How secure is QKD?

Renato Renner

Centre for Quantum Computation

University of Cambridge, UK

Overview

Key S: uniformly distributed n-bit string

Question: How to define "security"?

Overview

Key S: uniformly distributed n-bit string

Informal definition of security

S is *perfectly secure* with respect to an adversary E

if E has no information on S.

Overview

Key S: uniformly distributed n-bit string

Informal definition of security

S is ε-*secure* if the information of E (adversary) on S is not larger than ε.

Overview

Key S: uniformly distributed n-bit string

Informal definition of security

S is ε-*secure* if the information of E (adversary) on S is not larger than ε.

Questions

- How to measure E's information?

  Should we use, e.g., *Shannon (mutual) information*?

Overview

Key S: uniformly distributed n-bit string

Informal definition of security

S is ε-*secure* if the information of E (adversary) on S is not larger than ε.

Questions

- How to measure E's information?

  Should we use, e.g., *Shannon (mutual) information*?

- How to choose ε?

  Is $\varepsilon := 2^{-1000}$ sufficient?

Overview

Key S: uniformly distributed n-bit string

Informal definition of security

S is ε-*secure* if the information of E (adversary) on S is not larger than ε.

Questions

- How to measure E's information?

  Should we use, e.g., *Shannon (mutual) information*?

- How to choose ε?

  Is $\varepsilon := 2^{-1000}$ sufficient?

Goal of this talk

- Answer these questions $\longrightarrow$ "good" security definition.

Overview

Key S: uniformly distributed n-bit string

Informal definition of security

S is ε-*secure* if the information of E (adversary) on S is not larger than ε.

Questions

- How to measure E's information?

  Should we use, e.g., *Shannon (mutual) information*?

- How to choose ε?

  Is $\varepsilon := 2^{-1000}$ sufficient?

Goal of this talk

- Answer these questions $\longrightarrow$ "good" security definition.
- Generate fully secure keys from only partially secure data.

Classical situation

Notation

S	secret key
Z	(overall) information of adversary
P_{SZ}	joint distribution of S and Z

Classical situation

Notation

S	secret key
Z	(overall) information of adversary
P_{SZ}	joint distribution of S and Z

Definition

S is *perfectly secure with respect to* Z if

$$P_{SZ} = P_U \times P_Z$$

where P_U is the uniform distribution.

Classical situation

Notation

S	secret key
Z	(overall) information of adversary
P_{SZ}	joint distribution of S and Z

Definition

S is ε-*secure* with respect to Z if

$$\|P_{SZ} - P_U \times P_Z\| \leq \varepsilon$$

where P_U is the uniform distribution.

Classical situation

Notation

S	secret key
Z	(overall) information of adversary
P_{SZ}	joint distribution of S and Z

Definition

S is ε-*secure* with respect to Z if

$$\left\| P_{SZ} - P_U \times P_Z \right\| \leq \varepsilon$$

where P_U is the uniform distribution.

Statistical distance: $\left\| P_X - P_{X'} \right\| := \frac{1}{2} \sum_x \left| P_X(x) - P_{X'}(x) \right|$

Classical situation: interpretation

Lemma

Let S_ε be an ε-secure key (with respect to Z).

Then there exists a key S_0 which is perfectly secure (with respect to Z)

and

$$\Pr[S_\varepsilon \neq S_0] \leq \varepsilon \, .$$

Classical situation: interpretation

Lemma

Let S_ε be an ε-secure key (with respect to Z).

Then there exists a key S_0 which is perfectly secure (with respect to Z)

and

$$\mathsf{Pr}[S_\varepsilon \neq S_0] \leq \varepsilon \; .$$

Main implication for applications

If we use an ε-secure key S_ε instead of a perfectly secure key S_0, then the error probability cannot grow by more than ε.

$\longrightarrow$ parameter ε has a well-defined interpretation: failure probability

Keys in a quantum world

Notation

S secret key

ρ_E state of adversary's quantum system E (might depend on S)

Keys in a quantum world

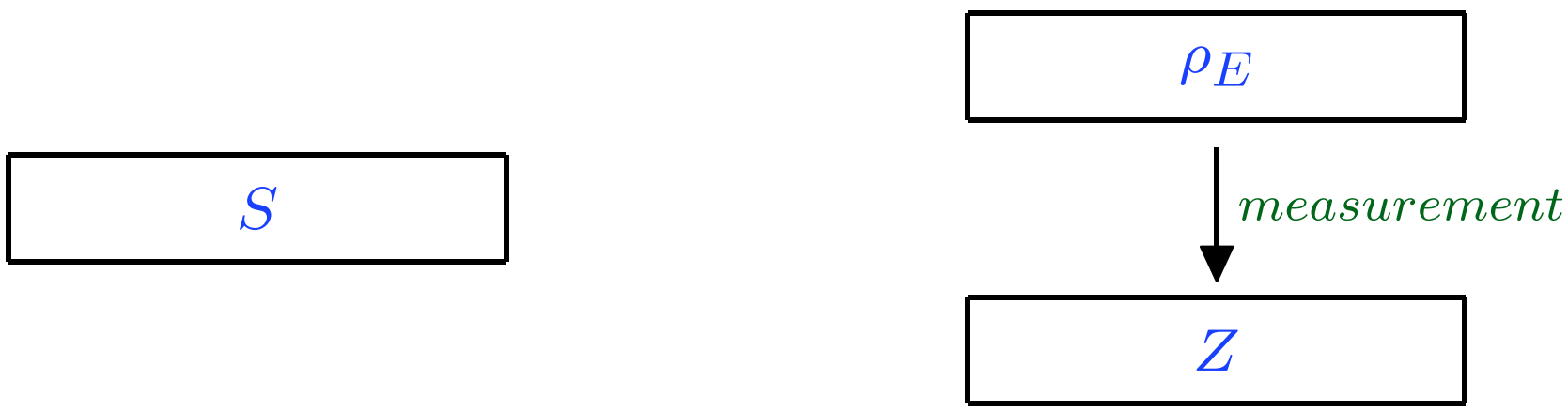
Notation

S secret key

ρ_E state of adversary's quantum system E (might depend on S)

Definition

S is *perfectly secure w.r.t.* E if $P_{SZ} = P_U \times P_Z$ for any measurment of E giving Z.



Keys in a quantum world

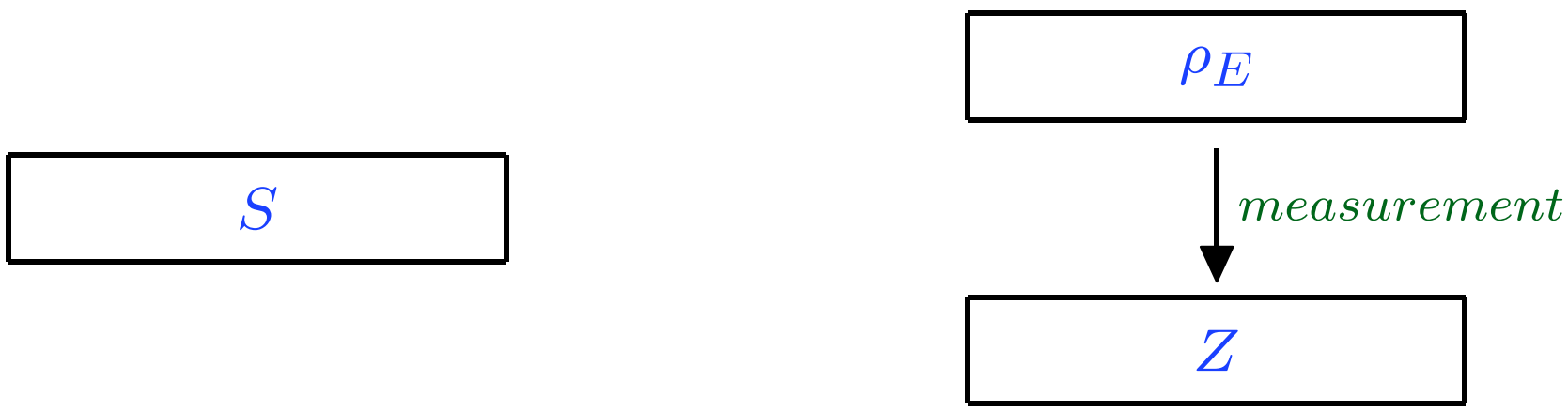
Notation

S secret key

ρ_E state of adversary's quantum system E (might depend on S)

Definition

S is *perfectly secure w.r.t.* E if $P_{SZ} = P_U \times P_Z$ for any measurment of E giving $Z \quad \longleftrightarrow \quad \rho_E$ completely independent of S.

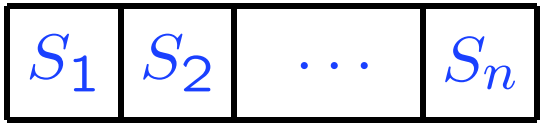


Keys in a quantum world

Example

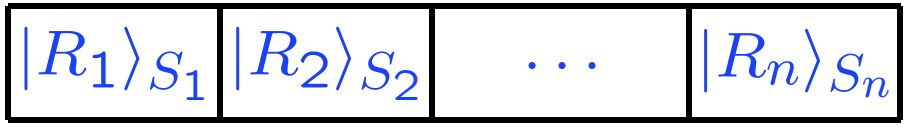
adv. E has encodings of rand. bits R_i w.r.t. basis depending on key bits S_i

uniform key S



0 1 0

adversary's state ρ_E



$|R_1\rangle_+$ $|R_2\rangle_\times$ $|R_n\rangle_+$

$S_i = 0$ rectilinear basis $+$
$S_i = 1$ diagonal basis $\times$

Keys in a quantum world

Example

adv. E has encodings of rand. bits R_i w.r.t. basis depending on key bits S_i

uniform key S

S_1	S_2	$\cdots$	S_n
0	1		0

adversary's state ρ_E

$\|R_1\rangle_{S_1}$	$\|R_2\rangle_{S_2}$	$\cdots$	$\|R_n\rangle_{S_n}$
$\|R_1\rangle_+$	$\|R_2\rangle_\times$		$\|R_n\rangle_+$

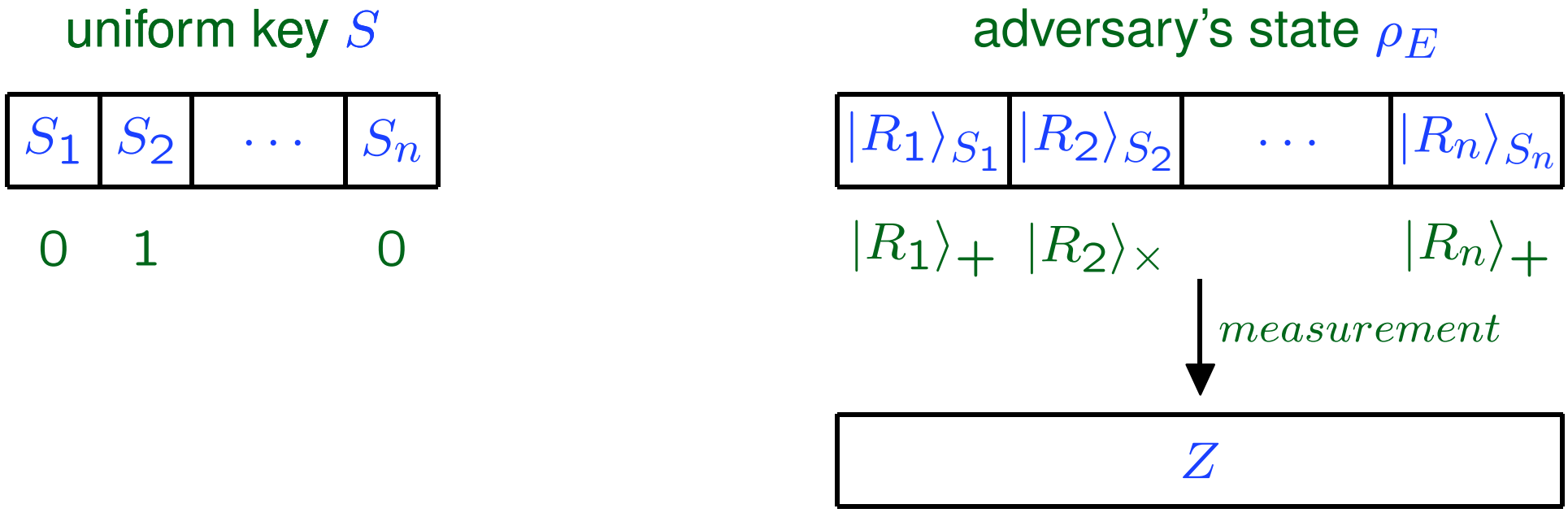
$S_i = 0$ rectilinear basis $+$
$S_i = 1$ diagonal basis $\times$

Observation: S and ρ_E are completely independent.

Keys in a quantum world

Example

adv. E has encodings of rand. bits R_i w.r.t. basis depending on key bits S_i



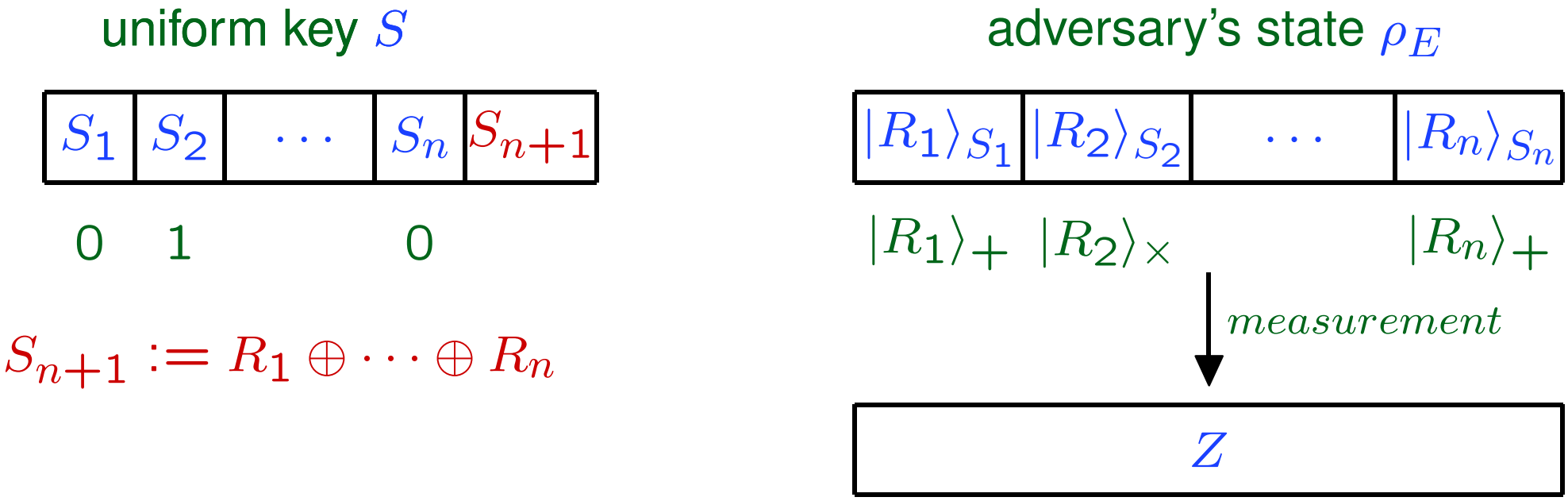
Observation: S and ρ_E are completely independent.

In particular: $P_{SZ} = P_U \times P_Z \quad \longrightarrow \quad S$ is perfectly secure w.r.t. E.

Keys in a quantum world

Example

adv. E has encodings of rand. bits R_i w.r.t. basis depending on key bits S_i

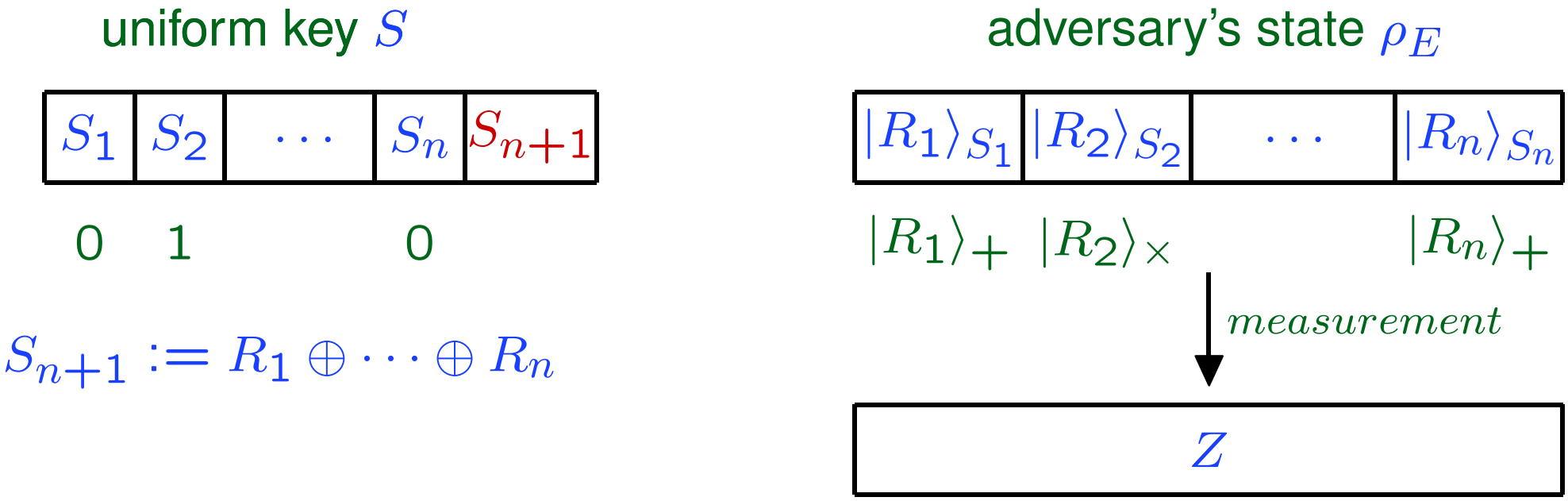


Consider additional key bit S_{n+1}.

Keys in a quantum world

Example

adv. E has encodings of rand. bits R_i w.r.t. basis depending on key bits S_i

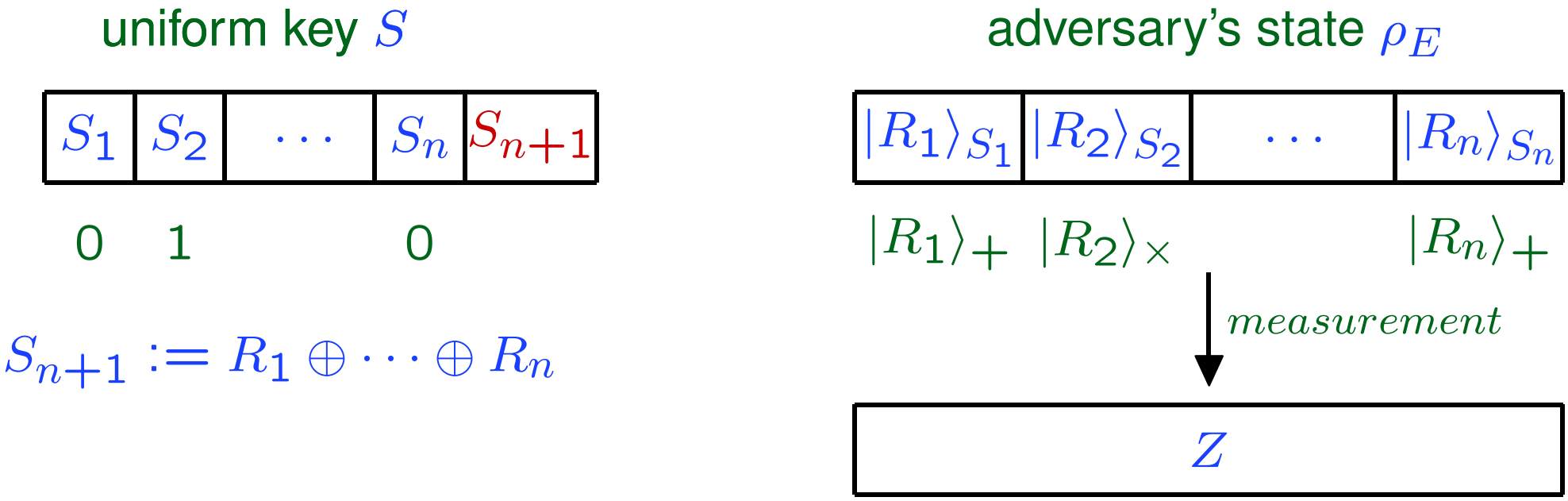


Observation: S is still ε-secure w.r.t. Z, for $\varepsilon \leq 2^{-\gamma n}$.

Keys in a quantum world

Example

adv. E has encodings of rand. bits R_i w.r.t. basis depending on key bits S_i



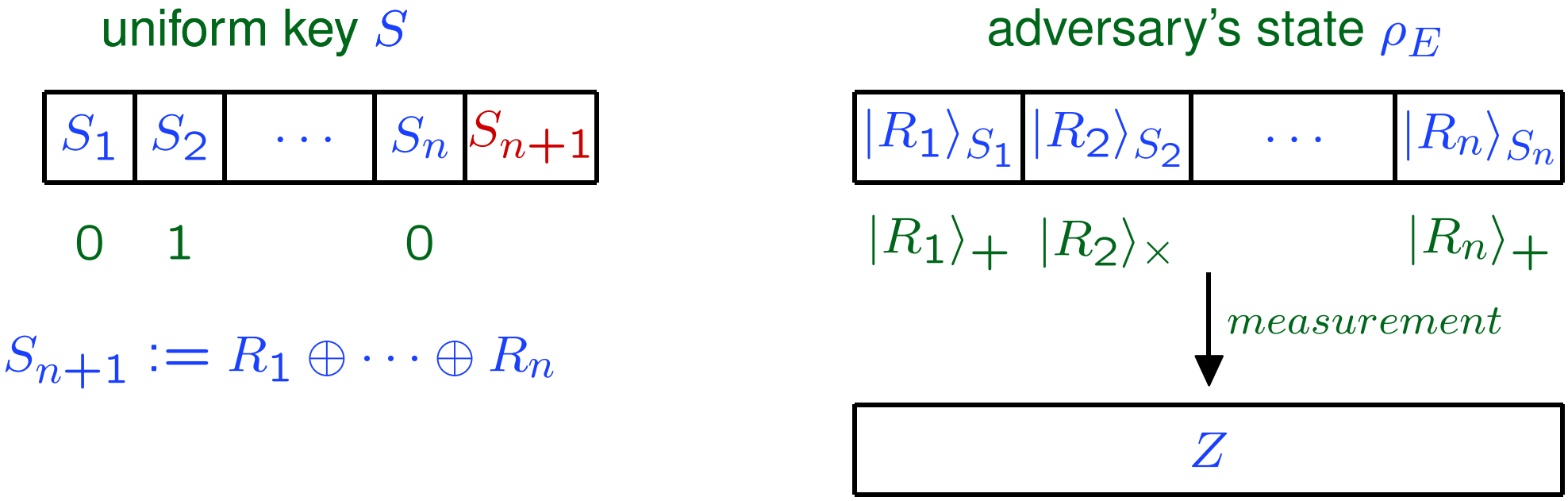
Observation: S is still ε-secure w.r.t. Z, for $\varepsilon \leq 2^{-\gamma n}$.

Remark: Shannon (mutual) information is small as well: $I(S;Z) \leq \varepsilon$.

Keys in a quantum world

Example

adv. E has encodings of rand. bits R_i w.r.t. basis depending on key bits S_i

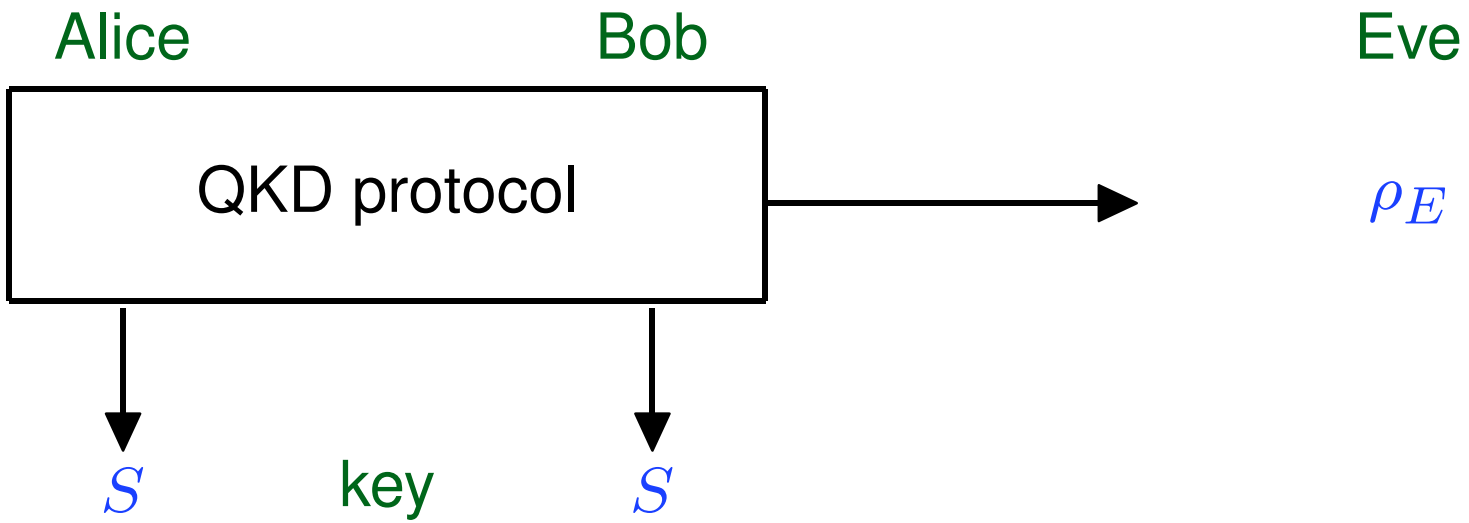


Observation: S is still ε-secure w.r.t. Z, for $\varepsilon \leq 2^{-\gamma n}$.

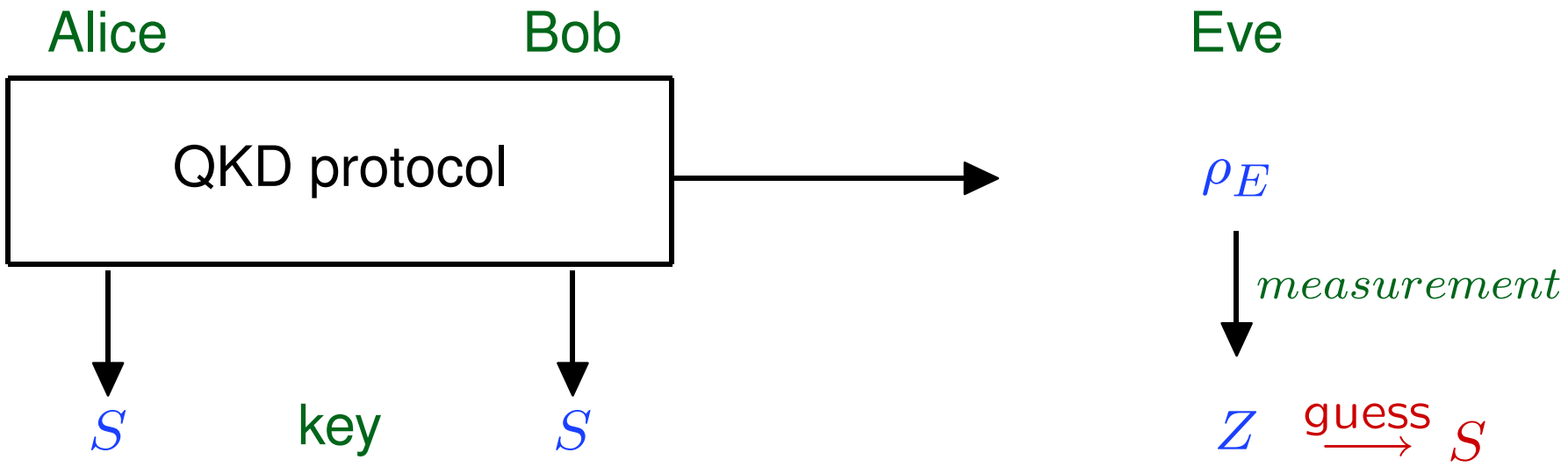
Remark: Shannon (mutual) information is small as well: $I(S;Z) \leq \varepsilon$.

But: Given $S_1, \ldots, S_n$, the bit S_{n+1} is completely insecure w.r.t. E!

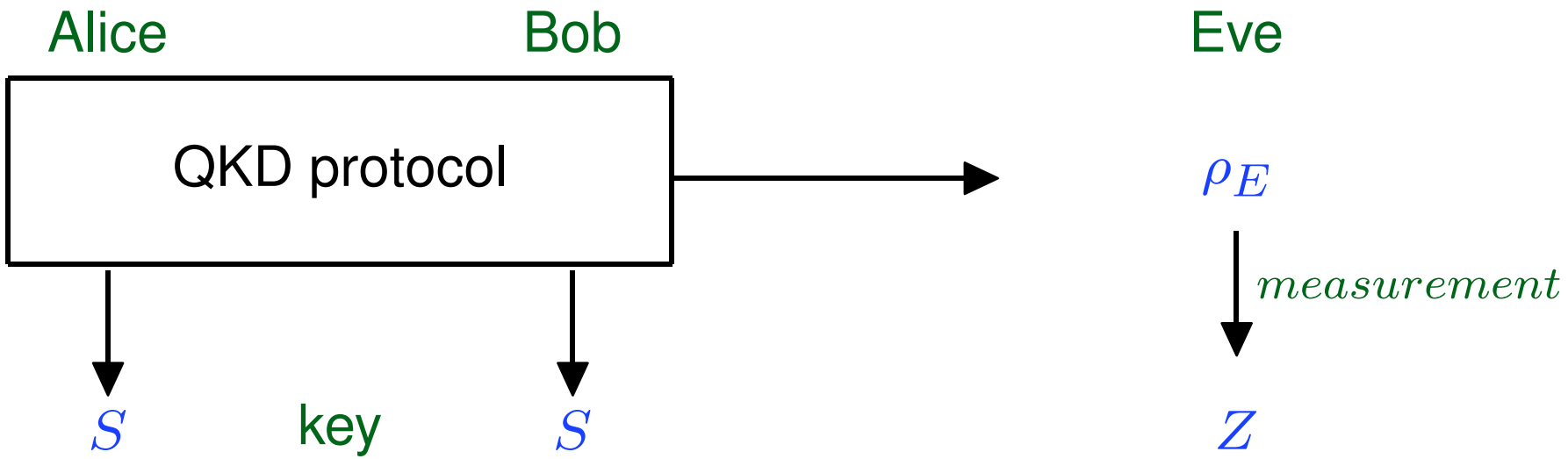
Implications for QKD



Implications for QKD

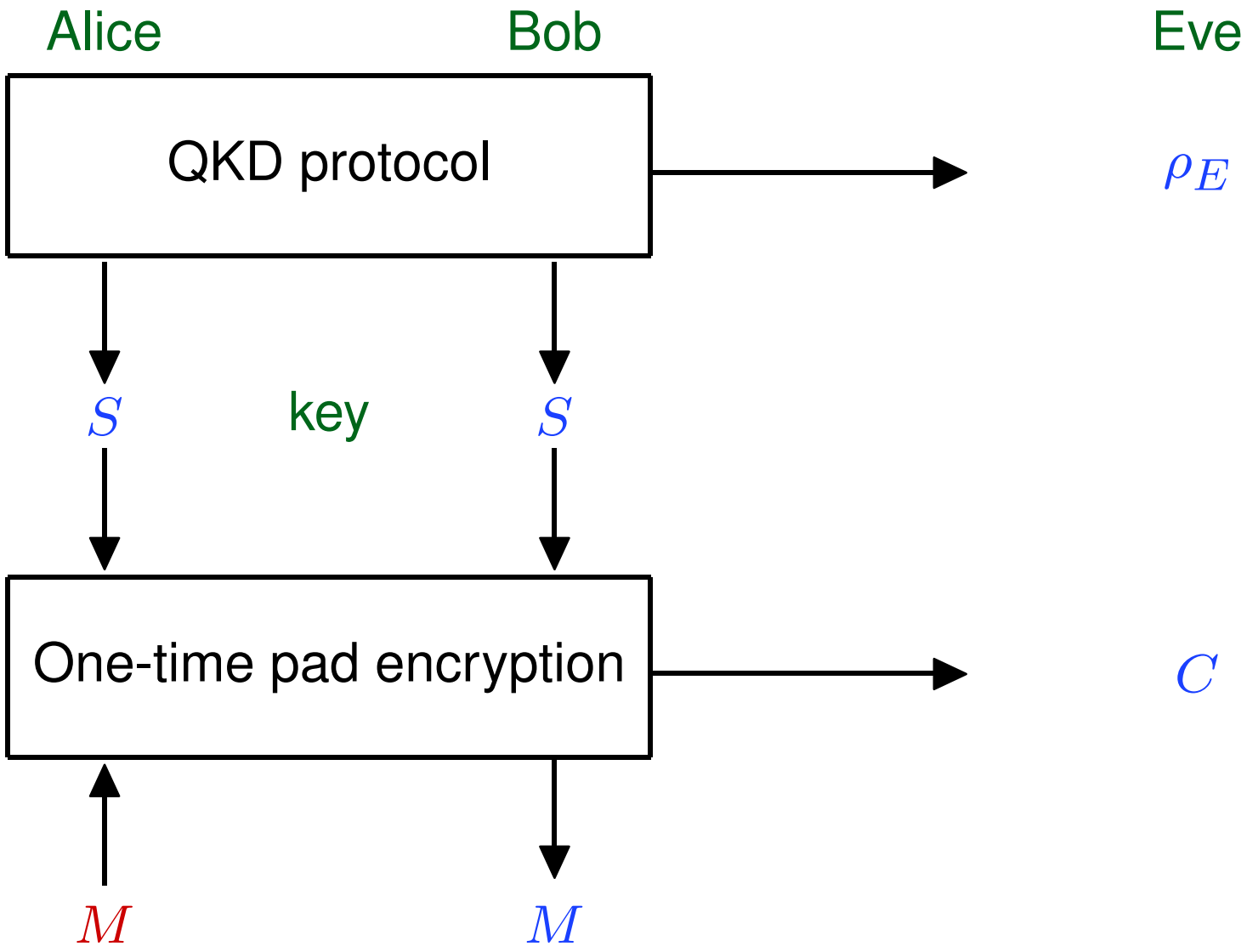


Implications for QKD

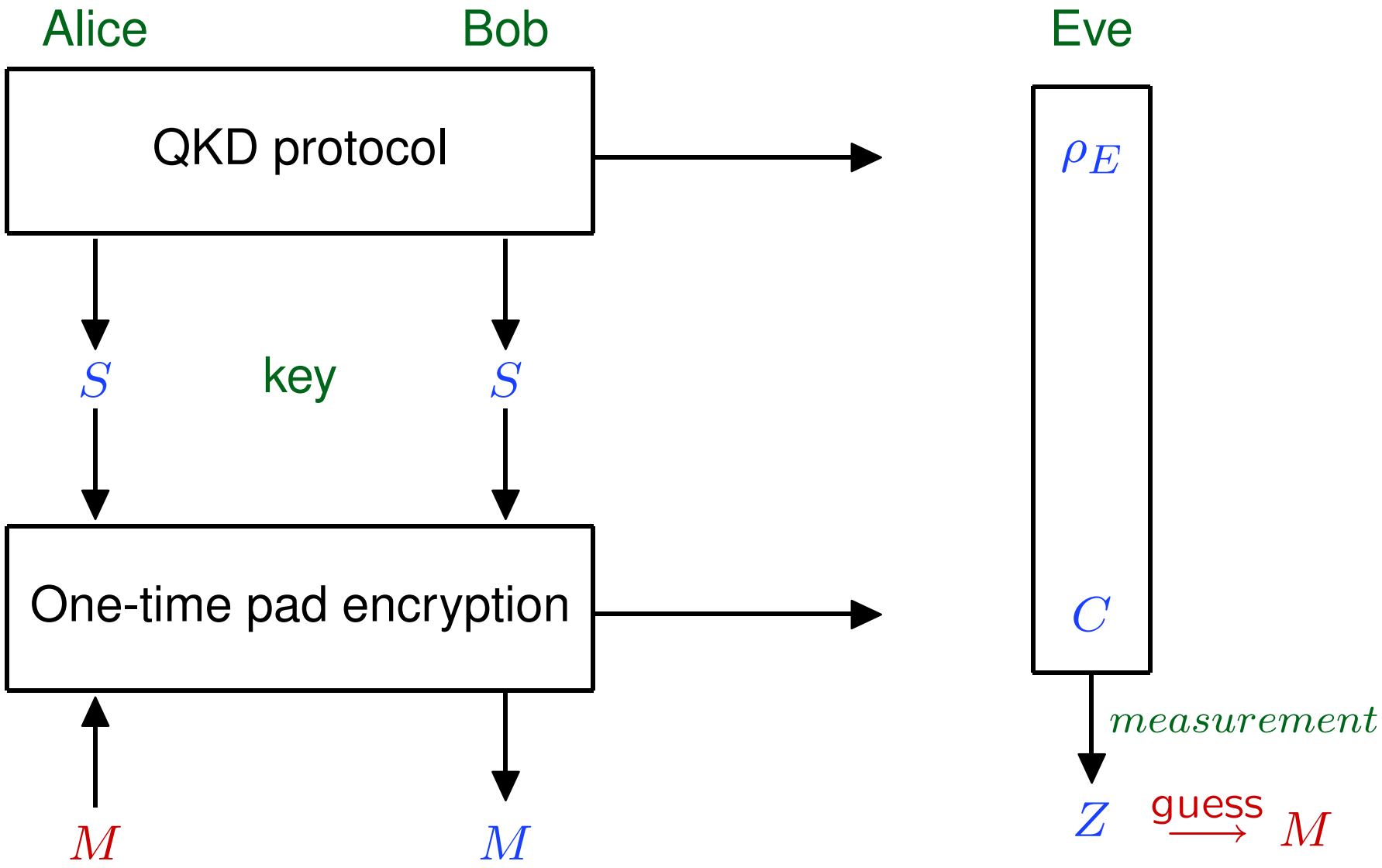


$I(Z;S) \leq \varepsilon \iff$ guessing of S not possible $\overset{?}{\iff}$ S secure

Implications for QKD



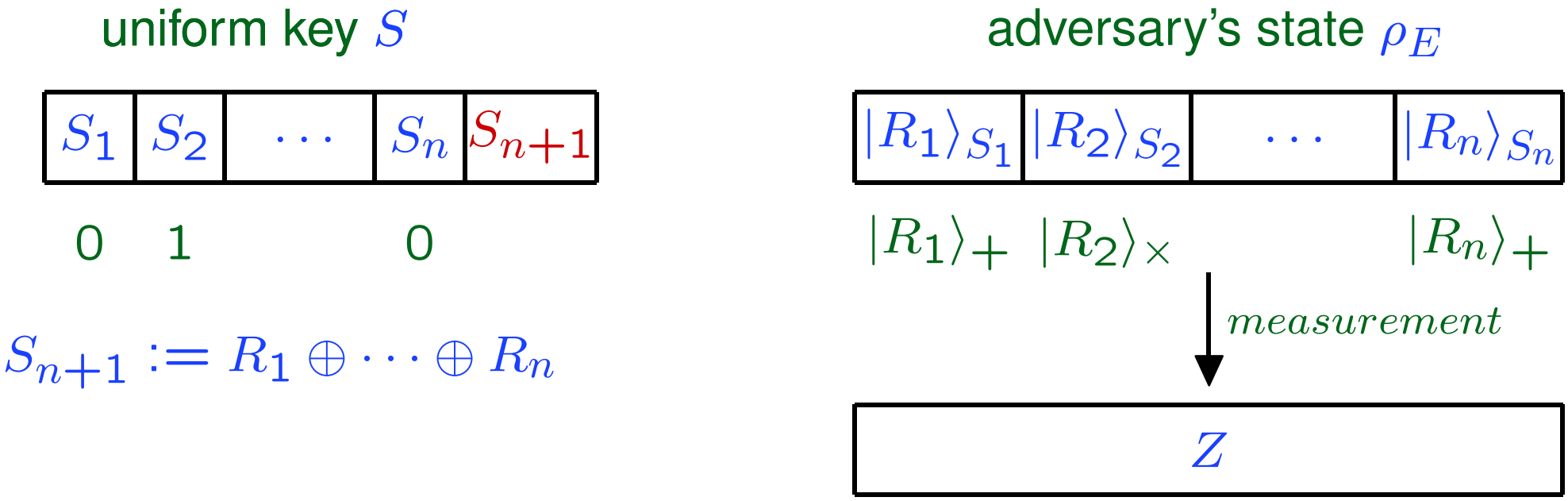
Implications for QKD



Keys in a quantum world

Example

adversary has encodings of random bits R_i w.r.t. basis dep. on key bits S_i



Observation: S and Z almost independent: $I(S;Z) \leq 2^{-\Omega(n)}$.

But: Given $S_1, \ldots, S_n$, the bit S_{n+1} is completely insecure w.r.t. E!

Keys in a quantum world

Recall the classical definition

S is ε-*secure* with respect to Z if $\left\| P_{SZ} - P_U \times P_Z \right\| \leq \varepsilon$ for P_U uniform.

Keys in a quantum world

Recall the classical definition

S is ε-*secure* with respect to Z if $\left\| P_{SZ} - P_U \times P_Z \right\| \leq \varepsilon$ for P_U uniform.

Idea: Translate this definition to quantum states.

Keys in a quantum world

Recall the classical definition

S is ε-*secure* with respect to Z if $\left\| P_{SZ} - P_U \times P_Z \right\| \leq \varepsilon$ for P_U uniform.

Idea: Translate this definition to quantum states.

Let $\rho_{SE} := \sum_s P_S(s) \cdot |s\rangle\langle s| \otimes \rho_E^s$ where

- $|s\rangle$ orthogonal states representing the value of S
- ρ_E^s state of E conditioned on $S = s$.

Keys in a quantum world

Recall the classical definition

S is ε-*secure* with respect to Z if $\left\| P_{SZ} - P_U \times P_Z \right\| \leq \varepsilon$ for P_U uniform.

Idea: Translate this definition to quantum states.

Let $\rho_{SE} := \sum_s P_S(s) \cdot |s\rangle\langle s| \otimes \rho_E^s$ where

$\|s\rangle$	orthogonal states representing the value of S
ρ_E^s	state of E conditioned on $S = s$.

Definition [BHLMO04, RK04]

S is ε-*secure* with respect to E if $\left\| \rho_{SE} - \rho_U \otimes \rho_E \right\| \leq \varepsilon$.

ρ_U	fully mixed state
$\|\cdot\|$	trace norm

Generating secure keys

Question

Is the definition achievable?

(Can we generate ε-secure keys, e.g., by QKD?)

If yes, how?

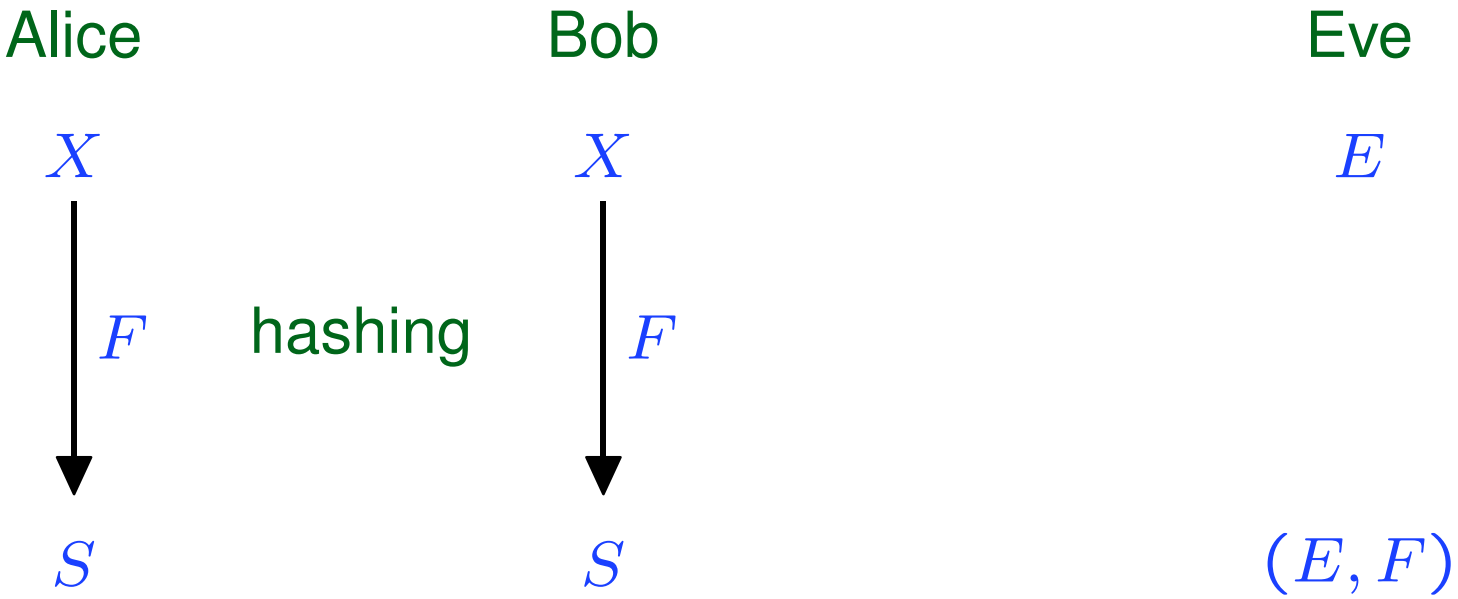
Generating secure keys

Transforming partially secure data X into a fully secure key S

Alice	Bob	Eve
X	X	E

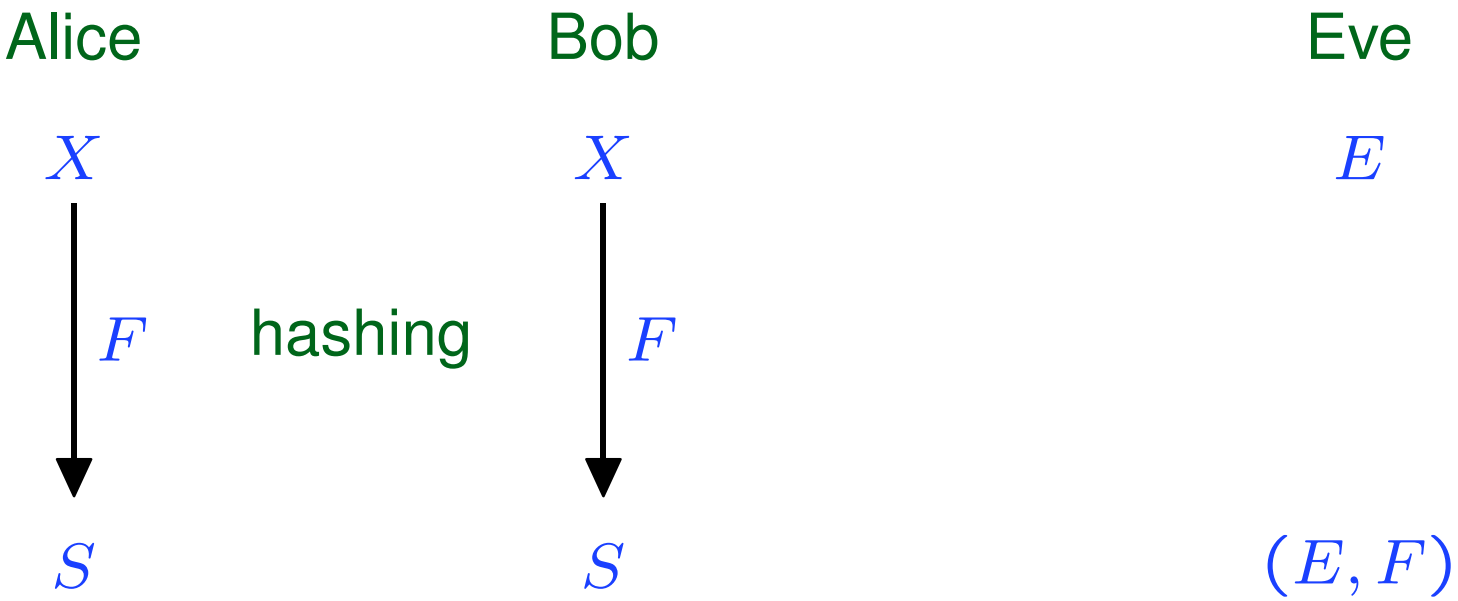
Generating secure keys

Transforming partially secure data X into a fully secure key S



Generating secure keys

Transforming partially secure data X into a fully secure key S



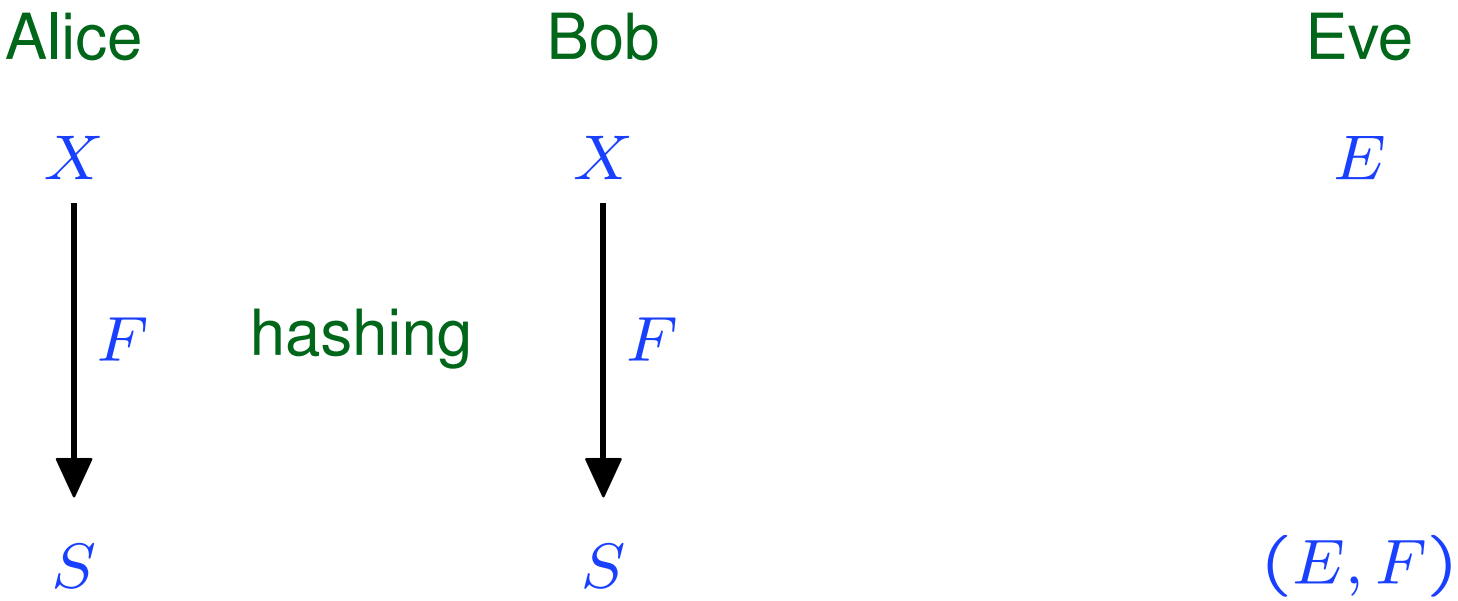
Informal result (Privacy amplification)

If X has sufficient entropy given E and if F is a two-universal hash funct.

then $S = F(X)$ is ε-secure with respect to (E, F).

Generating secure keys

Transforming partially secure data X into a fully secure key S



Result [BBR88,ILL89,BBCM95] (for class. adv.); [RK05] (for quant. adv.)

If X has sufficient entropy given E and if F is a two-universal hash funct.

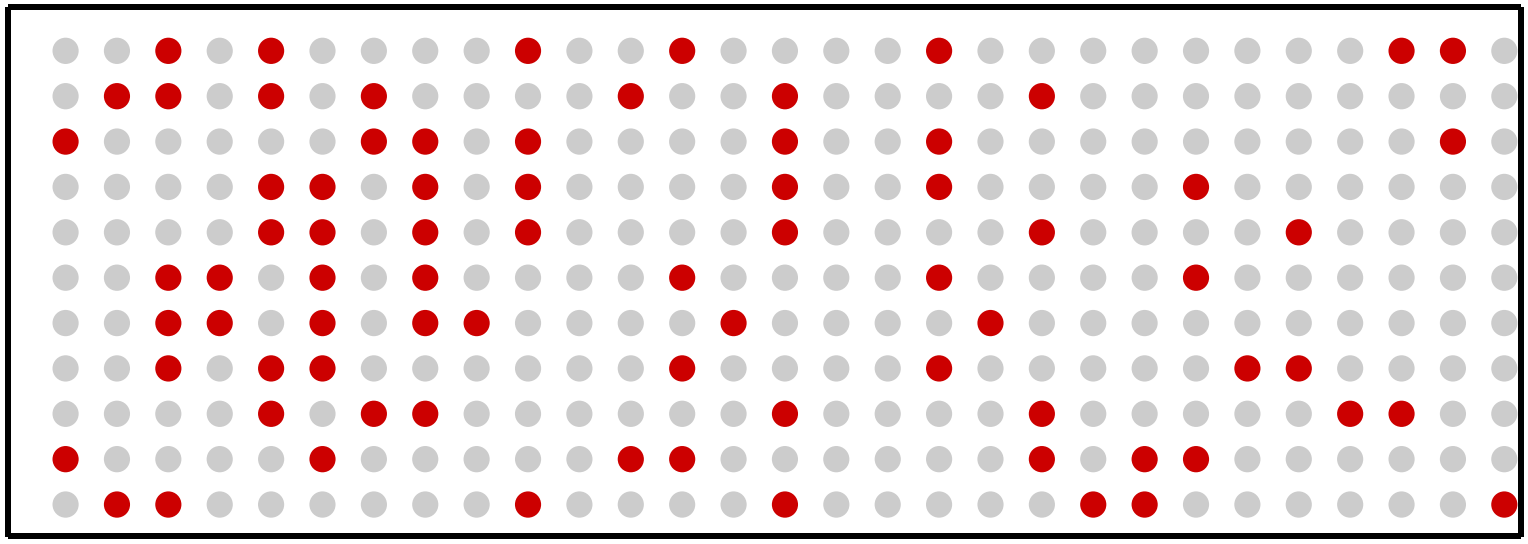
then $S = F(X)$ is ε-secure with respect to (E, F).

Generating secure keys

How does privacy amplification work?

(random) hash function $F : \mathcal{X} \mapsto \{0,1\}$

$\mathcal{X}$ (range of X)

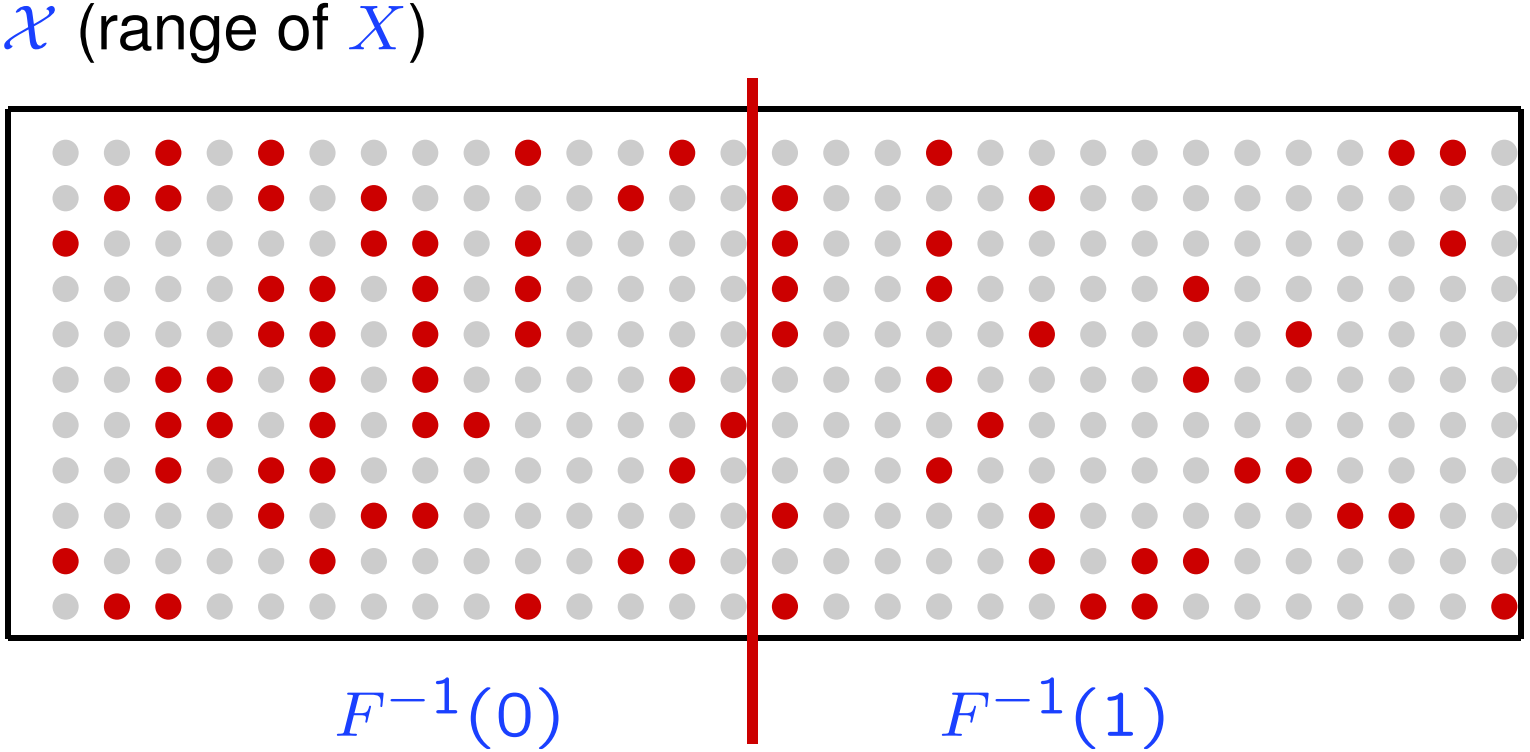


- $x \in \mathcal{X}$ with $P_{X|Z=z}(x) > 0$

Generating secure keys

How does privacy amplification work?

(random) hash function $F : \mathcal{X} \mapsto \{0, 1\}$



- $x \in \mathcal{X}$ with $P_{X|Z=z}(x) > 0$

Generating secure keys

Definition

A family $\mathcal{F}$ of functions from $\mathcal{X}$ to $\mathcal{Y}$ is called two-universal if

$$\Pr_{F \leftarrow \mathcal{F}}\left[F(x) = F(x')\right] \leq \frac{1}{|\mathcal{Y}|}$$

for all $x \neq x'$.

Generating secure keys

Definition

A family $\mathcal{F}$ of functions from $\mathcal{X}$ to $\mathcal{Y}$ is called two-universal if

$$\Pr_{F \leftarrow \mathcal{F}}\left[F(x) = F(x')\right] \leq \frac{1}{|\mathcal{Y}|}$$

for all $x \neq x'$.

Examples

- The set of all functions from $\mathcal{X}$ to $\mathcal{Y}$.
- $\{F_a\}_{a \in \mathsf{GF}(2^M)}$, where $F_a(x) := [a \cdot x]_n$ (computed in $\mathsf{GF}(2^M)$).

Generating secure keys

How to measure the entropy?

Generating secure keys

How to measure the entropy?

Classical case

X	initial key
Z	information of adversary on S
P_{XZ}	joint distribution of X and Z

Generating secure keys

How to measure the entropy?

Classical case

X	initial key
Z	information of adversary on S
P_{XZ}	joint distribution of X and Z

Definition

The *min-entropy* of X given Z is defined by

$$H_{\min}(X|Z) := -\log \max_{x,z} \frac{P_{XZ}(x,z)}{P_Z(z)}$$

Remark: There are alternative definitions (e.g., Dodis, Smith).

Generating secure keys

Classical case

X	initial key
Z	information of adversary on S
P_{XZ}	joint distribution of X and Z

Definition

The *min-entropy* of X given Z is defined by

$$H_{\min}(X|Z) := -\log \max_{x,z} \frac{P_{XZ}(x,z)}{P_Z(z)}$$

Theorem (Privacy amplification) [ILL89,BBCM95]

Two-universal hashing gives a secure key of length $n \approx H_{\min}(X|Z)$.

Generating secure keys

Quantum case

X	initial key
E	information of adversary on S
ρ_{XE}	$\sum_x P_X(x) \cdot \|x\rangle\langle x\| \otimes \rho_E^x$

Definition

The *min-entropy* of X given E is defined by

$$H_{\min}(X|E) := -\log \max \mathrm{ev}\left[(\mathrm{id}_X \otimes \rho_E)^{-1/2} \rho_{XE} (\mathrm{id}_X \otimes \rho_E)^{-1/2}\right]$$

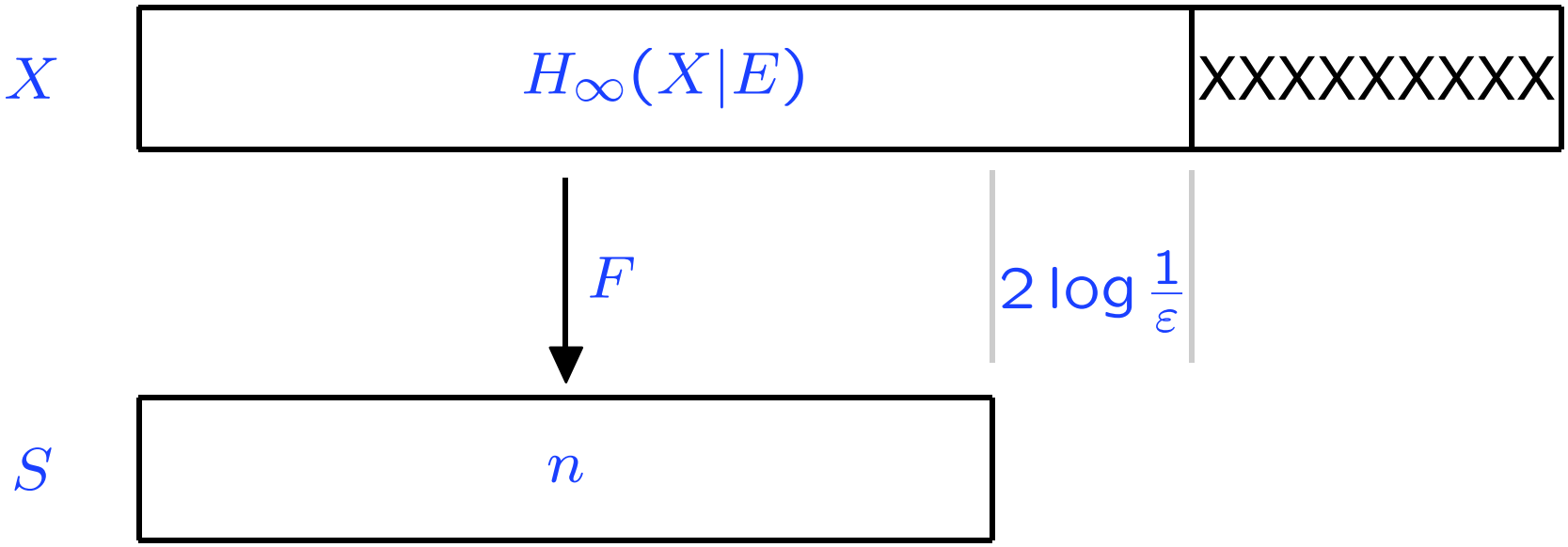
Theorem (Privacy amplification) [R05]

Two-universal hashing gives a secure key of length $n \approx H_{\min}(X|E)$.

Generating secure keys

Theorem (Privacy amplification against quantum adv.) [R05]

$S = F(X)$ is ε-secure with respect to (E, F), for $\varepsilon = 2^{-\frac{1}{2}\left(H_\infty(X|E) - n\right)}$.



Conclusions

Main points

- Definition of ε-security where ε is a finite and well-defined parameter (ε: failure probability).
- ε-secure keys can be generated from partially secure data X with sufficiently large entropy $H_\infty(X|E)$ (two-universal hashing).

Conclusions

Main points

- Definition of ε-security where ε is a finite and well-defined parameter (ε: failure probability).
- ε-secure keys can be generated from partially secure data X with sufficiently large entropy $H_\infty(X|E)$ (two-universal hashing).

Remarks related to QKD

- definitions based on Shannon information are not sufficient (even if the security parameter is exponentially small)
- use two-universal hashing as a last protocol step to get ε-secure keys (choice of ε might be left to the user).

For more details: quant-ph/0512021, quant-ph/0512258 .

For more details: quant-ph/0512021, quant-ph/0512258 .

I would like to thank my collaborators

- Andor Bariska
- Robert König
- Ueli Maurer

Thanks.