Gap between QKD security proof and its implementation -Challenges in QKD Certification in Japan-

NICT

Go Kato

Position of theorists proving the security of QKD

QKD system is secure,
if the equipment fulfills
all the requirements.

Requirements are
mathematically defined.

Ex.

Sender (Alice) generates a coherent state:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{n!} |n\rangle$$

Any fluctuation is unacceptable.

We need to find requirements that are acceptable to theorists and in the certification process.

Since gaps exist between mathematically defined and verifiable requirements, there is no solution that satisfies everyone.

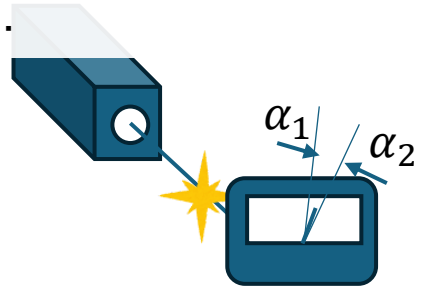
Circumstances when certifying a QKD system

Certification is made by confirming that the requirements approved by the expert have been fulfilled.

Requirements must be
defined in a verifiable manner.

Ex.

The intensity of the laser light produced by Alice is between α_1 and α_2 with a probability of 99.9%.



Contents

- Gaps of physical requirements for the components
- Gaps of requirements for the information processing
- Discussion
- Conclusion

Contents

- Gaps of physical requirements for the components
- Gaps of requirements for the information processing
- Discussion
- Conclusion

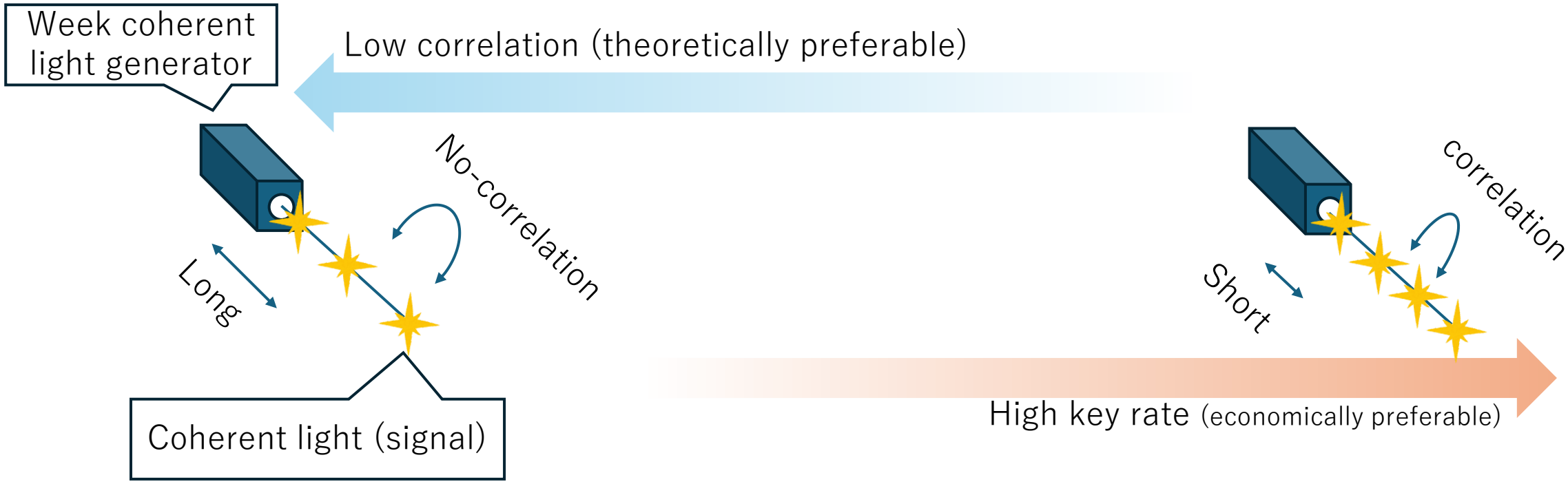
The primary issue in establishing certification criteria for QKD equipment is how to evaluate the physical characteristics of the components.

This is because it is impossible to verify that the physical requirements are perfectly fulfilled.

Gaps of physical requirements for the components Example1

Causes of Imperfection ： Hysteresis effects in state preparation

- Increasing the repetition rate causes correlation between signals.

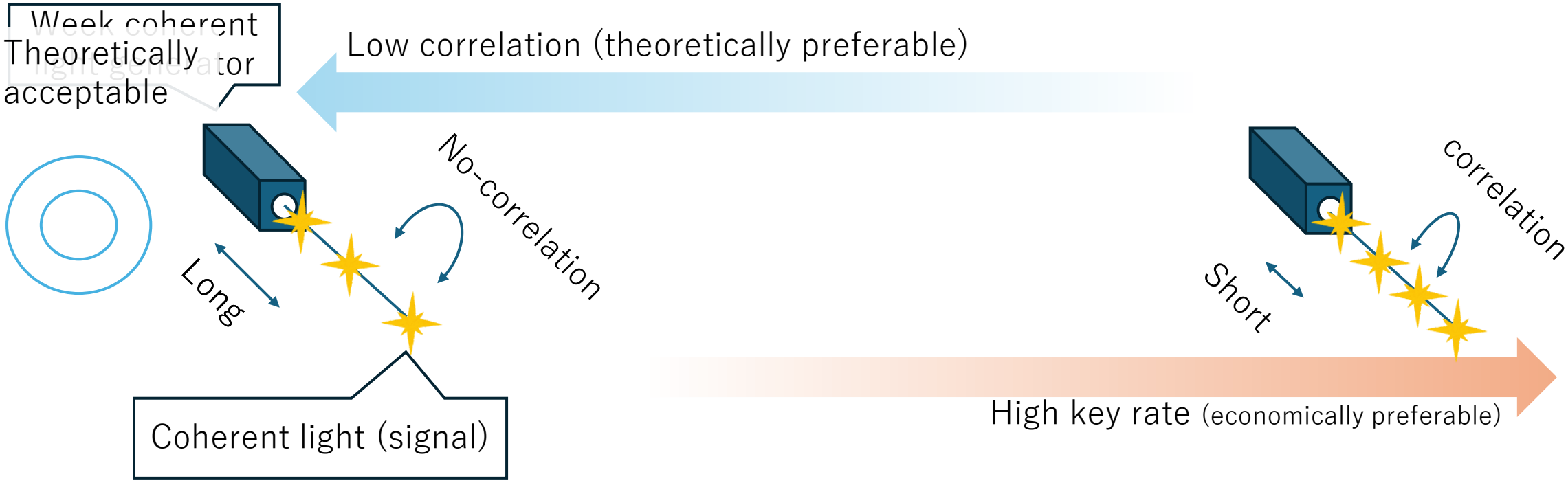


Plane of the polarization is randomly selected

Gaps of physical requirements for the components
Example1

Causes of Imperfection ： Hysteresis effects in state preparation

- Almost all the security proofs require that
  there is no correlation between signals.

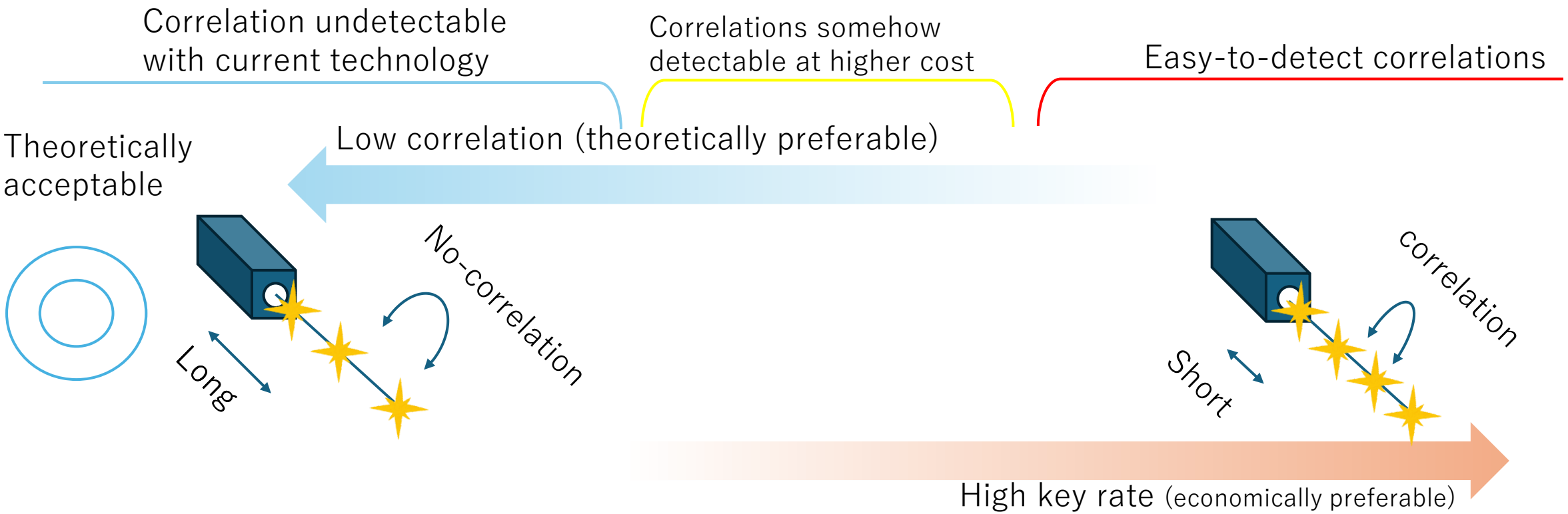


Plane of the polarization is randomly selected

Gaps of physical requirements for the components Example1

Causes of Imperfection ： Hysteresis effects in state preparation

- No testing device can prove a complete absence of correlation.

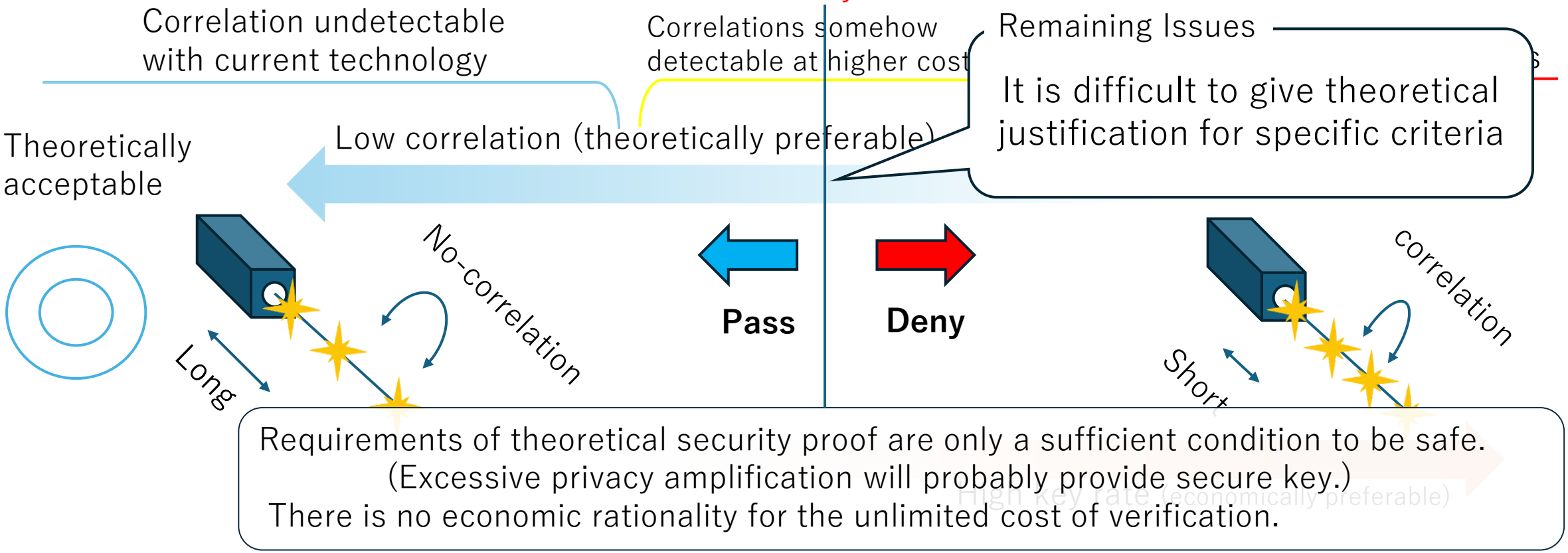


Gaps of physical requirements for the components
Countermeasure1

Causes of Imperfection ： Hysteresis effects in state preparation

- We will accept any equipment that is not rejected by the hypothesis test.

※We do not test at the limit accuracy of the measurement

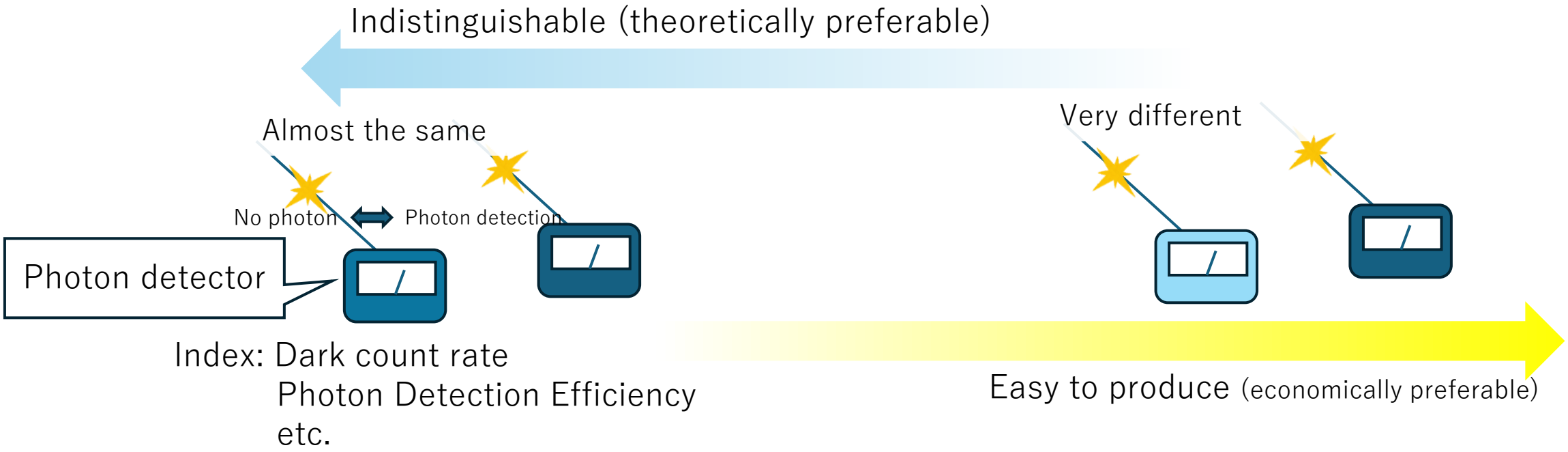


Requirements of theoretical security proof are only a sufficient condition to be safe.
(Excessive privacy amplification will probably provide secure key.)
There is no economic rationality for the unlimited cost of verification.

Gaps of physical requirements for the components Example2

Causes of Imperfection ： Variance of measuring instruments

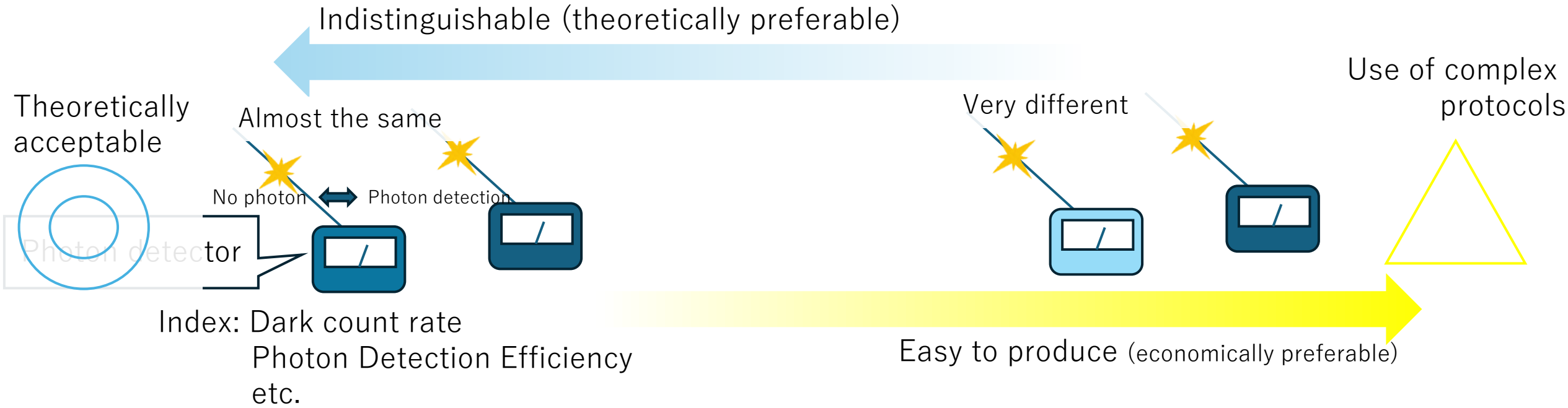
- The presence of individuality in photon detectors is inevitable.



Gaps of physical requirements for the components Example2

Causes of Imperfection ： Variance of measuring instruments

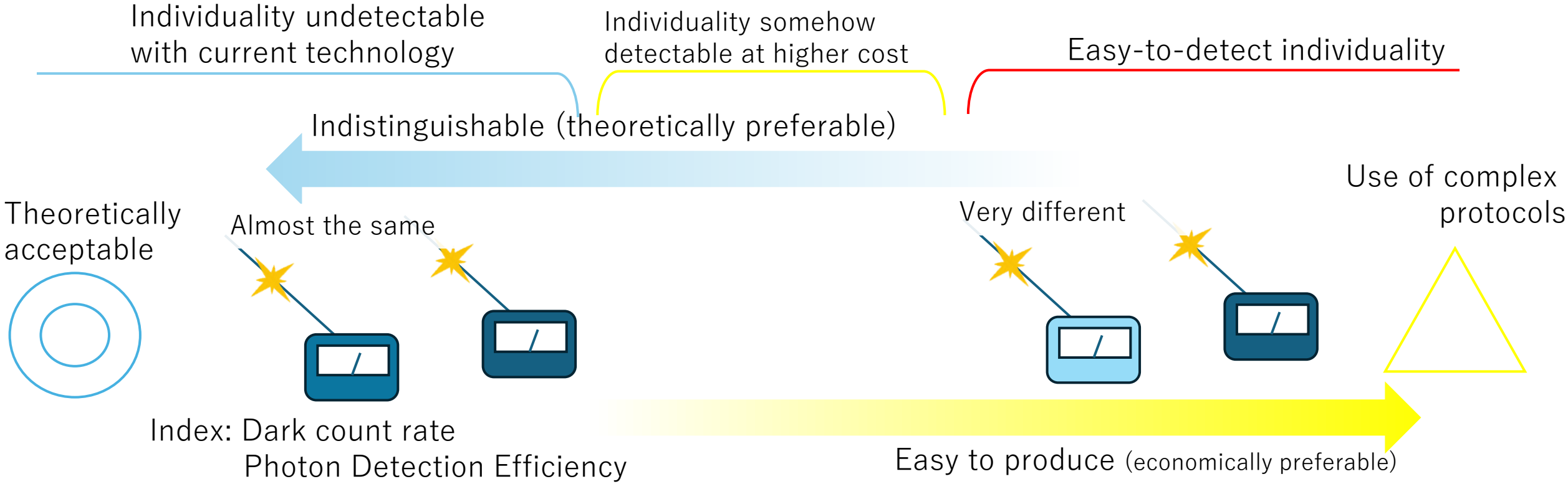
- By modifying the protocol, this problem can be avoided.
  However, there are drawbacks, such as increased equipment complexity.



Gaps of physical requirements for the components Example2

Causes of Imperfection ： Variance of measuring instruments

- By modifying the protocol, this problem can be avoided.
  However, there are drawbacks, such as increased equipment complexity.



Gaps of physical requirements for the components

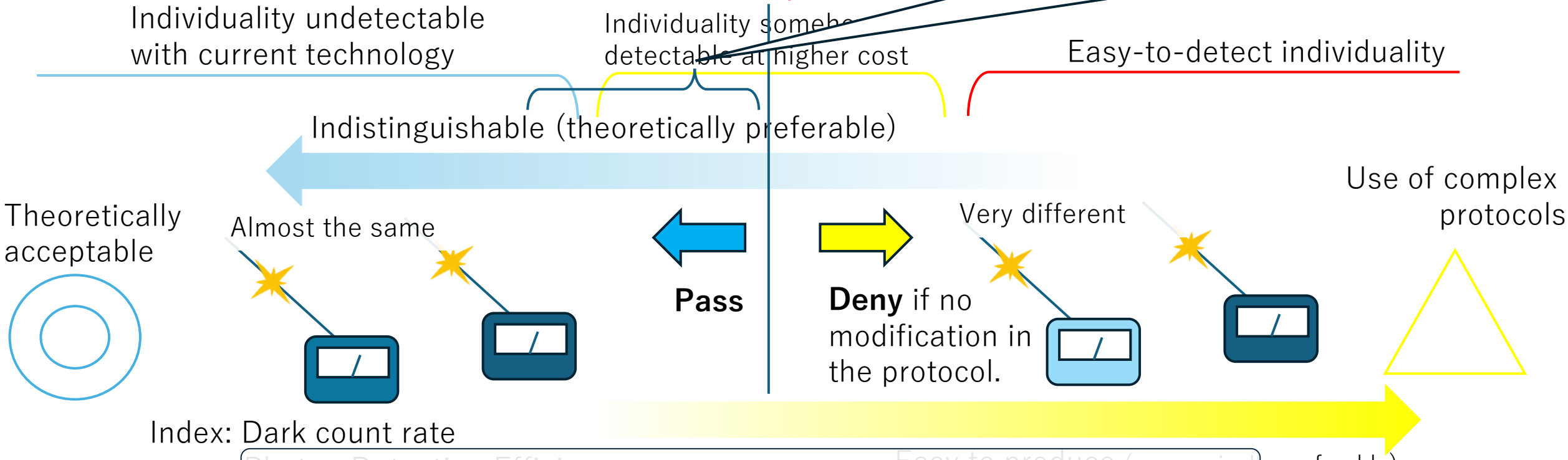
Remaining Issues countermeasure?

Causes of Imperfection ： Variance of measuring instrur

- We will accept any equipment that is n

※We do not test at the limit accuracy of t

Can we ignore the problem of imperfection, which can be completely resolved, just for economic reasons?



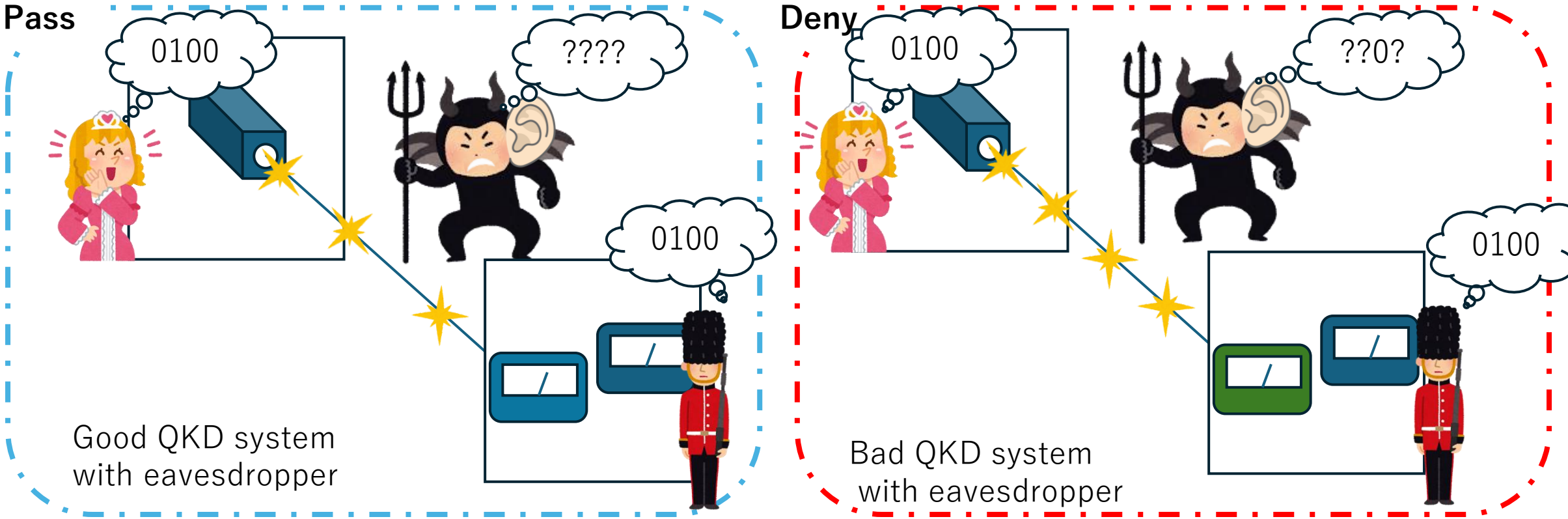
There is no economic rationality for the unlimited cost of verification.

We can not exclude all equipment which has imperfection.

Gaps of physical requirements for the components
Additional Countermeasure

(Safety net)

- We will additionally check the QKD system with penetration testing.

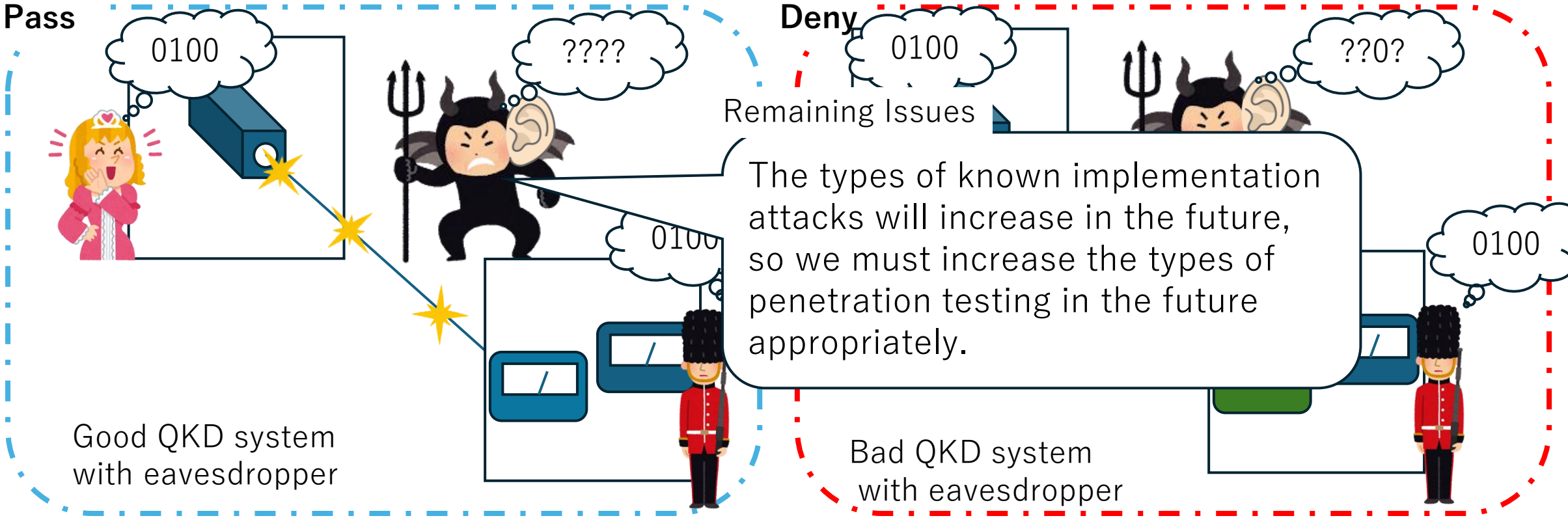


※"A Study on Implementation Attacks against QKD Systems" by federal office for information security

Gaps of physical requirements for the components
Additional Countermeasure

(Safety net)

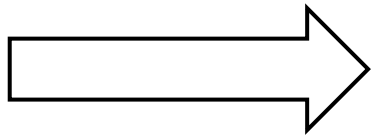
- We will additionally check the QKD system with penetration testing.



※"A Study on Implementation Attacks against QKD Systems" by federal office for information security

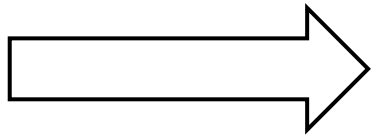
Short summary

- It is impossible to reject all equipment with imperfections through testing.
- It is practically impossible to achieve ε -security in a strict manner.
- Some imperfections can be resolved theoretically, though economically costly.



Even on issues that can be solved theoretically, some compromises will be justified.

- Are the gaps that need to be dealt with only related to the physical components?



No. There is also room for justified compromise in gaps of requirements for the information processing.

Contents

- Gaps of physical requirements for the components
- Gaps of requirements for the information processing
- Discussion
- Conclusion

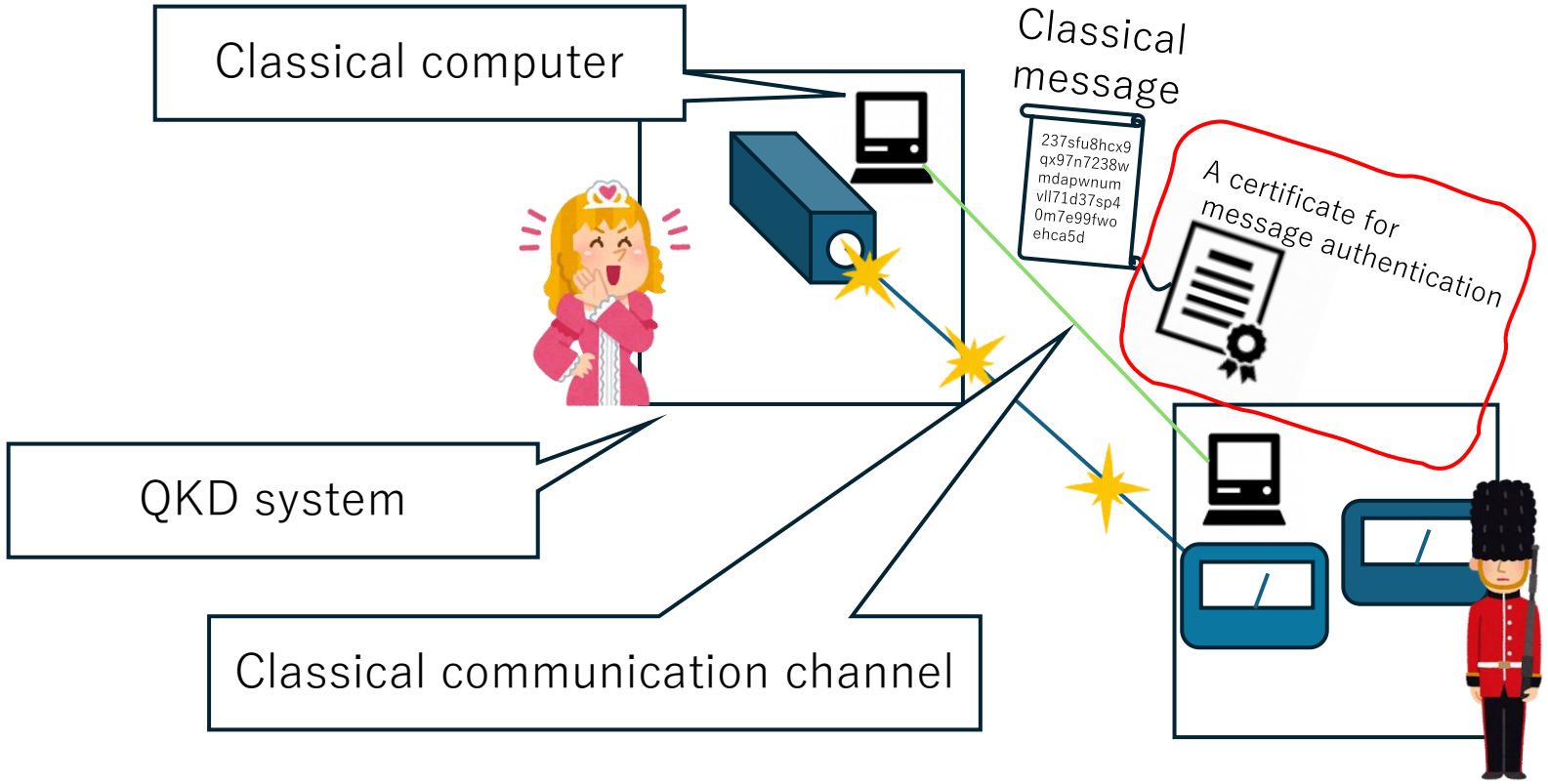
There is also room for justified compromise in gaps of requirements for the information processing.

(Requirements for information processing have not been discussed so much because they can be accomplished with economical costs.)

Gaps of requirements for the information processing Example1

Compromising Factor： Message authentication

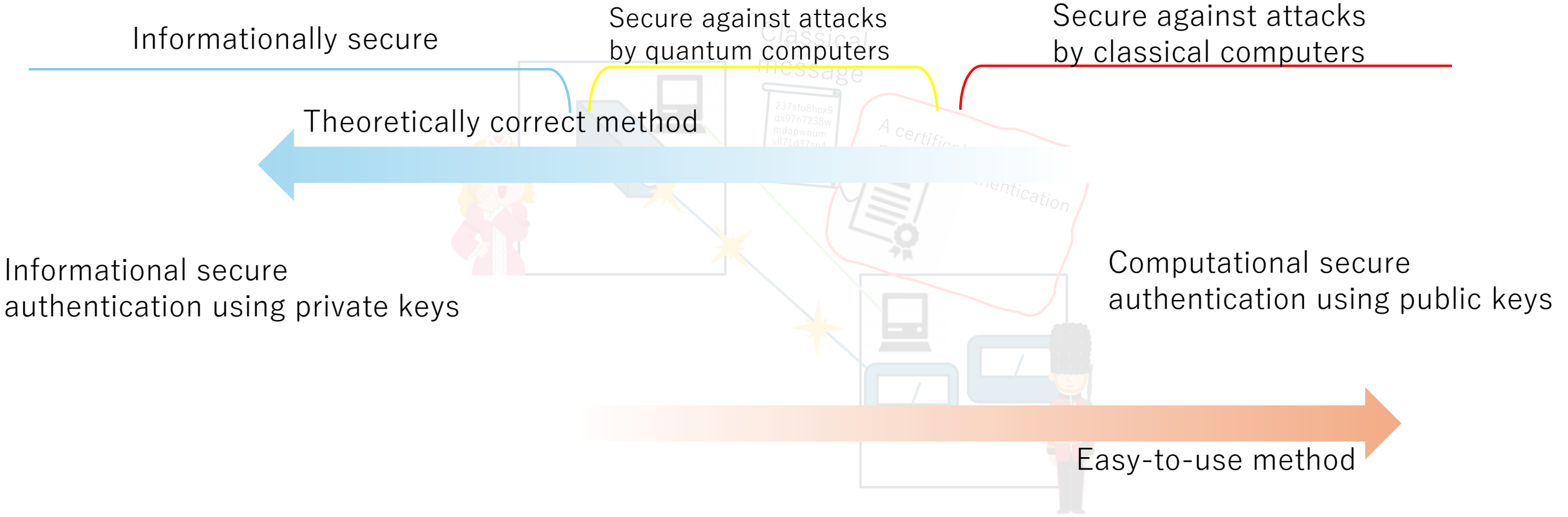
- There is a possibility that Post Quantum Cryptography (PQC) is used to ensure that the public classical communication channel has not been tampered with.



Gaps of requirements for the information processing Example1

Compromising Factor： Message authentication

- There is a possibility that Post Quantum Cryptography (PQC) is used to ensure that the public classical communication channel has not been tampered with.

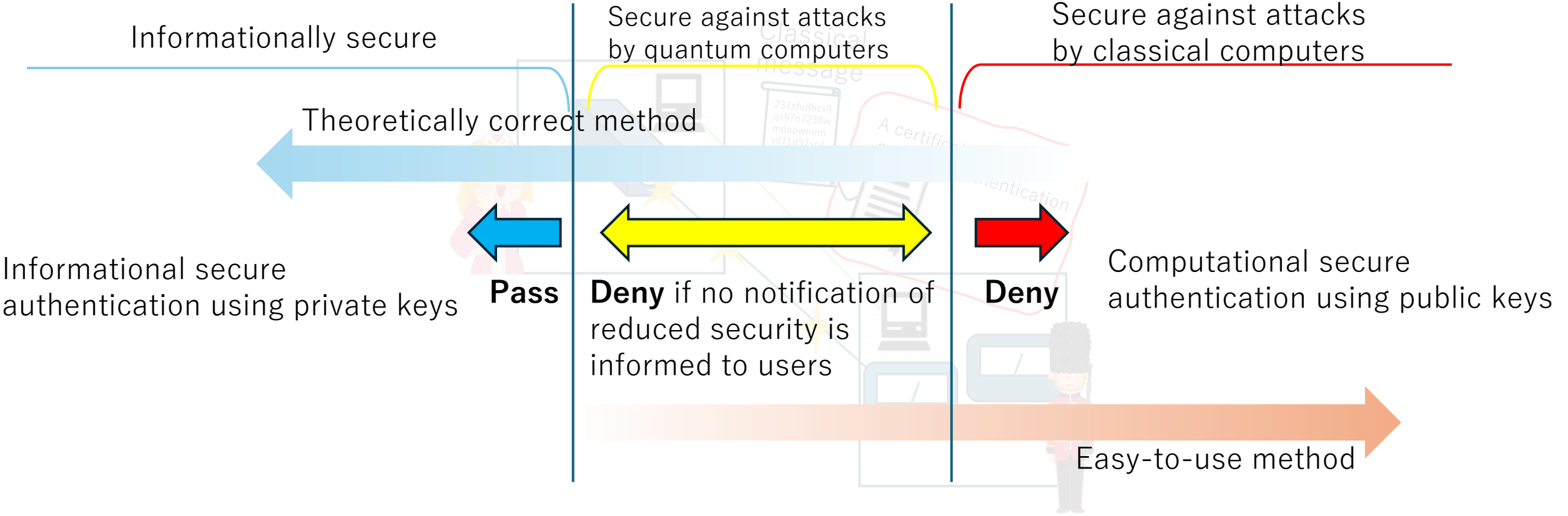


The strategy “Harvest Now, Decrypt Later” does not work

Gaps of requirements for the information processing Countermeasure1

Compromising Factor： Message authentication

- We will require users to be explicitly informed that there is only a lower level of security when the QKD system using message authentication by PQC etc.



The strategy “Harvest Now, Decrypt Later” does not work

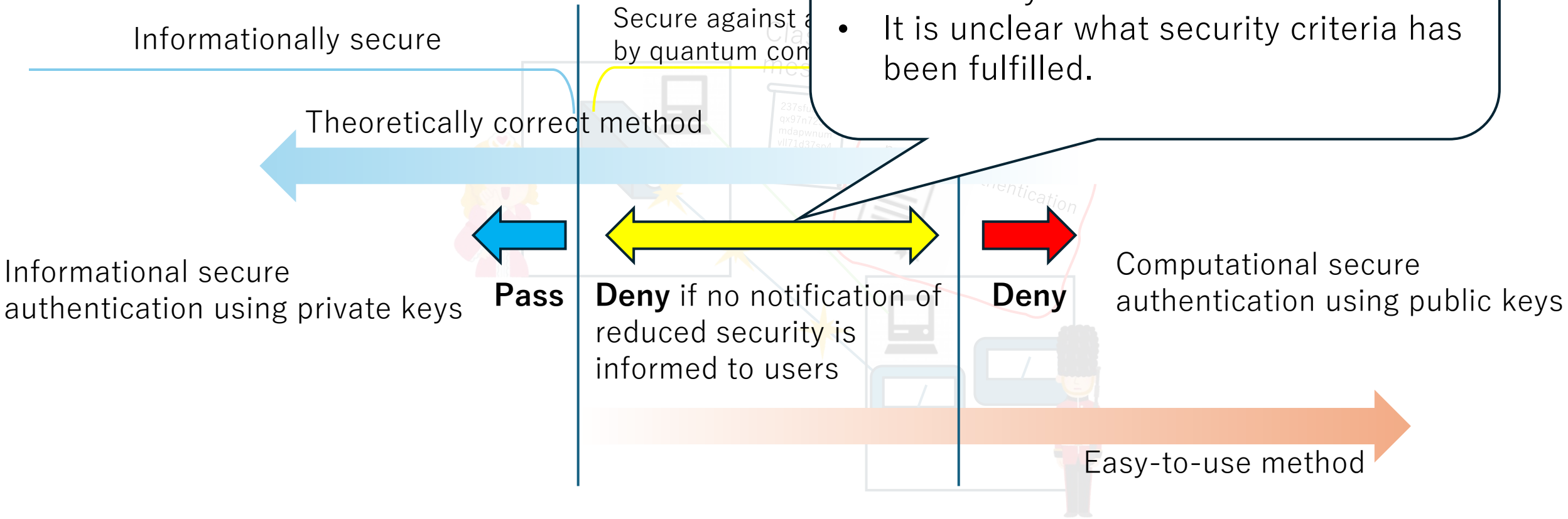
Gaps of requirements for the information processing

Compromising Factor： Message authentication

- We will require users to be explicitly inf
  of security when the QKD system using

Remaining Issues countermeasure1

- We lose the most important selling point of QKD, "the ability to generate information-theoretically secure secret keys.“
- It is unclear what security criteria has been fulfilled.

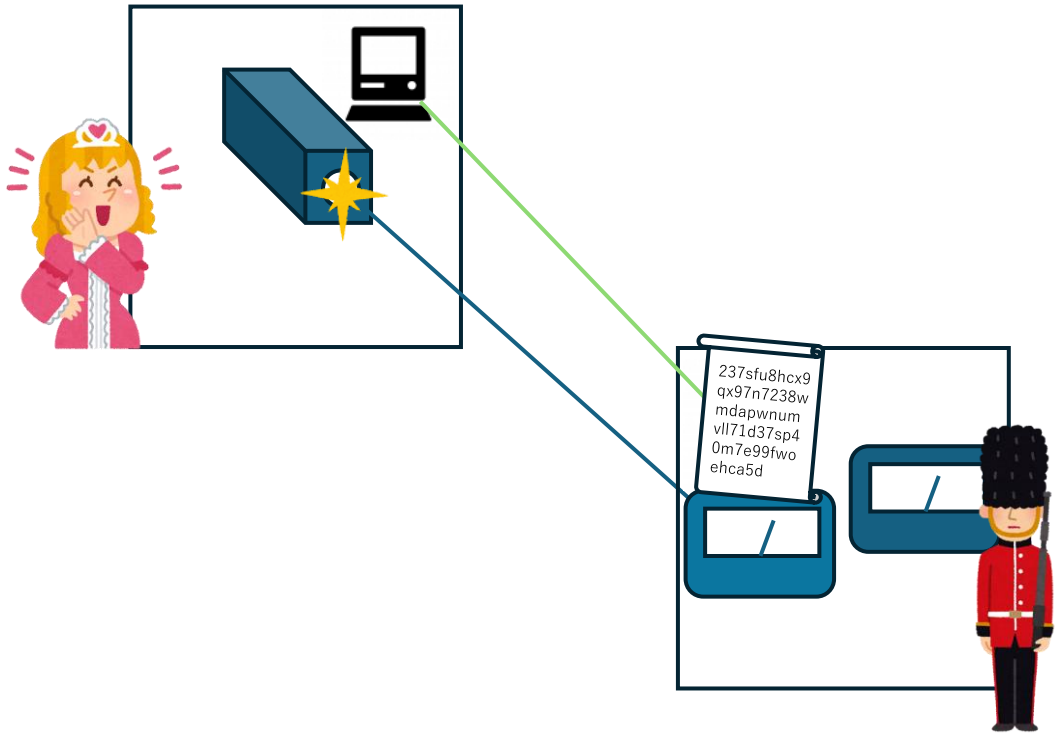


The strategy “Harvest Now, Decrypt Later” does not work

Gaps of requirements for the information processing Example2

Compromising Factor : Order of communication

- Flexible handling with respect to the order of communication gives economic benefits.



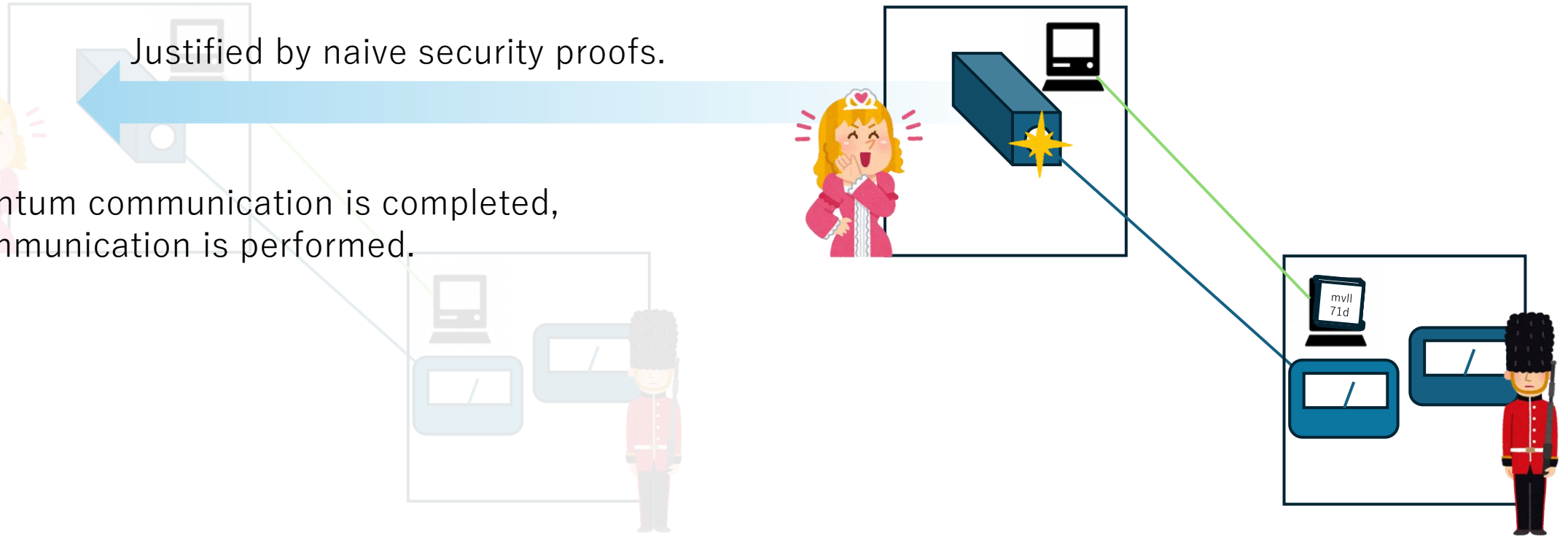
Gaps of requirements for the information processing
Example2

Compromising Factor : Order of communication

- Flexible handling with respect to the order of classical communication gives economic benefits.

Justified by naive security proofs.

After all quantum communication is completed,
classical communication is performed.



Gaps of requirements for the information processing Example2

Compromising Factor : Order of communication

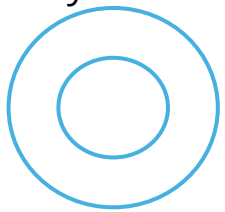
- Flexible handling with respect to the order of classical communication gives economic benefits.

A carefully designed protocol which uses small memory

Justified by naive security proofs.

After all quantum communication is completed, classical communication is performed.

A simple protocol which uses large memory



Sending classical information in parallel with quantum signals.

Reduction of memory size and other resources that must be used by the equipment.

Gaps of requirements for the information processing Countermeasure2

Compromising Factor : Order of communication

- We will force vendors to produce a security proof precisely for the used protocol.

A carefully designed protocol which uses small memory

Justified by naive security proofs.

After all quantum communication is completed, classical communication is performed.

A simple protocol which uses large memory

Sending classical information in parallel with quantum signals.

Reduction of memory size and other resources that must be used by the equipment.

Gaps of requirem ocessing ermeasure2

Compromising Factor : Order of co

- We will force vendors to the used protocol.

Remaining Issues

- QKD theorists need to understand the details of the protocols used by the QKD system and carefully build security proofs.
- Despite the theoretical difficulties in dealing with this point, this treatment often do not have a serious effect for the security.

A carefully designed protocol which uses small memory

Justified by naive security proofs.

After all quantum communication is completed, classical communication is performed.

A simple protocol which uses large memory

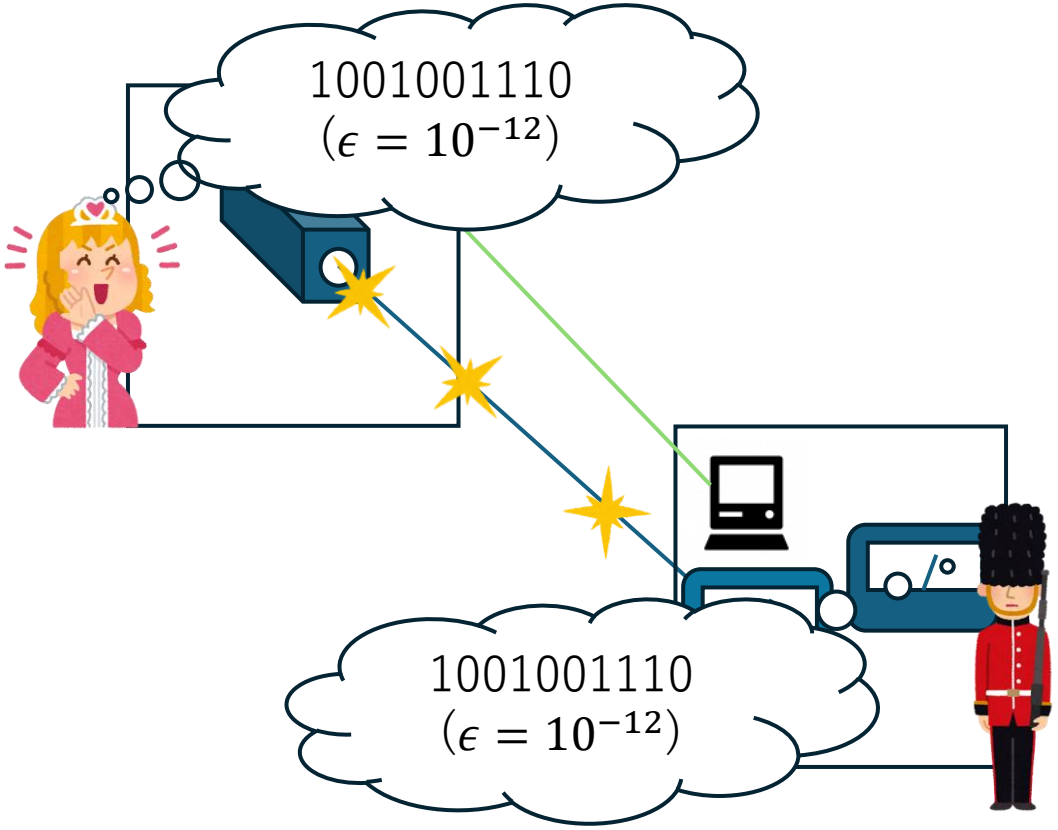
Sending classical information in parallel with quantum signals.

Reduction of memory size and other resources that must be used by the equipment.

Gaps of requirements for the information processing Example3

Compromising Factor：treatment of the security parameter

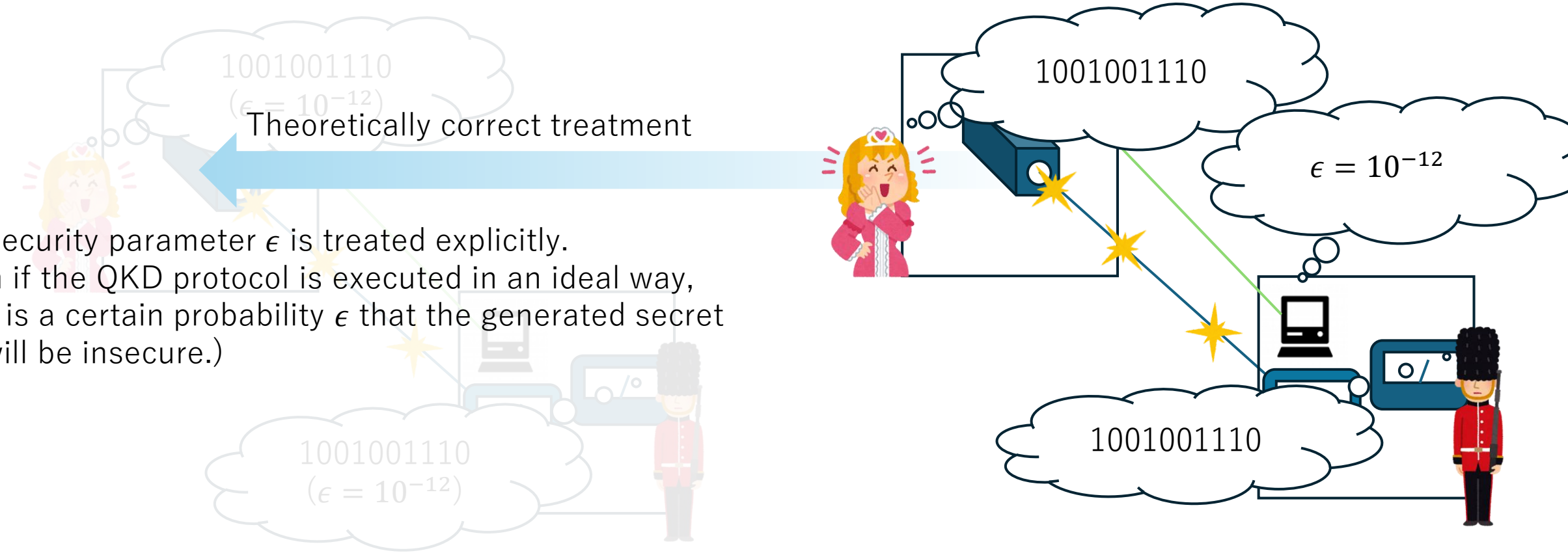
- Due to the imperfections of the physical devise,
  the security parameters that theory suggests do not make much sense.



Gaps of requirements for the information processing Example3

Compromising Factor：treatment of the security parameter

- Due to the imperfections of the physical devise,
  the security parameters that theory suggests do not make much sense.

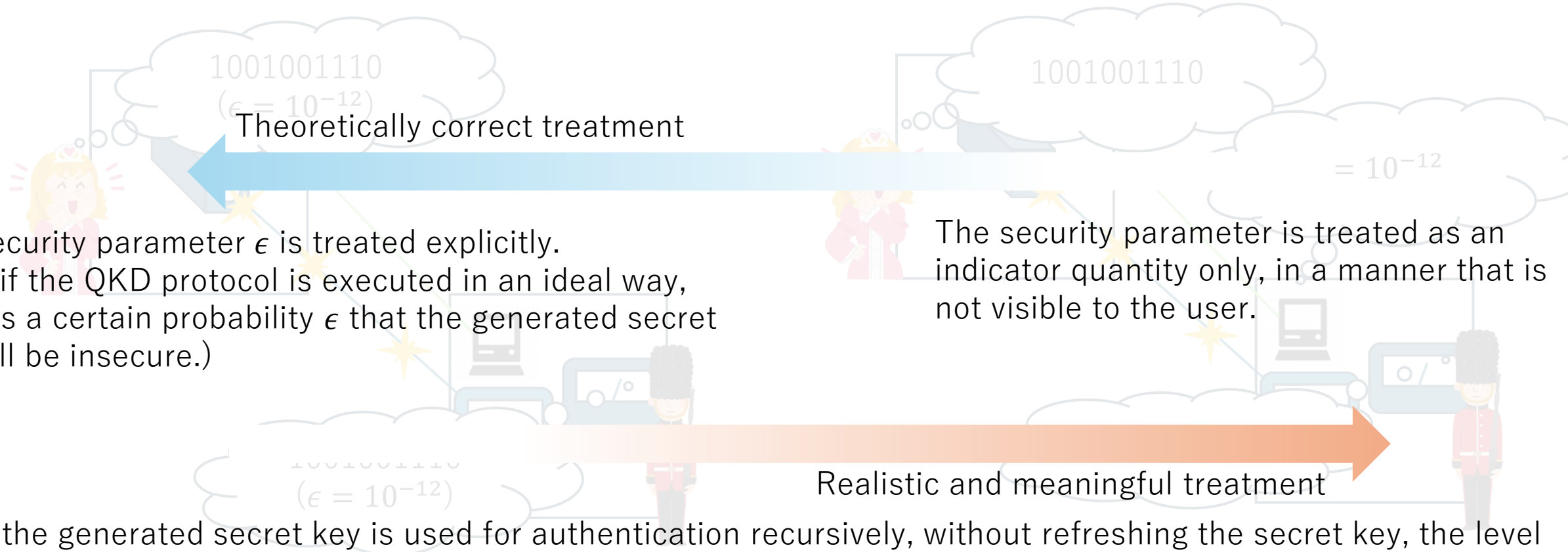


The security parameter ϵ is treated explicitly.
(Even if the QKD protocol is executed in an ideal way, there is a certain probability ϵ that the generated secret key will be insecure.)

Gaps of requirements for the information processing Example3

Compromising Factor：treatment of the security parameter

- Due to the imperfections of the physical devise,
  the security parameters that theory suggests do not make much sense.

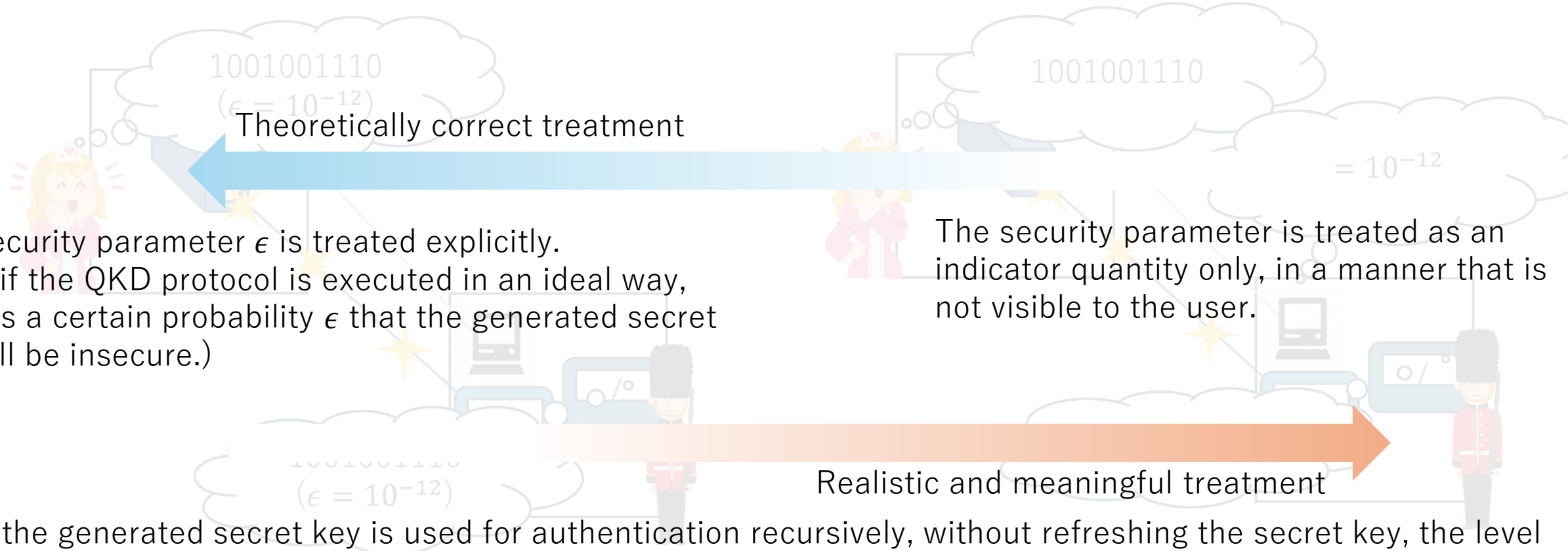


Since the generated secret key is used for authentication recursively, without refreshing the secret key, the level of security is certainly reduced gradually with continuous use of QKD, i.e. ϵ must gradually increase.

Gaps of requirements for the information processing Countermeasure3

Compromising Factor：treatment of the security parameter

- We will limit the number of recursive uses of the secret key generated for message authentication.



The security parameter ϵ is treated explicitly.
(Even if the QKD protocol is executed in an ideal way, there is a certain probability ϵ that the generated secret key will be insecure.)

The security parameter is treated as an indicator quantity only, in a manner that is not visible to the user.

Since the generated secret key is used for authentication recursively, without refreshing the secret key, the level of security is certainly reduced gradually with continuous use of QKD, i.e. ϵ must gradually increase.

Gaps of requirements for the information processing Countermeasure3

Compromising Factor：treatment of the security parameter

- We will limit the number of recursive uses of the secret key generated for message authentication.

Remaining Issues

- There is no logical justification for the number of limits.

Theoretically

The security parameter ϵ is treated explicitly.
(Even if the QKD protocol is executed in an ideal way, there is a certain probability ϵ that the generated secret key will be insecure.)

The security parameter is treated as an indicator quantity only, in a manner that is not visible to the user.

Realistic and meaningful treatment

Since the generated secret key is used for authentication recursively, without refreshing the secret key, the level of security is certainly reduced gradually with continuous use of QKD, i.e. ϵ must gradually increase.

Discussion

- Even if there is a theory which claims unconditional security, "compromises" are necessary because the gap between reality and theory cannot be reduced to zero.
- Even if there are a way to partially fill the gap theoretically, there is room to consider whether it would be better not to do so.
- The lack of a basis for determining what level of compromise is reasonable is a major problem.

The usual security criteria of the QKD are defined for the capabilities of eavesdroppers, such as coherent attack and individual attack. This definition is convenient to the analysis. However, as we have shown here, when we consider realistic security, it will be valuable to construct a security proof with a completely different security criteria.

Conclusion

- In some cases, trying to fill the gap between theory and reality as much as possible does not necessarily contribute to improved security or value for the user of QKD system. In other words, certain compromises must be made even from a theoretical perspective.
- It is strongly desired to establish a logic to determine acceptable levels for gaps that cannot be filled.