Quantum Key Distribution Platform and Its Applications

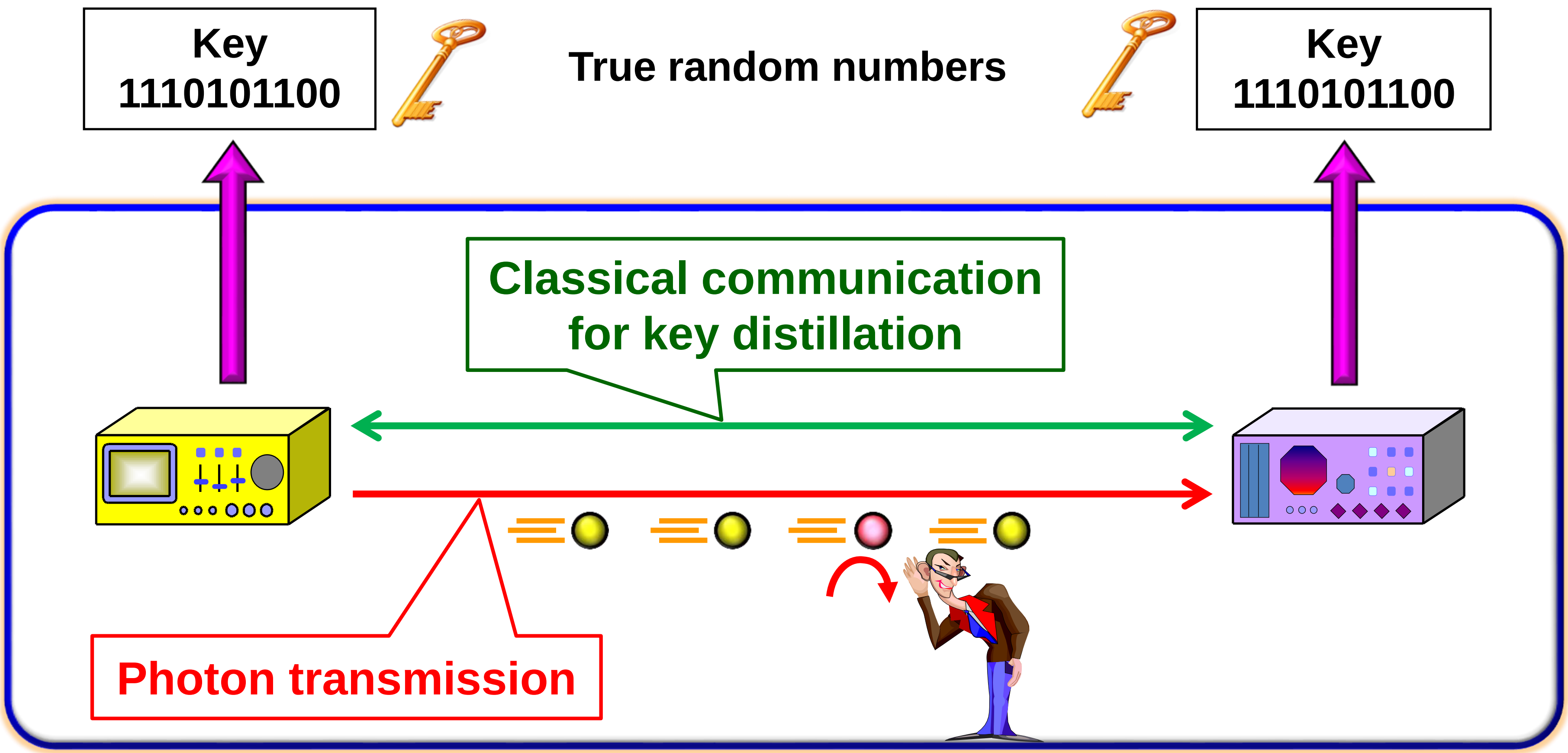
Masahide Sasaki

独立行政法人 情報通信研究機構

Quantum ICT Laboratory
Email: psasaki@nict.go.jp, Tel: 042-327-6524

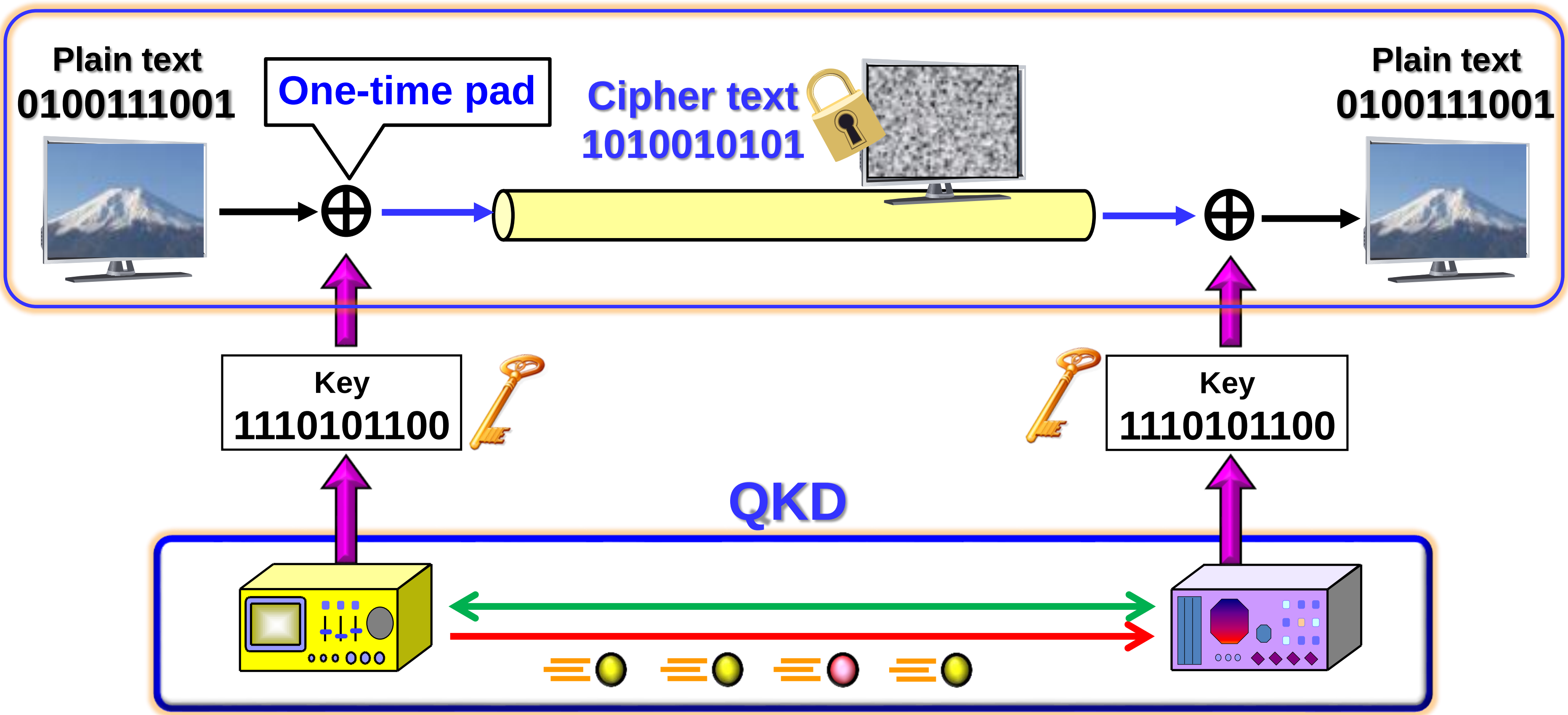
Quantum key distribution (QKD)

- A scheme to share a symmetric key
- Quantum safe;
  Security is based not on the difficulty of mathematical problems but on **the laws of physics**



Quantum cryptography

Mathematically proven to be completely secure,
“unbreakable by any means that can occur even in future”



QKD

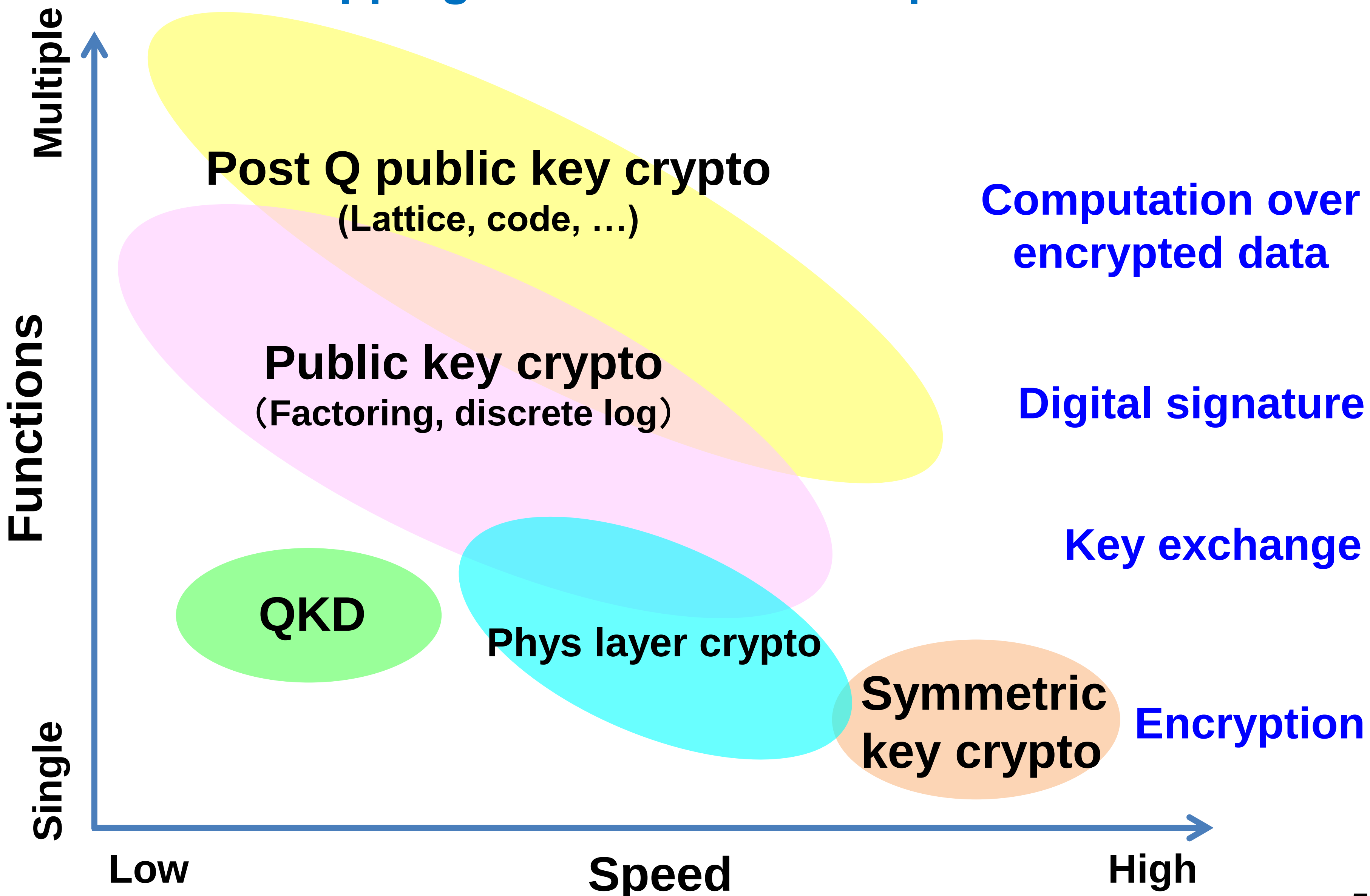
- It protects security of data transmission
- It works in a point-to-point link, not in a multi-party link
- Speed and distance of a direct link are limited

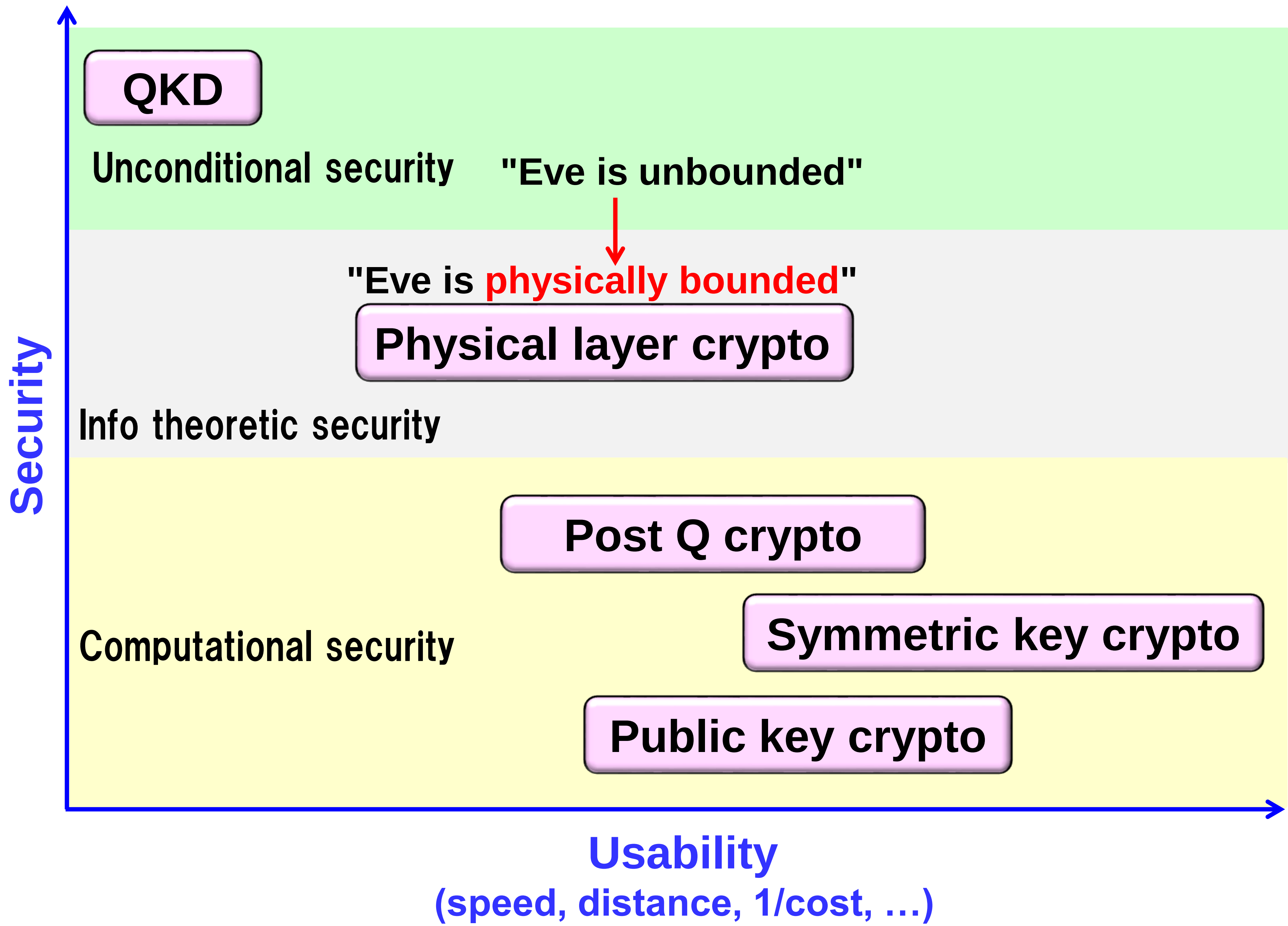
  1M bits/s at 50km (Movie data, e.g. MPEG4)
  1k bits/s at 100km (Voice data)
  (for standard optical fiber with loss rate of 0.2dB/km)

- Networking is made by introducing the trusted nodes, and by relaying a key via the nodes

Cryptographic technologies

Mapping in “Functions vs Speed”




QKD
Unconditional security
"Eve is unbounded"
"Eve is physically bounded"
Physical layer crypto
Info theoretic security
Post Q crypto
Symmetric key crypto
Computational security
Public key crypto
Security
Usability
(speed, distance, 1/cost, …)

Contents

Network security

Crypto technologies in a network layer stack

Physical layer security

- Secrecy message transmission
- Secret key agreement
- Quantum key distribution

“Theoretical framework”

“Implementation and use cases”

Summary

“Perspectives”

Network security

L7	Application layer
L6	Presentation layer
L5	Session layer
L4	Transport layer
L3	Network layer
L2	Data layer
L1	Physical layer

SSL/TLS

IPsec

- Authentication
- Signature
- Key exchange
- Encryption

Data-transmission, processing, storage

Algorithmic cryptography

- Public key crypto
- Symmetric key crypto
- Hash function

....

Computational security

Network security

L7	Application layer
L6	Presentation layer
L5	Session layer
L4	Transport layer
L3	Network layer
L2	Data layer
L1	Physical layer

- Secrecy message transmission
- Secret key agreement

Physical layer cryptography

QKD

- Key exchange
- Encryption

Data-transmission

Coding in a physical channel

Information theoretic security

Contents

Network security

Crypto technologies in a network layer stack

Physical layer security

- Secrecy message transmission
- Secret key agreement
- Quantum key distribution

"Theoretical framework"

"Implementation and use cases"

Summary

"Perspectives"

Basic concept of information theoretic security

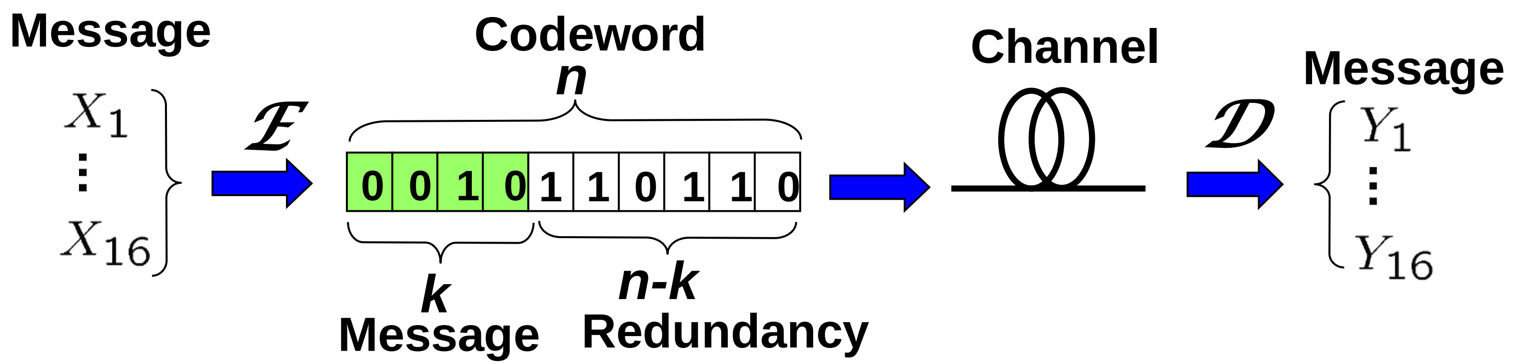
Channel coding

Channel coding

The method to realize error free transmission even when the channel is lossy and noisy.

⇓

Add *redundancy* to protect message from noise.



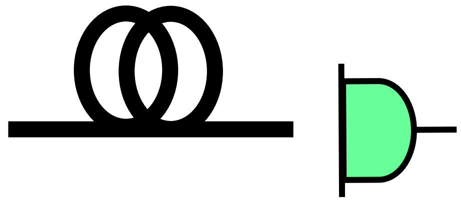
$$R = \frac{k}{n} \quad > \quad C \quad \Rightarrow \quad Pe \not\to 0$$

Transmission rate | **Channel capacity** | **Decoding error**

Shannon, 1948

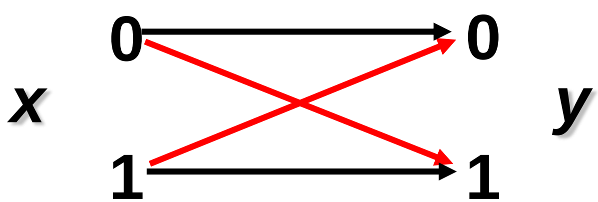
Channel capacity (Shannon, 1948)

… 0 0 1 0 1 1 0 1 1 0 …



… 0 1 1 0 1 0 0 1 1 0 …

$P(x)$



Channel matrix $P(y|x)$

Mutual information

$$I(X:Y) \equiv \sum_{x,y} P(x)P(y|x) \log_2 \frac{P(y|x)}{\sum_{x'} P(y|x')P(x')}$$

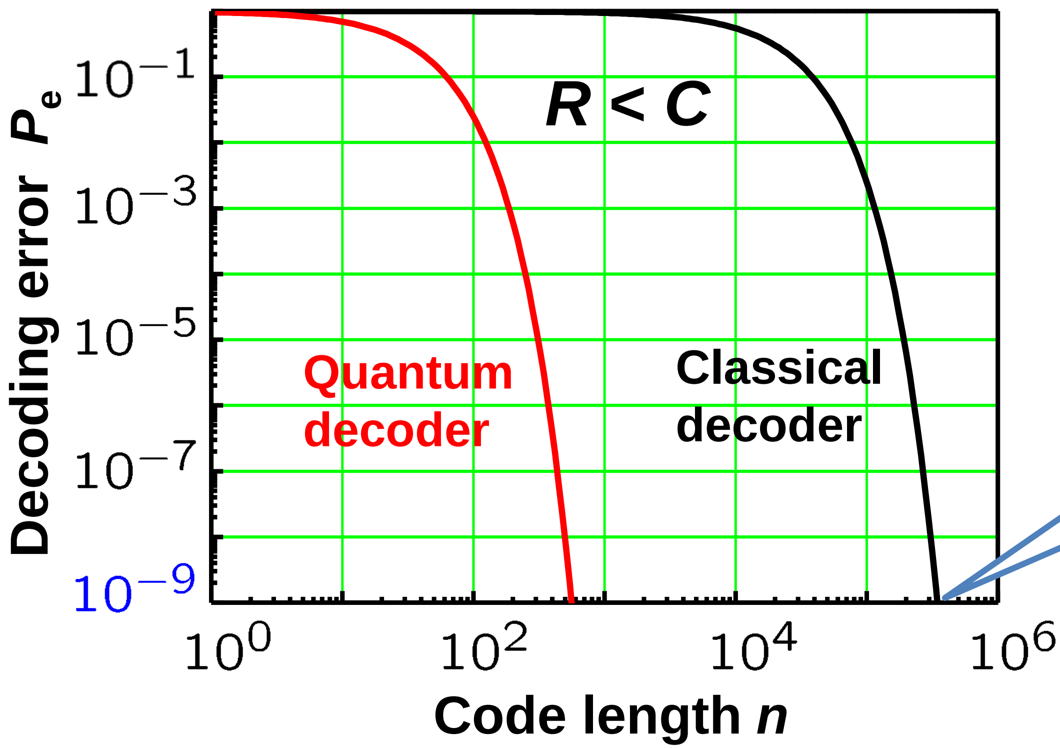
Channel capacity $C = \max_{P(x)} I(X;Y)$

The capacity alone gives only the asymptotic rate at $n \to \infty$

A stronger characterization is given by the reliability function.

$$P_e \leq e^{-nE(R)}$$

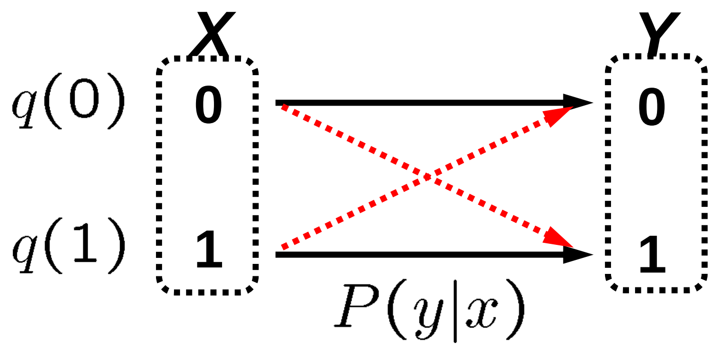
Specify how fast the decoding error decreases as code length *n*?



How long code length required to achieve a given level of reliability

Reliability function $E(R)$

R. G. Gallager, *Information Theory and Reliable Communication* (John Wiley & Sons, New York, 1968).



$$E_0(\rho, \boldsymbol{q}) \equiv -\log\left[\sum_y \left(\sum_x q(x)P(y|x)^{\frac{1}{1+\rho}}\right)^{1+\rho}\right]$$

Gallager function

Reliability function

$$\boxed{E(R) = \sup_{0\le\rho\le1} \sup_{\boldsymbol{q}} \left[E_0(\rho, \boldsymbol{q}) - \rho R\right]}$$

$$R = \frac{k}{n}$$

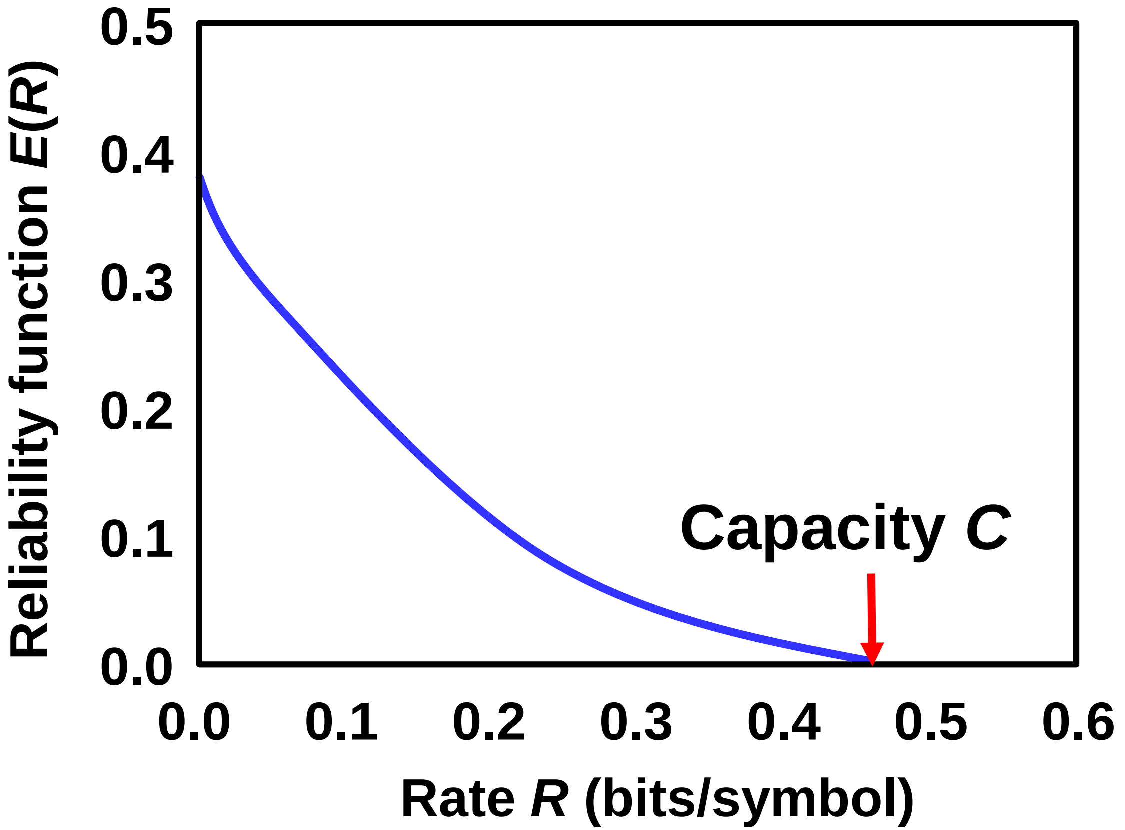
Function of a rate *R*, depending only on $P(y|x)$

Coding theorem

$R < C \Rightarrow E(R) > 0$

$\Rightarrow P_e < \exp[-n\, E(R)]$

There exists a code which can decrease the decoding error exponentially as code length *n* increases.



Converse theorem ⇔ Security

$$E_0(\rho, \boldsymbol{q}) \equiv -\log\left[\sum_y \left(\sum_x q(x) P(y|x)^{\frac{1}{1+\rho}}\right)^{1+\rho}\right]$$

Gallager function

Dual quantity to the reliability function

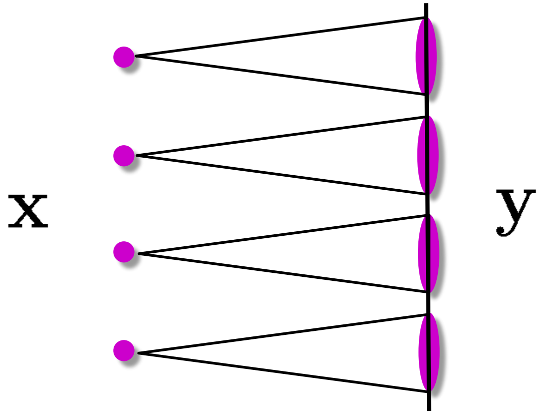
$$E_0(\rho) \equiv \inf_{\boldsymbol{q}} E_0(\rho, \boldsymbol{q})$$

$$E_E(R) = \sup_{-1 \le \rho \le 0} [E_0(\rho) - \rho R]$$

R* > *C ⇨ ***P*$_e$> 1 - exp[-*n* *E*$_E$(*R*)]**

with whatever code, the decoding error approaches the unity exponentially as the code length *n* increases.

$R < C$ ⇨ **Reliable transmission is possible.**

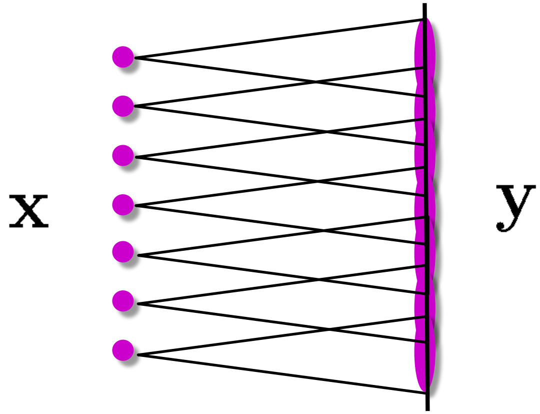


Coding theorem

$$P_e \leq e^{-nE(R)}$$

$$\to 0$$

$R > C$ ⇨ **With whatever code, messages are mostly misread.**



Converse coding theorem

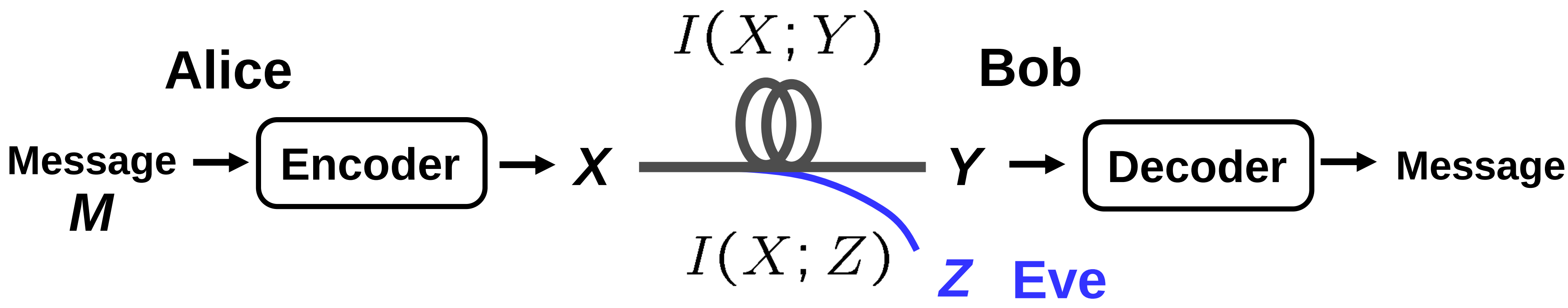
$$P_e \geq 1 - \exp\left[-nE_E(R)\right]$$

$$\to 1$$

Impose this situation on Eve.

The very essence of information theoretic security

Wiretap channel



If Eve's channel is degraded $I(X;Z) < I(X;Y)$

$$I(X;Z) < R < I(X;Y)$$

Message *M* just looks completely random for Eve.

Bob can decode message *M* correctly.

Converse coding theorem

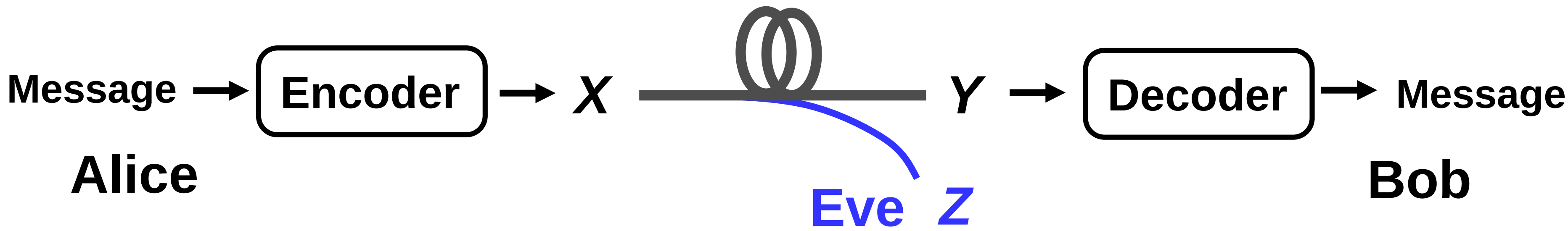
Coding theorem

Secrecy capacity

Wiretap channel

Eve's channel is worse than that of Bob

$$I(X;Z) < I(X;Y)$$



$$C_S = \max_{P_x}[I(X; \ldots ; Z)]$$

There exists a co… …ansmit this amount of bits faithfully r… …ing leaked information to Eve arbitrar… …ll.

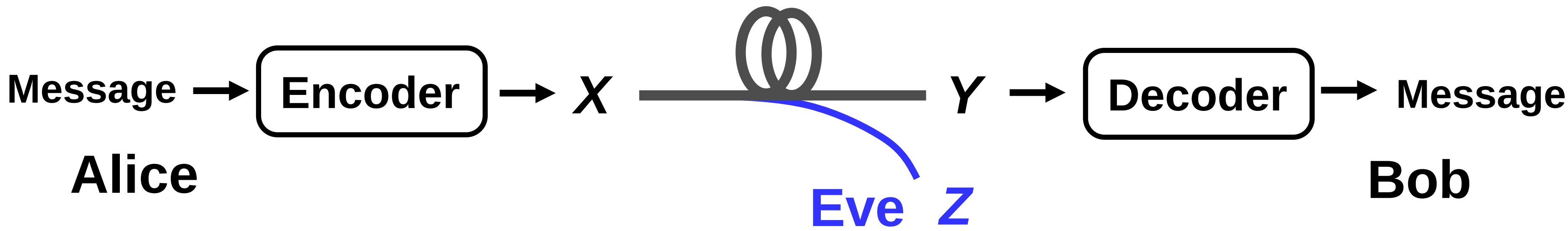
Information theoretic security

Wyner, Bell Syst. Tech. J., 54(8),1355 (1975).
Csiszár and Körner, IEEE Trans. Inf. Theory, IT-24(3), 339 (1978).

Any powerful computers cannot decrypt messages sent by such a wiretap channel code

Eve's channel is worse than that of Bob

$(\mathrm{SNR})_{\text{Alice-Bob}} > (\mathrm{SNR})_{\text{Alice-Eve}}$



$$C_S = \max_{P_x}[I(X;Y \ldots ;Z)]$$

There exists a co… …ansmit this amount of bits faithfully … …ing leaked information to Eve arbitrar… …ll.

Information theoretic security

Wyner, Bell Syst. Tech. J., 54(8),1355 (1975).
Csiszár and Körner, IEEE Trans. Inf. Theory, IT-24(3), 339 (1978).

Contents

Network security

Crypto technologies in a network layer stack

Physical layer security

- Secrecy message transmission
- Secret key agreement
- Quantum key distribution

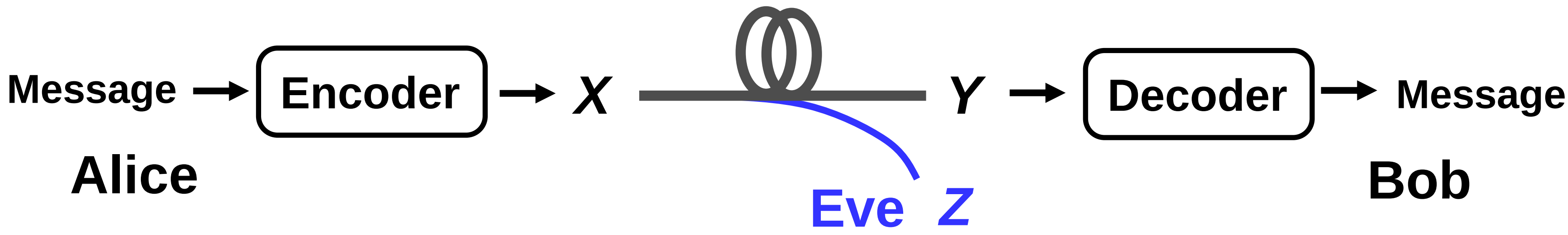
"Theoretical framework"

"Implementation and use cases"

Summary

"Perspectives"

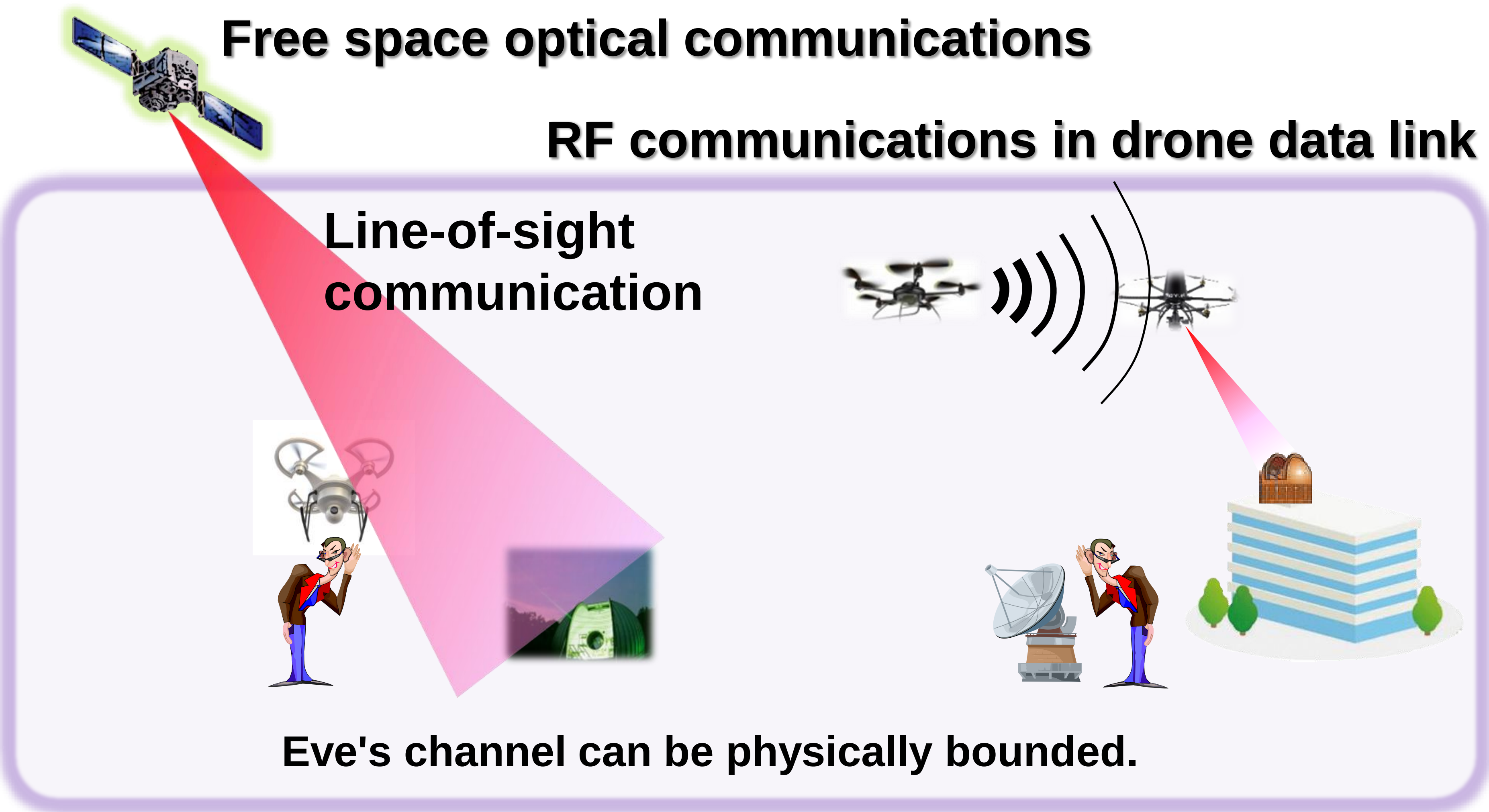
Eve's channel is worse than that of Bob



How can we certify this assumption?

It is generally hard for wired channels.

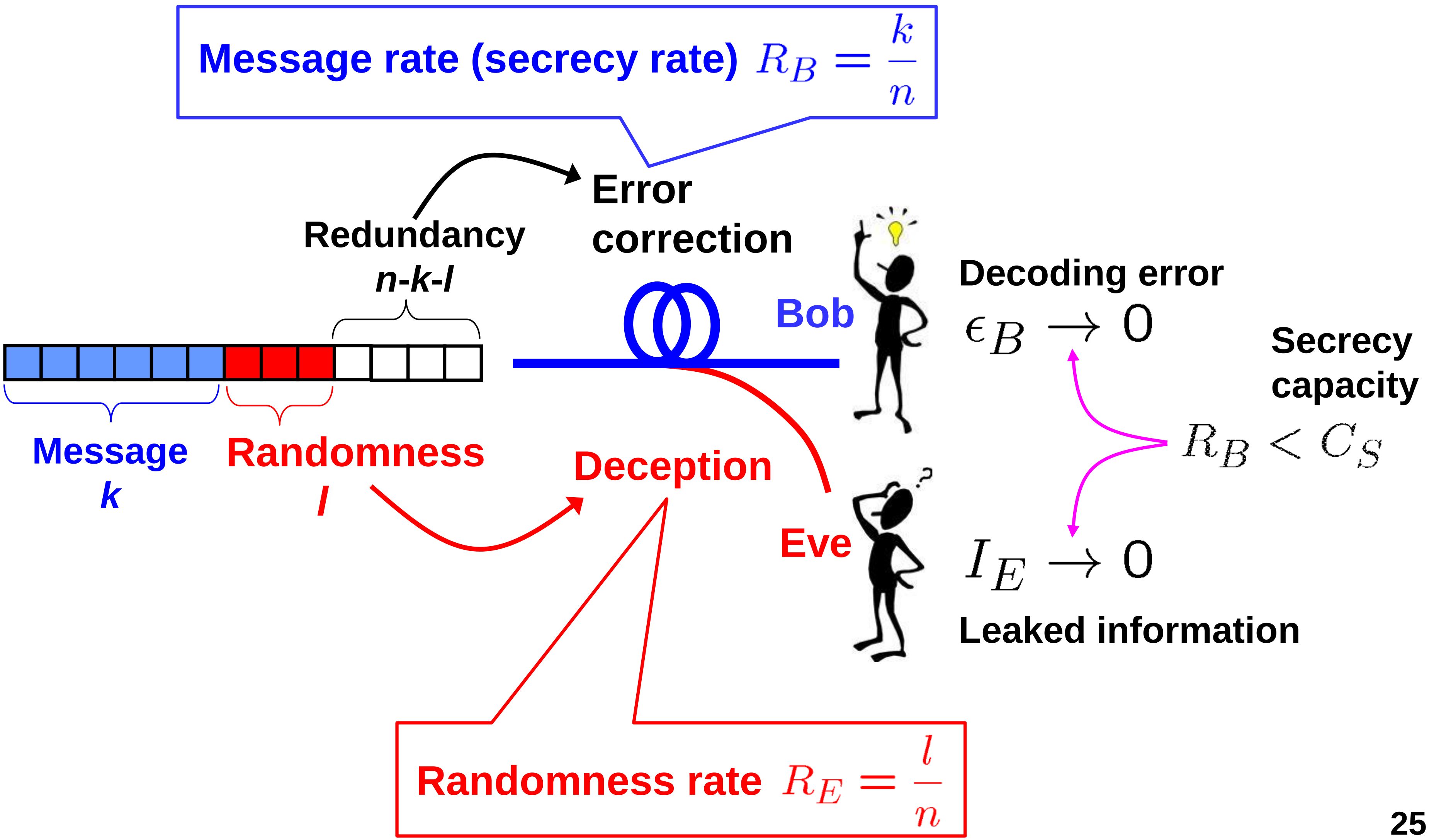
Wireless communications

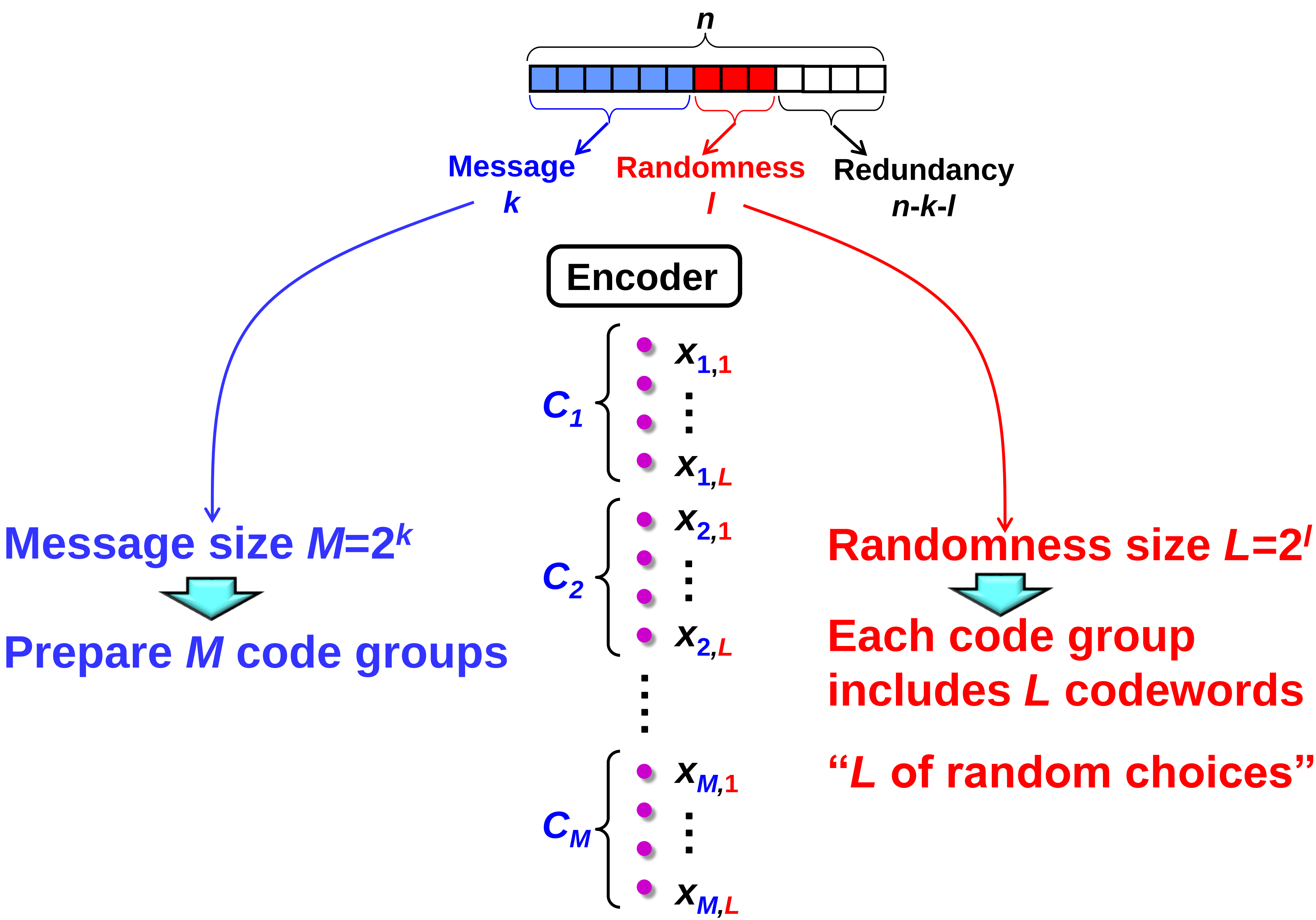


Wireless communications with the information theoretic security

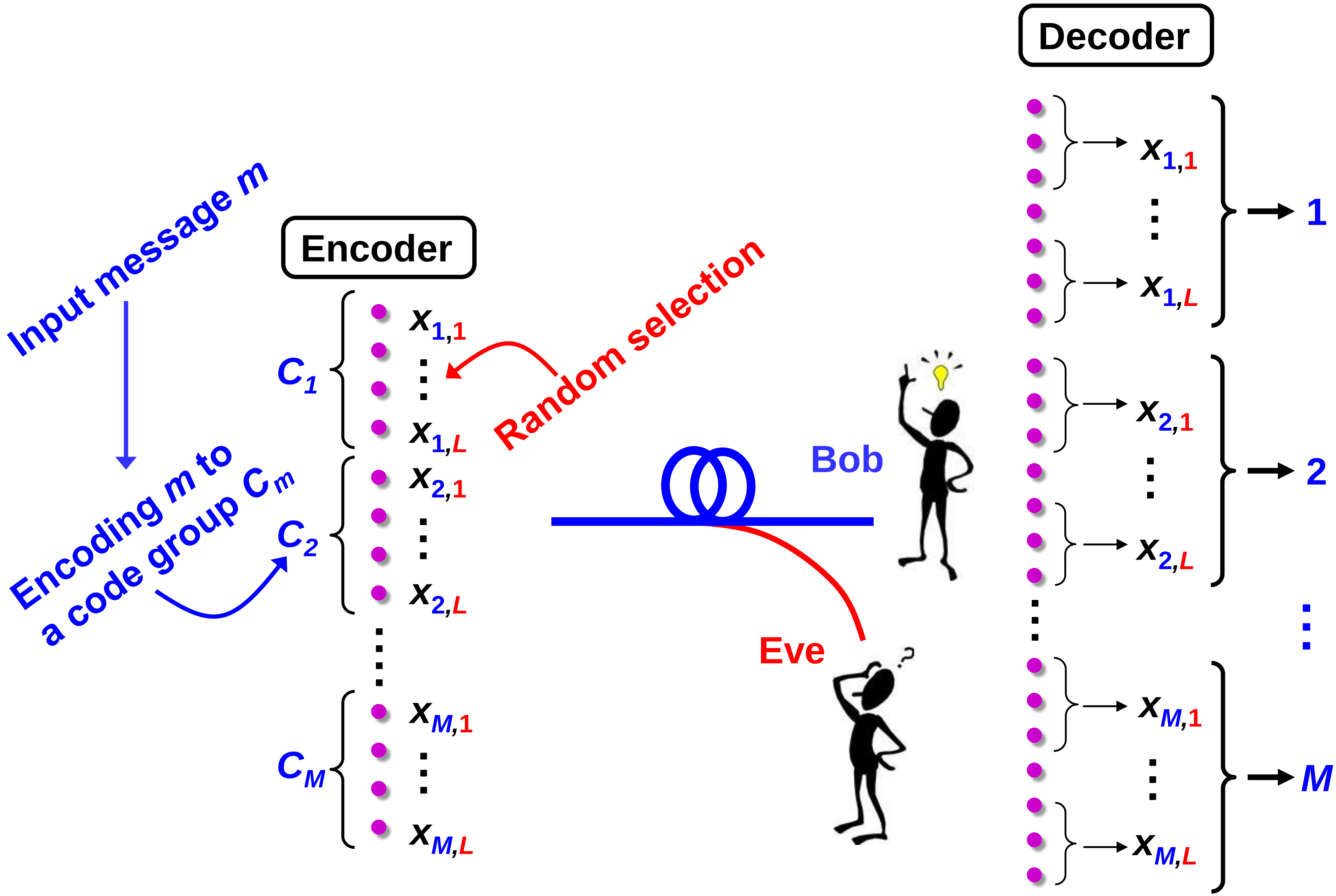
Wiretap channel coding

Add not only redundancy but also randomness.



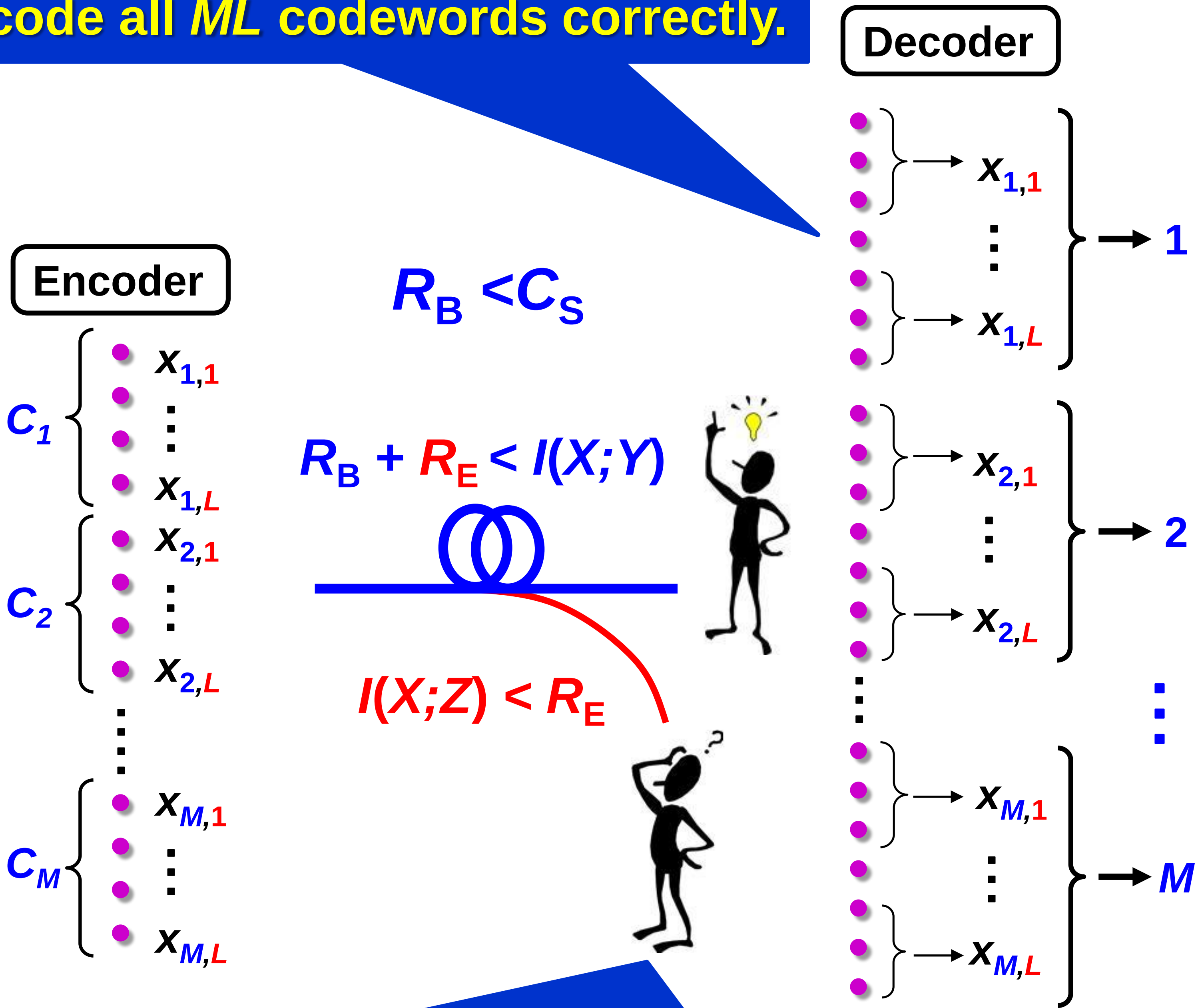


There are totally ML codewords.



Input message m
Encoding m to a code group C_m
Encoder
C_1
C_2
C_M
$x_{1,1}$
$x_{1,L}$
$x_{2,1}$
$x_{2,L}$
$x_{M,1}$
$x_{M,L}$
Random selection
Bob
Eve
Decoder
$x_{1,1}$
$x_{1,L}$
$x_{2,1}$
$x_{2,L}$
$x_{M,1}$
$x_{M,L}$
1
2
M

Bob can decode all *ML* codewords correctly.



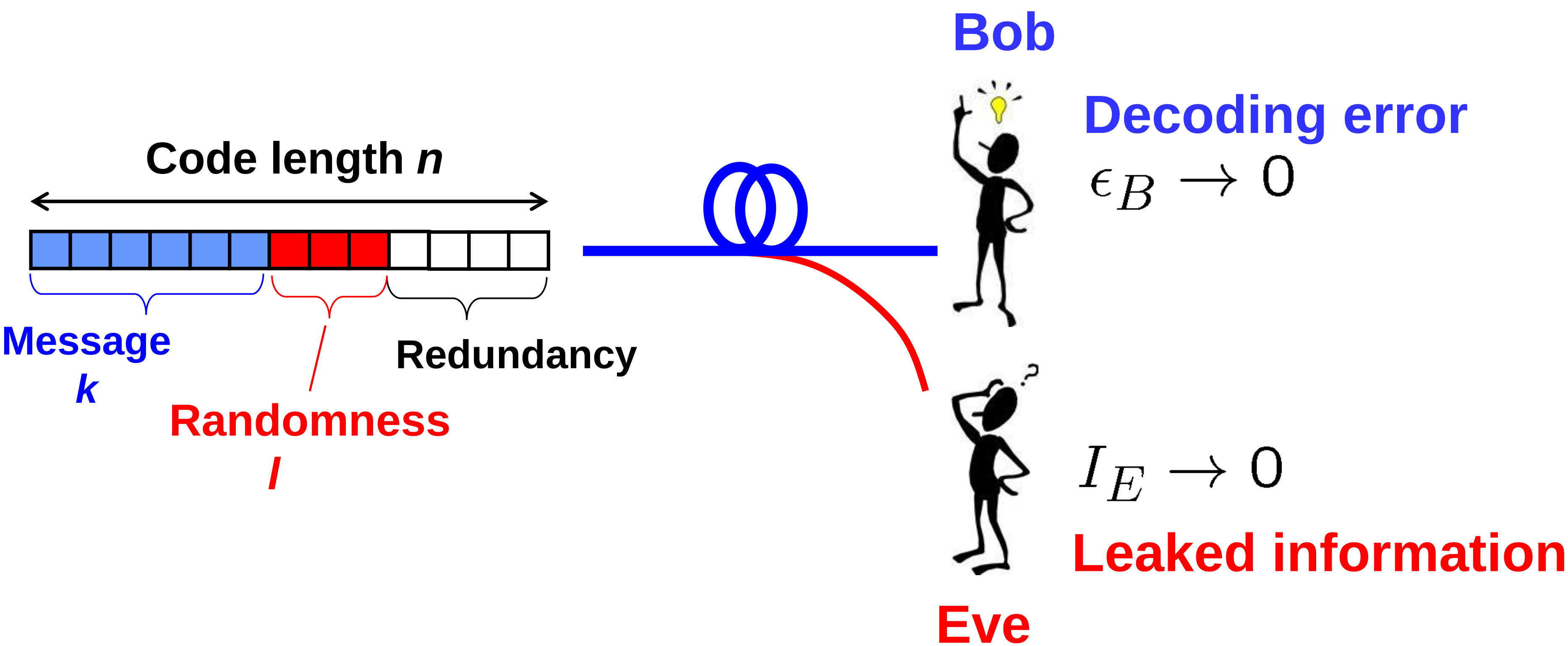
All codewords look completely random for Eve.

Quantification of information theoretic security

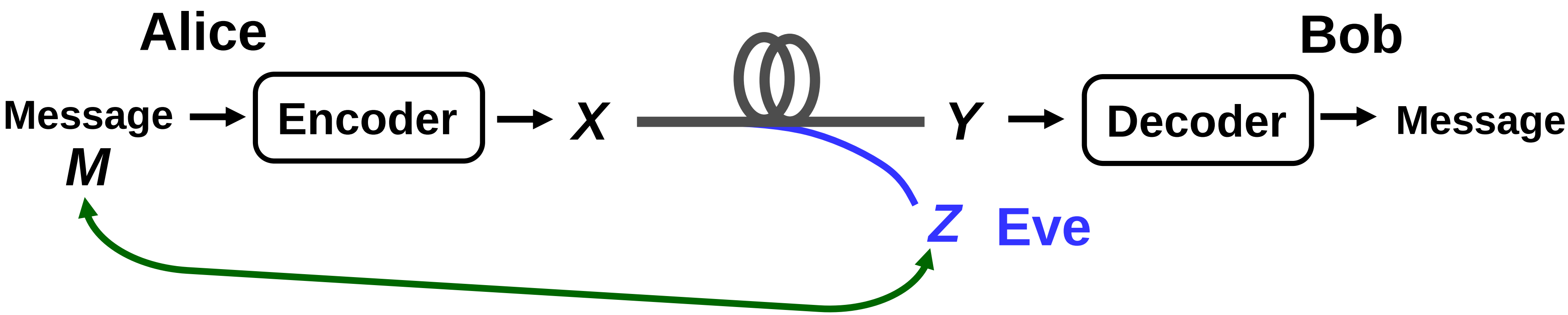
Finite length analysis

Finite length analysis

How fast do the decoding error for Bob and the leaked information against Eve decrease as code length *n* increases?



What kind of measures of leaked information ?



We want statistical independence of *M* and *Z*, and need to measure it.

Stronger

Average mutual information $\frac{1}{n} I_n(M;Z) \to 0$

Variable distance $d(P_{\mathrm{in}}, P_{\mathrm{target}}) = \sum_{m \in \mathcal{M}} |P_{\mathrm{in}}(m) - P_{\mathrm{target}}(m)| \to 0$

Mutual information $I_n(M;Z) \to 0$

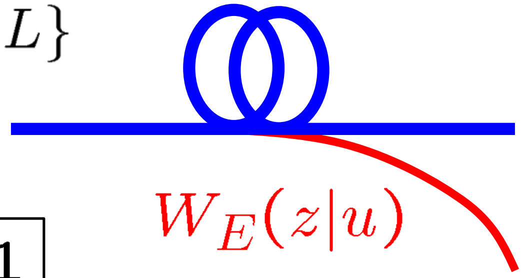
Kullback-Leiber distance $\delta_n^E \equiv \frac{1}{M_n} \sum_{m \in \mathcal{M}_n} D(P_n^{(m)} \| \pi_n) \to 0$

To input random numbers into the channel to simulate Eve's probability distribution

Random numbers

$\mathcal{U} \equiv \{1, \cdots, u, \cdots, L\}$

u



Uniform distribution $\frac{1}{L}$

u

Output probability distribution for input *u*

$P_n^{(u)}$

z

Target probability distribution at Eve

π_n

z

If $P_n^{(u)}$ is identical to π_n, then messages *u* are statistically indistinguishable for Eve observing *z* alone.

Eve can be deceived.

Minimize the KL distance; $\delta_n^E \equiv \frac{1}{M_n} \sum_{m \in \mathcal{M}_n} D(P_n^{(m)} || \pi_n)$

Reliability

Metrics

Security

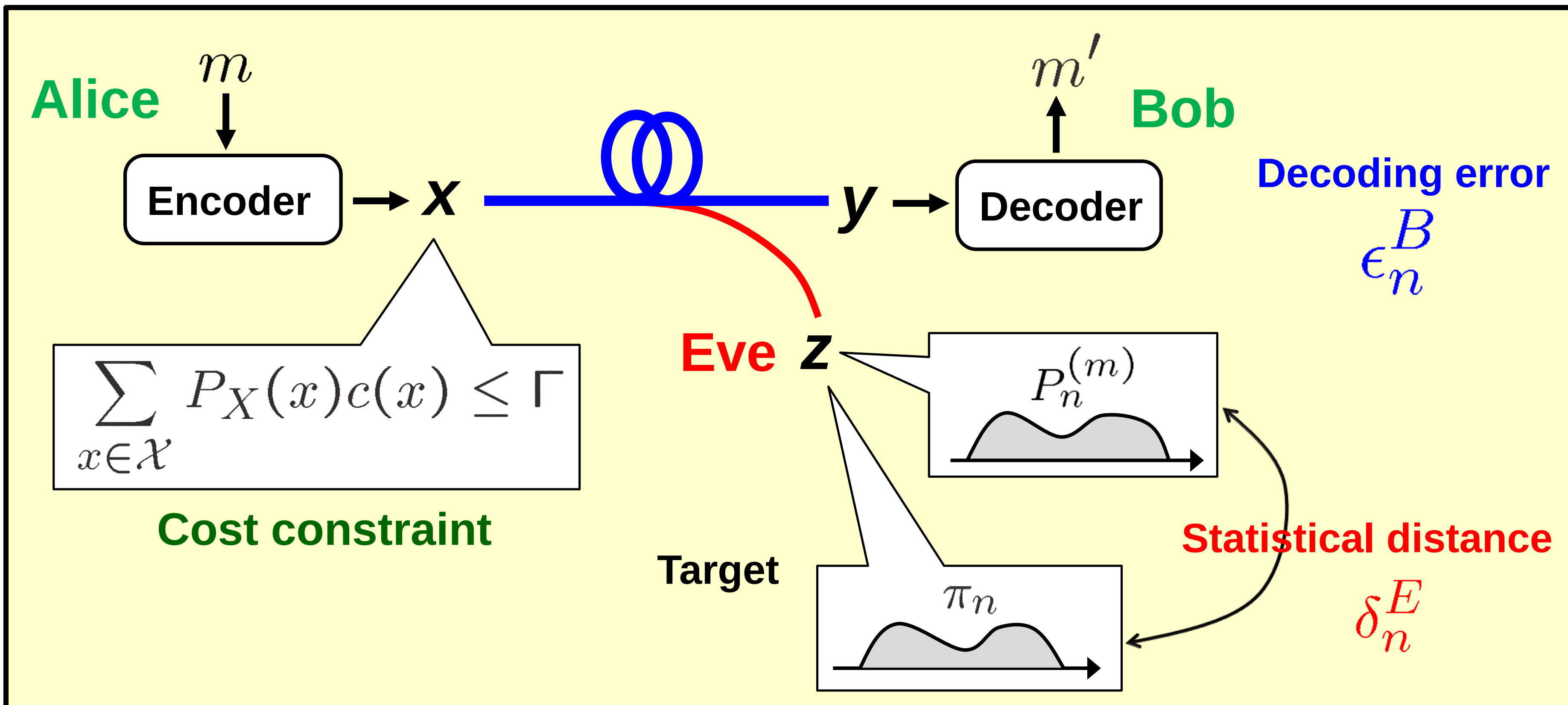
Bob's decoding error

$$\epsilon_n^B \equiv \frac{1}{M_n} \sum_{m \in \mathcal{M}_n} \Pr\left\{m' \neq m\right\}$$

KL distance between the output and target distributions at Eve

$$\delta_n^E \equiv \frac{1}{M_n} \sum_{m \in \mathcal{M}_n} D(P_n^{(m)} \| \pi_n)$$

Make these two as small as desired under cost constraint.



Quantification of tradeoff between reliability and secrecy

T.-S. Han, H. Endo, and M. Sasaki, IEEE-IT60(11), 6819 (2014).

Reliability function

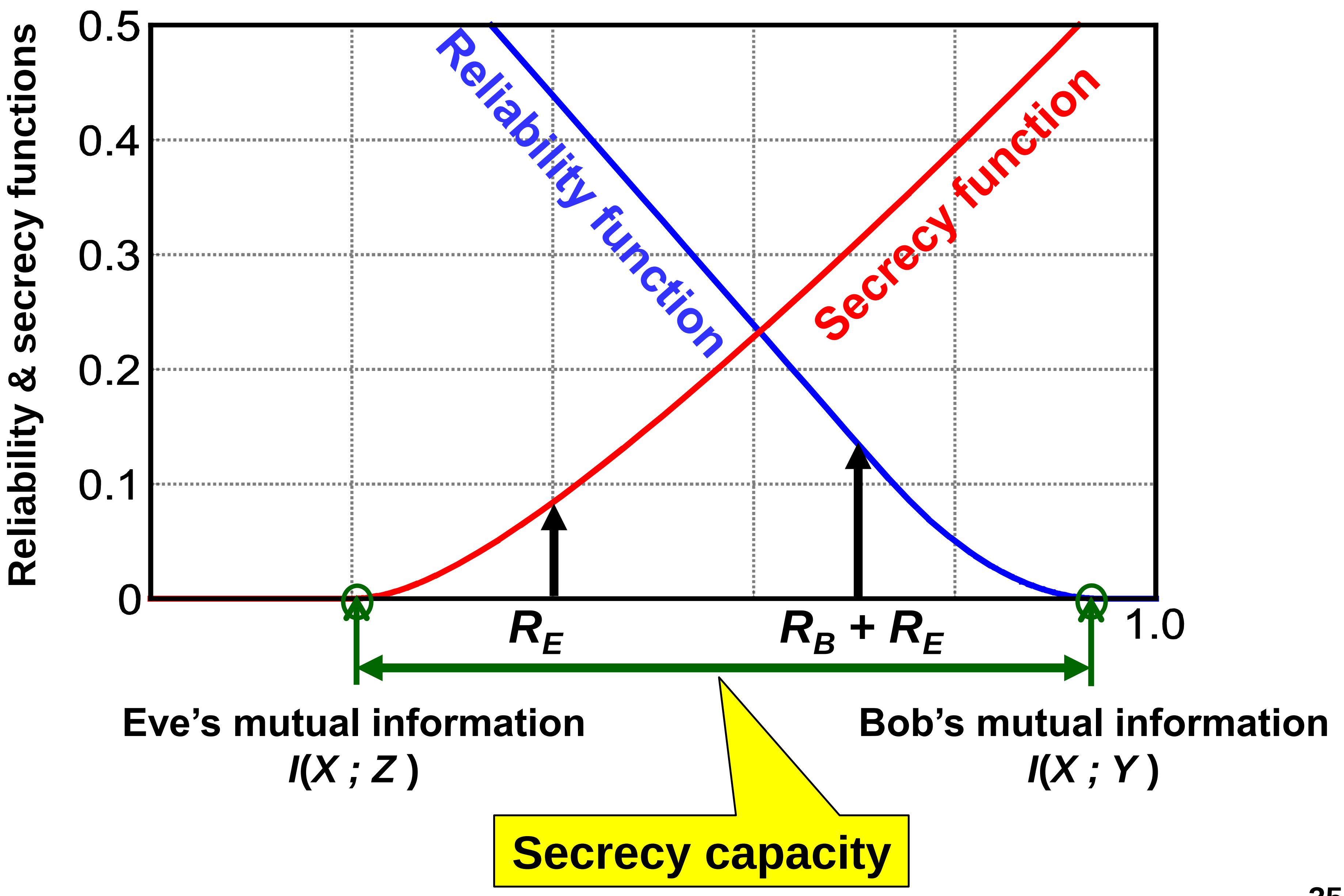
$$\epsilon_n^B \leq 2e^{-nF(q,R_B,R_E,+\infty)}$$

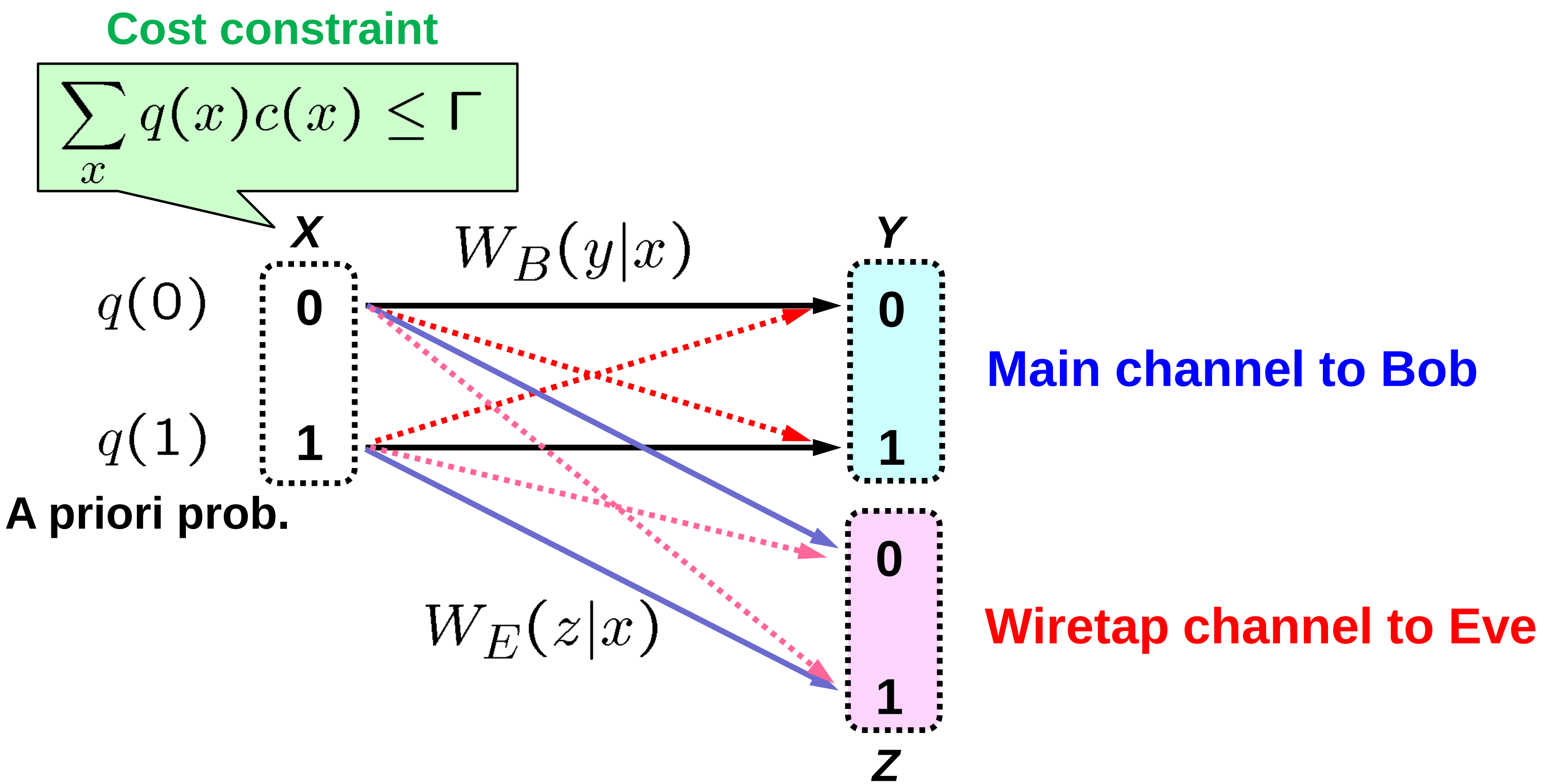
Secrecy function

$$\delta_n^E \leq 2e^{-nH(q,R_E,n)}$$

How rapid the KL distance decreases as code length *n*?

T.-S. Han, H. Endo, and M. Sasaki, IEEE-IT60(11), 6819 (2014).





Define dual quantities ϕ

$$\phi(\rho|W_B,q,r) = -\log\left[\sum_{y\in\mathcal{Y}}\left(\sum_{x\in\mathcal{X}} q(x)W_B(y|x)^{\frac{1}{1+\rho}}e^{r[\Gamma-c(x)]}\right)^{1+\rho}\right]$$

$$\phi(-\rho|W_E,q,r) = -\log\left[\sum_{z\in\mathcal{Z}}\left(\sum_{x\in\mathcal{X}} q(x)W_E(z|x)^{\frac{1}{1-\rho}}e^{r[\Gamma-c(x)]}\right)^{1-\rho}\right]$$

Reliability function

$$F(q, R_B, R_E, \infty) = \sup_{0\le\rho\le1} \sup_{r\ge0} \left[\phi(\rho|W_B, q, r) - \rho(R_B + R_E)\right]$$

Secrecy function

$$H(q, R_E, \infty) = \sup_{0<\rho<1} \sup_{r\ge0} \left[\phi(-\rho|W_E, q, r) + \rho R_E\right]$$

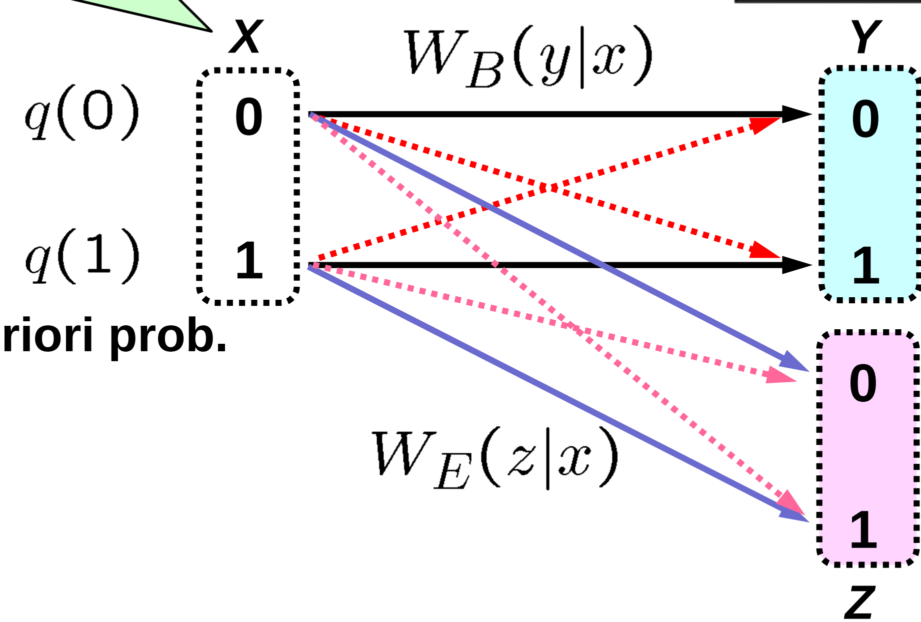
Han, Endo, & Sasaki, IEEE-IT60(11), 6819 (2014).

Theorem

Decoding error and KL distance can be upper-bounded in the following way.

Cost constraint

$$\sum_x q(x)c(x) \le \Gamma$$



A priori prob.

Decoding error

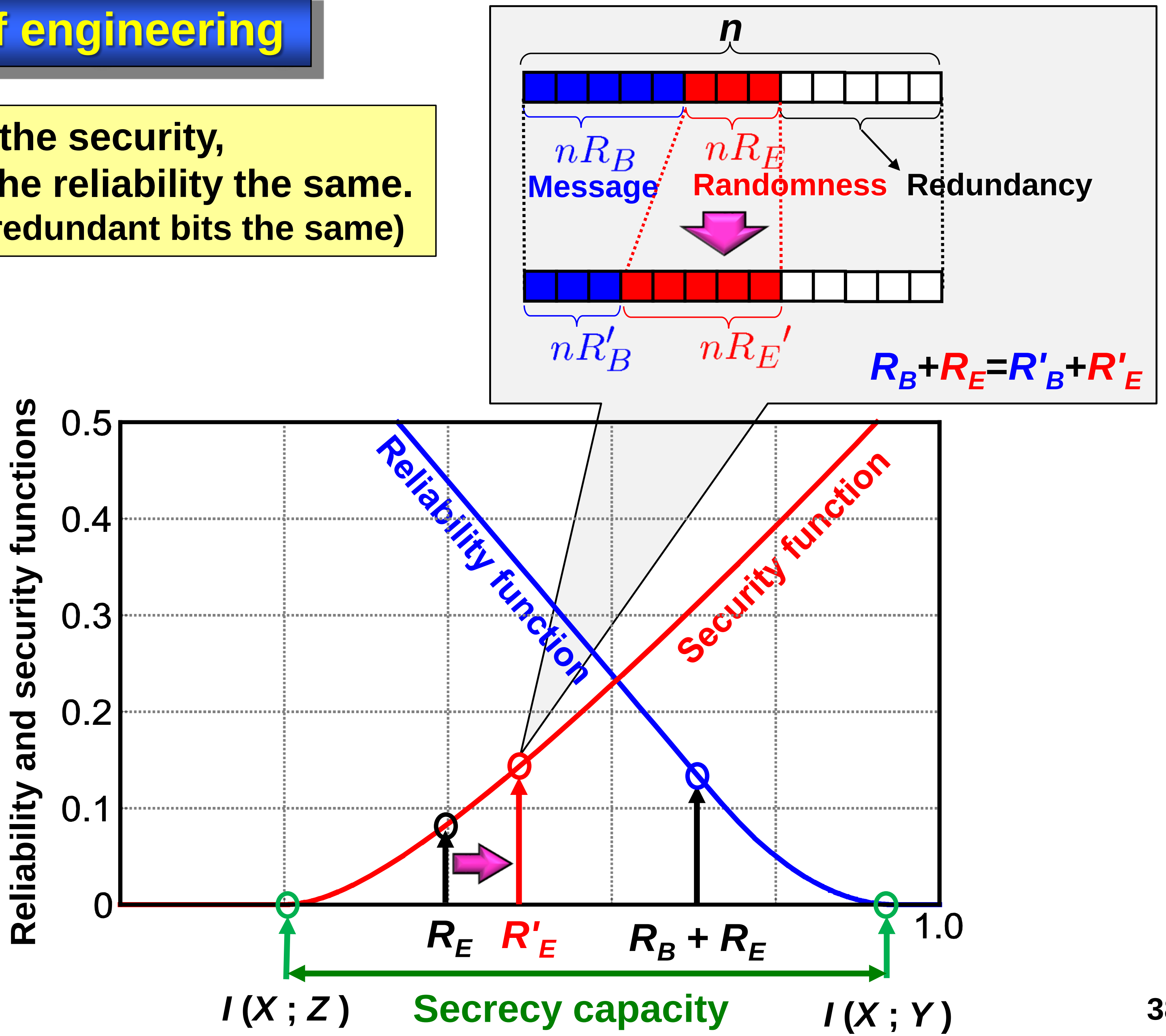
$$\epsilon_n^B \le 2e^{-nF(q,R_B,R_E,+\infty)}$$

KL distance

$$\delta_n^E \le 2e^{-nH(q,R_E,n)}$$

Tradeoff engineering

Enhance the security,
keeping the reliability the same.
(keep the redundant bits the same)



Contents

Network security

Crypto technologies in a network layer stack

Physical layer security

- Secrecy message transmission
- Secret key agreement
- Quantum key distribution

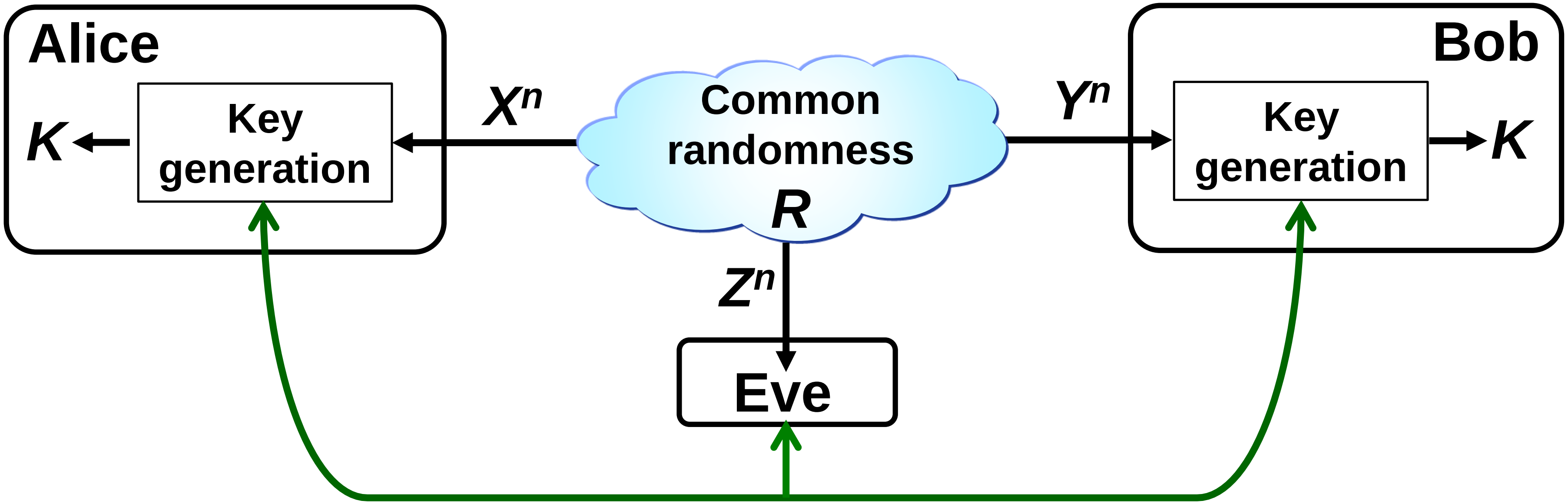
"Theoretical framework"

"Implementation and use cases"

Quantum safe infrastructure

"Perspectives"

Secret key agreement



Public authenticated channel
for interactive two way communications

Secret key agreement is possible **even if Eve's channel is the most reliable channel,** $I(X;R) < I(Z;R)$ and $I(Y;R) < I(Z;R)$

U. M. Maurer, IEEE Trans. Inf. Theory, 39, pp. 733–742, 1993.
R. Ahlswede and I. Csiszár, IEEE Trans. Inf. Theory, 39, pp. 1121–1132, 1993.

Secret key agreement

(1) Advantage distillation

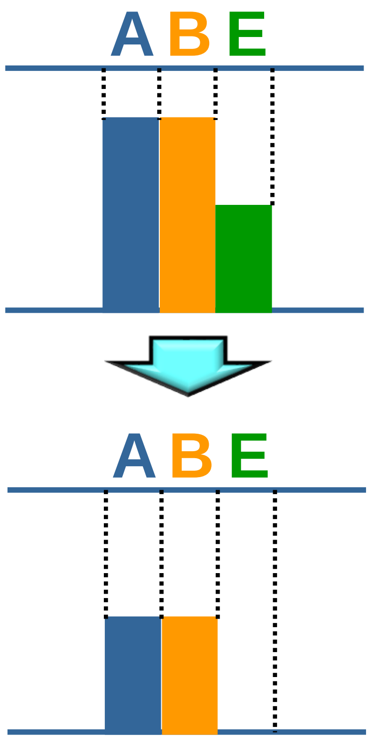
A random sequence between Alice and Bob through public discussion

(2) Reconciliation

Exchange information to recover the common sequence

(3) Privacy amplification

Compress the common sequence by a universal hash function and get the secret key



$$S(X;Y\|Z) \geq \max[I(Y;X) - I(Z;X), \\ I(X;Y) - I(Z;Y)].$$

Still need some information on Eve's channel

Applications are restricted, wireless communications, …

Contents

Network security

Crypto technologies in a network layer stack

Physical layer security

- Secrecy message transmission
- Secret key agreement
- Quantum key distribution

"Theoretical framework"

"Implementation and use cases"

Quantum safe infrastructure

"Perspectives"

C. H. Bennett

Quantum mechanics

1982

Cryptography

G. Brassard

Quantum Key Distribution (QKD)

BB84

Classical

Channel matrix $P(y|x)$ is given.

Quantum

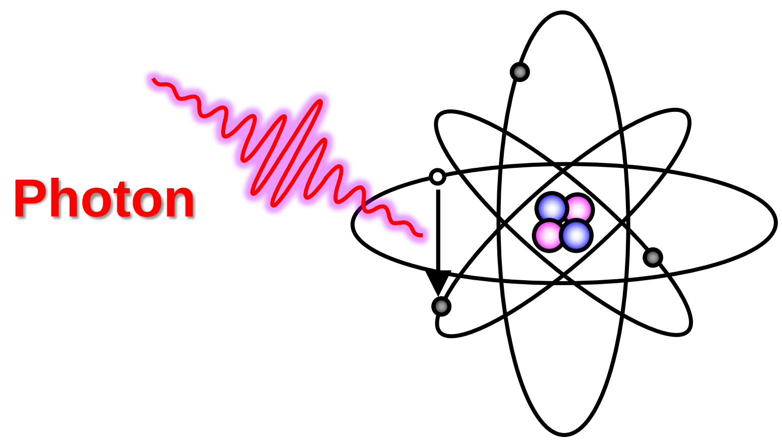
Measurement vector

Signal state vector

$$P(y|x) = \left| \underbrace{\langle m_y | \psi_x \rangle}_{\text{Q. probability amplitude}} \right|^2$$

"A lower layer structure of the channel matrix"

Quantum layer



Signal state vector

Polarized single photon

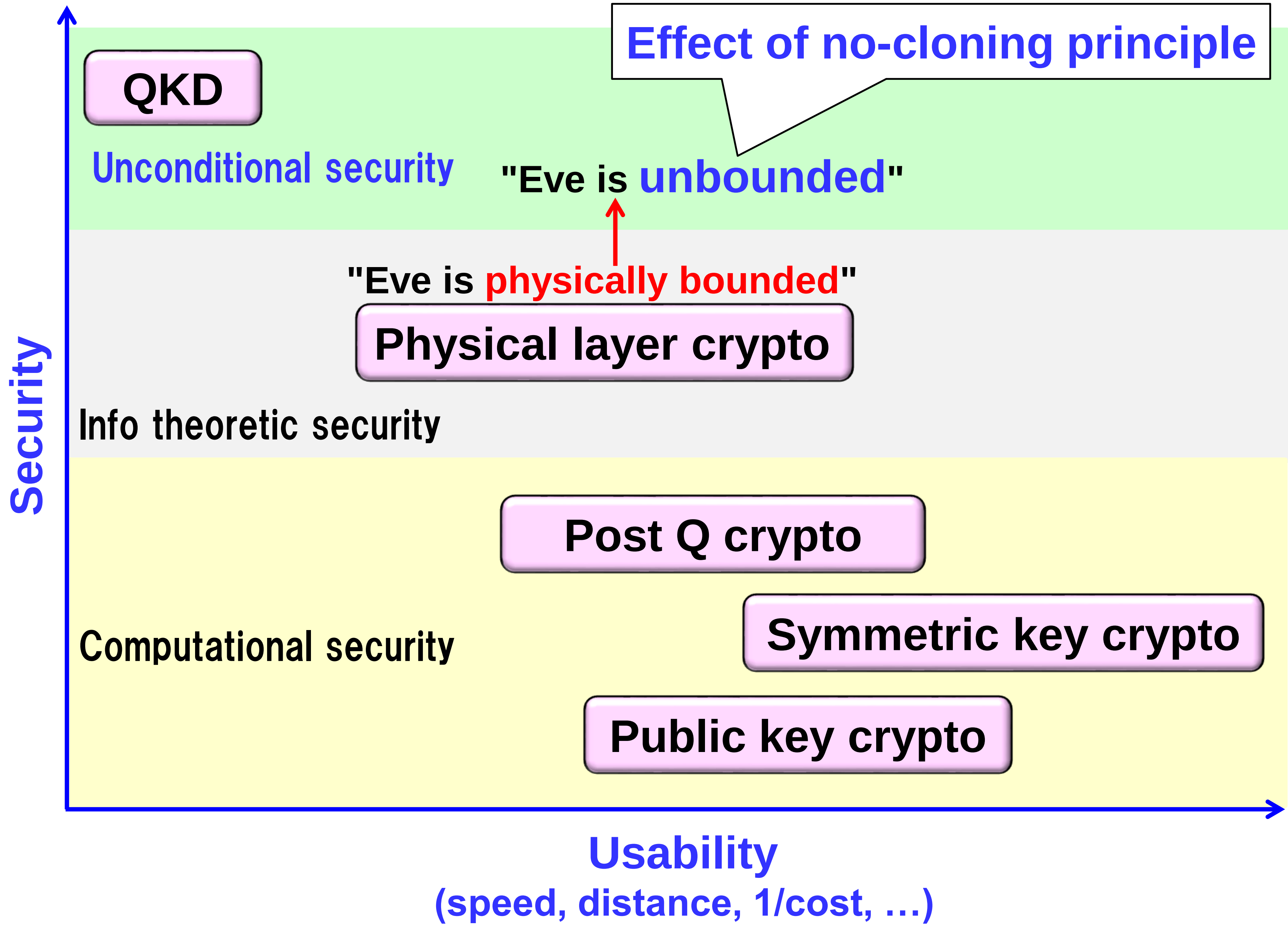
$$|45°\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle + |V\rangle\Big),$$
$$|{-45°}\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle - |V\rangle\Big)$$

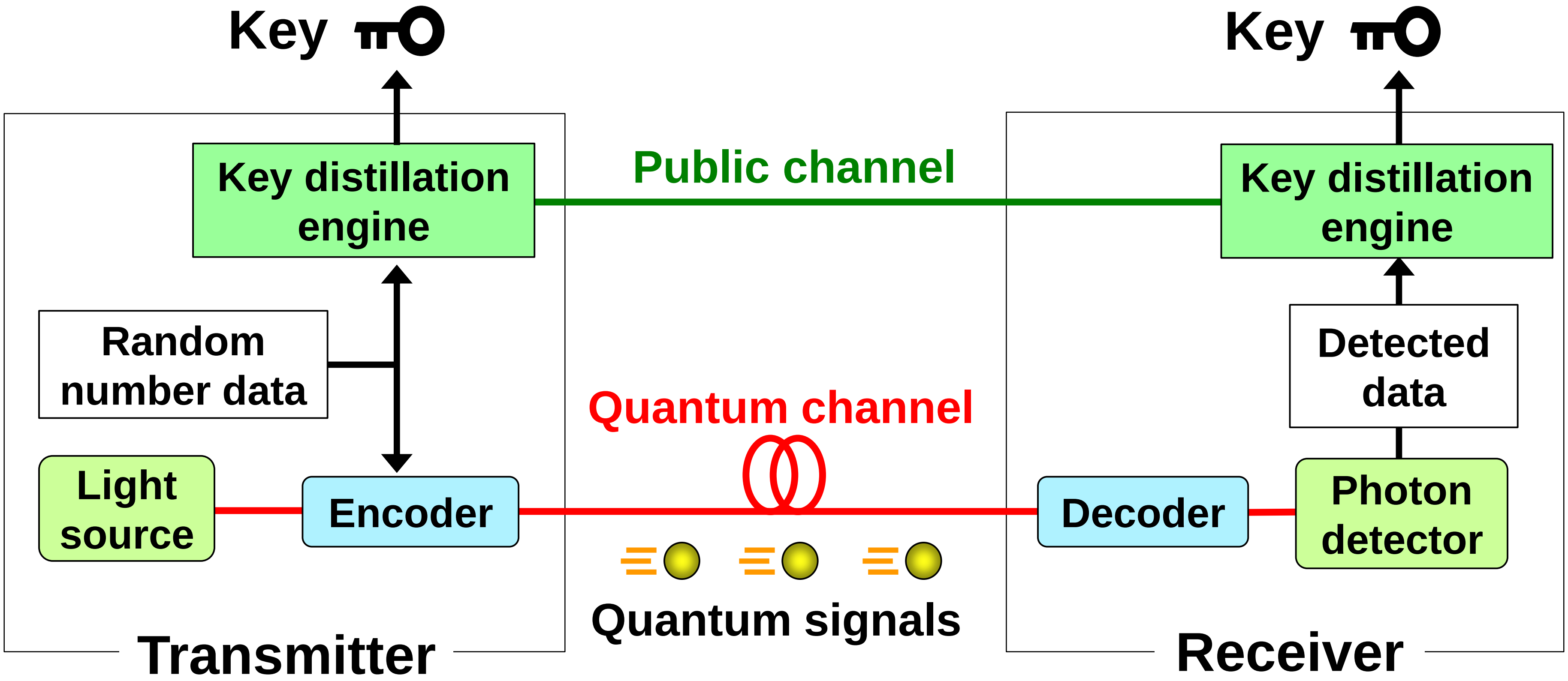
Superposition states

Laws of quantum mechanics

Non-orthogonal states cannot be cloned without disturbing their states (no-cloning principle).

Eavesdropping attempts always cause disturbances.

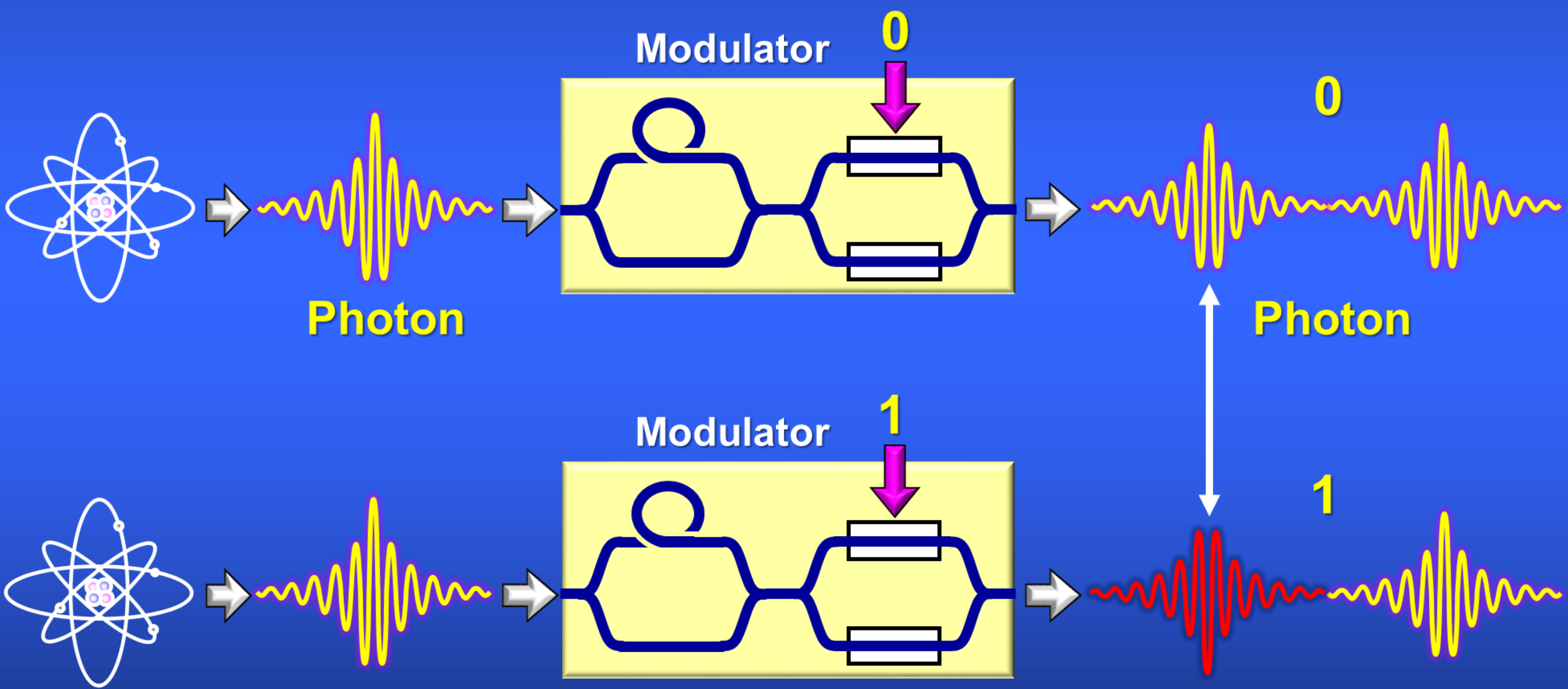

Effect of no-cloning principle
QKD
Unconditional security
"Eve is unbounded"
"Eve is physically bounded"
Physical layer crypto
Info theoretic security
Post Q crypto
Symmetric key crypto
Computational security
Public key crypto
Security
Usability
(speed, distance, 1/cost, …)


Key
Key
Key distillation engine
Public channel
Key distillation engine
Random number data
Detected data
Quantum channel
Light source
Encoder
Decoder
Photon detector
Quantum signals
Transmitter
Receiver

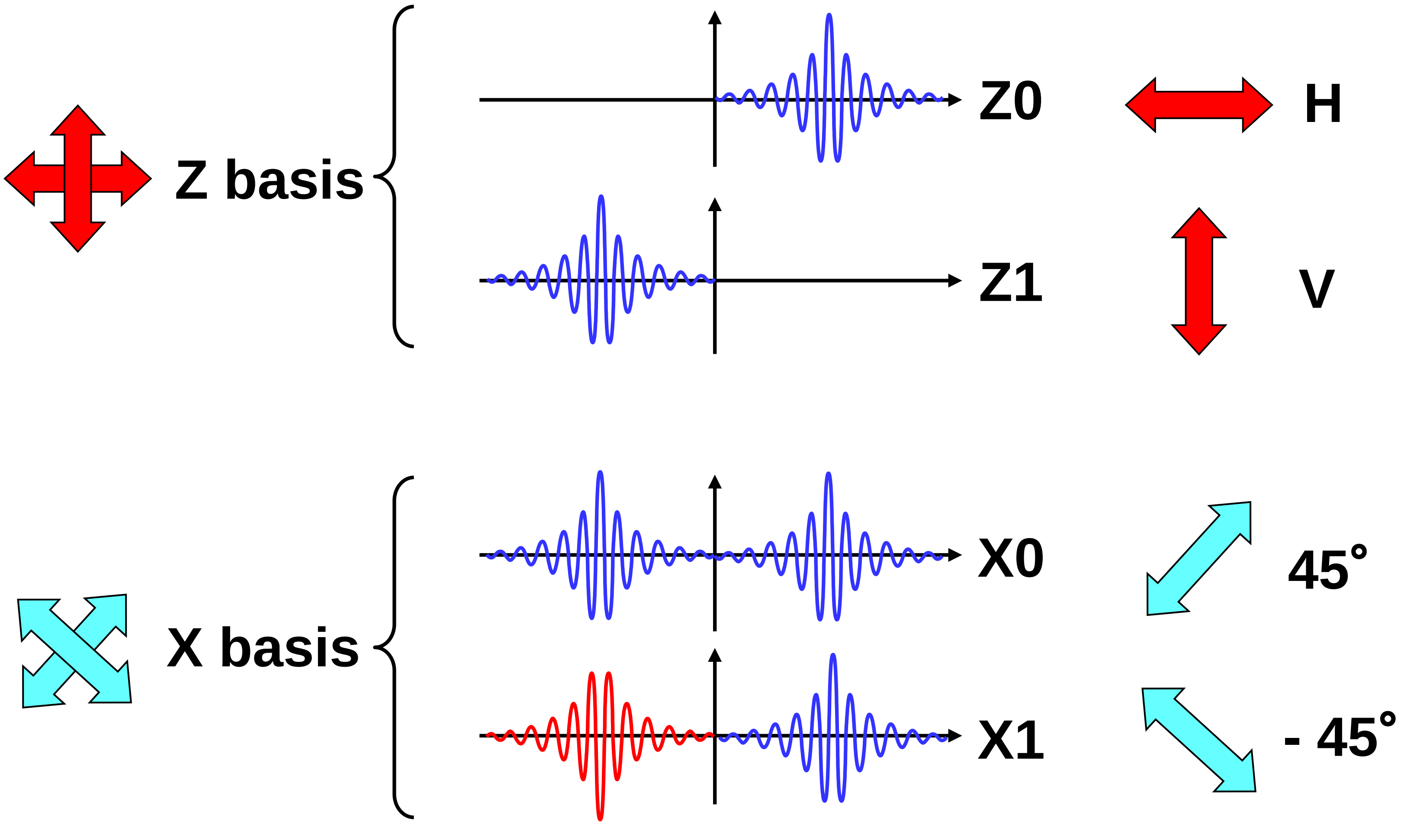
QKD system

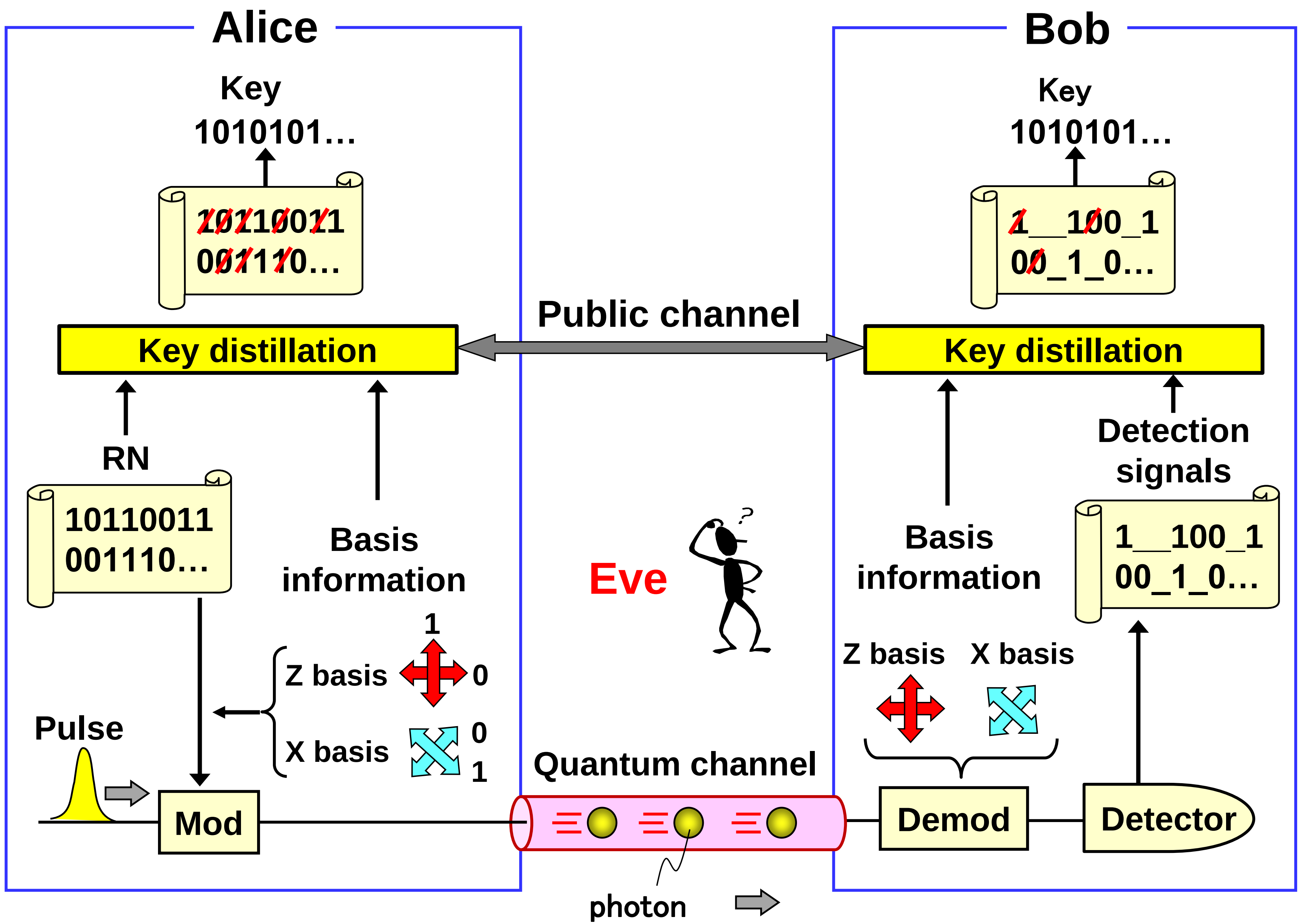
In practical fiber transmission,

we encode key information of 0 and 1
by modulating the photon pulse envelope.



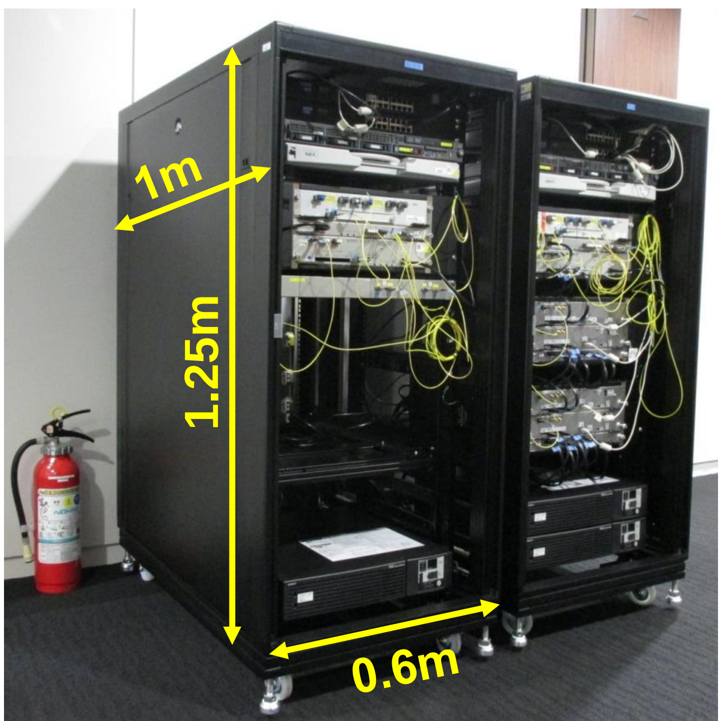
Time bin signals

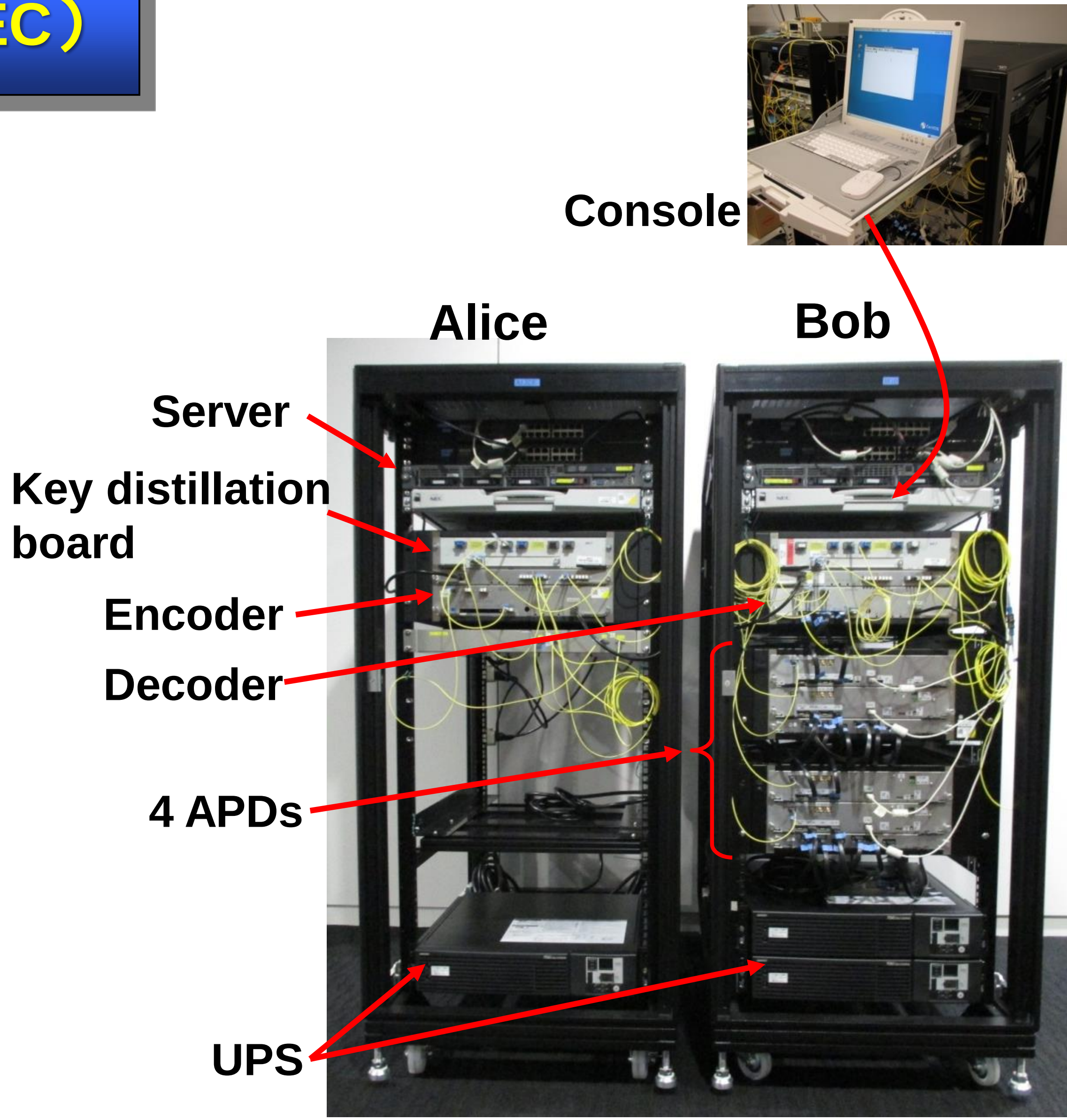


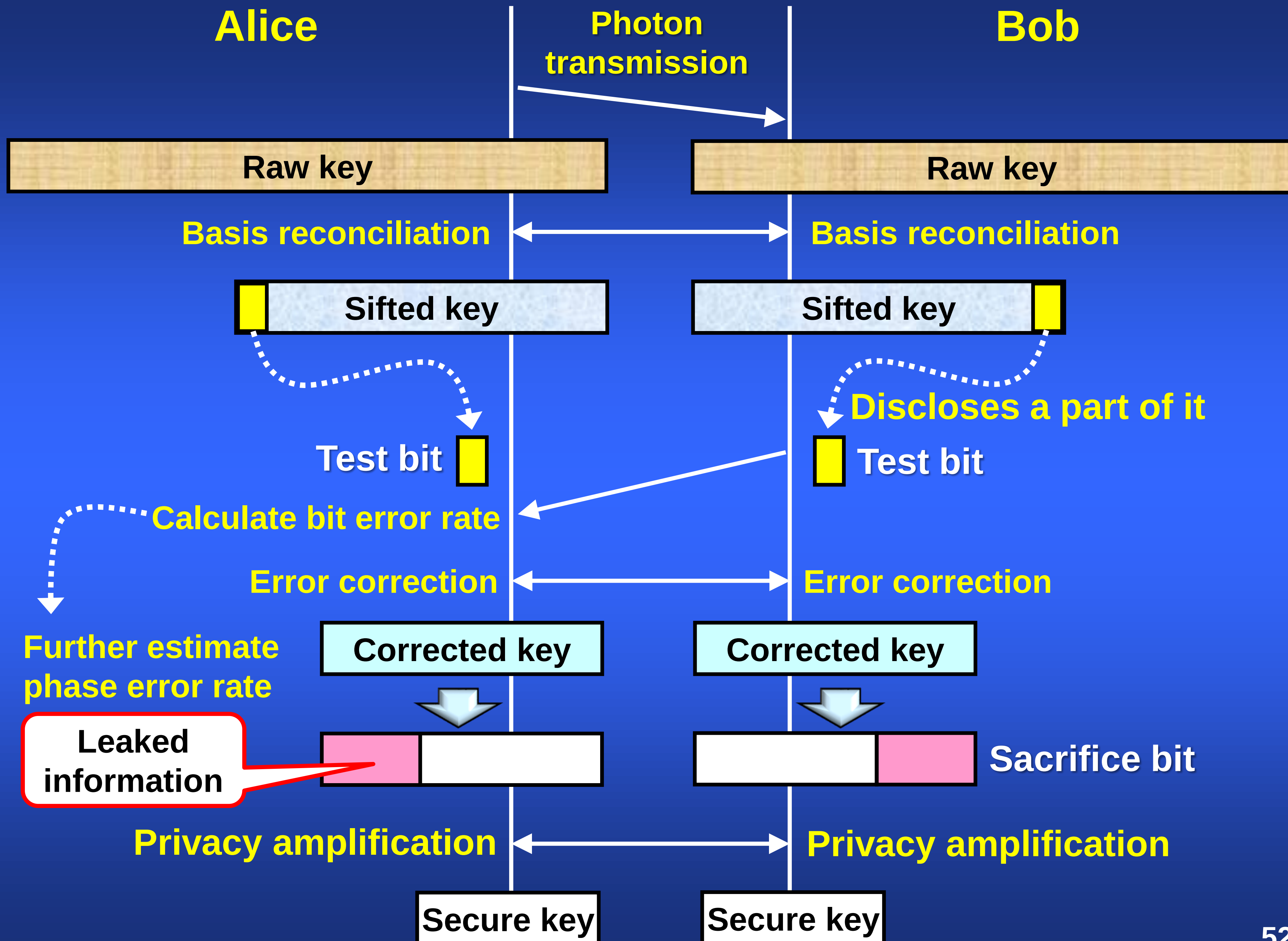

Alice
Key
1010101…
10110011
001110…
Key distillation
RN
10110011
001110…
Basis
information
1
Z basis
0
0
X basis
1
Pulse
Mod
Public channel
Eve
Quantum channel
photon
Bob
Key
1010101…
1__100_1
00_1_0…
Key distillation
Detection
signals
Basis
information
1__100_1
00_1_0…
Z basis
X basis
Demod
Detector

Latest model of QKD (Decoyed BB84, by NEC)

Key rate 100kbps
Distance 60km
(for fiber loss 0.2dB/km)
Clock rate 1.24GHz







Alice
Photon transmission
Bob
Raw key
Raw key
Basis reconciliation
Basis reconciliation
Sifted key
Sifted key
Discloses a part of it
Test bit
Test bit
Calculate bit error rate
Error correction
Error correction
Further estimate phase error rate
Corrected key
Corrected key
Leaked information
Sacrifice bit
Privacy amplification
Privacy amplification
Secure key
Secure key

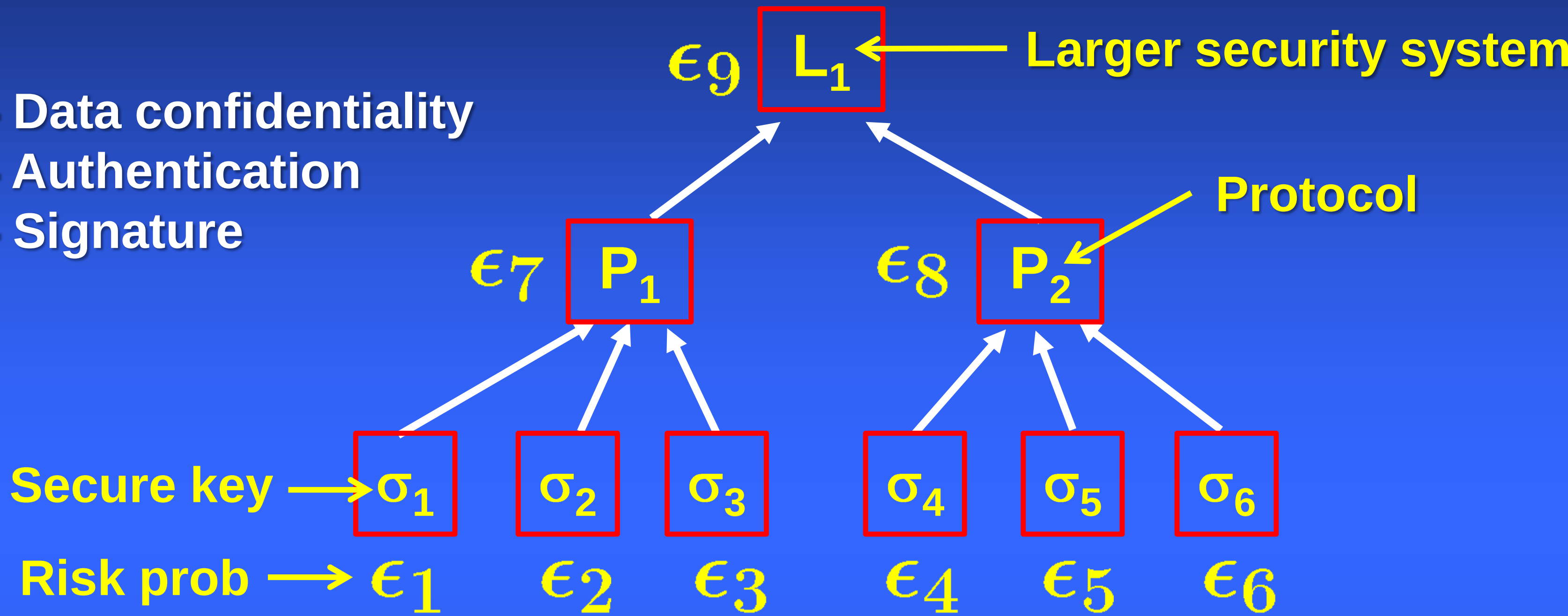
Introductory videos are available at the web site of

UQCC 2015

http://2015.uqcc.org/program/index.html

Ensure composable security

- Data confidentiality
- Authentication
- Signature



- The security risk should not increase even if the key σ_i is used in a larger protocol.
- The total risk of the system should be given by the sum of the risk probability of the components.

$$\sum_i \epsilon_i$$

Criterion for composable security : Trace distance

$$\|\rho_{SE} - \rho_U \otimes \rho_E\|_1 \leq \epsilon$$

Security parameter

Eve's system can be correlated with the generated key

Perfect key *U*

Some other state

Independent

Real situation

Ideal situation

Basic property in operator algebra (completely positive map)

Any physical operations in any other protocols can *NOT* increase the trace distance. $\longrightarrow$ Composability

Lecture Notes in Computer Science, vol. 3378, Springer Verlag 2005
- M. Ben-Or, et al., p 386.
- R. Renner, and R. Koenig, p 407.

Do not use the mutual information.

R. Koenig, et al., PRL98, 140502 (2007)

Contents

Network security

Crypto technologies in a network layer stack

Physical layer security

- Secrecy message transmission
- Secret key agreement
- Quantum key distribution

"Theoretical framework"

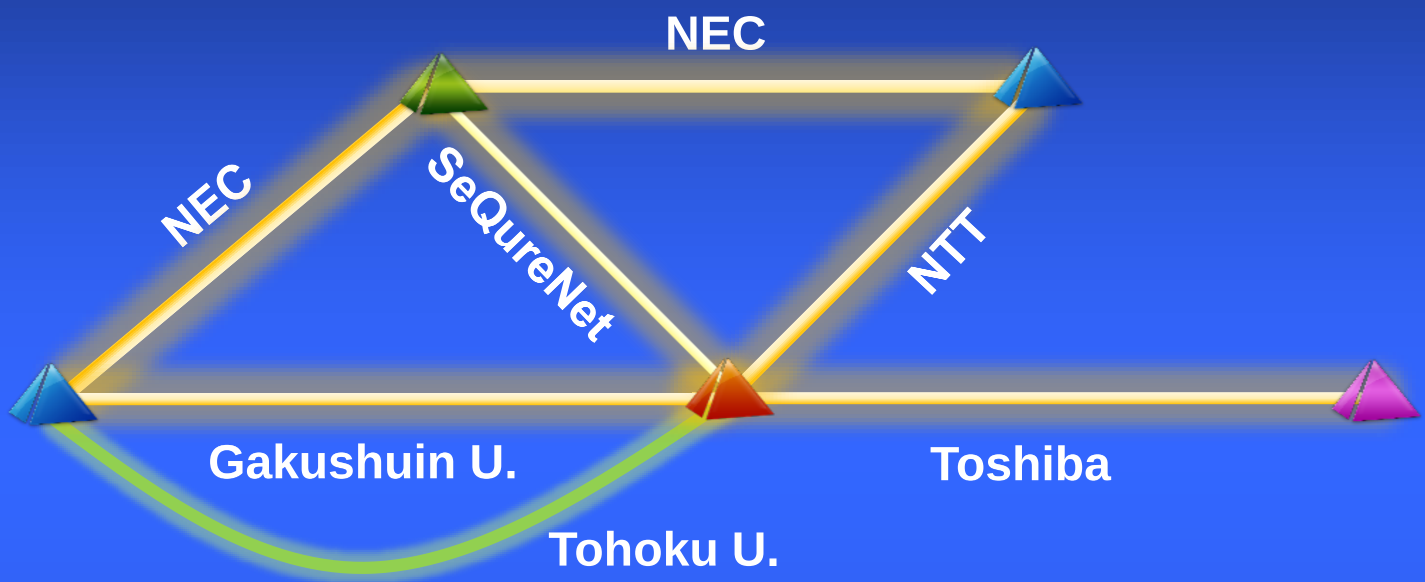
"Implementation and use cases"

Quantum safe infrastructure

"Perspectives"

Tokyo QKD Network

since 2010

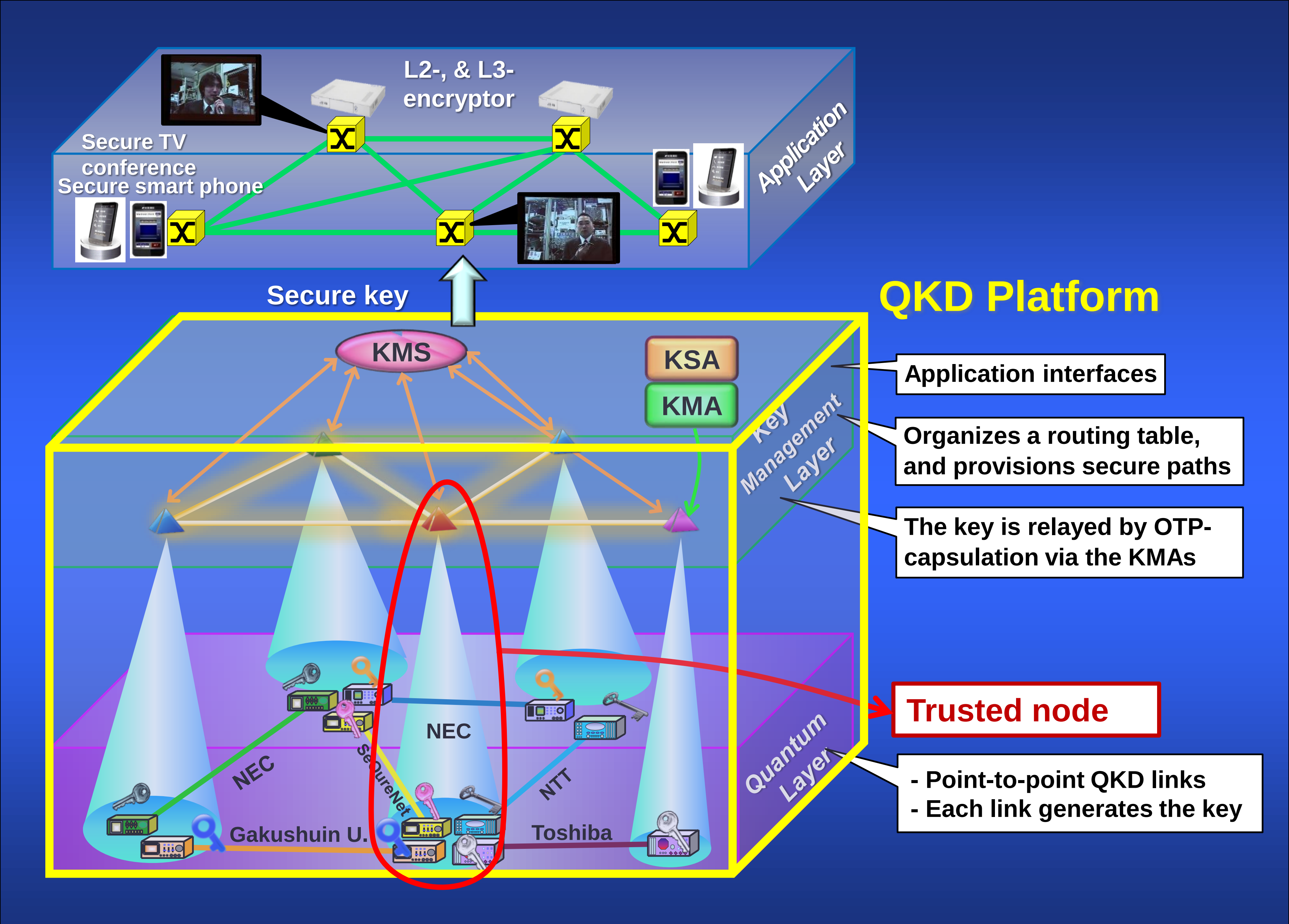


(1) BB84 : NEC and Toshiba

(2) Continuous variable-QKD : Gakushuin U. and SeQureNet

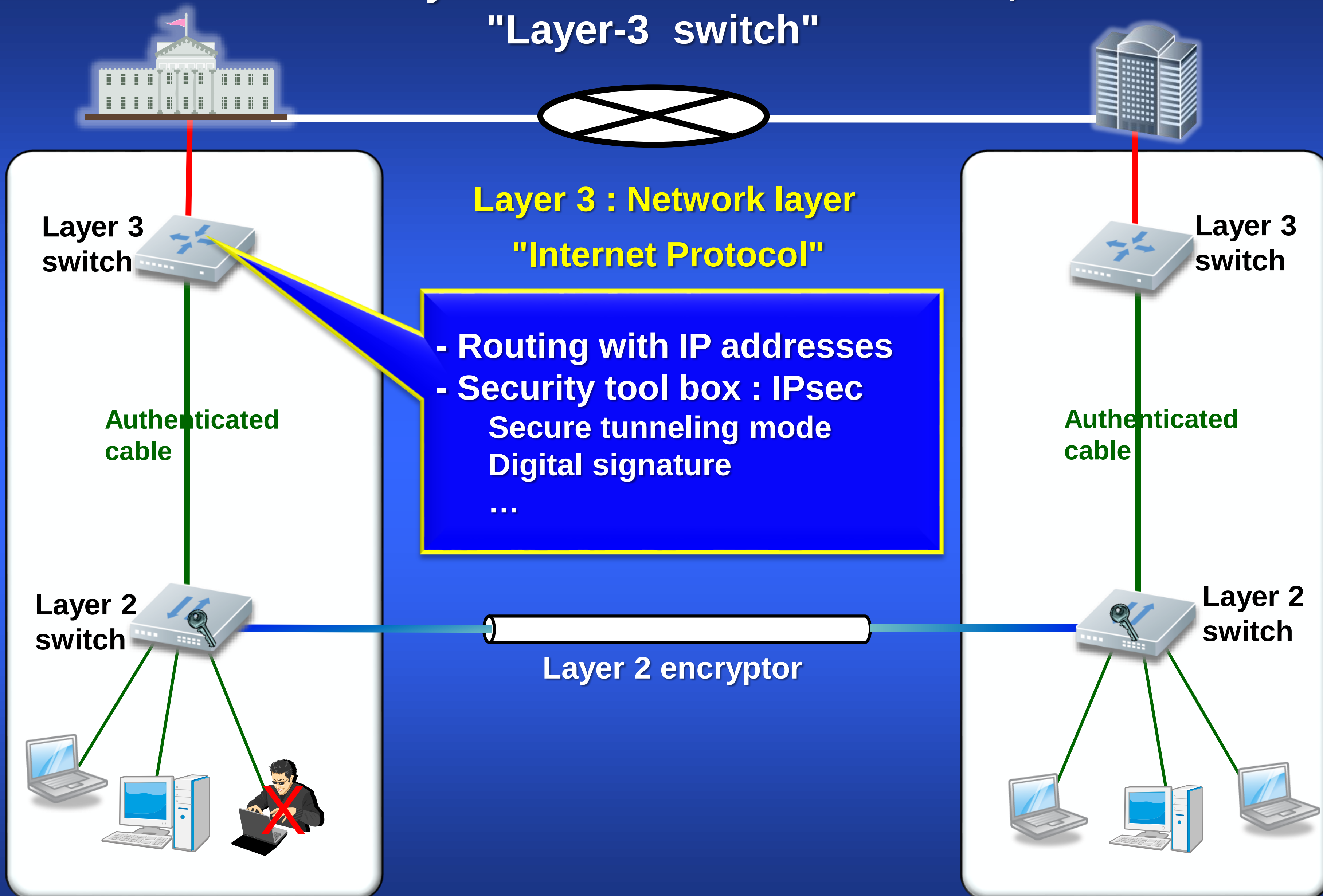
(3) DPS-QKD : NTT

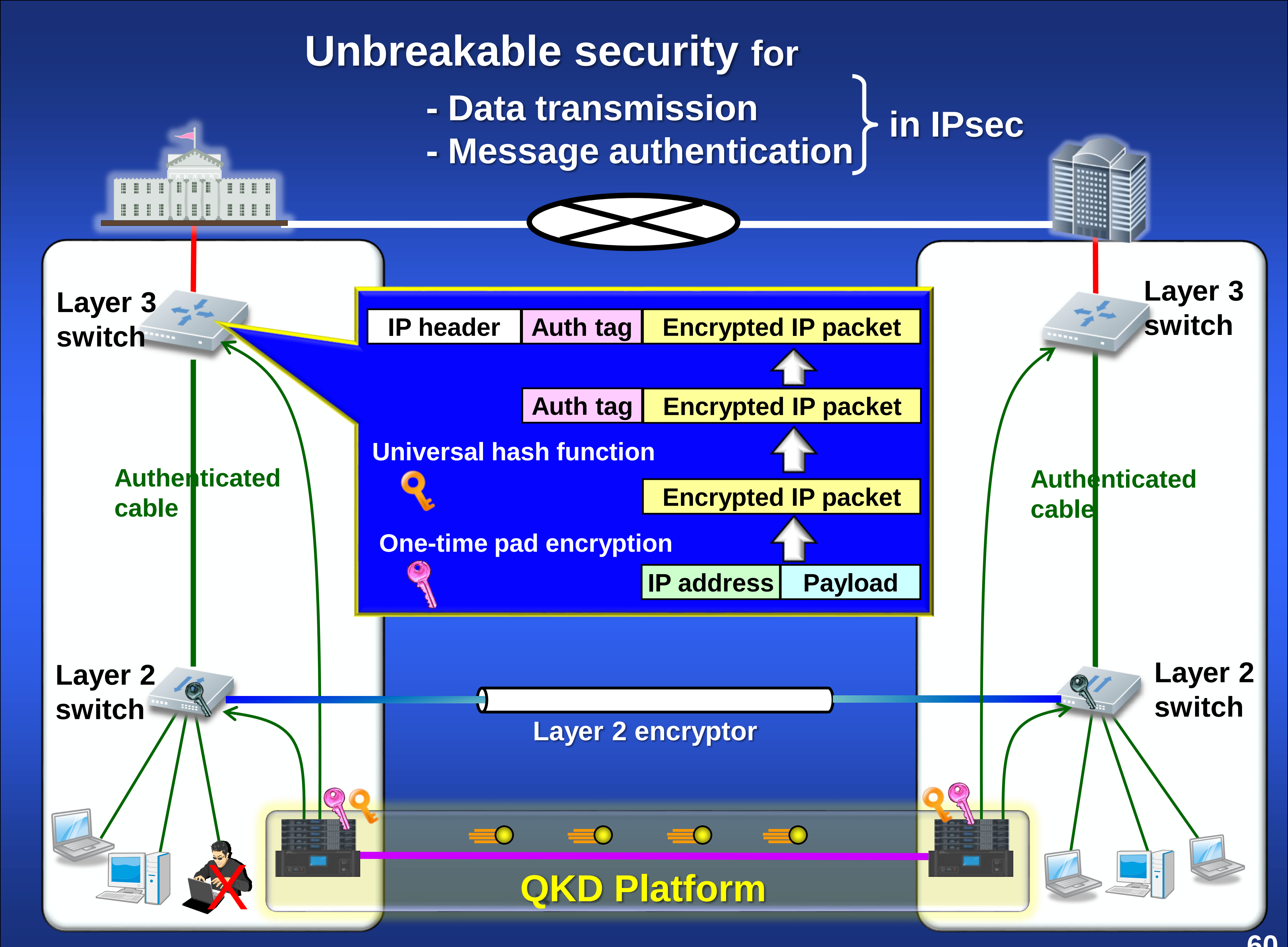
(4) Quantum Stream Cypher : Tohoku U.



L2-, & L3-
encryptor
Secure TV
conference
Secure smart phone
Application
Layer
Secure key
QKD Platform
KMS
KSA
KMA
Key
Management
Layer
Application interfaces
Organizes a routing table,
and provisions secure paths
The key is relayed by OTP-
capsulation via the KMAs
NEC
SeQureNet
NEC
NTT
Gakushuin U.
Toshiba
Quantum
Layer
Trusted node
- Point-to-point QKD links
- Each link generates the key

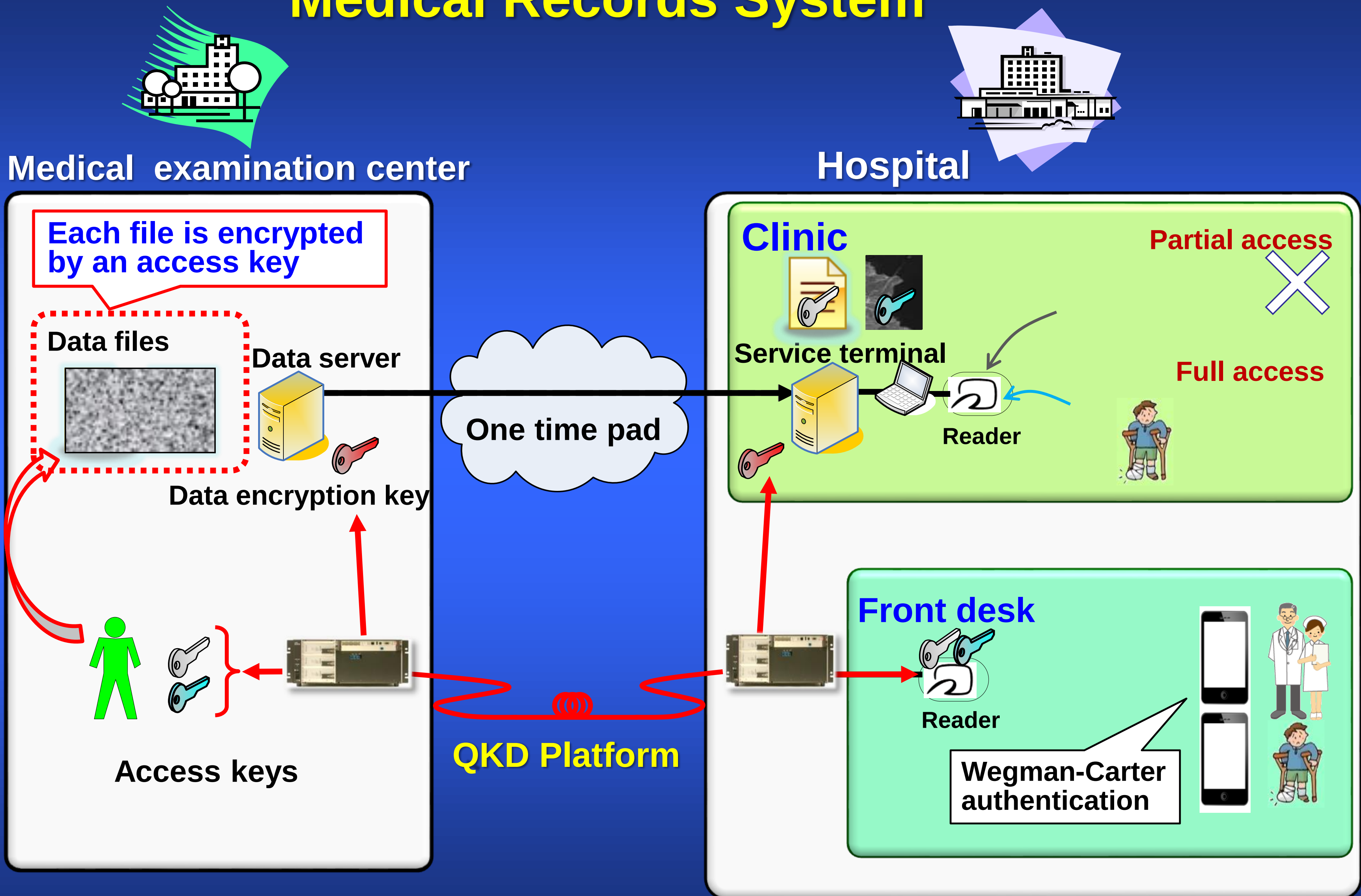
Security enhancement of an IP router, "Layer-3 switch"





Unbreakable security for
- Data transmission
- Message authentication
in IPsec
Layer 3 switch
Layer 3 switch
IP header
Auth tag
Encrypted IP packet
Auth tag
Encrypted IP packet
Universal hash function
Encrypted IP packet
One-time pad encryption
IP address
Payload
Authenticated cable
Authenticated cable
Layer 2 switch
Layer 2 switch
Layer 2 encryptor
QKD Platform

Medical Records System

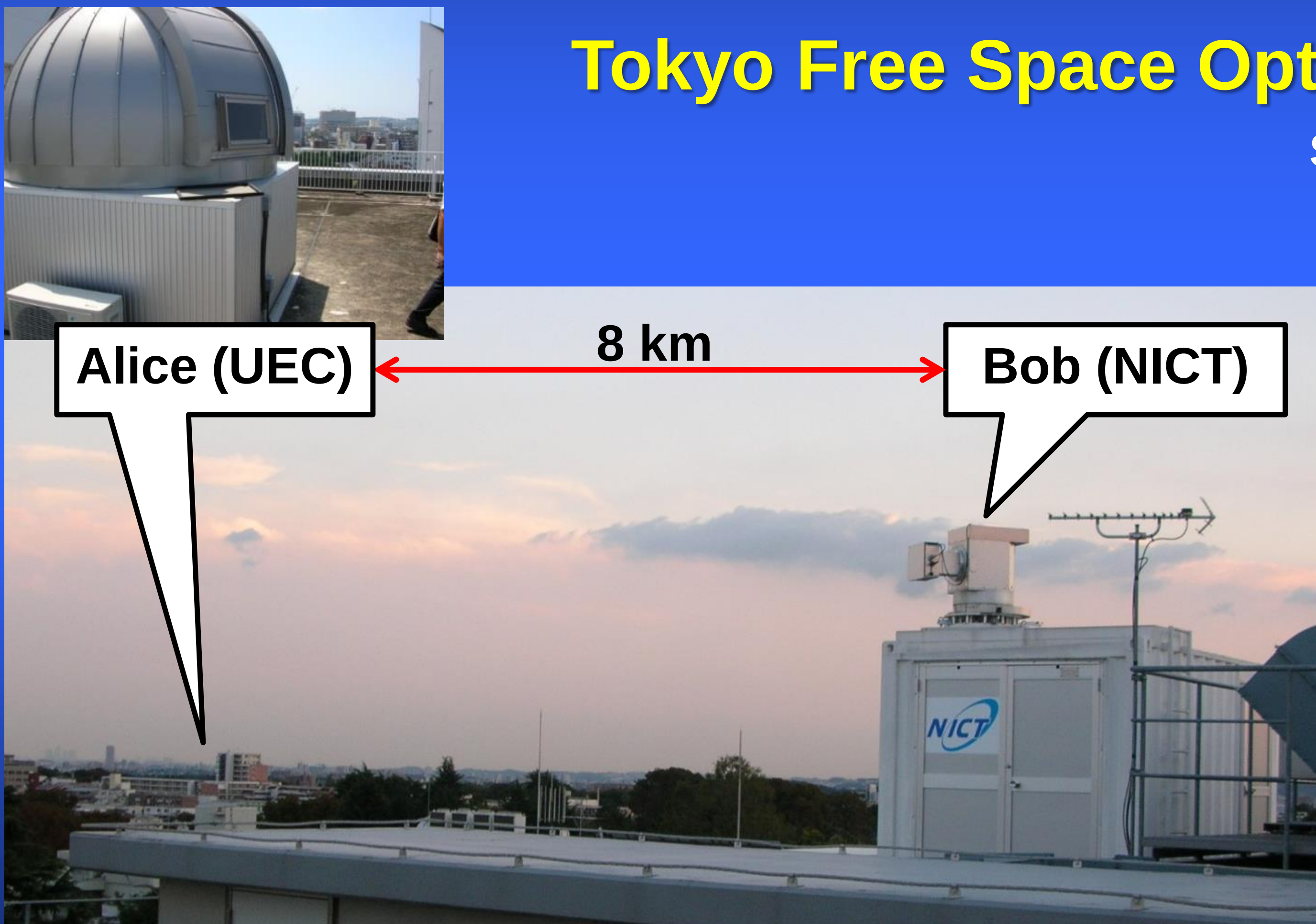



Area A
Area B
Area C
Area D

Physical layer security in space network

Tokyo Free Space Optical Testbed

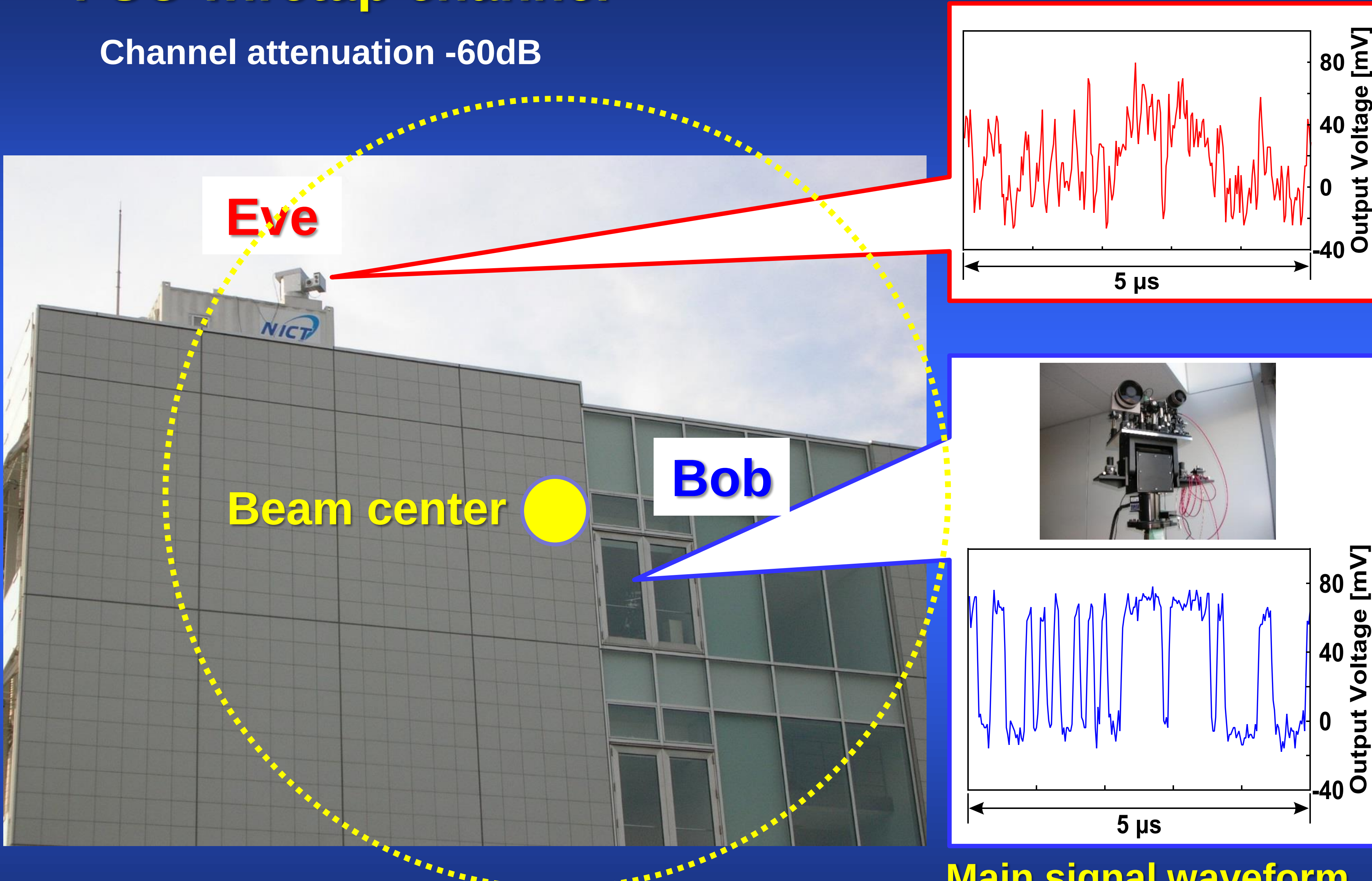
Since August 2014



FSO wiretap channel

Channel attenuation -60dB

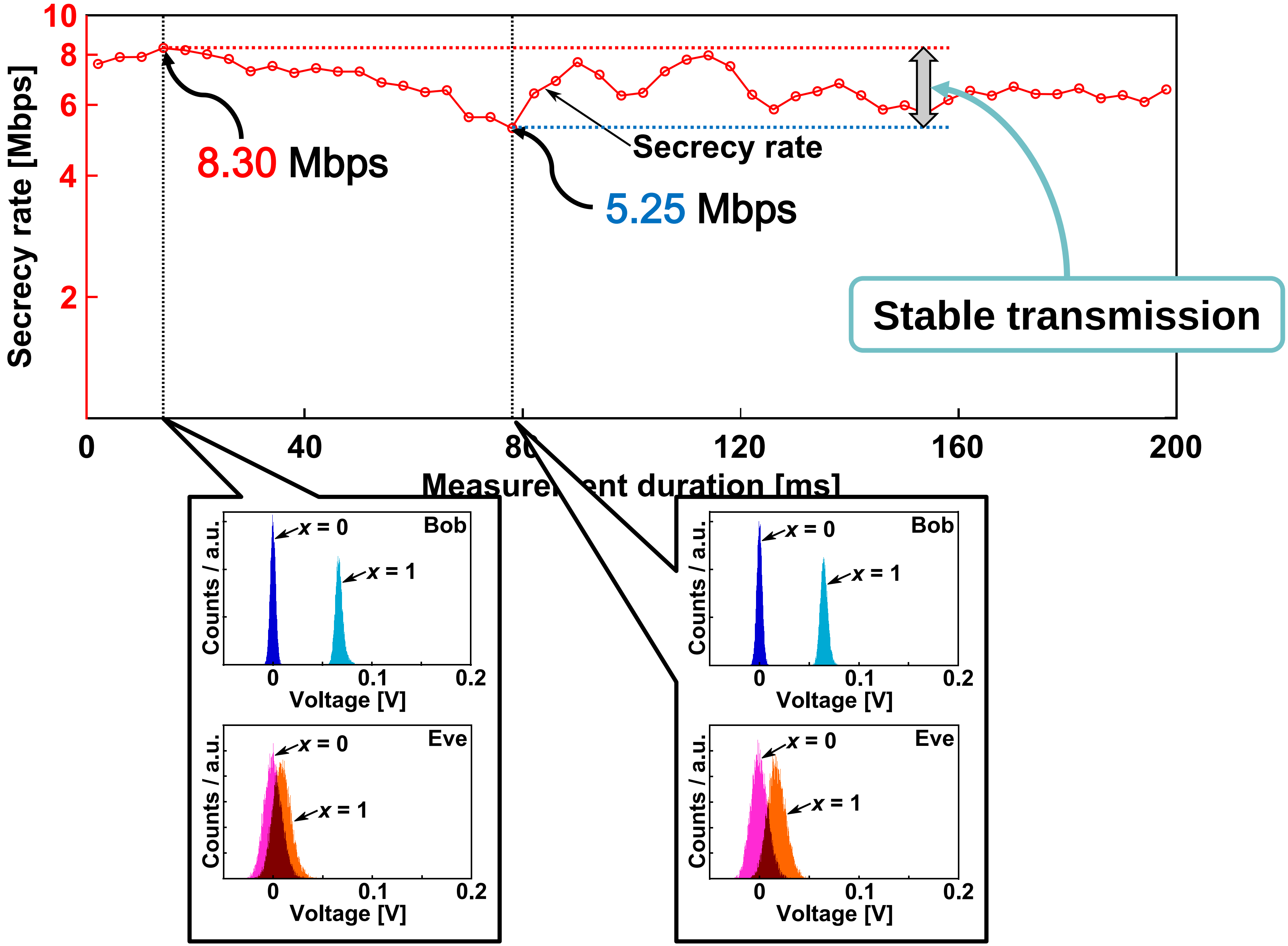
Tapped signal waveform



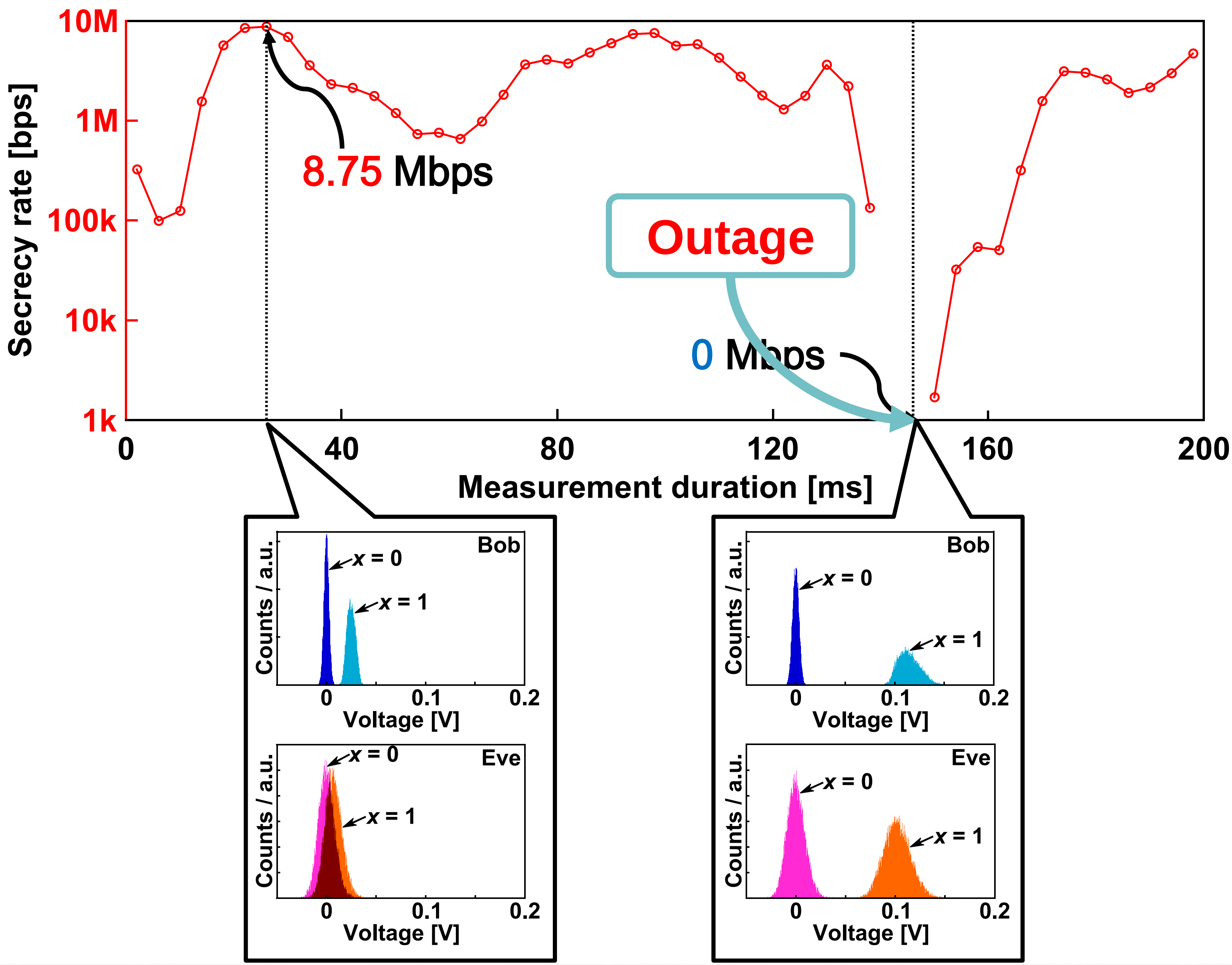
Beam footprint

Main signal waveform
(10 MHz on-off keying)

Secrecy rate : after sunset (Nov 2015)



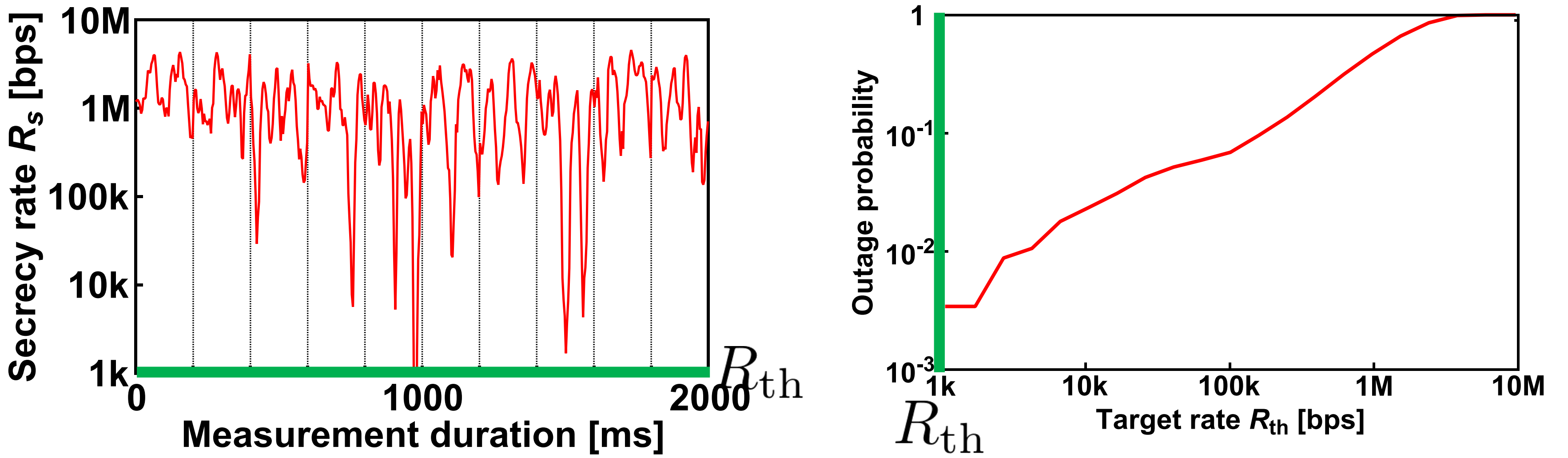
Secrecy rate : before sunset (Nov 2015)



Outage probability

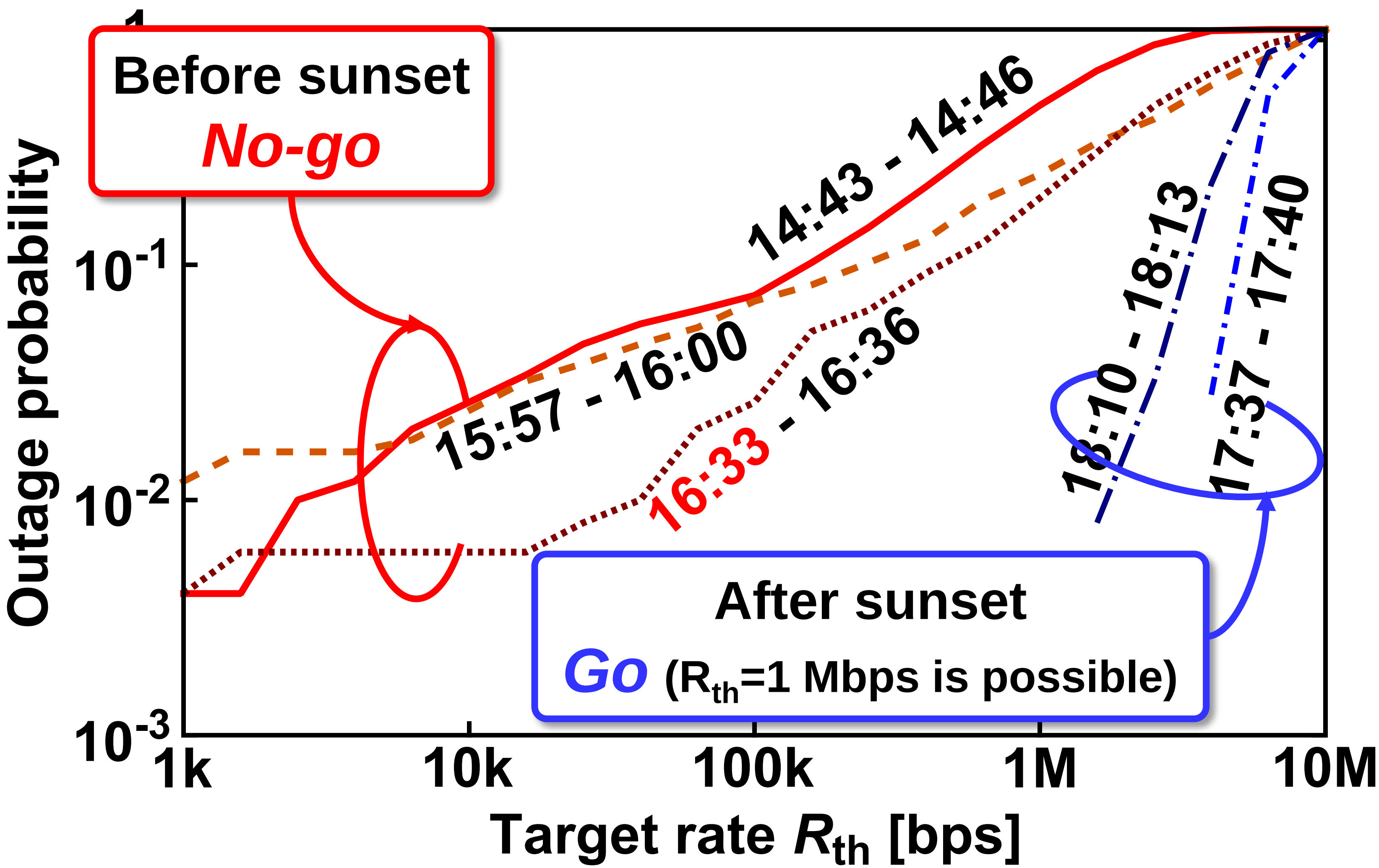
$$P_{out}(R_{th}) = \text{Prob}(R_s < R_{th})$$

Cumulative probability
that the secrecy rate decreases below the target rate R_{th}



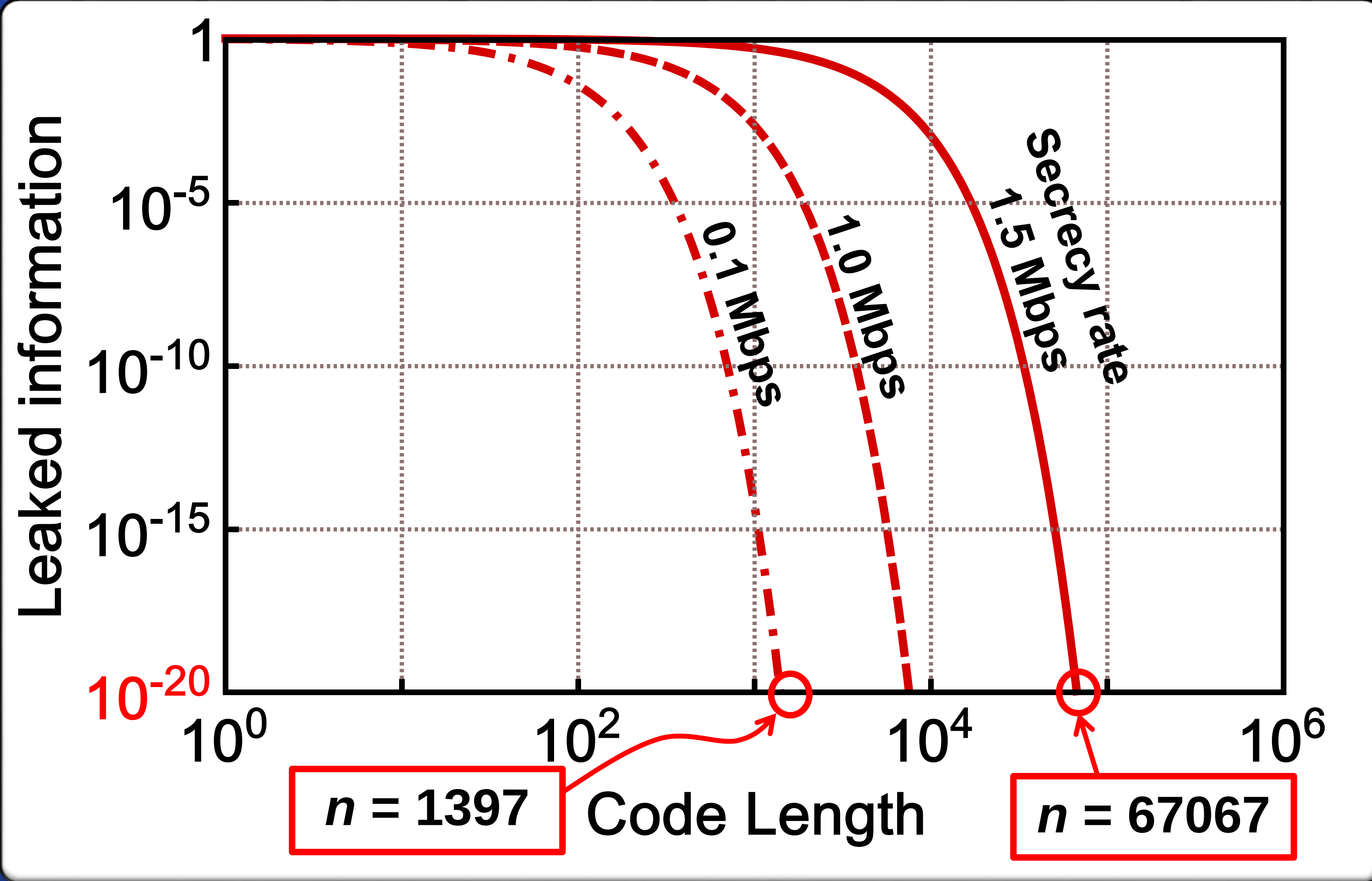
go/no-go measure
of secrecy message transmission

Outage probabilities

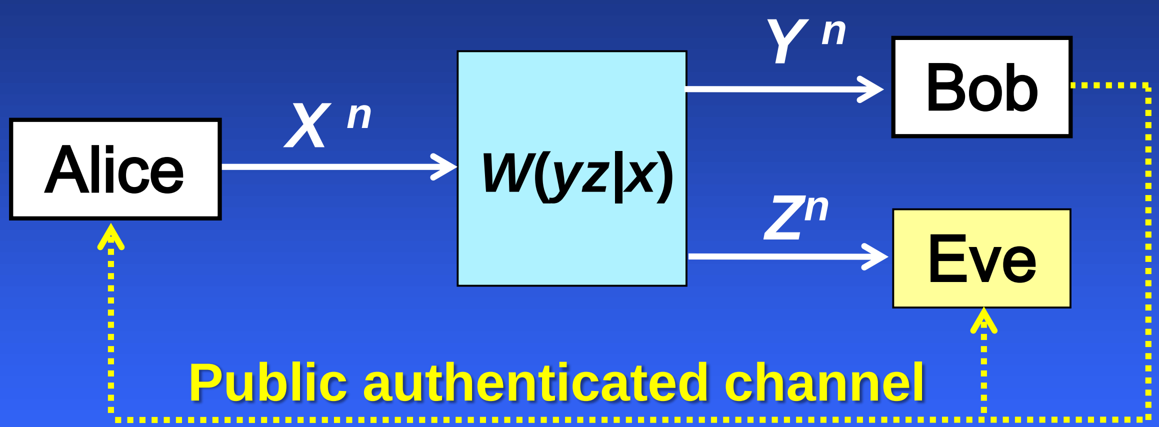


Finite length analysis

Han, Endo, and Sasaki, IEEE-IT60(11), 6819 (2014).

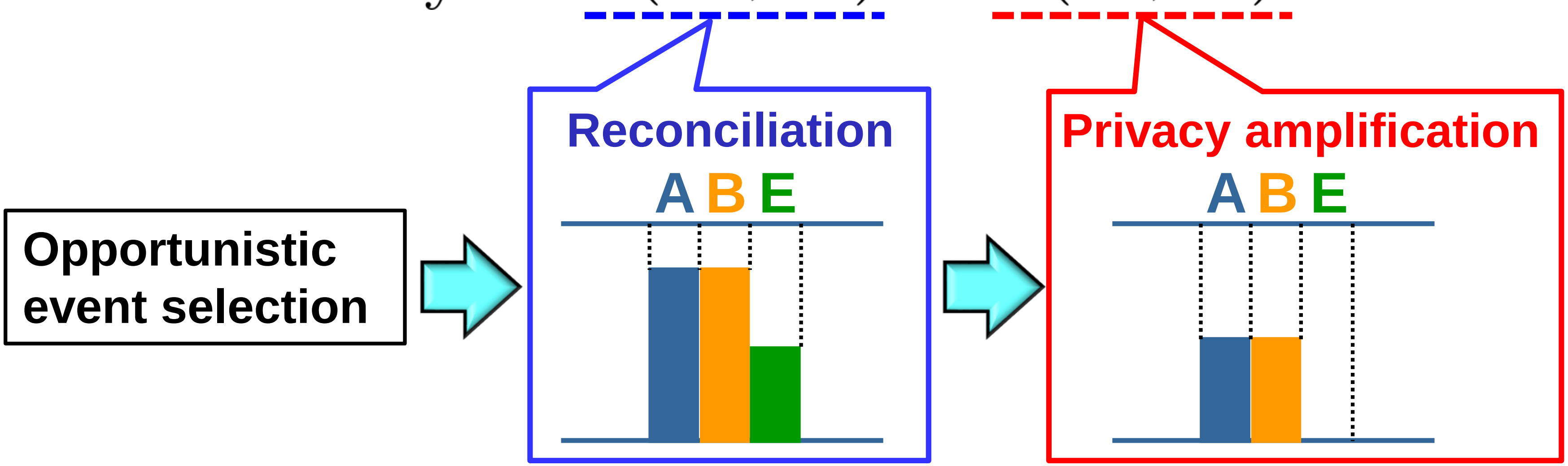


Secret key agreement

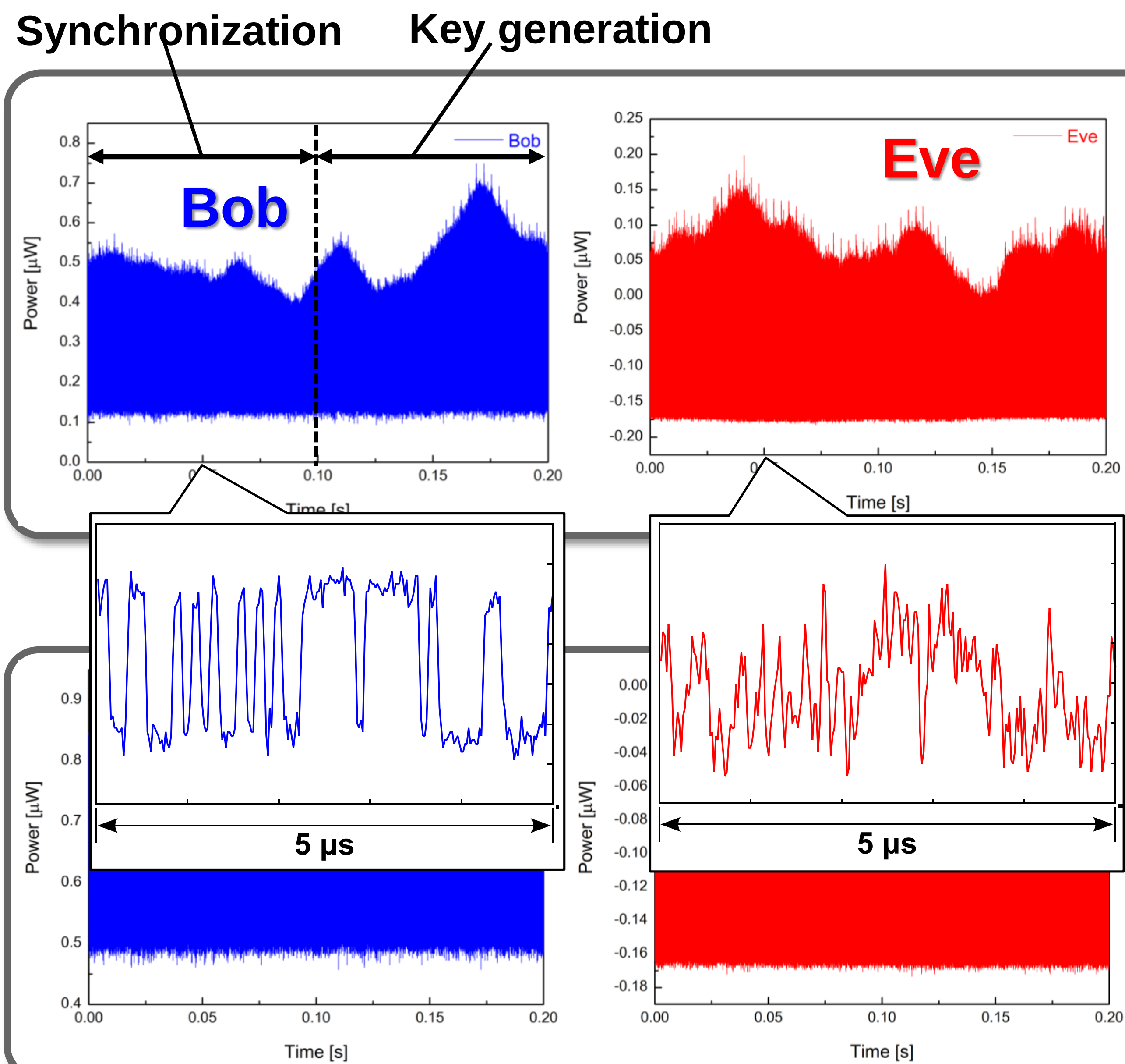


Secret key rate

$$R_{\mathrm{Key}} = I(X;Y) - I(Y;Z)$$



Secret key agreement



2015/11/17 14:53

Key rate

4.21 Mbps

(421 kbits/100 ms)

Channel attenuation
-60dB

2015/11/17 18:20

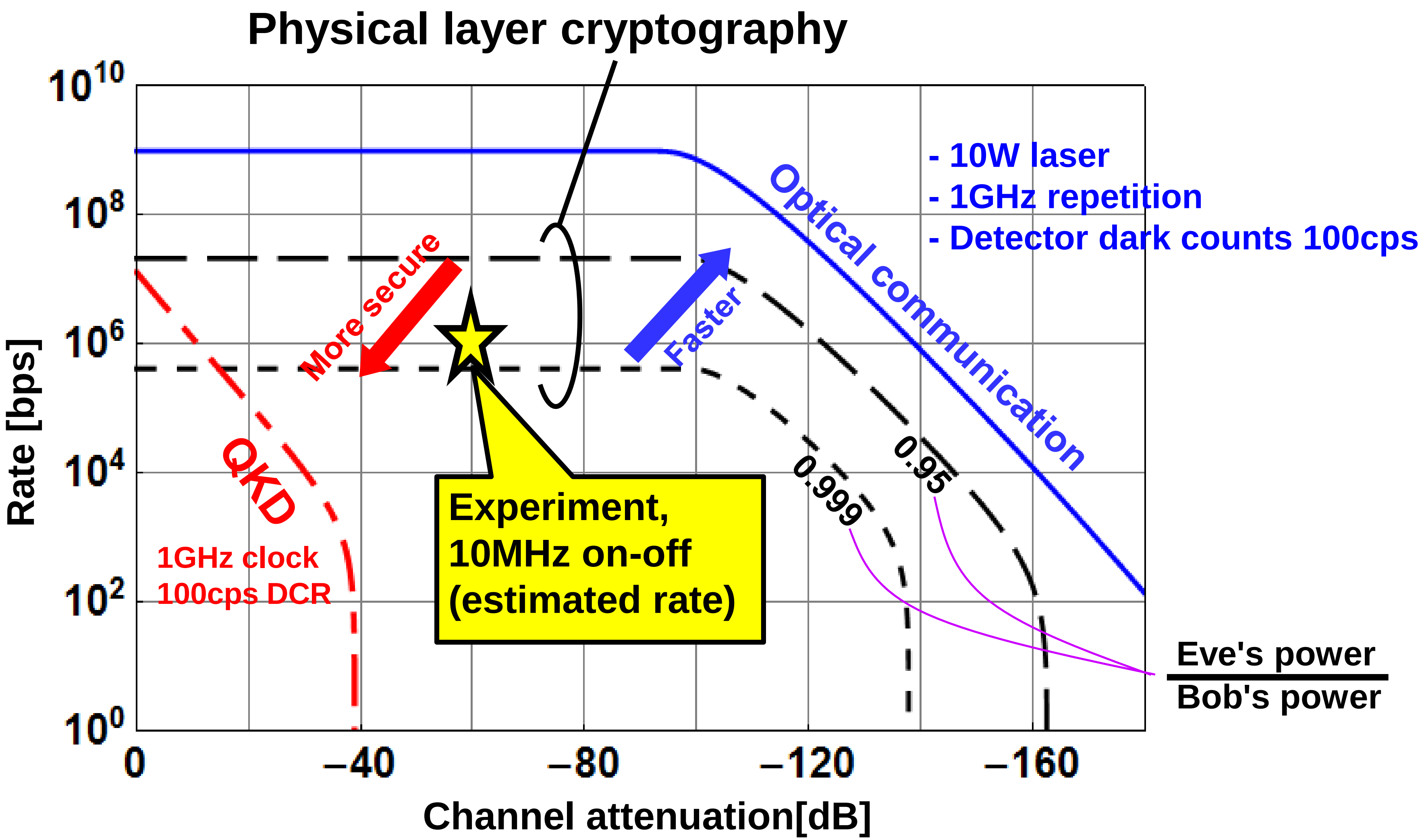
Key rate

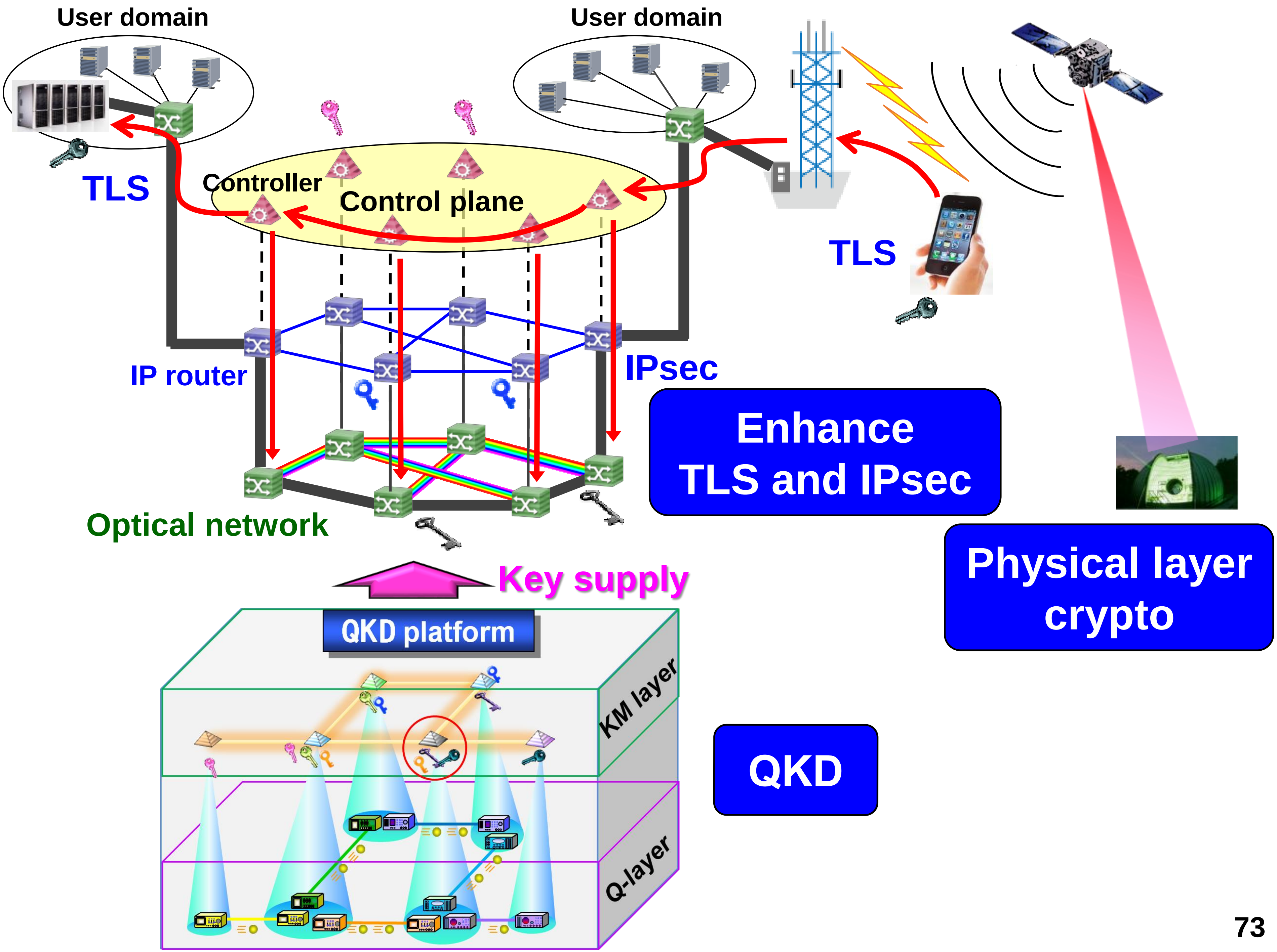
24 kbps

(2.4 kbits/100 ms)

Channel attenuation
-60dB

Simulation for FSO links




User domain
User domain
TLS
Controller
Control plane
TLS
IP router
IPsec
Enhance
TLS and IPsec
Optical network
Physical layer
crypto
Key supply
QKD platform
KM layer
QKD
Q-layer

Thank you for your attention