Quantum Cryptography Beyond QKD

CHRISTIAN SCHAFFNER

QuSoft RESEARCH CENTER FOR QUANTUM SOFTWARE

INSTITUTE FOR LOGIC, LANGUAGE AND COMPUTATION (ILLC)

UNIVERSITY OF AMSTERDAM

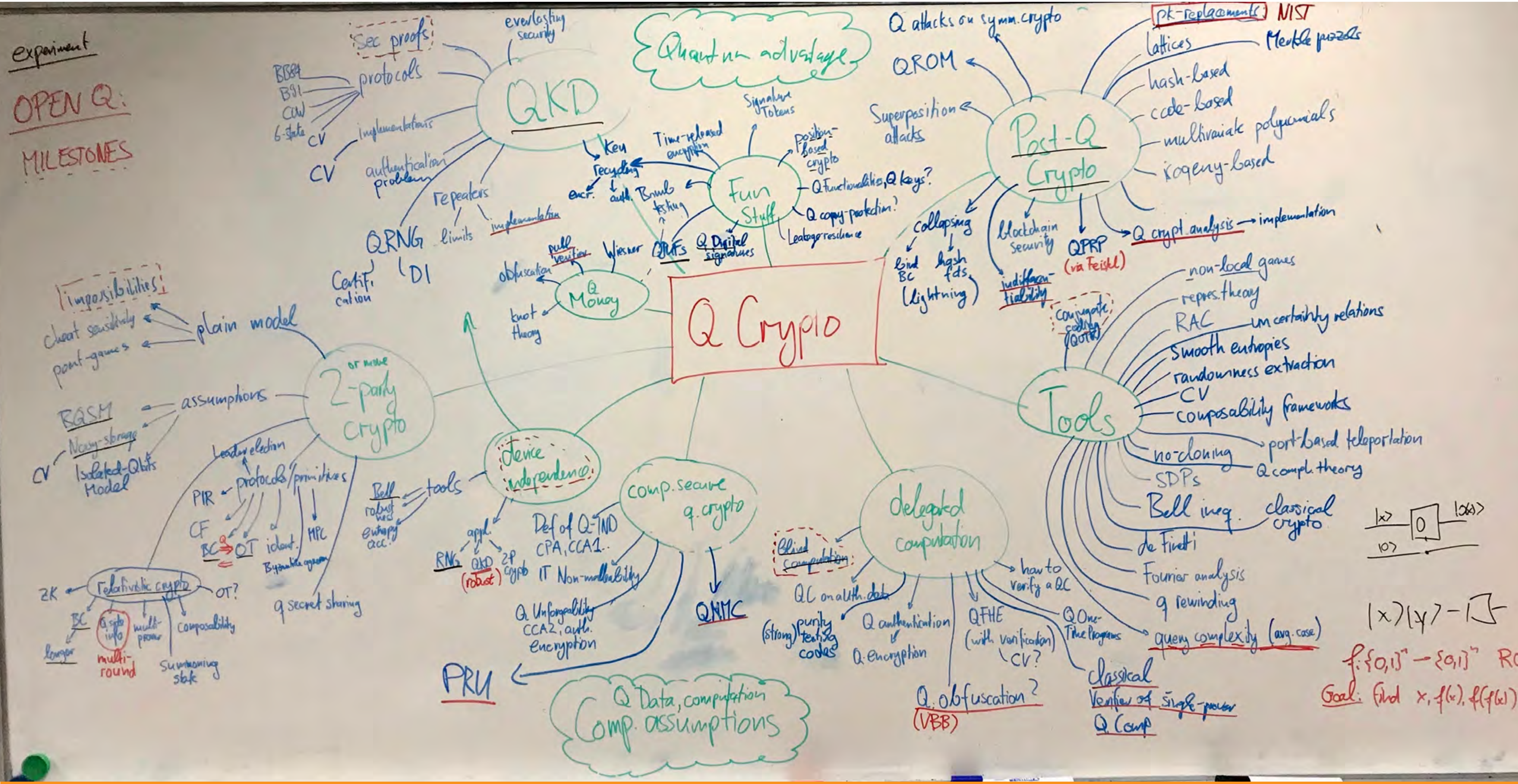
CWI CENTRUM WISKUNDE & INFORMATICA

Nederlandse Organisatie voor Wetenschappelijk Onderzoek

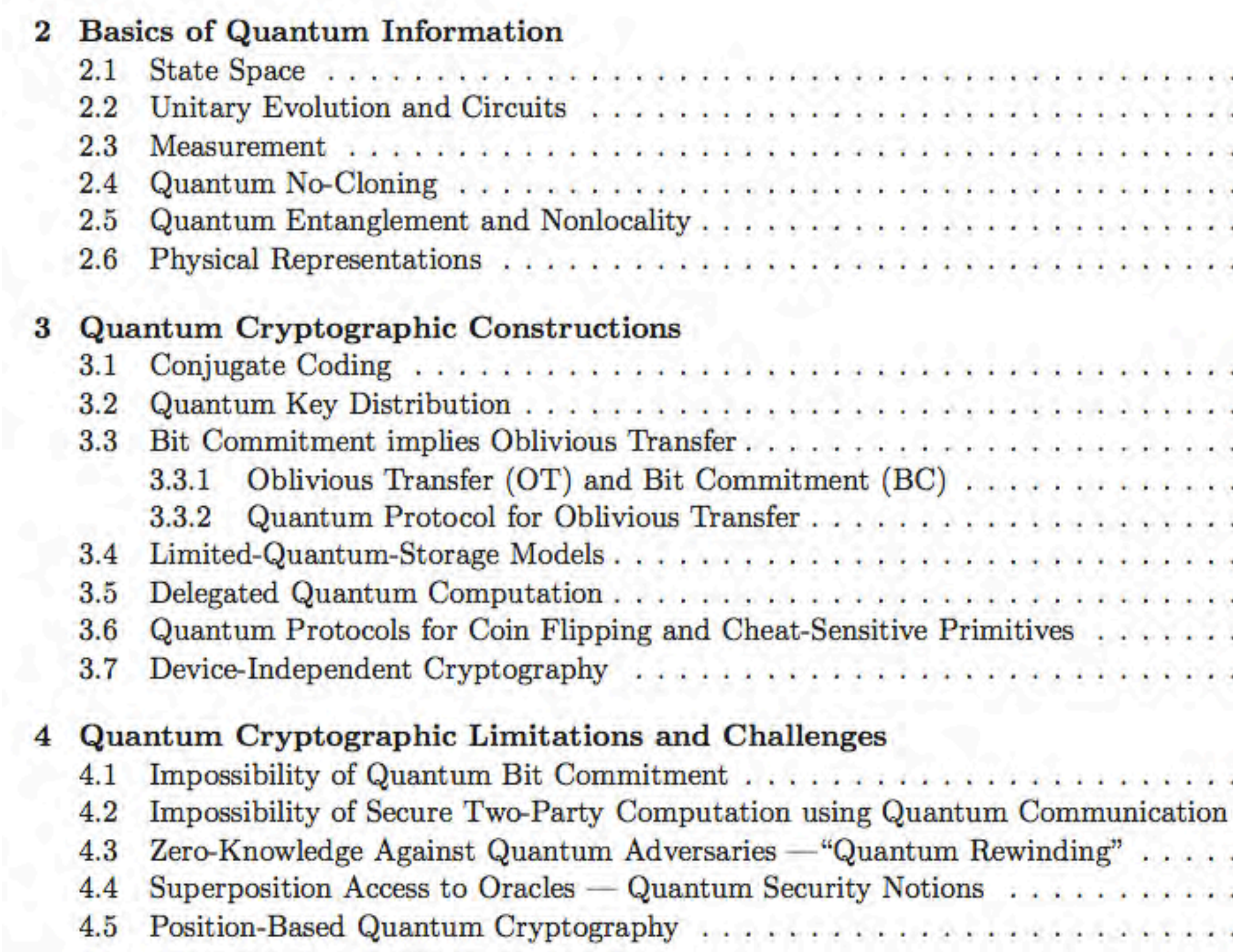
All material available on https://homepages.cwi.nl/~schaffne

QIP 2018 Tutorial in Delft

Sunday, 14 January 2018


experiment
OPEN Q:
MILESTONES
Q Crypto
QKD
Sec proofs
everlasting security
protocols
BB84
B91
COW
6-state
CV
implementations
CV
authentication problem
repeaters
limits
implementation
QRNG
Certification
DI
Quantum advantage
Fun Stuff
Signature Tokens
Time-released encryption
Key recycling
encr.
auth.
Bomb testing
position-based crypto
Q Functionalities, Q keys?
Q copy-protection?
Leakage resilience
QPUFs
Q Digital signatures
Q Money
publ. verifier
Wiesner
obfuscation
knot theory
Q attacks on symm. crypto
QROM
Superposition attacks
Post-Q Crypto
pk-replacements
NIST
lattices
Merkle puzzles
hash-based
code-based
multivariate polynomials
isogeny-based
collapsing
bind BC
hash fcts
(lightning)
blockchain security
indifferentiability
QPRP
(via Feistel)
Q crypt. analysis
implementation
Conjugate coding (QOTP)
Tools
non-local games
repres. theory
RAC
uncertainty relations
smooth entropies
randomness extraction
CV
composability frameworks
port-based teleportation
no-cloning
Q compl. theory
SDPs
Bell ineq.
classical crypto
de Finetti
Fourier analysis
q rewinding
query complexity (avg. case)
impossibilities
cheat sensitivity
point-games
plain model
2-party crypto
or more
assumptions
BQSM
Noisy-storage
CV
Isolated-Qbits Model
Leader election
protocols/primitives
PIR
CF
BC
OT
ident.
MPC
Byzantine agreement
Relativistic crypto
ZK
OT?
BC
longer
Q side info
multi-round
multi-prover
composability
summoning state
q secret sharing
device independence
tools
Bell
robust
entropy acc.
appl.
RNG
QKD
(robust)
2P crypto
comp. secure q. crypto
Def of Q-IND CPA, CCA1
IT Non-malleability
Q Unforgeability CCA2, auth. encryption
QNMC
PRU
Q Data, computation
Comp. assumptions
delegated computation
Blind computation
QC on auth. data
(strong) purity testing codes
Q authentication
Q encryption
QFHE (with verification)
CV?
Q One-Time Programs
how to verify a QC
Q obfuscation?
(VBB)
classical Verifier of Q Comp
single-prover
|x⟩
0
|0⟩
|x⟩|y⟩
f: {0,1}ⁿ → {0,1}ⁿ
RO
Goal: find x, f(x), f(f(x))

Quantum Cryptography Beyond QKD



- survey article with Anne Broadbent
- aimed at classical cryptographers

http://arxiv.org/abs/1510.06120
In Designs, Codes and Cryptography 2016

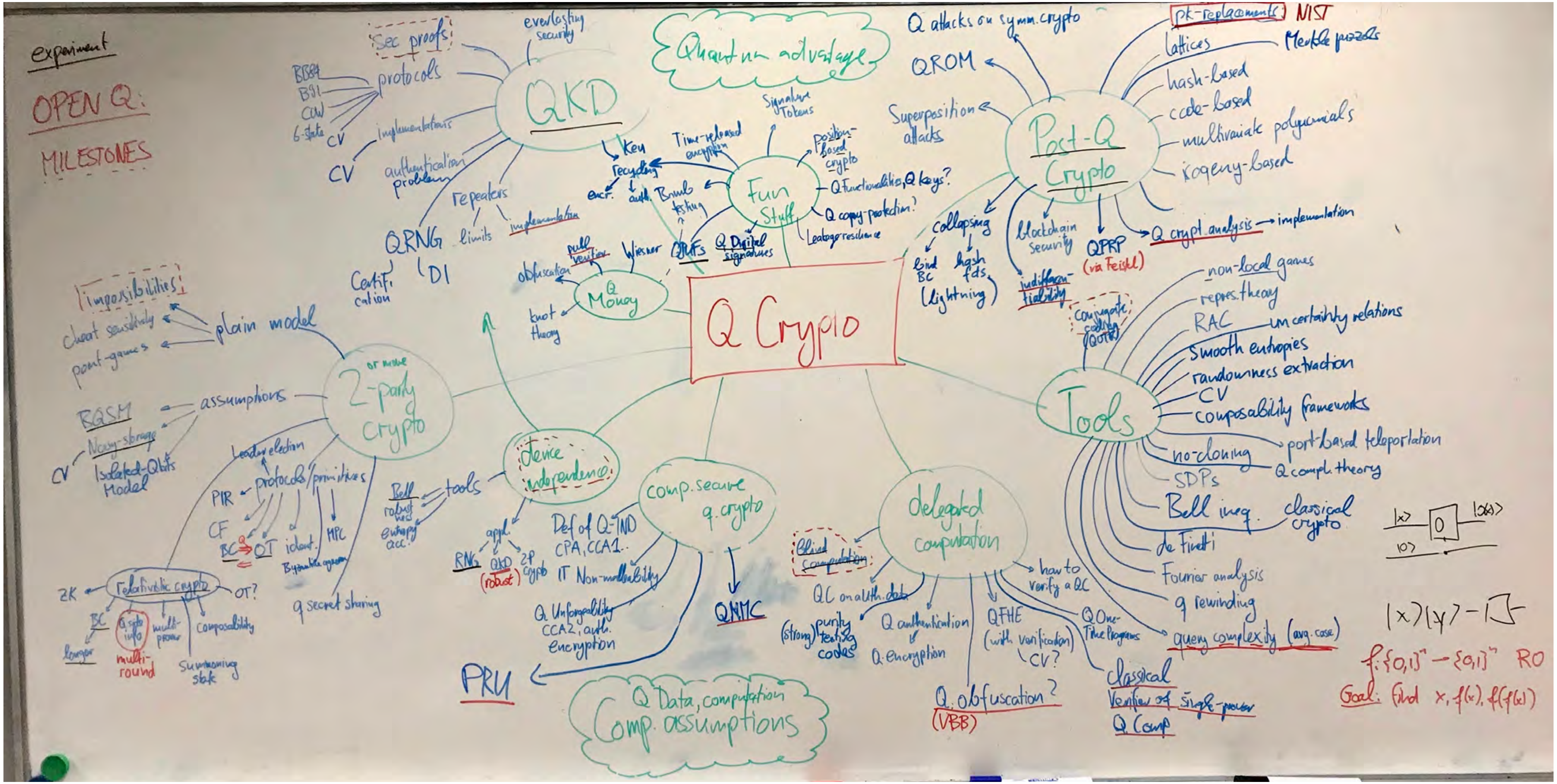
[Broadbent Schaffner 16 in Designs, Codes and Cryptography]

QCrypt Conference Series

- Started in 2011 by Christandl and Wehner
- Steadily growing since then:
  approx. 100 submissions, 30 accepted as contributions,
  330 participants in Cambridge 2017. This year: Shanghai, China
- It is the goal of the conference to represent the previous year’s best results on quantum cryptography, and to support the building of a research community
- Trying to keep a healthy balance between theory and experiment
- Half the program consists of 4 tutorials of 90 minutes, 6-8 invited talks
- present some statistical observations about the last 4 editions

[QCrypt charter, QCrypt 2017 business meetings slides]

Overview

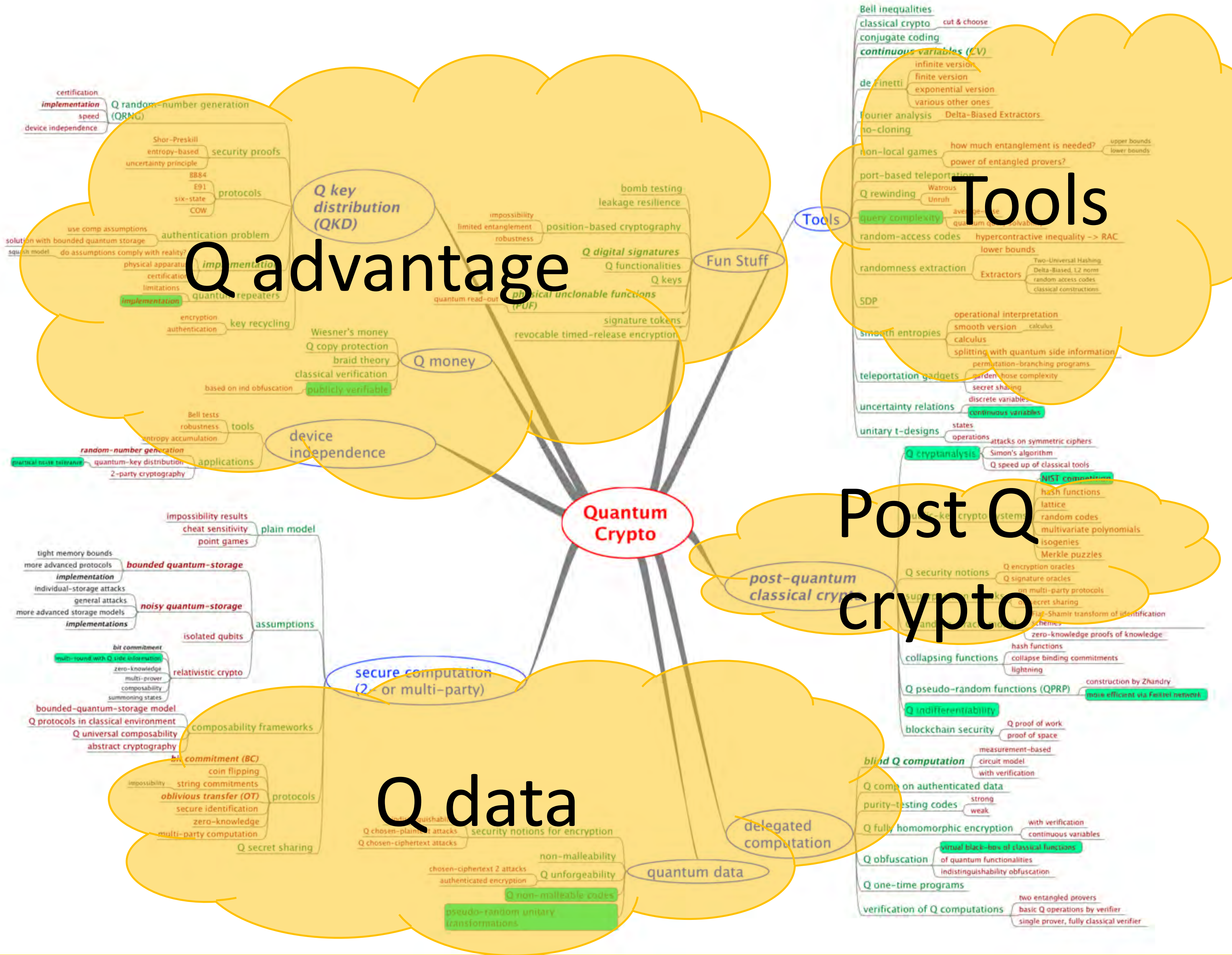


[thanks to Serge Fehr, Stacey Jeffery, Chris Majenz, Florian Speelman, Ronald de Wolf]

MindMap

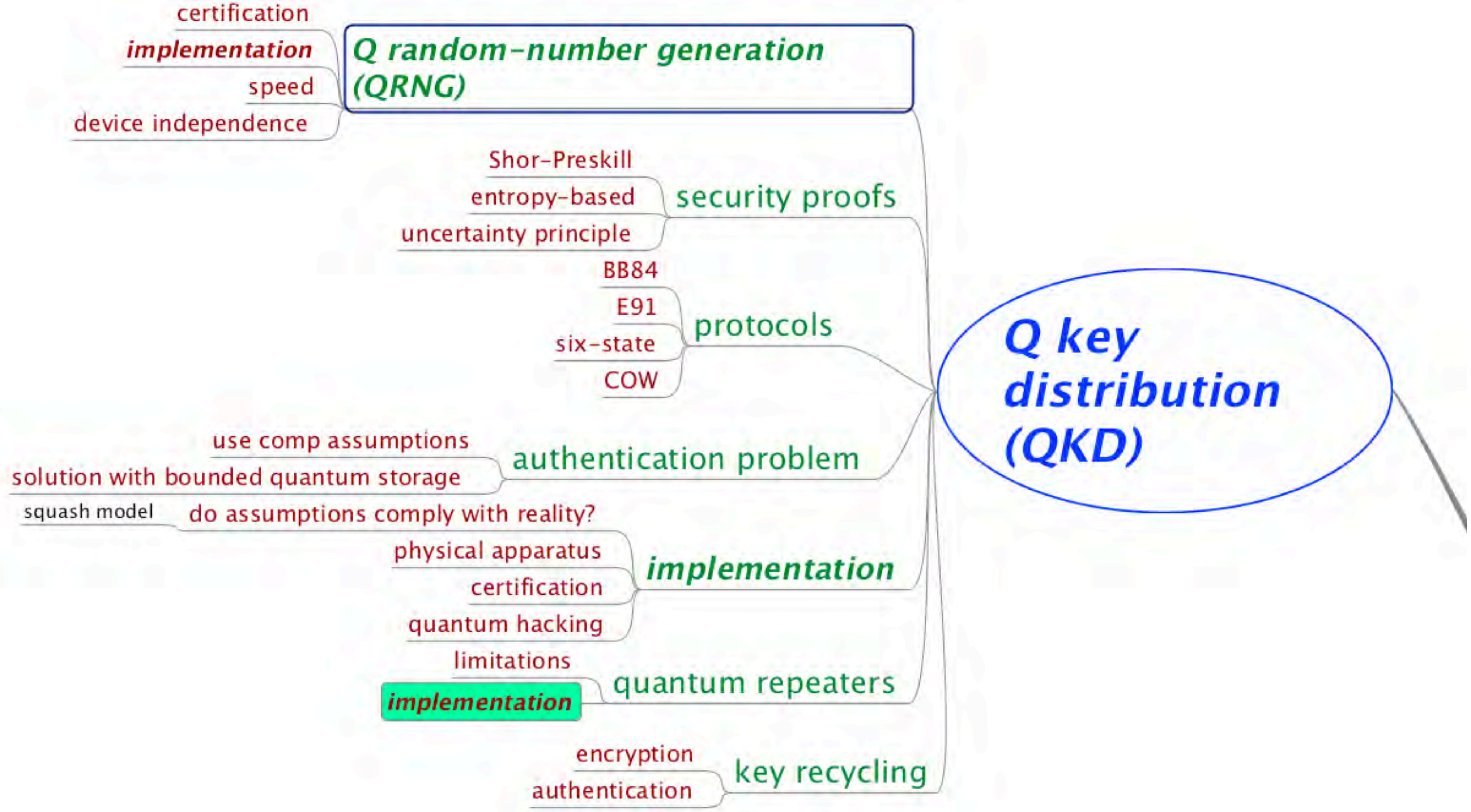
- ***experiments***
- Selection of open questions

- Fork me on github!

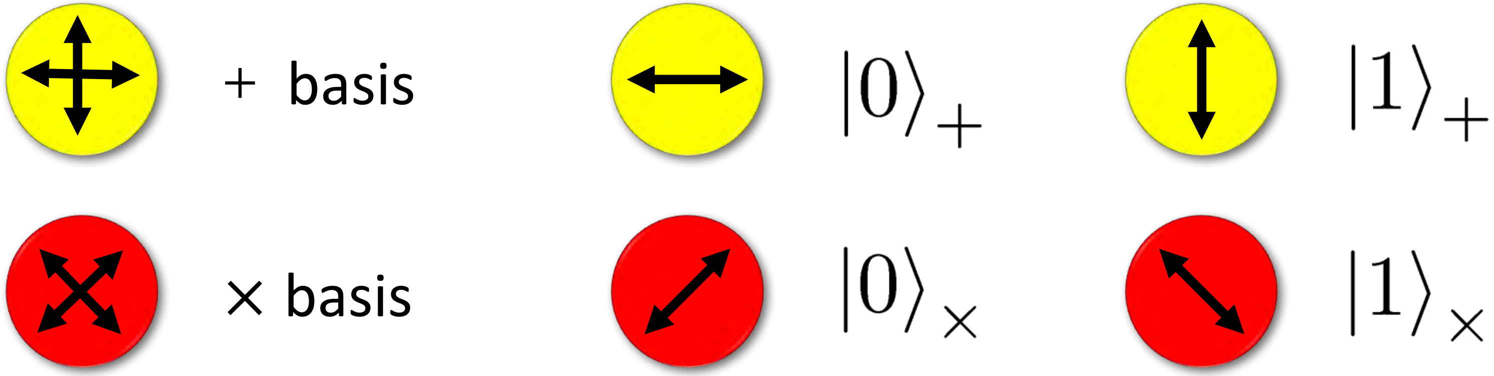


[https://github.com/cschaffner/QCryptoMindmap]

Quantum Key Distribution (QKD)



Quantum Mechanics

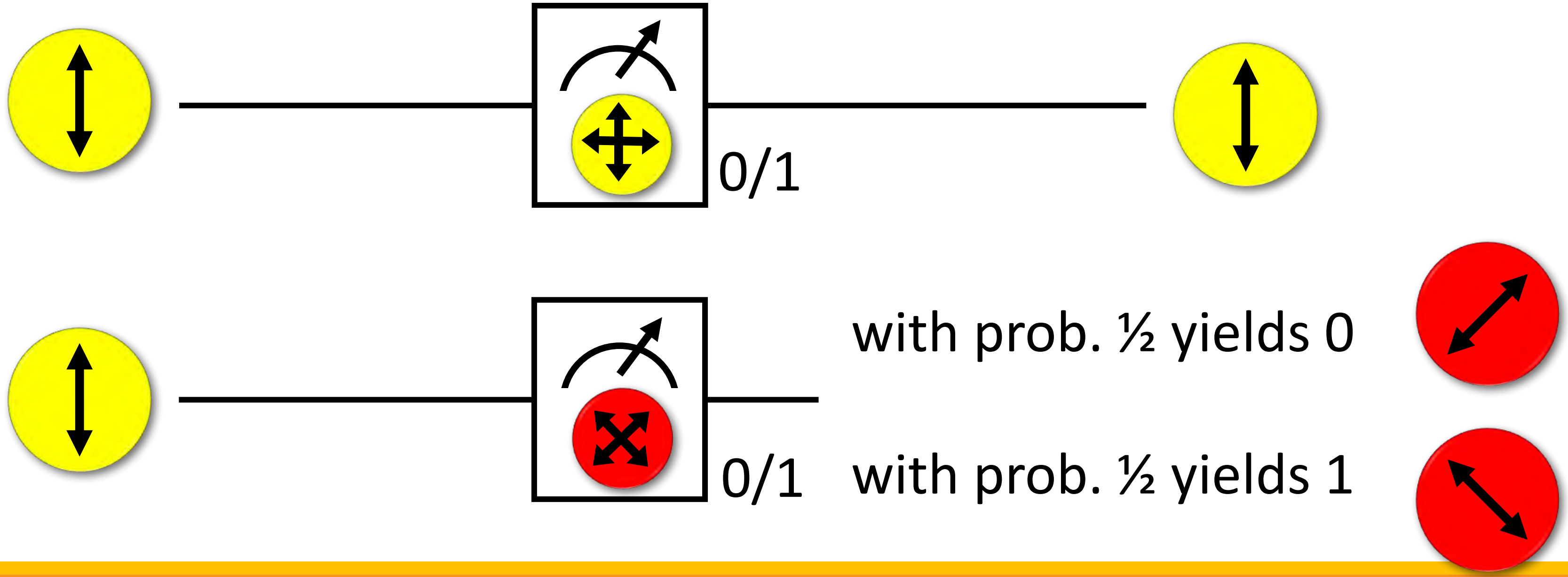


+ basis $|0\rangle_+$ $|1\rangle_+$

× basis $|0\rangle_\times$ $|1\rangle_\times$

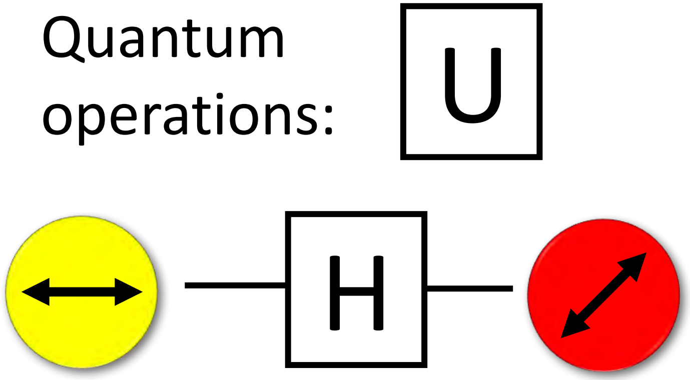
Measurements:

with prob. 1 yields 1



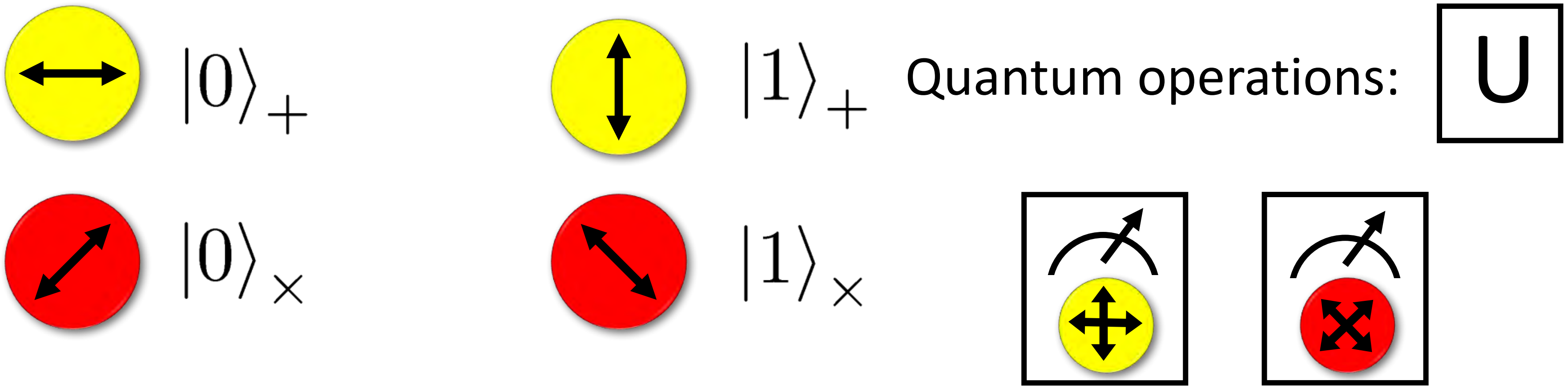
with prob. ½ yields 0

with prob. ½ yields 1



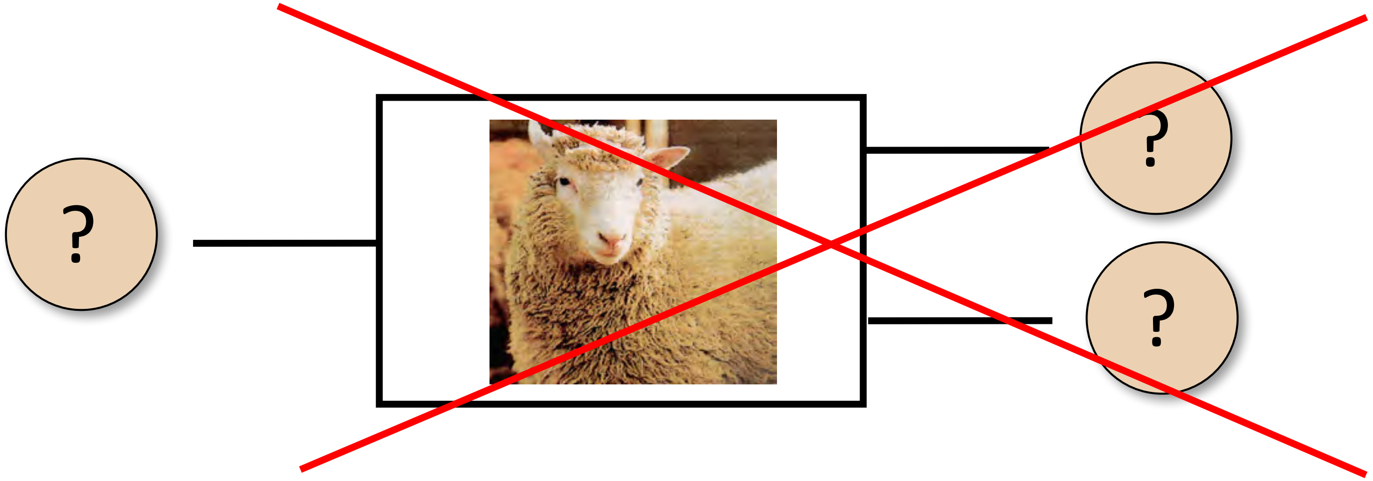
Quantum operations:

No-Cloning Theorem



$|0\rangle_+$ $|1\rangle_+$ Quantum operations: $\boxed{U}$

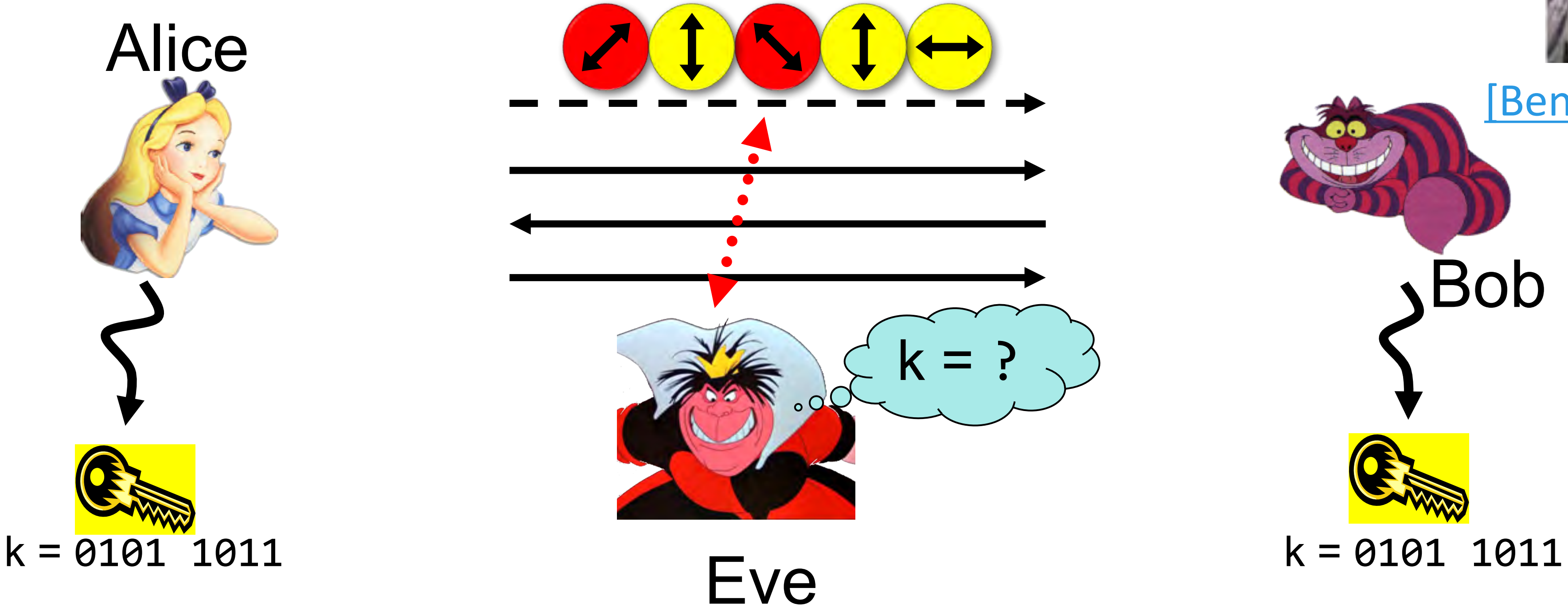
$|0\rangle_\times$ $|1\rangle_\times$



Proof: copying is a non-linear operation

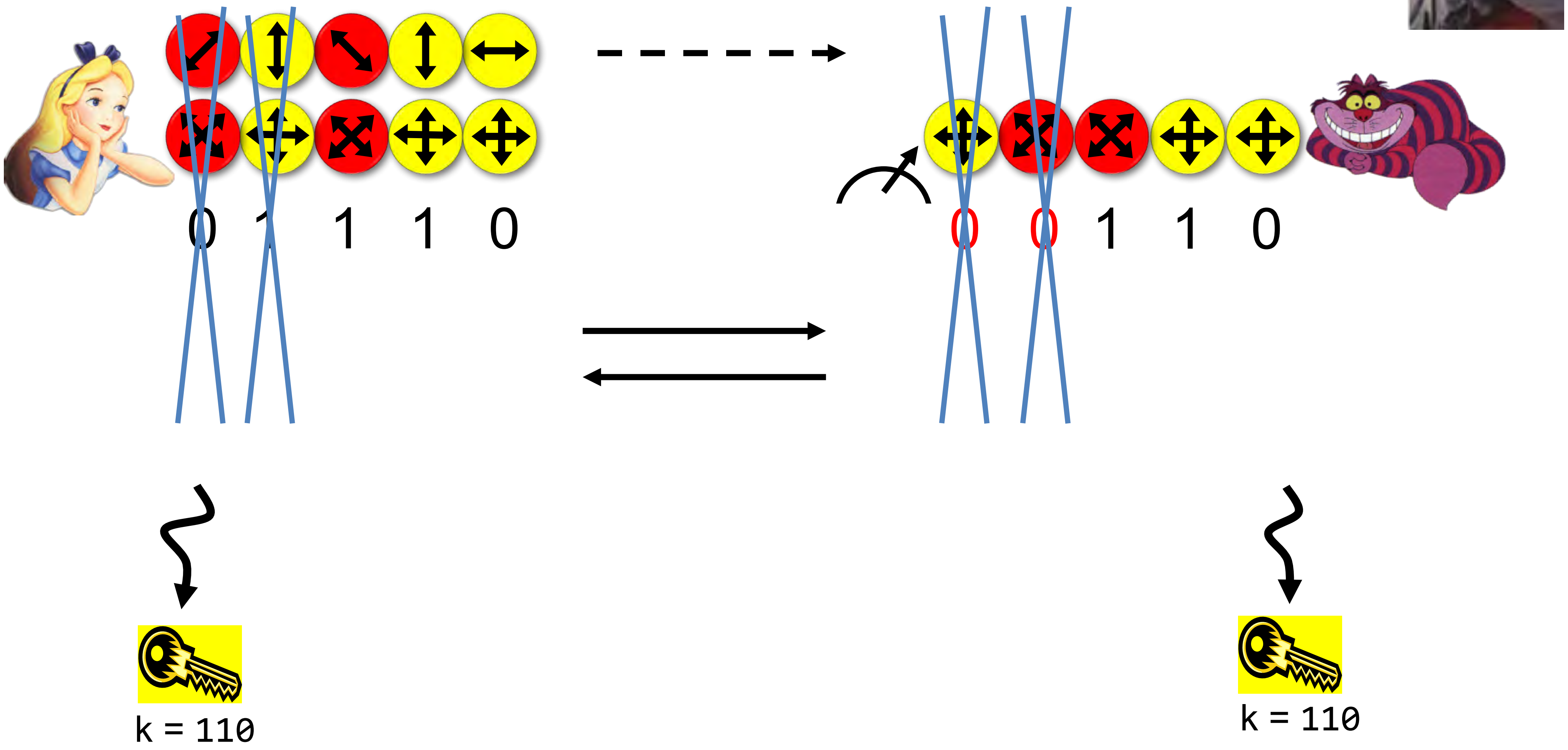
Quantum Key Distribution (QKD)

[Bennett Brassard 84]



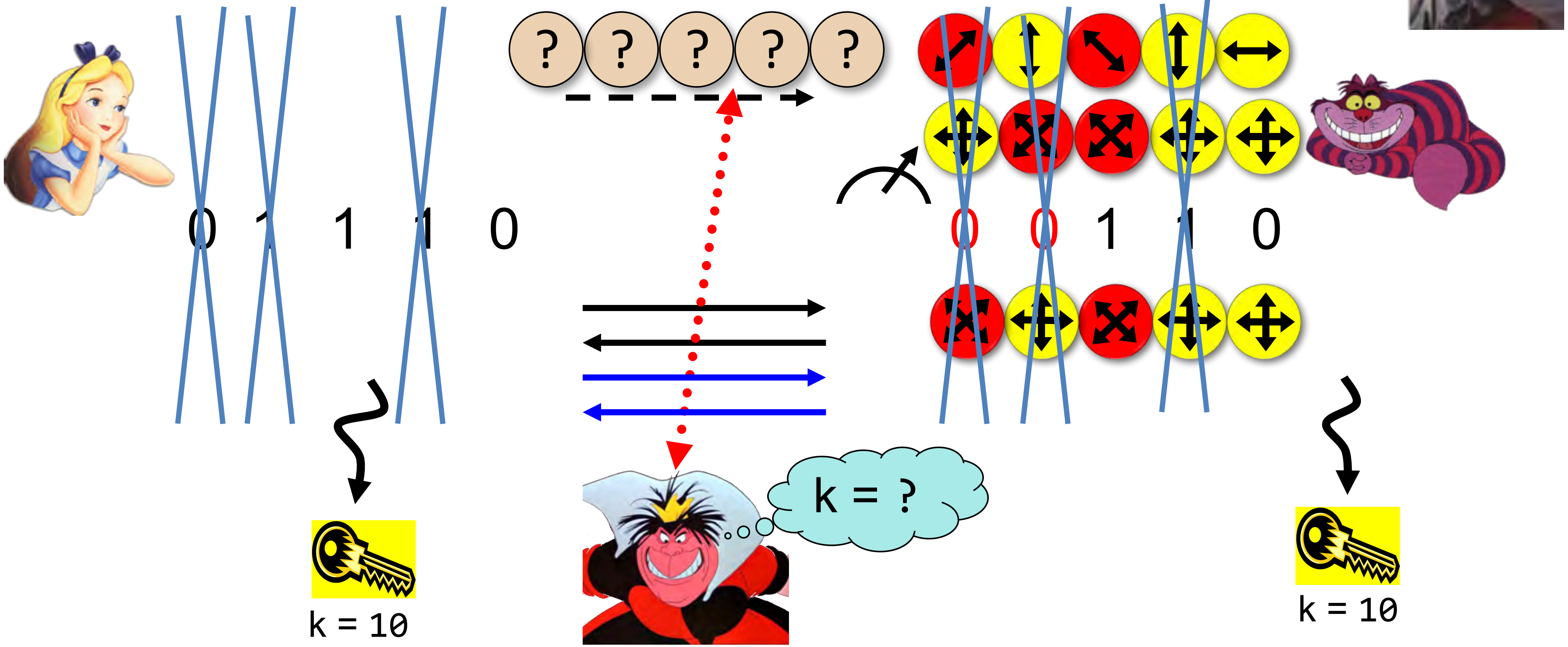
- Offers an quantum solution to the key-exchange problem which does not rely on computational assumptions (such as factoring, discrete logarithms, security of AES, SHA-3 etc.)
- Caveat: classical communication has to be authenticated to prevent man-in-the-middle attacks

Quantum Key Distribution (QKD)

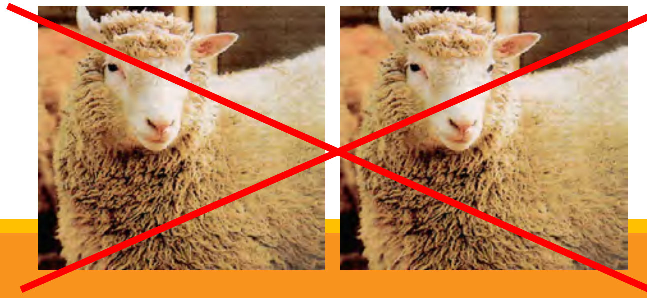


[Bennett Brassard 84]

Quantum Key Distribution (QKD)

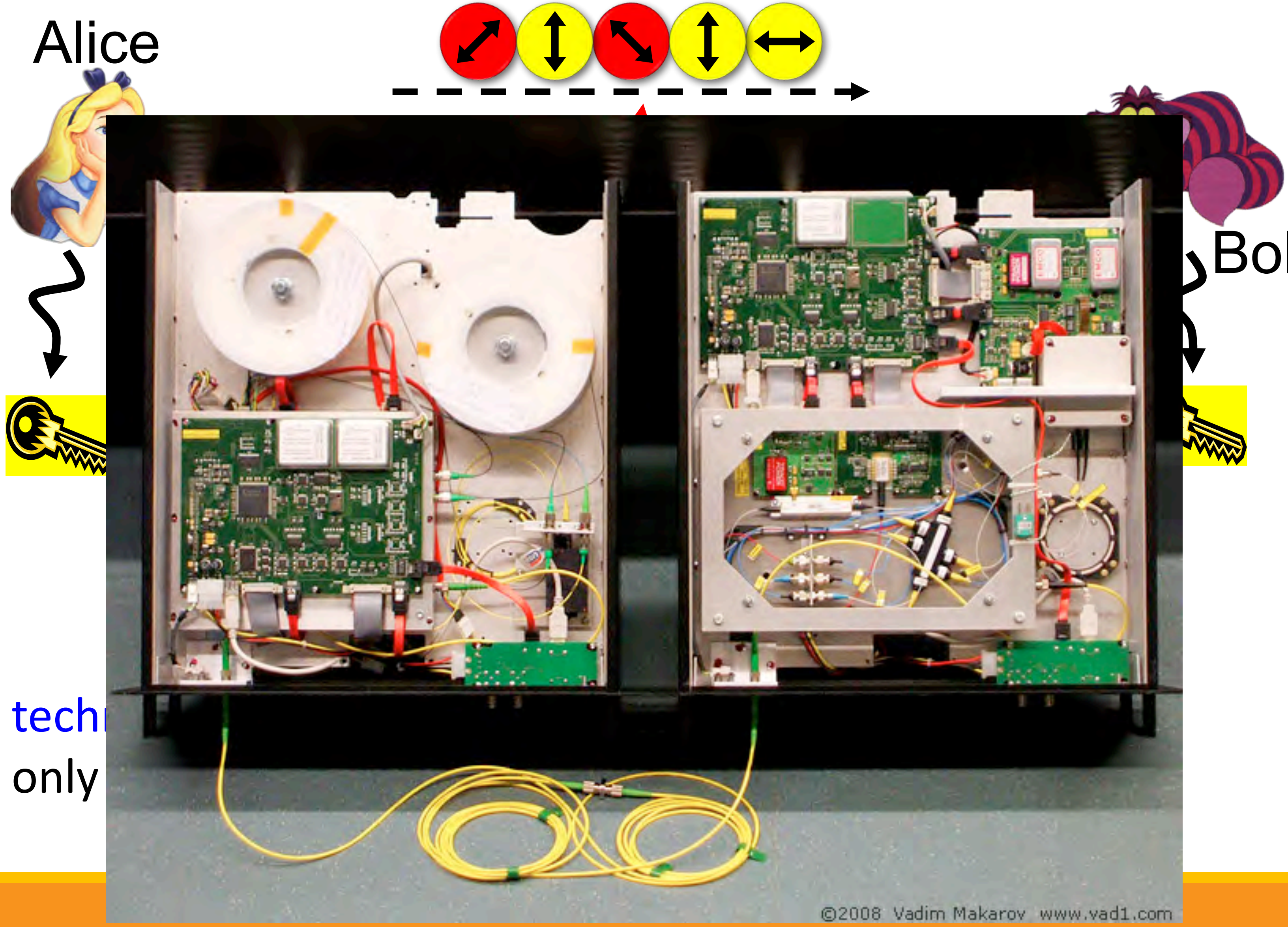


- Quantum states are unknown to Eve, she cannot copy them.
- Honest players can test whether Eve interfered.



[Bennett Brassard 84]

Quantum Key Distribution (QKD)

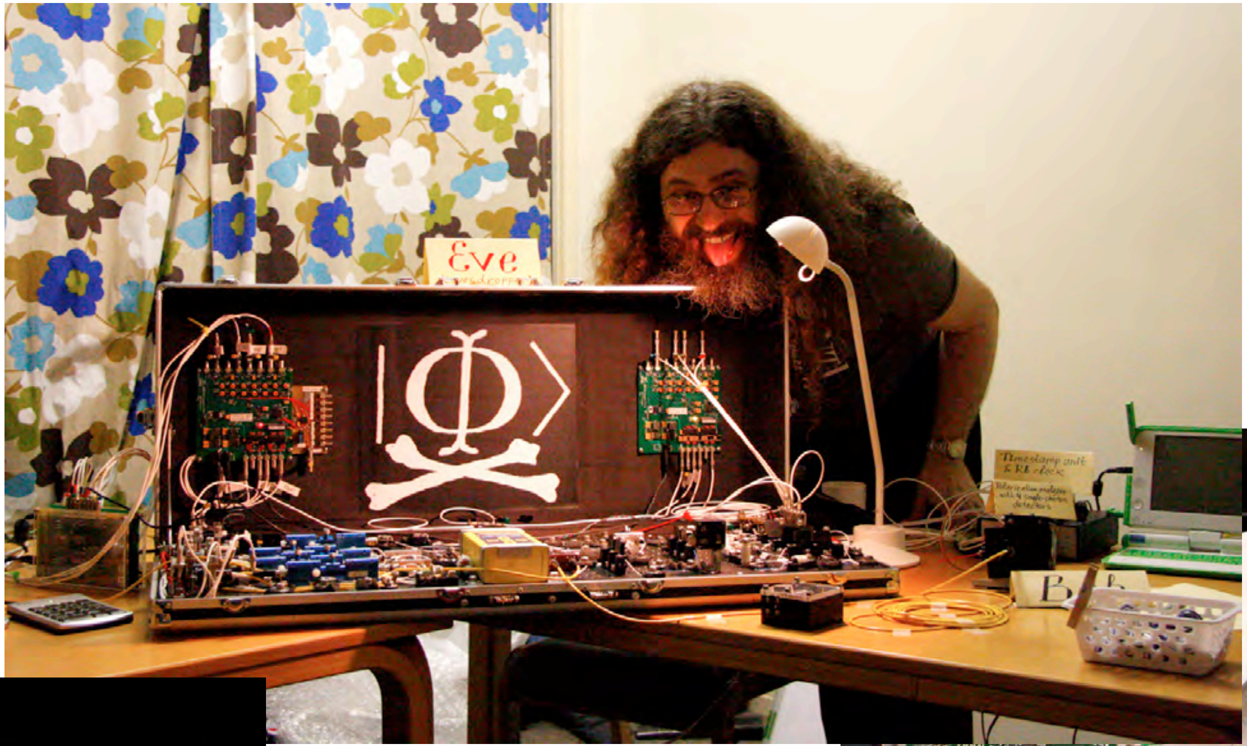


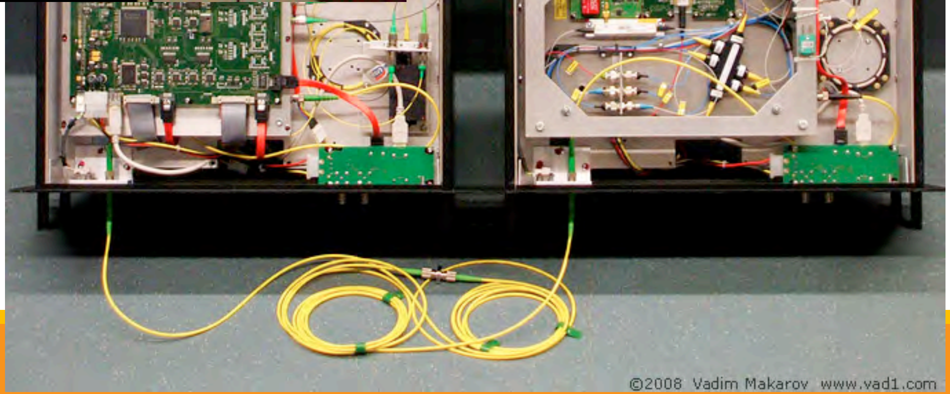
©2008 Vadim Makarov www.vad1.com

- techn
  only

Quantum Hacking

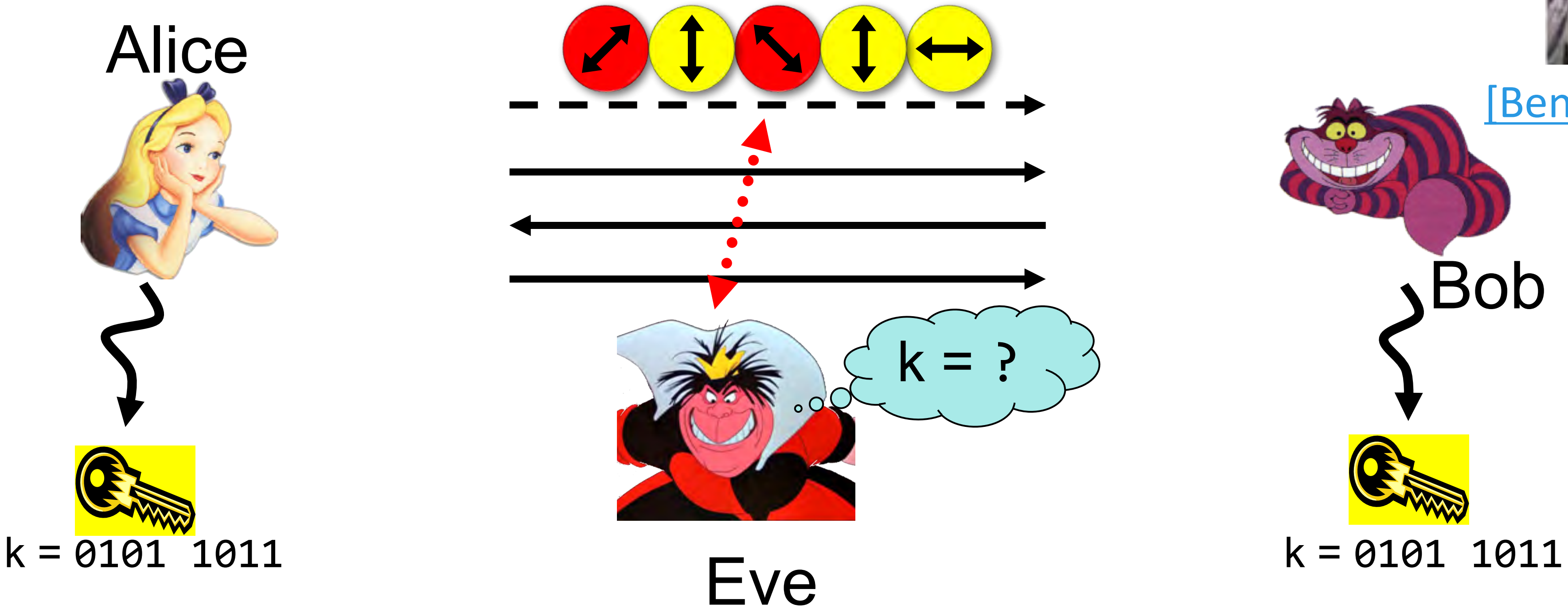
e.g. by the group of Vadim Makarov (University of Waterloo, Canada)




©2008 Vadim Makarov www.vad1.com

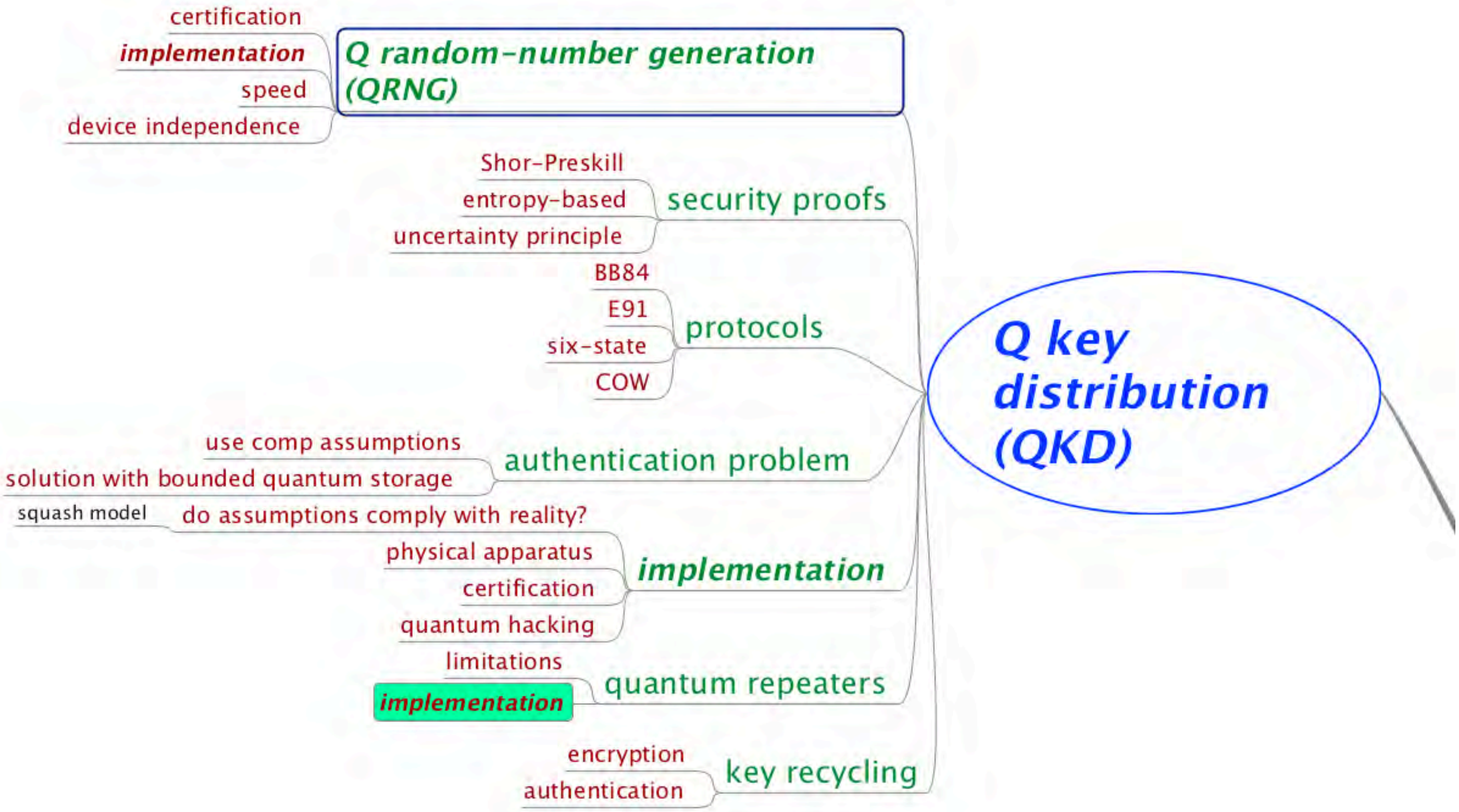
Quantum Key Distribution (QKD)

[Bennett Brassard 84]



- **Three-party scenario**: two honest players versus one dishonest eavesdropper
- **Quantum Advantage:** Information-theoretic security is provably impossible with only classical communication (Shannon’s theorem about perfect security)

Quantum Key Distribution (QKD)



Q key distribution (QKD)

Q random-number generation (QRNG)

- certification
- *implementation*
- speed
- device independence

security proofs

- Shor-Preskill
- entropy-based
- uncertainty principle

protocols

- BB84
- E91
- six-state
- COW

authentication problem

- use comp assumptions
- solution with bounded quantum storage

implementation

- do assumptions comply with reality?
  - squash model
- physical apparatus
- certification
- quantum hacking

quantum repeaters

- limitations
- *implementation*

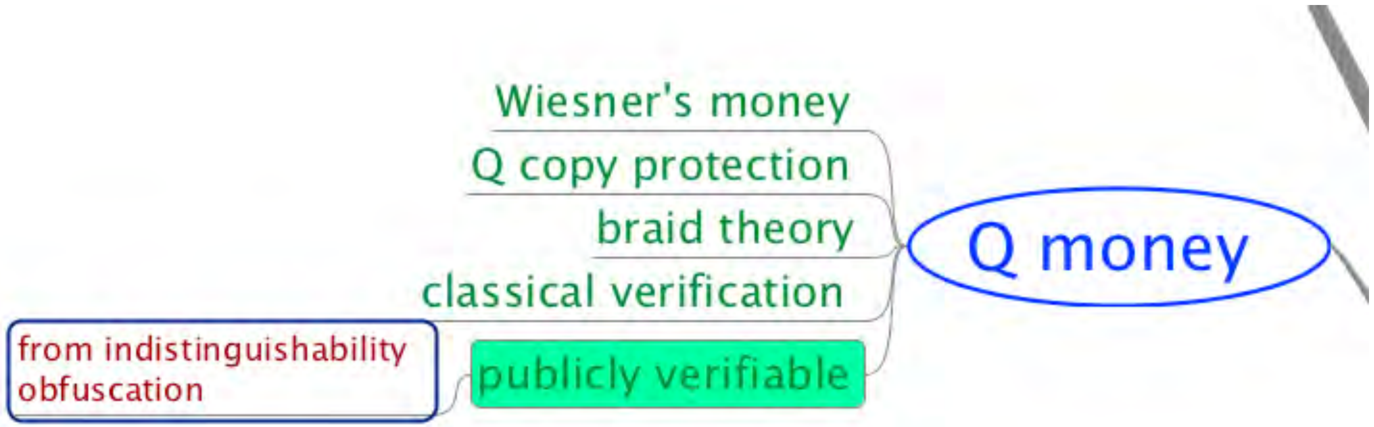
key recycling

- encryption
- authentication

Conjugate Coding & Q Money

[Wiesner 68]

also known as **quantum coding** or **quantum multiplexing**



Wiesner's money

Q copy protection

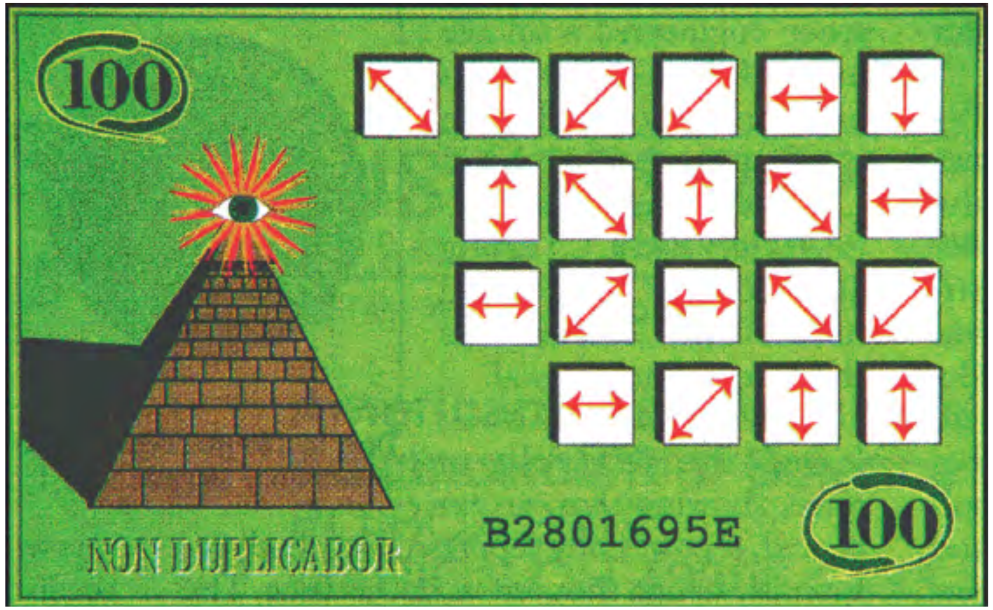
braid theory

classical verification

publicly verifiable

from indistinguishability obfuscation

Q money



- Originally proposed for securing quantum banknotes (private-key quantum money)
- Adaptive attack if money is returned after successful verification
- Publicly verifiable quantum money is still a topic of active research, e.g. very recent preprint by Zhandry17

[Molina Vidick Watrous 13, Brodutch Nagaj Sattath Unruh 14]

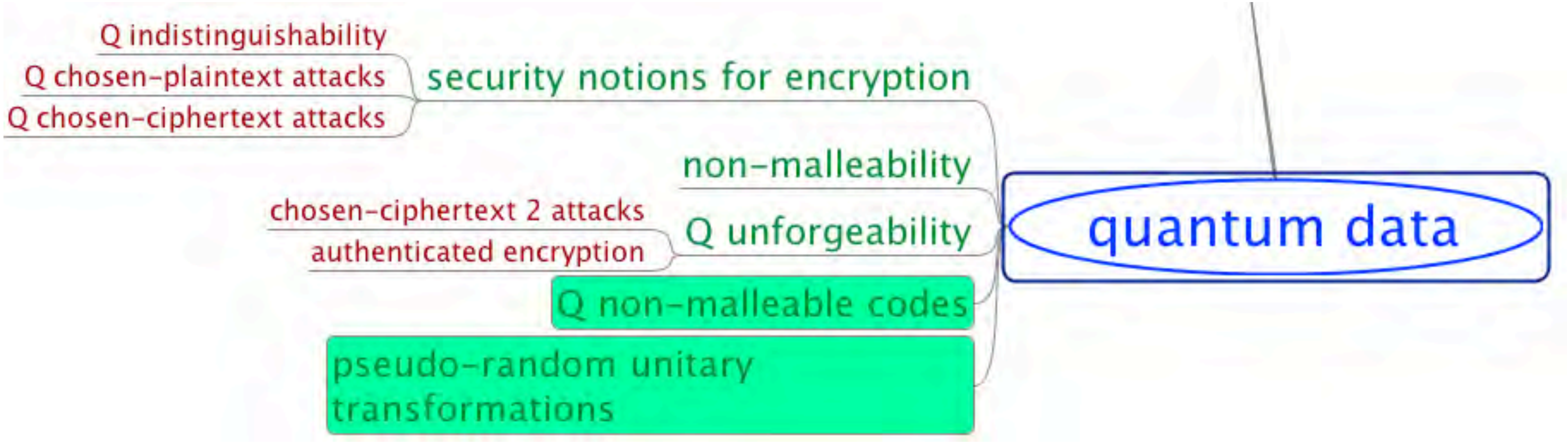
Computational Security of Quantum Encryption

GORJAN ALAGIC, COPENHAGEN
ANNE BROADBENT, OTTAWA
BILL FEFFERMAN, MARYLAND
TOMMASO GAGLIARDONI, DARMSTADT
MICHAEL ST JULES, OTTAWA

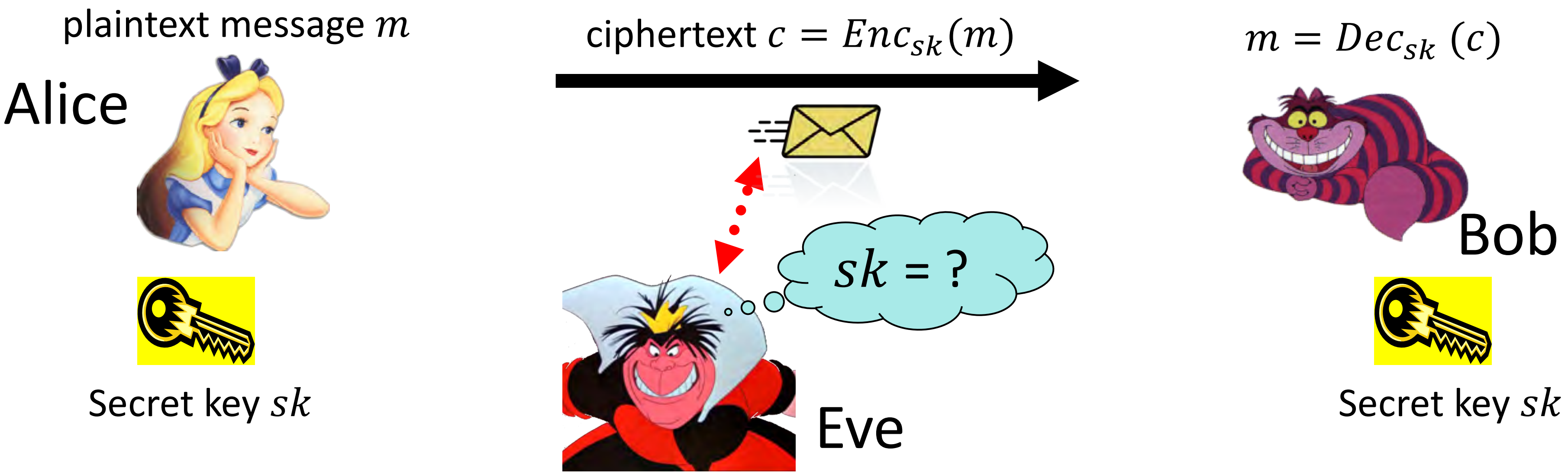
http://arxiv.org/abs/1602.01441
at ICITS 2016

CHRISTIAN SCHAFFNER,
AMSTERDAM

Computational Security of Quantum Encryption


quantum data
security notions for encryption
Q indistinguishability
Q chosen-plaintext attacks
Q chosen-ciphertext attacks
non-malleability
Q unforgeability
chosen-ciphertext 2 attacks
authenticated encryption
Q non-malleable codes
pseudo-random unitary transformations

Secure Encryption



plaintext message m

ciphertext $c = Enc_{sk}(m)$

$m = Dec_{sk}\ (c)$

Secret key sk

Secret key sk

One-Time Pad:

Classical: $c = Enc_{sk}(m) := m \oplus sk$, $Dec_{sk}(c) := c \oplus sk$

Quantum: $Enc_{a,b}(\rho_M) := X^a Z^b \rho_M Z^b X^a$

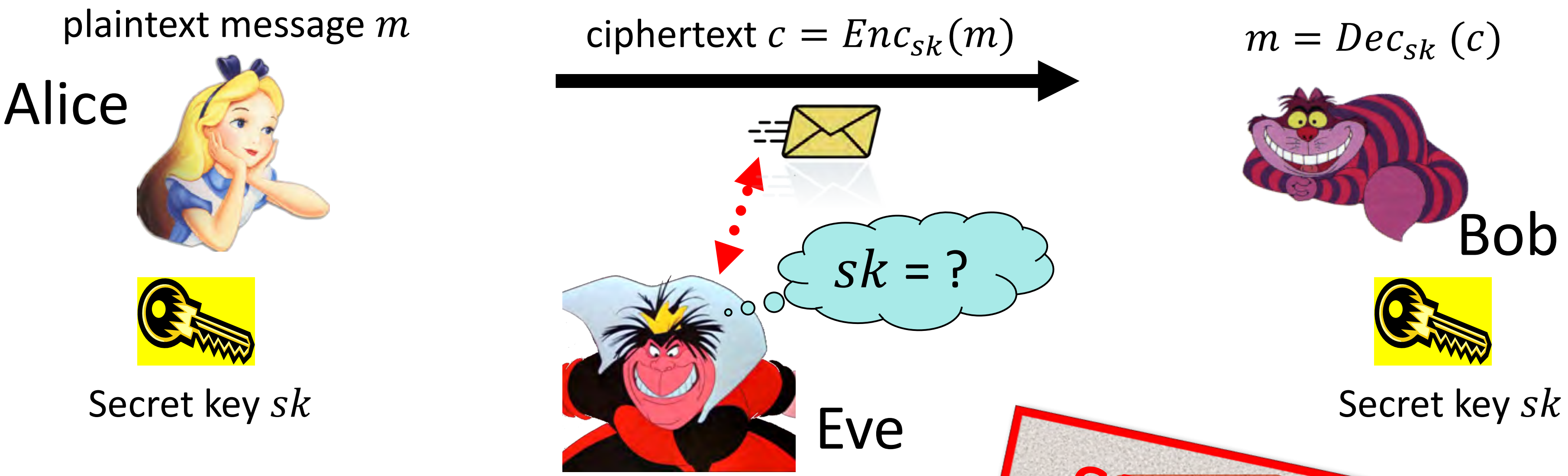
$Dec_{a,b}(\rho_C) := X^a Z^b \rho_C Z^b X^a$

SECURE

QOTP

[Miller 1882, Vernam 1919, Ambainis Mosca Tapp de Wolf 00, Boykin Roychowdhury 03]

Information-Theoretic Security



SECURE

QOTP

Perfect / information-theoretic security:

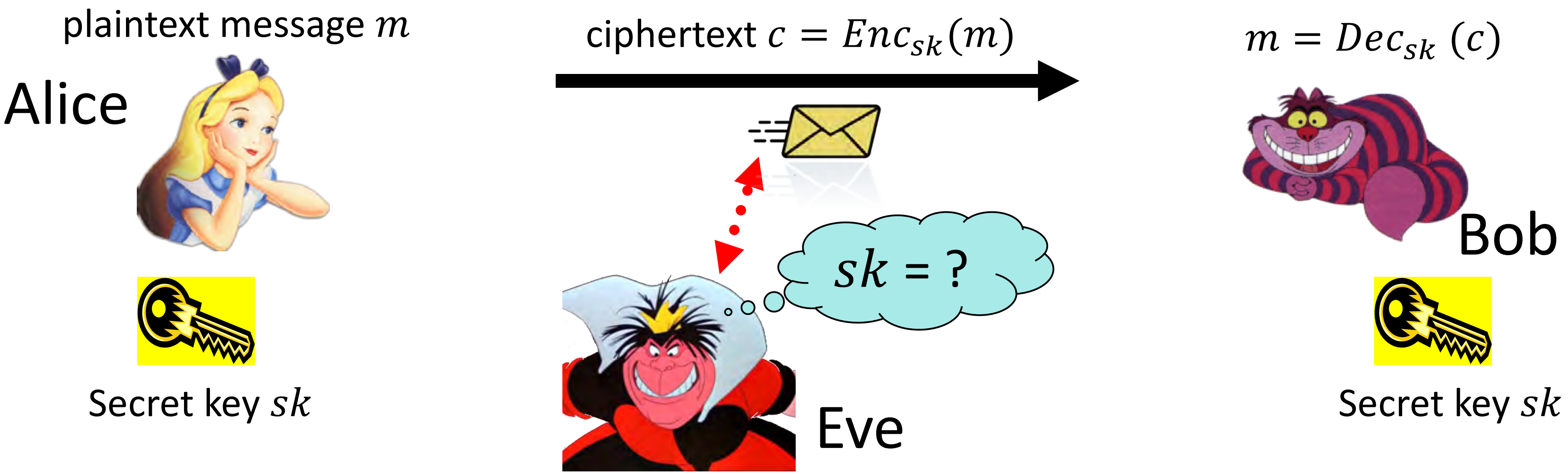
Ciphertext distribution P_C is statistically independent of message distribution P_M.

Theorem: Secret key has to be as large as the message.

Highly impractical, e.g. for encrypting a video stream…

[Shannon 48, Dodis 12, Ambainis Mosca Tapp de Wolf 00, Boykin Roychowdhury 03]

Computational Security



plaintext message m

Alice

Secret key sk

ciphertext $c = Enc_{sk}(m)$

sk = ?

Eve

$m = Dec_{sk}\ (c)$

Bob

Secret key sk

Threat model:

- Eve sees ciphertexts (eavesdropper)
- Eve knows plaintext/ciphertext pairs
- Eve chooses plaintexts to be encrypted
- Eve can decrypt ciphertexts

Security guarantee:

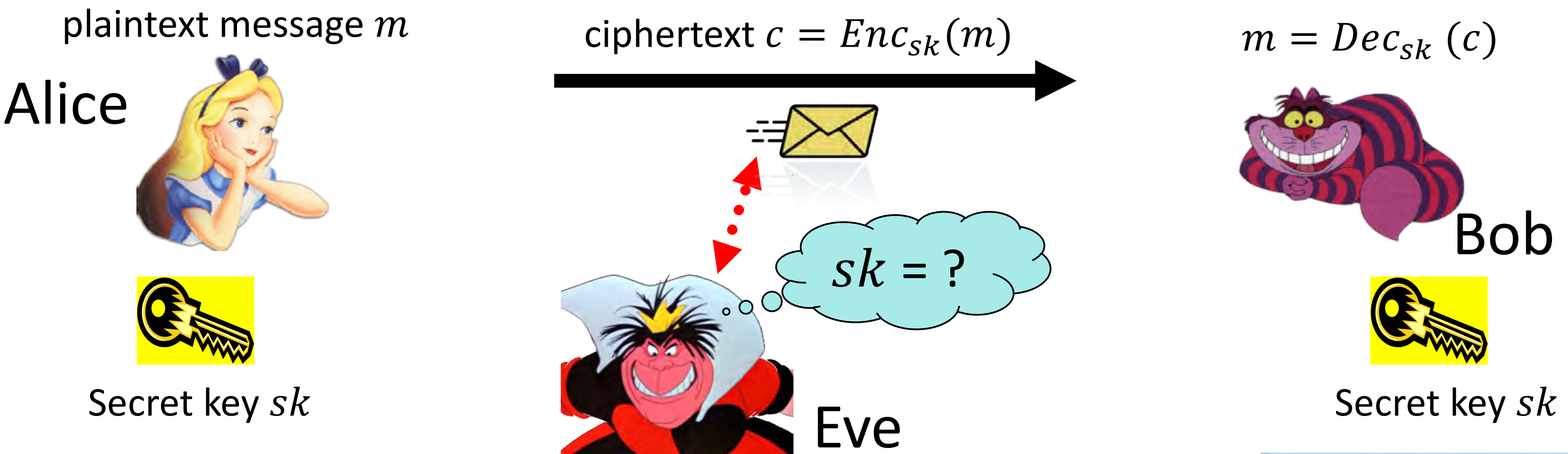
c does not reveal sk

c does not reveal the whole m

c does not reveal any bit of m

c does not reveal “anything” about m

Semantic Security



plaintext message m

Alice

ciphertext $c = Enc_{sk}(m)$

$m = Dec_{sk}(c)$

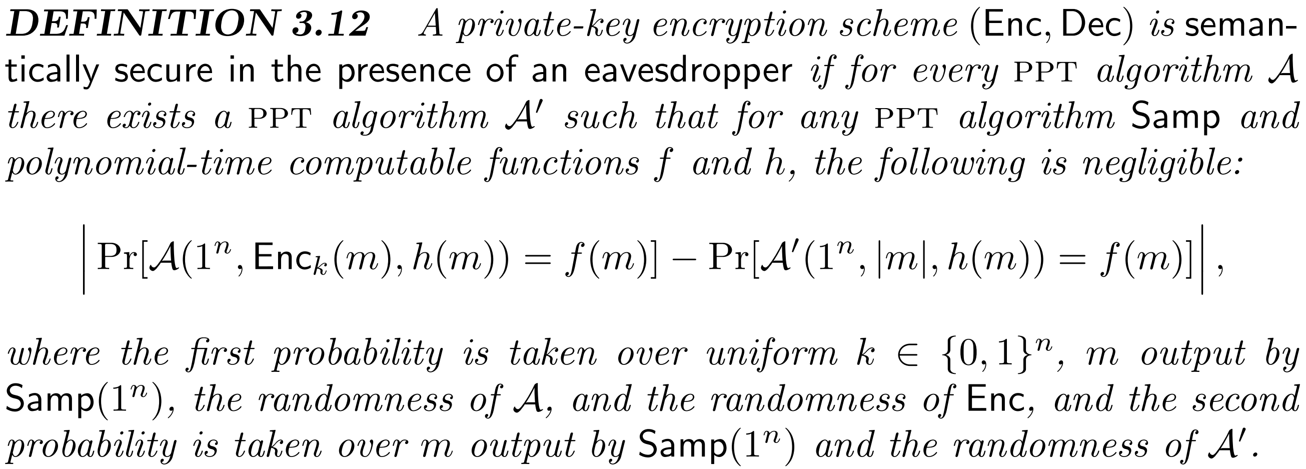
Bob

sk = ?

Eve

Secret key sk

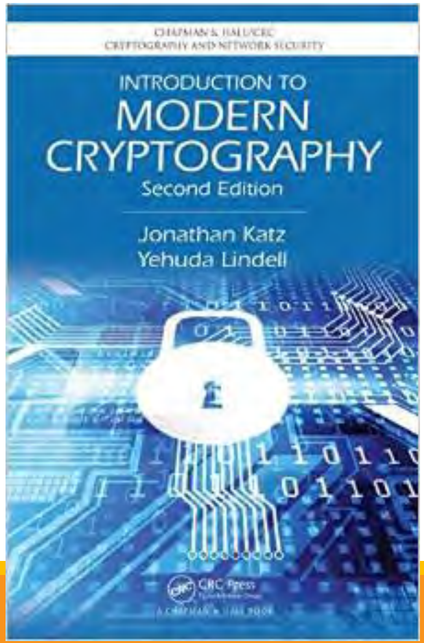
Secret key sk



DEFINITION 3.12 *A private-key encryption scheme* (Enc, Dec) *is* semantically secure in the presence of an eavesdropper *if for every* PPT *algorithm* $\mathcal{A}$ *there exists a* PPT *algorithm* $\mathcal{A}'$ *such that for any* PPT *algorithm* Samp *and polynomial-time computable functions* f *and* h*, the following is negligible:*

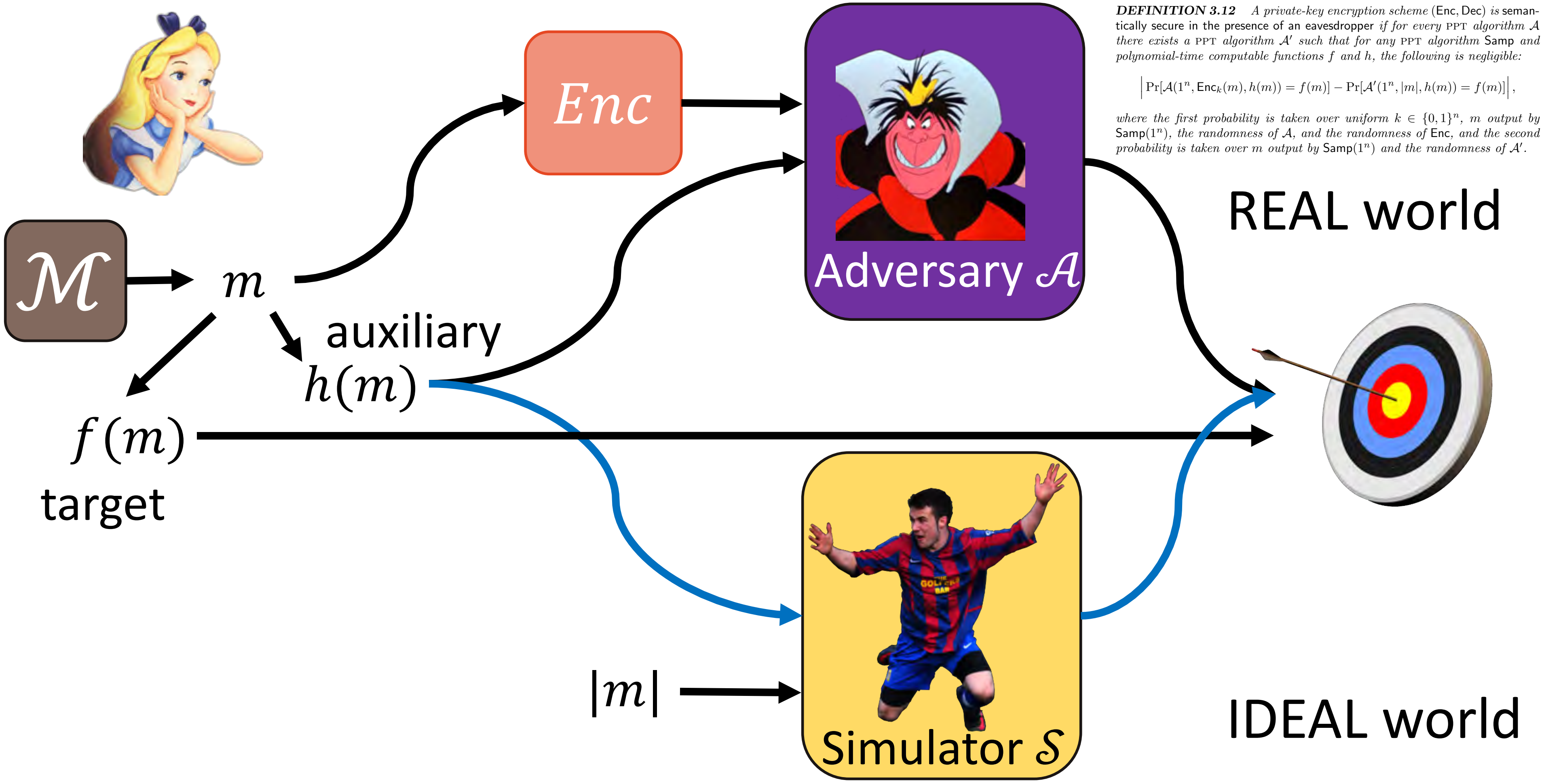
$$\left| \Pr[\mathcal{A}(1^n, \mathsf{Enc}_k(m), h(m)) = f(m)] - \Pr[\mathcal{A}'(1^n, |m|, h(m)) = f(m)] \right|,$$

where the first probability is taken over uniform $k \in \{0,1\}^n$*,* m *output by* $\mathsf{Samp}(1^n)$*, the randomness of* $\mathcal{A}$*, and the randomness of* Enc*, and the second probability is taken over* m *output by* $\mathsf{Samp}(1^n)$ *and the randomness of* $\mathcal{A}'$*.*



[Goldwasser Micali 84] leading to Turing-Award (Noble price for CS)

Classical Semantic Security



DEFINITION 3.12 *A private-key encryption scheme* (Enc, Dec) *is* semantically secure in the presence of an eavesdropper *if for every* PPT *algorithm* $\mathcal{A}$ *there exists a* PPT *algorithm* $\mathcal{A}'$ *such that for any* PPT *algorithm* Samp *and polynomial-time computable functions* f *and* h, *the following is negligible:*

$$\left| \Pr[\mathcal{A}(1^n, \mathsf{Enc}_k(m), h(m)) = f(m)] - \Pr[\mathcal{A}'(1^n, |m|, h(m)) = f(m)] \right|,$$

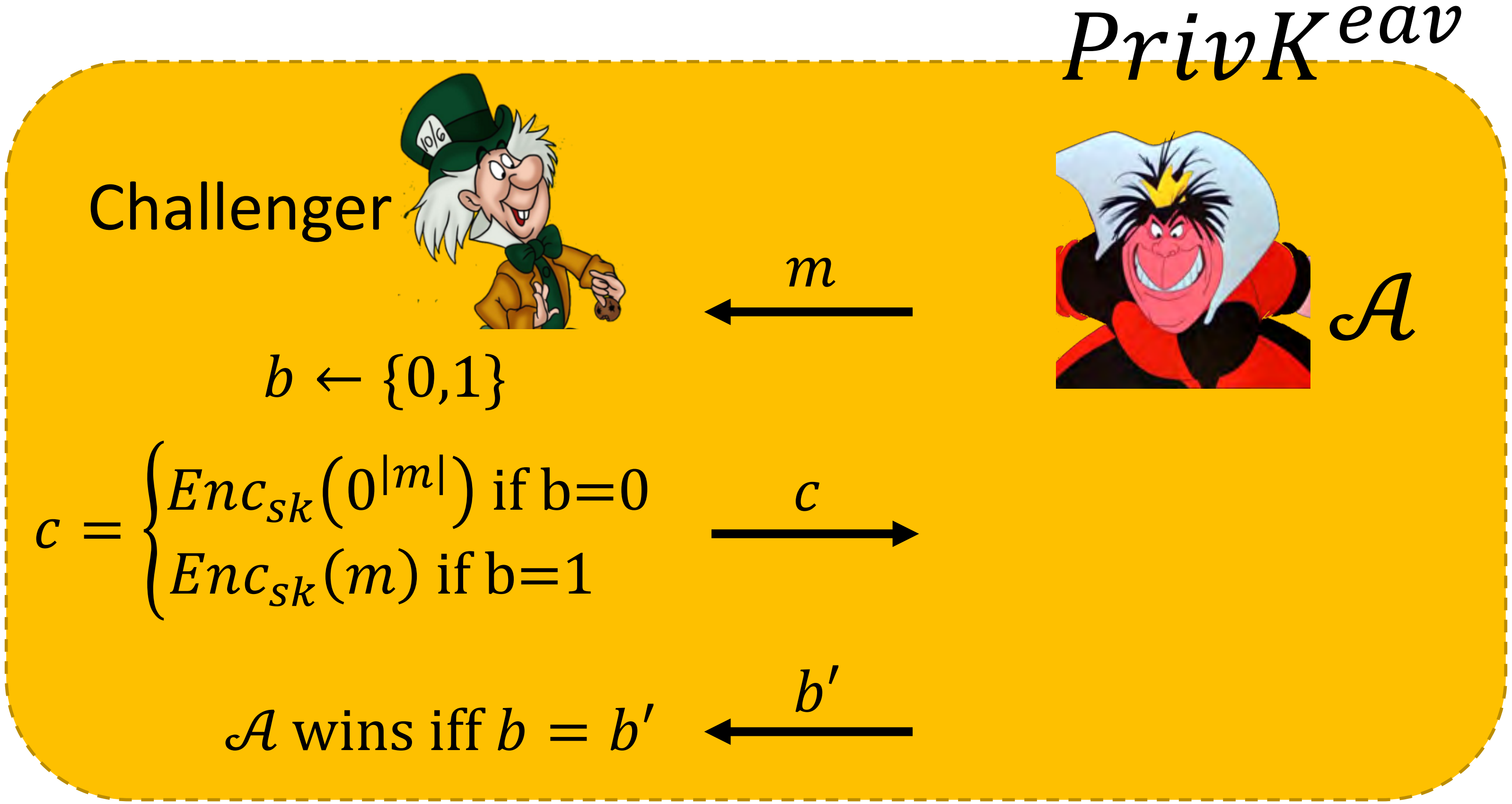
where the first probability is taken over uniform $k \in \{0,1\}^n$, m *output by* $\mathsf{Samp}(1^n)$, *the randomness of* $\mathcal{A}$, *and the randomness of* Enc, *and the second probability is taken over* m *output by* $\mathsf{Samp}(1^n)$ *and the randomness of* $\mathcal{A}'$.

Definition (SEM): $\forall \mathcal{A}\ \exists \mathcal{S} : \forall(\mathcal{M}, h, f)$

$$\Pr[\mathcal{A}(Enc_k(m), h(m)) = f(m)] \approx \Pr[\mathcal{S}(|m|, h(m)) = f(m)]$$

[Goldwasser Micali 84] leading to Turing-Award (Noble price for CS)

Classical Indistinguishability



$PrivK^{eav}$

Challenger

$\mathcal{A}$

m

$b \leftarrow \{0,1\}$

$$c = \begin{cases} Enc_{sk}\left(0^{|m|}\right) \text{ if b=0} \\ Enc_{sk}(m) \text{ if b=1} \end{cases}$$

c

b'

$\mathcal{A}$ wins iff $b = b'$

Definition (IND): $\forall \mathcal{A}\colon\ \Pr[\mathcal{A} \text{ wins } PrivK^{eav}] \leq \frac{1}{2} + \ negl(n)$

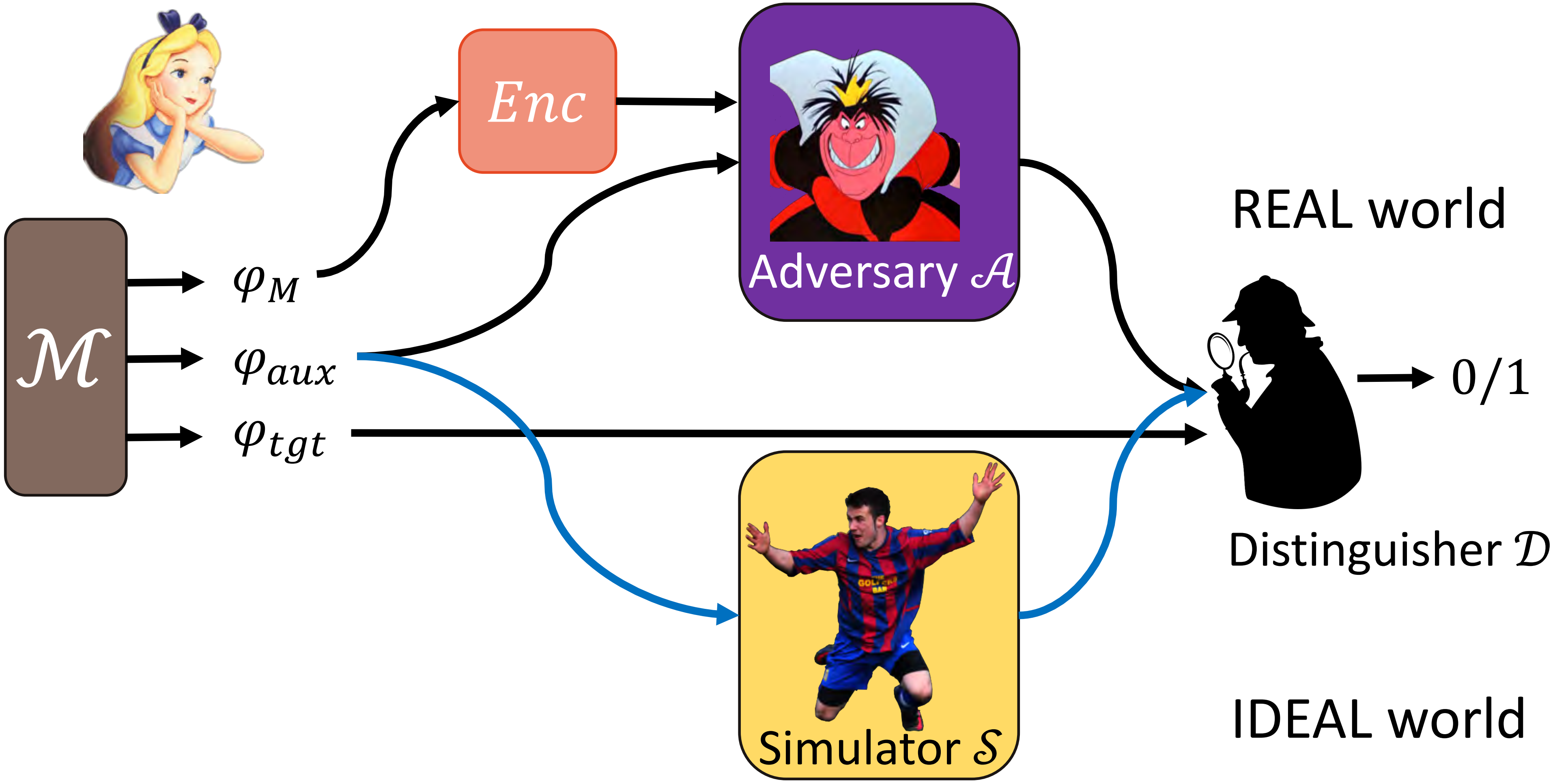
Theorem: SEM ⇔ IND

[Goldwasser Micali 84] leading to Turing-Award (Noble price for CS)

Our Contributions

1. Formal definition of Quantum Semantic Security
2. Equivalence to Quantum Indistinguishability
3. Extension to CPA and CCA1 scenarios
4. Construction of IND-CCA1 Quantum Secret-Key Encryption from One-Way Functions
5. Construction of Quantum Public-Key Encryption from One-Way Trapdoor Permutations

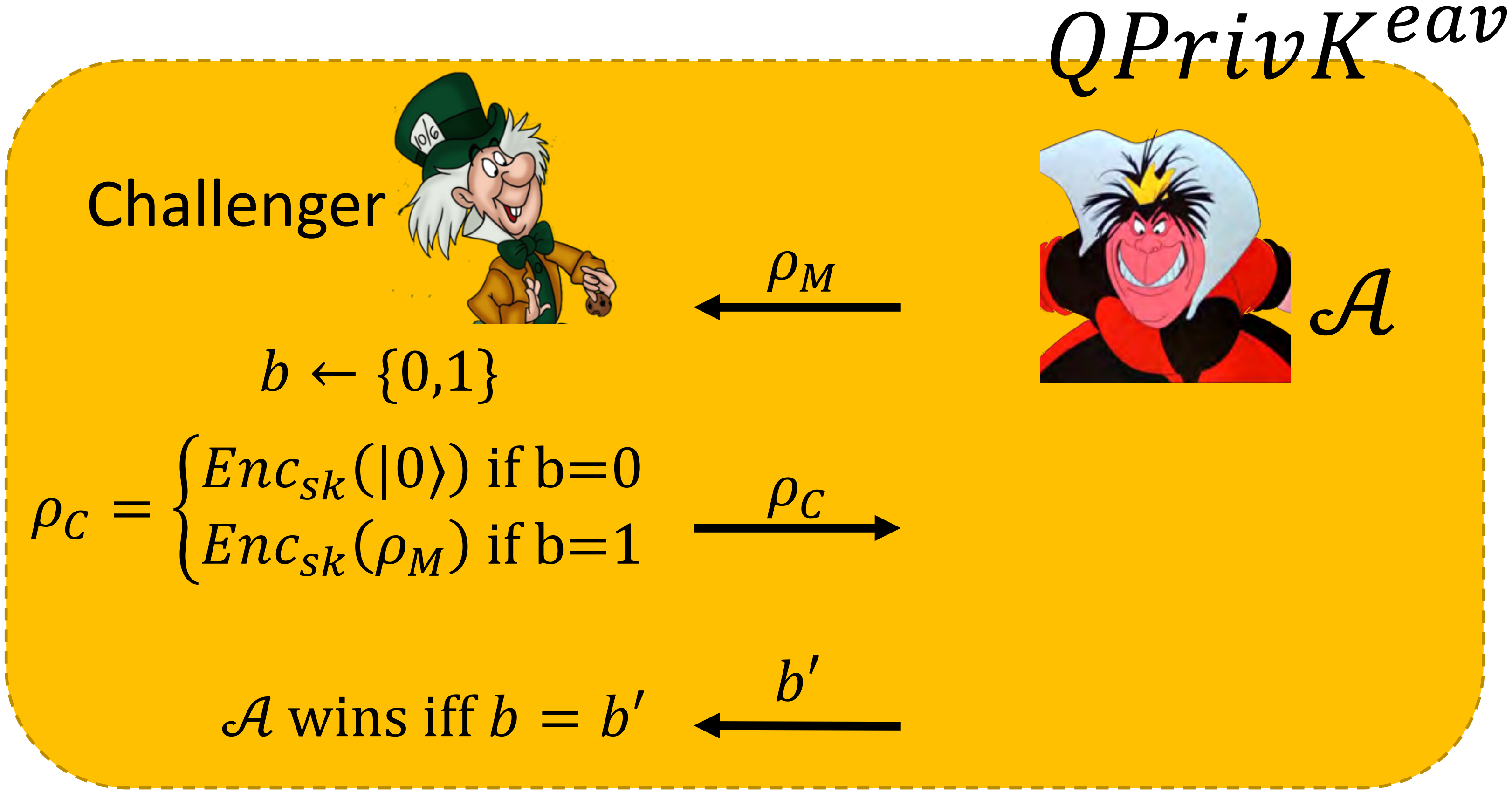
Quantum Semantic Security



Definition (QSEM): $\forall \mathcal{A}\ \exists \mathcal{S}\ \forall (\mathcal{M}, \mathcal{D})$:

$$\Pr[\mathcal{D}(\text{REAL}) = 1] \approx \Pr[\mathcal{D}(\text{IDEAL}) = 1]$$

Quantum Indistinguishability



$QPrivK^{eav}$

Challenger

$\mathcal{A}$

$\xleftarrow{\rho_M}$

$b \leftarrow \{0,1\}$

$$\rho_C = \begin{cases} Enc_{sk}(|0\rangle) \text{ if b=0} \\ Enc_{sk}(\rho_M) \text{ if b=1} \end{cases}$$

$\xrightarrow{\rho_C}$

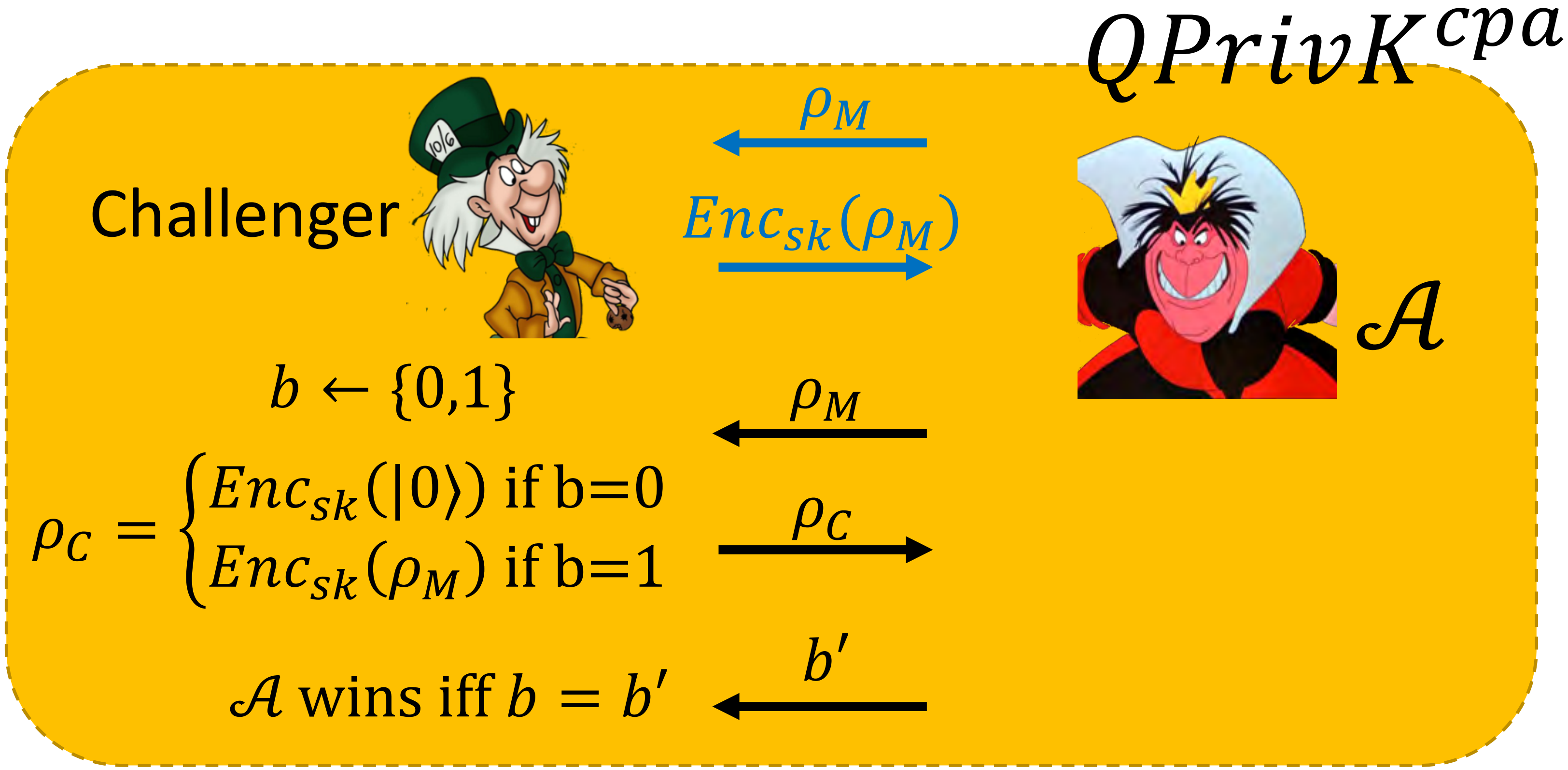
$\mathcal{A}$ wins iff $b = b'$ $\xleftarrow{b'}$

Definition (QIND): $\forall \mathcal{A}\colon\ \Pr[\mathcal{A} \text{ wins } QPrivK^{eav}] \leq \frac{1}{2} + negl(n)$

Theorem: QSEM ⇔ QIND

QIND: [Broadbent Jeffery 15, Gagliardoni Huelsing Schaffner 16]

Chosen-Plaintext Attacks (CPA)



$QPrivK^{cpa}$

Challenger

$\mathcal{A}$

ρ_M ←

$Enc_{sk}(\rho_M)$ →

$b \leftarrow \{0,1\}$

ρ_M ←

$$\rho_C = \begin{cases} Enc_{sk}(|0\rangle) \text{ if b=0} \\ Enc_{sk}(\rho_M) \text{ if b=1} \end{cases}$$

ρ_C →

b' ←

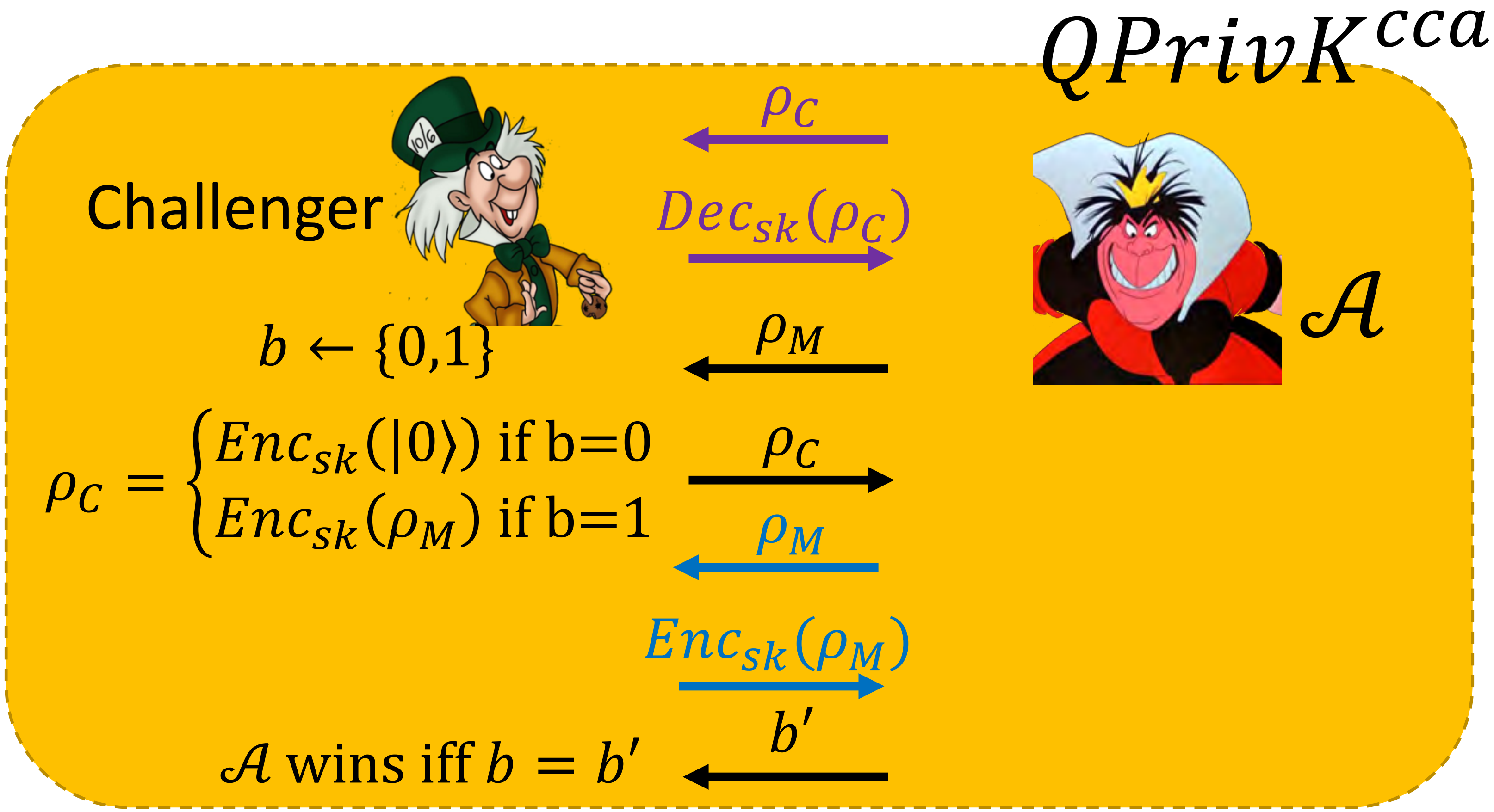
$\mathcal{A}$ wins iff $b = b'$

Definition (QIND-CPA): $\forall \mathcal{A}:\ \Pr[\mathcal{A} \text{ wins } QPrivK^{cpa}] \leq \frac{1}{2} + \ negl(n)$

Theorem: QSEM-CPA ⇔ QIND-CPA

Fact: CPA security requires **randomized encryption**

Chosen-Ciphertext Attacks (CCA1)



$QPrivK^{cca}$

Challenger

$\mathcal{A}$

$b \leftarrow \{0,1\}$

$$\rho_C = \begin{cases} Enc_{sk}(|0\rangle) \text{ if b=0} \\ Enc_{sk}(\rho_M) \text{ if b=1} \end{cases}$$

$\mathcal{A}$ wins iff $b = b'$

Definition (QIND-CCA1): $\forall \mathcal{A}\text{: } \Pr[\mathcal{A} \text{ wins } QPrivK^{cca}] \leq \frac{1}{2} + \ negl(n)$

Theorem: QSEM-CCA1 ⇔ QIND-CCA1

Fact: QSEM-CCA1 $\overset{\neq}{\Rightarrow}$ QIND-CPA $\overset{\neq}{\Rightarrow}$ QIND,

stronger adversaries yield stronger encryption schemes

Our Contributions

✓Formal definition of Quantum Semantic Security

✓Equivalence to Quantum Indistinguishability

✓Extension to CPA and CCA1 scenarios

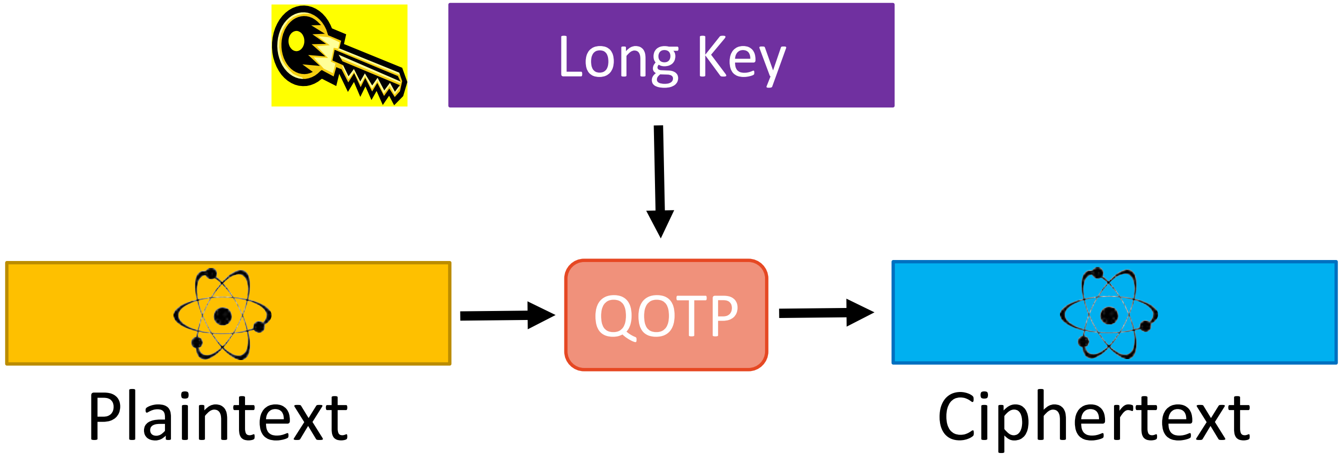
4. Construction of IND-CCA1 Quantum Secret-Key Encryption from One-Way Functions
5. Construction of Quantum Public-Key Encryption from One-Way Trapdoor Permutations

Quantum Secret-Key Encryption

Goal: build CCA1-secure quantum secret-key encryption

Ingredients:

quantum one-time pad (QOTP)



Not even CPA secure, scheme is not randomized!

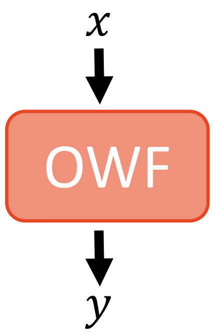
Quantum Secret-Key Encryption

Goal: build CCA1-secure quantum secret-key encryption

Ingredients:

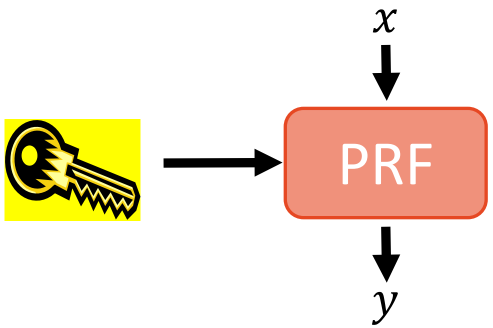
quantum one-time pad (QOTP)

quantum-secure one-way function (OWF)

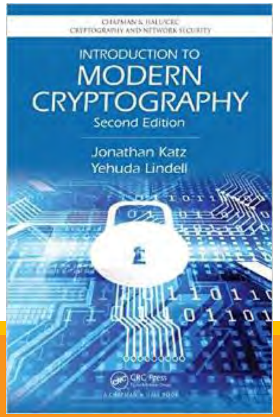


$f: x \mapsto y$ easy to compute, but hard to invert even for quantum adversaries, e.g. lattice-problems, …

Theorem: One-Way Function $\Longrightarrow$ Pseudo-Random Function



$\{f_k: x \mapsto y\}_k$ is indistinguishable from random function if key k is unknown



CHAPMAN & HALL/CRC
CRYPTOGRAPHY AND NETWORK SECURITY

INTRODUCTION TO
MODERN
CRYPTOGRAPHY
Second Edition

Jonathan Katz
Yehuda Lindell

[Hastad Impagliazzo Levin Luby 99]

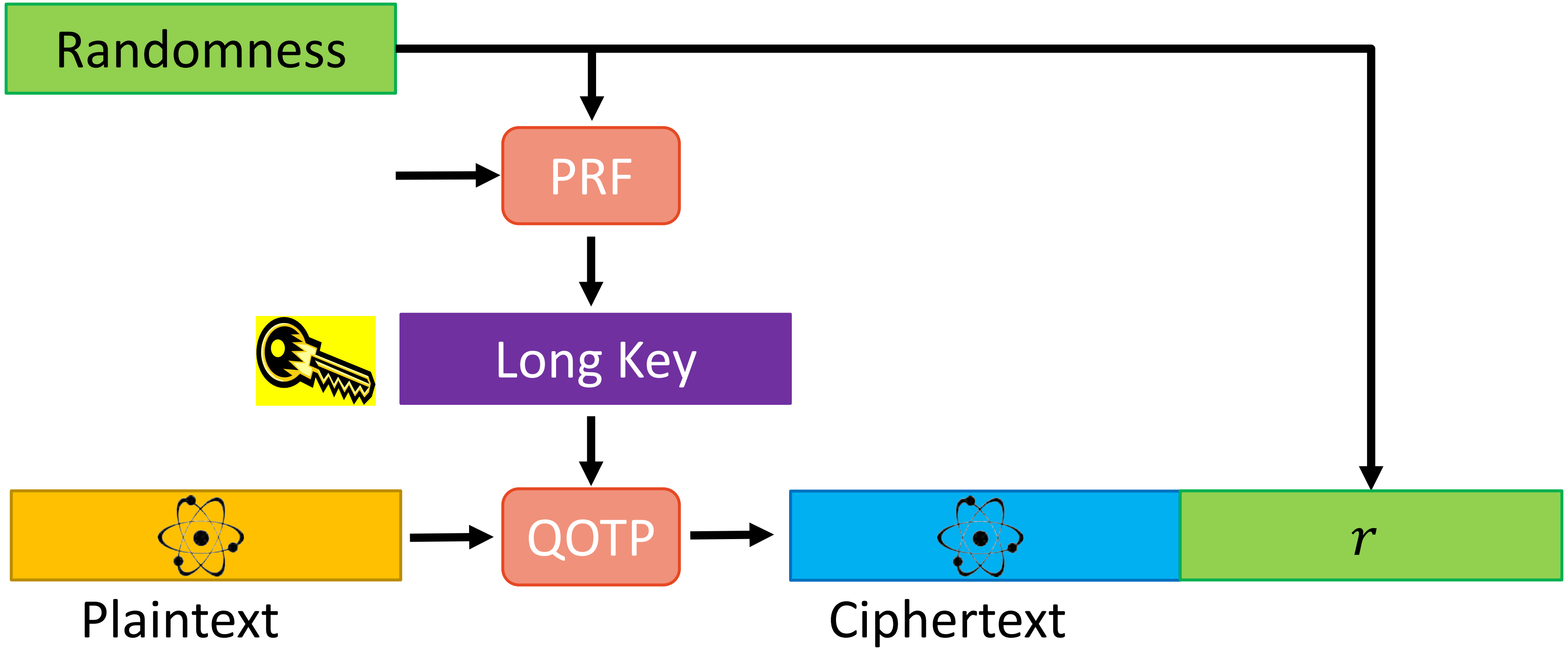
Quantum Secret-Key Encryption

Goal: build CCA1-secure quantum secret-key encryption

Ingredients:

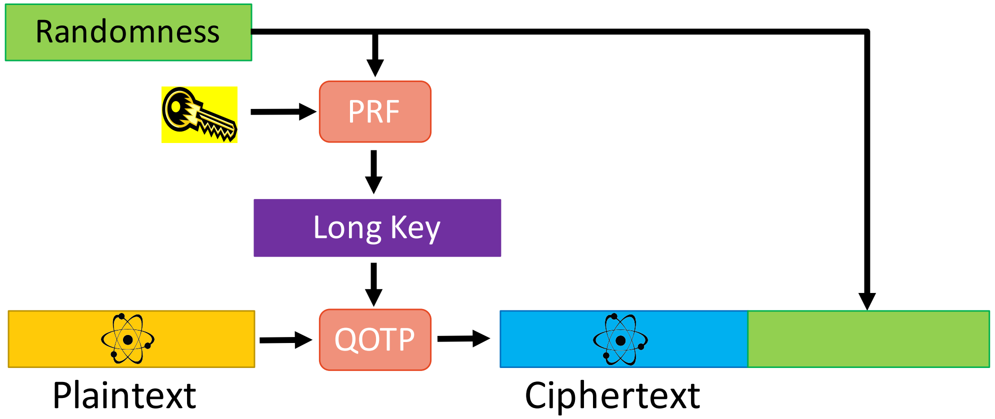
quantum one-time pad (QOTP)

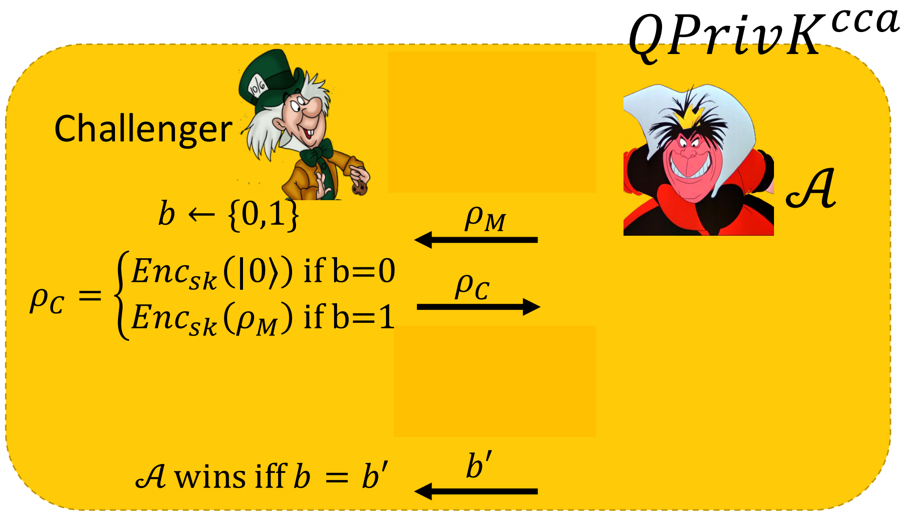
quantum-secure one-way function (OWF) ⟹ PRF



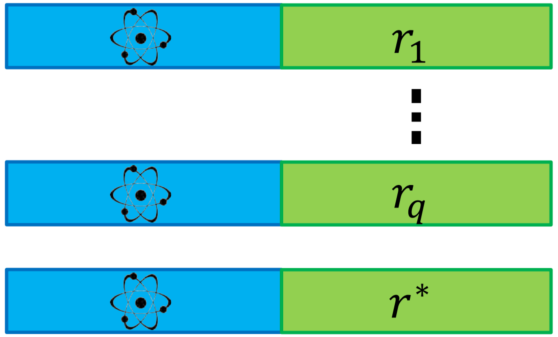
Classical version: [Goldreich Goldwasser Micali 85]

Intuition of CCA1 security




$QPrivK^{cca}$
Challenger
$\mathcal{A}$
$b \leftarrow \{0,1\}$
ρ_M
$\rho_C = \begin{cases} Enc_{sk}(|0\rangle) \text{ if b=0} \\ Enc_{sk}(\rho_M) \text{ if b=1} \end{cases}$
ρ_C
$\mathcal{A}$ wins iff $b = b'$
b'

1. Replace pseudo-random function with totally random function
2. Encryption queries result in polynomially many ciphertexts with different randomness:
3. With overwhelming probability the randomness of the challenge ciphertext will be different from previous r’s.



Our Contributions

✓Formal definition of Quantum Semantic Security

✓Equivalence to Quantum Indistinguishability

✓Extension to CPA and CCA1 scenarios

✓Construction of IND-CCA1 Quantum Secret-Key Encryption from One-Way Functions

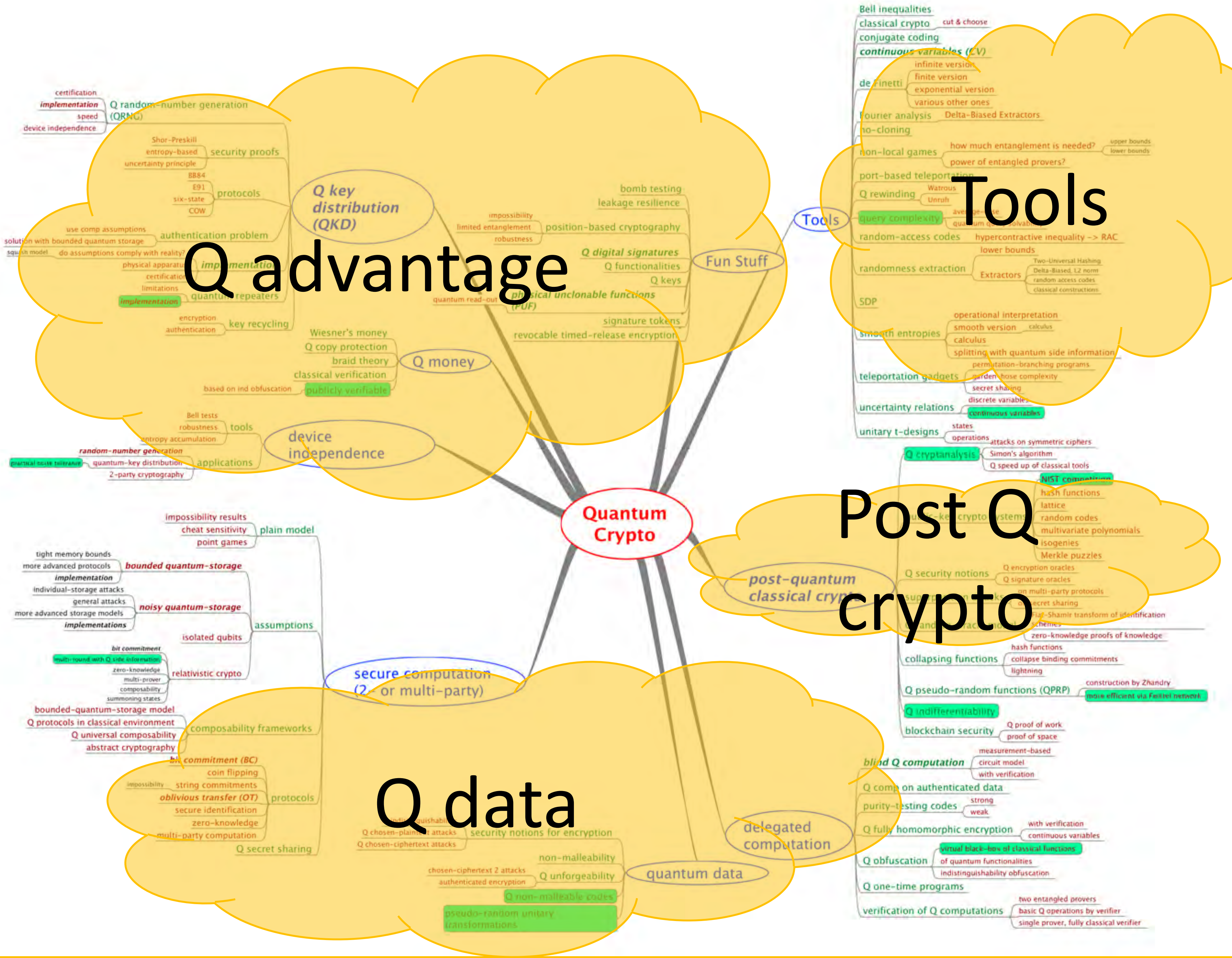
5. Construction of Quantum Public-Key Encryption from One-Way Trapdoor Permutations

MindMap

- ***experiments***
- Selection of open questions

- Fork me on github!

[https://github.com/cschaffner/QCryptoMindmap]

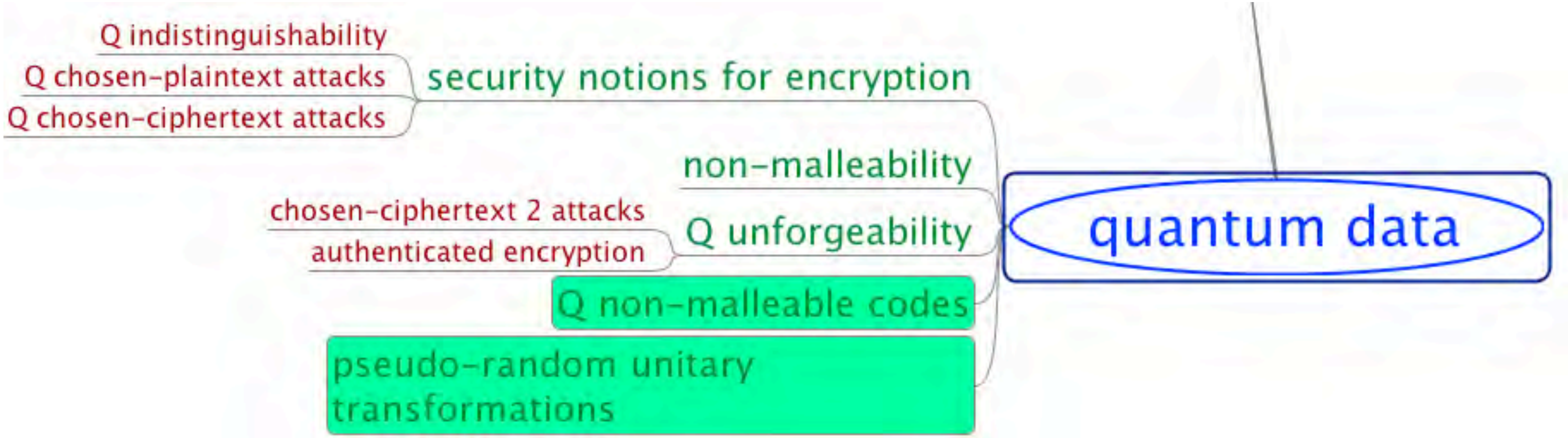


Q advantage

Tools

Post Q crypto

Q data



quantum data

security notions for encryption

Q indistinguishability

Q chosen-plaintext attacks

Q chosen-ciphertext attacks

non-malleability

Q unforgeability

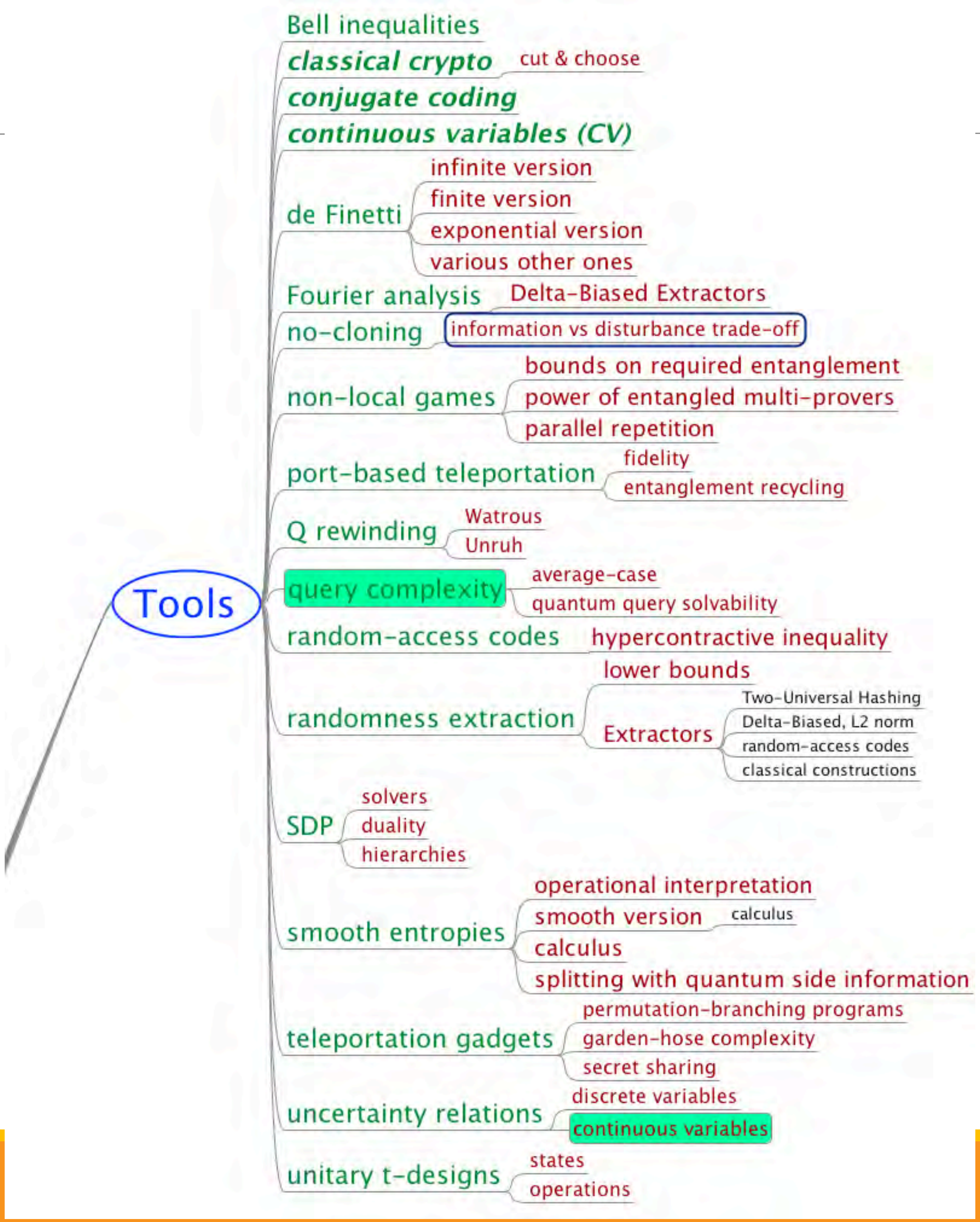
chosen-ciphertext 2 attacks

authenticated encryption

Q non-malleable codes

pseudo-random unitary transformations

Tools



- Tools
  - Bell inequalities
  - *classical crypto*
    - cut & choose
  - *conjugate coding*
  - *continuous variables (CV)*
  - de Finetti
    - infinite version
    - finite version
    - exponential version
    - various other ones
  - Fourier analysis
    - Delta-Biased Extractors
  - no-cloning
    - information vs disturbance trade-off
  - non-local games
    - bounds on required entanglement
    - power of entangled multi-provers
    - parallel repetition
  - port-based teleportation
    - fidelity
    - entanglement recycling
  - Q rewinding
    - Watrous
    - Unruh
  - query complexity
    - average-case
    - quantum query solvability
  - random-access codes
    - hypercontractive inequality
  - randomness extraction
    - lower bounds
    - Extractors
      - Two-Universal Hashing
      - Delta-Biased, L2 norm
      - random-access codes
      - classical constructions
  - SDP
    - solvers
    - duality
    - hierarchies
  - smooth entropies
    - operational interpretation
    - smooth version
      - calculus
    - calculus
    - splitting with quantum side information
  - teleportation gadgets
    - permutation-branching programs
    - garden-hose complexity
    - secret sharing
  - uncertainty relations
    - discrete variables
    - continuous variables
  - unitary t-designs
    - states
    - operations

Open Query-Complexity Question

- Let $f: \{0,1\}^n \rightarrow \{0,1\}^n$ be a random function
- **Goal:** Given quantum oracle access to f, output a ”chain of values” $x, f(x), f(f(x))$
- **Observation:** easy to do with 2 classical queries
- **Question:** Prove hardness with a single quantum query
- **More interesting:** Prove hardness with polynomially many non-adaptive quantum queries
- **Classical hardness:** straightforward
- **Partial result:** iterated hashing analyzed by Unruh in context of revocable quantum timed-released encryption

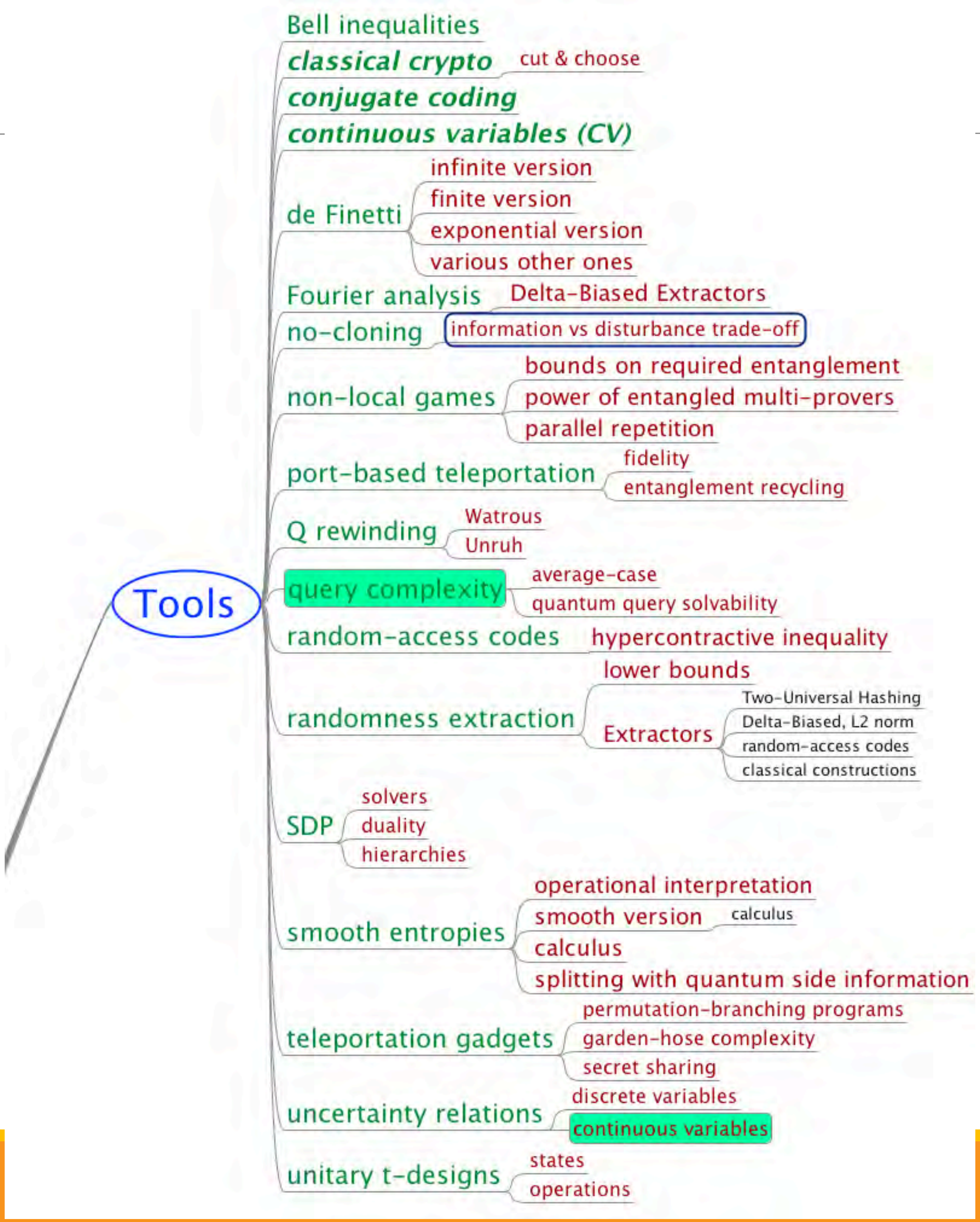
[question by Serge Fehr 17, Unruh 13]

Quantum Query Solvability

- Notion introduced by Mark Zhandry at QuICS workshop 2015: https://www.youtube.com/watch?v=kaS7OFAm-6M
- Often, quantum query-complexity bounds are given in the form: "$\Theta(g(N))$ queries are required to solve a problem with success probability 2/3 (in the worst case)"
- For crypto, it would be way more useful to have: "Given q quantum queries, the maximal success probability is $\Theta(g(q,N))$, in the average case"
- Example: Given a function $F: [N] \to \{0,1\}$, find x such that $F(x) = 1$.
- Q query-complexity answer: $\Theta\left(N^{1/2}\right)$ by (optimality of) Grover search
- But is the success probability $\Theta\left(q/N^{1/2}\right)$, $\boxed{\Theta(q^2/N)}$, or $\Theta(q^4/N^2)$?
- Matters for efficiency when choosing crypto parameters in order to get tiny security errors

[Zhandry 15]

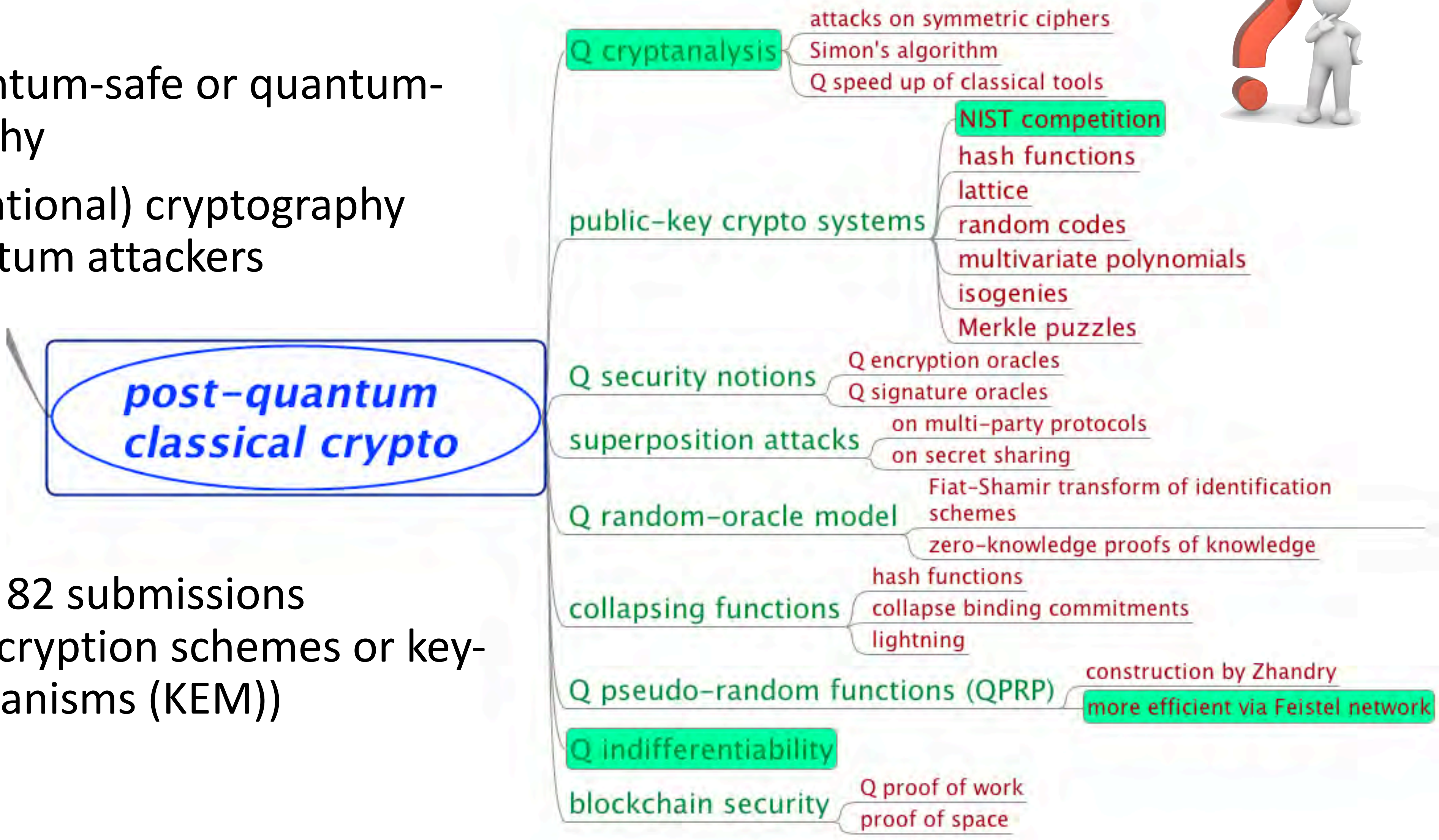
Tools



- Tools
  - Bell inequalities
  - ***classical crypto***
    - cut & choose
  - ***conjugate coding***
  - ***continuous variables (CV)***
  - de Finetti
    - infinite version
    - finite version
    - exponential version
    - various other ones
  - Fourier analysis
    - Delta-Biased Extractors
  - no-cloning
    - information vs disturbance trade-off
  - non-local games
    - bounds on required entanglement
    - power of entangled multi-provers
    - parallel repetition
  - port-based teleportation
    - fidelity
    - entanglement recycling
  - Q rewinding
    - Watrous
    - Unruh
  - query complexity
    - average-case
    - quantum query solvability
  - random-access codes
    - hypercontractive inequality
  - randomness extraction
    - lower bounds
    - Extractors
      - Two-Universal Hashing
      - Delta-Biased, L2 norm
      - random-access codes
      - classical constructions
  - SDP
    - solvers
    - duality
    - hierarchies
  - smooth entropies
    - operational interpretation
    - smooth version
      - calculus
    - calculus
    - splitting with quantum side information
  - teleportation gadgets
    - permutation-branching programs
    - garden-hose complexity
    - secret sharing
  - uncertainty relations
    - discrete variables
    - continuous variables
  - unitary t-designs
    - states
    - operations

Post-Quantum Cryptography

- Also known as: quantum-safe or quantum-resistant cryptography
- Classical (i.e. conventional) cryptography secure against quantum attackers
- NIST “competition”: 82 submissions (23 signature, 59 encryption schemes or key-encapsulation mechanisms (KEM))



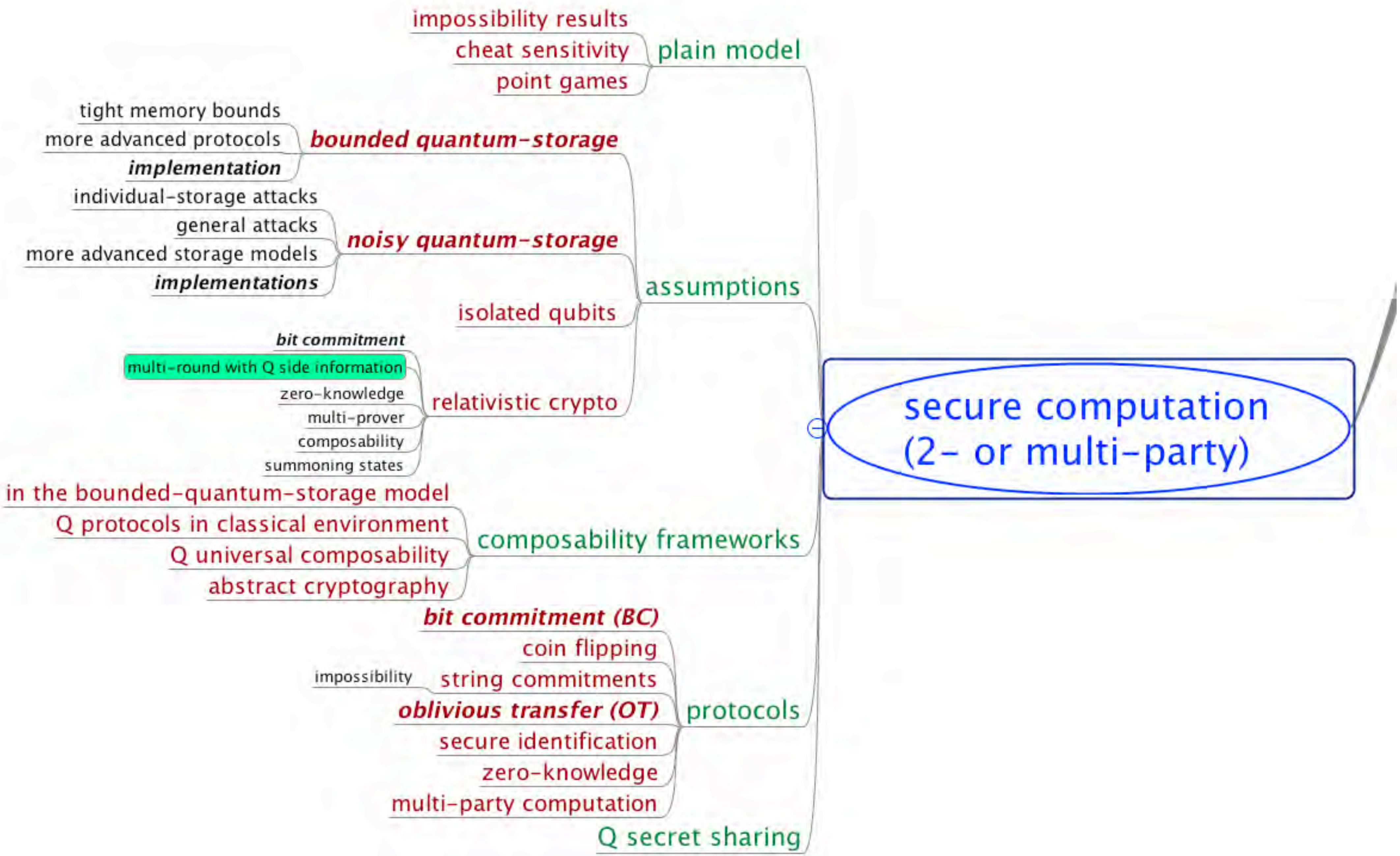
post-quantum classical crypto

- Q cryptanalysis
  - attacks on symmetric ciphers
  - Simon's algorithm
  - Q speed up of classical tools
- public-key crypto systems
  - NIST competition
  - hash functions
  - lattice
  - random codes
  - multivariate polynomials
  - isogenies
  - Merkle puzzles
- Q security notions
  - Q encryption oracles
  - Q signature oracles
- superposition attacks
  - on multi-party protocols
  - on secret sharing
- Q random-oracle model
  - Fiat-Shamir transform of identification schemes
  - zero-knowledge proofs of knowledge
- collapsing functions
  - hash functions
  - collapse binding commitments
  - lightning
- Q pseudo-random functions (QPRP)
  - construction by Zhandry
  - more efficient via Feistel network
- Q indifferentiability
- blockchain security
  - Q proof of work
  - proof of space

[https://csrc.nist.gov/Projects/Post-Quantum-Cryptography]

Observations from QCrypts 2014-17

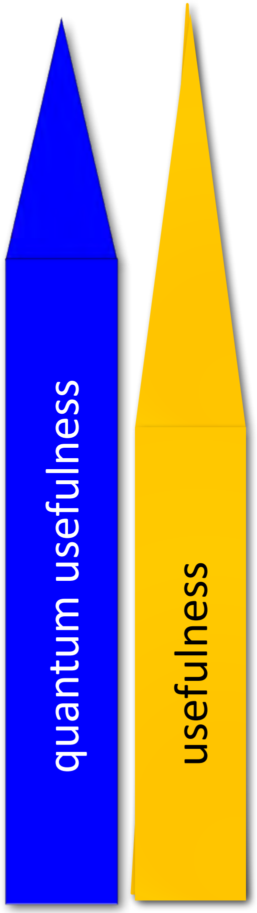
- Rough classification of contributed, invited and tutorial talks
- QKD is the most developed branch of Q crypto, closest to implementation
- When looking at experimental talks: mostly QKD and (closely) related topics
- Tools and post-quantum crypto are consistently of interest
- 2-party crypto was en vogue in 2014/15, not anymore in 2016/17
- Taken over by delegated computation and authentication, started in 2016
- 2016/17: DI has made a comeback
- Long tail: lots of other topics



- secure computation (2- or multi-party)
  - plain model
    - impossibility results
    - cheat sensitivity
    - point games
  - assumptions
    - ***bounded quantum-storage***
      - tight memory bounds
      - more advanced protocols
      - ***implementation***
    - ***noisy quantum-storage***
      - individual-storage attacks
      - general attacks
      - more advanced storage models
      - ***implementations***
    - isolated qubits
    - relativistic crypto
      - ***bit commitment***
      - multi-round with Q side information
      - zero-knowledge
      - multi-prover
      - composability
      - summoning states
  - composability frameworks
    - in the bounded-quantum-storage model
    - Q protocols in classical environment
    - Q universal composability
    - abstract cryptography
  - protocols
    - ***bit commitment (BC)***
    - coin flipping
    - string commitments
      - impossibility
    - ***oblivious transfer (OT)***
    - secure identification
    - zero-knowledge
    - multi-party computation
  - Q secret sharing

Secure Two-Party Cryptography

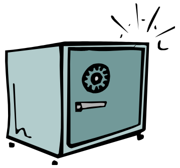
- Information-theoretic security
- No computational restrictions

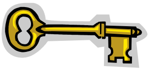


- Coin-Flipping

$\Uparrow \quad \not\Downarrow$

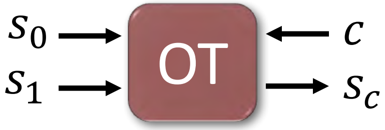
- Bit Commitment





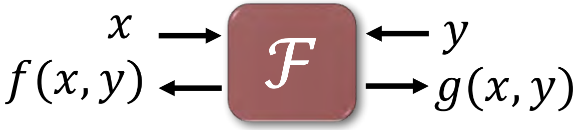
$\Uparrow \quad \not\Downarrow \quad \Downarrow$

- Oblivious Transfer



$\Uparrow \quad \Downarrow$

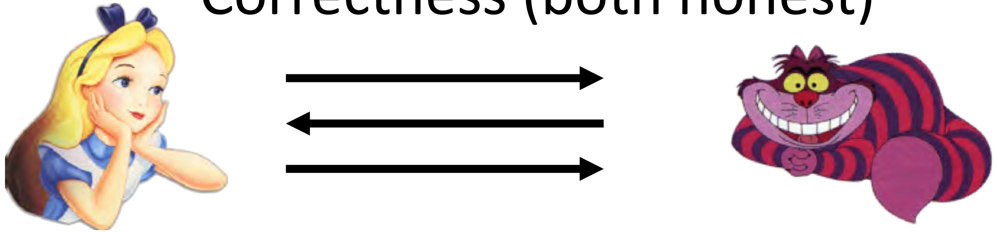
- 2-Party Function Evaluation



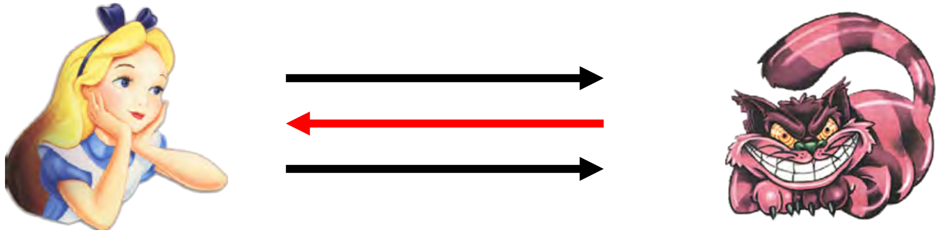
$\Updownarrow$

- Multi-Party Computation (with dishonest majority)

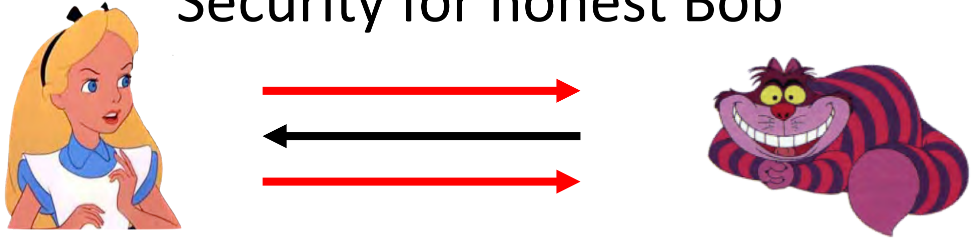
Correctness (both honest)



Security for honest Alice



Security for honest Bob



[Blum 83, Kilian 88]

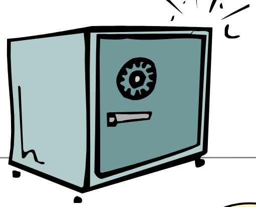
Coin Flipping (CF)

- Strong CF: No dishonest player can bias the outcome
- Classically: a cheater can always obtain his desired outcome with prob 1
- Quantum: [Kitaev 03] lower bounds the bias by $\frac{1}{\sqrt{2}} - \frac{1}{2} \approx 0.2$

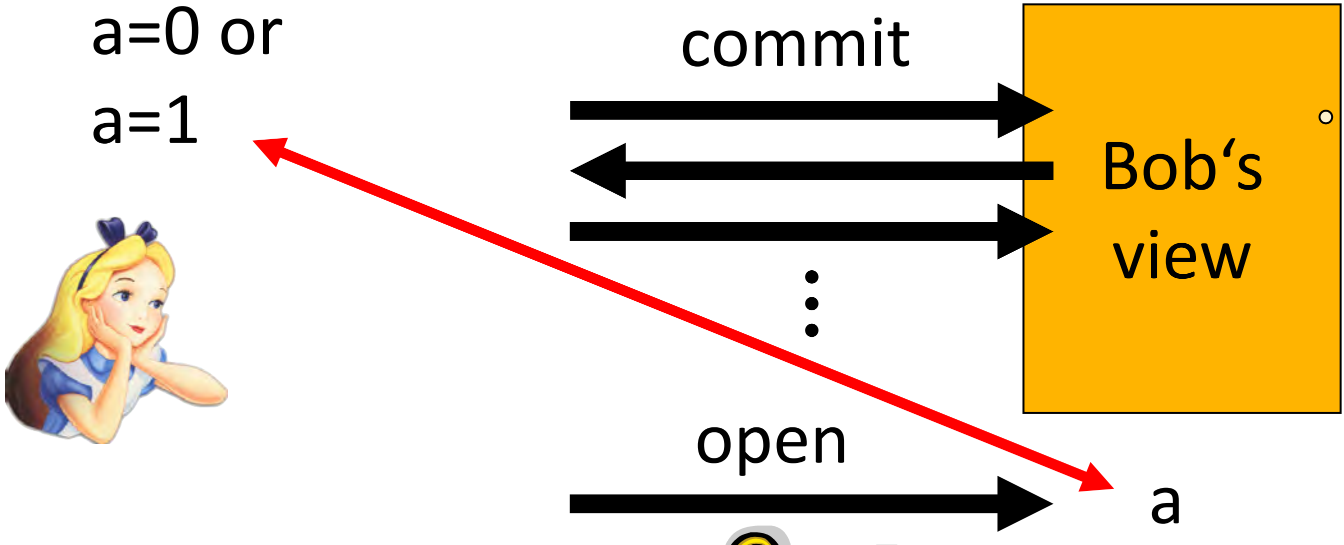
  [Chailloux Kerenidis 09] give optimal quantum protocol for strong CF with this bias

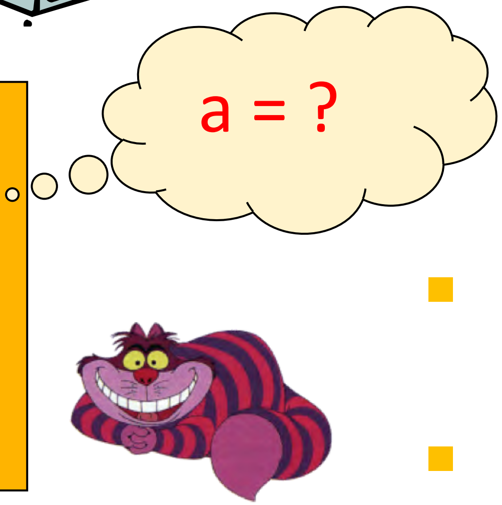
- Weak CF (“who has to do the dishes?”): Alice wants heads, Bob wants tails
- [Mochon 07] uses Kitaev’s formalism of point games to give a quantum protocol for weak CF with arbitrarily small bias $\varepsilon > 0$
- [Aharonov Chailloux Ganz Kerenidis Magnin 14] reduce the proof complexity from 80 to 50 pages… explicit protocol?

Bit Commitment (BC)

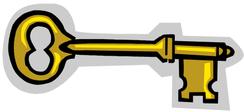


- Two-phase (reactive) protocol:





- Hiding: even dishonest Bob does not learn a
- Binding: dishonest Alice cannot change her mind



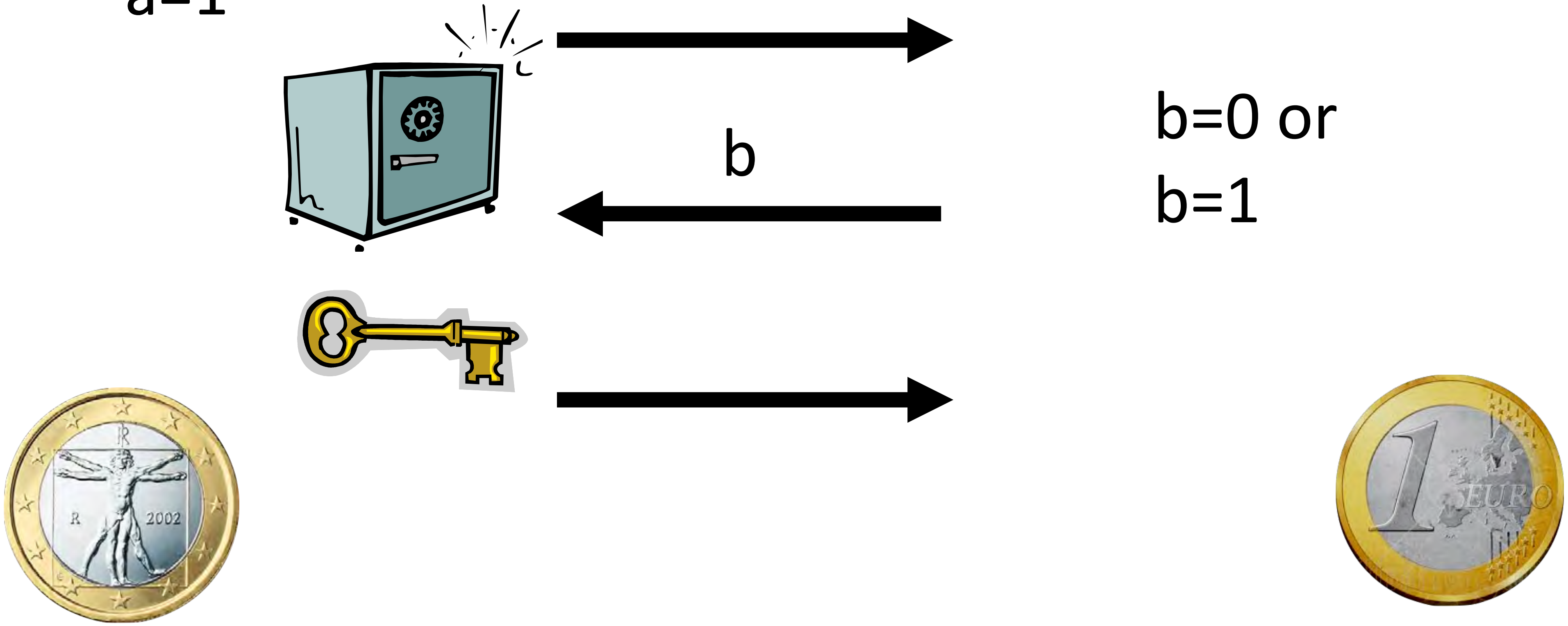
- Classically: impossible
- Quantum: believed to be possible in the early 90s
- shown impossible by [Mayers 97, LoChau 97] by a beautiful argument (purification and Uhlmann’s theorem)
- [Chailloux Kerenidis 11] show that in any quantum BC protocol, one player can cheat with prob 0.739. They also give an optimal protocol achieving this bound. Crypto application?

[Brassard Crepeau Jozsa Langlois: A quantum BC scheme provably unbreakable by both parties, FOCS 93]

Bit Commitment ⇒ Strong Coin Flipping

a=0 or
a=1

a



b

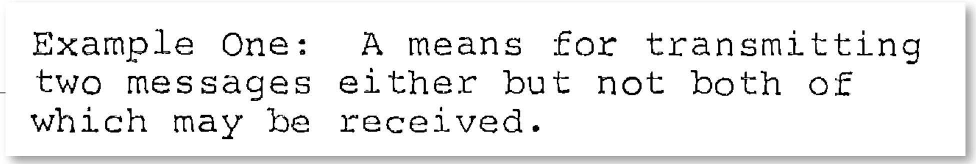
b=0 or
b=1

a = b

a ≠ b

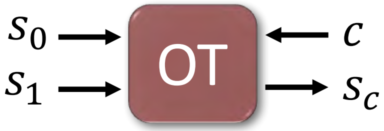
[Blum 83]

Oblivious Transfer (OT)



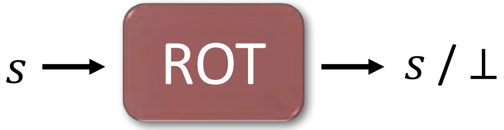
```
Example One:  A means for transmitting
two messages either but not both of
which may be received.
```

- 1-out-of-2 Oblivious Transfer:

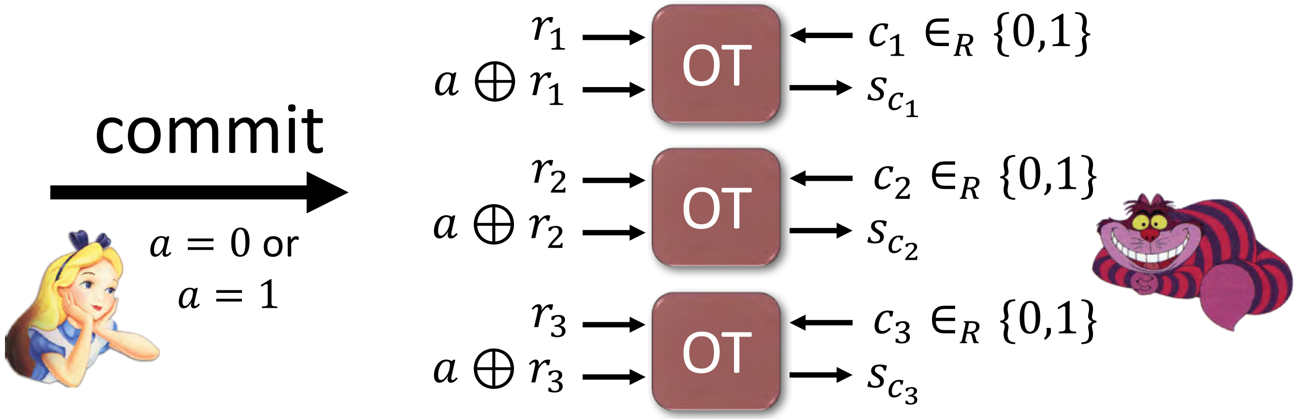


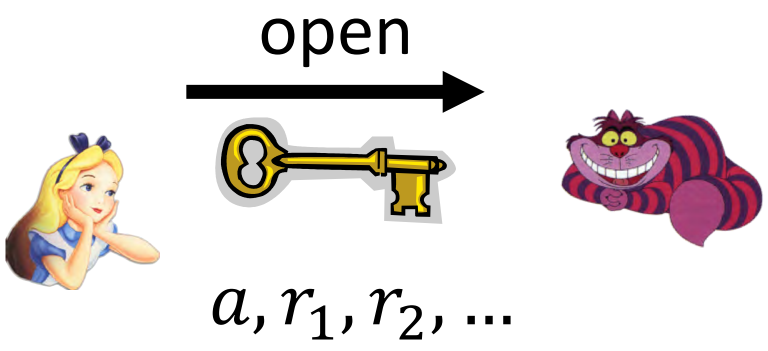
- Dishonest Alice does not learn choice bit
- Dishonest Bob can only learn one of the two messages

- Rabin OT: (secure erasure)



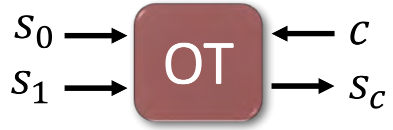
- These OT variants are information-theoretically equivalent (homework! 😉)
- OT is symmetric [Wolf Wullschleger at EuroCrypt 2006, only 10 pages long]
- 1-2 OT ⇒ BC:

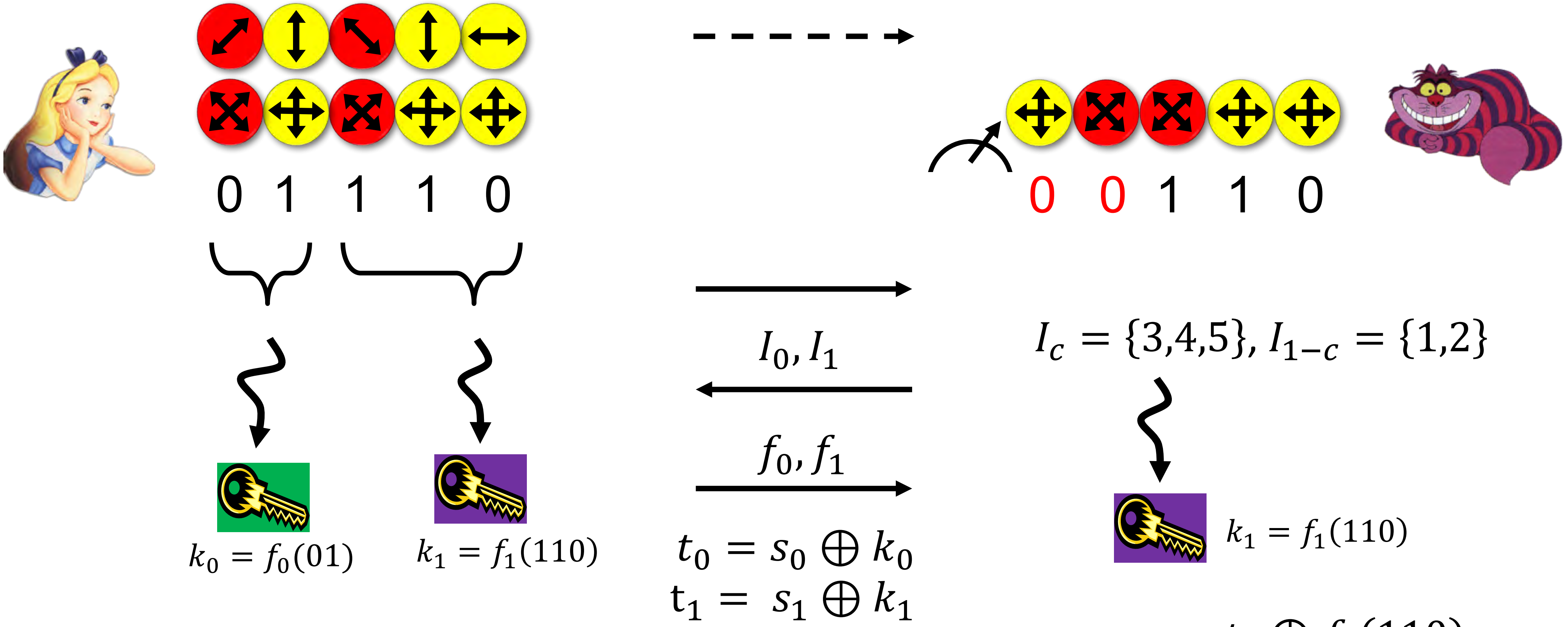




[Wiesner 68, Even Goldreich Lempel 85, Rabin 81]

Quantum Protocol for Oblivious Transfer





0 1 1 1 0

0 0 1 1 0

I_0, I_1

$I_c = \{3,4,5\}, I_{1-c} = \{1,2\}$

f_0, f_1

$k_0 = f_0(01)$ $k_1 = f_1(110)$

$t_0 = s_0 \oplus k_0$

$t_1 = s_1 \oplus k_1$

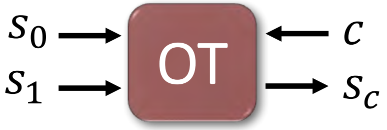
$k_1 = f_1(110)$

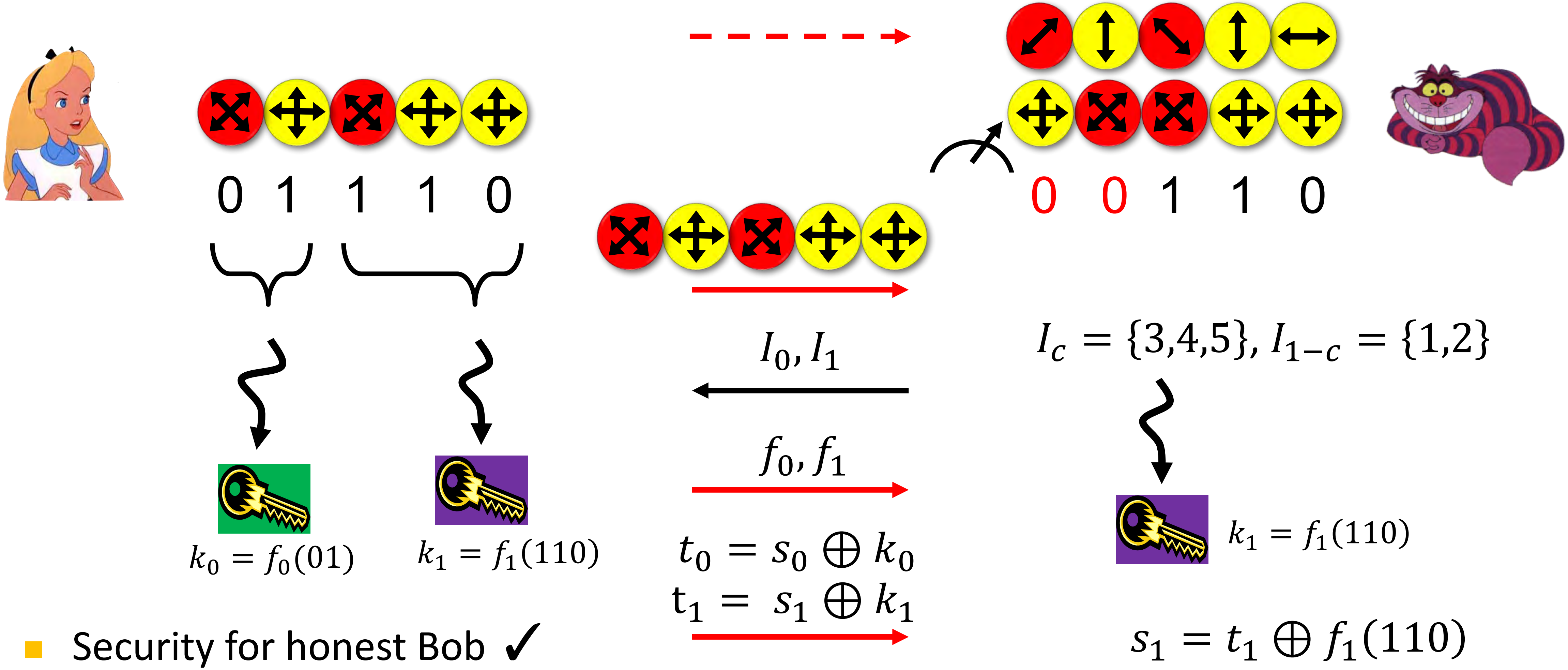
$s_1 = t_1 \oplus f_1(110)$

Correctness ✓

[Wiesner 61, Bennett Brassard Crepeau Skubiszewska 91]

Quantum Protocol for Oblivious Transfer





$k_0 = f_0(01)$

$k_1 = f_1(110)$

I_0, I_1

f_0, f_1

$t_0 = s_0 \oplus k_0$
$t_1 = s_1 \oplus k_1$

$I_c = \{3,4,5\}, I_{1-c} = \{1,2\}$

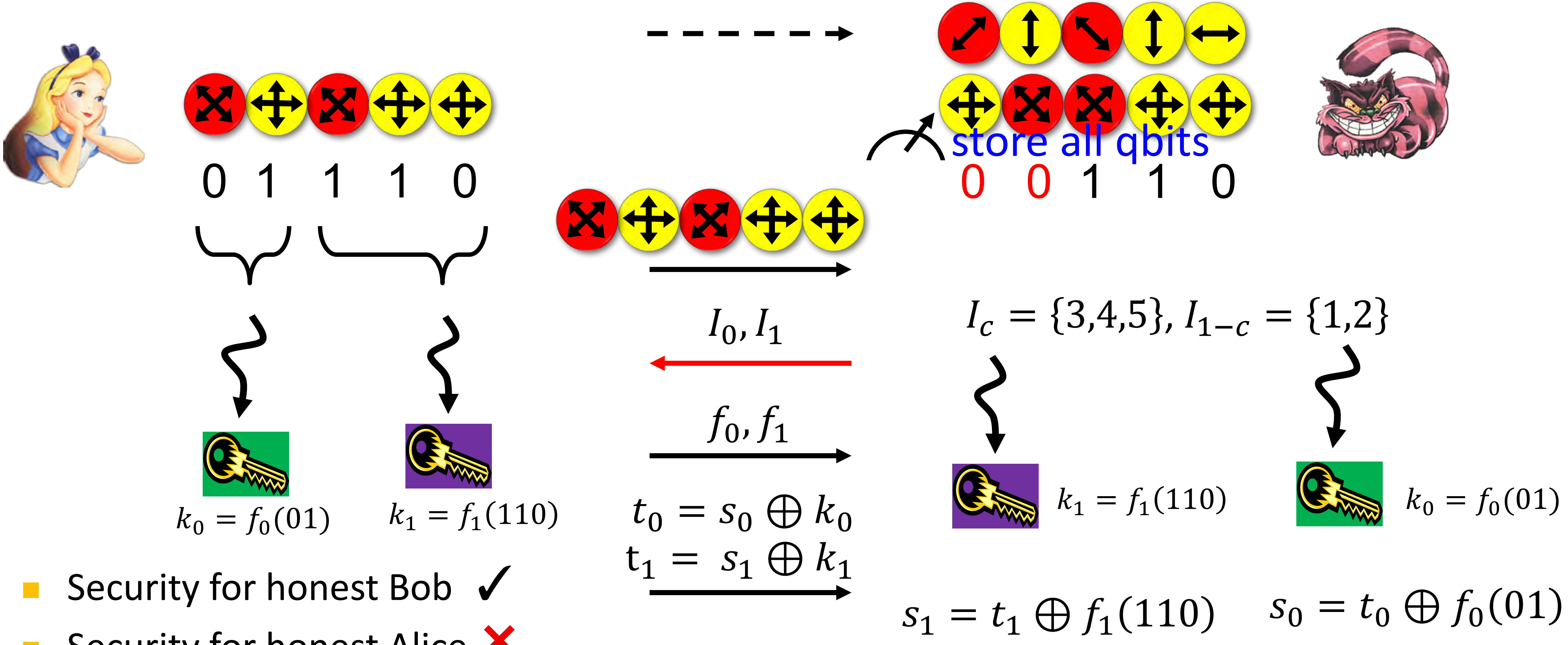
$k_1 = f_1(110)$

$s_1 = t_1 \oplus f_1(110)$

- Security for honest Bob ✓

[Wiesner 61, Bennett Brassard Crepeau Skubiszewska 91]

Quantum Protocol for Oblivious Transfer



I_0, I_1

f_0, f_1

$I_c = \{3,4,5\}, I_{1-c} = \{1,2\}$

$k_0 = f_0(01)$ $k_1 = f_1(110)$

$t_0 = s_0 \oplus k_0$
$\text{t}_1 = s_1 \oplus k_1$

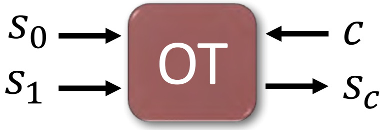
$k_1 = f_1(110)$ $k_0 = f_0(01)$

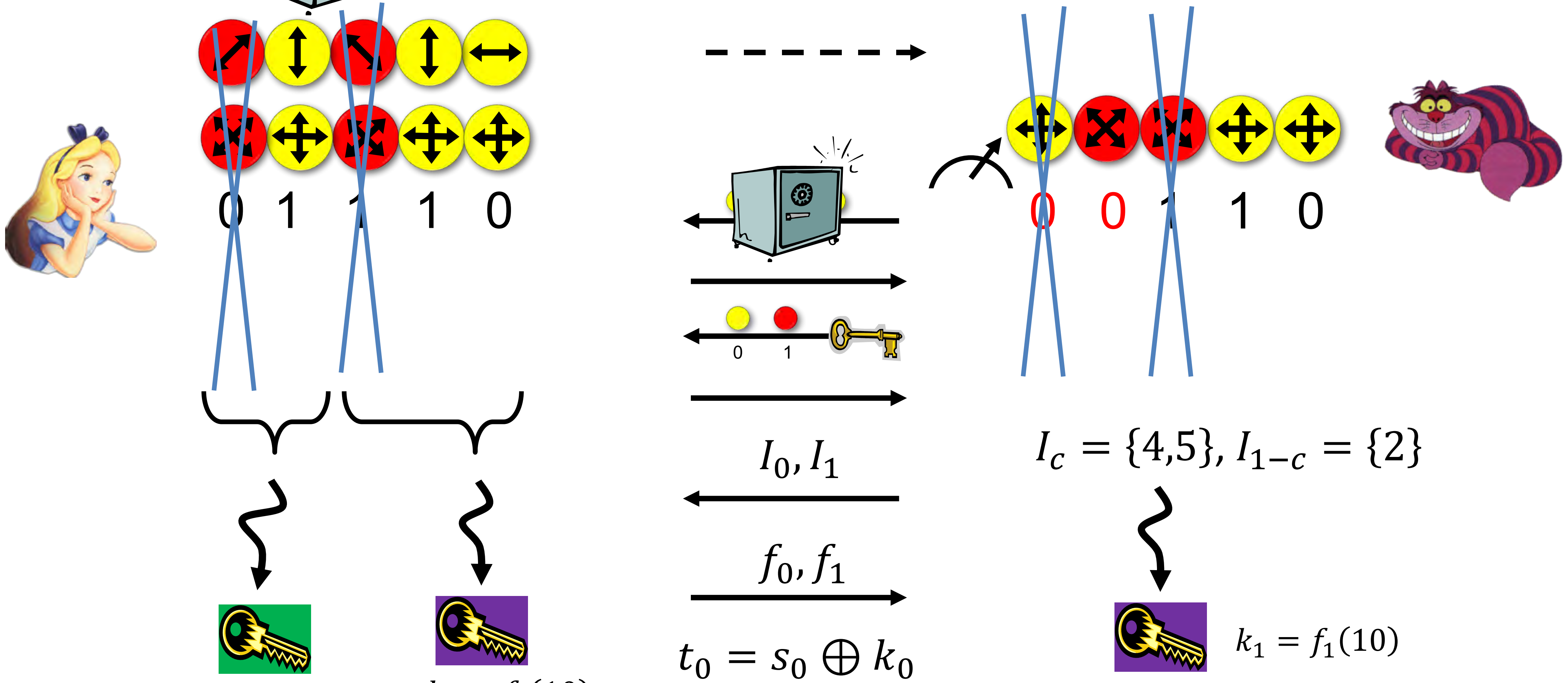
$s_1 = t_1 \oplus f_1(110)$ $s_0 = t_0 \oplus f_0(01)$

- Security for honest Bob ✓
- Security for honest Alice ✗

[Wiesner 61, Bennett Brassard Crepeau Skubiszewska 91]

BC ⇒ Oblivious Transfer





I_0, I_1

f_0, f_1

$I_c = \{4,5\}, I_{1-c} = \{2\}$

$k_0 = f_0(1)$

$k_1 = f_1(10)$

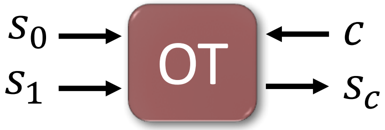
$t_0 = s_0 \oplus k_0$
$t_1 = s_1 \oplus k_1$

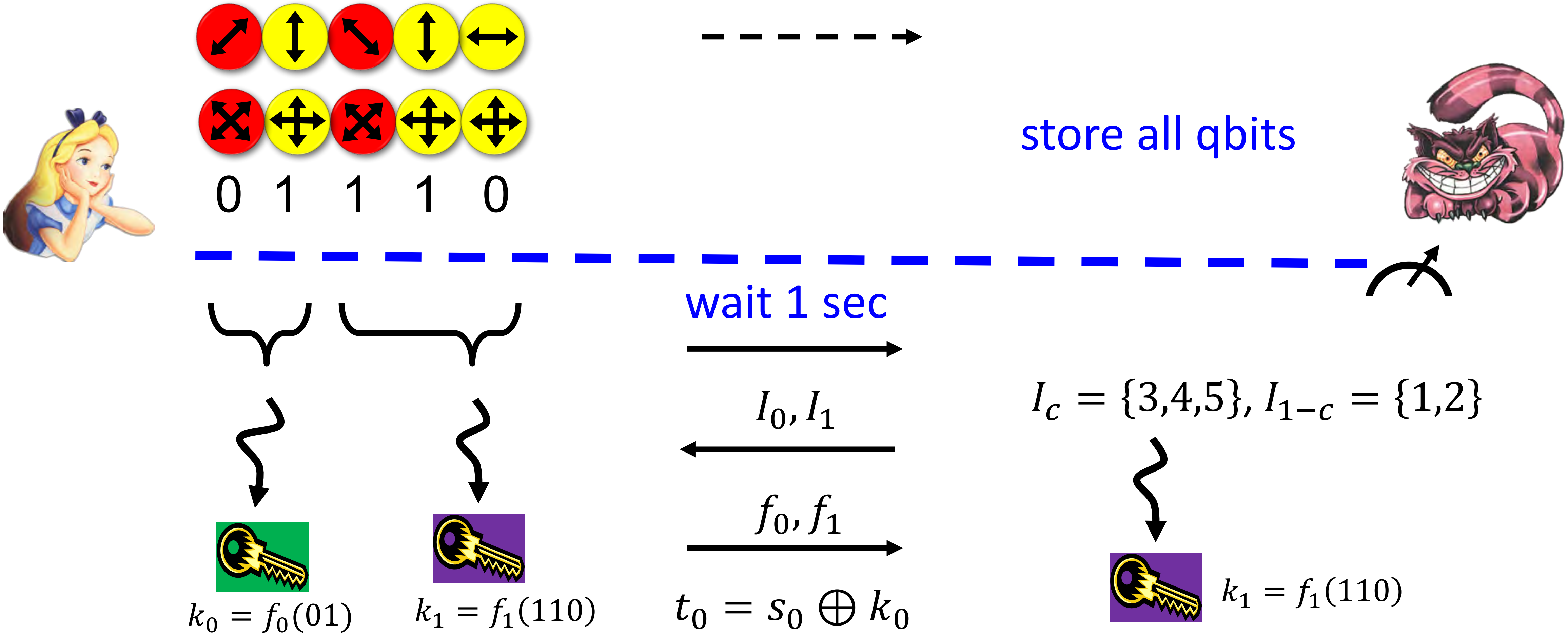
$k_1 = f_1(10)$

$s_1 = t_1 \oplus f_1(10)$

[Bennett Brassard Crepeau Skubiszewska 91, Damgaard Fehr Lunemann Salvail Schaffner 09, Unruh 10]

Limited Quantum Storage





store all qbits

wait 1 sec

I_0, I_1

f_0, f_1

$I_c = \{3,4,5\}, I_{1-c} = \{1,2\}$

$k_0 = f_0(01)$

$k_1 = f_1(110)$

$k_1 = f_1(110)$

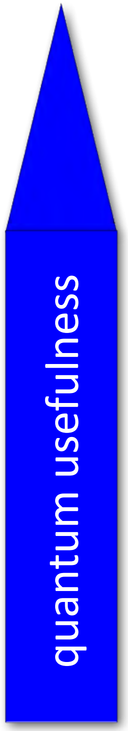
$t_0 = s_0 \oplus k_0$
$t_1 = s_1 \oplus k_1$

$s_1 = t_1 \oplus f_1(110)$

[Damgaard Fehr Salvail Schaffner 05, Wehner Schaffner Terhal 09]

Summary of Quantum Two-Party Crypto

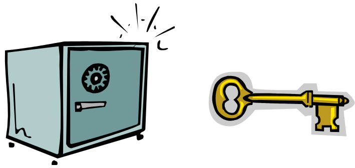
- Information-theoretic security
- No computational restrictions



- Coin-Flipping

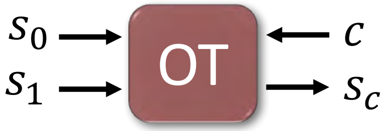
$\Uparrow$ $\not\Downarrow$

- Bit Commitment



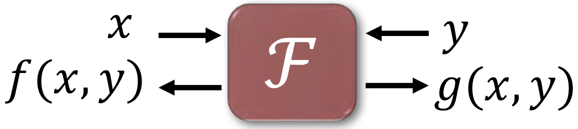
$\Uparrow$ $\not\Downarrow$ $\Downarrow$

- Oblivious Transfer

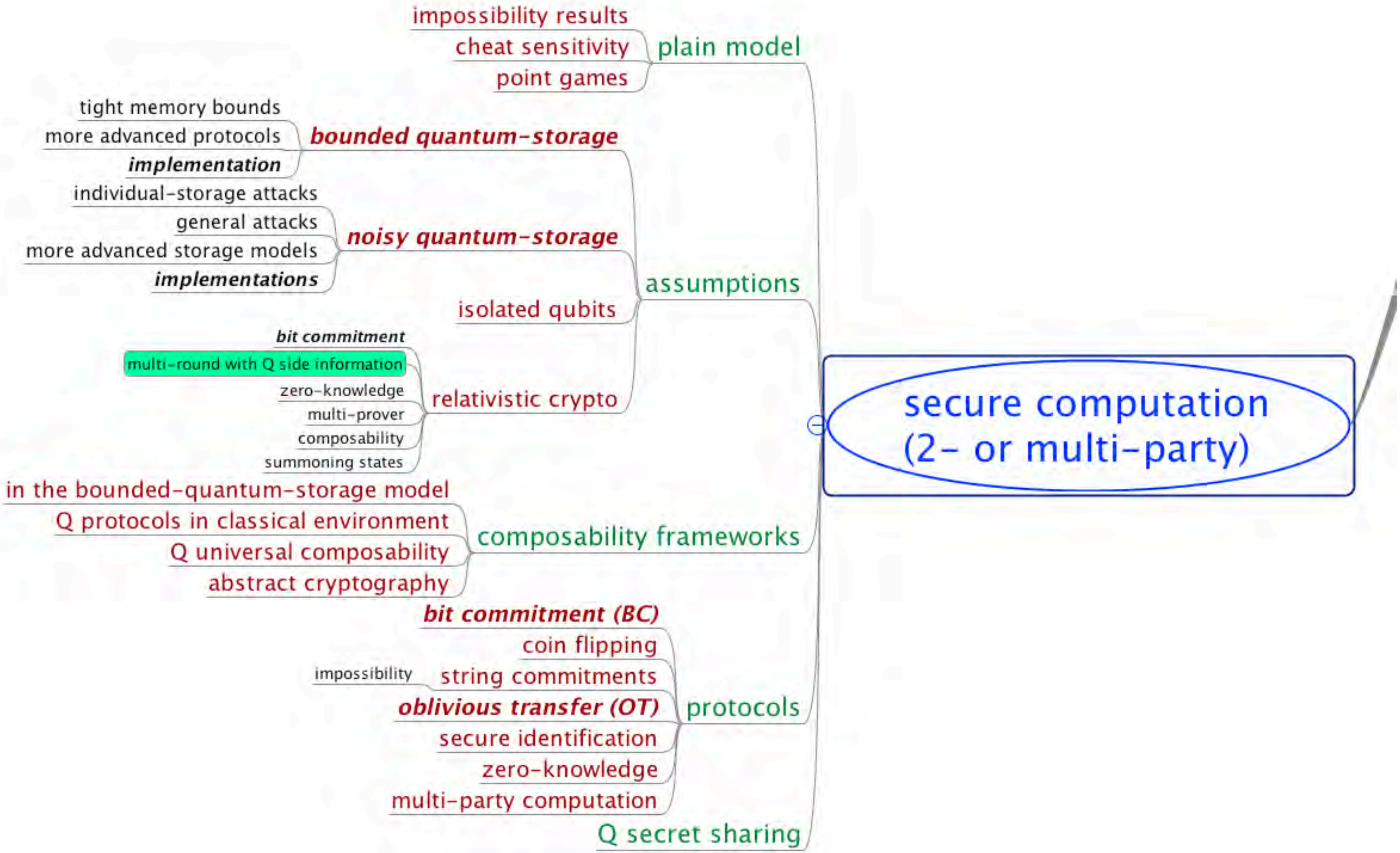


$\Uparrow$ $\Downarrow$

- 2-Party Function Evaluation



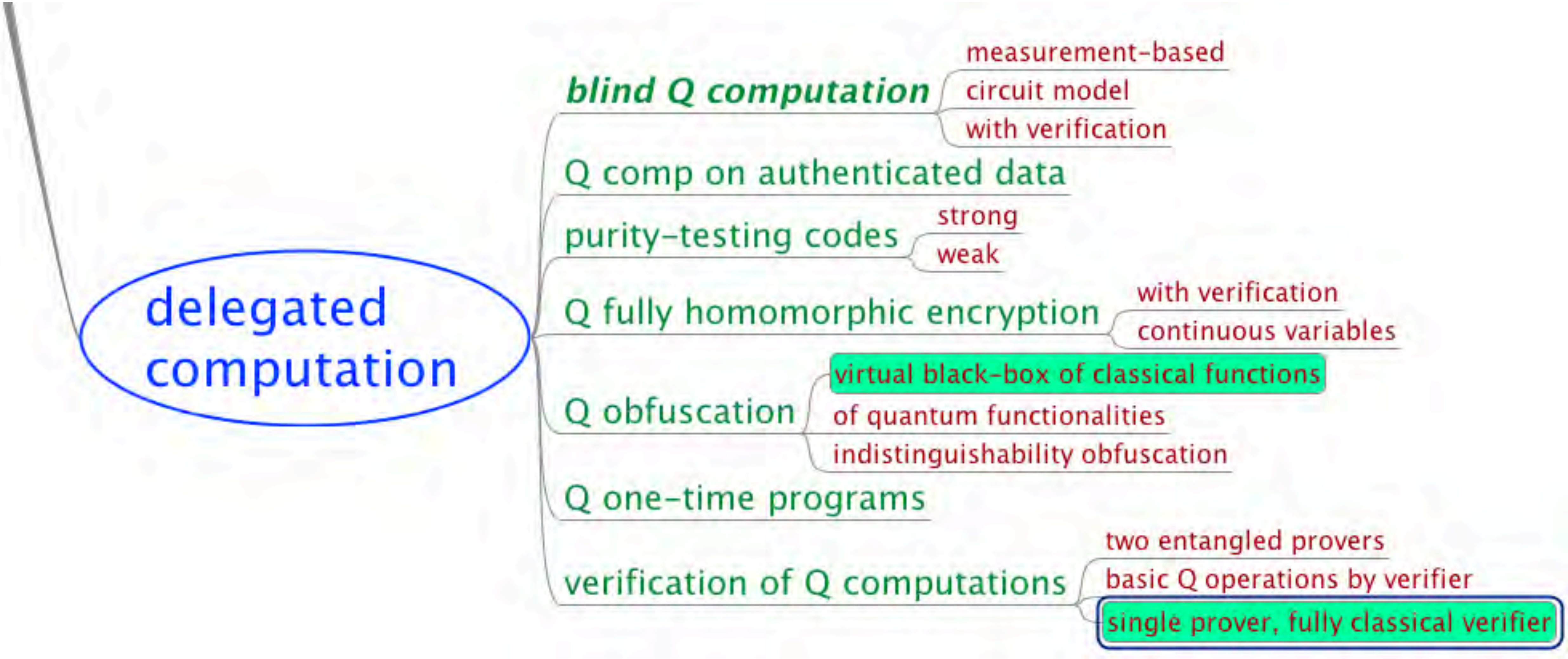
[Blum 83, Kilian 88]



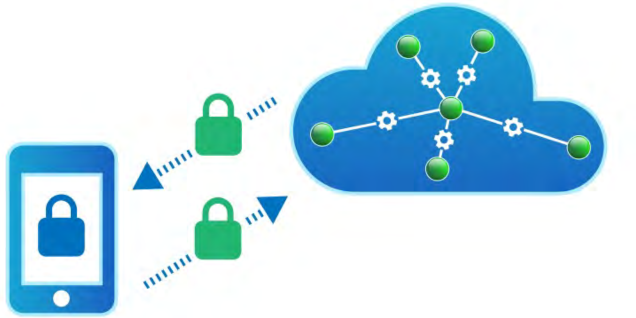
secure computation (2- or multi-party)

- plain model
  - impossibility results
  - cheat sensitivity
  - point games
- assumptions
  - ***bounded quantum-storage***
    - tight memory bounds
    - more advanced protocols
    - ***implementation***
  - ***noisy quantum-storage***
    - individual-storage attacks
    - general attacks
    - more advanced storage models
    - ***implementations***
  - isolated qubits
  - relativistic crypto
    - ***bit commitment***
    - multi-round with Q side information
    - zero-knowledge
    - multi-prover
    - composability
    - summoning states
- composability frameworks
  - in the bounded-quantum-storage model
  - Q protocols in classical environment
  - Q universal composability
  - abstract cryptography
- protocols
  - ***bit commitment (BC)***
  - coin flipping
  - string commitments
    - impossibility
  - ***oblivious transfer (OT)***
  - secure identification
  - zero-knowledge
  - multi-party computation
- Q secret sharing

Delegated Q Computation


delegated computation
blind Q computation
measurement-based
circuit model
with verification
Q comp on authenticated data
purity-testing codes
strong
weak
Q fully homomorphic encryption
with verification
continuous variables
Q obfuscation
virtual black-box of classical functions
of quantum functionalities
indistinguishability obfuscation
Q one-time programs
verification of Q computations
two entangled provers
basic Q operations by verifier
single prover, fully classical verifier

Delegated Computation

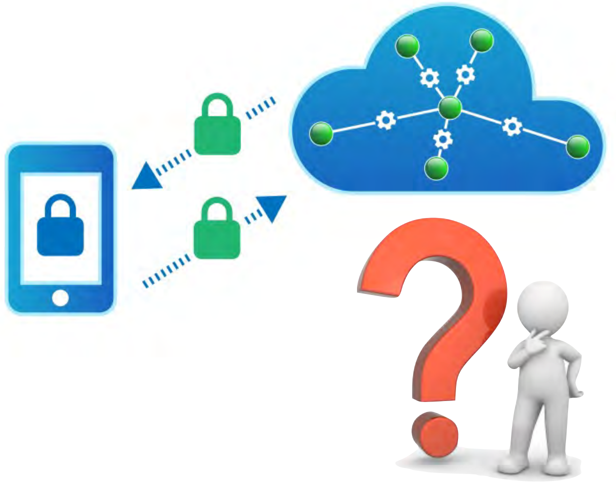


- QCloud Inc. promises to perform a BQP computation for you.
- How can you securely delegate your quantum computation to an untrusted quantum prover while maintaining privacy and/or integrity?
- Various parameters:
  1. Quantum capabilities of verifier: state preparation, measurements, q operations
  2. Type of security: blindness (server does not learn input), integrity (client is sure the correct computation has been carried out)
  3. Amount of interaction: single round (fully homomorphic encryption) or multiple rounds
  4. Number of servers: single-server, unbounded / computationally bounded or multiple entangled but non-communicating servers

[Childs 05, …. see e.g. Broadbent 17 or Fitzsimons 16 for overviews and references]

Image: Tremani / TU Delft

Classical Verification of Q Computation

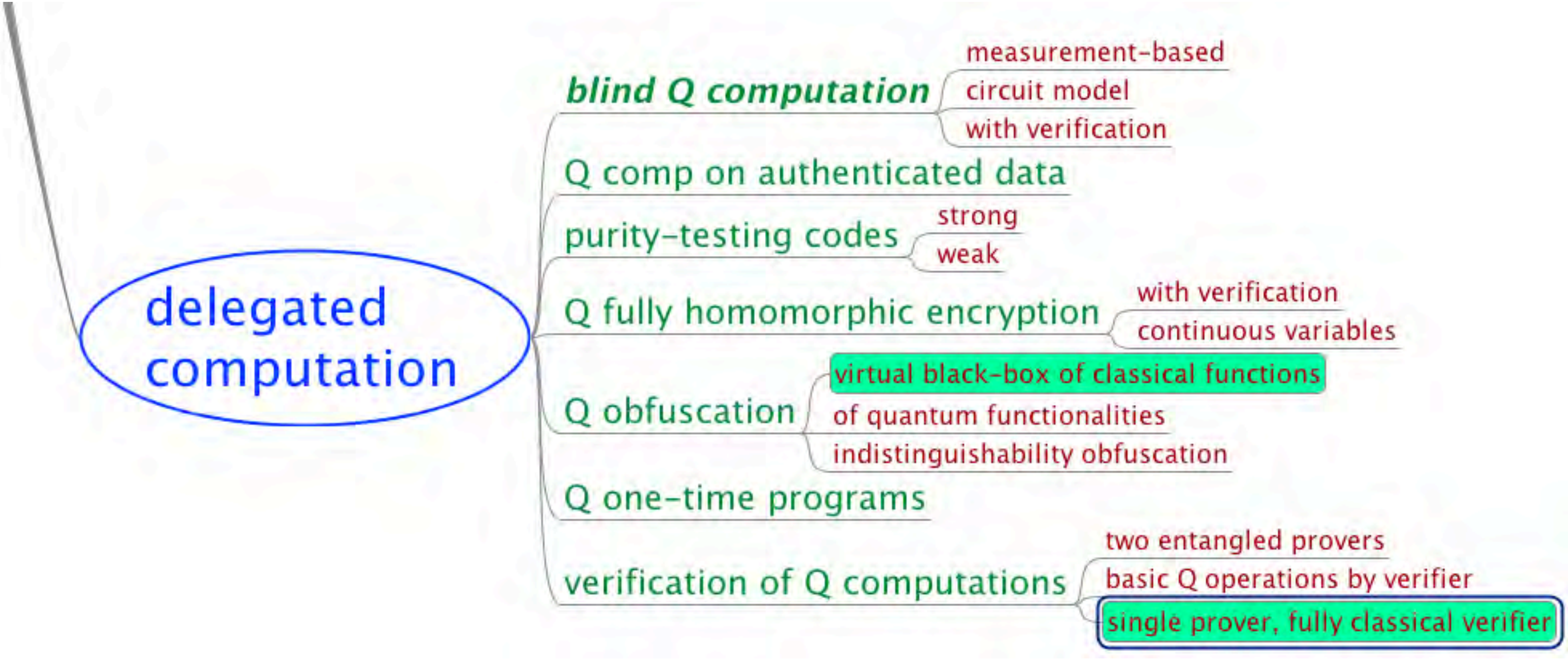


- QCloud Inc. promises you to perform a BQP computation
- How can a **purely classical verifier** be convinced that this computation actually was performed?

- Partial solutions:
  1. Using interactive protocols with quantum communication between prover and verifier, this task can be accomplished, using a certain minimum quantum ability of the verifier. [Fitzsimons Kashefi 17, Broadbent 17, AlagicDulekSpeelmanSchaffner17]
  2. Using two entangled, but non-communicating provers, verification can be accomplished using rigidity results [ReichardtUngerVazirani12]. Recently made way more practical by [ColadangeloGriloJefferyVidick17]
- Indications that information-theoretical blind computation is impossible [AaronsonCojocaruGheorghiuKashefi17]

[see Broadbent 17 or Fitzsimons 16 for overview and more complete references]

Delegated Q Computation



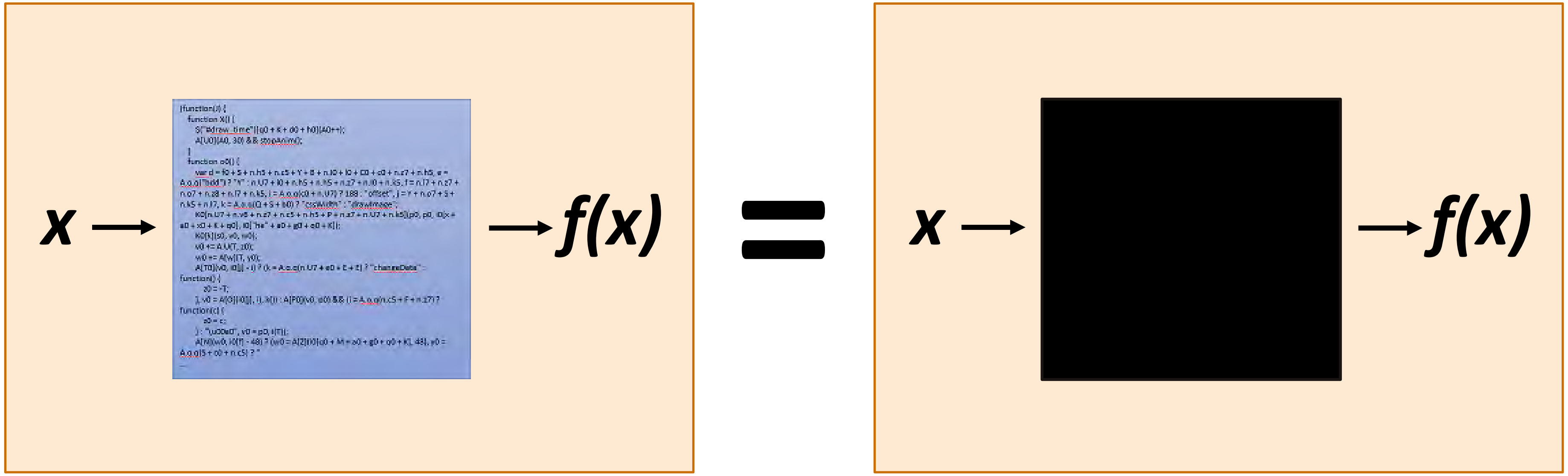
- delegated computation
  - ***blind Q computation***
    - measurement-based
    - circuit model
    - with verification
  - Q comp on authenticated data
  - purity-testing codes
    - strong
    - weak
  - Q fully homomorphic encryption
    - with verification
    - continuous variables
  - Q obfuscation
    - virtual black-box of classical functions
    - of quantum functionalities
    - indistinguishability obfuscation
  - Q one-time programs
  - verification of Q computations
    - two entangled provers
    - basic Q operations by verifier
    - single prover, fully classical verifier

Black-Box Obfuscation

Idea: an obfuscator is an algorithm which rewrites programs, such that

1. efficiency is preserved;
2. input-output functionality is preserved;
3. output programs are hard to understand: *"If something is efficiently learnable from reading the code, then it is also efficiently learnable purely from input-output behavior."*

"black-box obfuscation"



```
!function(t) {
  function X() {
    $("#draw_time")[q0 + K + d0 + h0](A0++);
    A[U0](A0, 30) && stopAnim();
  }
  function o0() {
    var d = f0 + S + n.h5 + n.c5 + Y + B + n.I0 + I0 + C0 + c0 + n.z7 + n.h5, e =
A.o.o["bold"] ? "Y" : n.U7 + I0 + n.h5 + n.h5 + n.z7 + n.I0 + n.k5, f = n.I7 + n.z7 +
n.o7 + n.z8 + n.I7 + n.k5, i = A.o.o(c0 + n.U7) ? 188 : "offset", j = Y + n.o7 + S +
n.k5 + n.I7, k = A.o.o(Q + S + I0) ? "cssWidth" : "drawImage";
    K0[n.U7 + n.v8 + n.z7 + n.c5 + n.h5 + P + n.z7 + n.U7 + n.k5](p0, p0, I0[x +
a0 + x0 + K + q0], I0["he" + a0 + g0 + e0 + K]);
    K0[k](s0, v0, w0);
    v0 += A.U(T, z0);
    w0 += A[w](T, y0);
    A[T0](v0, I0[j] - i) ? (k = A.o.o(n.U7 + e0 + E + E) ? "changeData" :
function() {
      z0 = -T;
    }, v0 = A[O](I0[j], i), k()) : A[P0](v0, s0) && (i = A.o.o(n.c5 + F + n.z7) ?
function(c) {
      s0 = c;
    } : "\u00e0", v0 = p0, i(T));
    A[N](w0, I0[f] - 48) ? (w0 = A[Z](I0[c0 + M + a0 + g0 + q0 + K], 48), y0 =
A.o.o(S + c0 + n.c5) ? "
...
```

[Alagic Fefferman 16, slide by Gorjan Alagic, thanks a lot!]

Classical Obfuscation

Idea: an obfuscator is an algorithm which rewrites programs, such that

1. efficiency is preserved;
2. input-output functionality is preserved;
3. output programs are hard to understand: *"If something is efficiently learnable from reading the code, then it is also efficiently learnable purely from input-output behavior."*

Formal:

"black-box obfuscation"

A black-box obfuscator *O* is an algorithm which maps circuits *C* to circuits *O(C)* such that:

1. efficiency-preserving: $|\mathcal{O}(C)| \leq \text{poly}(|C|)$
2. functionality-preserving: $f_{\mathcal{O}(C)} = f_C$
3. virtual black-box: for every poly-time *A* there exists a poly-time *S* such that

$$|\Pr\underbrace{[\mathcal{A}(\mathcal{O}(C)) = 1]}_{\textbf{learn something by reading circuit}} - \Pr\underbrace{[\mathcal{S}^{f_C}(\bar{1}) = 1]}_{\textbf{learn same thing from input-output}}| \leq \text{negl}(|C|)\,.$$

[Alagic Fefferman 16, slide by Gorjan Alagic, thanks a lot!]

Classical Obfuscation

Why care? Lots of applications:

1. **Protecting IP:** obfuscate before publishing (already done, but ad-hoc);
2. **Secure patching:** revealing what is being patched exposes unpatched machines;
3. **Public-key crypto:** private-key encryption → public-key encryption:

$$k_{\mathrm{decrypt}} := k \qquad k_{\mathrm{encrypt}} := \mathcal{O}(\mathrm{Enc}_k)\,.$$

4. **One-way functions:** choose delta-function circuit, make obfuscator's coins part of input;
5. **FHE:** encryption → fully-homomorphic encryption:

$$k_{\mathrm{eval}} := \mathcal{O}(\mathrm{Enc}_k \circ U \circ \mathrm{Dec}_k)$$

universal circuit

"top of the crypto scheme hierarchy"

Bad news: classical black-box obfuscation is impossible [Barak et al '01].

Other definitions? "Computational indistinguishability" (first schemes proposed in 2013);

[Alagic Fefferman 16, slide by Gorjan Alagic, thanks a lot!]

Quantum Obfuscation

A quantum obfuscator *O* is a (quantum) algorithm which rewrites quantum circuits, and is:

1. efficiency-preserving: $|\mathcal{O}(C)| \leq \mathrm{poly}(|C|)$
2. functionality-preserving: $\|U_C - U_{\mathcal{O}(C)}\| \leq \mathrm{negl}(|C|)$
3. virtual black-box: for every QPT A there exists a QPT S such that

quantum polynomial-time algorithm

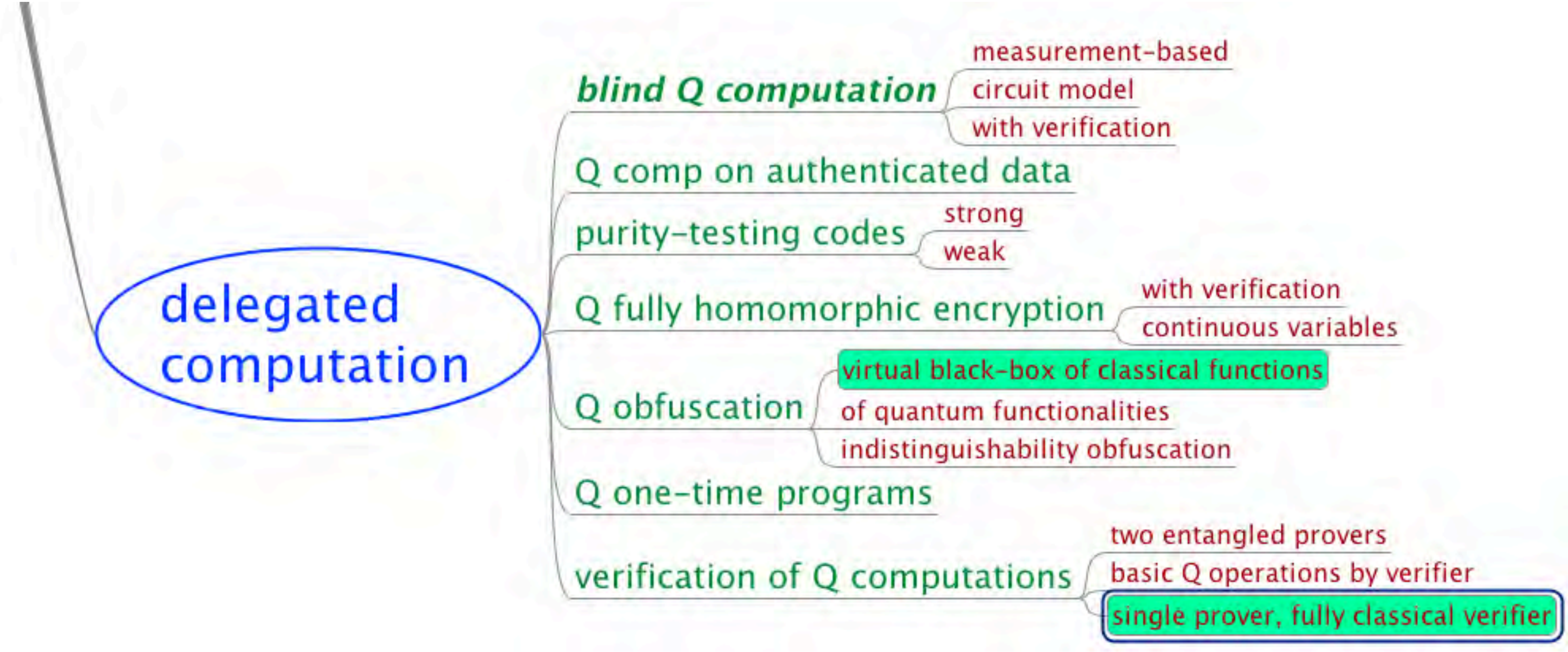
$$|\Pr[\mathcal{A}(\mathcal{O}(C)) = 1] - \Pr[\mathcal{S}^{U_C}(\bar{1}) = 1]| \leq \mathrm{negl}(|C|)\,.$$

Obfuscation	Input	Output	Adversary	Possibility?
Black-box	Quantum circuit	Quantum circuit	QPT	Impossible
Black-box	Quantum circuit	Quantum state (reusable)	QPT	Impossible
Black-box	Quantum circuit	Quantum state (uncloneable)	QPT	Open
Statistical I.O	Quantum circuit	Quantum state	QPT	Impossible
Computational I.O	Quantum circuit	Quantum state	QPT	Open

1. construct a black-box quantum obfuscator (that outputs states that cannot be reused);
2. construct a computational indistinguishability quantum obfuscator (that outputs circuits);

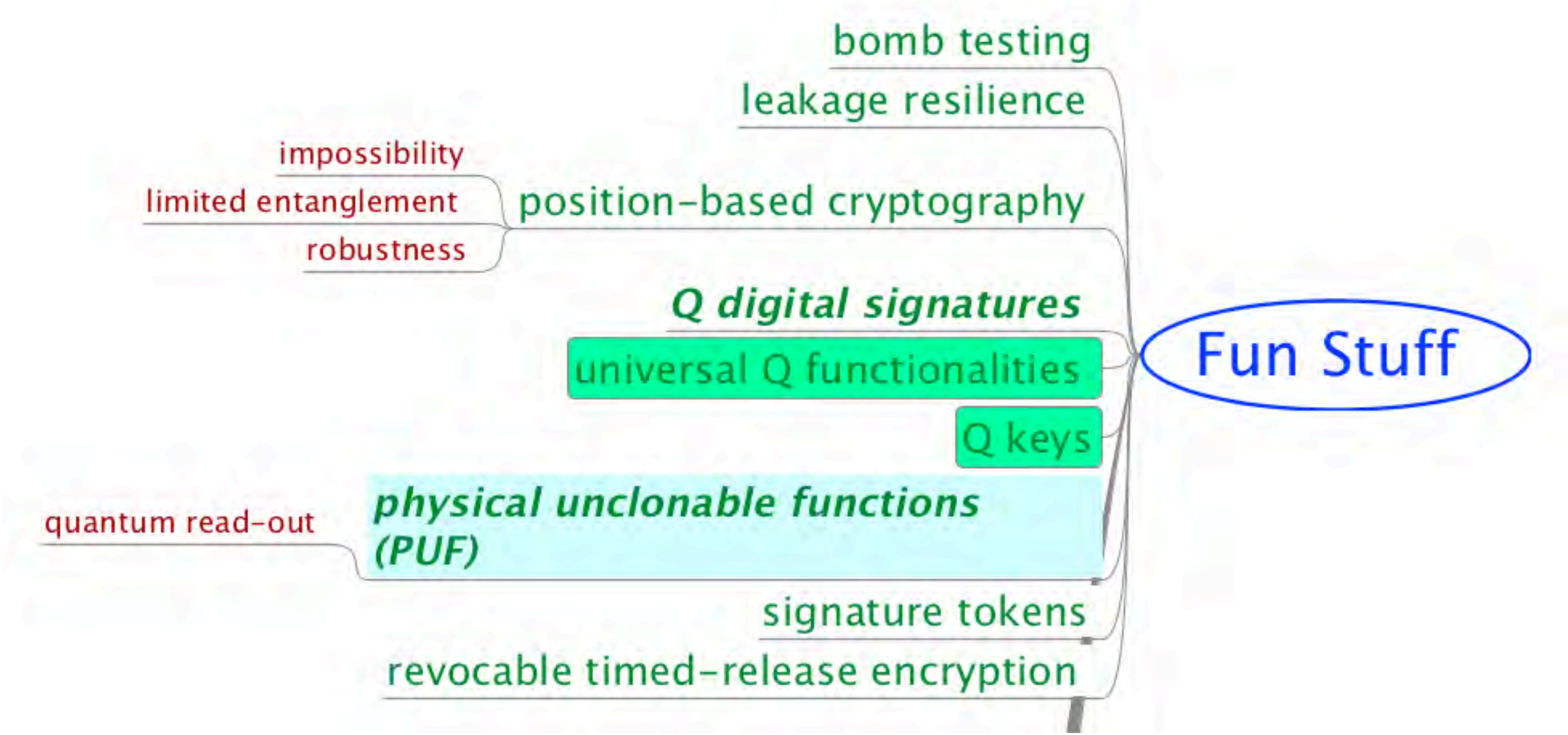
[Alagic Fefferman 16, slide by Gorjan Alagic, thanks a lot!]

Delegated Q Computation

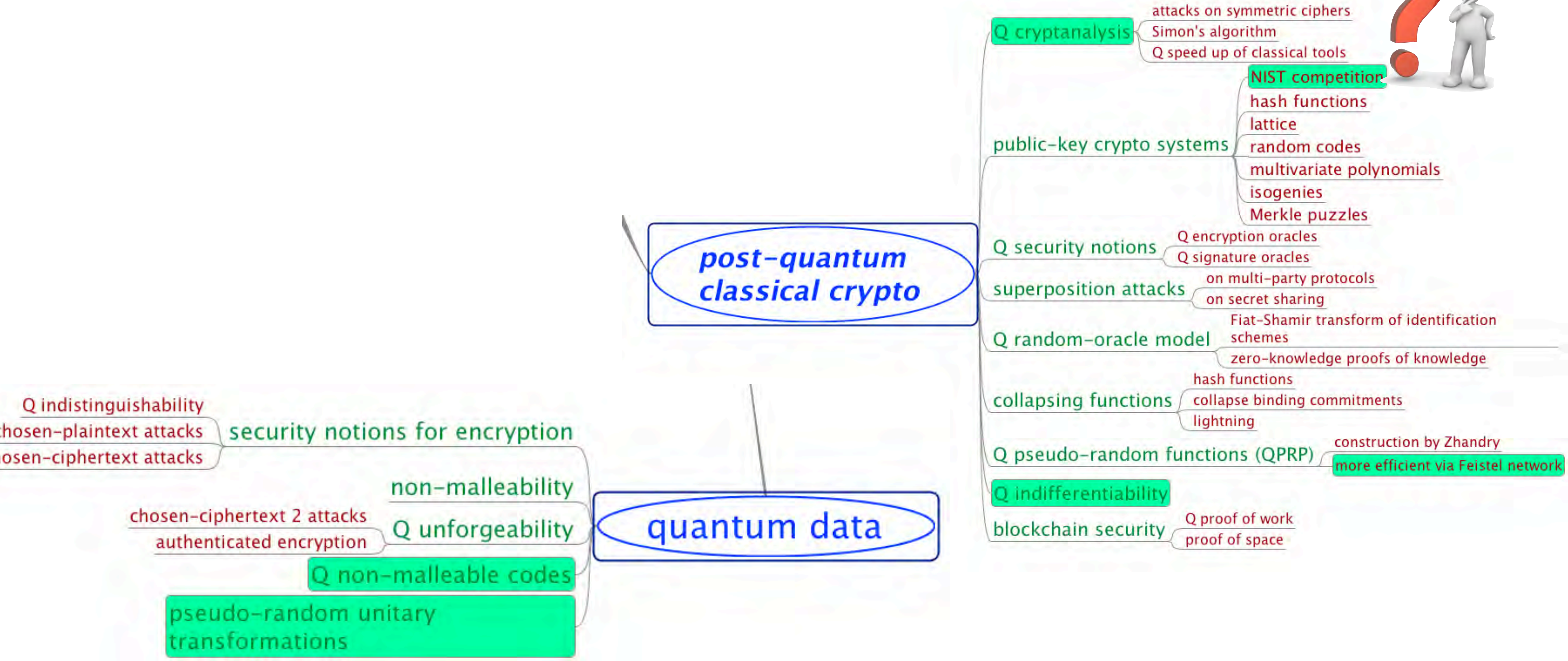


- delegated computation
  - ***blind Q computation***
    - measurement-based
    - circuit model
    - with verification
  - Q comp on authenticated data
  - purity-testing codes
    - strong
    - weak
  - Q fully homomorphic encryption
    - with verification
    - continuous variables
  - Q obfuscation
    - virtual black-box of classical functions
    - of quantum functionalities
    - indistinguishability obfuscation
  - Q one-time programs
  - verification of Q computations
    - two entangled provers
    - basic Q operations by verifier
    - single prover, fully classical verifier

More Fun Stuff



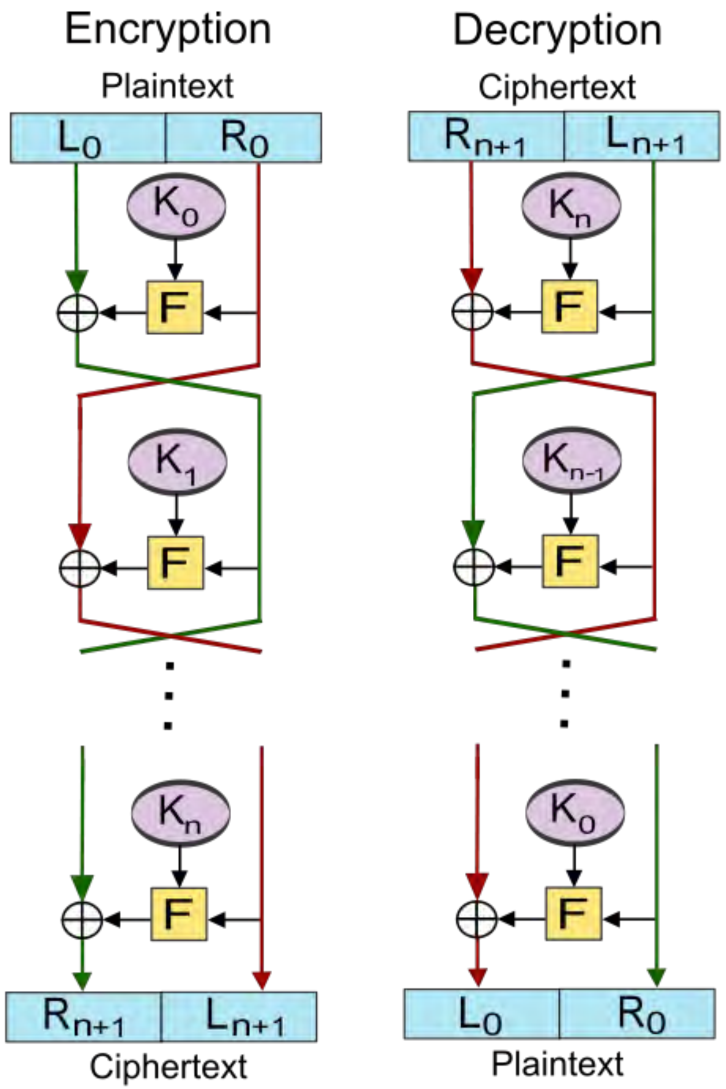
Pseudorandom Operations



- *post-quantum classical crypto*
  - Q cryptanalysis
    - attacks on symmetric ciphers
    - Simon's algorithm
    - Q speed up of classical tools
  - public-key crypto systems
    - NIST competition
    - hash functions
    - lattice
    - random codes
    - multivariate polynomials
    - isogenies
    - Merkle puzzles
  - Q security notions
    - Q encryption oracles
    - Q signature oracles
  - superposition attacks
    - on multi-party protocols
    - on secret sharing
  - Q random-oracle model
    - Fiat-Shamir transform of identification schemes
    - zero-knowledge proofs of knowledge
  - collapsing functions
    - hash functions
    - collapse binding commitments
    - lightning
  - Q pseudo-random functions (QPRP)
    - construction by Zhandry
    - more efficient via Feistel network
  - Q indifferentiability
  - blockchain security
    - Q proof of work
    - proof of space
- quantum data
  - security notions for encryption
    - Q indistinguishability
    - hosen-plaintext attacks
    - osen-ciphertext attacks
  - non-malleability
  - Q unforgeability
    - chosen-ciphertext 2 attacks
    - authenticated encryption
  - Q non-malleable codes
  - pseudo-random unitary transformations

[https://csrc.nist.gov/Projects/Post-Quantum-Cryptography]

Pseudorandom Permutation from Function



- Feistel network
- If F is a (pseudo)random function, the 3-round Feistel function H_3 is a pseudo-random permutation.
- Question: Show that 4-random Feistel H_4 is a quantum-secure pseudo-random permutation

For any QPT A, we want

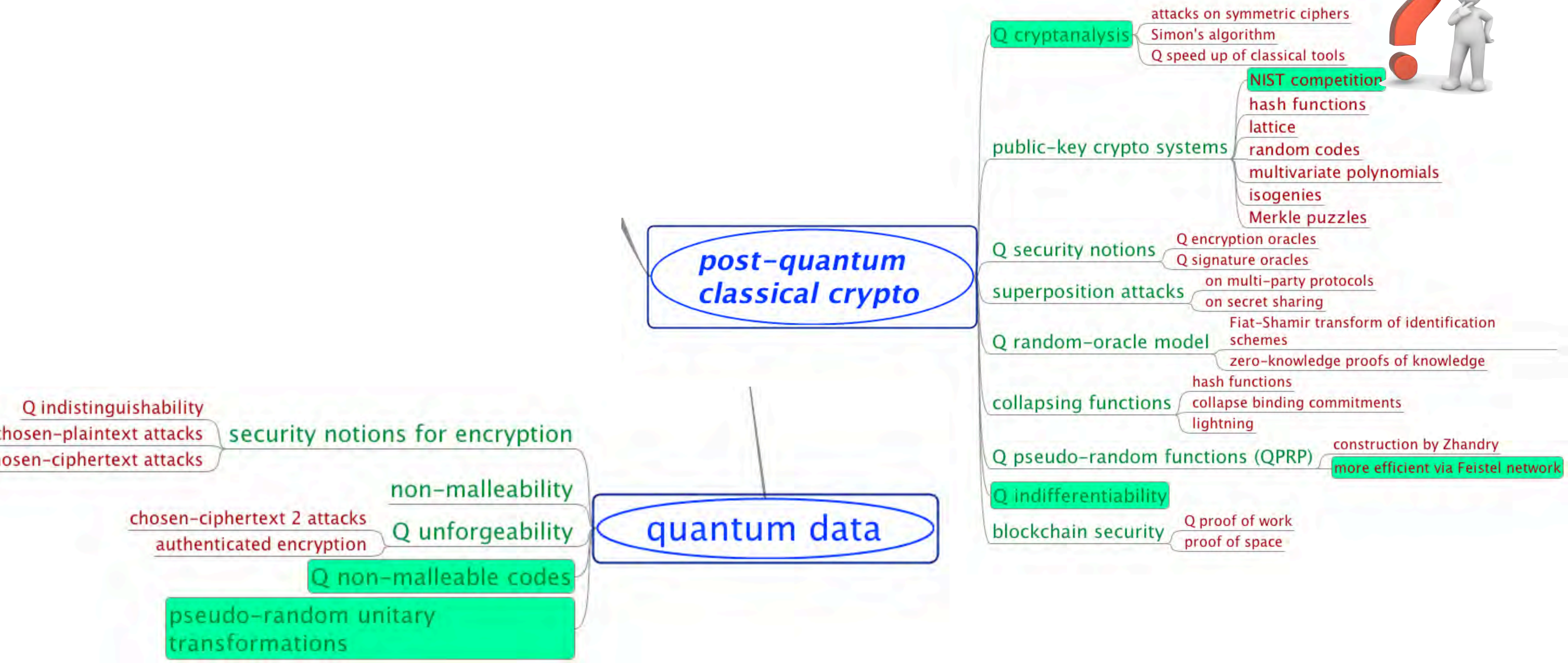
$$|\Pr[A^{|H_4>,|H_4^{-1}>}(1^n) = 1] - \Pr[A^{|rnd>,|rnd^{-1}>}(1^n) = 1]| < negl(n$$

- Partial result: Quantum attack based Simon's algorithm can distinguish 3-round Feistel H_3 from random function.

- Quantum pseudo-random unitaries?

[Kuwakado Morii 10, Ji Liu Song 17]

Pseudorandom Operations



post-quantum classical crypto

- Q cryptanalysis
  - attacks on symmetric ciphers
  - Simon's algorithm
  - Q speed up of classical tools
- public-key crypto systems
  - NIST competition
  - hash functions
  - lattice
  - random codes
  - multivariate polynomials
  - isogenies
  - Merkle puzzles
- Q security notions
  - Q encryption oracles
  - Q signature oracles
- superposition attacks
  - on multi-party protocols
  - on secret sharing
- Q random-oracle model
  - Fiat-Shamir transform of identification schemes
  - zero-knowledge proofs of knowledge
- collapsing functions
  - hash functions
  - collapse binding commitments
  - lightning
- Q pseudo-random functions (QPRP)
  - construction by Zhandry
  - more efficient via Feistel network
- Q indifferentiability
- blockchain security
  - Q proof of work
  - proof of space

quantum data

- security notions for encryption
  - Q indistinguishability
  - hosen-plaintext attacks
  - osen-ciphertext attacks
- non-malleability
- Q unforgeability
  - chosen-ciphertext 2 attacks
  - authenticated encryption
- Q non-malleable codes
- pseudo-random unitary transformations

[https://csrc.nist.gov/Projects/Post-Quantum-Cryptography]

Thank you!

https://github.com/cschaffner/QCryptoMindmap

http://arxiv.org/abs/1510.06120

In Designs, Codes and Cryptography 2016

- Thanks to all friends and colleagues that contributed to quantum cryptography and to this presentation.

TECHNISCHE UNIVERSITÄT DARMSTADT

0011011100001011 Cryptoplexity
qed
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

cost
EUROPEAN COOPERATION IN SCIENCE AND TECHNOLOGY

NWO
Nederlandse Organisatie voor Wetenschappelijk Onderzoek

CWI

KØBENHAVNS UNIVERSITET

uOttawa

UNIVERSITY OF MARYLAND

QuSoft

Questions