Quantum Encryption with Certified Deletion, Revisited: Public Key, Attribute-Based, and Classical Communication

arXiv:2105.05393

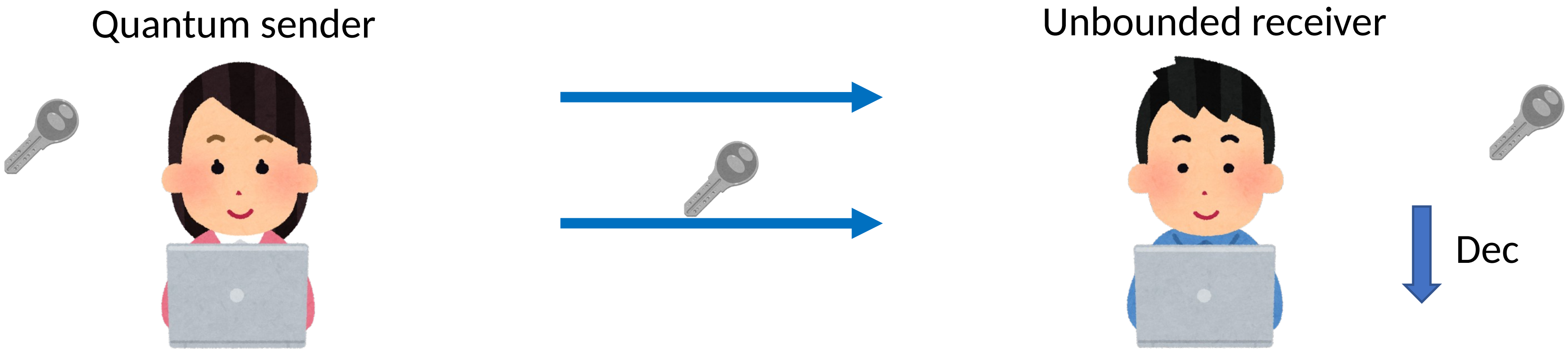
Taiga Hiroka[1] Tomoyuki Morimae[1] Ryo Nishimaki[2] Takashi Yamakawa[2]

[1]Yukawa Institute for Theoretical Physics, Kyoto University

[2]NTT Corporation

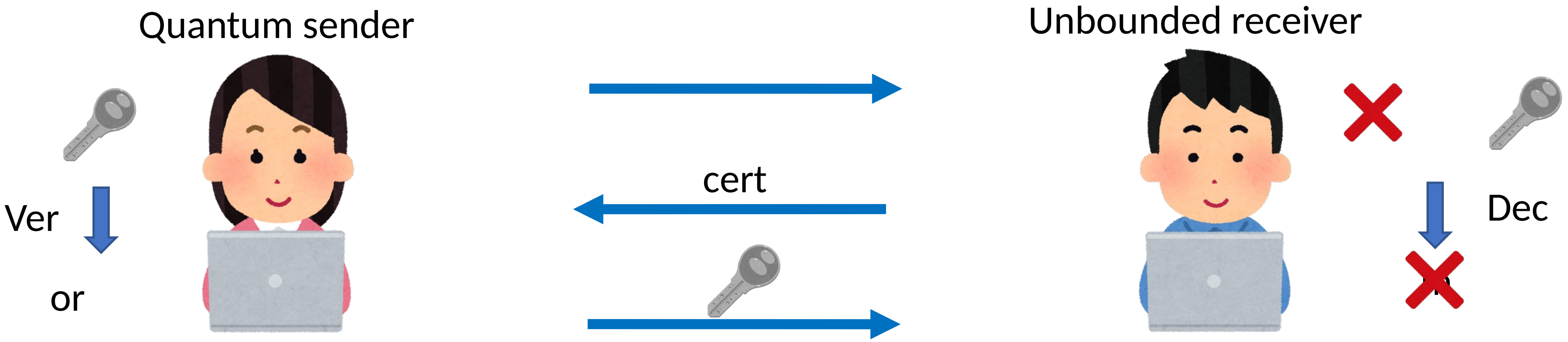
Prior work

SKE with Certified Deletion[Broadbent Islam TCC20]



Prior work

SKE with Certified Deletion[Broadbent Islam TCC20]



Quantum sender

Unbounded receiver

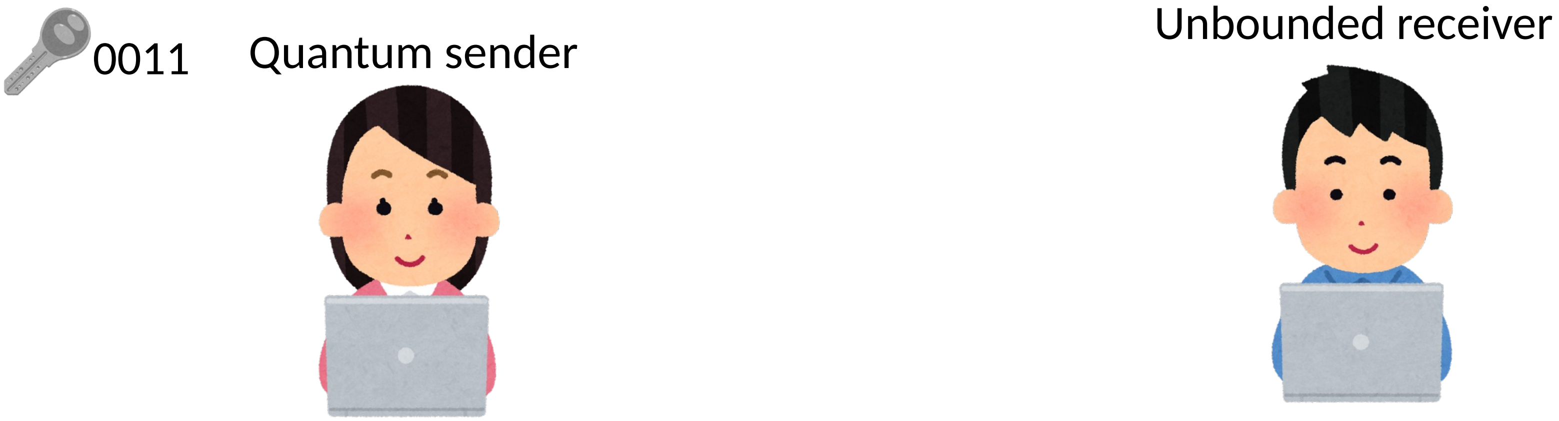
Ver

or

cert

Dec

Their construction



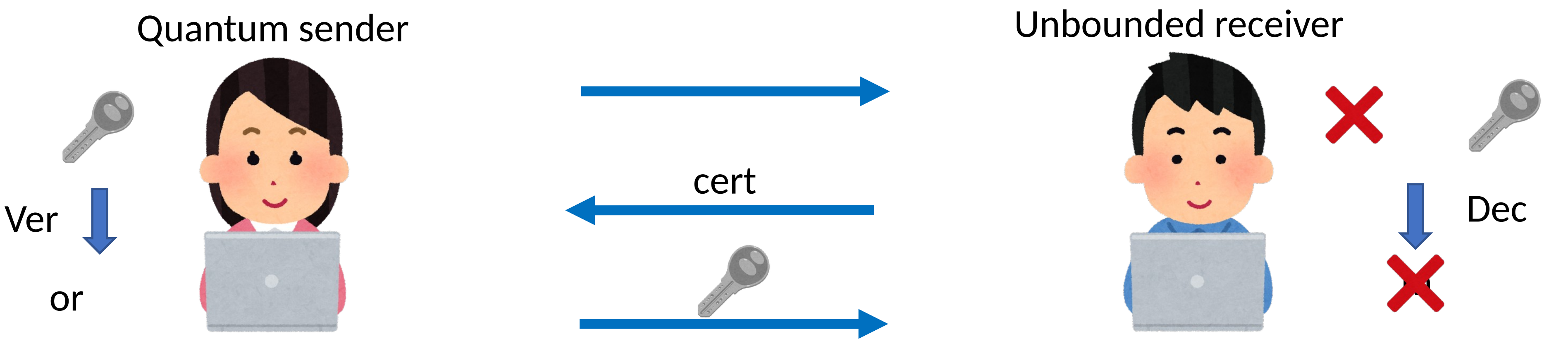
0011

Quantum sender

Unbounded receiver

Prior work

SKE with Certified Deletion[Broadbent Islam TCC20]



Quantum sender

Unbounded receiver

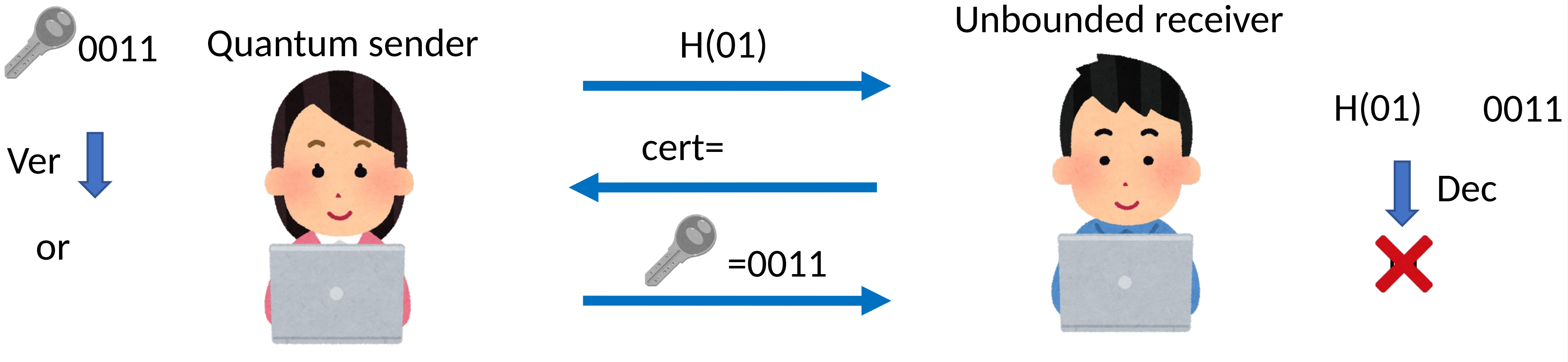
Ver

or

cert

Dec

Their construction



0011

Quantum sender

H(01)

Unbounded receiver

H(01)

0011

Ver

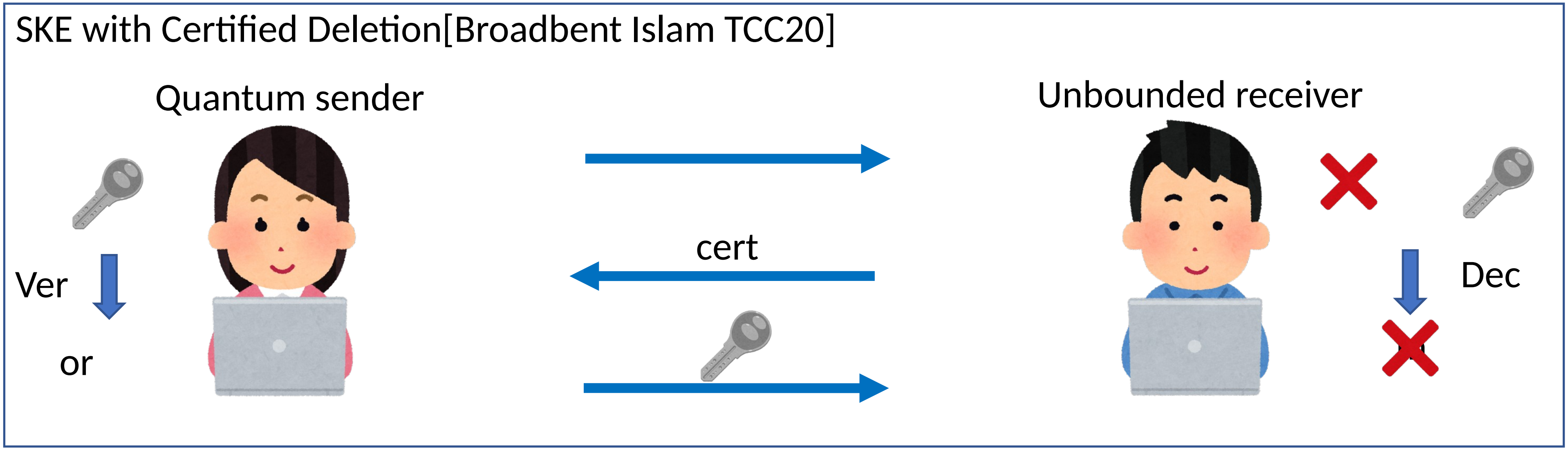
cert=

Dec

or

=0011

Prior work



Disadvantages of their construction
1. SKE
2. Sender needs quantum operation
3. Privately verifiable

Contribution of our work
1. PKE
2. ABE
3. Sender is completely classical
4. Publicly verifiable

Content of talk

arXiv:2105.05393

1. PKE with Certified Deletion

2. ABE with Certified Deletion

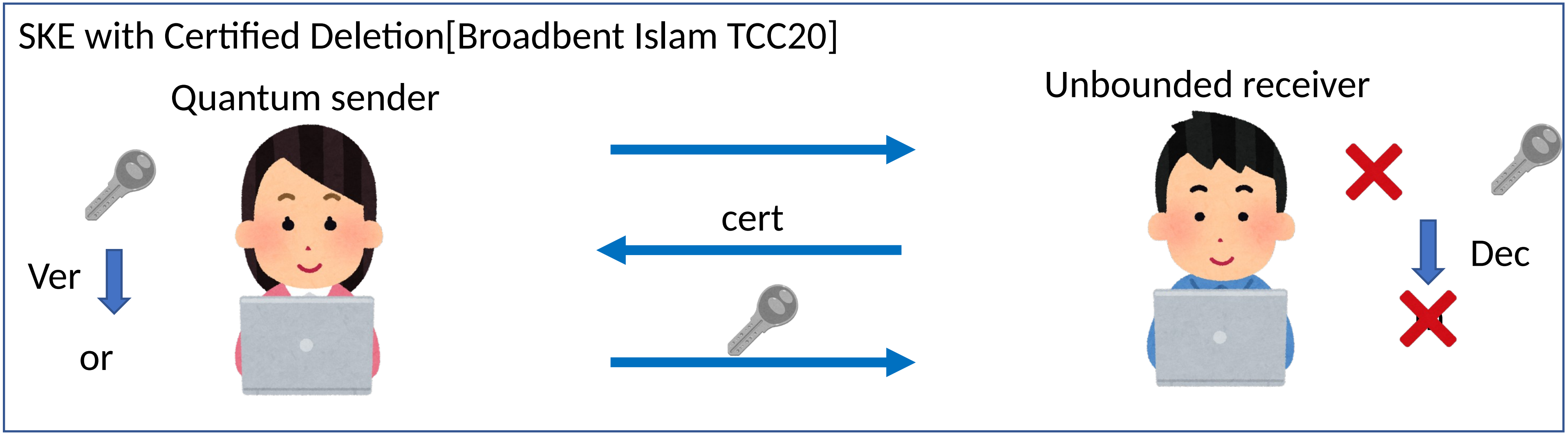
3. Certified Deletion with classical communication

4. Publicly Certified Deletion

Construction

Idea of construction

Encrypt 🔑 using public key encryption.



SKE with Certified Deletion[Broadbent Islam TCC20]

Quantum sender

Unbounded receiver

🔑

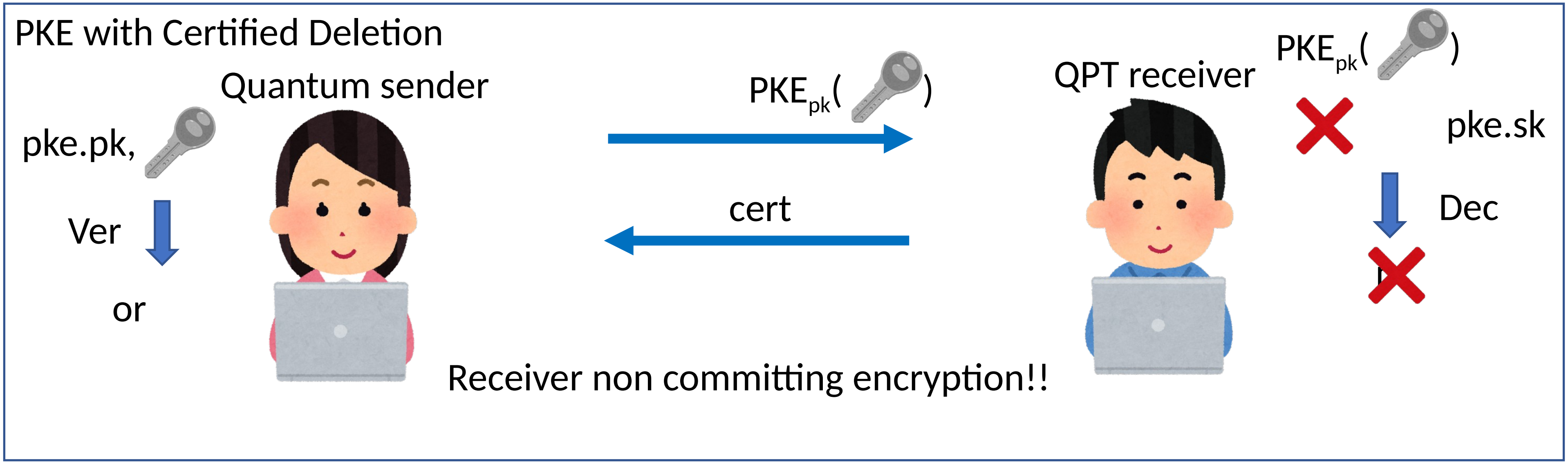
Ver

or

cert

🔑

Dec



PKE with Certified Deletion

Quantum sender

pke.pk, 🔑

Ver

or

PKE_{pk}(🔑)

cert

QPT receiver

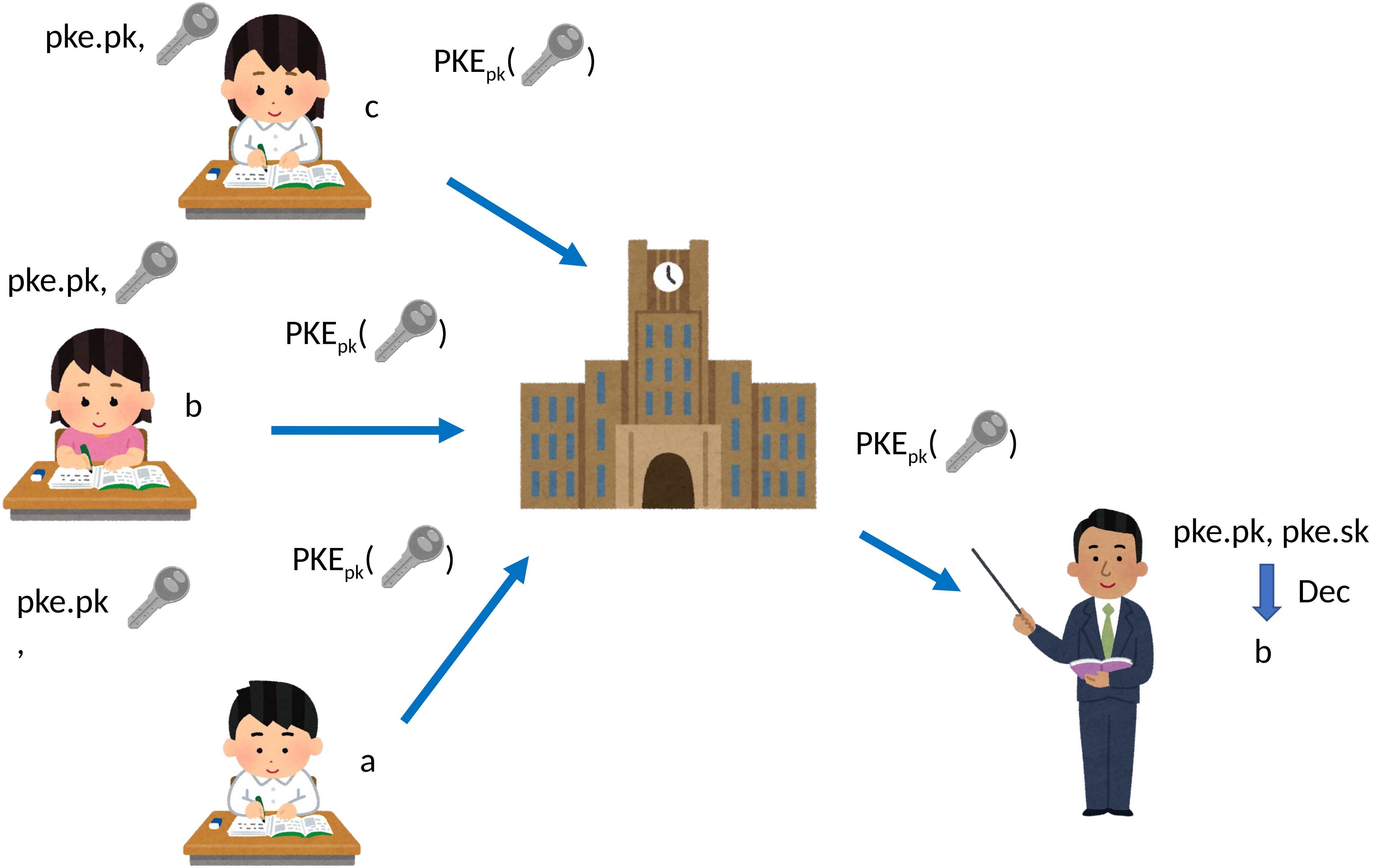
PKE_{pk}(🔑)

pke.sk

Dec

Receiver non committing encryption!!

Application



pke.pk, 🔑

c

PKE_{pk}(🔑)

pke.pk, 🔑

PKE_{pk}(🔑)

b

PKE_{pk}(🔑)

pke.pk 🔑

,

PKE_{pk}(🔑)

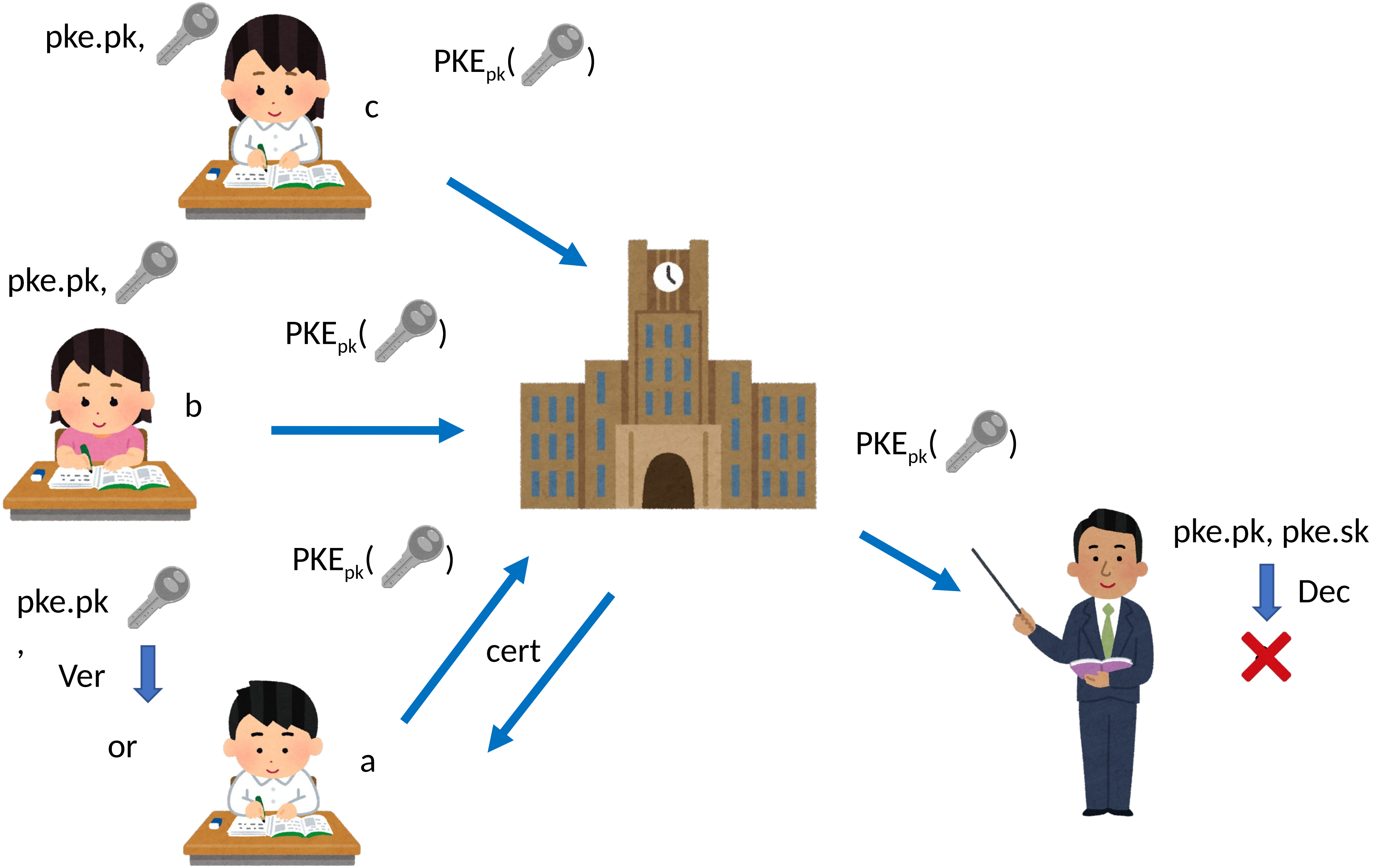
a

pke.pk, pke.sk

Dec

b

Application



Content of talk

arXiv:2105.05393

1. PKE with Certified Deletion

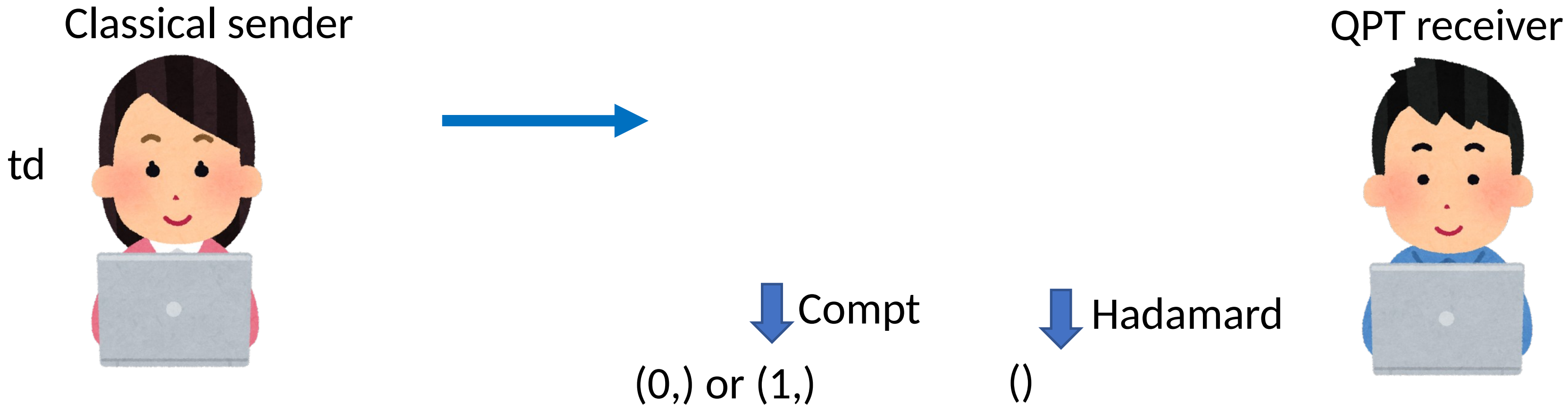
2. ABE with Certified Deletion

3. Certified Deletion with classical communication

4. Publicly Certified Deletion

Preparation

NTCF function [Brakerski et al FOCS18]



Classical sender

QPT receiver

td

Compt

Hadamard

(0,) or (1,)

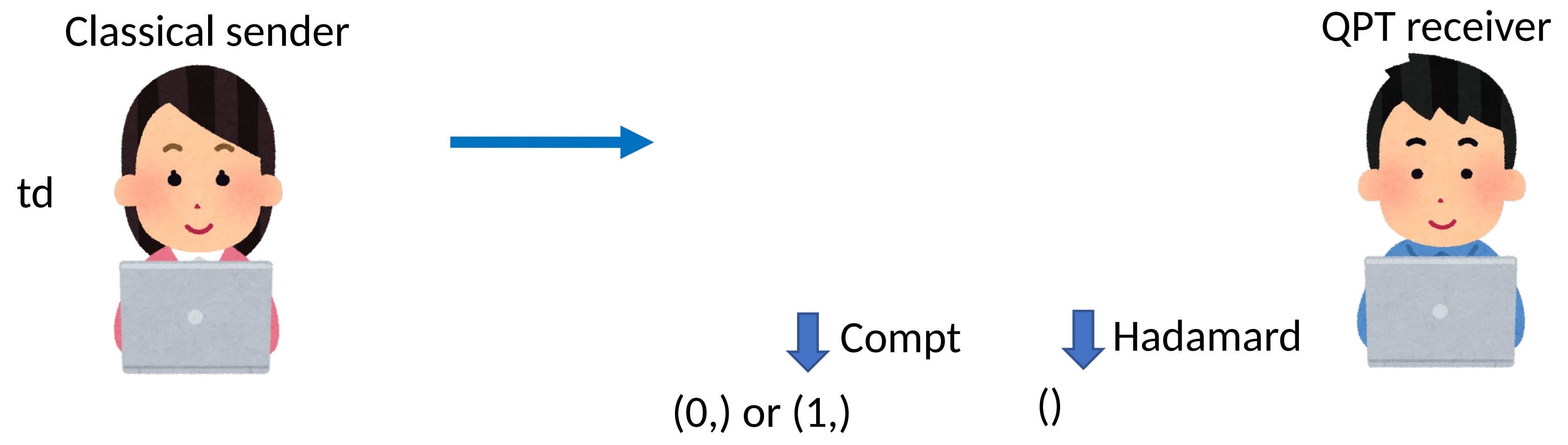
()

Adaptive hard core bit property:
QPT receiver cannot obtain both (0,) or (1,) and () at the same time
with the probability more than 1/2.

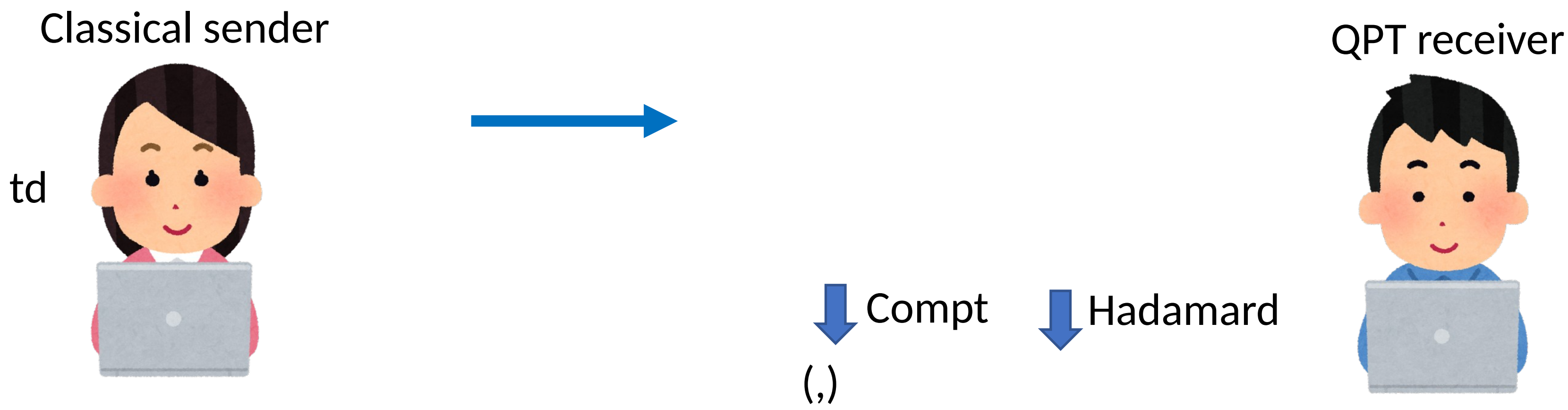
Amplified adaptive hard core bit property[Radian Sattath 19],[Kitagawa et al 20]:
Adaptive hardcore bit can be amplified by parallel repetition.

Preparation

NTCF function [Brakerski et al FOCS18]



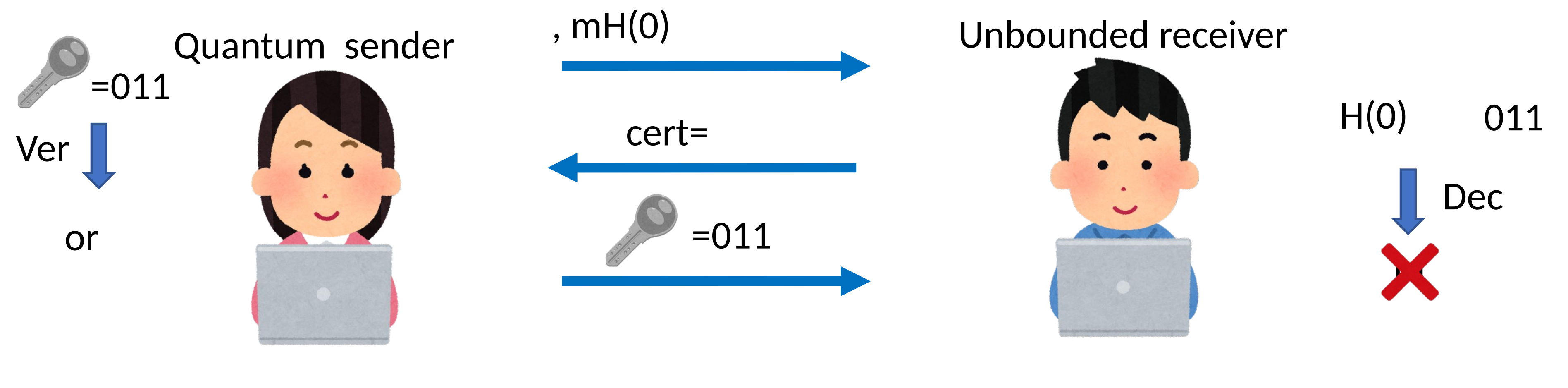
Injective invariant trapdoor function[Mahadev FOCS18]



Injective invariance:
QPT receiver cannot distinguish from .

Construction

Construction of [BI20]



=011

Ver

or

Quantum sender

, mH(0)

cert=

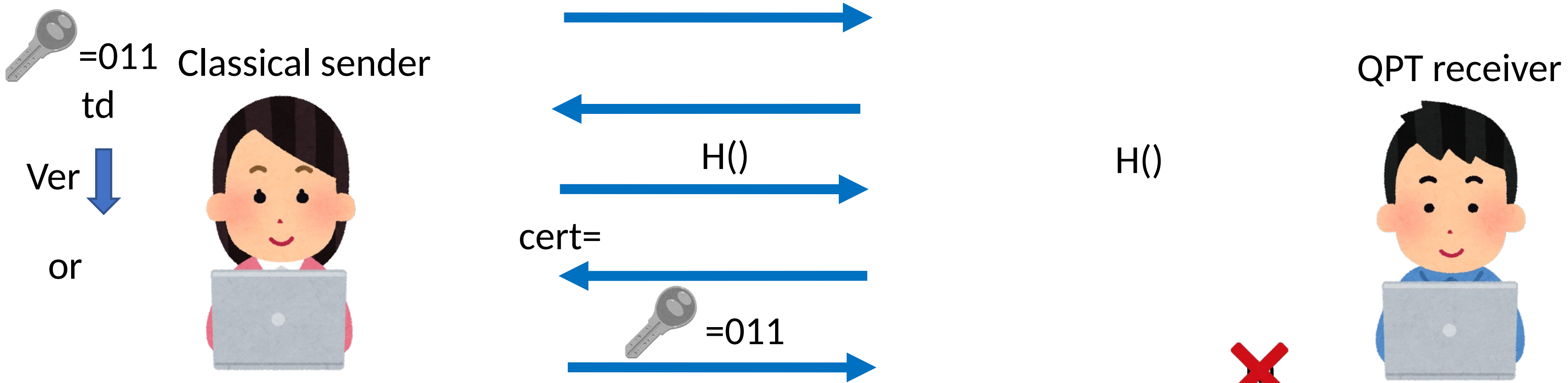
=011

Unbounded receiver

H(0) 011

Dec

Our construction



=011

td

Ver

or

Classical sender

H()

cert=

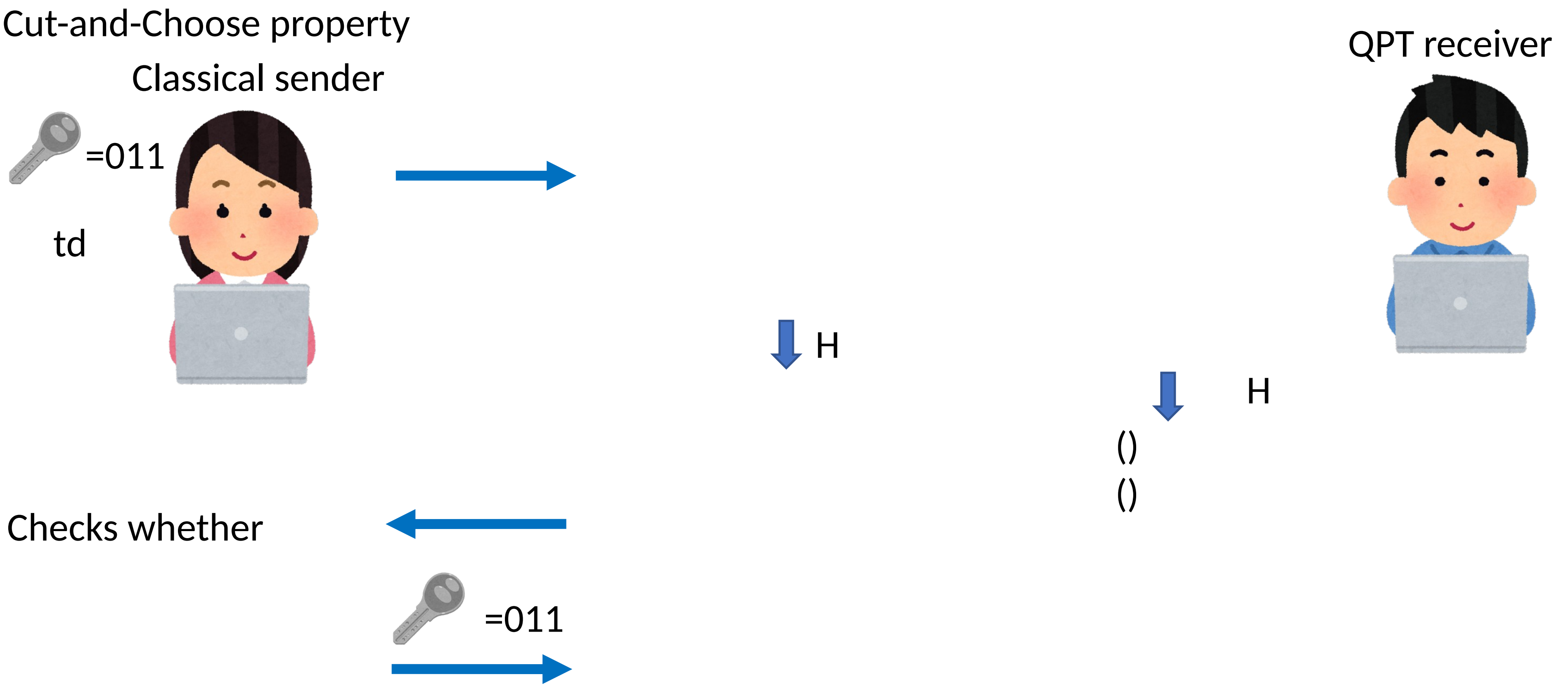
=011

QPT receiver

H()

Adaptive hardcore bit property guarantees that he cannot obtain or and or .

Cut-and-Choose property



Cut-and-Choose property

Classical sender

QPT receiver

=011

td

H

H

()

()

Checks whether

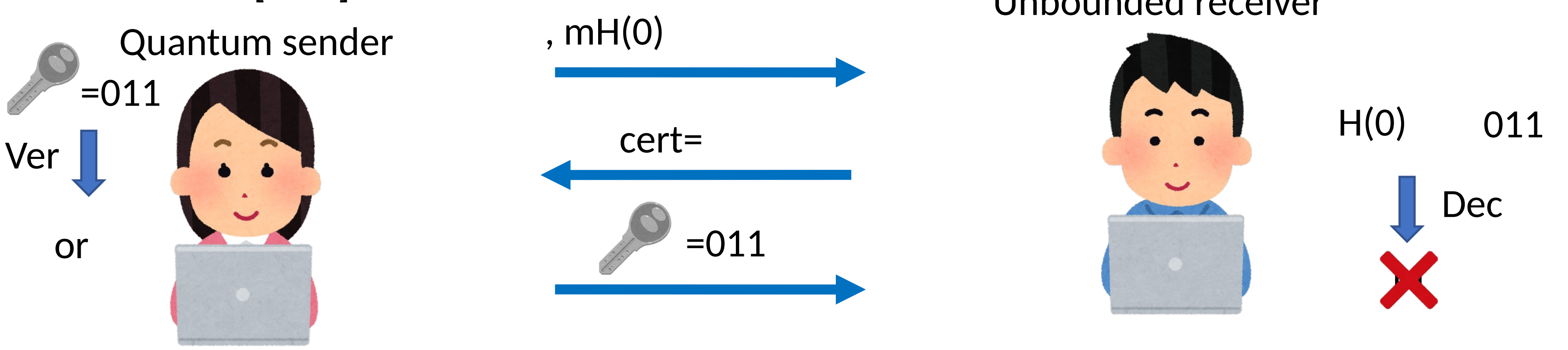
=011

Cut-and-Choose property:

If for i={2,3}, the QPT receiver can no longer obtain .

Construction

Construction of [BI20]



Quantum sender

Unbounded receiver

=011

Ver

or

, mH(0)

cert=

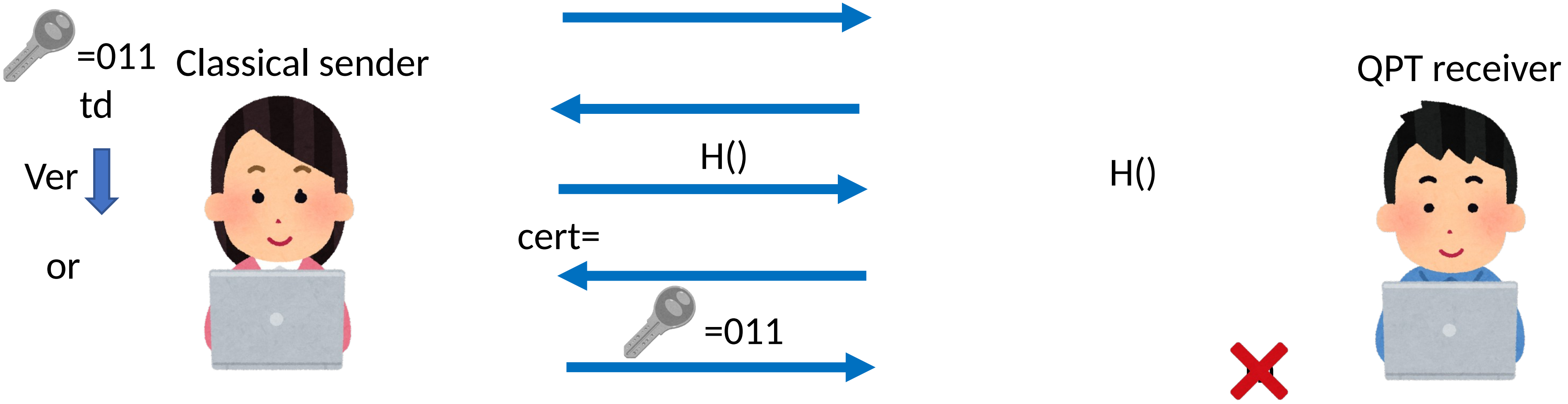
=011

H(0)

011

Dec

Our construction



=011

Classical sender

td

Ver

or

QPT receiver

H()

H()

cert=

=011

Thank you!

arXiv:2105.05393