Quantum Computation & Cryptography
Day 4

Quantum cryptography

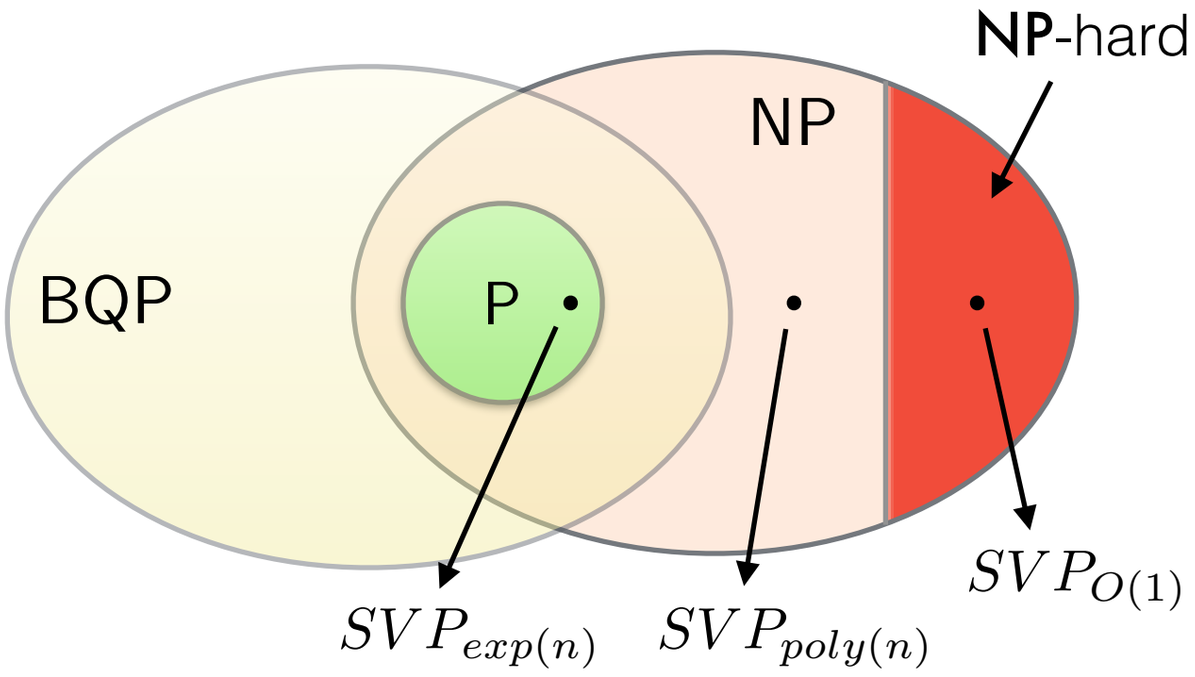
Andru Gheorghiu

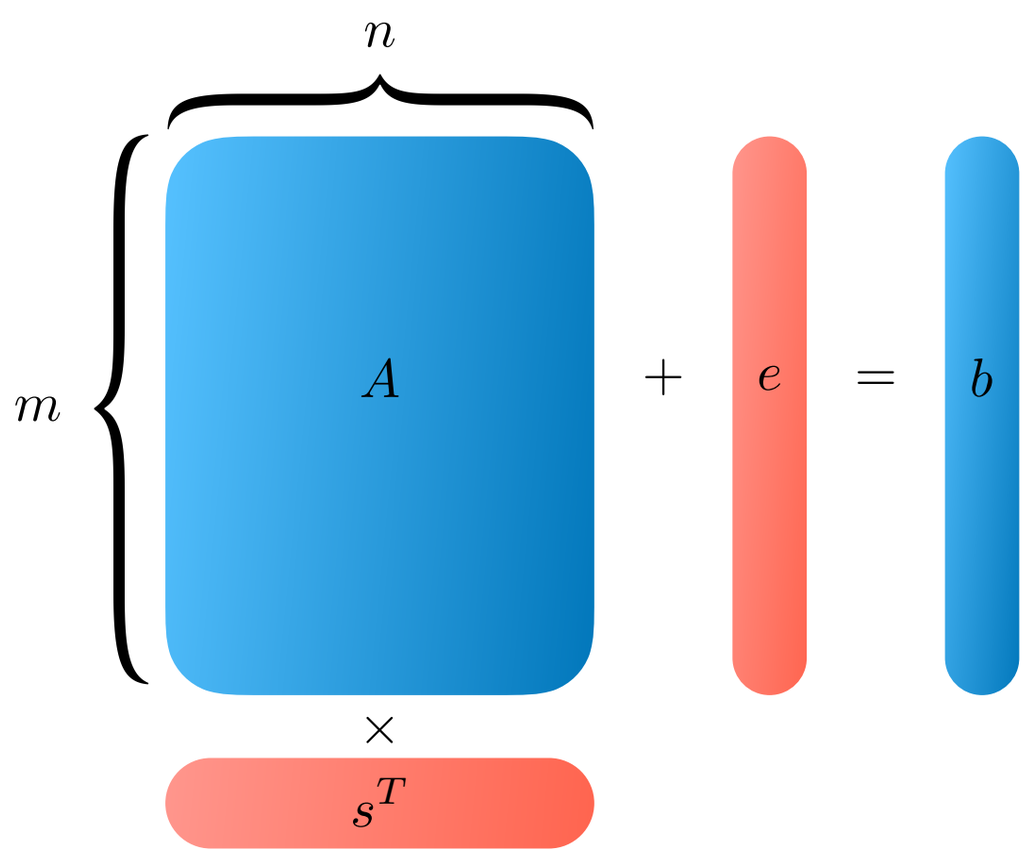
Recap

Post-quantum crypto

Using problems that are hard for QC

Lattice problems and LWE





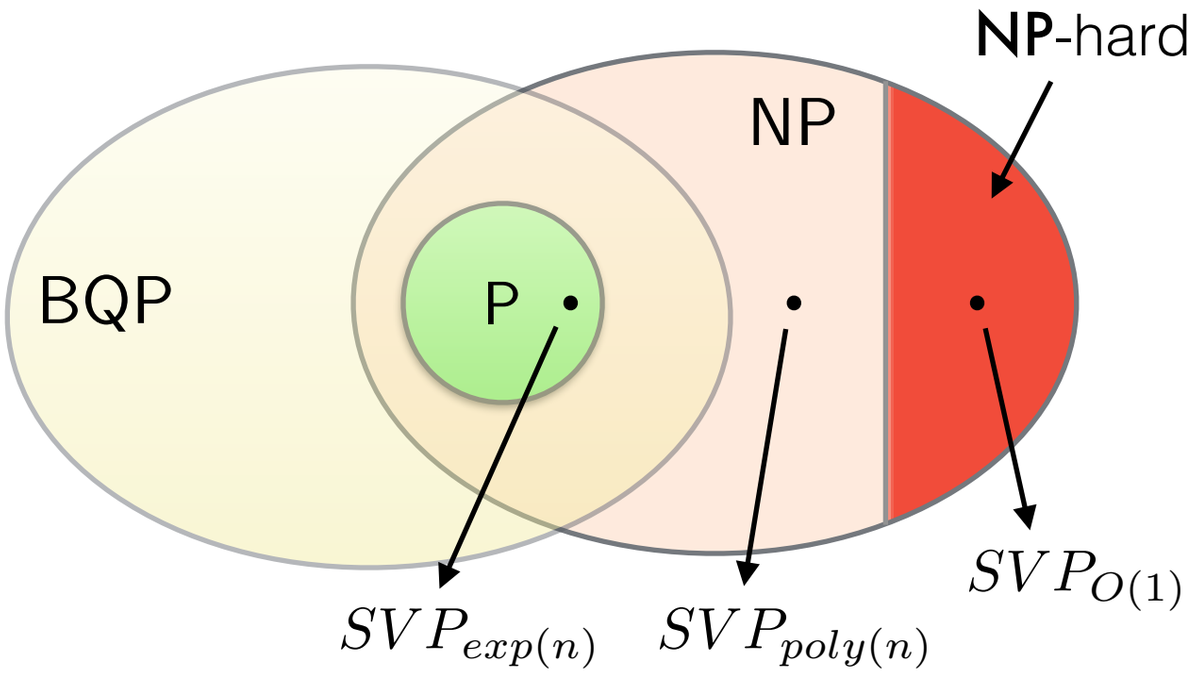
Recap

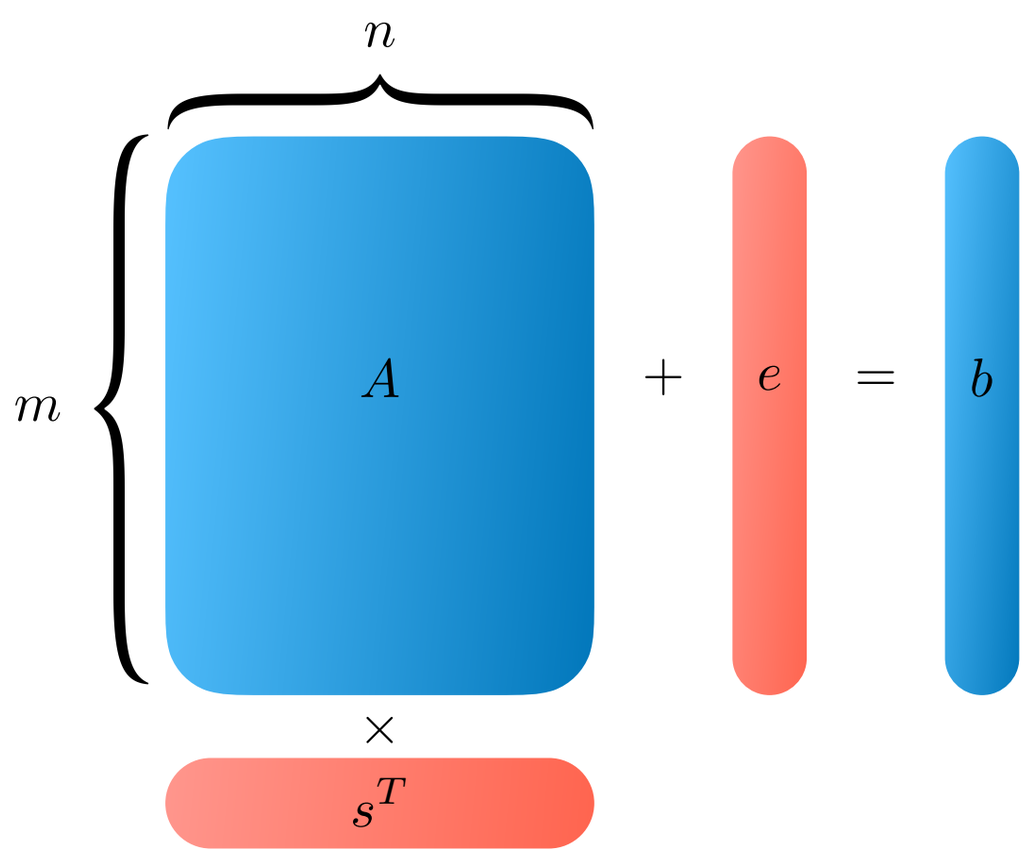
Post-quantum crypto

Using problems that are hard for QC

Lattice problems and LWE

$$\text{worst case } SVP_{poly(n)} \leq_Q \text{ average case } LWE \leq \text{ crypto}$$





The post-quantum problem

"Even if a classical protocol is proven secure based on the hardness of some problem, and that problem is hard even for quantum computers, we have no guarantee that the protocol is secure against quantum computers" - **Dominique Unruh**

Why?

$$\text{average case LWE} \leq \text{crypto}$$

The reduction might not hold against quantum adversaries

How is this reduction performed?

Hard problem to crypto reduction

$$\text{problem X} \leq \text{protocol P}$$

Typically, in security proofs, one shows the following

If adversary A can break security of protocol P, then one can construct an algorithm B that solves X

B can use A as a subroutine

B also has access to A's memory

Rewinding proof

Hard problem to crypto reduction

Rewinding proof

B runs A and copies the content of its memory

B then *rewinds* A to a previous point in the computation

B changes A's input/memory at that point and runs it again

This does not work if A is a quantum algorithm!

Quantum information cannot be copied, in general!

The post-quantum problem

"Even if a classical protocol is proven secure based on the hardness of some problem, and that problem is hard even for quantum computers, we have no guarantee that the protocol is secure against quantum computers" - **Dominique Unruh**

What can we do?

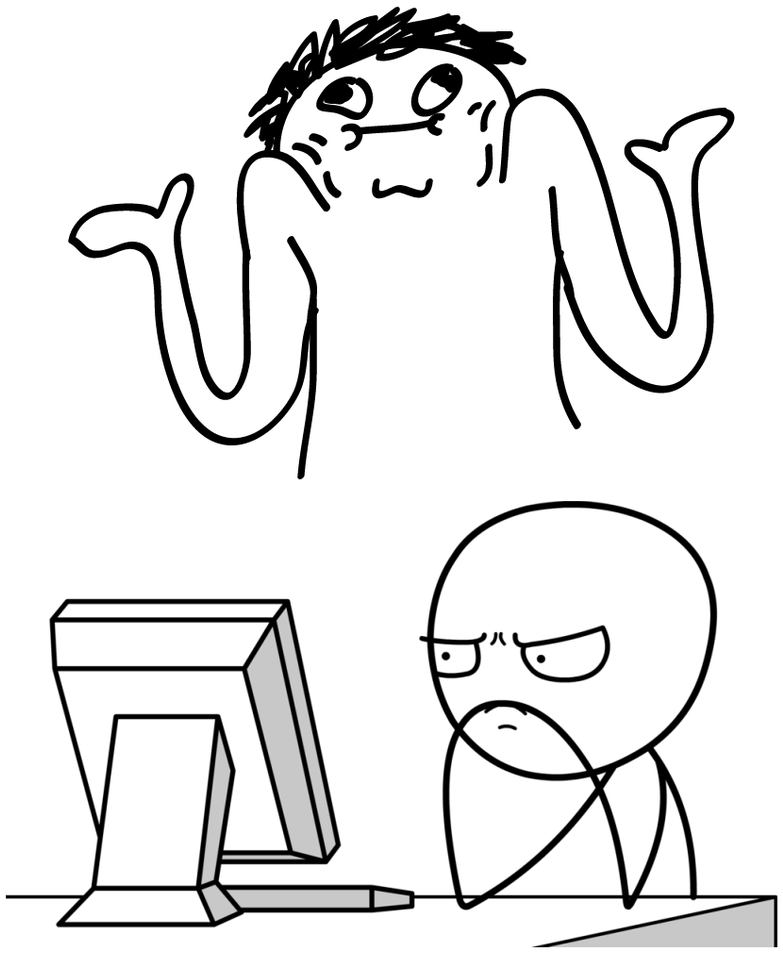
Better proofs

(this is the case for most LWE-based applications)

Quantum cryptography

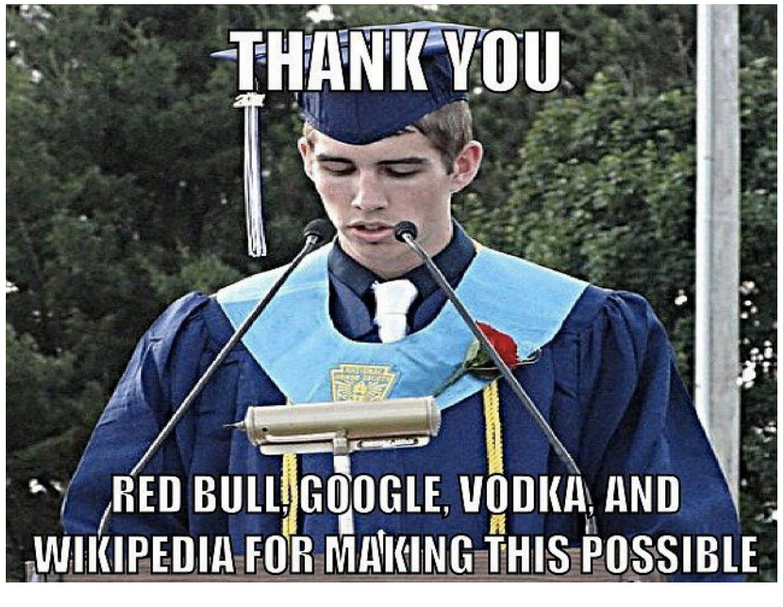
Learning

Prior state, uncertainty



Information updating, learning

Posterior state, reduced uncertainty



Learning

Bayesian inference

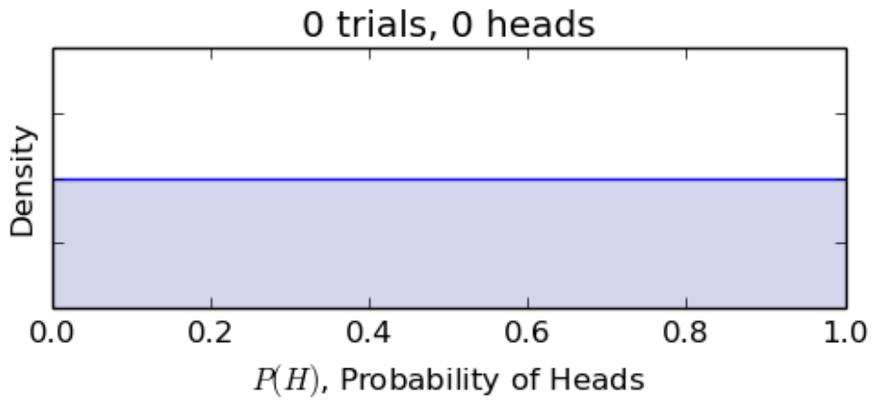
$$Pr(A|B) = \frac{Pr(B|A)Pr(A)}{Pr(B)}$$

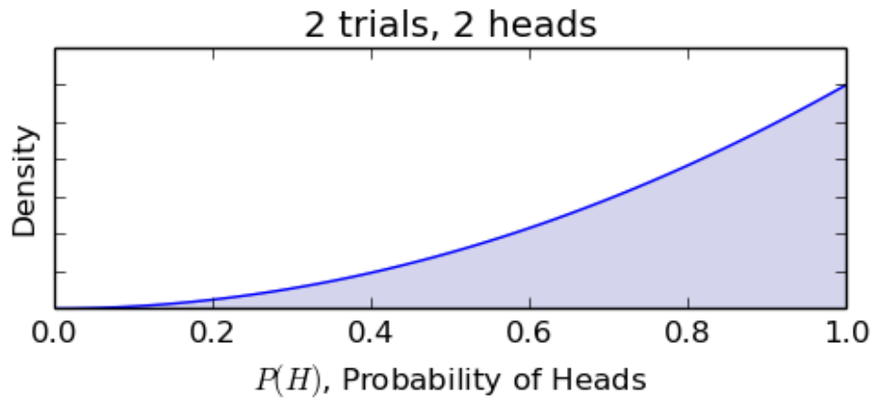
Given some data, find best hypothesis that fits the data

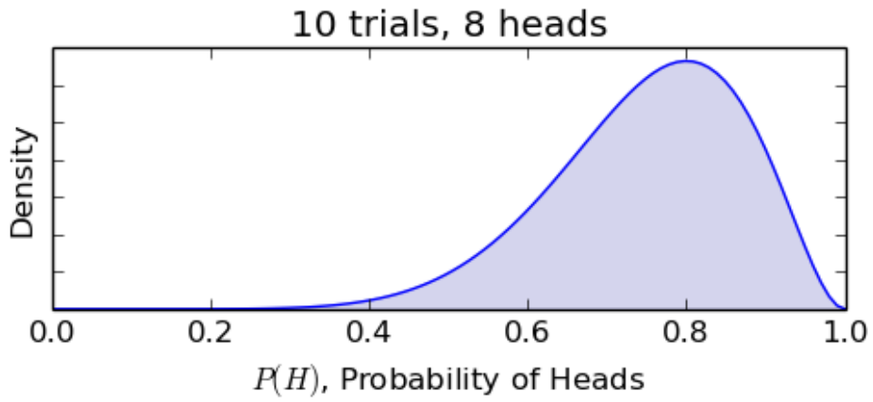
$$Pr(hypothesis|data) = \frac{Pr(data|hypothesis)Pr(hypothesis)}{Pr(data)}$$

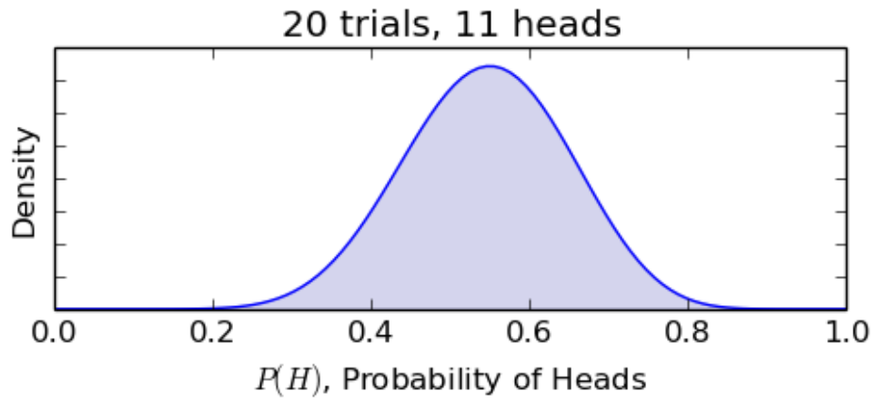
$$\underbrace{Pr(hypothesis|data)}_{\text{Posterior}} \approx \underbrace{Pr(data|hypothesis)}_{\text{Likelihood}} \underbrace{Pr(hypothesis)}_{\text{Prior}}$$

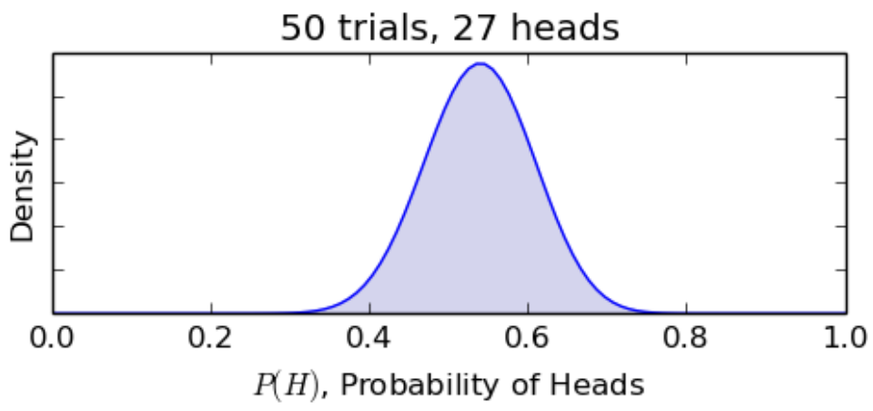
Learning

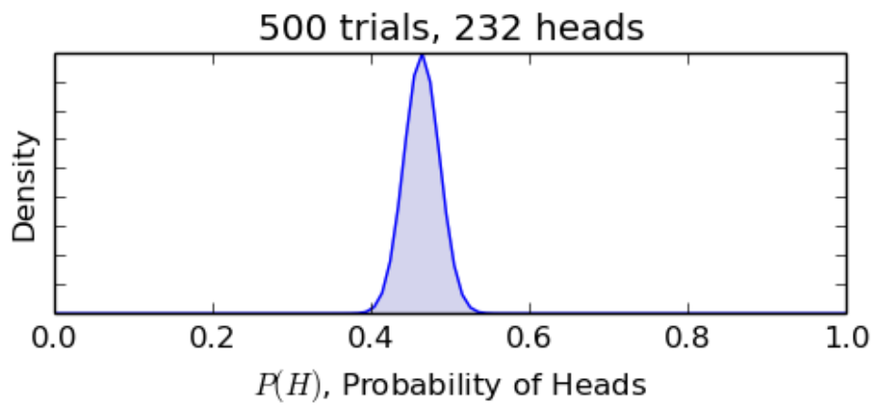

0 trials, 0 heads
Density
0.0
0.2
0.4
0.6
0.8
1.0
$P(H)$, Probability of Heads


2 trials, 2 heads
Density
0.0
0.2
0.4
0.6
0.8
1.0
$P(H)$, Probability of Heads


10 trials, 8 heads
Density
0.0
0.2
0.4
0.6
0.8
1.0
$P(H)$, Probability of Heads


20 trials, 11 heads
Density
0.0
0.2
0.4
0.6
0.8
1.0
$P(H)$, Probability of Heads


50 trials, 27 heads
Density
0.0
0.2
0.4
0.6
0.8
1.0
$P(H)$, Probability of Heads


500 trials, 232 heads
Density
0.0
0.2
0.4
0.6
0.8
1.0
$P(H)$, Probability of Heads

Learning vs. cryptography

Learning and cryptography are dual to each other

Learning — Design algorithms that can efficiently find models for observed data

Cryptography — Design protocols to encrypt data such that no efficient algorithm can learn anything about it

Let’s remove the “efficiency” condition

Information-theoretic security

Let PM denote the set of **physical machines**

I.e. machines that operate according to the laws of physics

No restriction on run-time

$$\forall A \in PM$$

Given any two messages M_1 and M_2 it must be that

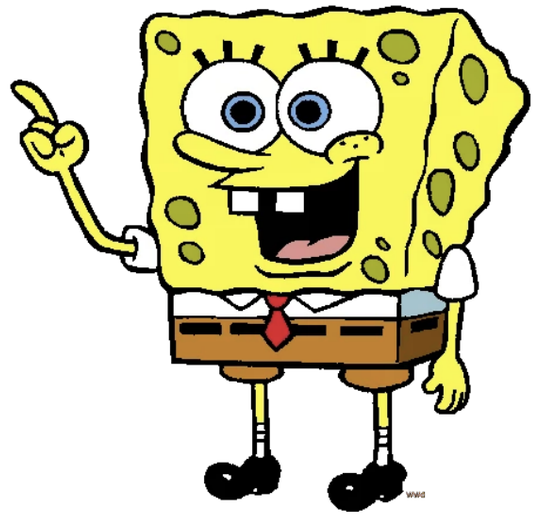
$$Pr[A(Enc(M_1)) = 1] \approx Pr[A(Enc(M_2)) = 1]$$

Equivalently, we can simply write

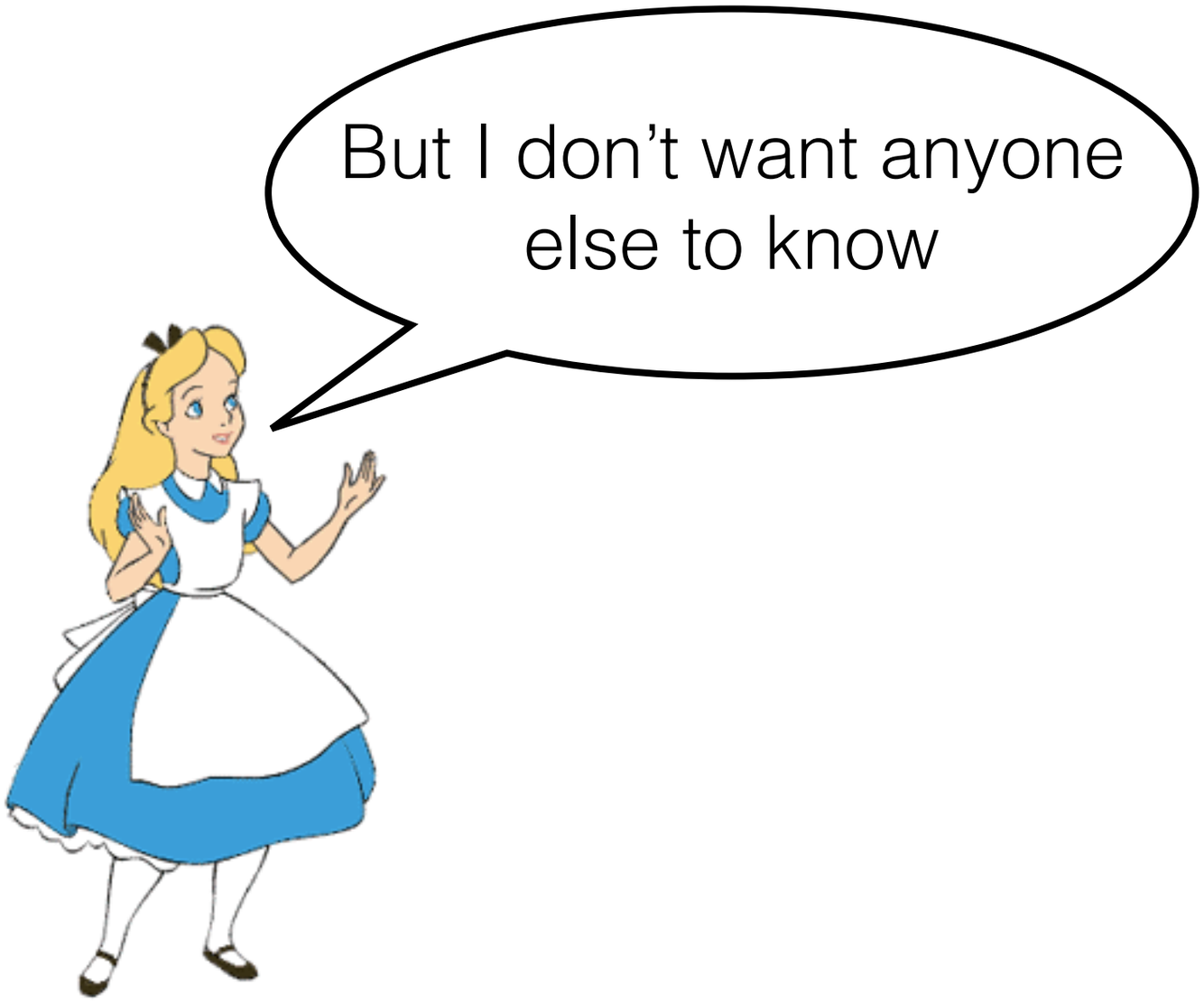
$$Pr[M_1|Enc(M_1)] \approx Pr[M_2|Enc(M_1)]$$

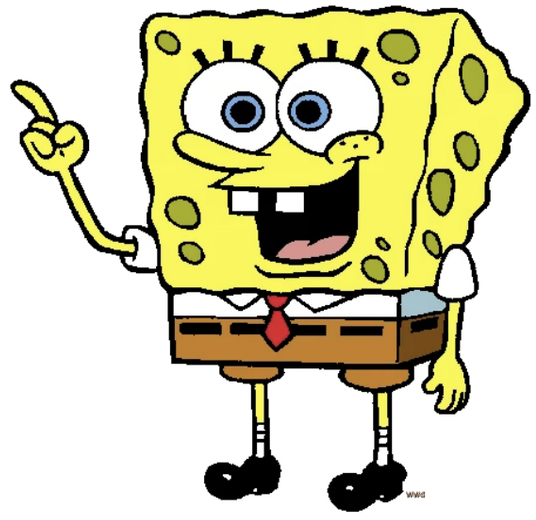
Are there classical protocols with IT security?

One-time pad (OTP)

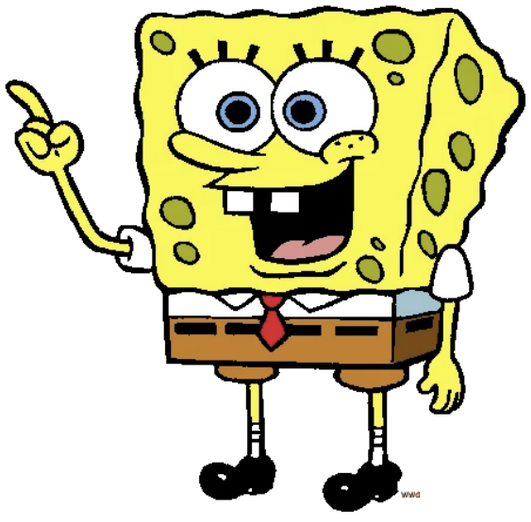


One-time pad (OTP)



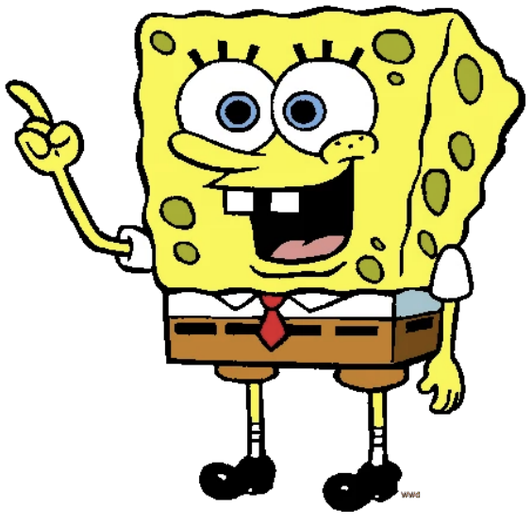


One-time pad (OTP)



$M =$ The Last Jedi was ...

One-time pad (OTP)

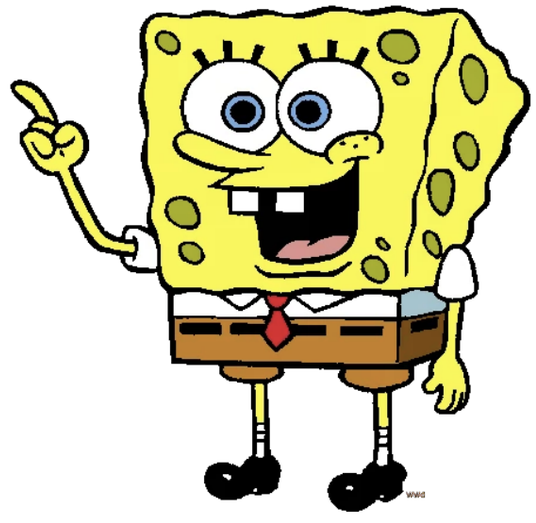


$$M = 01010111101100100110 1$$

One-time pad (OTP)

$$K, M$$

$$|K| = |M|$$



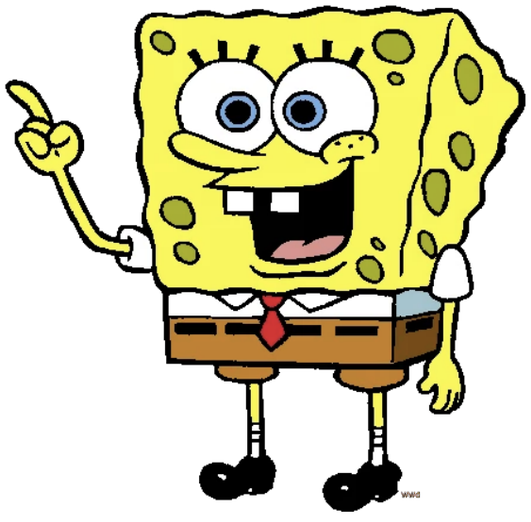
$$K$$

K is essentially random

One-time pad (OTP)

K, M

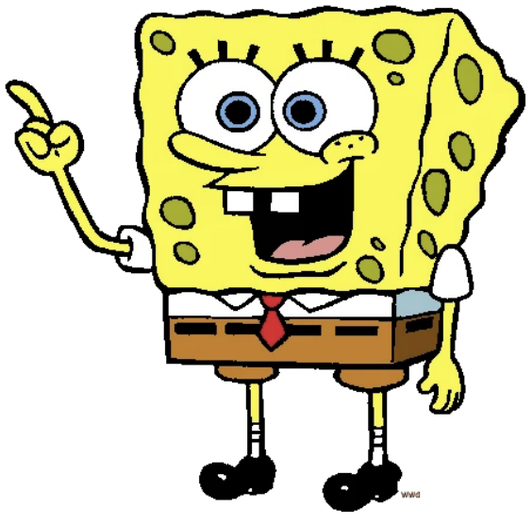
$$S = K \oplus M$$



K

One-time pad (OTP)

K, M

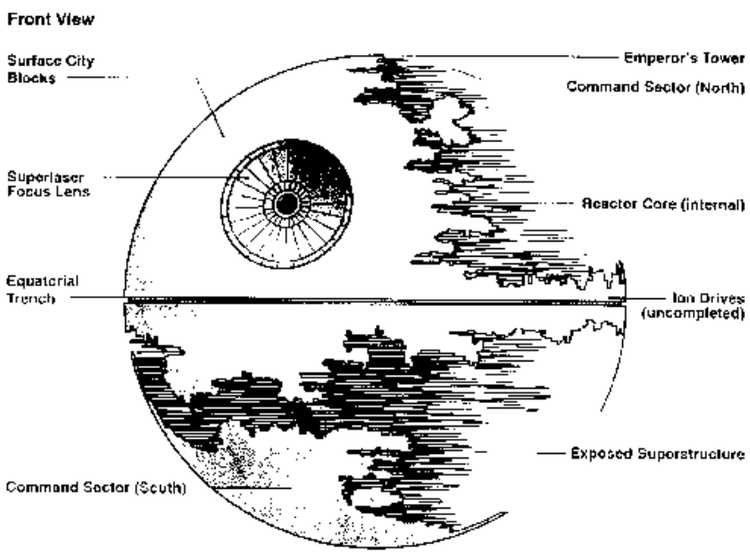


K

$S \oplus K = M$

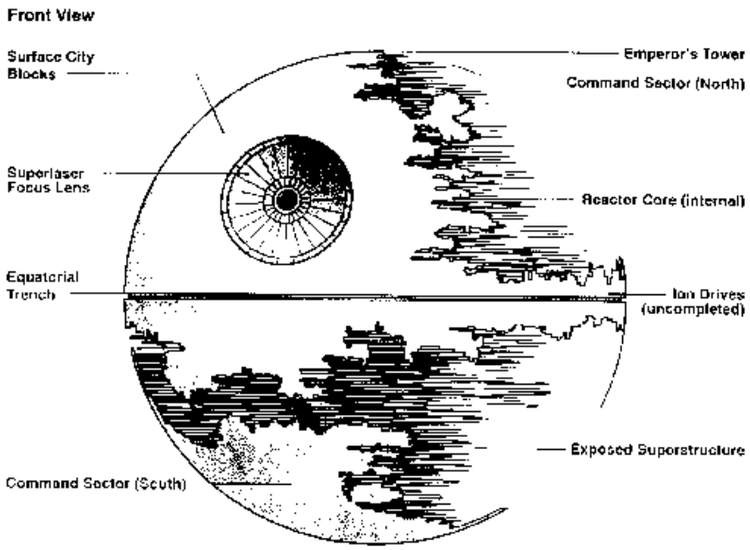
One-time pad (OTP)

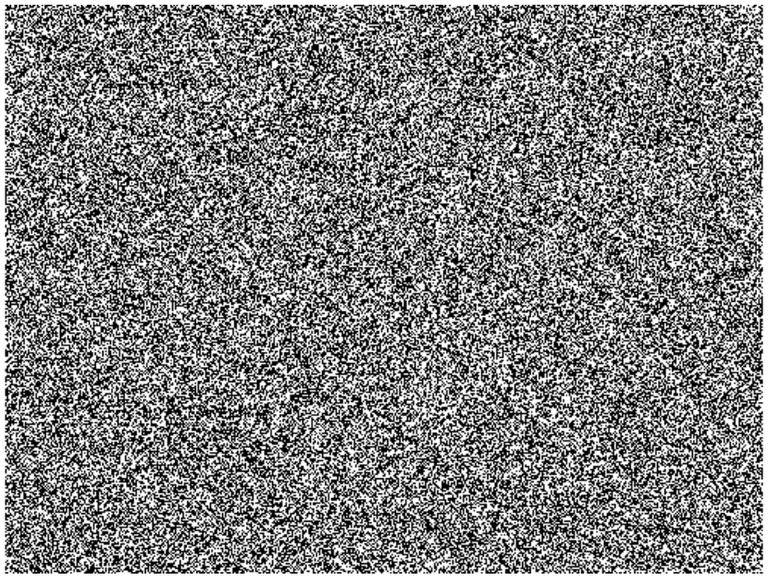
$$M$$



One-time pad (OTP)

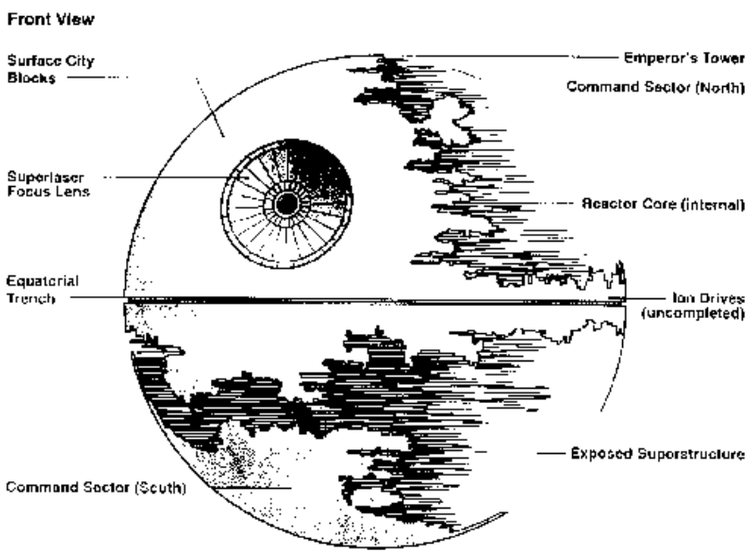
$$M \qquad \oplus \qquad K$$

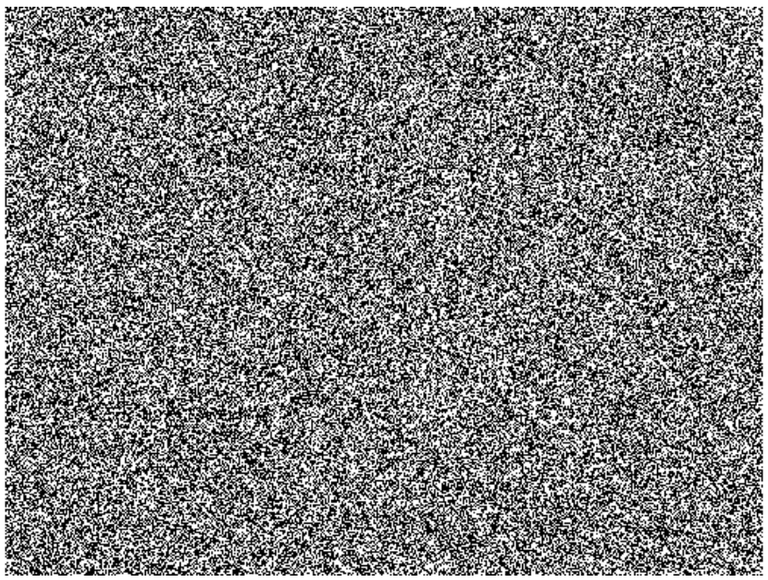


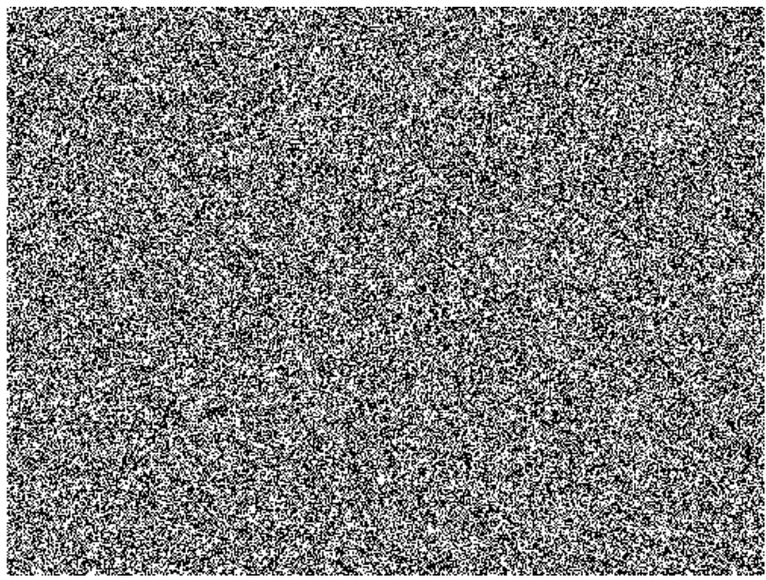


One-time pad (OTP)

$$M \oplus K = S$$

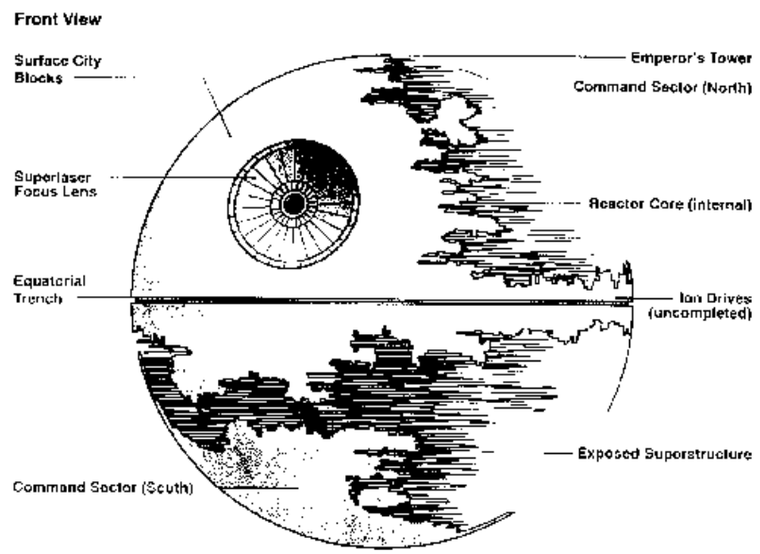


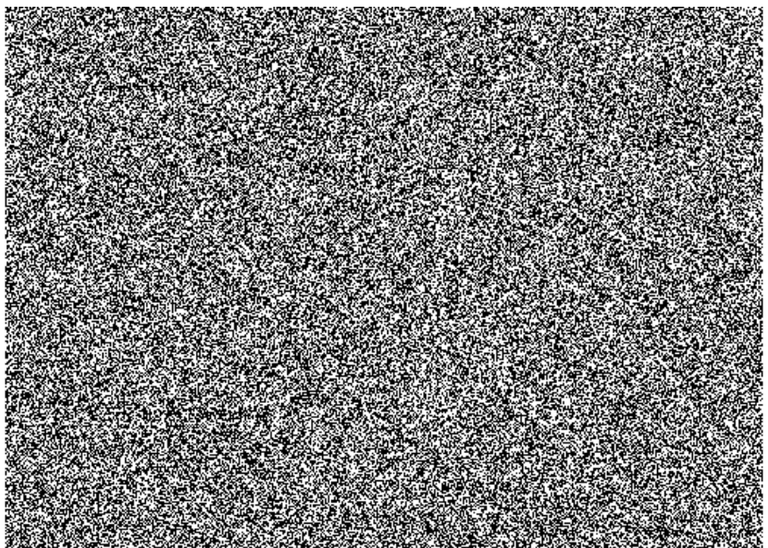


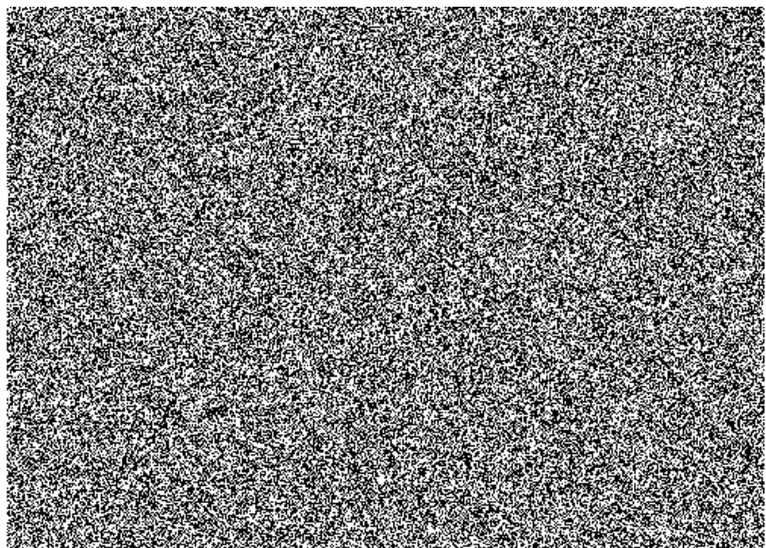


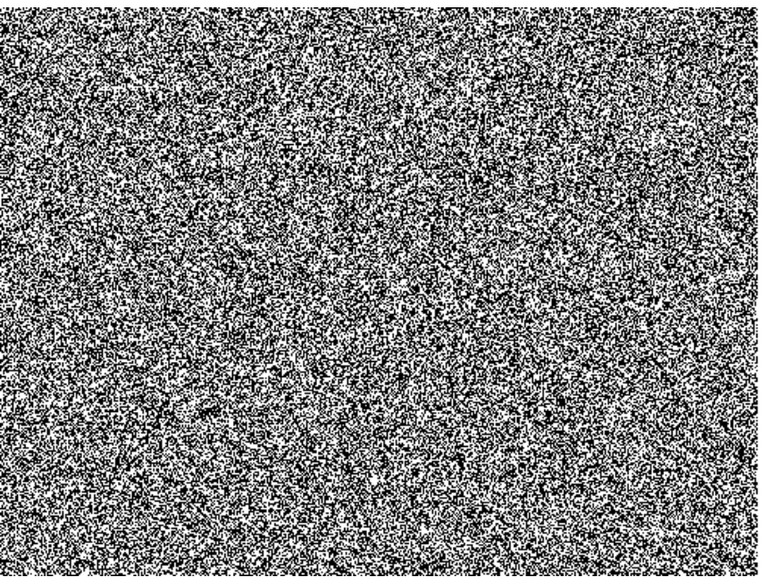
One-time pad (OTP)

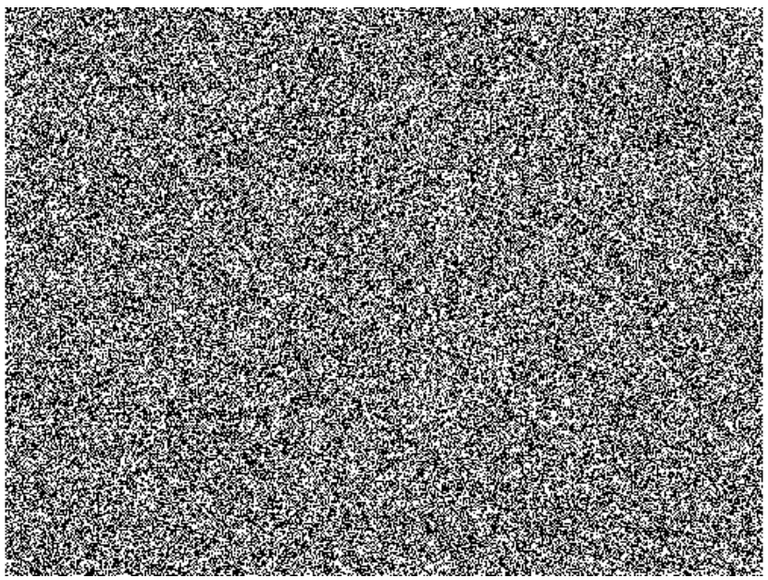
$$M \oplus K = S$$

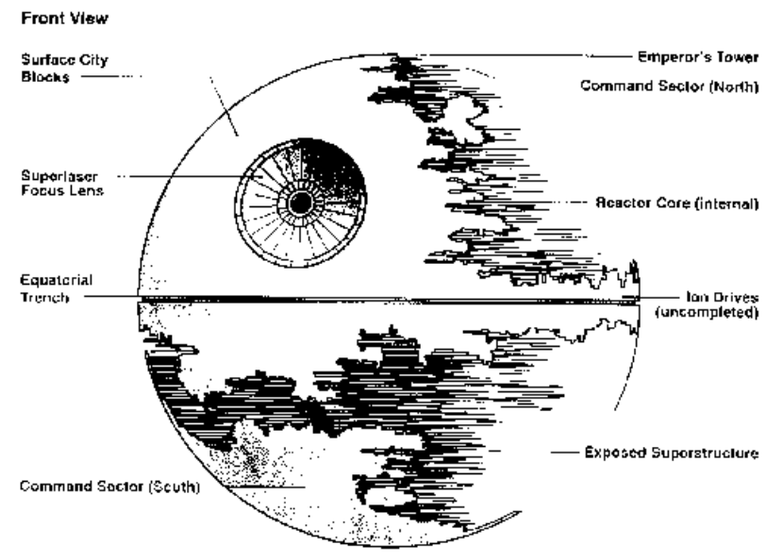










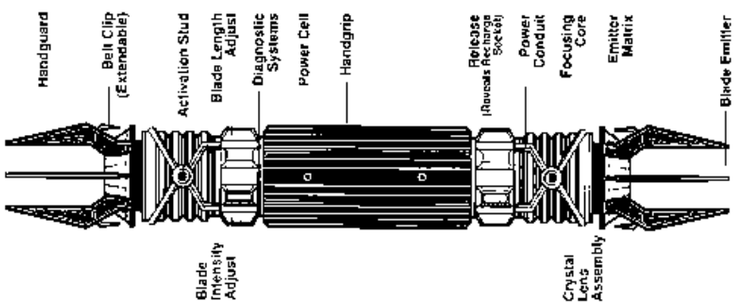


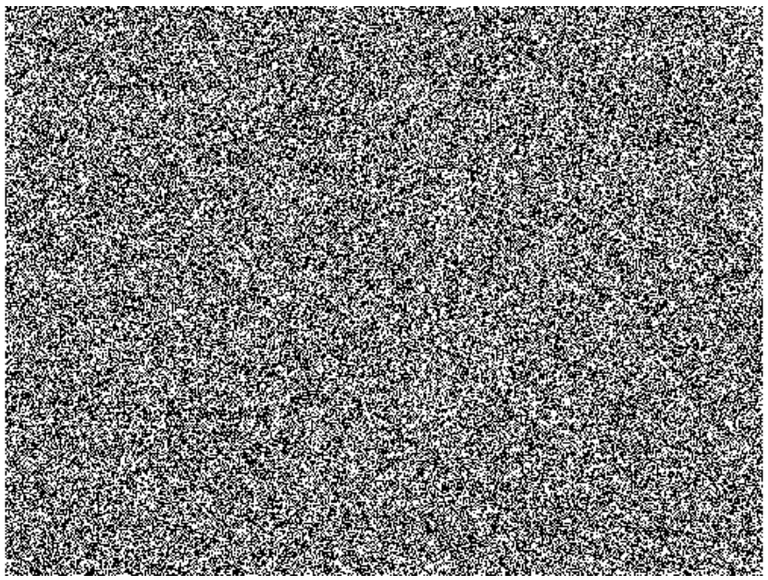
$$S \oplus K = M$$

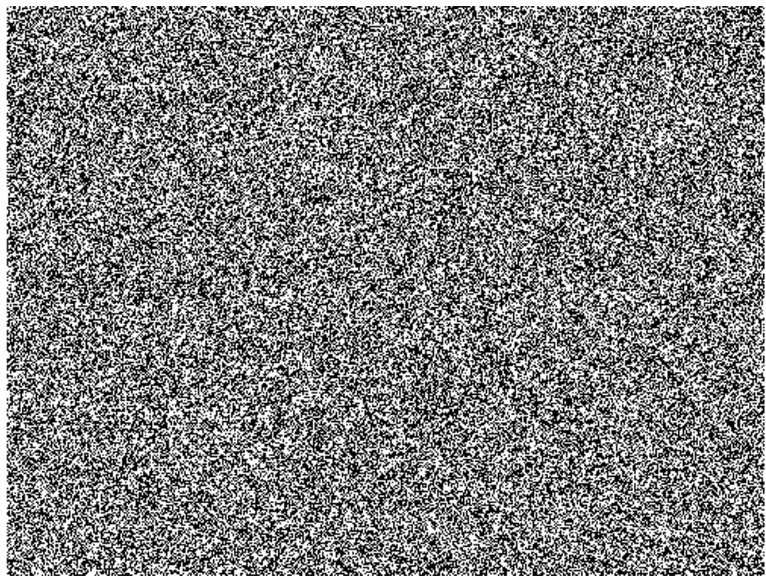
One-time pad (OTP)

Why is it one-time?

$$M' \quad \oplus \quad K \quad = \quad S'$$



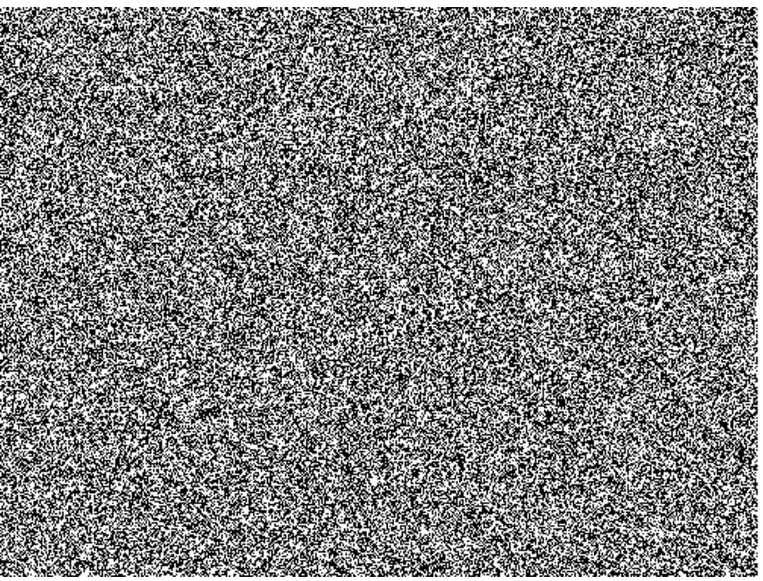


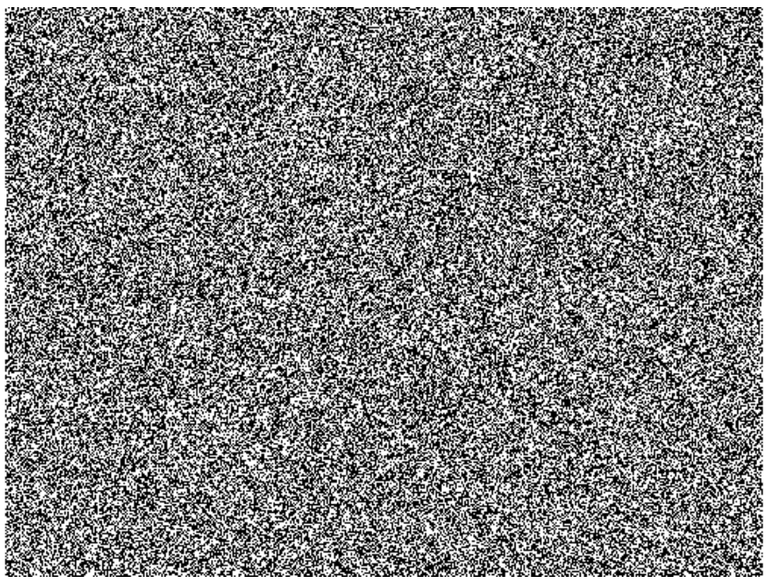


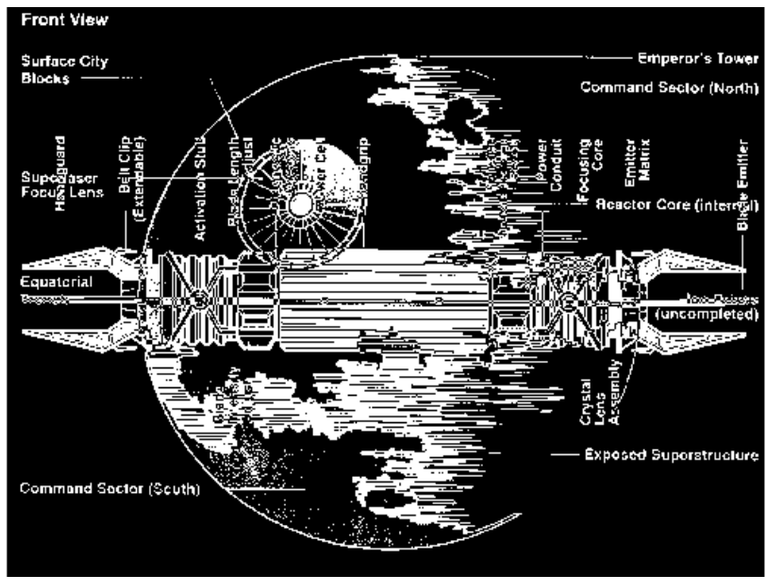
An attacker will have both S and S’

One-time pad (OTP)

$$S \quad \oplus \quad S' \quad = \quad M \oplus M'$$







$M \oplus M'$ reveals information about the messages

This has happened in the Cold War!

But if we use the key only once, then OTP has IT security!

Quantum Key Distribution (QKD)

Solves the problem of distributing arbitrary size keys between two parties (Alice and Bob)

Assumptions

1. Alice and Bob share classical *authenticated* channel
2. Alice and Bob share unsecure quantum channel
3. Quantum mechanics is correct

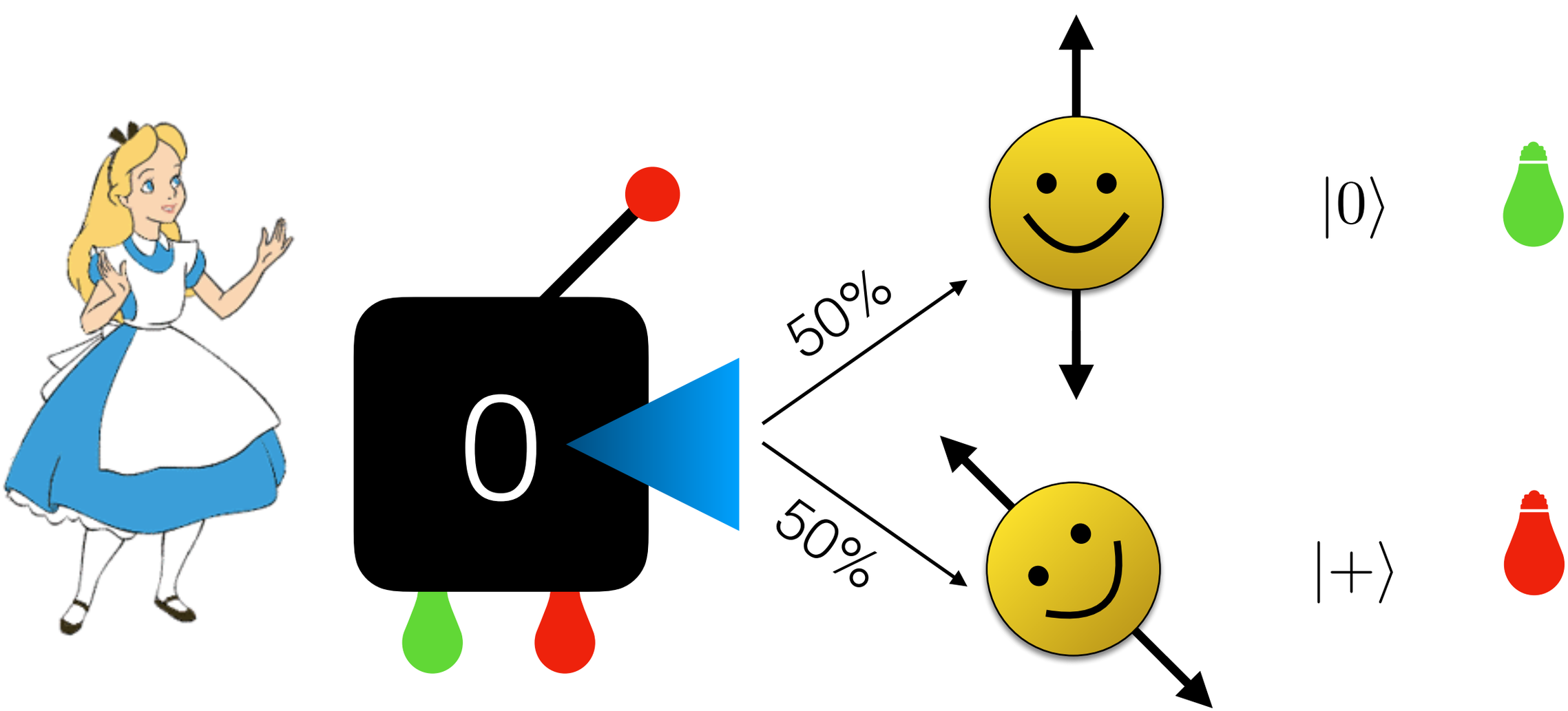
Under these assumptions we can have an IT-secure quantum key distribution protocol

Quantum Key Distribution (QKD)

Protocol of Bennet and Brassard from 1984 (BB84)

The setup

Alice has a qubit preparation device with 2 settings

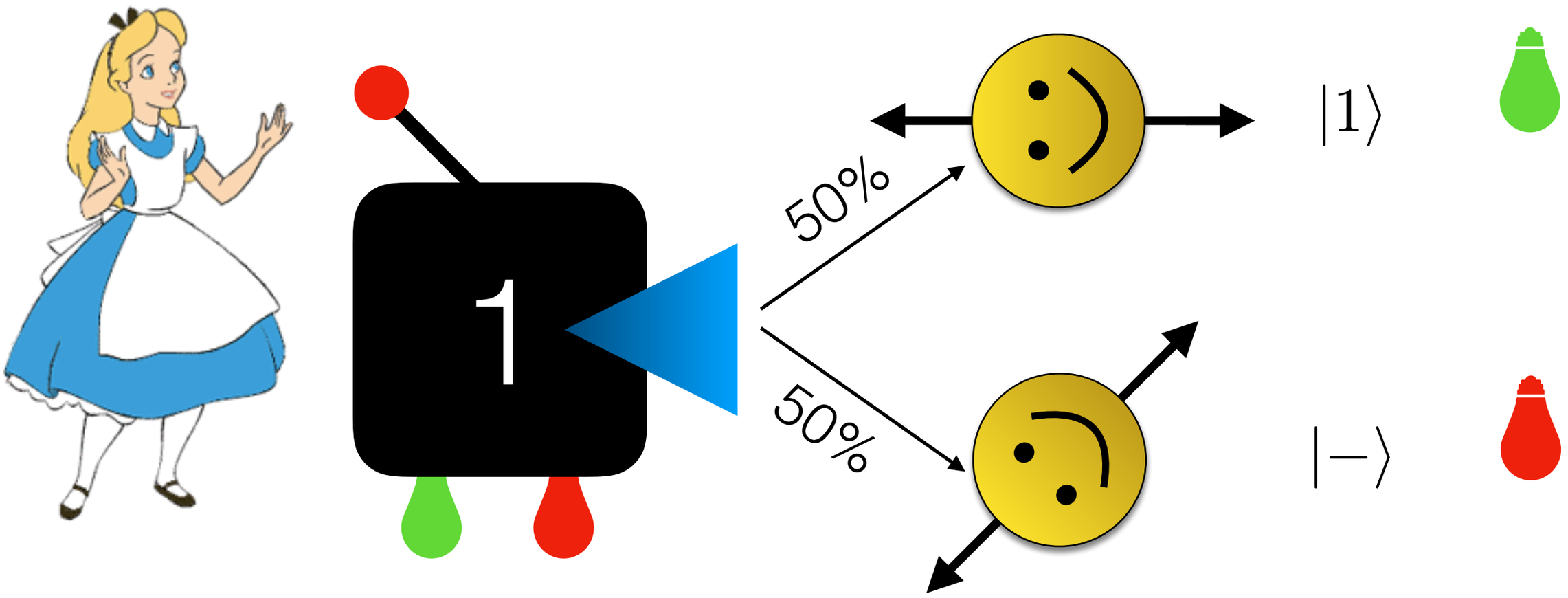


Quantum Key Distribution (QKD)

Protocol of Bennet and Brassard from 1984 (BB84)

The setup

Alice has a qubit preparation device with 2 settings



Quantum Key Distribution (QKD)

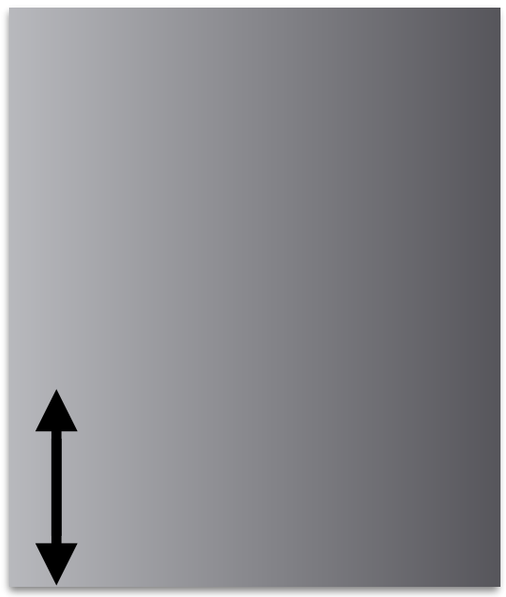
Protocol of Bennet and Brassard from 1984 (BB84)

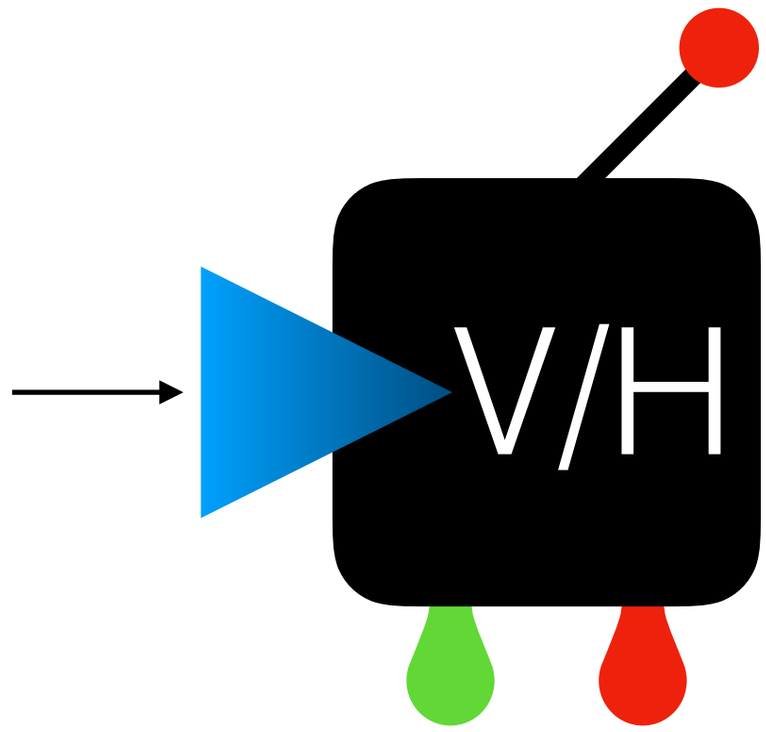
The setup

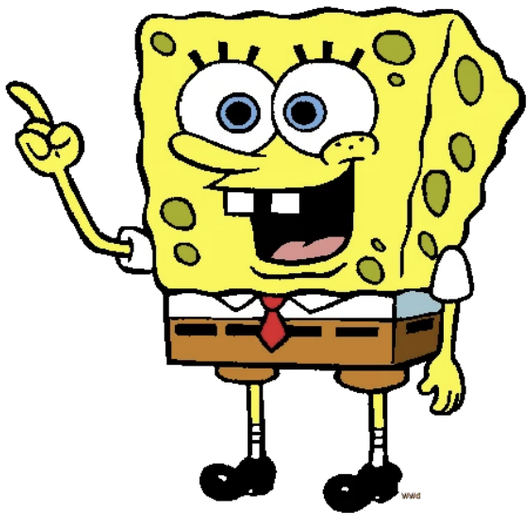
Alice has a qubit preparation device with 2 settings

Bob has a qubit measurement device with 2 settings

$(|0\rangle, |1\rangle)$







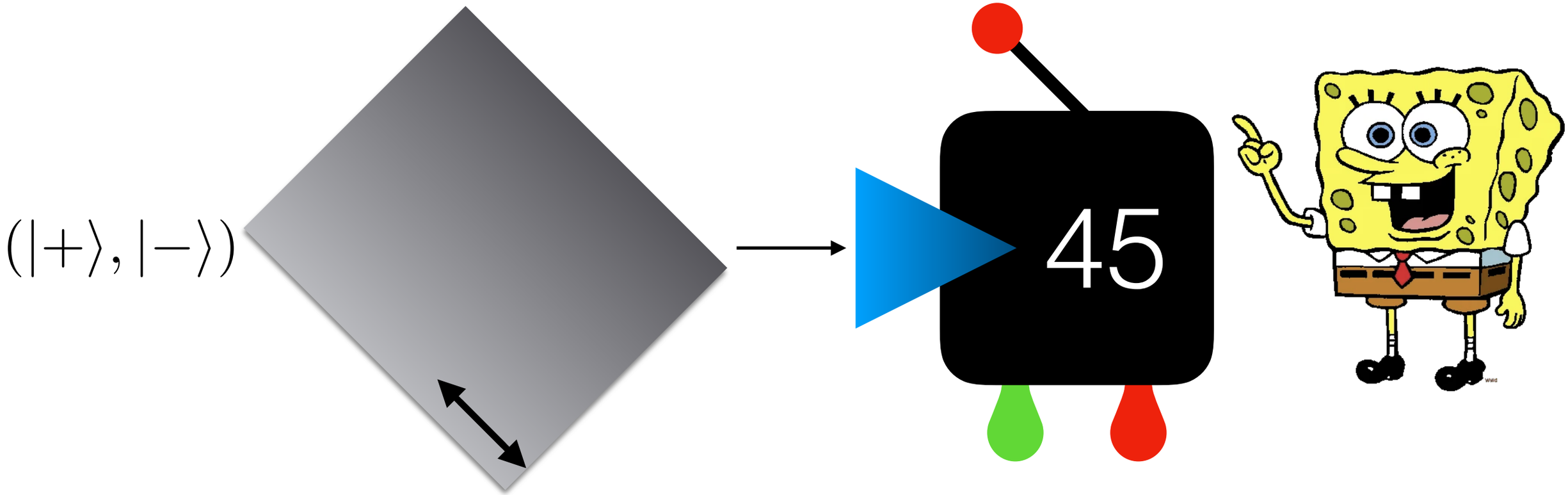
Quantum Key Distribution (QKD)

Protocol of Bennet and Brassard from 1984 (BB84)

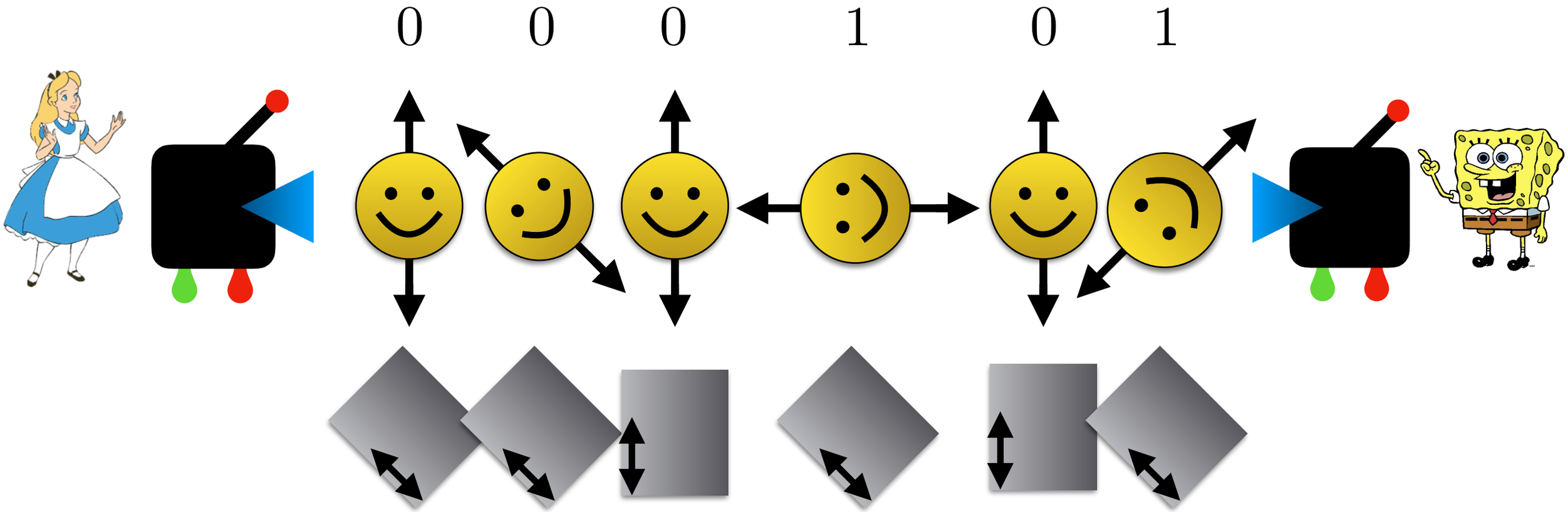
Setting

Alice has a qubit preparation device with 2 settings

Bob has a qubit measurement device with 2 settings



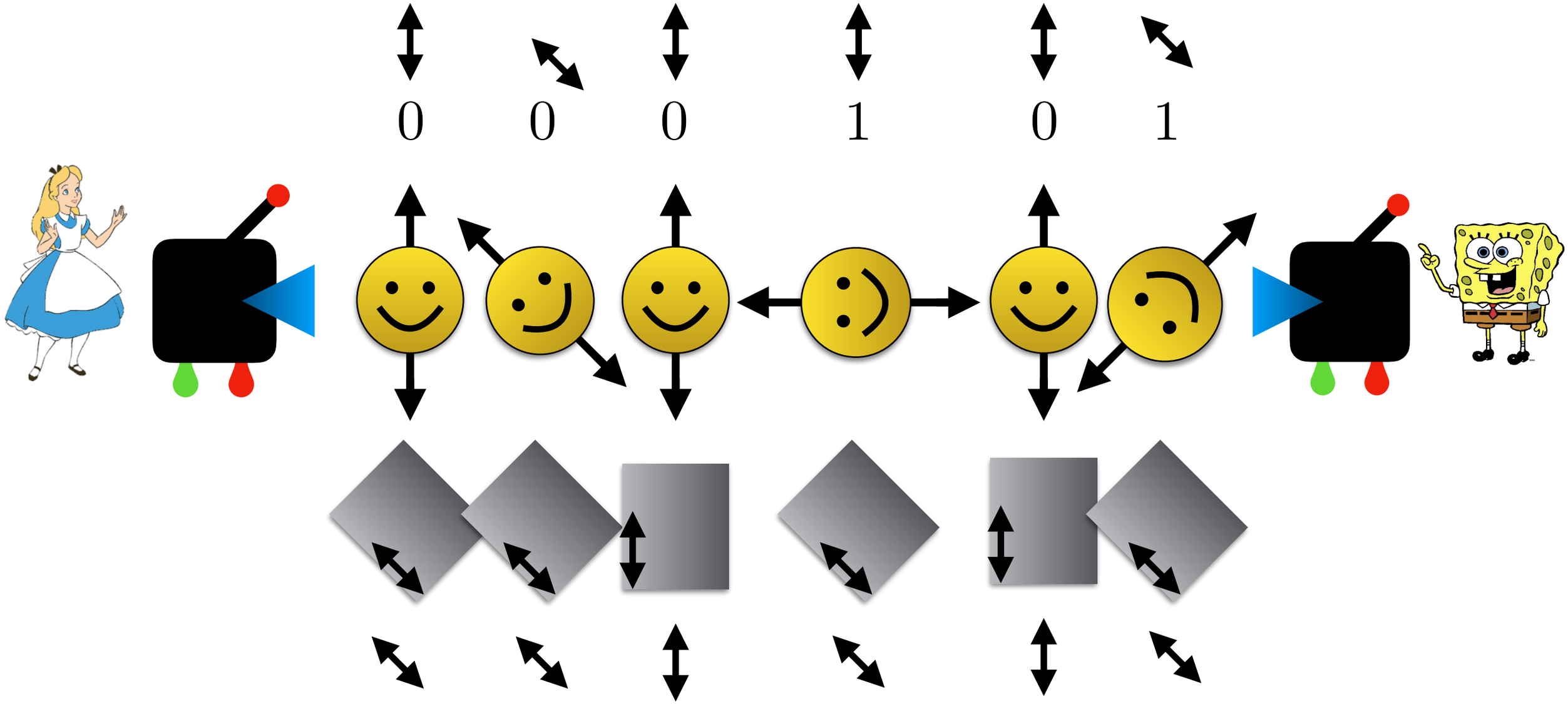
Quantum Key Distribution (QKD)



Alice chooses uniformly at random to send either 0 or 1
(each of the 4 states is chosen uniformly at random)

Bob chooses uniformly at random to measure
in either H/V basis or +45/-45

Quantum Key Distribution (QKD)

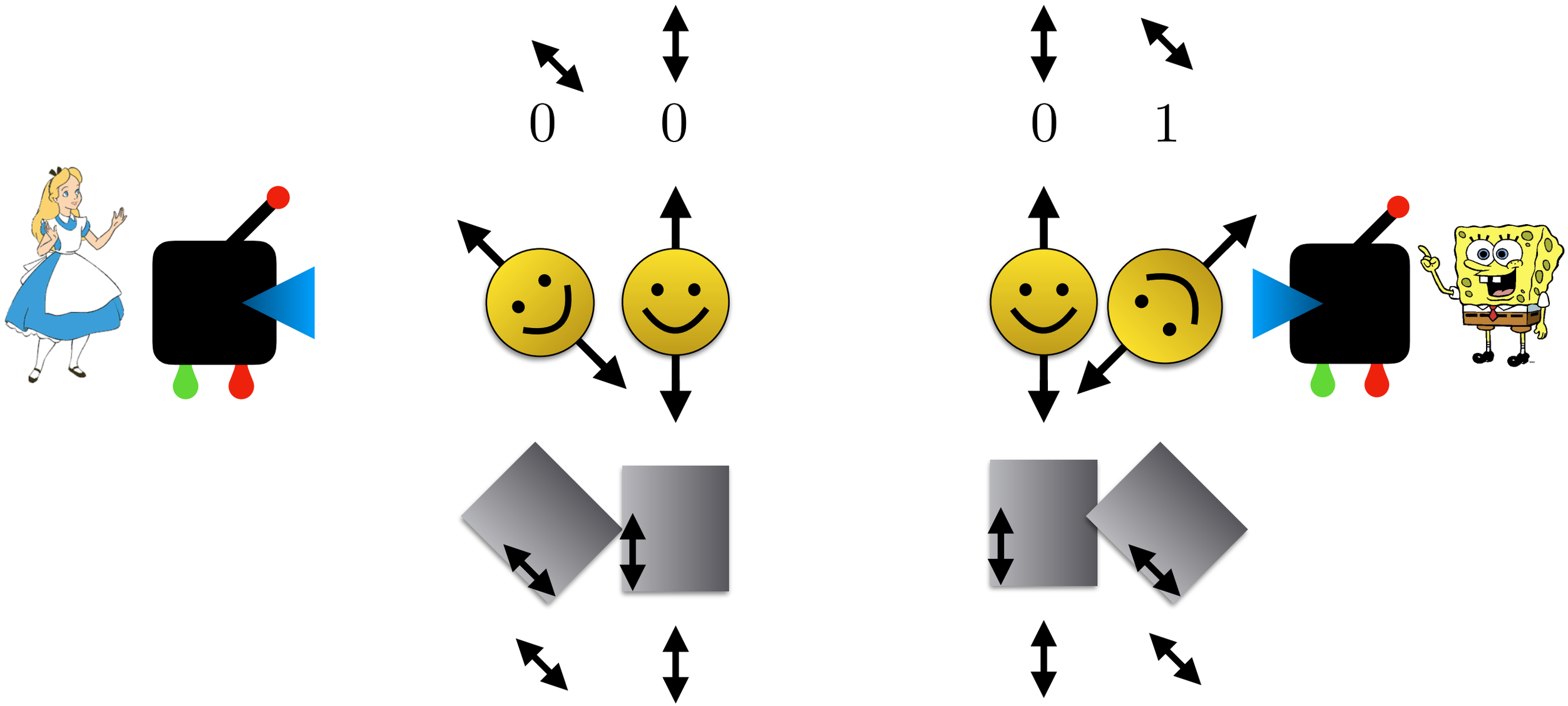


Alice announces preparation basis for each qubit

Bob announces measurement basis for each qubit

Keep only results that match!

Quantum Key Distribution (QKD)



Keep only results that match!

The outcomes they have for these results is the **raw key**

Quantum Key Distribution (QKD)

Alice and Bob now announce the preparation and measurement results for a small fraction of the raw key (say 10%)

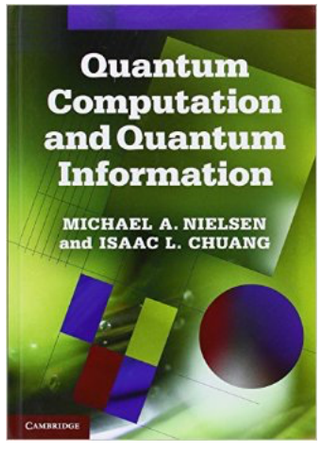
This is called **parameter estimation**
It's used to detect errors and/or tampering

If the results match for more than say 90% of outcomes they proceed to do **information reconciliation**

Use error correcting codes to make the 2 raw keys be identical (with very high probability)

Scan

Error correction



40£

Quantum Key Distribution (QKD)

In information reconciliation Alice and Bob will leak some information about the key

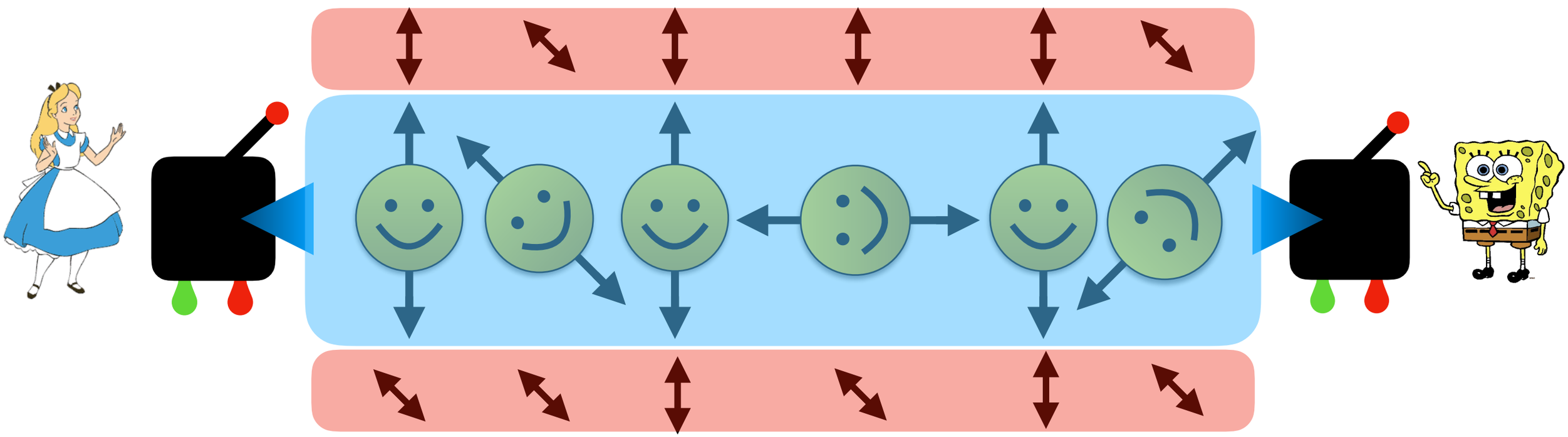
Last step is **privacy amplification**

Use hash functions to “randomize” the shared key (ensuring that an eavesdropper learns very little about it)

Now Alice and Bob can use OTP with their shared key

This process can go on forever so that they are constantly producing keys (at a certain **key-rate**)

Quantum Key Distribution (QKD)

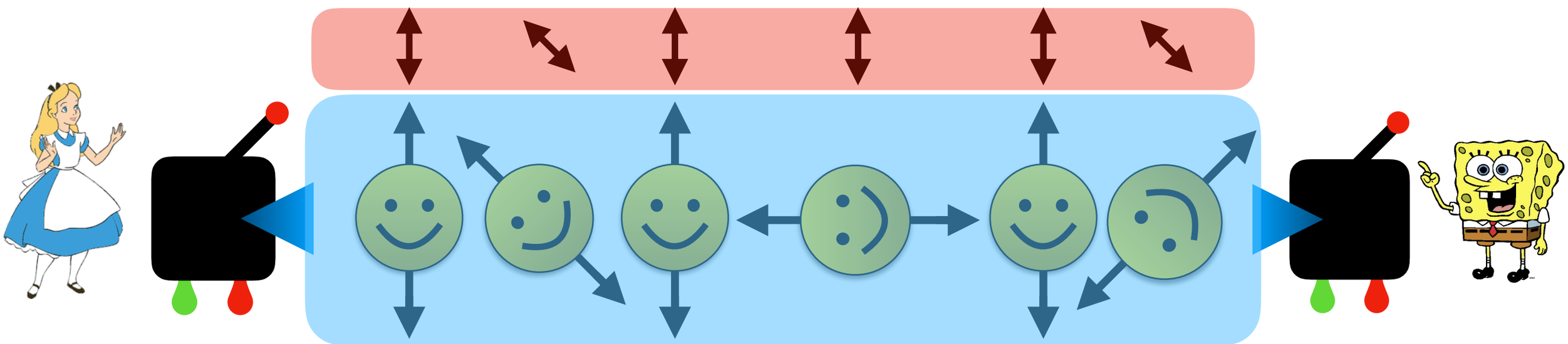


Classical authenticated channel

Unsecure quantum channel

What about an eavesdropper?

Quantum Key Distribution (QKD)



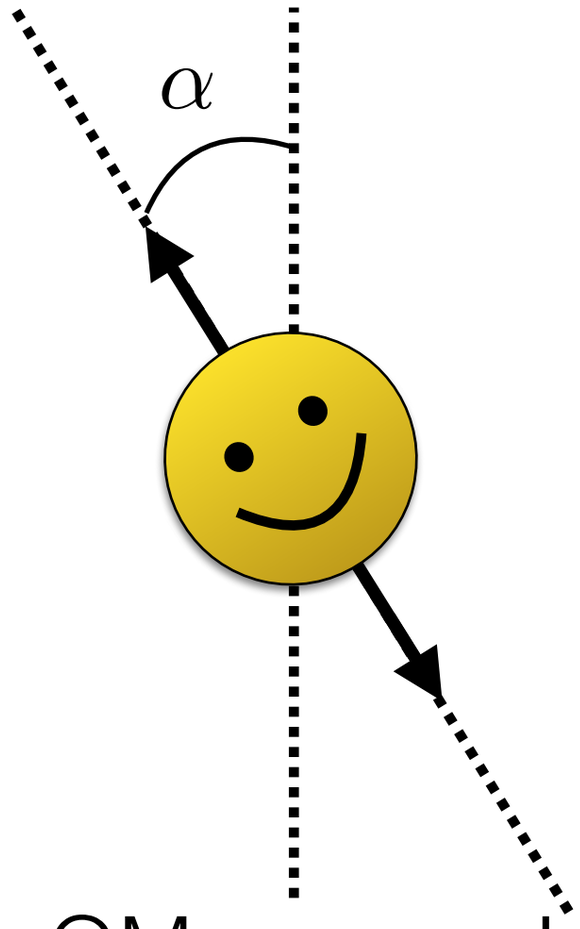
Can **observe** the communication on the classical channel

Can **tamper with** the communication on the quantum channel

Recall…

Pick α at random from $\{-\pi/4, 0, \pi/4, \pi/2\}$

Given **one** photon in the state



Can you find α?

QM says no!

Cannot guess α with probability greater than $\frac{1}{2}$

Measurements disturb quantum states

Cannot copy unknown quantum states

Quantum Key Distribution (QKD)

The eavesdropper has no better chance of finding Alice's bit than random guessing

If the eavesdropper tampers with the qubits this will be detected in the parameter estimation phase

In a loose sense we can say that the security of QKD is due to no-cloning and quantum uncertainty

This is not a proof!

Actual proof is quite involved :)

Quantum Key Distribution (QKD)

How can Alice and Bob establish the authenticated channel?

Pre-share a short secret key

Given a common short key there are classical protocols for establishing the authenticated channel

Wegman-Carter scheme (IT secure)

Use public key post-quantum crypto to establish common key

Needs to be secure only for a short time

Forward-secrecy

Without the authenticated channel, QKD is vulnerable to **Man-in-the-middle attacks (MITM)**

Commercial QKD

Companies specifically focused on quantum crypto

ID Quantique, MagiQ Technologies Inc,
QuintessenceLabs, SeQureNet

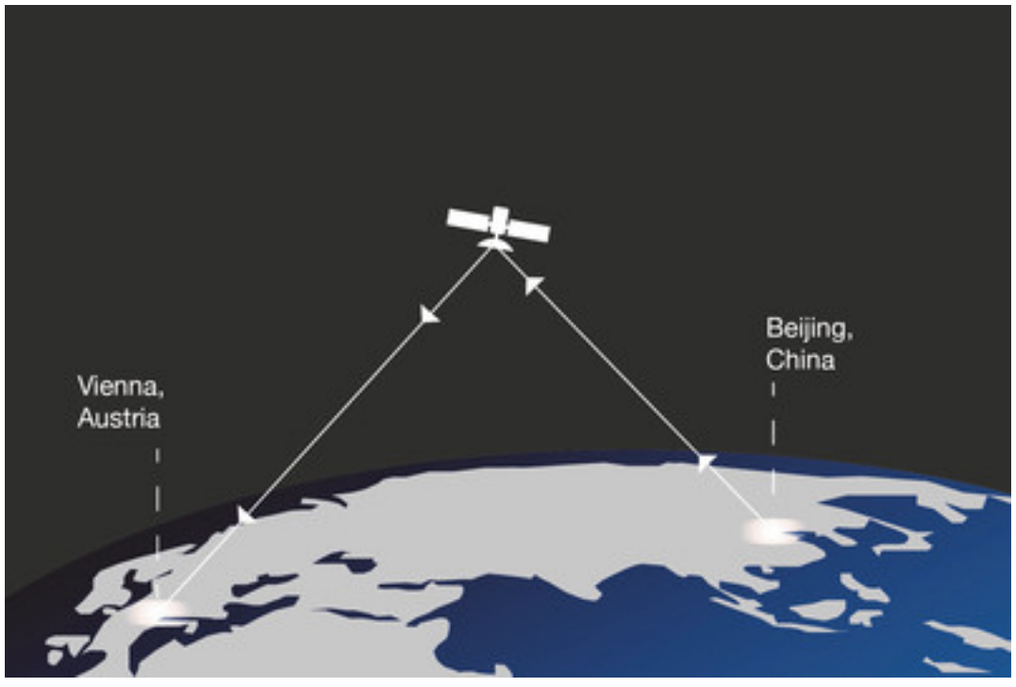
Companies that also do quantum crypto:
Toshiba, IBM, HP, Mitsubishi, NEC etc

Most commercial devices achieve key rates on
the order of Mbps over ~200km

Use existing fibre optic networks

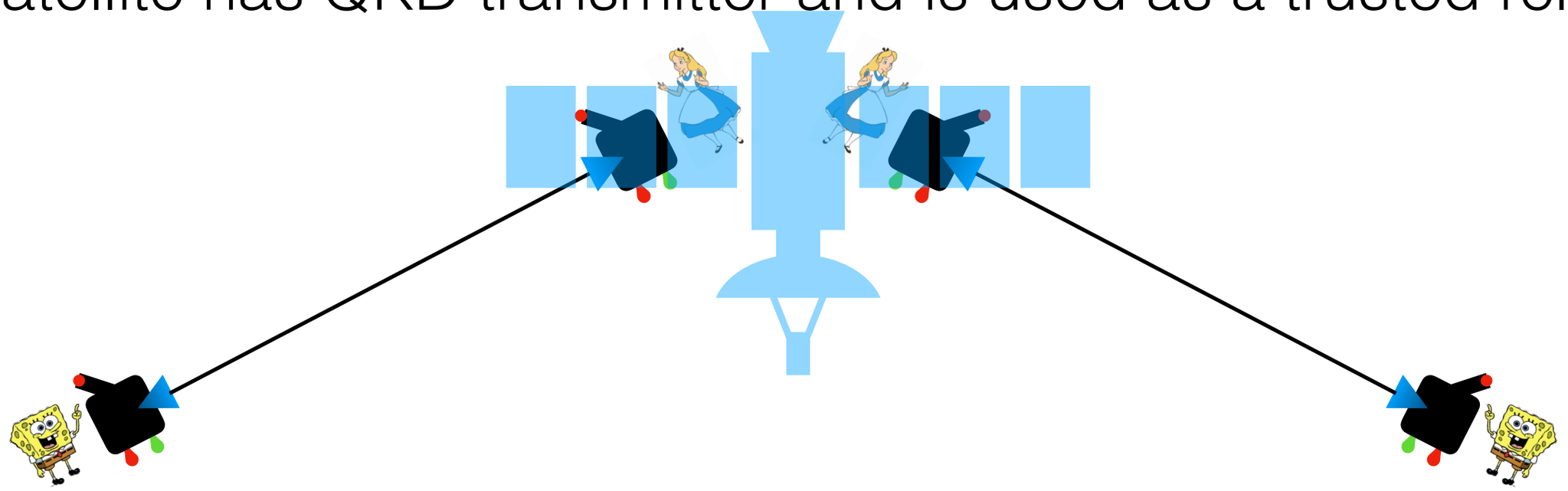
Single or multi-photon sources; single-photon detectors

QKD in space



Chinese satellite *Micius*

Satellite has QKD transmitter and is used as a trusted relay



QKD in space

Key rate 3-9kbps
(depending on distance to satellite)

Used to encrypt a teleconference between Vienna and Beijing
on 29th of September 2017

Teleconference lasted for 75mins and used ~2GB of data

The QKD key was used as a seed for 128-bit AES block cipher

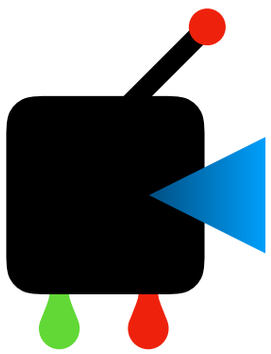
Seed-key refreshed every second, requiring only 70kB

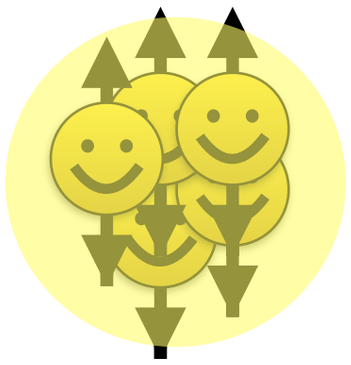
Side-channel attacks

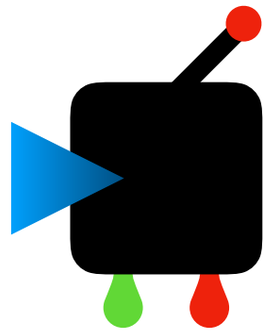
In practice we cannot implement the ideal version of the protocol

There can be attacks that exploit the physical implementation

E.g. photon splitting attack





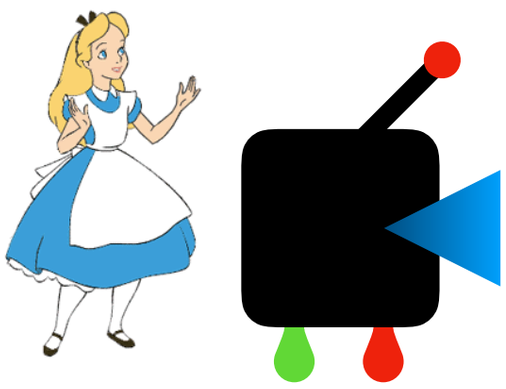


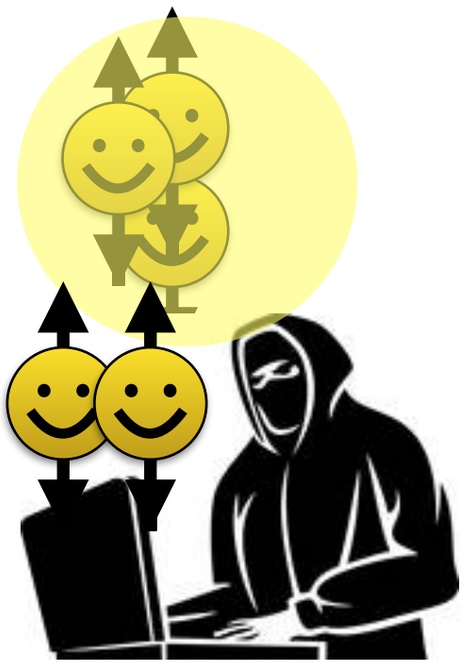
Side-channel attacks

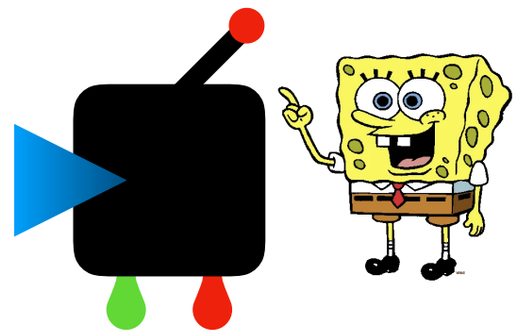
In practice we cannot implement the ideal version of the protocol

There can be attacks that exploit the physical implementation

E.g. photon splitting attack





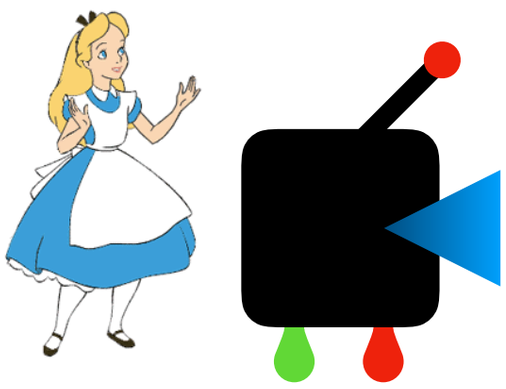


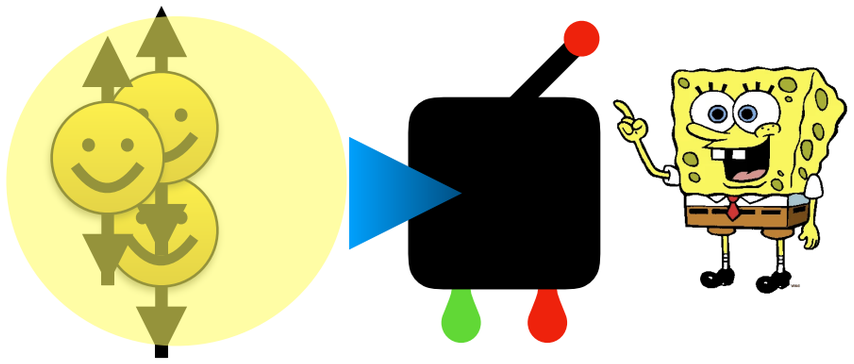
Side-channel attacks

In practice we cannot implement the ideal version of the protocol

There can be attacks that exploit the physical implementation

E.g. photon splitting attack





Side-channel attacks

In practice we cannot implement the ideal version of the protocol

There can be attacks that exploit the physical implementation

E.g. photon splitting attack
(can be detected using *decoy states*)

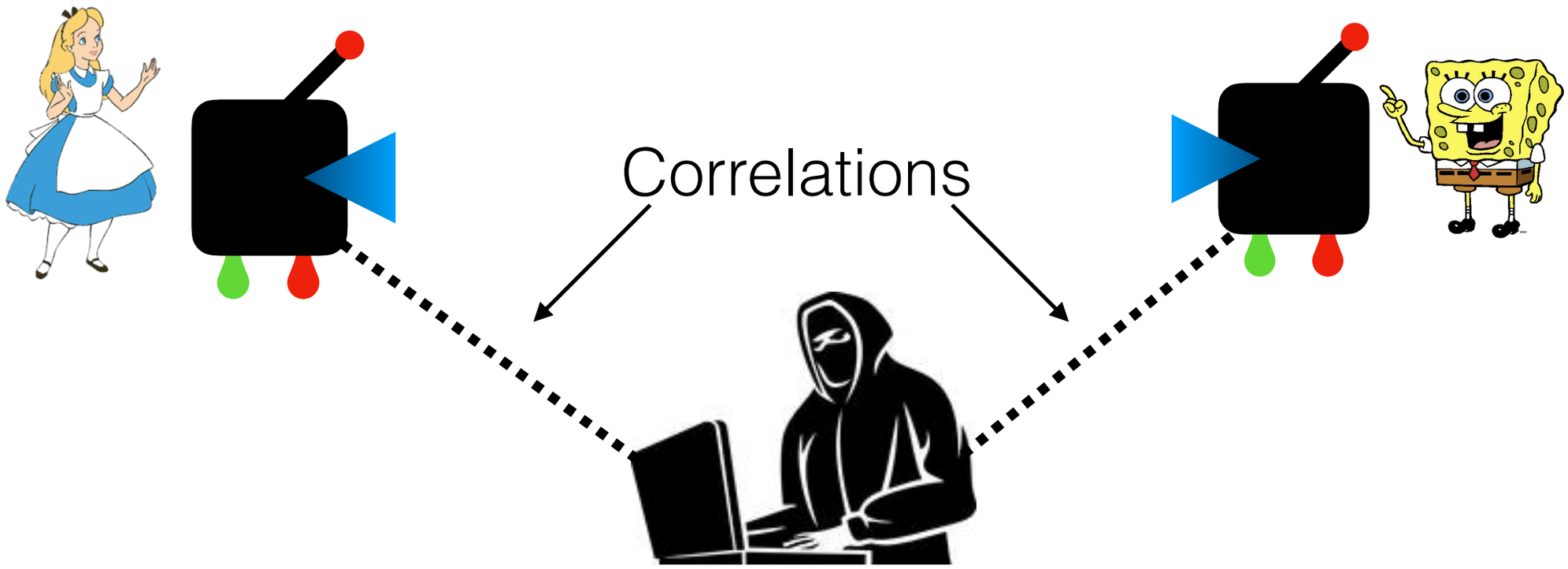
But there might be other attacks

Quantum hacking

The `trust issue'

Should Alice and Bob trust their devices?

What if the manufacturer has embedded trapdoors?



Amazingly, there is a way to detect this!

Device-independent cryptography

Quantum Cryptography

Quantum cryptography isn't just QKD
(though QKD is a large focus)

Quantum digital signatures (QDS)

Quantum secure random number generation (QRNG)

Quantum money

Blind quantum computation

Quantum secure multi-party computation

References and resources

Quantum Proofs of Knowledge, D. Unruh
(source of quote on slide 4)
https://eprint.iacr.org/2010/212.pdf
(two talks about it by D. Unruh)
https://www.youtube.com/watch?v=foIJM_f0Ij0
https://www.youtube.com/watch?v=DgxnNyeWEuE

Cryptography and Machine Learning, R. Rivest
https://people.csail.mit.edu/rivest/pubs/Riv91.pdf

Quantum cryptography courses
https://courses.cs.ut.ee/all/MTAT.07.024/2015_fall/uploads/
http://users.cms.caltech.edu/~vidick/teaching/120_qcrypto/index.html#lectures

References and resources

BB84 and quantum optics course

https://www.coursera.org/lecture/quantum-optics-single-photon/7-4-quantum-cryptography-the-bb84-qkd-scheme-Ym4Yy

Review paper on quantum cryptography

https://arxiv.org/abs/quant-ph/0101098

QKD and BB84

https://cs.uwaterloo.ca/~watrous/LectureNotes/CPSC519.Winter2006/18.pdf

QKD and proof of security

https://arxiv.org/pdf/quant-ph/0011056.pdf

References and resources

Satellite QKD and Beijing-Vienna video-conference

https://arxiv.org/pdf/1707.00542.pdf

https://arxiv.org/pdf/1801.04418.pdf

Section 12.6 from Nielsen & Chuang