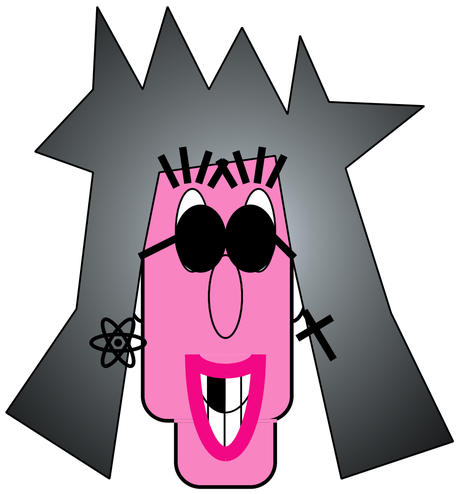
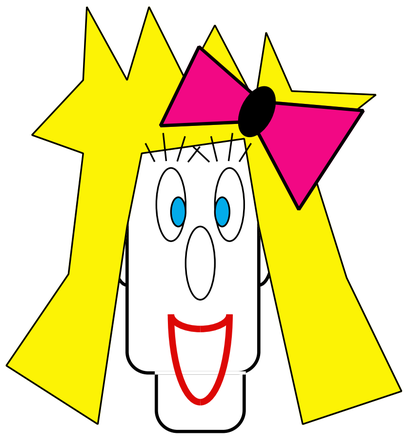
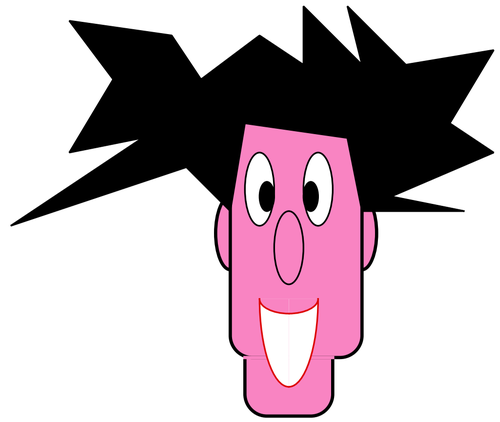
(3.1.2) One-Time-Pad





|Will you marry me ?⟩

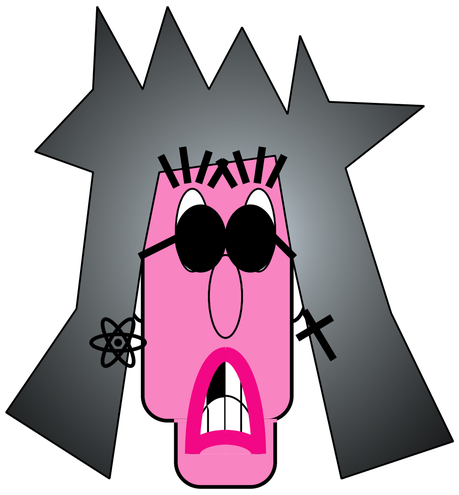


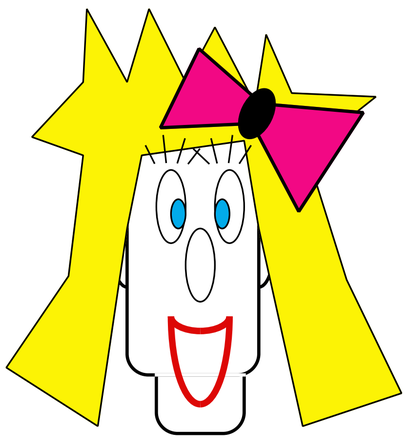
|Divorce your wife first !⟩

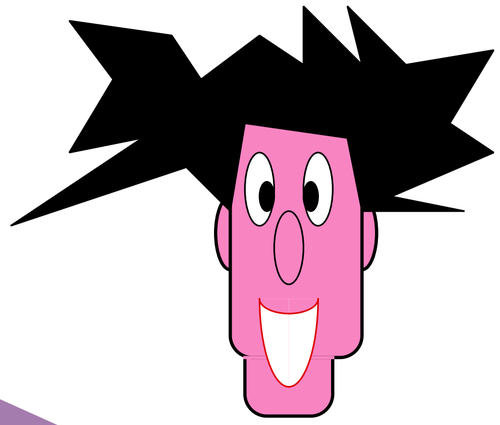
|The papers are in the mail...⟩

|OK, I will !⟩

(3.1.2Q) One-time Q-pad







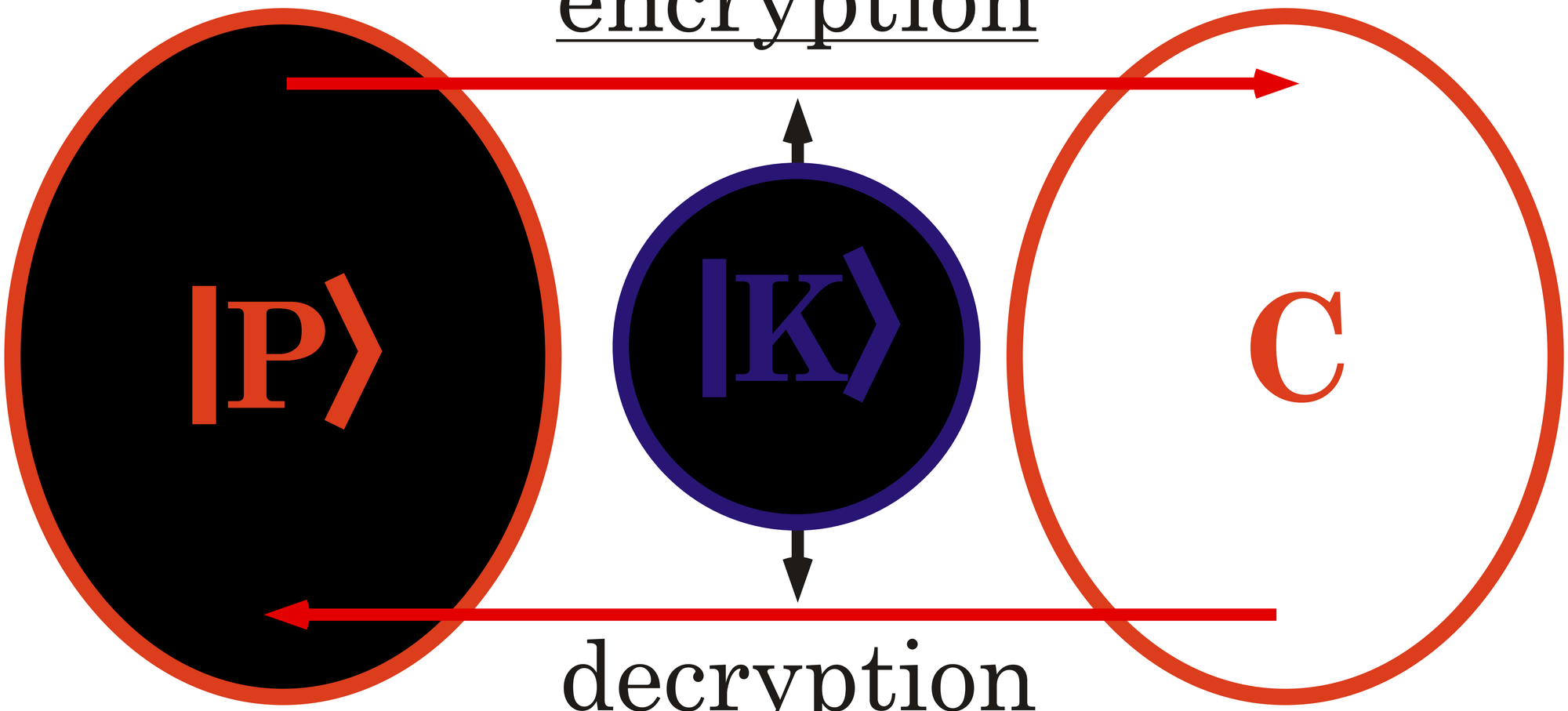
8RdewtU5qkLa$es!T9@

I(D%eXhDqIiykl#2cV7dEwnMs

H&fs@tyHvFGhaOKpTrGbl.Z/rUih*

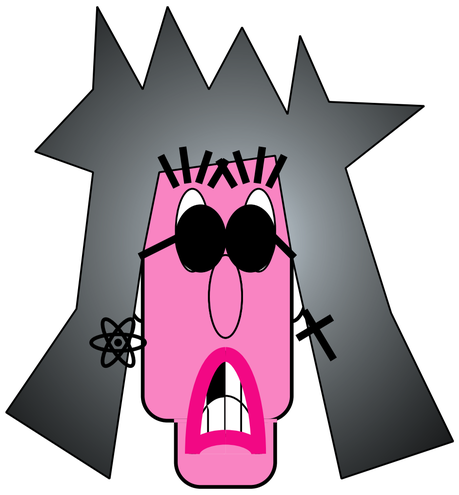
B7B3tdsjUila

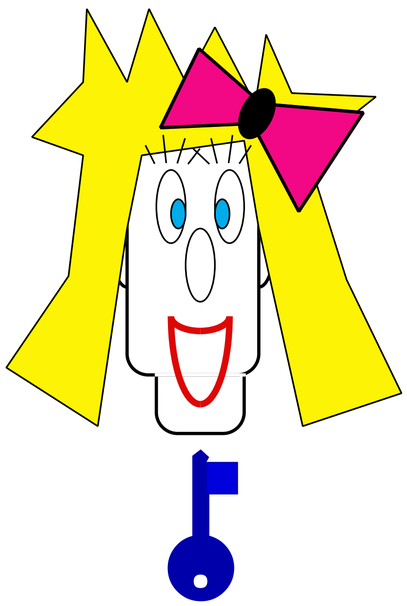
symmetric encryption of Quantum messages



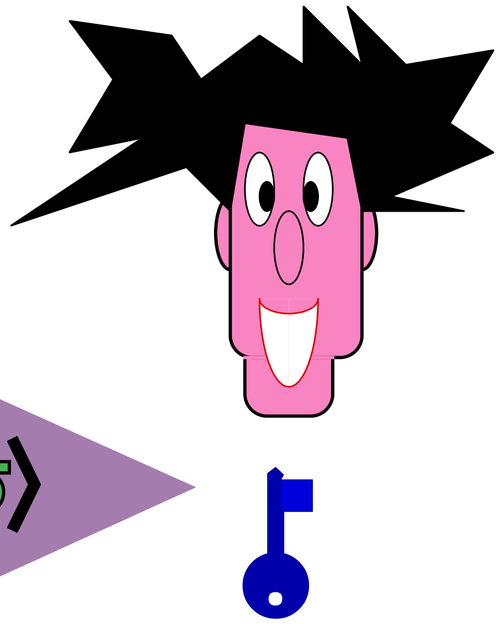
Information Theoretical Security

(3.1.2C) Vernam Ω-cipher





|8PδεωτY5θκΛαΞεσ!T9≅⟩

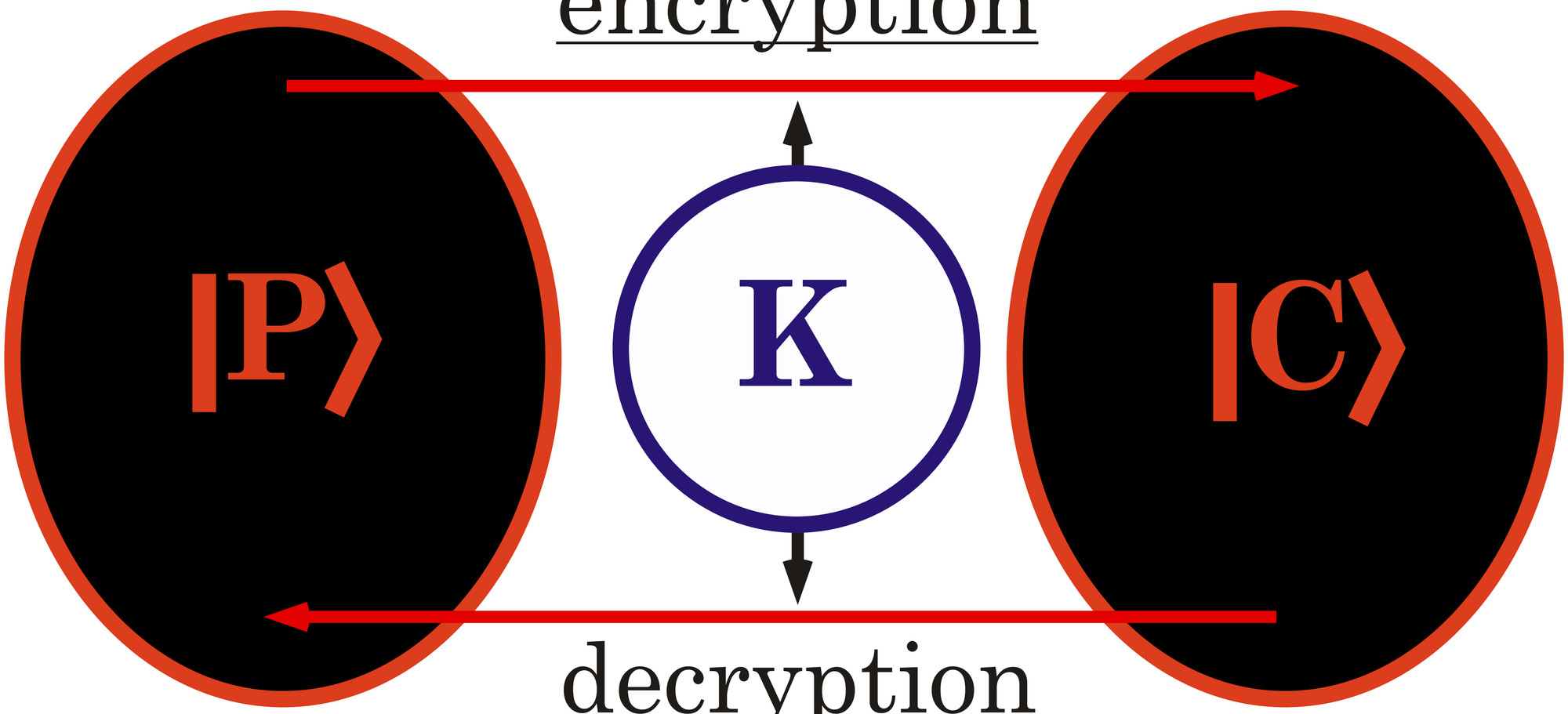


|I(Δ%εΞηΔθIιψκλ#2χς7δEωνMσ⟩

|H&φσ≅τψϖΦηαOKπTρΓβλ.Z/ρYιη*⟩

|B7B3τδσφYιλα⟩

symmetric encryption of Quantum messages

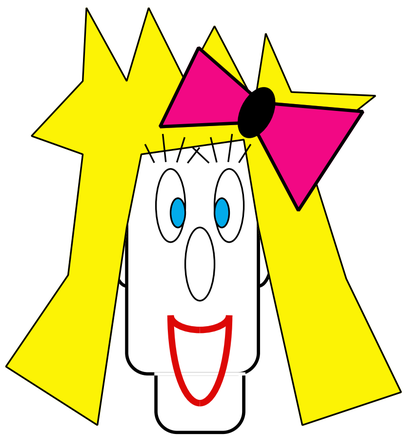


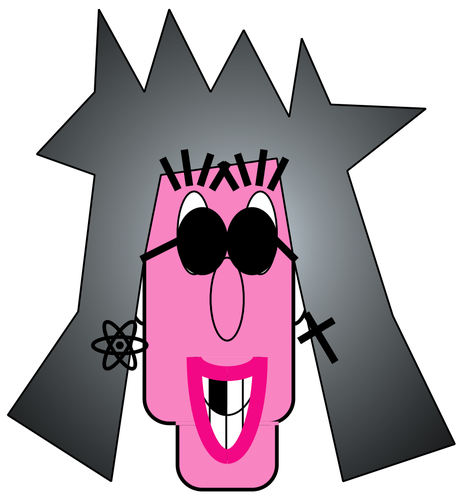
Information Theoretical Security

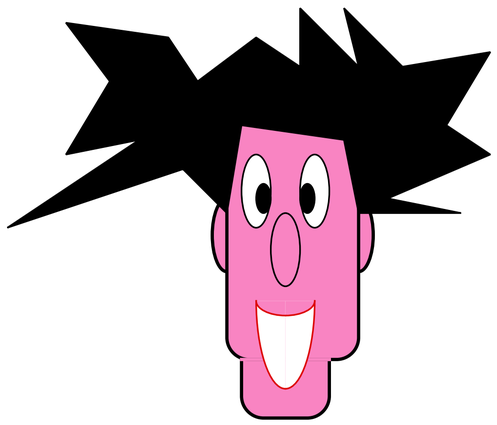
(3.1.2) One-time pad

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

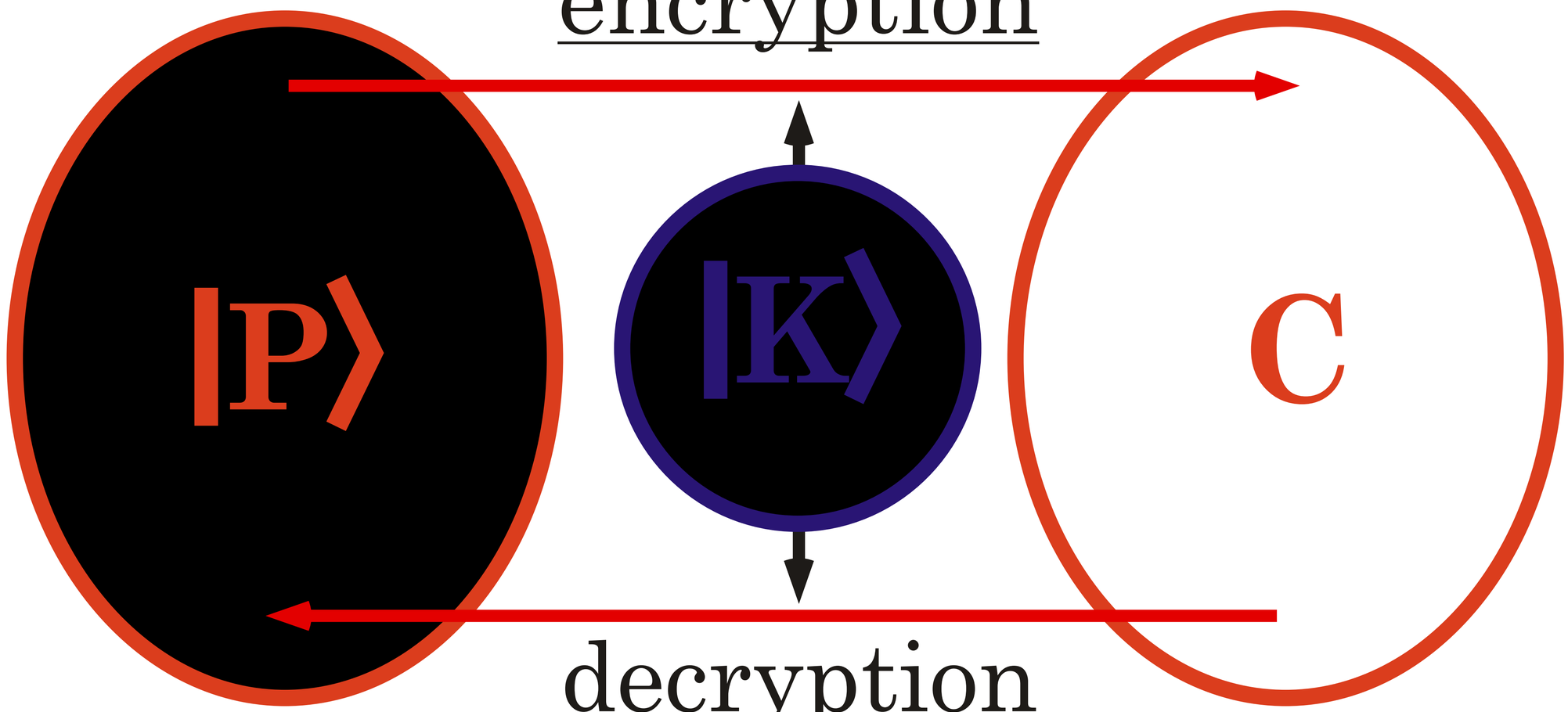
Quantum key : one-time **Q**-pad (**Q**-teleportation) (BBCJPW)
Classical Ciphertext





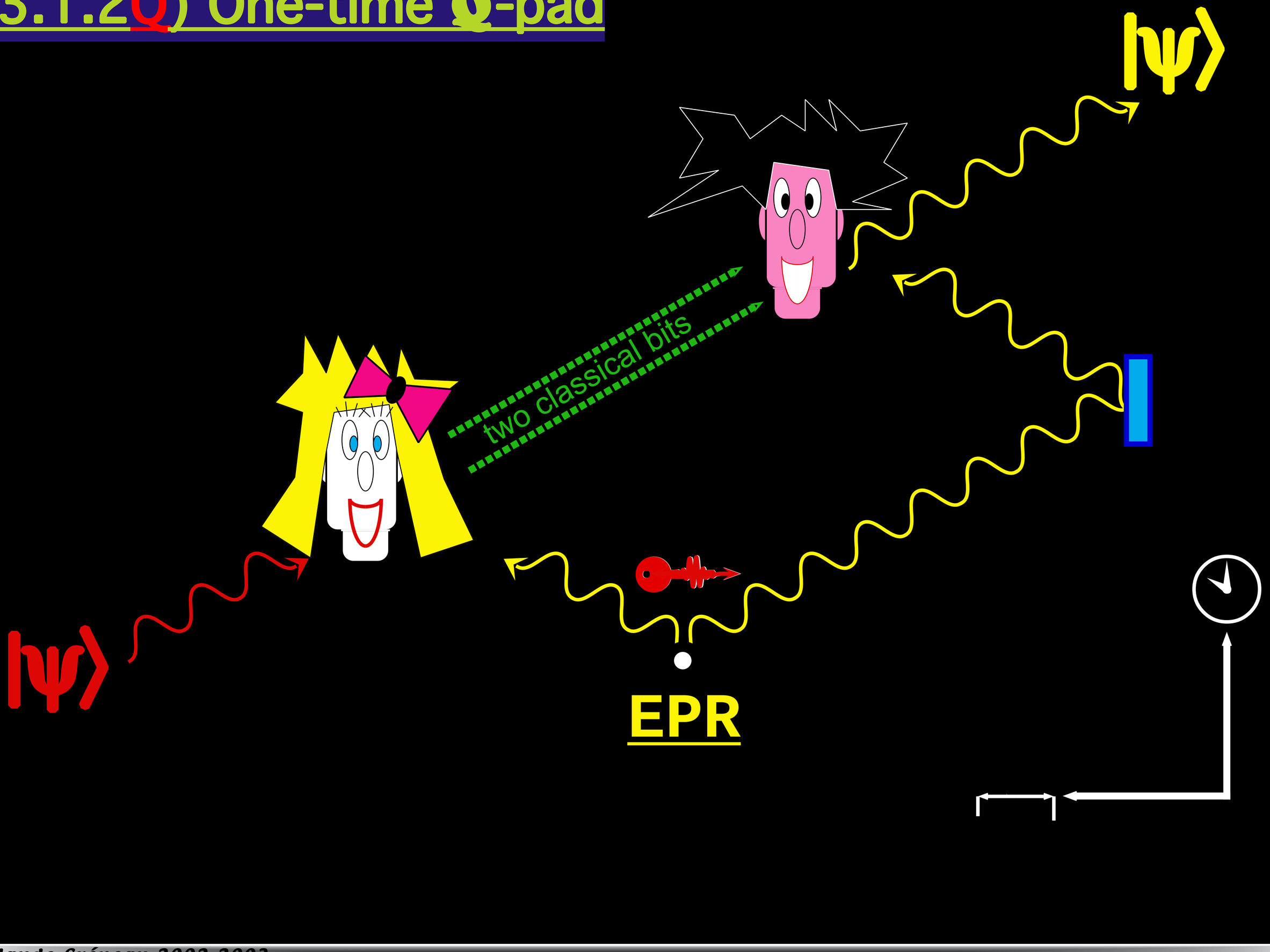


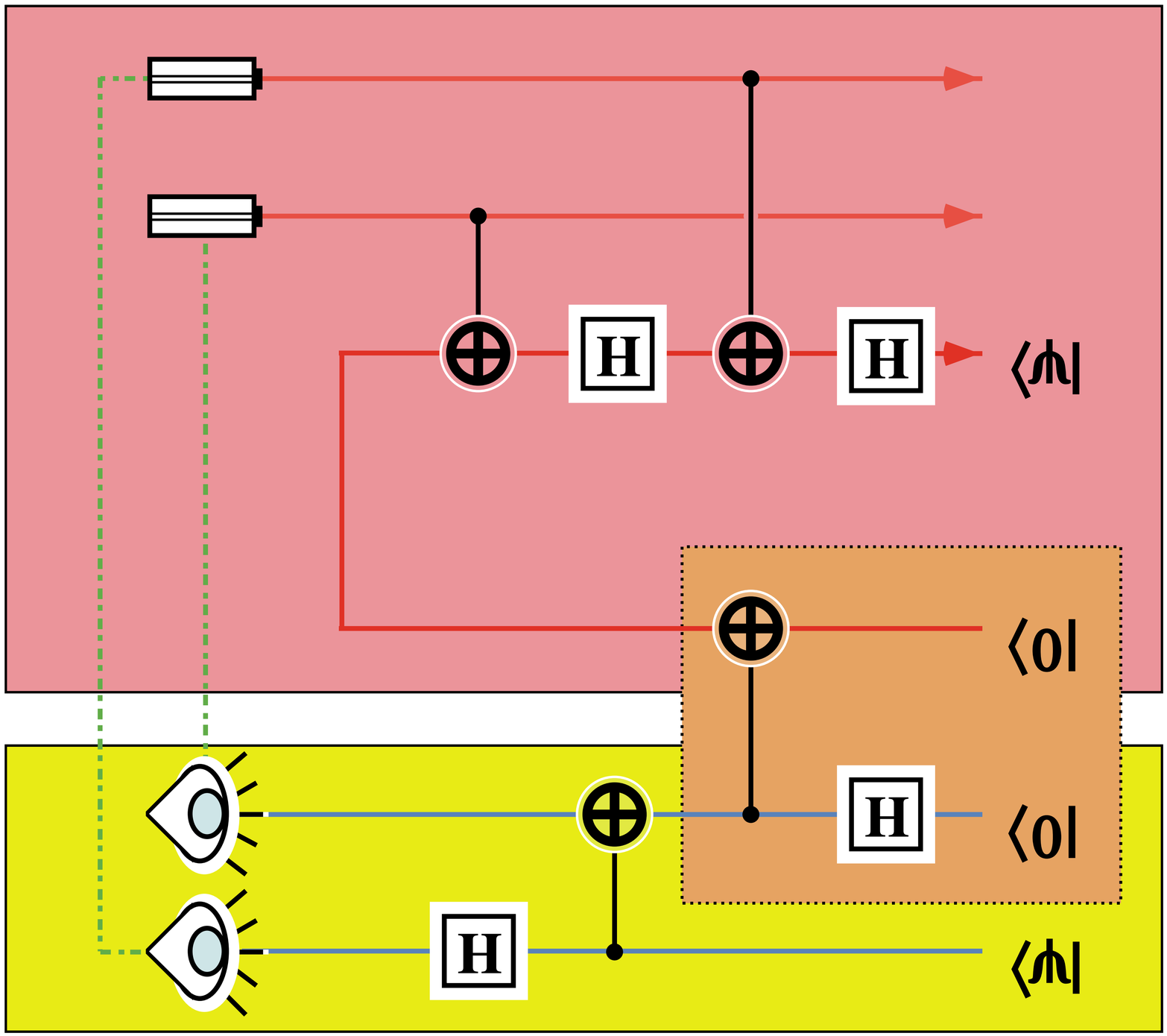
symmetric encryption of Quantum messages

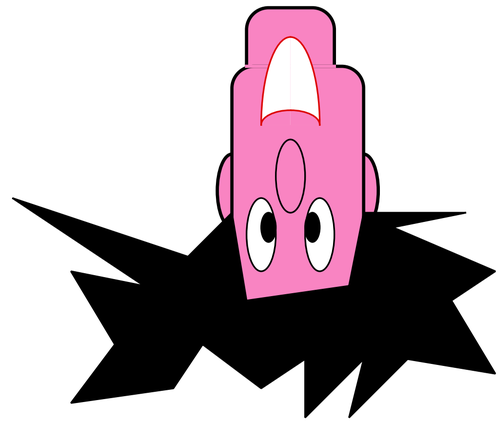


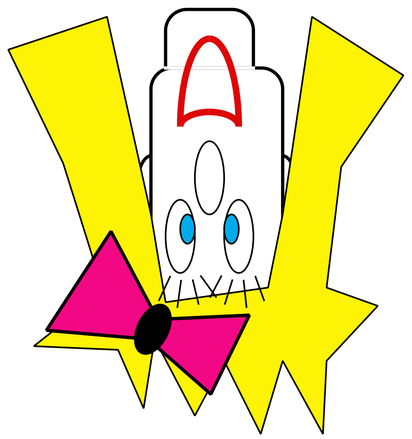
Information Theoretical Security

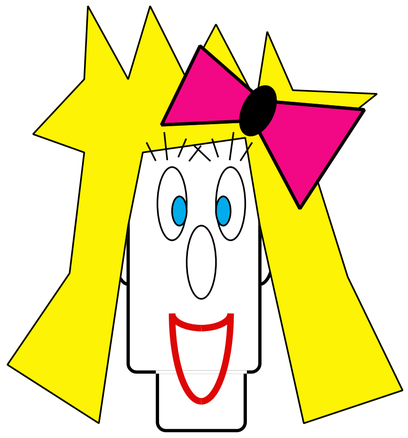
(3.1.2Q) One-time Q-pad

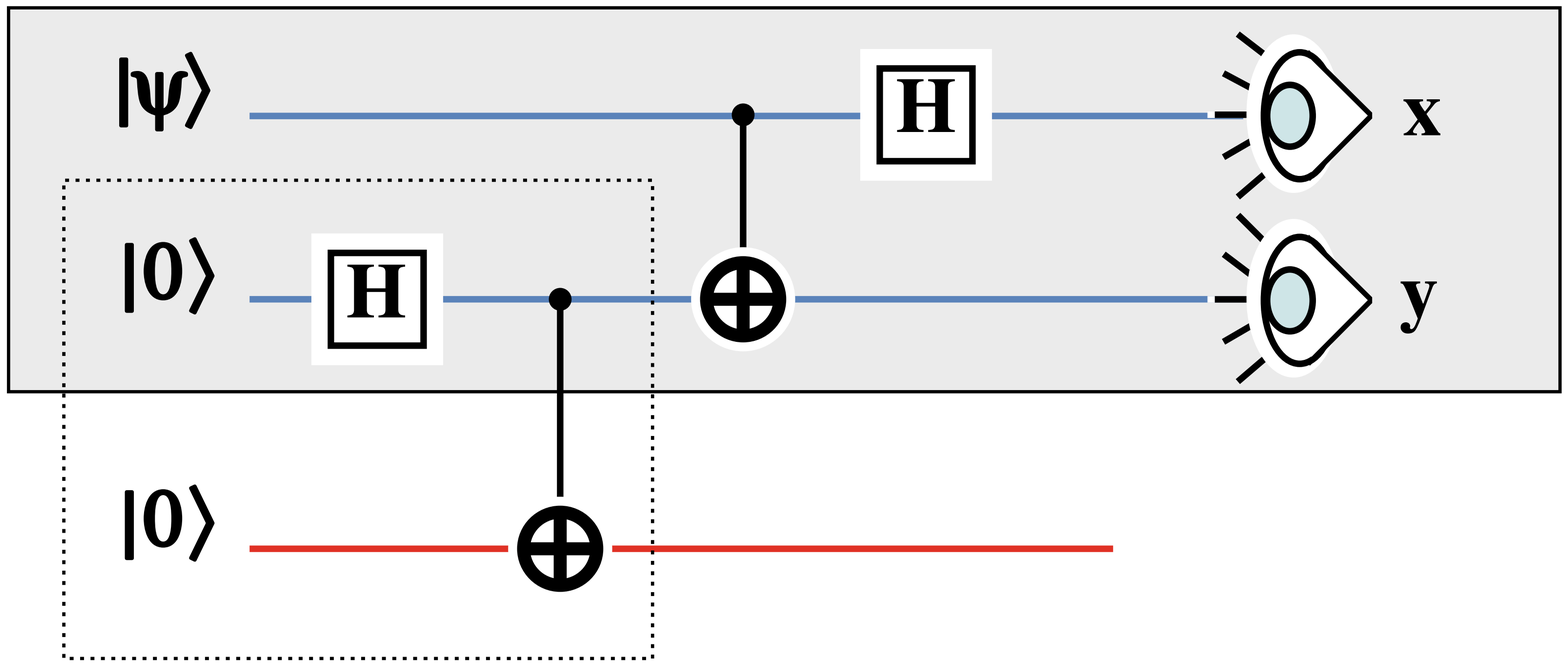



H
H
|ψ⟩
|0⟩
|0⟩
H
H
|ψ⟩









$|\psi\rangle|0\rangle|0\rangle$

H $|\psi\rangle(|0\rangle+|1\rangle)|0\rangle$

⊕ $|\psi\rangle(|0\rangle|0\rangle+|1\rangle|1\rangle)$

$(\alpha|0\rangle+\beta|1\rangle)(|00\rangle+|11\rangle)$

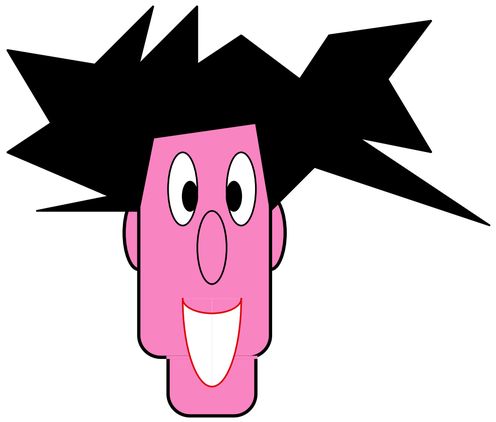
$\alpha|0\rangle|00\rangle+\alpha|0\rangle|11\rangle+\beta|1\rangle|00\rangle+\beta|1\rangle|11\rangle$

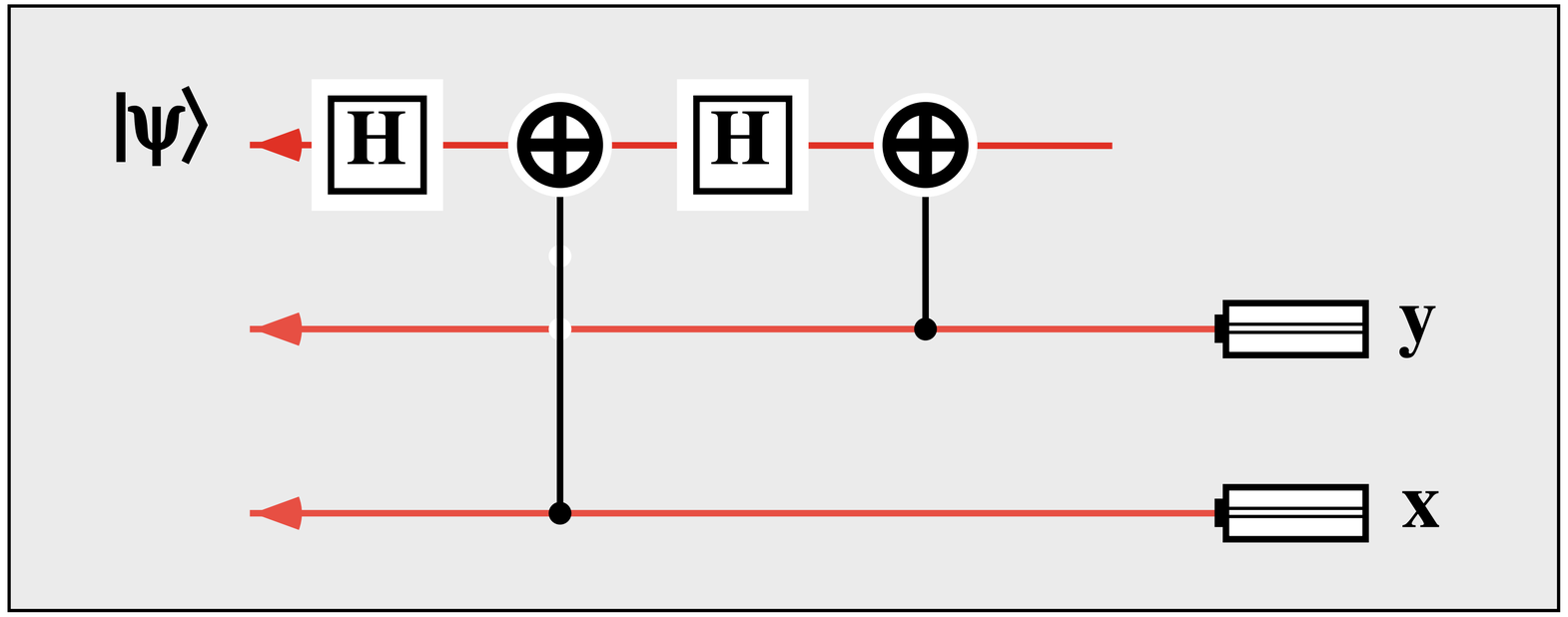
⊕ $\alpha|0\rangle|00\rangle+\alpha|0\rangle|11\rangle+\beta|1\rangle|10\rangle+\beta|1\rangle|01\rangle$

H $\alpha(|0\rangle+|1\rangle)|00\rangle+\alpha(|0\rangle+|1\rangle)|11\rangle+\beta(|0\rangle-|1\rangle)|10\rangle+\beta(|0\rangle-|1\rangle)|01\rangle$

$|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle+\beta|0\rangle)+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(\alpha|1\rangle-\beta|0\rangle)$

$|xy\rangle(\alpha|y\rangle+(-1)^{x}\beta|\neg y\rangle)$





$|xy\rangle(\alpha|y\rangle+(-1)^{x}\beta|\neg y\rangle)$

$\oplus$ $|xy\rangle(\alpha|0\rangle+(-1)^{x}\beta|1\rangle)$

H $|xy\rangle(\alpha(|0\rangle+|1\rangle)+(-1)^{x}\beta(|0\rangle-|1\rangle))$

$\oplus$ $|xy\rangle(\alpha(|x\rangle+|\neg x\rangle)+(-1)^{x}\beta(|x\rangle-|\neg x\rangle))$

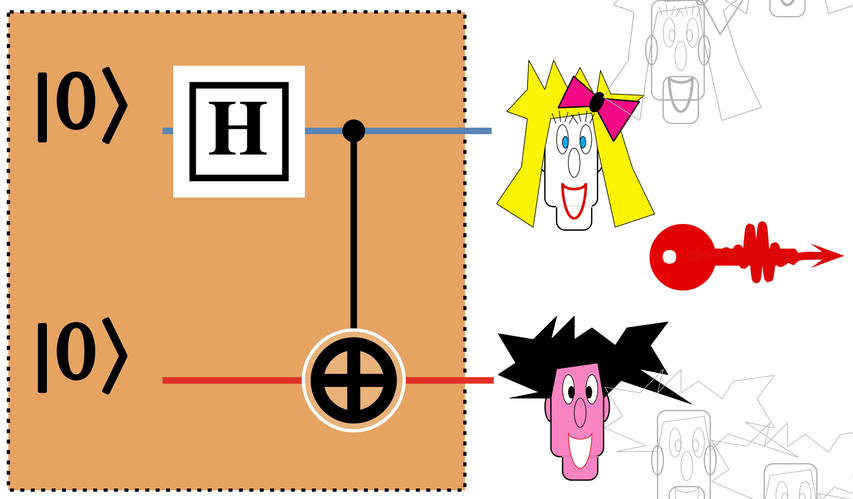
H $|xy\rangle(\alpha([|0\rangle+(-1)^{x}|1\rangle]+[|0\rangle+(-1)^{\neg x}|1\rangle])$

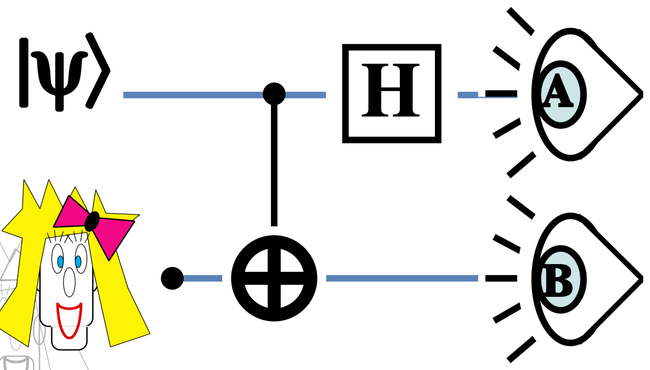
$+(-1)^{x}\beta([|0\rangle+(-1)^{x}|1\rangle]-[|0\rangle+(-1)^{\neg x}|1\rangle]))$

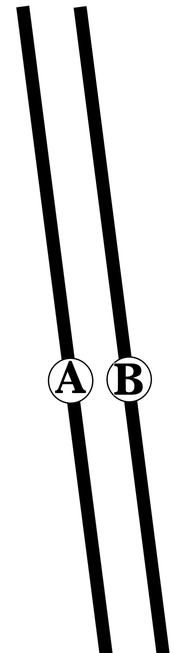
$|xy\rangle(\alpha|0\rangle+\beta|1\rangle)$

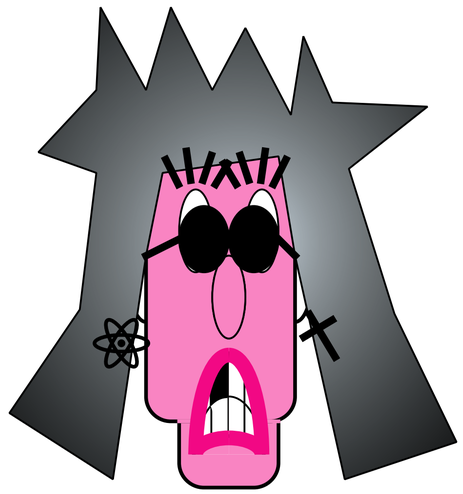
$|xy\rangle|\psi\rangle$

(3.1.2Q)
One-time Q-pad

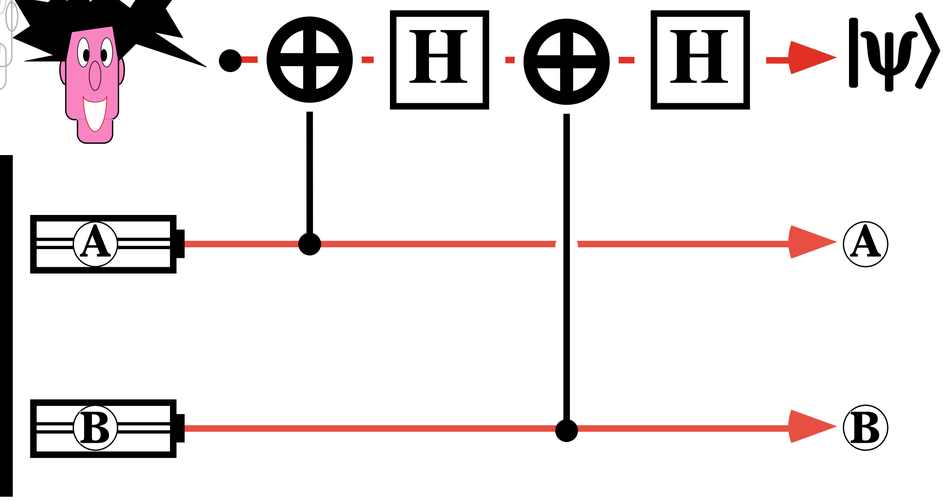








$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



¼ : $|\Psi\rangle$

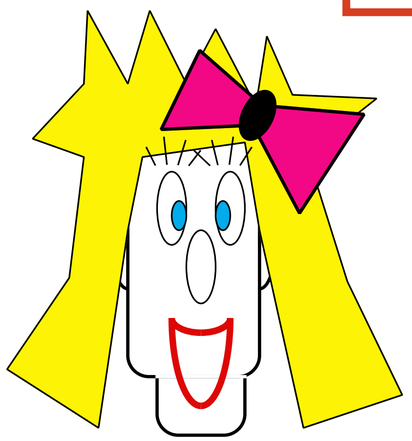
¼ : $\sigma_x|\Psi\rangle$

¼ : $\sigma_z|\Psi\rangle$

¼ : $\sigma_x\sigma_z|\Psi\rangle$

(3.1.2Q) One-time Q-pad

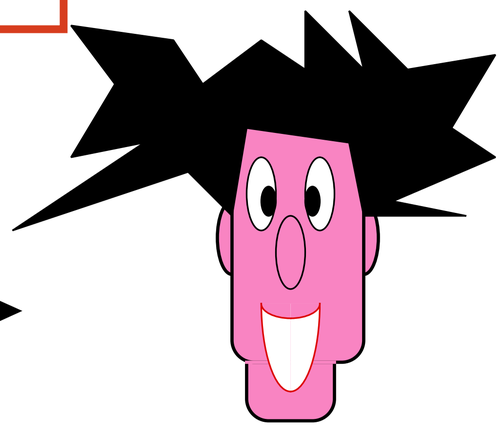
Quantum key : one-time Q-pad
Classical Ciphertext

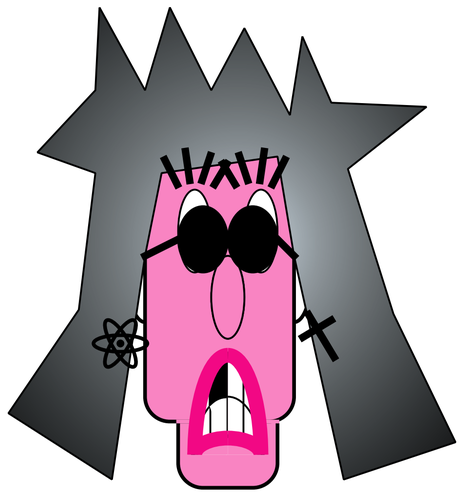


$|\Psi\rangle$

Ⓐ Ⓑ

two random bits

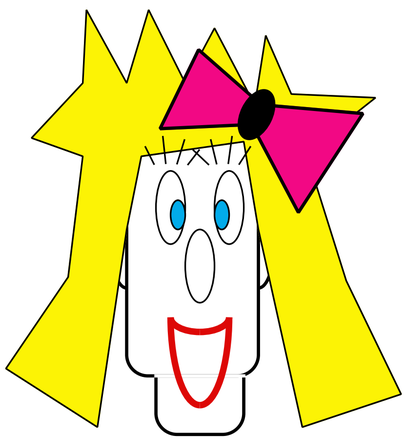


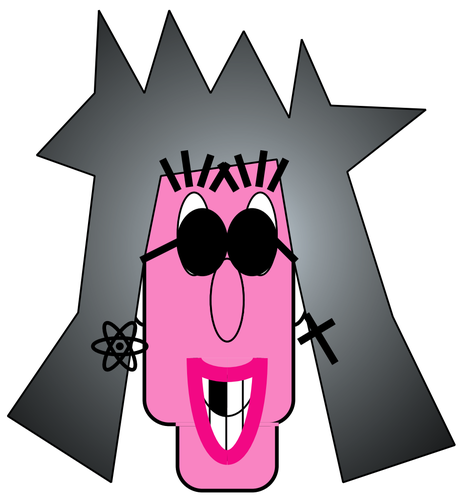


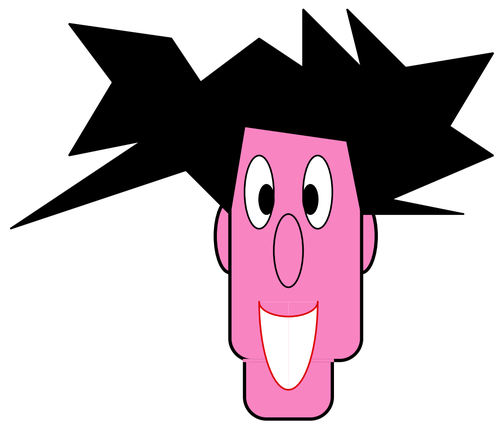
(3.1.2) One-time pad

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

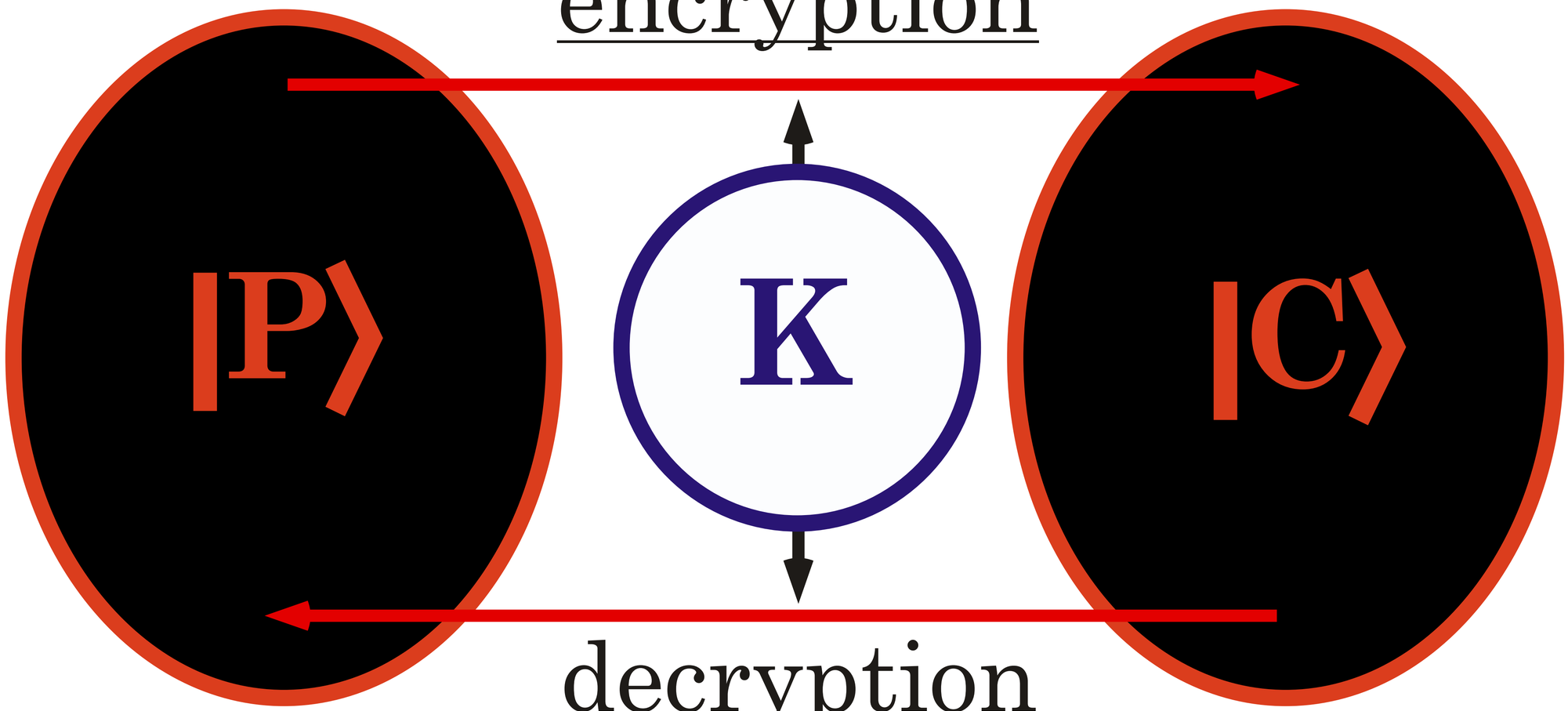
Quantum key : one-time Q-pad (BBCJPW)
Classical Ciphertext







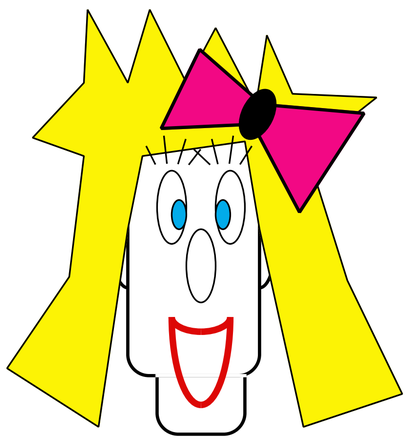
symmetric encryption of Quantum messages



Information Theoretical Security

(3.1.2C) Vernam Q-cipher

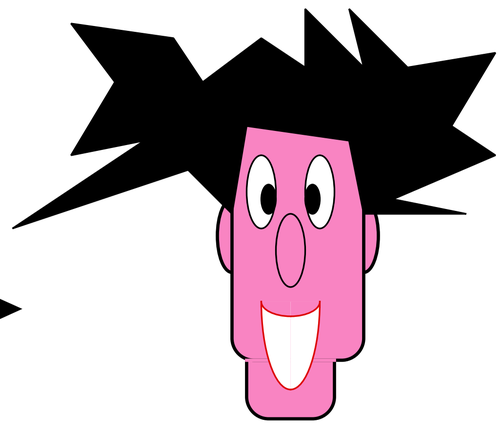
Classical key : Vernam Q-cipher
Quantum Ciphertext
Quantum key : one-time Q-pad
Classical Ciphertext

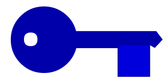


$|\Psi\rangle$

$|\Psi'\rangle$

¼ : $|\Psi\rangle$
¼ : $\sigma_x|\Psi\rangle$
¼ : $\sigma_z|\Psi\rangle$
¼ : $\sigma_x\sigma_z|\Psi\rangle$

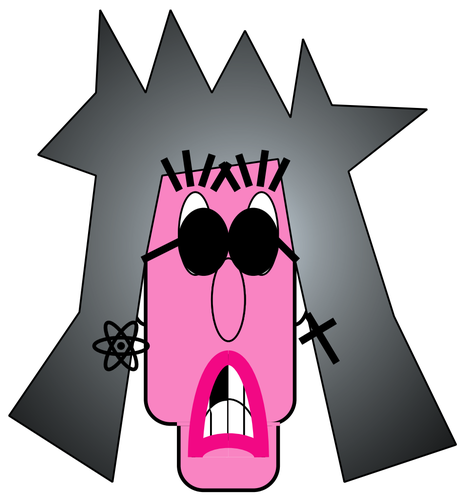




a,b random bit key

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

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



a,b random bit key

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

Theorems

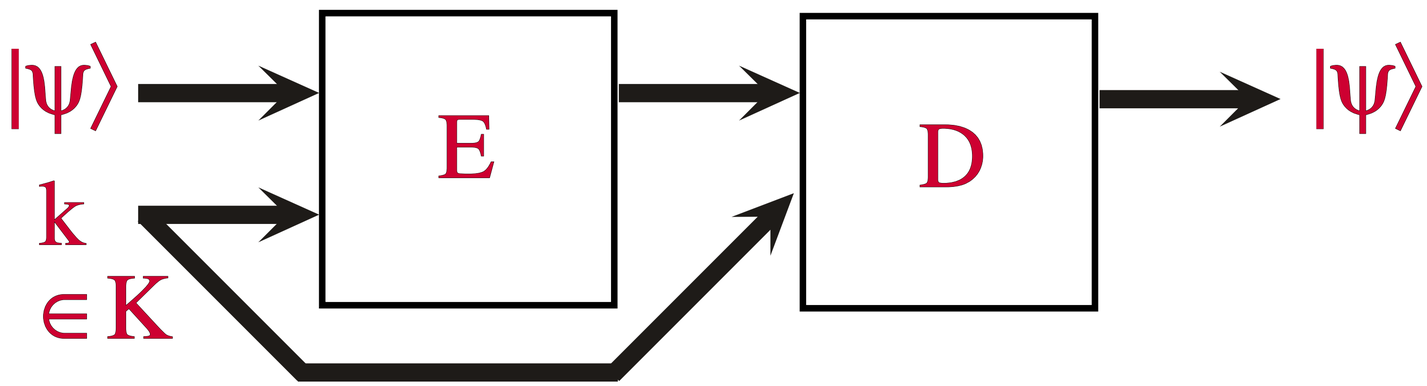
[AMTW00] showed

a QES (with error probability 0)

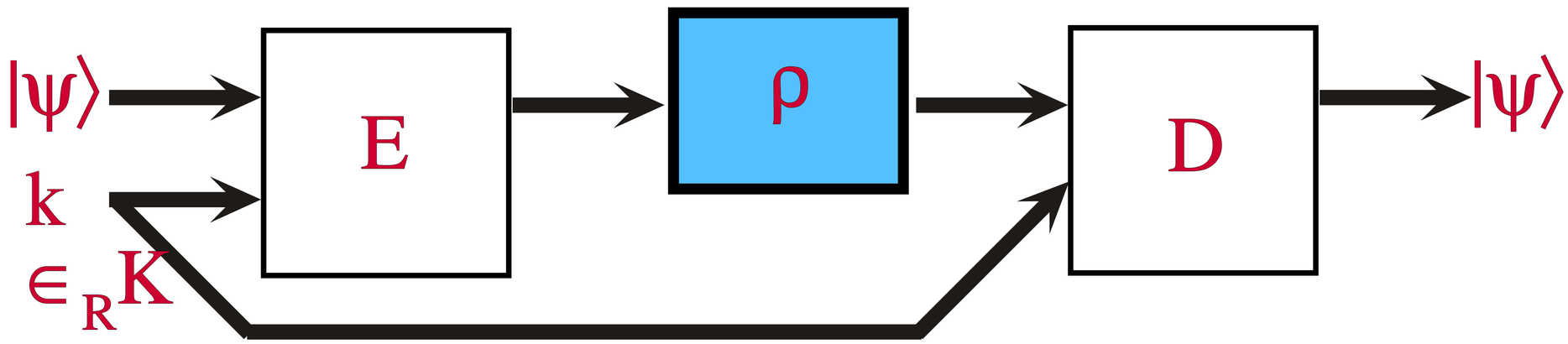
—> 2n bits to encrypt n qubits

One-time Q-encryption with error ε

Completeness:



Secrecy:



$$\forall|\psi_0\rangle,|\psi_1\rangle \quad D(\rho_0,\rho_1)=Tr(|\rho_0-\rho_1|)<\varepsilon$$

Theorems

[AMTW00] showed

a QES (with error probability 0)
—> 2n bits to encrypt n qubits

a QES with error probability $\varepsilon>0$
—> (2-poly(ε))n bits
to encrypt n qubits.

Theorems

a CES (with error probability 0)
—> n bits to encrypt n bits

a CES with error probability $\varepsilon>0$
—> $(1-\text{poly}(\varepsilon))n$ bits
to encrypt n bits.

Theorems

[AMTW00] showed

a QES (with error probability 0)
—> 2n bits to encrypt n qubits

a QES with error probability $\varepsilon>0$
—> (2-poly(ε))n bits
to encrypt n *Eve-entangled* qubits

[HLSW03] showed

a QES with error probability $\varepsilon>0$
—> n+o(n) bits
to encrypt n *Eve-separated* qubits.