Implementation of Practical Unforgeable Quantum Money

Mathieu Bozzio, Adeline Orieux, Luis Trigo Vidarte,
Isabelle Zaquine, Frédéric Grosshans,
Iordanis Kerenidis, Eleni Diamanti

LTCI Laboratoire de Traitement et Communication de l'Information

LIP6

université PARIS DIDEROT PARIS 7

cnrs

LABORATOIRE Aimé Cotton

Experimental Investigation of Practical Unforgeable Quantum Money
npj Quantum Information 4, 5 (2018)

Semi Device-Independent Practical Quantum Money
to appear on arXiv

Background : Quantum Communications

Background : Quantum Communications

Quantum Money (Wiesner ~1970) :

- First idea of using the uncertainty principle for security.
- Never implemented until now (lack of quantum memories).

Background : Quantum Communications

Quantum Money (Wiesner ~1970) :

- First idea of using the uncertainty principle for security.
- Never implemented until now (lack of quantum memories).

Quantum Key Distribution (~1980) :

- Alice and Bob share a secret key publicly with unconditional security.
- Implementations are advanced, some industrial.

Background : Quantum Communications

Quantum Money (Wiesner ~1970) :

- First idea of using the uncertainty principle for security.
- Never implemented until now (lack of quantum memories).

Quantum Key Distribution (~1980) :

- Alice and Bob share a secret key publicly with unconditional security.
- Implementations are advanced, some industrial.

Quantum Communication Protocols (~2000) :

- Quantum fingerprinting allows communication speed-up.

Background : Quantum Communications

Quantum Money (Wiesner ~1970) :

- First idea of using the uncertainty principle for security.
- Never implemented until now (lack of quantum memories).

Quantum Key Distribution (~1980) :

- Alice and Bob share a secret key publicly with unconditional security.
- Implementations are advanced, some industrial.

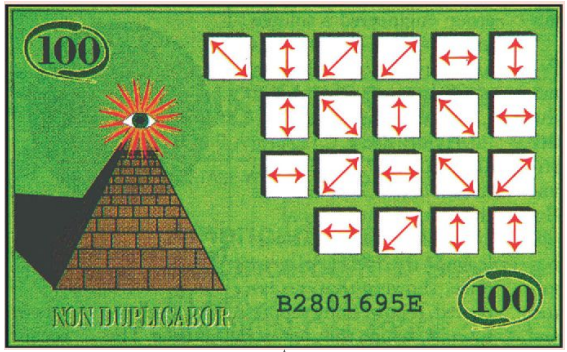
Quantum Communication Protocols (~2000) :

- Quantum fingerprinting allows communication speed-up.

And many more...

Quantum Banknotes

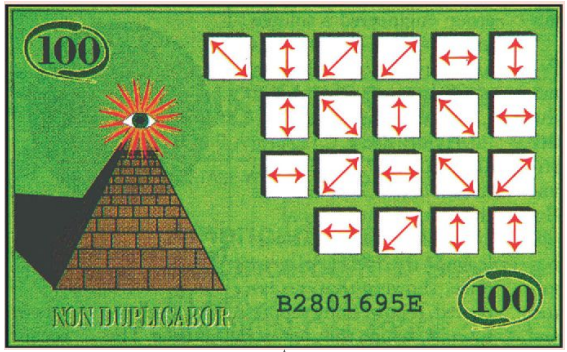
Quantum Banknotes



MINT
public serial number **s,**
secret classical key **k(s)**

Quantum Banknotes

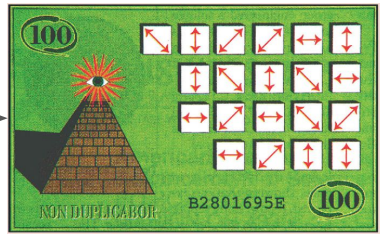
CLIENT
stores banknote in a quantum memory



MINT
public serial number **s,**
secret classical key **k(s)**

Quantum Banknotes

CLIENT
stores banknote in a quantum memory

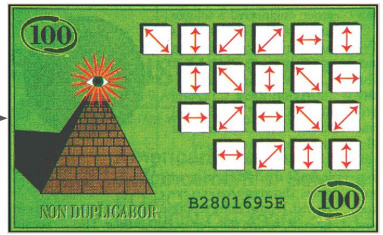


BANK
measurements for
quantum verification

MINT
public serial number **s,**
secret classical key **k(s)**

Quantum Banknotes

CLIENT
stores banknote in a quantum memory

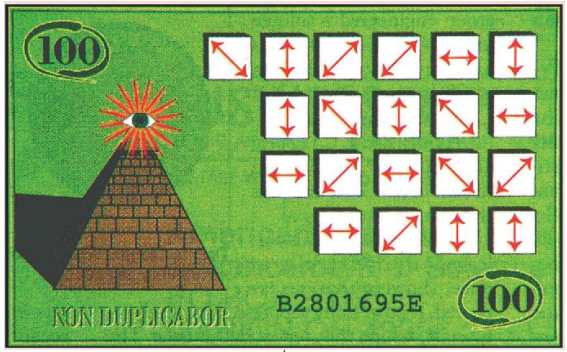


BANK
measurements for
quantum verification

MINT
public serial number **s,**
secret classical key **k(s)**

Quantum Banknotes

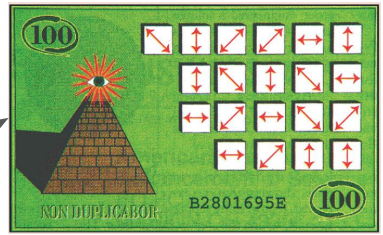
CLIENT
stores banknote in a quantum memory

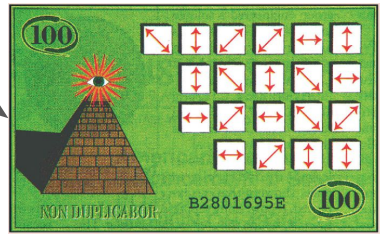


MINT
public serial number **s,**
secret classical key **k(s)**

Quantum Banknotes

CLIENT
stores banknote in a quantum memory



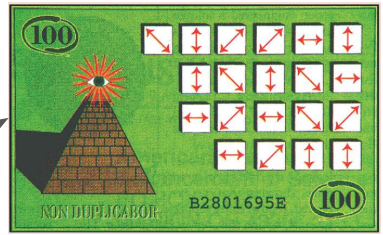


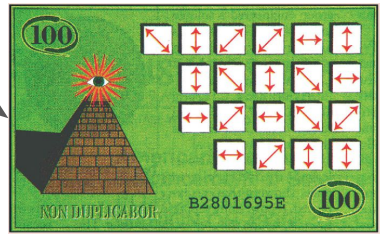
NO-CLONING THEOREM

MINT
public serial number **s,**
secret classical key **k(s)**

Quantum Banknotes

CLIENT
stores banknote in a quantum memory



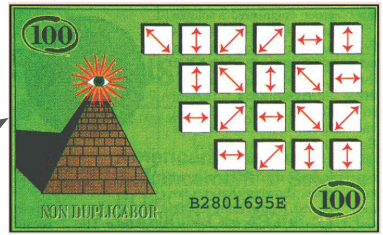


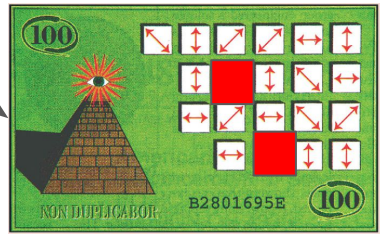
BANK
measurements for **quantum verification**

MINT
public serial number **s,**
secret classical key **k(s)**

Quantum Banknotes

CLIENT
stores banknote in a quantum memory





BANK
measurements for
quantum verification

MINT
public serial number **s,**
secret classical key **k(s)**

Quantum Credit Cards

Quantum Credit Cards

CLIENT
stores banknote in a quantum memory

MINT
public serial number **s,**
secret classical key **k(s)**

Quantum Credit Cards

CLIENT
stores banknote in a quantum memory

MERCHANT
performs measurements

MINT
public serial number **s,**
secret classical key **k(s)**

Quantum Credit Cards

CLIENT
stores banknote in a quantum memory

MERCHANT
performs measurements

BANK
acceptance of
classical data

01001...

01111...

MINT
public serial number **s,**
secret classical key **k(s)**

Quantum Credit Cards

CLIENT
stores banknote in a quantum memory

MERCHANT
performs measurements

BANK
acceptance of
classical data

01001...

01111...

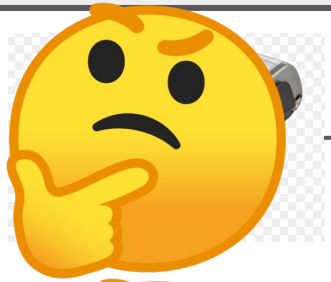
MINT
public serial number **s,**
secret classical key **k(s)**

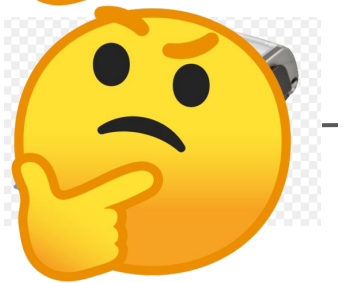
Quantum Credit Cards

CLIENT
stores banknote in a quantum memory

MERCHANT
performs measurements

BANK
acceptance of
classical data





SHOULD WE TRUST THE TERMINAL ?

MINT
public serial number **s**,
secret classical key **k(s)**

Trusted Terminal : Protocol

Trusted Terminal : Protocol

Allow classical verification by choosing **qubit pairs** :

$$S_{pair} = \{|0,+\rangle, |0,-\rangle, |1,+\rangle, |1,-\rangle, |+,0\rangle, |+,1\rangle, |-,0\rangle, |-,1\rangle\}$$

Secret classical key : 3 bits $\{b, c_0, c_1\}$, $b =$ basis of the first qubit,
$c_i =$ information contained in each qubit.

Trusted Terminal : Protocol

Allow classical verification by choosing **qubit pairs** :

$$S_{pair} = \{|0,+\rangle, |0,-\rangle, |1,+\rangle, |1,-\rangle, |+,0\rangle, |+,1\rangle, |-,0\rangle, |-,1\rangle\}$$

Secret classical key : 3 bits $\{b, c_0, c_1\}$, b = basis of the first qubit,
c_i = information contained in each qubit.

Correctness challenges (c=1, asked by the bank)
Q_{xx} : Guess the two bits c_0 and c_1 such that the guess corresponding to the qubit prepared in the σ_x basis is correct.
Q_{zz} : Guess the two bits c_0 and c_1 such that the guess corresponding to the qubit prepared in the σ_z basis is correct.

Trusted Terminal : Protocol

Allow classical verification by choosing **qubit pairs** :

$$S_{pair} = \{|0,+\rangle, |0,-\rangle, |1,+\rangle, |1,-\rangle, |+,0\rangle, |+,1\rangle, |-,0\rangle, |-,1\rangle\}$$

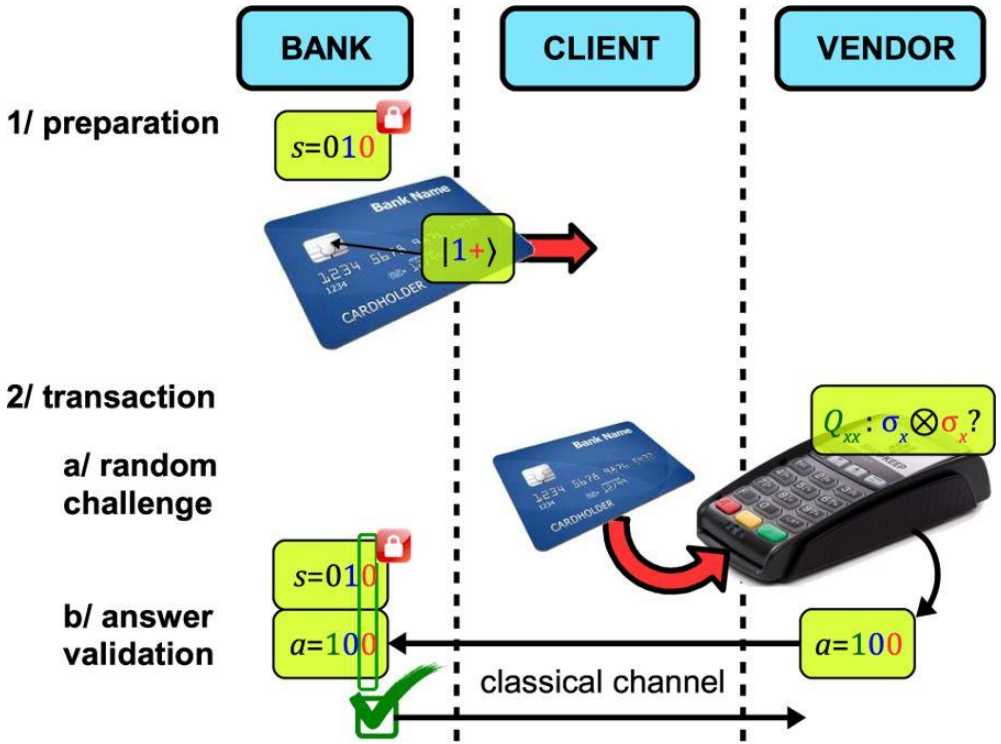
Secret classical key : 3 bits $\{b, c_0, c_1\}$, b = basis of the first qubit,
c_i = information contained in each qubit.

Correctness challenges (c=1, asked by the bank)
Q_{xx} : Guess the two bits c_0 and c_1 such that the guess corresponding to the qubit prepared in the σ_x basis is correct.
Q_{zz} : Guess the two bits c_0 and c_1 such that the guess corresponding to the qubit prepared in the σ_z basis is correct.

Security challenge ($\epsilon = 3/4$ = cloning probability)
Q_ϵ = Guess the two bits c_0 and c_1.

Trusted Terminal : Protocol

Trusted Terminal : Protocol



Mapping onto Coherent States

Mapping onto Coherent States

Qubit states may be mapped onto 2-mode coherent states as:

$$|0\rangle \rightarrow |\alpha\rangle \otimes |vac\rangle \qquad |1\rangle \rightarrow |vac\rangle \otimes |-\alpha\rangle$$
$$|+\rangle \rightarrow |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |\tfrac{\alpha}{\sqrt{2}}\rangle \qquad |-\rangle \rightarrow |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |-\tfrac{\alpha}{\sqrt{2}}\rangle$$
$$|+i\rangle \rightarrow |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |i\tfrac{\alpha}{\sqrt{2}}\rangle \qquad |-i\rangle \rightarrow |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |-i\tfrac{\alpha}{\sqrt{2}}\rangle$$

Mapping onto Coherent States

Qubit states may be mapped onto 2-mode coherent states as:

$$|0\rangle \rightarrow |\alpha\rangle \otimes |vac\rangle \qquad |1\rangle \rightarrow |vac\rangle \otimes |-\alpha\rangle$$
$$|+\rangle \rightarrow |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |\tfrac{\alpha}{\sqrt{2}}\rangle \qquad |-\rangle \rightarrow |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |-\tfrac{\alpha}{\sqrt{2}}\rangle$$
$$|+i\rangle \rightarrow |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |i\tfrac{\alpha}{\sqrt{2}}\rangle \qquad |-i\rangle \rightarrow |\tfrac{\alpha}{\sqrt{2}}\rangle \otimes |-i\tfrac{\alpha}{\sqrt{2}}\rangle$$

What are the security implications of such a mapping ?

Trusted Terminal : Security

Trusted Terminal : Security

- **True single photon scenario**

  $\Rightarrow$ Single emitter quantum memories with coherent state input.

  $\Rightarrow$ Atomic ensemble quantum memories with single photon input.

  $\Rightarrow$ Upper bound on cheating probability $\epsilon = \frac{3}{4}$.

$$c > \frac{\epsilon + 1}{2} = \frac{7}{8}$$

Trusted Terminal : Security

- **True single photon scenario**

  $\Rightarrow$ Single emitter quantum memories with coherent state input.
  $\Rightarrow$ Atomic ensemble quantum memories with single photon input.
  $\Rightarrow$ Upper bound on cheating probability $\epsilon = \frac{3}{4}$.

$$c > \frac{\epsilon + 1}{2} = \frac{7}{8}$$

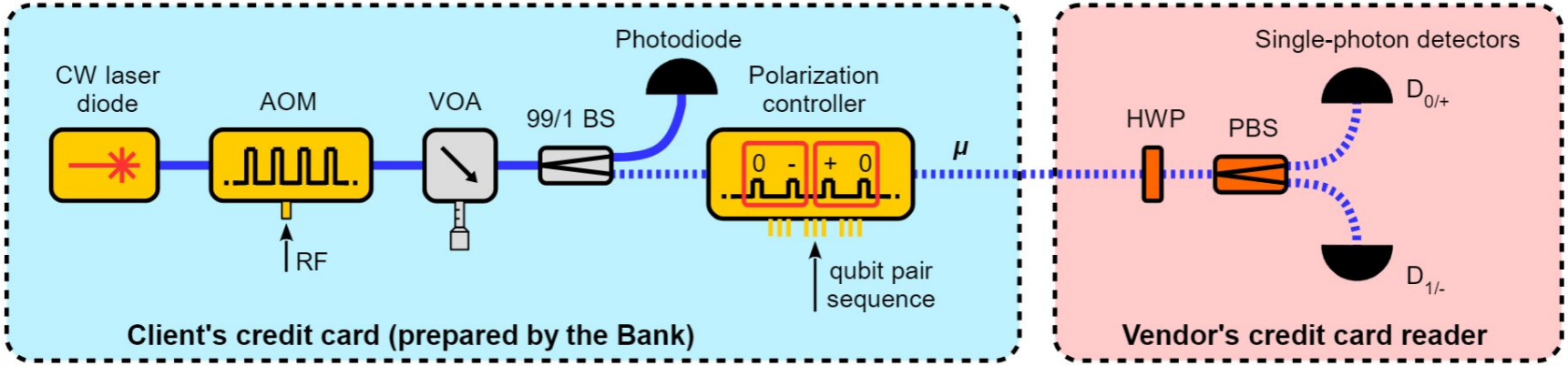
- **Weak coherent state scenario (μ)**

  $\Rightarrow$ Atomic ensemble quantum memories with coherent state input.
  $\Rightarrow$ New attacks such as Unambiguous State Discrimination.
  $\Rightarrow$ Memory introduces attenuation, therefore :

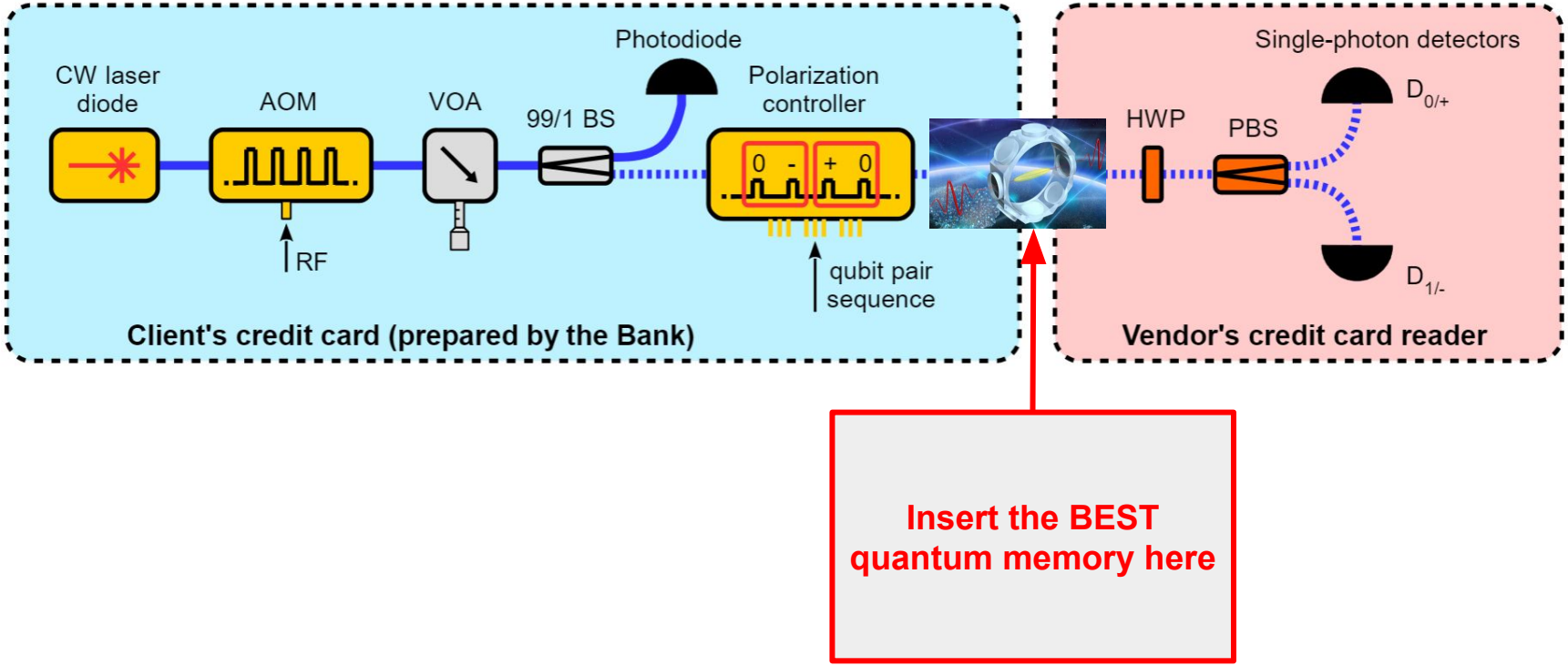
$$c > f(\mu, \epsilon)$$

Trusted Terminal : Experimental Setup

Trusted Terminal : Experimental Setup

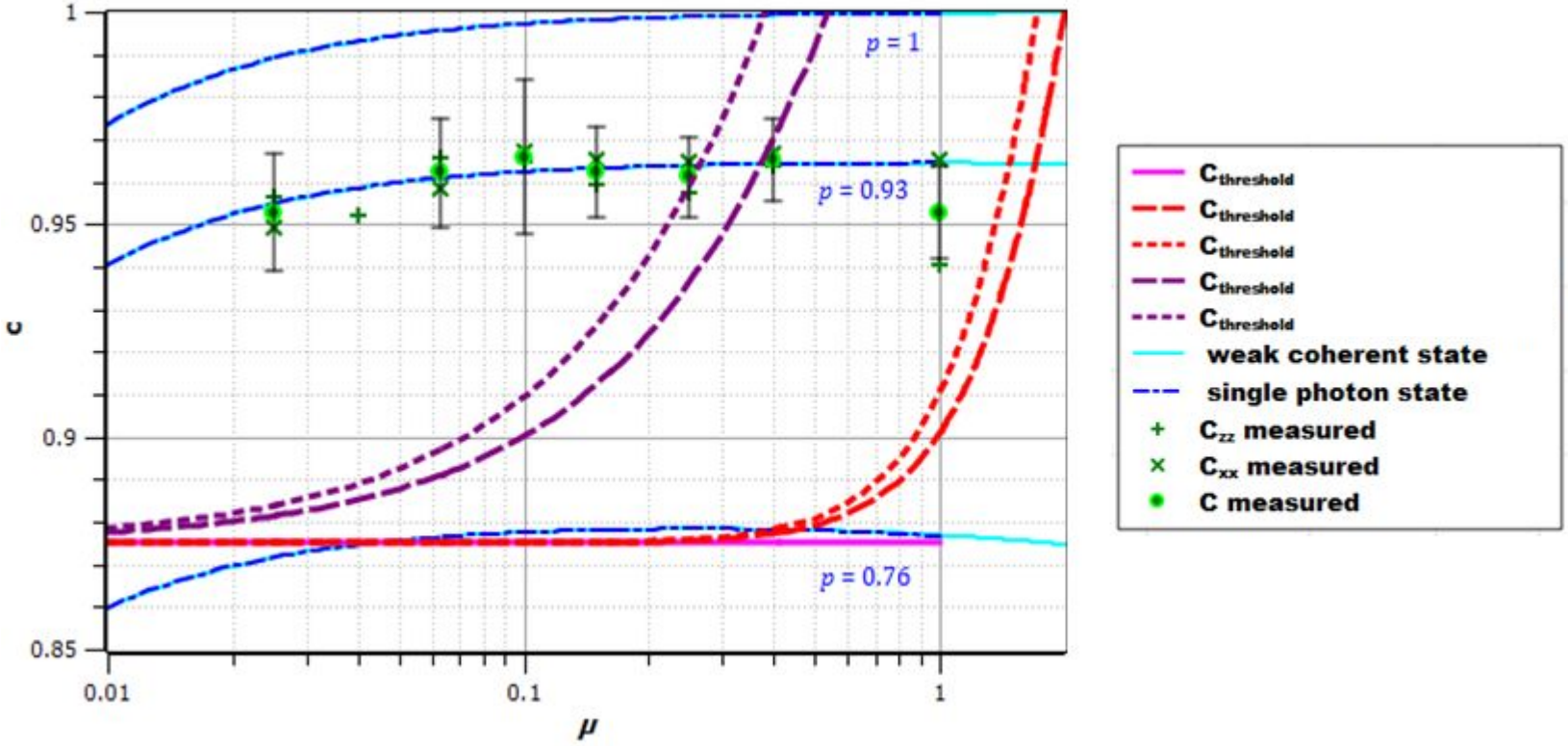


Trusted Terminal : Experimental Setup

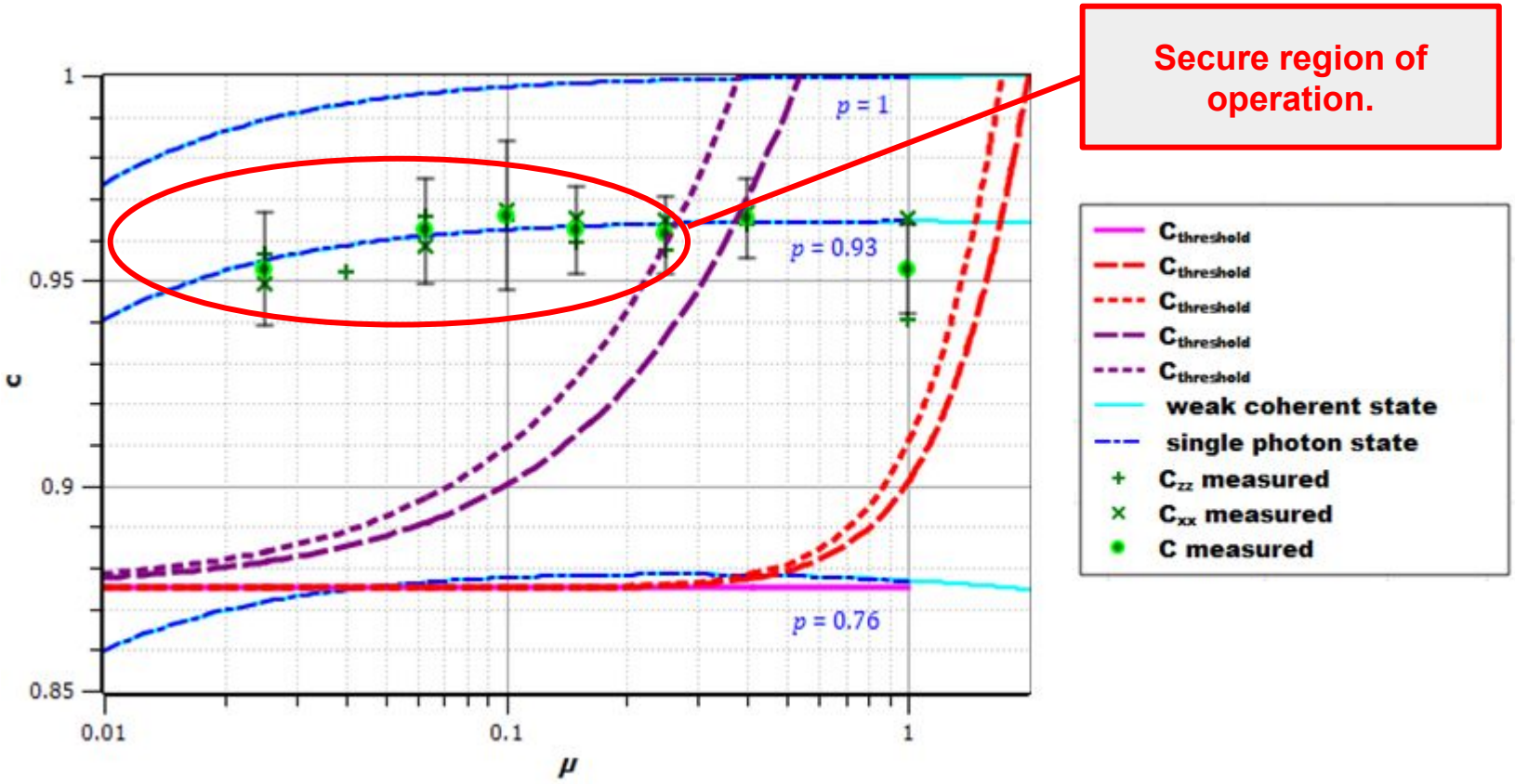


Trusted Terminal : Results

Trusted Terminal : Results



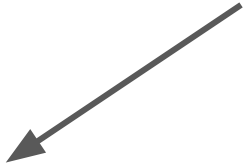
Trusted Terminal : Results



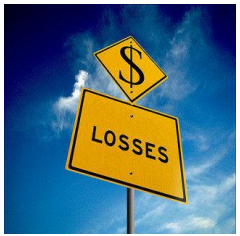
General Security Framework

General Security Framework

General Security Framework

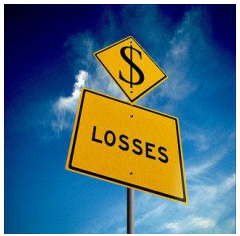


General Security Framework



General Security Framework

General Security Framework



Minimize losses AND error using semidefinite programming (SDP)

Theoretical Challenges

Theoretical Challenges

Unified Optimization Framework :

- Find the optimal adversarial cloning map
- Optimize over both errors **and** losses with semidefinite programming (SDP)

Theoretical Challenges

Unified Optimization Framework :

- Find the optimal adversarial cloning map
- Optimize over both errors **and** losses with semidefinite programming (SDP)

Discrete Variables with Infinite Dimensions :

- How can we express our problem in finite dimensions ?

Theoretical Challenges

Unified Optimization Framework :

- Find the optimal adversarial cloning map
- Optimize over both errors **and** losses with semidefinite programming (SDP)

Discrete Variables with Infinite Dimensions :

- How can we express our problem in finite dimensions ?

Figures of Merit :

- Trusted terminal : quantum measurements
- Untrusted terminal : acceptance of classical data

Theoretical Challenges

Unified Optimization Framework :

- Find the optimal adversarial cloning map
- Optimize over both errors **and** losses with semidefinite programming (SDP)

Discrete Variables with Infinite Dimensions :

- How can we express our problem in finite dimensions ?

Figures of Merit :

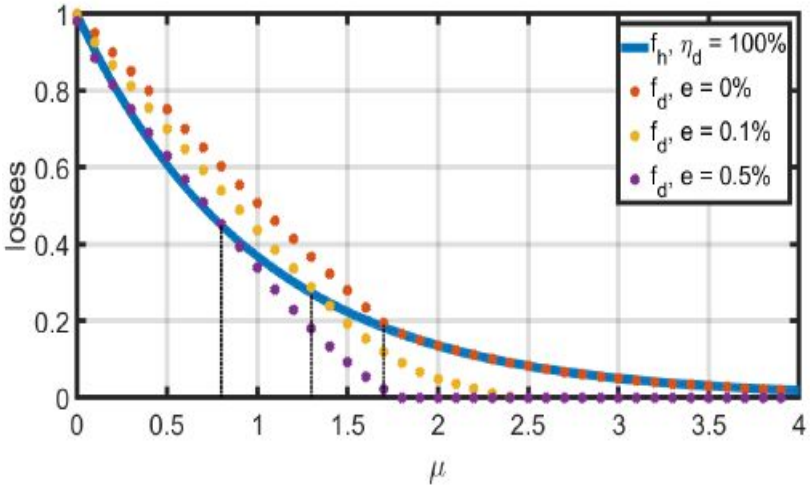
- Trusted terminal : quantum measurements
- Untrusted terminal : acceptance of classical data

Quantum Memory :

- Time-dependent security proof

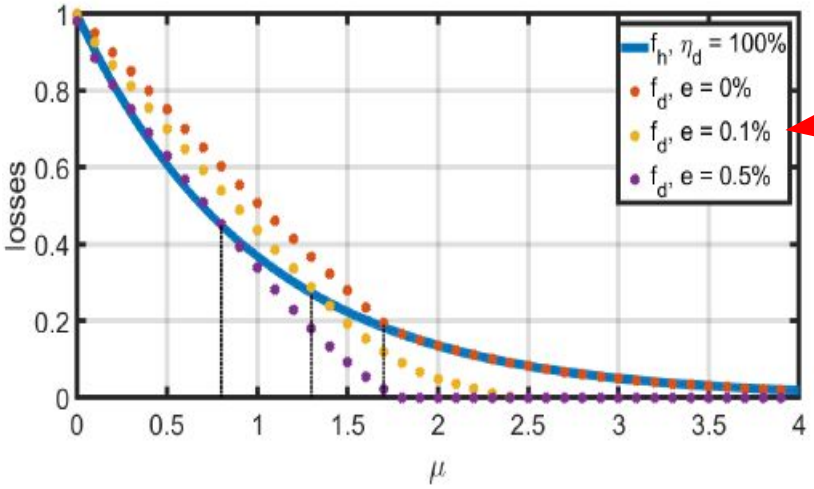
Numerical Results (SDP)

Numerical Results (SDP)



Trusted terminal

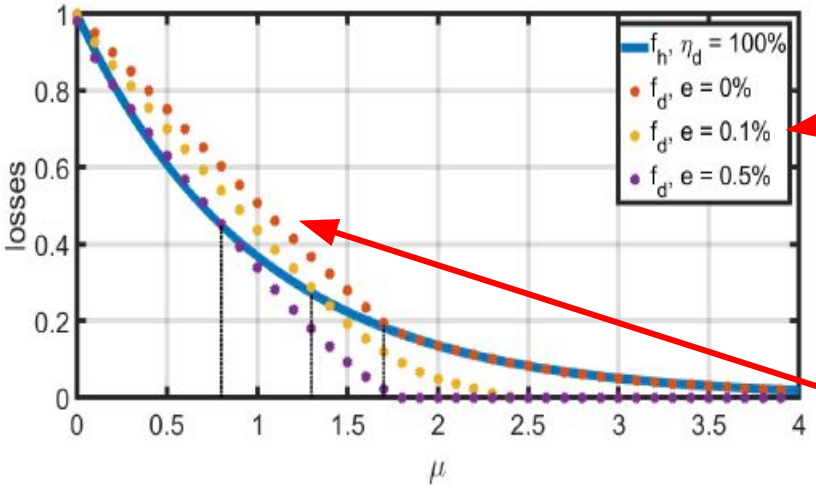
Numerical Results (SDP)



The error rate e is fixed before performing the optimization.

Trusted terminal

Numerical Results (SDP)

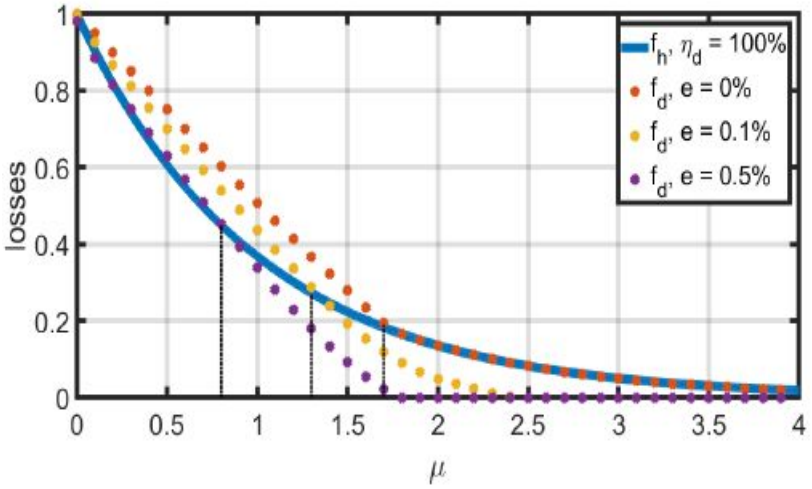


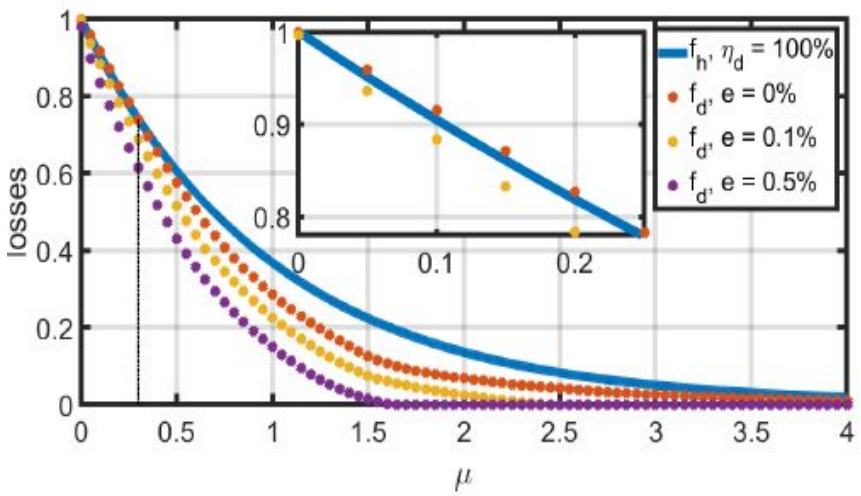
The error rate e is fixed before performing the optimization.

The dishonest excess losses f_d must lie above the honest losses f_h for the bank to detect the attack.

Trusted terminal

Numerical Results (SDP)

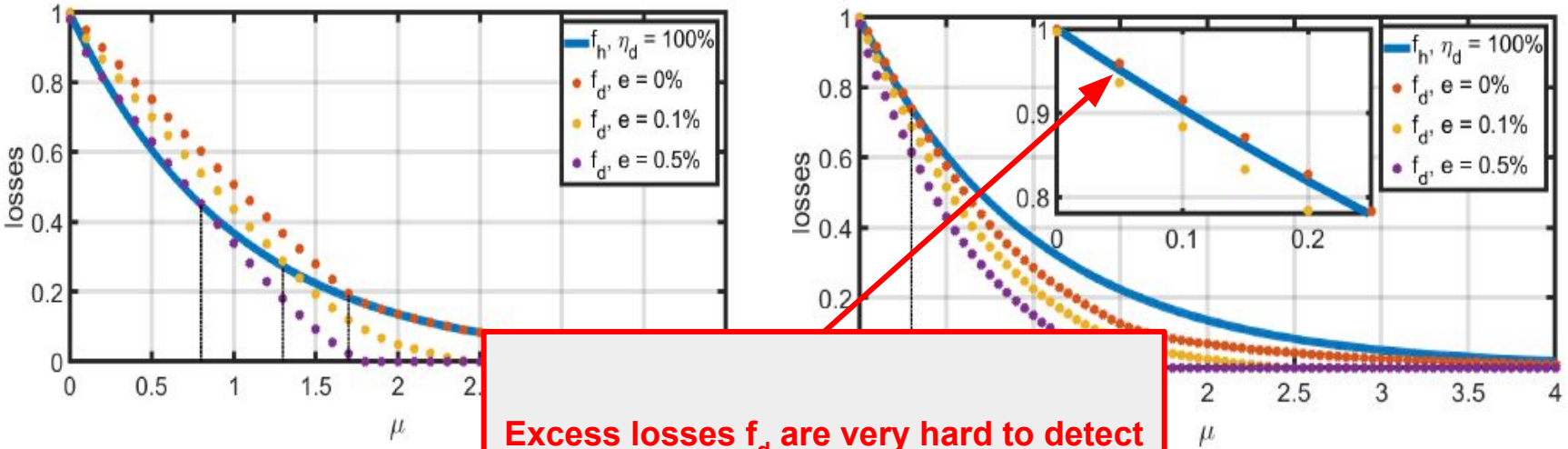




Trusted terminal

Untrusted terminal

Numerical Results (SDP)



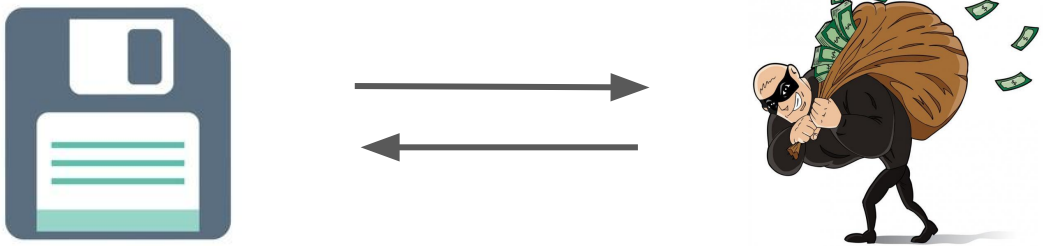
Trusted termi … usted terminal

Excess losses f_d are very hard to detect even for zero error.

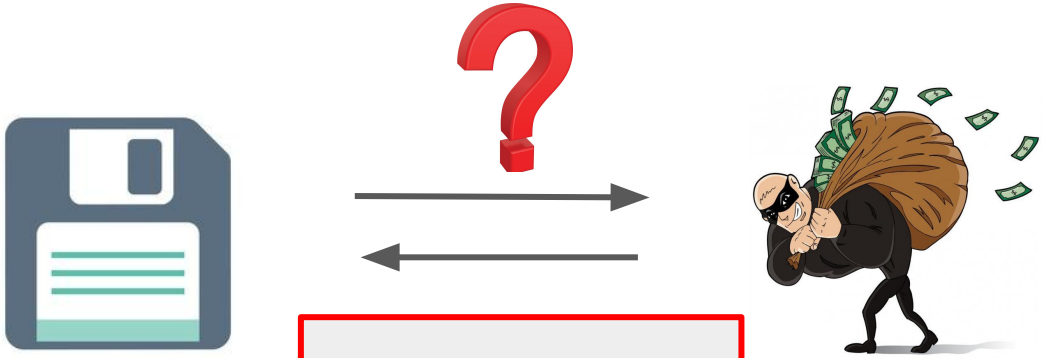
Noise and loss tolerance can be improved with phase randomization.

Security and Quantum Memories

Security and Quantum Memories

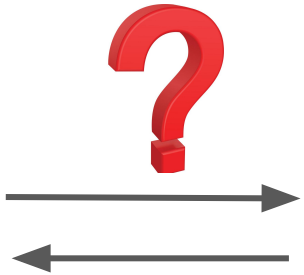


Security and Quantum Memories



How can the adversary exploit the quantum memory to get more information?

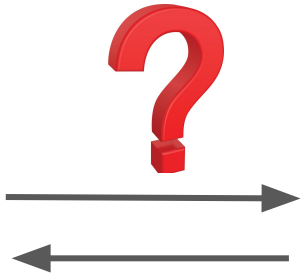
Security and Quantum Memories



How can the adversary exploit the quantum memory to get more information?

Retrieval efficiency decreases with time

Security and Quantum Memories



How can the adversary exploit the quantum memory to get more information?

Retrieval efficiency decreases with time

Some physical processes preserve information

Summary

Summary

Experimental demonstration in the trusted terminal case without a quantum memory.

Summary

Experimental demonstration in the trusted terminal case without a quantum memory.

Practical security proof for both trusted and untrusted terminals.

Summary

Experimental demonstration in the trusted terminal case without a quantum memory.

Practical security proof for both trusted and untrusted terminals.

Time-dependent security with a quantum memory.

Summary

Experimental demonstration in the trusted terminal case without a quantum memory.

Practical security proof for both trusted and untrusted terminals.

Time-dependent security with a quantum memory.

NEXT : Implement the protocol with a quantum memory !

S.Wiesner, ACM Sigact News 15, 78 (1983).
D.Gavinsky, Proc. IEEE 27th Annual Conference on Computational Complexity (CCC), pp. 42–52 (2012).
F.Pastawski, N.Y.Yao, L.Jiang, M.D.Lukin, and J.I.Cirac, PNAS 109, 16079 (2012)
P.Vernaz-Gris, K.Huang, M.Cao, A.S.Sheremet and J.Laurat, Nature Communications, 9, 363 (2018)

Thanks for listening !

Mathieu Bozzio, Adeline Orieux, Luis Trigo Vidarte,
Isabelle Zaquine, Frédéric Grosshans,
Iordanis Kerenidis, Eleni Diamanti

Experimental Investigation of Practical Unforgeable Quantum Money
npj Quantum Information 4, 5 (2018)

Semi Device-Independent Practical Quantum Money
to appear on arXiv