On the Power of Quantum Memory

Ueli Maurer, ETH Zurich

Joint work with Robert König and Renato Renner

paper at: quant-ph/0305154

7th Workshop on Quantum Information Processing (QIP 2004), Waterloo, Jan. 15–19, 2004

Basic questions:

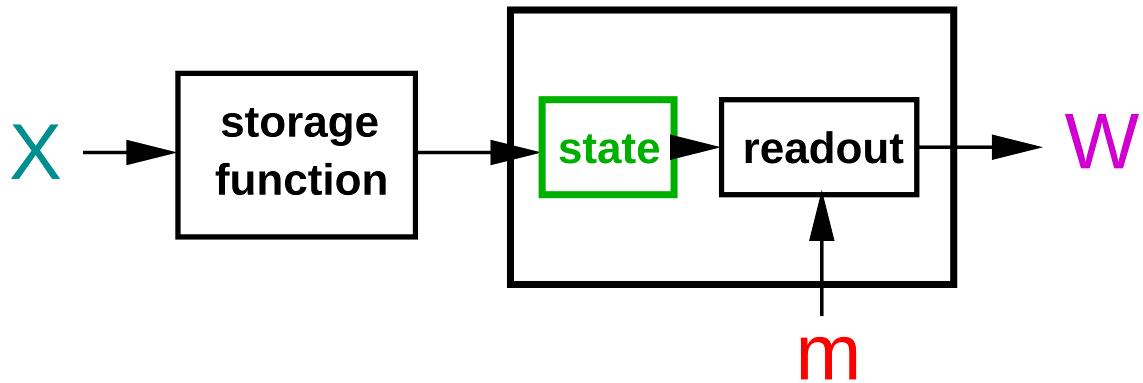
- **How to characterize the power of (quantum) memory?**

Basic questions:

- **How to characterize the power of (quantum) memory?**
- **Are r quantum bits more powerful than r classical bits?**

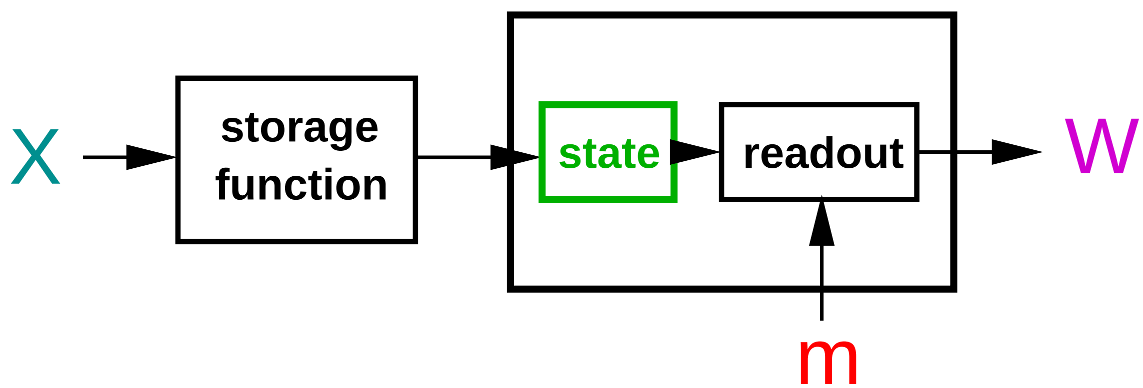
Basic questions:

- How to characterize the power of (quantum) memory?
- Are r quantum bits more powerful than r classical bits?



Basic questions:

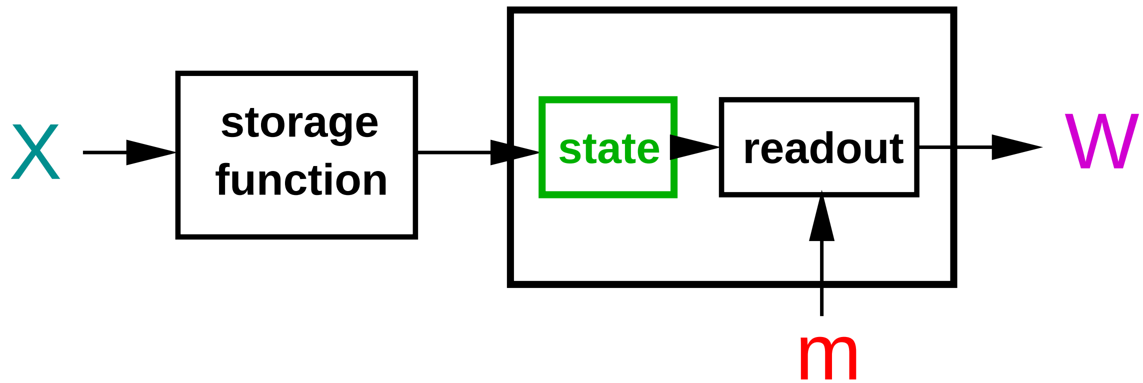
- How to characterize the power of (quantum) memory?
- Are r quantum bits more powerful than r classical bits?



- Is privacy amplification secure against an adversary holding quantum information?

Basic questions:

- How to characterize the power of (quantum) memory?
- Are r quantum bits more powerful than r classical bits?



- Is privacy amplification secure against an adversary holding quantum information?
- Christandel's talk: Implications to quantum cryptography?

Overview

1. **Information-theoretic cryptography**

2. **Characterizing the power of quantum storage**

3. **Privacy amplification is secure against quantum adversaries**

Assumptions in cryptographic security proofs

Assumptions in cryptographic security proofs

Every security proof is relative to certain assumptions !

- **Randomness exists (generation of secret keys)**
- **Independence exists ($\nexists$ telepathy)**

Assumptions in cryptographic security proofs

Every security proof is relative to certain assumptions !

- **Randomness exists (generation of secret keys)**
- **Independence exists ($\nexists$ telepathy)**
- **Computational intractability assumptions**

Assumptions in cryptographic security proofs

Every security proof is relative to certain assumptions !

- **Randomness exists (generation of secret keys)**
- **Independence exists ($\nexists$ telepathy)**
- **Computational intractability assumptions**
- **Correct behavior (trustworthiness) of entities**

Assumptions in cryptographic security proofs

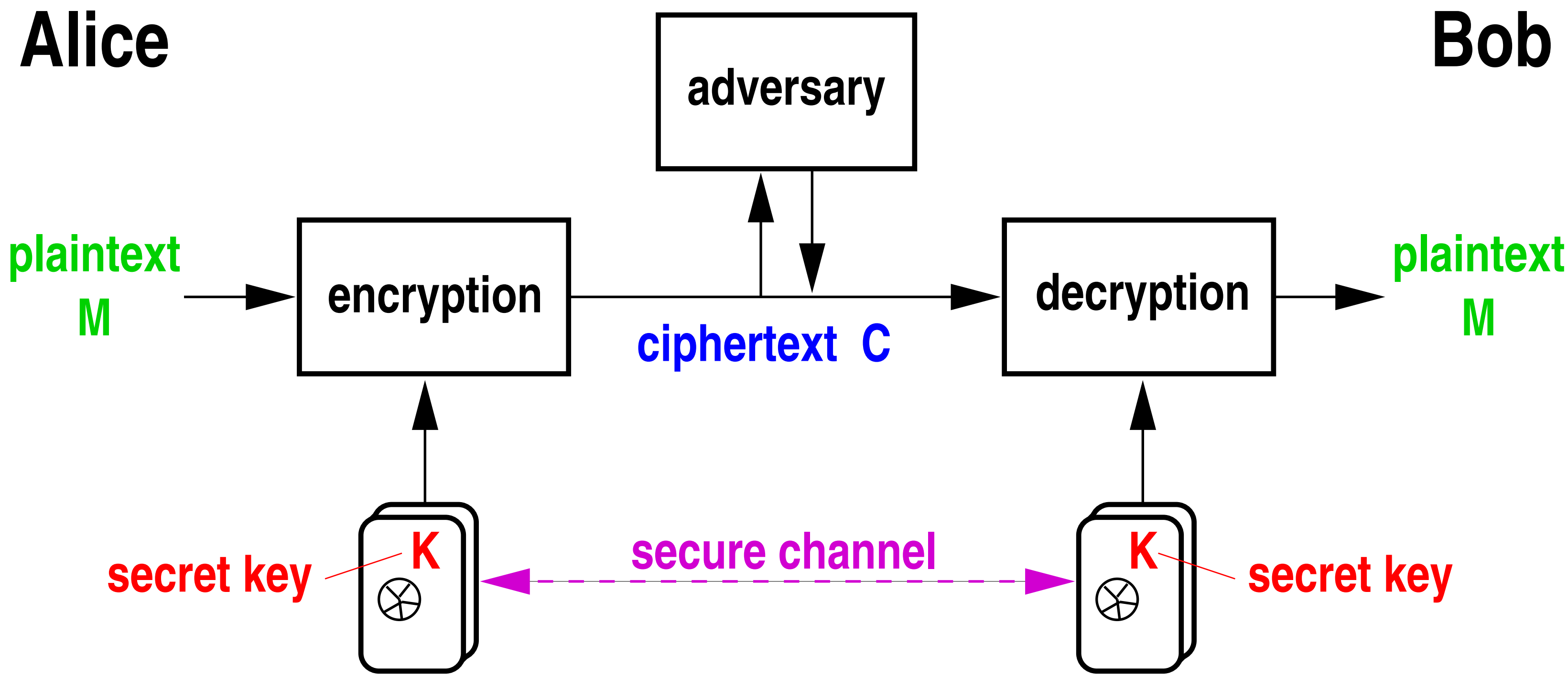
Every security proof is relative to certain assumptions !

- **Randomness exists (generation of secret keys)**
- **Independence exists ($\nexists$ telepathy)**
- **Computational intractability assumptions**
- **Correct behavior (trustworthiness) of entities**
- **Physical assumptions**
  - **Tamper-resistance**
  - **Noise in communication systems**
  - **Restrictions on adversary's memory capacity**
  - **Quantum theory**

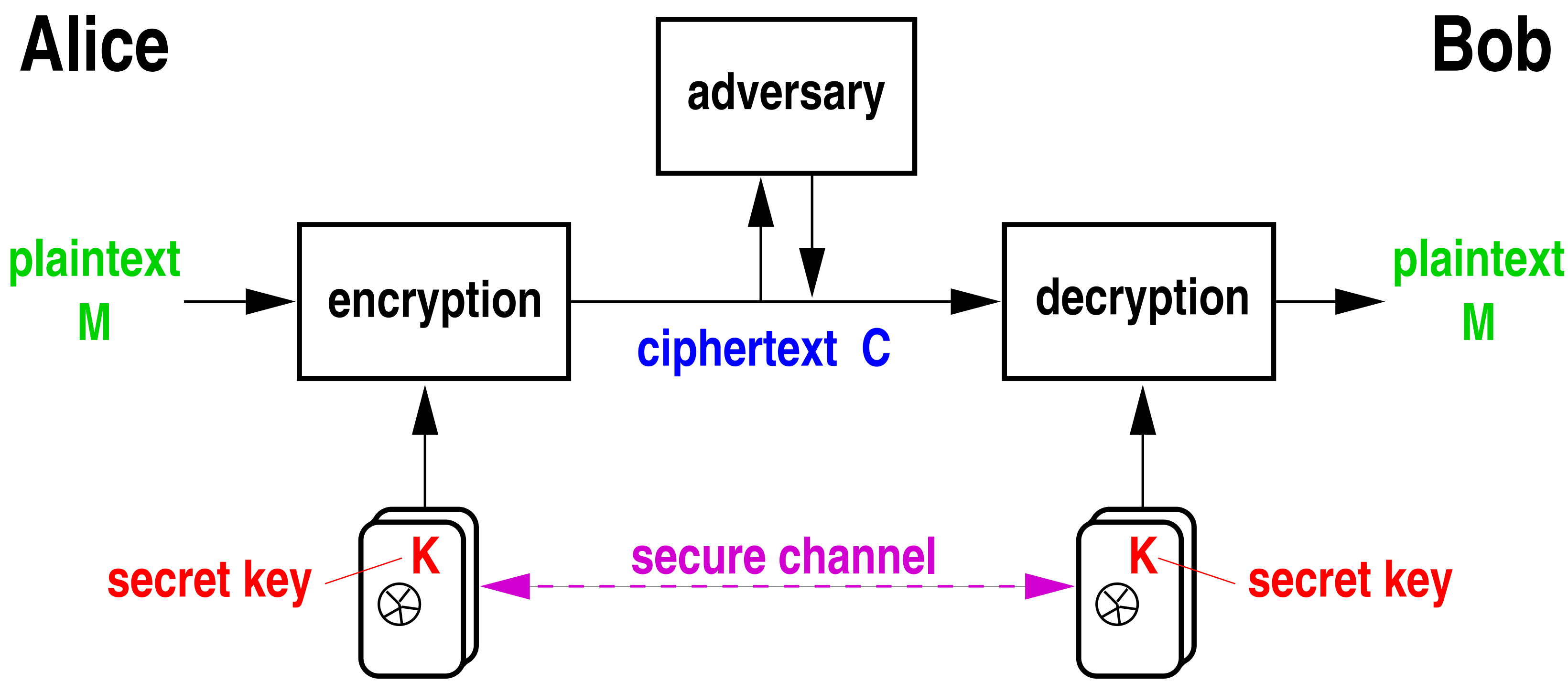
Why cryptography without comp. assumptions

- Which is the right model of computation?
- No lower bound proofs for any useful comput. model.
- Clean security definitions.
- Physical assumptions are more sound than comp. ass.

Symmetric cryptosystem

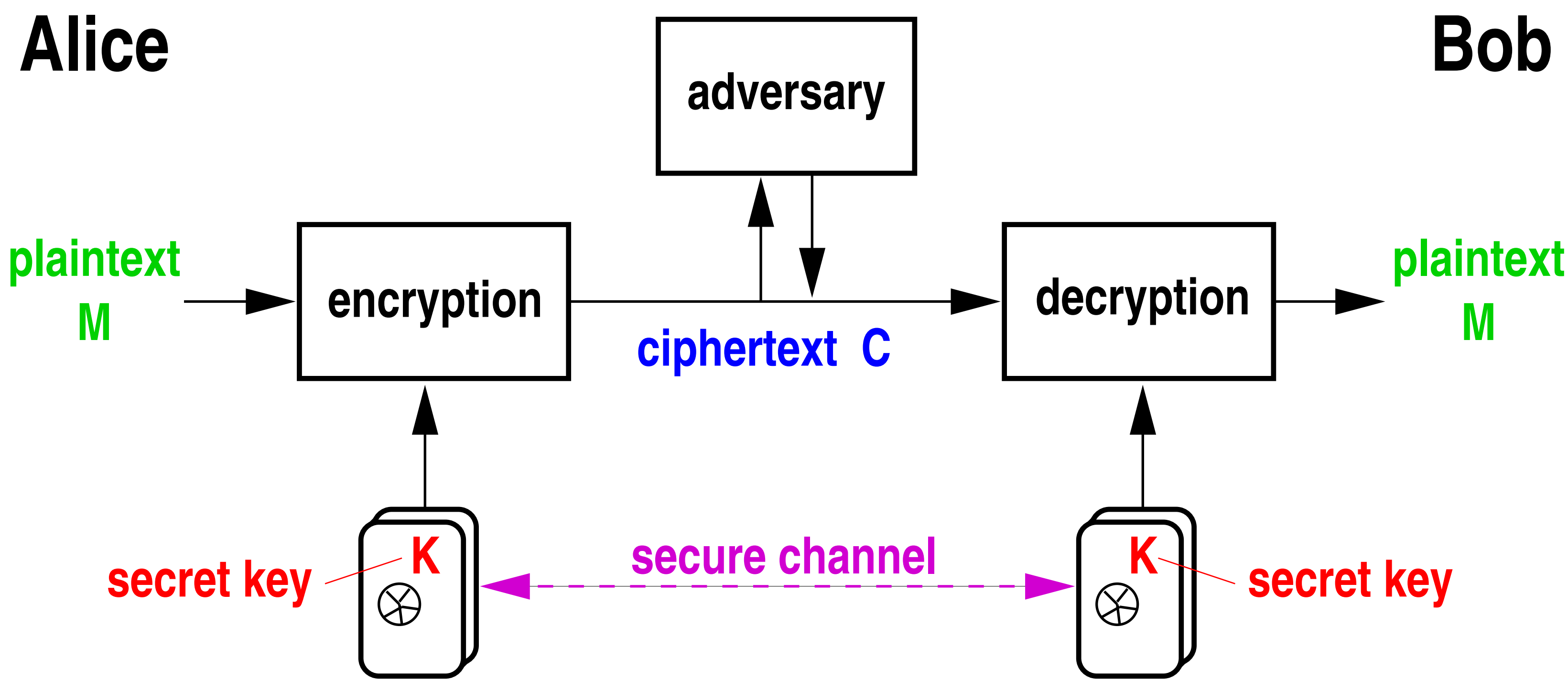


Symmetric cryptosystem



Definition: A cryptosystem is perfect if $I(M;C) = 0$.

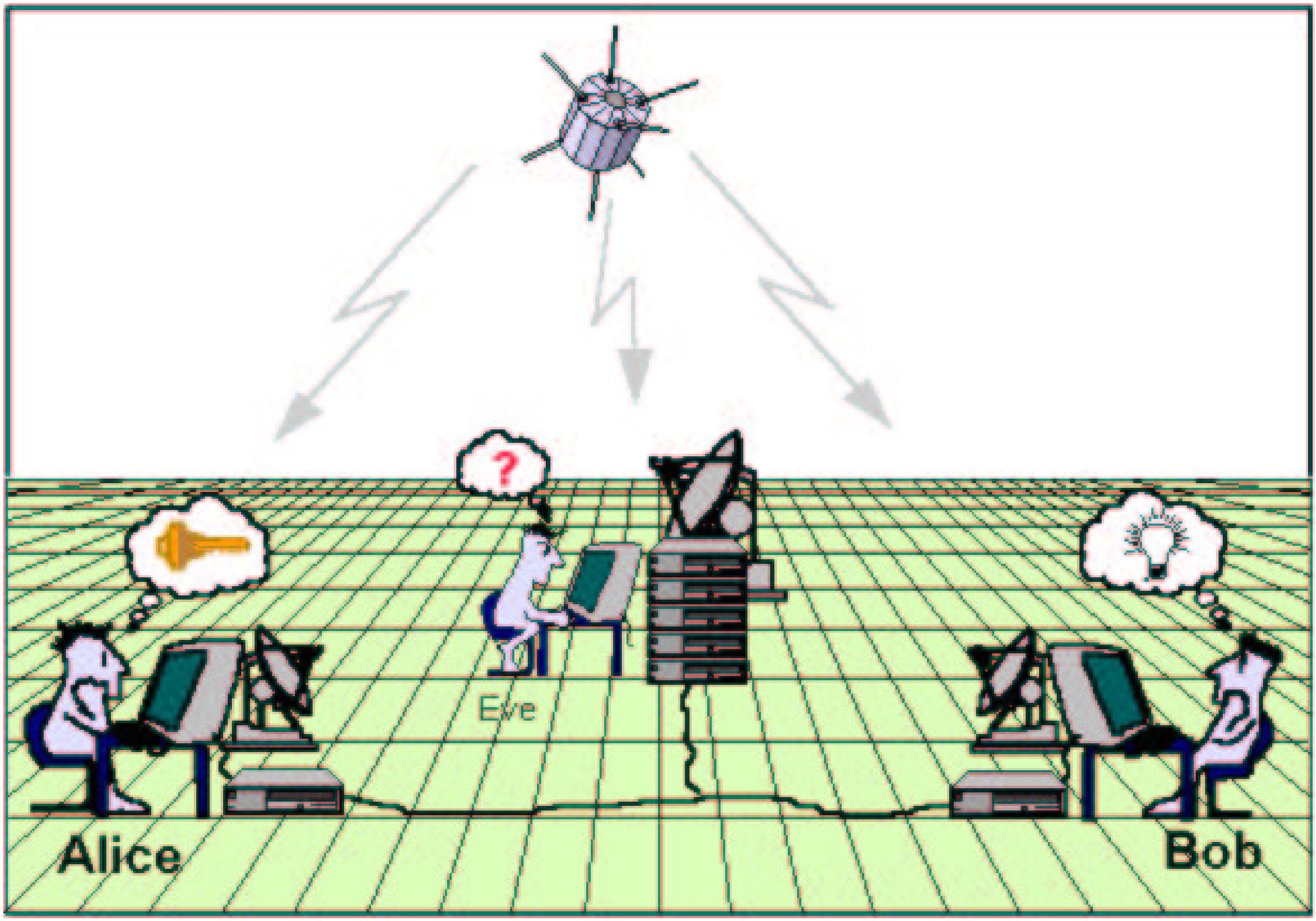
Symmetric cryptosystem

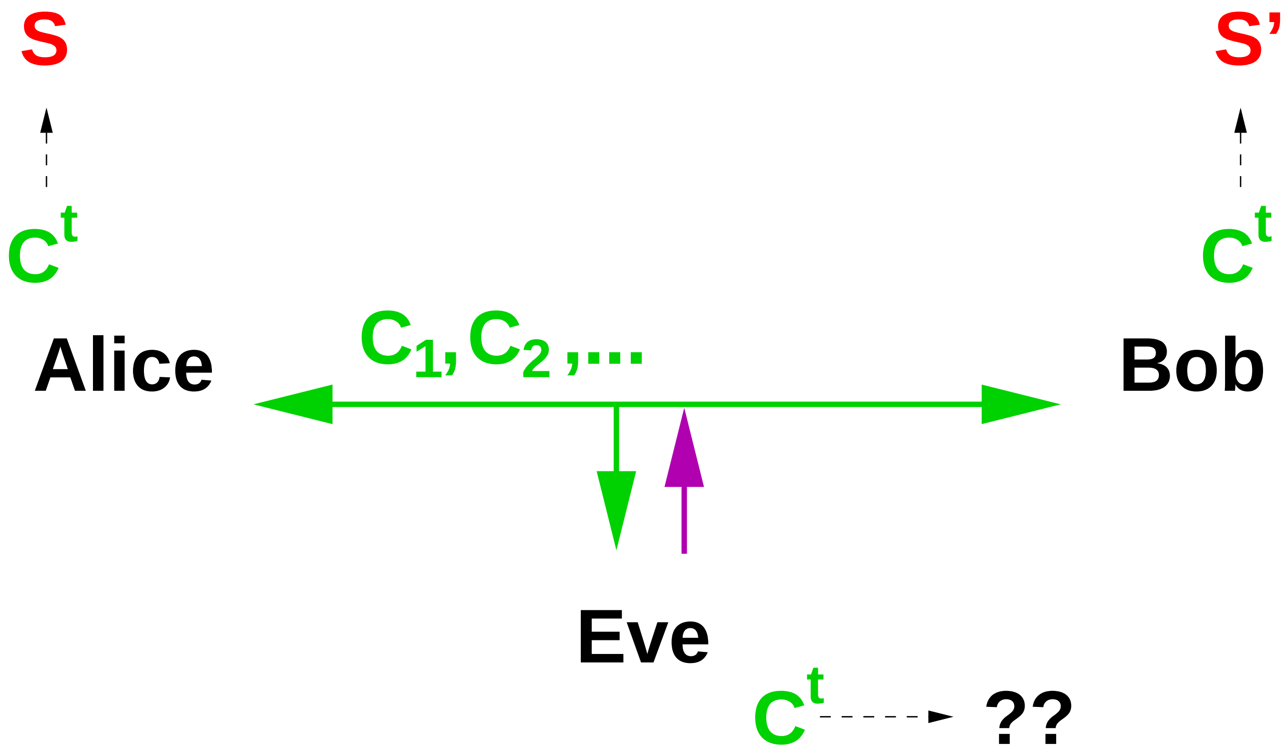


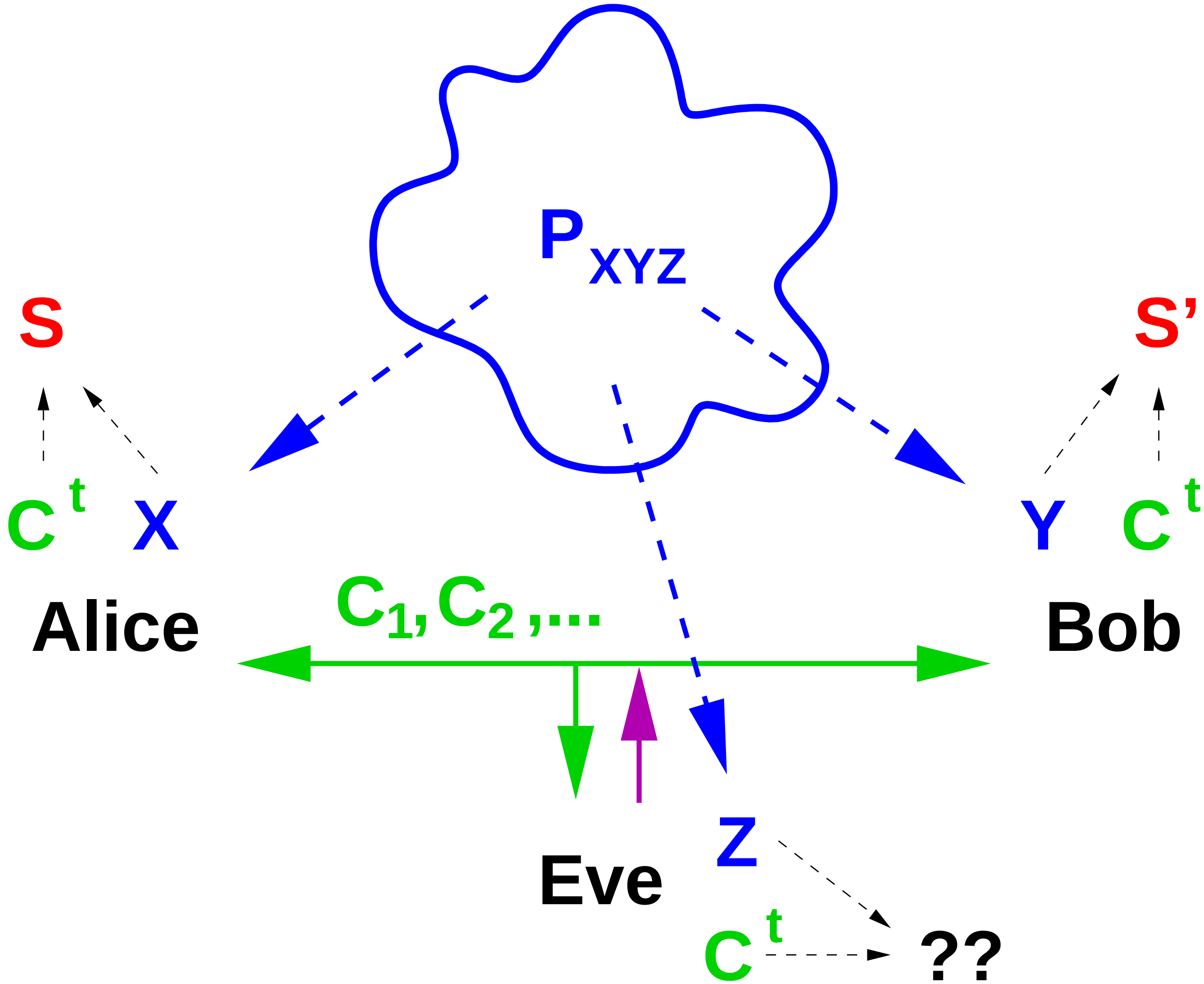
Definition: A cryptosystem is perfect if $I(M;C) = 0$.

Theorem [Sha49]: For every perfect cipher, $H(K) \geq H(M)$.

Information-theoretic key agreement by public discussion [M93]




S
S'
C^t
C^t
C1, C2 ,...
Alice
Bob
Eve
C^t
??



P_{XYZ}
S
S'
C^t
X
Y
C^t
Alice
$C_1, C_2, \dots$
Bob
Z
Eve
C^t
??

Theorem [M93]: $H(S) \leq \min [\, I(X;Y), I(X;Y|Z) \,]$.

Theorem [M93]: $H(S) \leq \min [\, I(X;Y), I(X;Y|Z) \,]$.

Corollary: $H(K) \geq H(M)$ **holds also in an interactive setting.**

Theorem [M93]: $H(S) \leq \min [I(X;Y), I(X;Y|Z)]$.

Corollary: $H(K) \geq H(M)$ **holds also in an interactive setting.**

Corollary: A public-key cryptosystem cannot be i.-t. secure.

Theorem [M93]: H(S) $\leq$ min [I(X;Y), I(X;Y|Z)] .

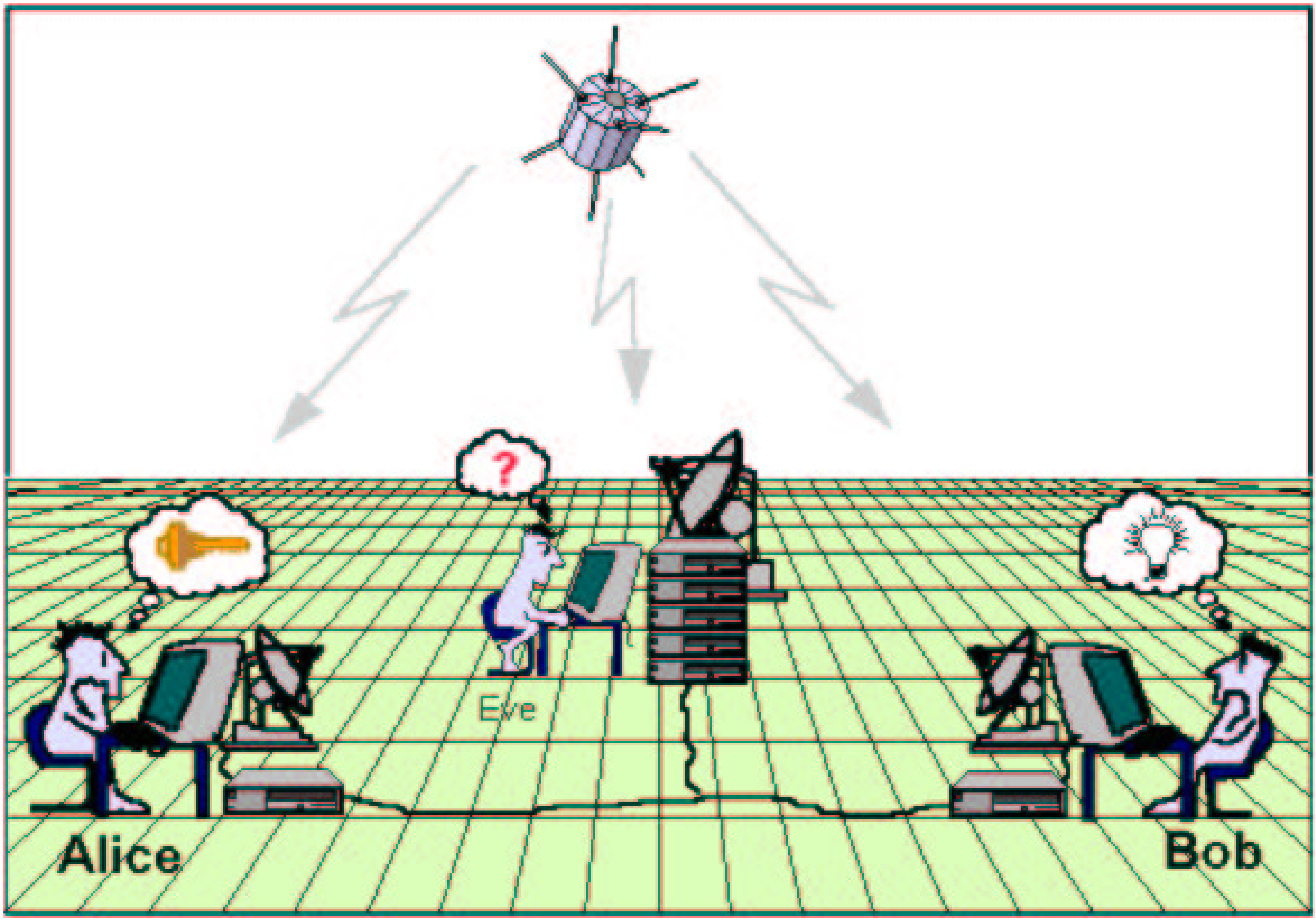
Corollary: H(K) $\geq$ H(M) holds also in an interactive setting.

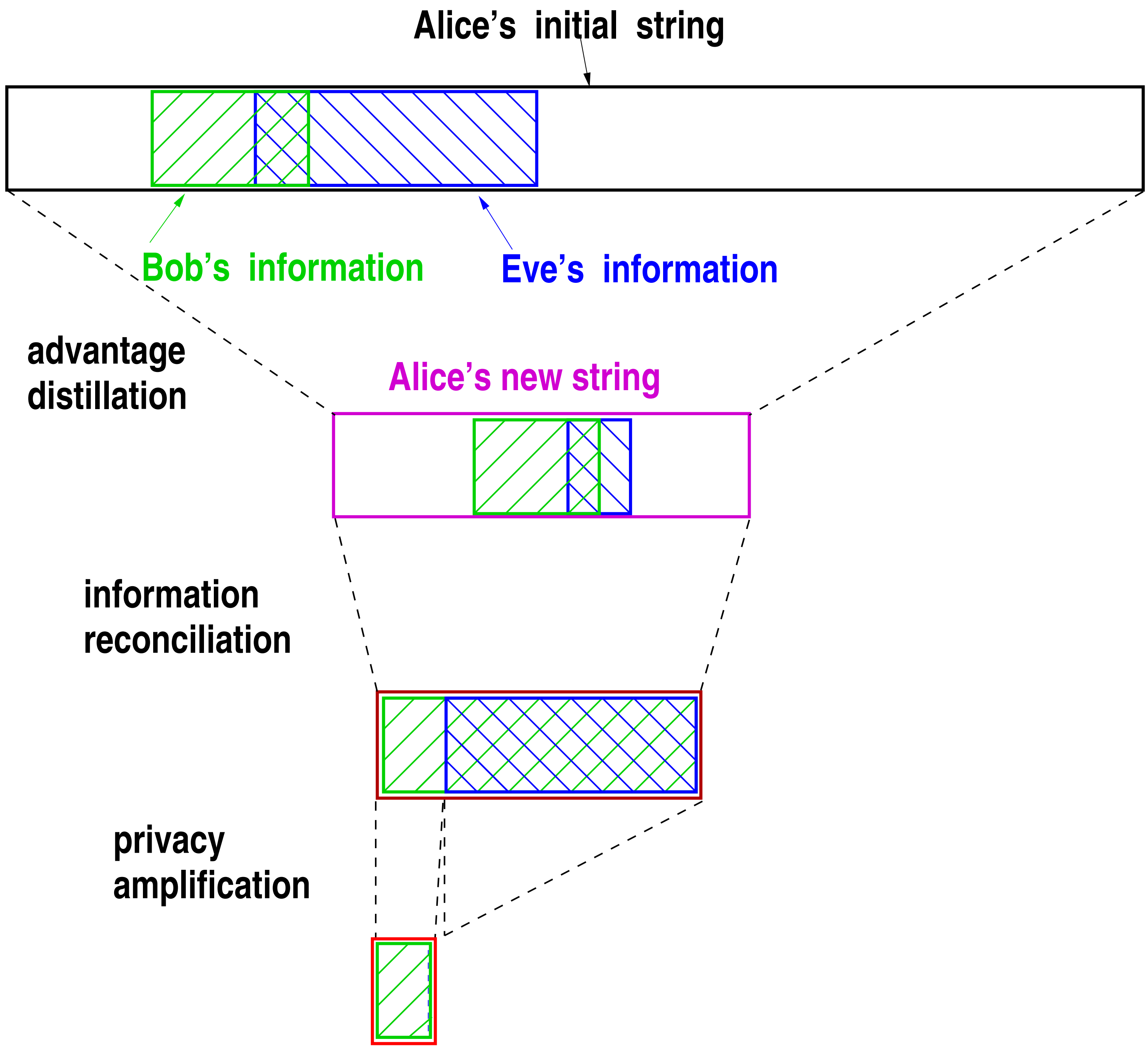
Corollary: A public-key cryptosystem cannot be i.-t. secure.

Theorem: In the satellite model, H(S) $>$ 0 is possible whenever it is not obviously impossible, i.e., if

- Eve's channel is not perfectly noiseless and
- Alice's and Bob's channels have positive capacity.

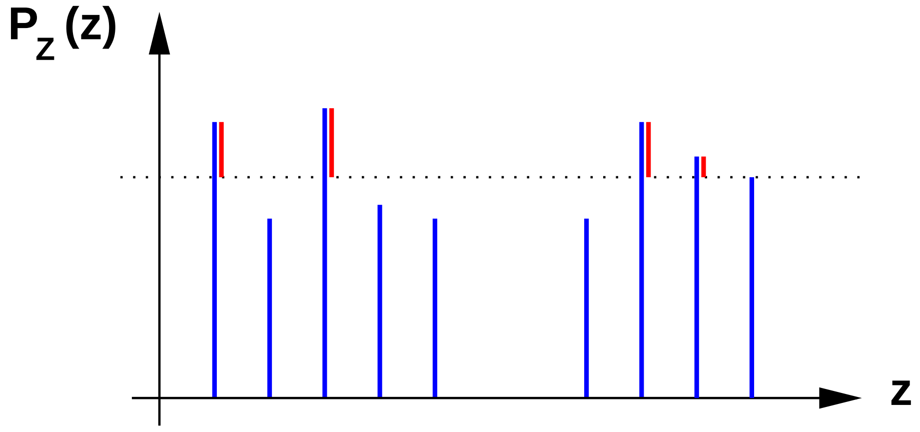
Information-theoretic key agreement by public discussion





Alice's initial string
Bob's information
Eve's information
advantage distillation
Alice's new string
information reconciliation
privacy amplification

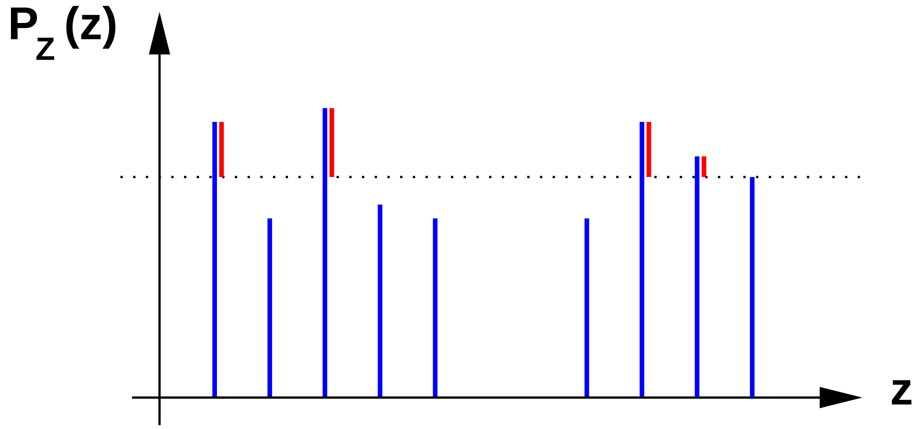
Distance from uniformity



$$\mathbf{d}(\mathbf{Z}) := \frac{1}{2}\sum_{z\in\mathcal{Z}}\left|P_{\mathbf{Z}}(z) - \frac{1}{|\mathcal{Z}|}\right|$$

(= sum of red quantities)

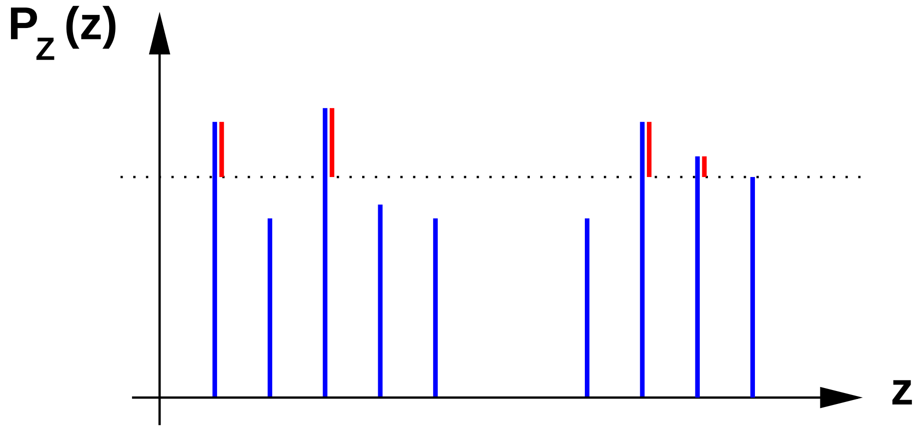
Distance from uniformity



$$\mathbf{d}(Z) := \frac{1}{2}\sum_{z\in\mathcal{Z}}\left|P_Z(z) - \frac{1}{|\mathcal{Z}|}\right|$$ **(= sum of red quantities)**

$$\mathbf{d}(Z|W) := E_W\left[\mathbf{d}(P_{Z|W}(\cdot|W))\right]$$

Distance from uniformity



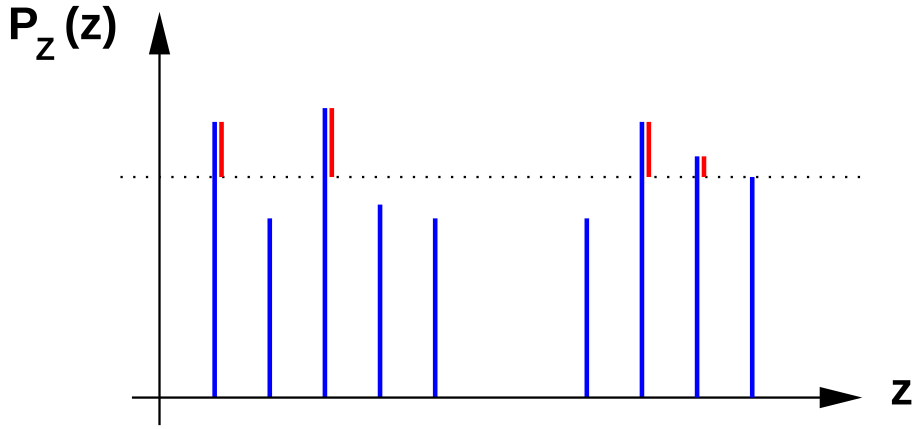
$$\mathbf{d}(\mathbf{Z}) := \frac{1}{2} \sum_{z \in \mathcal{Z}} \left| P_{\mathbf{Z}}(z) - \frac{1}{|\mathcal{Z}|} \right|$$

(= sum of red quantities)

$$\mathbf{d}(\mathbf{Z}|\mathbf{W}) := E_{\mathbf{W}} \left[\mathbf{d}(P_{\mathbf{Z}|\mathbf{W}}(\cdot|\mathbf{W})) \right]$$

Lemma: One can define a uniform random variable Z that is independent of W and such that $\mathbf{Z} = \mathbf{Z}$ holds with probability $1 - \mathbf{d}(\mathbf{Z}|\mathbf{W})$.

Distance from uniformity



$$\mathbf{d}(Z) := \frac{1}{2} \sum_{z \in \mathcal{Z}} \left| P_Z(z) - \frac{1}{|\mathcal{Z}|} \right|$$

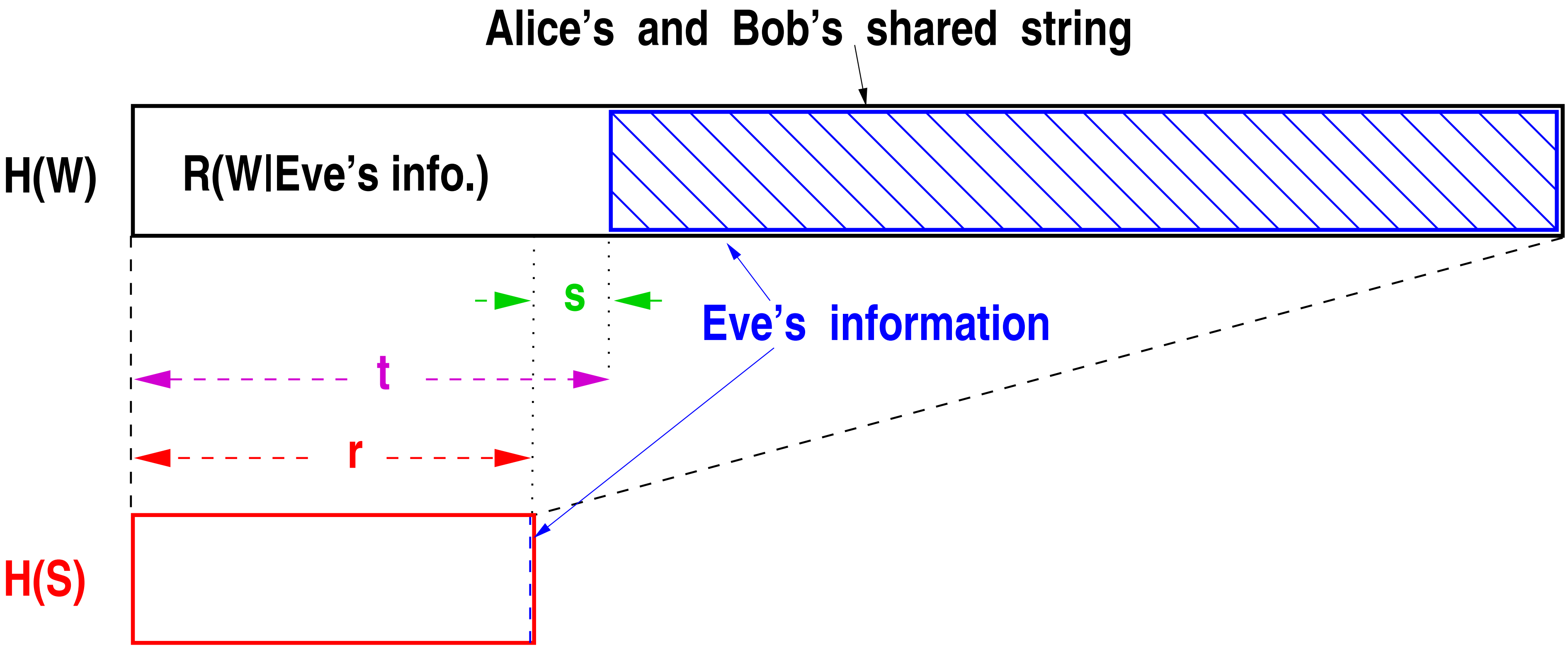
(= sum of red quantities)

$$\mathbf{d}(Z|W) := E_W \left[\mathbf{d}(P_{Z|W}(\cdot|W)) \right]$$

Lemma: One can define a uniform random variable Z that is independent of W and such that Z $=$ Z holds with probability $1 -$ d$(Z|W)$.

In other words, with probability $1 -$ d$(Z|W)$ the setting with W and Z is equivalent to an ideal setting with W and independent uniform Z.

Privacy amplification



Privacy amplification by universal hashing [BBR86,BBCM95]

Definition: **An $(\mathcal{X}, \mathcal{Y})$-random function G is a random variable taking as values functions $\mathcal{X} \to \mathcal{Y}$.**

Privacy amplification by universal hashing [BBR86,BBCM95]

Definition: **An $(\mathcal{X}, \mathcal{Y})$-random function G is a random variable taking as values functions $\mathcal{X} \to \mathcal{Y}$.**

G is called 2-universal if for any distinct $x, x' \in \mathcal{X}$, $\quad P\left(\mathbf{G}(x) = \mathbf{G}(x')\right) \le \frac{1}{|\mathcal{Y}|}$.

Privacy amplification by universal hashing [BBR86,BBCM95]

Definition: **An** $(\mathcal{X},\mathcal{Y})$**-random function G is a random variable taking as values functions** $\mathcal{X} \to \mathcal{Y}$**.**

G is called 2-universal if for any distinct $x, x' \in \mathcal{X}$**,** $\quad P\left(\mathbf{G}(x) = \mathbf{G}(x')\right) \leq \frac{1}{|\mathcal{Y}|}$.

Theorem: **Let X and W be arbitrary random variable with** $H_2(\mathbf{X}|\mathbf{W}) \geq t$ **and let G be a 2-universal random function from** $\mathcal{X}$ **to** $\{0,1\}^s$**. Then**

$$\mathbf{d}(\mathbf{G}(\mathbf{X})|\mathbf{WG}) \;\geq\; O(2^{-\frac{1}{2}(t-s)}).$$

Privacy amplification by universal hashing [BBR86,BBCM95]

Definition: **An $(\mathcal{X},\mathcal{Y})$-random function G is a random variable taking as values functions $\mathcal{X} \to \mathcal{Y}$.**

G is called 2-universal if for any distinct $x, x' \in \mathcal{X}$, $\quad P\left(\mathbf{G}(x) = \mathbf{G}(x')\right) \le \frac{1}{|\mathcal{Y}|}$.

Theorem: **Let X and W be arbitrary random variable with $H_2(\mathbf{X}|\mathbf{W}) \ge t$ and let G be a 2-universal random function from $\mathcal{X}$ to $\{0,1\}^s$. Then**

$$\mathbf{d}(\mathbf{G}(\mathbf{X})|\mathbf{WG}) \;\ge\; O(2^{-\frac{1}{2}(t-s)}).$$

Corollary: **If X is uniform over $\{0,1\}^n$ and W consists of r arbitrary (classical) bits about X, then**

$$\mathbf{d}(\mathbf{G}(\mathbf{X})|\mathbf{WG}) \;=\; O(2^{-\frac{1}{2}(n-r-s)}).$$

Privacy amplification by universal hashing [BBR86,BBCM95]

Definition: **An $(\mathcal{X},\mathcal{Y})$-random function G is a random variable taking as values functions $\mathcal{X} \to \mathcal{Y}$.**

G is called 2-universal if for any distinct $x, x' \in \mathcal{X}$, $\quad P(\mathbf{G}(x) = \mathbf{G}(x')) \leq \frac{1}{|\mathcal{Y}|}$.

Theorem: **Let X and W be arbitrary random variable with $H_2(\mathbf{X}|\mathbf{W}) \geq t$ and let G be a 2-universal random function from $\mathcal{X}$ to $\{0,1\}^s$. Then**

$$\mathbf{d}(\mathbf{G}(\mathbf{X})|\mathbf{WG}) \;\geq\; O(2^{-\frac{1}{2}(t-s)}).$$

Corollary: **If X is uniform over $\{0,1\}^n$ and W consists of r arbitrary (classical) bits about X, then**

$$\mathbf{d}(\mathbf{G}(\mathbf{X})|\mathbf{WG}) \;=\; O(2^{-\frac{1}{2}(n-r-s)}).$$

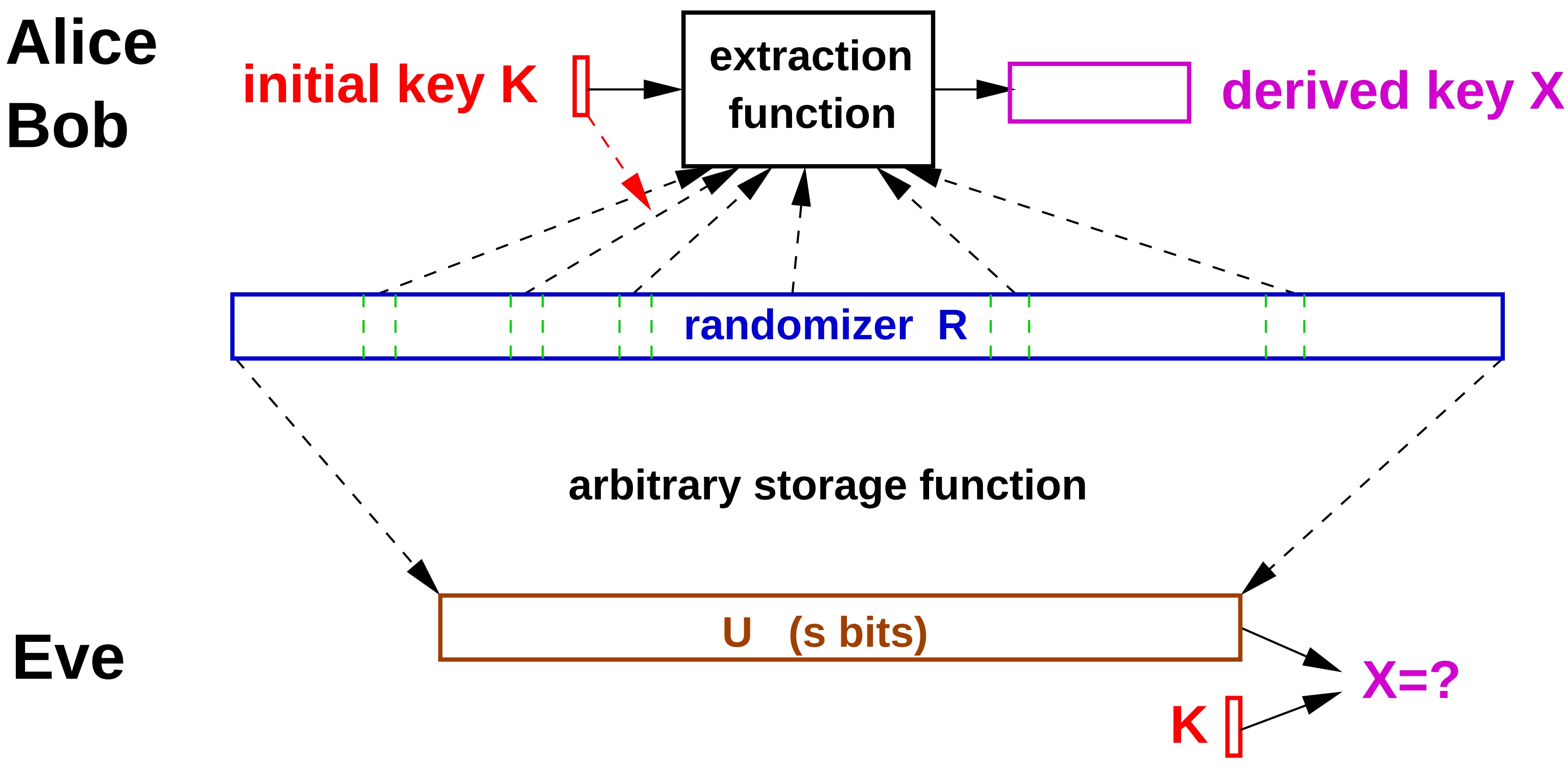
Question: What about quantum knowledge about X?

The bounded-storage model (BSM) [M90]

Basic idea: Eve has bounded storage capacity of s bits, but otherwise unlimited computing power.

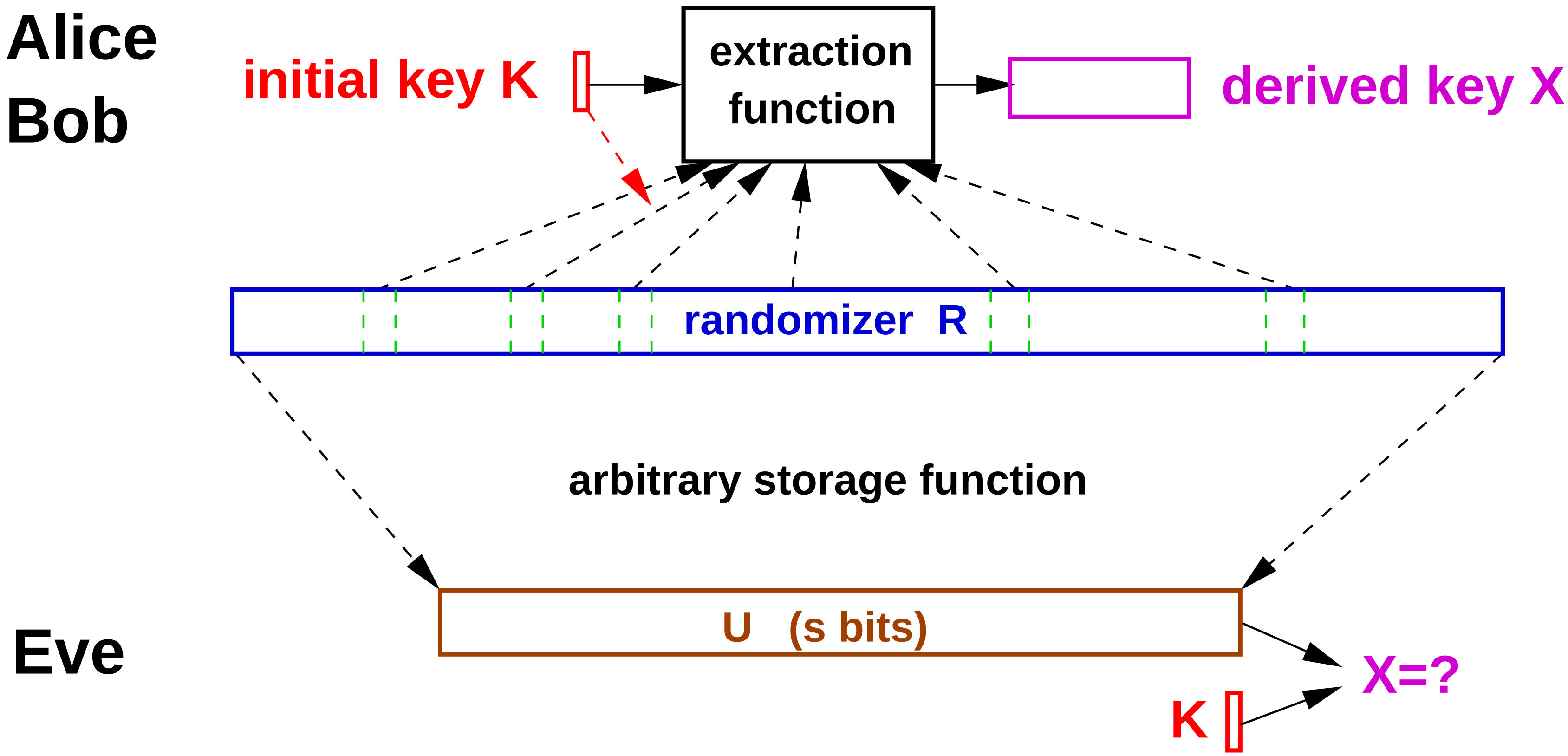
The bounded-storage model (BSM) [M90]

Basic idea: Eve has bounded storage capacity of s bits, but otherwise ~~unlimited computing power~~.

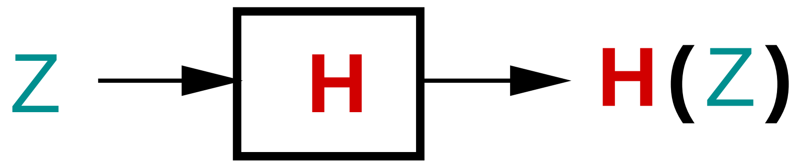


The bounded-storage model (BSM) [M90]

Basic idea: Eve has bounded storage capacity of s bits, but otherwise ~~unlimited computing power~~.

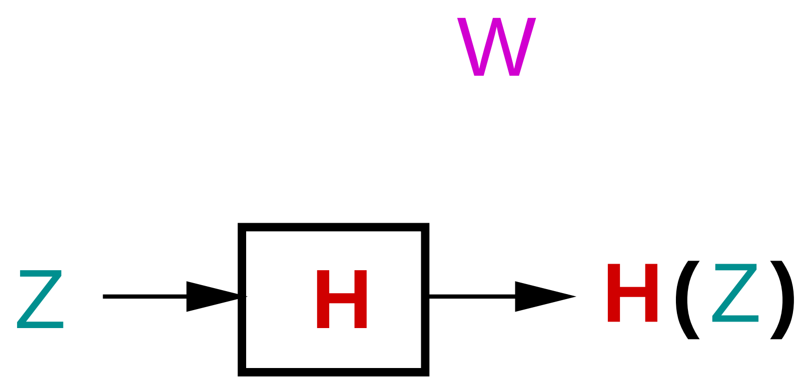


Question: What about quantum storage?



Lemma: **Consider any random variable Z over $\mathcal{Z}$. If H is a uniform balanced Boolean random function, then**

$$\mathbf{d}(\mathbf{Z}) \leq \frac{3}{2}\sqrt{|\mathcal{Z}|}\ \mathbf{d}(\mathbf{H}(\mathbf{Z})|\mathbf{H}).$$

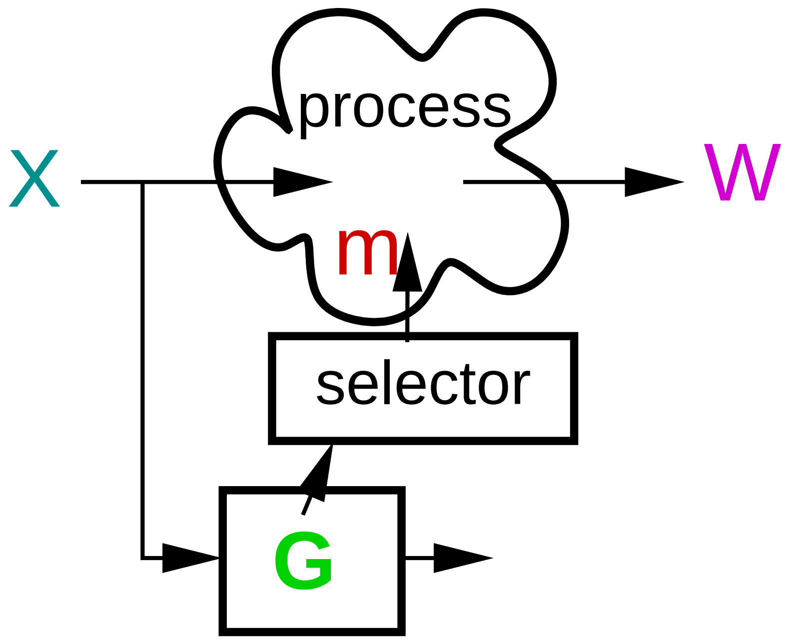


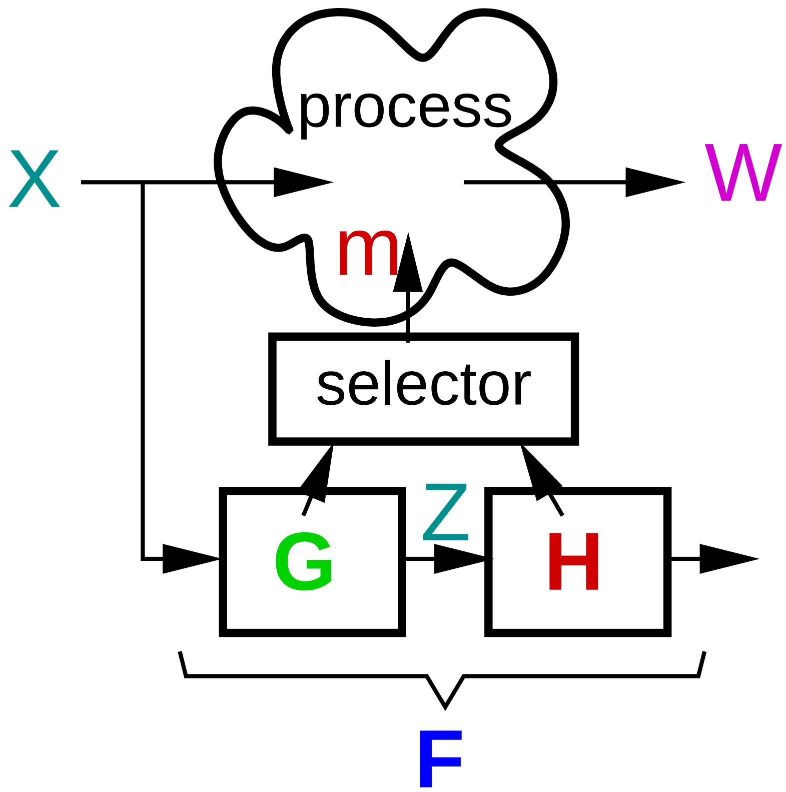
Lemma: **Consider any random variable Z over $\mathcal{Z}$. If H is a uniform balanced Boolean random function, then**

$$\mathbf{d}(\mathbf{Z}) \leq \frac{3}{2}\sqrt{|\mathcal{Z}|}\ \mathbf{d}(\mathbf{H}(\mathbf{Z})|\mathbf{H}).$$

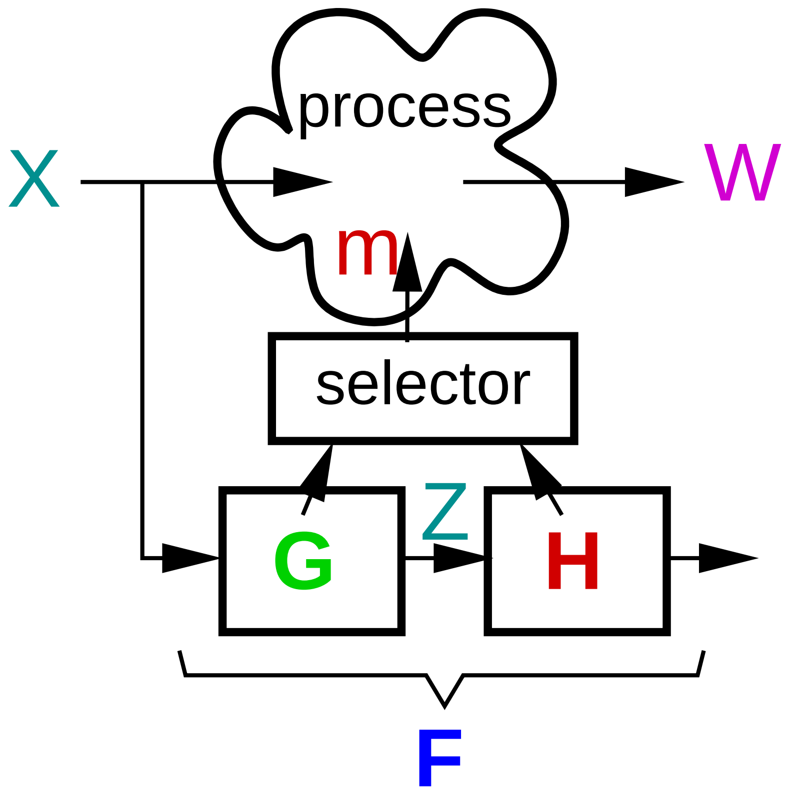
More generally,

$$\mathbf{d}(\mathbf{Z}|\mathbf{W}) \leq \frac{3}{2}\sqrt{|\mathcal{Z}|}\ \mathbf{d}(\mathbf{H}(\mathbf{Z})|\mathbf{W}\mathbf{H}).$$


process
X
W
m
selector
G



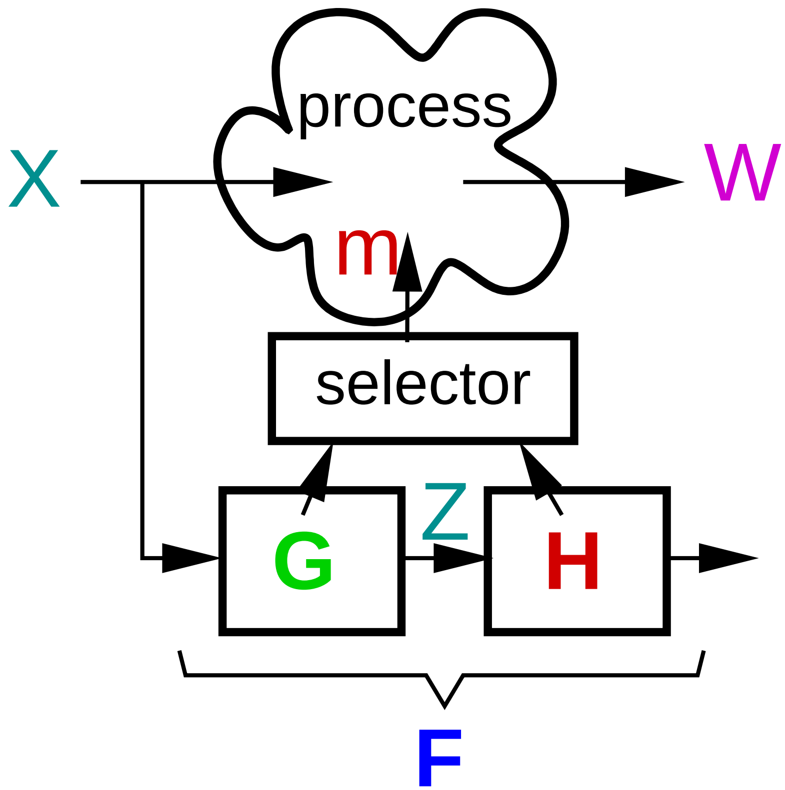
Lemma: If G is 2-universal and H is a uniform balanced Boolean function, then $F = H \circ G$ is a 2-universal Boolean function.



Lemma: If G is 2-universal and H is a uniform balanced Boolean function, then $\mathbf{F} = \mathbf{H} \circ \mathbf{G}$ is a 2-universal Boolean function.

Corollary: Consider any process generating W from a random variable X and a selection input m. If for any 2-universal $(\mathcal{X}, \{0,1\})$-random function F and for any selector with input F we have

$$\mathbf{d}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) \leq \epsilon,$$



Lemma: If **G** is 2-universal and **H** is a **uniform balanced Boolean function**, then $\mathbf{F} = \mathbf{H} \circ \mathbf{G}$ is a 2-universal Boolean function.

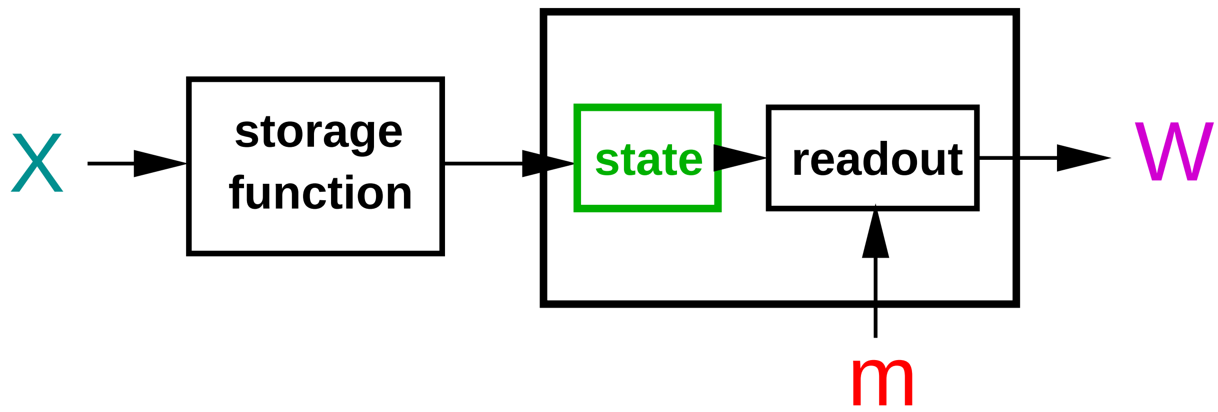
Corollary: Consider any process generating **W** from a random variable **X** and a selection input **m**. If for any 2-universal $(\mathcal{X}, \{0,1\})$-random function **F** and for any selector with input **F** we have

$$\mathbf{d}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) \leq \epsilon,$$

then for any 2-universal $(\mathcal{X}, \{0,1\}^s)$-random function **G** and for any selector with input **G**

$$\mathbf{d}(\mathbf{G}(\mathbf{X})|\mathbf{WG}) \leq \frac{3}{2} 2^{s/2} \epsilon.$$

r-qubit quantum storage device



State: **Normalized vector ψ in the d-dimensional Hilbert space $\mathcal{H}_d$ ($d = 2^r$).**

Equivalently, state space = $\mathcal{P}(\mathcal{H}_d) := \{P_\psi : \psi \in \mathcal{H}_d, \|\psi\| = 1\}$ (pure states), where P_ψ is the projection operator in $\mathcal{H}_d$ along the vector ψ.

Most general read-out operation: m $\in$ POVM$(\mathcal{H}_d)$, resulting in W.

m is specified by a family $\{E_w\}$ of nonneg. op. on $\mathcal{H}_d$ with $\sum_w E_w =$ id$_{\mathcal{H}_d}$.

System in state $P_\psi \;\Rightarrow\; P_{\mathbf{W}}(w) =$ tr$(E_w P_\psi)$.

The quantum binary decision problem

Given: A QS prepared in one of two mixed states $\rho_0, \rho_1 \in \mathcal{S}(\mathcal{H})$,
with a priori probabilities q and $1-q$, respectively.

QBDP: Decide which of the two is the case.

The quantum binary decision problem

Given: A QS prepared in one of two mixed states $\rho_0, \rho_1 \in \mathcal{S}(\mathcal{H})$**,**
with a priori probabilities q **and** $1-q$**, respectively.**

QBDP: Decide which of the two is the case.

General decision strategy: POVM $\{E_0, E_1\}$

$$\mathrm{Prob}[\mathbf{W} = i | \rho = \rho_j] = \mathbf{tr}(E_i \rho_j), \quad \textbf{for } i, j \in \{0, 1\}.$$

Success probability: $q\,\mathbf{tr}(E_0\rho_0) + (1-q)\,\mathbf{tr}(E_1\rho_1)$.

The quantum binary decision problem

Given: A QS prepared in one of two mixed states $\rho_0, \rho_1 \in \mathcal{S}(\mathcal{H})$**,**
with a priori probabilities q **and** $1-q$**, respectively.**

QBDP: Decide which of the two is the case.

General decision strategy: POVM $\{E_0, E_1\}$

$$\mathrm{Prob}[\mathbf{W} = i|\rho = \rho_j] = \mathbf{tr}(E_i\rho_j), \quad \textbf{for } i,j \in \{0,1\}.$$

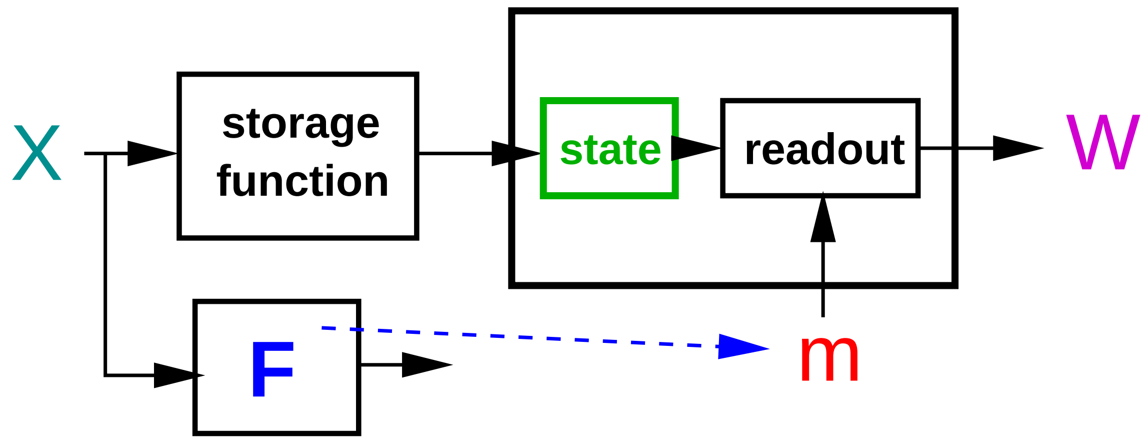
Success probability: $q\,\mathbf{tr}(E_0\rho_0) + (1-q)\,\mathbf{tr}(E_1\rho_1)$.

Theorem [Hel76]**: The maximum achievable success probability is**

$$\tfrac{1}{2} + \tfrac{1}{2}\textstyle\sum_{j=1}^{d} |\mu_j| \ ,$$

where $\{\mu_j\}_{j=1}^{d}$ **are the eigenvalues of the hermitian operator**

$$\Gamma := q\,\rho_0 - (1-q)\,\rho_1.$$



Lemma: **Let**

- **X** = **random variable with range $\mathcal{X}$, stored in an r-qubit quantum system using storage function $\varphi : x \mapsto P_{\psi_x}$.**
- **F** = **any Boolean random function on $\mathcal{X}$.**
- **W** = **measurement outcome of any measurement on the state, depending on F.**

Then

$$\mathbf{d}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) \leq \frac{1}{2} E_{\mathbf{F}}\Big[\sum_{j=1}^{d} |\mu_j^{\mathbf{F}}| \Big] ,$$

where for every f, $\{\mu_j^f\}_{j=1}^d$ are the eigenvalues of the hermitian operator

$$\Lambda_f := \sum_{x:f(x)=0} P_{\mathbf{X}}(x) P_{\psi_x} - \sum_{x:f(x)=1} P_{\mathbf{X}}(x) P_{\psi_x}$$

Let

$$\lambda_{x,x'} \;:=\; 2\,\mathrm{Prob}[\mathbf{F}(x) = \mathbf{F}(x')] - 1 \;=\; E_{\mathbf{F}}[\delta_{f(x),f(x')} - 1]$$

Note: For 2-universal F, $\lambda_{x,x'} \leq 0$ **for** $x \neq x'$**.**

Let

$$\lambda_{x,x'} \;:=\; 2\,\mathrm{Prob}[\mathbf{F}(x) = \mathbf{F}(x')] - 1 \;=\; E_{\mathbf{F}}[\delta_{f(x),f(x')} - 1]$$

Note: For 2-universal F, $\lambda_{x,x'} \leq 0$ **for** $x \neq x'$**.**

Theorem: Let X, F, and W be as above. Then

$$\mathbf{d}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) \;\leq\; \frac{1}{2} d^{\frac{1}{2}} \sqrt{\sum_{x,x' \in \mathcal{X}} P_{\mathbf{X}}(x)\, P_{\mathbf{X}}(x')\, \lambda_{x,x'} \;\; \mathbf{tr}(P_{\psi_x} P_{\psi_{x'}})}$$

Let

$$\lambda_{x,x'} \; := \; 2\,\mathrm{Prob}[\mathbf{F}(x) = \mathbf{F}(x')] - 1 \; = \; E_{\mathbf{F}}[\delta_{f(x),f(x')} - 1]$$

Note: For 2-universal F, $\lambda_{x,x'} \leq 0$ **for** $x \neq x'$**.**

Theorem: Let X, F, and W be as above. Then

$$\mathbf{d}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) \; \leq \; \tfrac{1}{2} d^{\frac{1}{2}} \sqrt{\sum_{x,x' \in \mathcal{X}} P_{\mathbf{X}}(x)\, P_{\mathbf{X}}(x')\, \lambda_{x,x'} \; \mathbf{tr}(P_{\psi_x} P_{\psi_{x'}})}$$

Corollary: If F is 2-universal, then

$$\mathbf{d}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) \; \leq \; \tfrac{1}{2} d^{\frac{1}{2}} \sqrt{\sum_{x \in \mathcal{X}} P^2_{\mathbf{X}}(x)} = \tfrac{1}{2}\, 2^{\frac{1}{2}(H_2(\mathbf{X}) - r)}$$

Moreover, if X is a uniform n-bit string, then

$$\mathbf{d}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) \; \leq \; \tfrac{1}{2}\, 2^{\frac{1}{2}(n-r)}$$

Theorem: **Let X, F, and W be as above. Then**

$$\mathbf{d}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) \;\le\; \tfrac{1}{2}d^{\frac{1}{2}}\sqrt{\sum_{x,x'\in\mathcal{X}} P_{\mathbf{X}}(x)\,P_{\mathbf{X}}(x')\,\lambda_{x,x'}\;\;\mathbf{tr}(P_{\psi_x}P_{\psi_{x'}})}$$

Proof: **For any** f**,**

$$\sum_{j=1}^{d}|\mu_j^f| \;\le\; d^{\frac{1}{2}}\sqrt{\sum_{j=1}^{d}|\mu_j^f|^2} \;=\; d^{\frac{1}{2}}\sqrt{\mathbf{tr}(\Lambda_f^2)}\;,$$

(using Jensen's inequality and Schur's (in)equality).

$$\mathbf{d}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) \;\le\; \tfrac{1}{2}E_{\mathbf{F}}\Big[\sum_{j=1}^{d}|\mu_j^{\mathbf{F}}|\Big] \;\le\; \tfrac{1}{2}\,d^{\frac{1}{2}}\,E_{\mathbf{F}}\Big[\sqrt{\mathbf{tr}(\Lambda_{\mathbf{F}}^2)}\Big] \le \tfrac{1}{2}\,d^{\frac{1}{2}}\sqrt{E_{\mathbf{F}}[\mathbf{tr}(\Lambda_{\mathbf{F}}^2)]}\;.$$

$$\mathbf{tr}(\Lambda_f^2) \;=\; \sum_{\substack{x,x'\in\mathcal{X}\\ f(x)=f(x')}} P_X(x)P_X(x')\,\mathbf{tr}(P_{\psi_x}P_{\psi_{x'}}) - \sum_{\substack{x,x'\in\mathcal{X}\\ f(x)\neq f(x')}} P_X(x)P_X(x')\,\mathbf{tr}(P_{\psi_x}P_{\psi_{x'}})$$

$$=\; \sum_{x,x'\in\mathcal{X}} \underbrace{2(\delta_{f(x),f(x')}-1)}_{E[.]\,=\,\lambda_{x,x'}}\; P_{\mathbf{X}}(x)P_{\mathbf{X}}(x')\,\mathbf{tr}(P_{\psi_x}P_{\psi_{x'}})$$

Comparing classical and quantum storage devices

Lemma: For a uniform 2-bit random variable X, a uniform Boolean balanced random function F, and a 1-(qu)bit storage system,

$$d^{\mathsf{c}}_{\mathsf{opt}}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) = \tfrac{1}{4}$$

and

$$d^{\mathsf{q}}_{\mathsf{opt}}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) = \frac{1}{2\sqrt{3}} \approx 0.289 \, .$$

Comparing classical and quantum storage devices

Lemma: For a uniform 2-bit random variable X, a uniform Boolean balanced random function F, and a 1-(qu)bit storage system,

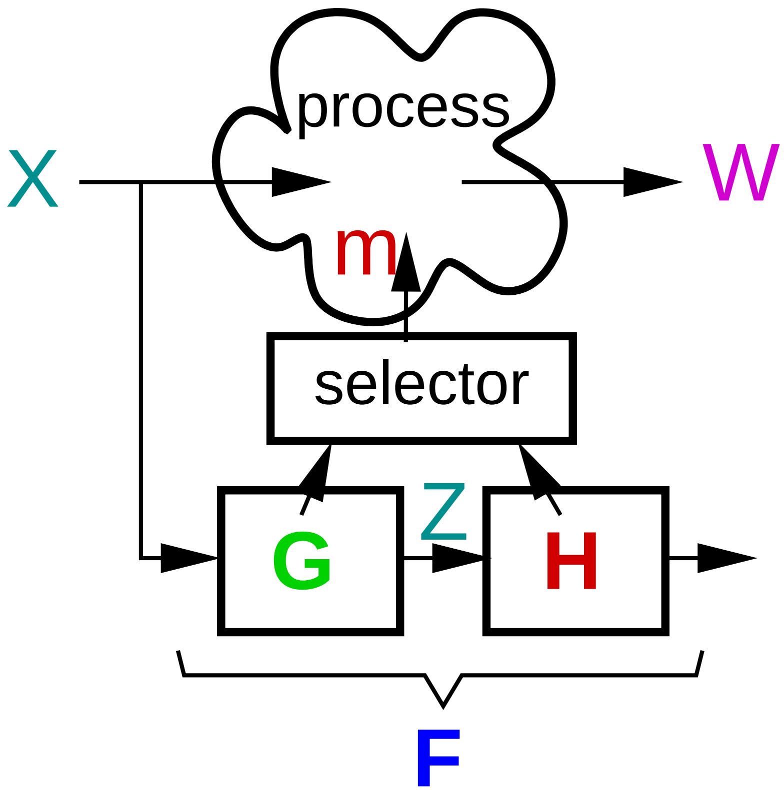
$$d^{\mathsf{c}}_{\mathsf{opt}}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) = \tfrac{1}{4}$$

and

$$d^{\mathsf{q}}_{\mathsf{opt}}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) = \frac{1}{2\sqrt{3}} \approx 0.289\,.$$

Lemma: For any random variable X and any uniform random function F,

$$\frac{1}{\sqrt{2\pi}}\left(1+O(2^{-(n-r)})\right)2^{-\frac{n-r}{2}} \leq d^{\mathsf{c}}_{\mathsf{opt}}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) \leq d^{\mathsf{q}}_{\mathsf{opt}}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) \leq \tfrac{1}{2}2^{-\frac{n-r}{2}}\,.$$



Lemma: If **G** is 2-universal and **H** is a uniform balanced Boolean function, then $\mathbf{F} = \mathbf{H} \circ \mathbf{G}$ is a 2-universal Boolean function.

Corollary: Let **X** be a random variable over $\mathcal{X}$. If for any 2-universal $(\mathcal{X}, \{0,1\})$-random function **F** and for any process generating **W** from **X** and **F** we have

$$\mathbf{d}(\mathbf{F}(\mathbf{X})|\mathbf{WF}) \leq \epsilon,$$

then for any 2-universal $(\mathcal{X}, \{0,1\}^s)$-random function **G** and any process generating a random variable **W** from **X** and **G** we have

$$\mathbf{d}(\mathbf{G}(\mathbf{X})|\mathbf{WG}) \leq \frac{3}{2} 2^{s/2} \epsilon.$$

Privacy amplification is secure against quantum adversaries

Theorem: Let X be uniformly distributed over $\{0,1\}^n$ and let G be a 2-universal random function from $\{0,1\}^n$ to $\{0,1\}^s$. If all information about X is stored in r qubits, then

$$d_{\mathsf{opt}}^{\mathsf{q}}(\mathbf{G}(\mathbf{X})|\mathbf{WG}) \leq \frac{3}{4}\, 2^{-\frac{1}{2}(n-r-s)} .$$

Note:

$$d_{\mathsf{opt}}^{\mathsf{c}}(\mathbf{G}(\mathbf{X})|\mathbf{WG}) = O\left(2^{-\frac{1}{2}(n-r-s)}\right)$$

Conclusions

- **In a quite general context quantum memory is only marginally more powerful than classical memory.**

Conclusions

- **In a quite general context quantum memory is only marginally more powerful than classical memory.**
- **Is this always true? What about the bounded-storage model?**

Conclusions

- **In a quite general context quantum memory is only marginally more powerful than classical memory.**
- **Is this always true? What about the bounded-storage model?**
- **Privacy amplification is secure even against adversaries with quantum knowledge.**

  This has applications for security proofs of quantum cryptographic schemes.