Information-Theoretic Quantum Cryptography

Anne Broadbent


uOttawa

IPAM summer school

July 27, 2022

Outline

- Quantum Money
- Quantum Key Distribution
- Impossibility of Quantum Bit Commitment
- Blind Quantum Computation
- Certified Deletion

Some References

- Broadbent, A., Schaffner, C. Quantum cryptography beyond quantum key distribution. *Des. Codes Cryptogr.* **78,** 351–382 (2016). https://doi.org/10.1007/s10623-015-0157-4
- Wiesner, S. (1983). Conjugate coding. ACM Sigact News, 15(1), 78-88. https://dl.acm.org/doi/pdf/10.1145/1008908.1008920
- Watrous, J. Lecture 19: Impossibility of Quantum Bit Commitment. https://cs.uwaterloo.ca/~watrous/QC-notes/QC-notes.19.pdf
- Broadbent, A. (2015). Delegating private quantum computations. Canadian Journal of Physics, 93(9), 941-946. https://doi.org/10.1139/cjp-2015-0030
- Bouman, N. J., & Fehr, S. (2010, August). Sampling in a quantum population, and applications. In Annual Cryptology Conference (pp. 724-741).
- https://link.springer.com/chapter/10.1007/978-3-642-14623-7_39
- Bennett, C. H., & Brassard, G. (2020). Quantum cryptography: Public key distribution and coin tossing. https://arxiv.org/ftp/arxiv/papers/2003/2003.06557.pdf
- Broadbent, A., & Islam, R. (2020, November). Quantum encryption with certified deletion. In Theory of Cryptography Conference (pp. 92-122). https://link.springer.com/chapter/10.1007/978-3-030-64381-2_4
- Bouman, N. J., & Fehr, S. (2010). Sampling in a quantum population, and applications. In *Annual Cryptology Conference CRYPTO* (pp. 724-741).
- Fehr, S. (2010). Quantum cryptography. *Foundations of Physics*, *40*(5), 494-531.
- James Bartusek, Dakshita Khurana. Cryptography with Certified Deletion, https://arxiv.org/abs/2207.01754
- And many more…

Quantum States Can't be Cloned

Quantum rewinding
Quantum oracle queries

Quantum money
Quantum encodings
Copy-protected software

"Quantum no-cloning theorem"
Park (1970); Dieks & Wootters-Zurek (1982)

Quantum Information

Can be tasted, but this leaves a mark.

Can be shared, but there is a total of
1 item to be shared.

Cannot be copied.

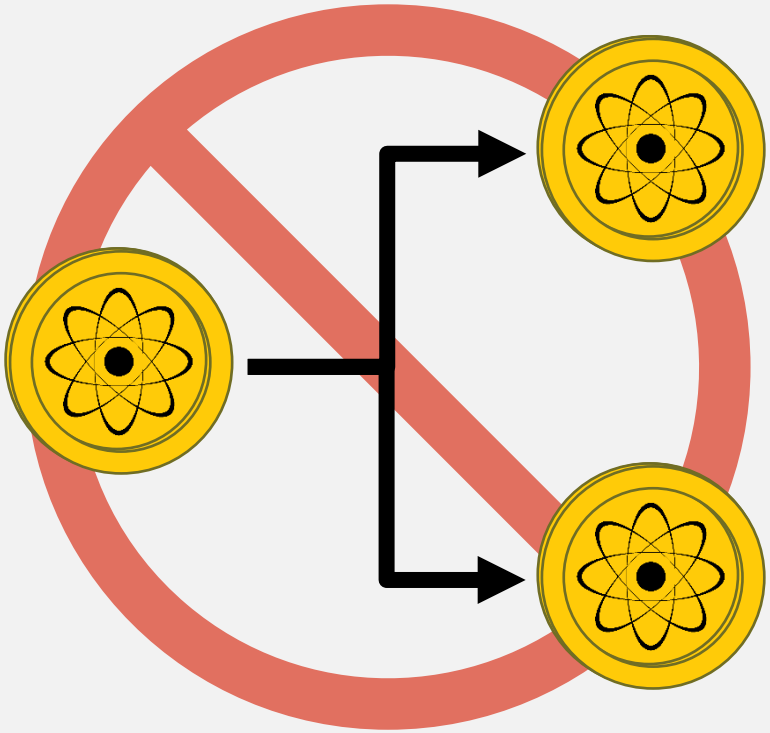
Conventional Information

Can be observed without changing it.

Can be shared at will.

Can be copied.

Unclonable Authenticity



Quantum Money

Wiesner (ca. 1969)

Written in 1968
Published 1983

Submitted to IEEE, Information Theory

This paper treats a class of codes made possible by restrictions on measurement related to the uncertainty principal. Two concrete examples and some general results are given.

Conjugate Coding *

Stephen Wiesner

Columbia University, New York, N.Y.
Department of Physics

The uncertainty principle imposes restrictions on the capacity of certain types of communication channels. This paper will show that in compensation for this "quantum noise", quantum mechanics allows us novel forms of coding without analogue in communication channels adequately described by classical physics.

* Research supported in part by the National Science Foundation.

Wiesner's conjugate coding

Pick basis $\theta \in \{0,1\}$.
Pick bit $b \in \{0,1\}$.
let $|b\rangle_\theta = H^\theta |b\rangle$

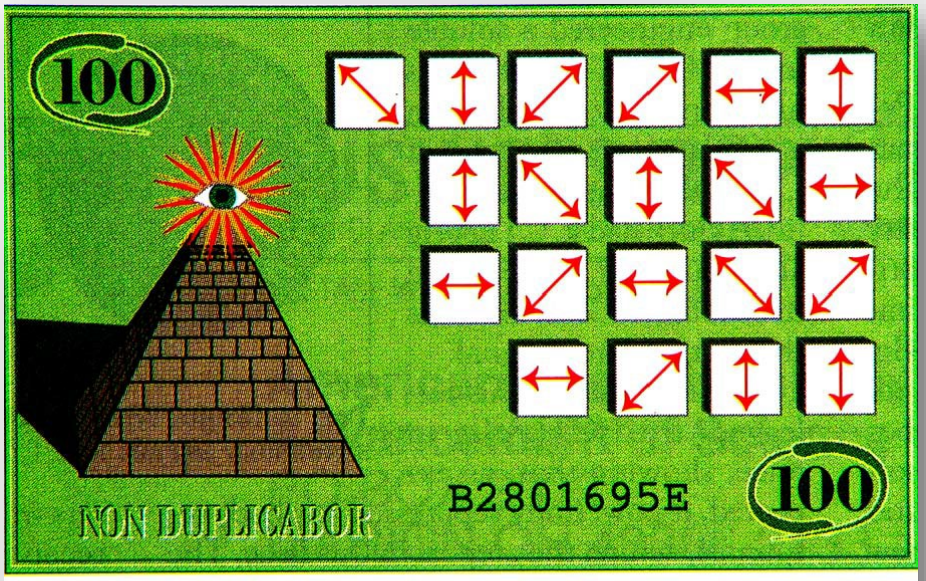
θ	b	$\|b\rangle_\theta$
0	0	$\|0\rangle$
0	1	$\|1\rangle$
1	0	$\|+\rangle$
1	1	$\|-\rangle$

Given a single copy of $|b\rangle_\theta$ for uniform b, θ:

- Can easily verify $|b\rangle_\theta$ if b, θ are known (how?).
- Intuitively: without knowledge of the encoding basis, and given $|b\rangle_\theta$, no third party can create two quantum states that **both** pass this verification with high probability.

For bit-strings $\theta = \theta_1\theta_2 \dots \theta_n$, $b = b_1 b_2 \dots b_n$, define
$|b\rangle_\theta = |b_1\rangle_{\theta_1} \otimes |b_2\rangle_{\theta_2} \dots \otimes |b_n\rangle_{\theta_n}$

A quantum banknote is $|b\rangle_\theta$ for random $b, \theta \in \{0,1\}^n$:

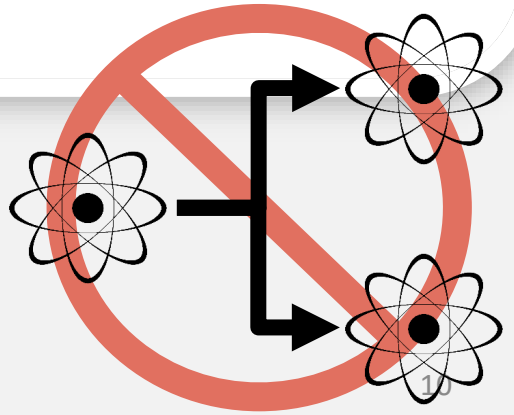


A quantum banknote, containing particles in a secret set of quantum states, cannot be copied by counterfeiters, who would disturb the particles by attempting to observe them.

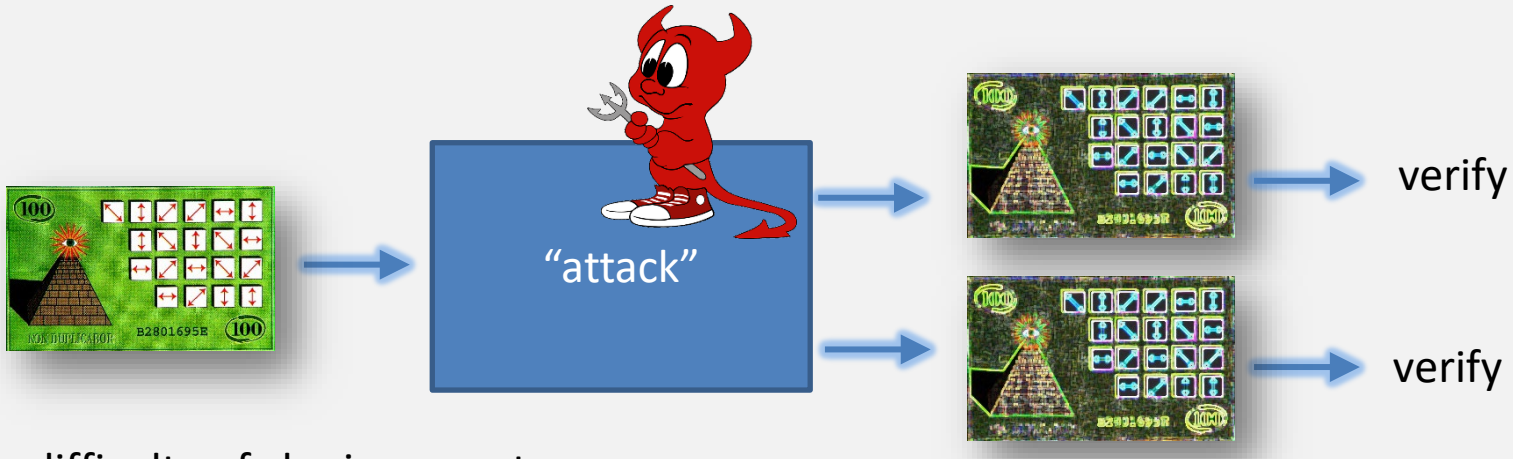
©AAAS (1992)

Wiesner's security argument

Could there be some way of duplicating the money without learning the sequence N_i? No, because if one copy can be made (so that there are two pieces of the money) then many copies can be made by making copies of copies. Now given an unlimited supply of systems in the same state, that state can be determined. Thus, the sequence N_i could be recovered. But this is impossible.



Security of Wiesner's quantum money



How does the difficulty of cloning quantum money scale with the number of qubits, n?

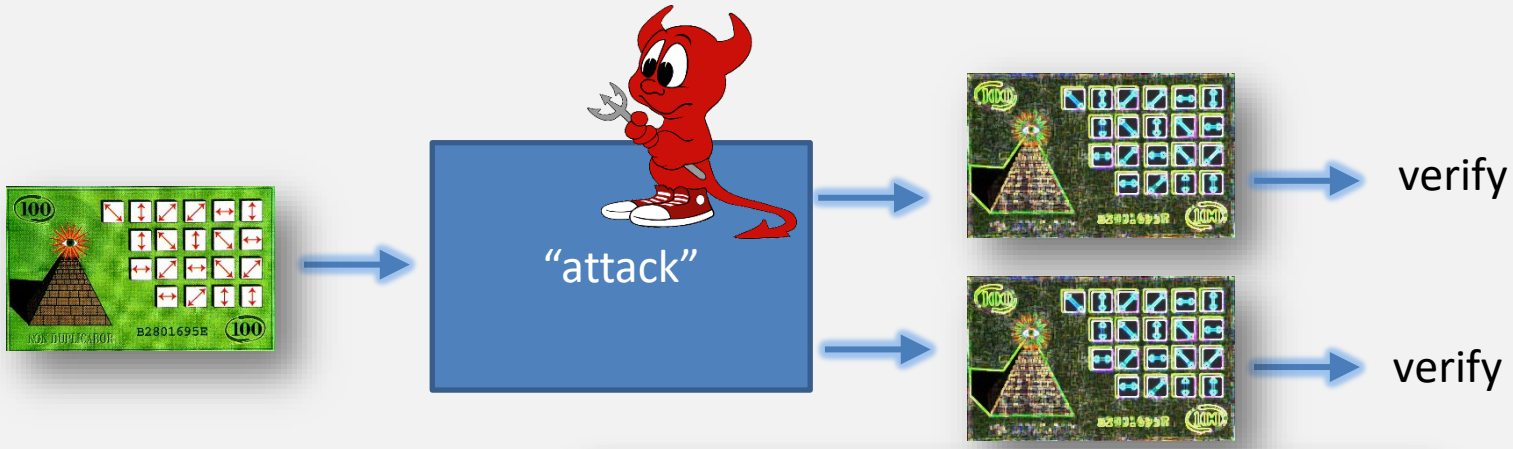
For a single qubit, one possible attack is to guess a basis uniformly, measure in that basis, and re-send two qubits that correspond to this measurement

- If the basis is correct (prob= ½), the attack succeeds with prob. 1.
- If the basis is incorrect, the attack success with prob. 1/4 since the attack prepares qubits in the complementary basis, and the probability that both verifiers accept is ½*½ = ¼.

Success prob. of attack = ½ + ½*¼ = 5/8.

Can actually achieve ¾ (and this is optimal).

Security of Wiesner's quantum money



How does the difficulty of cloning quantum money scale with the number of qubits, n?

Answer:

$$(3/4)^n$$

Optimal counterfeiting attacks and generalizations for Wiesner's quantum money

Abel Molina,* Thomas Vidick,† and John Watrous*

February 20, 2012

Abstract

We present an analysis of Wiesner's quantum money scheme, as well as some natural generalizations of it, based on semidefinite programming. For Wiesner's original scheme, it is determined that the optimal probability for a counterfeiter to create two copies of a bank note from one, where both copies pass the bank's test for validity, is $(3/4)^n$ for n being the number of qubits used for each note. Generalizations in which other ensembles of states are substituted for the one considered by Wiesner are also discussed, including a scheme recently proposed by Pastawski, Yao, Jiang, Lukin, and Cirac, as well as schemes based on higher dimensional quantum systems. In addition, we introduce a variant of Wiesner's quantum money in which the verification protocol for bank notes involves only classical communication with the bank. We show that the optimal probability with which a counterfeiter can succeed in two independent verification attempts, given access to a single valid n-qubit bank note, is $(3/4 + \sqrt{2}/8)^n$. We also analyze extensions of this variant to higher-dimensional schemes.

QUANTUM MONEY "REVIVAL"

Noise-tolerant ('feasible with current technology') quantum money

- Pastawski, Yao, Jiang, Lukin, Cirac (2012)

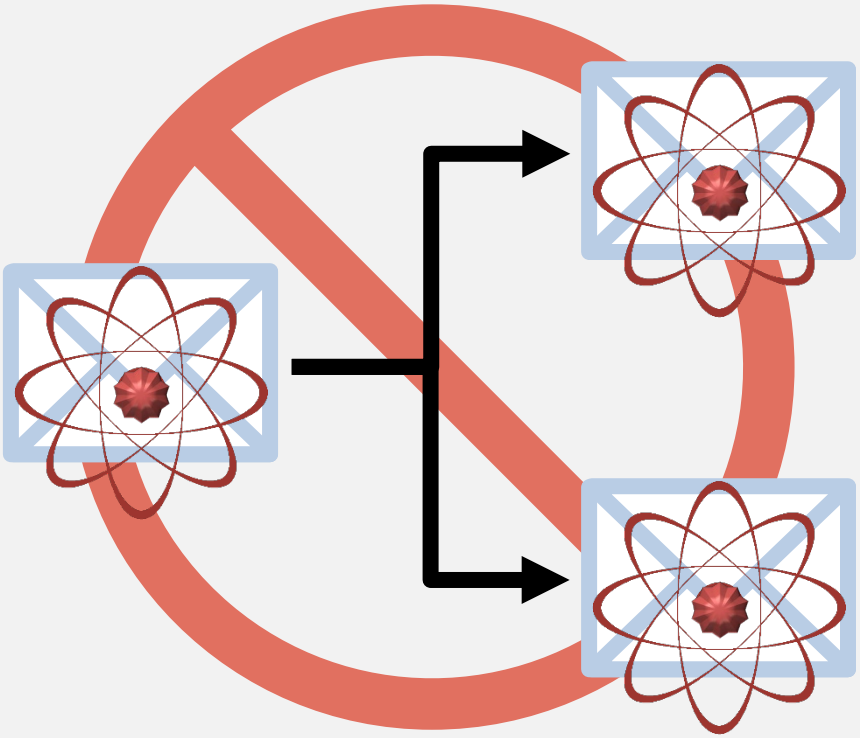
Quantum Money with **classical verification**

- Gavinsky (2012)

Public-key quantum money (can be verified by any user)

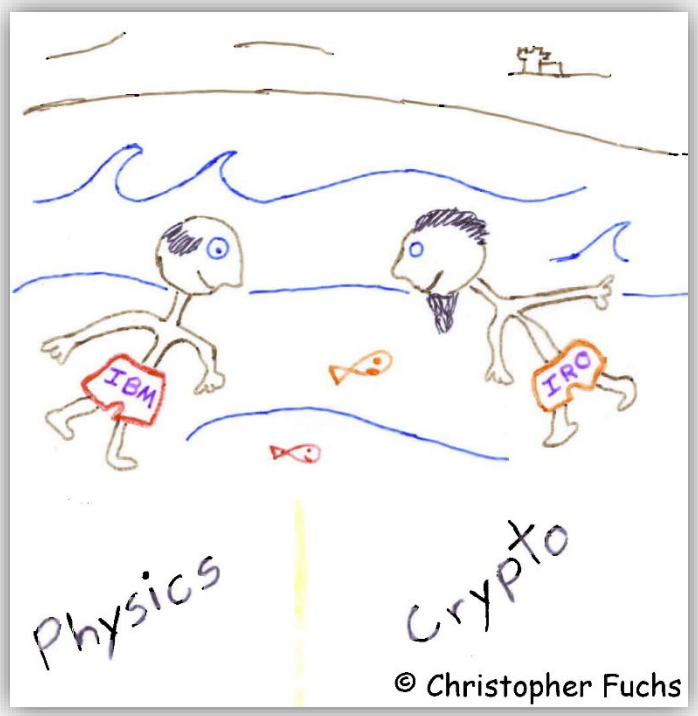
- Farhi, Gosset, Hassidim, Lutomirski, and Shor (2012)
- Aaronson and Christiano (2012)
- Zhandry (2017)

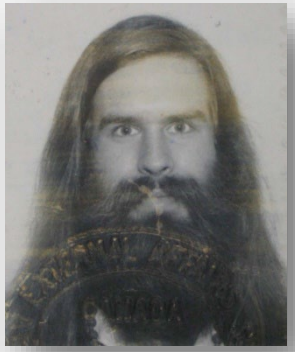
Unclonable Information



1979

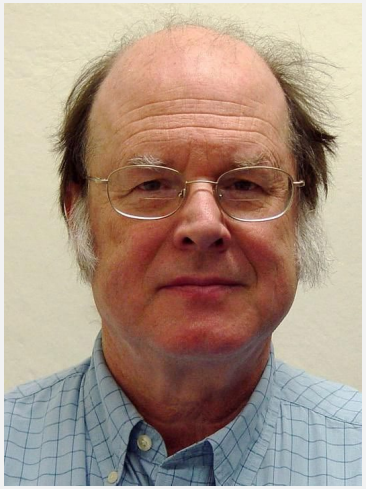
Charles
Bennett
Physicist
IBM, USA





Gilles
Brassard
Computer
Scientist
Université
de Montréal,
Canada

2018



Ultimate goal:
unconditional security

AES ?

No !

RSA ?

No !

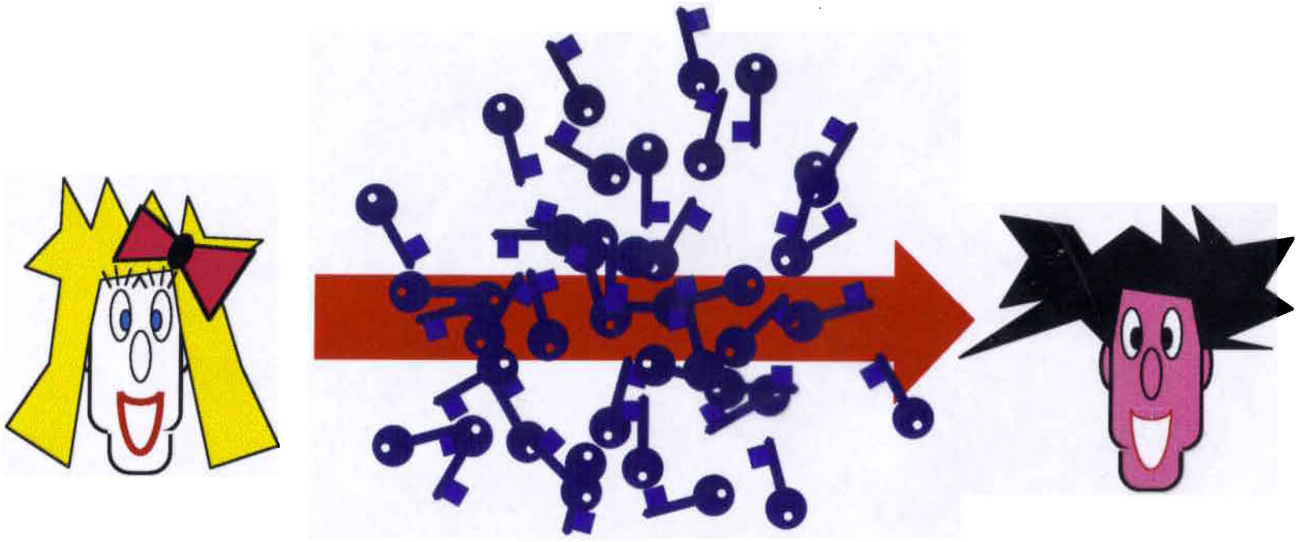
The One-time Pad Encryption Scheme

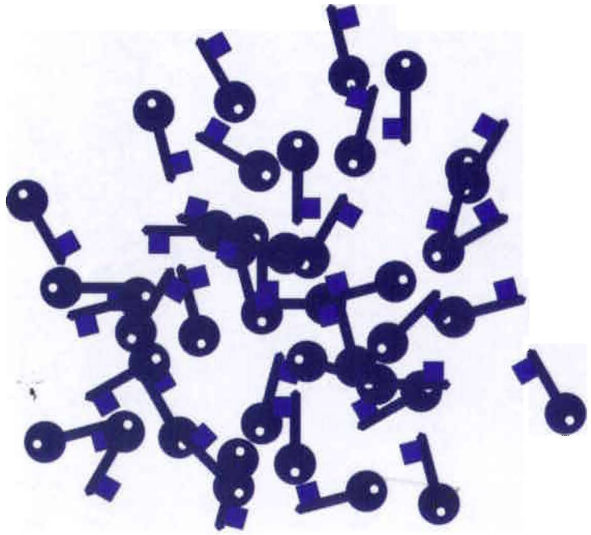
Plaintext	$x \in \{0,1\}$
Key	$k \in_R \{0,1\}$
Ciphertext	$x \oplus k$

Since the ciphertext is uniformly random (as long as *k* is random, unknown and used only once), the plaintext is perfectly concealed.

Le masque jettable

The Washington-Moscow Hot Line (est.1963)





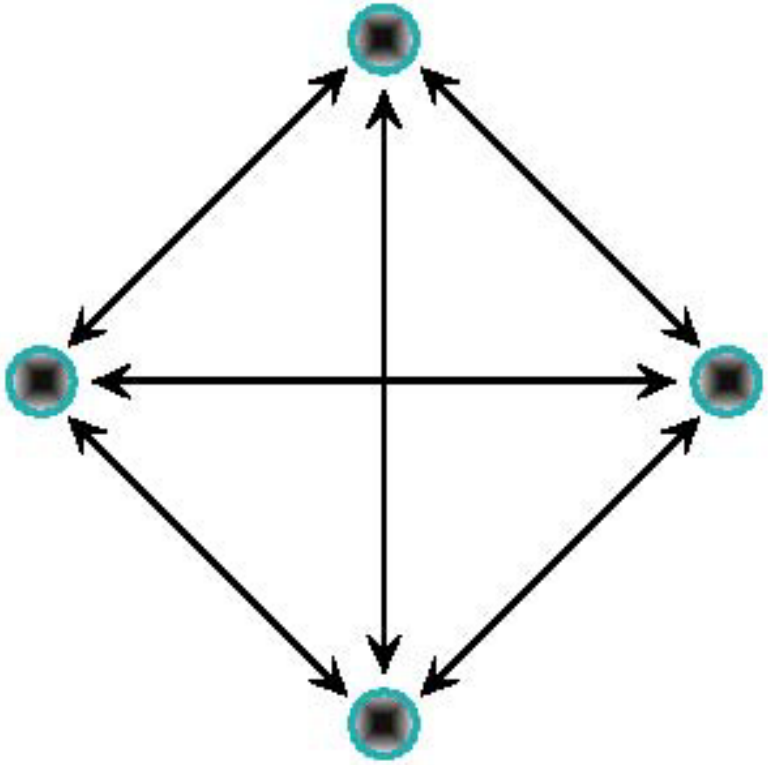
The Quadratic Curse

2 users

1 secret key

The Quadratic Curse

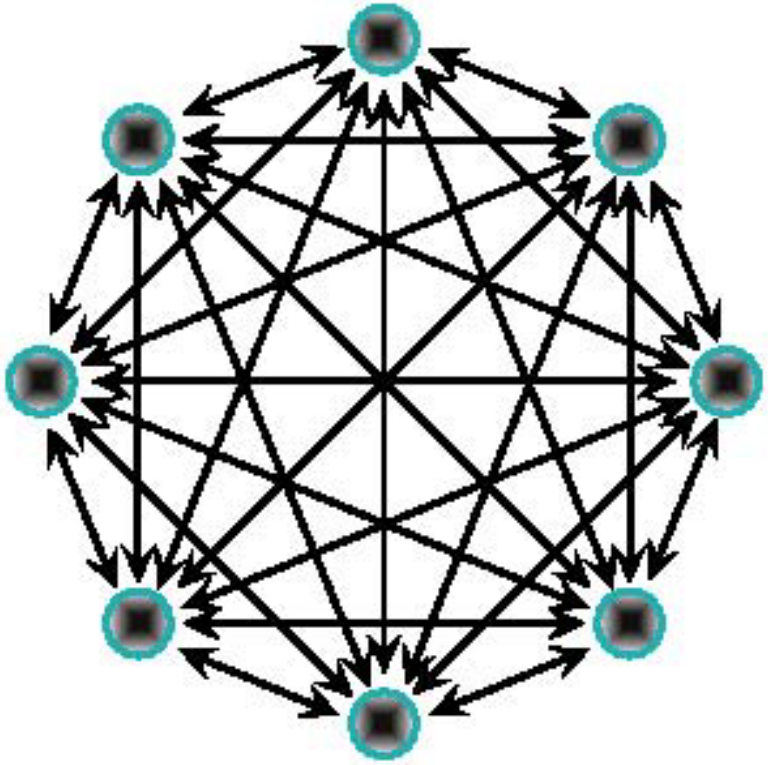
4 users



6 secret keys

The Quadratic Curse

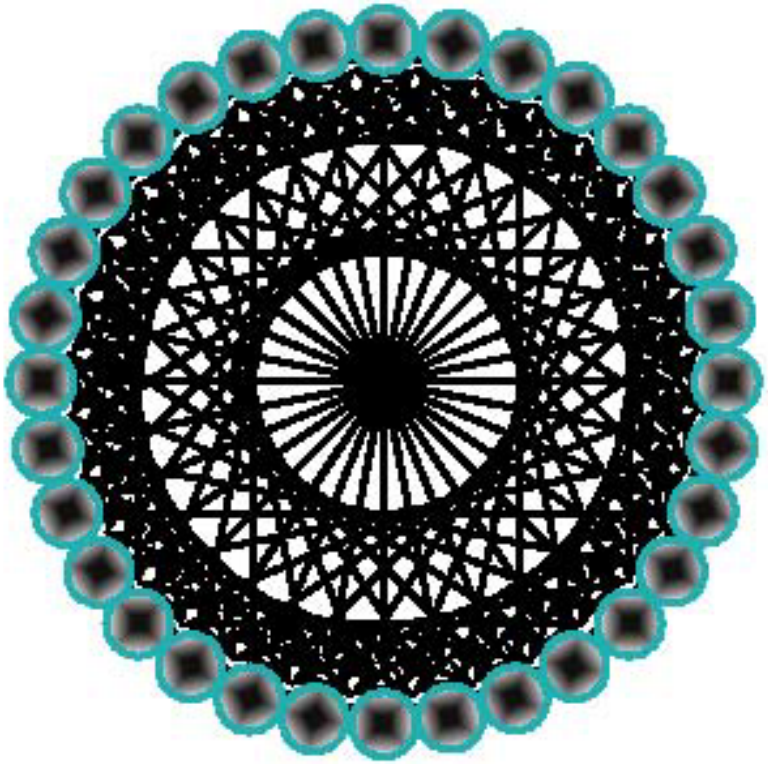
8 users



28 secret keys

The Quadratic Curse

n users



$\frac{n^2-n}{2}$ secret keys

CONJUGATE CODING TO THE RESCUE!

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

"BB84 quantum key distribution"

BB84 QKD

Version 1

A very high-level

Quantum Key Distribution

Bennett and Brassard (1984)

Quantum Key Distribution

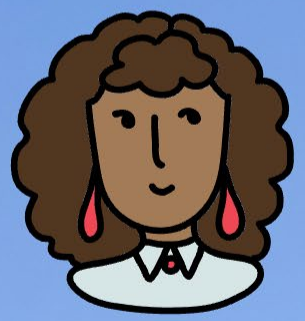
Bennett and Brassard (1984)

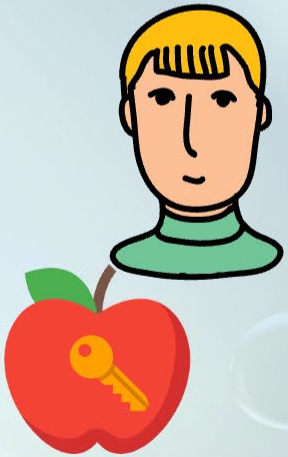
Quantum Key Distribution

Bennett and Brassard (1984)

Quantum Key Distribution

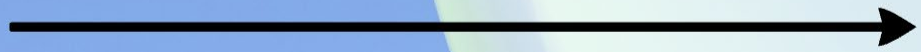
Bennett and Brassard (1984)

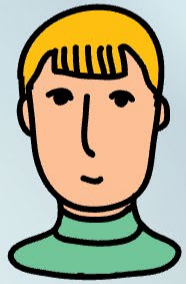




Quantum Key Distribution

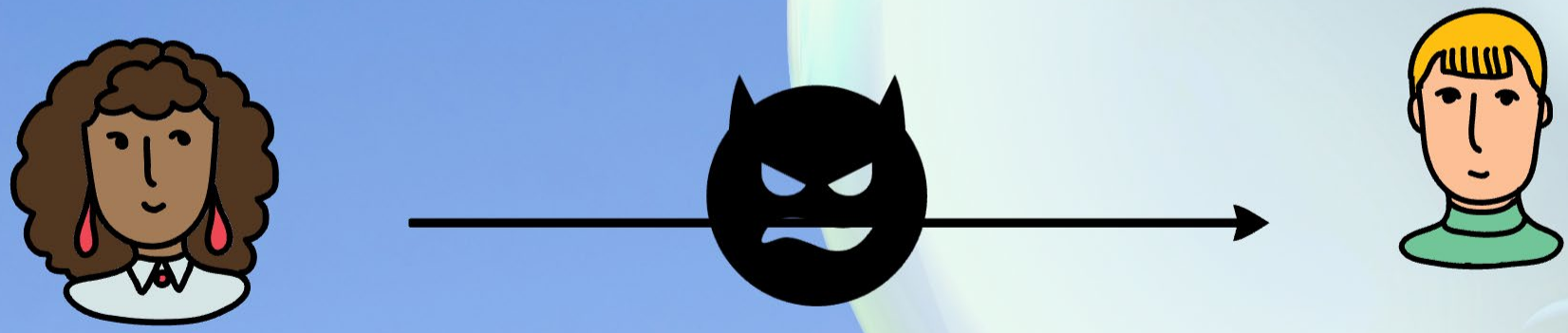
Bennett and Brassard (1984)





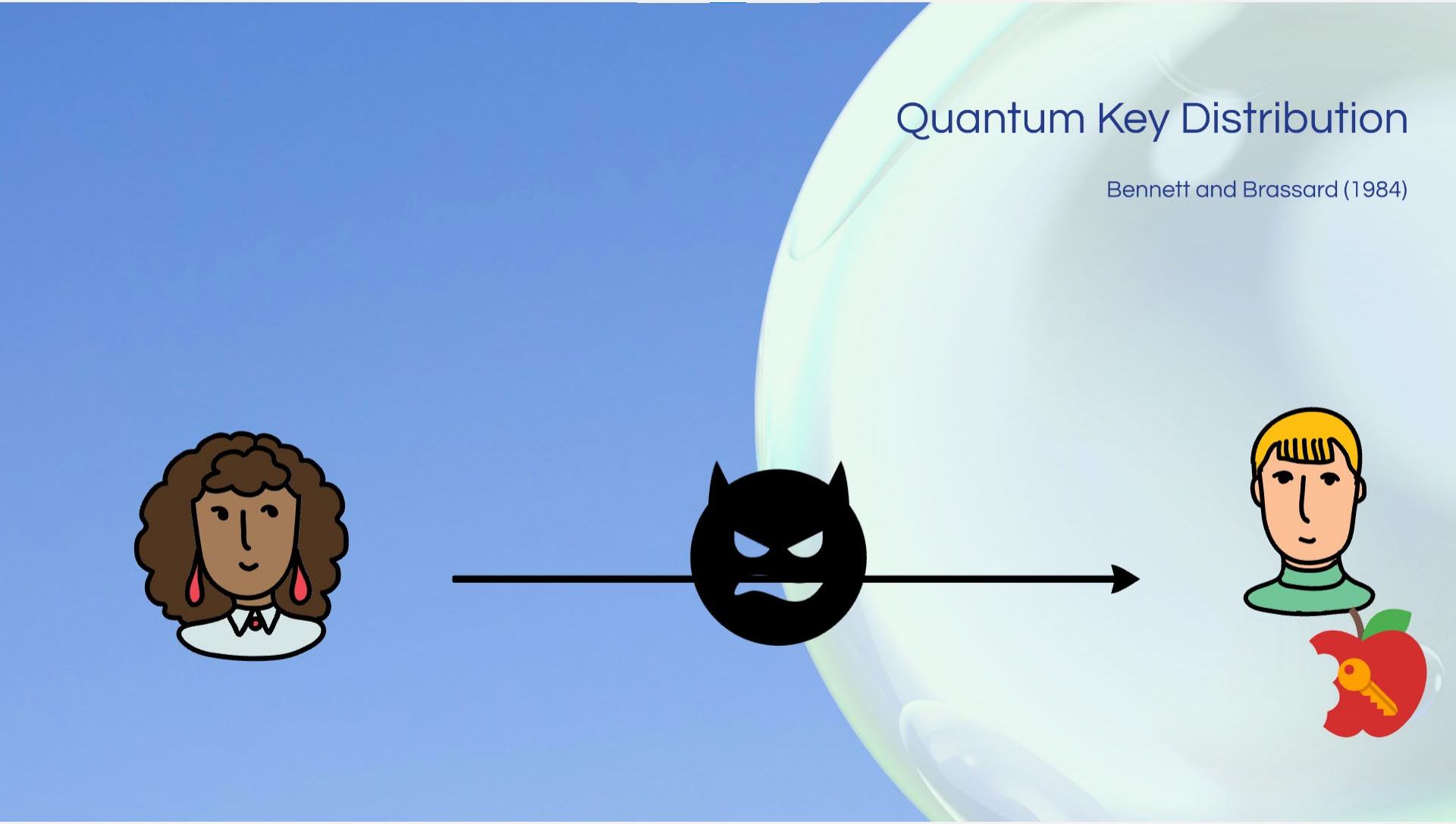
Quantum Key Distribution

Bennett and Brassard (1984)



Quantum Key Distribution

Bennett and Brassard (1984)



Quantum Key Distribution

- Use quantum channel to send a random key
- If no eavesdropping detected, use the one-time pad to send message

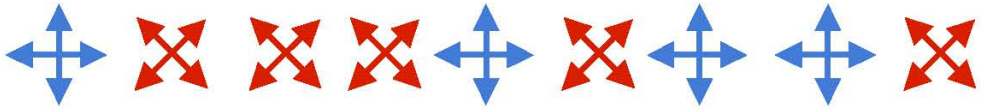
BB84 QKD

Version 2

A high-level

« BB84 » Protocol (Bennett & Brassard, 1984)

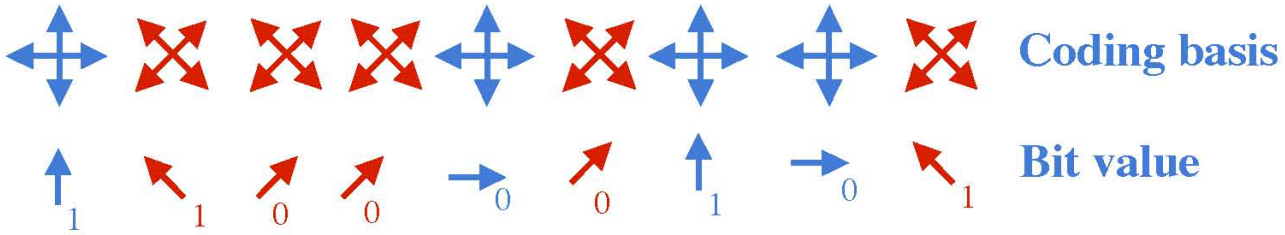
Alice



Coding basis

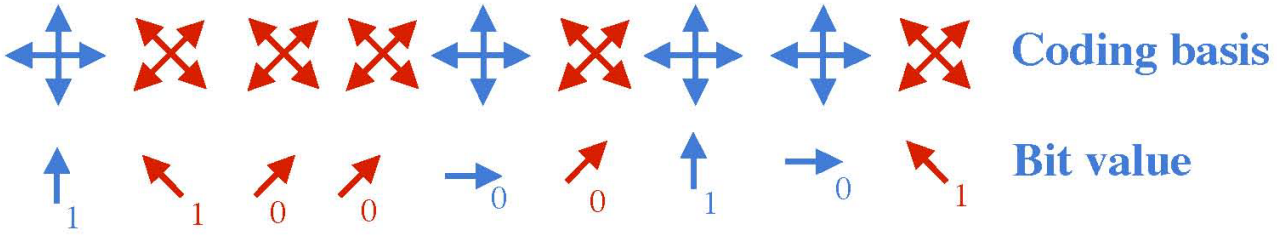
« BB84 » Protocol (Bennett & Brassard, 1984)

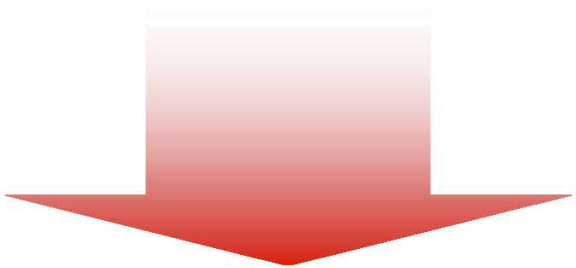
Alice



« BB84 » Protocol (Bennett & Brassard, 1984)

Alice

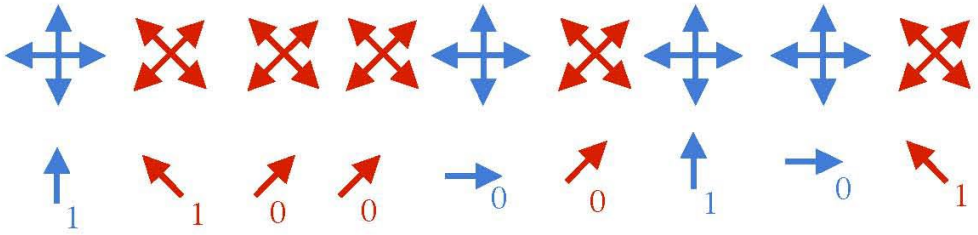


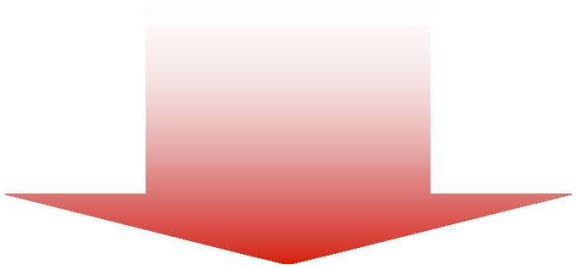


Bob

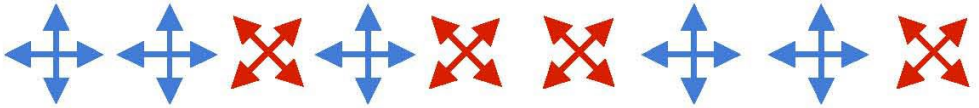
« BB84 » Protocol (Bennett & Brassard, 1984)

Alice



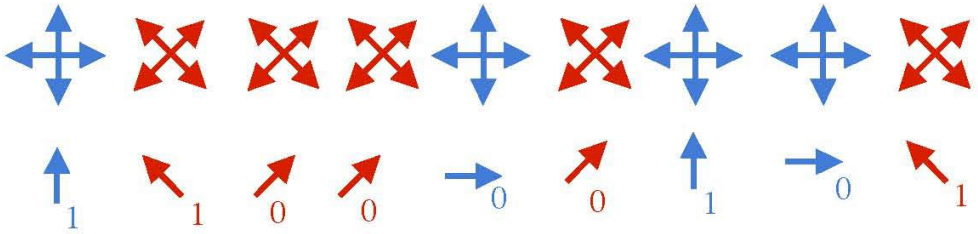


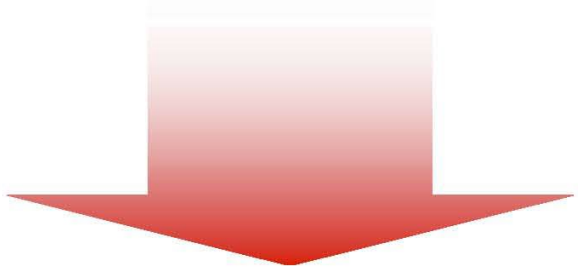
Bob



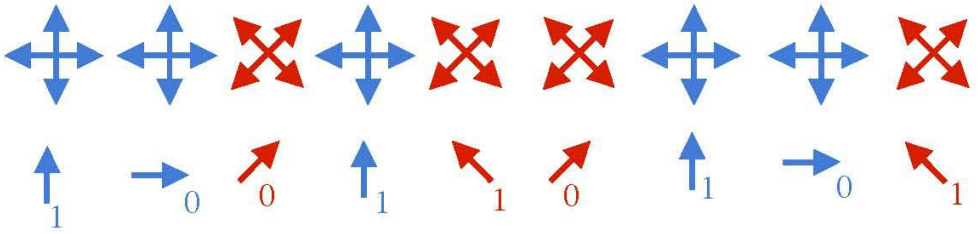
« BB84 » Protocol (Bennett & Brassard, 1984)

Alice



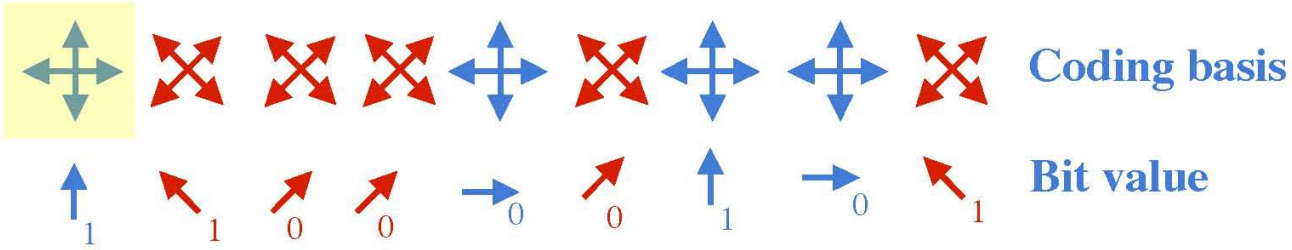


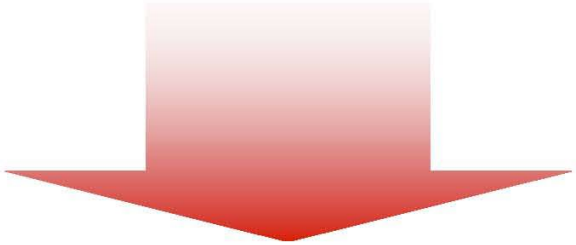
Bob



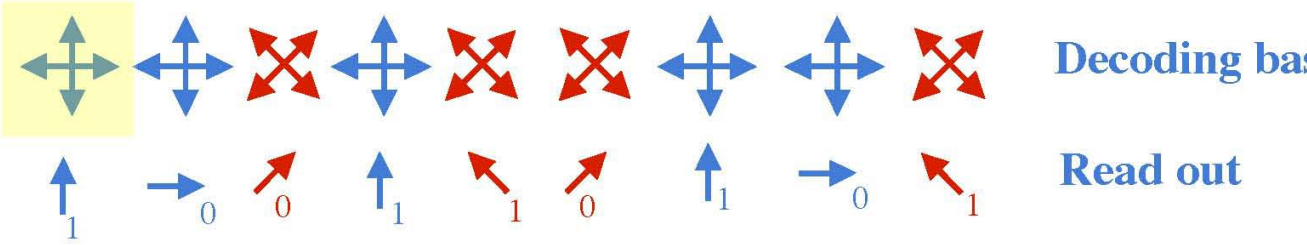
« BB84 » Protocol (Bennett & Brassard, 1984)

Alice



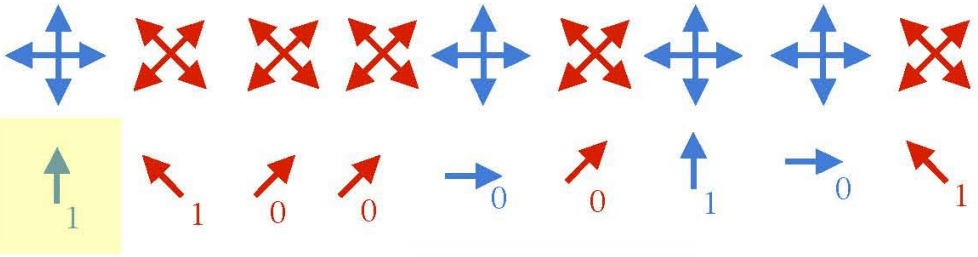


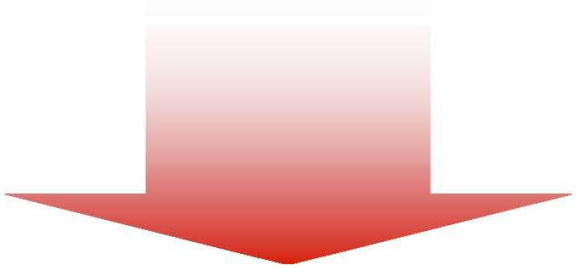
Bob



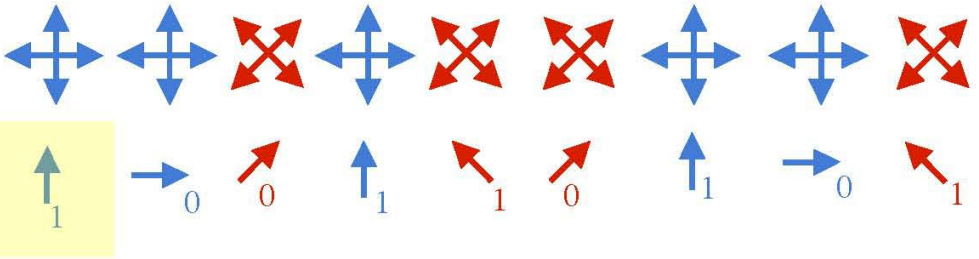
« BB84 » Protocol (Bennett & Brassard, 1984)

Alice



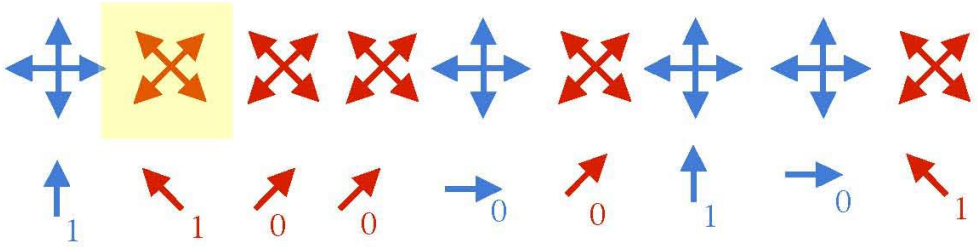


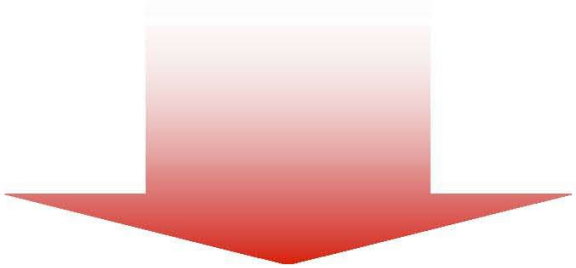
Bob



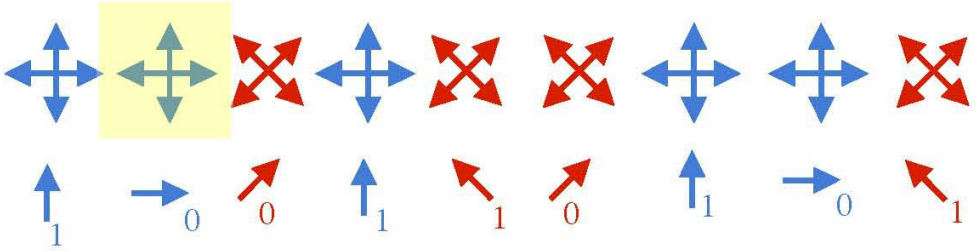
« BB84 » Protocol (Bennett & Brassard, 1984)

Alice



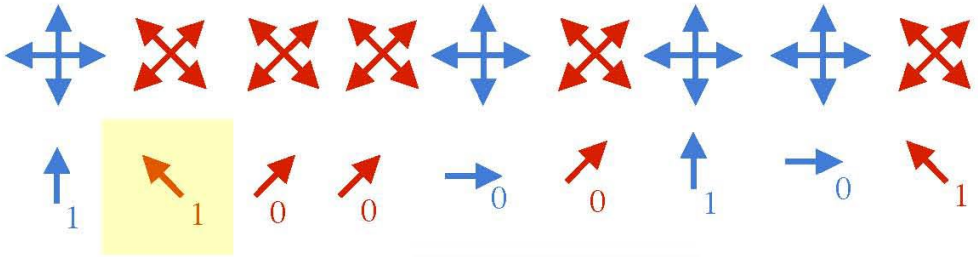


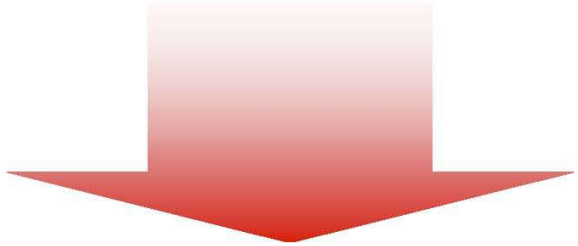
Bob



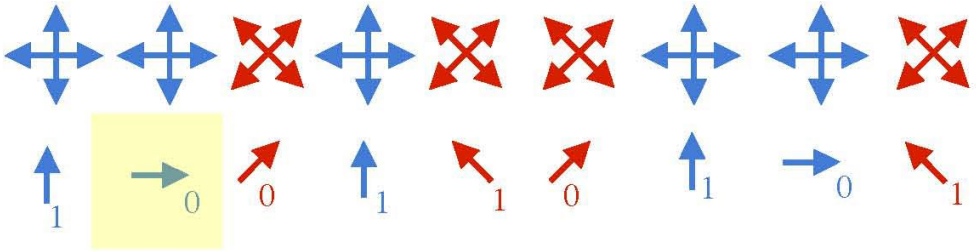
« BB84 » Protocol (Bennett & Brassard, 1984)

Alice



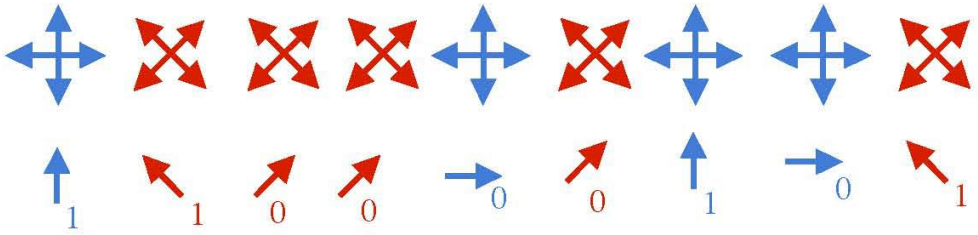


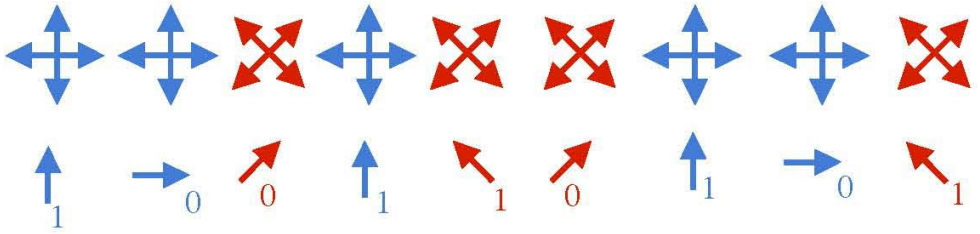
Bob



« BB84 » Protocol (Bennett & Brassard, 1984)

Alice



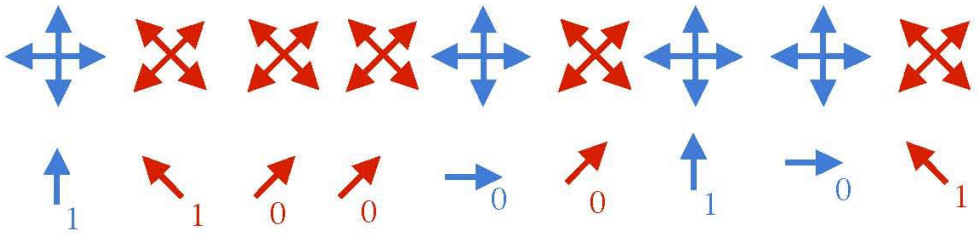


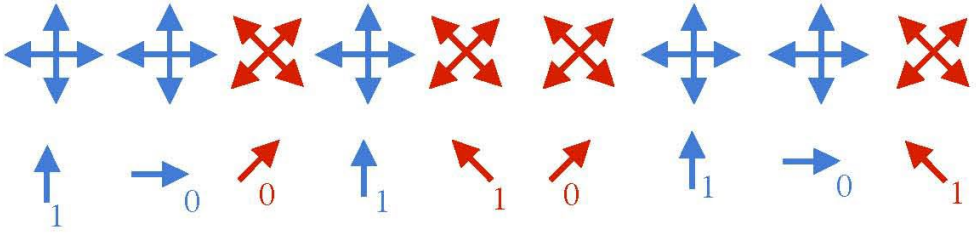
Bob

« BB84 » Protocol (Bennett & Brassard, 1984)

Alice

Bob

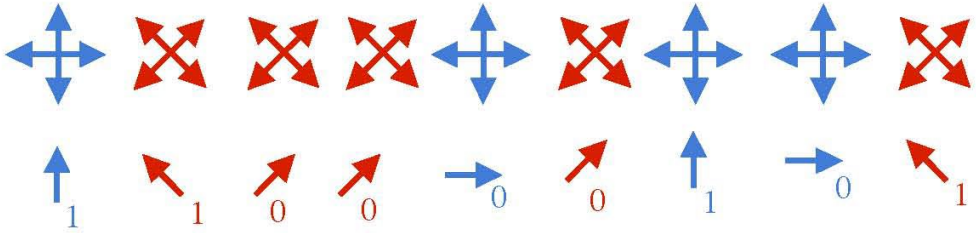


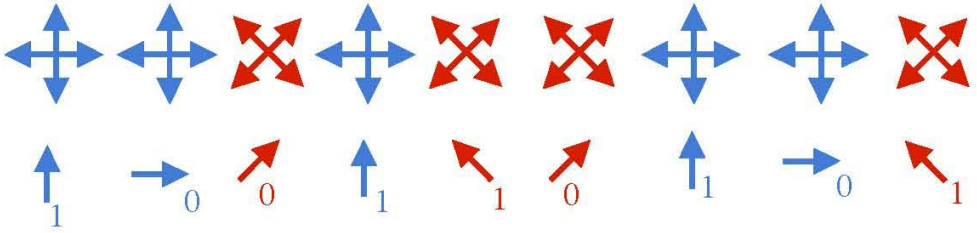


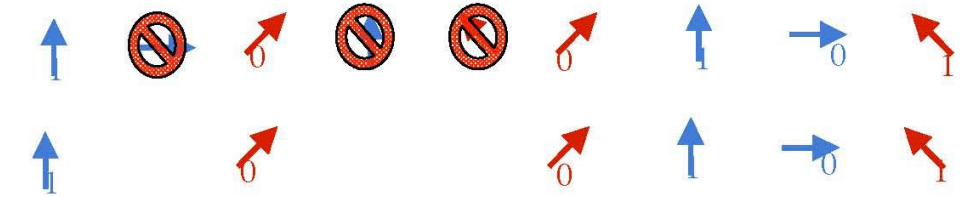
« BB84 » Protocol (Bennett & Brassard, 1984)

Alice

Bob



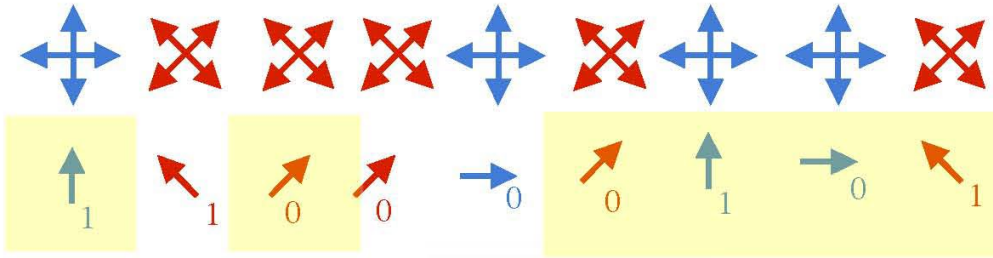


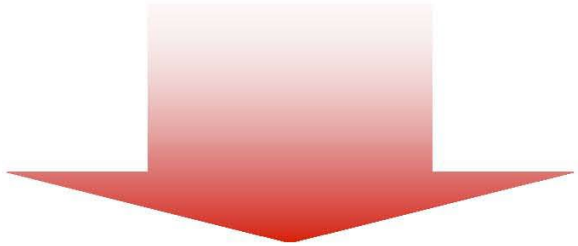


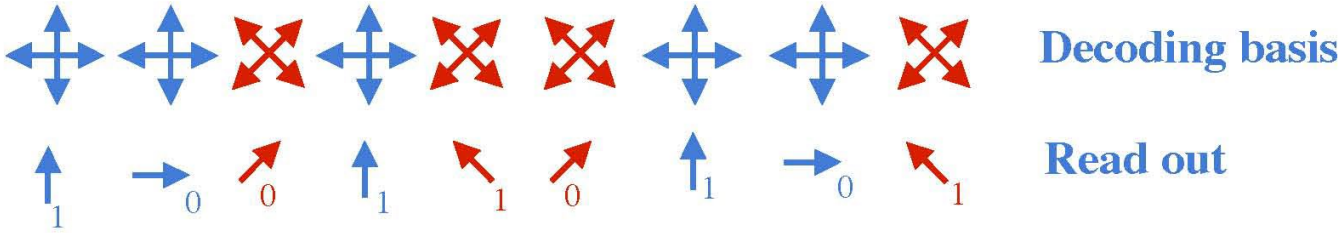
« BB84 » Protocol (Bennett & Brassard, 1984)

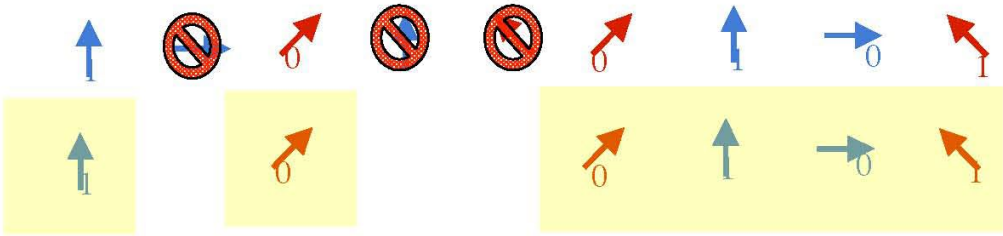
Alice

Bob

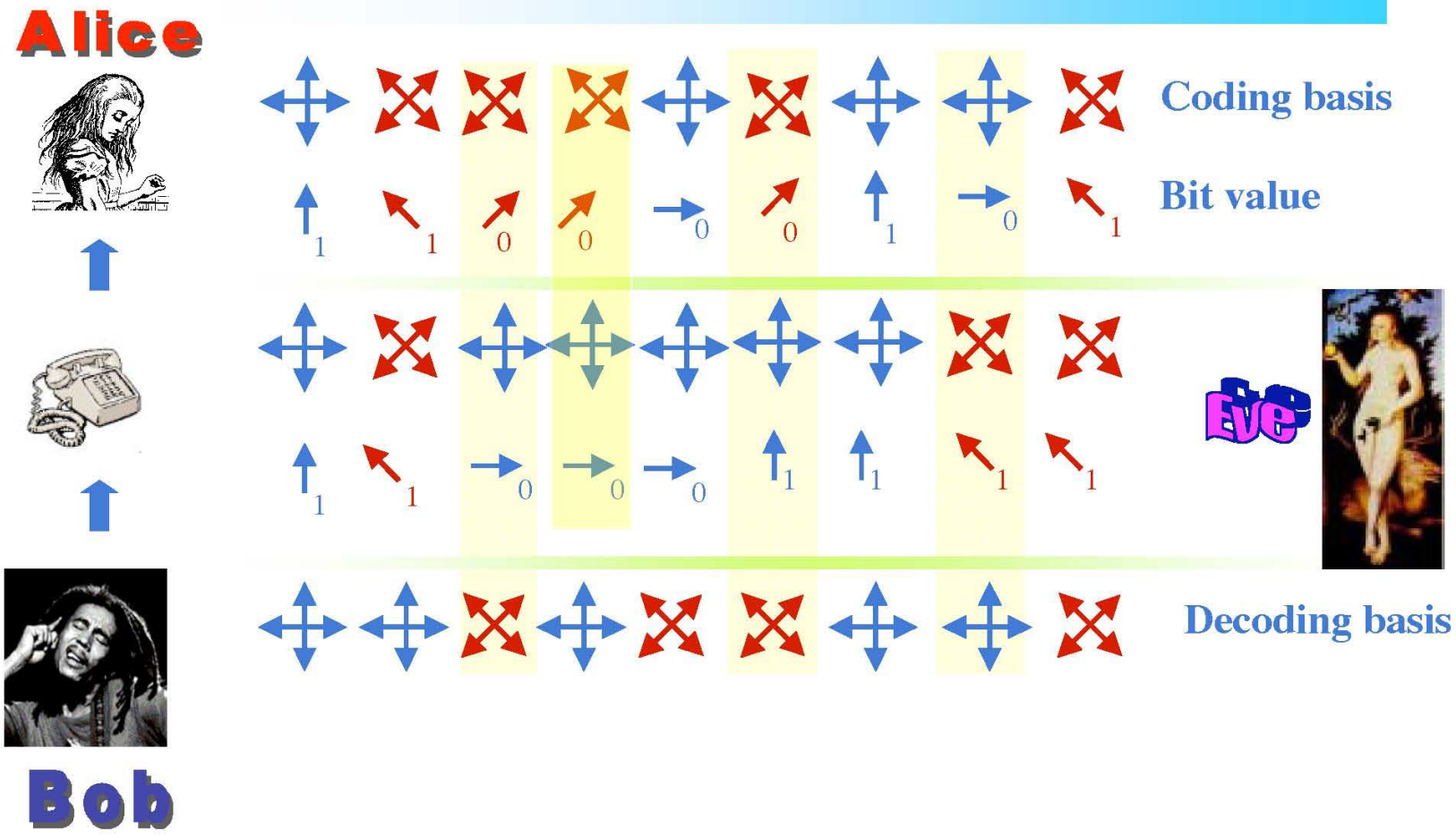








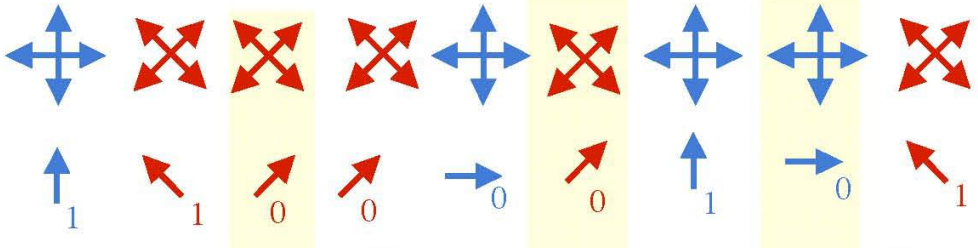
« BB84 » Protocol (Bennett & Brassard, 1984)



« BB84 » Protocol (Bennett & Brassard, 1984)

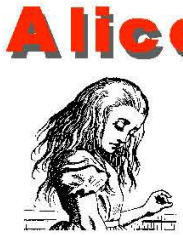
Alice

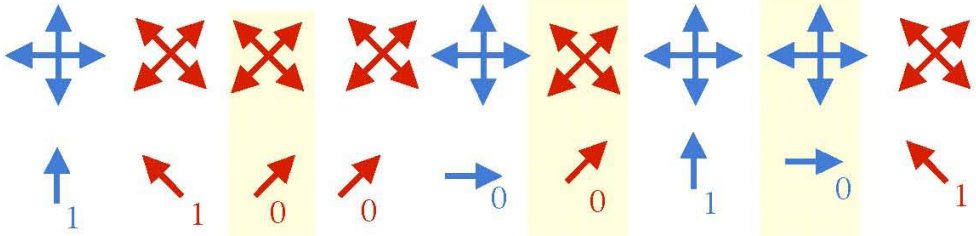
Bob

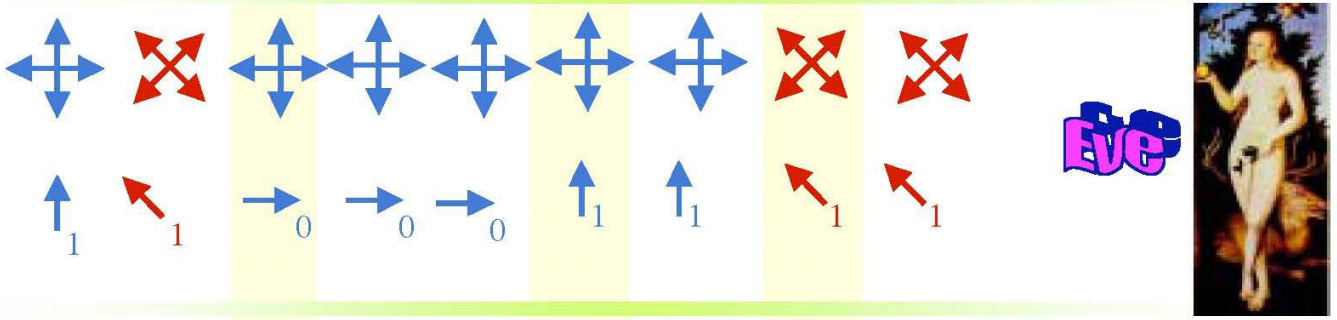


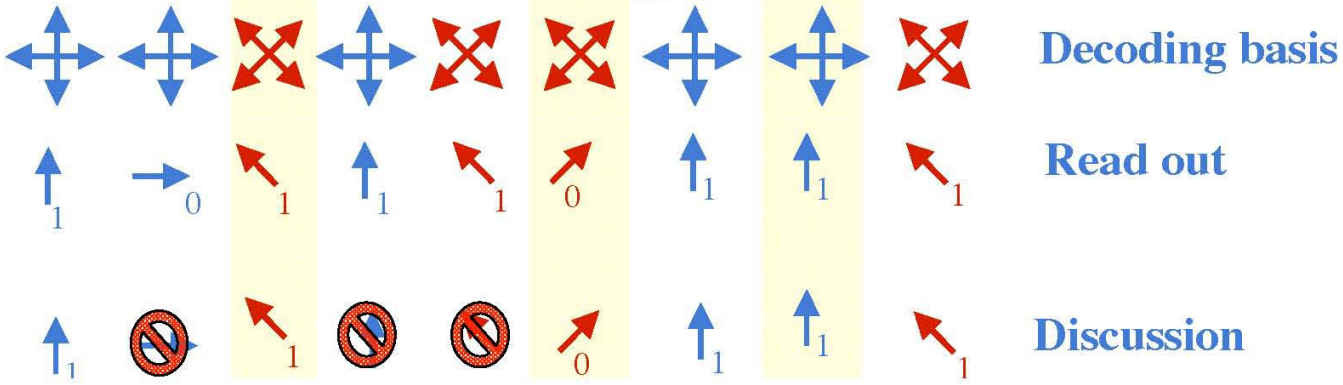
Eve

« BB84 » Protocol (Bennett & Brassard, 1984)

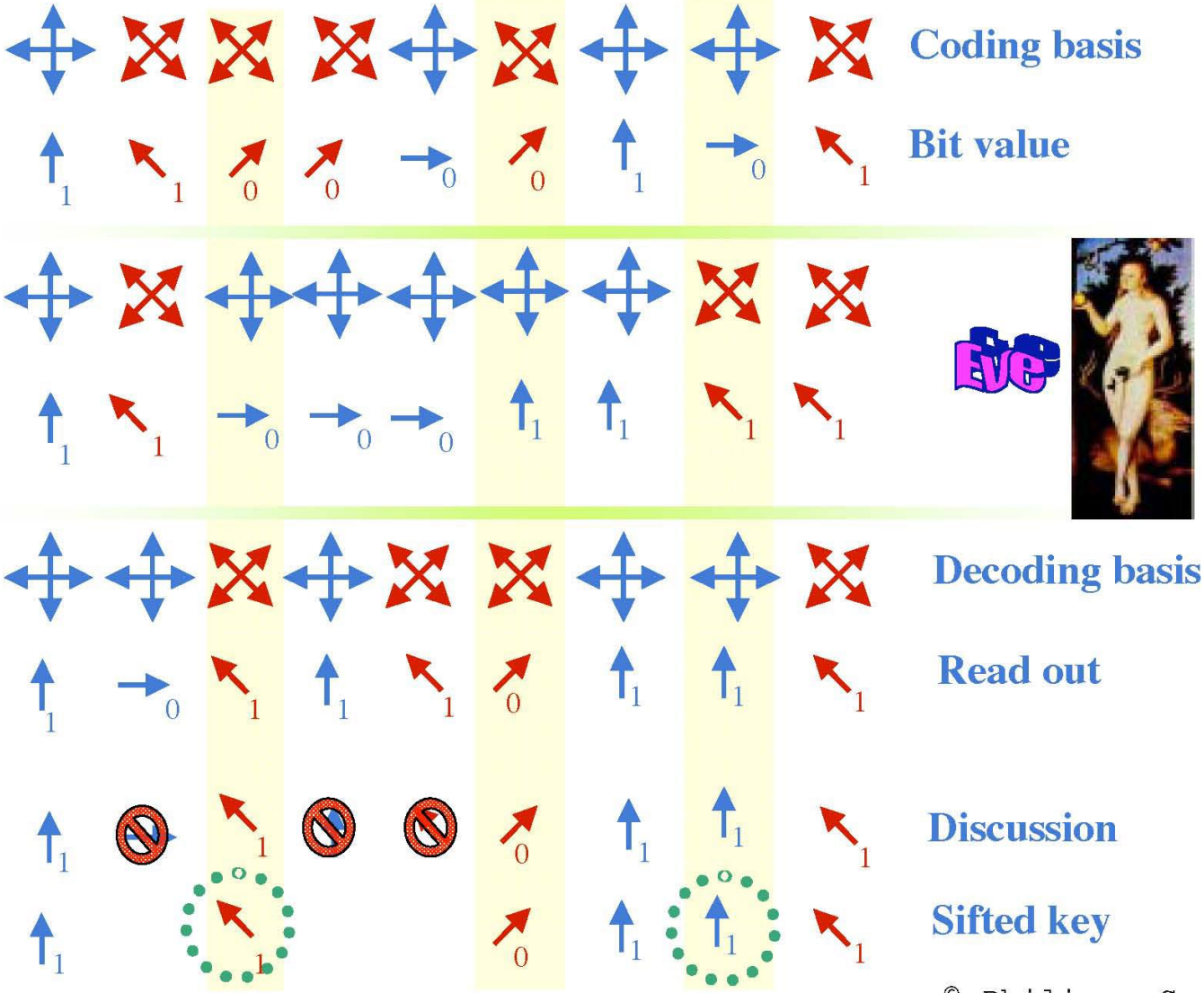




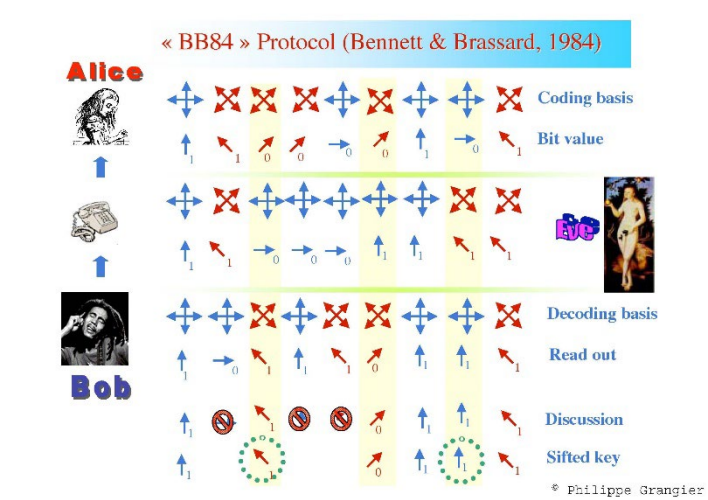




« BB84 » Protocol (Bennett & Brassard, 1984)



- QKD Assumes authenticated classical communication
  - Information-theoretic authentication can be achieved with a short initial shared secret (Wegman-Carter authentication)
  - Thus, QKD is more accurately described as a **key expansion** protocol.



- From a Sifted key to a private key (in a nutshell)
  - **Publicly compare** half of the sifted bits to obtain estimate of **error rate**. Abort if the error rate is too high (specific rate depends on parameter choice; approx. 11% is the theoretical maximum)
  - **Information Reconciliation (aka Error Correction):** corrects the remaining strings so that they agree in all positions with high probability.
    - Can be done via a series of parity checks, or more generally, using error correcting codes.
  - **Privacy amplification:** Eve has some information about the key (from eavesdropping and Information Reconciliation).
    - Alice and Bob apply a **random hash function** $\{0,1\}^n \rightarrow \{0,1\}^l$

Security of BB84 Quantum Key distribution?

- Security of QKD is often informally attributed to the no-cloning theorem.
- Actual proofs (which appeared 15 years later or more) use much more sophisticated techniques
  - Quantum error correcting codes
  - De Finetti reductions
  - Entropic uncertainty relations
  - **Sampling**
- More formal presentation and analysis of QKD to come.

QKD Firsts

- 1989: First Experimental demonstration
- 1998-2000: First proofs of security for QKD
- 2004: First bank transfer using QKD
- 2008: First network secured with QKD (200km, 6 nodes)
- 2016: First quantum satellite for space-to-ground quantum communication.

QKD Commercial Products

IDQ
FROM VISION TO TECHNOLOGY

MagiQ

Quintessence Labs
Data Uncompromised

Practicality of BB84 Quantum Key

- Alice only needs to prepare & send single-qubits.
- Bob only needs to measure single qubits in a random basis
- Error correction is integrated into the protocol so that under a small amount of noise:
  - The protocol does not abort
  - The noise is corrected and the final keys agree.

Noise-tolerant, single-qubit prepare-and-measure

Recent Direction in QKD

- Device-independent and one-sided device-independent QKD
  - See Qcrypt 2019 Tutorial by Rotem Arnon Friedman (https://youtu.be/5KsW0d9JeqQ)
- Continuous-Variable QKD
- Finite-size effects in QKD
- Side-channel attacks
- ….

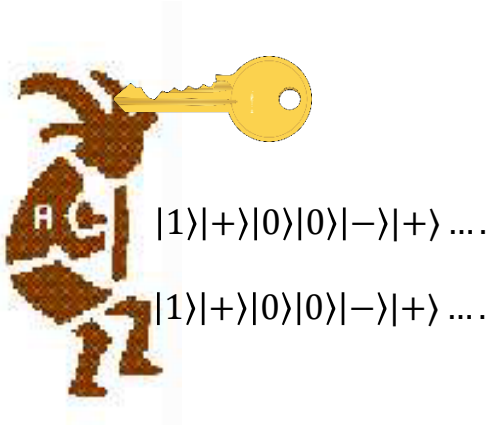
A Sampling-based proof of QKD

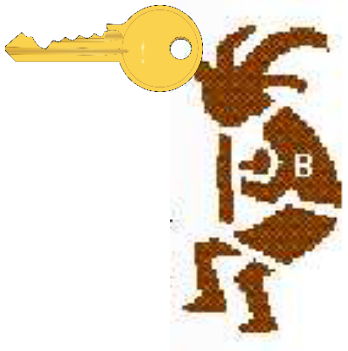
Bouman, N. J., & Fehr, S. (2010). Sampling in a quantum population, and applications. In *Annual Cryptology Conference CRYPTO* (pp. 724-741).

Fehr, S. (2010). Quantum cryptography. *Foundations of Physics*, *40*(5), 494-531.*

*notation, equations and figures from this reference

BB84 quantum key distribution protocol



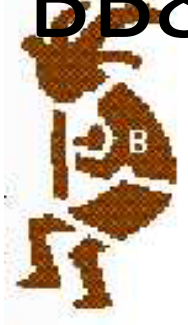


Prepare $|b\rangle_\theta$
for random $b, \theta \in \{0,1\}^n$

- Measure each qubit in a *random* basis.
- Compare a sample of (basis, outcome) pairs with Alice.
- Either noise level is too high and they abort, or they amplify the secrecy of the remaining measurement outcomes.

Entanglement-based BB84

Measure each qubit in a *random* basis θ.



- Same as before.

A B E

ρ_{ABE}

If Eve sends $\rho_{ABE} = 1/\sqrt{2}\,(|00\rangle + |11\rangle) \otimes \rho_E$, then:

- $\theta = 0$: If Alice observes $|\mathrm{i}\rangle$, Bob's system becomes $|\mathrm{i}\rangle$
- $\theta = 1$: If Alice observes $\mathrm{H}|\mathrm{i}\rangle$, Bob's system becomes $\mathrm{H}|\mathrm{i}\rangle$ (check)

Claim: security of entanglement-based scheme implies security of original scheme

From now on: show security of the Entanglement-based QKD

Review : Hybrid classical-quantum systems

X: random variable with finite range $\mathcal{X}$, P_X probability distribution

$$\rho_E = \sum_x P_X(x)\rho_{E|X=x}$$

a quantum system E that is randomized: with probability P_X, the system is $\rho_{E|X=x}$.

We can "encode" the choice of x into a quantum state $|x\rangle$, and denote the hybrid classical-quantum ("c-q") system:

$$\rho_{XE} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_{E|X=x}$$

Let $\rho_X = \mathrm{tr}_E(\rho_{XE}) = \sum_x P_X(x)|x\rangle\langle x|$

X is **independent** of E if and only if $\rho_{XE} = \rho_X \otimes \rho_E$

Let μ_X denote the completely mixed state $\mu_X = \frac{1}{|\mathcal{X}|}\sum_x |x\rangle\langle x| = \frac{1}{|\mathcal{X}|}\mathbb{I}_X$

X is **random-and-independent** of E if and only if

$$\rho_{XE} = \mu_X \otimes \rho_E$$

Trace distance and Security of a key

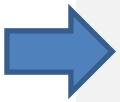
For two density matrices ρ, σ, the ***trace distance*** $\delta(\rho, \sigma) = \frac{1}{2} tr|\rho - \sigma|$ where $|\rho - \sigma|$ is the unique positive semi-definite square root of $(\rho - \sigma)(\rho - \sigma)^*$

The **operational meaning** is more important for us: for any physical processing, the two states behave identically, except with probability at most $\delta(\rho, \sigma)$

For key distribution, we'll say that the scheme is **secure** if the trace distance $\delta(\rho_{XE}, \mu_X \otimes \rho_E)$ is small.

- Shown to be the "right" ("composable") definition [Koenig-Renner 2005, Ben-Or et al. 2005]

Error Correction



- From a Sifted key to a private key :
  - **Publicly compare** half of the sifted bits to obtain estimate of **error rate**. Abort if the error rate is too high (specific rate depends on parameter choice; approx. 11% is the theoretical maximum)
  - **Information Reconciliation (aka Error Correction):** corrects the remaining strings so that they agree in all positions with high probability.
    - Can be done via a series of parity checks, or more generally, using error correcting codes.
  - **Privacy amplification:** Eve has some information about the key (from eavesdropping and Information Reconciliation).
    - Alice and Bob apply a **random hash function** $\{0,1\}^n \to \{0,1\}^k$

- Let X_i be Alice's bit string and Y_i be Bob's ($i = 1, \ldots n$),
- Error Correction: Alice chooses a random codeword $\mathrm{C} \in \{0,1\}^n$ from a suitable error correcting code and sends $\mathrm{U} = \mathrm{C} \oplus X$ to Bob. Bob decodes $\mathrm{C}' = U \oplus Y$ to the closest codeword $\hat{C}$ and computes $\hat{X} = \hat{C} \oplus U$ as his guess for X.
  - If X, Y differ in only a few positions, $\mathrm{C}' = U \oplus Y = \mathrm{C} \oplus X \oplus Y$ is close to C, so $\hat{C}$ =C, and Bob's guess for X is $\hat{X} = \hat{C} \oplus U = \mathrm{C} \oplus \mathrm{C} \oplus X = X$.
- For efficiency, note that in a linear code, Alice can send the syndrome of X instead of U. (Let k be the log of the size of the code; then the syndrome is $\mathrm{n} - \mathrm{k}$ bits in length)
- Error correction leaks information about X. We'll show how to compensate for this later.

Privacy Amplification

- From a Sifted key to a private key :
  - **Publicly compare** half of the sifted bits to obtain estimate of **error rate**. Abort if the error rate is too high (specific rate depends on parameter choice; approx. 11% is the theoretical maximum)
  - **Information Reconciliation (aka Error Correction):** corrects the remaining strings so that they agree in all positions with high probability.
    - Can be done via a series of parity checks, or more generally, using error correcting codes.
  - **Privacy amplification:** Eve has some information about the key (from eavesdropping and Information Reconciliation).
    - Alice and Bob apply a **random hash function** $\{0,1\}^n \to \{0,1\}^k$

Entropy: a measure of uncertainty in a system

- Shannon entropy: $\mathrm{H}(P_X) = -\sum_x P_X(x) \log P_X(x)$
- Min-entropy: $\mathrm{H}_\infty(P_X) = -\log\left(\max_x P_X(x)\right)$ (captures how hard it is to guess the value described by the random variable X)
- Conditional min-entropy: $\mathrm{H}_\infty(P_{XY}|Y)$ same as entropy, with an auxiliary Y.
- **Quantum conditional min-entropy** for a c-q state ρ_{XE} is the negative-log of the success probability of predicting X when using an optimal strategy and having access to the quantum system E.

Privacy Amplification

- **Quantum conditional min-entropy** for a c-q state ρ_{XE} is the negative-log of the success probability of predicting X when using an optimal strategy and having access to the quantum system E.
- **Quantifies how much uncertainty Eve has on classical X.**

Privacy Amplification: transforms a bound the conditional min-entropy into a uniform key.

- Key K is computed as $K = f(S, X)$ ($S^{P[f(S,x)=f(S,x')] \leq \frac{1}{|\mathcal{K}|}}$);
- f is a **universal hash function** if for all $x \neq x'$,
- The privacy amplification theorem [Renner and Koening (2005)] tells us that for such an f with an ℓ-bit output:

Next step: bounding the conditional quantum min-entropy!

$$\delta(\rho_{KSE}, \mu_K \otimes \rho_{SE}) \leq \frac{1}{2} \cdot 2^{-\frac{1}{2}(\mathrm{H}_\infty(X|E)-\ell)}$$

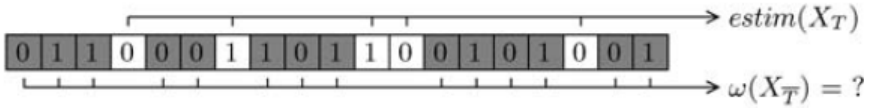
For ℓ at most the quantum conditional min-entropy, we get an ℓ-bit, uniform key (up to some exponentially small error)

Classical sampling: estimating the relative Hamming weight

- **Hamming weight** of bit string $X = X_1, X_2, \ldots X_m$ is $\mathrm{W}(X) = \sum_i X_i$;
- **Relative Hamming weight** is $\omega(X) = \frac{W(X)}{m}$
- Define $\omega(X) \approx_\epsilon \beta$ if $|\omega(X) - \beta| \leq \epsilon$.

Given a unknown $X = X_1, X_2, \ldots X_m$, consider the following "sample-and-estimate strategy" :

  - Choose a random subset $T(X)$ of $\{1, \ldots, m\}$ of size linear in m, and output $\omega(X_T)$ as estimate of $\omega(X_{\bar{T}})$.

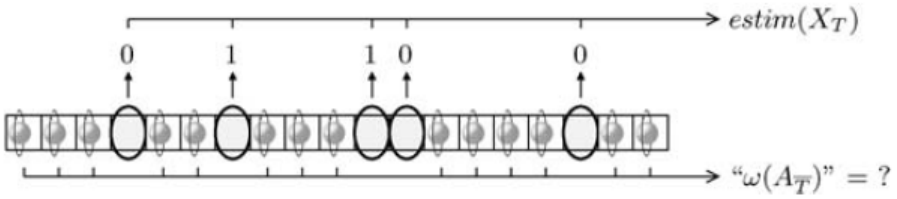


- Define the **error probability** $err_\varepsilon(m) := \max_{x \in \{0,1\}^m} P\left[\omega(x_{\bar{T}}) \not\approx_\varepsilon estim(x_T)\right]$
- **Claim:** for the above strategy: $err_\varepsilon(m) \leq 2e^{-\varepsilon^2 \alpha m/2}$,

  where T is of size αm.

Quantum sampling

Given an unknown $A = A_1, A_2, \ldots A_m$, (possibly entangled with a system E), consider the strategy of measuring a subset T of the qubits in the computational basis, as an estimate of the "relative Hamming weight".



Theorem [Bouman, Fehr 2010]: (informal) If the estimation strategy has a small error in the classical case, then it also has a small error in the quantum case: after the measurement of A_T (giving estimate β) the state of $A_{\bar{T}}E$ is of the form

$$|\varphi_{A_{\bar{T}}E}\rangle = \sum_y \alpha_y |y\rangle \otimes |\varphi_E^y\rangle$$

where the y's are such that $\omega(y) \approx \beta$; except with some small error.

Quantum sampling in QKD

Let $\rho_{\theta \mathrm{ABE}}$ be the c-q state after the sifting.
Alice obtains X_i when measuring in basis θ
Bob obtains Y_i when measuring in basis θ

Define $$S_i = X_i \oplus Y_i \quad \text{and} \quad W_i = \begin{cases} X_i & \text{if } \Theta_i = 0, \\ Y_i & \text{if } \Theta_i = 1, \end{cases}$$

Let $\rho_{\theta XYSWE}$ be the corresponding c-q state. We can obtain this state instead by applying the unitary $U|b\rangle|c\rangle = H|b\rangle|b \oplus c\rangle$: Note that $U(H|b\rangle H|c\rangle) = |b \oplus c\rangle H|c\rangle)$, so after U, S_i is in the first or second register depending on θ_i, and W_i is in the other register. From these, we can compute X_i, Y_i. Let $\sigma_{\theta XYSWE}$ be the resulting state. Then $\rho_{\theta XYSWE}$ = $\sigma_{\theta XYSWE}$.

Idea: take $\theta_i = 0$ to be the sample subset T in the sampling technique on the state obtained after U. So the estimate β of the relative Hamming weight is the computed error rate in QKD. By the Bouman-Fehr Theorem, the error in the estimate β of the relative Hamming weight for the **rest** of the system is exponentially small, hence we are close to $\sum_z \alpha_z |z\rangle \otimes |\varphi_E^z\rangle$, where each z has Hamming weight approx. β.

Quantum sampling in QKD

We are close to $\sum_z \alpha_z |z\rangle \otimes |\varphi_E^z\rangle$, where each z has Hamming weight approx. β.

Lemma (Bouman-Fehr): Given the state above and thanks to the fact that β is small, we can bound the min-entropy of W, obtained by measuring in the Hadamard basis

$$\mathrm{H}_\infty(W|ES\Theta Test) \geq n - \mathrm{h}(\beta+\varepsilon)n$$

$$\mathrm{h}(p) = -(p\cdot\log(p) + (1-p)\cdot\log(1-p))$$

This implies the same bound for $\mathrm{H}_\infty(X|ES\Theta Test)$.

It remains to compensate for the further classical information that Eve gets. By the chain rule, each bit of communication costs at most a bit of quantum min-entropy. After compensating for X_{test} and the error-correction syndrome, we are left with min-entropy at least at least $(1-2\mathrm{h}(\beta))n$.

Privacy amplification completes the proof.