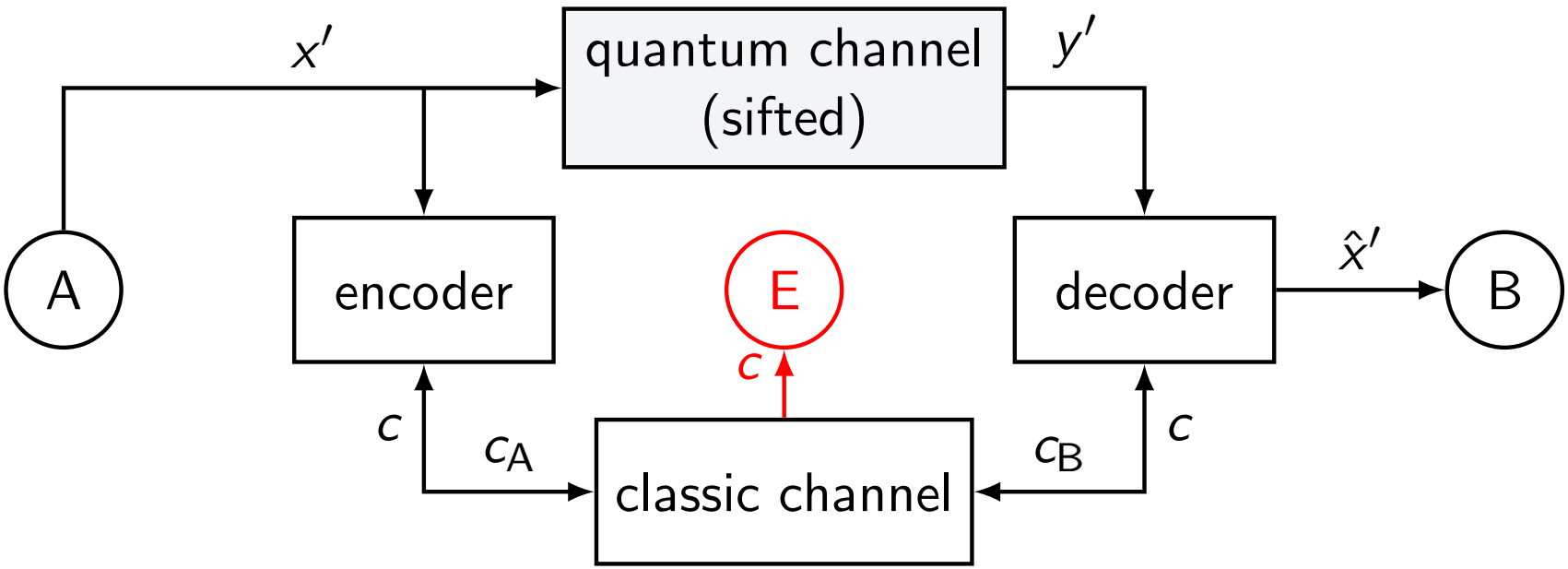


Outline

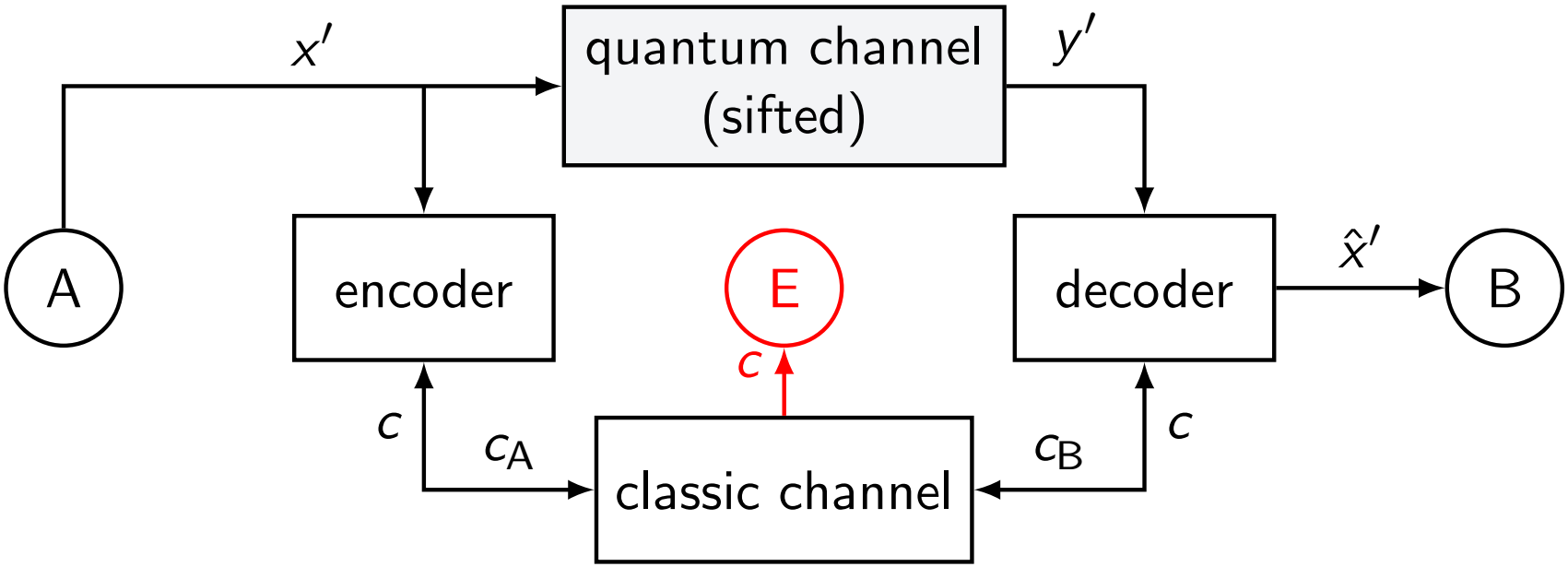
Key reconciliation



Key reconciliation



Key reconciliation



Goals

1. Correctness: $P[x' = \hat{x}'] \approx 1$
2. Minimum information leakage: $I(x'; c) \to 0$

Key reconciliation approaches (I)

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

Key reconciliation approaches (I)

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 $\mathbf{G} = \begin{bmatrix} \mathbf{I}_n \\ \mathbf{A} \end{bmatrix}$:

   Alice transmits $\mathbf{c} = \mathbf{A}\mathbf{x}'$
   Bob chooses $\hat{\mathbf{x}}' = \arg\min_{\mathbf{a} \in \mathcal{C}} d(\mathbf{a}, \mathbf{y})$
   Examples: LDPC [Mondin *et al.*, '10]
   BCH [Traisilanun *et al.*, '07]

Key reconciliation approaches (I)

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 $\mathbf{G} = \begin{bmatrix} \mathbf{I}_n \\ \mathbf{A} \end{bmatrix}$:

   Alice transmits $\mathbf{c} = \mathbf{A}\mathbf{x}'$
   Bob chooses $\hat{\mathbf{x}}' = \arg\min_{\mathbf{a}\in\mathcal{C}} d(\mathbf{a}, \mathbf{y})$
   Examples: LDPC [Mondin *et al.*, '10]
   BCH [Traisilanun *et al.*, '07]
3. *Hashing* - given a $(n, n-r)$ parity check matrix $\mathbf{H}$:
   Alice transmits $\mathbf{c} = \mathbf{H}\mathbf{x}'$
   Bob chooses $\hat{\mathbf{x}}' = \arg\min_{\mathbf{a}:\mathbf{H}\mathbf{a}=\mathbf{c}} d(\mathbf{a}, \mathbf{y})$
   Examples: Winnow [Buttler *et al.*, '03]
   LDPC [Elkouss *et al.*, '09]

Key reconciliation approaches (II)

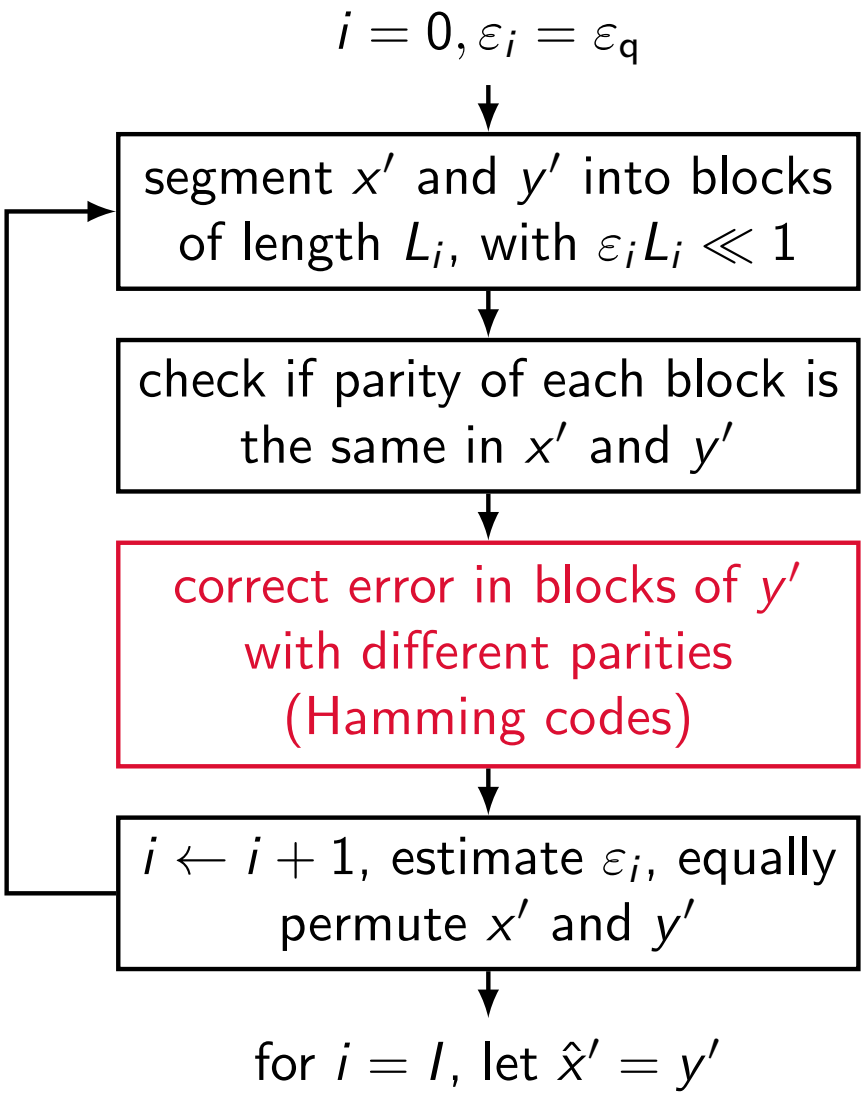
The choice of the coding technique for reconciliation depends on the model for the classical channel

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

Case study: Winnow

- Hashing-based key reconciliation protocol
- Ingredients
  - parity check
  - Hamming codes
  - syndrome decoding

Case study: Winnow



- Hashing-based key reconciliation protocol
- Ingredients
  - parity check
  - Hamming codes
  - syndrome decoding

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

Case study: Winnow optimization (I)

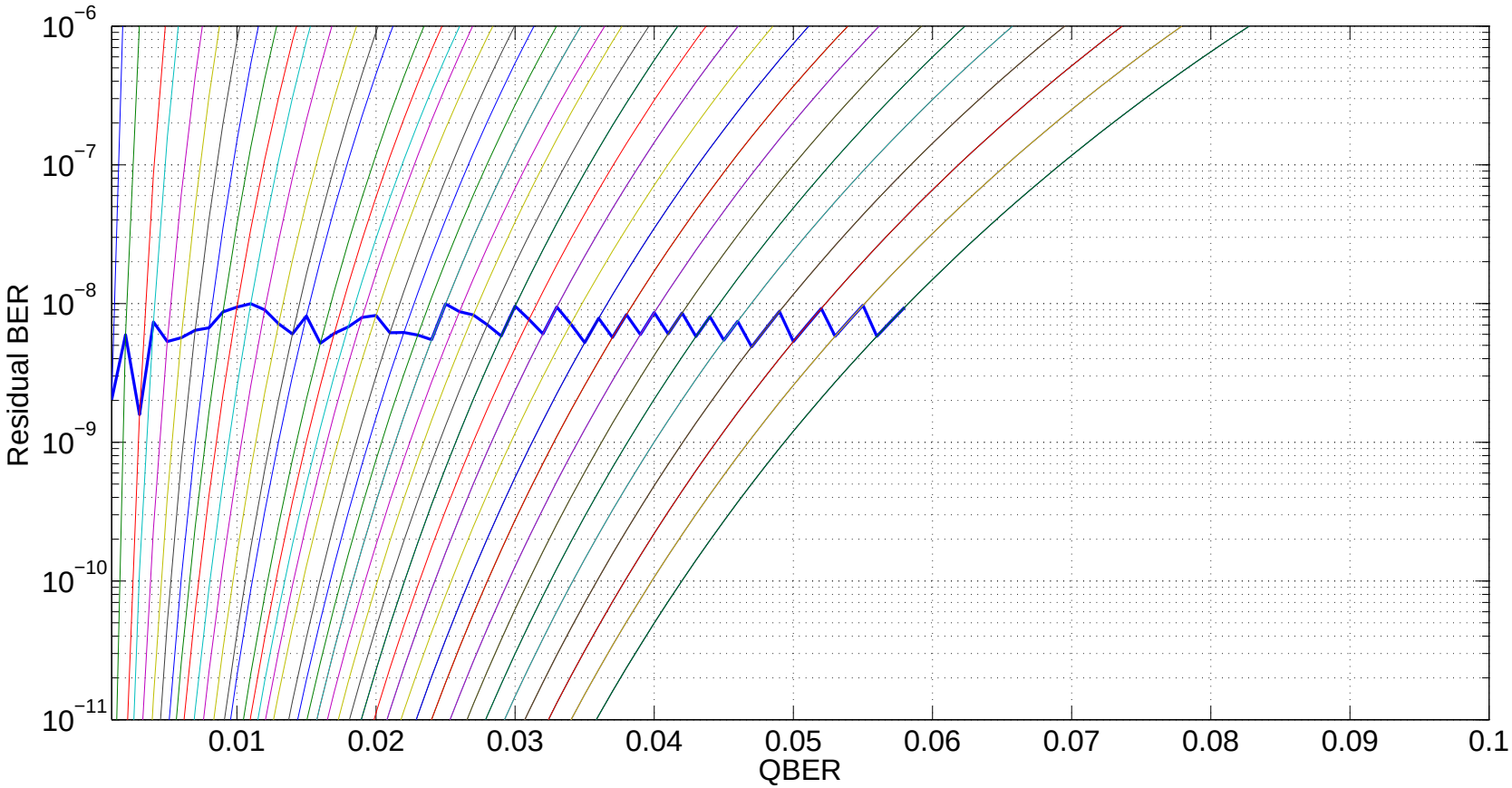


Figure: Winnow block size optimization: residual BER with target BER equal to 10^{-8}, max 4 iterations, max block size 512 bit.

Case study: Winnow optimization (II)

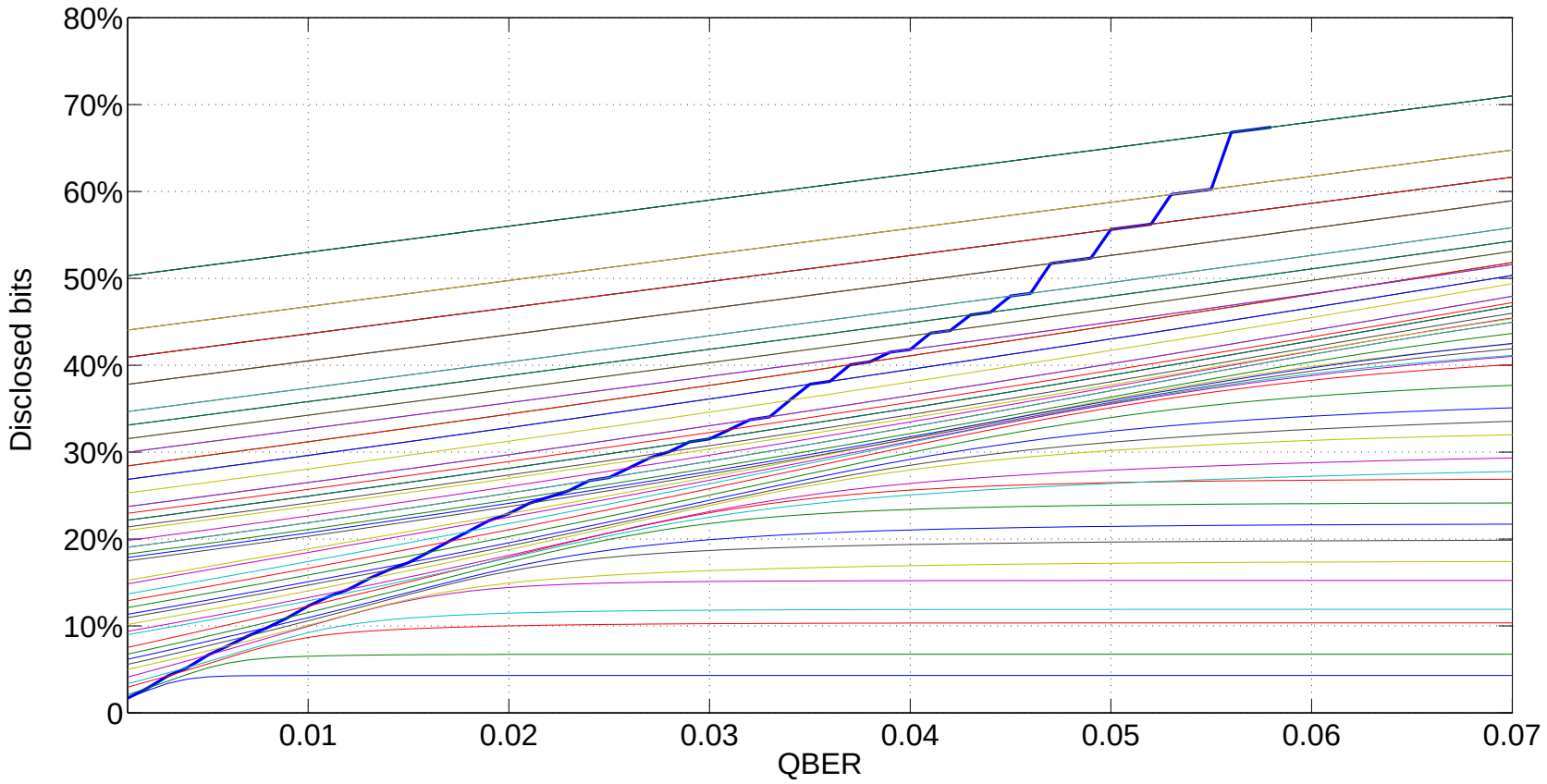


Figure: Winnow block size optimization: fraction of disclosed bits with target BER equal to 10^{-8}, max 4 iterations, max block size 512 bit.

Case study: Winnow optimization (III)

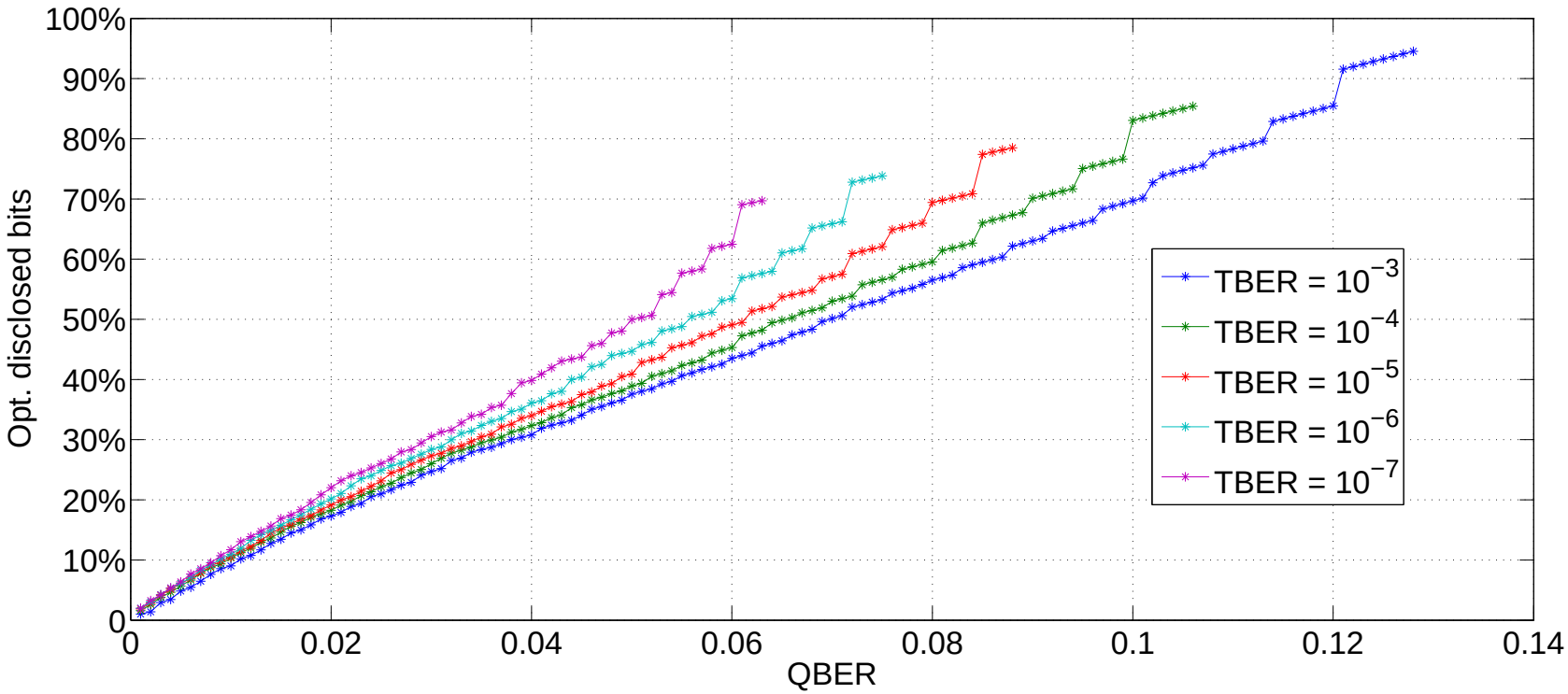
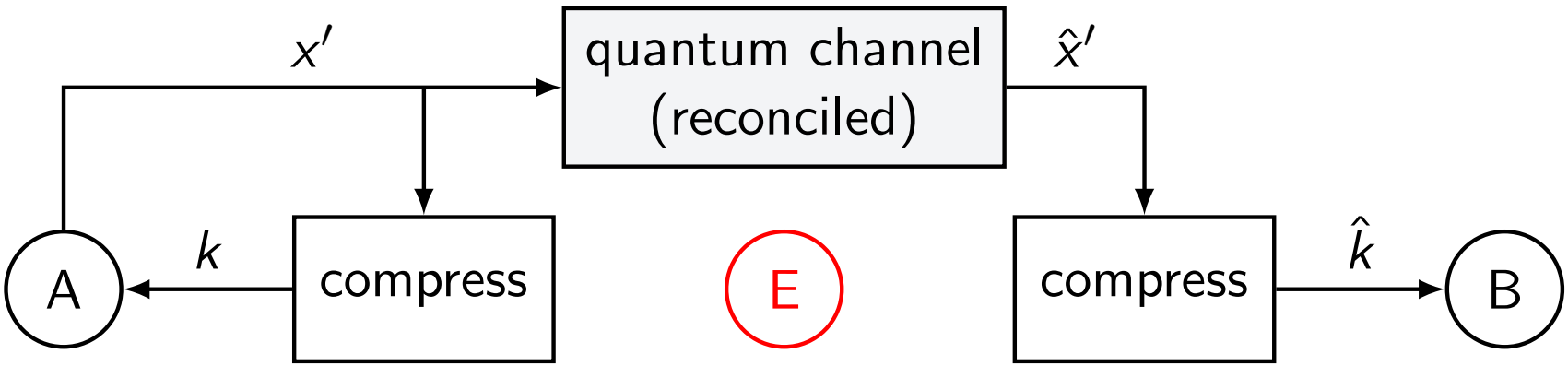


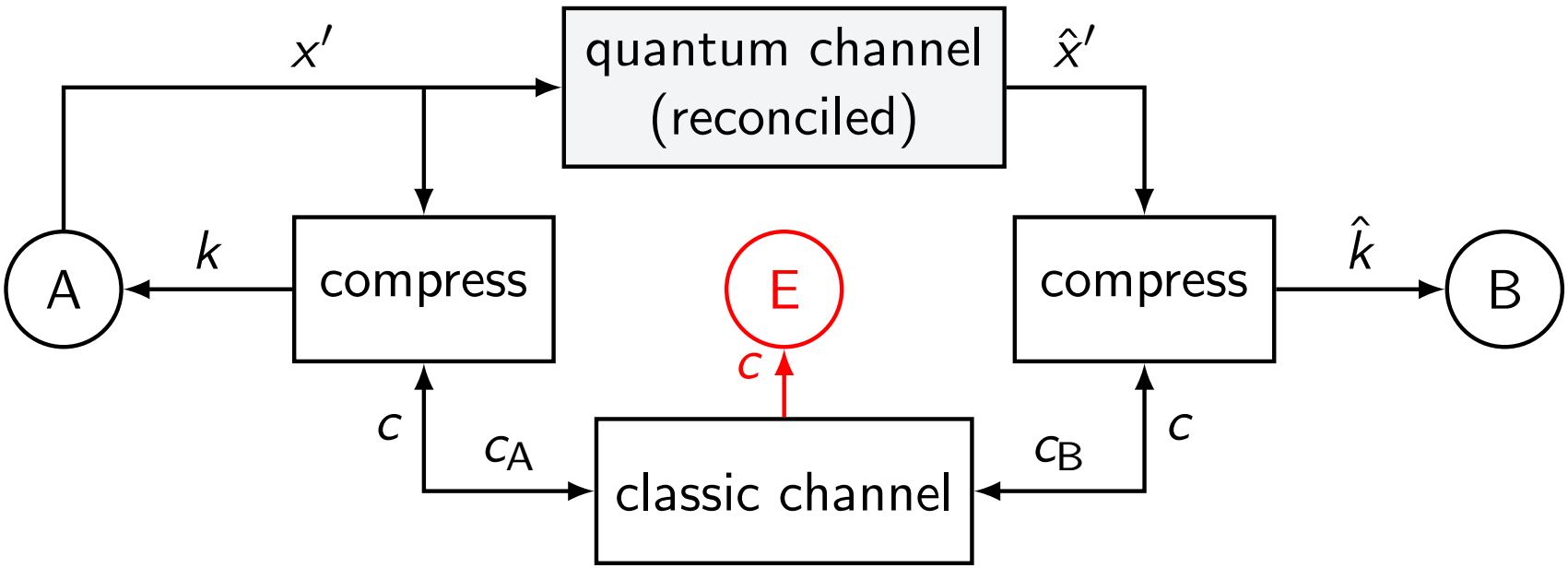
Figure: Winnow, optimal percentage of disclosed bits for different target bit error rates, max 4 iterations, max block size 512 bit.

Outline

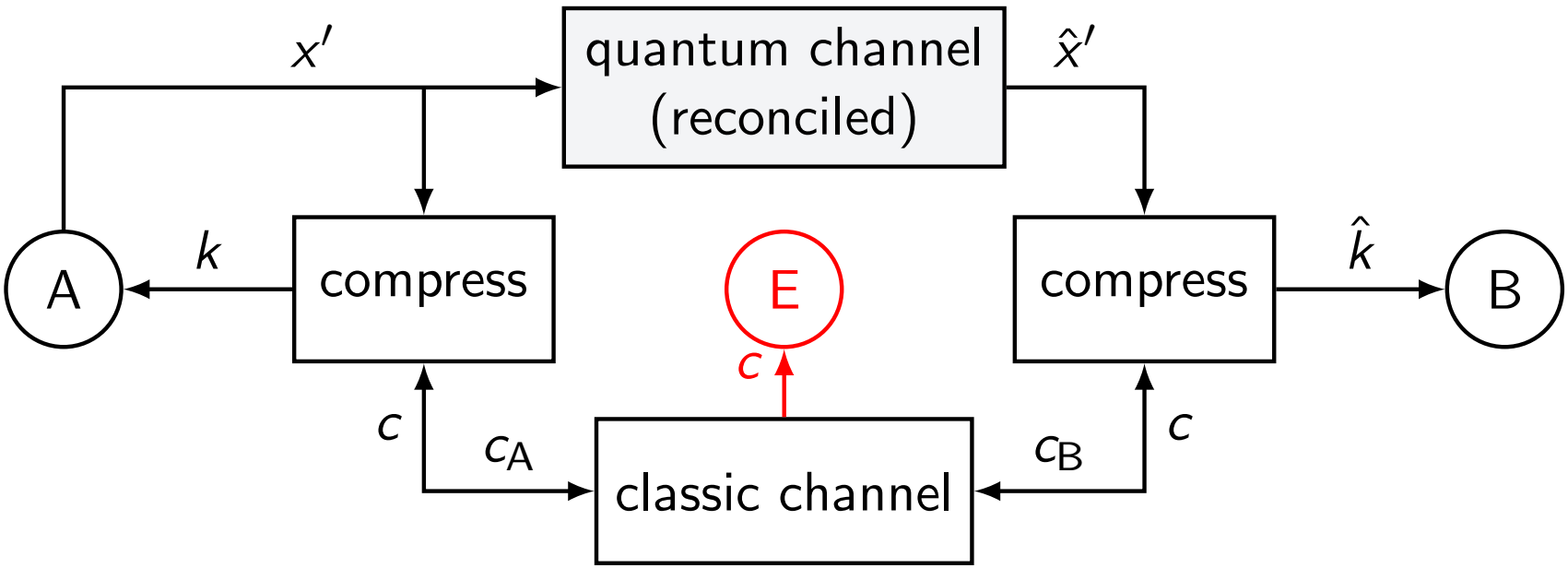
Privacy amplification



Privacy amplification



Privacy amplification



Goals

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

Choosing a compression function

How to choose a compression function?

Choosing a compression function

How to choose a compression function?

- Must be chosen randomly, after transmission

Choosing a compression function

How to choose a compression function?

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

Choosing a compression function

How to choose 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

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

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

Choosing a compression function: known results

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

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

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

Choosing a compression function: known results

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

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

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

Theorem (Point-wise bound [Gilbert *et al.*, '01])

In order to achieve a failure probability $P_{fail} \leq s'$ *and a mutual information* $I(\mathbf{k}; \mathbf{z} = z^*, \mathbf{A}) \leq \frac{2^{-s''}}{\ln 2}$*, the privacy amplification compression factor should be at least* $s = s' + s''$*.*

Choosing a compression function: open problems

Open problems

- Bennett's theorem gives only an *average* bound on the value of $I(\mathbf{k}; \mathbf{z}, \mathbf{A})$ over random choices of $\mathbf{A}$.

Choosing a compression function: open problems

Open problems

- Bennett's theorem gives only an *average* bound on the value of $I(\mathbf{k}; \mathbf{z}, \mathbf{A})$ over random choices of $\mathbf{A}$.
- Gilbert's theorem provides a point-wise bound given a specific observation, but does not ensure anything w.r.t. a specific compression function $\mathbf{A} = \mathbf{a}^*$.

Choosing a compression function: open problems

Open problems

- Bennett's theorem gives only an *average* bound on the value of $I(\mathbf{k}; \mathbf{z}, \mathbf{A})$ over random choices of $\mathbf{A}$.
- Gilbert's theorem provides a point-wise bound given a specific observation, but does not ensure anything w.r.t. a specific compression function $\mathbf{A} = \mathbf{a}^*$.

Idea

Find a tool for establishing a point-wise bound on the mutual information, i.e., $I(\mathbf{k}; \mathbf{z}, \mathbf{A} = \mathbf{a}^*)$.

Choosing a compression function

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

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

Lemma 1

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

Choosing a compression function

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

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

Lemma 1

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

Example: binary Toeplitz matrices

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

Choosing a compression function

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

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

Lemma 1

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

Example: binary Toeplitz matrices

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

Lemma 2

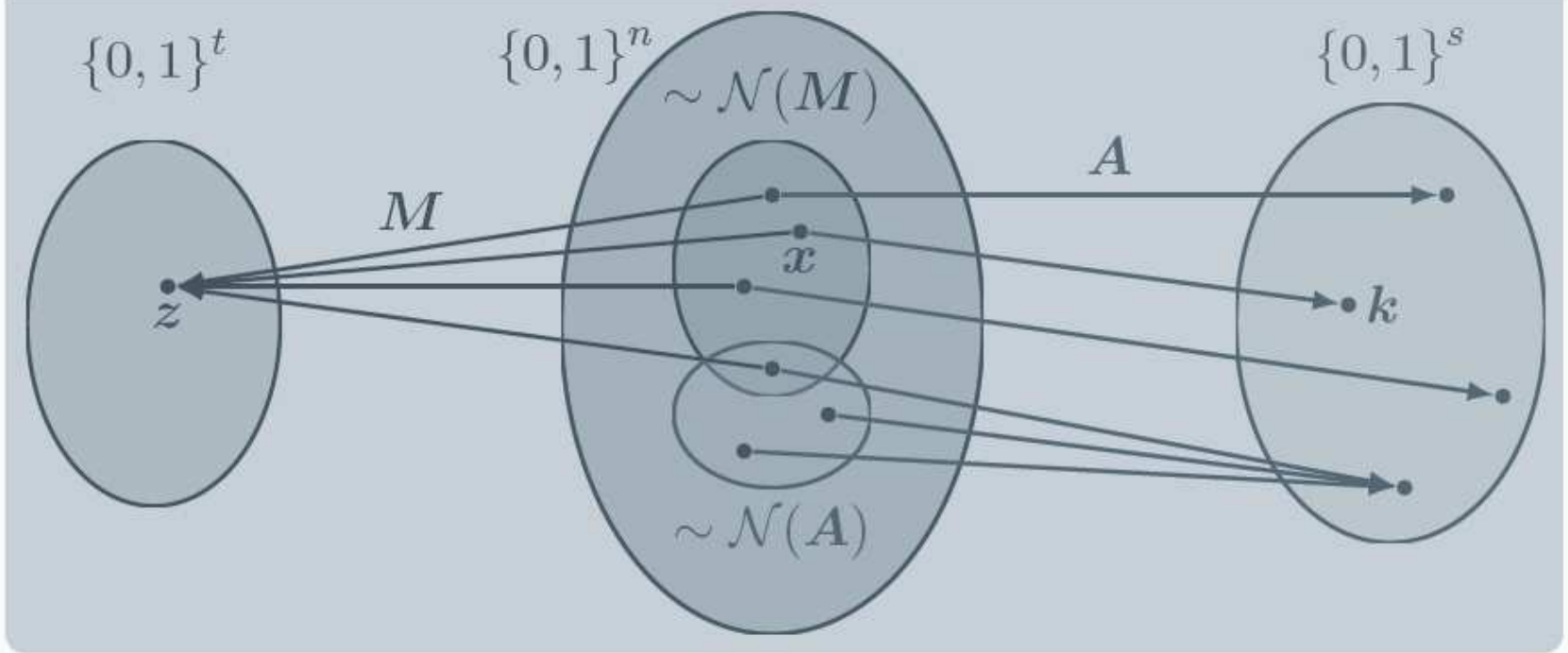
If $\dim \mathcal{N}(\mathbf{M}) - \dim\left(\mathcal{N}(\mathbf{M}) \cap \mathcal{N}(\mathbf{A})\right) = \text{rank}(\mathbf{A})$ and $\mathbf{x}'$ is uniform over $\{0,1\}^n$, then $I(\mathbf{k}; \mathbf{z}) = 0$

Choosing a compression function

Theorem

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

Illustration



Choosing a compression function

Are we done now?

Choosing a compression function

Are we done now?

The previous theorem states a sufficient condition for designing the optimal compression function...

Choosing a compression function

Are we done now?

The previous theorem states a sufficient condition for designing the optimal compression function...

BUT

Choosing a compression function

Are we done now?

The previous theorem states a sufficient condition for designing the optimal compression function...

BUT

... do we perfectly know **M**, that is, the matrix summarizing Eve's information?

Choosing a compression function

The nature of leaked information is twofold:

Choosing a compression function

The nature of leaked information is twofold:

- deterministic and known to the legitimate parties on one hand, due to the disclosure of some bits sent over the public channel

Choosing a compression function

The nature of leaked information is twofold:

- deterministic and known to the legitimate parties on one hand, due to the disclosure of some bits sent over the public channel
  - ✓ it can be optimally counteracted

Choosing a compression function

The nature of leaked information is twofold:

- deterministic and known to the legitimate parties on one hand, due to the disclosure of some bits sent over the public channel

  ✓ it can be optimally counteracted

- random and not known to the legitimate parties on the other hand, due to eavesdropping on the quantum channel

Choosing a compression function

The nature of leaked information is twofold:

- deterministic and known to the legitimate parties on one hand, due to the disclosure of some bits sent over the public channel

  ✓ it can be optimally counteracted

- random and not known to the legitimate parties on the other hand, due to eavesdropping on the quantum channel

  × it is not feasible to perfectly compensate for it!

Choosing a compression function

The nature of leaked information is twofold:

- deterministic and known to the legitimate parties on one hand, due to the disclosure of some bits sent over the public channel

  ✓ it can be optimally counteracted

- random and not known to the legitimate parties on the other hand, due to eavesdropping on the quantum channel

  × it is not feasible to perfectly compensate for it!

Possible solution (future work): assume a specific, though probabilistic attack model (e.g., selective intercept and resend) and bound the mutual information given its statistical description.

Summary

- Achievements
  - extended analysis and optimization of the Winnow protocol
  - deployment of a framework for the design of the optimal privacy-amplification function
- Future works
  - investigation of different techniques for key reconciliation (e.g., LDPC codes)
  - further development of the above framework

Questions

Essential references (I)

- 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, C.G. Peterson.
  Fast, efficient error reconciliation for quantum cryptography.
  Physical Review A, 67(5), 052303.
- D. Elkouss, A. Leverrier, R. Allaume, J. J. Boutros.
  Efficient reconciliation protocol for discrete-variable quantum key distribution.
  ISIT 2009 (pp. 1879-1883).

Essential references (II)

- M. Mondin, M. Delgado, F. Mesiti, F. Daneshgaran.
  Soft-processing for Information Reconciliation in QKD Applications.
  International Journal of Quantum Information (2010).
- W. Traisilanun, K. Sripimanwat, O. Sangaroon.
  Secret key reconciliation using BCH code in quantum key distribution.
  ISCIT 2007 (pp. 1482-1485).

Essential references (III)

- U. Maurer.
  Secret key agreement by public discussion from common information.
  IEEE Transactions on Information Theory, 39(3), 733-742.
- C. H. Bennett, G. Brassard, C. Crepeau, U. Maurer.
  Generalized privacy amplification.
  IEEE Transactions on Information Theory, 41(6), 1915-1923.
- G. Gilbert, M. Hamrick, F.J. Thayer.
  Privacy Amplification in Quantum Key Distribution: Pointwise Bound versus Average Bound.
  `http://arxiv.org/abs/quant-ph/0108013`.