Introduction to theoretical quantum CRYPTOGRAPHY

Claude Crépeau

School of Computer Science
McGill University

(1) Classical Cryptography

(1.1) Information Theoretical Cryptography

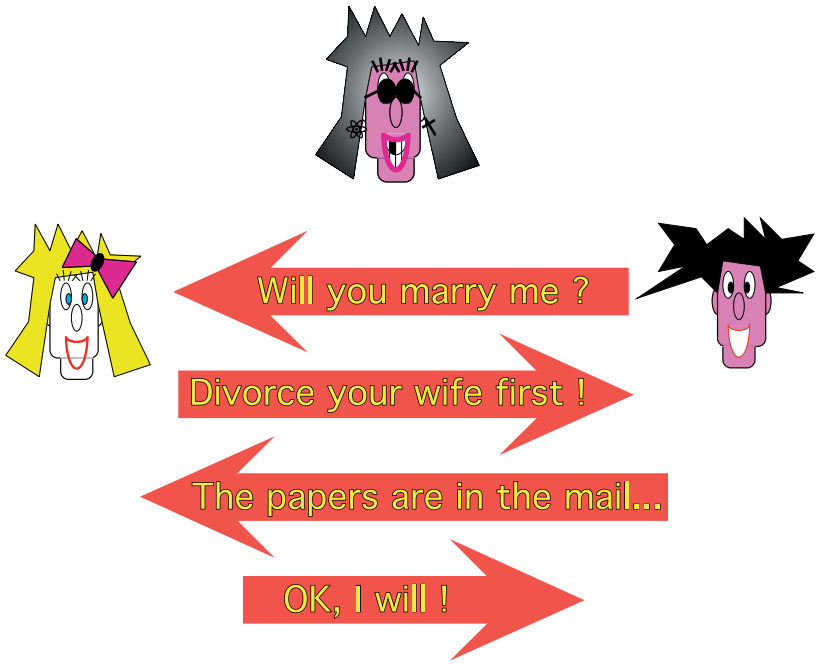
(1.1) Information Theoretical Cryptography

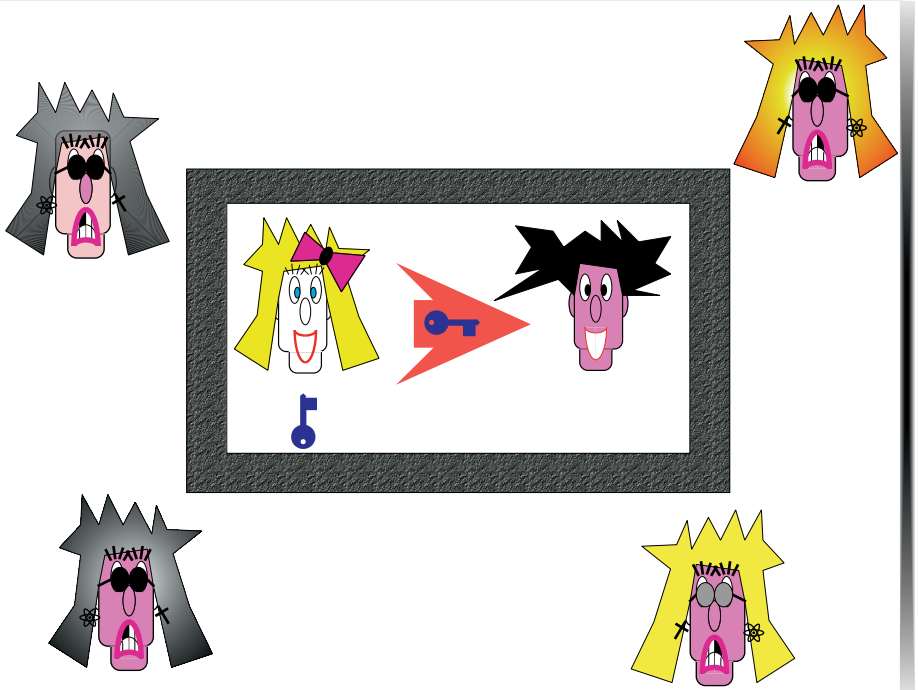
(1.1.1) key distribution

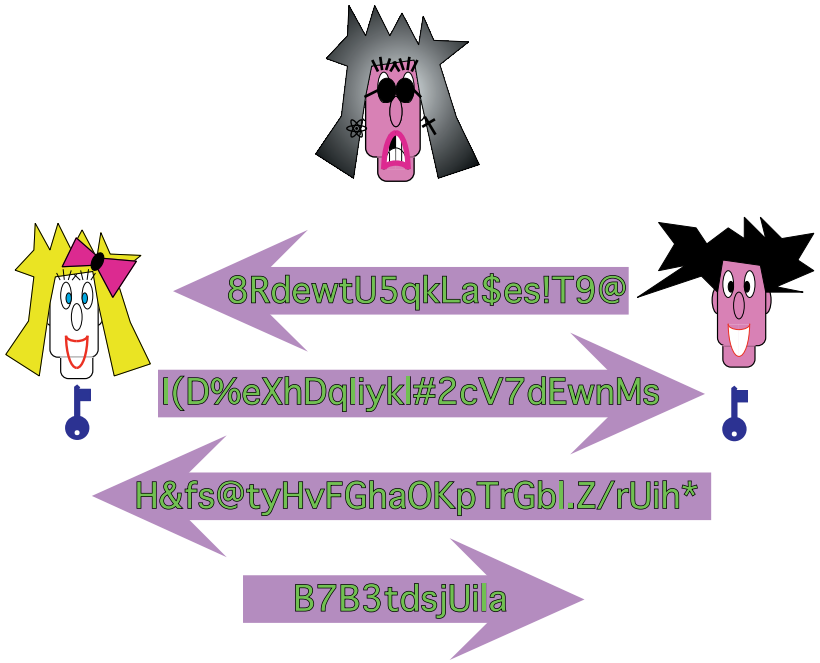
(1.1.2) Encryption

(1.1.3) Authentication

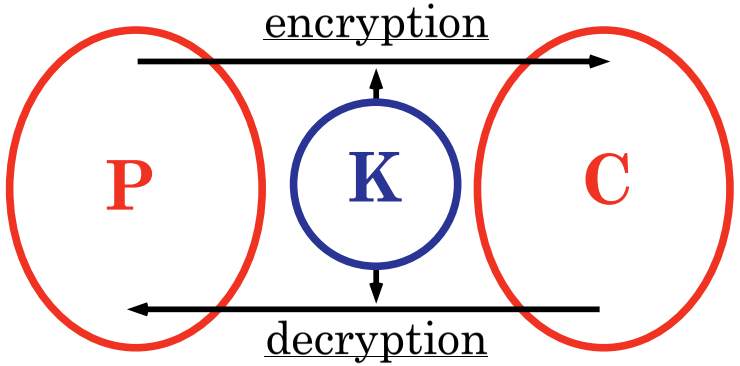
.....





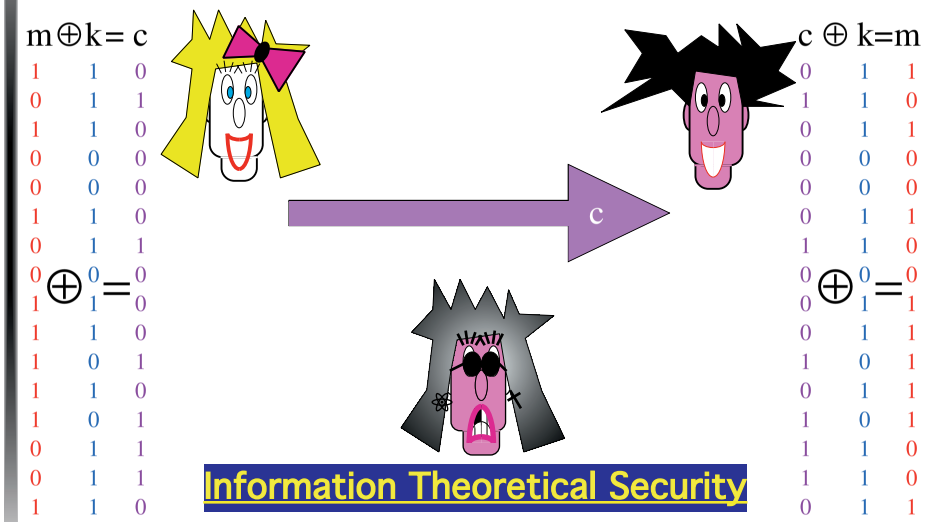


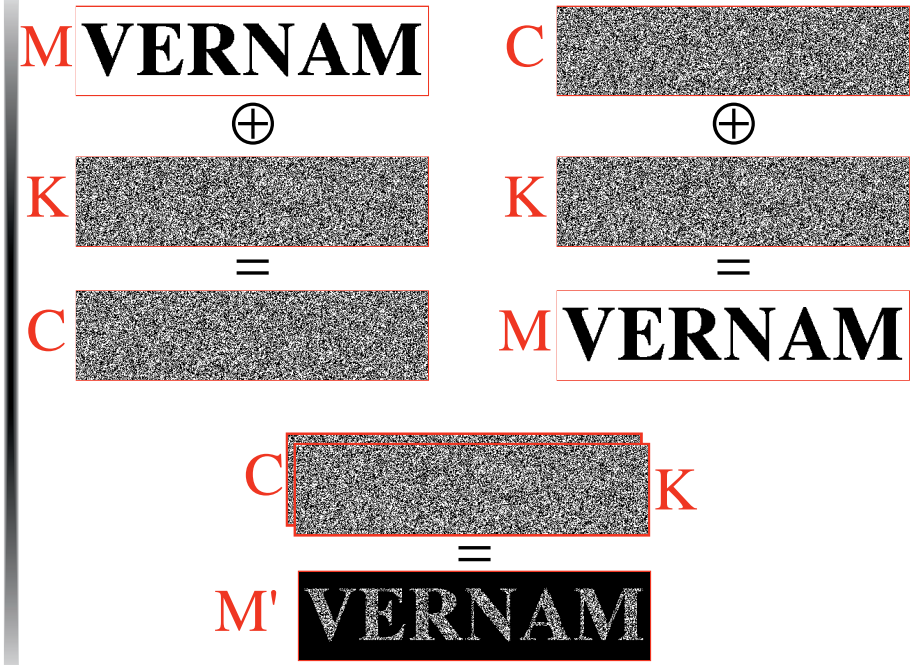
symmetric encryption



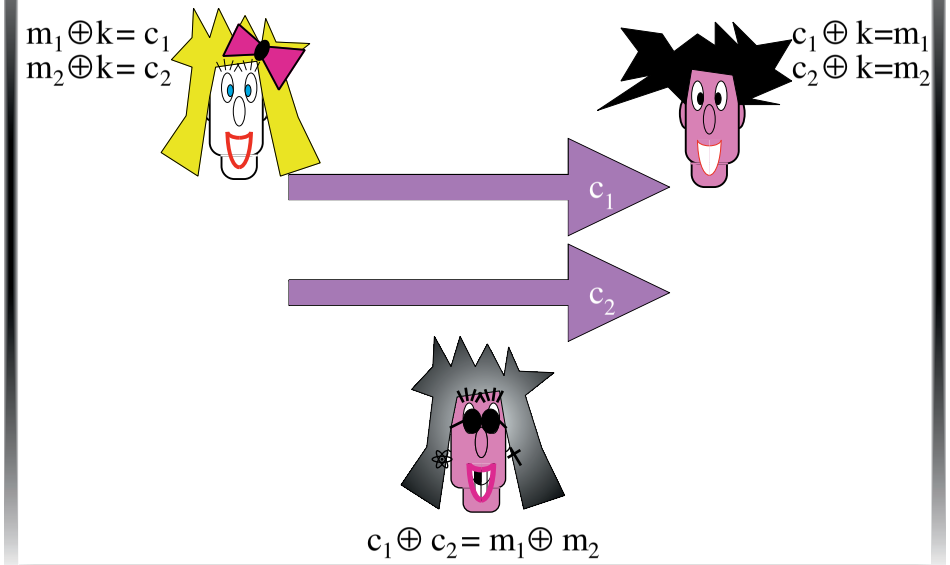
Information Theoretical Security

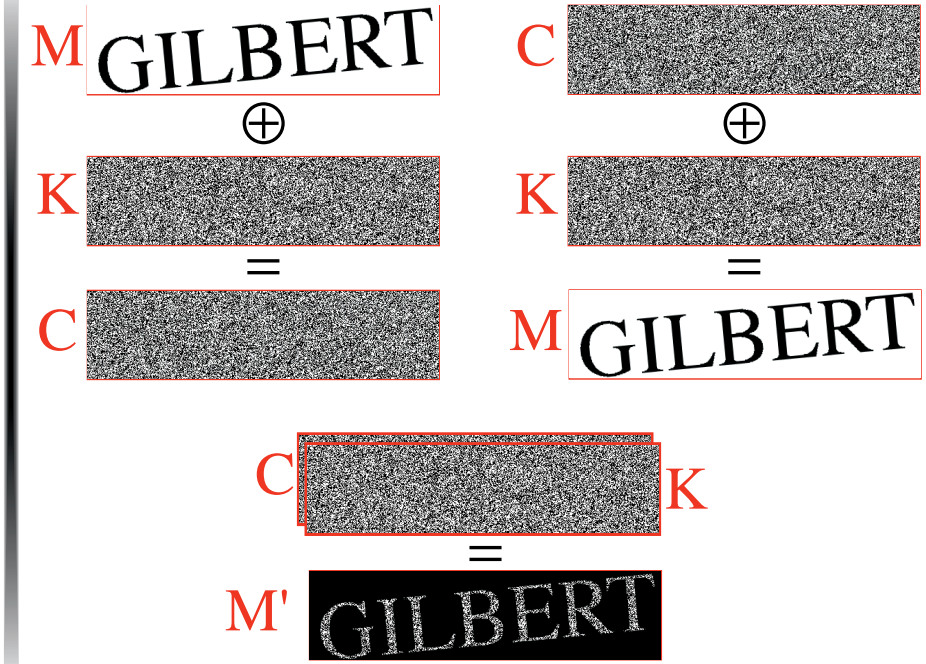
Vernam's One-Time-Pad

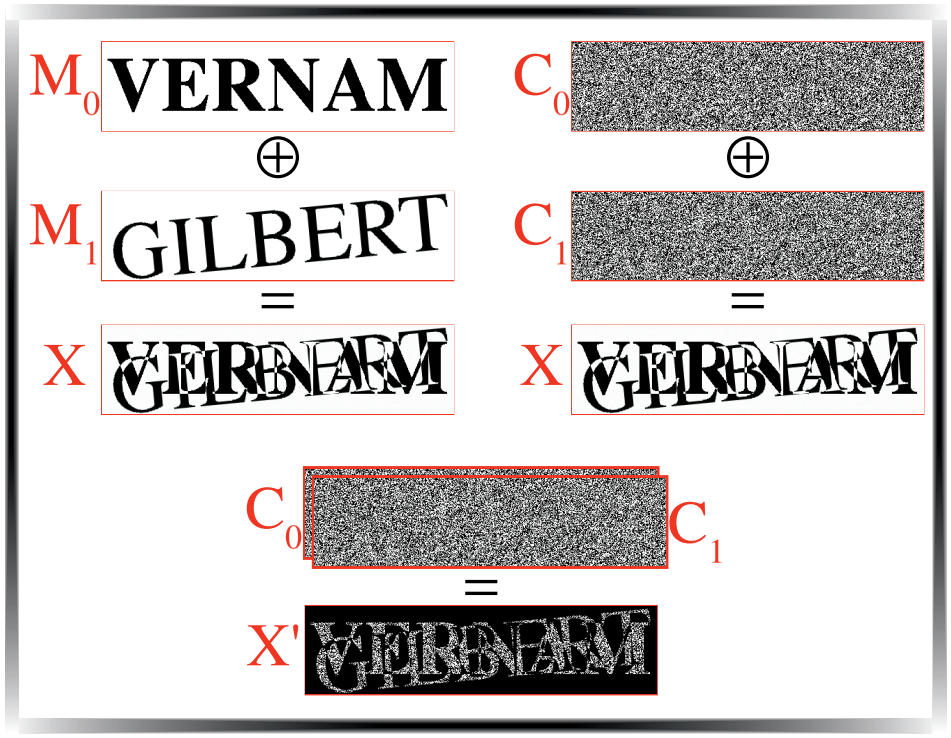


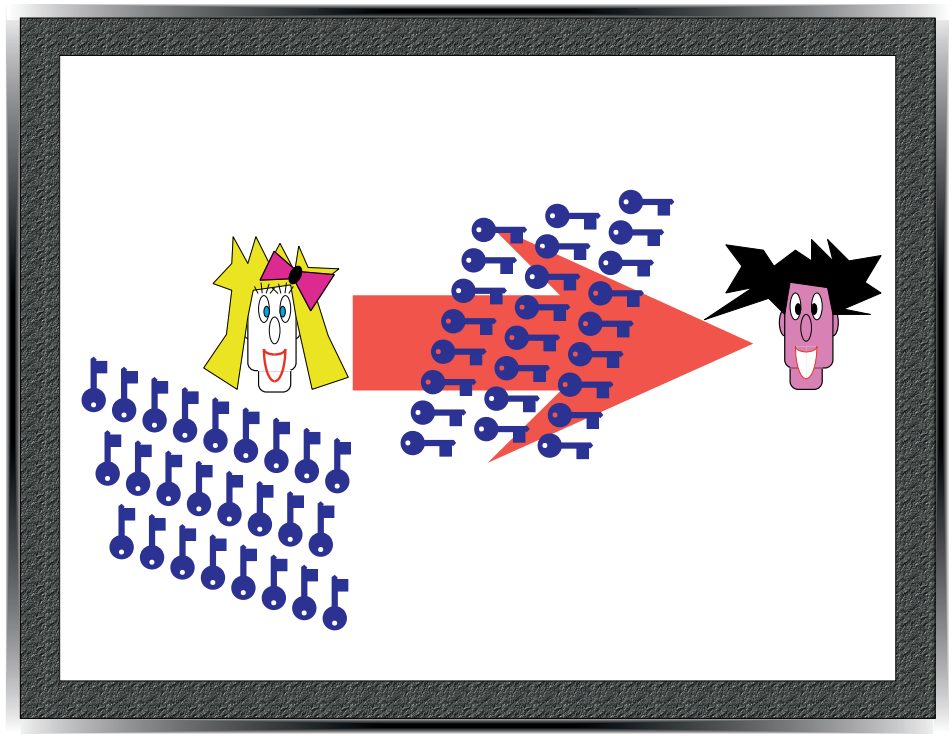


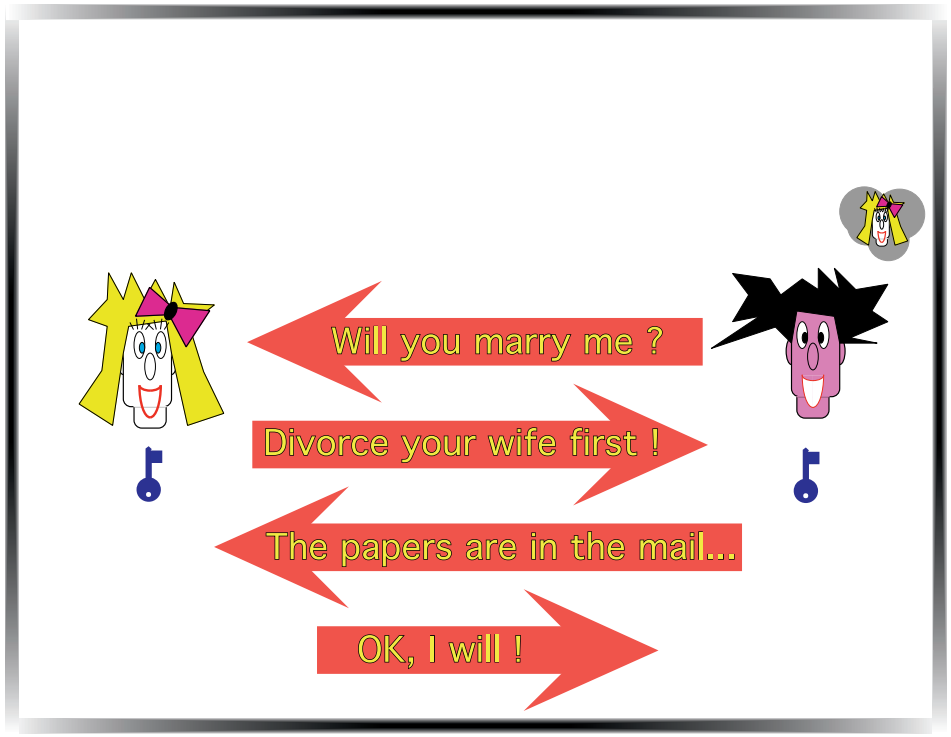
Vernam's One-Time-Pad

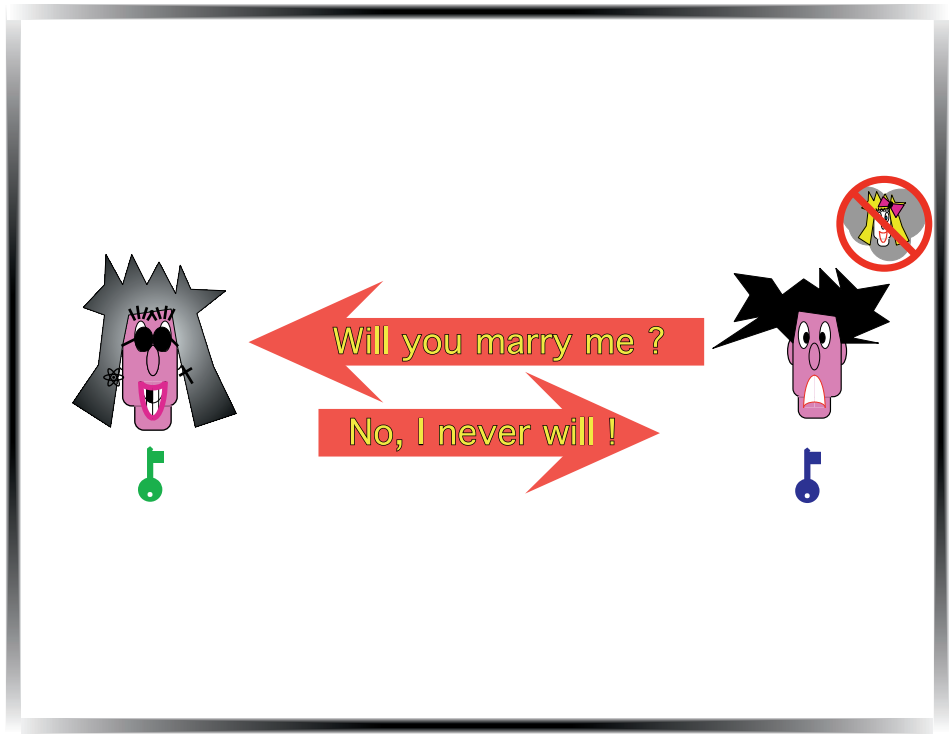




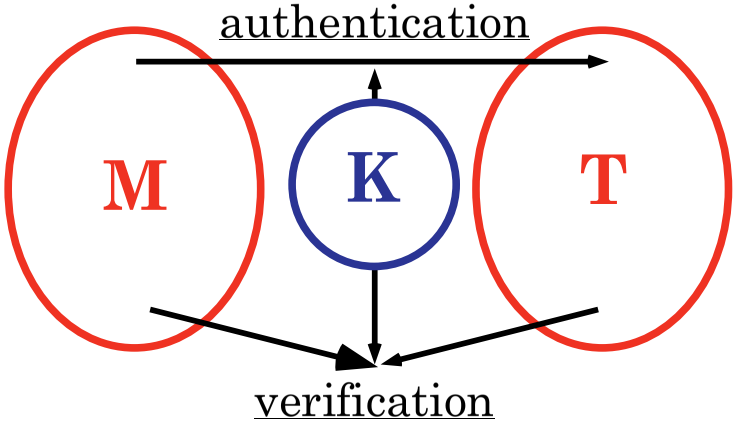

M0 VERNAM
⊕
M1 GILBERT
=
X
C0
⊕
C1
=
X
C0
C1
=
X'




Will you marry me ?
Divorce your wife first !
The papers are in the mail...
OK, I will !

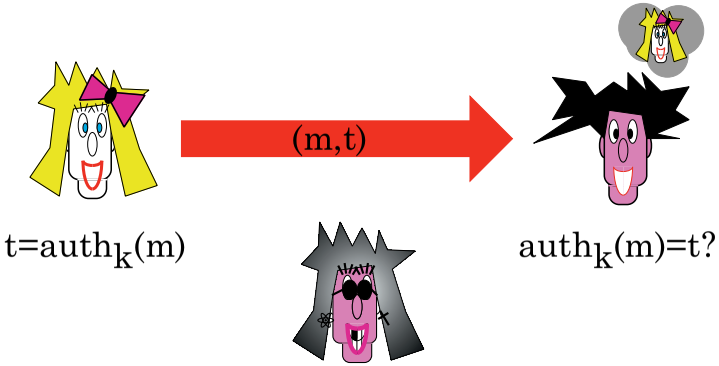

Will you marry me ?
No, I never will !

symmetric authentication



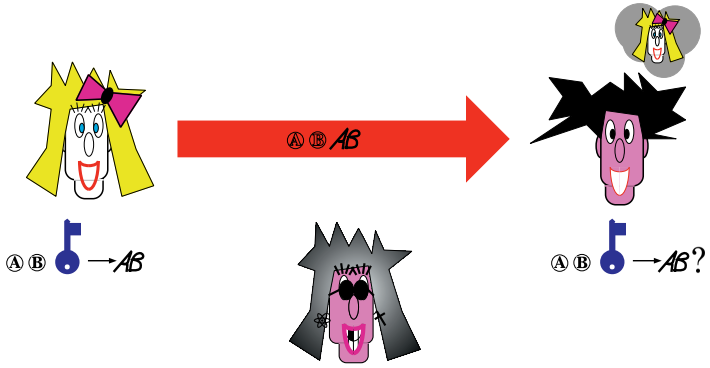
Information Theoretical Security

Authentication



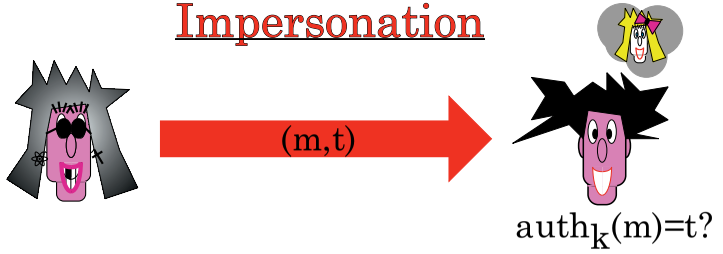
Information Theoretical Security

Authentication

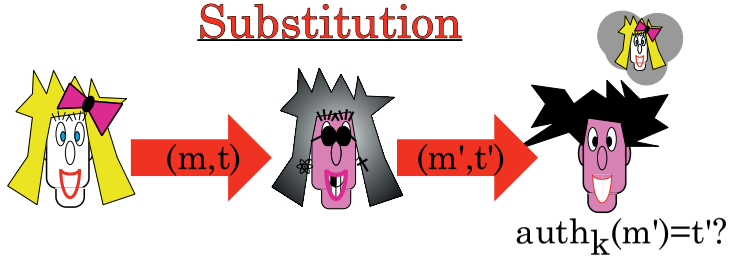


Information Theoretical Security

Impersonation



Substitution



Information Theoretical Security

WC One-Time-Authentication

$$\text{auth}_{\mathbf{M},b}(x) = \mathbf{M}x \oplus b$$

$|x| = n,\ |\mathbf{M}| = n \cdot n',\ |b| = n'$

$\forall m \in M, \forall t \in T$

$\Pr(\text{auth}_{\mathbf{M},b}(m)=t) = 1/|T| = 1/2^{n'}$

$\forall m \neq m' \in M, \forall t,t' \in T$

$\Pr(\ \text{auth}_{\mathbf{M},b}(m')=t' \ \mid\ \text{auth}_{\mathbf{M},b}(m)=t\ ) = 1/|T| = 1/2^{n'}$

WC One-Time-Authentication and (linear) error correction

$$\text{auth}_{\mathbf{M},b}(x) = \mathbf{M}x \oplus b$$

$[\mathbf{I}:\mathbf{M}]m \oplus [0:b] = [m:t]$

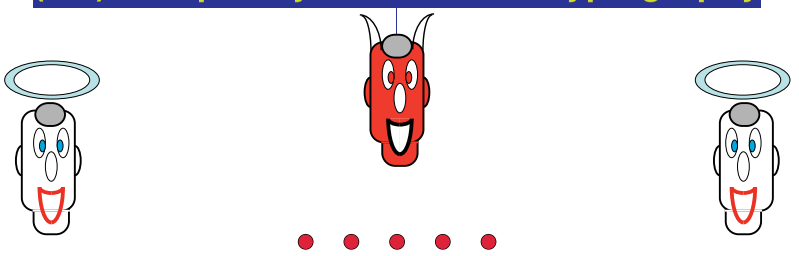
G=[**I**:**M**] (systematic) generating matrix of error correcting code

[0:b] error pattern = one-time pad encryption of tag

[m:t] systematic form of (message,tag)

(1.2) Complexity Theoretical Cryptography

(1.2) Complexity Theoretical Cryptography

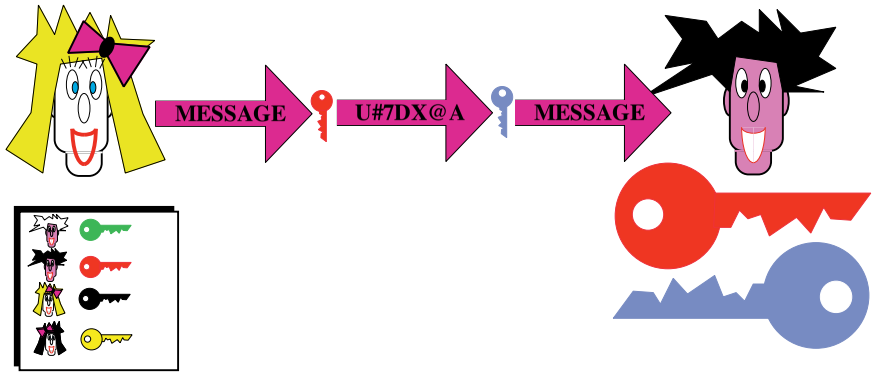


(1.2.1) Public key cryptosystem

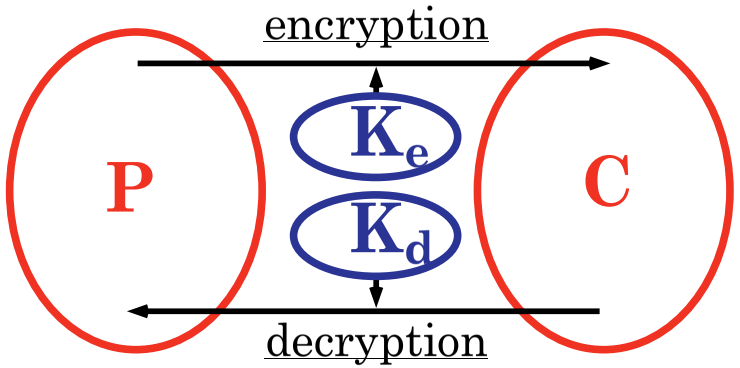
(1.2.2) Digital signature scheme

• • • • •

PUBLIC-KEY CRYPTOGRAPHY



asymmetric encryption
(public-key cryptography)



Complexity Theoretical Security

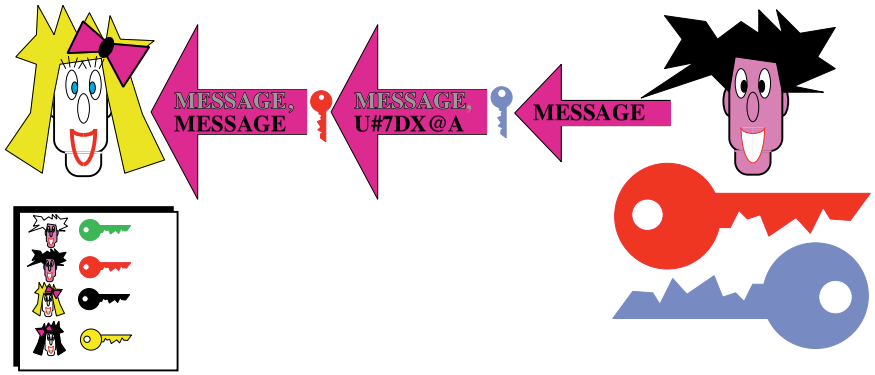
RSA public-key cryptosystem

- n = p*q, two large primes
- e s.t. gcd(e,(p-1)(q-1))=1
- d s.t. e*d = 1 **mod** (p-1)(q-1)

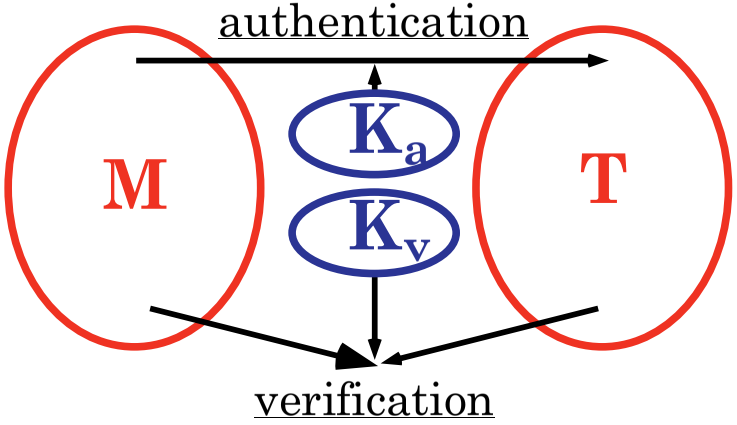
- K_e = (n,e), K_d = (n,d)

- **encryption** E(m): m^e **mod** n
- **decryption** D(c): c^d **mod** n

Digital Signature



asymmetric authentication
(digital signature schemes)



Complexity Theoretical Security

RSA digital signature

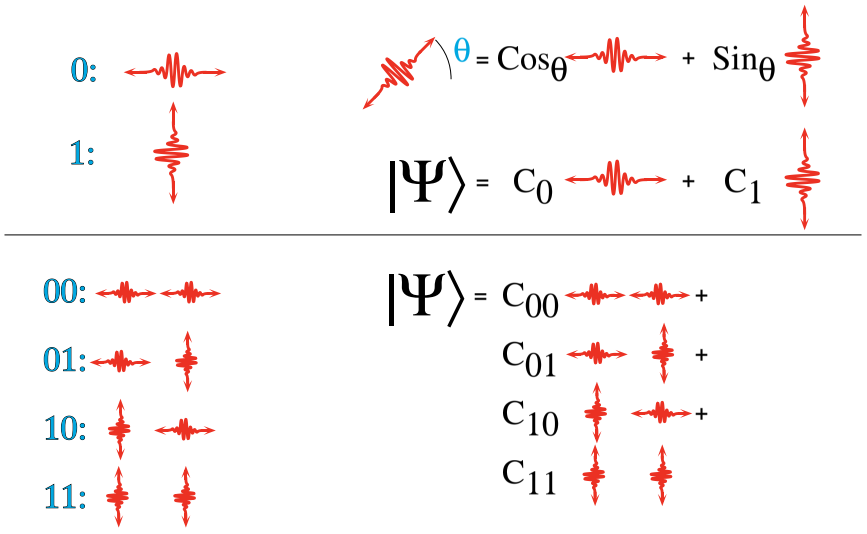
- n = p*q, two large primes
- e s.t. gcd(e,(p-1)(q-1))=1
- d s.t. e*d = 1 **mod** (p-1)(q-1)

- $K_a = (n,d)$, $K_v = (n,e)$

- **authentication** A(m): m^d **mod** n
- **verification** V(m,t): $t^e \equiv m$ **mod** n ?

(2)
Quantum Information & Computations

Bits & QuBits



Albert Einstein

$|¿?\rangle = {}^{1}/\sqrt{2}|\mathbf{01}\rangle - {}^{1}/\sqrt{2}|\mathbf{10}\rangle$

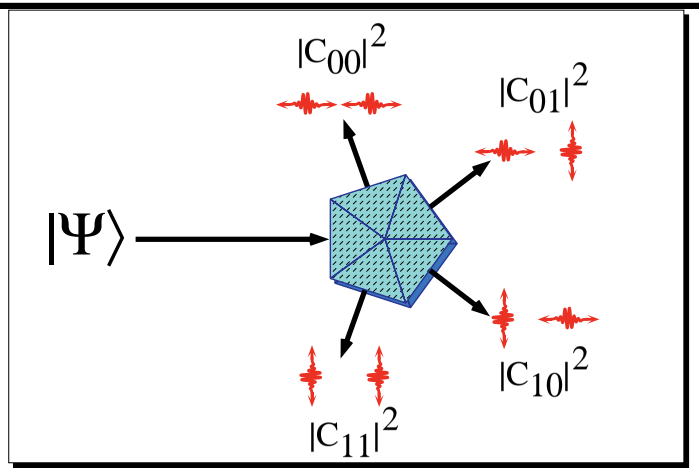
Boris Podolsky

Nathan Rosen

EPR

Quantum Measurements

$|\Psi\rangle = C_{00} + C_{01} + C_{10} + C_{11}$



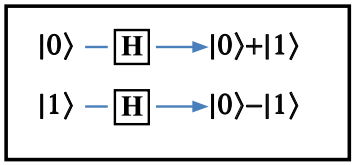
Quantum Evolution: Unitary Operators

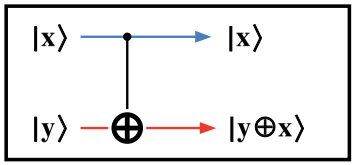
$|\Psi\rangle \xrightarrow{U} |\Psi'\rangle$

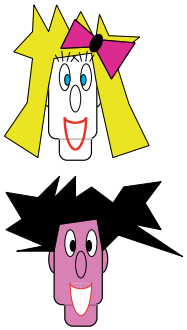
$\xrightarrow{U} |\Psi_0\rangle$

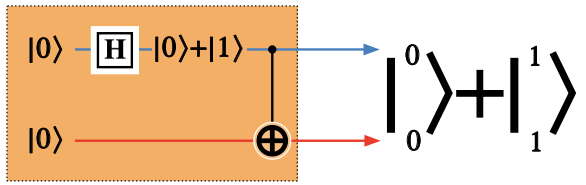
$\xrightarrow{U} |\Psi_1\rangle$

$C_0 + C_1 \xrightarrow{U} C_0|\Psi_0\rangle + C_1|\Psi_1\rangle$









$|{}^{0}_{0}\rangle + |{}^{1}_{1}\rangle$

$|??\rangle$

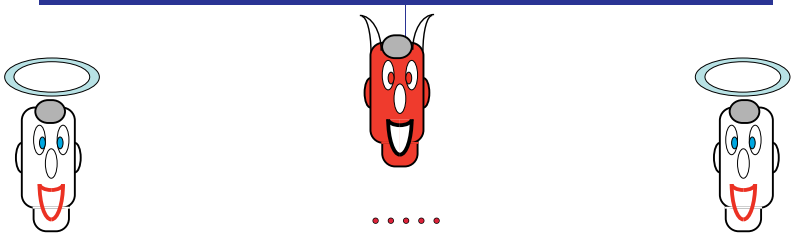
Classical & Quantum Information

00110111000110 Classical		Quantum
Copying:	Yes	NO
Measuring:	Yes	partial
Broadcasting:	Yes	NO
Superposing:	NO	Yes
Interfering:	NO	Yes

(3)
Quantum Cryptography

(3.1)
Information Theoretical Quantum Cryptography

(3.1) Information Theoretical Cryptography



(3.1.1) Key distribution : Q-key distribution +
Q-distillation (formerly purification)

(3.1.2) One-time pad : one-time Q-pad (Q-teleportation)
Vernam Q-cipher

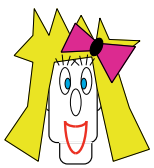
(3.1.3) one-time authentication : authenticated Q-teleportation +
one-time Q-authentication

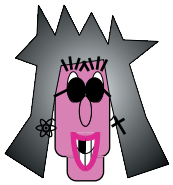
.....

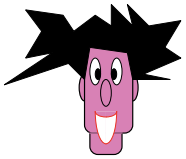
(3.1.1) Key distribution

Classical key : Q-distribution of keys(BB84)
+ error-correction
+ privacy amplification

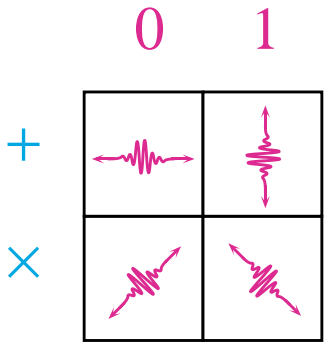
Quantum key : Q-key distribution(Ekert/ Lo-Chau)
+ Q-error-correction (CSS) or
+ Q-Distillation (Purification)



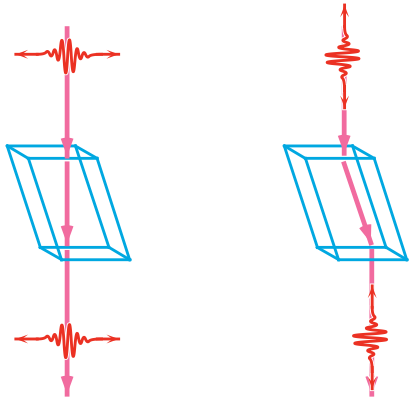




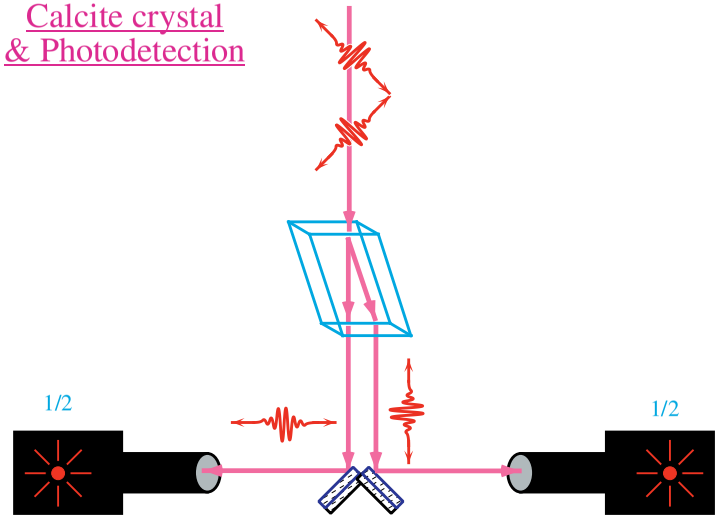
Ambiguous Coding Scheme



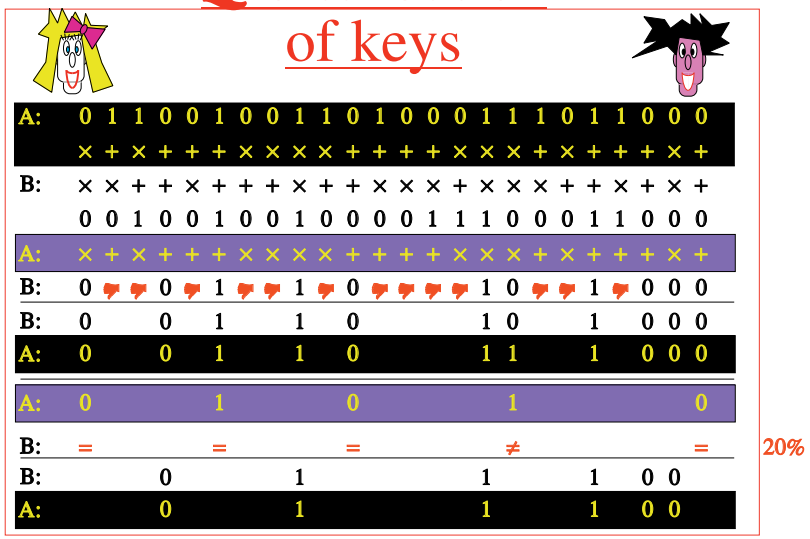
Calcite crystal



Calcite crystal & Photodetection

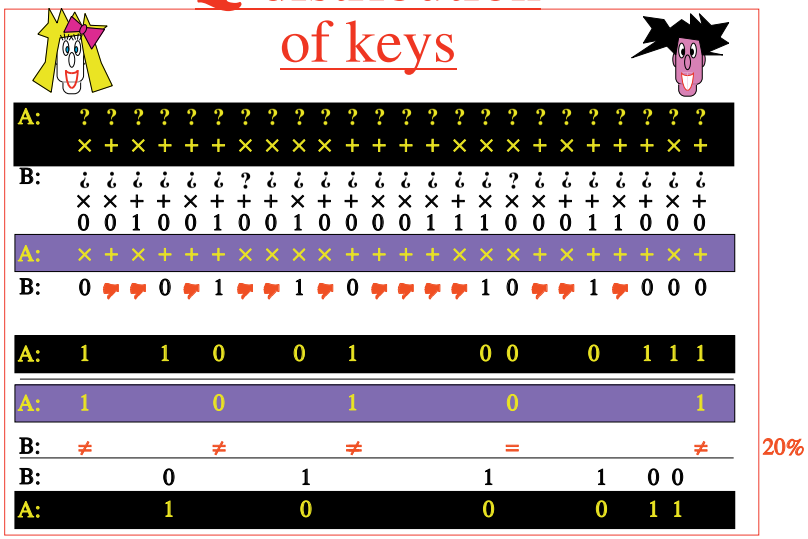


Q-distribution of keys



Bennett- Brassard

Q-distribution of keys



Ekert

Q-distribution of keys

.....

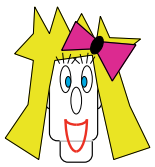
- Produces raw classical key
- Observed error rate indicates amount of eavesdropper information
- Error-correction is used to fix errors
- Random hash function is used to distill a smaller secret classical key

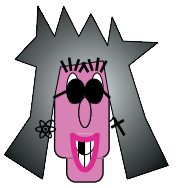
.....

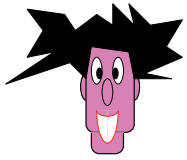
(3.1.1) Key distribution

Classical key : Q-distribution of keys(BB84)
+ error-correction
+ privacy amplification

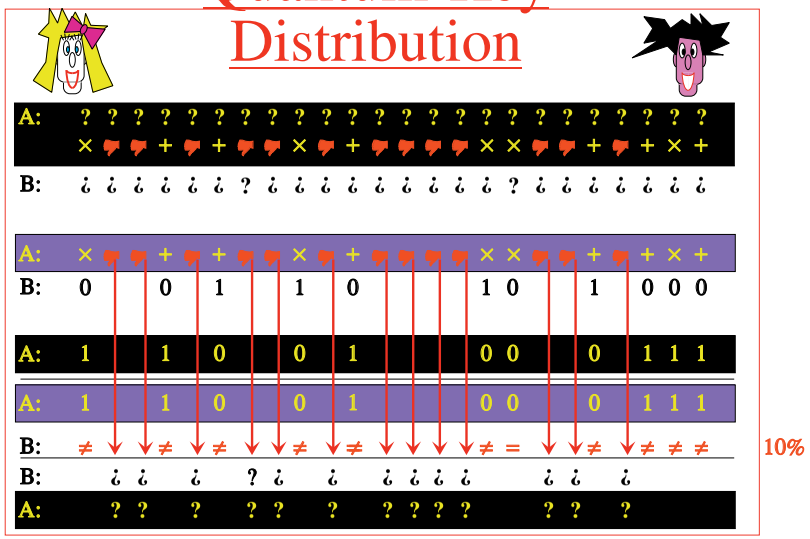
Quantum key : Q-key distribution(Ekert/ Lo-Chau)
+ Q-error-correction (CSS) or
Q-Distillation (Purification)





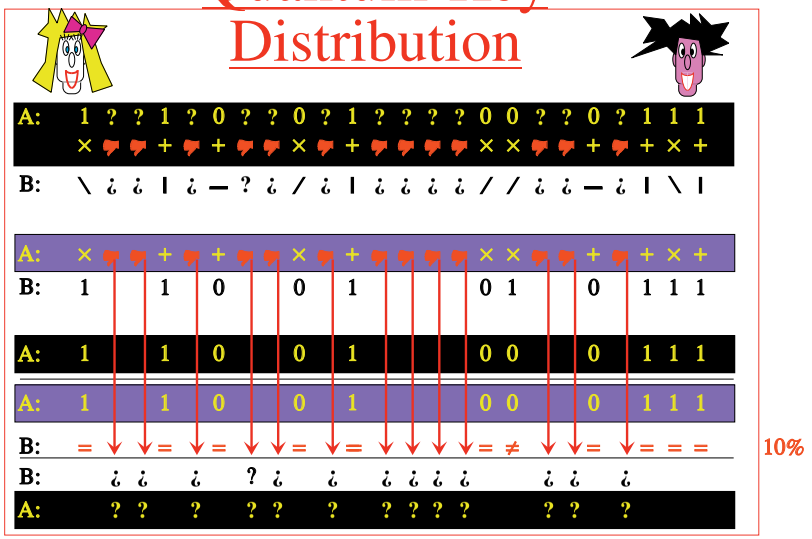


Quantum-Key Distribution



Ekert + Lo-Chau

Quantum-Key Distribution



Shor-Preskill

Quantum-Key Distribution

.....

• Produces raw quantum key (EPR states)

• Observed error rate indicates amount of impurity of EPR states

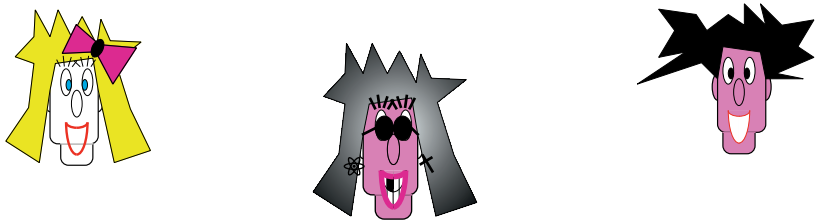
• Quantum error-correction (CSS) is used to purify raw EPR states into a smaller pure set

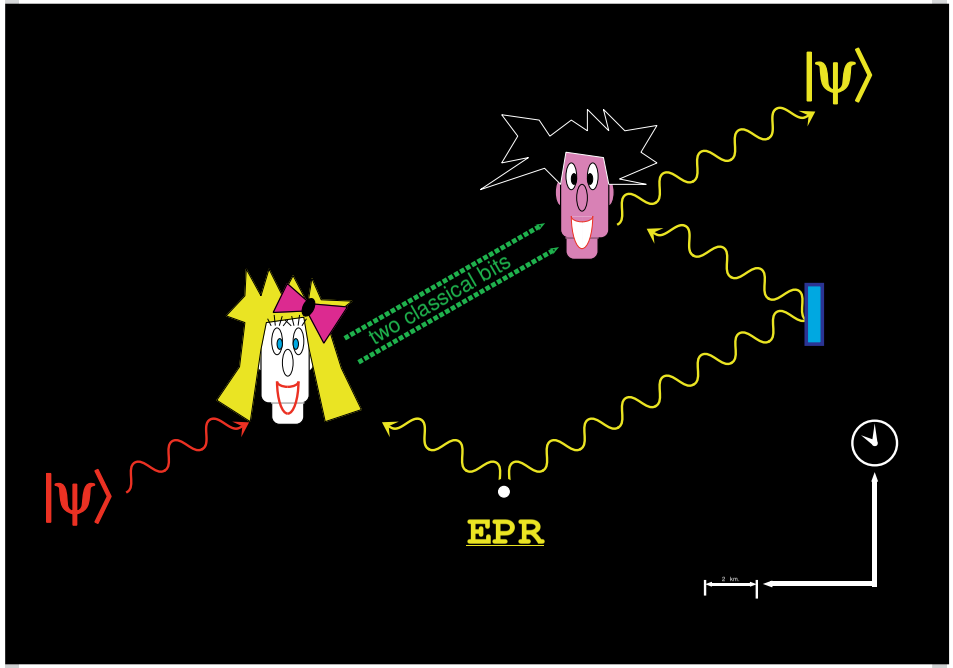
.....

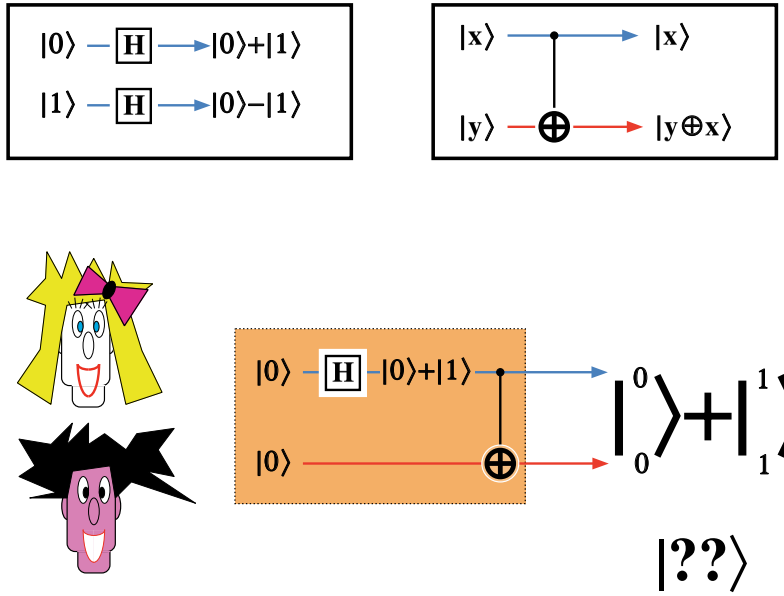
(3.1.2) One-time pad

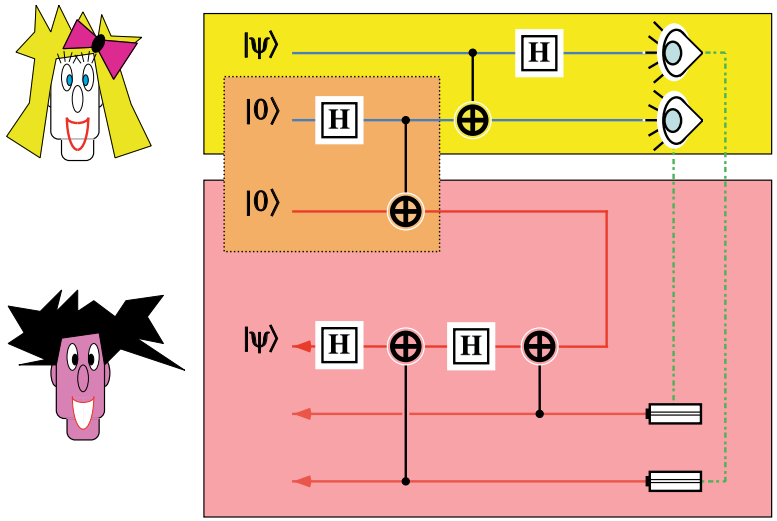
Classical key : Vernam Q-cipher (various sources)
Quantum Ciphertext

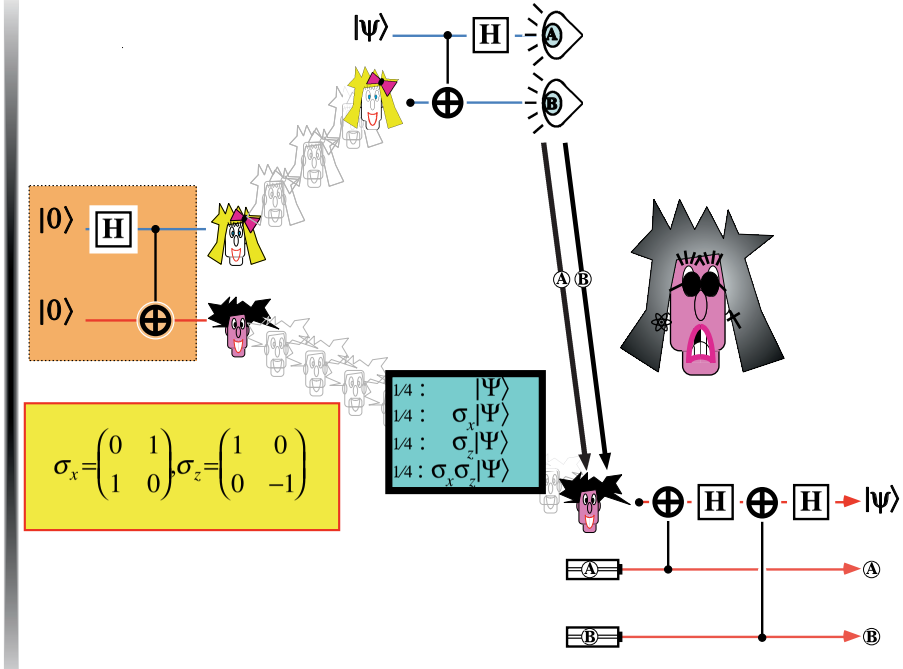
Quantum key : one-time Q-pad (Q-teleportation)
Classical Ciphertext (BBCJPW)




|ψ⟩
two classical bits
|ψ⟩
EPR


|0⟩ H |0⟩+|1⟩
|1⟩ H |0⟩−|1⟩
|x⟩ |x⟩
|y⟩ ⊕ |y⊕x⟩
|0⟩ H |0⟩+|1⟩
|0⟩ ⊕
|??⟩


|ψ⟩ H
|0⟩ H ⊕
|0⟩ ⊕
|ψ⟩ H ⊕ H ⊕


|ψ⟩ H Ⓐ
⊕ Ⓑ
|0⟩ H
|0⟩ ⊕
Ⓐ Ⓑ
¼ : |Ψ⟩
¼ : σx|Ψ⟩
¼ : σz|Ψ⟩
¼ : σxσz|Ψ⟩
σx = (0 1 / 1 0), σz = (1 0 / 0 −1)
⊕ H ⊕ H |ψ⟩
Ⓐ
Ⓑ

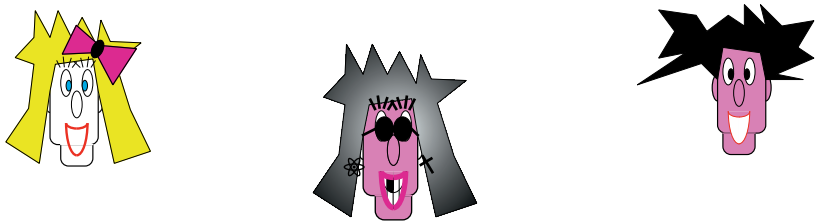
(3.1.2b) one-time pad

Quantum key : one-time Q-pad
Classical Ciphertext

(3.1.2a) One-time pad

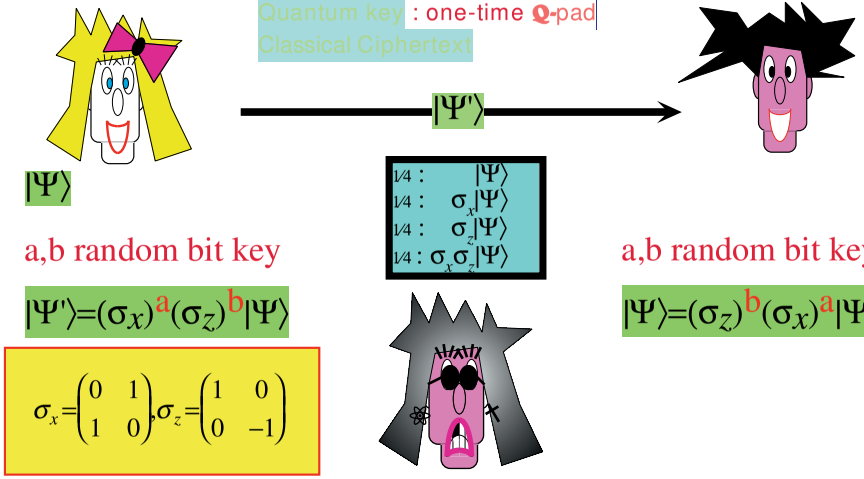
Classical key : Vernam Q-cipher (various sources)
Quantum Ciphertext

Quantum key : one-time Q-pad (BBCJPW)
Classical Ciphertext



(3.1.2a) one-time pad

Classical key : Vernam Q-cipher
Quantum Ciphertext
Quantum key : one-time Q-pad
Classical Ciphertext

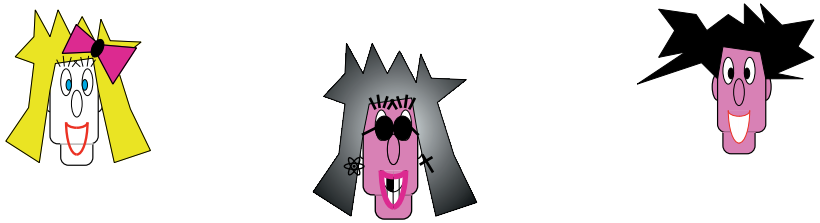


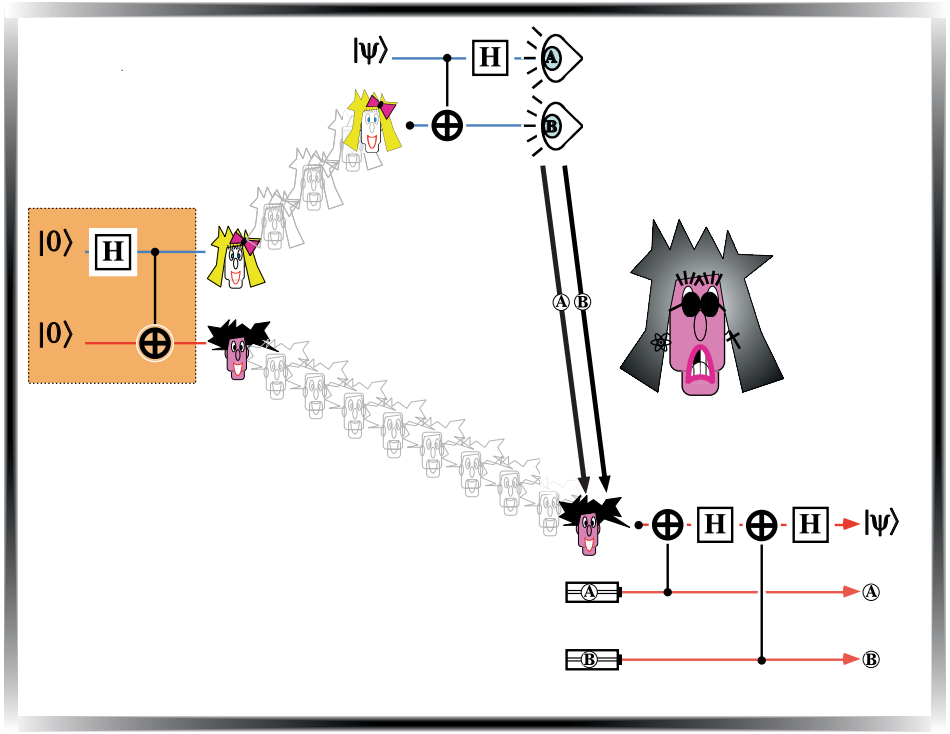
$$\sigma_x=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\sigma_z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

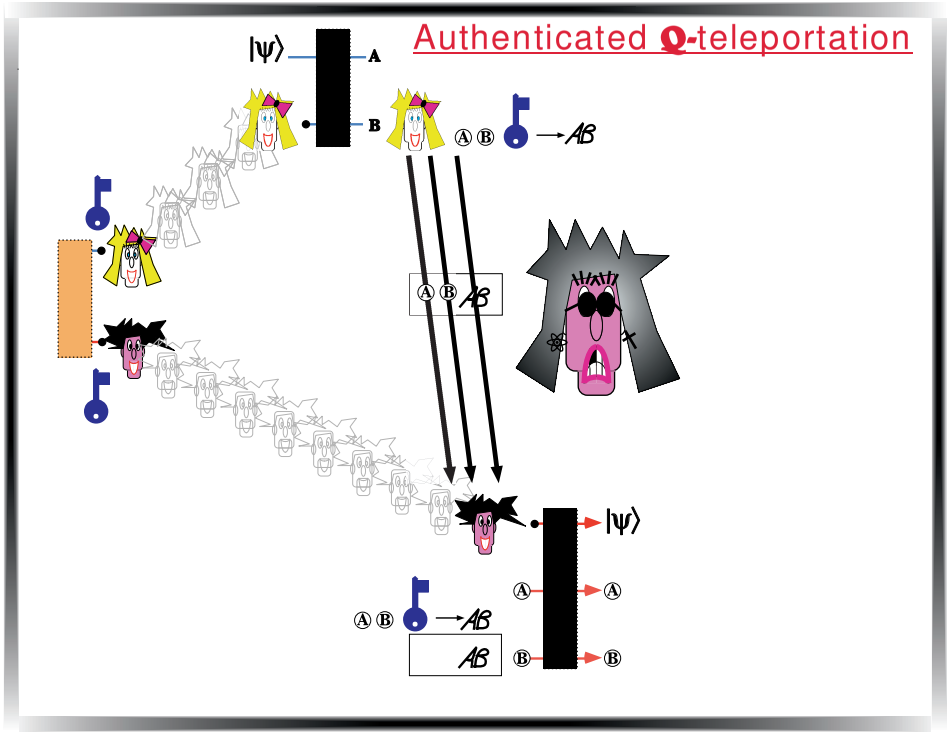
(3.1.3) One-time Q-Authentication

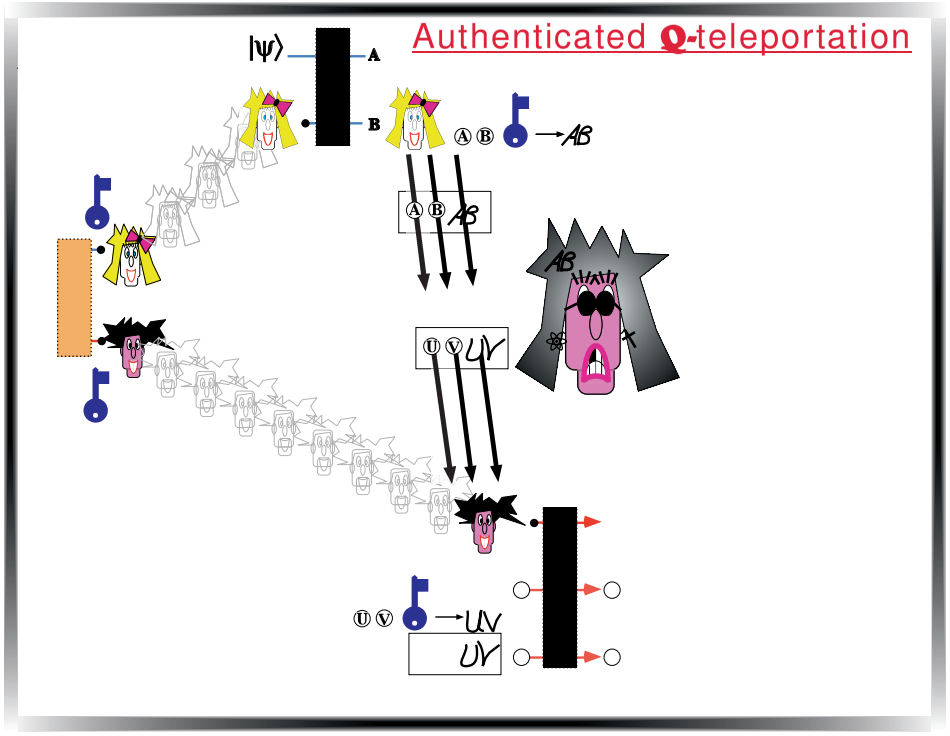
Classical key : Q-Authentication (BCGST)
Quantum message+tag

Quantum key : Authenticated Q-teleportation (BBCJPW)
Classical message+tag







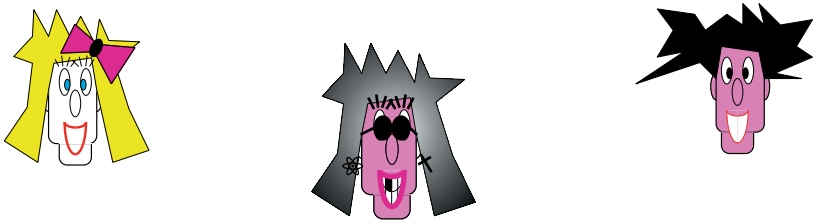


(3.1.3b) One-time Q-Authentication

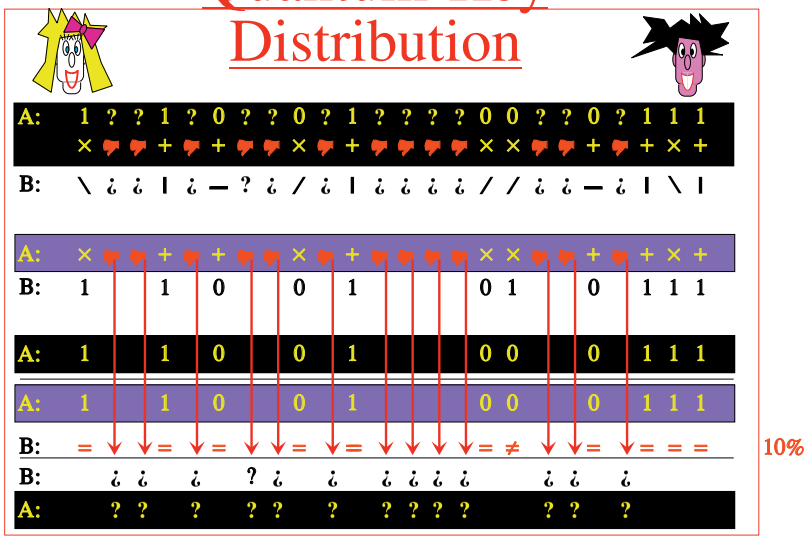
Quantum key : Authenticated Q-teleportation
Classical message+tag

(3.1.3a) One-time Q-Authentication

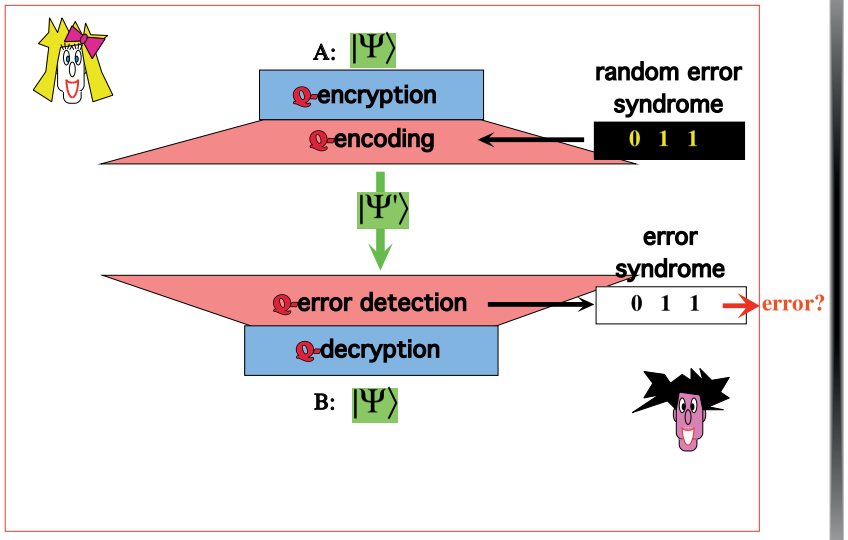
Classical key : Q-Authentication (BCGST)
Quantum message+tag
Quantum key : Authenticated Q-teleportation
Classical message+tag (BBCJPW)



Quantum-Key Distribution



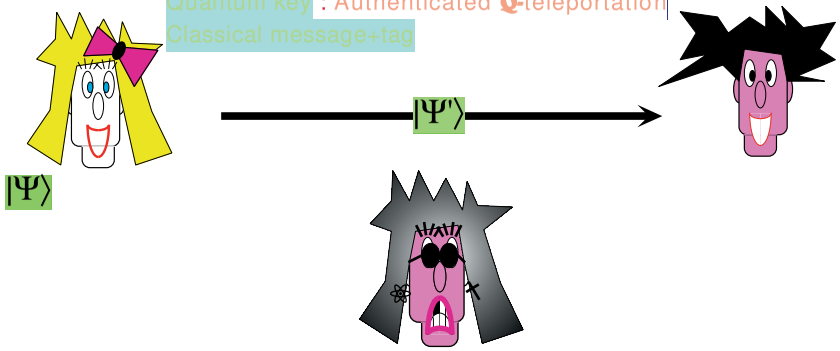
Shor-Preskill



Barnum-Crépeau-Gottesman-Smith-Tapp

(3.1.3a) one-time authentication

Classical key : one-time Q-authentication
Quantum message+tag
Quantum key : Authenticated Q-teleportation
Classical message+tag



- public Q-error-correcting code
- secret key for syndrome & encryption

Barnum-Crépeau-Gottesman-Smith-Tapp

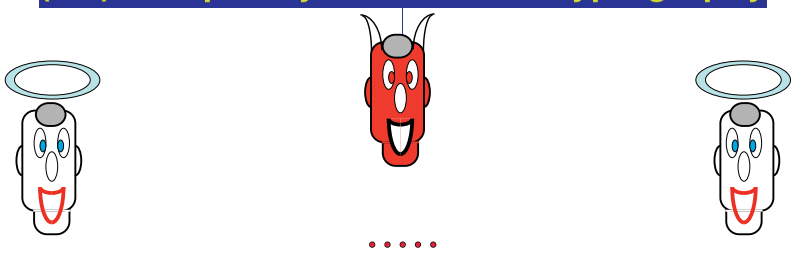
one-time Q-authentication

=>

Vernam Q-cipher

(3.2) Complexity Theoretical Quantum Cryptography

(3.2) Complexity Theoretical Cryptography



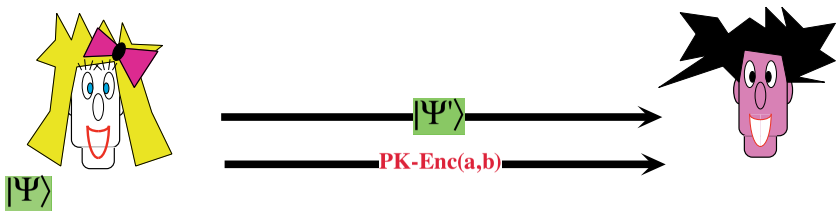
(3.2.1) Public key cryptosystem : public-key Q-cryptosystem

(3.2.2) Digital signature scheme : public-key Q-Authentication
Q-digital signature scheme

.....

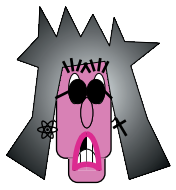
(3.2.1) Public-Key Q-Cryptosystem

Assuming Classical Public Key Cryptography



a,b random bits

$|\Psi'\rangle=(\sigma_x)^a(\sigma_z)^b|\Psi\rangle$

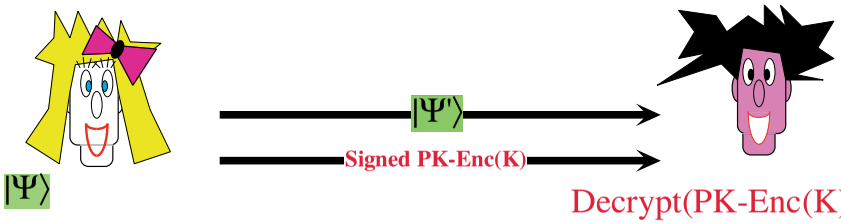


Dec(PK-Enc(a,b))

$|\Psi\rangle=(\sigma_z)^b(\sigma_x)^a|\Psi'\rangle$

(3.2.2a) Public-Key Q-Authentication

Assuming Classical Public Key Cryptography
Assuming Classical Digital Signature



Decrypt(PK-Enc(K))
check signature

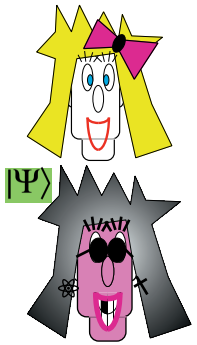
K random authentication key

$|\Psi'\rangle=BCGST(K,|\Psi\rangle)$

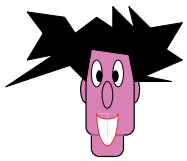
$|\Psi\rangle=BCGST^{-1}(K,|\Psi'\rangle)$

(3.2.2b) Q-Digital Signature Scheme

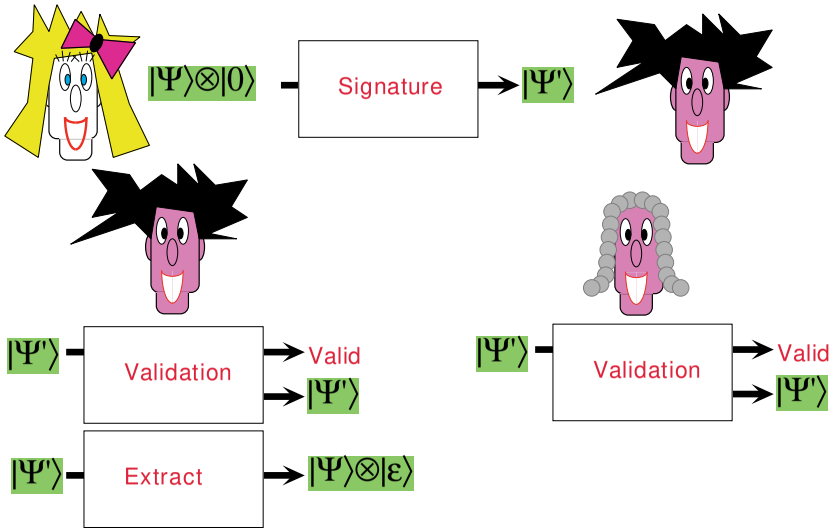
Assuming Classical Public Key Cryptography
Assuming Classical Digital Signature



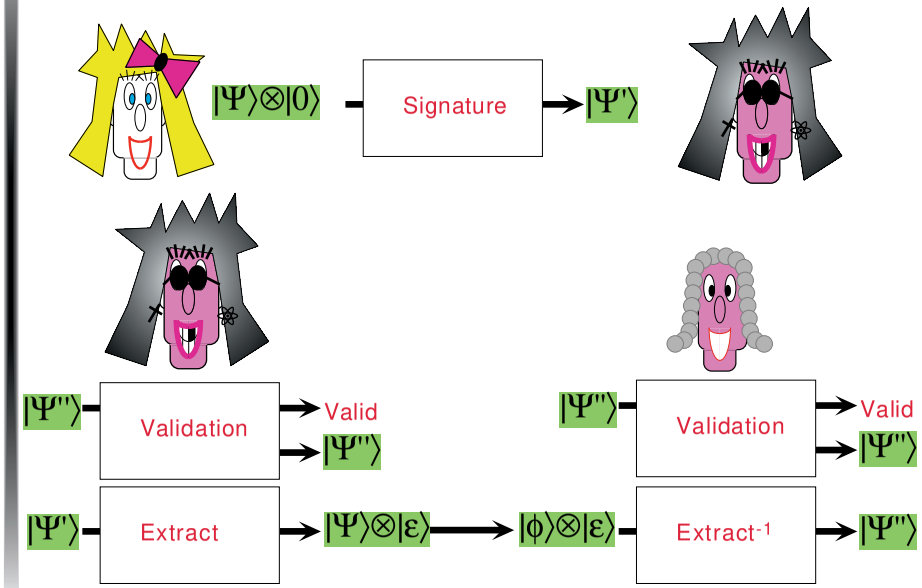
IMPOSSIBLE



(3.2.2b) Q-Digital Signature Scheme



(3.2.2b) Q-Digital Signature Scheme



(Trapdoor) One-way function

- generate a function f (and trapdoor) s.t.
- computing f(x) is easy
- finding x s.t. f(x)=y is hard
- finding x s.t. f(x)=y is easy with trapdoor

cryptanalysis : Shor

Q-One-way function

Fischer-Stern
one-way function
(error correction code based)

generation : classical easy
computing f : classical easy
inverting f : classical / quantum hard ???

Q-Trapdoor One-way function

Okamoto-Tanaka-Uchiyama
trapdoor one-way function
(subset products problem based)

generation : quantum easy
computing f : classical easy
inverting f : classical / quantum hard ???
trapdooring f : classical easy

Q-Trapdoor One-way function

McEliece
trapdoor one-way function
(error correction code based)

generation : classical easy
computing f : classical easy
inverting f : classical / quantum hard ???
trapdooring f : classical easy

Introduction to theoretical quantum CRYPTOGRAPHY

Claude Crépeau

School of Computer Science
McGill University