Quantum Cryptography (Beyond QKD)

CHRISTIAN SCHAFFNER

QuSoft RESEARCH CENTER FOR QUANTUM SOFTWARE

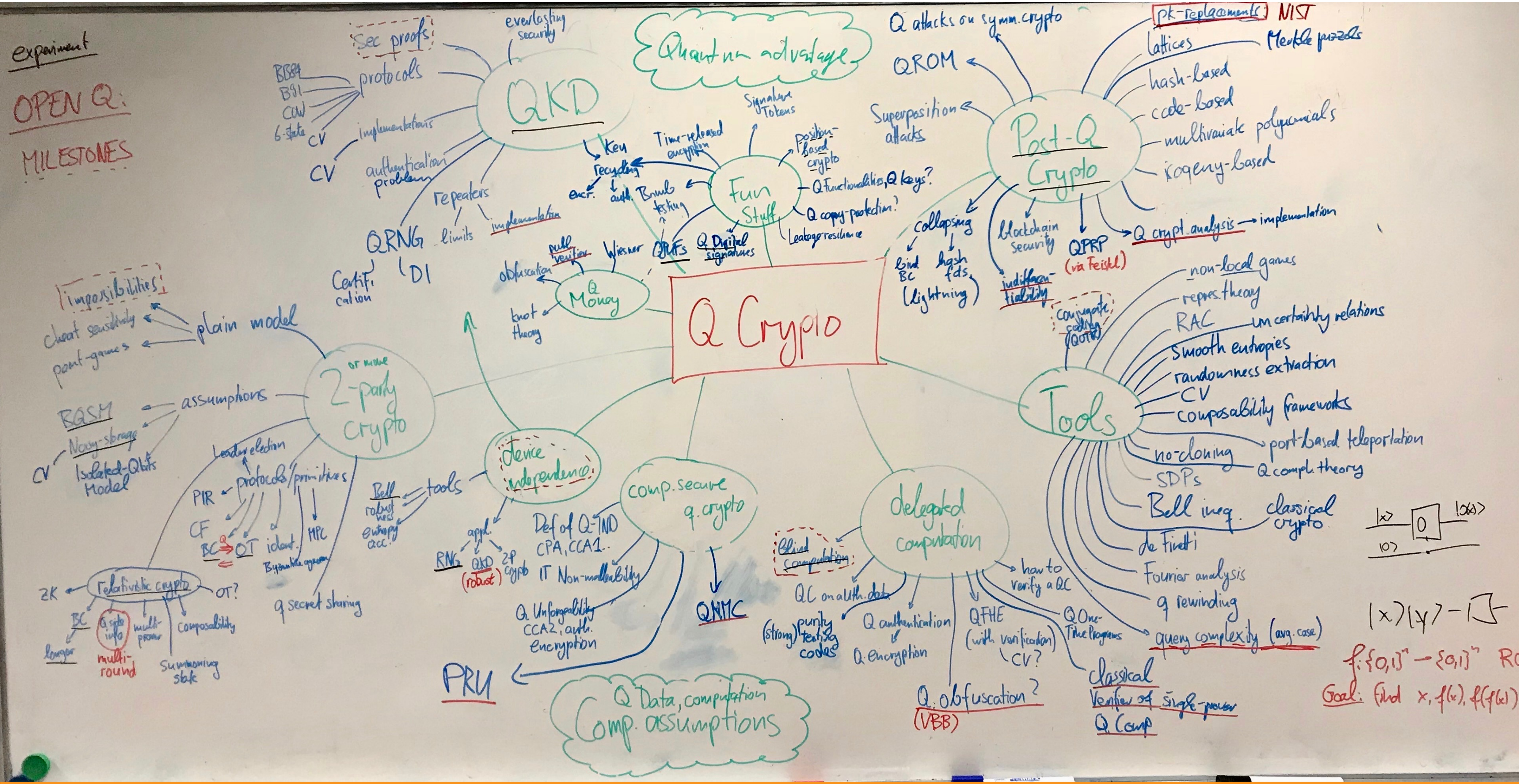
INSTITUTE FOR LOGIC, LANGUAGE AND COMPUTATION (ILLC)

UNIVERSITY OF AMSTERDAM

CWI CENTRUM WISKUNDE & INFORMATICA

Nederlandse Organisatie voor Wetenschappelijk Onderzoek

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


experiment
OPEN Q:
MILESTONES
Q Crypto
QKD
Sec proofs
everlasting security
protocols
BB84
B91
COW
6-state
CV
implementations
authentication problem
repeaters
limits
implementation
QRNG
DI
Certification
Quantum advantage
Fun Stuff
Key recycling
encr.
auth.
Time-released encryption
Signature Tokens
position-based crypto
Q functionalities, Q keys?
Q copy-protection?
Leakage resilience
Bomb testing
QPUFs
Q Digital signatures
Wiesner
publ. verification
obfuscation
Q Money
knot theory
Post-Q Crypto
pk-replacements
NIST
lattices
Merkle puzzles
hash-based
code-based
multivariate polynomials
isogeny-based
Q attacks on symm. crypto
QROM
Superposition attacks
collapsing
bind BC
hash fcts
(lightning)
blockchain security
indifferentiability
QPRP
(via Feistel)
Q crypt analysis
implementation
Tools
conjugate coding (QOTP)
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)
2-party crypto
or more
impossibilities
plain model
cheat sensitivity
point-games
assumptions
BQSM
Noisy-storage
Isolated-Qbits Model
protocols/primitives
Leader election
PIR
CF
BC
OT
ident.
MPC
Byzantine agreement
q secret sharing
Relativistic crypto
ZK
OT?
longer
Q side info
multi-round
multi-prover
composability
summoning state
device independence
tools
Bell
robustness
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
how to verify a QC
QC on auth. data
(strong) purity testing codes
Q authentication
Q encryption
QFHE
(with verification)
CV?
Q One-Time Programs
Q obfuscation?
(VBB)
classical Verifier of single-prover Q Comp
|x⟩
|0⟩
|f(x)⟩
|x⟩|y⟩
f: {0,1}ⁿ → {0,1}ⁿ
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

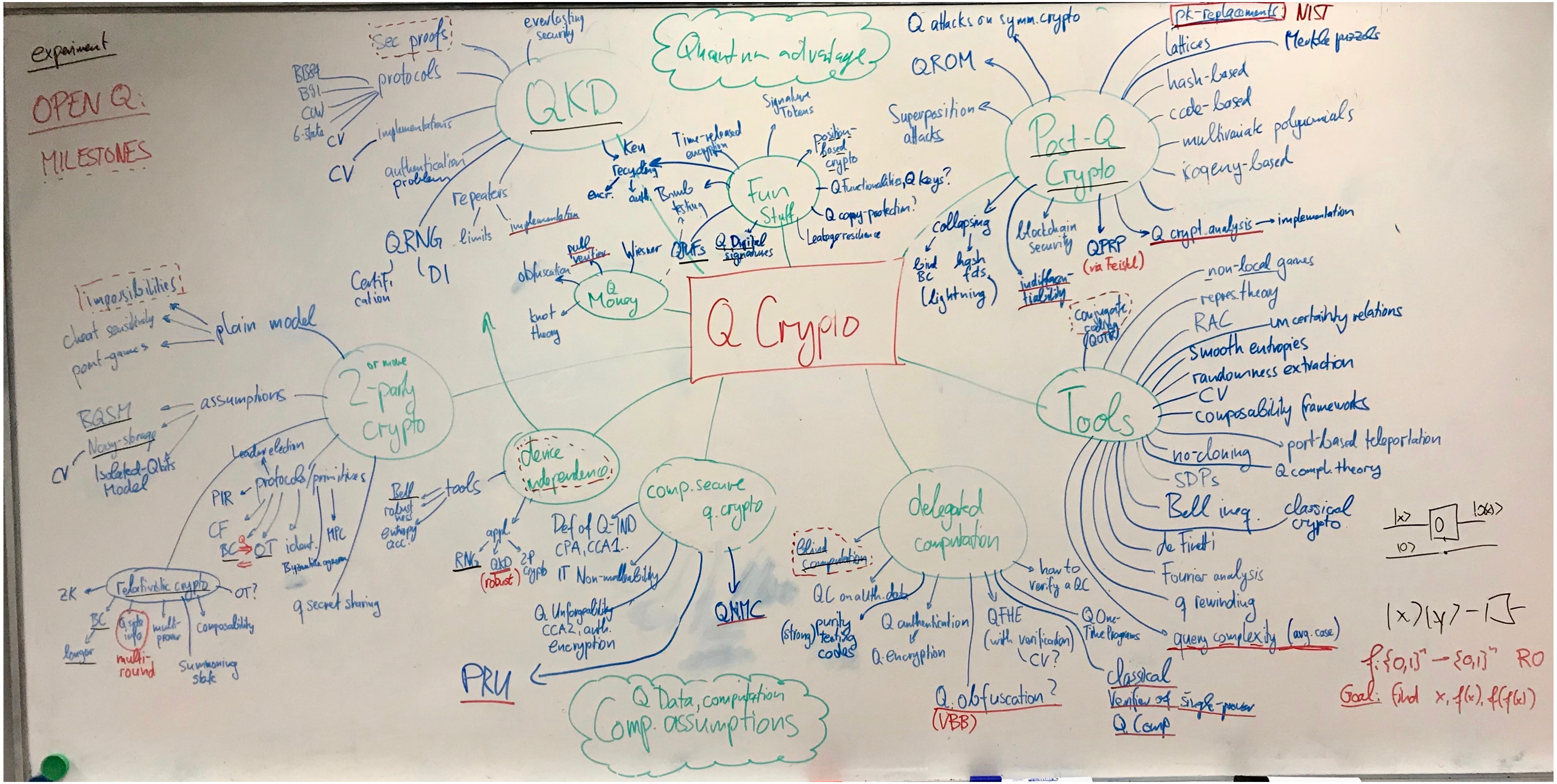
[Broadbent Schaffner 16 in Designs, Codes and Cryptography]

QCrypt Conference Series

- Started in 2011 by Christandl and Wehner
- Steadily growing since then:
  approx. 100 submissions, 30 accepted as contributions, ~300 participants in Montreal 2019. This year: Amsterdam
- goal of the conference: 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, approximately 6 invited talks

[QCrypt 2020, organized by Amsterdam group]

Overview

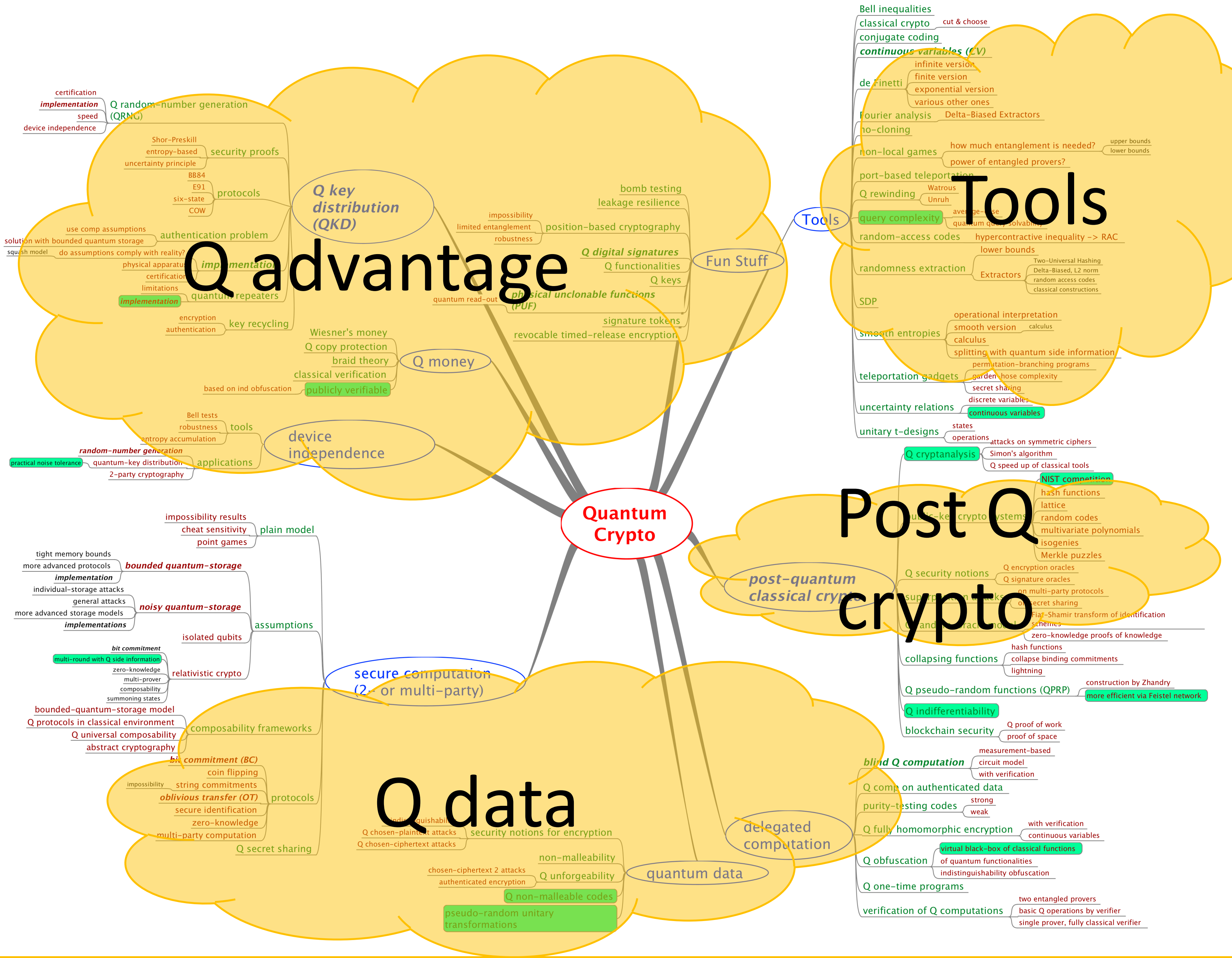


[thanks to Serge Fehr, Stacey Jeffery, Chris Majenz, Florian Speelman, Ronald de Wolf]

MindMap

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

- Fork me on github!

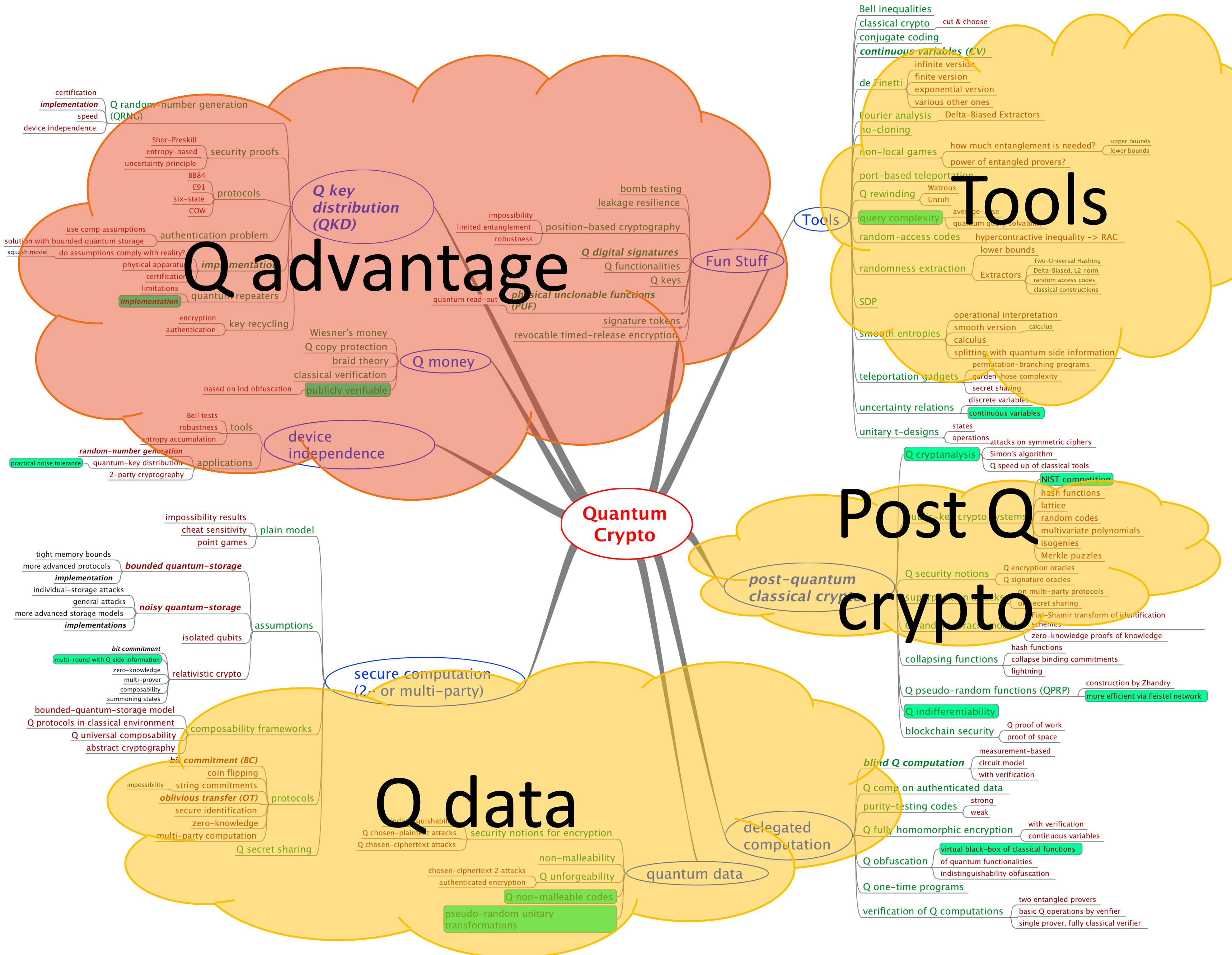


[from 2018! https://github.com/cschaffner/QCryptoMindmap]

MindMap

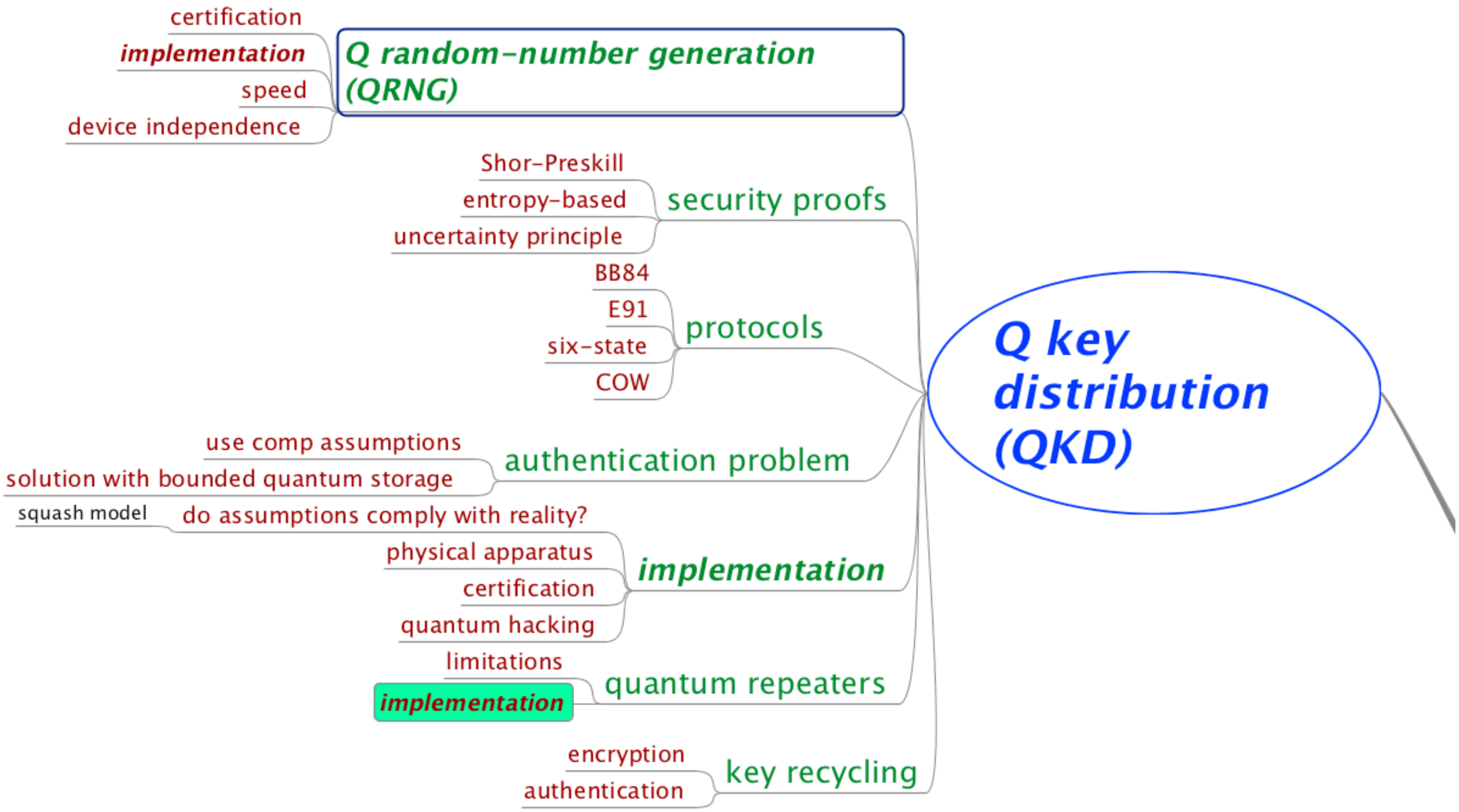
- ***experiments***
- Selection of open questions

- Fork me on github!

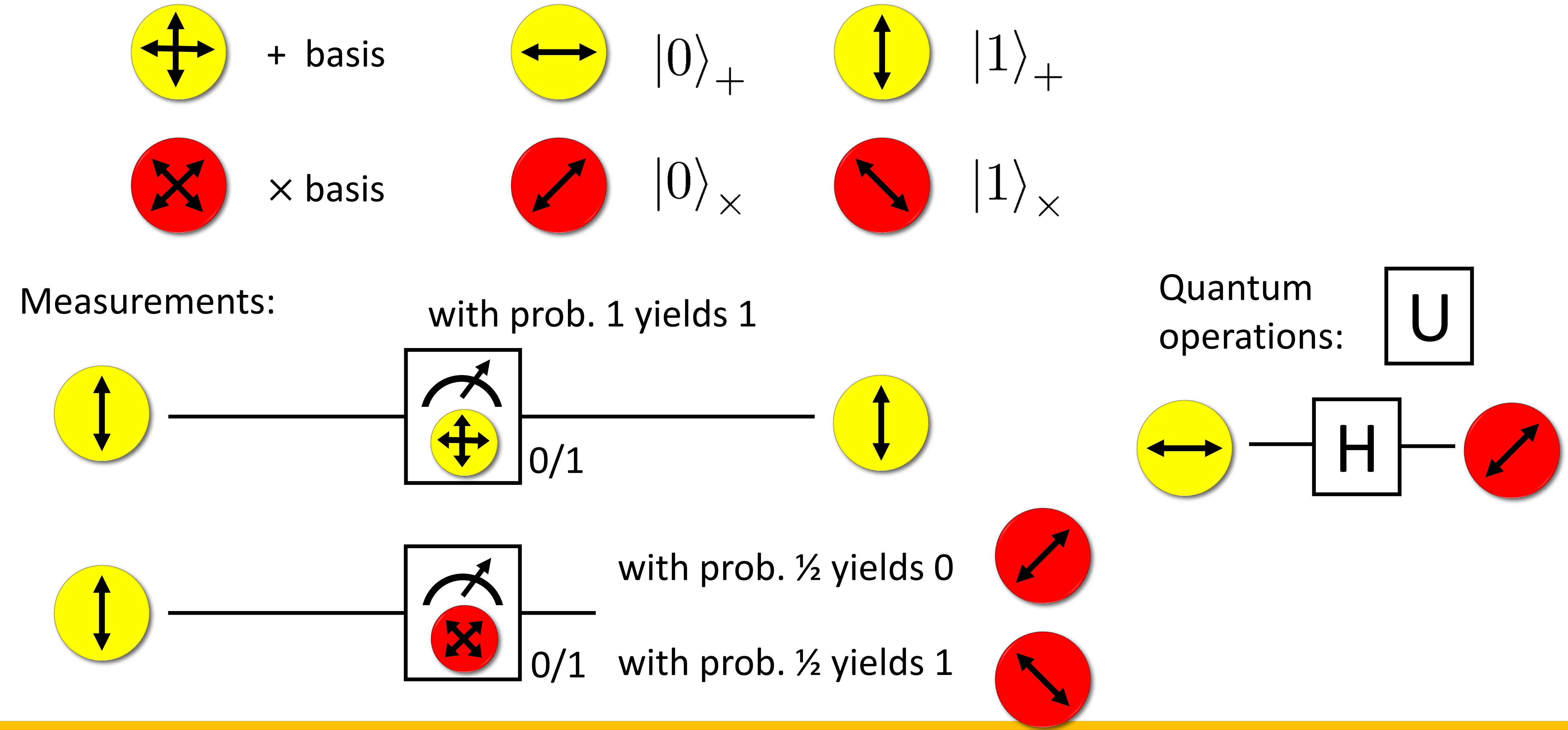


[https://github.com/cschaffner/QCryptoMindmap]

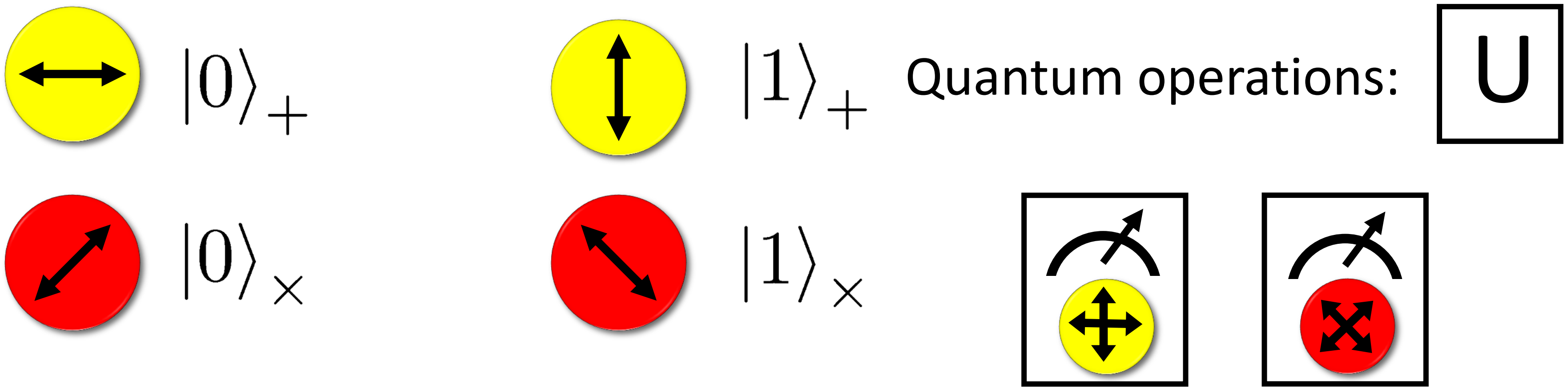
Quantum Key Distribution (QKD)

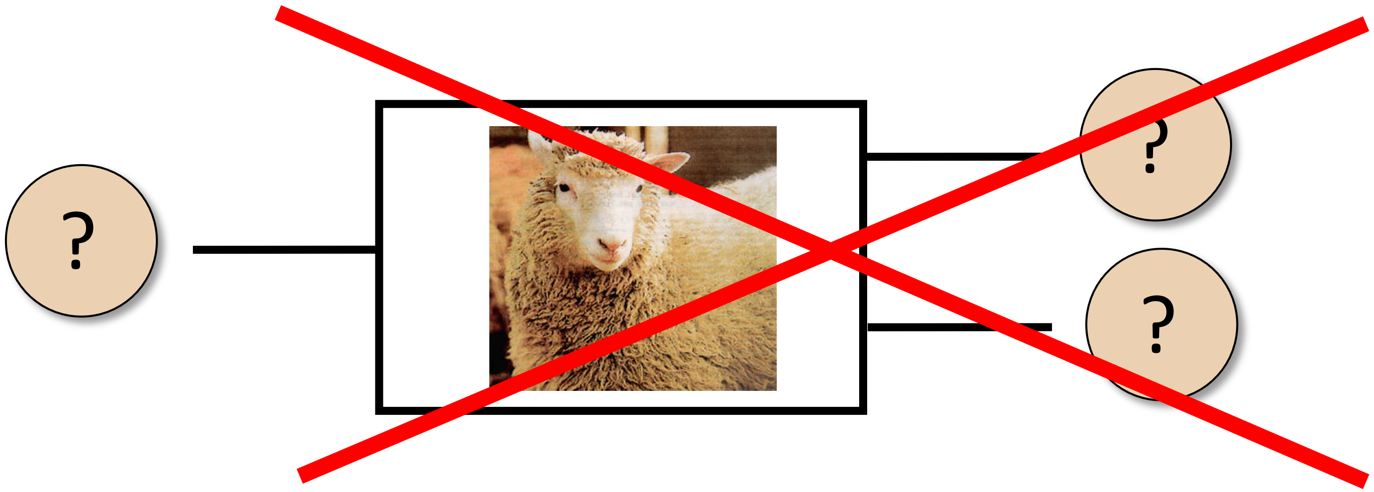


Quantum Mechanics



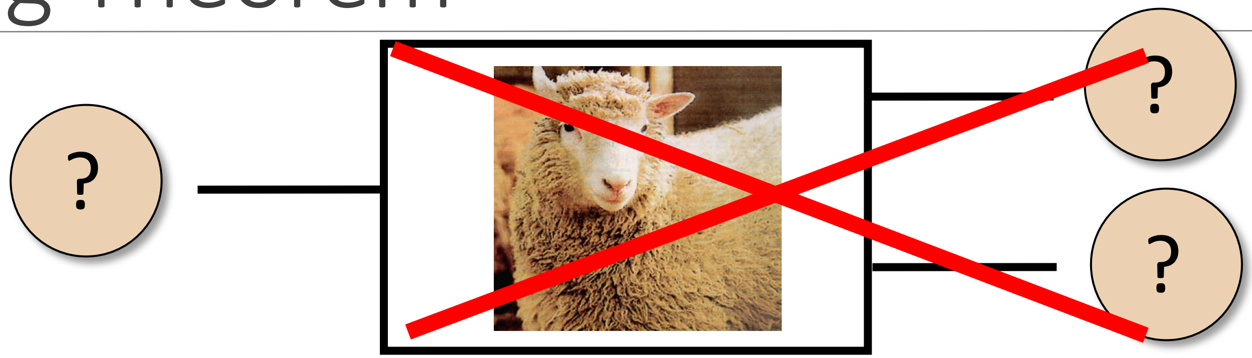
No-Cloning Theorem





Proof: copying is a non-linear operation

Proof of No-Cloning Theorem



Proof: Assume U such that for all $|\psi\rangle$: $U\,(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$.

Then, $U\,(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$ and $U\,(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle$.

By linearity of U, it holds that

$U\,((|0\rangle + |1\rangle) \otimes |0\rangle) = U\,(|0\rangle \otimes |0\rangle) + U\,(|1\rangle \otimes |0\rangle)$

$= |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$

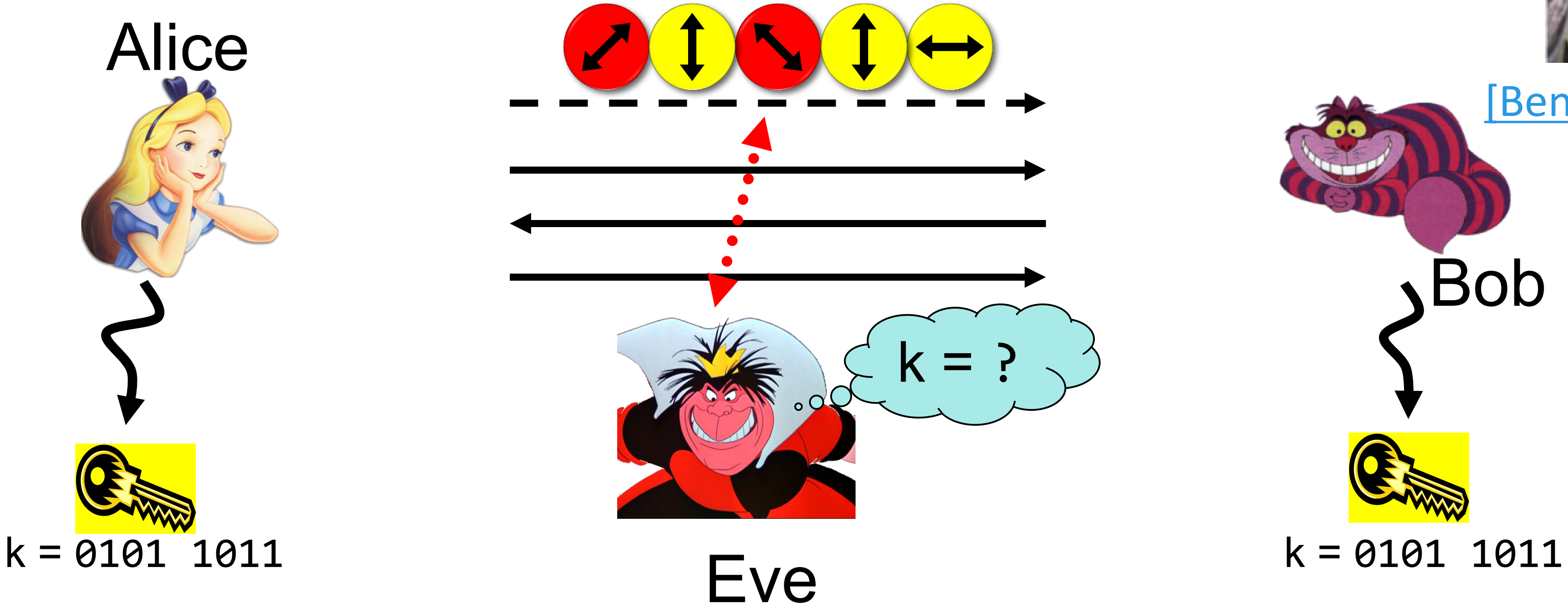
$\neq (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)$

$= |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$

Contradiction!

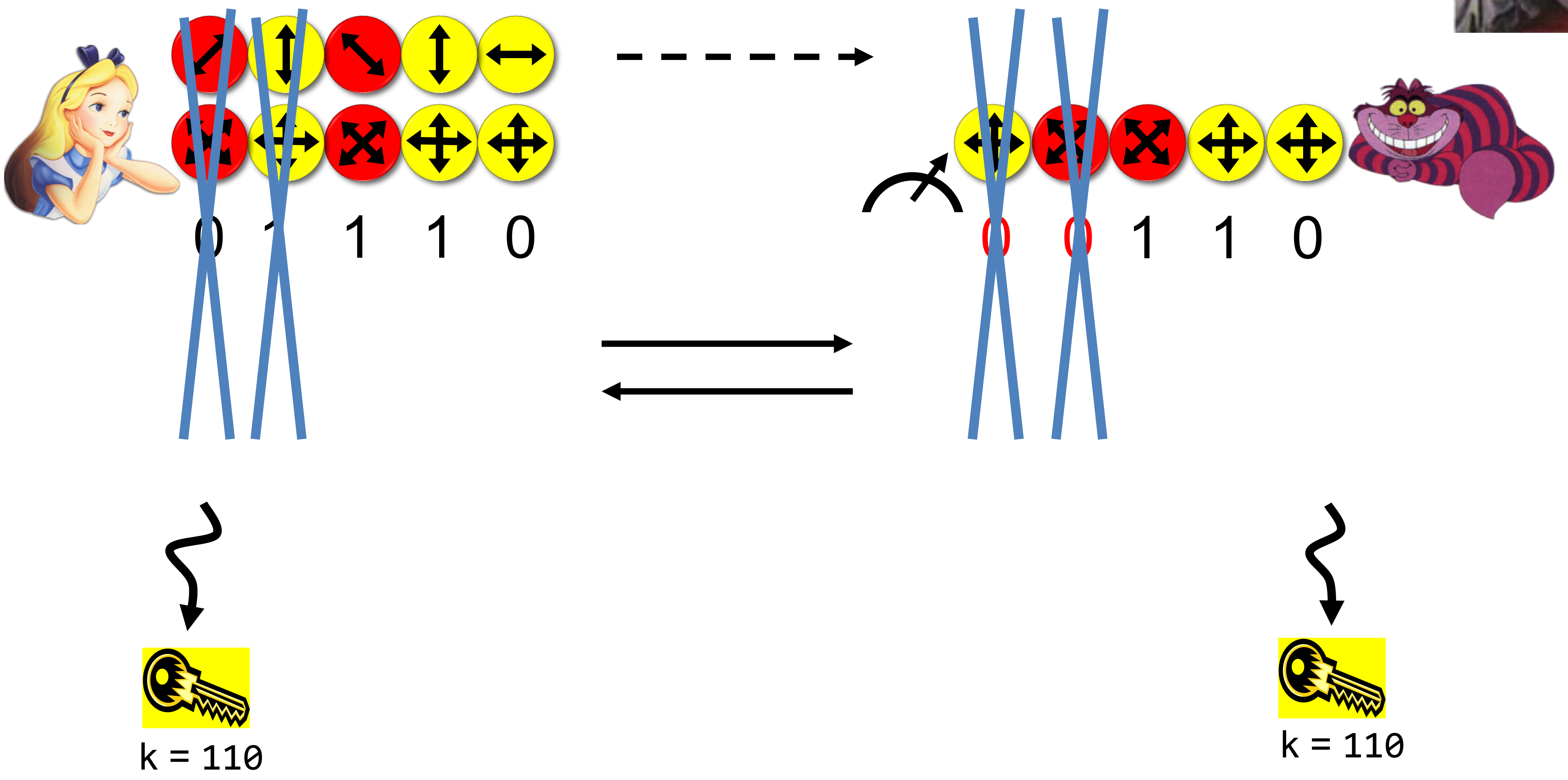
Quantum Key Distribution (QKD)

[Bennett Brassard 84]



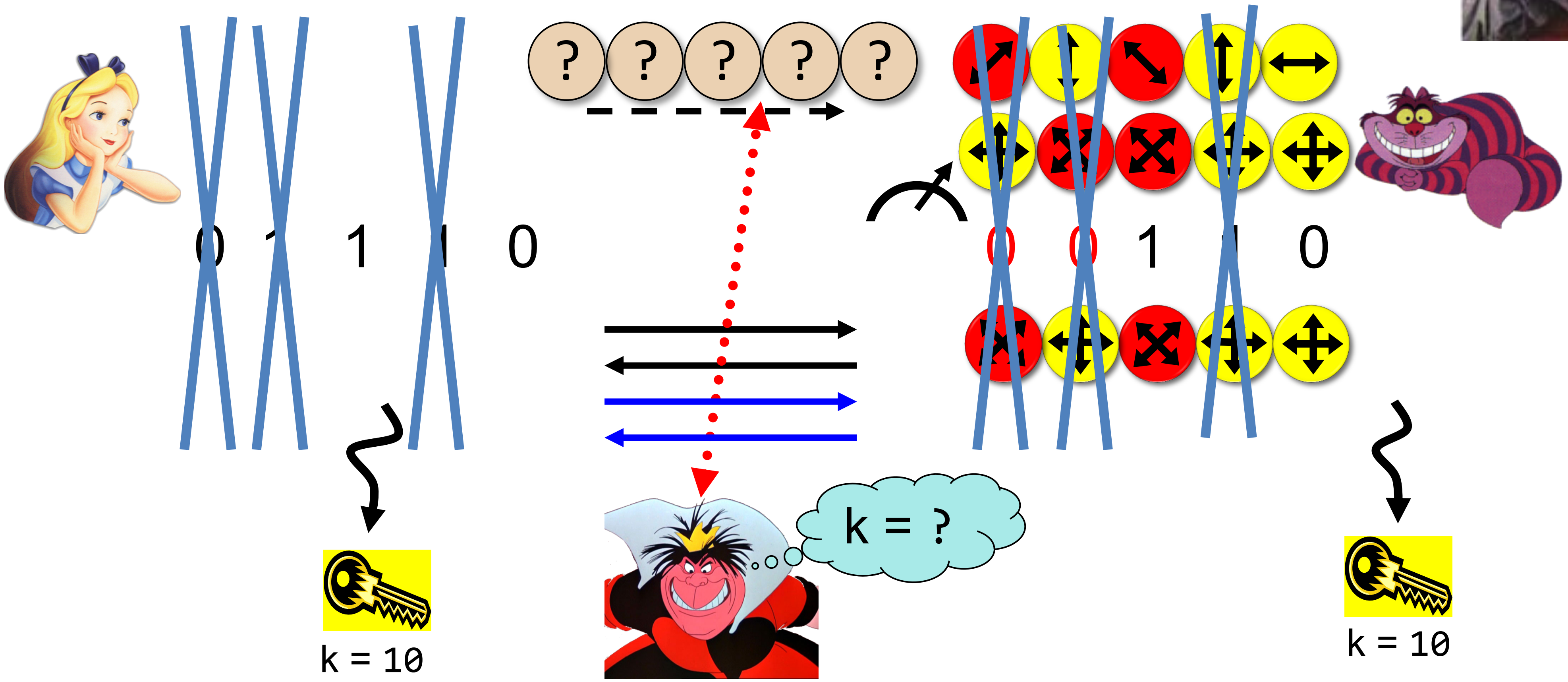
- Offers an quantum solution to the key-exchange problem which does not rely on computational assumptions (such as factoring, discrete logarithms, security of AES, SHA-3 etc.)
- Important caveat: classical communication has to be authenticated to prevent man-in-the-middle attacks

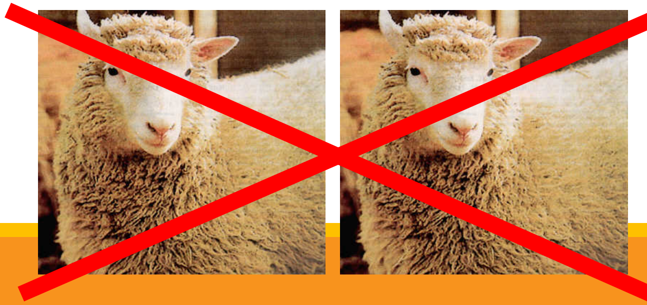
Quantum Key Distribution (QKD)



[Bennett Brassard 84]

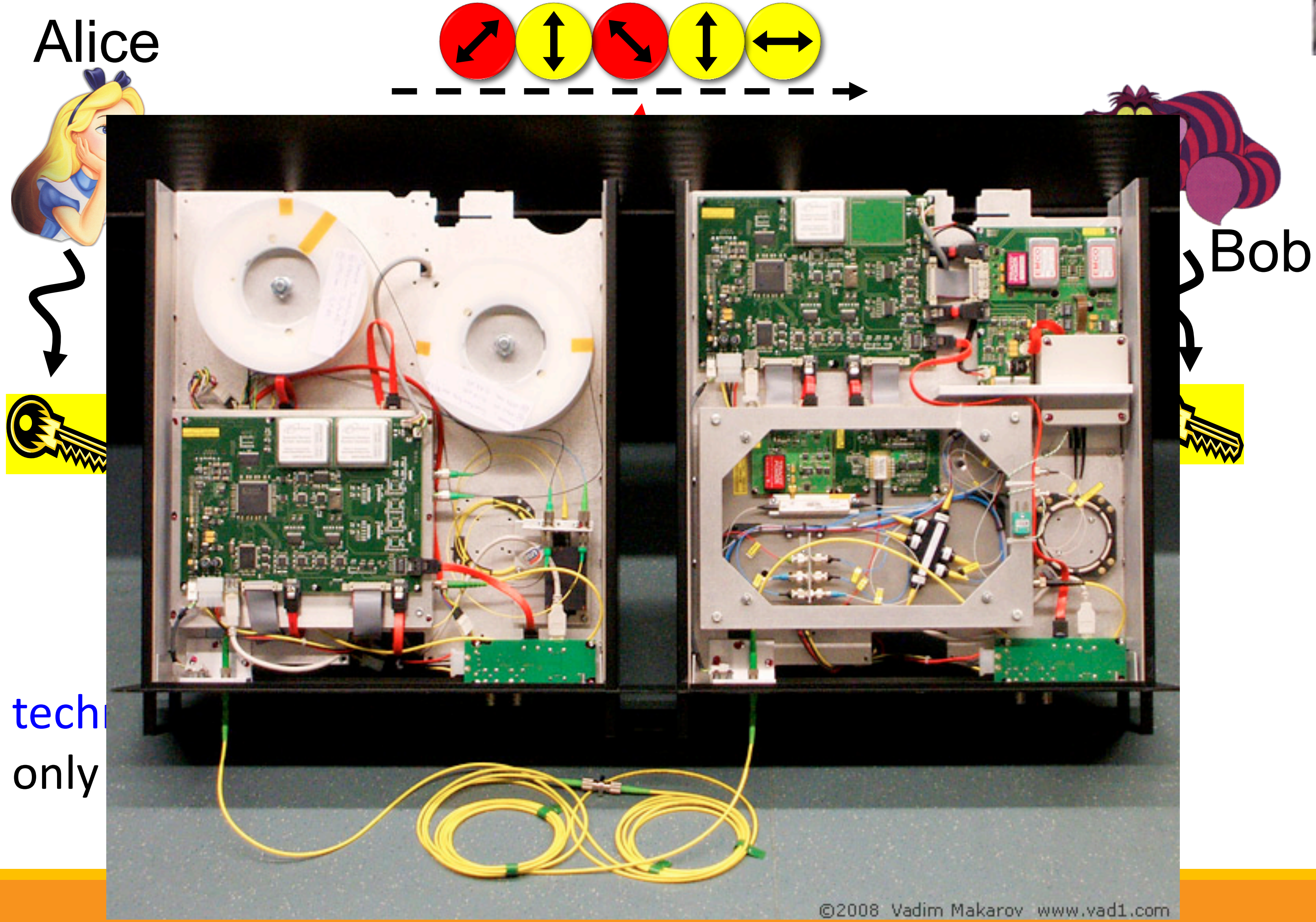
Quantum Key Distribution (QKD)





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

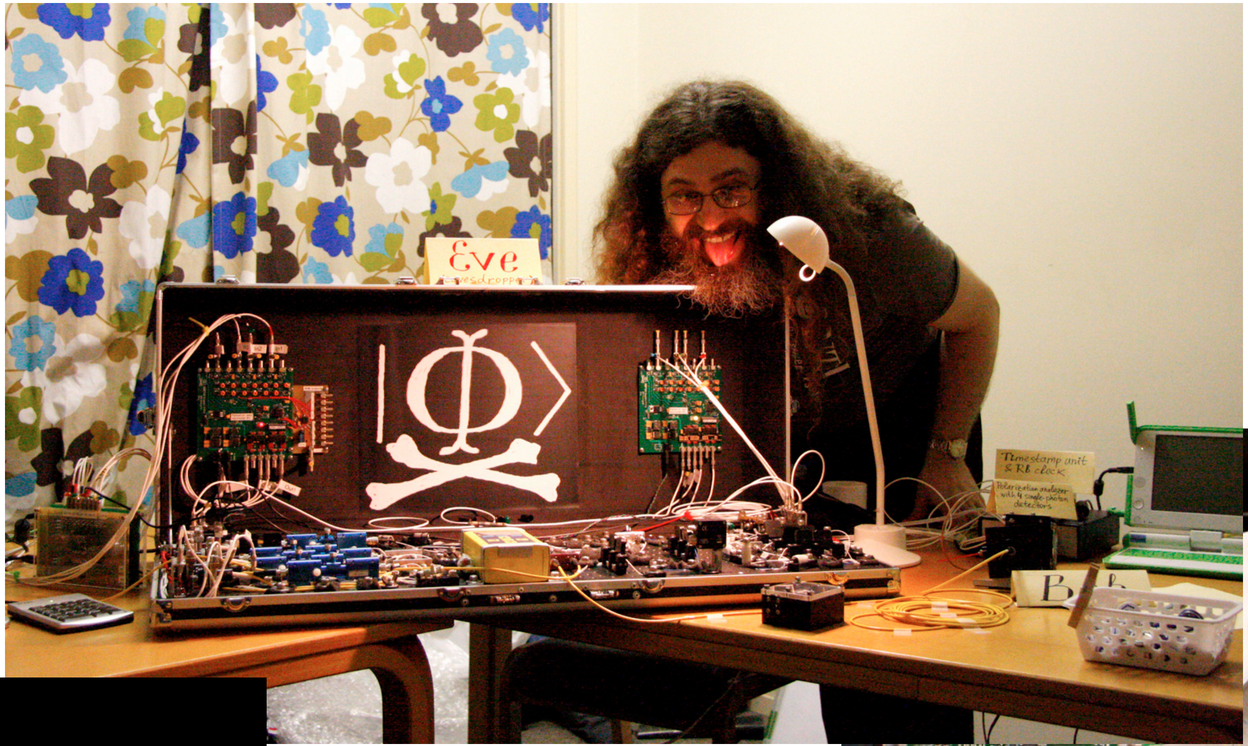
Quantum Key Distribution (QKD)

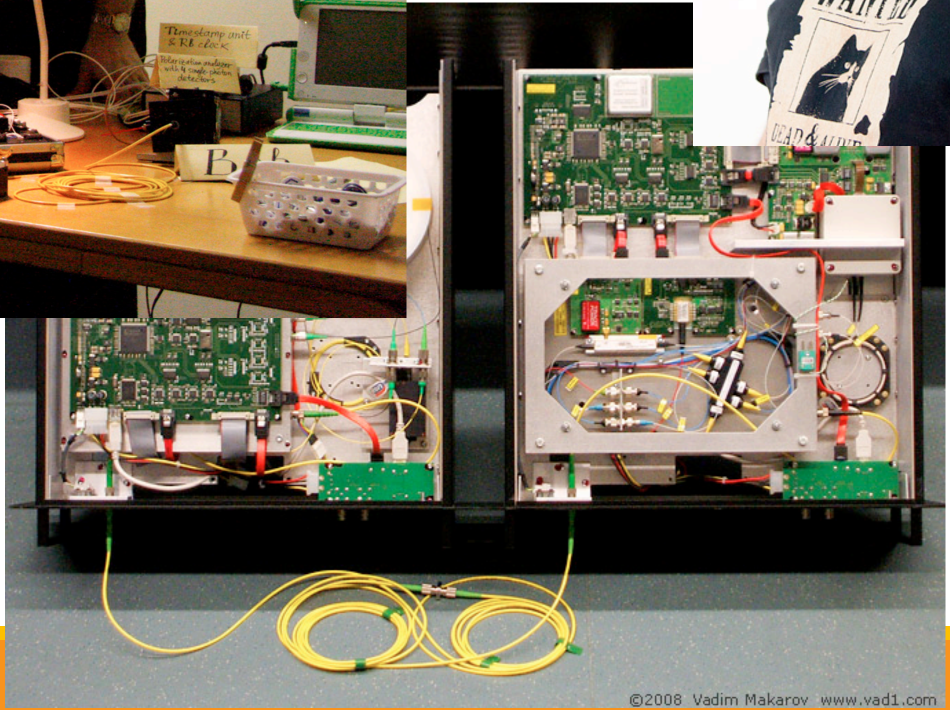


- techn
  only

Quantum Hacking

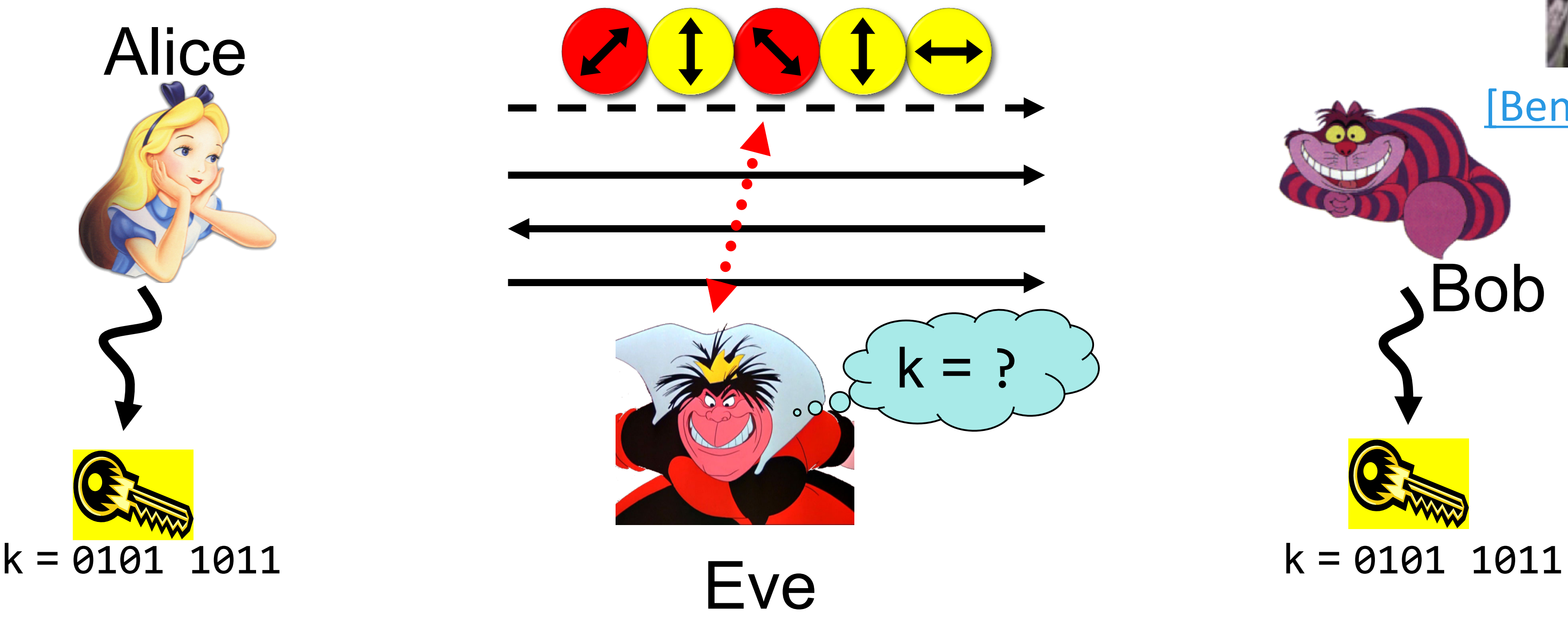
e.g. by the group of Vadim Makarov (Quantum Hacking Lab, Moscow)





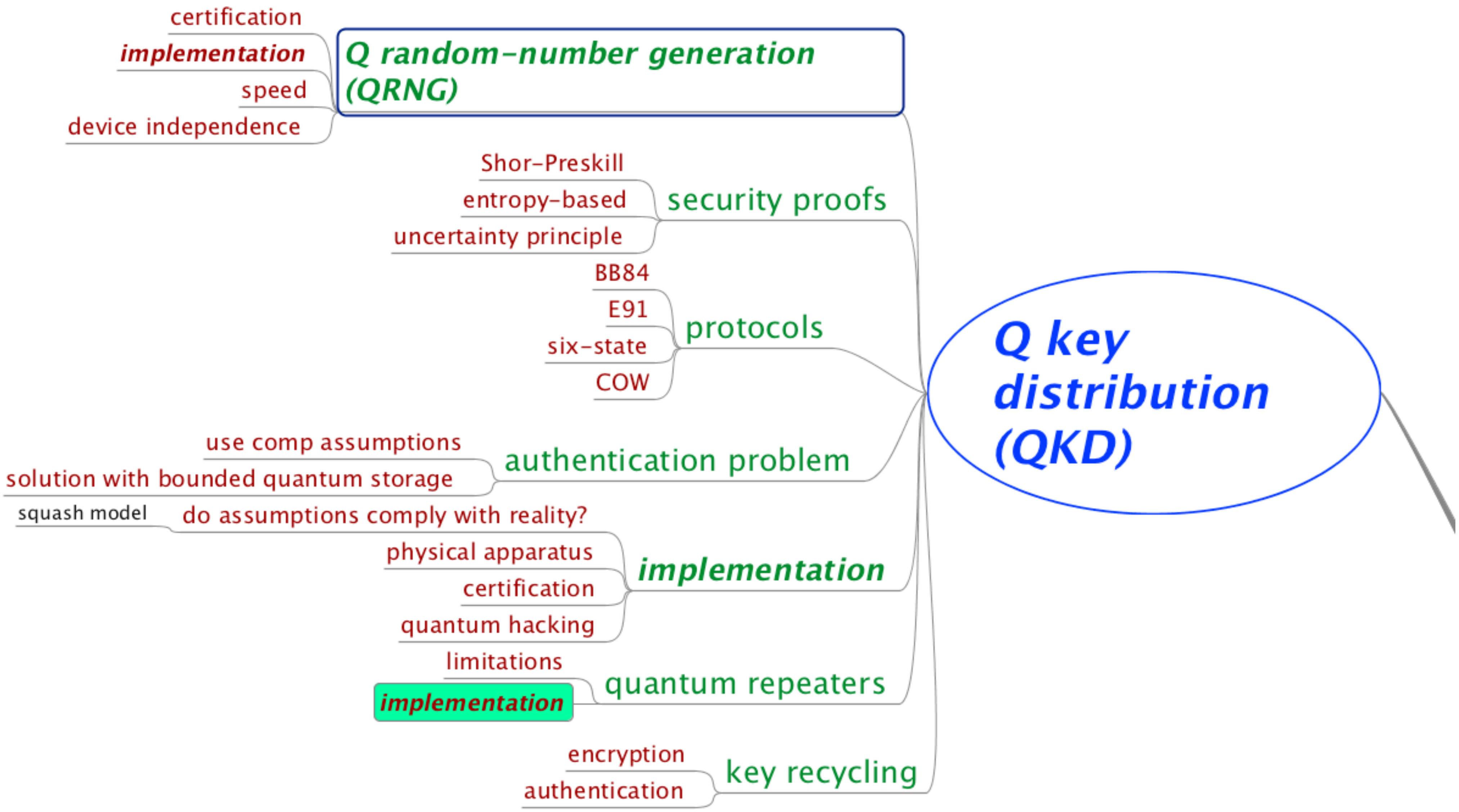
Quantum Key Distribution (QKD)

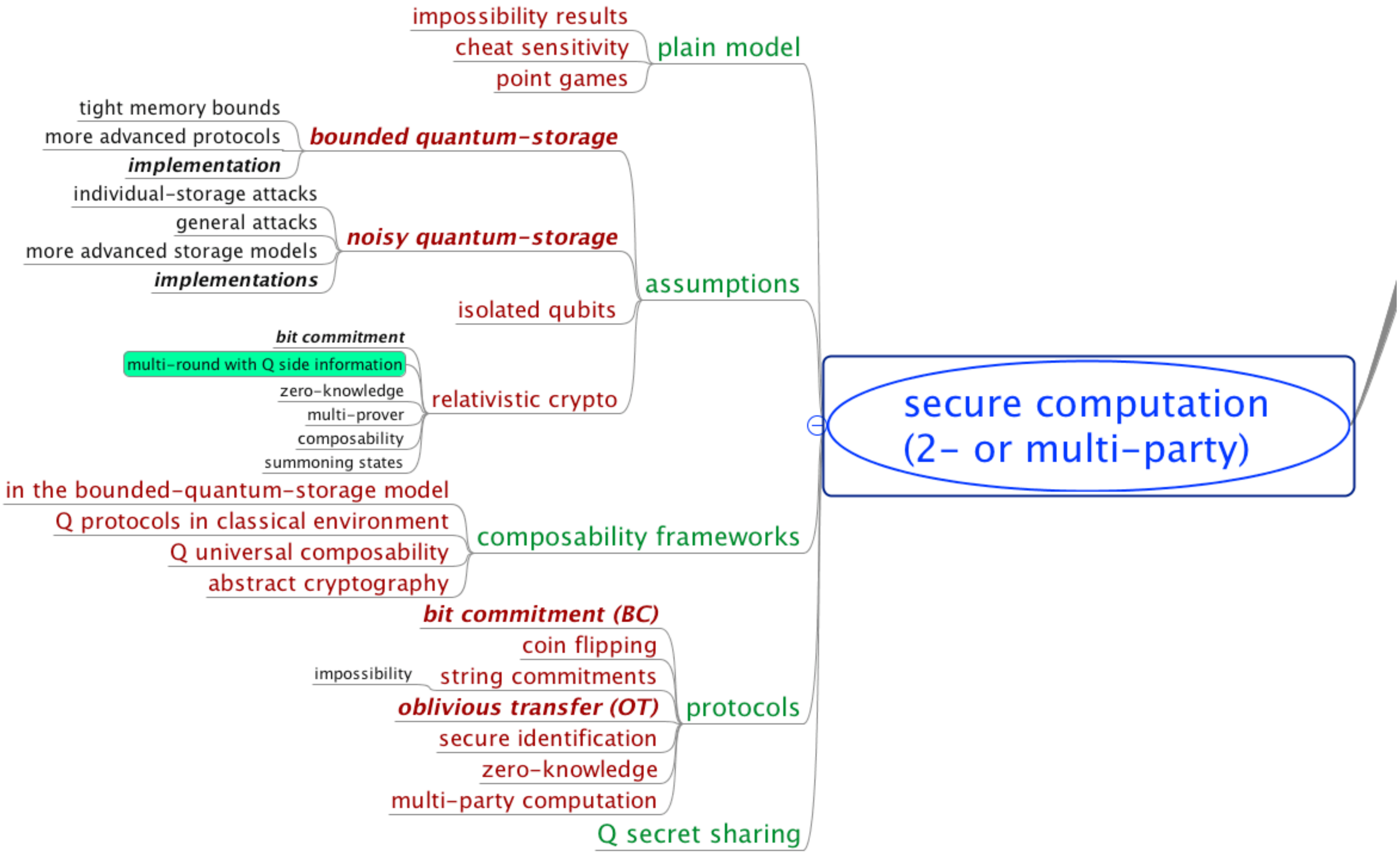
[Bennett Brassard 84]



- **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)

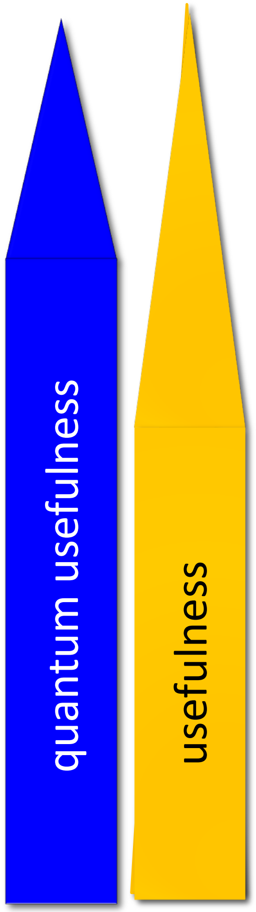




secure computation
(2- or multi-party)
plain model
impossibility results
cheat sensitivity
point games
assumptions
bounded quantum-storage
tight memory bounds
more advanced protocols
implementation
noisy quantum-storage
individual-storage attacks
general attacks
more advanced storage models
implementations
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

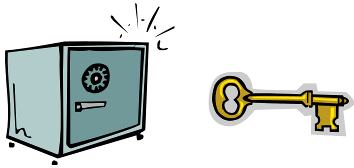
- Information-theoretic security
- No computational restrictions



- Coin-Flipping

$\Uparrow$ $\not\Downarrow$

- Bit Commitment



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

- Oblivious Transfer

$s_0 \rightarrow$ OT $\leftarrow c$
$s_1 \rightarrow$ OT $\rightarrow s_c$

$\Uparrow$ $\Downarrow$

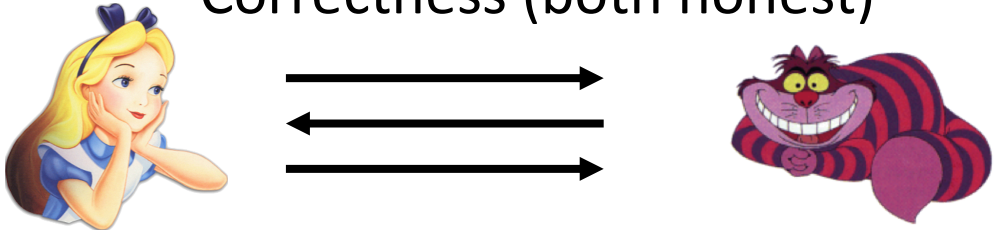
- 2-Party Function Evaluation

$x \rightarrow \mathcal{F} \leftarrow y$
$f(x,y) \leftarrow \mathcal{F} \rightarrow g(x,y)$

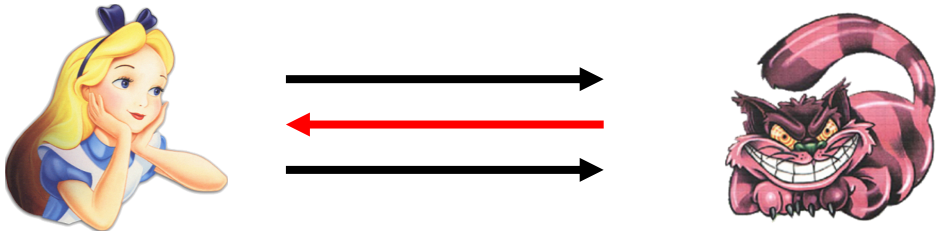
$\Updownarrow$

- Multi-Party Computation (with dishonest majority)

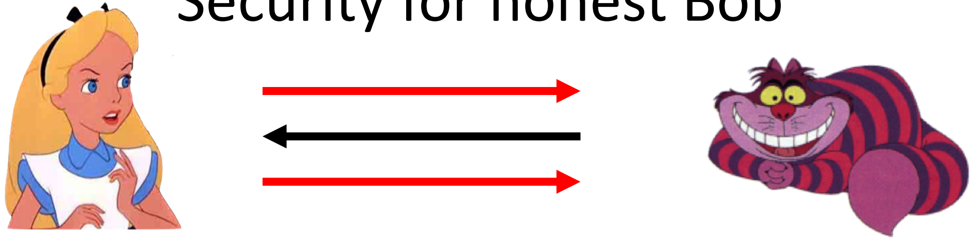
Correctness (both honest)



Security for honest Alice



Security for honest Bob



[Blum 83, Kilian 88]

Coin Flipping (CF)

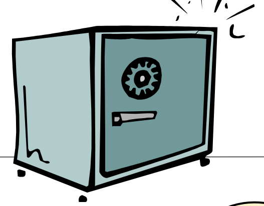
- Strong CF: No dishonest player can bias the outcome
- Classically: a cheater can always obtain his desired outcome with prob 1
- Quantum: [Ambainis 02] Quantum Protocol with bias 0.25

  [Kitaev 03] lower bounds the bias by $\frac{1}{\sqrt{2}} - \frac{1}{2} \approx 0.2$

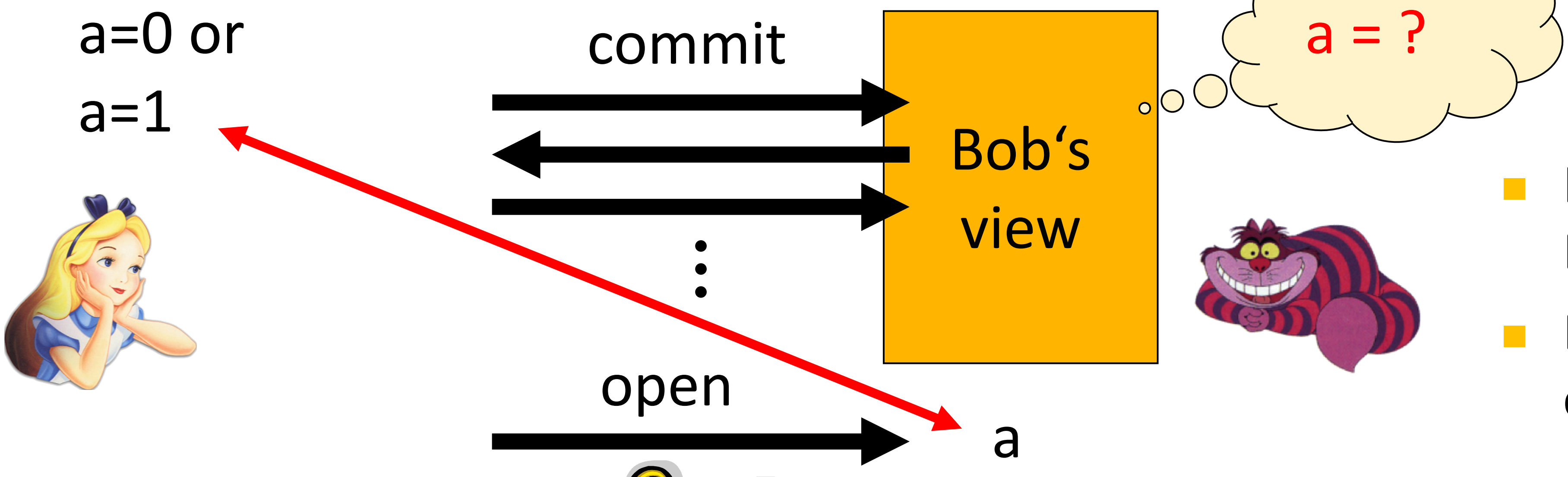
  [Chailloux Kerenidis 09] give optimal quantum protocol for strong CF with this bias

- 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?
- [Arora, Roland, Vlachou, Weis 18/19] explicit protcols

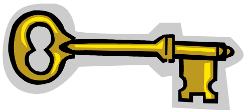
Bit Commitment (BC)



- Two-phase (reactive) protocol:



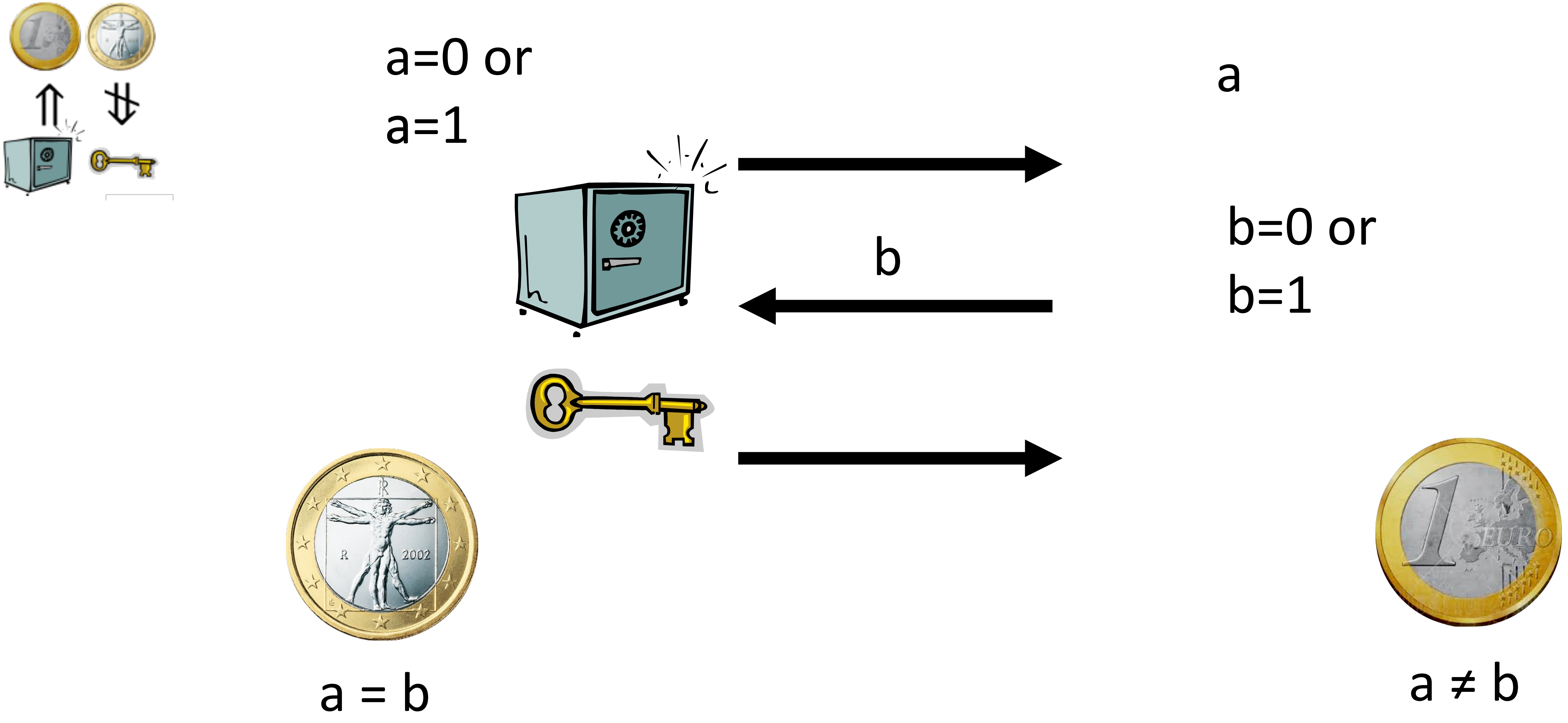
- Hiding: even dishonest Bob does not learn a
- Binding: dishonest Alice cannot change her mind



- 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

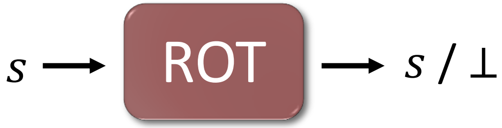


Oblivious Transfer (OT)

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

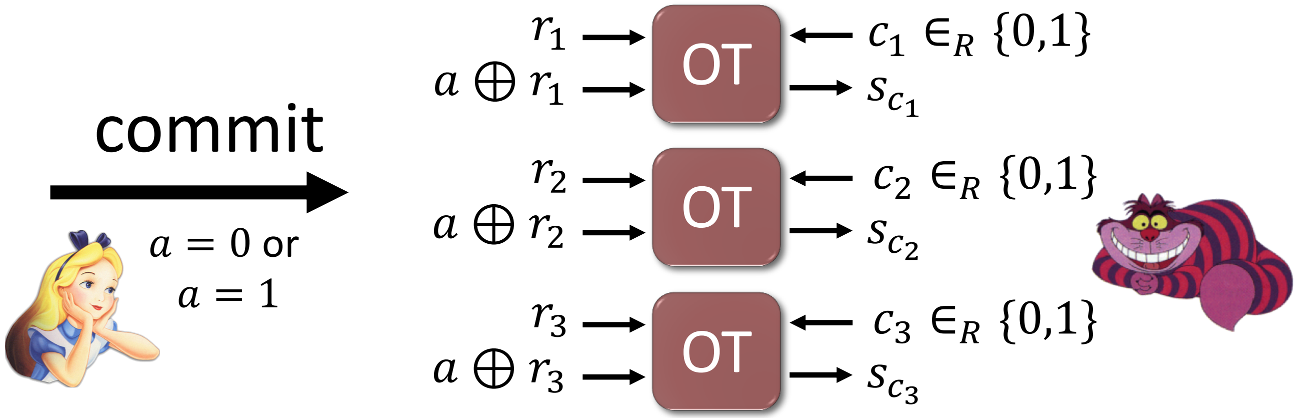
- 1-out-of-2 Oblivious Transfer:

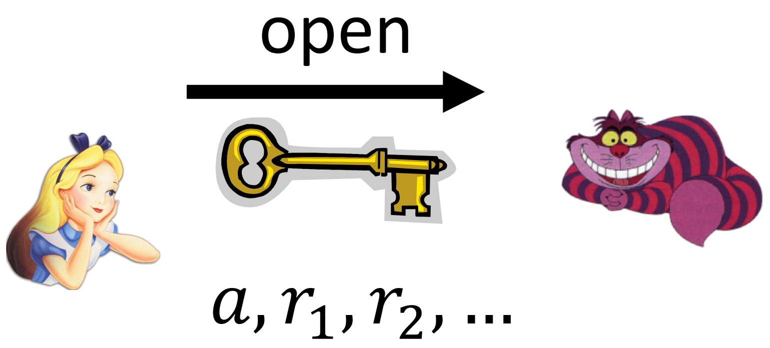
- Rabin OT:
(secure erasure)



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

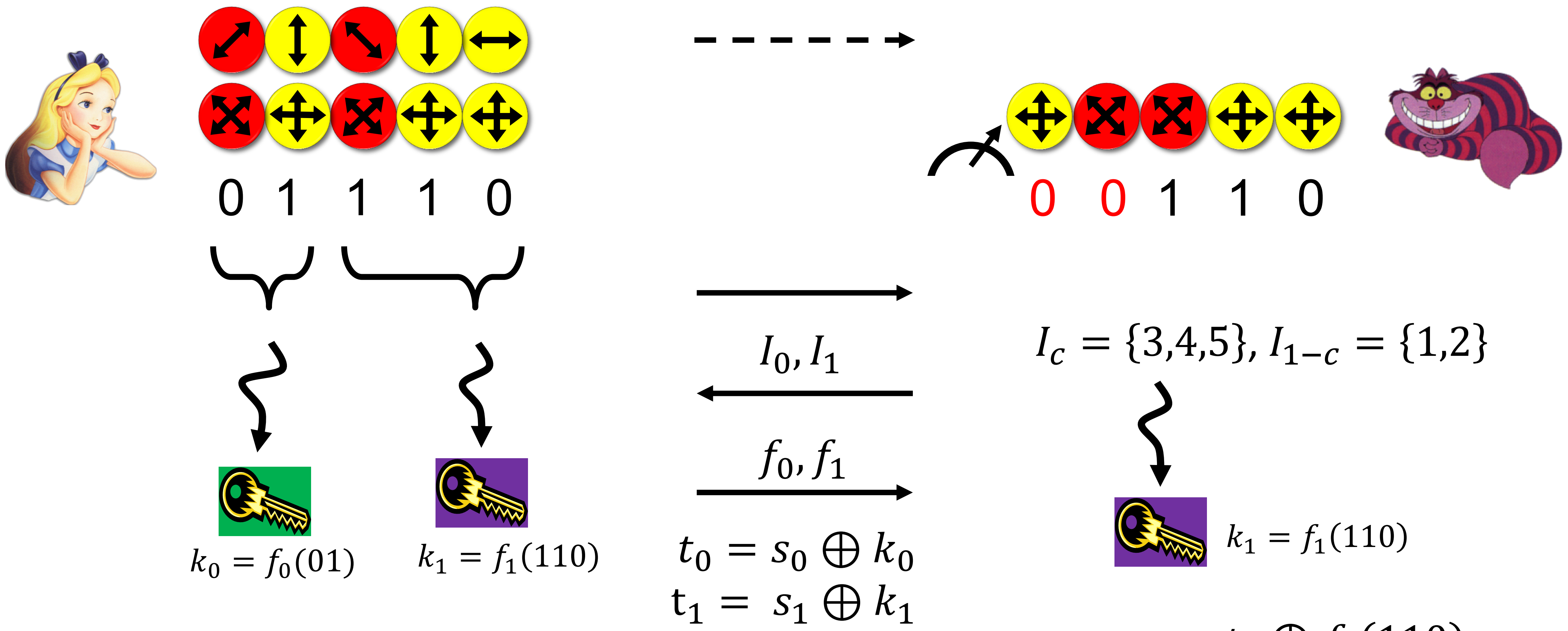
- These OT variants are information-theoretically equivalent (homework!)
- OT is symmetric [Wolf Wullschleger at EuroCrypt 2006, only 10 pages long]
- 1-2 OT ⇒ BC:





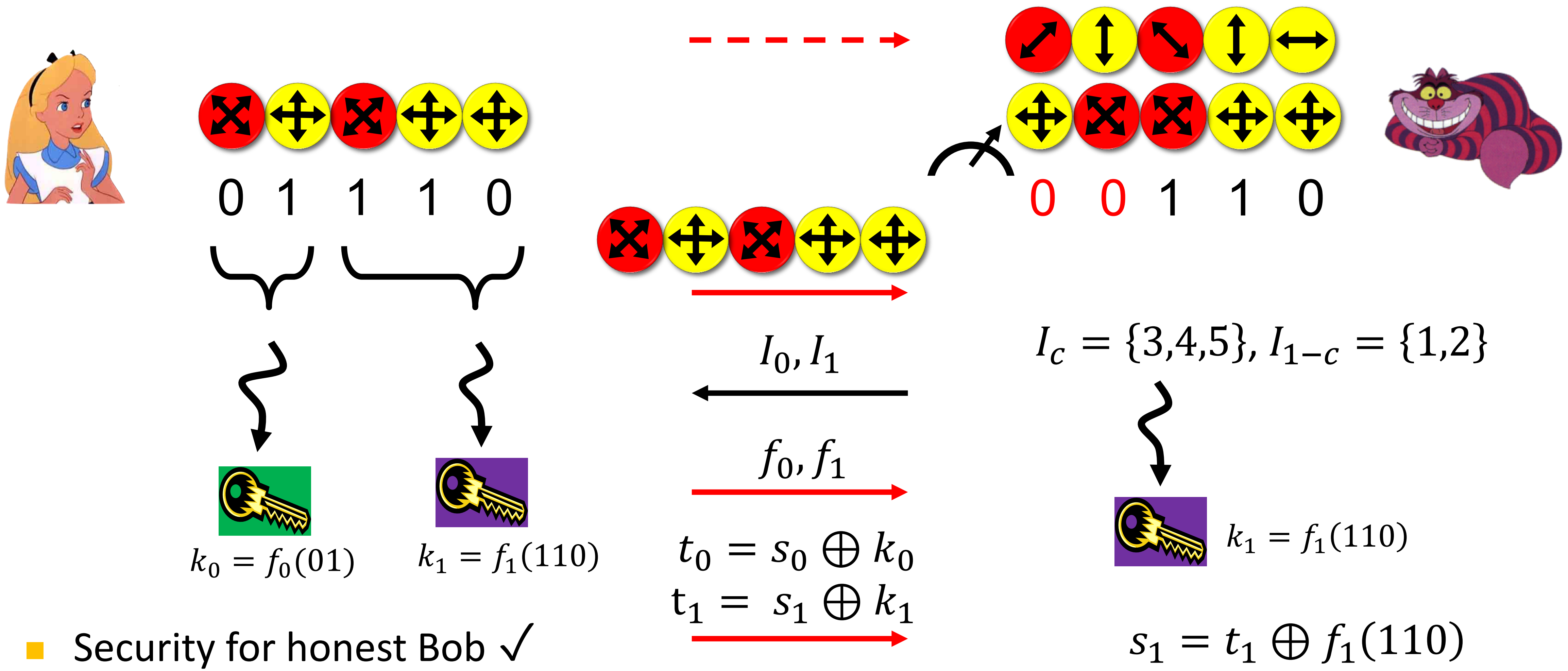
[Wiesner 68, Even Goldreich Lempel 85, Rabin 81]

Quantum Protocol for Oblivious Transfer



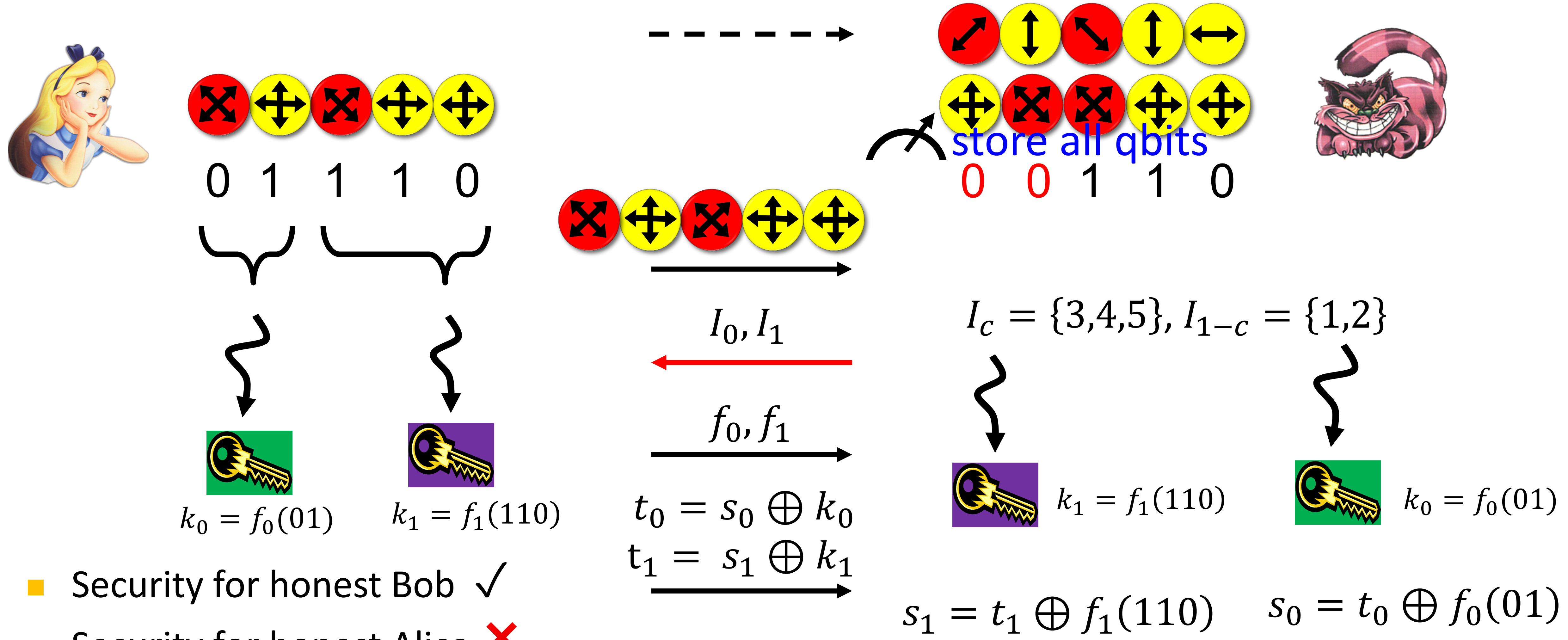
Correctness ✓

Quantum Protocol for Oblivious Transfer



- Security for honest Bob ✓

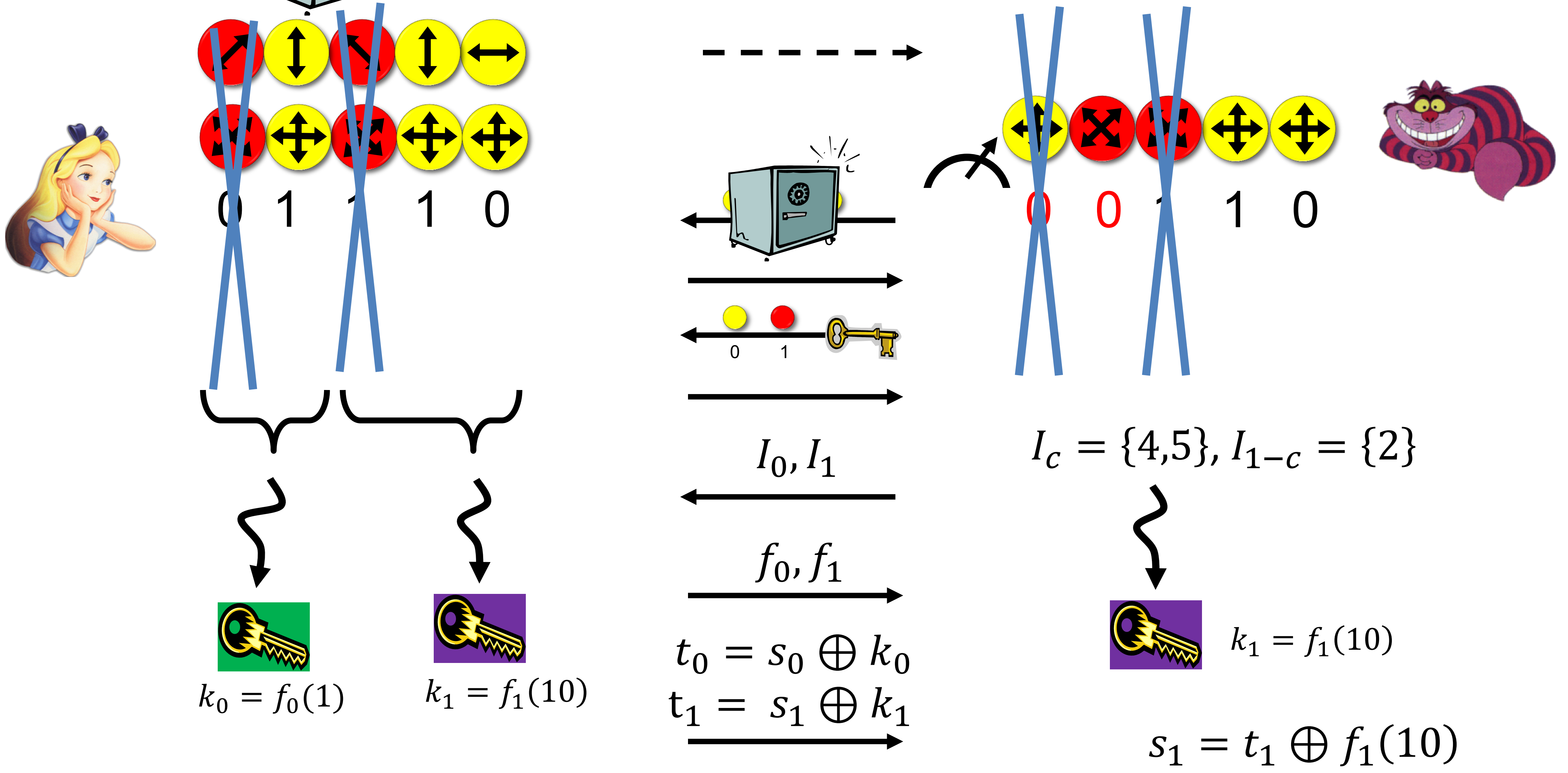
Quantum Protocol for Oblivious Transfer



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

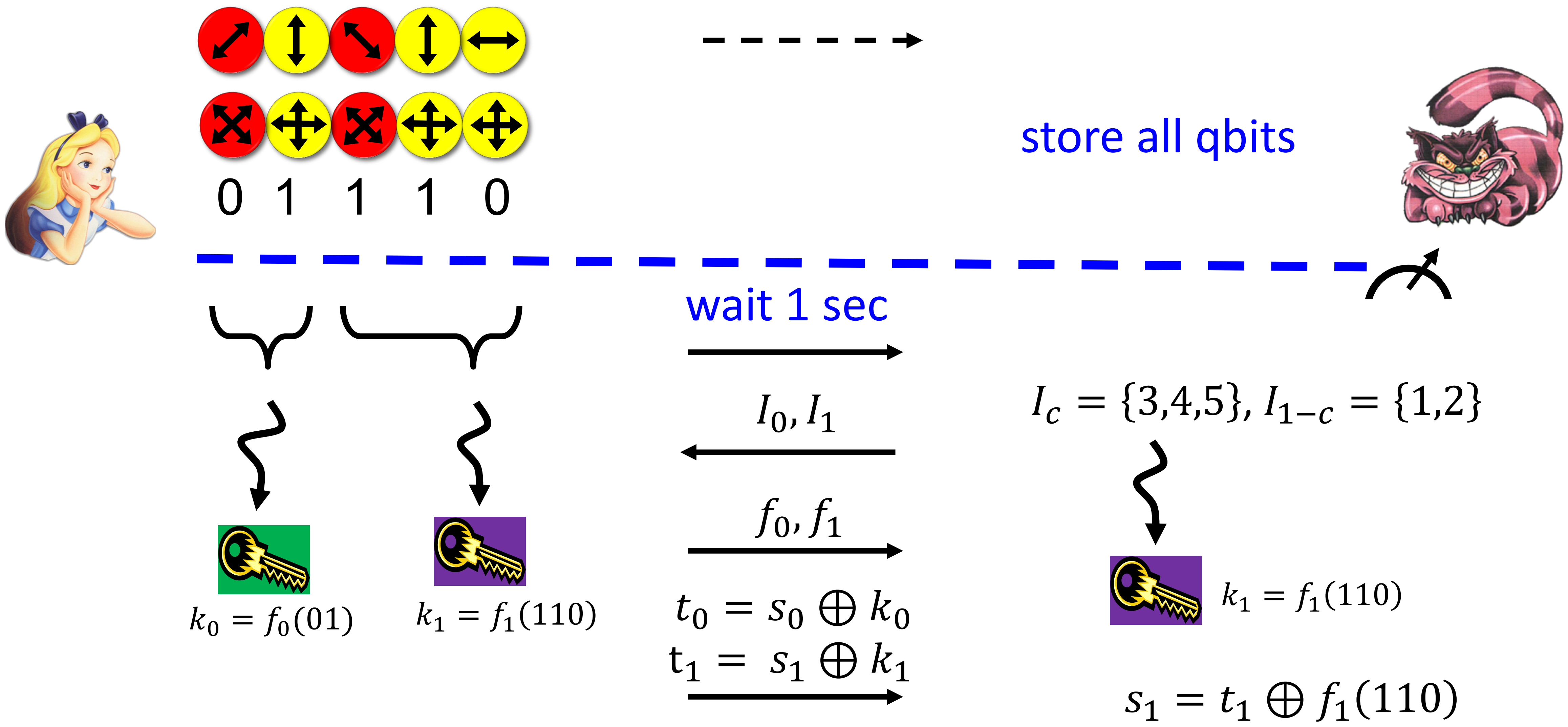
[Wiesner 68, Bennett Brassard Crepeau Skubiszewska 91]

BC ⇒ Oblivious Transfer



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

Limited Quantum Storage



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

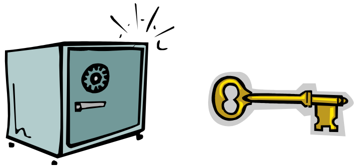
Summary of Quantum Two-Party Crypto

- Information-theoretic security
- No computational restrictions

- Coin-Flipping

$\Uparrow$ $\not\Downarrow$

- Bit Commitment



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

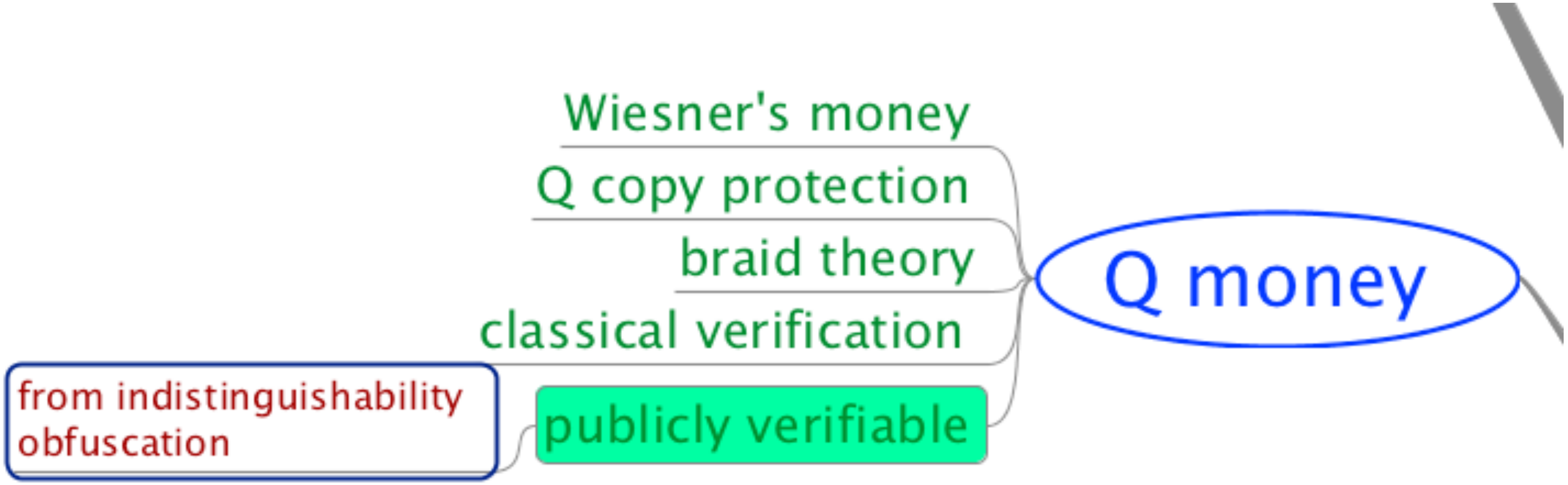
- Oblivious Transfer

$\Uparrow$ $\Downarrow$

- 2-Party Function Evaluation

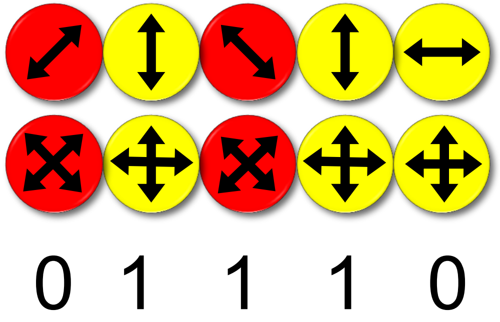
[Blum 83, Kilian 88]

Quantum Money



Conjugate Coding & Quantum Money

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



- Originally proposed for securing quantum banknotes (private-key quantum money)
- Bank holds list of serial numbers with according q states
- The note has to be transferred to the bank for verification
- **Theorem:** Given access to a single authentic bank note, attempts to create two bank notes having the same serial number that independently pass the bank's test for validity have success probability exactly $(3/4)^n$.

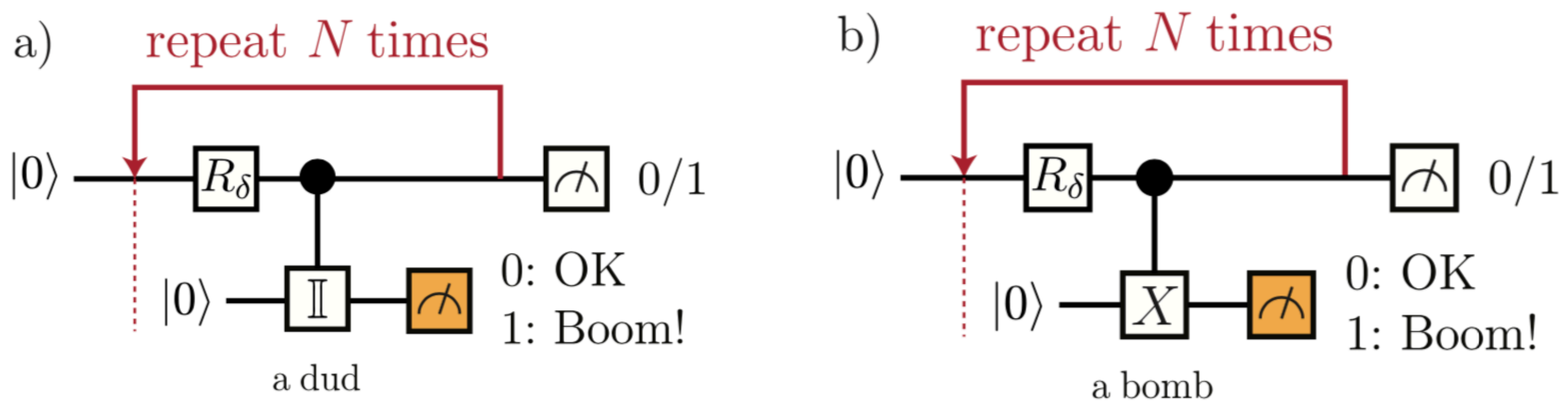
[Wiesner 68, Molina Vidick Watrous 13]

Quantum Money

- **Thm:** Given access to a single authentic bank note, attempts to create two bank notes having the same serial number that independently pass the bank's test for validity have success probability exactly $(3/4)^n$.
- Is it secure?
- No! Other attacks exists!
- For instance, use n EPR pairs on two bank notes with the same serial number, submit one for verification. Verification succeeds with probability p and you have another valid bank note in your hands. What is p?
- Furthermore, if the bank returns invalid bills, attacker can learn individual qubits by asking for validation of $X|\alpha\rangle$.
- Therefore, invalid bills should never be returned by the bank.

[Molina Vidick Watrous 13, Lutomorski 10]

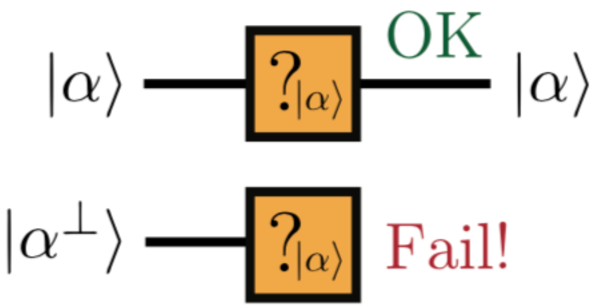
Elitzur-Vaidman's bomb quality tester

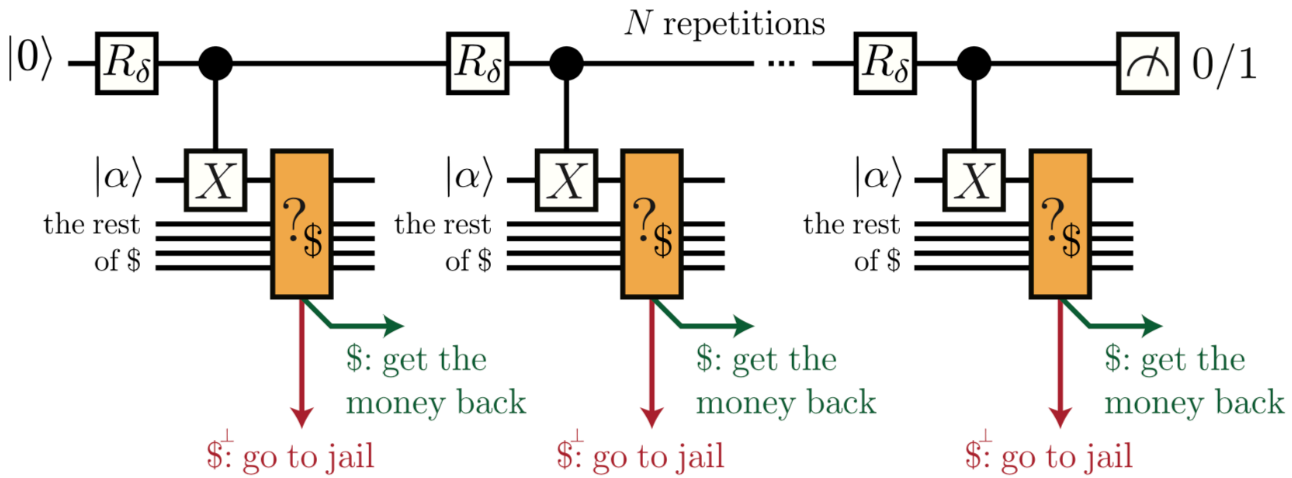


- Pick a large N, small angle $\delta = \frac{\pi}{2N}$, let $R_\delta = \begin{bmatrix} \cos\delta & -\sin\delta \\ \sin\delta & \cos\delta \end{bmatrix}$ be a counterclockwise rotation by δ.
- a) After first round: $(\cos\delta\,|0\rangle + \sin\delta|1\rangle)\,|0\rangle$, after N rotations: $|1\rangle|0\rangle$
- b) After first round: $(\cos\delta\,|0\rangle|0\rangle + \sin\delta|1\rangle|1\rangle)$. Prob of explosion: $\sin^2\delta$
- If no explosion, collapse back to $|0\rangle|0\rangle$, and start again
- After N rounds of rotation and tests: $|0\rangle|0\rangle$
- Overall prob of no explosion: $(1-\sin^2\delta)^N \geq 1 - \frac{\pi^2}{4N}$

[Elitzur Vaidman 93, figures from Brodutch Nagaj Sattath Unruh 14]

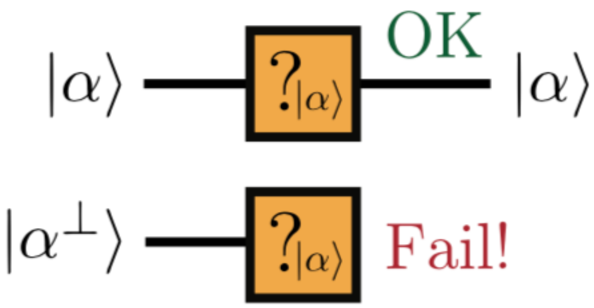
Bomb Testing to Counterfeit Q Money

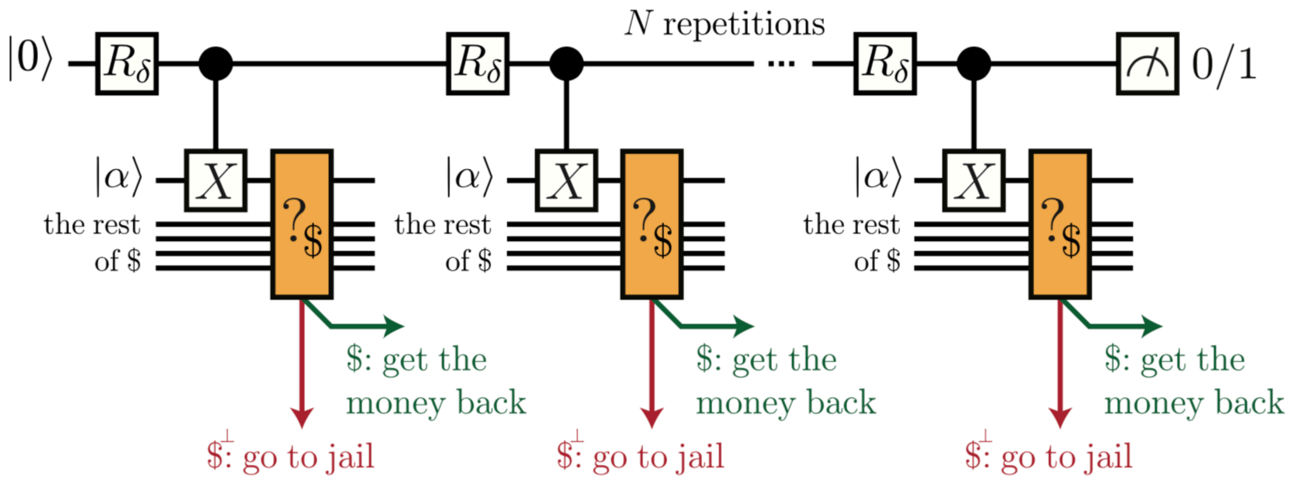




- Pick a large N, small angle $\delta = \frac{\pi}{2N}$, let $R_\delta = \begin{bmatrix} \cos\delta & -\sin\delta \\ \sin\delta & \cos\delta \end{bmatrix}$
- For $|\alpha\rangle = |0\rangle$ or $|1\rangle$, we are in the "bomb" case from before. Validation flips the state back to what it was, the probe does not rotate. Final outcome: 0
- For $|\alpha\rangle = |+\rangle$, an X operation does nothing, the probe is rotated by δ. Final outcome: 1
- For $|\alpha\rangle = |-\rangle$, one can check that for an even N, the final outcome is 0, and money is never rejected.

Bomb Testing to Counterfeit Q Money





- Hence, we can identify $|\alpha\rangle = |+\rangle$.
- $|\alpha\rangle = |-\rangle$ can be identified using controlled – X operation
- Otherwise, simply measure in the computational basis
- Hence we can identify all n qubits using at most $2n \times N$ adaptive queries to a strict tester
- Prob that attack succeeds: $\left(1 - \frac{\pi^2}{4N}\right)^{2n} \geq 1 - \frac{\pi^2 n}{2N}$

[Brodutch Nagaj Sattath Unruh 14]

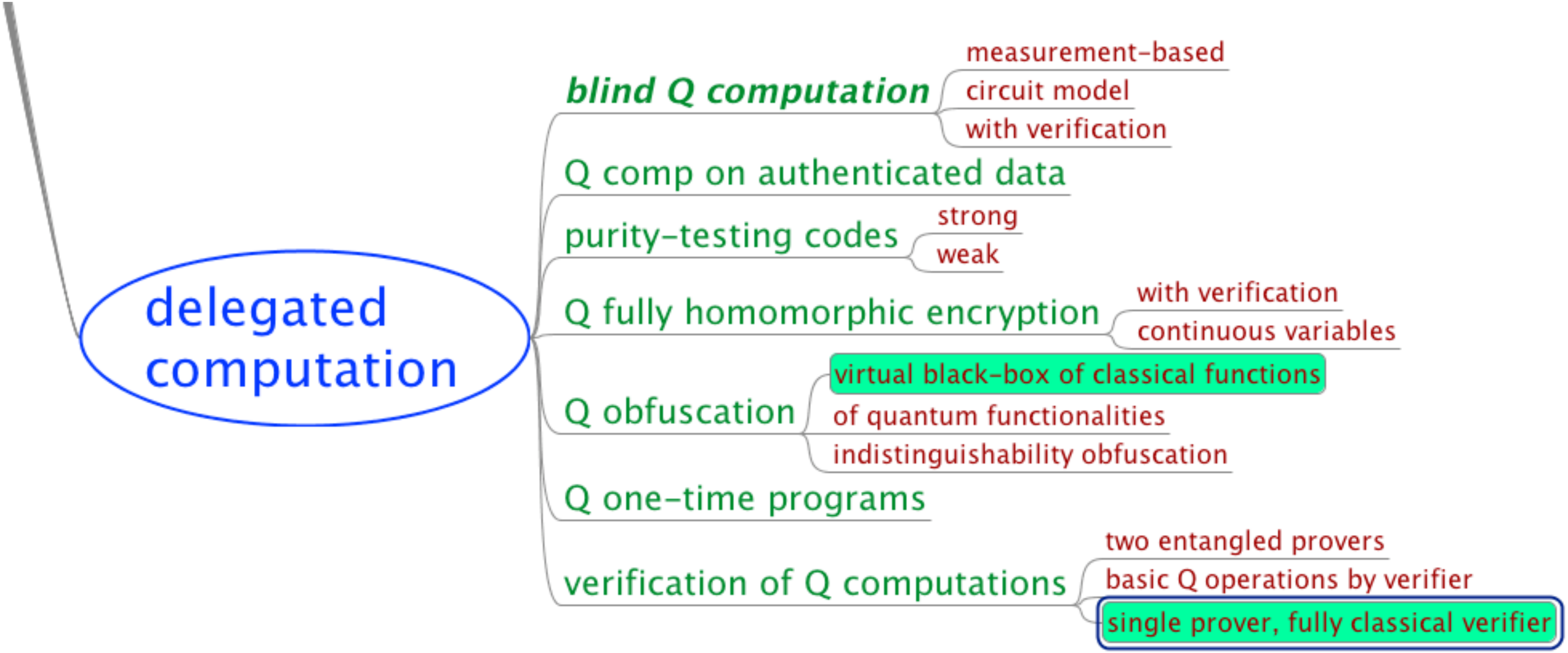
More practical Q Money

- Drawback of Wiesner's money: needs quantum interaction with bank
- Classically verifiable: bank sends basis string, client responds, bank checks
- **Theorem:** The probability that a counterfeiter succeeds in two independent classical verifications with the bank, given access to a single valid bank note is exactly $\left(\frac{3}{4}+\frac{\sqrt{2}}{8}\right)^n \approx (0.927)^n$.

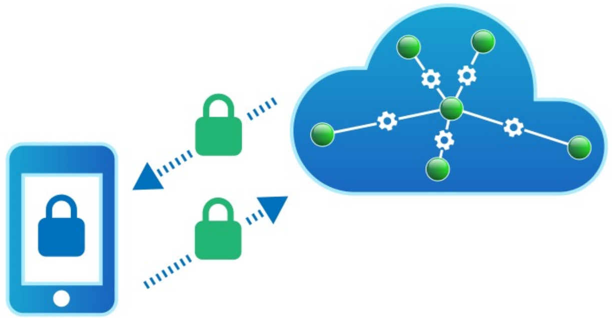
- In practice, one would like to have Q money schemes with **public verifiability**
- Several schemes were proposed **and broken** by Aaronson, Christiano, Lutomirski, Gosset, Kelner, Hassidim, Shor, Farhi, Pena, Faugere, Perret, Zhandry17, …
- Latest proposal by Shor
- Good overview in Chapters 8 and 9 of lecture notes by Aaronson.

[Molina Vidick Watrous 13, Aaronson 09, …]

Delegated Q Computation



Delegated Computation

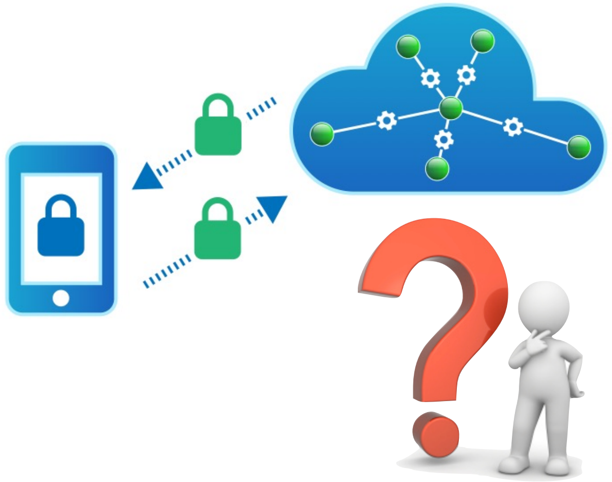


- QCloud Inc. promises to perform a BQP computation for you.
- How can you securely delegate your quantum computation to an untrusted quantum prover while maintaining privacy and/or integrity?
- Various parameters:
  1. Quantum capabilities of verifier: state preparation, measurements, q operations
  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

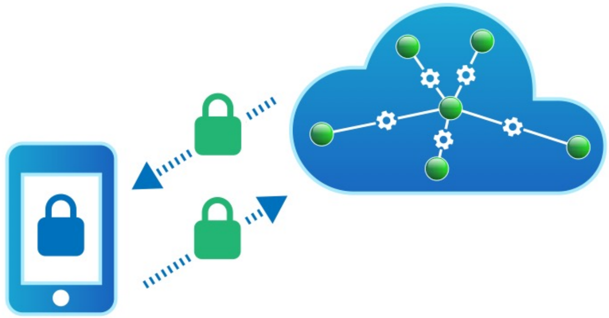
Classical Verification of Q Computation



- 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]

Classical Verification of Q Computation

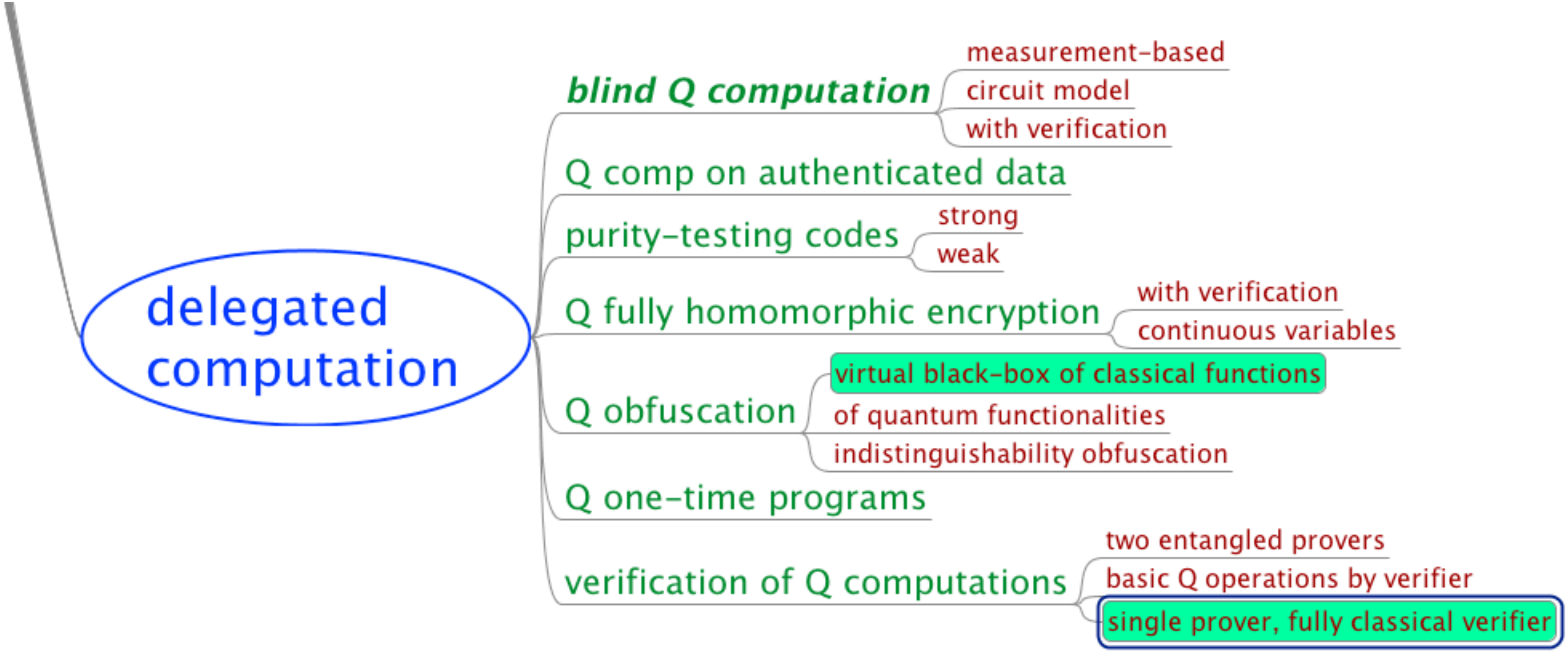


- QCloud Inc. promises you to perform a BQP computation
- How can a **purely classical verifier** be convinced that this computation actually was performed?

- [Mahadev18] Classical verification of Q Computations
- [Mahadev18] Quantum fully homomorphic encryption

- Verifiable quantum fully homomorphic encryption?

Delegated Q Computation



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

Cryptoplexity
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