Quantum Authentication

Claude Crépeau

School of Computer Science
McGill University

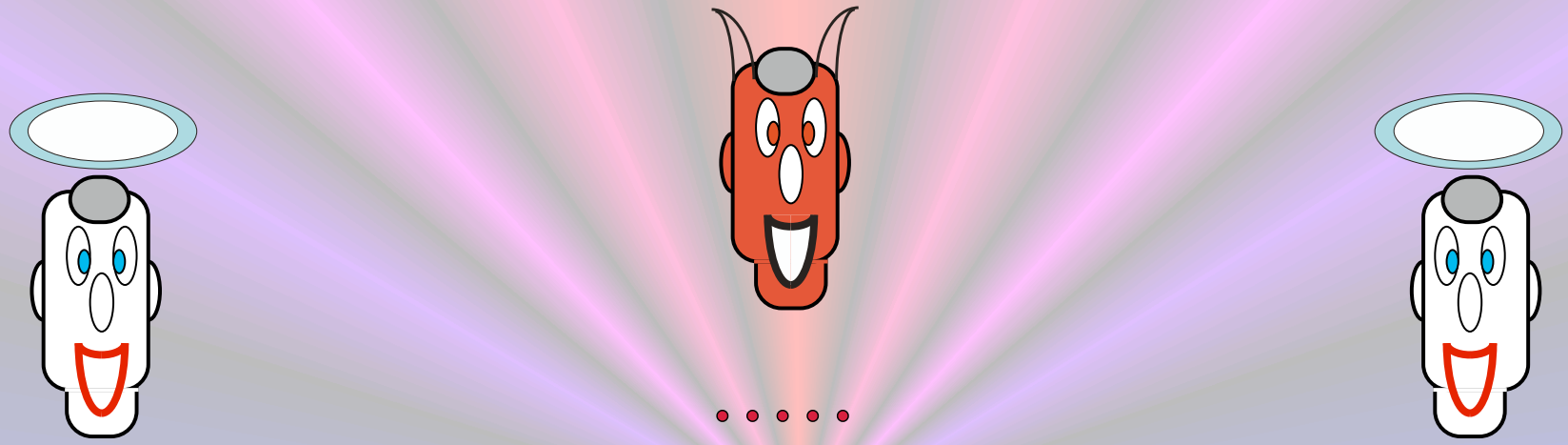
joint work with

H. Barnum, D. Gottesman, A. Smith, A. Tapp

(1)
Classical Cryptography

(1.1) Information Theoretical Cryptography

(1.1) Information Theoretical Cryptography

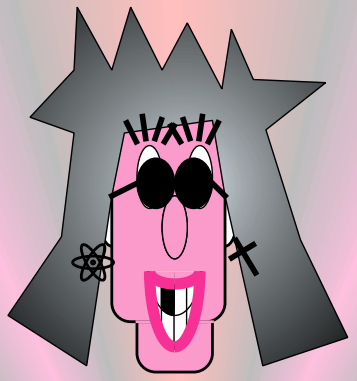


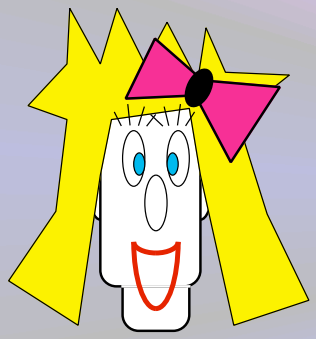
(1.1.1) key distribution

(1.1.2) Encryption

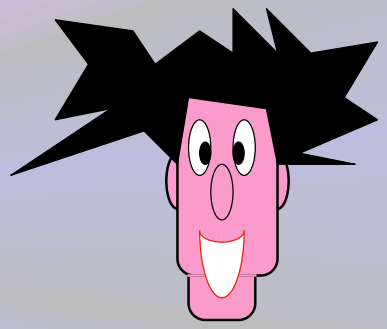
(1.1.3) Authentication

. . . . .





Will you marry me ?

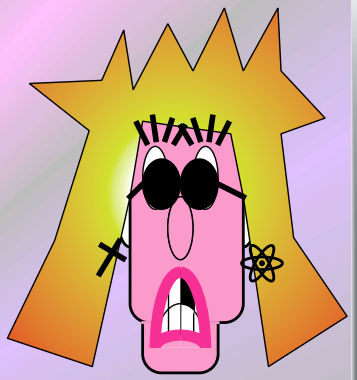


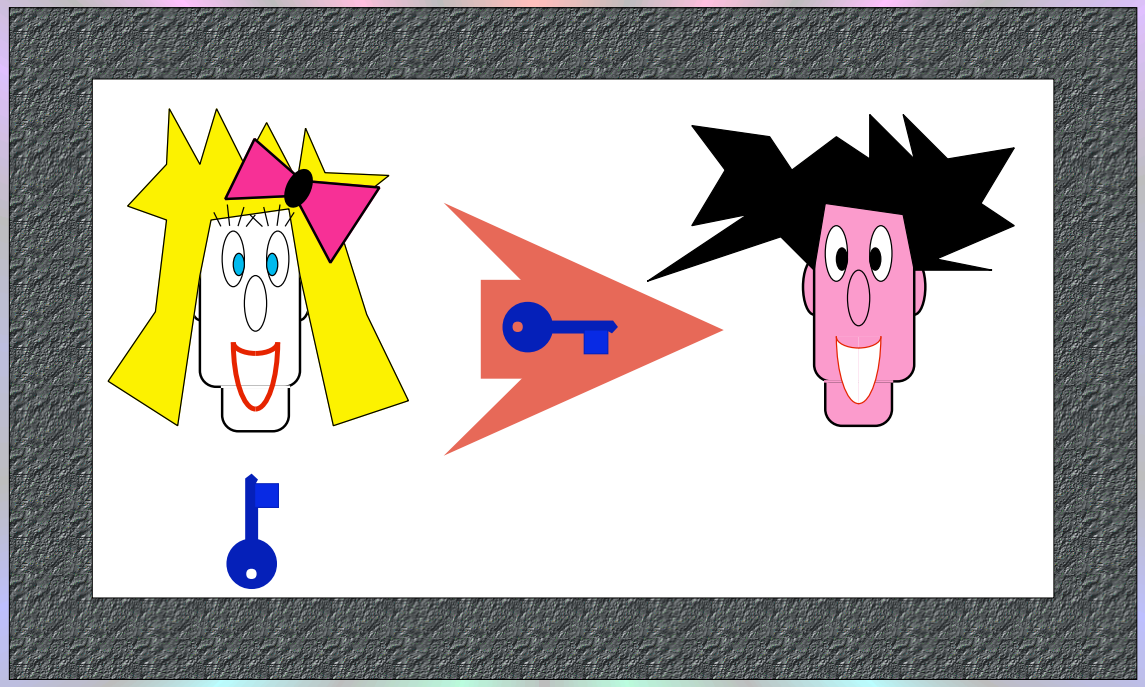
Divorce your wife first !

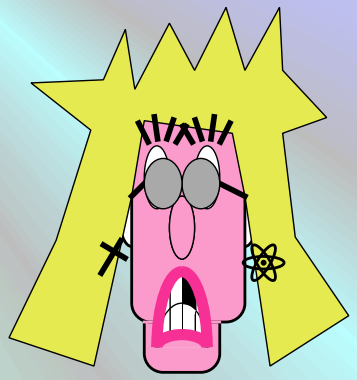
The papers are in the mail...

OK, I will !

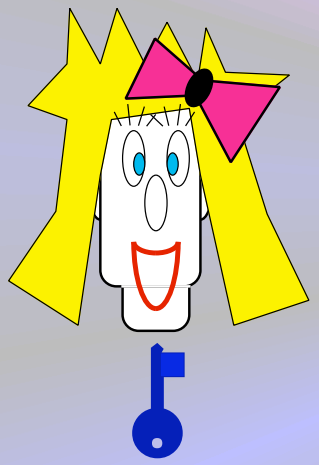
(1.1.1) key distribution



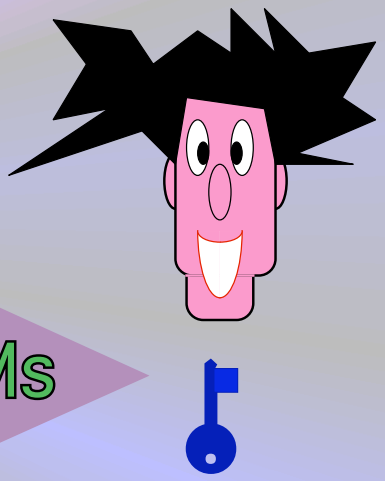




(1.1.2) Encryption



8RdewtU5qkLa$es!T9@

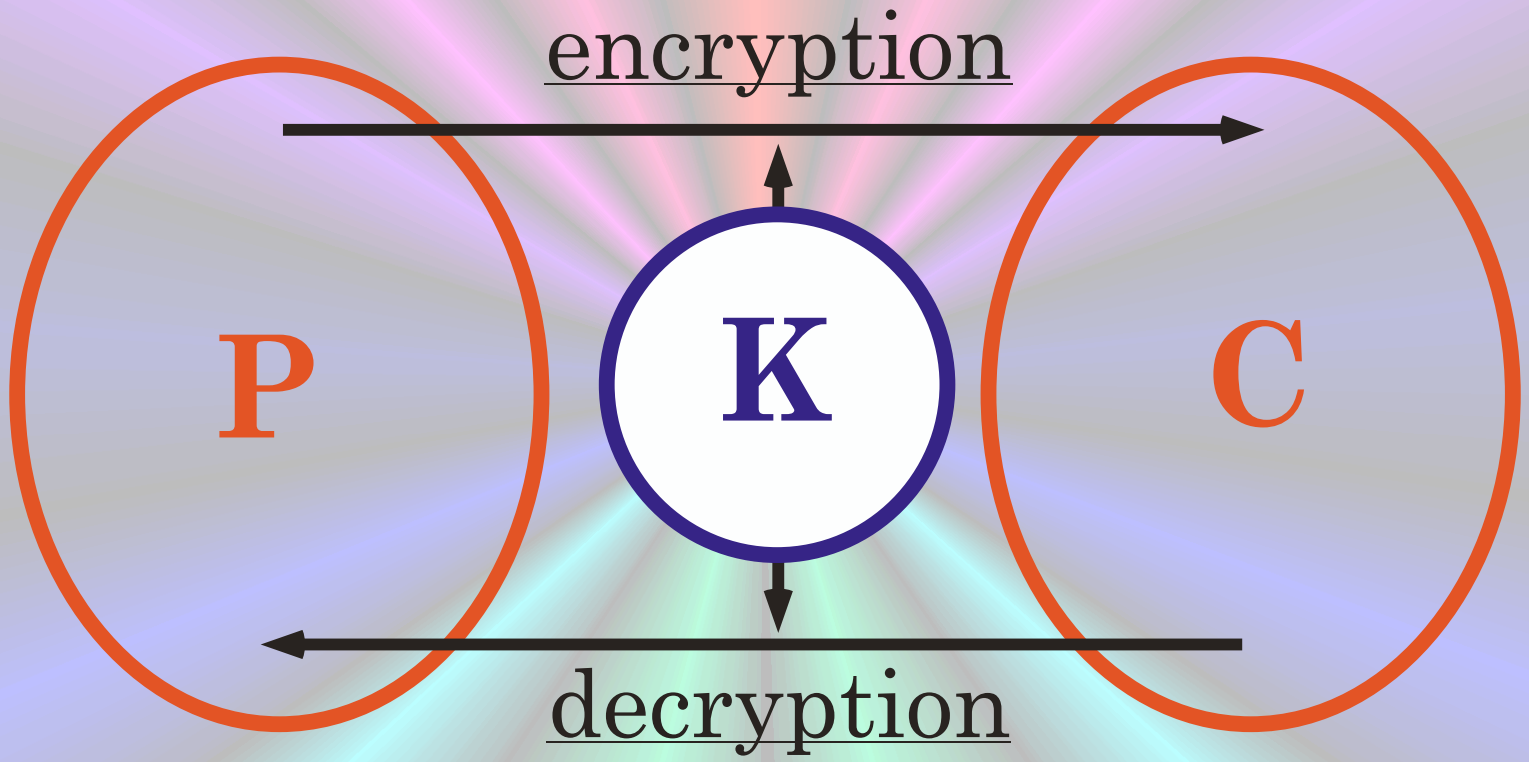


I(D%eXhDqIiykl#2cV7dEwnMs

H&fs@tyHvFGhaOKpTrGbl.Z/rUih*

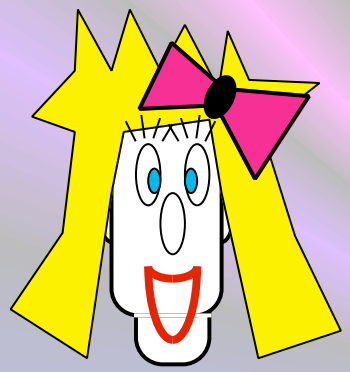
B7B3tdsjUila

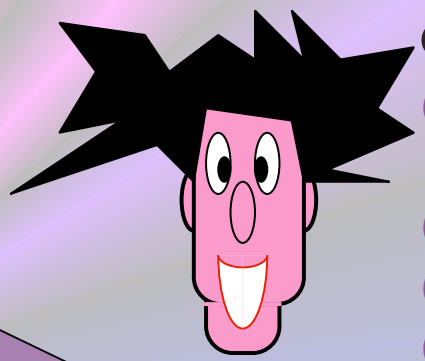
symmetric encryption

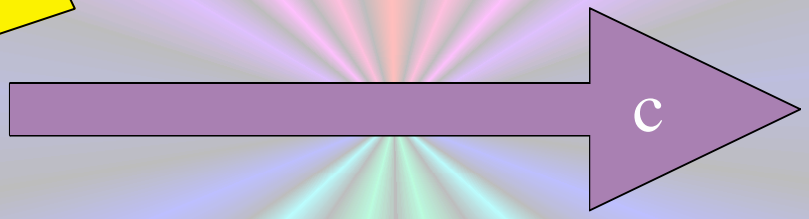


Information Theoretical Security

Vernam's One-Time-Pad







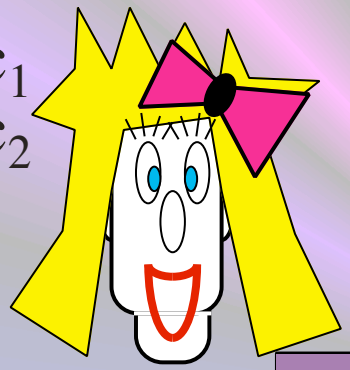
m		k	=	c
1		1		0
0		1		1
1		1		0
0		0		0
0		0		0
1		1		0
0		1		1
0		0	=	0
1		1	=	0
1		1		0
1		0		1
1		1		0
1		0		1
0		1		1
0		1		1
1		1		0

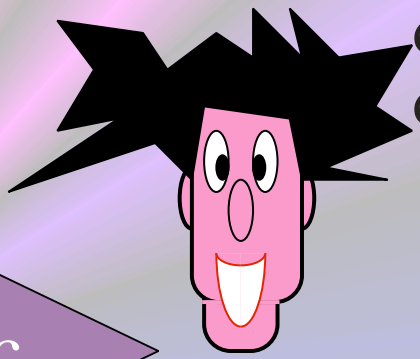
c		k	=	m
0		1		1
1		1		0
0		1		1
0		0		0
0		0		0
0		1		1
1		1		0
0		0	=	0
0		1	=	1
0		1		1
1		0		1
0		1		1
1		0		1
1		1		0
1		1		0
0		1		1

Information Theoretical Security

Vernam's One-Time-Pad

$m_1 \oplus k = c_1$
$m_2 \oplus k = c_2$





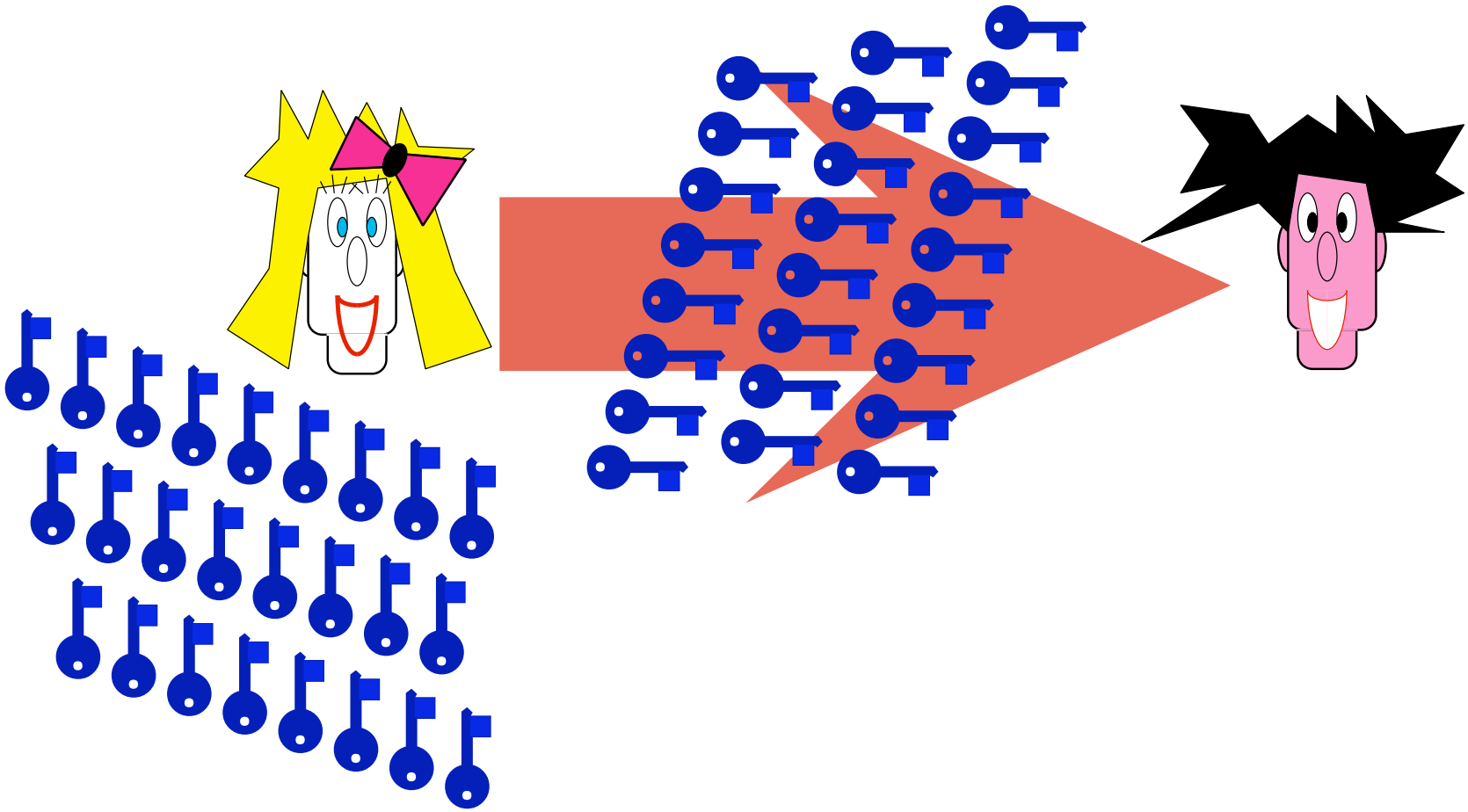
$c_1 \oplus k = m_1$
$c_2 \oplus k = m_2$

c_1

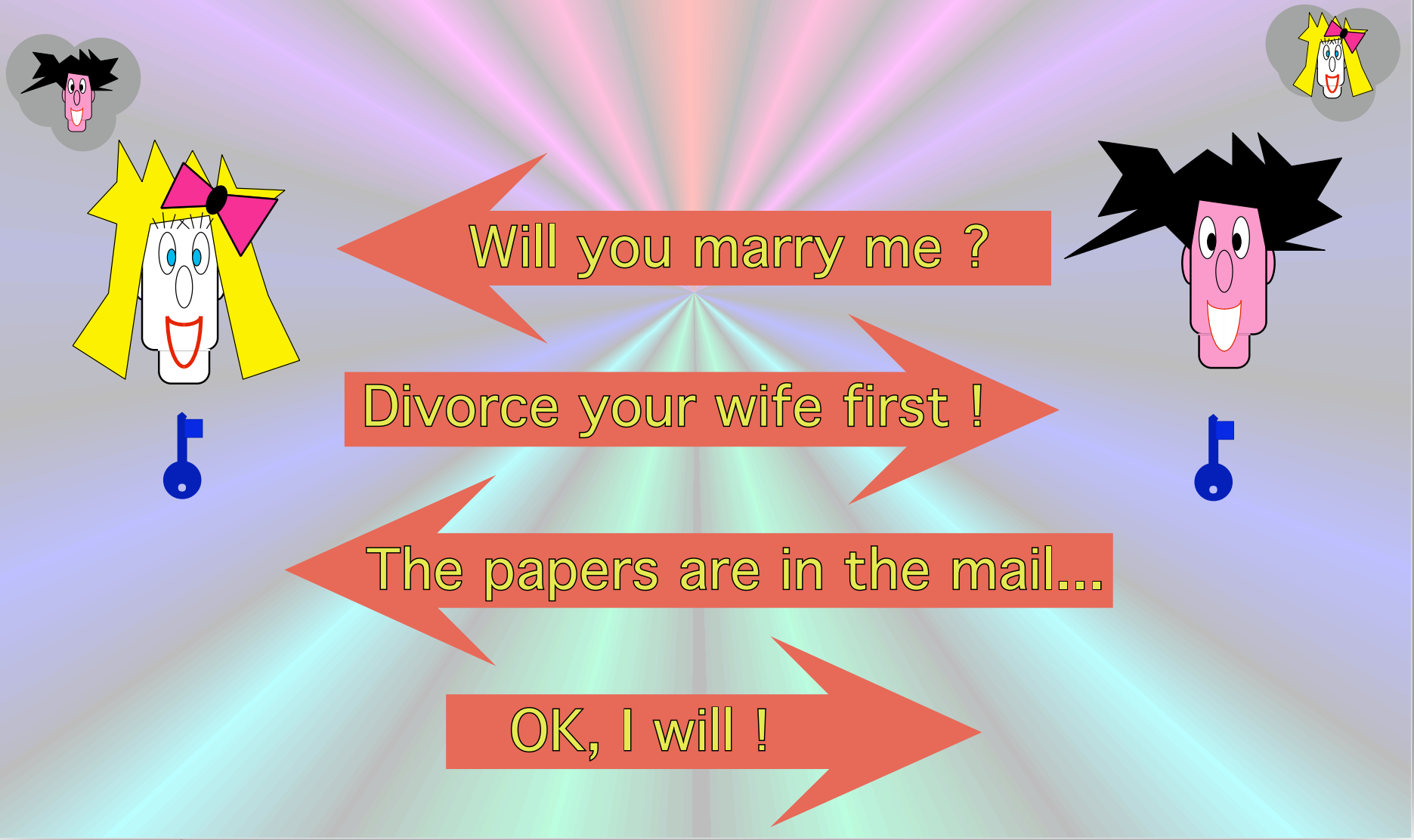
c_2

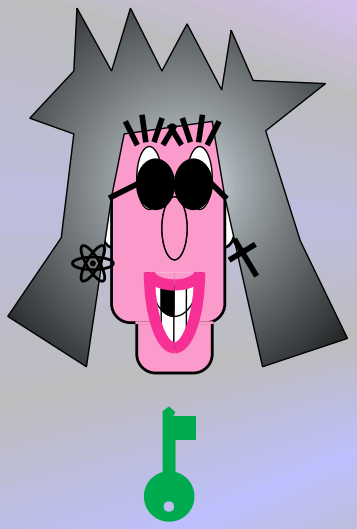
$c_1 \oplus c_2 = m_1 \oplus m_2$

(1.1.1) key distribution PROBLEM



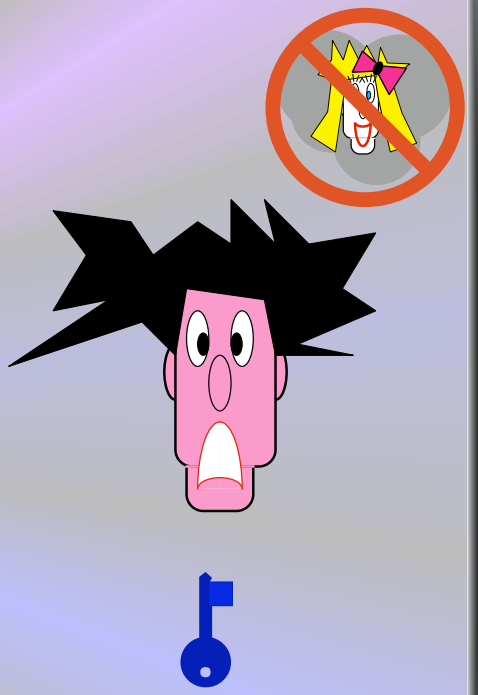
(1.1.3) Authentication



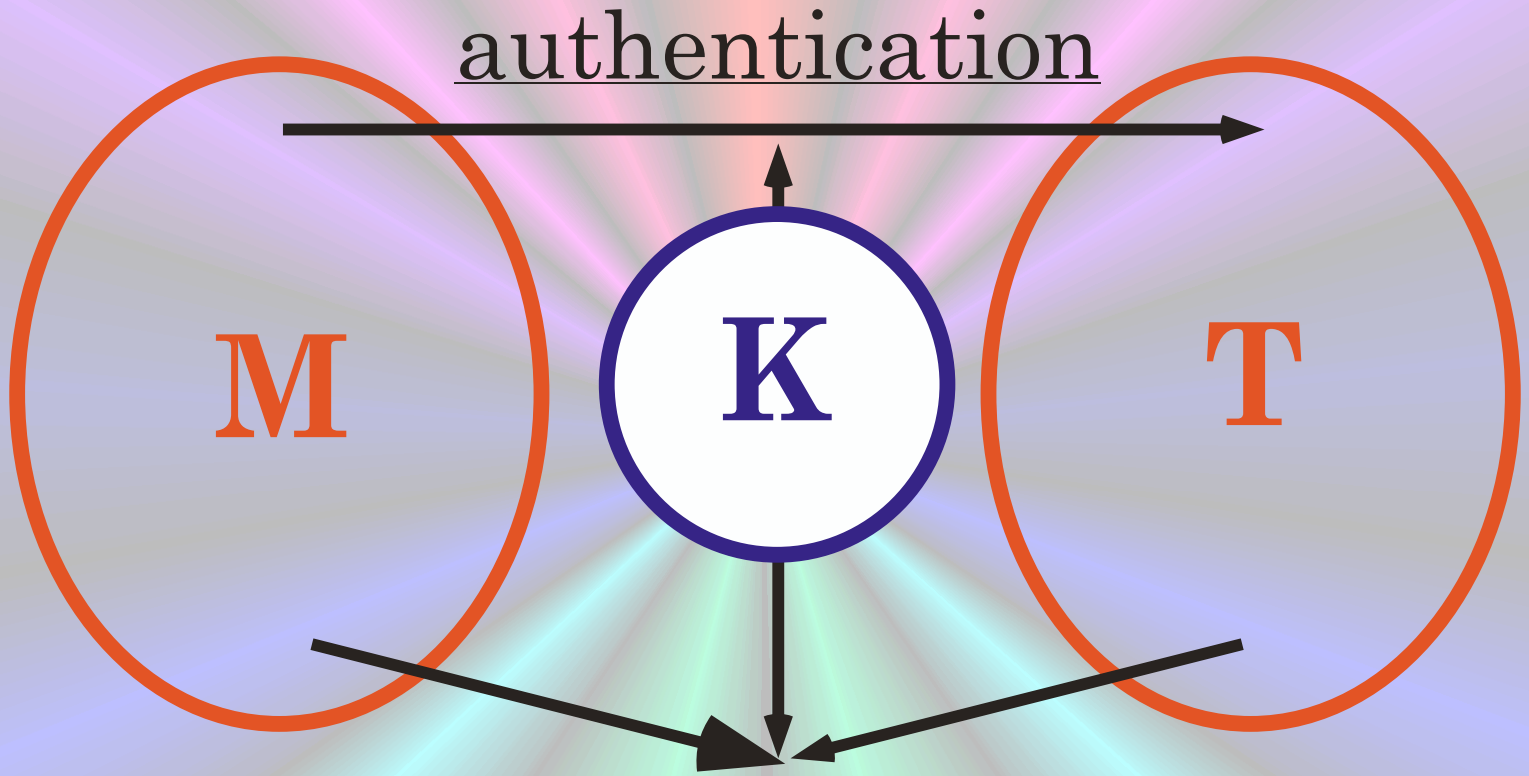


Will you marry me ?

No, I never will !

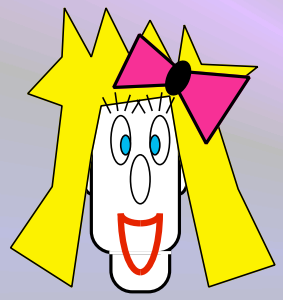


symmetric authentication

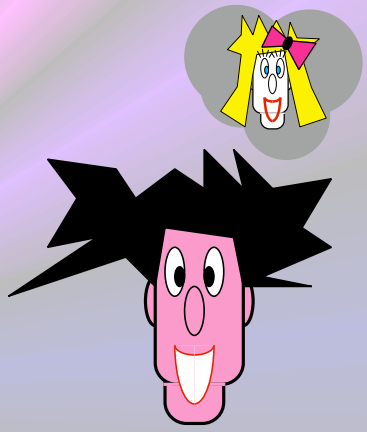


Information Theoretical Security

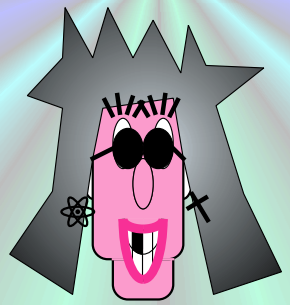
Authentication



(m,t)



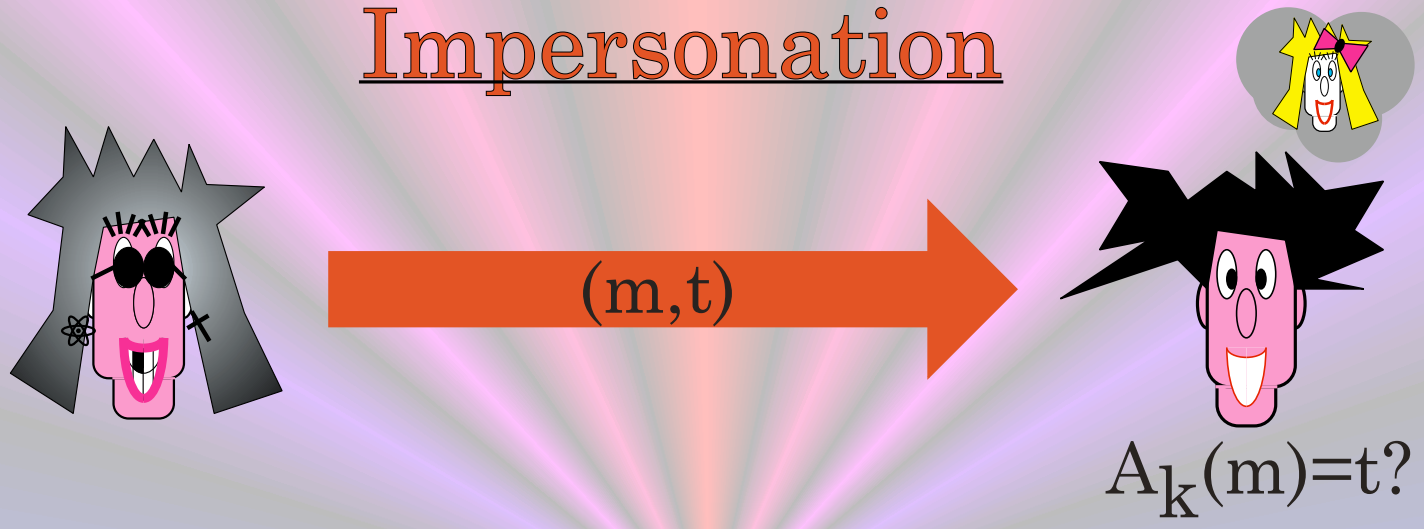
$t=A_k(m)$



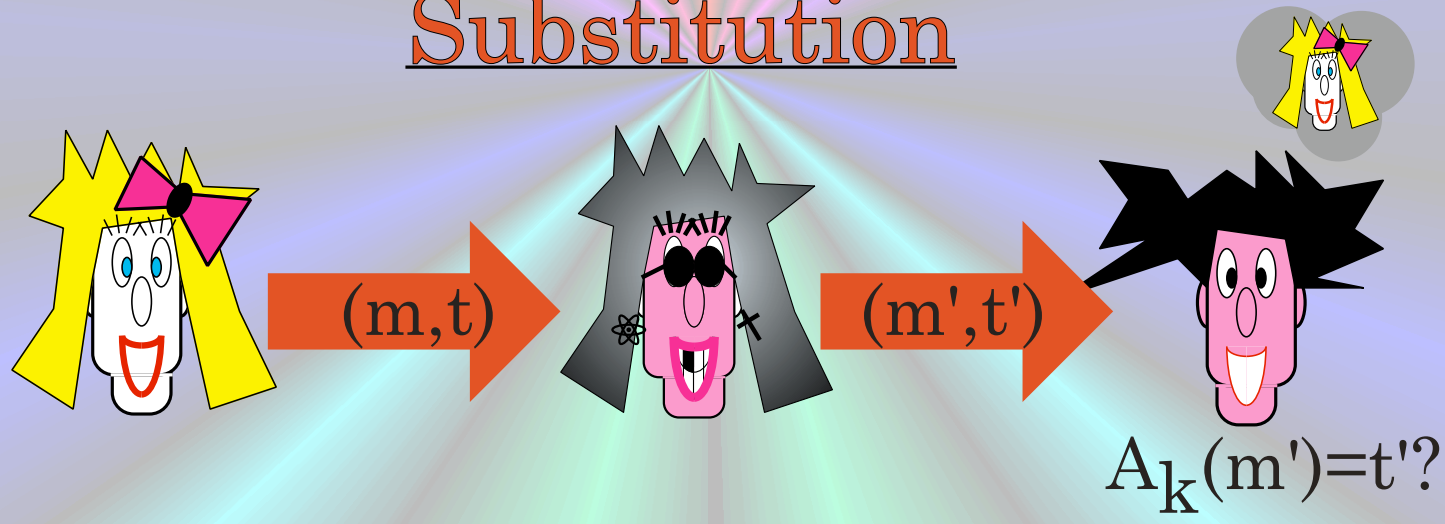
$A_k(m)=t?$

Information Theoretical Security

Impersonation



Substitution



Information Theoretical Security

WC One-Time-Authentication

$$A_{\mathbf{M},b}(x) = \mathbf{M}x \oplus b$$

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

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

$\Pr(A_{\mathbf{M},b}(m)=t) = 1/|T| = 1/2^s$

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

$\Pr(A_{\mathbf{M},b}(m')=t' \mid A_{\mathbf{M},b}(m)=t) = 1/|T| = 1/2^s$

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

$$A_{\mathbf{M},b}(x) = \mathbf{M}x \oplus b$$

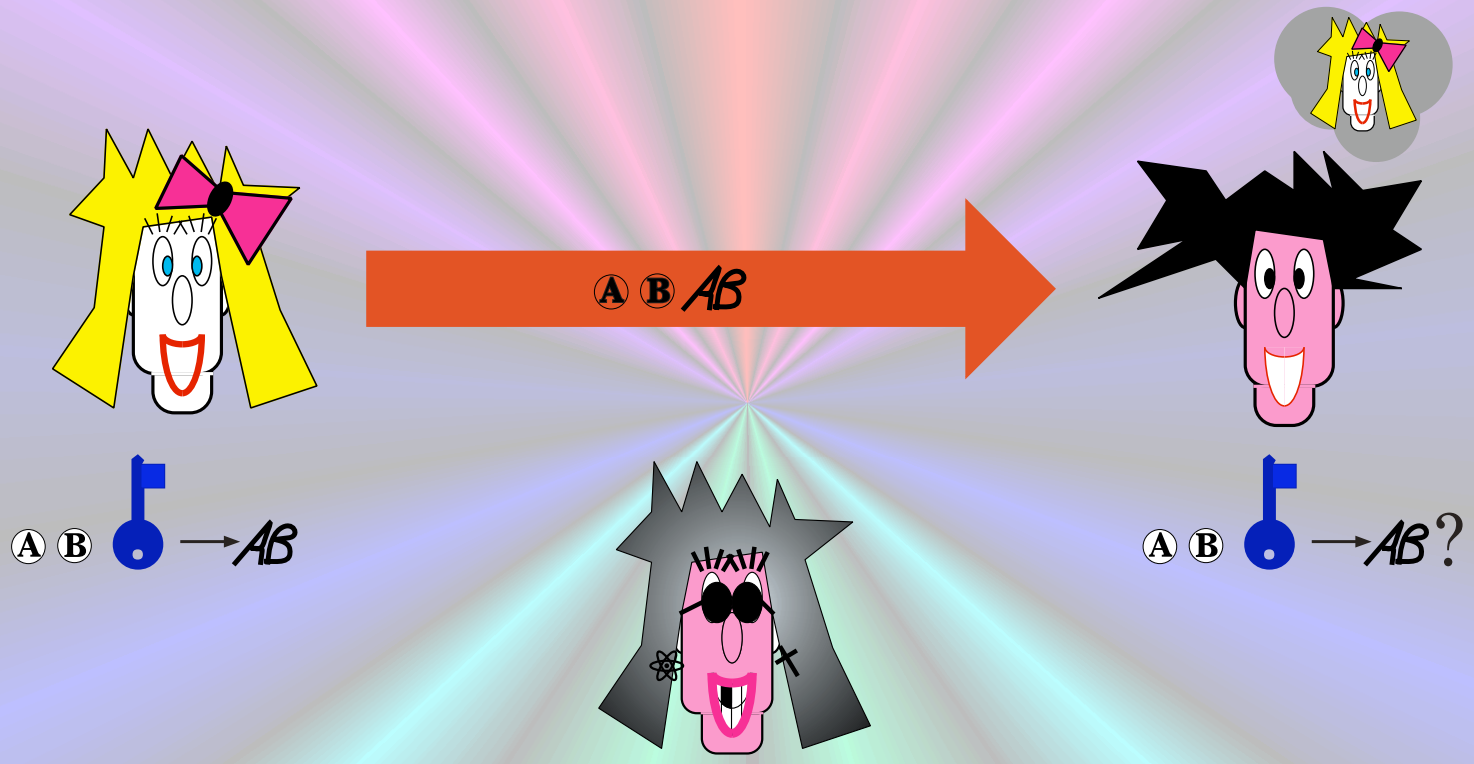
[**I**:**M**]m⊕[0:b]=[m:t]

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

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

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

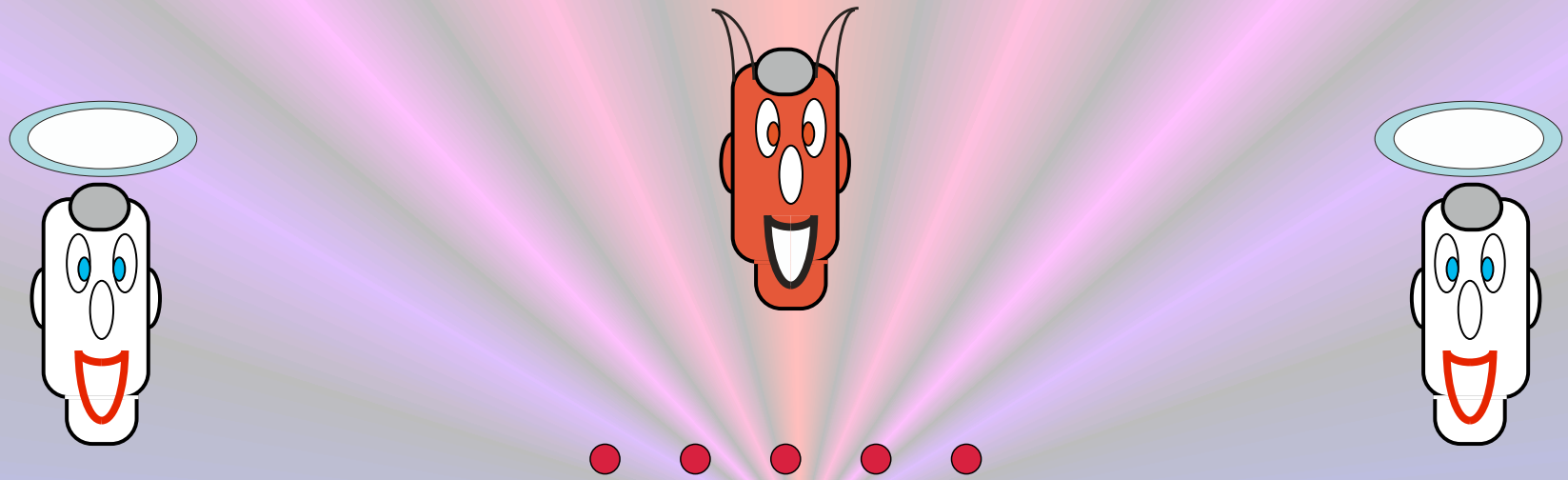
Authentication



Information Theoretical Security

(1.2) Complexity Theoretical Cryptography

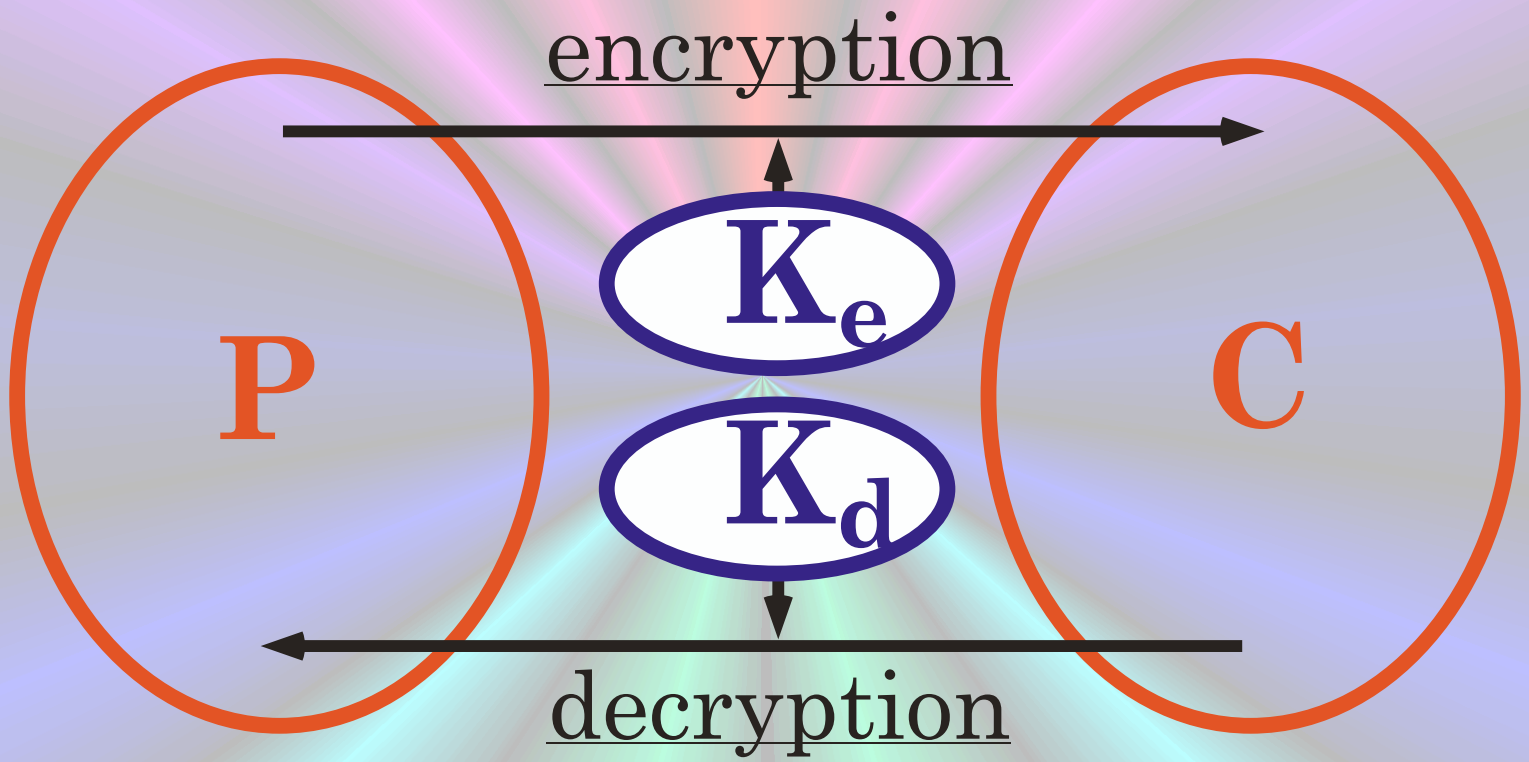
(1.2) Complexity Theoretical Cryptography



(1.2.1) Public key cryptosystem

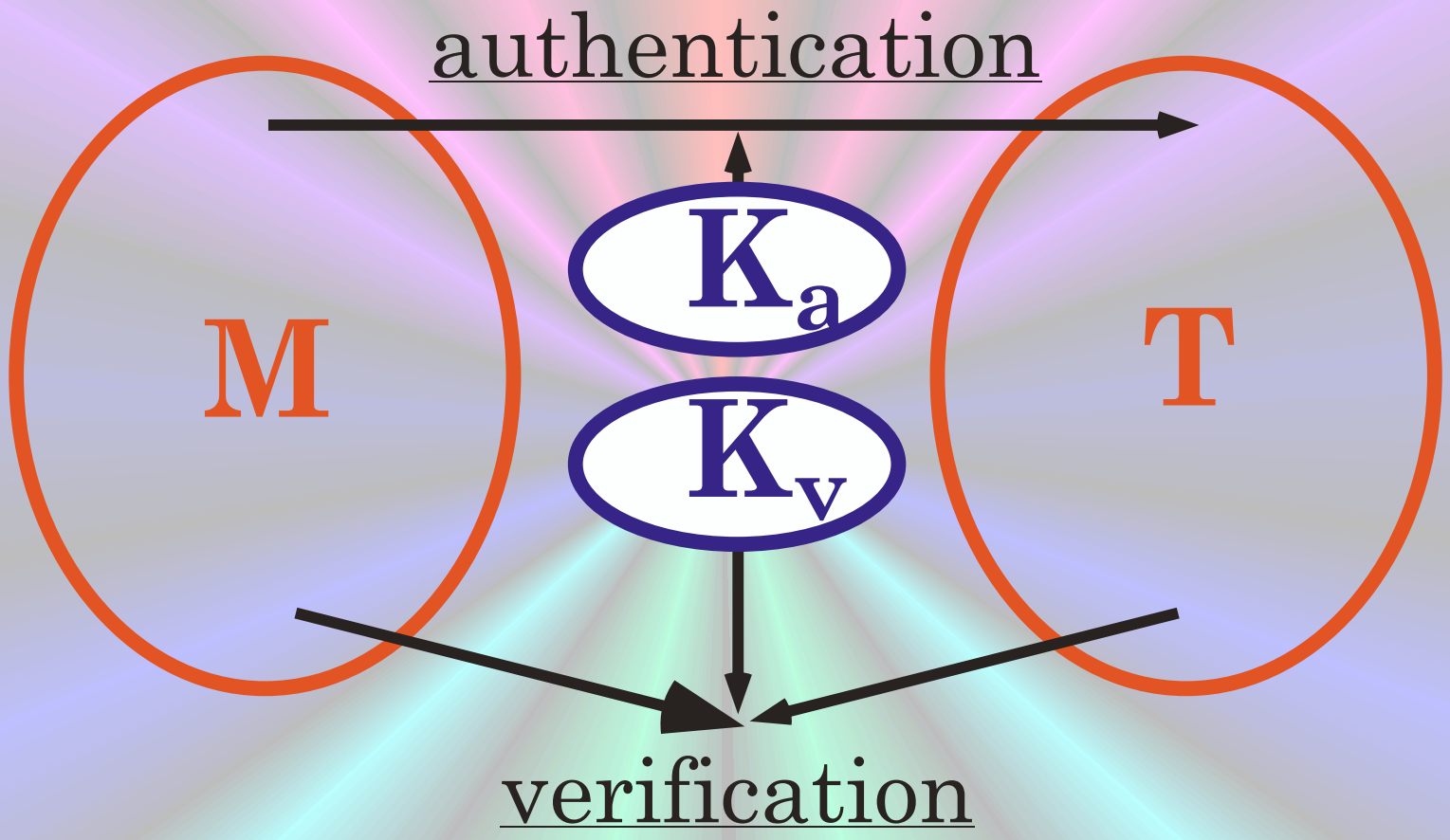
(1.2.2) Digital signature scheme

asymmetric encryption
(public-key cryptography)



Complexity Theoretical Security

asymmetric authentication
(digital signature schemes)



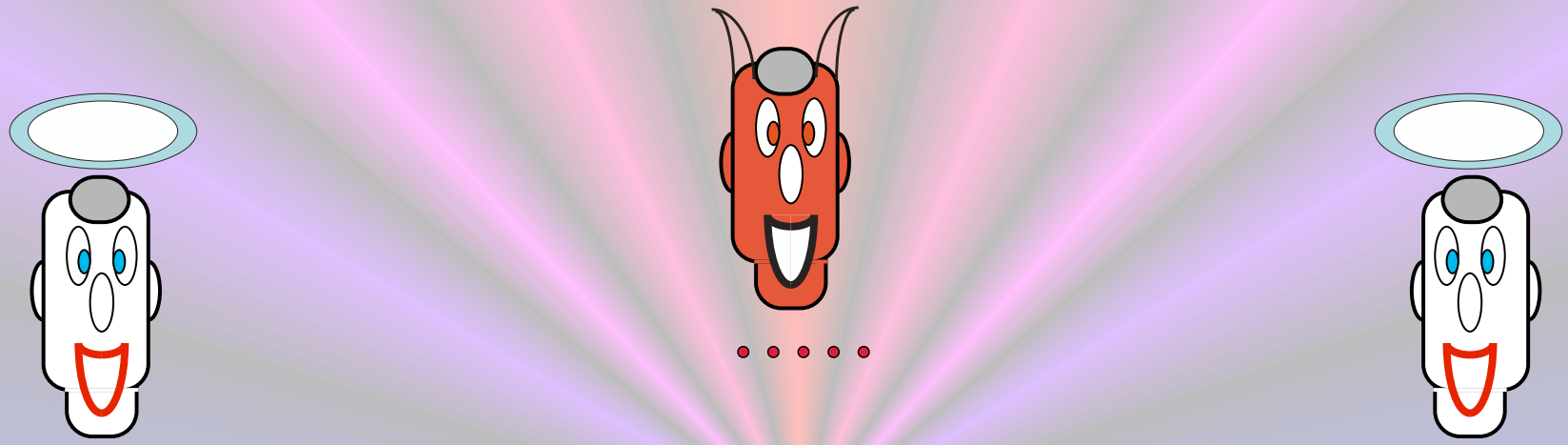
Complexity Theoretical Security

(2)
Quantum Information & Computations

(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)

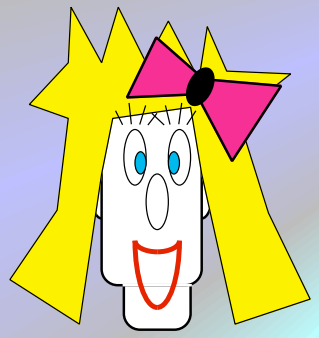
(3.1.2) One-time pad : one-time Q-pad (Q-teleportation)
Vernam Q-cipher

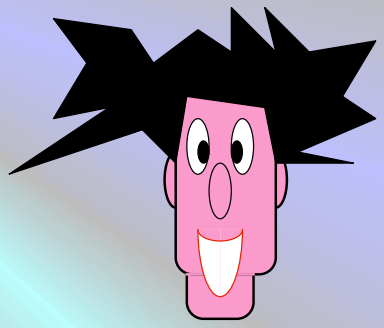
(3.1.3) one-time authentication : 1x authenticated Q-pad +
1x Q-authentication

(3.1.1) Key distribution

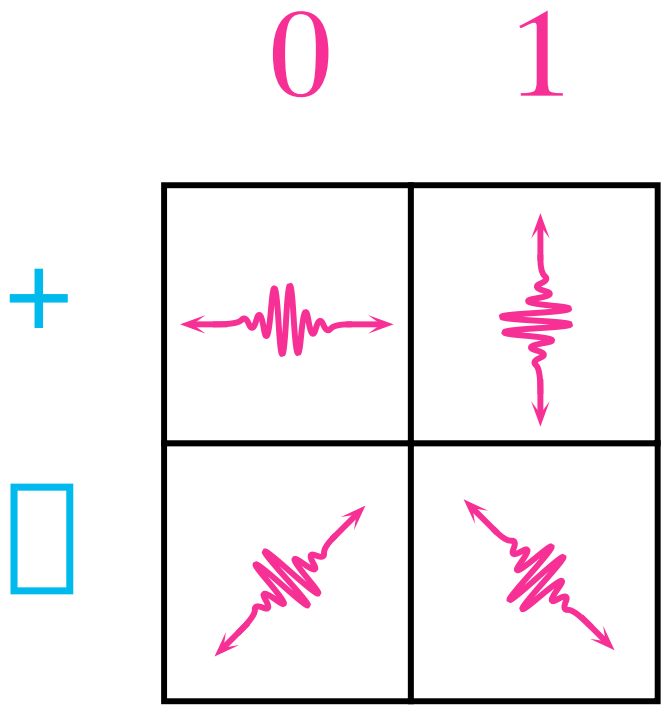
Classical key: Q-distribution of keys(BB84)
+ error-correction
+ privacy amplification

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

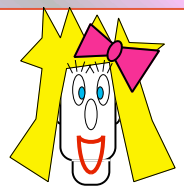


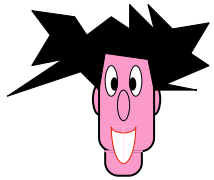


Ambiguous Coding Scheme



(3.1.1C) Quantum distribution of Keys



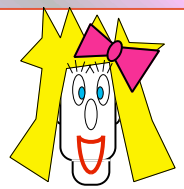


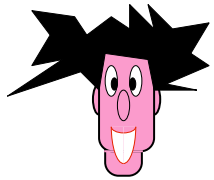
:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
:			+	+		+	+	+		+	+				+				+	+		+		+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
:	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
:	0	←	←	0	←	1	←	←	1	←	0	←	←	←	←	1	0	←	←	1	←	0	0	0
:	0			0		1			1		0					1	0			1		0	0	0
:	0			0		1			1		0					1	1			1		0	0	0
:	0					1					0						1					0		
:	=			=					=													=		
:				0					1							1				1		0	0	
:				0					1							1				1		0	0	

20%

Bennett- Brassard

(3.1.1C) Quantum distribution of Keys





:	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
	□	+	□	+	+	+	□	□	□	□	+	+	+	+	□	□	□	+	□	+	+	+	□	+
:	¿	¿	¿	¿	¿	¿	?	¿	¿	¿	¿	¿	¿	¿	¿	¿	?	¿	¿	¿	¿	¿	¿	¿
	□	□	+	+	□	+	+	+	□	+	+	□	□	□	+	□	□	□	+	+	□	+	□	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	0	1	1	1	0	0	0	1	1	0	0
:	□	+	□	+	+	+	□	□	□	□	+	+	+	+	□	□	□	+	□	+	+	+	□	+
:	0	↓	↓	0	↓	1	↓	↓	1	↓	0	↓	↓	↓	↓	1	0	↓	↓	1	↓	0	0	0

:	1			1		0			0		1					0	0			0		1	1	1
:	1					0					1						0							1
:	□					□			≠							=								□
:				0					1							1				1		0	0	
:				1					0							0				0		1	1	

20%

Ekert

(3.1.1C) Quantum 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)

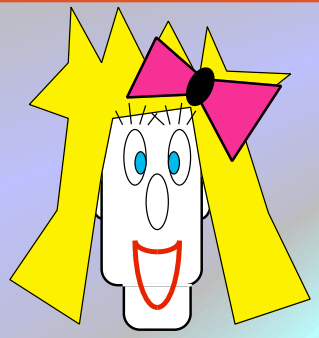
+ error-correction

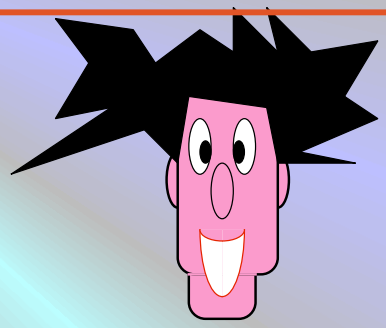
+ privacy amplification

Quantum key : Q-key distribution(Ekert/Lo-Chau)

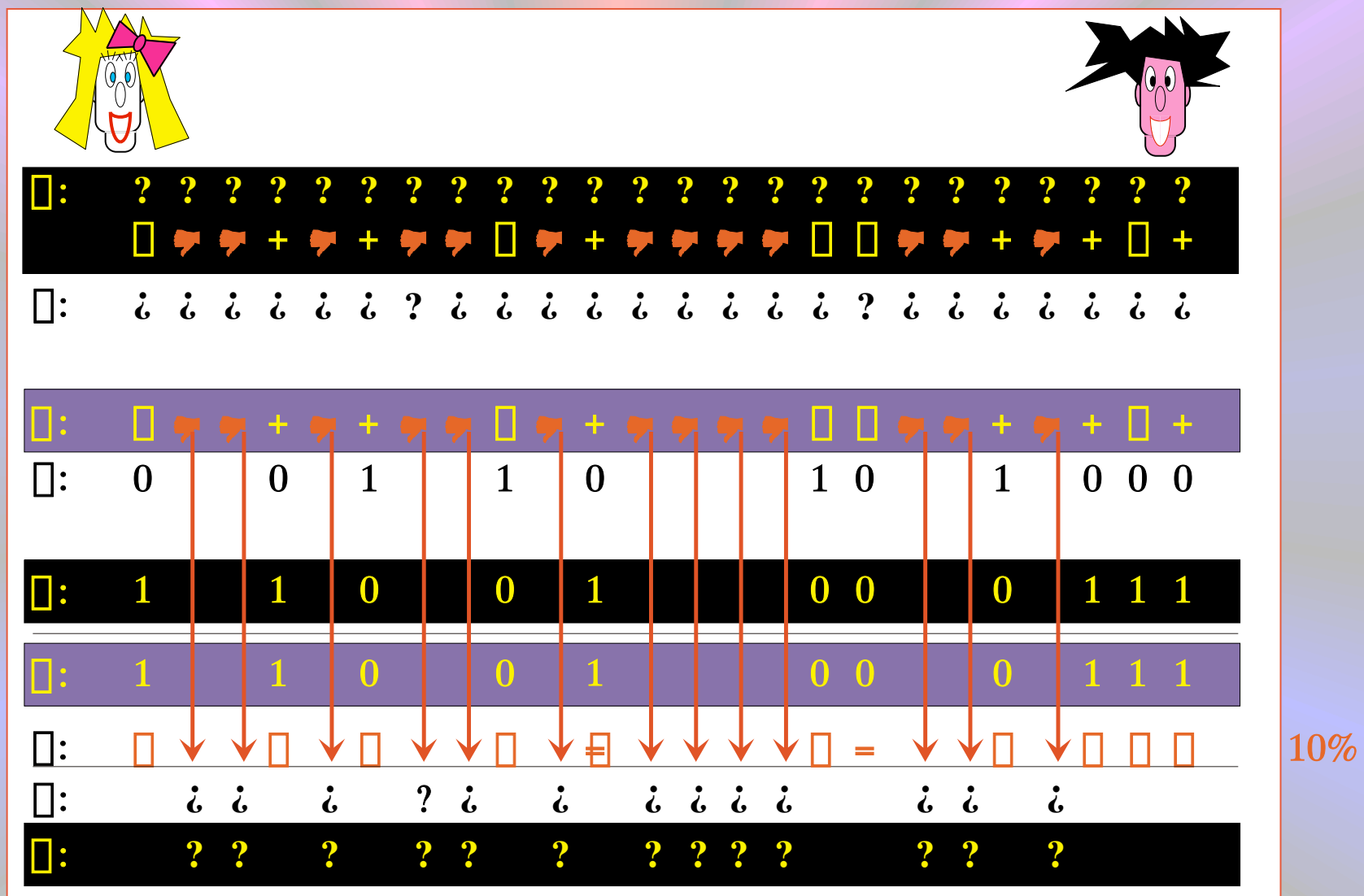
+ Q-error-correction (CSS) or

Q-Distillation (Purification)



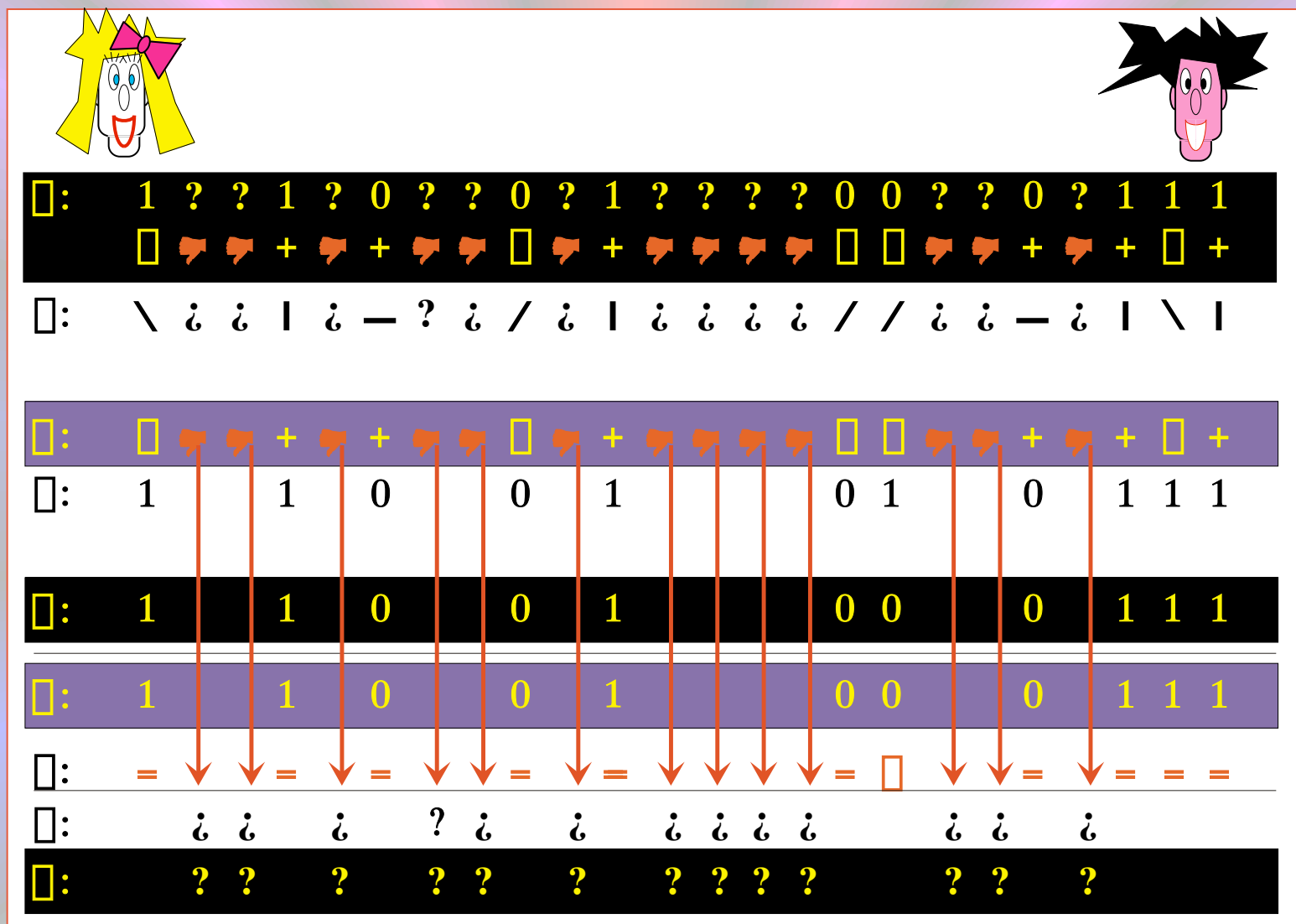


(3.1.1Q) Quantum-Key distribution



Ekert + Lo-Chau

(3.1.1Q) Quantum-Key distribution



Shor-Preskill

(3.1.1Q) Quantum-Key distribution

• • • • •

- Produces raw quantum key (EPR states)

- Observed error rate indicates amount of impurity of EPR states

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

• • • • •

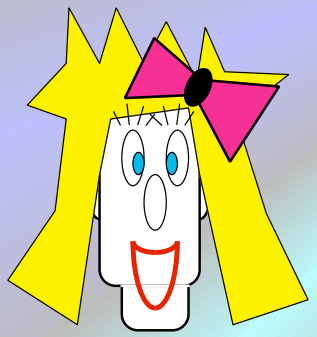
(3.1.2) One-time pad

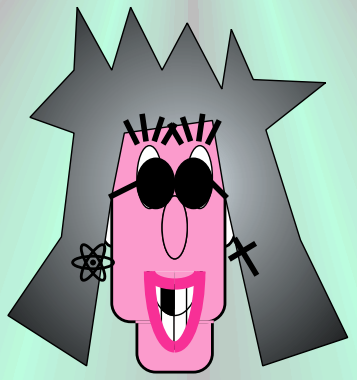
Classical key : Vernam Q-cipher (various sources)

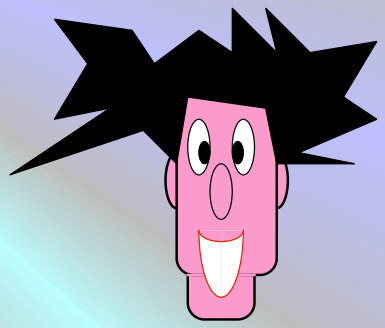
Quantum Ciphertext

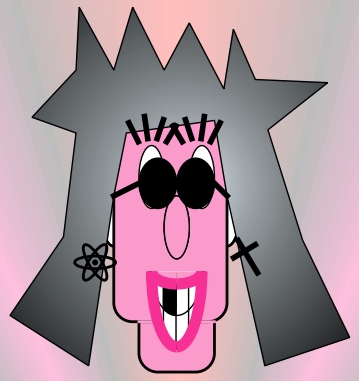
Quantum key : one-time Q-pad (Q-teleportation)

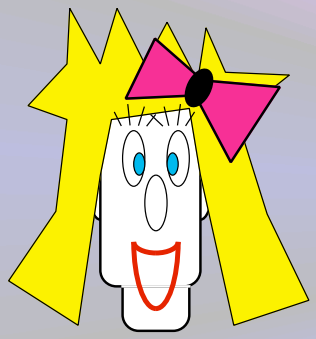
Classical Ciphertext (BBCJPW)



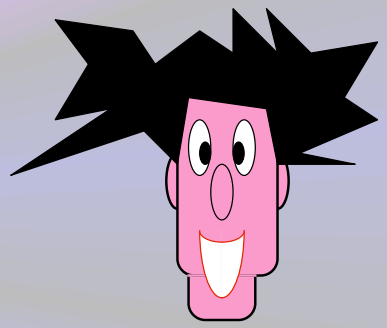








|Ωιλλ ψου μαρρψ με ?⟩

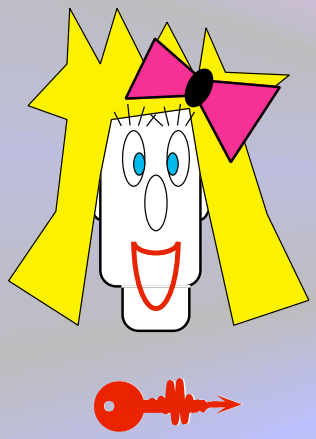


|Διωορχε ψουρ ωιφε φιρστ !⟩

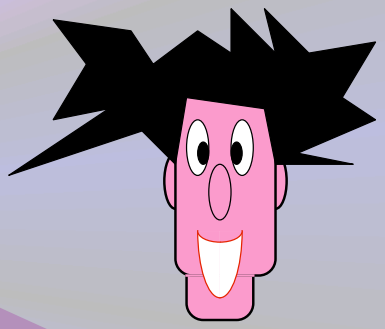
|Τηε παπερσ αρε ιν τηε μαιλ...⟩

|OK, I ωιλλ !⟩

(3.1.2Q) One-time Q-pad



8RdewtU5qkLa$es!T9@

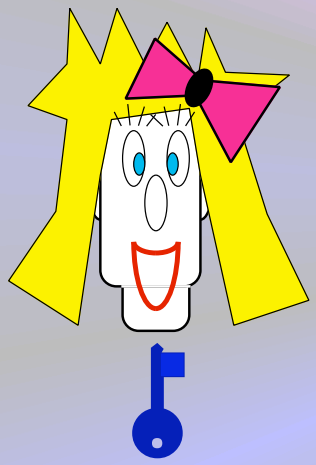


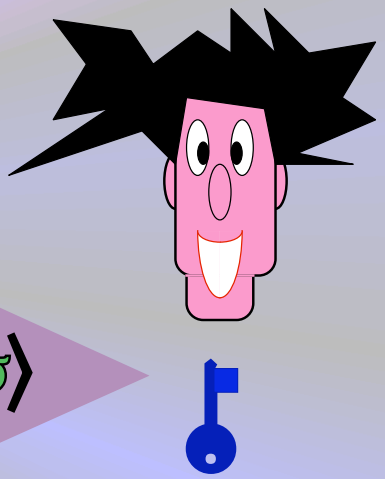
I(D%eXhDqIiykl#2cV7dEwnMs

H&fs@tyHvFGhaOKpTrGbl.Z/rUih*

B7B3tdsjUila

(3.1.2C) Vernam Q-cipher





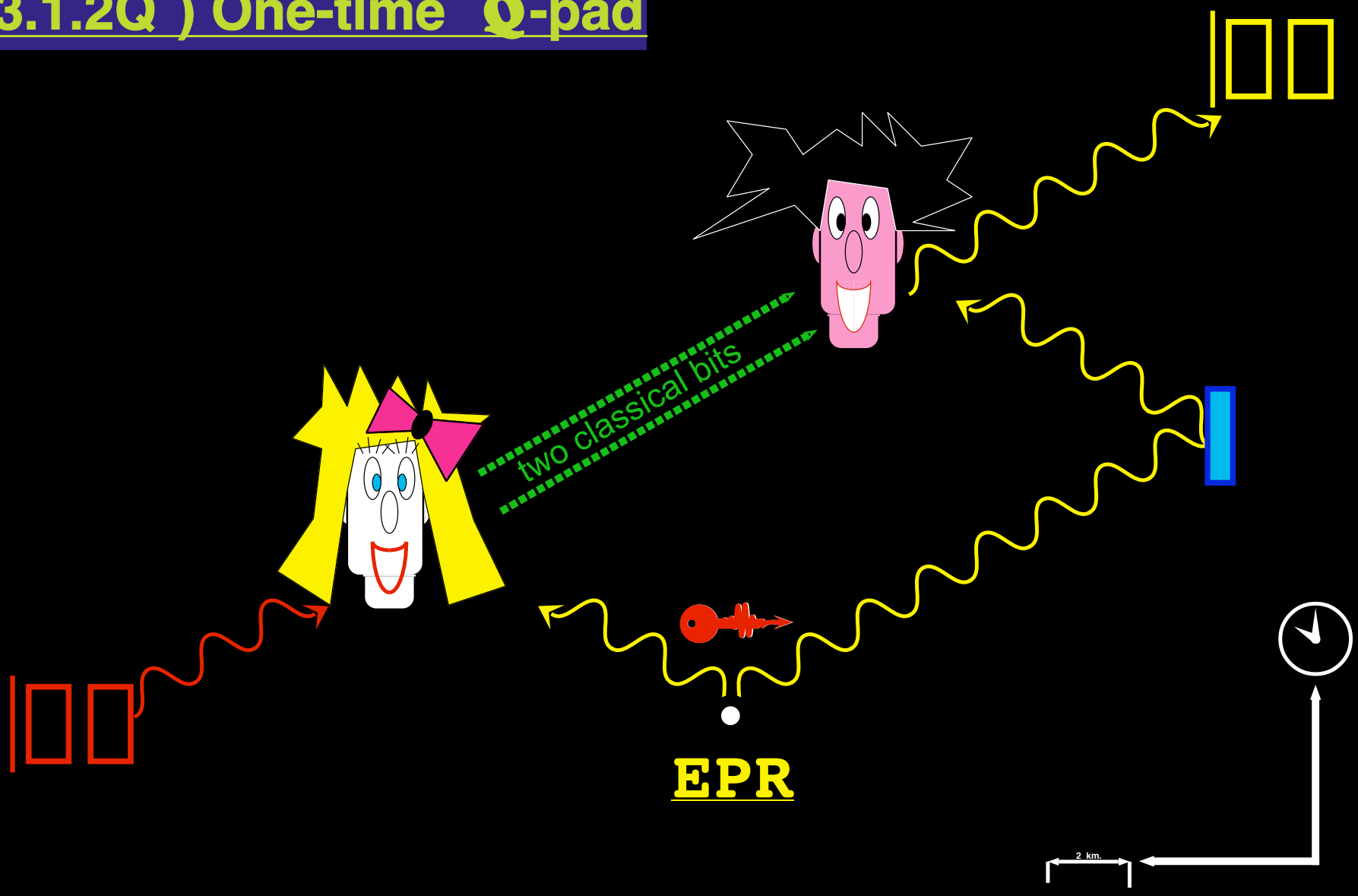
|8PδεωτY5θκΛαΞεσ!T9≅⟩

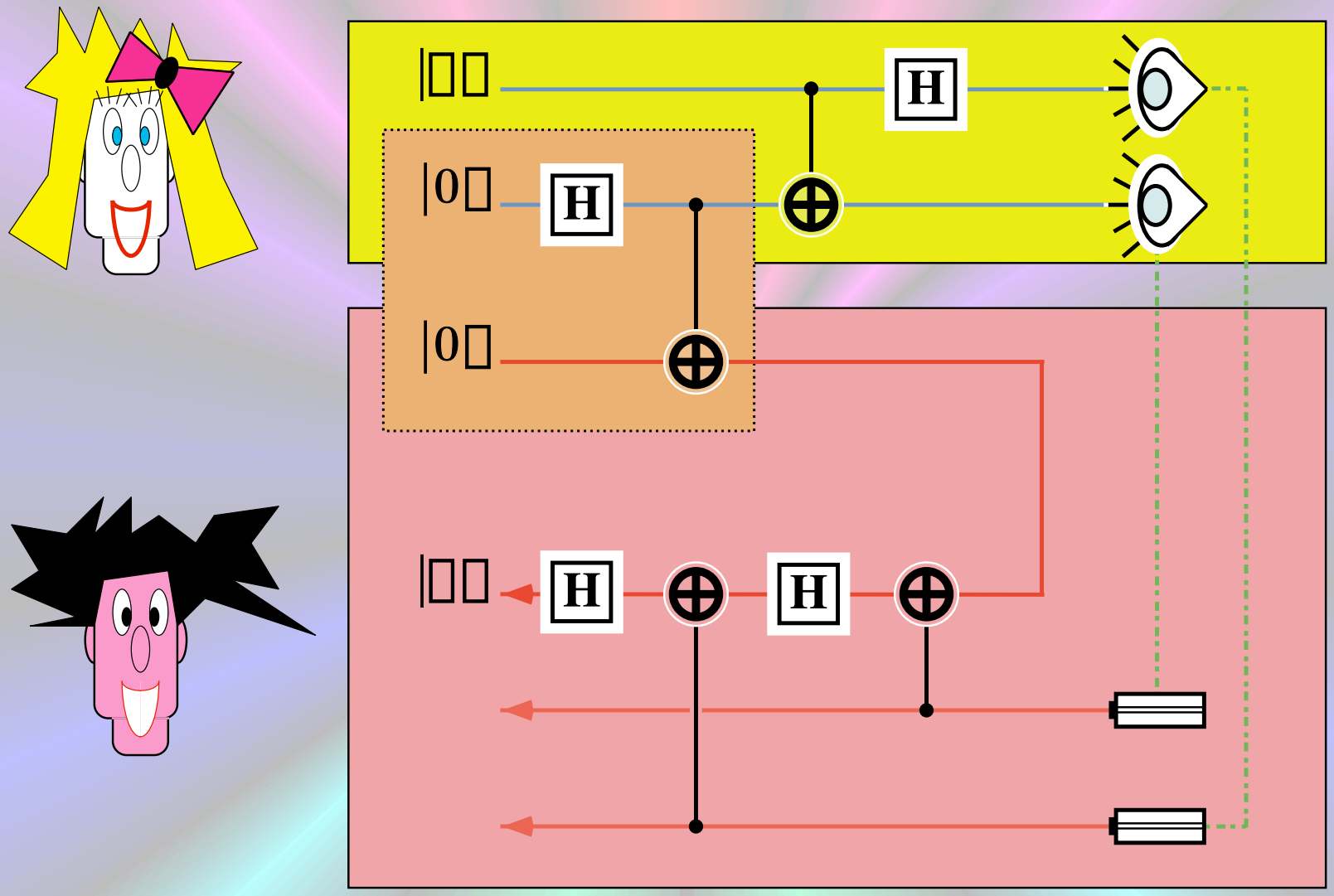
|I(Δ%εΞηΔθIιψκλ#2χς7δEωνMσ⟩

|H&φσ≅τψϖΦηαOKπTρΓβλ.Z/ρYιη*⟩

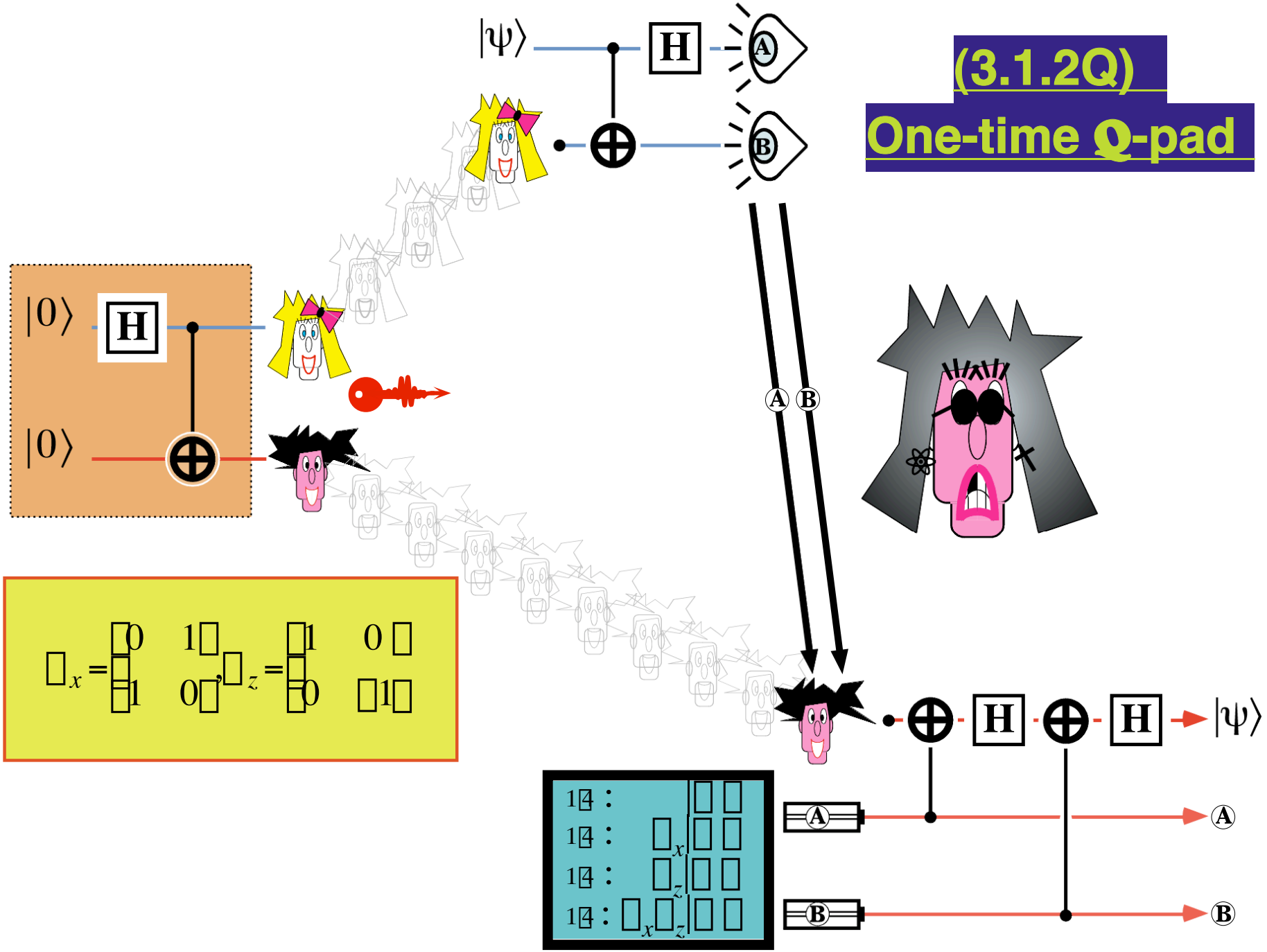
|B7B3τδσφYιλα⟩

(3.1.2Q) One-time Q-pad





(3.1.2Q) One-time Q-pad

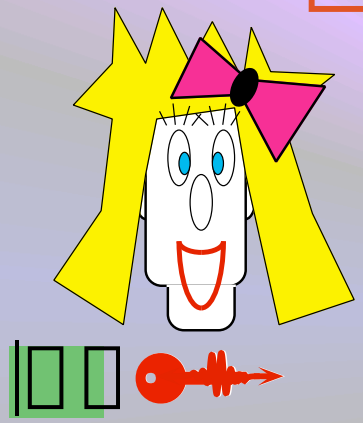


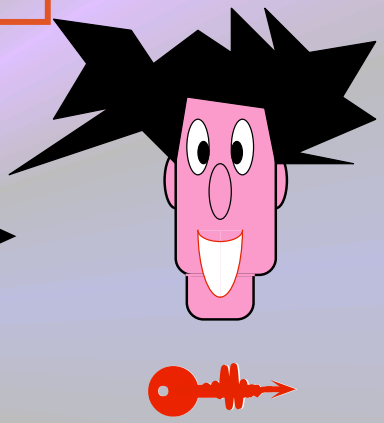
$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

(3.1.2Q) One-time Q-pad

Quantum key : one-time Q-pad

Classical Ciphertext





Ⓐ Ⓑ

two random bits

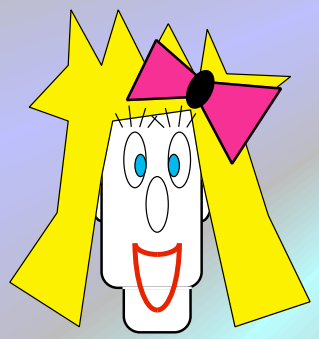
(3.1.2) One-time pad

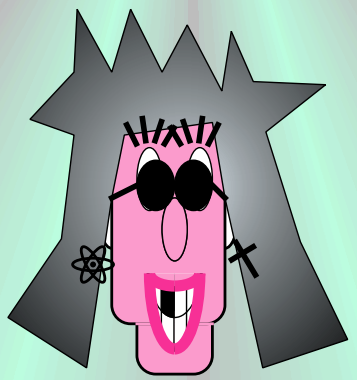
Classical key : Vernam Q-cipher (various sources)

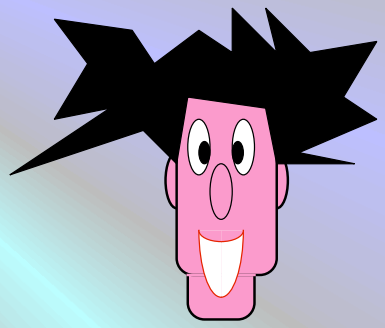
Quantum Ciphertext

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

Classical Ciphertext







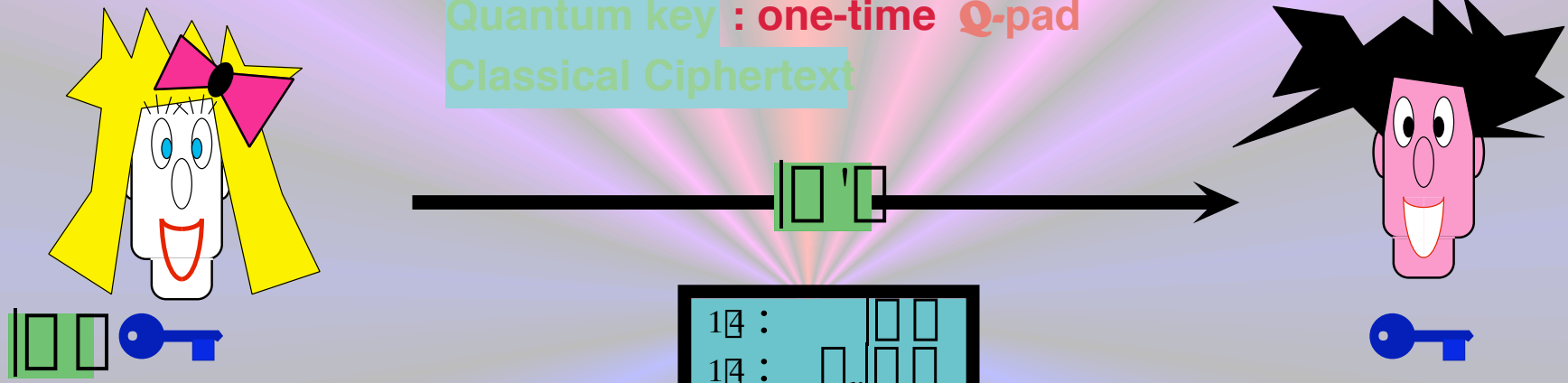
(3.1.2C) Vernam Q-cipher

Classical key: Vernam Q-cipher

Quantum Ciphertext

Quantum key : one-time Q-pad

Classical Ciphertext



a,b random bit key

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

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

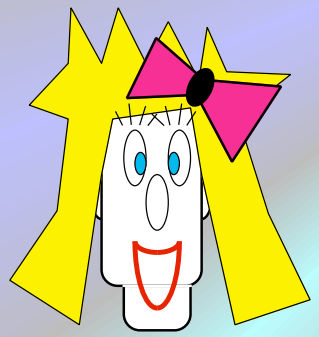
a,b random bit key

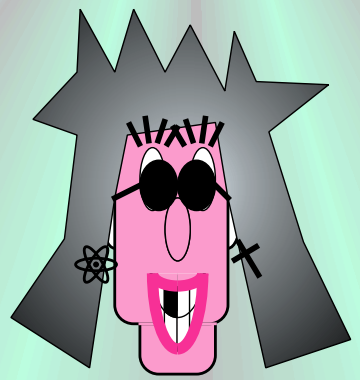
$|\psi\rangle = (\sigma_z)^b (\sigma_x)^a |\psi'\rangle$

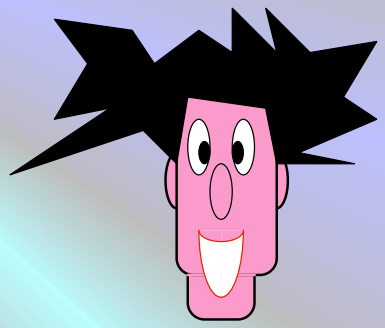
(3.1.3) One-time Authentication

Classical key : 1x Q-Authentication (BCGST)
Quantum message+tag

Quantum key : 1x Authenticated Q-pad
Classical message+tag (BBCJPW)

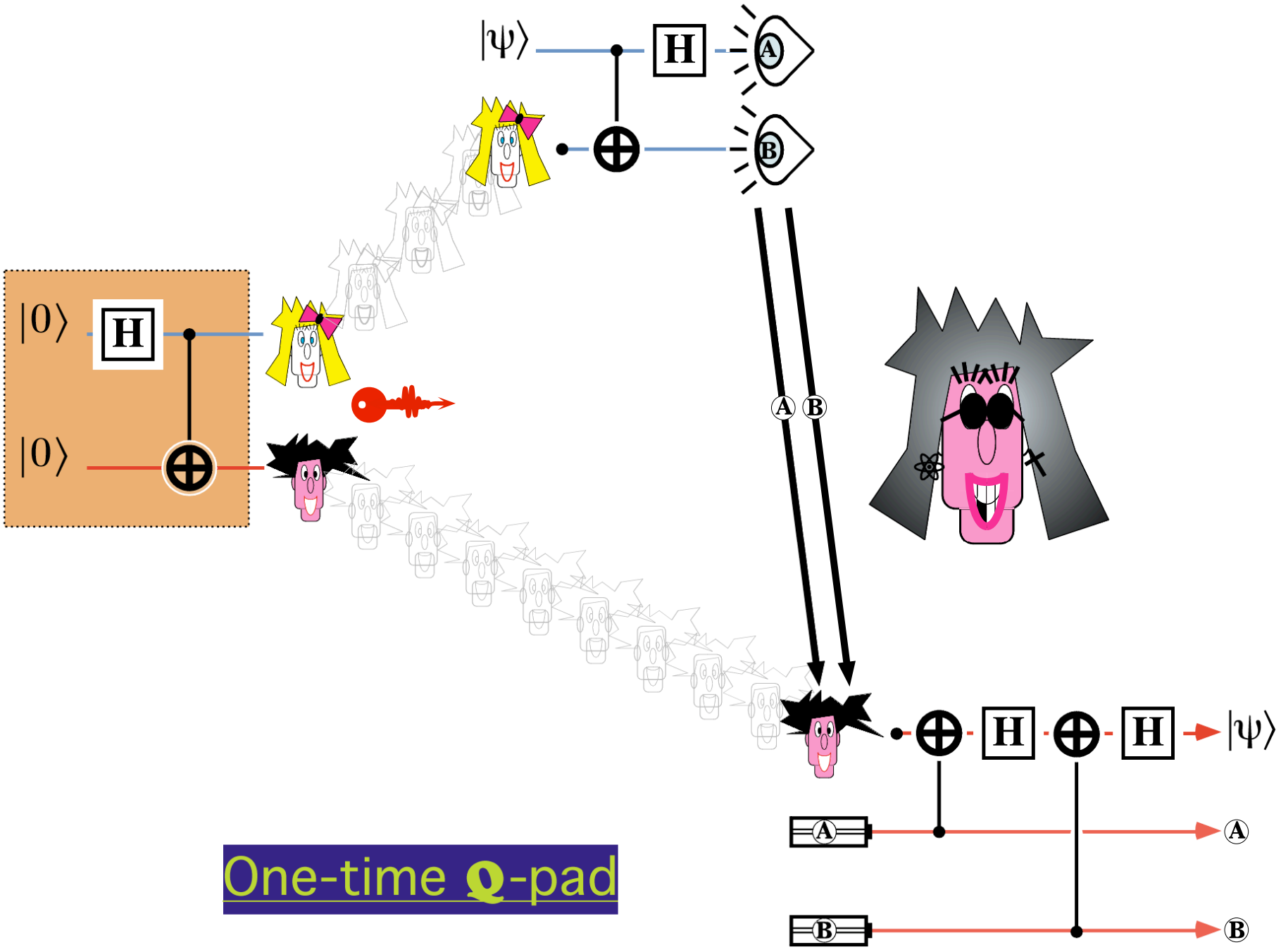




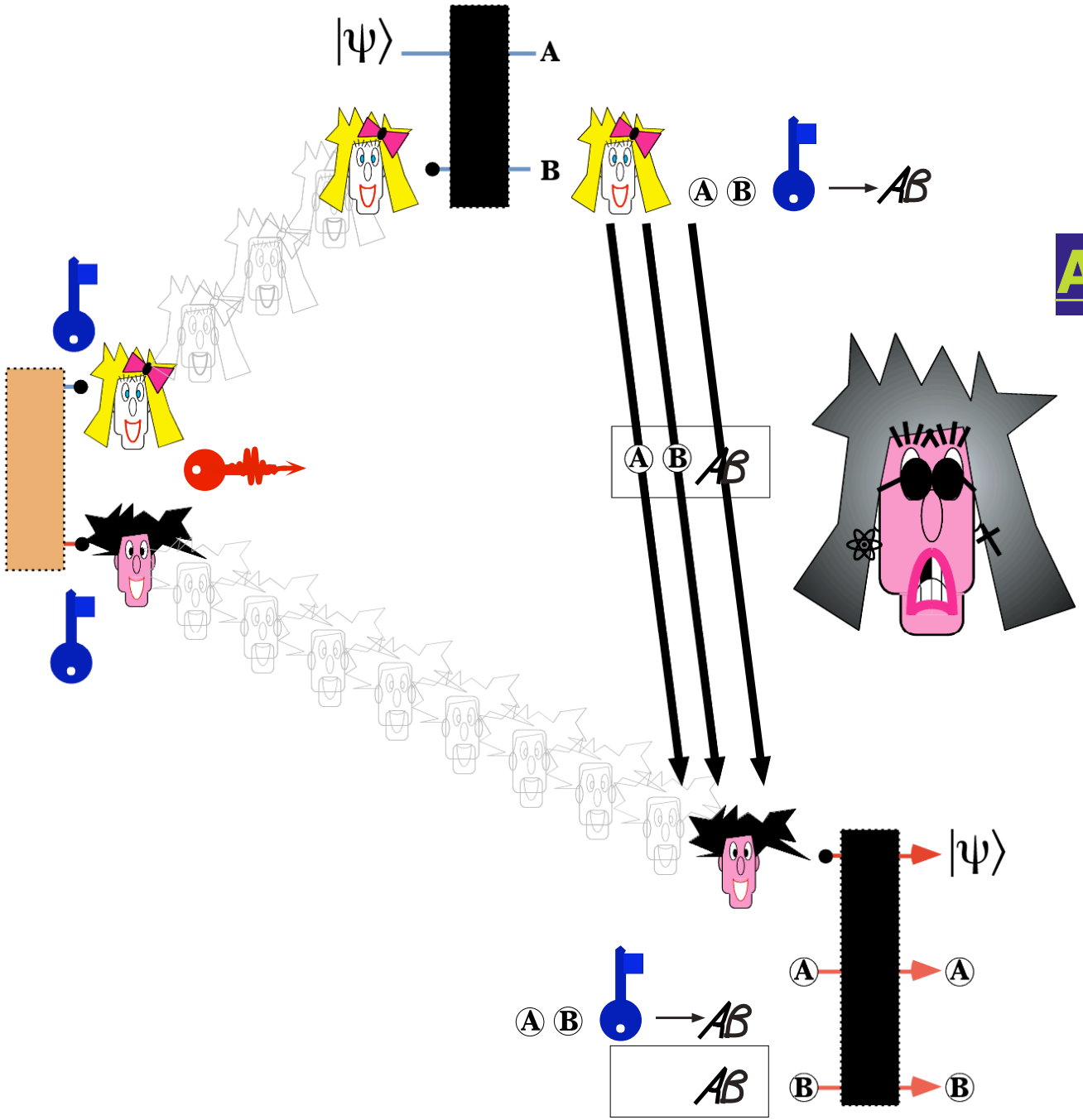


(3.1.3Q) One-time Authenticated Q-pad

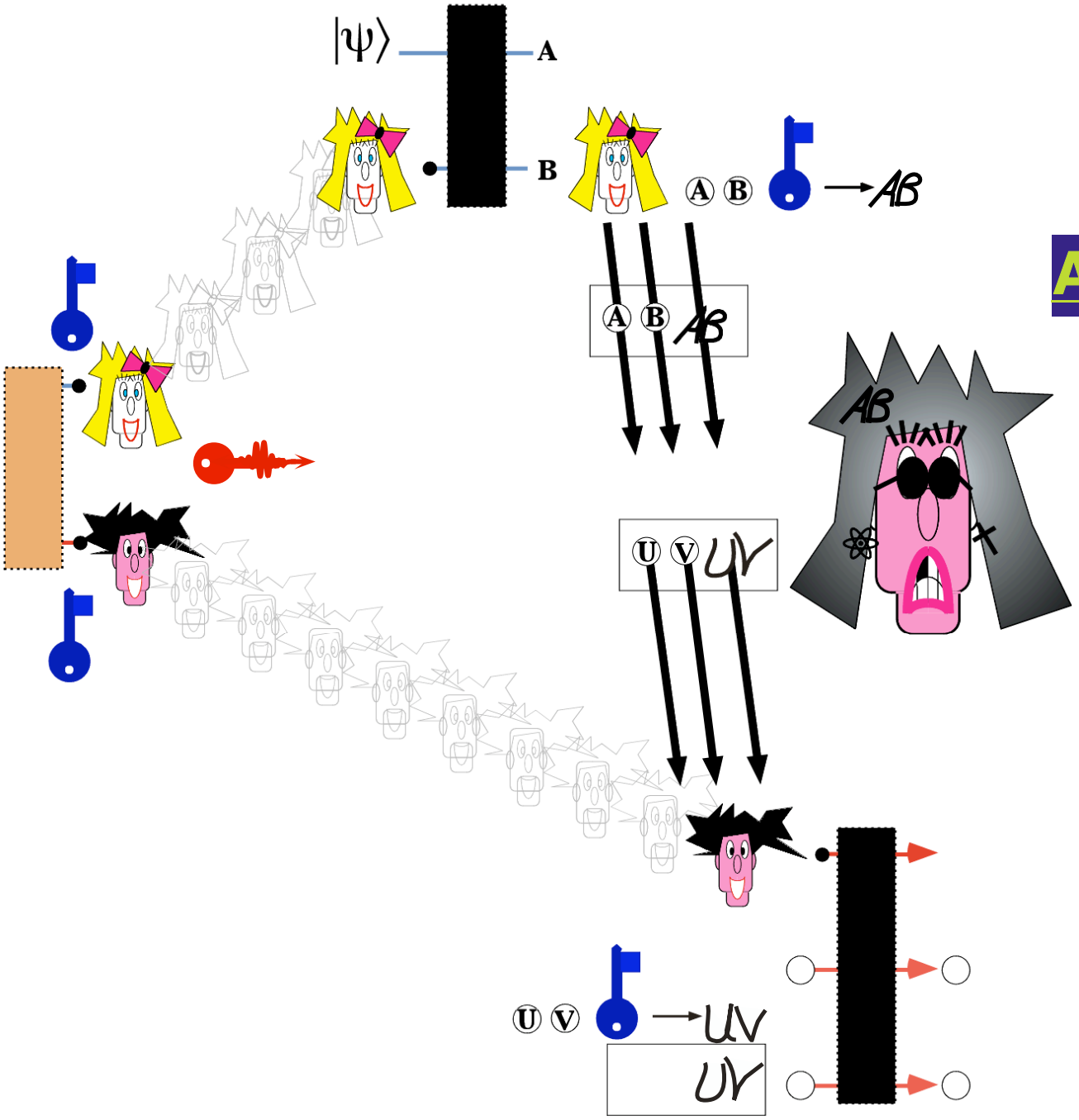
(3.1.3C) One-time Q-Authentication



One-time Q-pad



(3.1.3Q) One-time Authenticated Q-pad



(3.1.3Q) One-time Authenticated Q-pad

(3.1.3Q) One-time Authenticated Q-pad

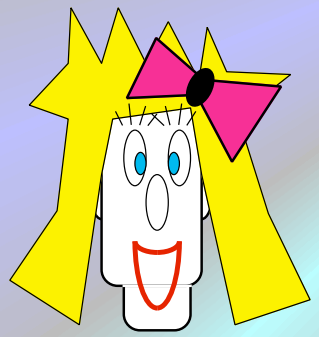
Quantum key : 1x Authenticated Q-pad

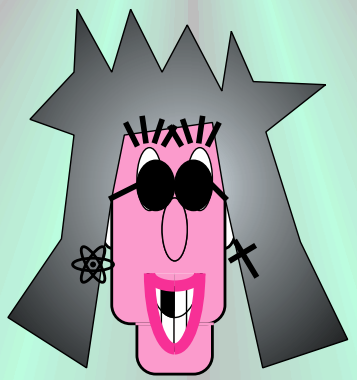
Classical message+tag

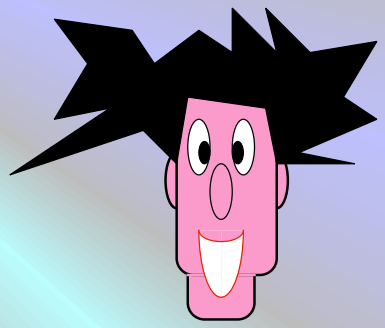
(3.1.3) One-time Authentication

Classical key: 1x Q-Authentication (BCGST)
Quantum message+tag

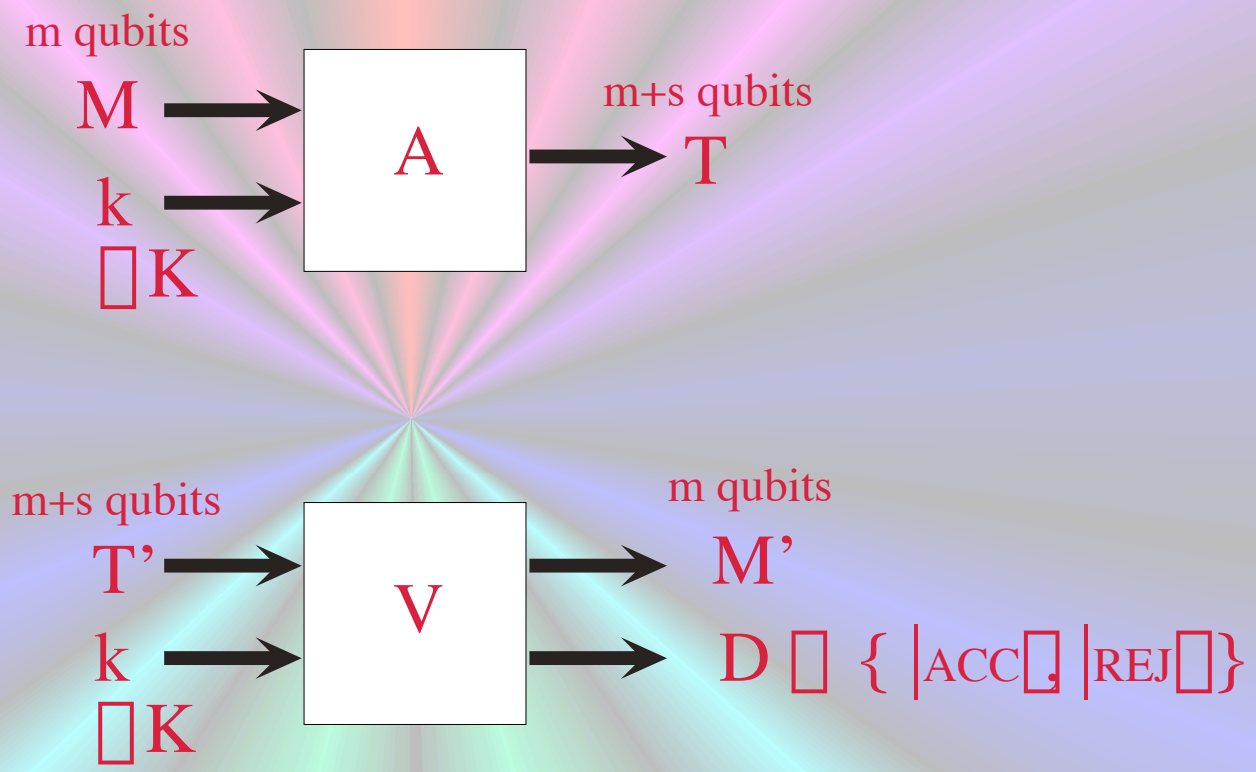
Quantum key : 1x Authenticated Q-pad
Classical message+tag (BBCJPW)







(3.1.3C) One-time Q-Authentication



(3.1.3C) One-time Q-Authentication

For any pure state $|\psi\rangle$ consider the measurement on (M',D) such that

- output Right if M'=$|\psi\rangle$ or if D=$|\mathrm{REJ}\rangle$
- output Wrong otherwise

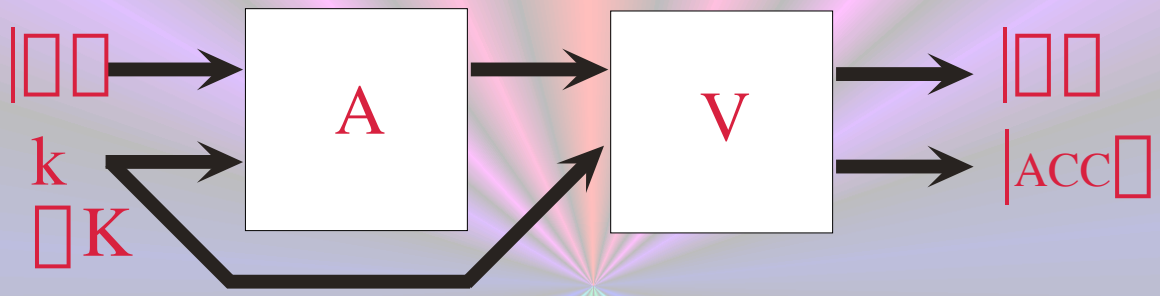
The corresponding projectors are

$$R_{|\psi\rangle} = |\psi\rangle\langle\psi| \otimes I_D + I_{M'} \otimes |\mathrm{REJ}\rangle\langle\mathrm{REJ}| - |\psi\rangle\langle\psi| \otimes |\mathrm{REJ}\rangle\langle\mathrm{REJ}|$$

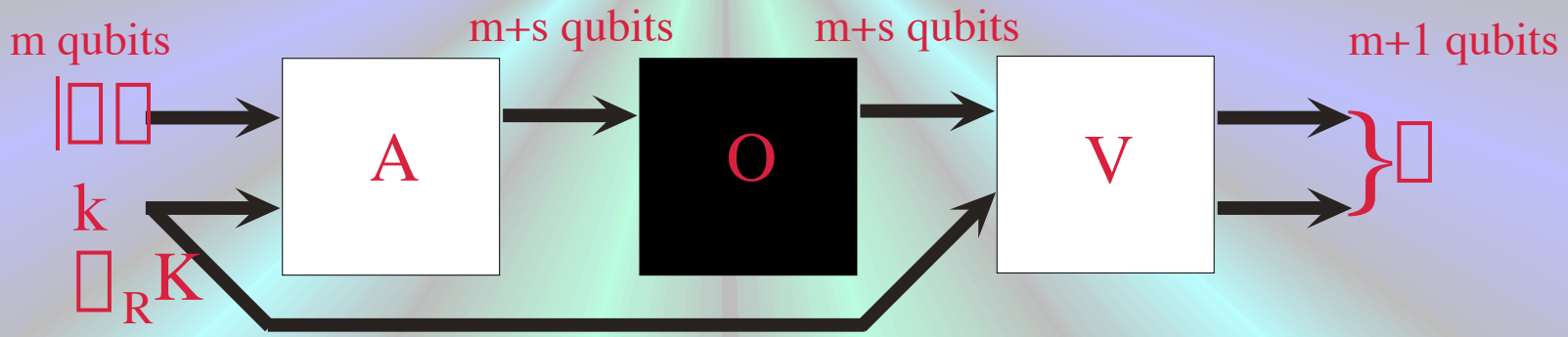
$$W_{|\psi\rangle} = (I_{M'} - |\psi\rangle\langle\psi|) \otimes |\mathrm{ACC}\rangle\langle\mathrm{ACC}|$$

(3.1.3C) One-time Q-Authentication

Completeness:

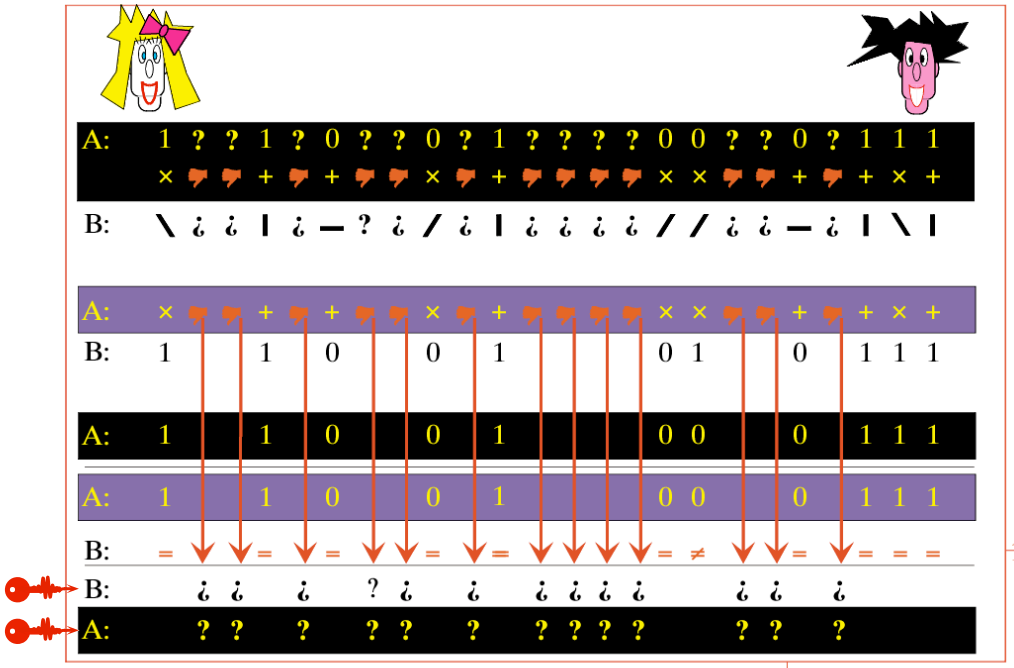


Soundness:



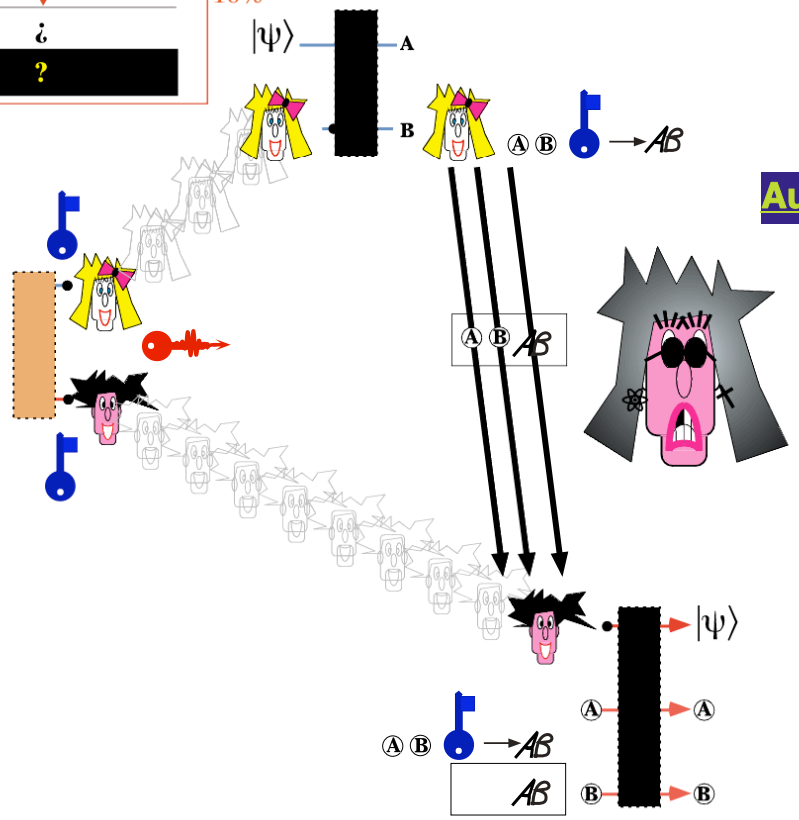
$$Tr(R_{|\Psi\rangle}) \geq 1-2^{-s}$$

(3.1.1Q) Quantum-Key distribution



Shor-Preskill

10%



(3.1.3Q) One-time Authenticated Q-pad

(3.1.3C) One-time *interactive* Q-Authentication

. . . . .

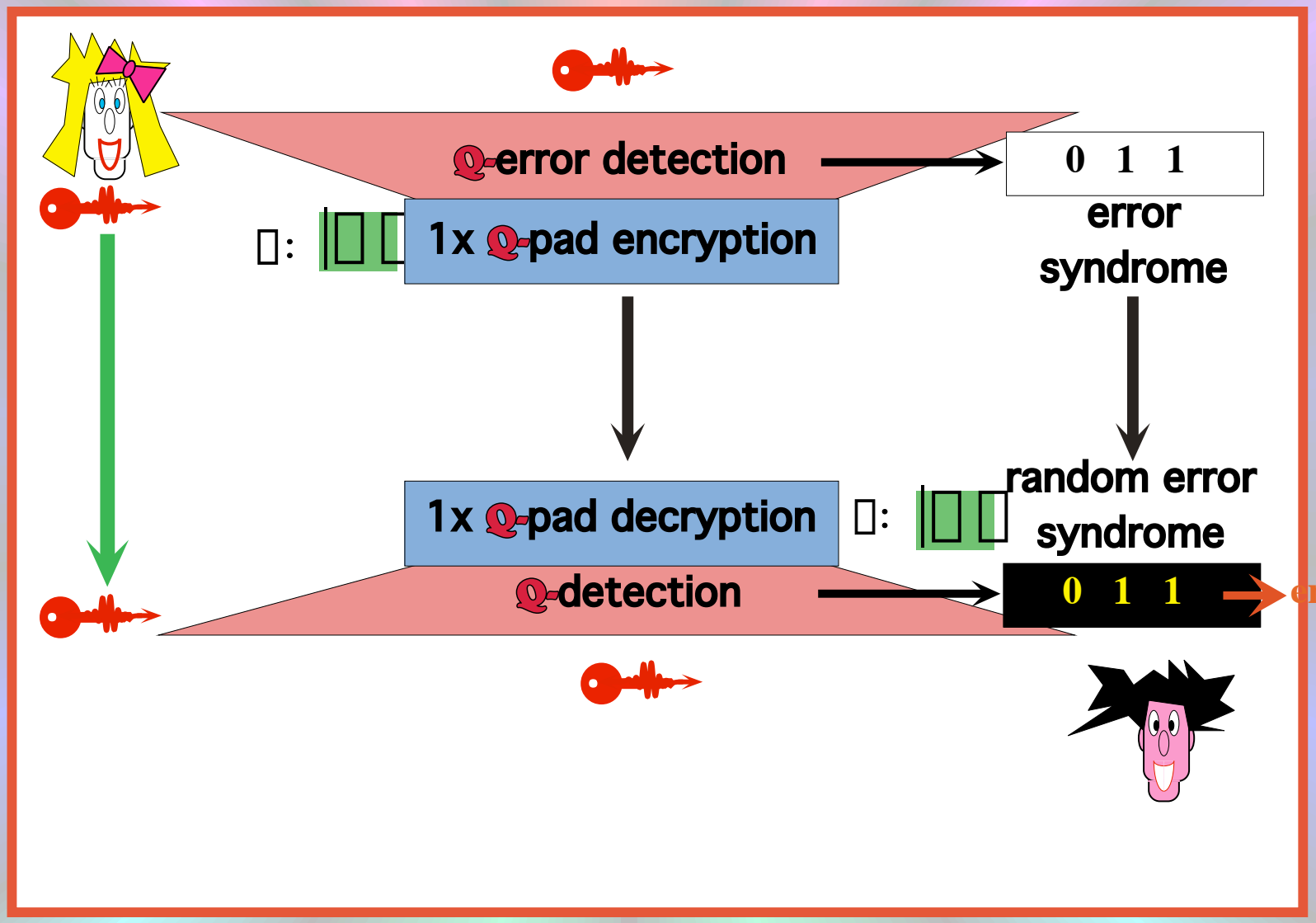
• Transmit quantum key (EPR states)

• Quantum error-correction is used to purify (or test purity of) EPR states to form a smaller pure set

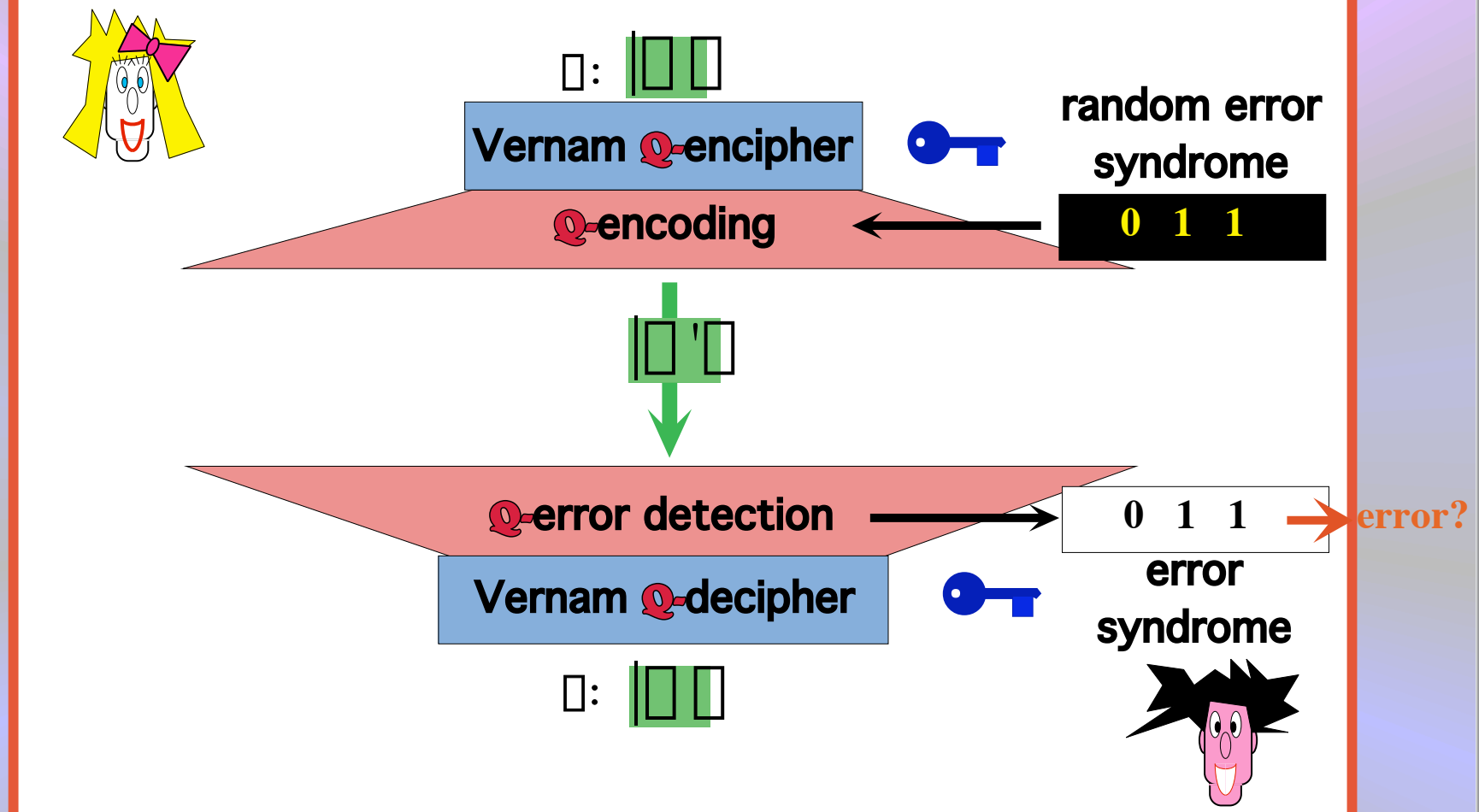
• one-time Authenticated Quantum pad is used to send message

. . . . .

(3.1.3C) One-time *interactive* Q-Authentication



(3.1.3C) One-time Q-Authentication



Barnum-Crépeau-Gottesman-Smith-Tapp

(3.1.3C) One-time Q-Authentication

. . . . .

• Quantum Vernam cipher message

• encode using Quantum error-correction with random syndrome

• Transmit result

. . . . .

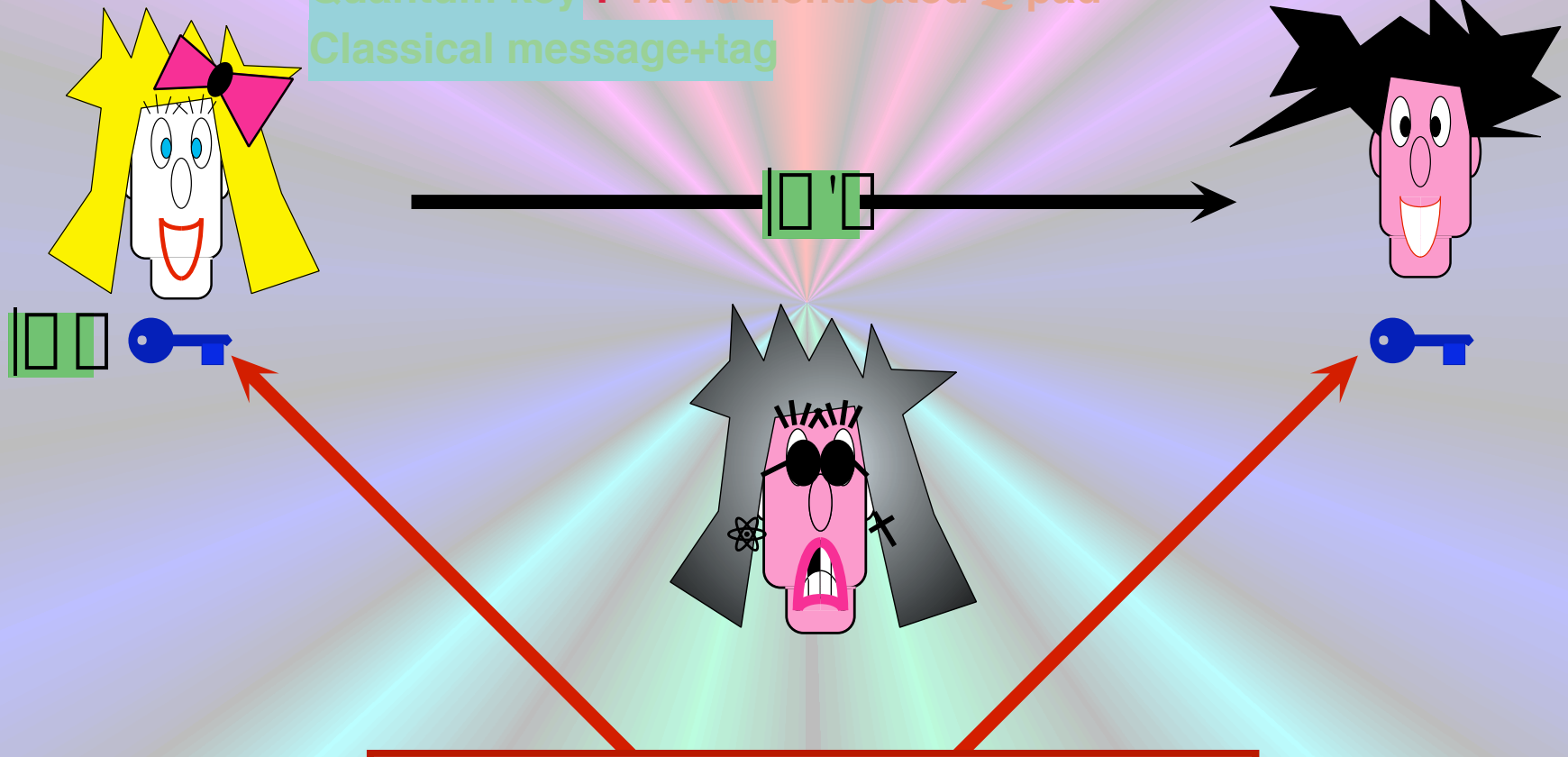
(3.1.3C) One-time Q-Authentication

Classical key : 1x Q-authentication

Quantum message+tag

Quantum key : 1x Authenticated Q-pad

Classical message+tag



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

Barnum-Crépeau-Gottesman-Smith-Tapp

one-time Q-authentication

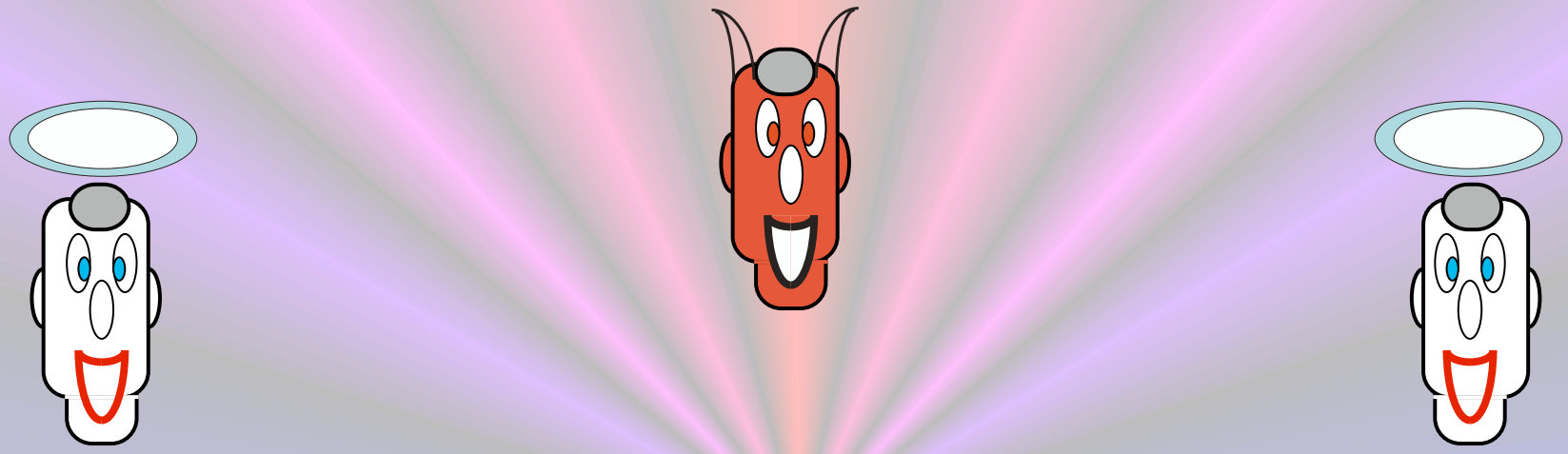
⟹

Vernam Q-cipher

(authenticated messages must be encrypted ;
this is false with classical messages!)

(3.2)
Complexity Theoretical Quantum Cryptography

(3.2) Complexity Theoretical Cryptography



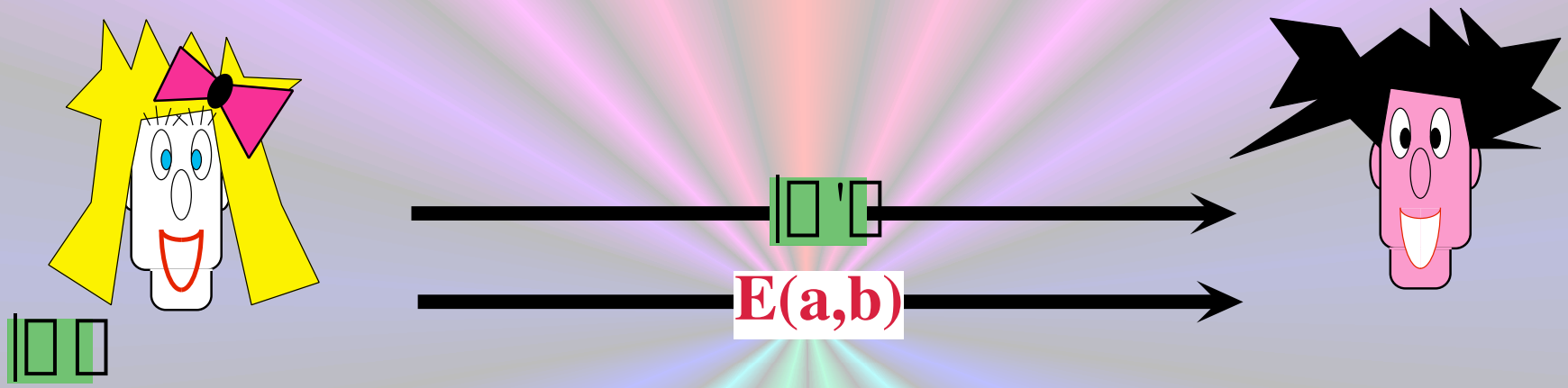
(3.2.1) Public key cryptosystem : public-key $\mathbb{Q}$-cryptosystem

(3.2.2) Digital signature scheme : public-key $\mathbb{Q}$-Authentication

$\mathbb{Q}$-digital signature scheme

(3.2.1) Public-Key Q-Cryptosystem

Assuming Classical Public Key Cryptography

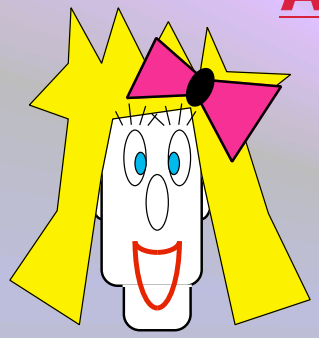


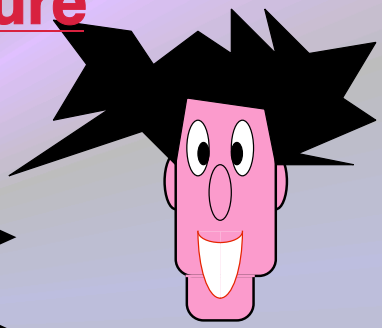
a,b random bits

(a,b) := D(E(a,b))

(3.2.2A) Public-Key Q-Authentication

Assuming Classical Public Key Cryptography
Assuming Classical Digital Signature





$|\Box'\Box$

Sign(E(k))

$|\Box\Box$

verify sign(E(k))
k := D(E(k))

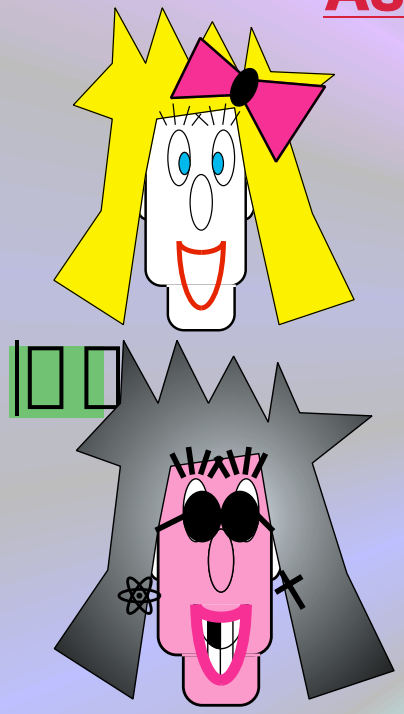
$k \Box_R K$

$|\Box'\Box := A_k(|\Box\Box)$

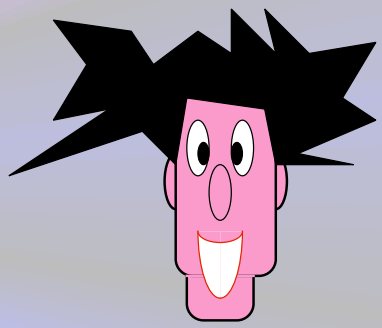
$|\Box\Box := A_k^{-1}(|\Box'\Box)$

(3.2.2S) Q-Digital Signature Scheme

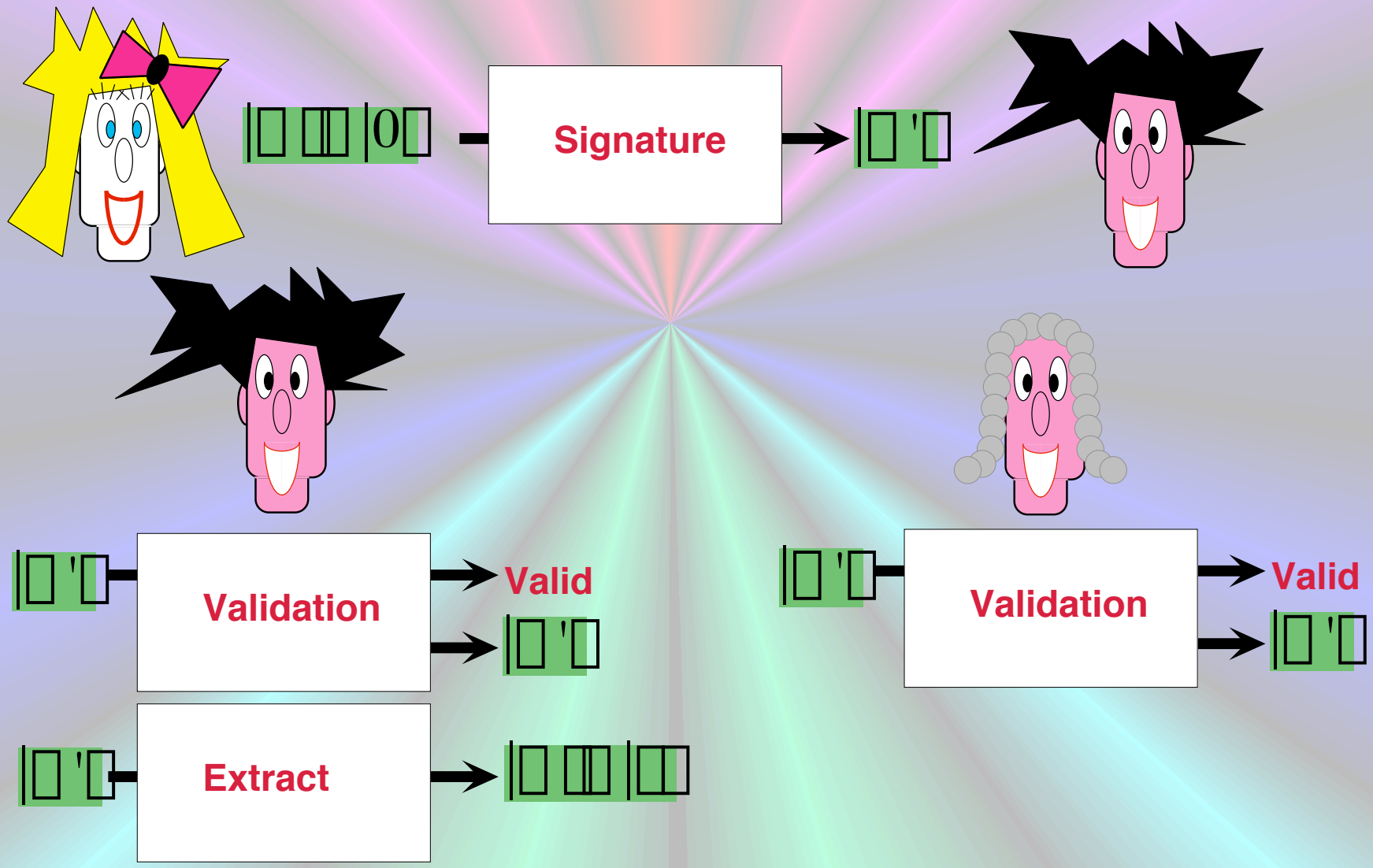
Assuming Classical Public Key Cryptography
Assuming Classical Digital Signature



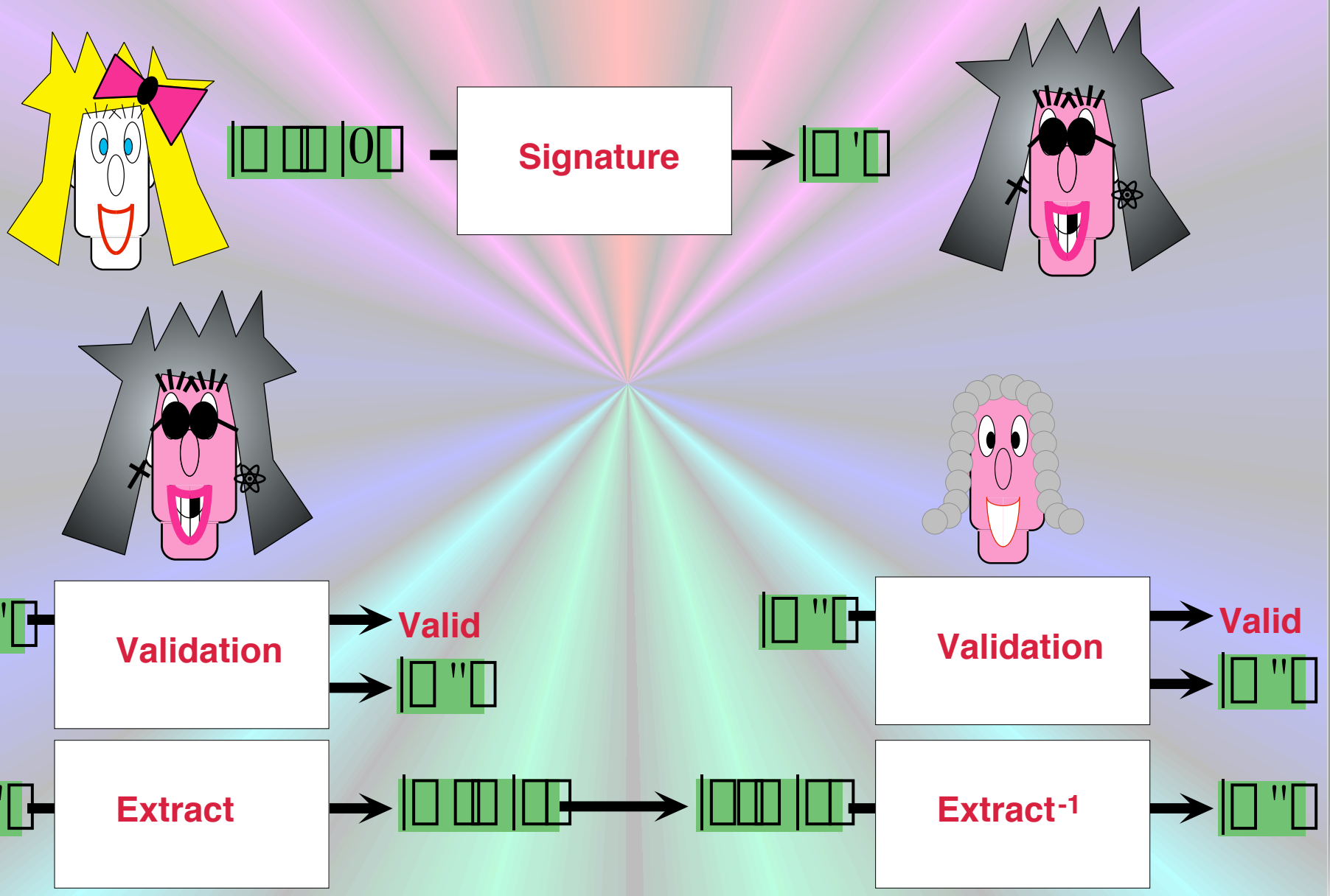
IMPOSSIBLE



(3.2.2S) Q-Digital Signature Scheme



(3.2.2S) Q-Digital Signature Scheme



Further Applications of one-time Q-Authentication

- Uncloneable Encryption
(Gottesman)

- Length n QECC correcting (n-1)/2 arbitrary errors
(with exponentially small probability)
(Crépeau,Gottesman,Smith)

- Achieving classical bounds for VQSS and MPQC
(Crépeau,Gottesman,Smith)

Quantum Authentication

Claude Crépeau

School of Computer Science
McGill University