Quantum one-time Authentication

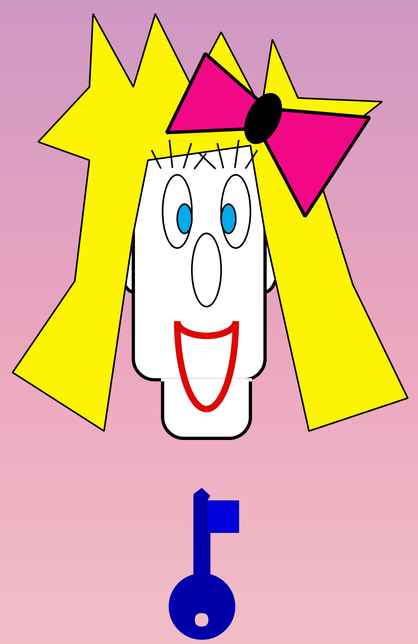
Claude Crépeau

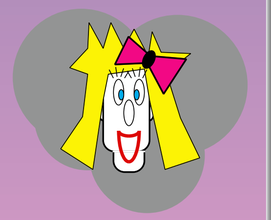
School of Computer Science
McGill University

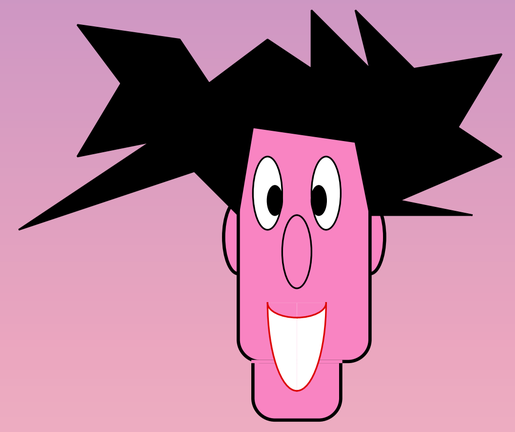
(1)

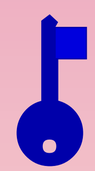
Classical Cryptography

(1.1.3) Authentication







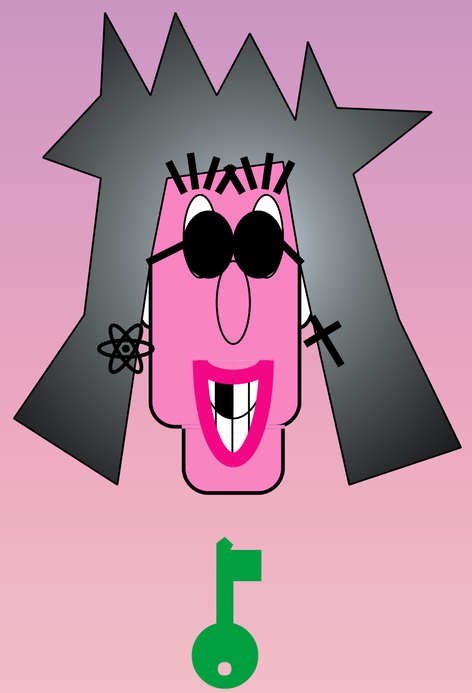


Will you marry me ?

Divorce your wife first !

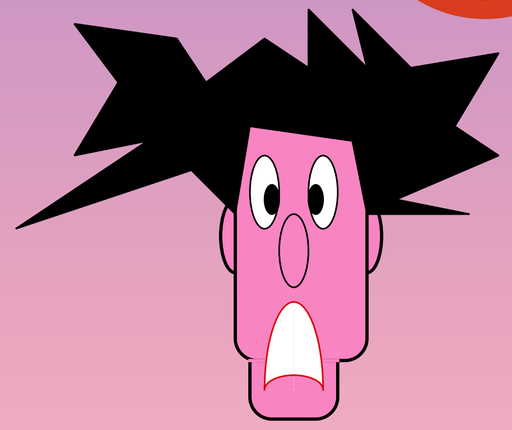
The papers are in the mail...

OK, I will !

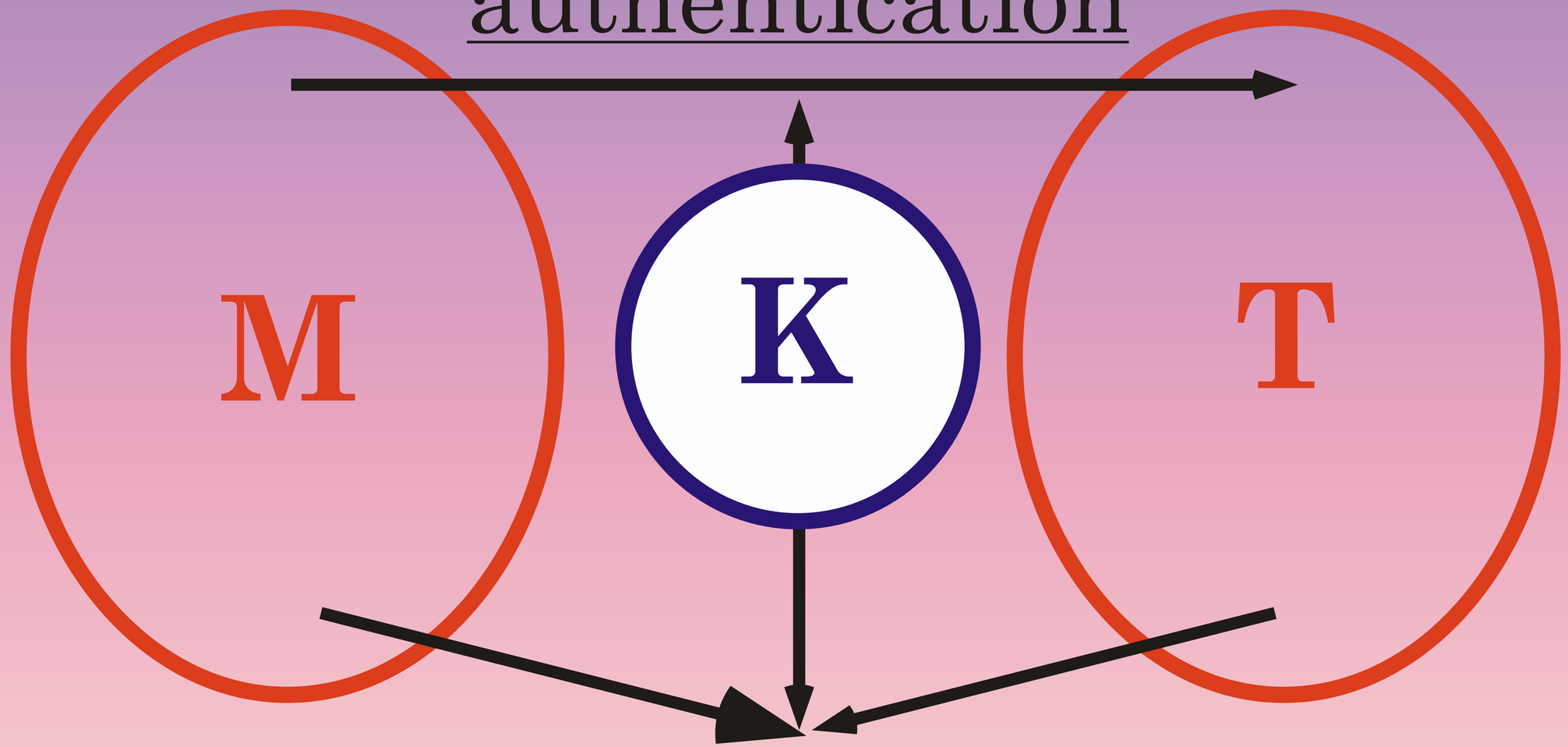


Will you marry me ?

No, I never will !

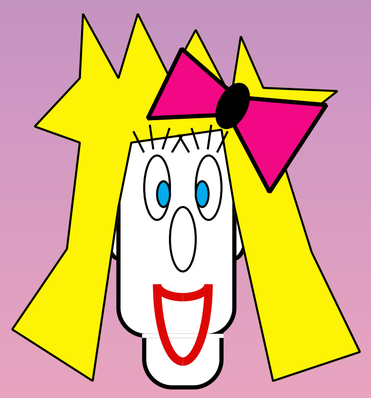


symmetric authentication

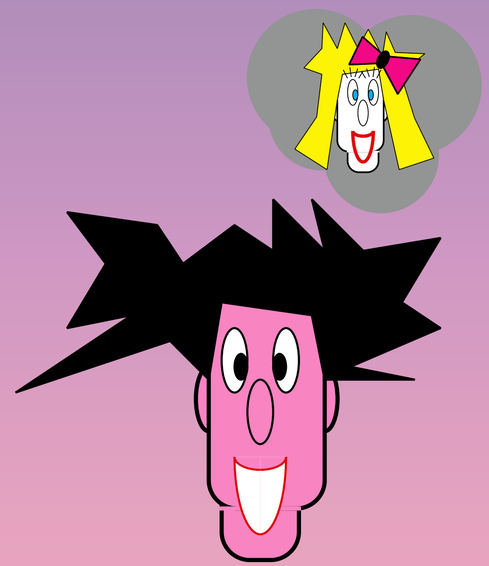


Information Theoretical Security

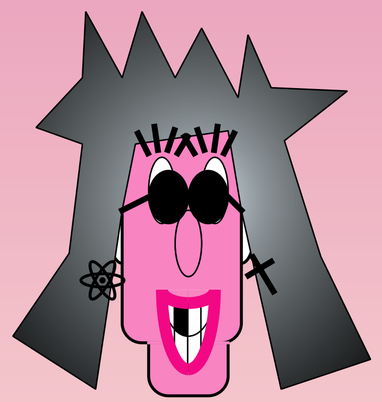
Authentication



(m,t)



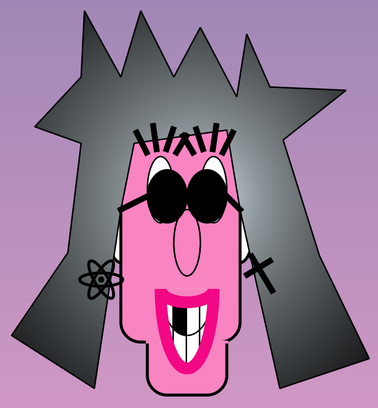
$t=auth_k(m)$



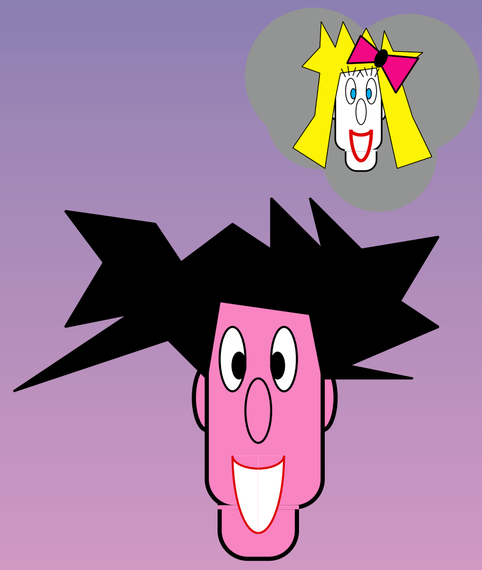
$auth_k(m)=t?$

Information Theoretical Security

Impersonation

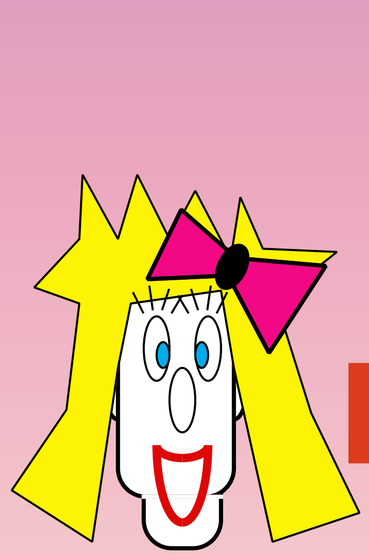


(m,t)



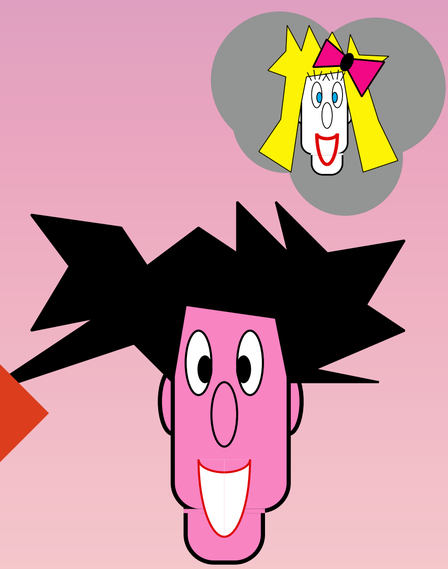
$auth_k(m)=t?$

Substitution



(m,t)

(m',t')



$auth_k(m')=t'?$

Information Theoretical Security

WC One-Time-Authentication

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

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

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

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

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

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

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

$$\mathrm{auth}_{\mathbf{M},b}(x) = \mathbf{M}x \,(+)\, b$$

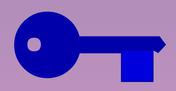
$[\mathbf{I}:\mathbf{M}]m(+)[0:b]=[m:t]$

G=$[\mathbf{I}:\mathbf{M}]$ (systematic) generating matrix of error correcting code

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

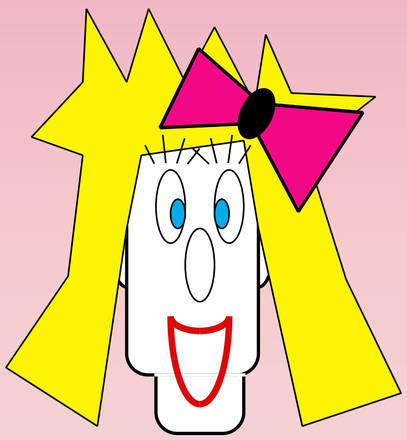
[m:t] systematic form of (message,tag)

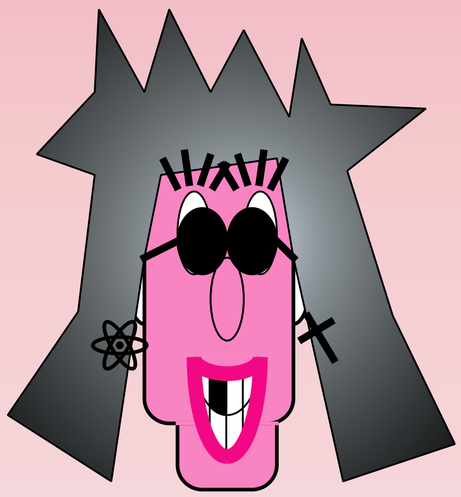
(3.1.3) One-time Q-Authentication

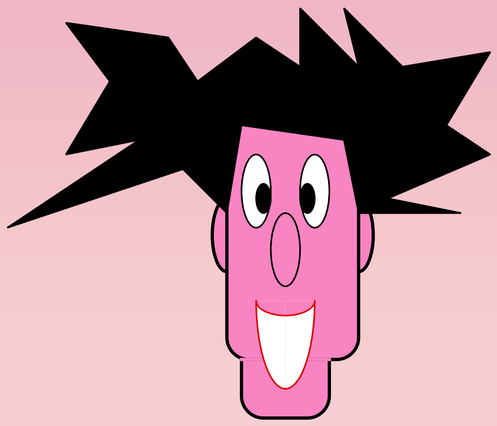


Classical key : Q-Authentication (BCGST)
Quantum message+tag

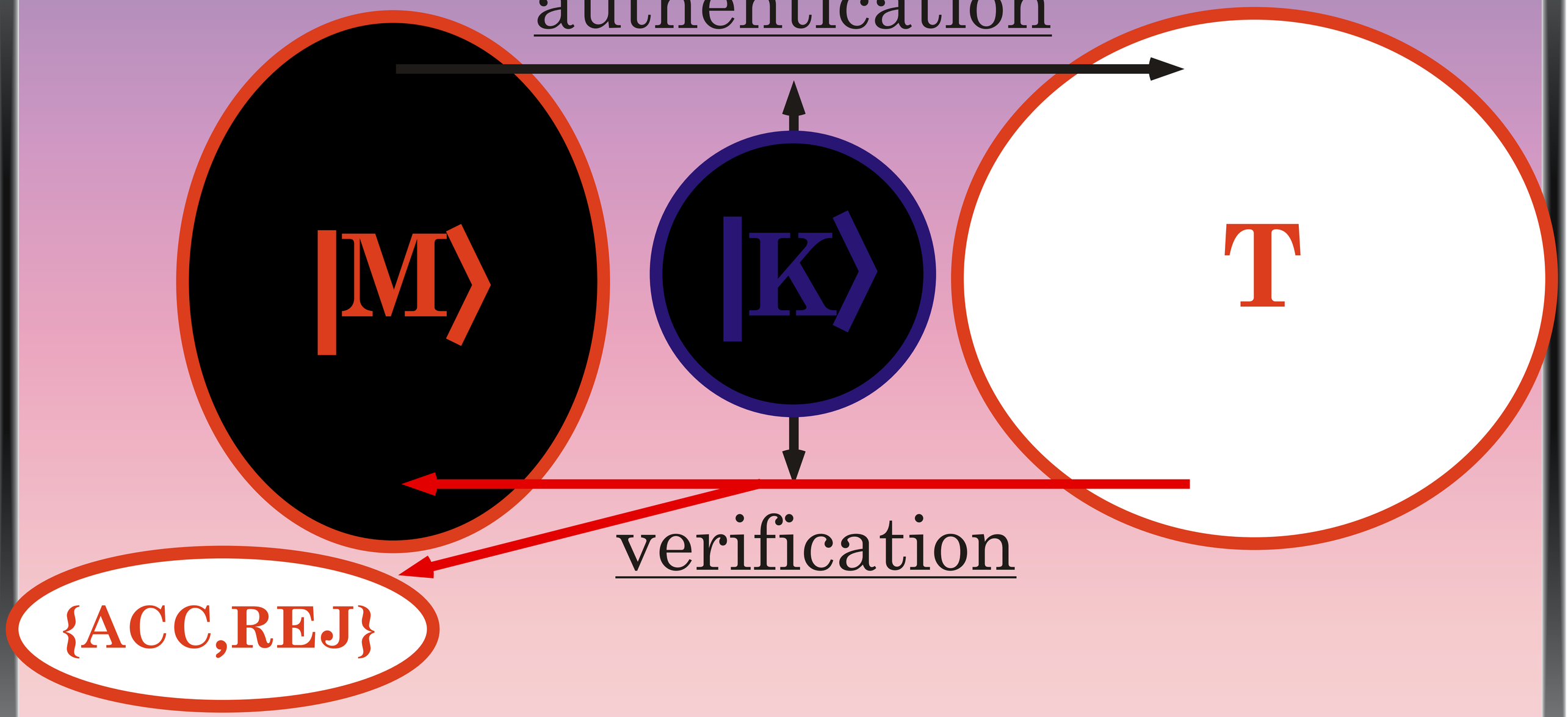
Quantum key : Authenticated Q-teleportation (BBCJPW)
Classical message+tag





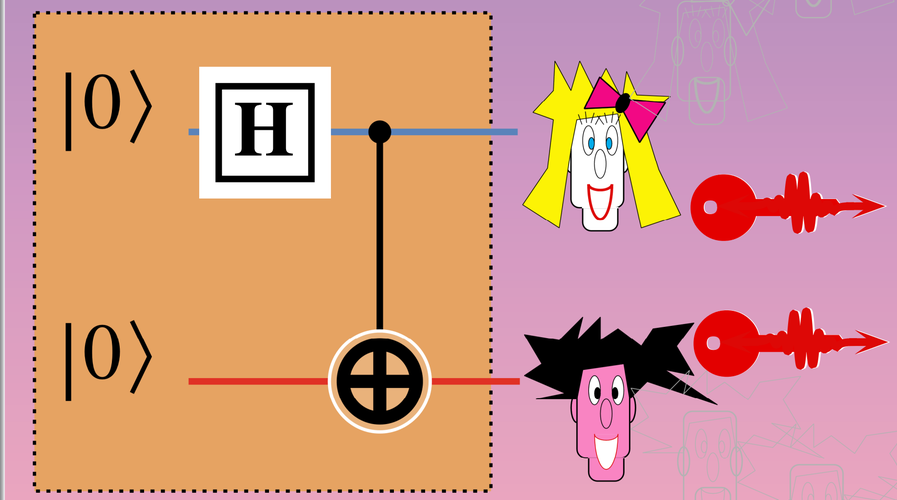


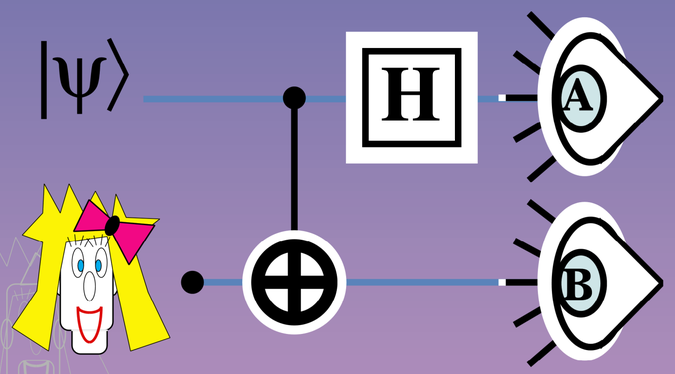
symmetric authentication

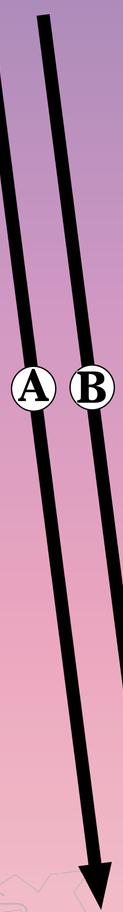


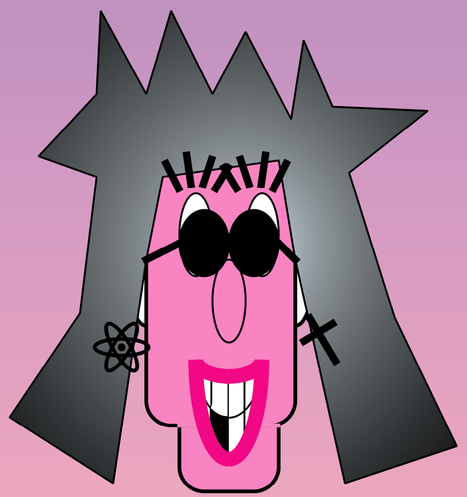
Information Theoretical Security

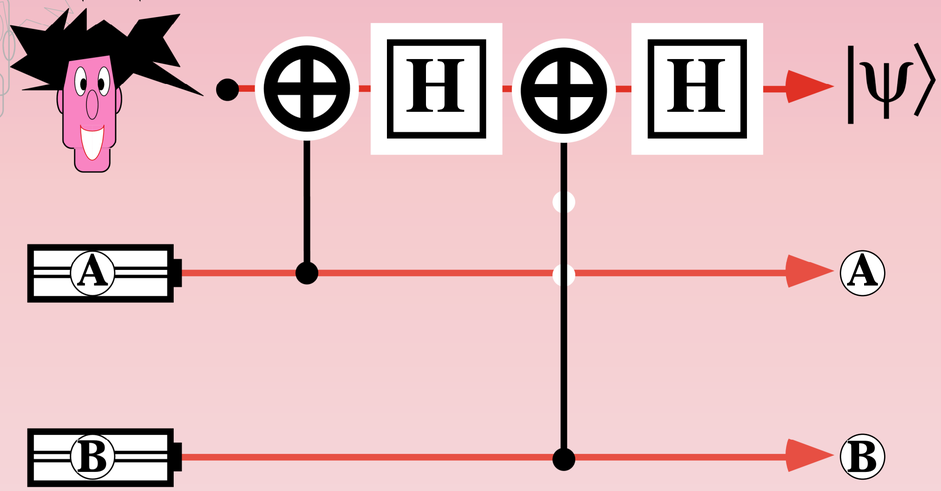
(3.1.3) One-time Q-Authentication



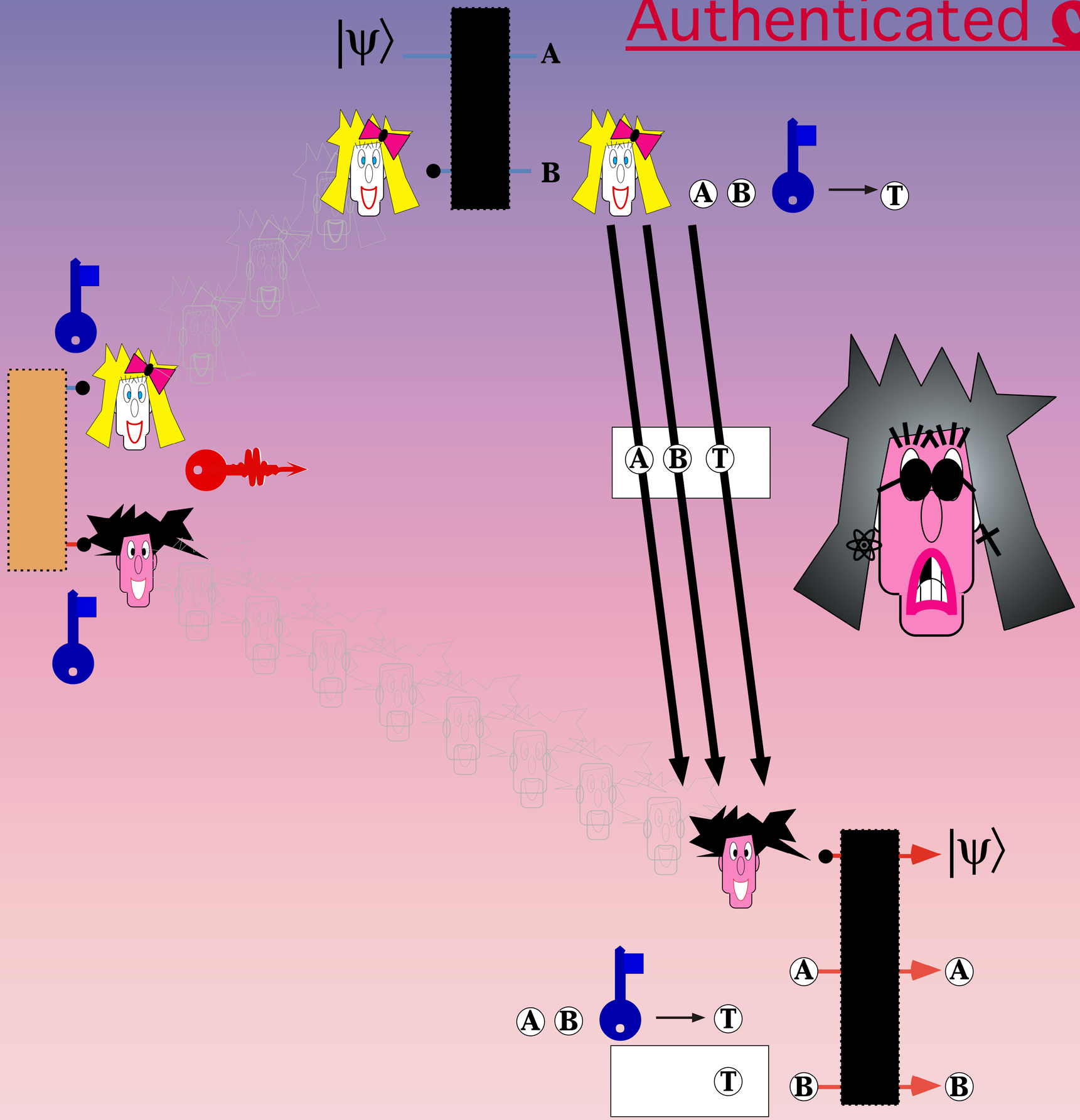




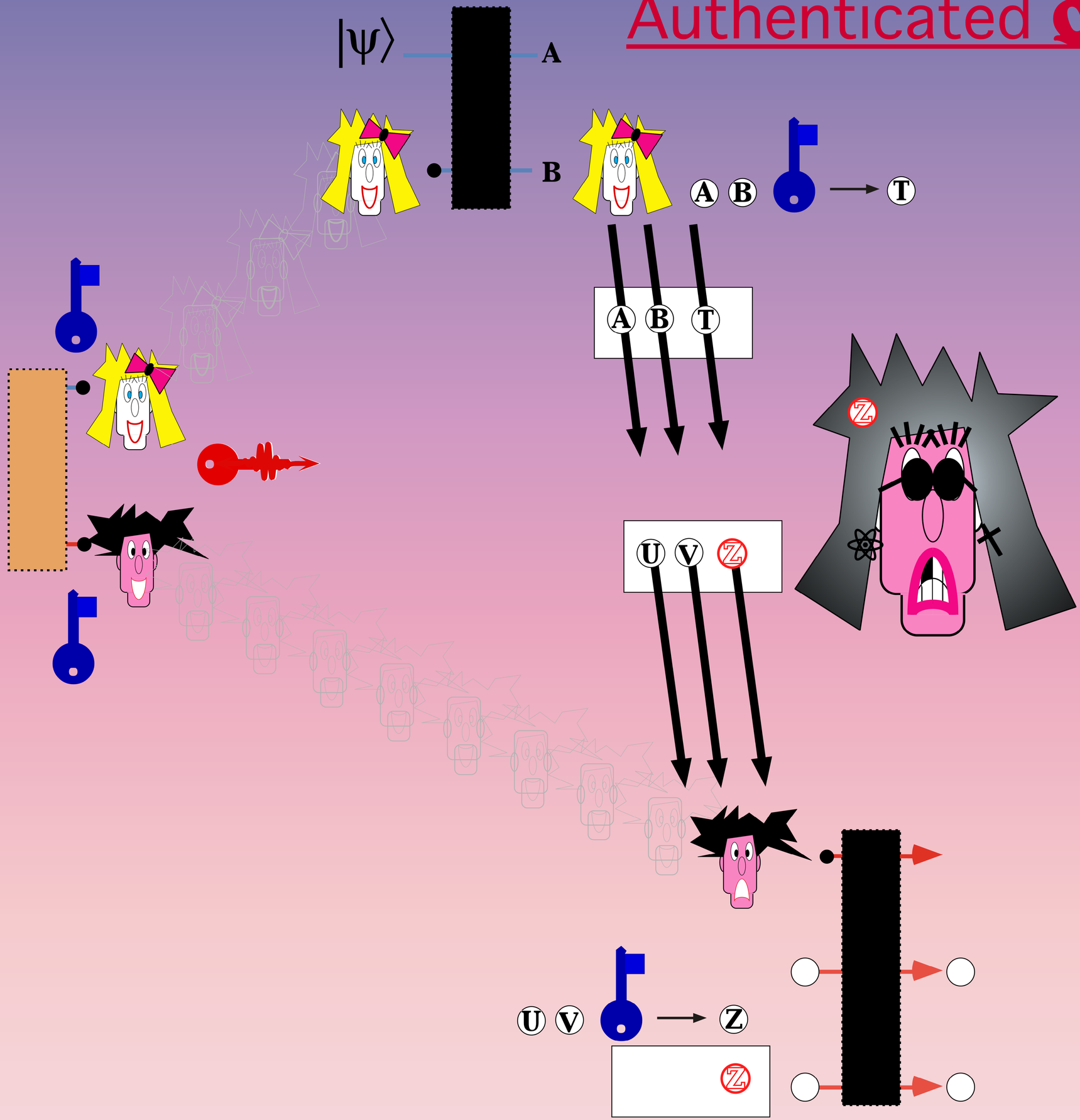




Authenticated Q-teleportation

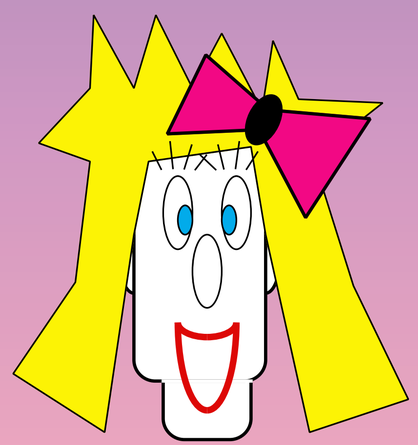


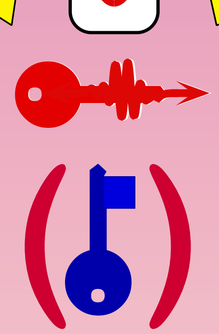
Authenticated Q-teleportation



(3.1.3b) One-time Q-Authentication

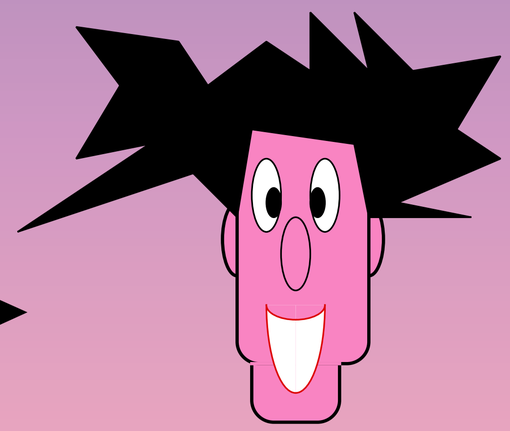
Quantum key : 1x Authenticated Q-pad
Classical message+tag

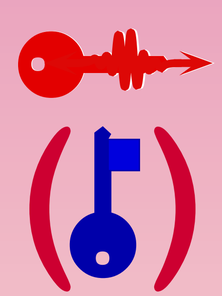


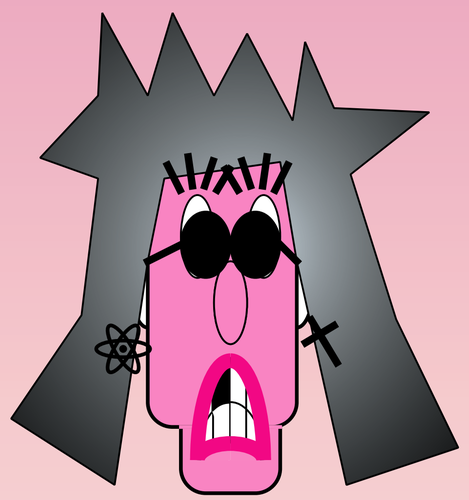


Ⓐ Ⓑ Ⓣ

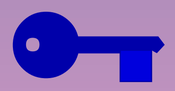
two authenticated random bits





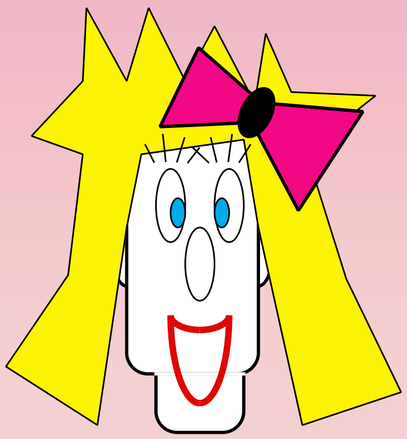


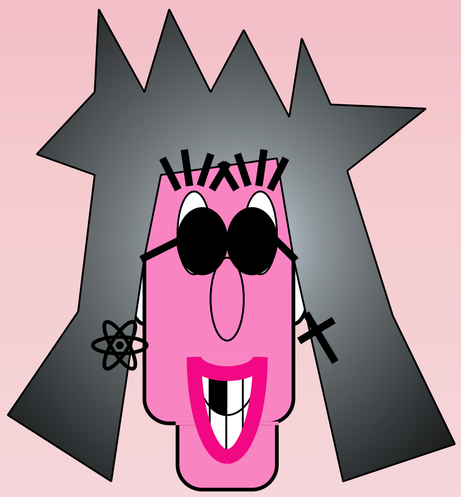
(3.1.3a) One-time Q-Authentication

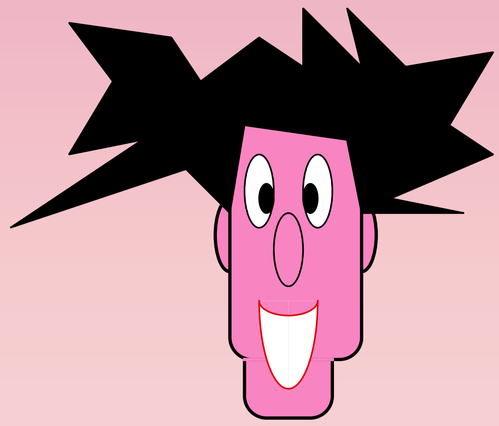


Classical key : Q-Authentication (BCGST)
Quantum message+tag

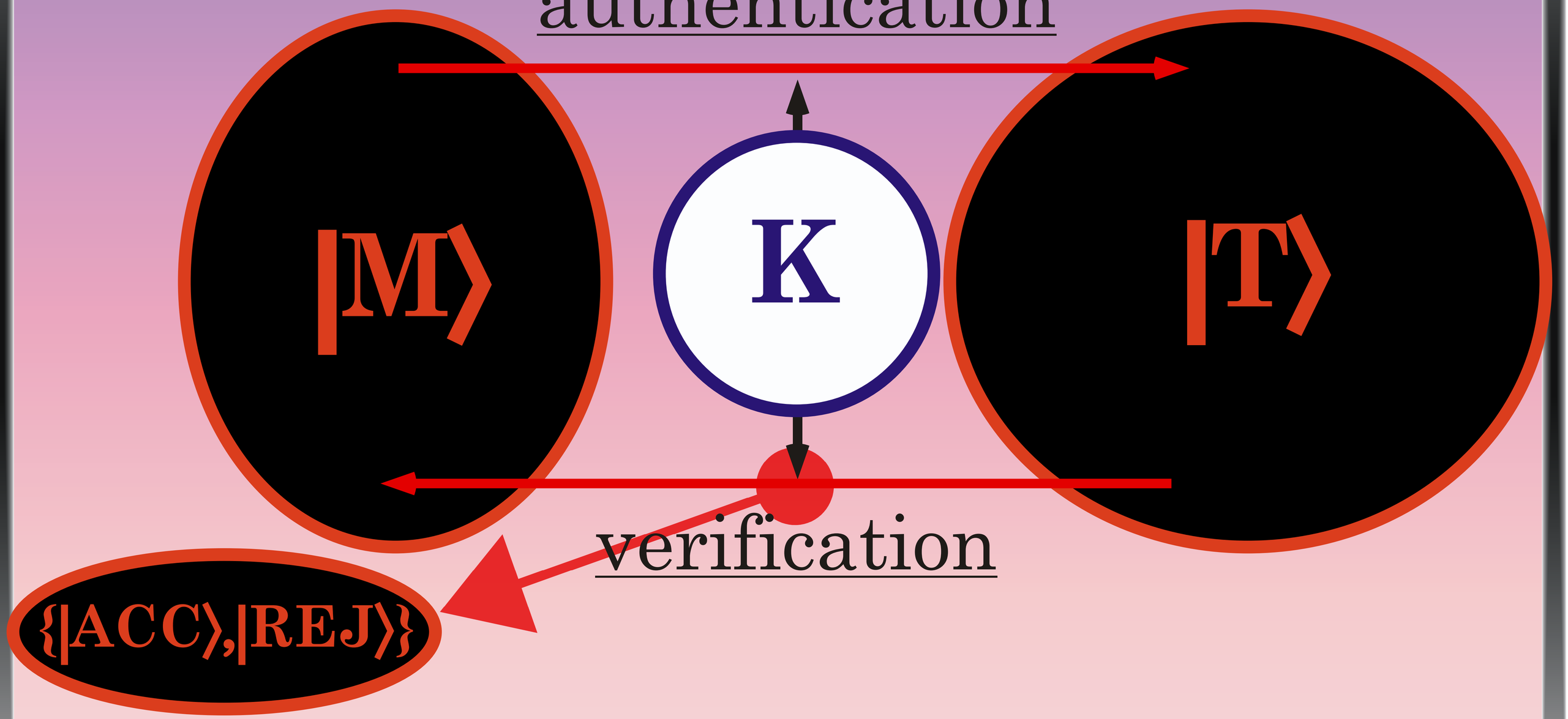
Quantum key : Authenticated Q-teleportation
Classical message+tag (BBCJPW)







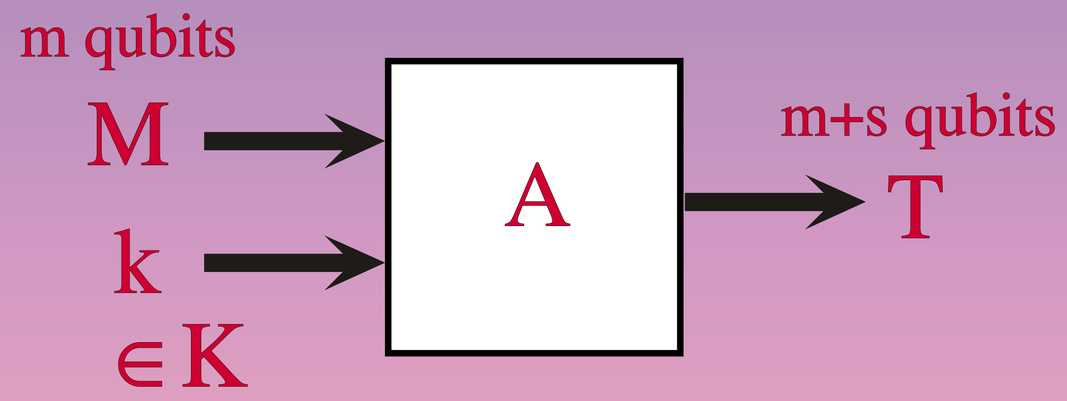
symmetric authentication of Quantum Messages



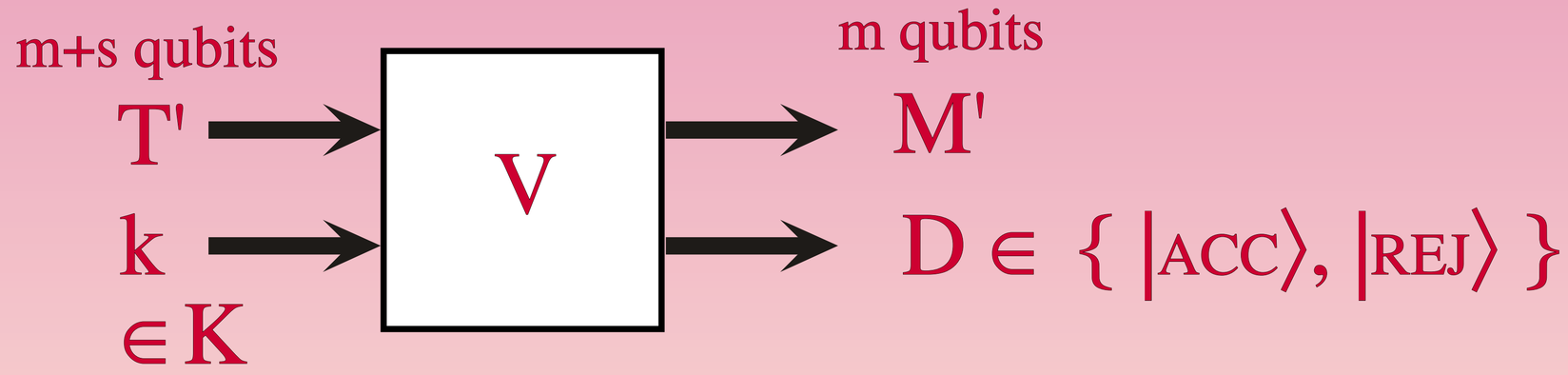
Information Theoretical Security

One-time Ω-Authentication

Authentication:



Verification:



One-time Ω-Authentication

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

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

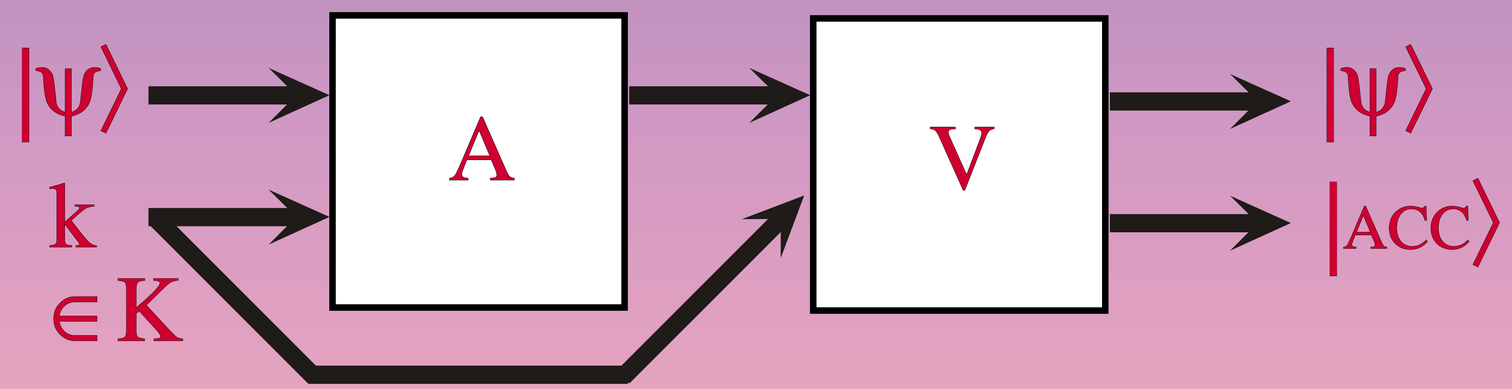
The corresponding projectors are

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

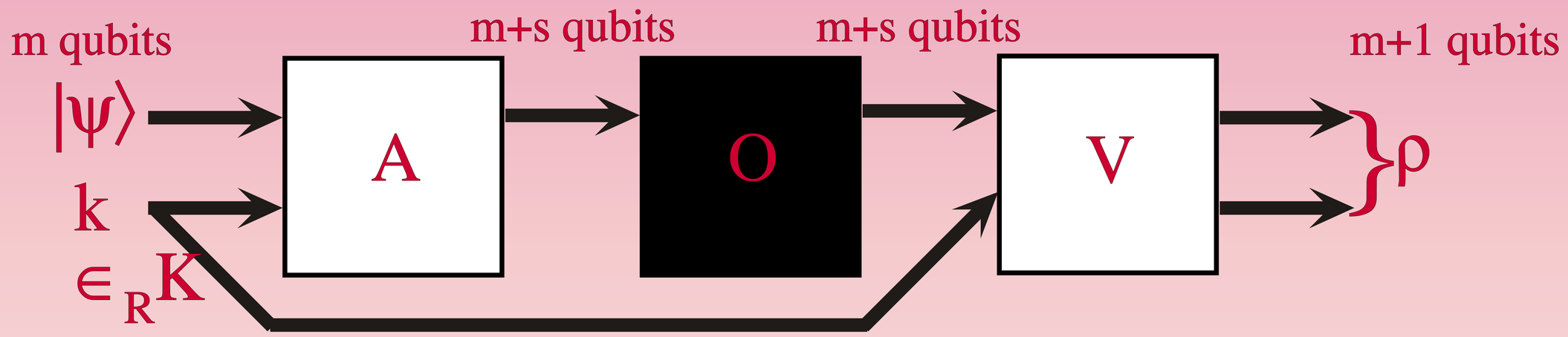
$$W_\psi = (I_{M'} - |\psi\rangle\langle\psi|) \otimes |ACC\rangle\langle ACC|$$

One-time Ω-Authentication

Completeness:

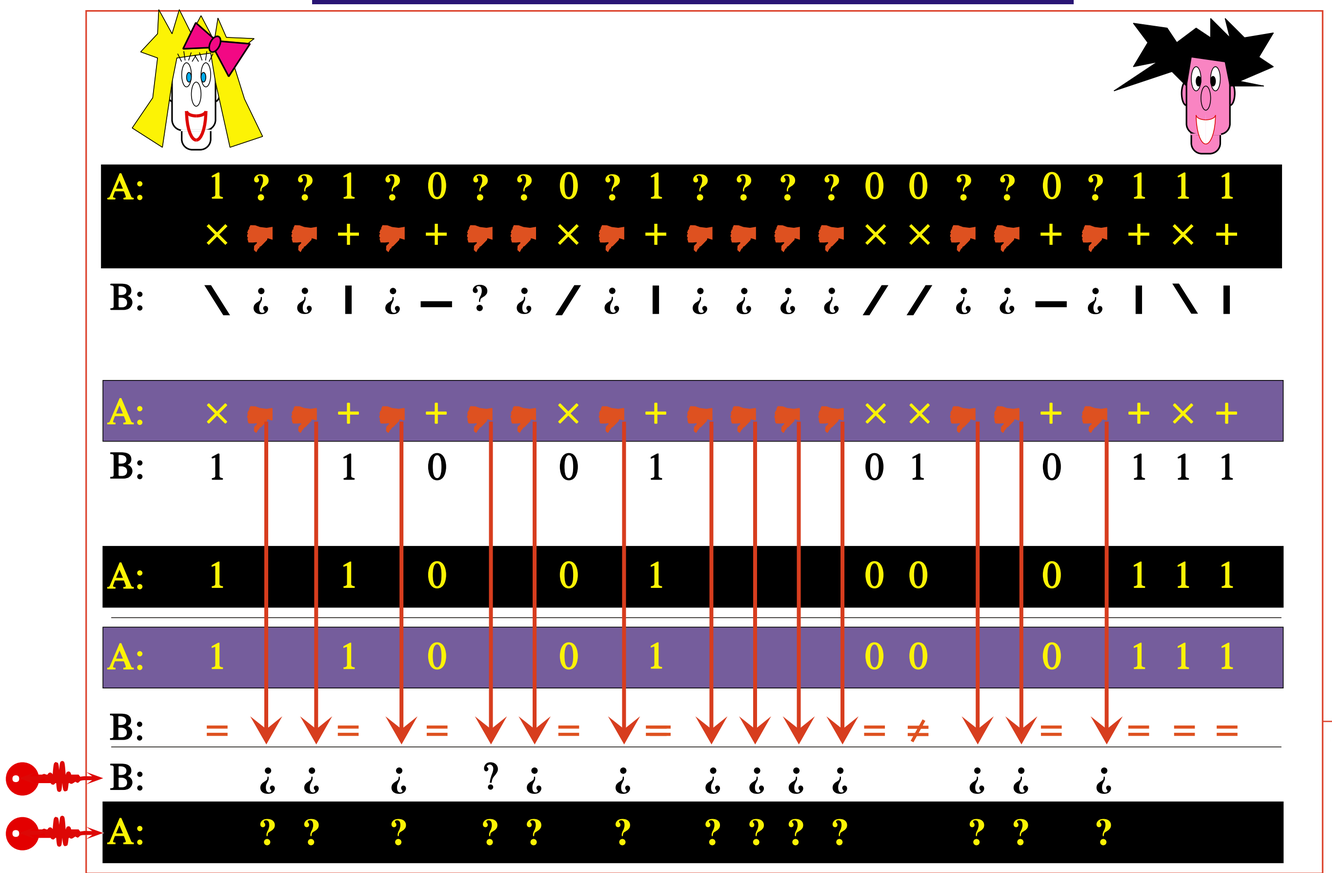


Soundness:



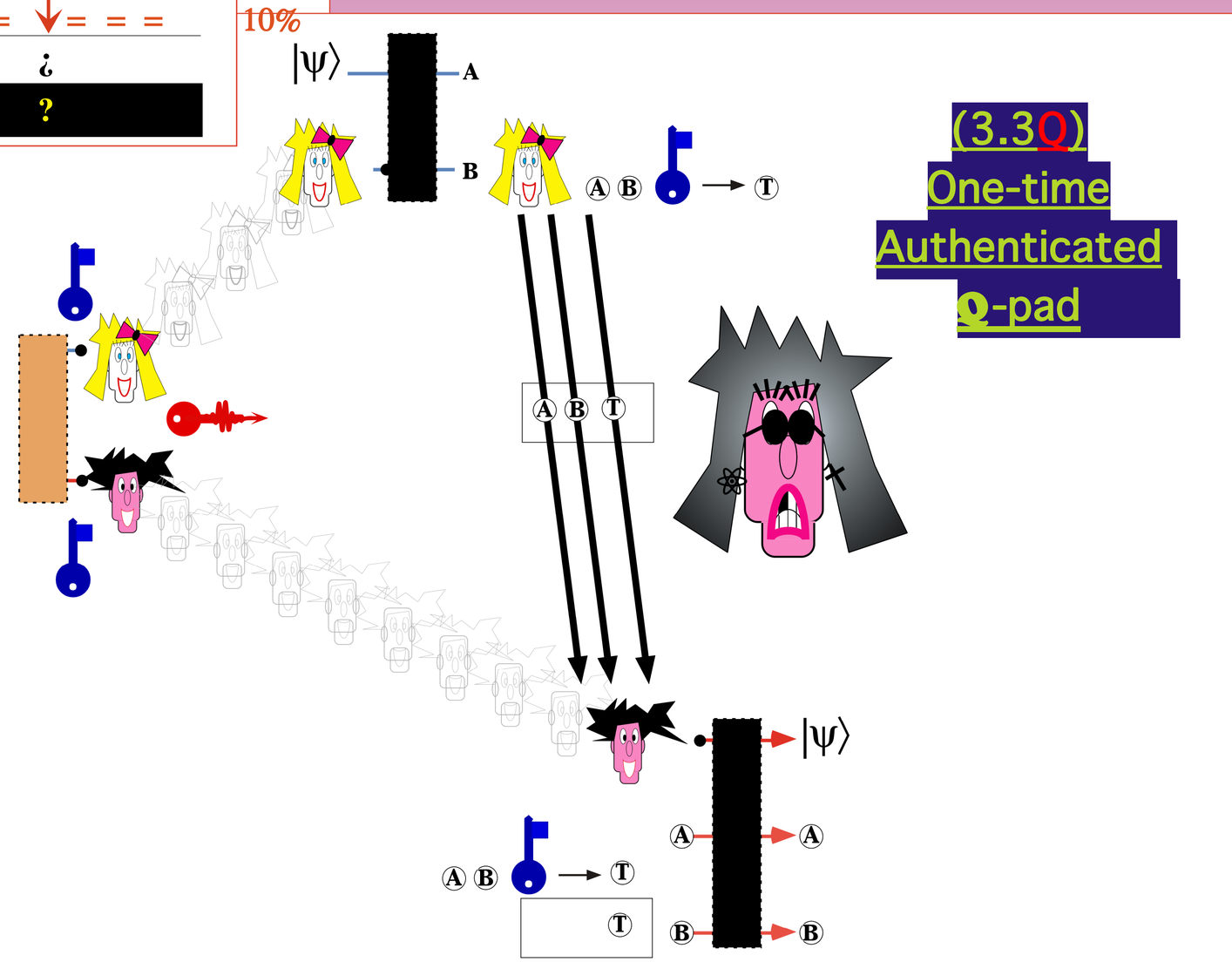
$$\forall|\psi\rangle \; Tr(R_\psi \rho) \geq 1-2^{-\Omega(s)}$$

(3.1Q) Quantum-Key distribution



Shor-Preskill

10%



(3.3Q) One-time Authenticated Q-pad

(3.3C) One-time interactive Q-Authentication

.....

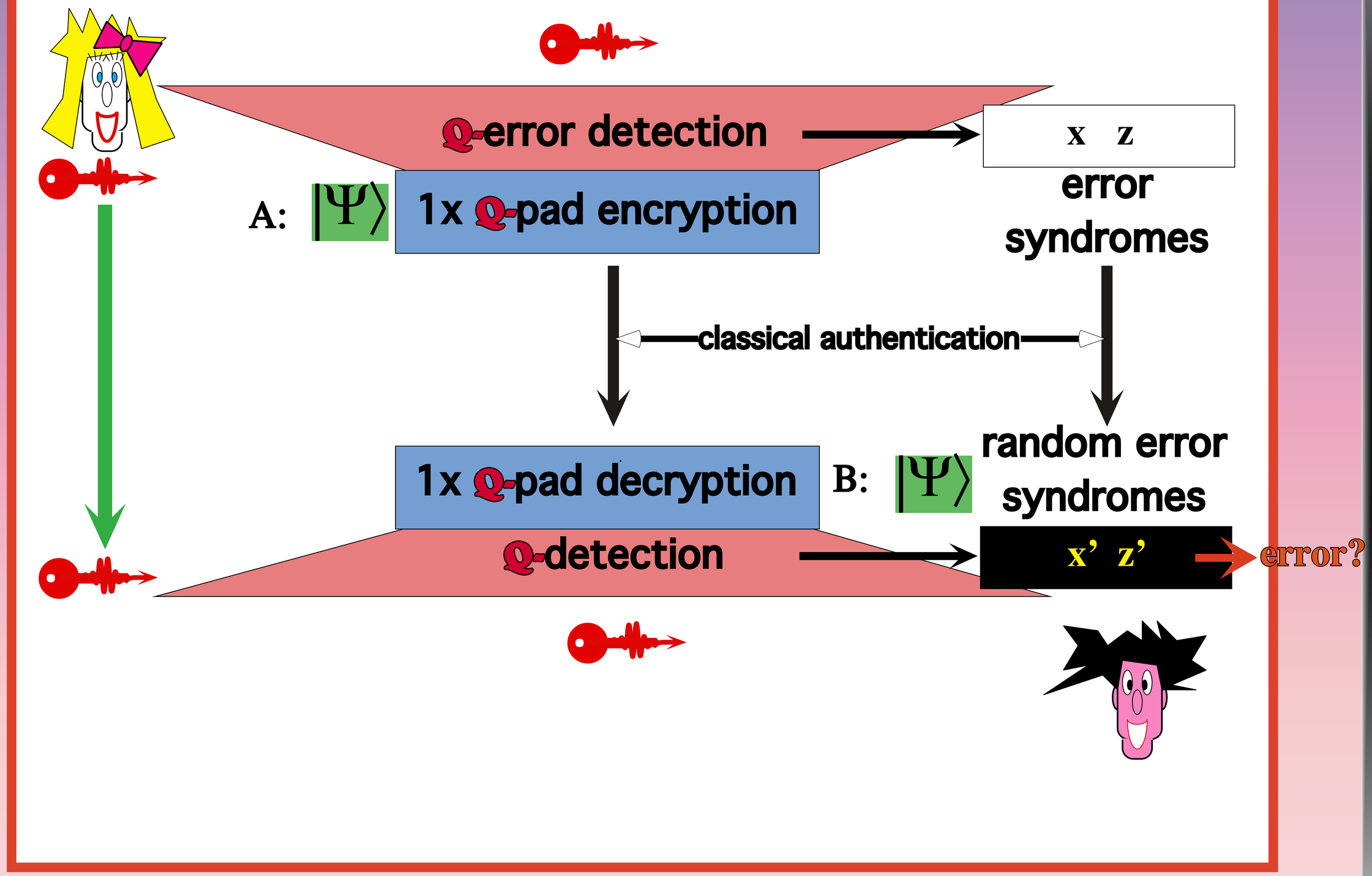
- Transmit quantum key (EPR states)

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

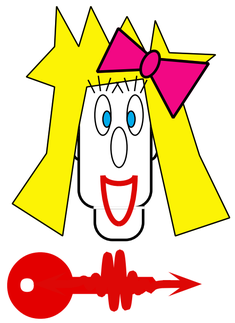
- one-time Authenticated Quantum pad is used to send message

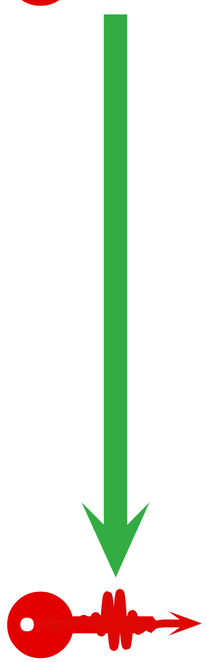
.....

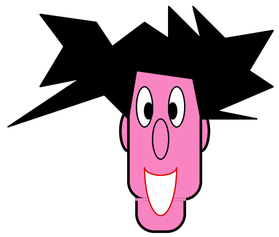
(3.3C) One-time interactive Q-Authentication



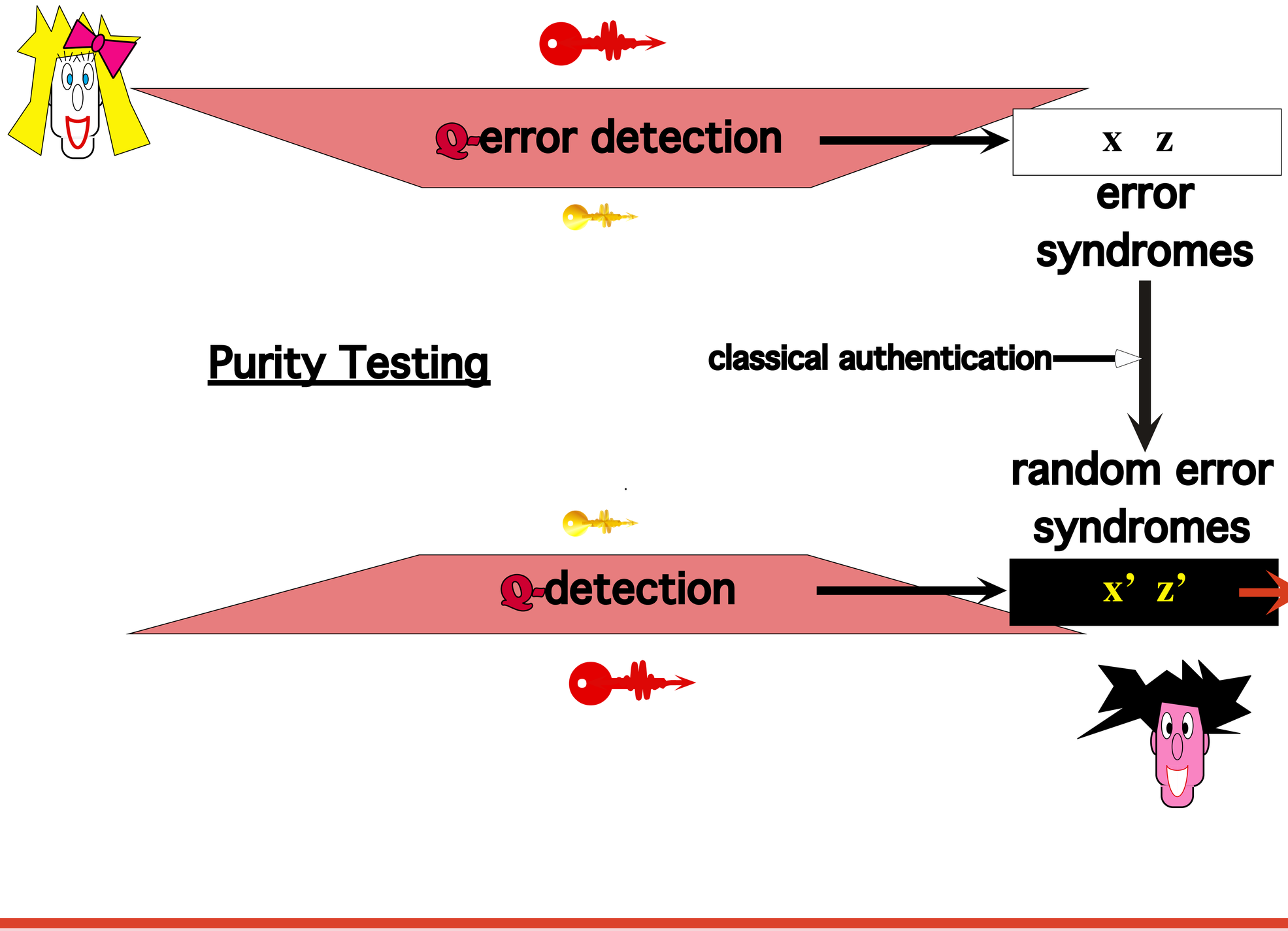
(3.3C) One-time interactive Q-Authentication



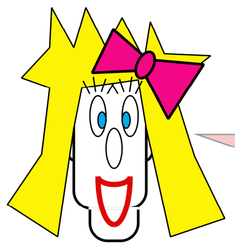




(3.3C) One-time interactive Q-Authentication



(3.3C) One-time interactive Q-Authentication

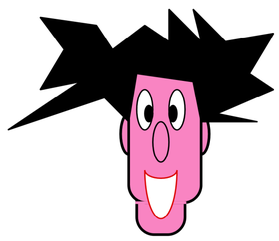


A: $|\Psi\rangle$ 1x Q-pad encryption

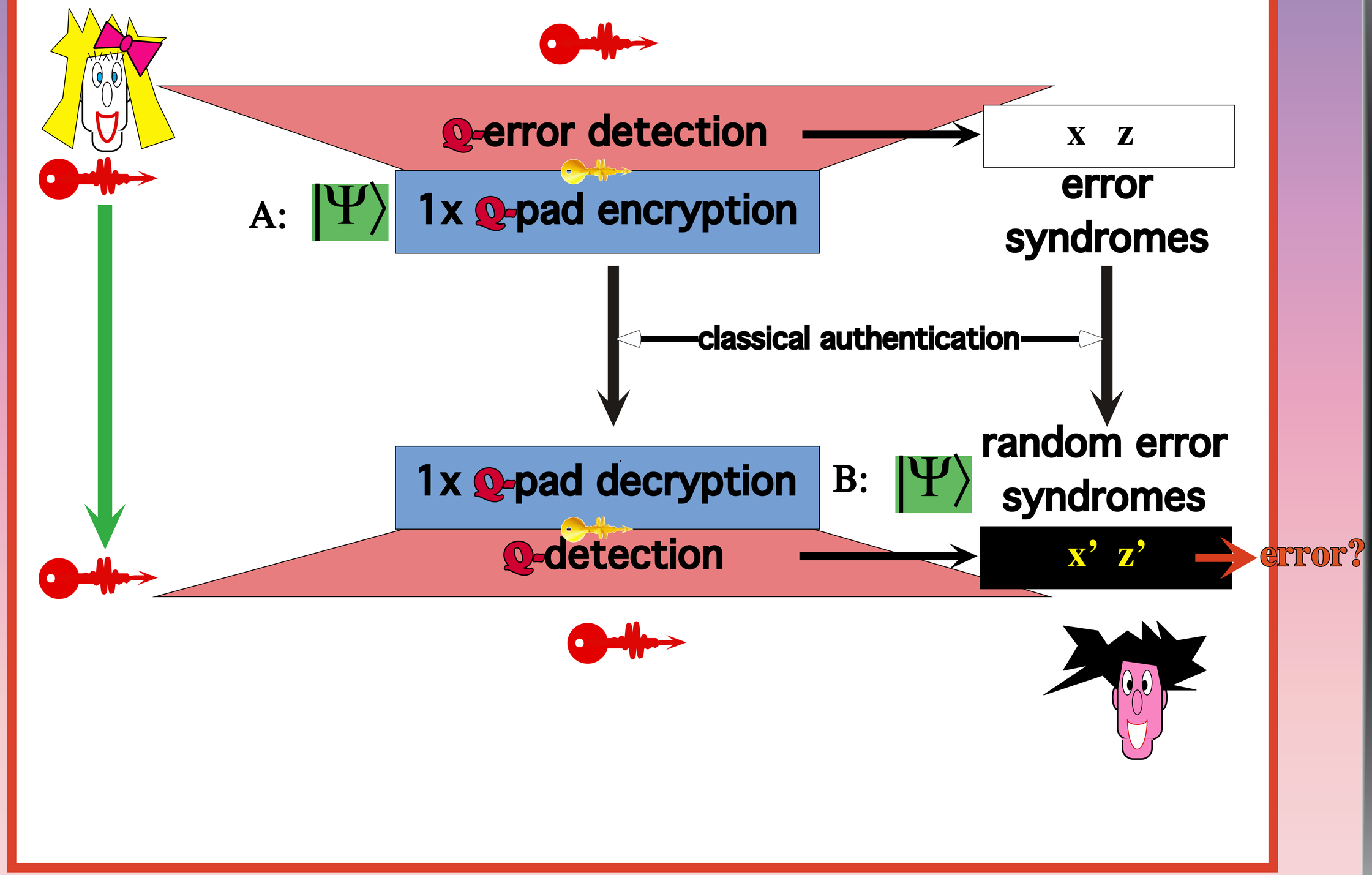
teleportation

classical authentication

1x Q-pad decryption B: $|\Psi\rangle$



(3.3C) One-time interactive Q-Authentication



(3.3C) One-time interactive Q-Authentication

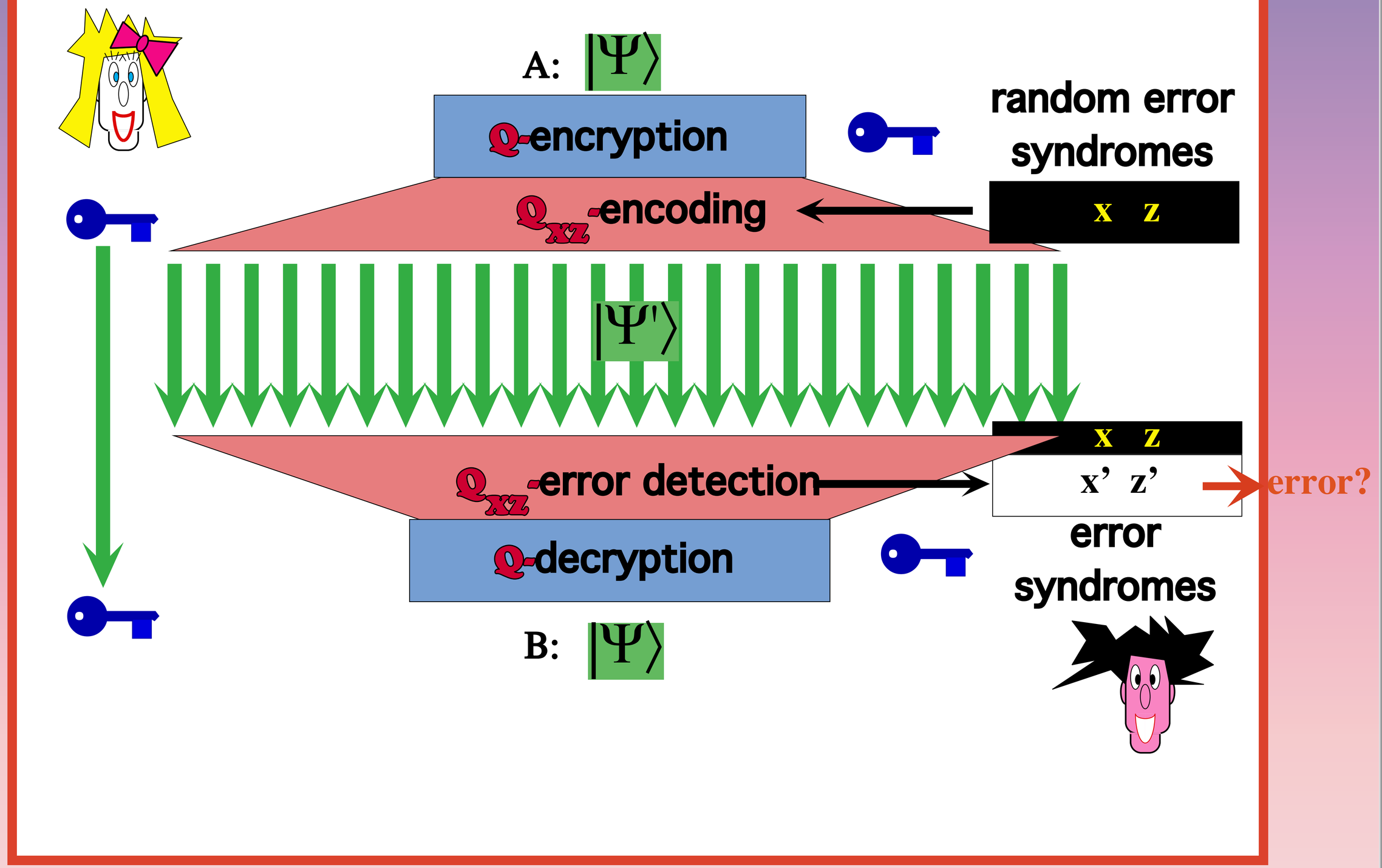
. . . . .

- Replace One-time Q-pad by Vernam Q-cipher

- Replace Entanglement Purity Testing by Quantum Error-Correction

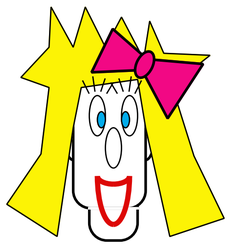
. . . . .

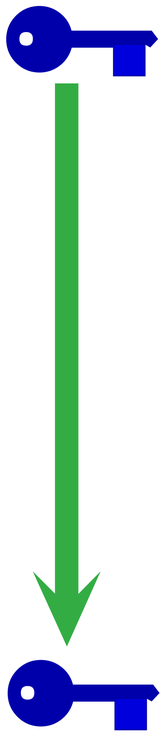
(3.1.3a) One-time Q-Authentication

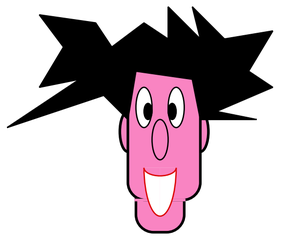


Barnum-Crépeau-Gottesman-Smith-Tapp

(3.1.3a) One-time Q-Authentication

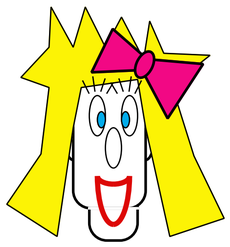






Barnum-Crépeau-Gottesman-Smith-Tapp

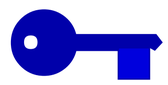
(3.1.3a) One-time Q-Authentication



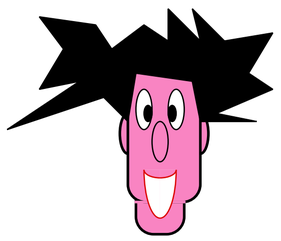
A: $|\Psi\rangle$

Q-encryption

Q-decryption

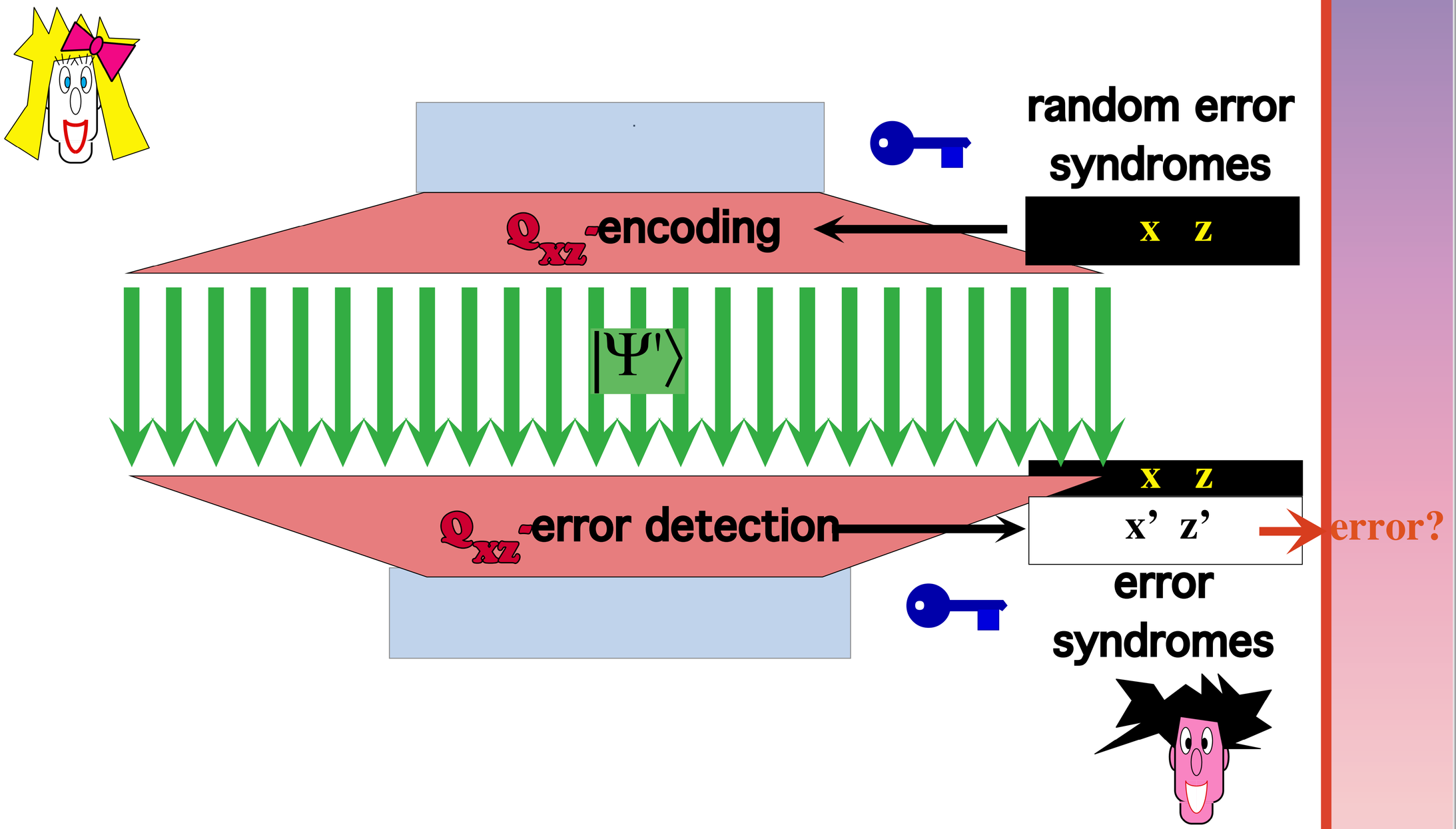


B: $|\Psi\rangle$



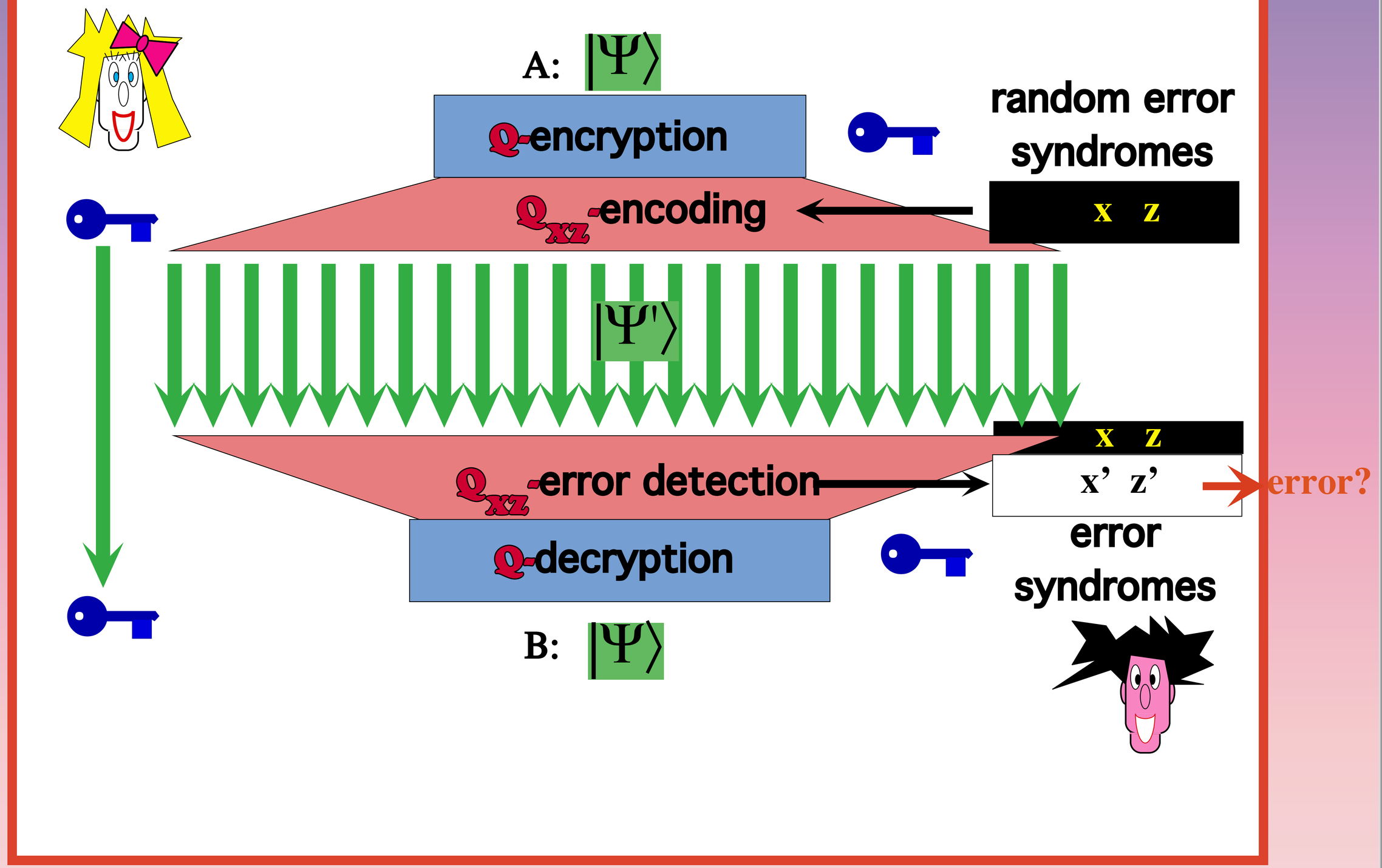
Barnum-Crépeau-Gottesman-Smith-Tapp

(3.1.3a) One-time Q-Authentication



Barnum-Crépeau-Gottesman-Smith-Tapp

(3.1.3a) One-time Q-Authentication



Barnum-Crépeau-Gottesman-Smith-Tapp

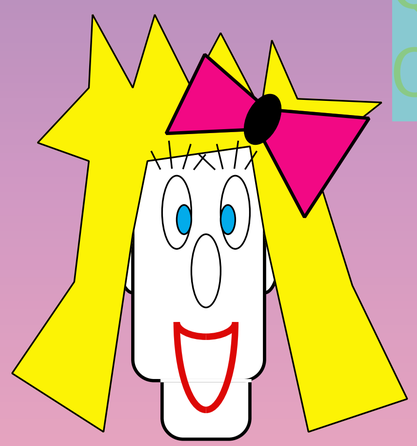
(3.1.3a) One-time Q-Authentication

Classical key : one-time Q-authentication

Quantum message+tag

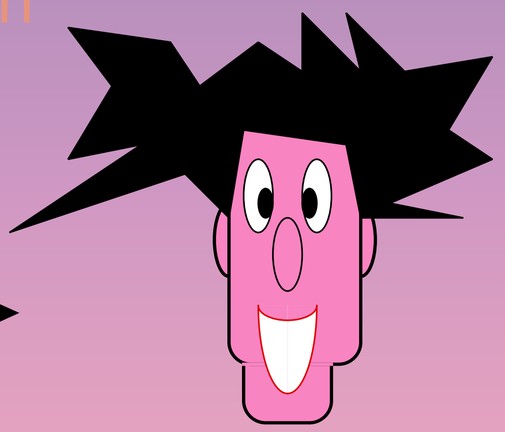
Quantum key : Authenticated Q-teleportation

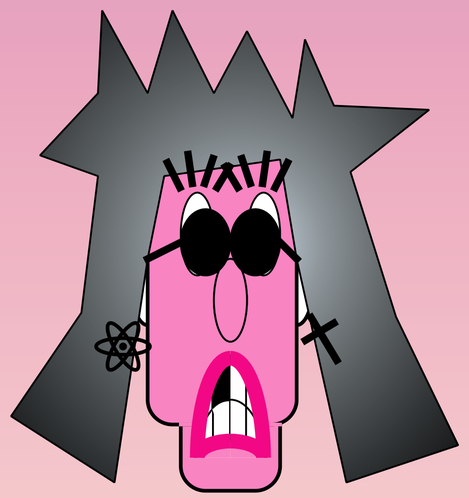
Classical message+tag



$|\Psi\rangle$

$|\Psi'\rangle$





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

Barnum-Crépeau-Gottesman-Smith-Tapp

one-time Q-authentication

-->

Vernam Q-cipher

(authenticated quantum messages must be encrypted
which is false for classical messages!)

Main Lower Bound

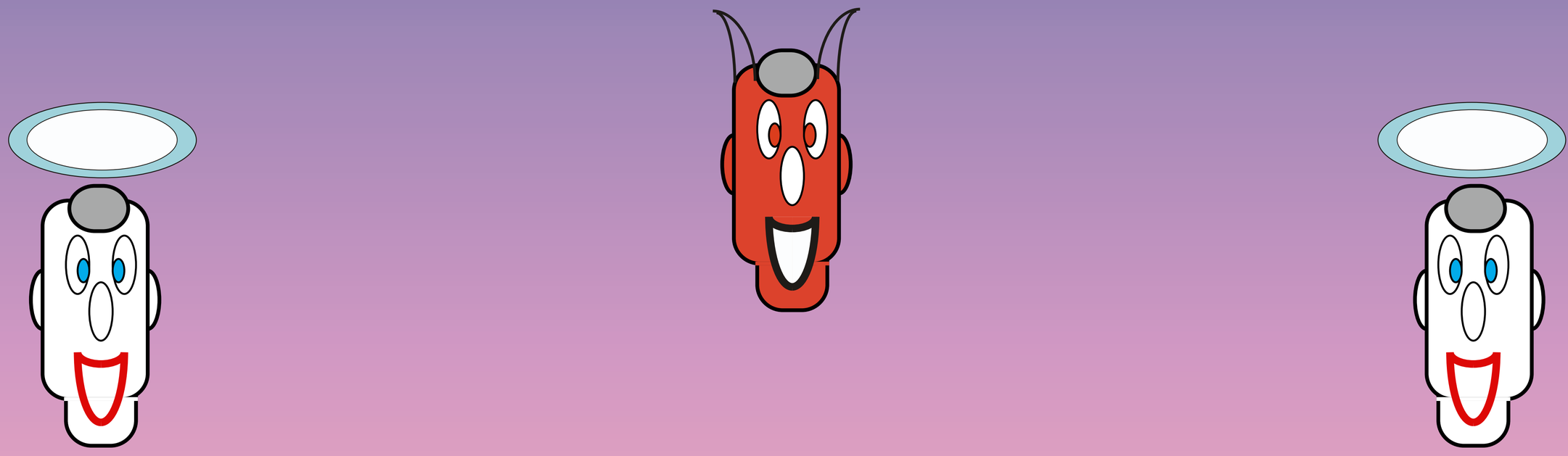
A Quantum Authentication Scheme with error probability ε

is

A Quantum Encryption Scheme with error probability $4\varepsilon^{1/6}$.

(3.2)
Complexity Theoretical Quantum Cryptography

(3.2) Complexity Theoretical Cryptography



. . . . .

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

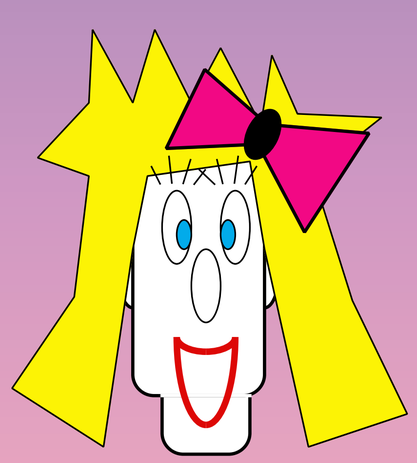
(3.2.2) Digital signature scheme : public-key **Q**-Authentication
Q-digital signature scheme

(3.2.3) (trapdoor) one-way functions : **Q**-cryptanalysis
(trapdoor) **Q**-one-way functions

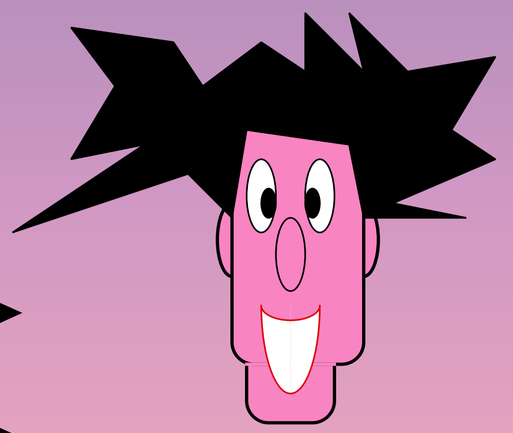
. . . . .

(3.2.1) Public-Key Q-Cryptosystem

Assuming Classical Public Key Cryptography



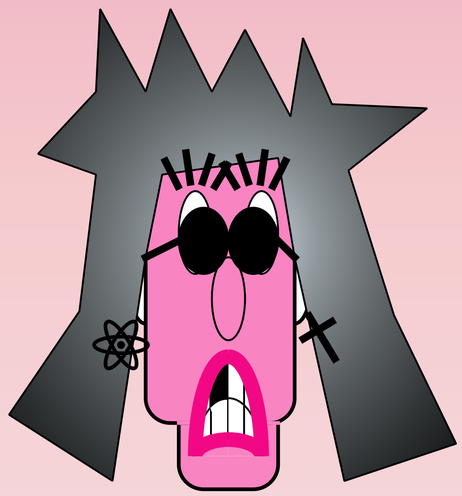
$|\Psi\rangle$



a,b random bits

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

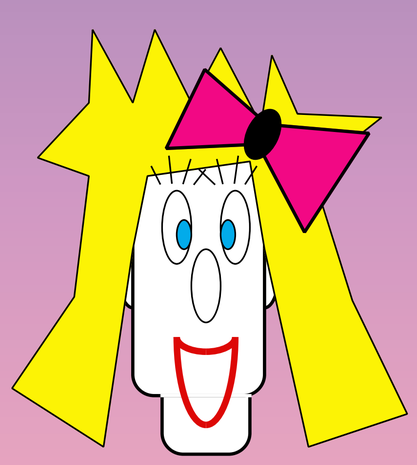
$|\Psi'\rangle=(\sigma_x)^a(\sigma_z)^b|\Psi\rangle$



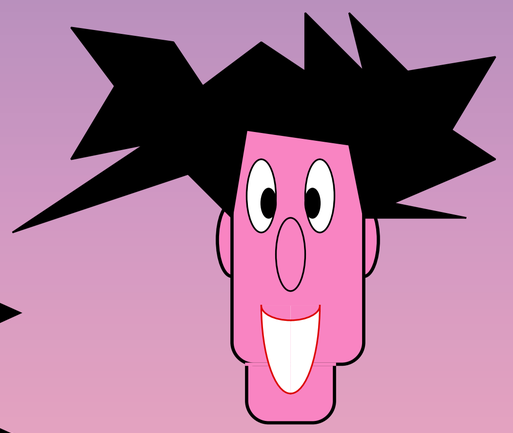
$|\Psi\rangle=(\sigma_z)^b(\sigma_x)^a|\Psi'\rangle$

(3.2.2a) Public-Key Q-Authentication

Assuming Classical Public Key Cryptography
Assuming Classical Digital Signature

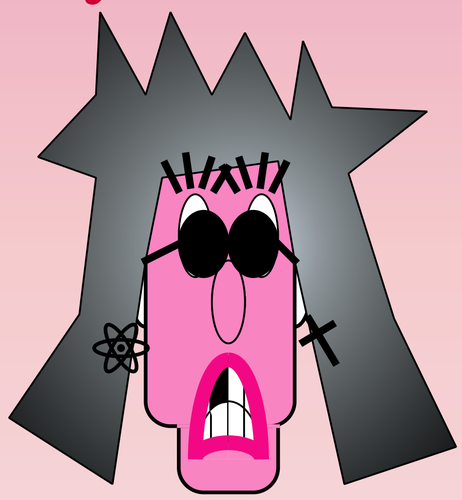


$|\Psi\rangle$



K random authentication key

$|\Psi'\rangle := \text{Auth}_K(|\Psi\rangle)$

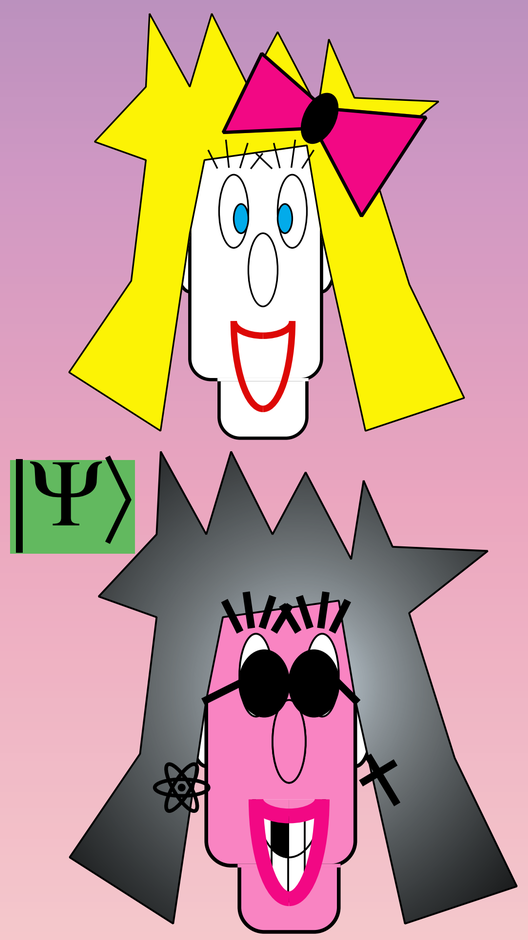


verify signed E(K)
K := D(E(K))

$|\Psi\rangle := \text{Auth}^{-1}_K(|\Psi'\rangle)$

(3.2.2b) Q-Digital Signature Scheme

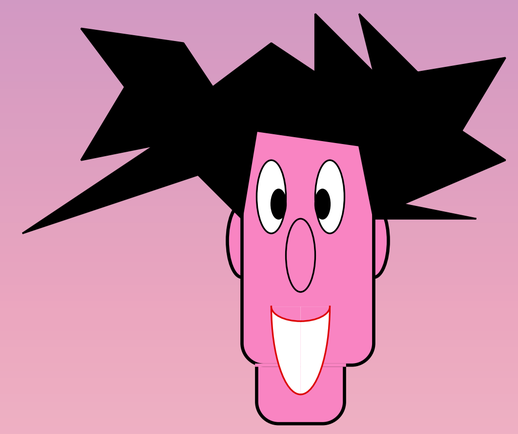
Assuming Classical Public Key Cryptography
Assuming Classical Digital Signature



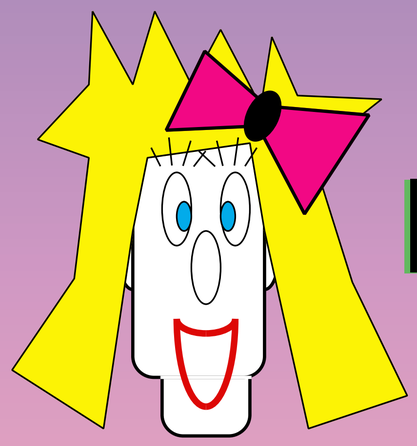
Signature

Validation

Extract



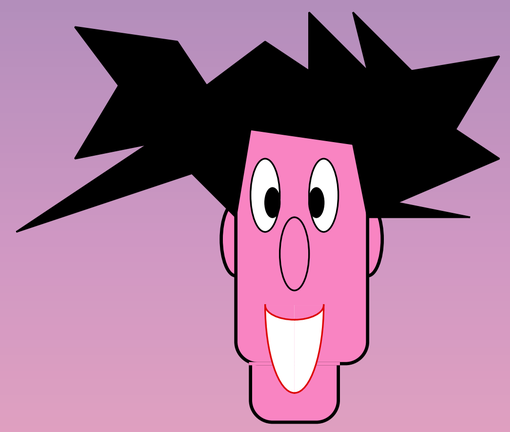
(3.2.2b) ϙ-Digital Signature Scheme

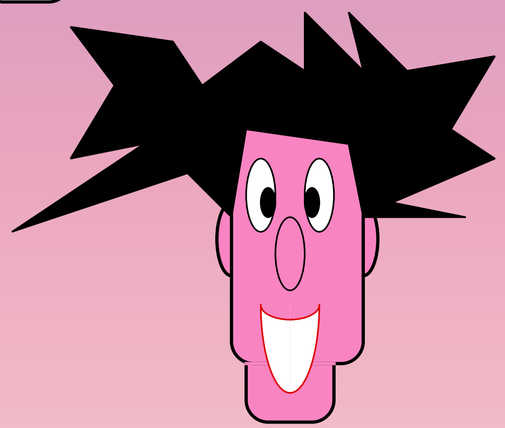


$|\Psi\rangle|0\rangle$

Signature

$\rho_.$





$\rho_.$

Validation

Valid

$\rho_.$

$\rho_.$

Extract

$|\Psi\rangle|\varepsilon\rangle$

$\rho_.$

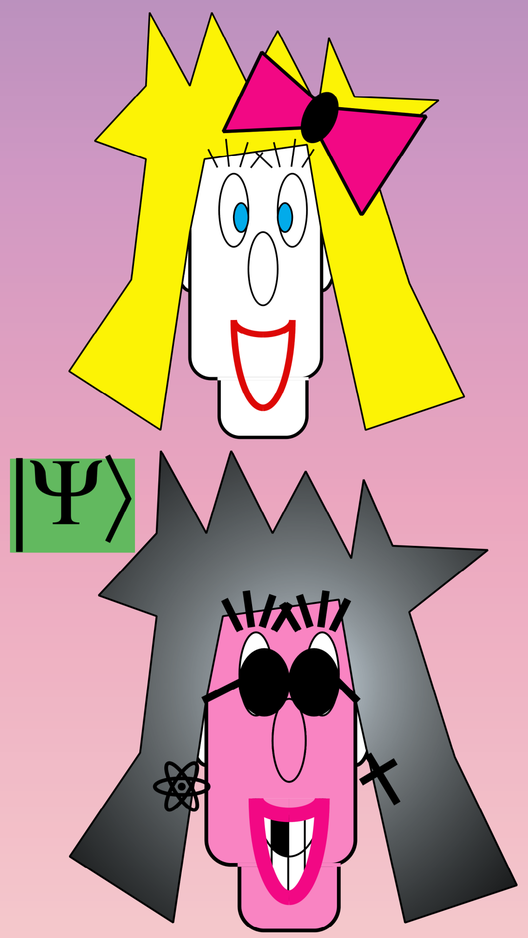
Validation

Valid

$\rho_.$

(3.2.2b) Q-Digital Signature Scheme

Assuming Classical Public Key Cryptography
Assuming Classical Digital Signature

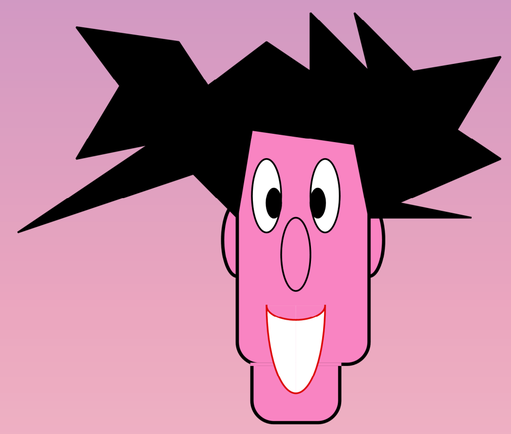


Signature

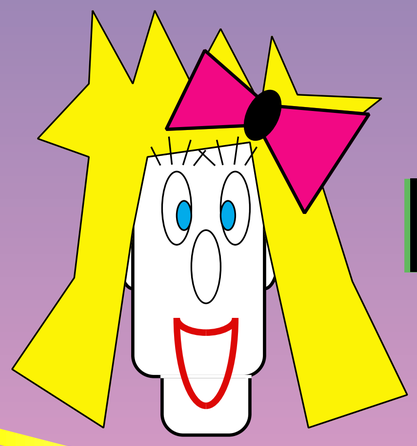
Validation

Extract

IMPOSSIBLE



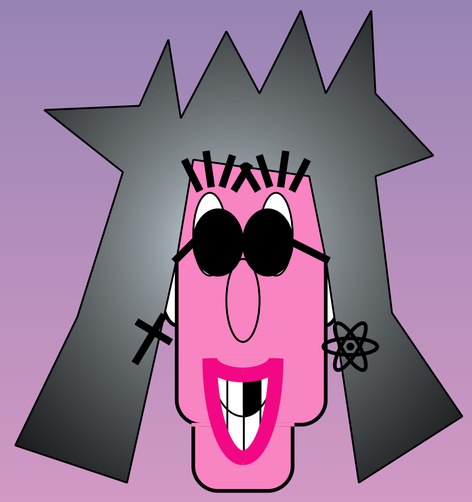
(3.2.2b) Q-Digital Signature Scheme



$|\Psi\rangle|0\rangle$

Signature

$\rho_.$

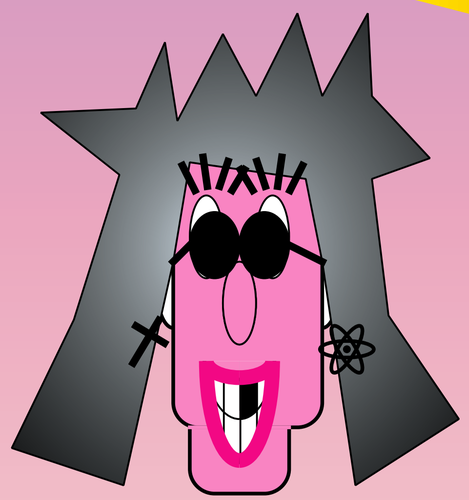


$\rho_.$

Validation

Valid

$\rho_.$



$\rho_.$

Extract

$|\Psi\rangle|\varepsilon\rangle$

$|\Psi\rangle/|\phi\rangle$

$|\phi\rangle|\varepsilon\rangle$

Extract^{-1}

$\rho'_.$

Validation

Valid

$\rho'_.$

Quantum one-time Authentication

Claude Crépeau

School of Computer Science
McGill University