Activity toward QKD certification in Japan

- Drafting of two types of documents are under way.
  - PP (protection profile)

    High-level description of security requirement for QKD systems.

    Targeted EAL (evaluation assurance level) : EAL 2

    A QKD module is in a trusted node.
    No site audit necessary.

    cf. ESTI PP: EAL 4+

    Collaboration with ESTI for drafting the PPs.

  - EMD (evaluation method document)

    Specifies or exemplifies evaluation methods for various security requirements for QKD modules.

- Japan team consists of

(National institute) NICT
(Vendors) Toshiba, NEC
(Academia) Univ of Tokyo
Hokkaido Univ
Keio Univ

consulting ECSEC Laboratory (Evaluation lab)

supported by Japanese government ministries

The security proof and QKD certification

Masato KOASHI

Univ. of Tokyo

The security proof of QKD

・Specify a particular protocol

1. Alice prepares an optical pulse in state ⋯
2. Bob receives the pulse and measures⋯
3. ⋯

10. Each of Alice and Bob extracts a final key of a length $K = f(data, \epsilon)$

・Specify a physical model of the transmitter and the receiver. Clarify the adopted assumptions.

・Quantum states of emitted optical pulses
・Quantum description of the receiver's measurement
・Round independence of preparations and measurements
・Security boundaries
・……

+ Law of quantum mechanics

・Prove the ϵ-security of the protocol

Sufficient for the security

Assumption 1

Assumption 2

Assumption 3

ϵ-security

Prob("a bad thing happens" | The actual QKD device was used)

$\leq$ Prob("a bad thing happens" | A perfect QKD device were used) + $\epsilon \times$(# of use)

e.g., $\epsilon = 10^{-15}$

Implementation security: relaxing the assumptions

The assumptions in a security proof should be relaxed all the way to ⋯

Impractical

Practical

Verifiable
(via a state-of-the-art technology)

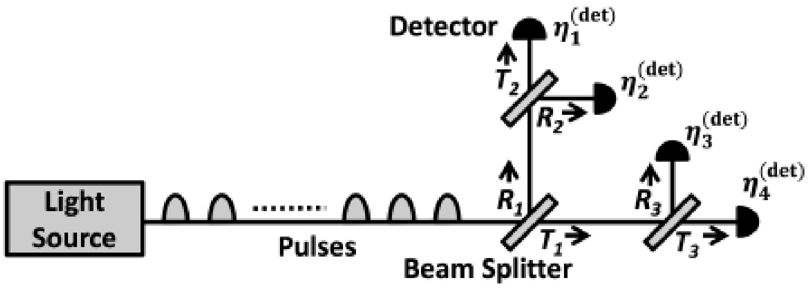
Verifiable
(at reasonable cost)

Example: Decoy-BB84 protocol
Photon number distribution $p(n)$ of a pulse emitted by the QKD transmitter.

$p(n) = e^{-\mu}\mu^n/n!$ for $n = 0,1,2,\ldots,\infty$

Poissonian distribution (ideal laser pulses)

$$\frac{e^{-\mu}\mu^n}{n!} - \Delta_n \le p(n) \le \frac{e^{-\mu}\mu^n}{n!} + \Delta_n$$
for $n = 0,1,2,\ldots,\infty$



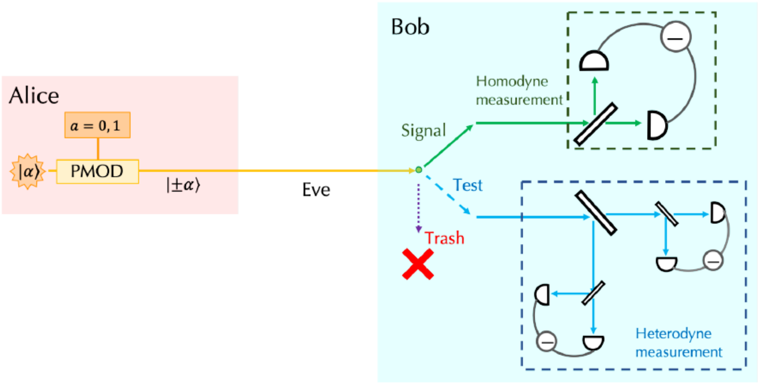
Coincidence rates for four photon detectors

Various QKD protocols

- Decoy-BB84 protocols
  - The most matured
- CV-QKD protocols

(Continuous-Value)

  - Homodyne receivers instead of photon detectors
  - Lower costs
  - Affinity to optical communication technology like WDM

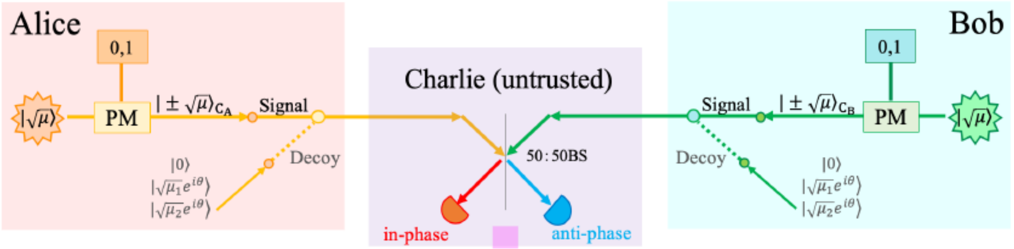


- Twin-Field-type protocols
  - Coves a longer distance
  - No security requirement for the receiver

(belonging to MDI protocols)

(Measurement-Device-Independent)

- Others ...



Implementation security: relaxing the assumptions

The assumptions in a security proof should be relaxed all the way to …

Impractical

Practical

Verifiable
(via a state-of-the-art technology)

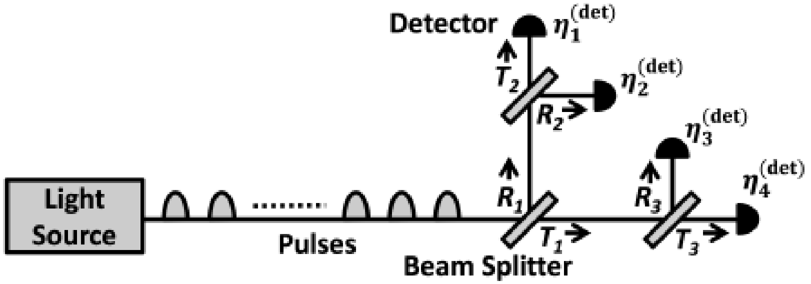
Verifiable
(at reasonable cost)

Example: Decoy-BB84 protocol
Photon number distribution $p(n)$ of a pulse emitted by the QKD transmitter.

$p(n) = e^{-\mu}\mu^n/n!$ for $n = 0,1,2,\ldots,\infty$

Poissonian distribution (ideal laser pulses)

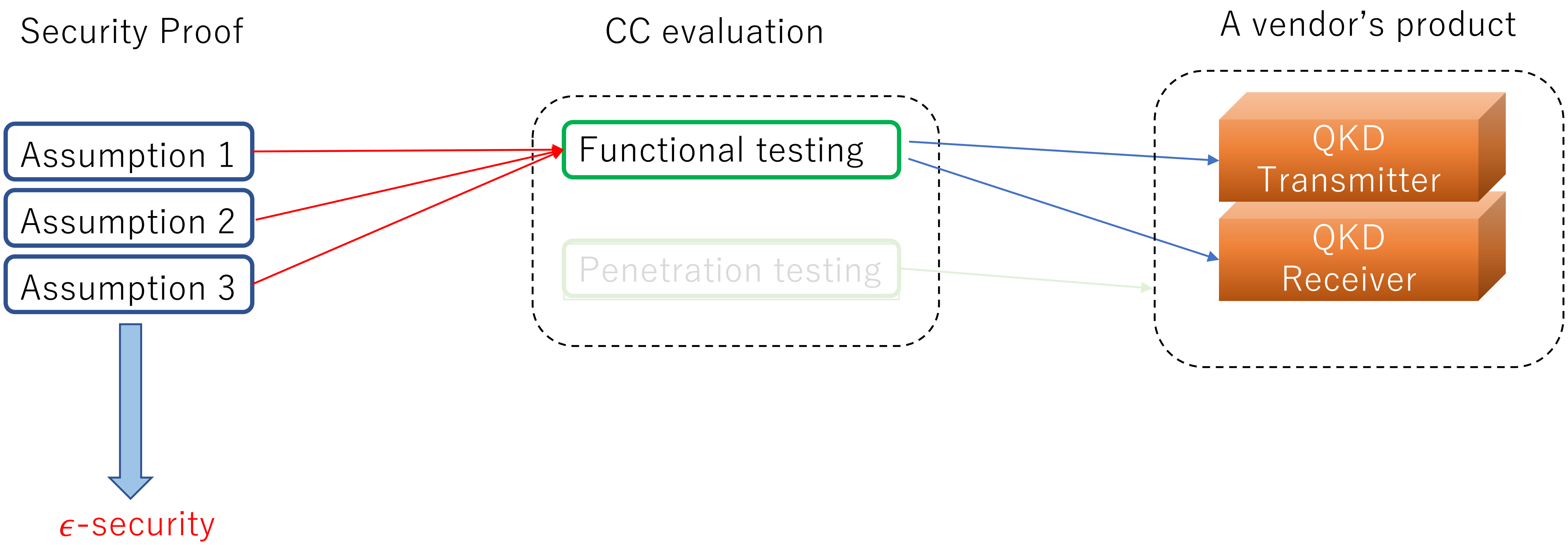
$$\frac{e^{-\mu}\mu^n}{n!} - \Delta_n \le p(n) \le \frac{e^{-\mu}\mu^n}{n!} + \Delta_n$$
for $n = 0,1,2,\ldots,\infty$



Coincidence rates for four photon detectors

In a perfect world …

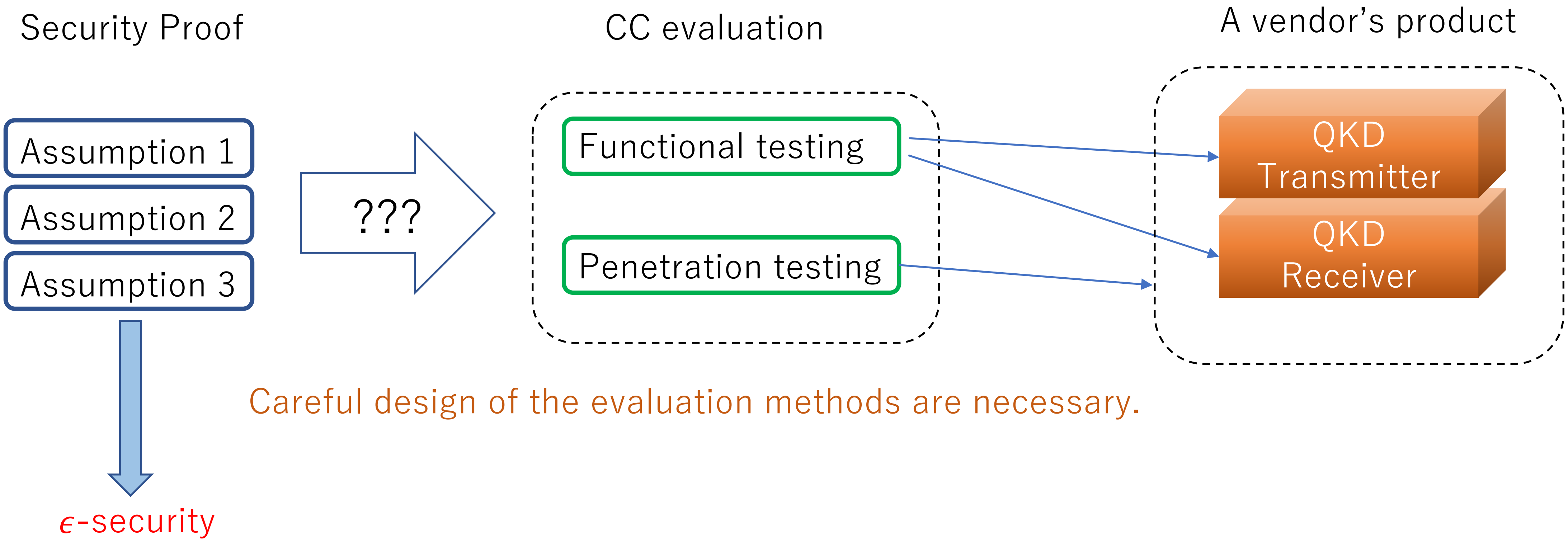
If every assumption were verified by a feasible test, it would be very simple ⋯



But this will not be the case.

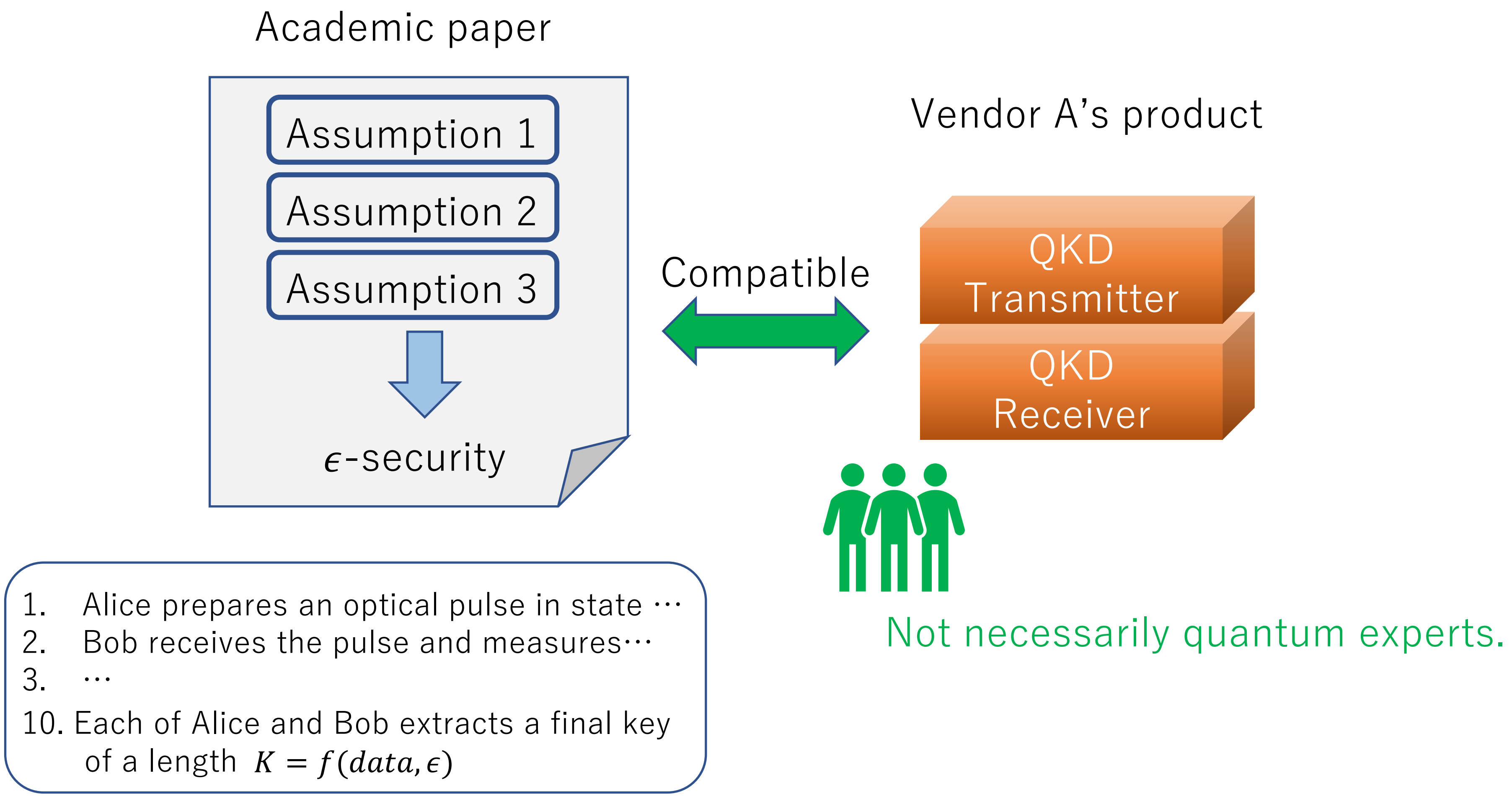
Design of the two types of tests

We must accept that there are unverifiable assumptions



Careful design of the evaluation methods are necessary.

Use of academic paper on security proof



Use of academic paper on security proof