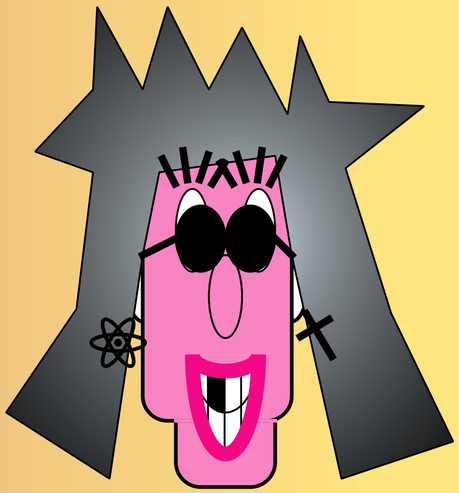
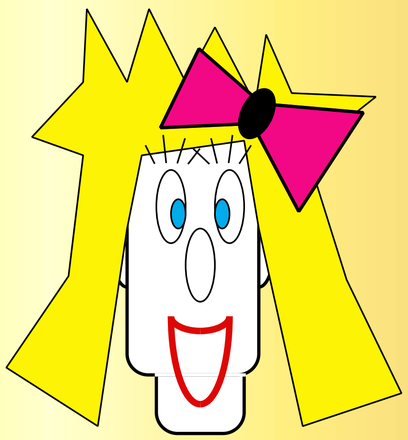
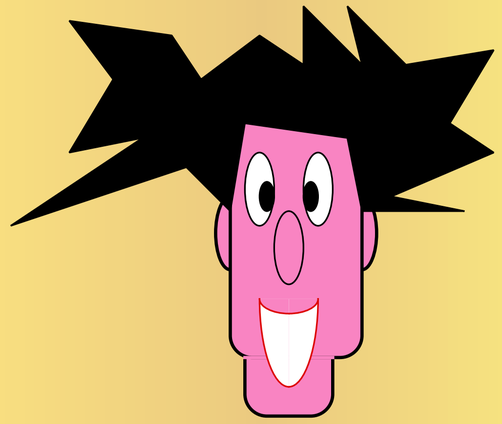
One-Time-Pad

Quantum





|Will you marry me ?⟩

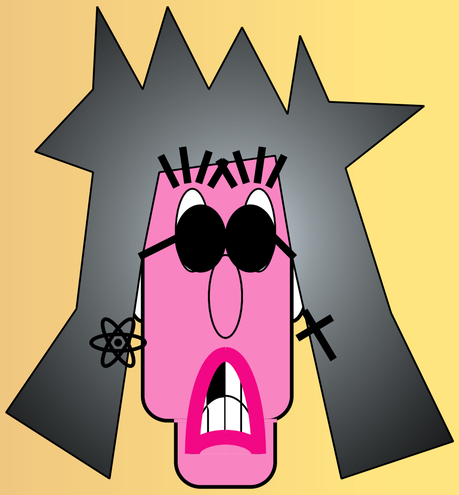


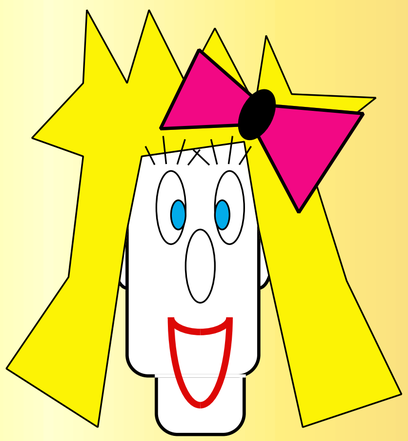
|Divorce your wife first !⟩

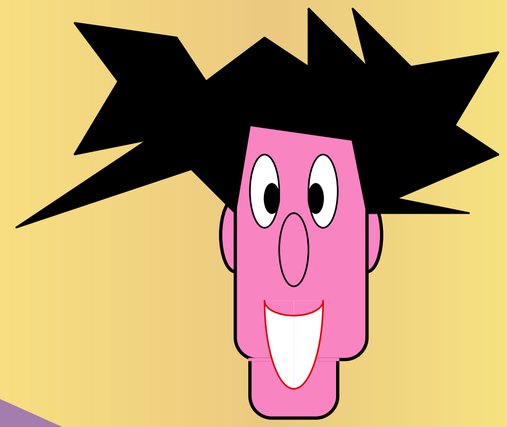
|The papers are in the mail...⟩

|OK, I will !⟩

(3.1.2Q) One-time Q-pad







8RdewtU5qkLa$es!T9@

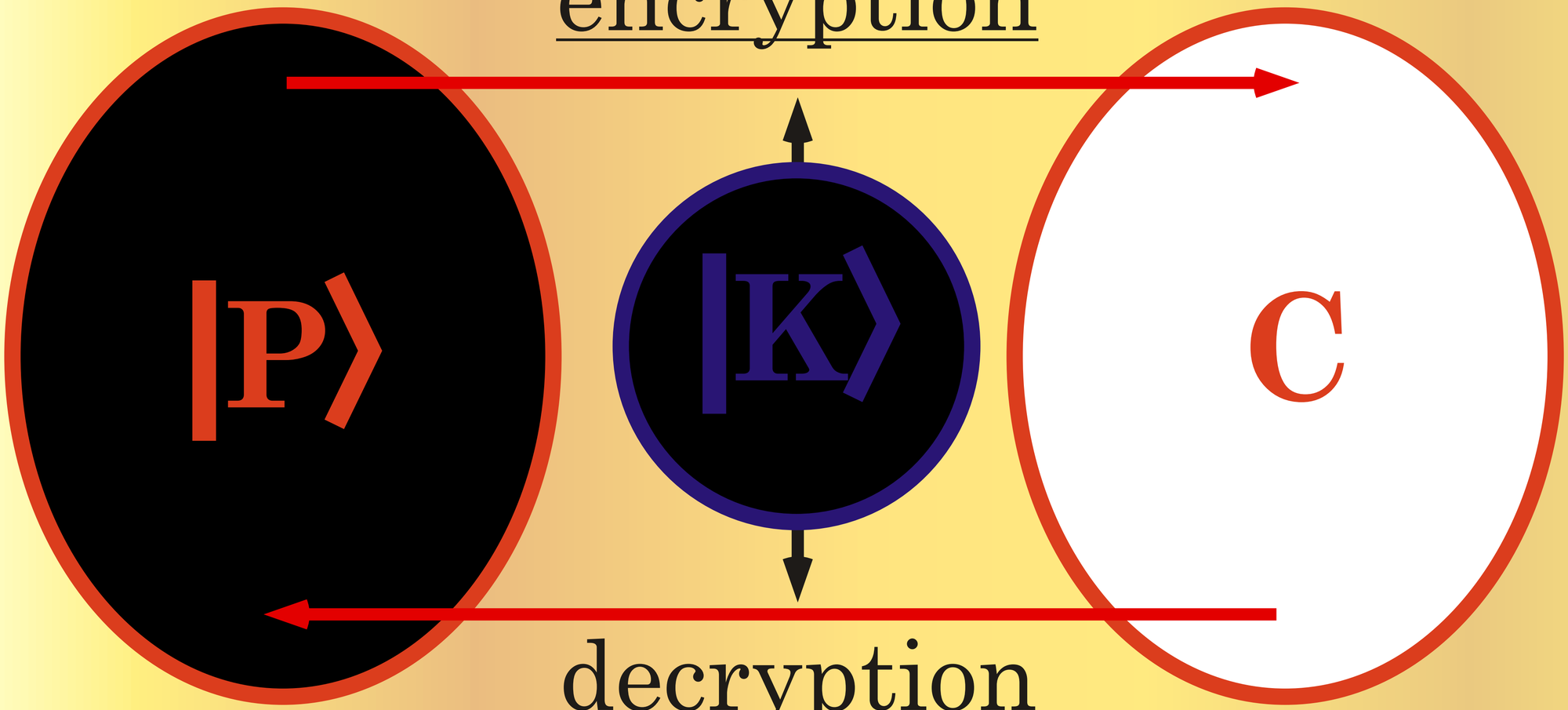
I(D%eXhDqIiykl#2cV7dEwnMs

H&fs@tyHvFGhaOKpTrGbl.Z/rUih*

B7B3tdsjUila

symmetric encryption of Quantum messages

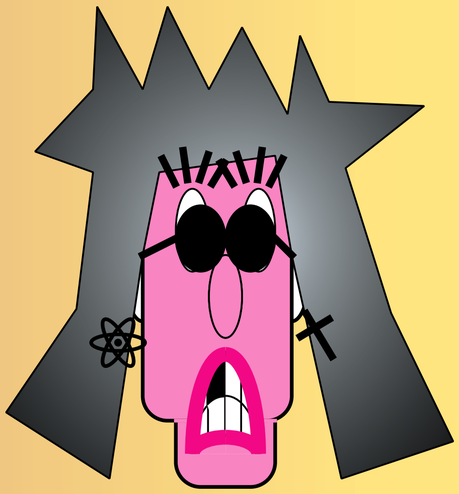
encryption

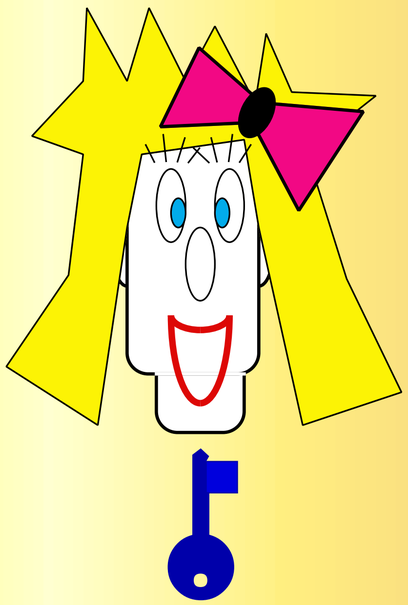


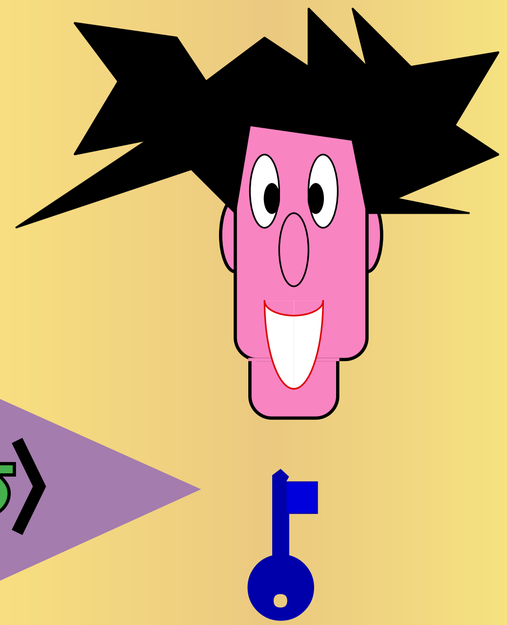
decryption

Information Theoretical Security

(3.1.2C) Vernam Ω-cipher







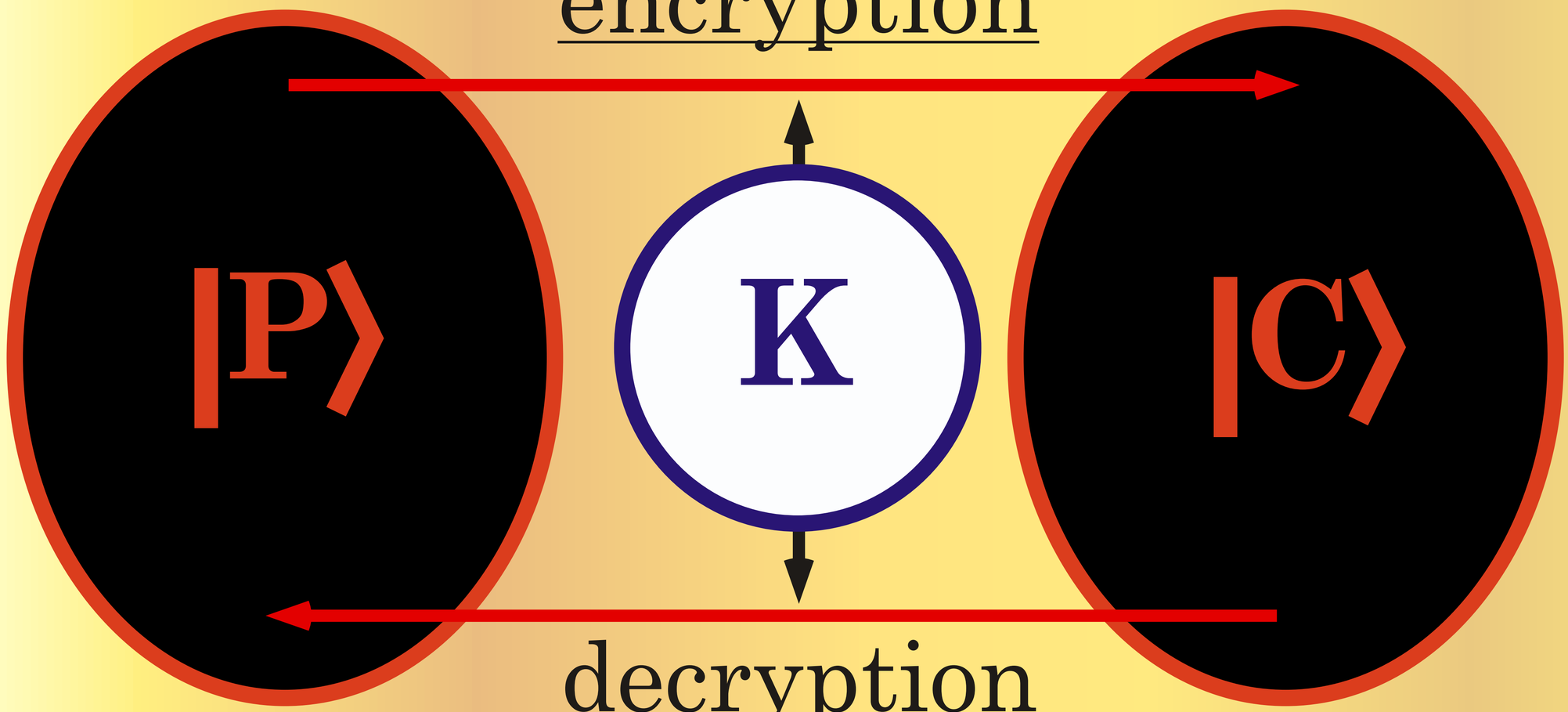
|8PδεωτY5θκΛαΞεσ!T9≅⟩

|I(Δ%εΞηΔθIιψκλ#2χς7δEωνMσ⟩

|H&φσ≅τψϖΦηαOKπTρΓβλ.Z/ρYιη*⟩

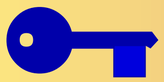
|B7B3τδσφYιλα⟩

symmetric encryption of Quantum messages



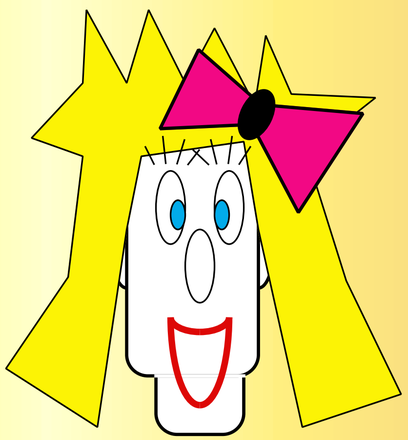
Information Theoretical Security

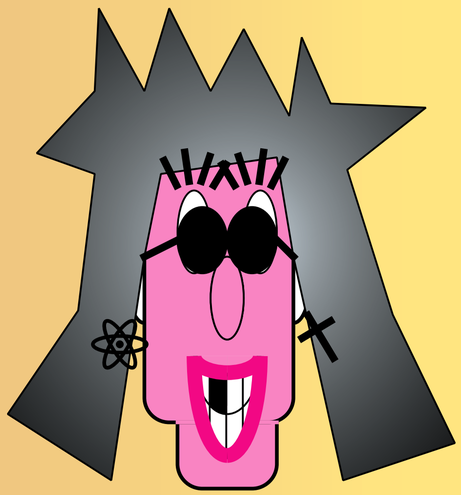
(3.1.2) One-time pad

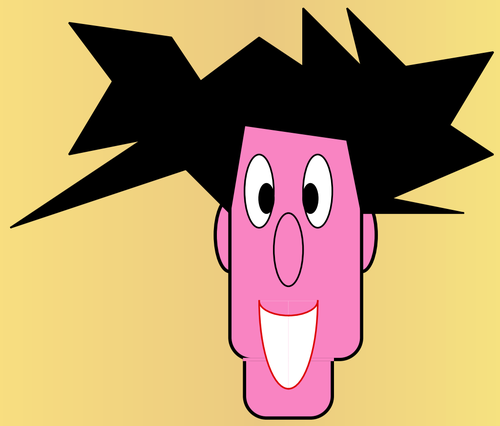


Classical key : Vernam Q-cipher (various sources)
Quantum Ciphertext

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

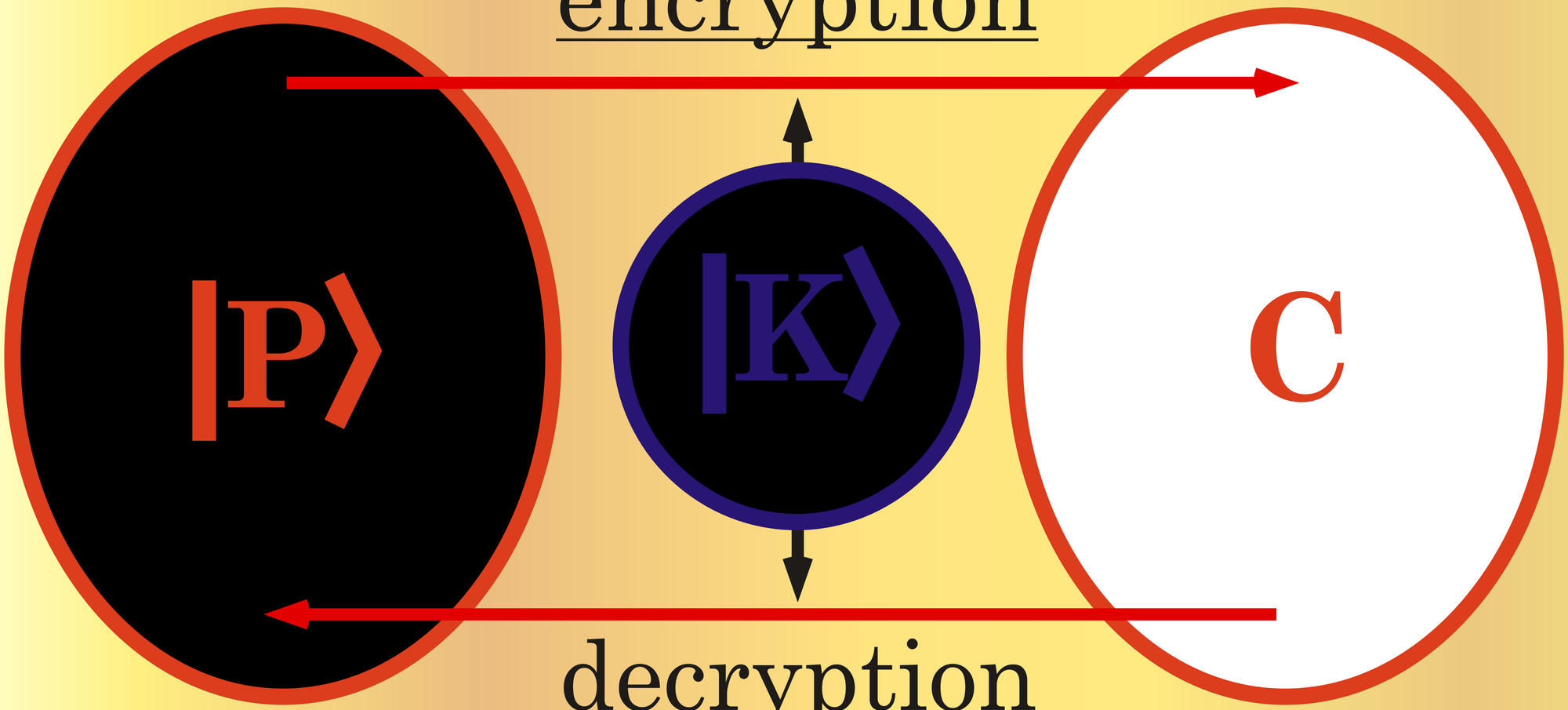






symmetric encryption of Quantum messages

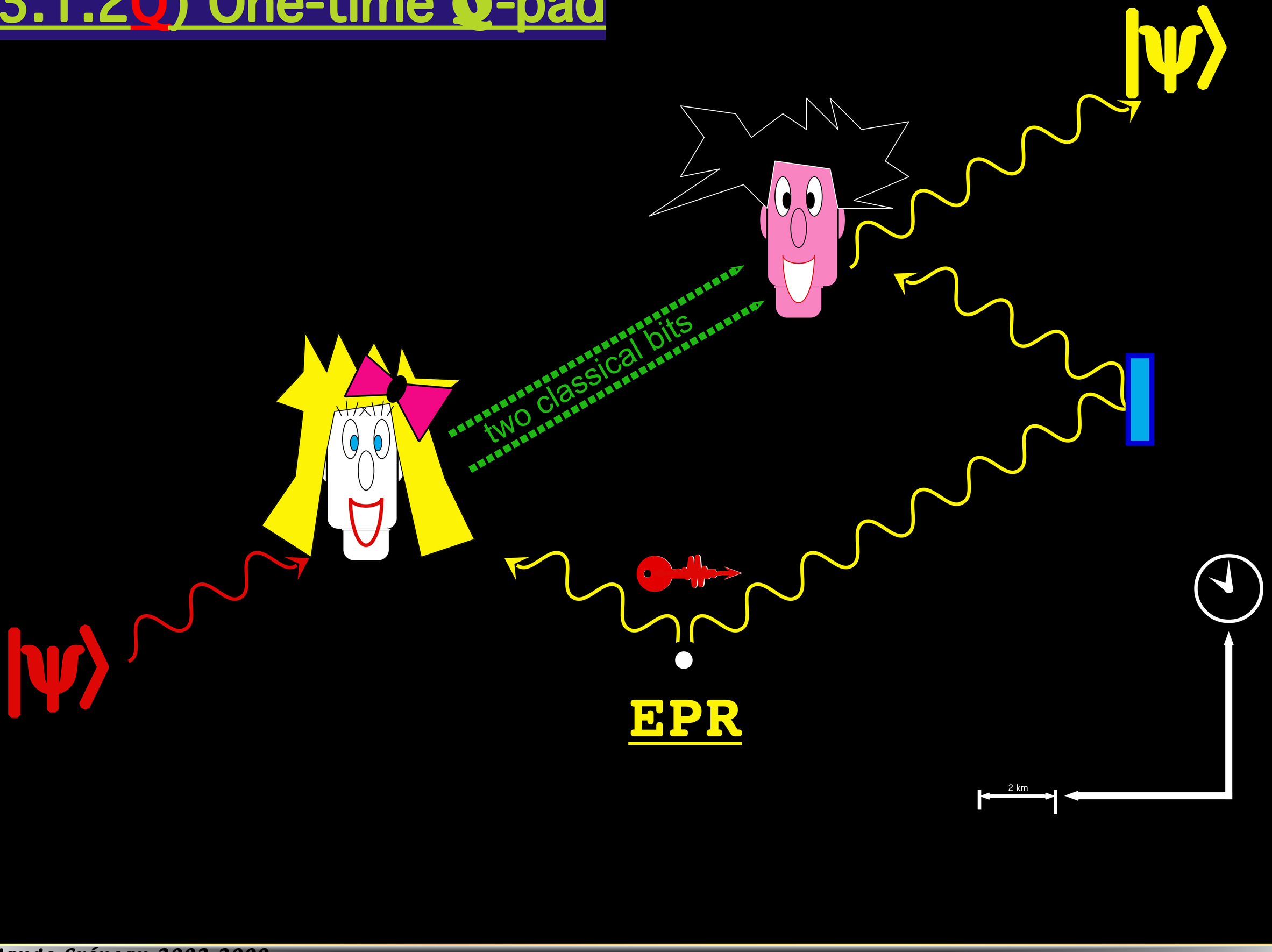
encryption

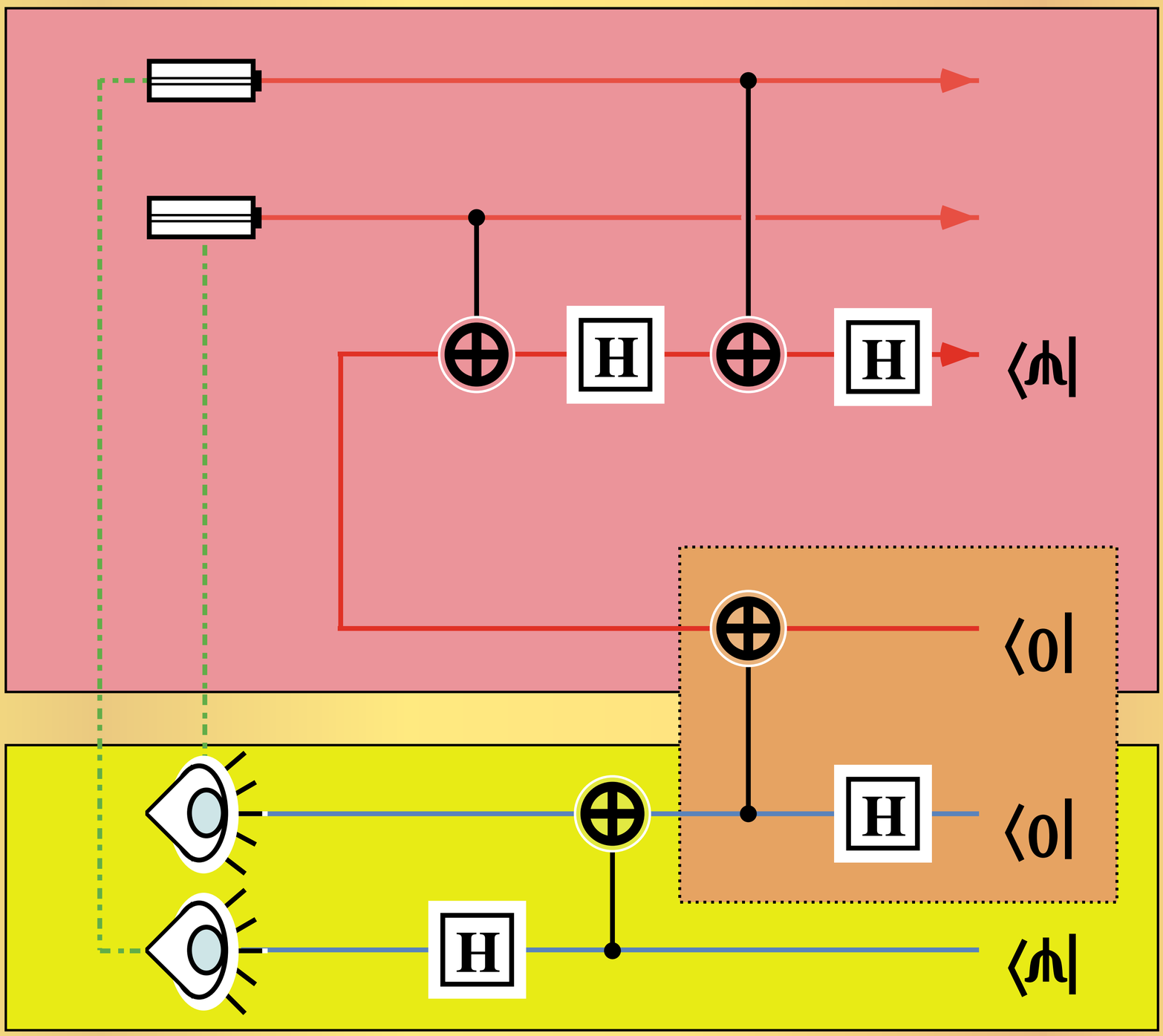


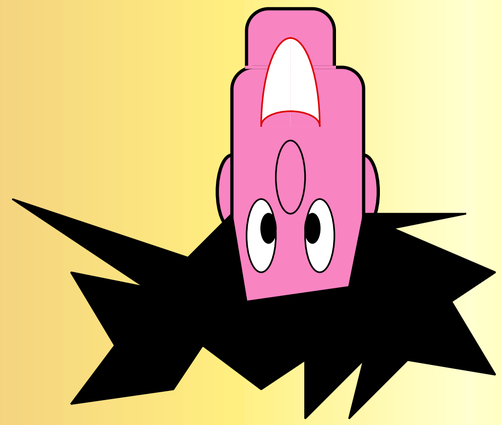
decryption

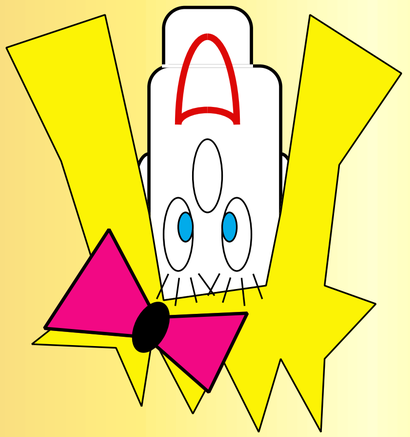
Information Theoretical Security

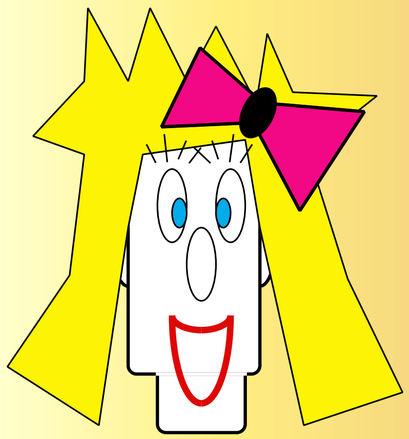
(3.1.2Q) One-time Q-pad

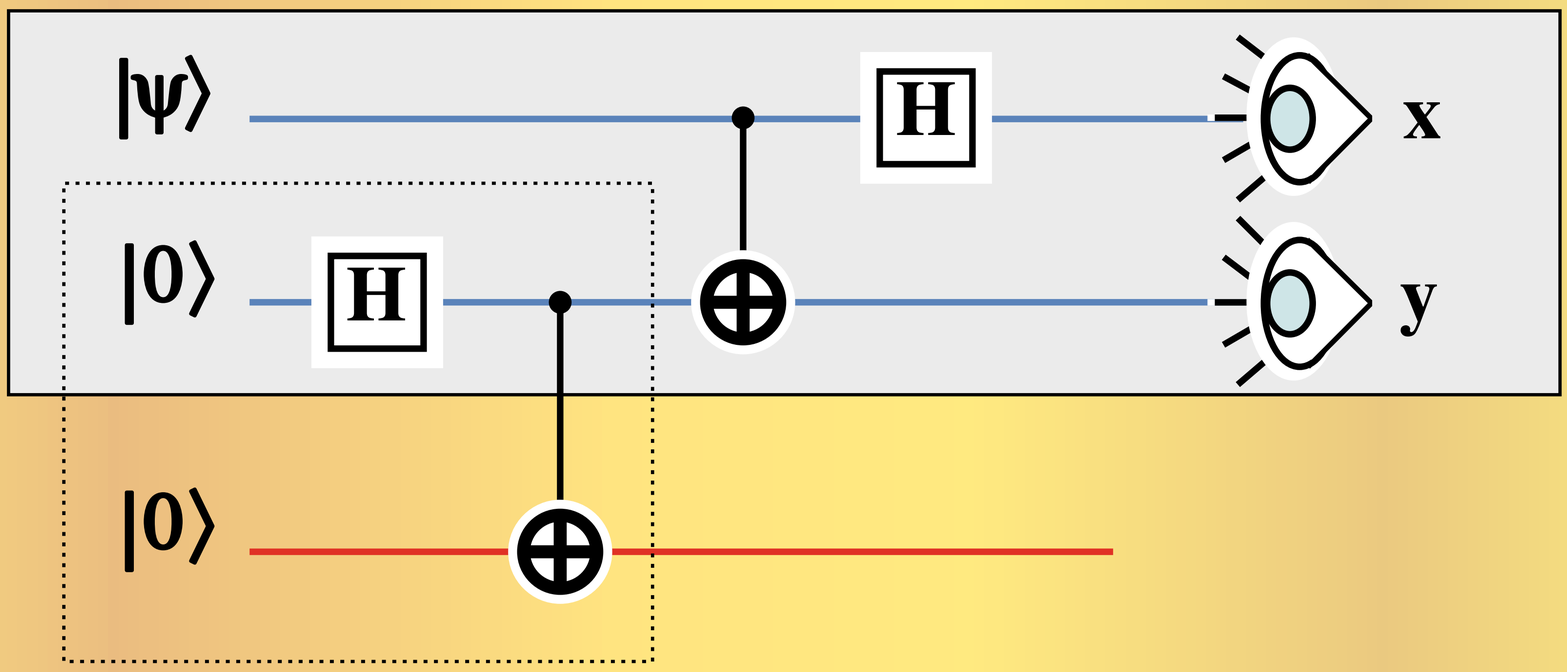












$|\psi\rangle|0\rangle|0\rangle$

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

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

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

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

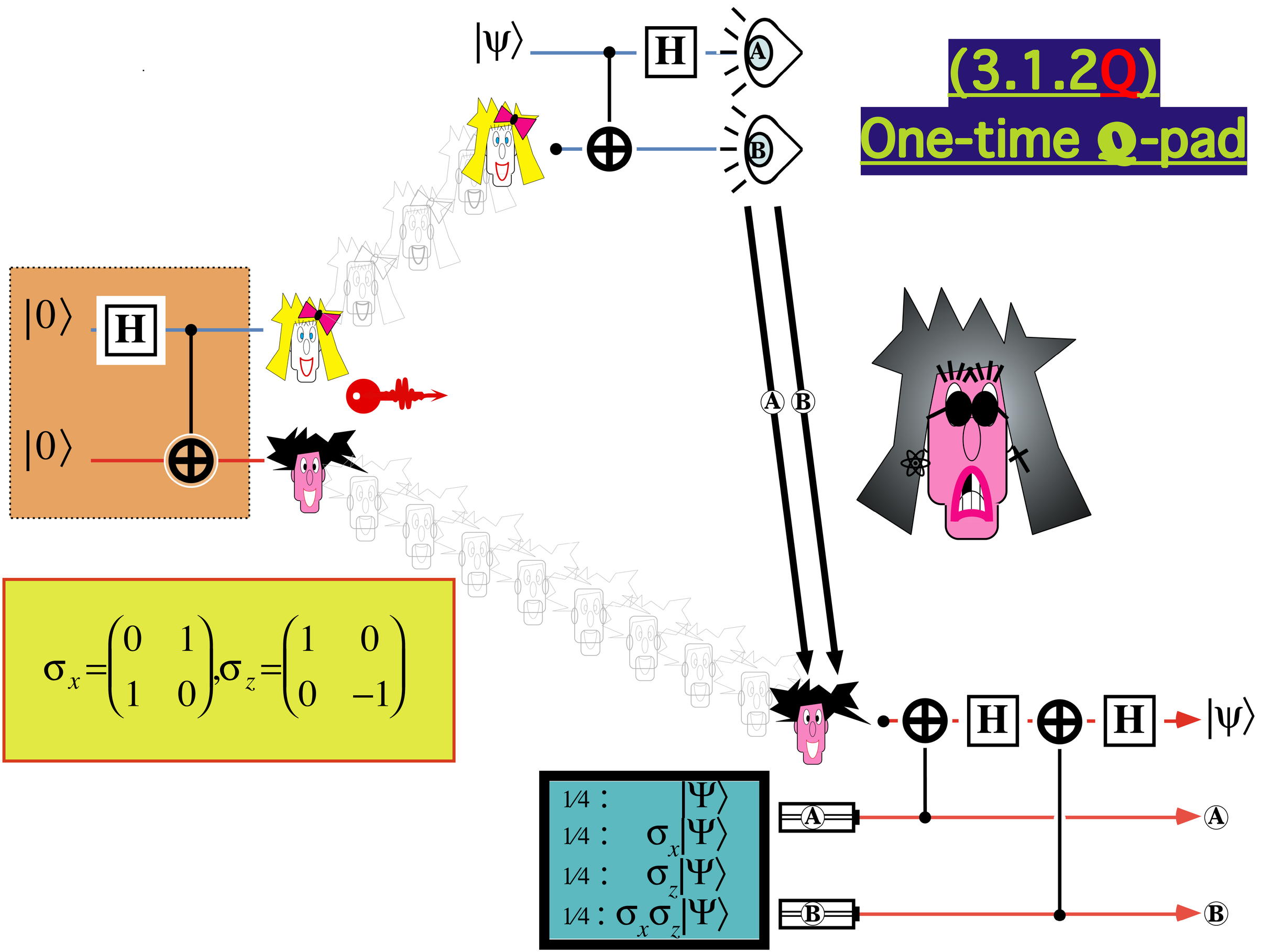
⊕ $\alpha|0\rangle|00\rangle+\alpha|0\rangle|11\rangle+\beta|1\rangle|10\rangle+\beta|1\rangle|01\rangle$

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

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

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

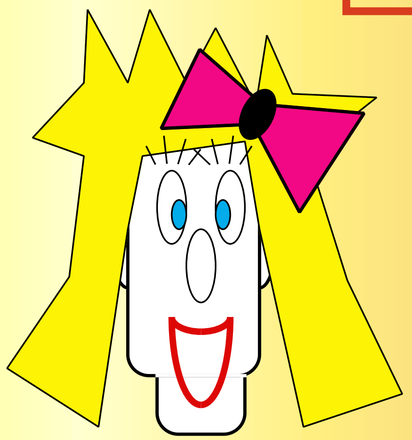
(3.1.2Q) One-time Q-pad



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

(3.1.2Q) One-time Q-pad

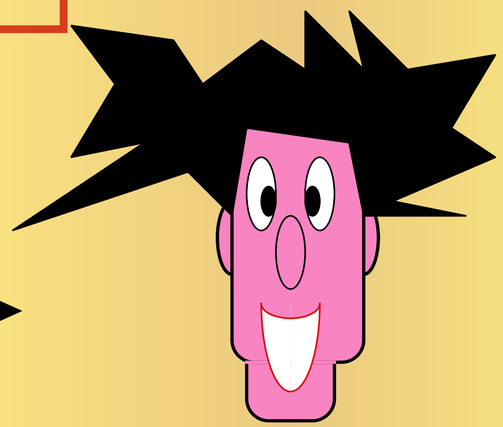
Quantum key : one-time Q-pad
Classical Ciphertext

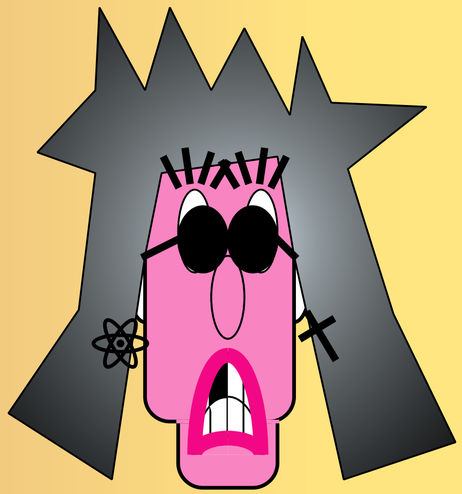


$|\Psi\rangle$

A B

two random bits

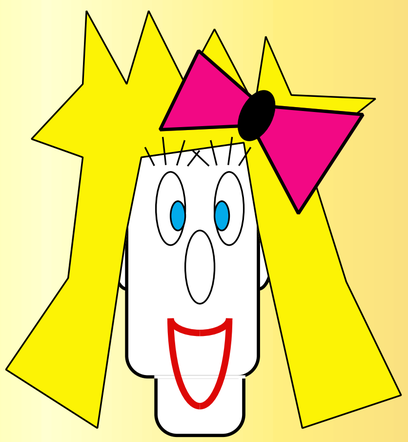


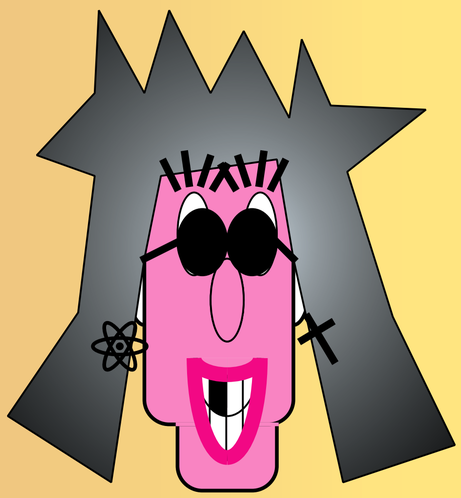


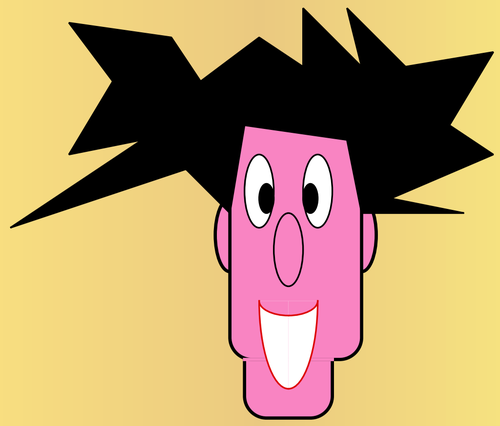
(3.1.2) One-time pad

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

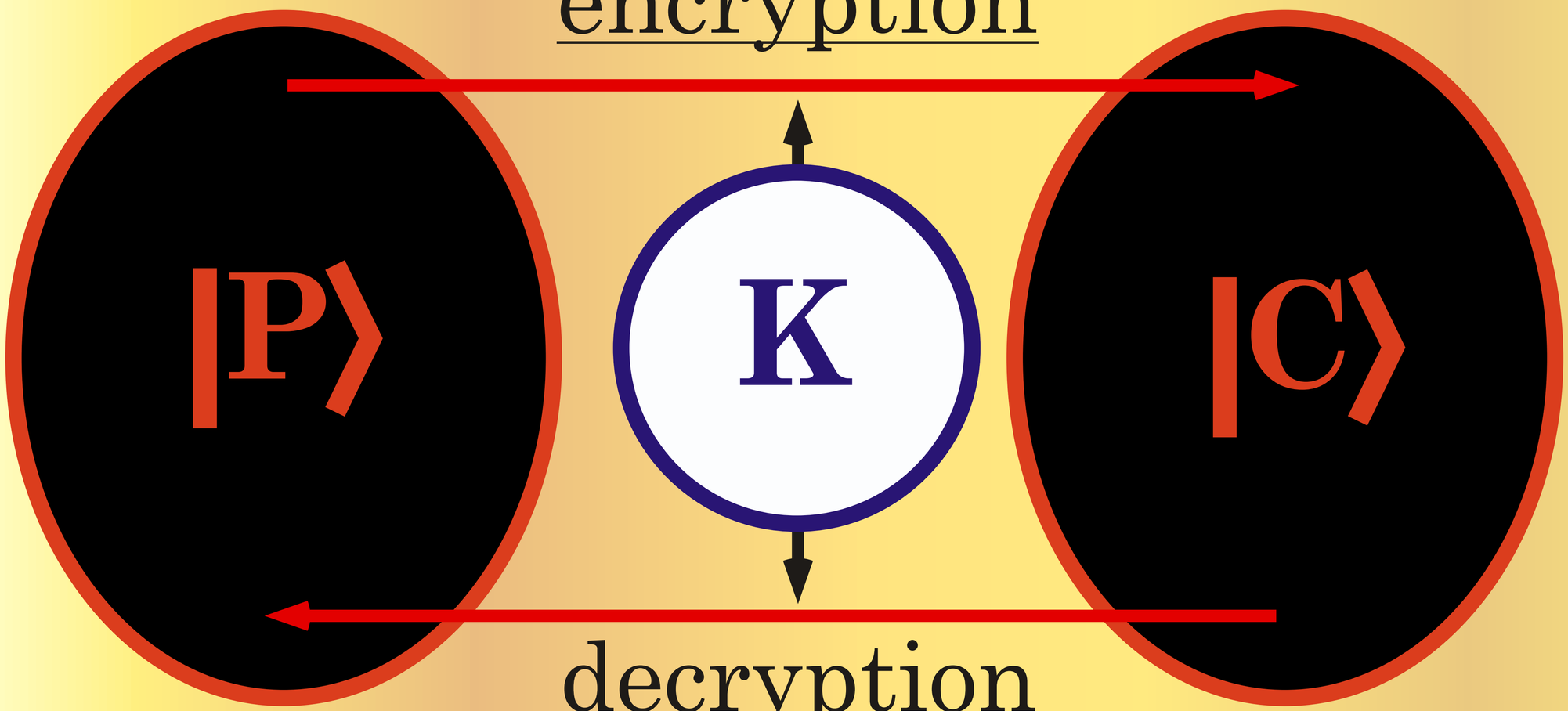
Quantum key : one-time Q-pad (BBCJPW)
Classical Ciphertext







symmetric encryption of Quantum messages

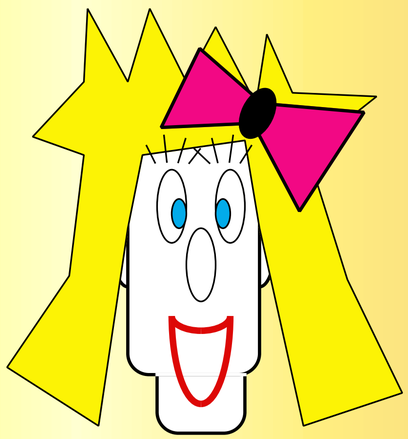


Information Theoretical Security

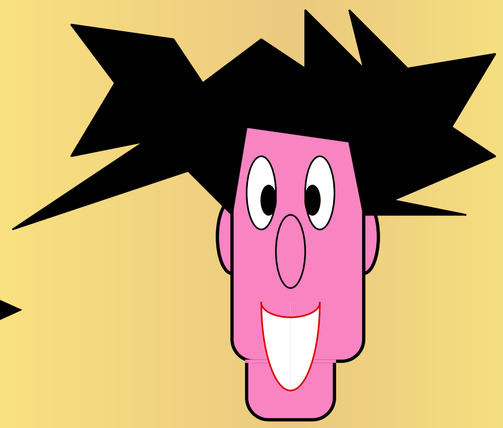
(3.1.2C) Vernam Q-cipher

Classical key : Vernam Q-cipher
Quantum Ciphertext

Quantum key : one-time Q-pad
Classical Ciphertext



$|\Psi\rangle$

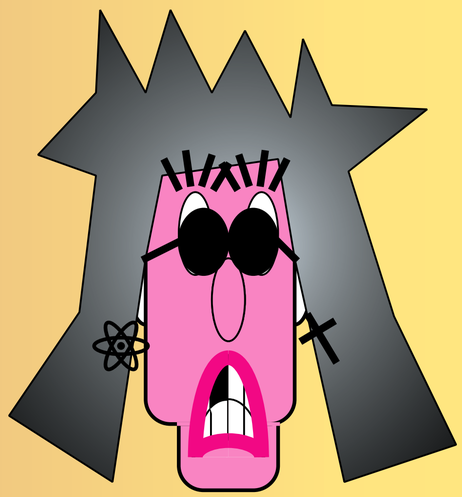


a,b random bit key

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

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

$$\rho:\ \tfrac{1}{4}:|\Psi\rangle,\ \tfrac{1}{4}:\sigma_x|\Psi\rangle,\ \tfrac{1}{4}:\sigma_z|\Psi\rangle,\ \tfrac{1}{4}:\sigma_x\sigma_z|\Psi\rangle$$



a,b random bit key

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

$$\rho=\begin{cases} 1/4: (\alpha|0\rangle+\beta|1\rangle) \\ 1/4: (\alpha|1\rangle+\beta|0\rangle) \\ 1/4: (\alpha|0\rangle-\beta|1\rangle) \\ 1/4: (\alpha|1\rangle-\beta|0\rangle) \end{cases}$$

$$4\rho=(\alpha|0\rangle+\beta|1\rangle)(\alpha^*\langle 0|+\beta^*\langle 1|)+(\alpha|1\rangle+\beta|0\rangle)(\alpha^*\langle 1|+\beta^*\langle 0|)+$$
$$(\alpha|0\rangle-\beta|1\rangle)(\alpha^*\langle 0|-\beta^*\langle 1|)+(\alpha|1\rangle-\beta|0\rangle)(\alpha^*\langle 1|-\beta^*\langle 0|)$$

$$=(2|\alpha|^2+2|\beta|^2)|0\rangle\langle 0|+(\alpha\beta^*+\beta\alpha^*-\alpha\beta^*-\beta\alpha^*)|0\rangle\langle 1|+$$
$$(\beta\alpha^*+\alpha\beta^*-\beta\alpha^*-\alpha\beta^*)|1\rangle\langle 0|+(2|\beta|^2+2|\alpha|^2)|1\rangle\langle 1|$$

$$=2|0\rangle\langle 0|+2|1\rangle\langle 1|$$

$$\rho=\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}=I/2$$

Theorems

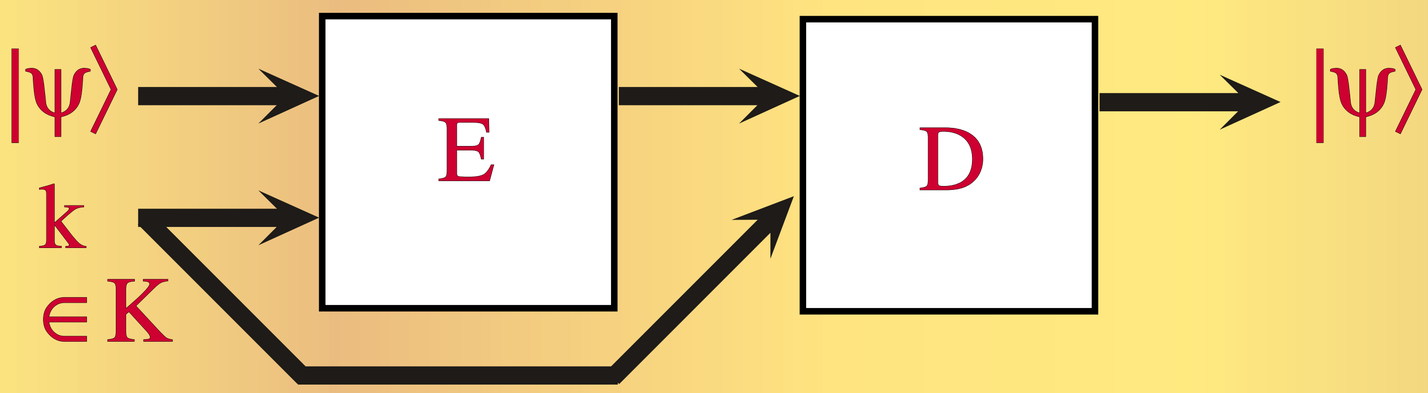
[AMTW00] showed

a QES (with error probability 0)

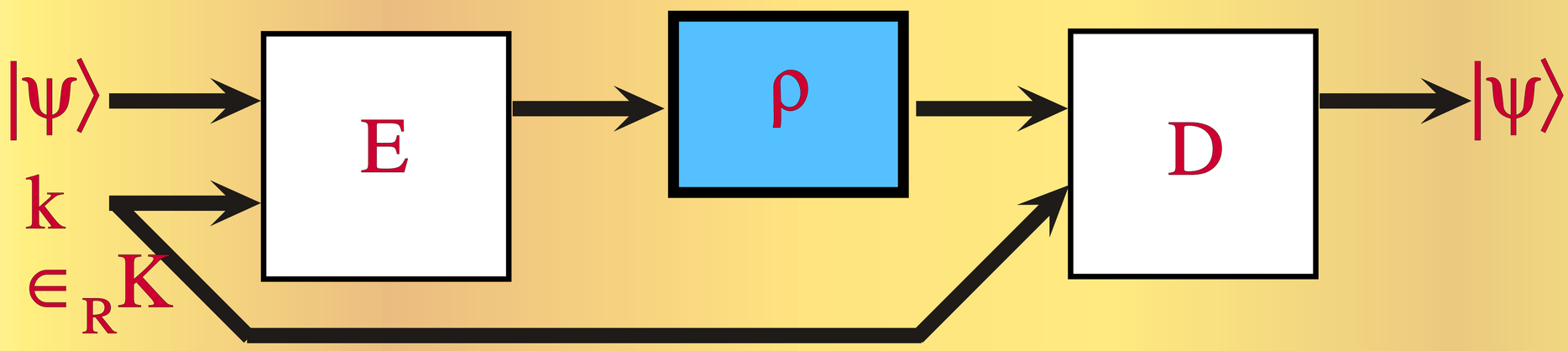
—> 2n bits to encrypt n qubits

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

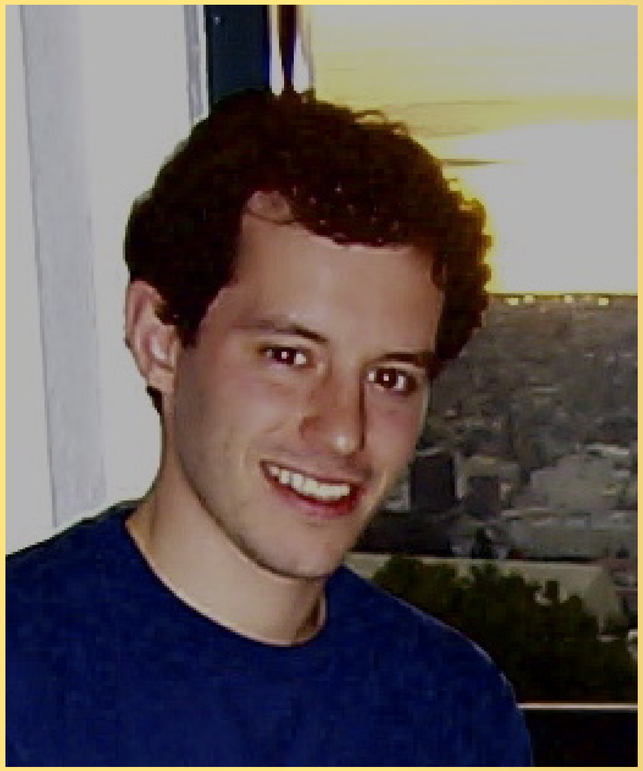
a QES with error probability $\varepsilon>0$

—> n+o(n) bits

to encrypt n *Eve-separated* qubits.

Small Pseudo-Random Families of Matrices: Derandomizing Approximate Quantum Encryption

Andris Ambainis



Adam Smith

Small-Bias Spaces The bias of a random variable A in $\{0\,,1\}^n$ with respect to a string $\alpha \in \{0,1\}^n$ is the distance from uniform of the bit $\alpha \odot A$, where $\odot$ refers to the standard dot product on $\mathbb{Z}_2^n$:

$$\hat{A}(\alpha) = \mathbb{E}_A\left[(-1)^{\alpha \odot A}\right] = 2\Pr[\alpha \odot A = 0] - 1.$$

The function $\hat{A}$ is the Fourier transform of the probability mass function of the distribution, taken over the group $\mathbb{Z}_2^n$.

The bias of a set $S \in \{0,1\}^n$ with respect to α is simply the bias of the uniform distribution over that set. A set S is called δ-biased if the absolute value of its bias is at most δ for all $\alpha \neq 0^n$.

Small-bias sets of size polynomial in n and $1/\delta$ were first constructed by Naor and Naor [10]. Alon, Bruck et al. (ABNNR , [1]) gave explicit (i.e. deterministic, polynomial-time) constructions of δ-biased sets in $\{0,1\}^n$ with size $O(n/\delta^3)$. Constructions with size $O(n^2/\delta^2)$ were provided by Alon, Goldreich, et al. (AGHP , [2]). The AGHP construction is better when $\delta = o(1/n)$. In both cases, the i^{th} string in a set can be constructed in roughly n^2 time (regardless of δ).

One can sample a random point from a δ-biased space over $\{0,1\}^n$ using either $\log n + 3\log(1/\delta) + O(1)$ bits of randomness (using ABNNR) or using $2\log n + 2\log(1/\delta)$ bits (using AGHP).

3 State Randomization and Approximate Encryption

3.1 Encrypting with a Small-Bias Space

The ideal quantum one-time pad applies a random Pauli matrix to the input [3]. Consider instead a scheme which first chooses a $2n$-bit string from some set with small bias δ (we will set δ later to be $\epsilon 2^{-n/2}$). If the set of strings is B we have:

$$\mathcal{E}(\rho_0) = \frac{1}{|B|} \sum_{(a,b)\in B} X^a Z^b \rho_0 Z^b X^a = \mathbb{E}_{a,b} \left[X^a Z^b \rho_0 Z^b X^a \right]$$

That is, we choose the key from the set B, which consists of $2n$-bit strings. To encrypt, we view a $2n$-bit string as the concatenation (a, b) of two strings of n bits, and apply the corresponding Pauli matrix.

Using the constructions of AGHP [2] for small-bias spaces, we get a polynomial-time scheme that uses $n + 2\log n + 2\log(1/\epsilon)$ bits of key.

Fact 1. *If ρ is d-dimensional quantum state and* $Tr\left(\rho^2\right) \leq \frac{1}{d}(1+\epsilon^2)$, *then* $D(\rho, \frac{1}{d}\mathbb{I}) \leq \epsilon$.

Main Theorem.

$$\mathrm{Tr}(\mathcal{E}(\rho_0)^2) \leq \frac{1}{2^n}(1 + \delta^2 2^n \mathrm{Tr}(\rho_0^2))$$

Quantum entropic security and approximate quantum encryption

Simon Pierre Desrosiers

Frédéric Dupuis

Theorem 3: If $H_\infty(\rho^{AE}|\rho^E) \geqslant t$, then the Ambainis-Smith scheme is ε-secure using $n - t + 2\log n + 2\log(\frac{1}{\varepsilon}) + 2$ bits of key, where $n = \log d_A$.