The finiteness of security (Tutorial)

Renato Renner

QSIT Quantum Science and Technology
National Centre of Competence in Research

ETH zürich

$\varepsilon > 0$
(Tutorial)

Renato Renner

QSIT Quantum Science and Technology
National Centre of Competence in Research

ETH zürich

Rationale

$$\varepsilon > 0$$

- Security is always finite.
- It is therefore crucial to understand how to quantify it.

Epsilon-security

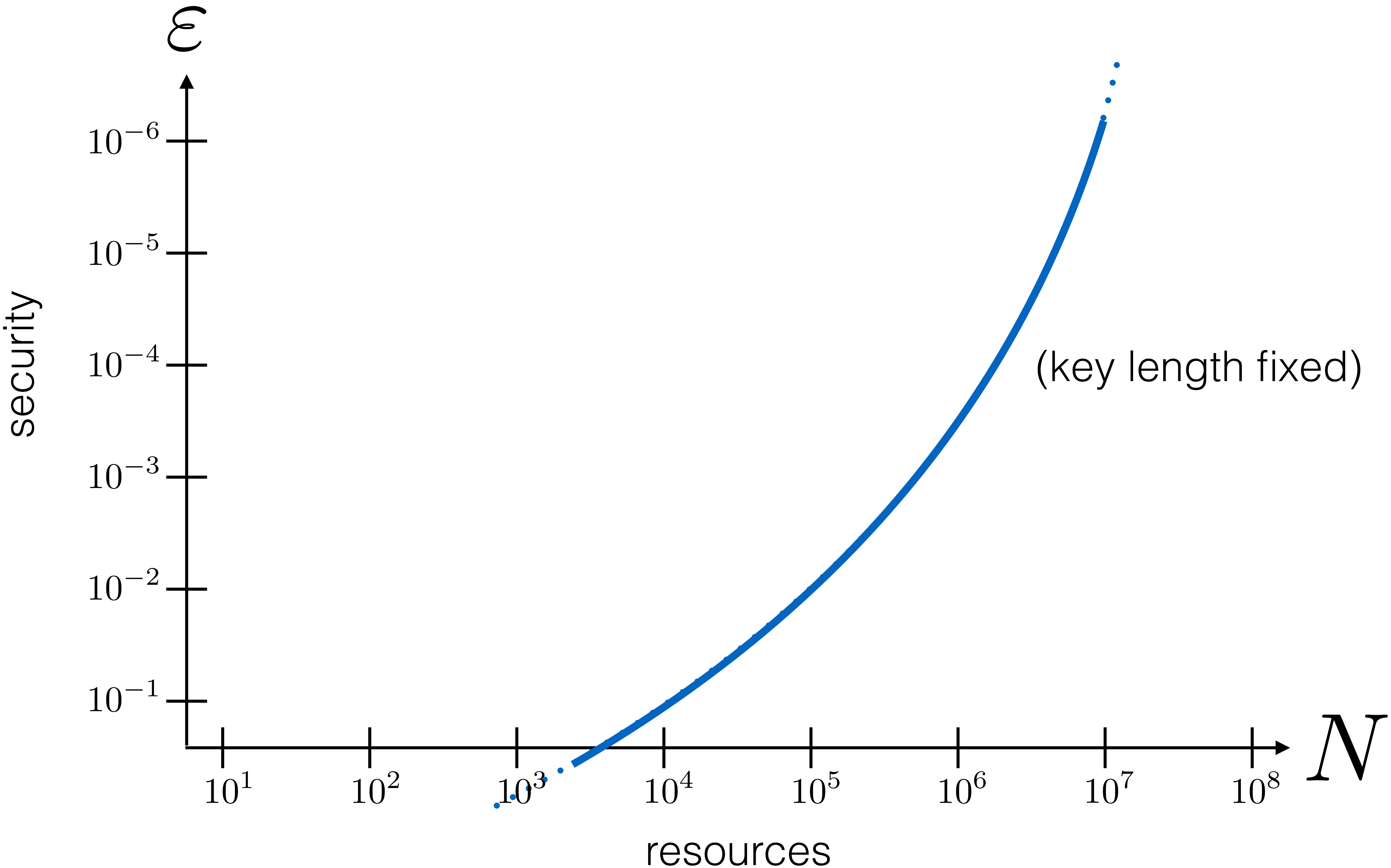
Certificate

The keys generated by this device have security

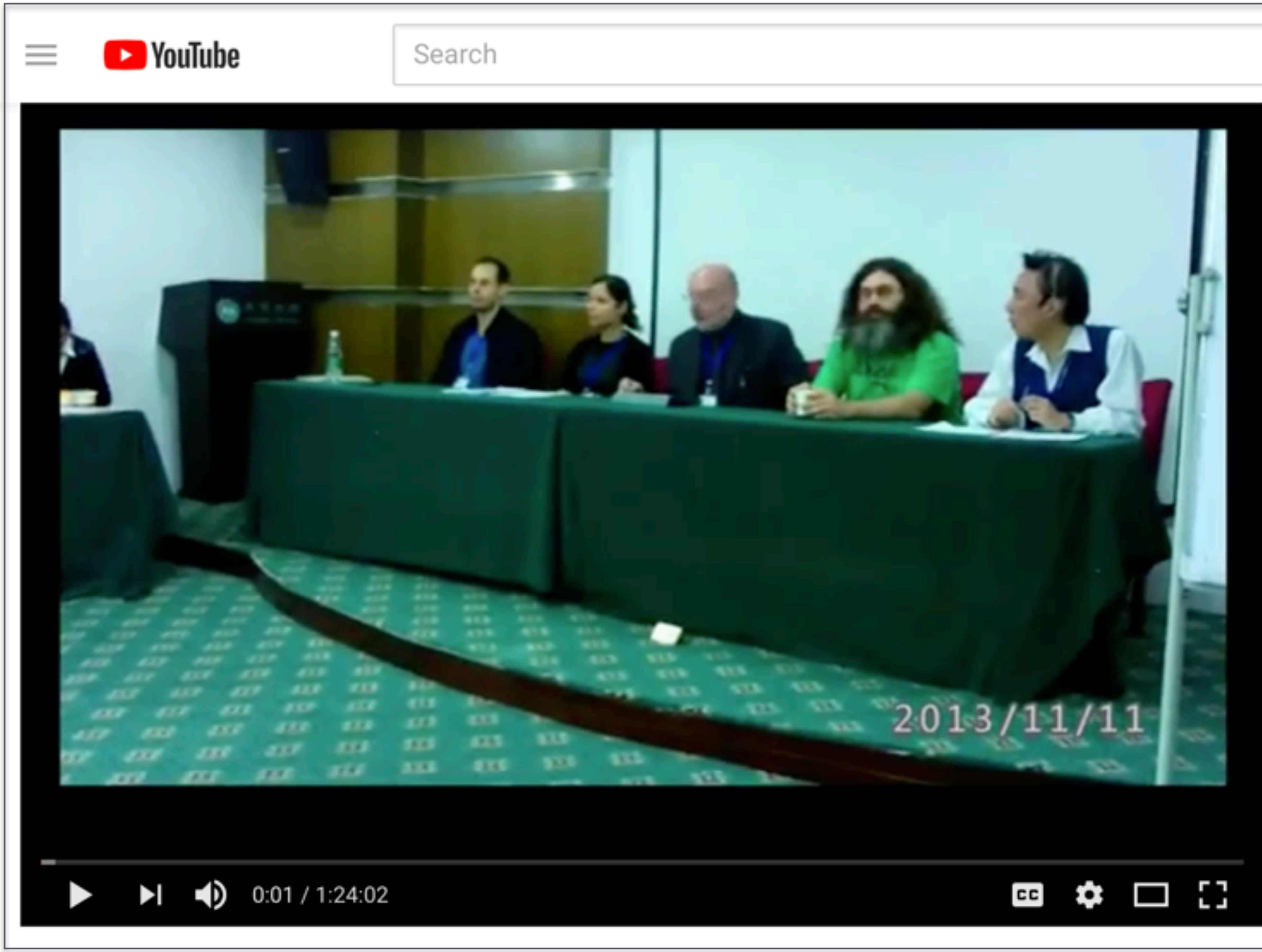
$$\varepsilon = 10^{-8}$$

METAS
Federal Office of Metrology

“Finite-size effects” sound rather boring …



… but the epsilon is hotly debated



Debate at the "HotPI" conference, Hunan University, Changsha

The debate is still ongoing …

Misconception in Theory of Quantum Key Distribution -Reply to Renner-

Osamu Hirota*
Quantum ICT Research Institute, Tamagawa University
6-1-1, Tamagawa-gakuen, Machida, Tokyo, 194-8610, JAPAN
(Dated: August 16, 2018)

It has been pointed out by Yuen that the security theory of quantum key distribution(QKD) guided by Shor-Preskill theory has serious defects, in particular their key rate theory is not correct. Theory groups of QKD tried to improve several defects. Especially, Renner employed trace distance

… and is basically about the epsilon

On the Foundations of Quantum Key Distribution — Reply to Renner and Beyond*

Horace P. Yuen
Department of Electrical Engineering and Computer Science
Department of Physics and Astronomy
Northwestern University, Evanston Il. 60208
yuen@eecs.northwestern.edu

August 4, 2018

Abstract

In a recent note (arXiv:1209.2423) Renner claims that the criticisms of Hirota and Yuen on the security foundation of quantum key distribution arose from a logical mistake. In this paper it is shown that Renner

What is the problem?

has been repeatedly given in [2-5]. Rather, Renner made a fundamental error in [7-8] which has become the standard interpretation of the trace distance criterion d widely employed in QKD. This incorrect interpretation leads to the current prevalent QKD security claim that the generated key K has a probability $p \geq 1 - d$ of being ideal [9-11]. In actuality, K is not

Security claim

Certificate

The keys generated by this device have security

$$\varepsilon = 10^{-8}$$

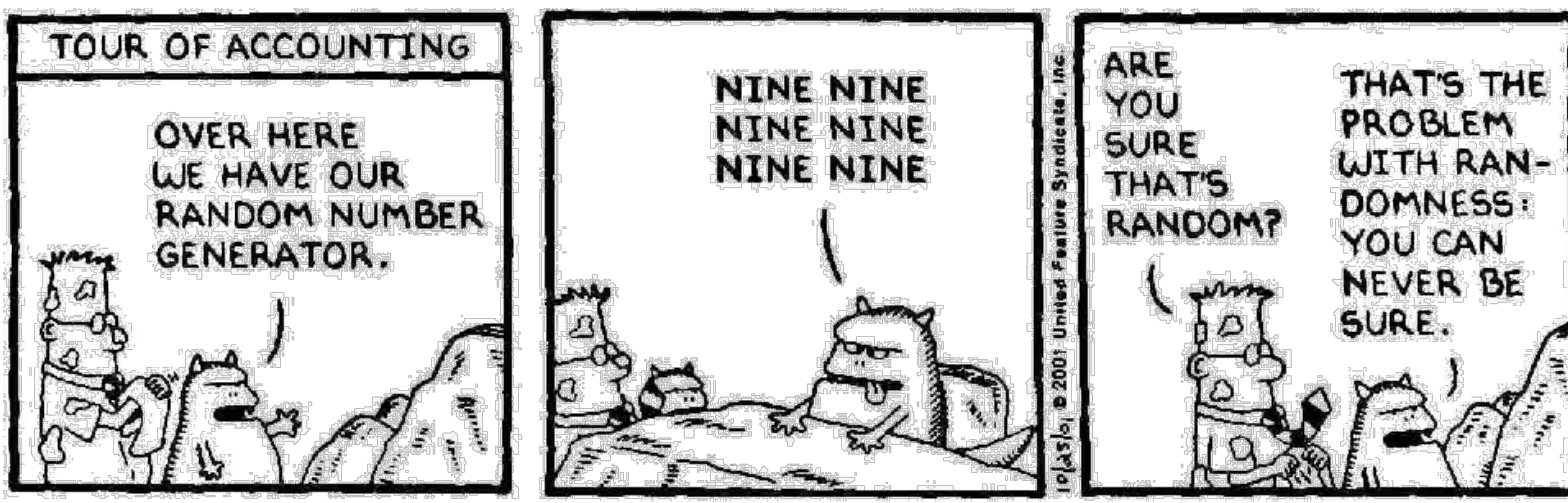
METAS
Federal Office
of Metrology

Operational meaning:

"An adversary cannot gain any information about the secret, except with probability epsilon."

Where does the epsilon come from?

From statistical fluctuations in the random choices .



Risk that adversary makes correct guesses

Recall that QKD protocols involve various random choices.

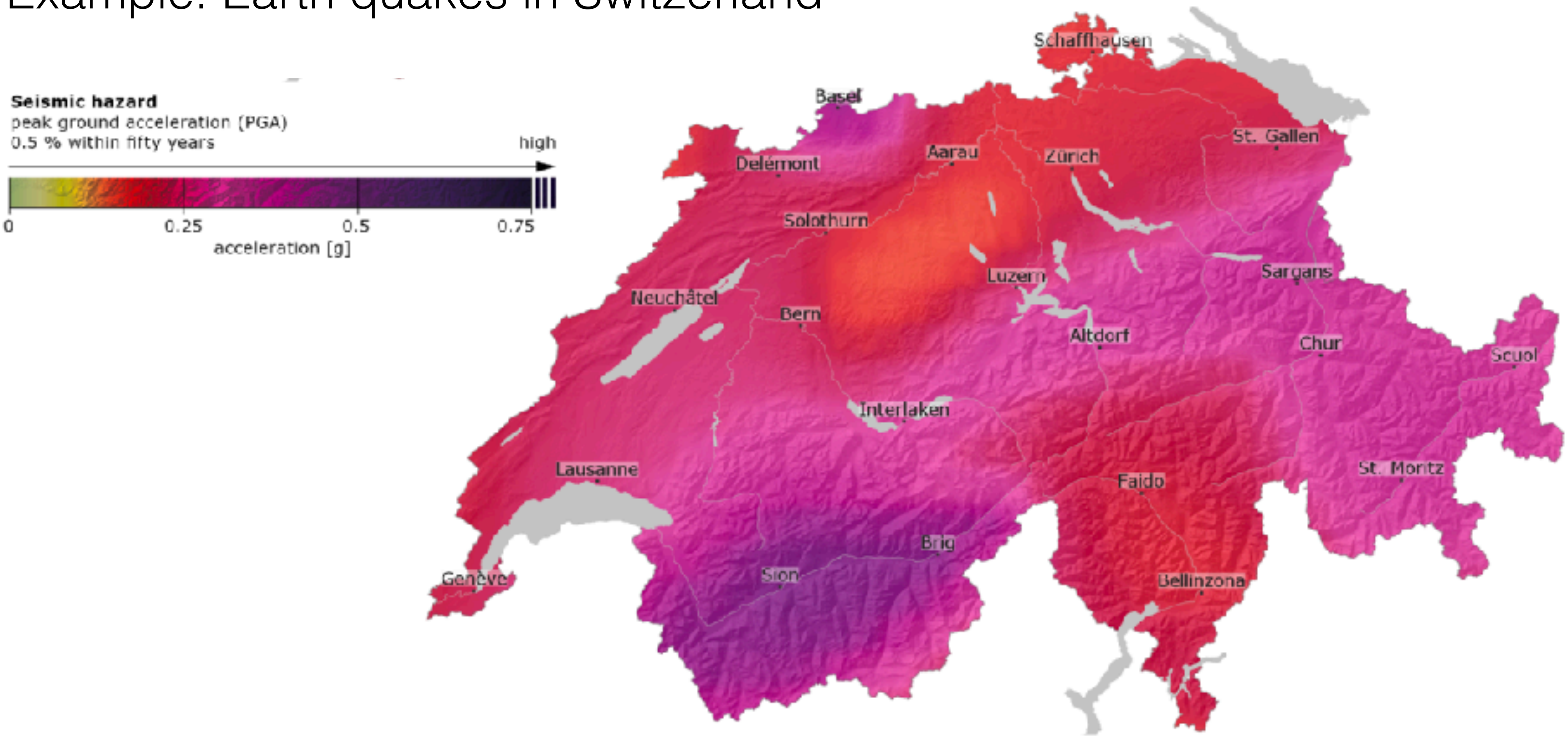
Alice's bit string	1	0	1	0	0	1	1	1	0	1	0	1	1	0	0
Alice's random basis								Rectilinear							
Photons Alice sends	↕	↔	↕	↔	↔	↕	↕	↕	↔	↕	↔	↕	↕	↔	↔
Bob's random bases	R	D	D	D	R	R	D	R	R	D	R	R	D	D	R
Bob's rectilinear table	1					1					0				0
Bob's diagonal table		0		1						1			0		
Bob's guess								'Rectilinear'							
Alice's reply								'You win'							
Alice sends her original bit string to certify	'1	0	1	0	0	1	1	1	0	1	0	1	1	0	0'
Bob's rectilinear table	1					1					0				0
Bob's diagonal table		0		1						1			0		

From Bennett and Brassard, Quantum cryptography: Public key distribution and coin tossing (1984)

Note: This risk cannot be reduced to zero.

Risks can have different levels of severeness

Example: Earth quakes in Switzerland



Operational meaning:

The probability of experiencing this is 0.5 % within fifty years.

Epsilon-security is “all or nothing”

Certificate

Any key generated by this device is secure, except with probability

$$\varepsilon = 10^{-8}$$

METAS
Federal Office
of Metrology

Epsilon-security is common in engineering

Certificate

A DBA does not occur,
except with probability

$$\varepsilon = 10^{-6}$$

per year.

METAS
Federal Office
of Metrology

Note: epsilon cannot be reduced to zero.

Epsilon-security is common in engineering

RSA SECURITY™

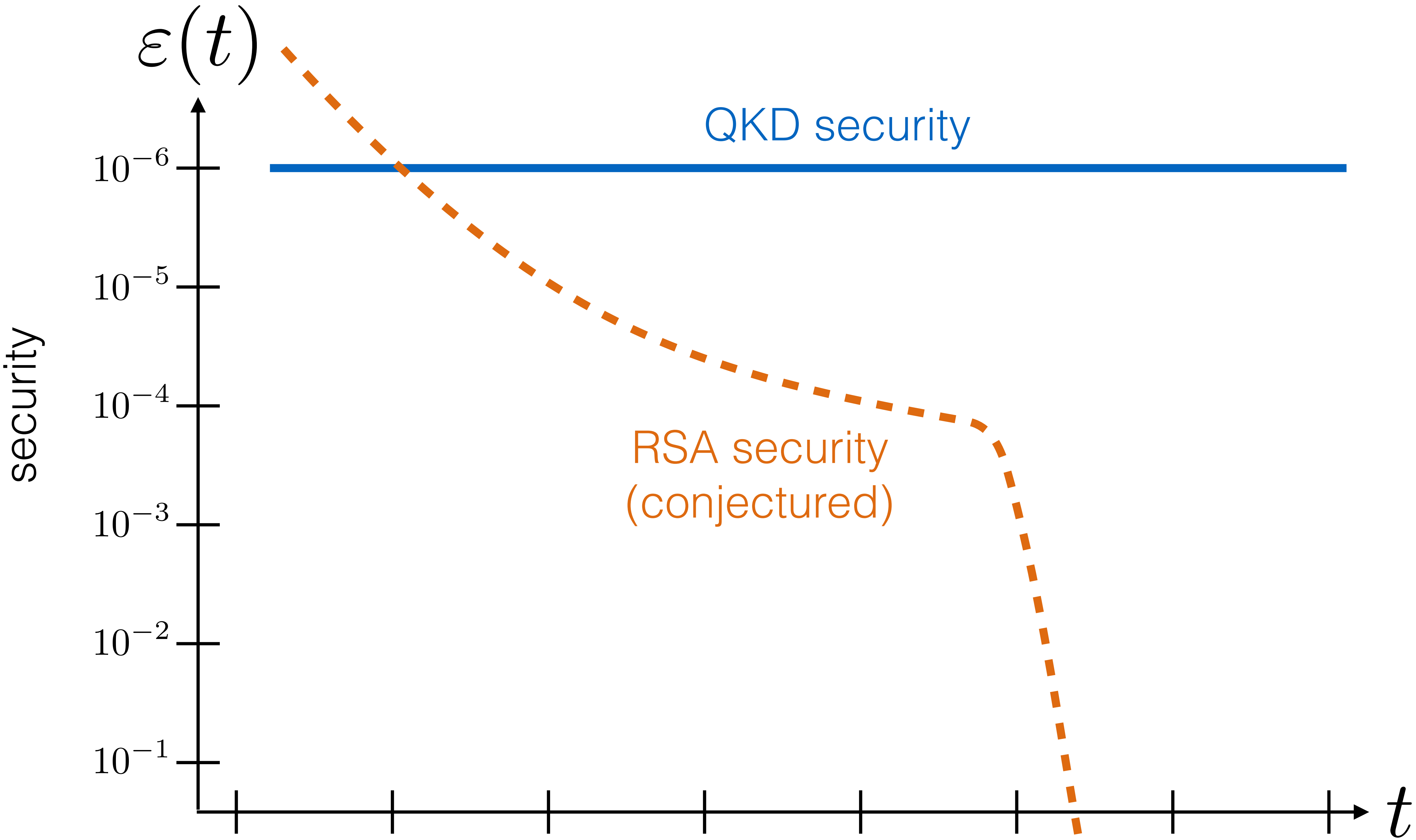
Certificate

The keys generated by RSA remain secure for time t, except with probability

$$\varepsilon(t)$$

which is related to the probability that large numbers can be factored in time $\mathrm{poly}(t)$.

Quantum versus computational cryptography



How is epsilon defined?

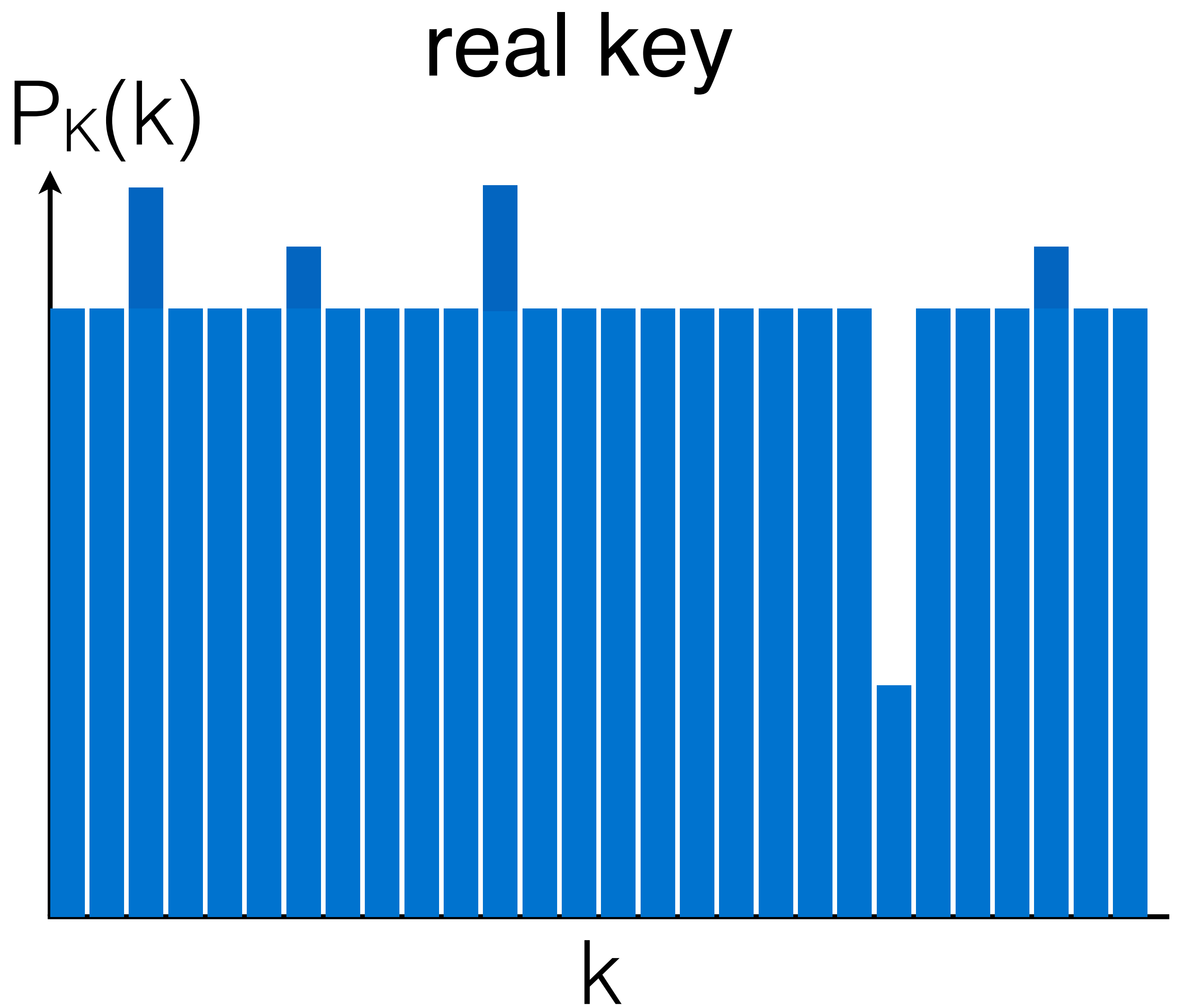
Certificate

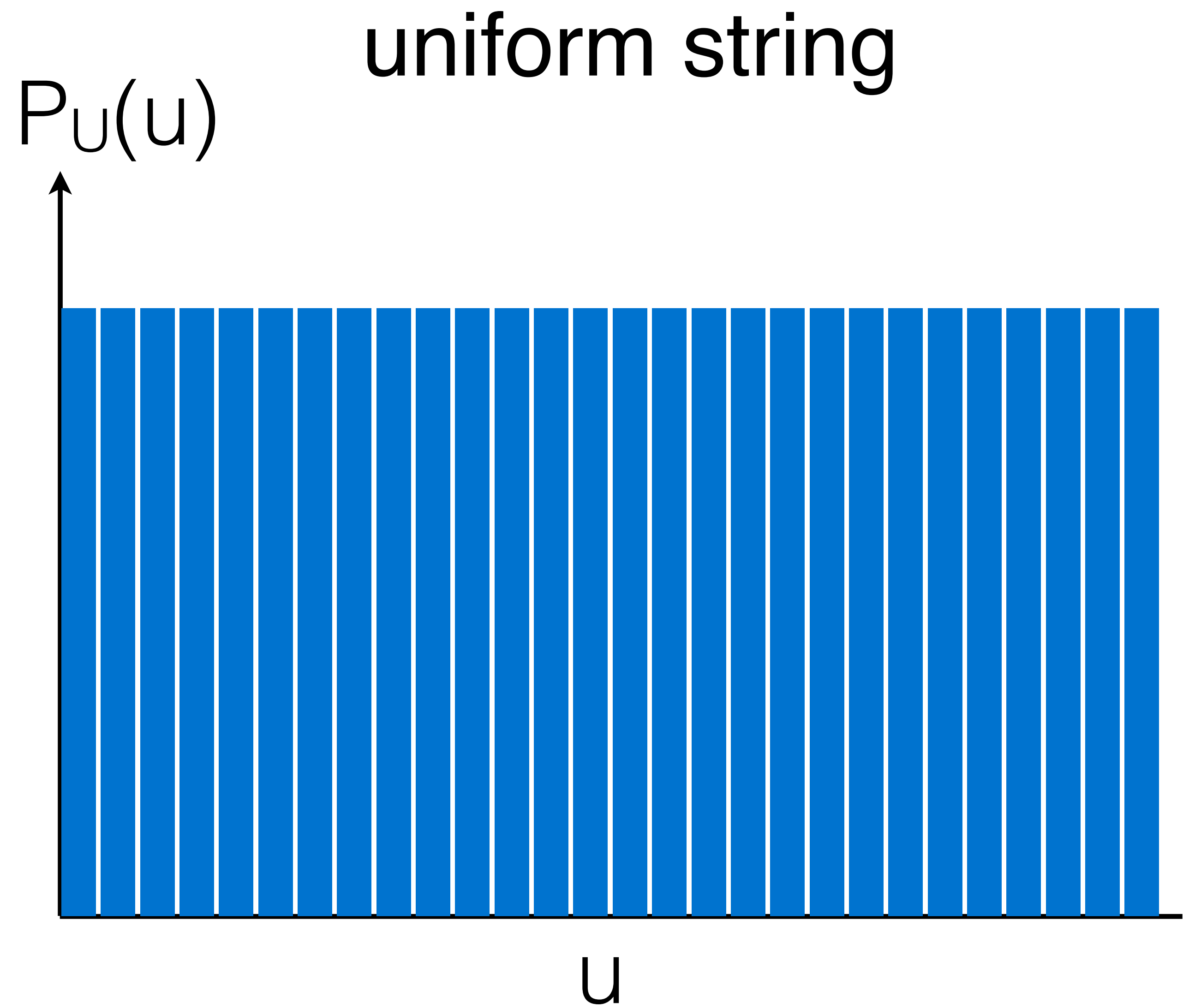
The keys generated by this device have security

$$\varepsilon = 10^{-8}$$

METAS
Federal Office of Metrology

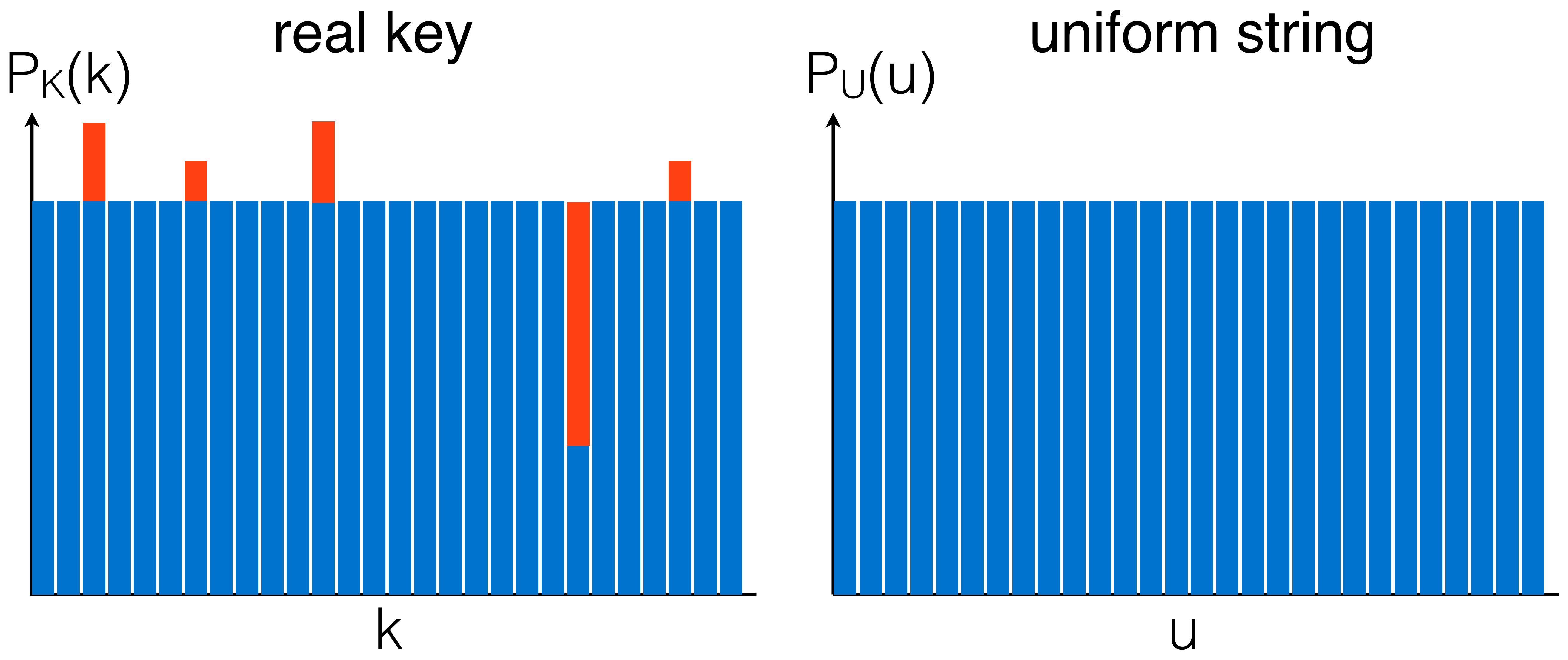
Technical definition (without Eve)





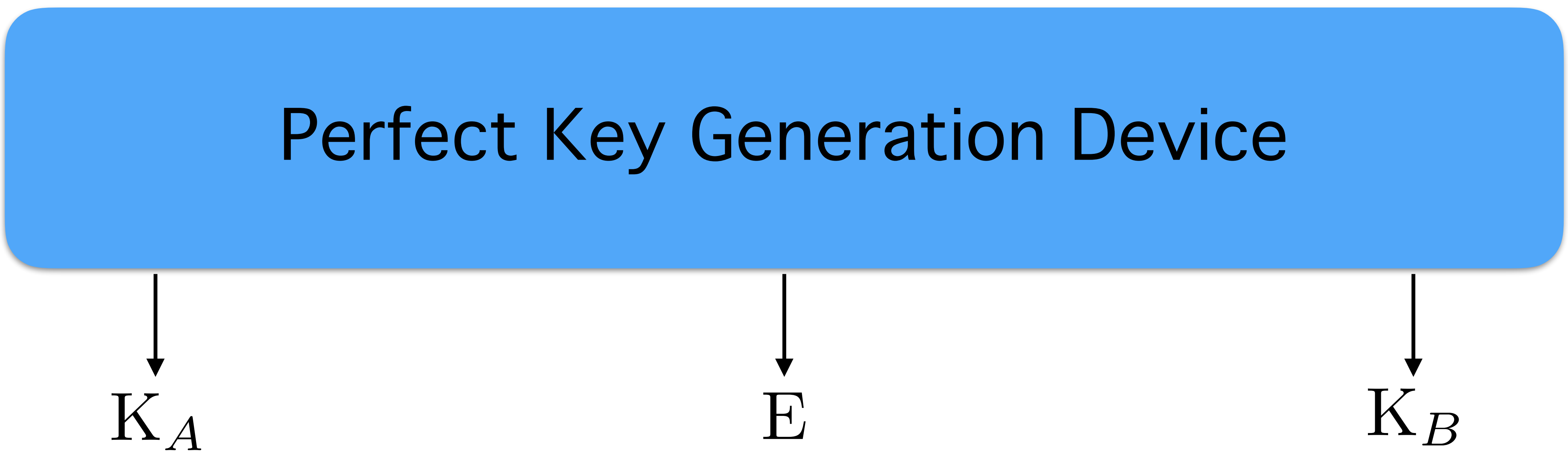
ε Trace distance between probability distribution of real key K and uniformly distributed string U.

Technical definition (without Eve)



ε corresponds to weight of red area.

Real world / ideal world paradigm

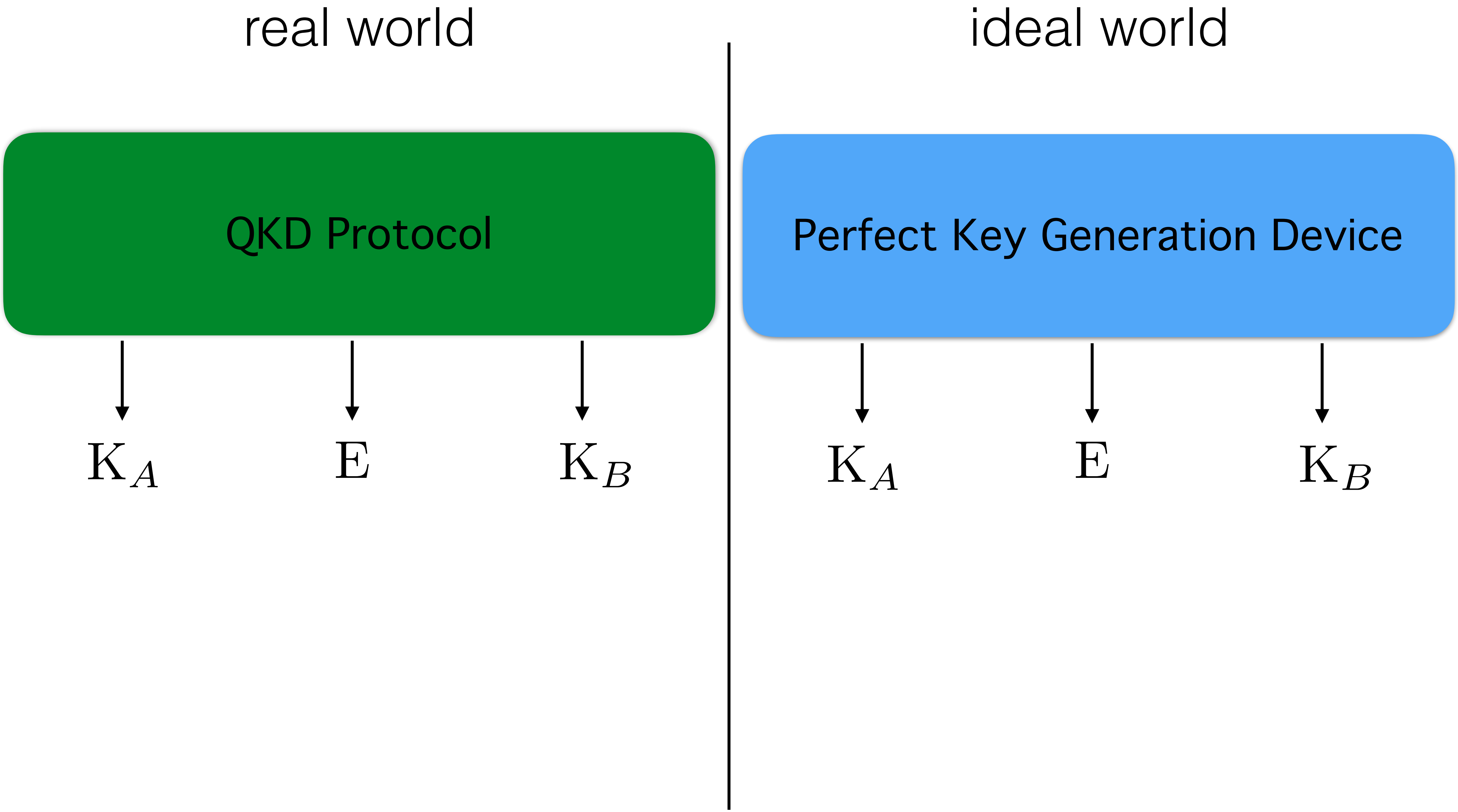


Requirements

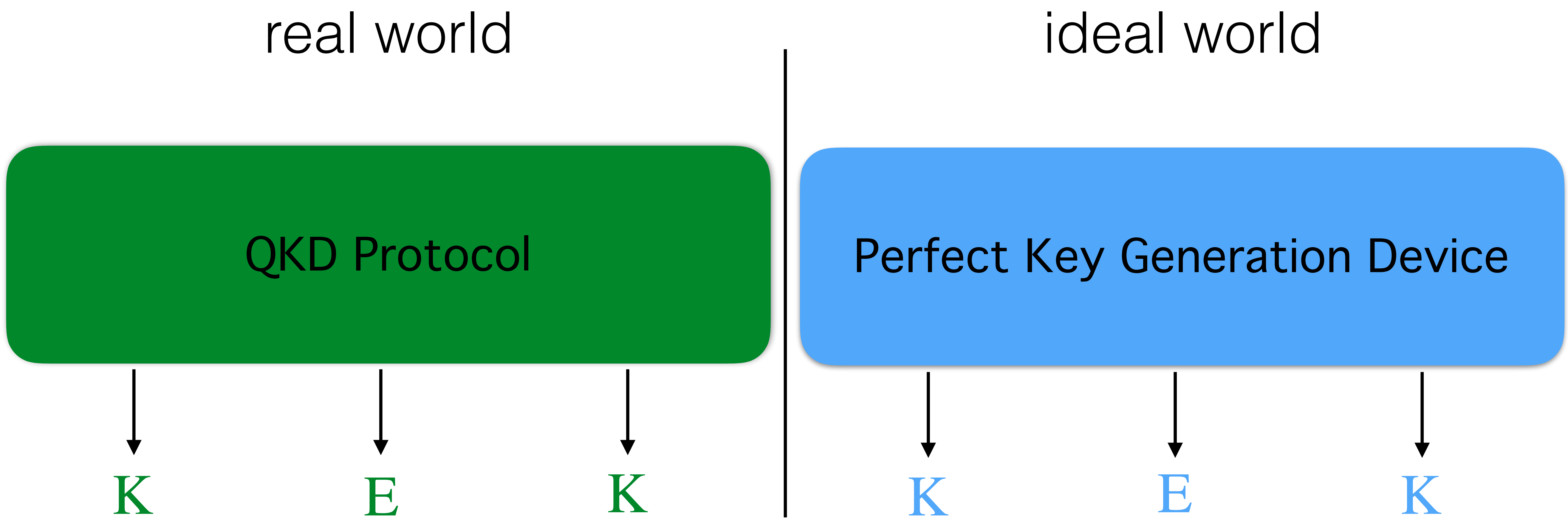
Correctness: $K_A = K_B = K$

Secrecy: K uniformly distributed and independent of E

Real world / ideal world paradigm

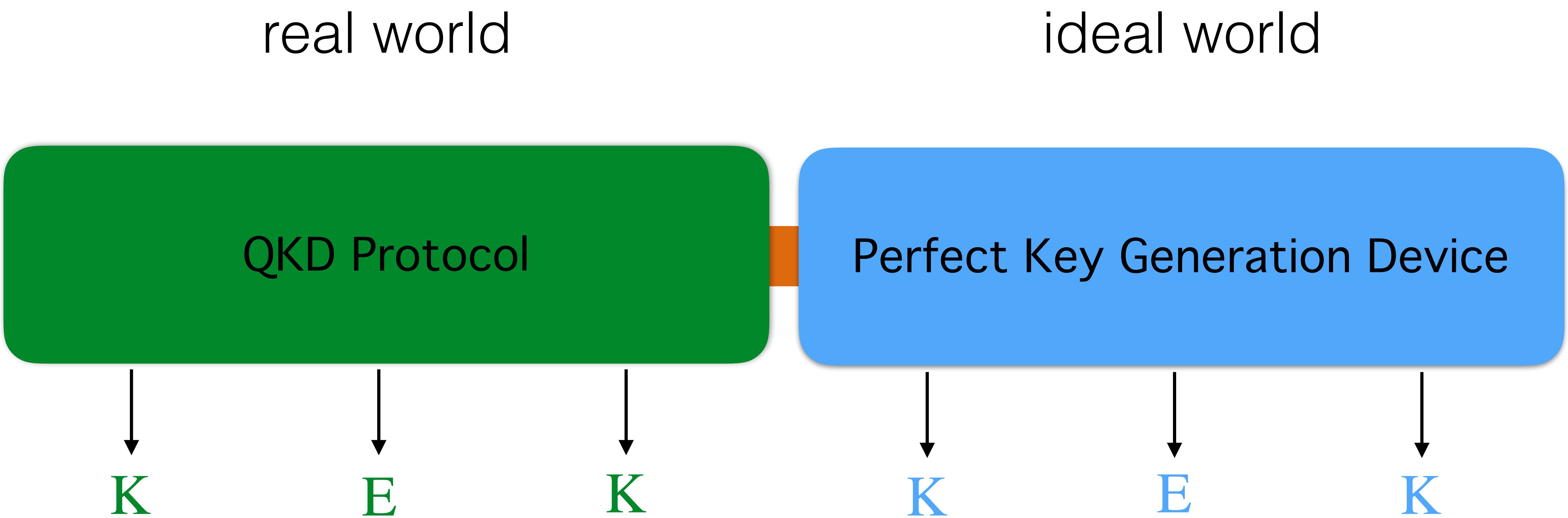


Real world / ideal world paradigm



Definition: The Protocol is ε-secure if P_{KE} and P_{KE} have trace distance ε from each other.

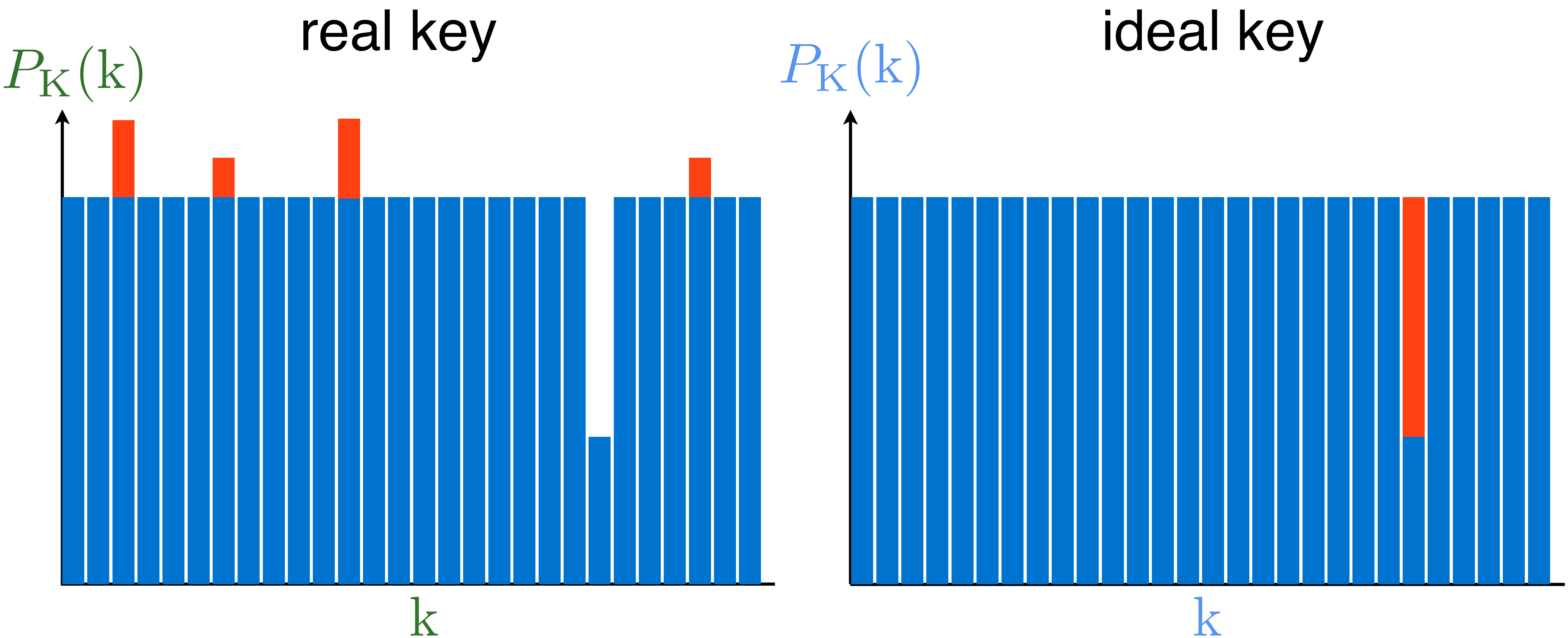
What does epsilon mean operationally?



Theorem: If the Protocol is ε-secure then there exists a joint distribution such that, with probability at least $1-\varepsilon$,

K = K and E = E

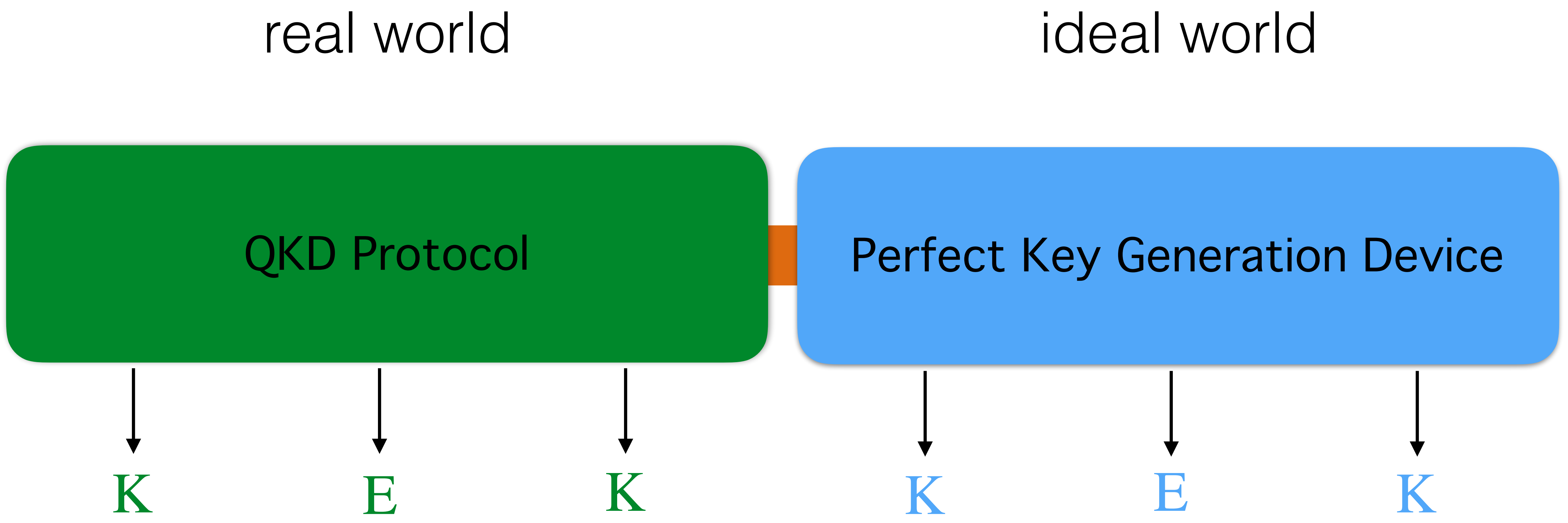
Proof idea



Recall: Red area corresponds to trace distance ε.

Idea: Define $\mathrm{K} = \mathrm{K}$, except when red.

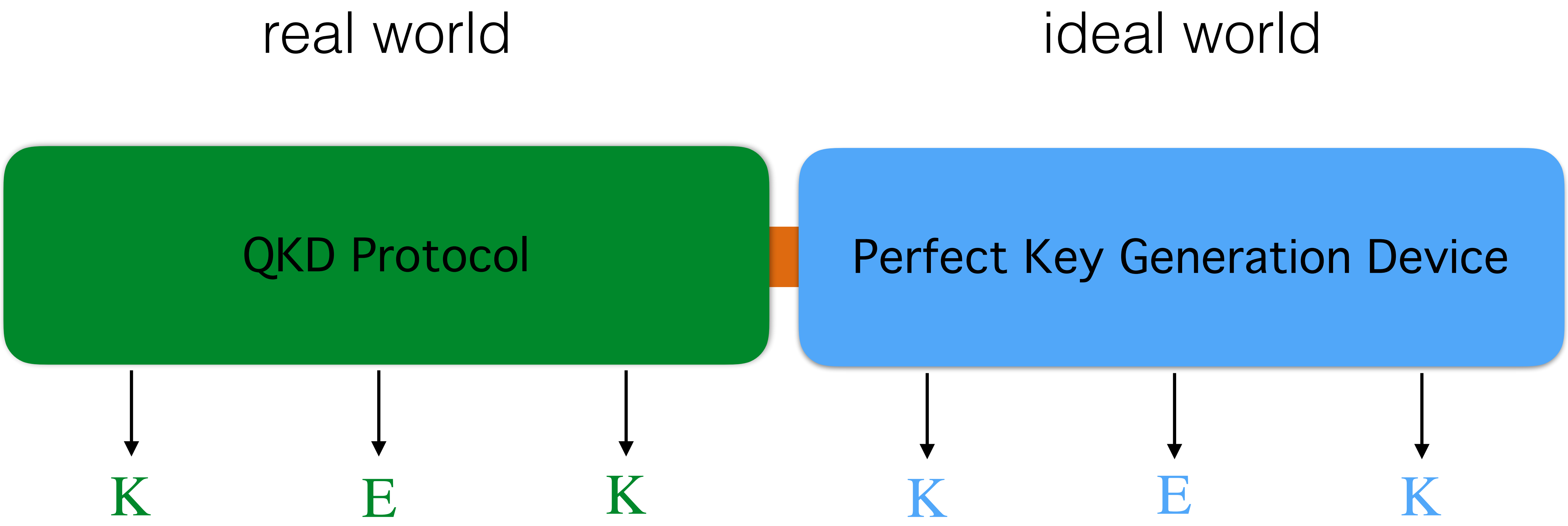
What does epsilon mean operationally?



Theorem: If the Protocol is ε-secure then there exists a joint distribution such that, with probability at least $1 - \varepsilon$,

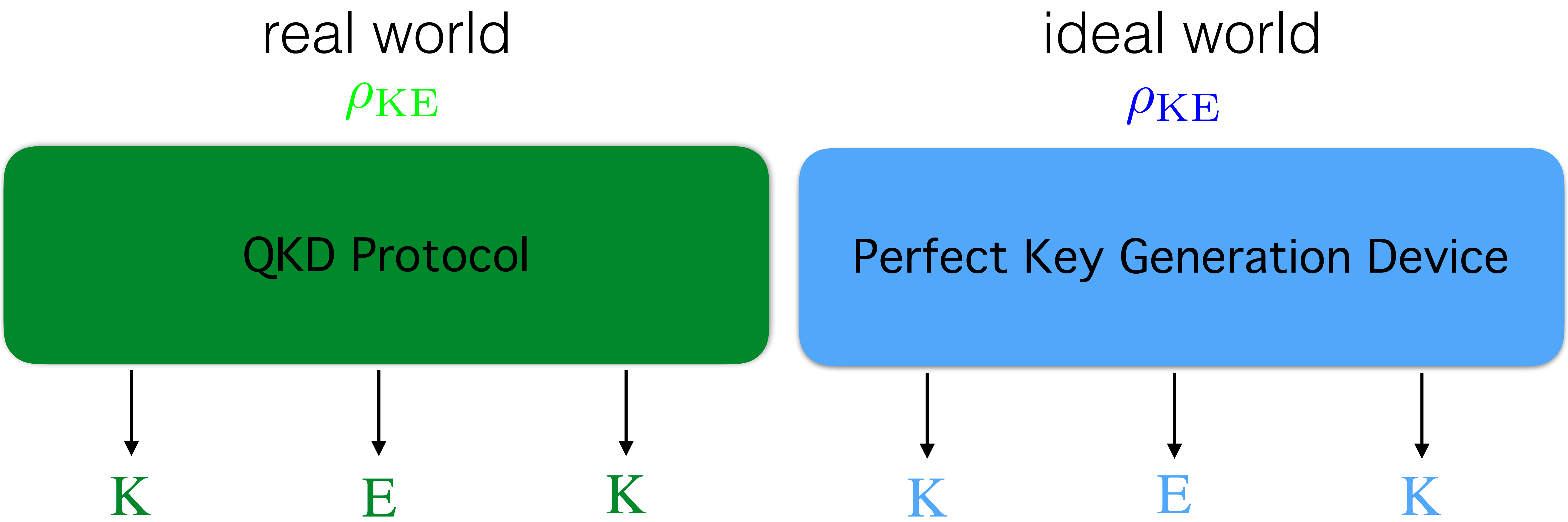
K = K and E = E

What does epsilon mean operationally?



Interpretation: If the Protocol is ε-secure then the probability that it behaves differently from a perfect device is at most ε.

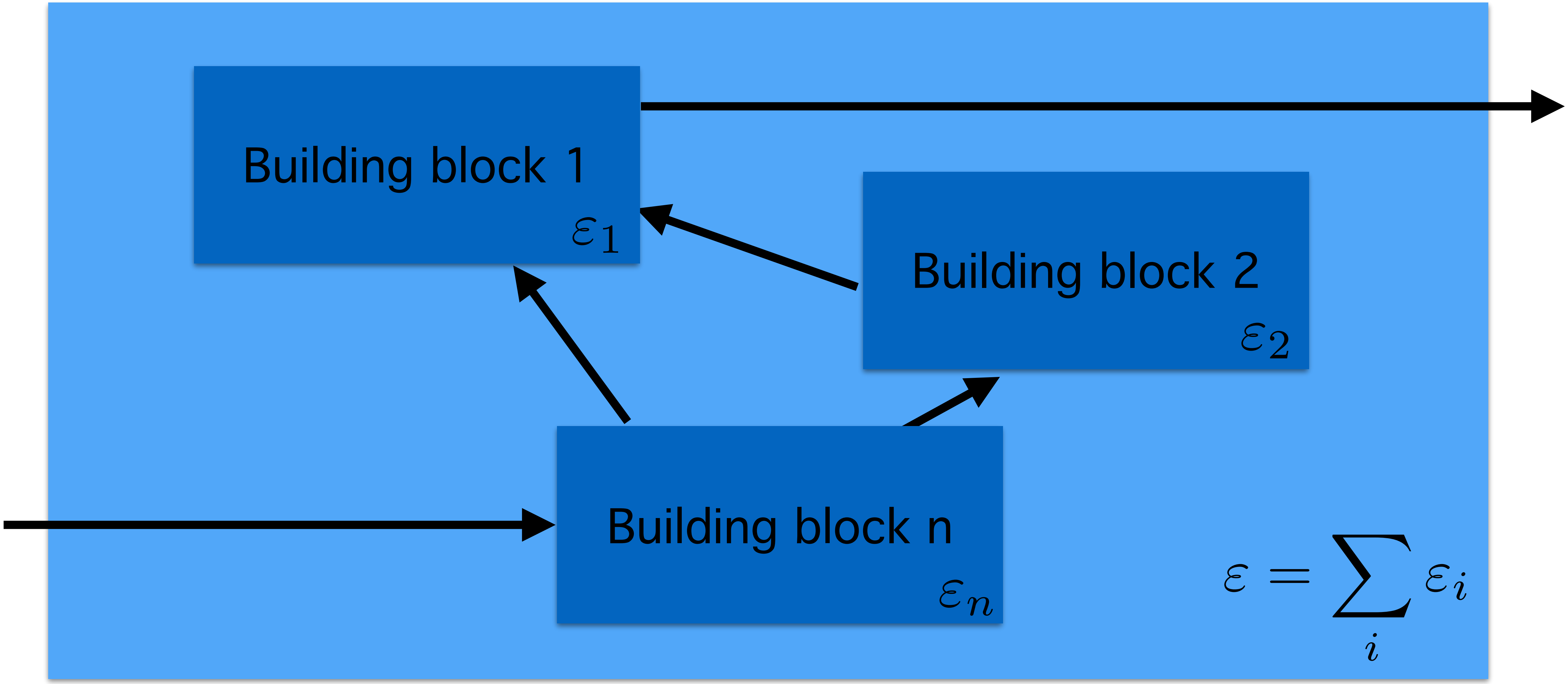
Quantum version



Theorem: If the Protocol is ε-secure then there exists a state ρ_{KE} and events Ω and Ω with probability $1-\varepsilon$ s.t.

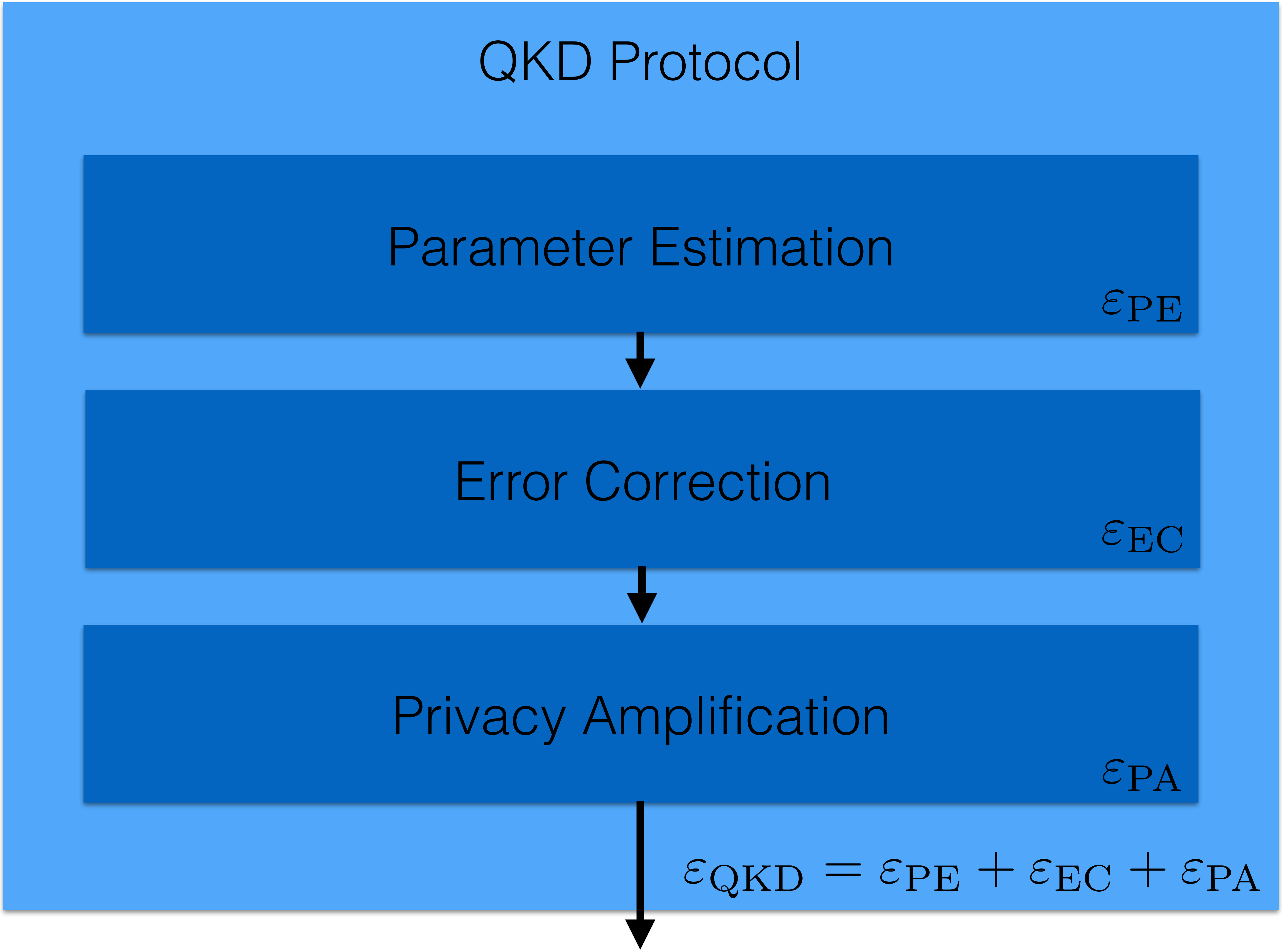
$$\rho_{\mathrm{KE}|\Omega} = \rho_{\mathrm{KE}} \quad \text{and} \quad \rho_{\mathrm{KE}|\Omega} = \rho_{\mathrm{KE}}$$

Composability: Summation rule



Epsilons add up (because failure probabilities add up).

Contributions to epsilon



Example: Privacy Amplification

raw key with min-entropy at least h

↓

Privacy Amplification

↓

final n-bit key

Theorem: Given a raw key with min-entropy at least equal to h, the n-bit key is uniform, except with probability

$$\varepsilon_{\mathrm{PA}} = 2^{-\frac{1}{2}(h-n)}$$

How to choose epsilon?

failure probability per key generated	$\varepsilon = 10^{-12}$ (recommended value)	$\varepsilon = 2 \cdot 10^{-5}$	failure probability per year
number of keys generated	$N = 10^9$	$N = 50$	number of years in operation
upper bound on failure	$p_{fail} = 1/1000$	$p_{fail} = 1/1000$	upper bound on failure

Summary

$$\varepsilon > 0$$

- Security is always finite.
- It is therefore crucial to understand how to quantify it.

Questions?

$$\varepsilon > 0$$