

Quantum one-time Authentication

Claude Crépeau

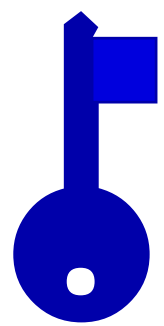
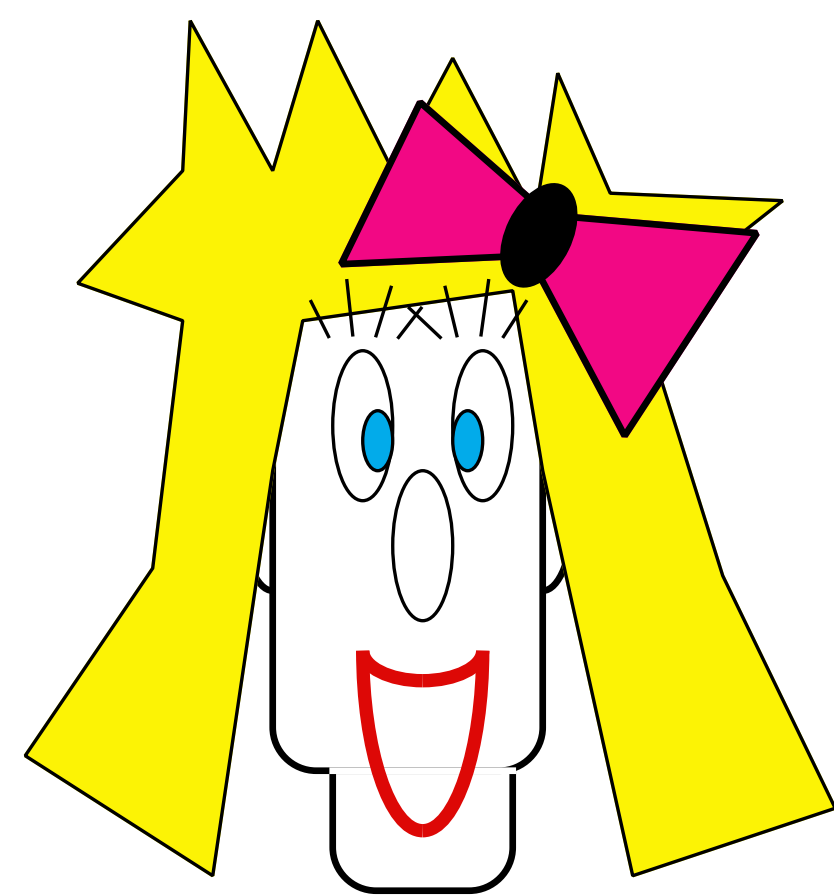
School of Computer Science
McGill University



(1)

Classical Cryptography

(1.1.3) Authentication

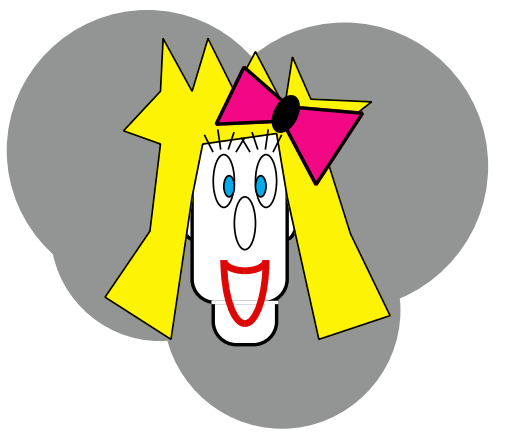
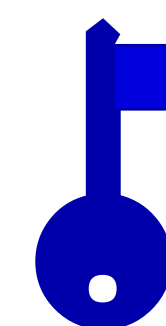
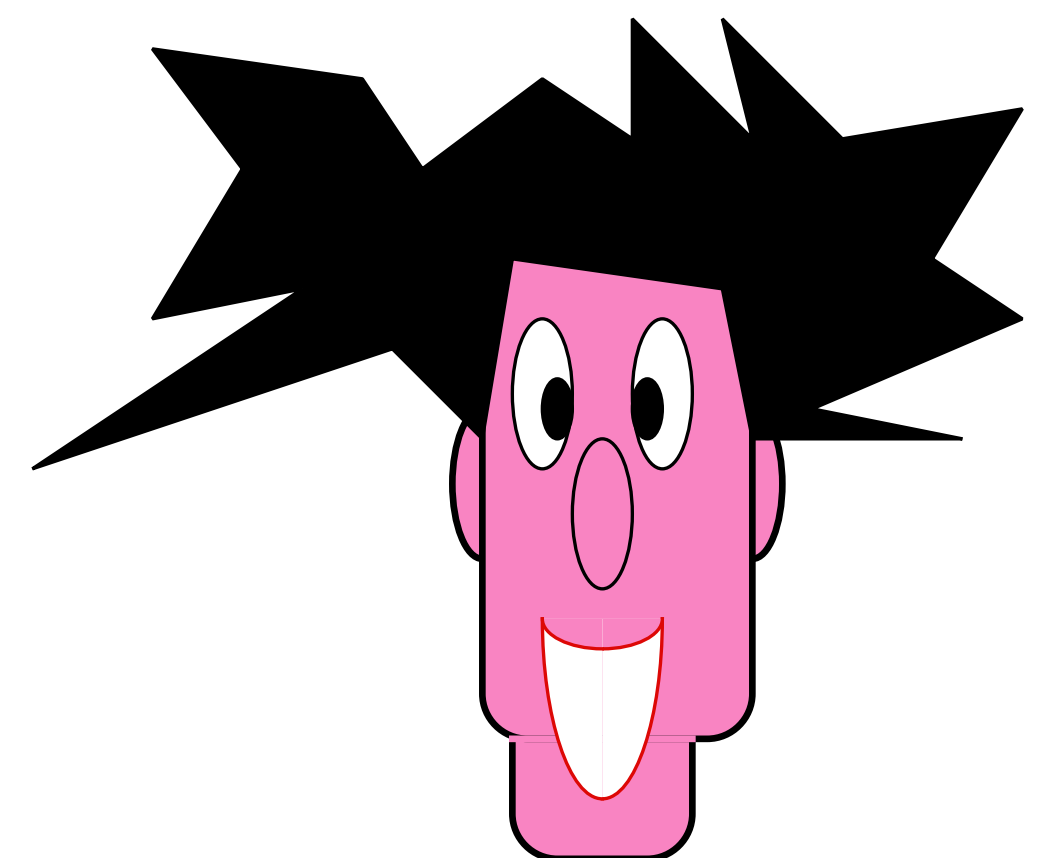


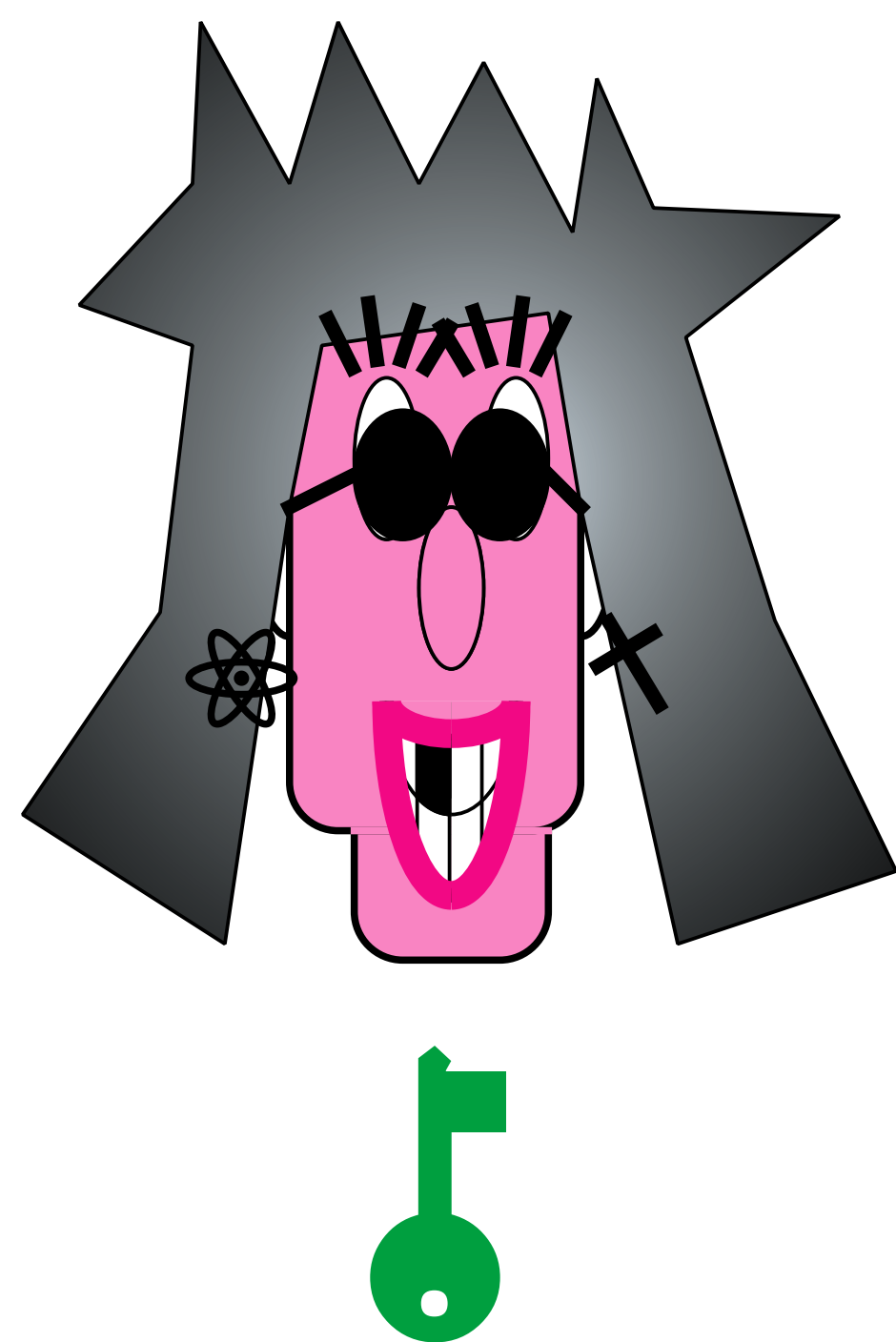
Will you marry me ?

Divorce your wife first !

The papers are in the mail...

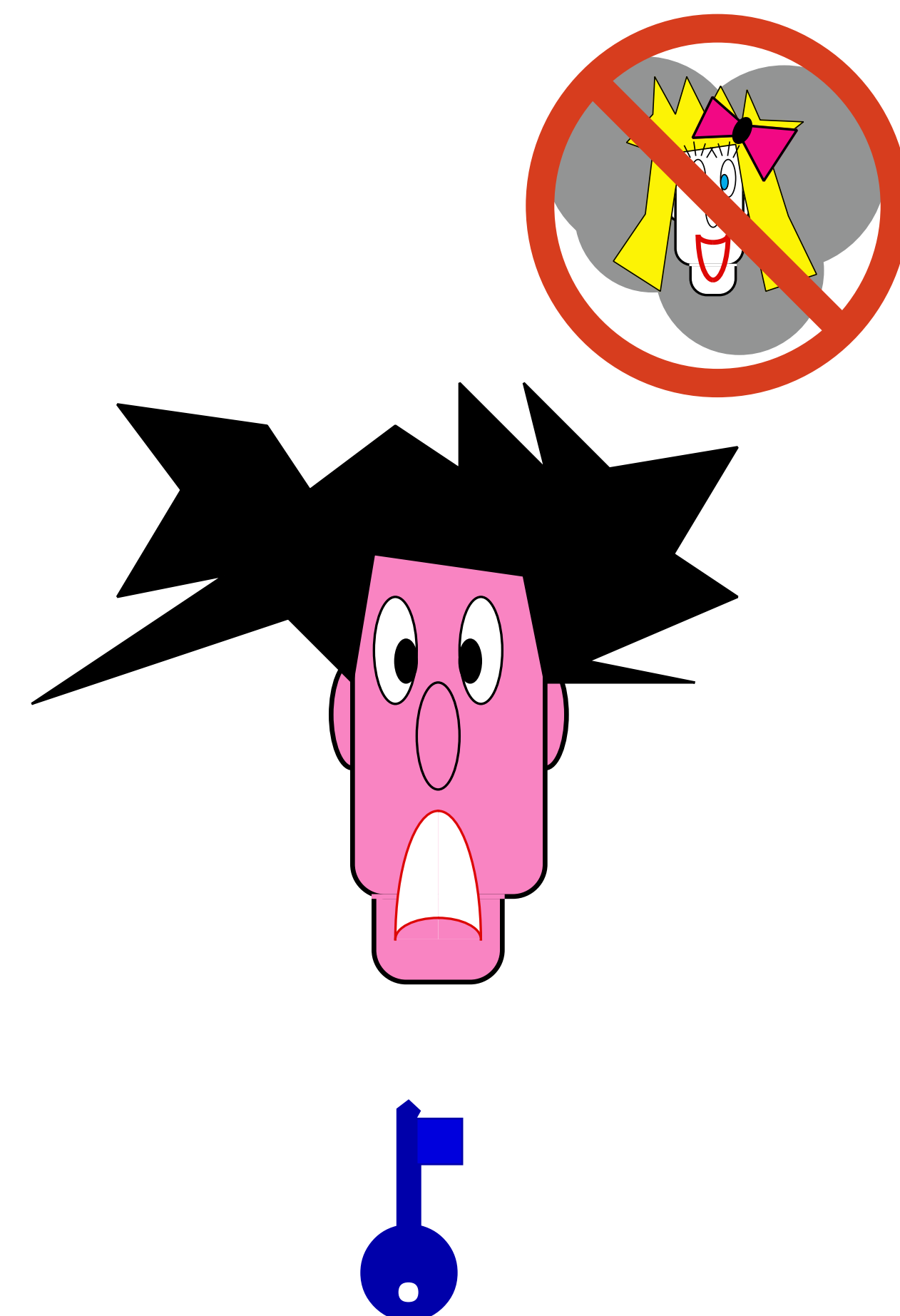
OK, I will !



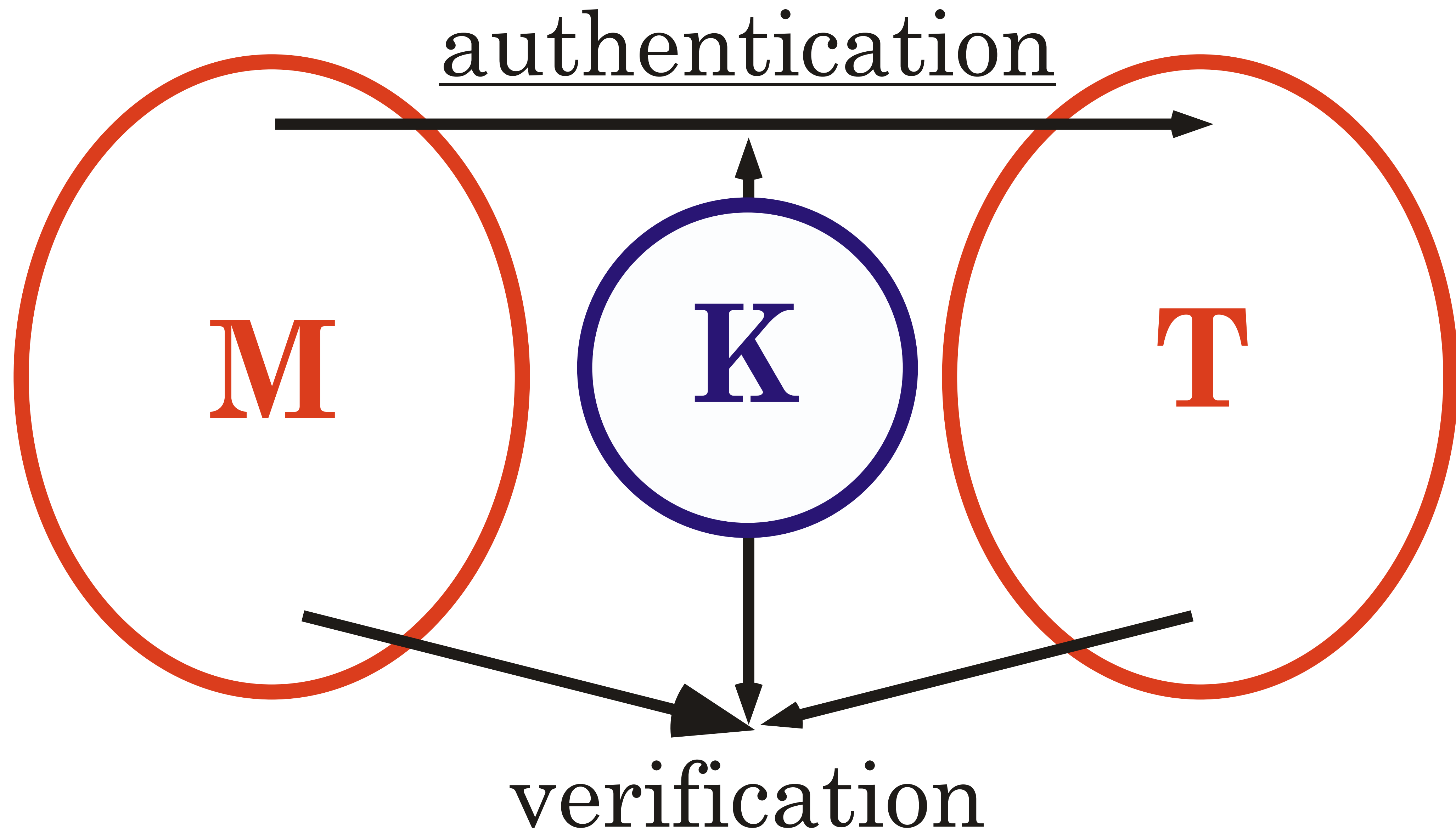


Will you marry me ?

No, I never will !

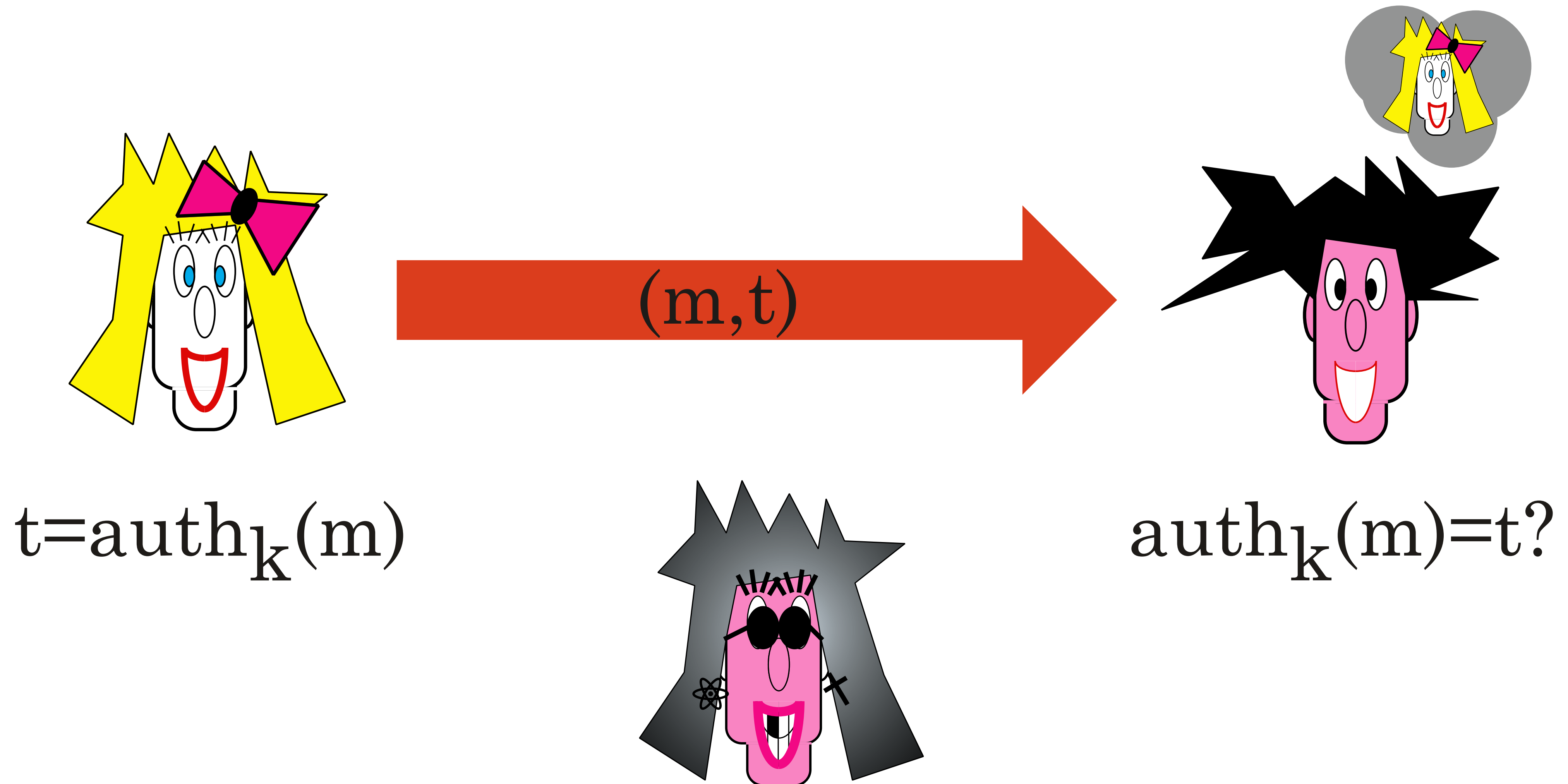


symmetric authentication



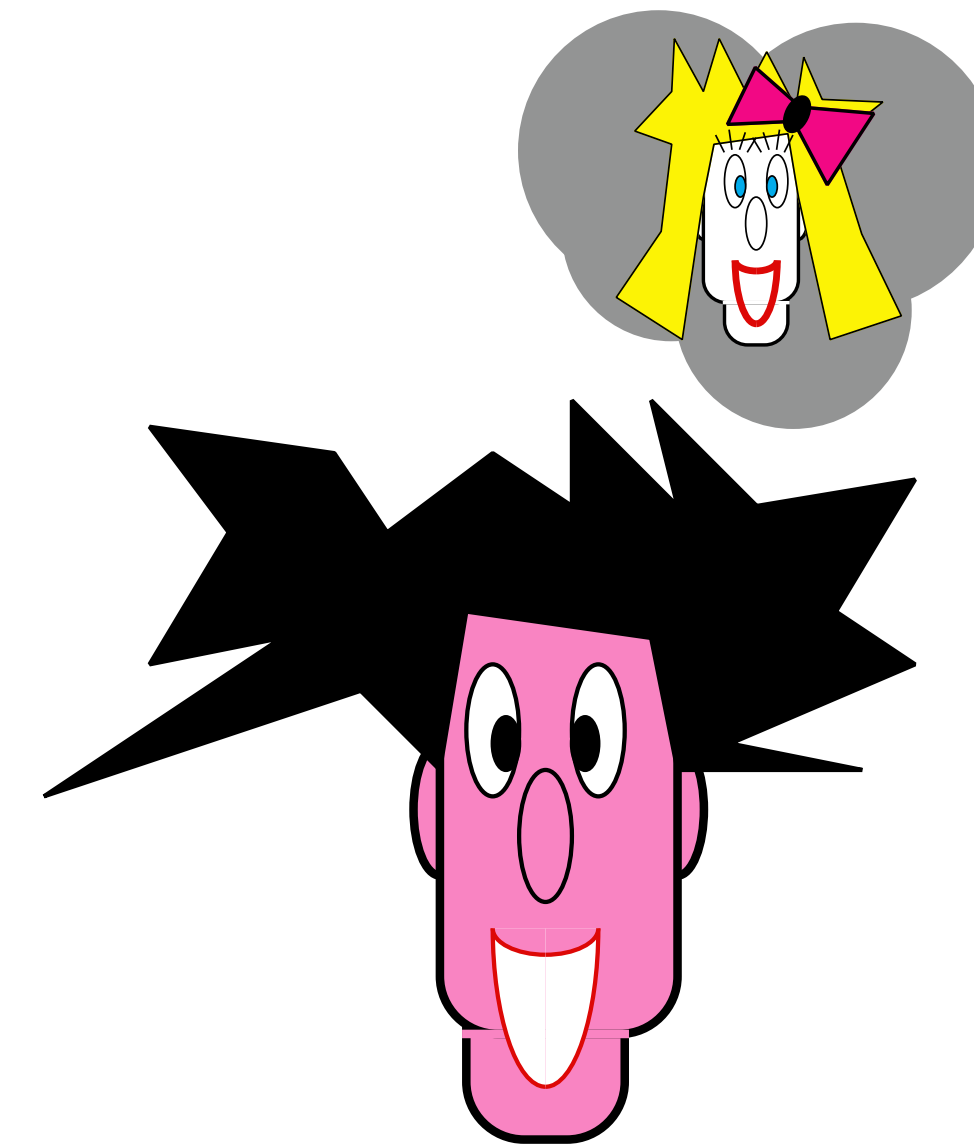
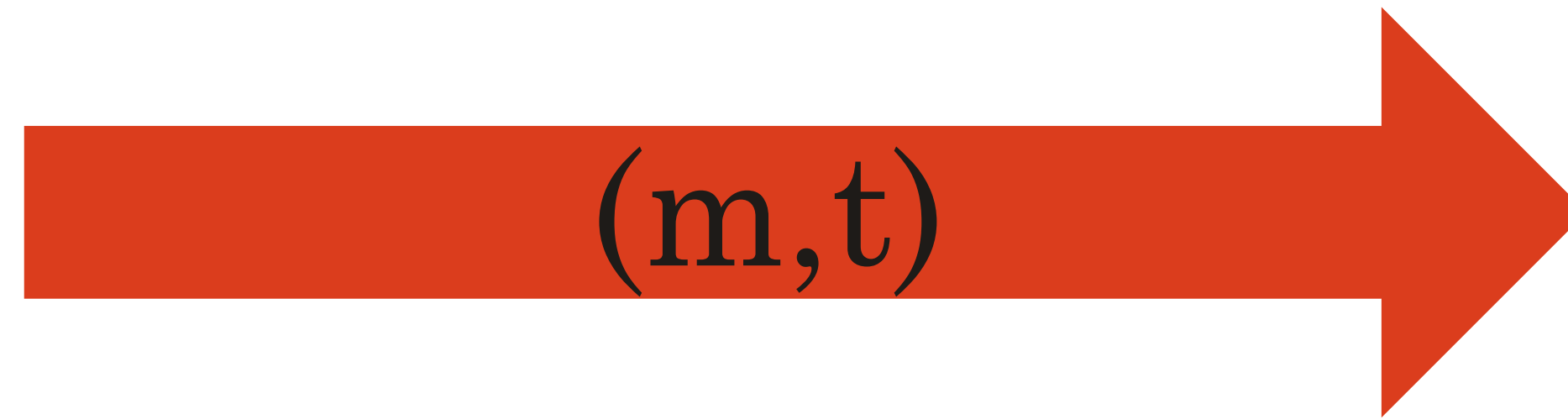
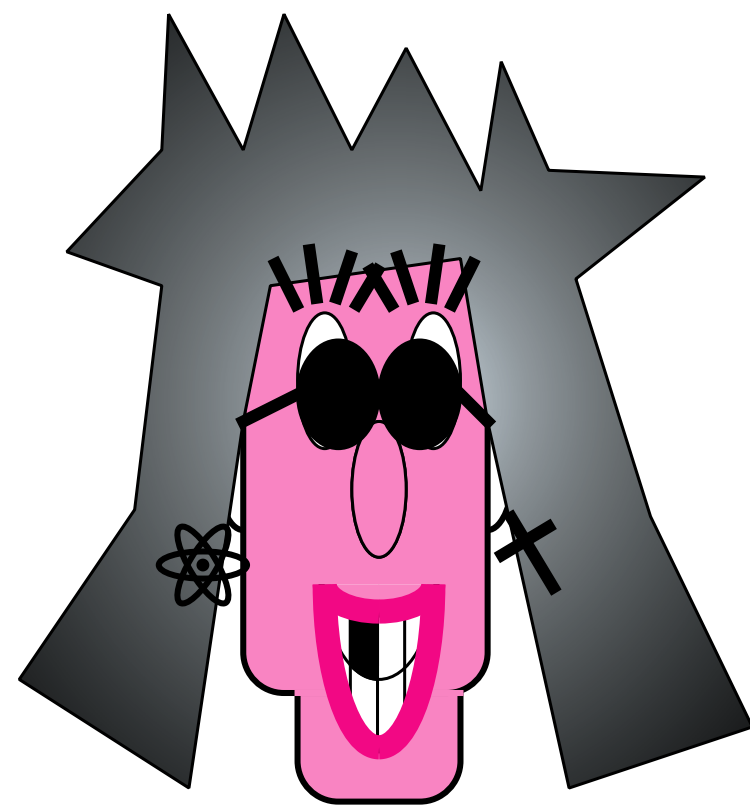
Information Theoretical Security

Authentication



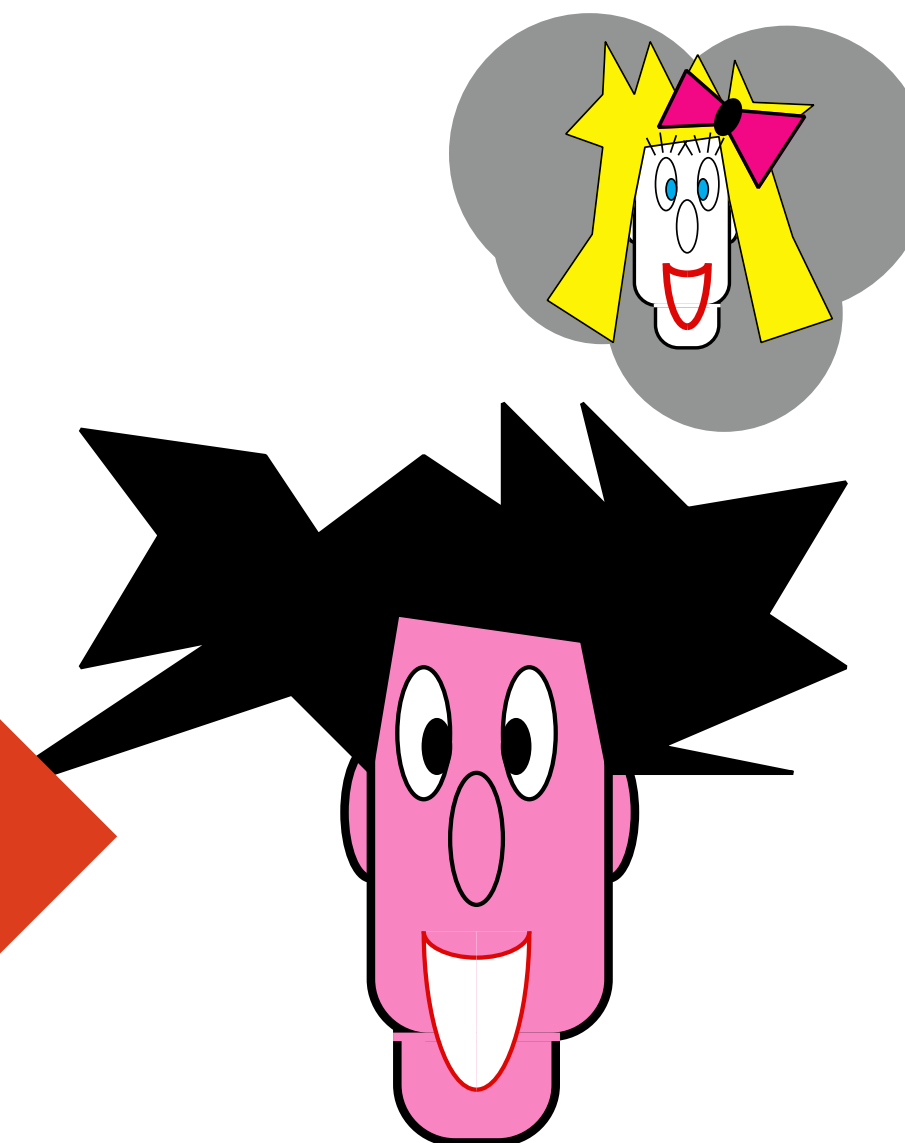
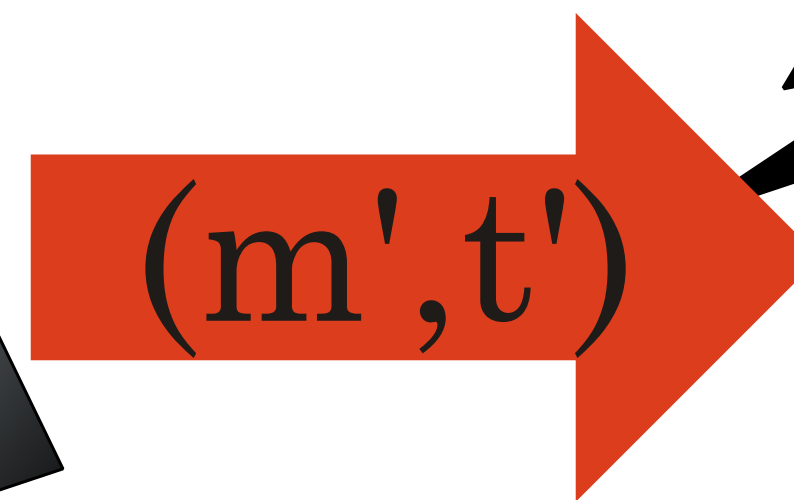
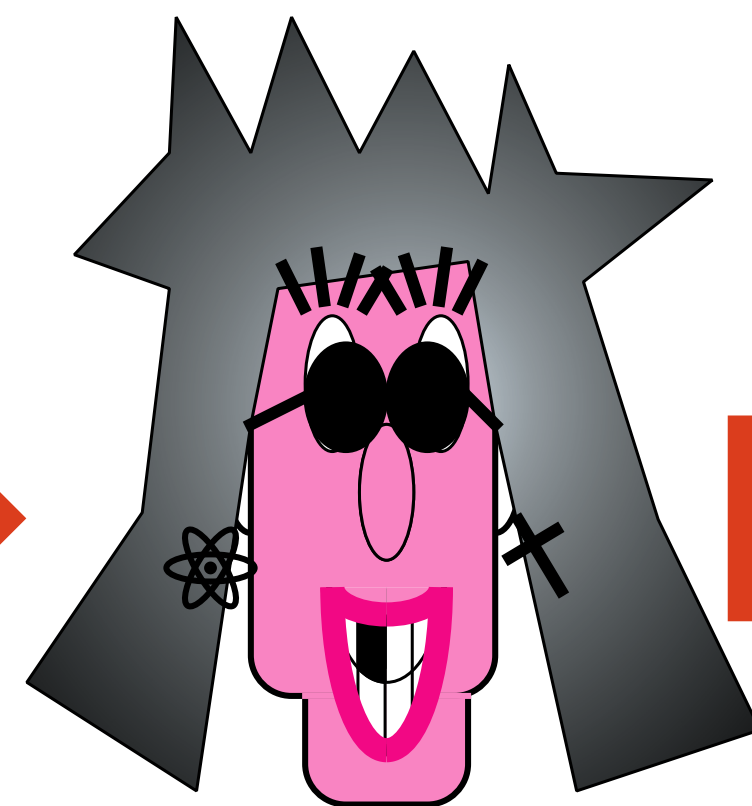
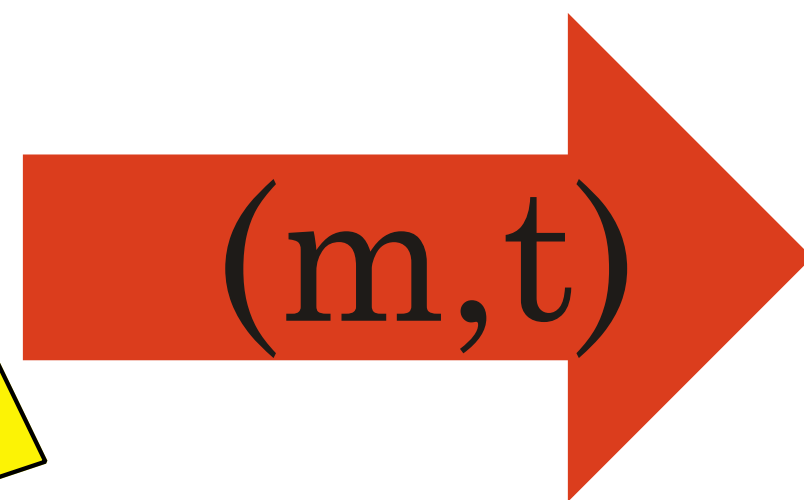
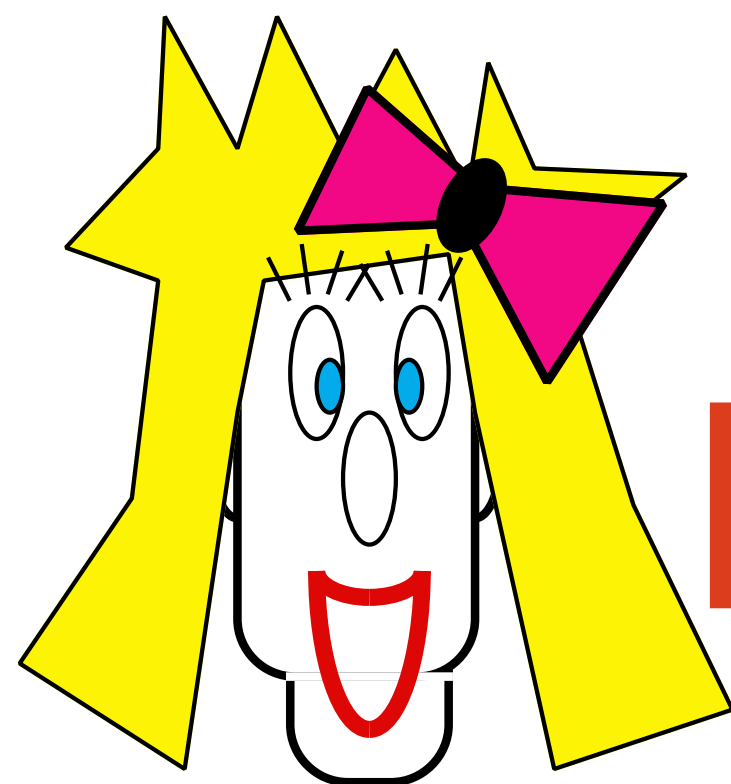
Information Theoretical Security

Impersonation



$\text{auth}_k(m)=t?$

Substitution



$\text{auth}_k(m')=t'?$

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

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

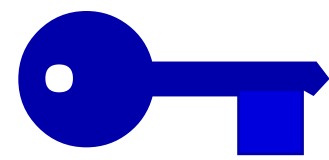
$$[\mathbf{I}:\mathbf{M}]m \oplus [0:b] = [m:t]$$

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

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

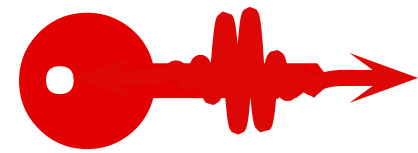
$[m:t]$ systematic form of (message, tag)

(3.1.3) One-time Q-Authentication



Classical key : Q-Authentication (BCGST)

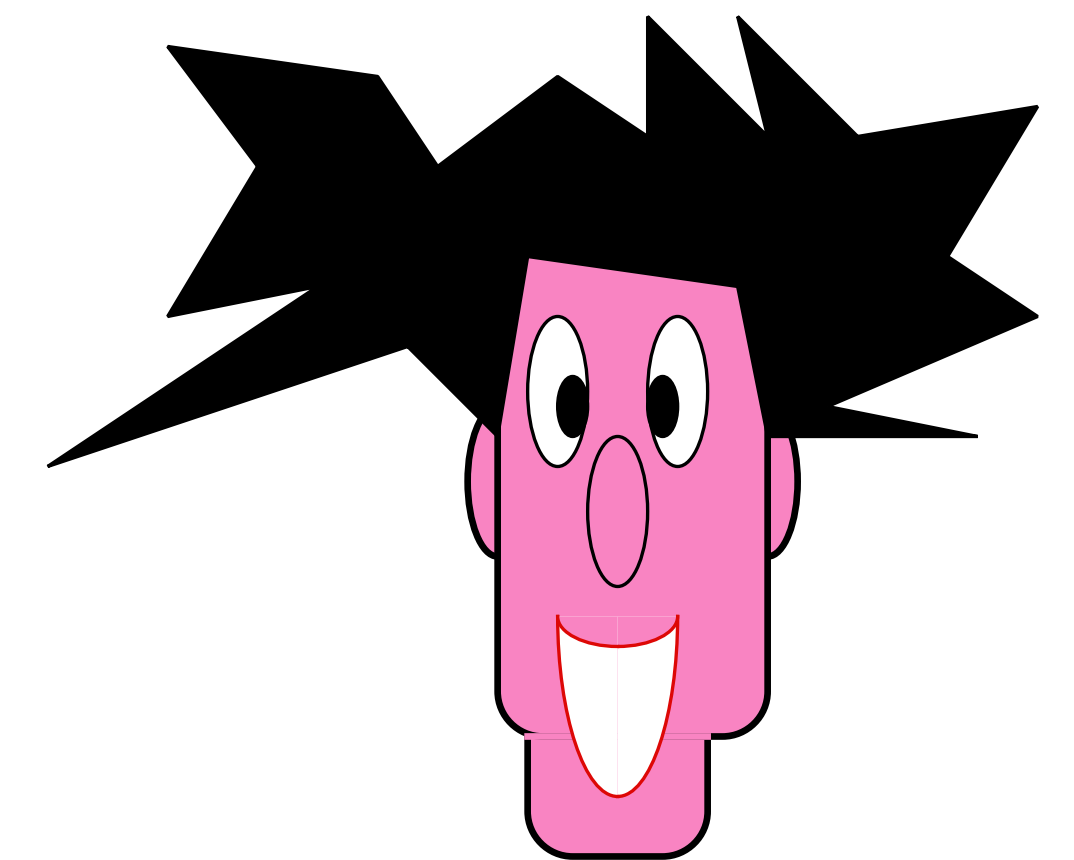
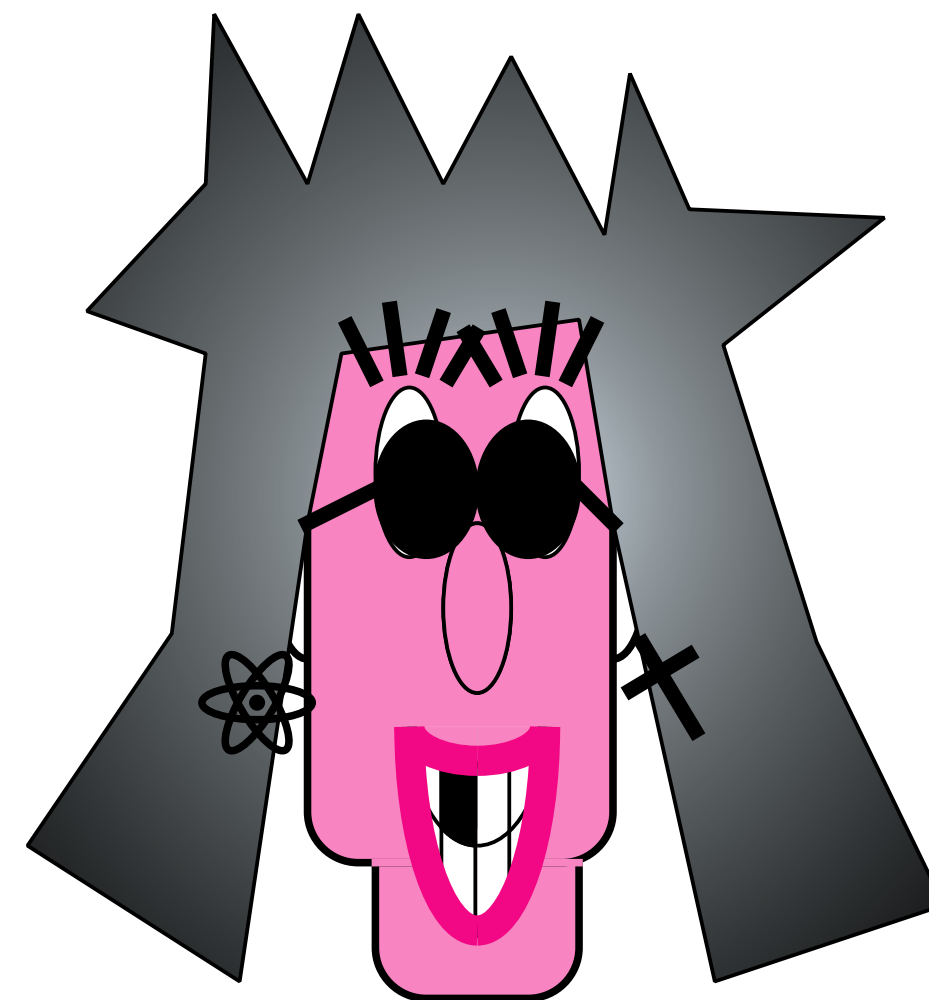
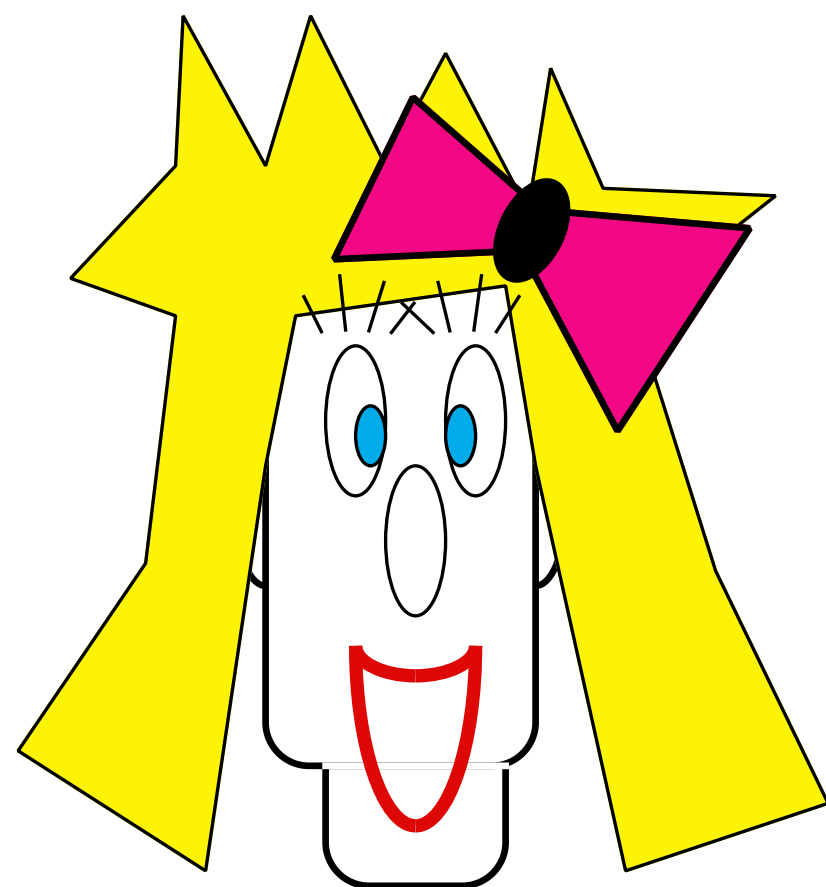
Quantum message+tag



Quantum key : Authenticated Q-teleportation

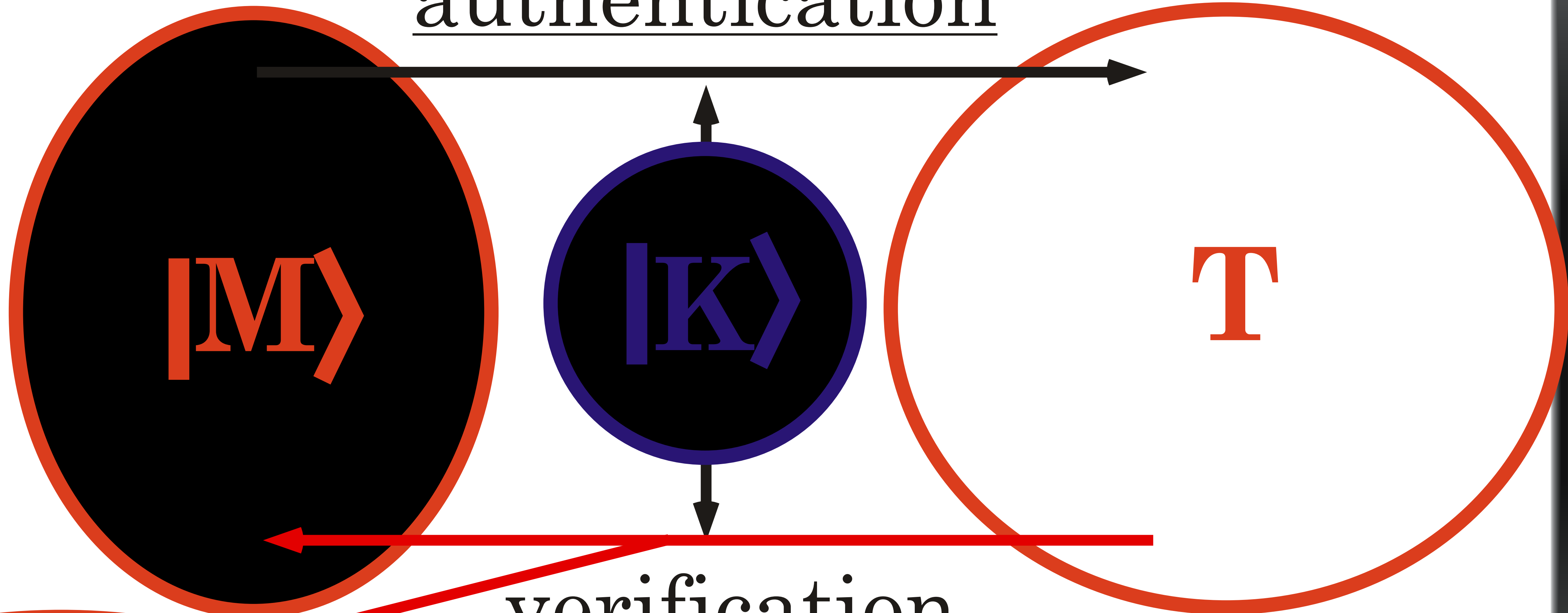
Classical message+tag

(BBCJPW)



symmetric authentication

authentication

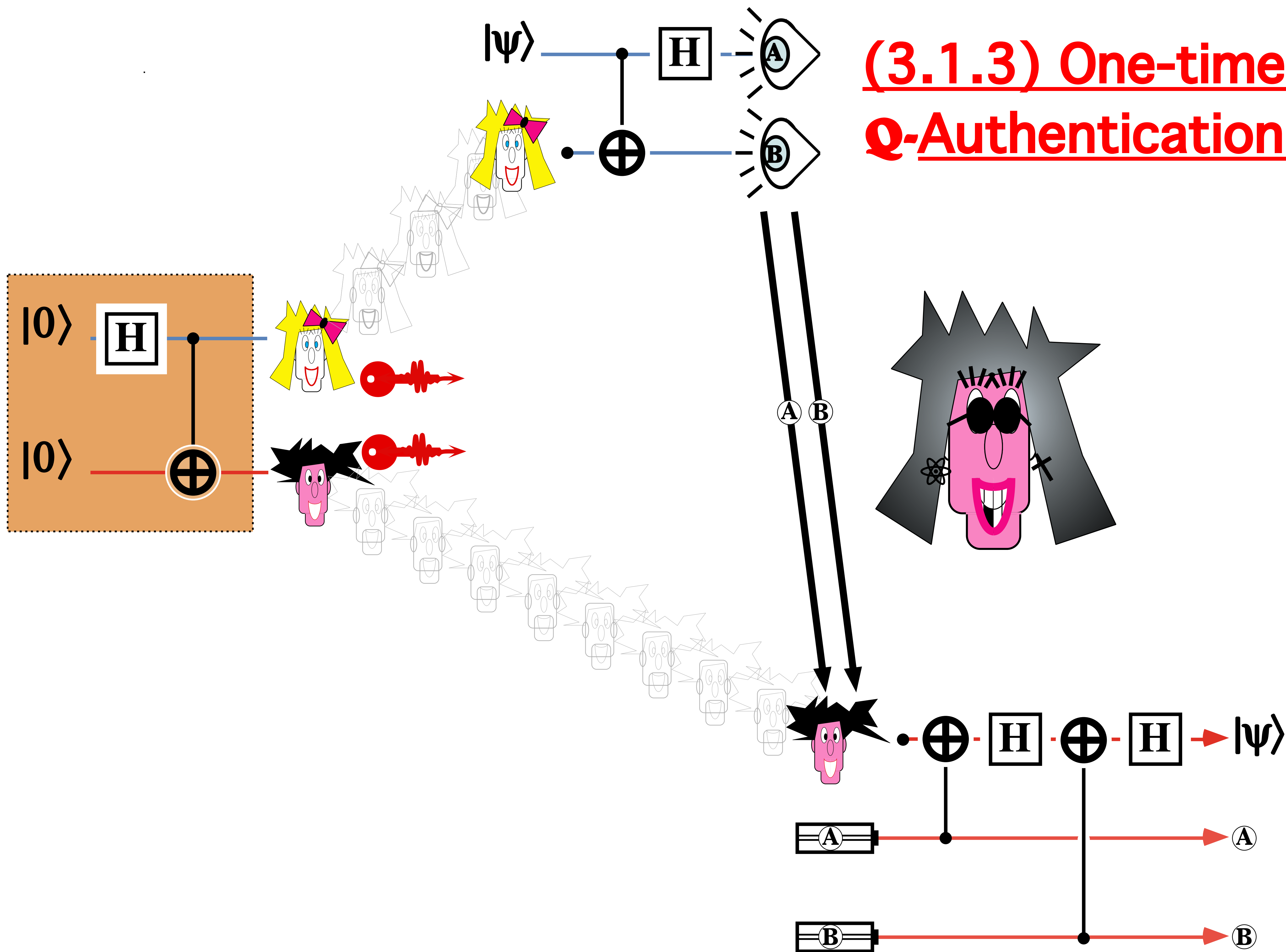


verification

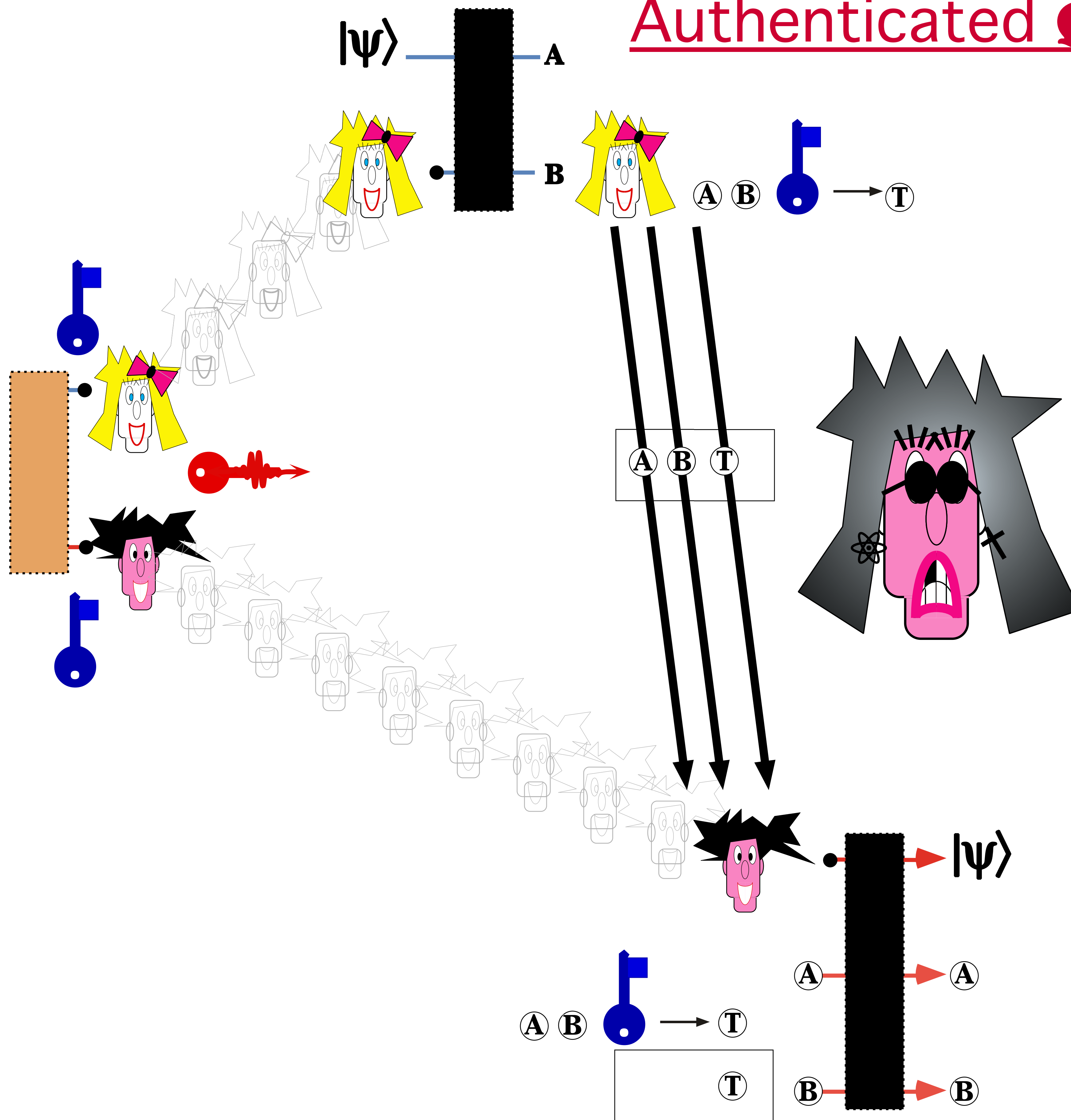
$\{ACC, REJ\}$

Information Theoretical Security

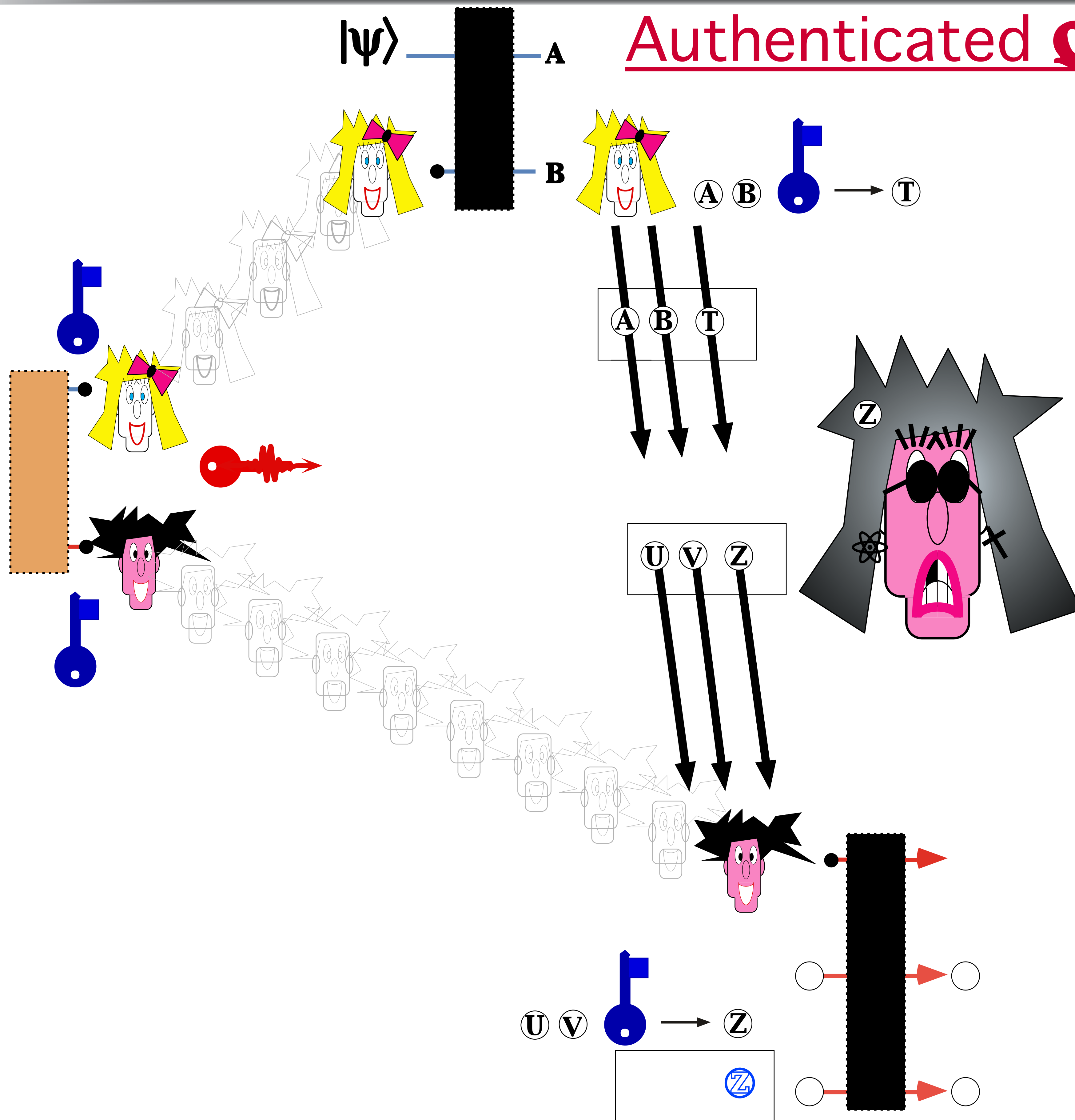
(3.1.3) One-time Q-Authentication



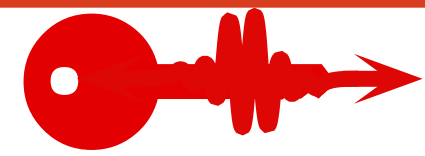
Authenticated Q-teleportation



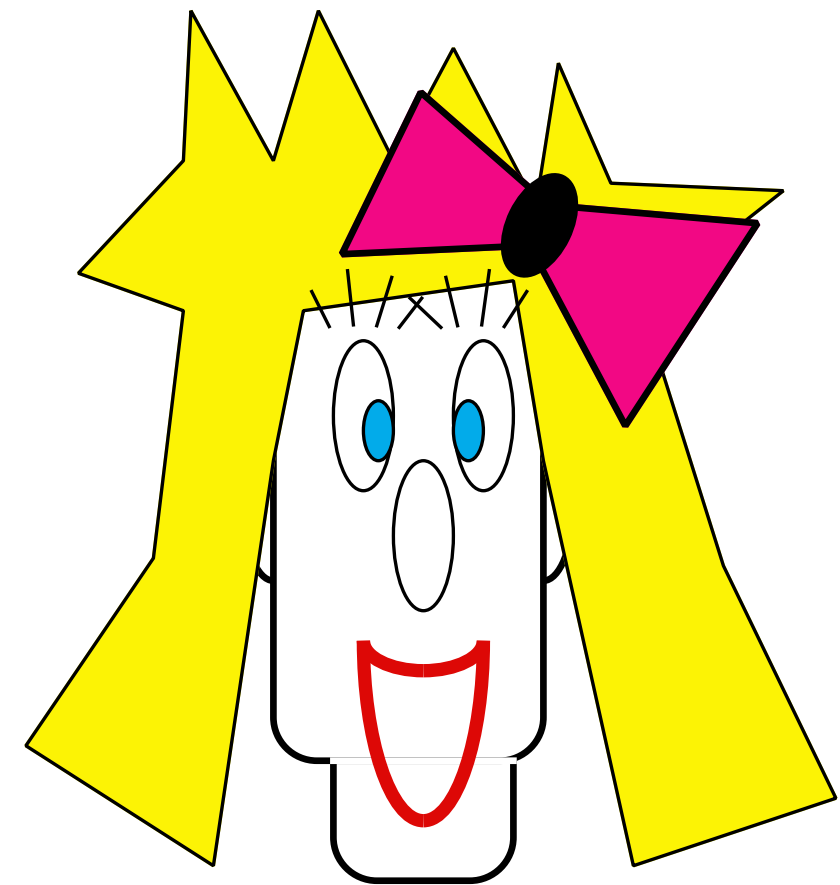
Authenticated \mathcal{Q} -teleportation



(3.1.3b) One-time Q-Authentication

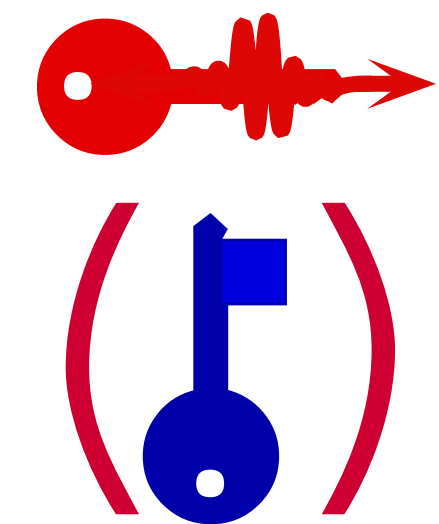
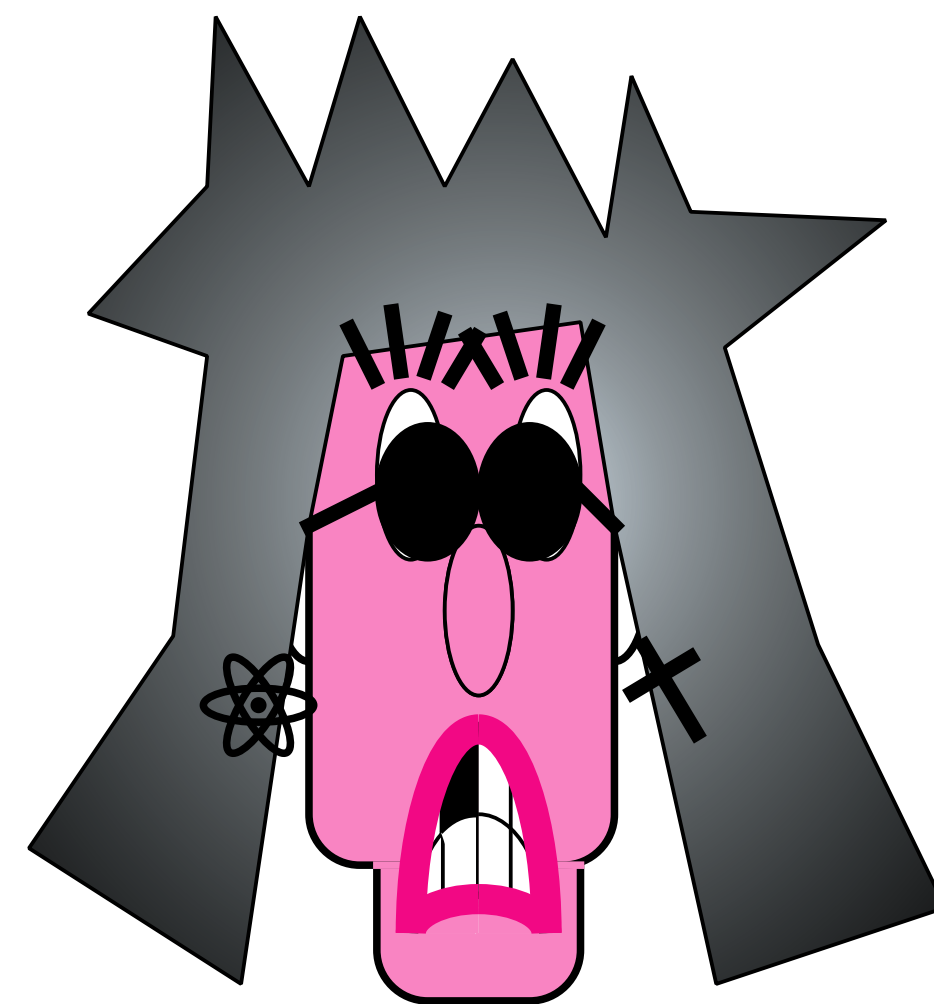
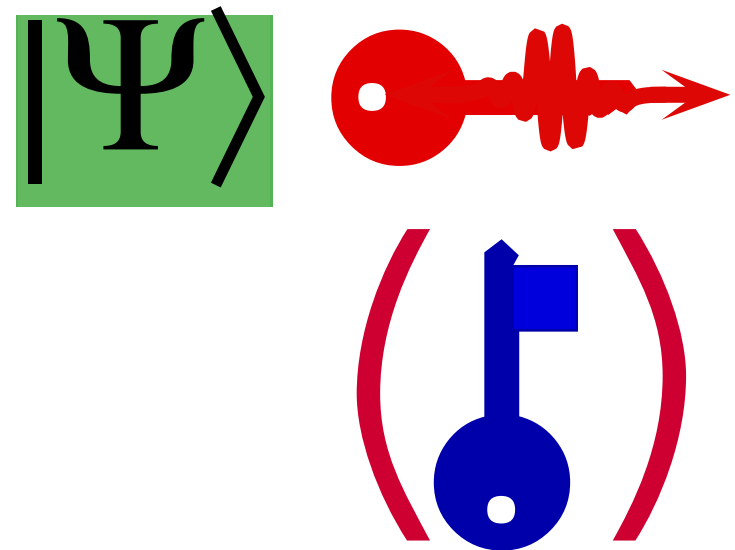
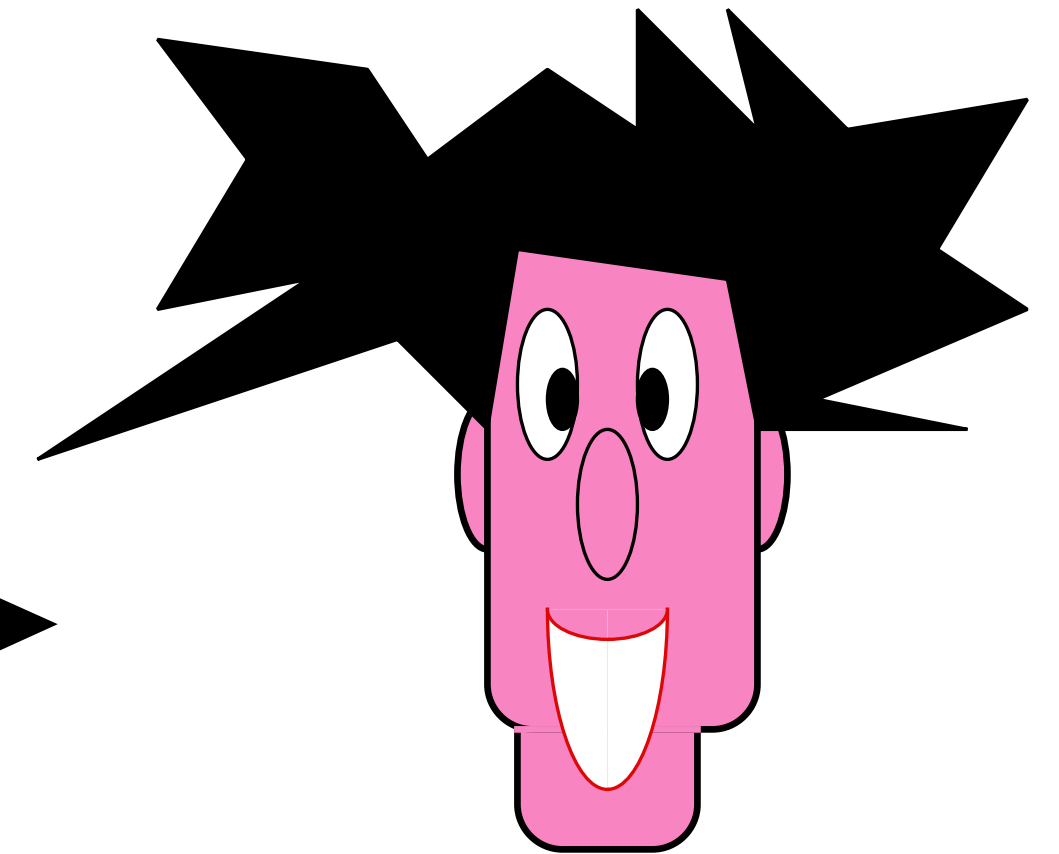


Quantum key : 1x Authenticated Q-pad
Classical message+tag

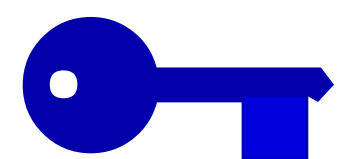


A B T

two authenticated random bits

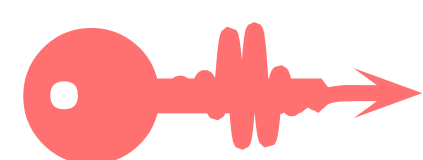


(3.1.3a) One-time Q-Authentication



Classical key : Q-Authentication (BCGST)

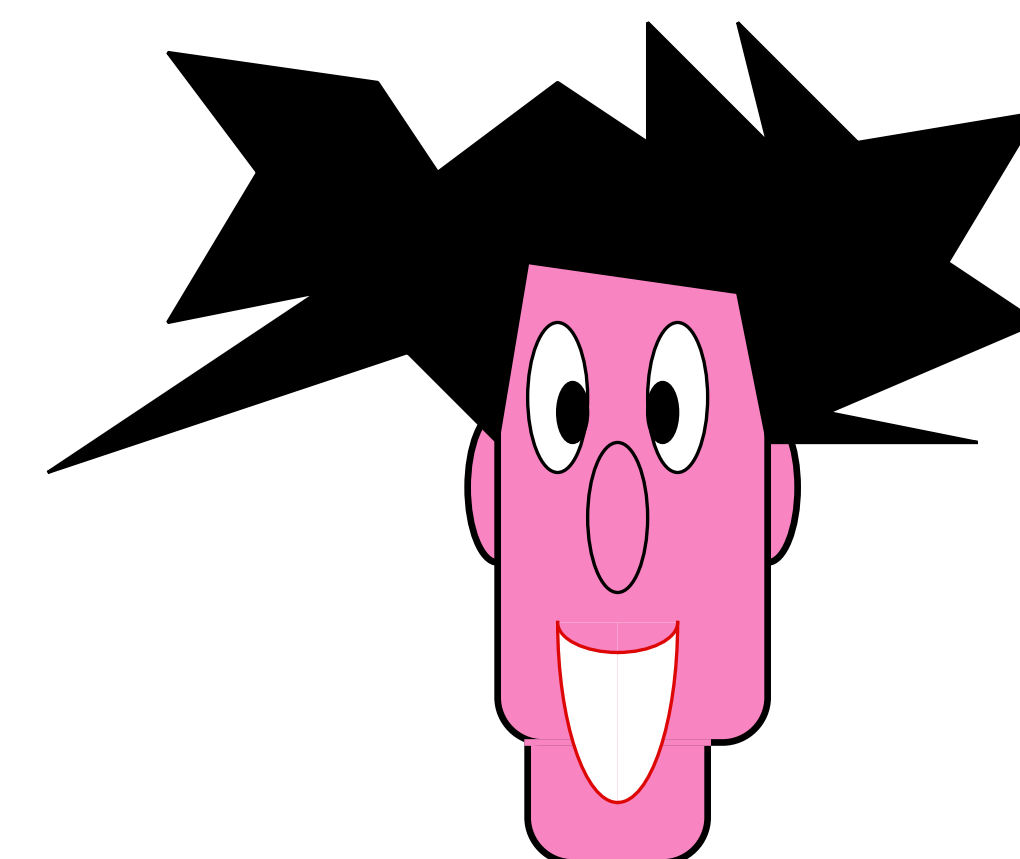
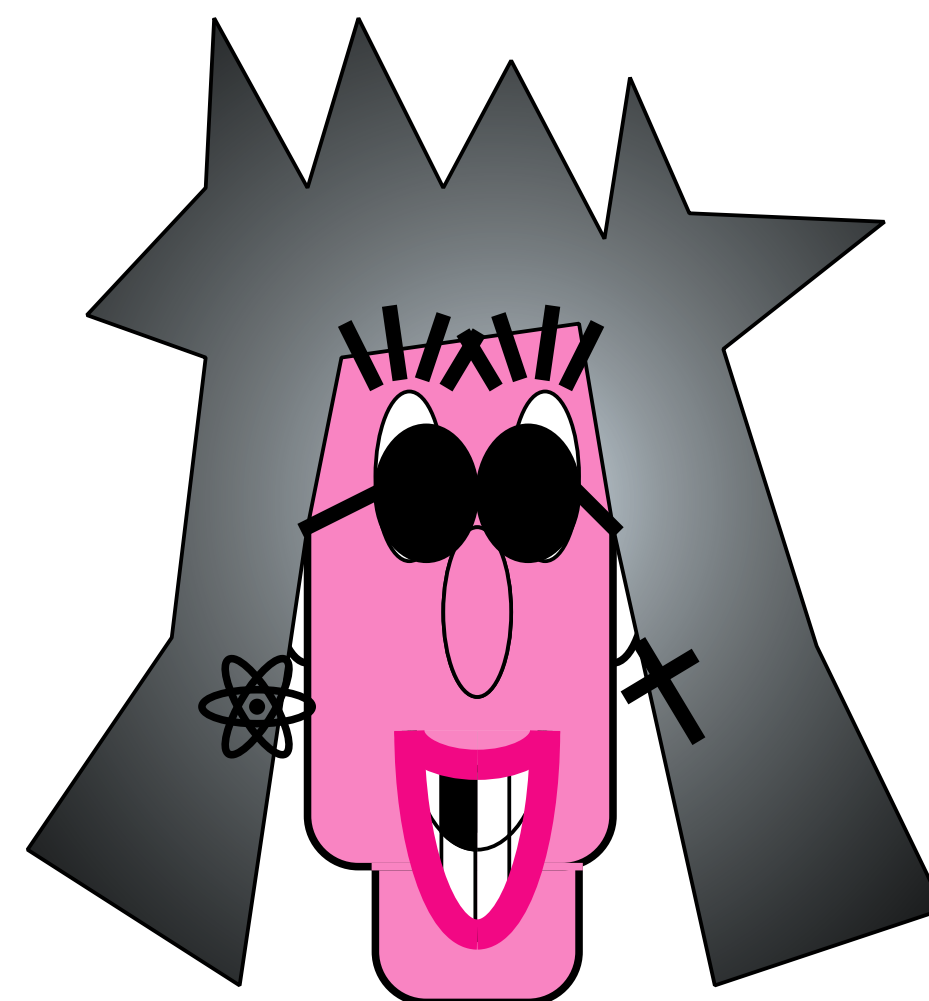
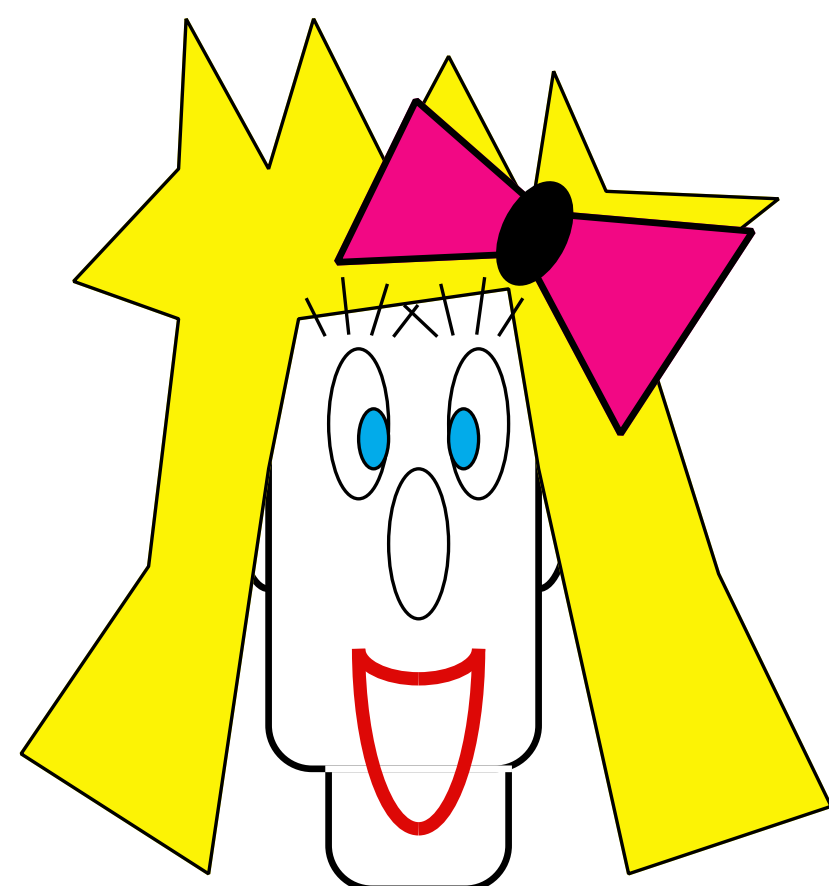
Quantum message+tag



Quantum key : Authenticated Q-teleportation

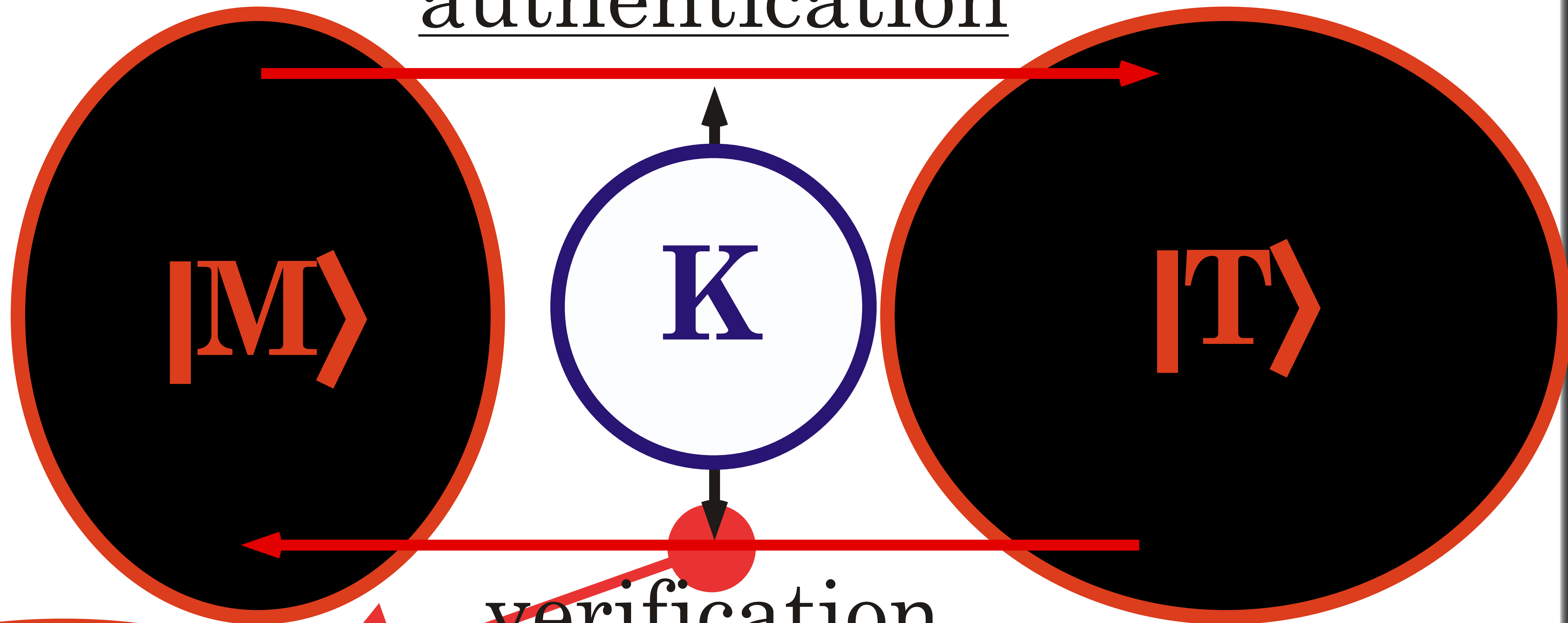
Classical message+tag

(BBCJPW)



symmetric authentication of Quantum Messages

authentication

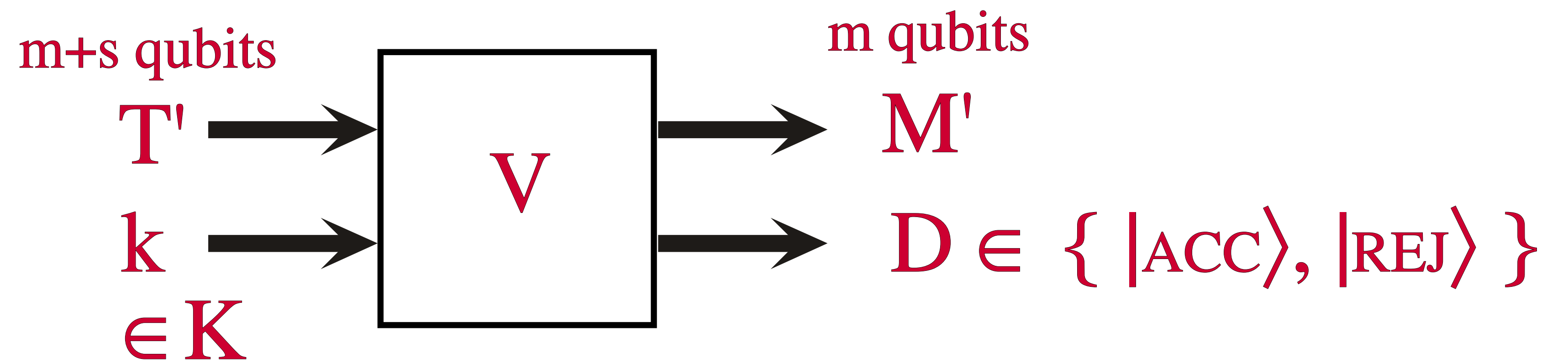
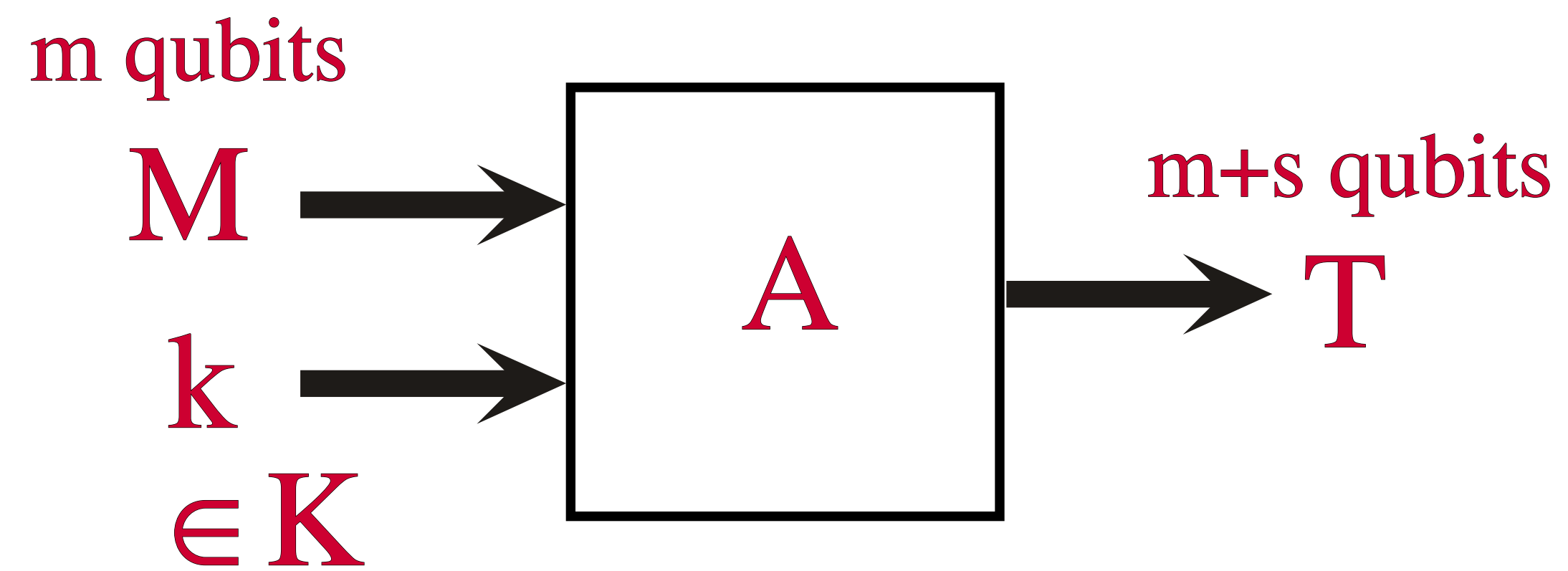


verification

$\{|ACC\rangle, |REJ\rangle\}$

Information Theoretical Security

One-time \mathcal{Q} -Authentication



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 $D=|\text{REJ}\rangle$
- output Wrong otherwise



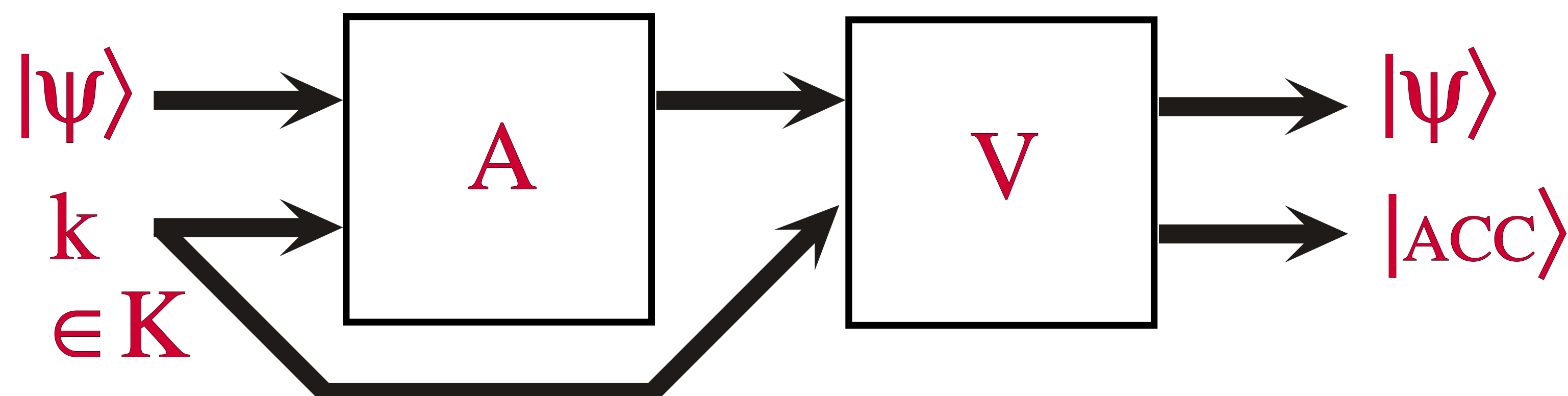
The corresponding projectors are

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

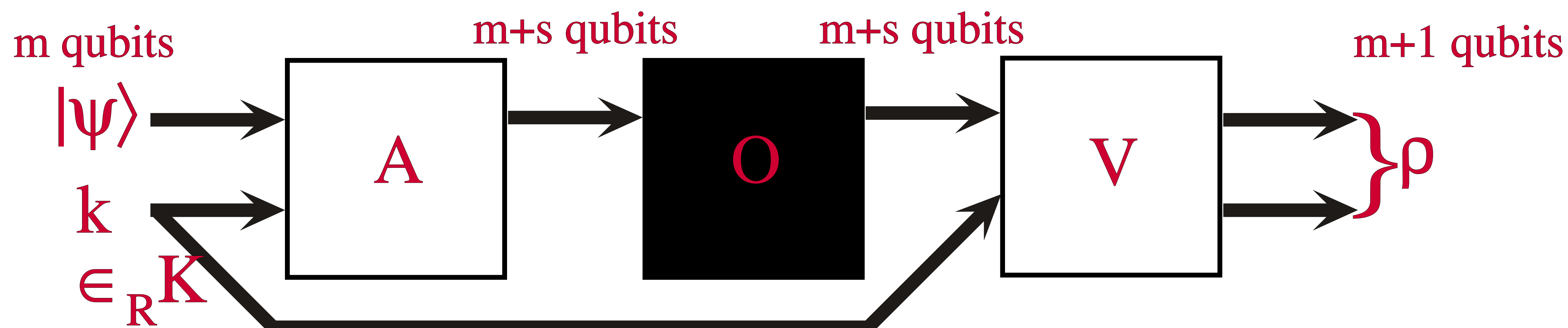
$$W_{|\psi\rangle} = (I_{M'} - |\psi\rangle\langle\psi|) \otimes |\text{ACC}\rangle\langle\text{ACC}|$$

One-time \mathcal{Q} -Authentication

Completeness:



Soundness:



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

(3.3C) One-time interactive Q-Authentication

• • • • •

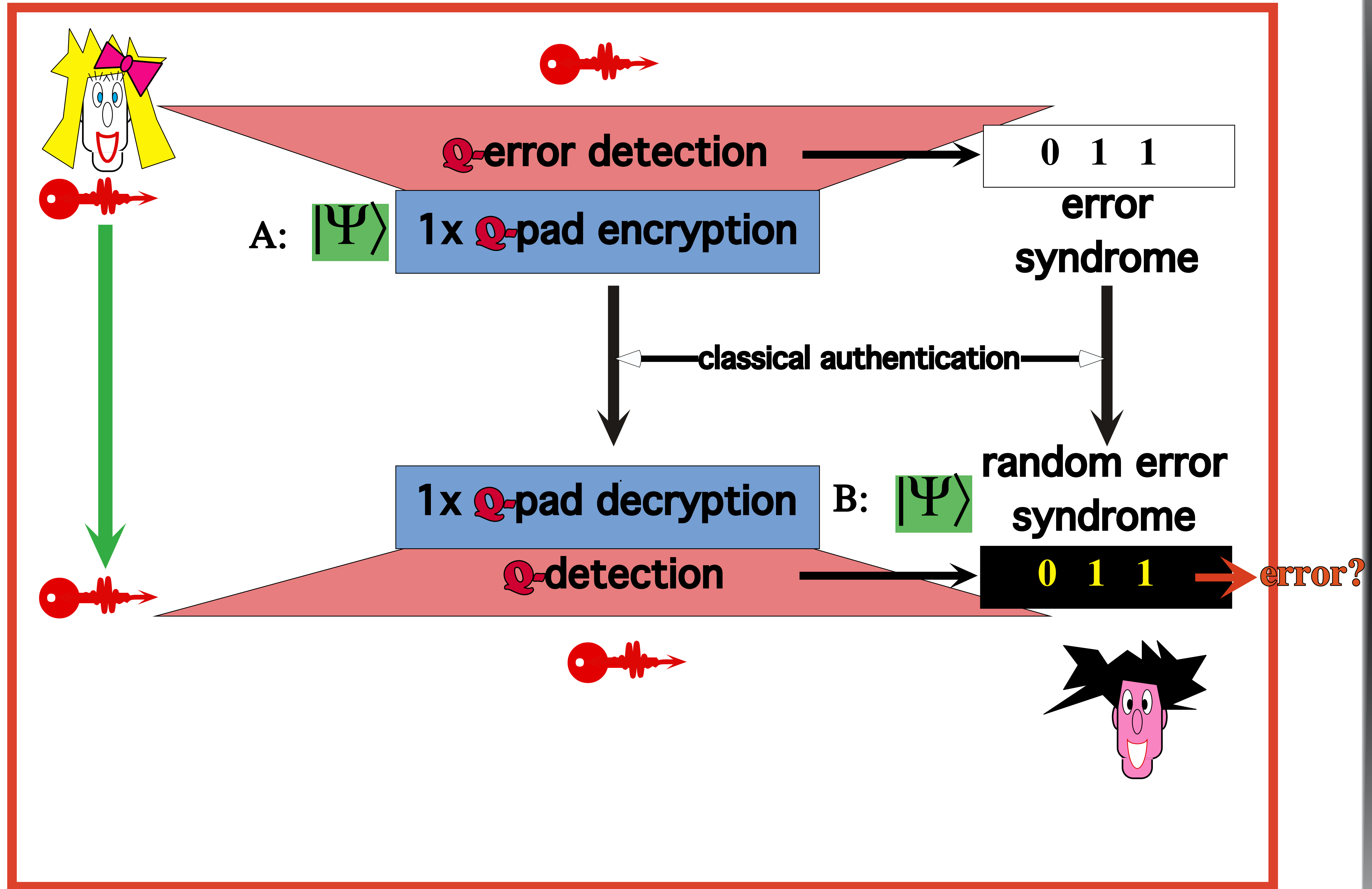
- Transmit quantum key (EPR states)

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

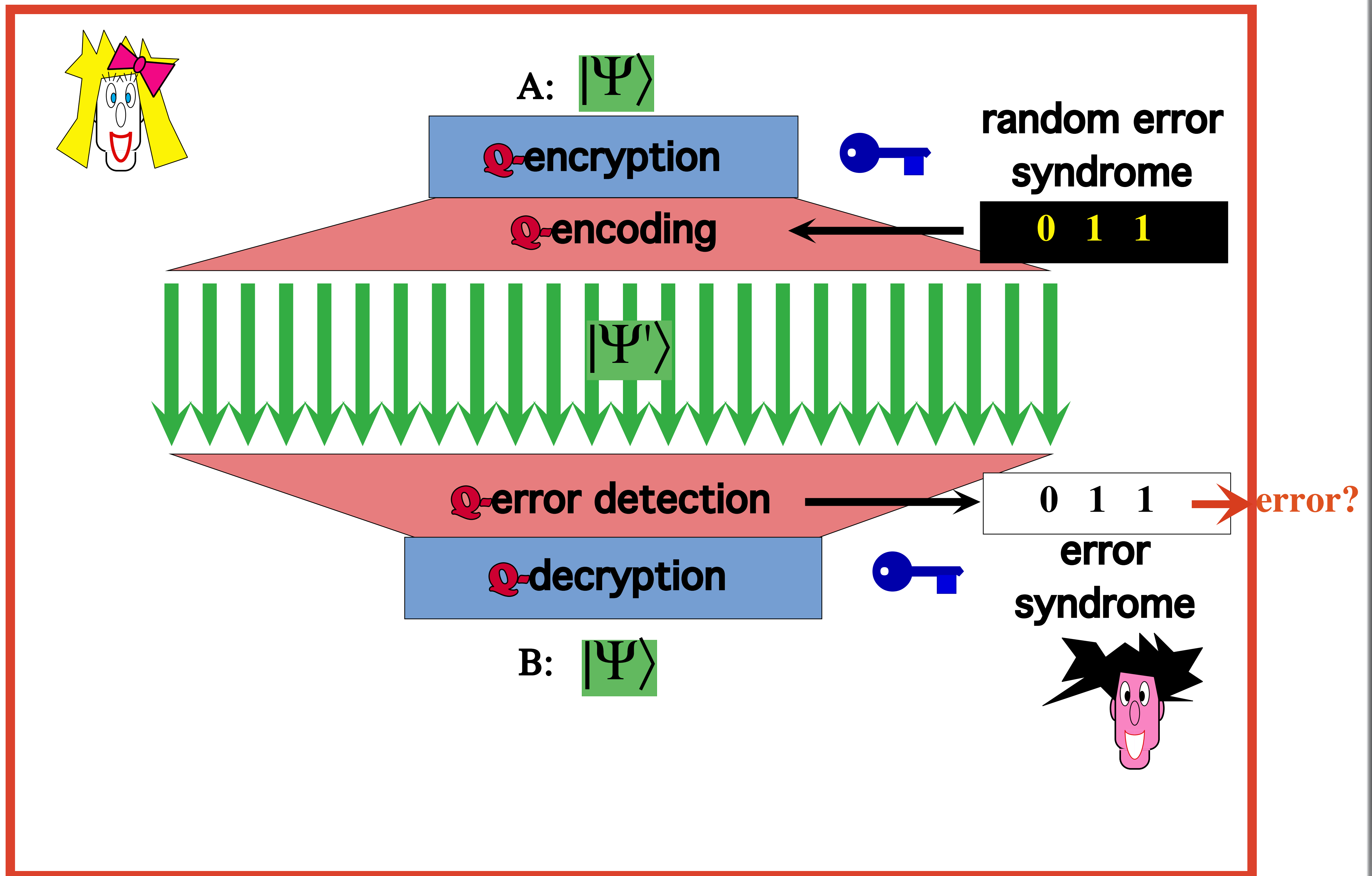
- one-time Authenticated Quantum pad is used to send message

• • • • •

(3.3C) One-time interactive Q-Authentication

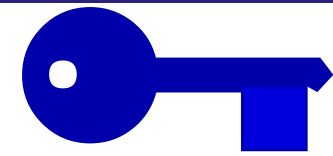


(3.1.3a) One-time Q-Authentication



Barnum-Crépeau-Gottesman-Smith-Tapp

(3.1.3a) One-time Q-Authentication

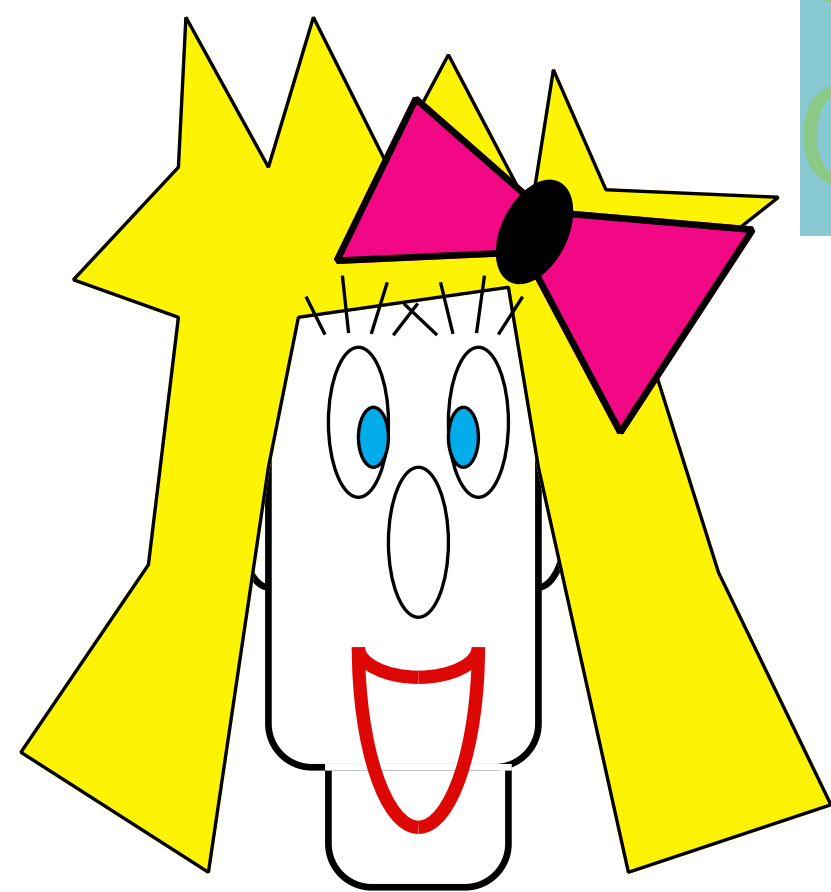


Classical key : one-time Q-authentication

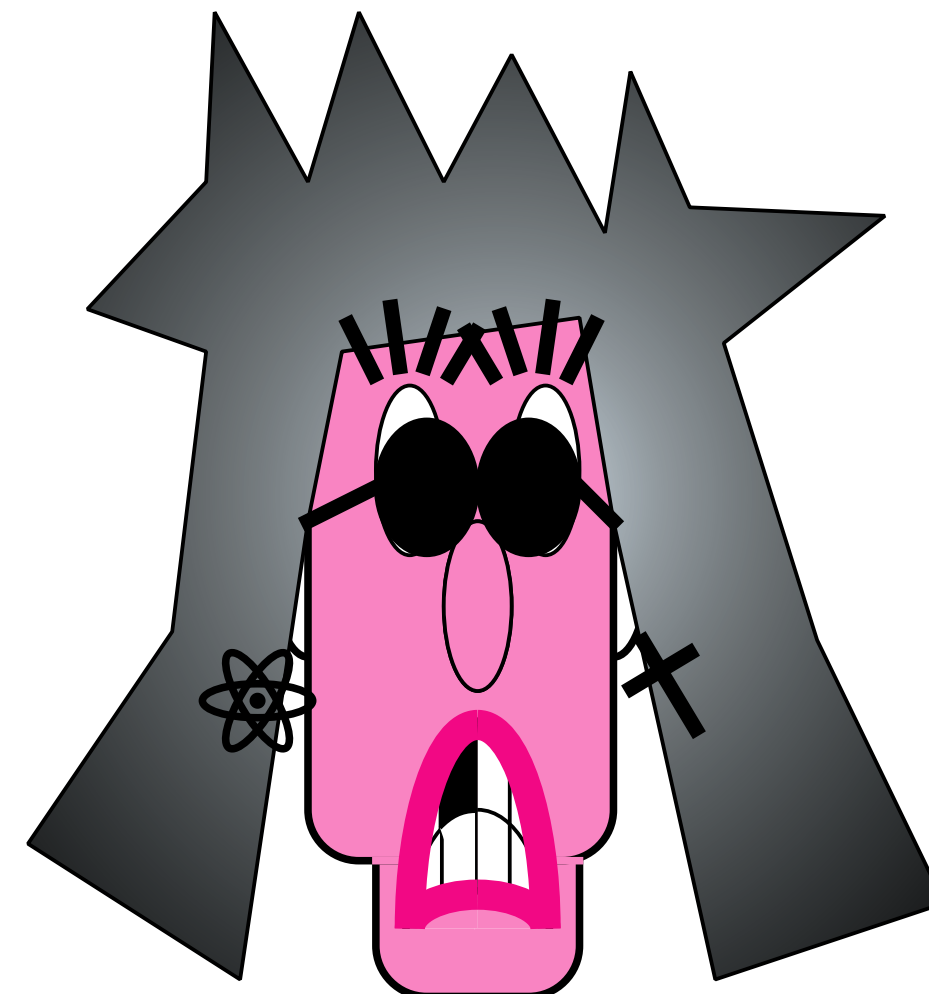
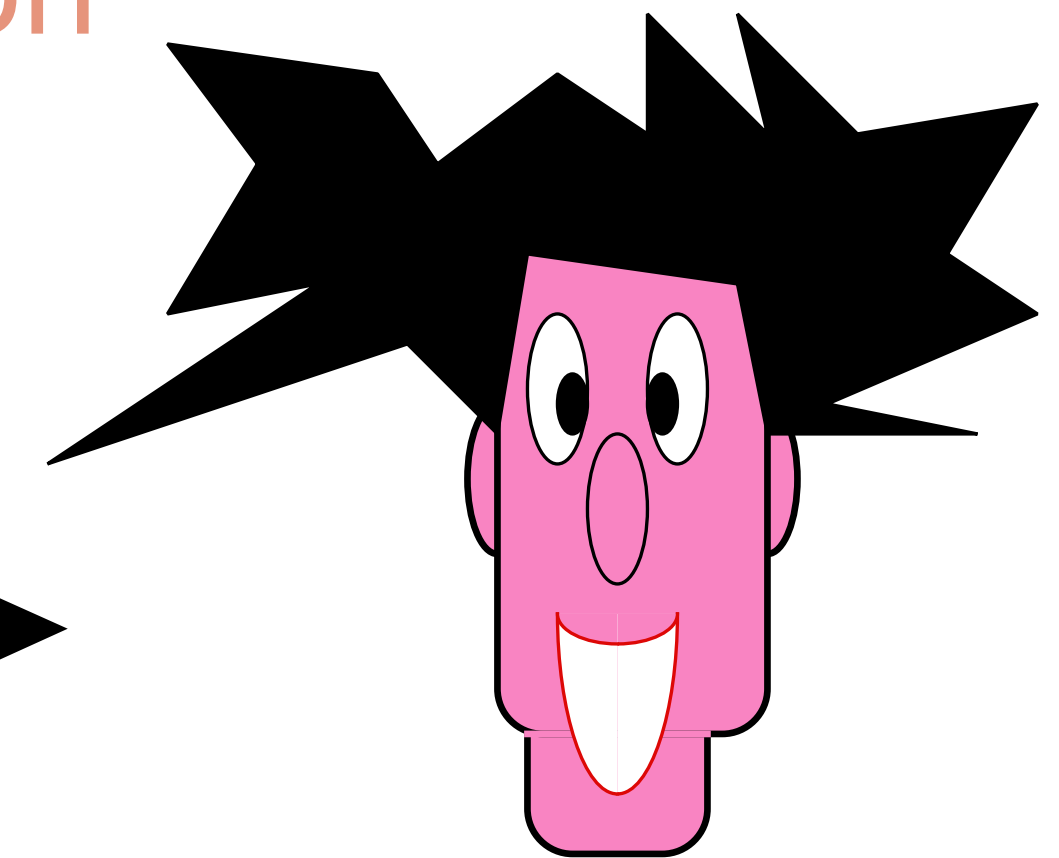
Quantum message+tag

Quantum key : Authenticated Q-teleportation

Classical message+tag

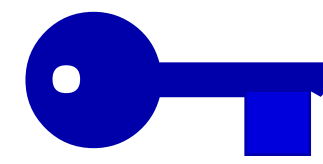


$|\Psi\rangle$



- public Q-error-correcting code

- secret key for encryption & syndrome



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

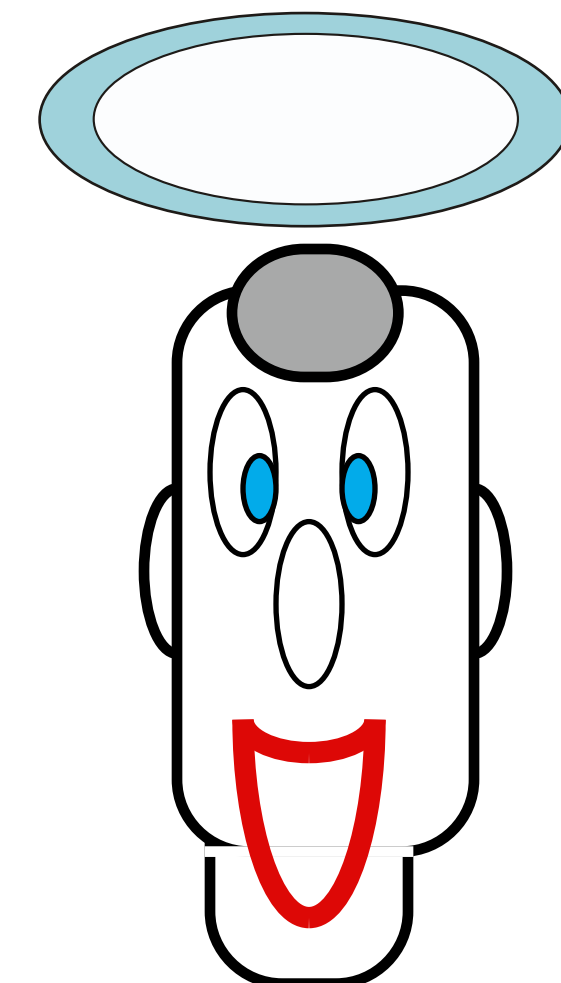
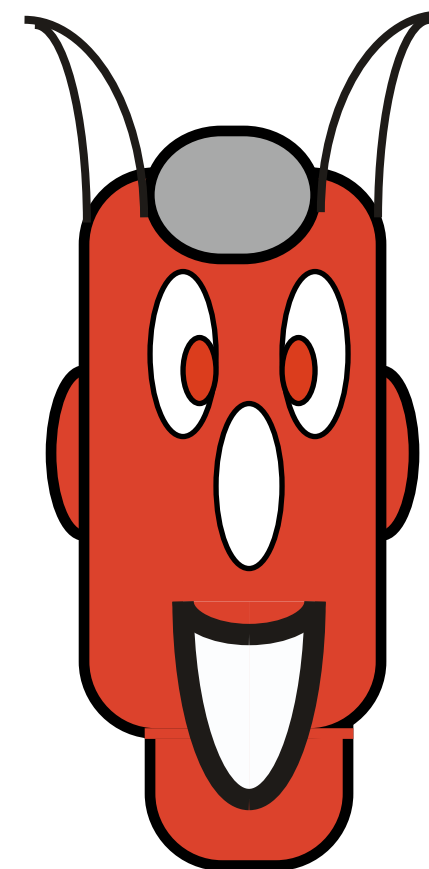
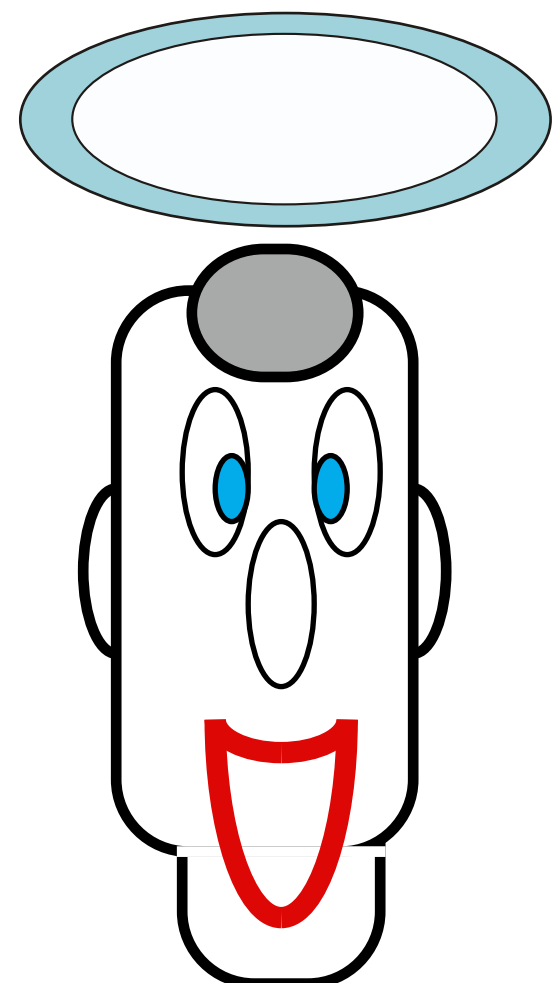
is

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 \mathcal{Q} -cryptosystem

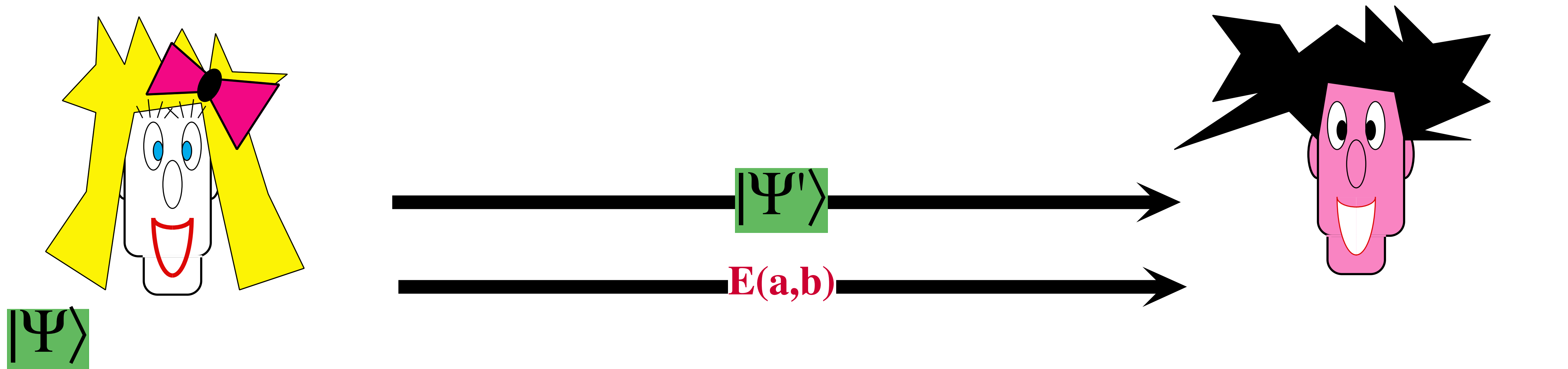
(3.2.2) Digital signature scheme : public-key \mathcal{Q} -Authentication
 \mathcal{Q} -digital signature scheme

(3.2.3) (trapdoor) one-way functions : \mathcal{Q} -cryptanalysis
(trapdoor) \mathcal{Q} -one-way functions



(3.2.1) Public-Key Q-Cryptosystem

Assuming Classical Public Key Cryptography

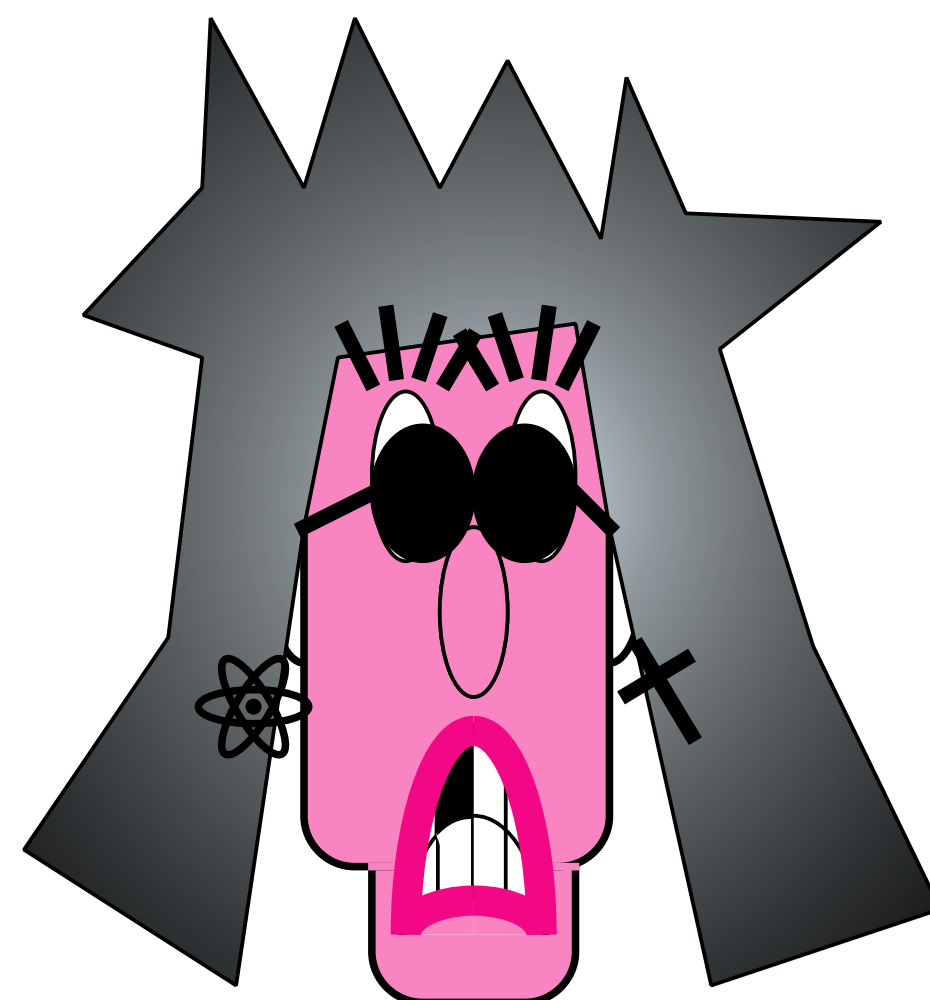


a, b random bits

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

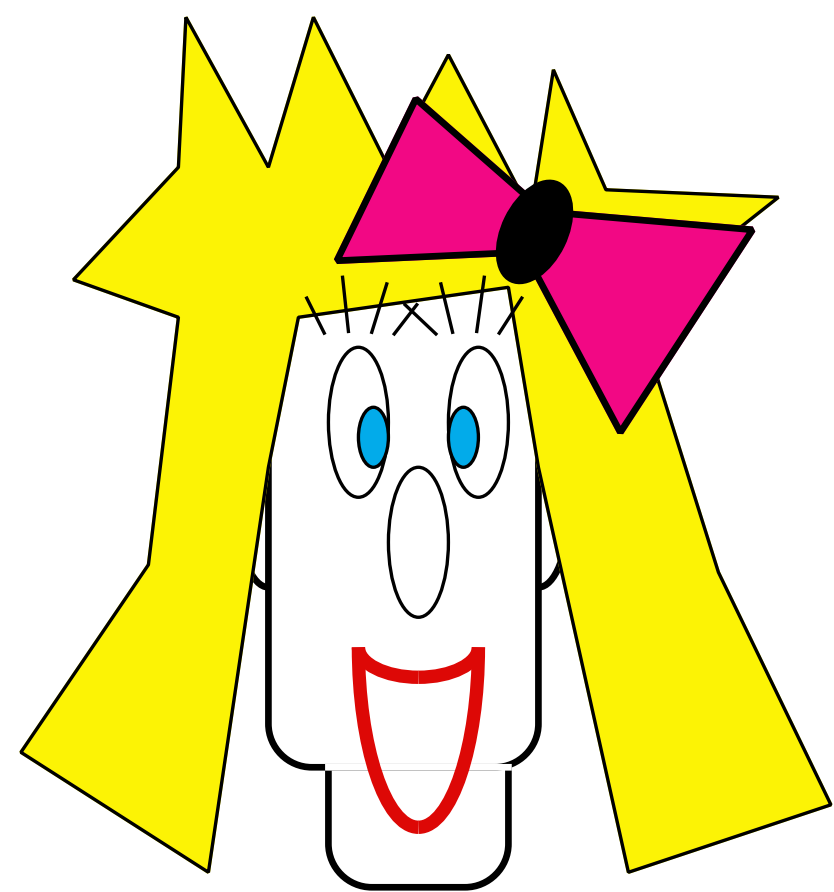
$$|\Psi'\rangle = (\sigma_x)^a (\sigma_z)^b |\Psi\rangle$$

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

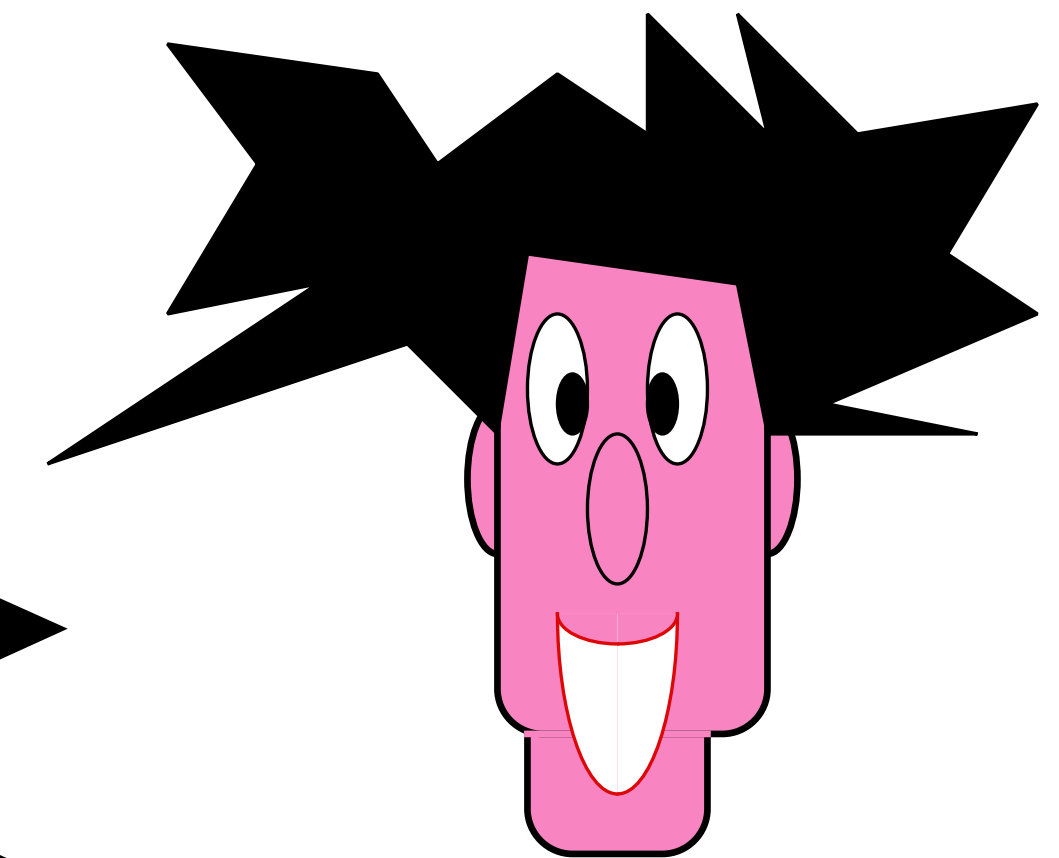
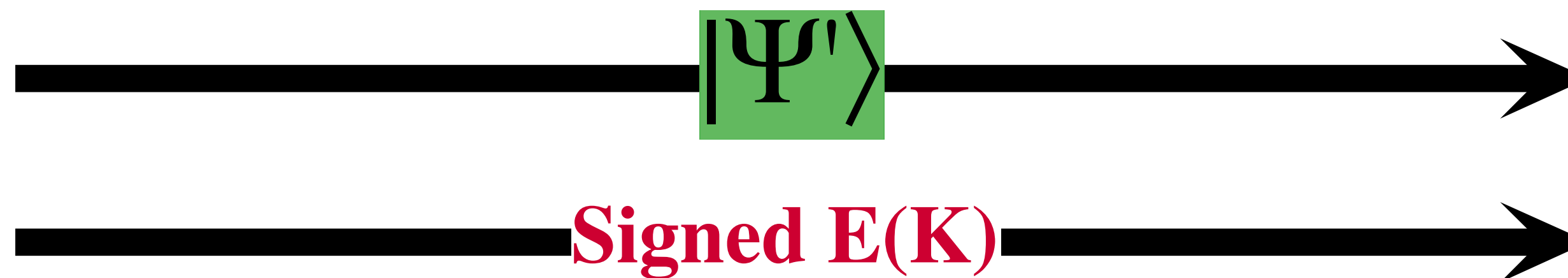


(3.2.2a) Public-Key Q-Authentication

Assuming Classical Public Key Cryptography
Assuming Classical Digital Signature



$|\Psi\rangle$

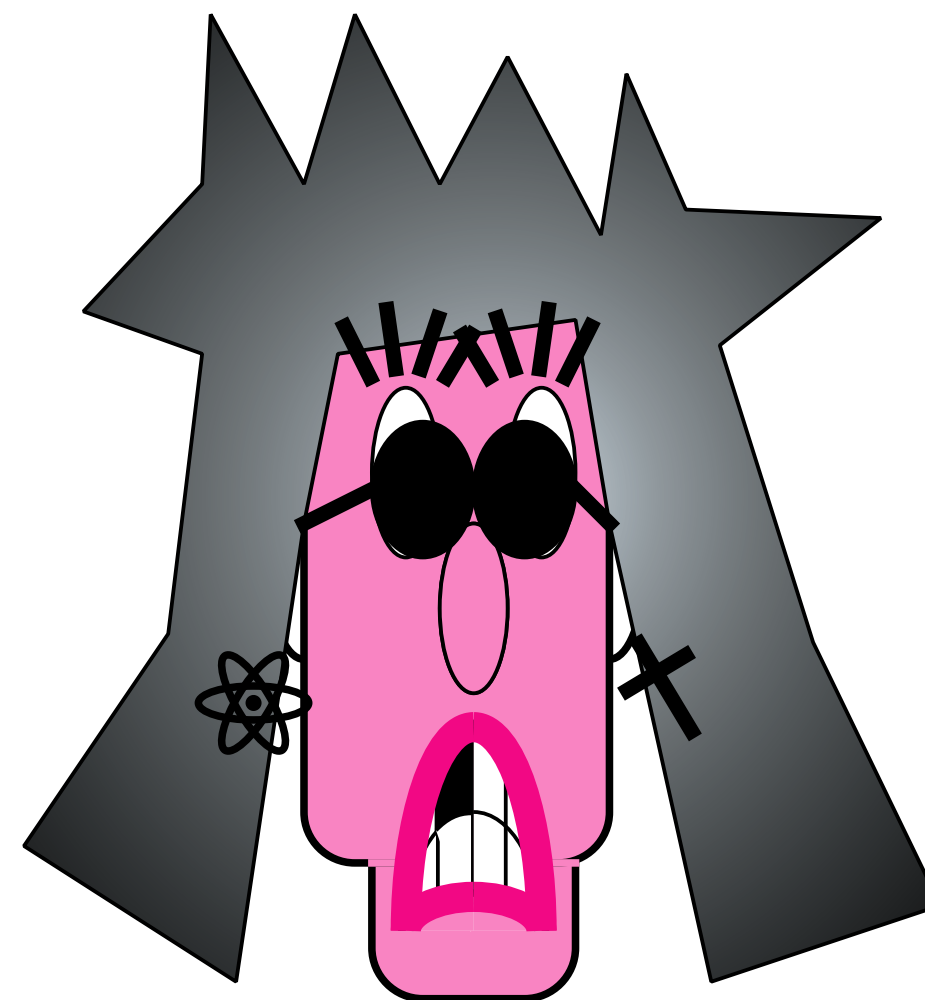


K random authentication key

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

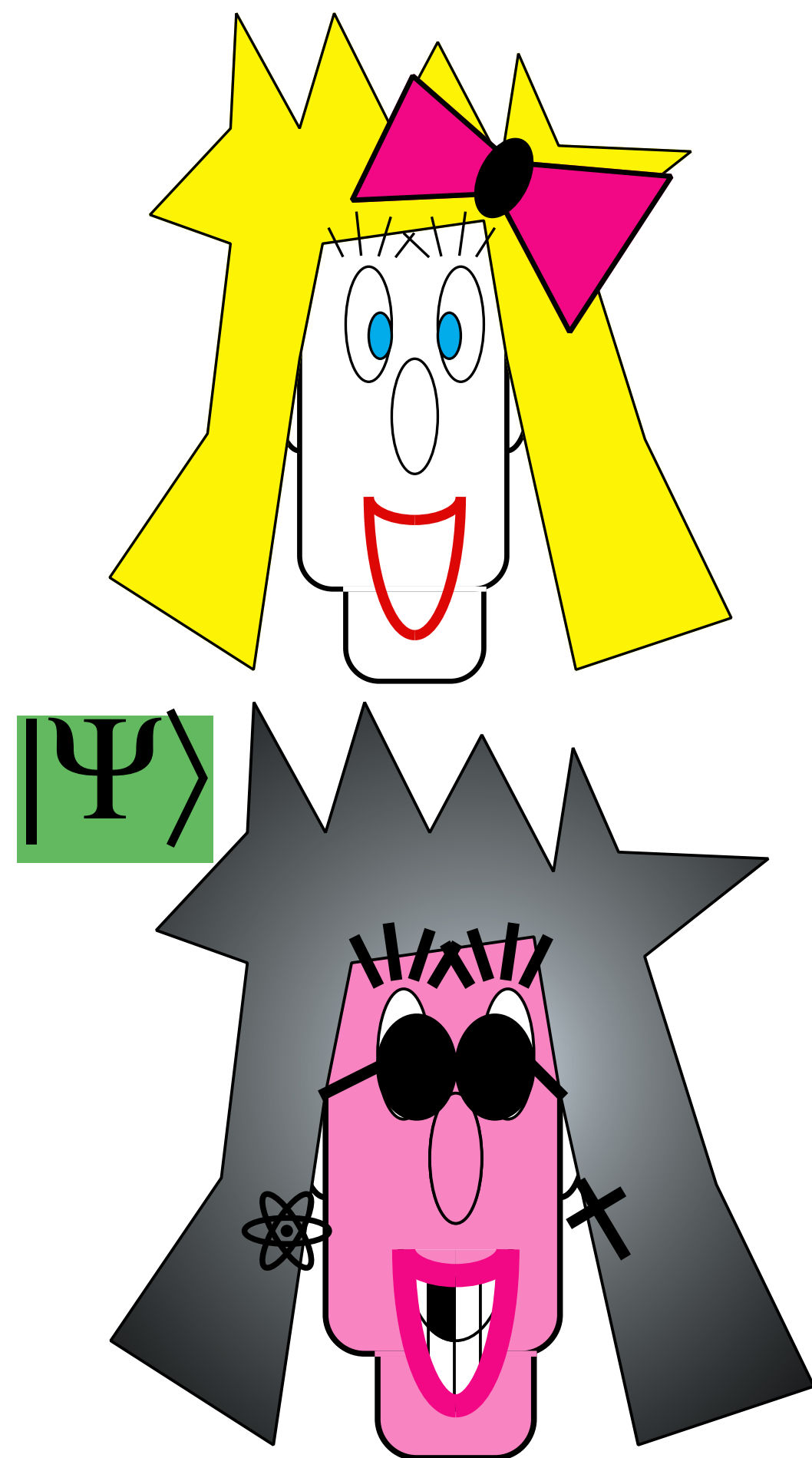
verify signed $E(K)$
 $K := D(E(K))$

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

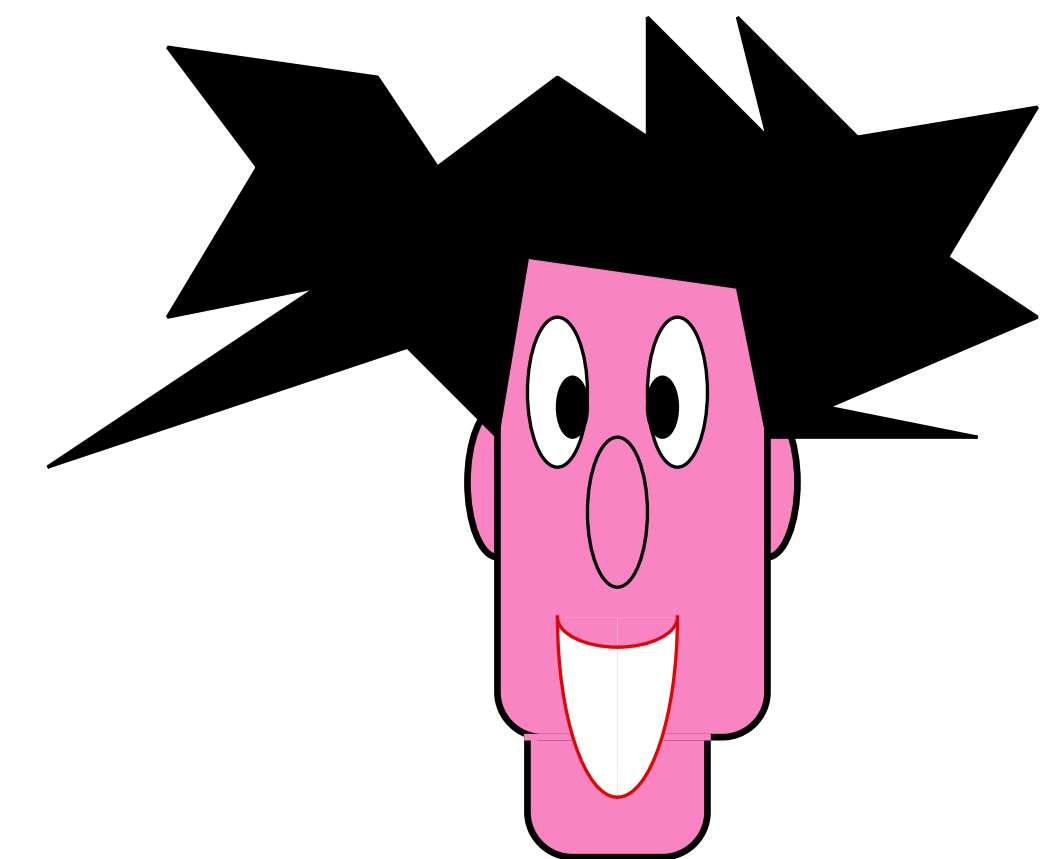


(3.2.2b) Q-Digital Signature Scheme

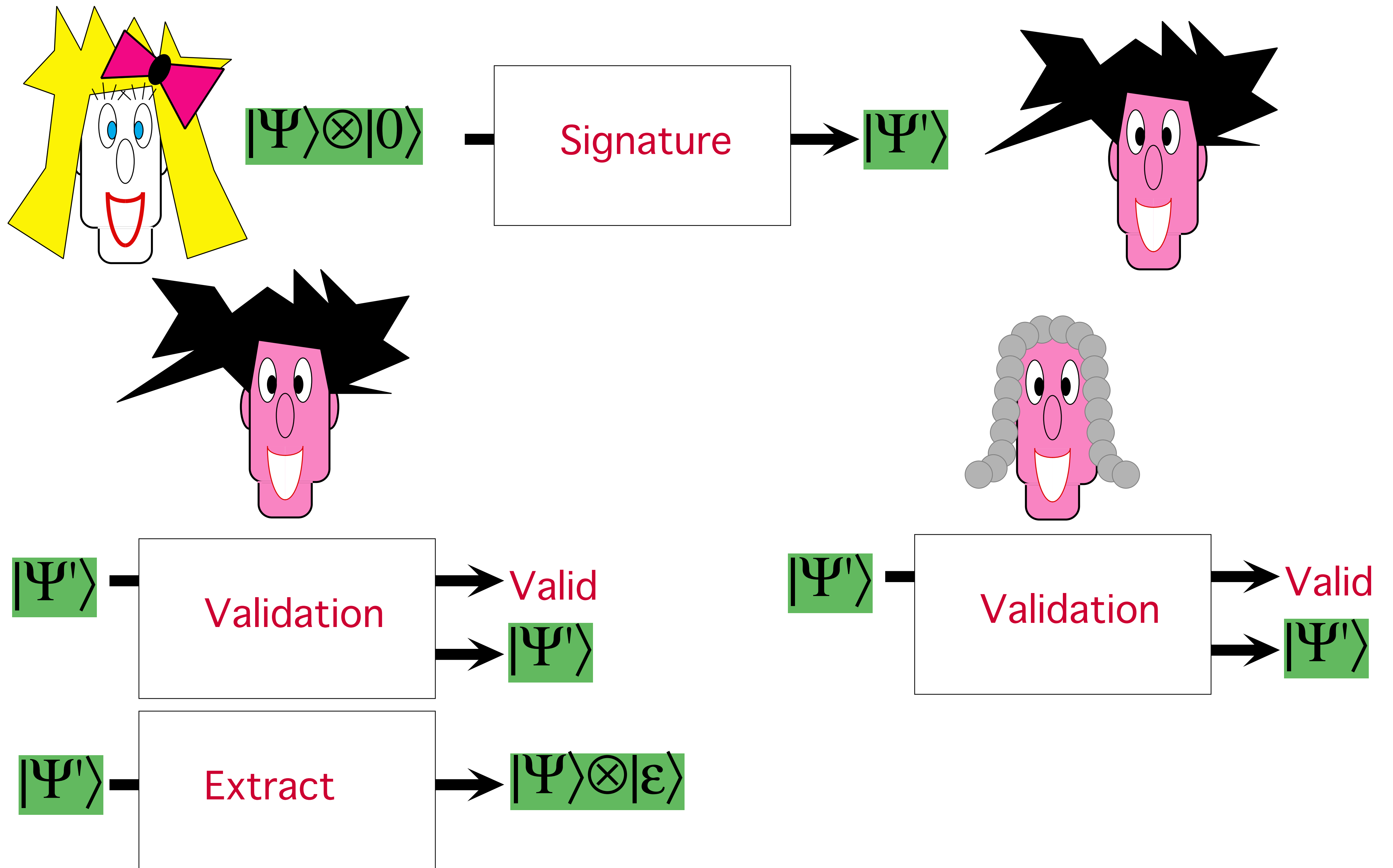
Assuming Classical Public Key Cryptography
Assuming Classical Digital Signature



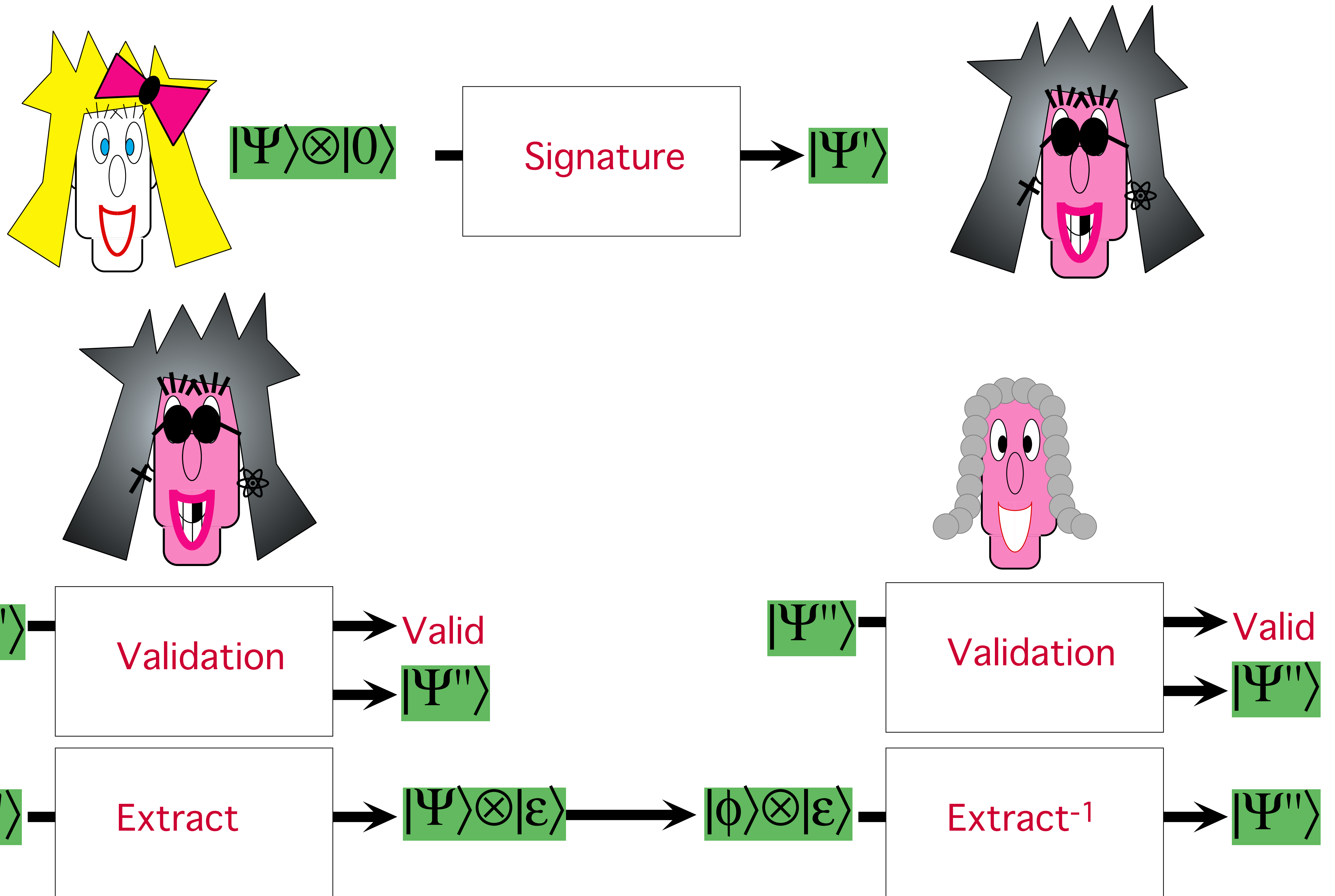
IMPOSSIBLE



(3.2.2b) Q-Digital Signature Scheme



(3.2.2b) Q-Digital Signature Scheme



Quantum one-time Authentication

Claude Crépeau

School of Computer Science
McGill University

