Quantum Codes Correcting* up to $(n\text{-}1)/2$ arbitrary errors

*except with exponentially small probability

Claude Crépeau

School of Computer Science
McGill University

joint work with

D. Gottesman and A. Smith

(1) Quantum Error Correcting Codes

Q: (over GF(3))

$$
\begin{aligned}
|0\rangle &\rightarrow |000\rangle + |111\rangle + |222\rangle \\
|1\rangle &\rightarrow |012\rangle + |120\rangle + |201\rangle \\
|2\rangle &\rightarrow |021\rangle + |102\rangle + |210\rangle
\end{aligned}
$$

$$Q|\psi\rangle = H_1 \otimes H_2 \otimes H_3$$

fixed

$Q = [[3,1,2]]$ **corrects one erasure.**

$$
\begin{aligned}
\varnothing \otimes H_2 \otimes H_3 &\longrightarrow (-H_2 - H_3 \bmod 3) \otimes H_2 \otimes H_3 \\
H_1 \otimes \varnothing \otimes H_3 &\longrightarrow H_1 \otimes (-H_3 - H_1 \bmod 3) \otimes H_3 \\
H_1 \otimes H_2 \otimes \varnothing &\longrightarrow H_1 \otimes H_2 \otimes (-H_1 - H_2 \bmod 3)
\end{aligned}
$$

Calderbank-Shor-Steane **Q**-ECCs

Let C_1, C_2 be two linear codes such that

$$\{0\} \subset C_2 \subset C_1 \subset \mathrm{F}^n \qquad \{0\} \subset C_1^{\perp} \subset C_2^{\perp} \subset \mathrm{F}^n$$

For $v \in C_1$ define

$$v \mapsto \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} |v+w\rangle$$

For $v \in C_2^{\perp}$ define

$$v \mapsto \frac{1}{\sqrt{|C_1^{\perp}|}} \sum_{w \in C_1^{\perp}} |v+w\rangle$$

$$Q = \left\{ \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} |w+v\rangle : v \in C_1 \right\}$$

$$Q^{*} = \left\{ \frac{1}{\sqrt{|C_1^{\perp}|}} \sum_{w \in C_1^{\perp}} |w+v\rangle : v \in C_2^{\perp} \right\}$$

CSS $\mathcal{Q}$-ECCs

Let $C_1=[n,k_1,d_1]$, $C_2^{\square}=[n,n-k_2,d_2]$ be two linear codes

$$\dim(Q) = \dim(C_1)\text{-}\dim(C_2) = k_1-k_2 = \dim(C_2^{\square})\text{-}\dim(C_1^{\square}) = \dim(Q^*)$$

$$\mathrm{d}(Q) = \mathrm{d}(Q^*) = \min\{\mathrm{d}(C_1),\mathrm{d}(C_2^{\square})\} = \min\{d_1,d_2\}$$

$$Q = [[\ n,\ k_1-k_2,\ \min\{d_1,d_2\}\ ]] = Q^*$$

CSS Q-ECCs

EXAMPLE: Quantum Reed-Solomon codes (Aharonov-BenOr)

fixed

Let q=4t

C_1 = [4t,2t+1,2t] ERS-code over GF(q)
C_2 = [4t,2t,2t+1] ERS-code over GF(q)

dim(Q) = dim(Q*) = 1
d(Q) = d(Q*) = 2t

Q,Q*= [[4t, 1 , 2t]] QRS-code over GF(q)

Q,Q*= [[n, 1 , n/2]] QRS-code over GF(q) , q=n

Theorem: No QECC tolerates $t \geq n/4$

Proof:

- No cloning says that no QECC can correct $n/2$ erasures
- Fact: Any QECC which corrects t errors can correct $2t$ erasures and conversely
- Thus no QECC tolerates $n/4$ errors
- All these arguments work regardless of the size of the components of QECC (size of the field of definition)

- ~~Fact: Any QECC which corrects t errors can correct $2t$ erasures and conversely~~

<u>If small error probability is acceptable</u>

Error probability of not correcting

is taken

over choices of code

but

NOT over distribution of errors

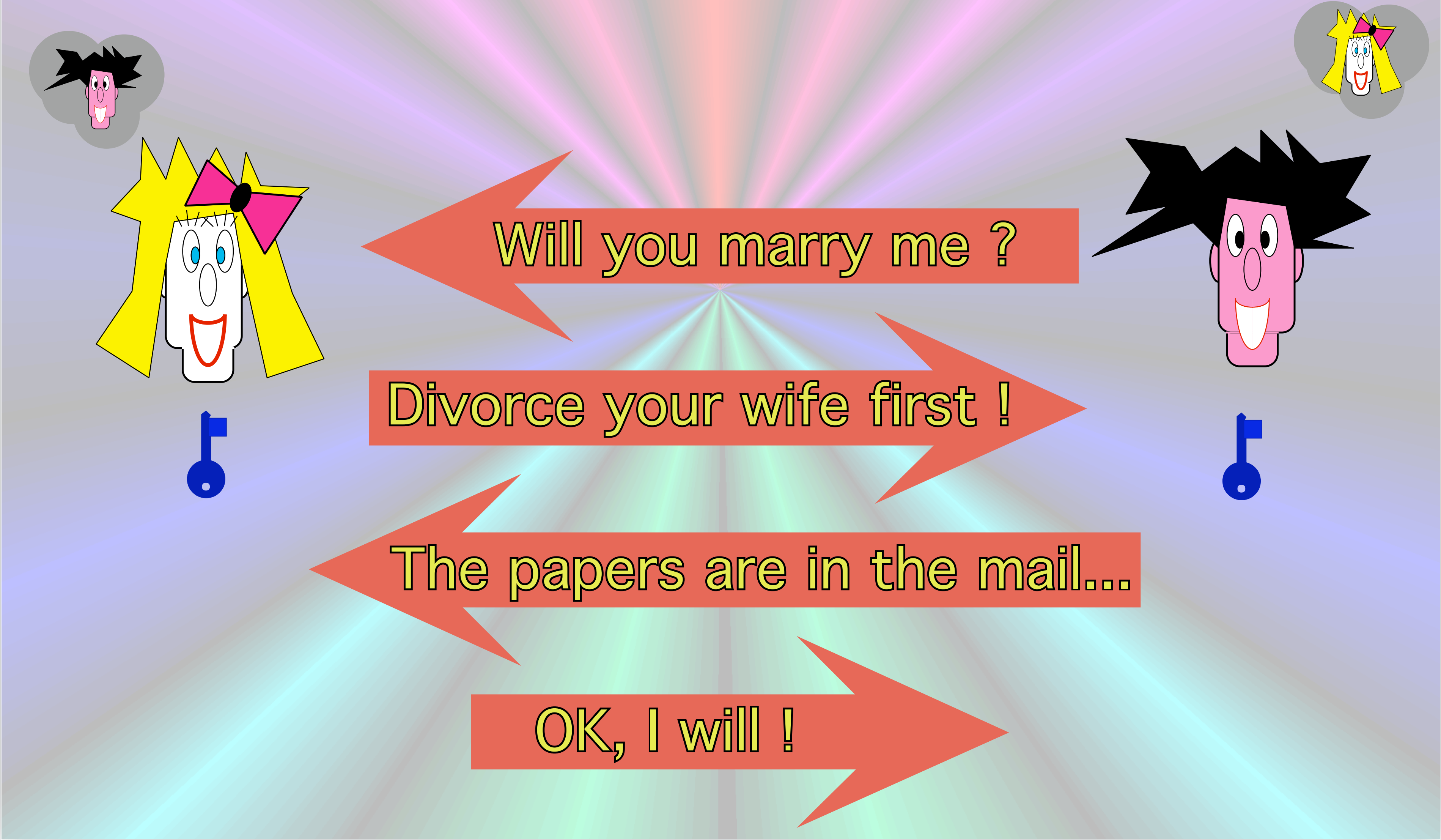
fixed

*Communication model needs to be specified completely to distinguish our work from earlier work of others. We do not allow classical private, authenticated, error-free channel between coder and decoder:

All communications MUST go through the noisy channel.

(2) Classical Authentication

Authentication

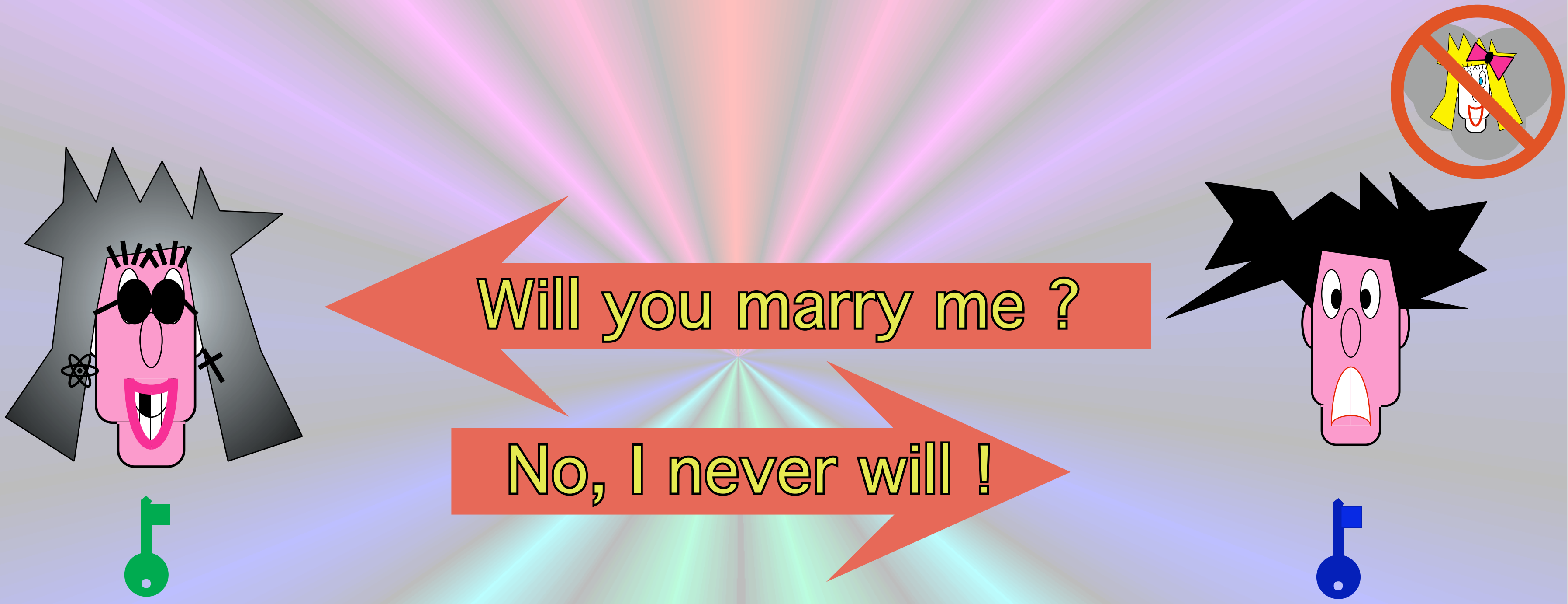


Will you marry me ?

Divorce your wife first !

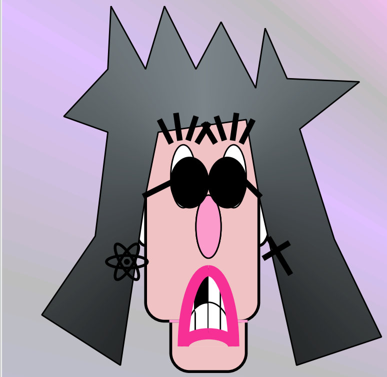
The papers are in the mail...

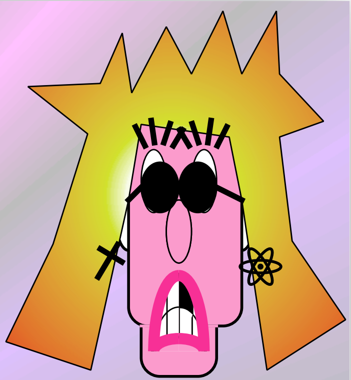
OK, I will !



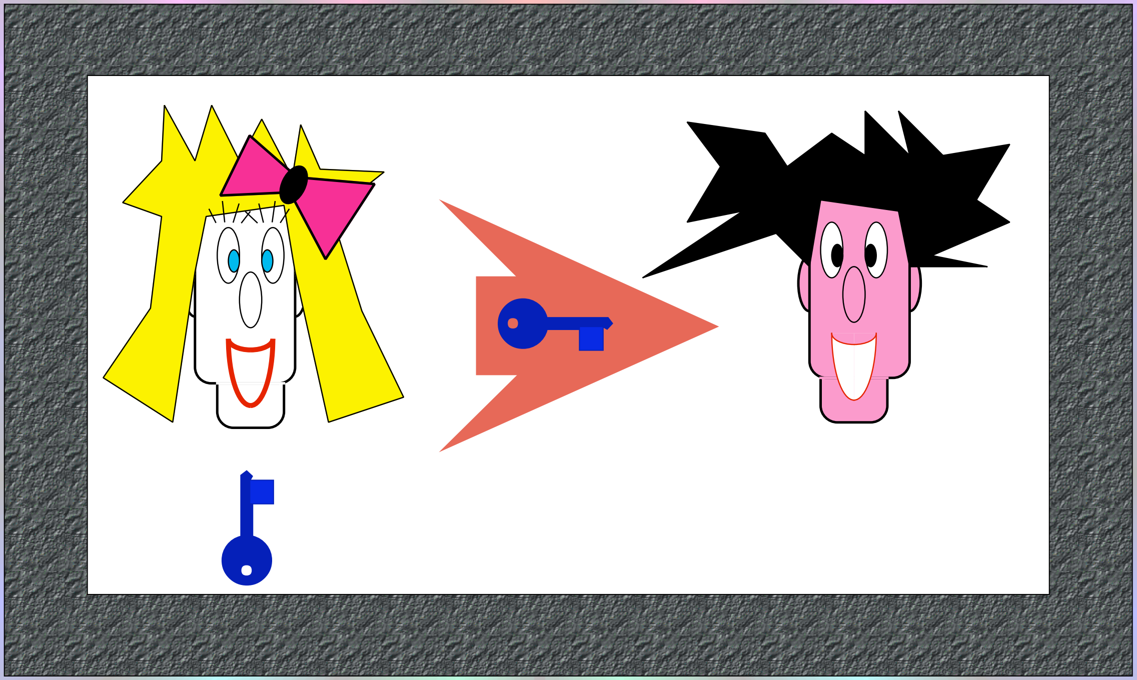
Will you marry me ?

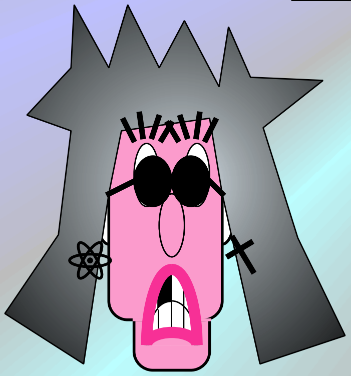
No, I never will !

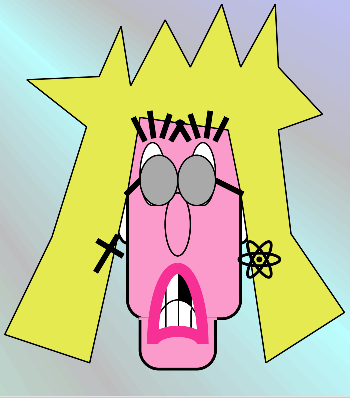




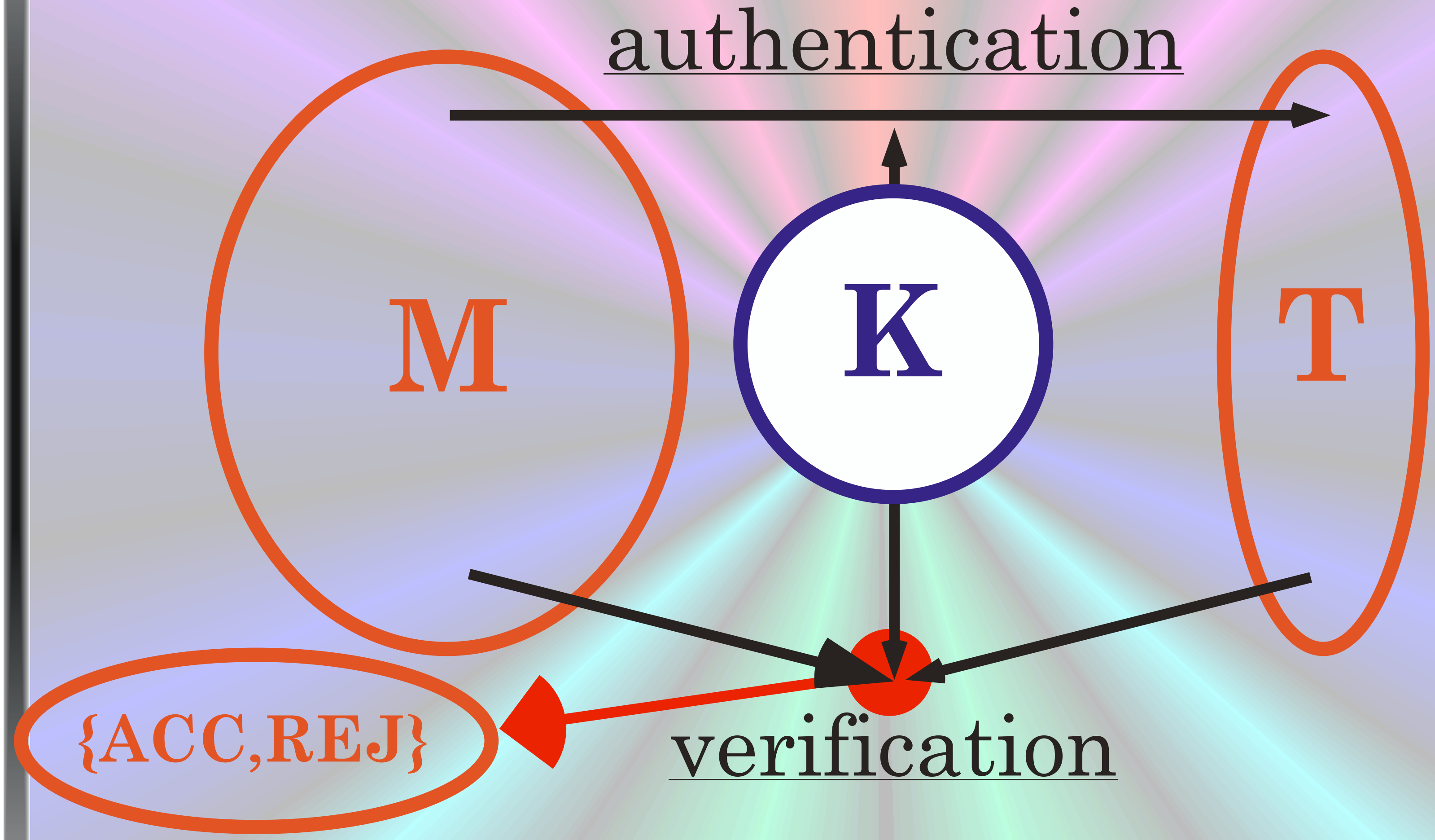
key distribution





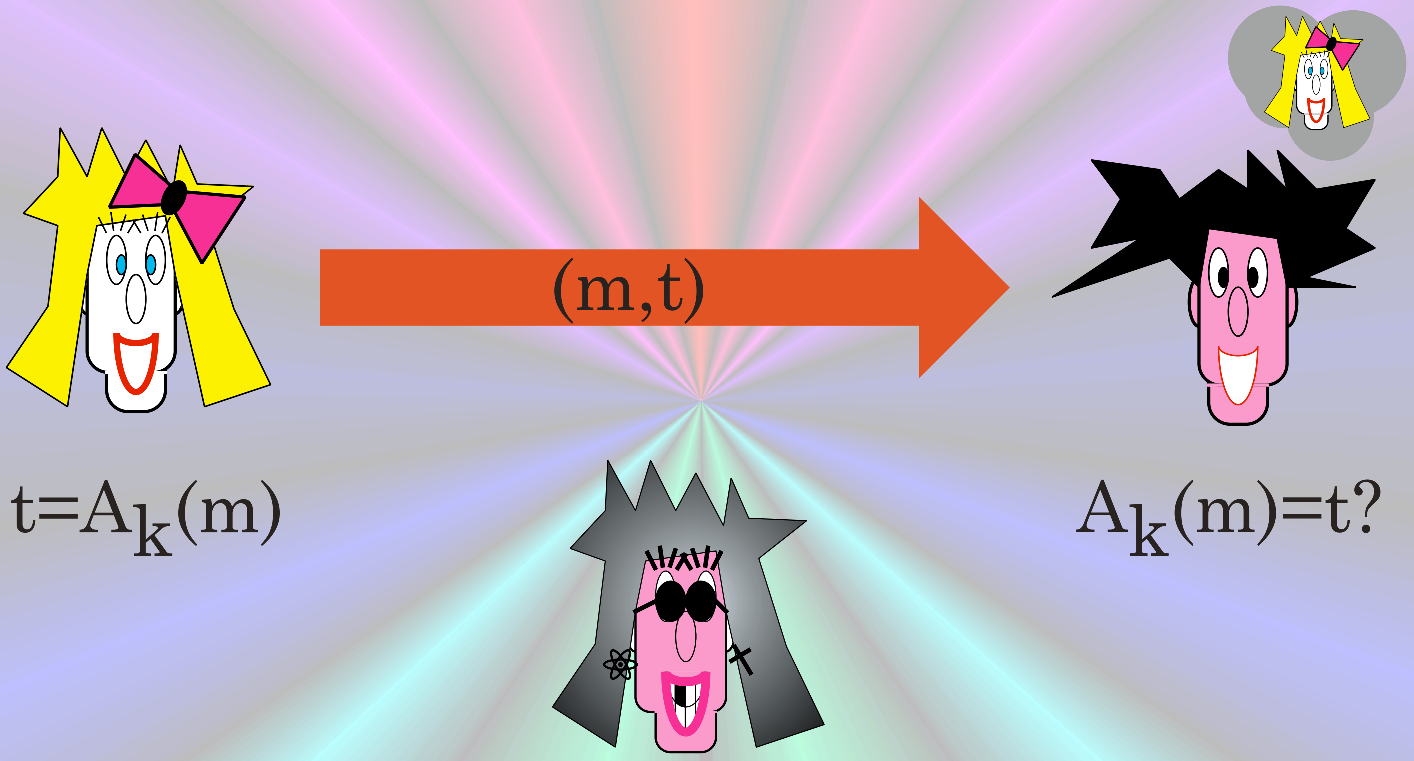


symmetric authentication



Information Theoretical Security

Authentication



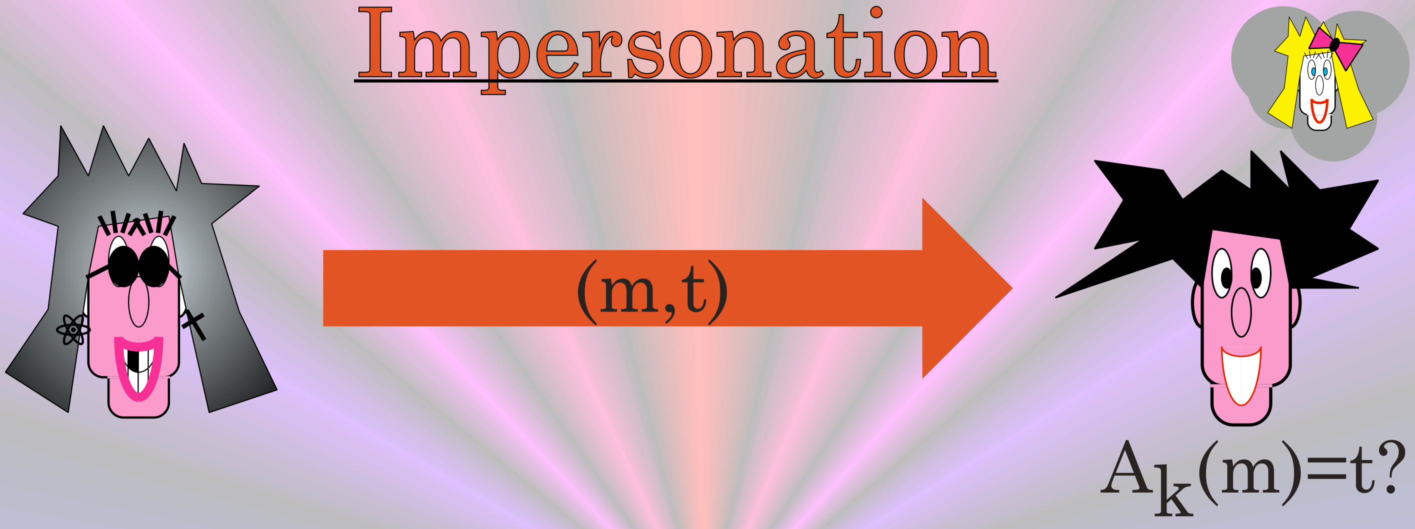
(m,t)

$t=A_k(m)$

$A_k(m)=t?$

Information Theoretical Security

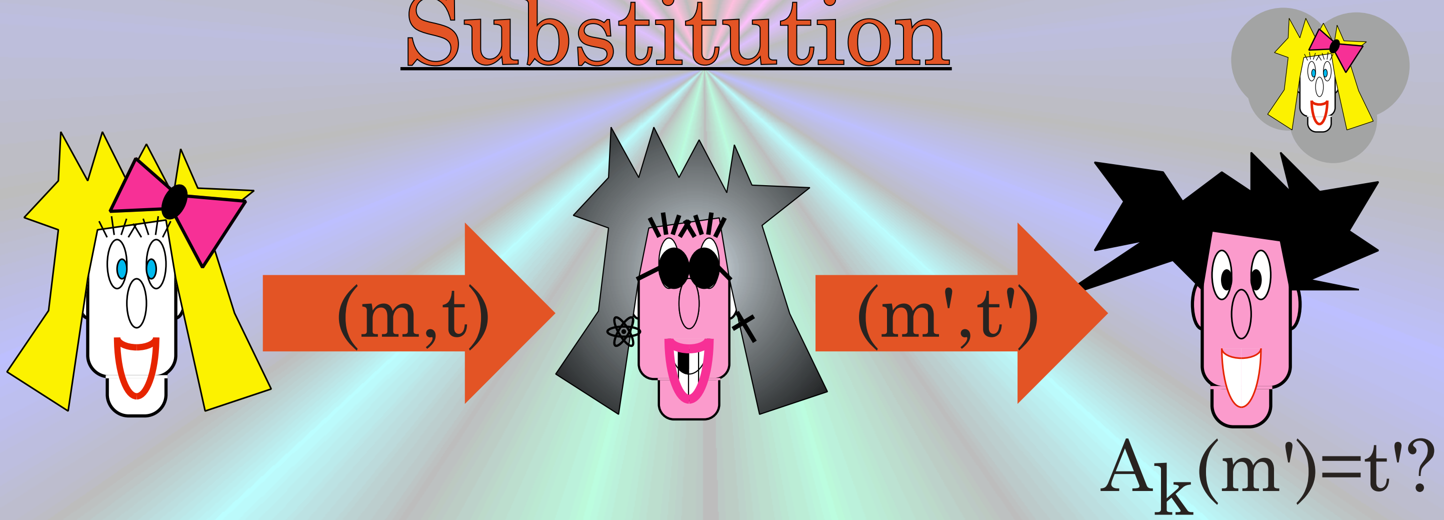
Impersonation



(m,t)

$A_k(m)=t$?

Substitution



(m,t)

(m',t')

$A_k(m')=t'$?

Information Theoretical Security

Wegman-Carter 1×-Authentication

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

$$|m| = n,\ \ |\mathbf{M}| = n\square s,\ \ |t| = |b| = s$$

$\square m \square M, \square t \square T$

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

$\square m \quad m' \square M, \square t,t' \square T$

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

Wegman-Carter 1×-Authentication and (linear) error correction

$$t = \mathbf{M}m \oplus b$$

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

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

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

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

Gemmel-Naor 1x-Authentication

$$t = A_k(m)$$

$|m| = n,\ |k| = \lg(n) + 5s,\ |t| = s$

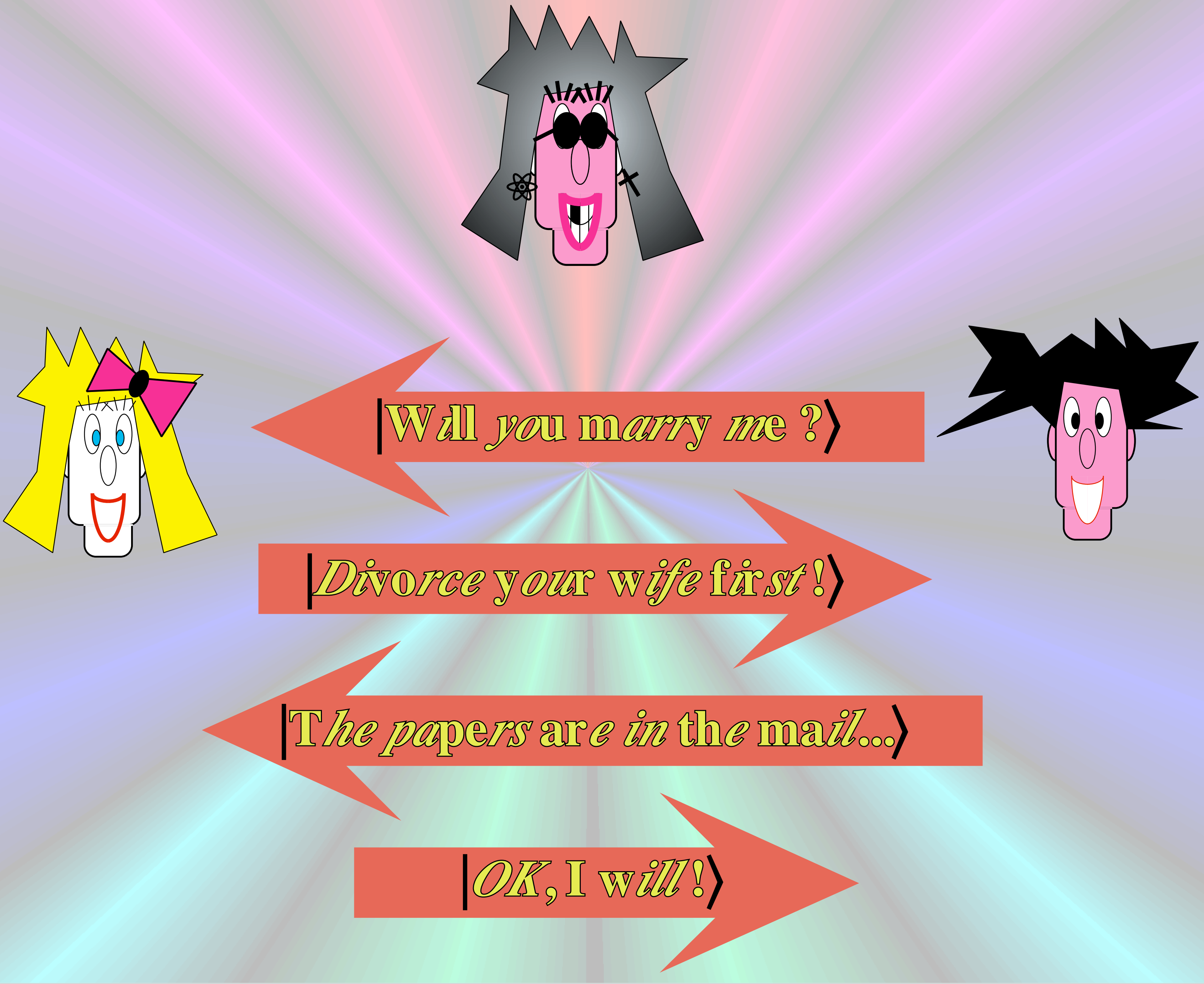
□m□M,□t□T

Pr(A_k(m)=t) □ 1/|T|= $1/2^{s-1}$

□m m'□M,□t,t'□T

Pr(A_k(m')=t' | A_k(m)=t) □ 1/|T|= $1/2^{s-1}$

(3)
Quantum Authentication



|Will you marry me ?⟩

|Divorce your wife first !⟩

|The papers are in the mail...⟩

|OK, I will !⟩

One-time Q-Authentication

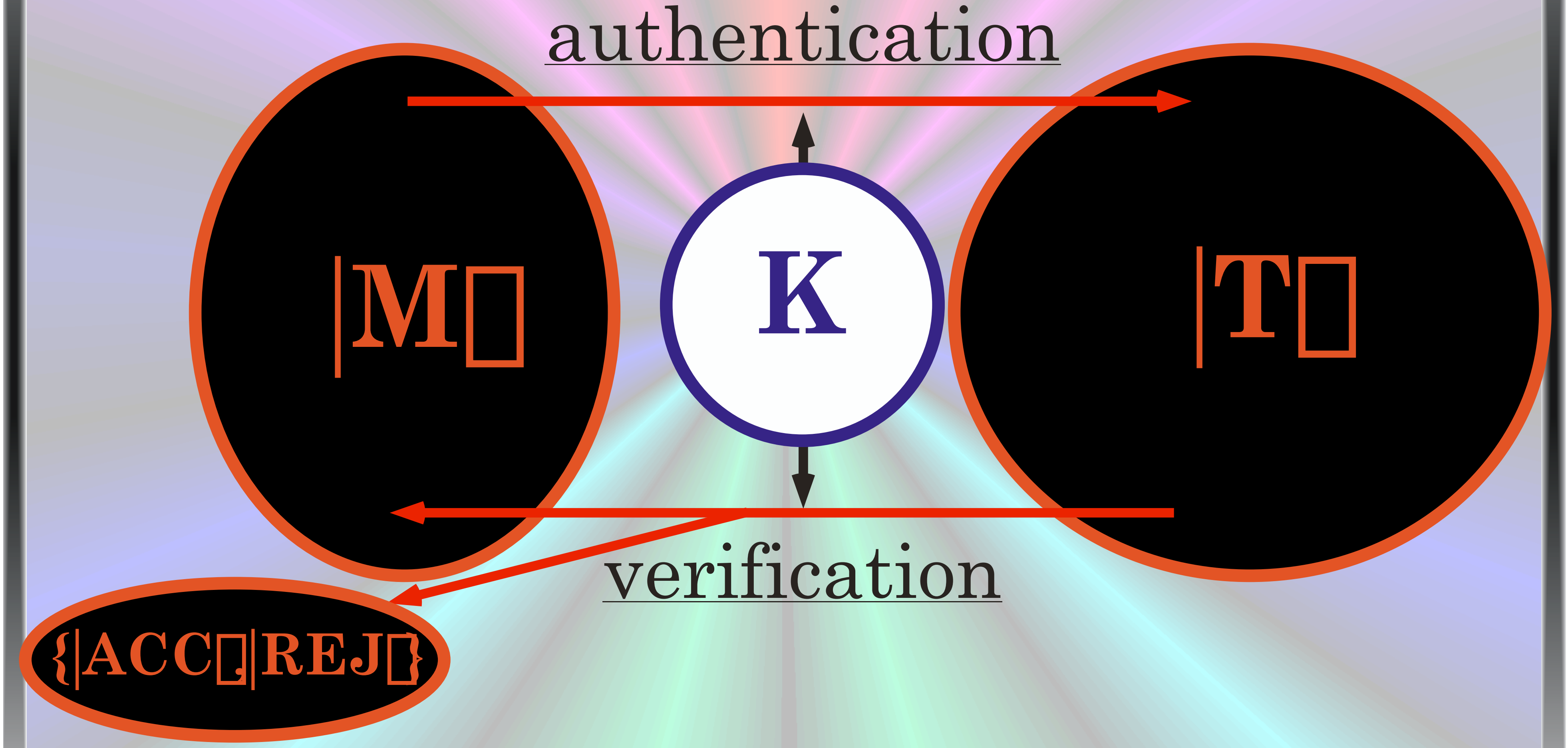
|8PYδεϑωτΥ5θκΛααƎεσ!T9≅⟩

|I(Δ%λεΞηΔκθΙιψκλ#Hι2χς7δξEωνMσ⟩

|H&φσ≅τψϖΦηαΟυδυδδΚπTρΓβλ.Z/ρYιη*⟩

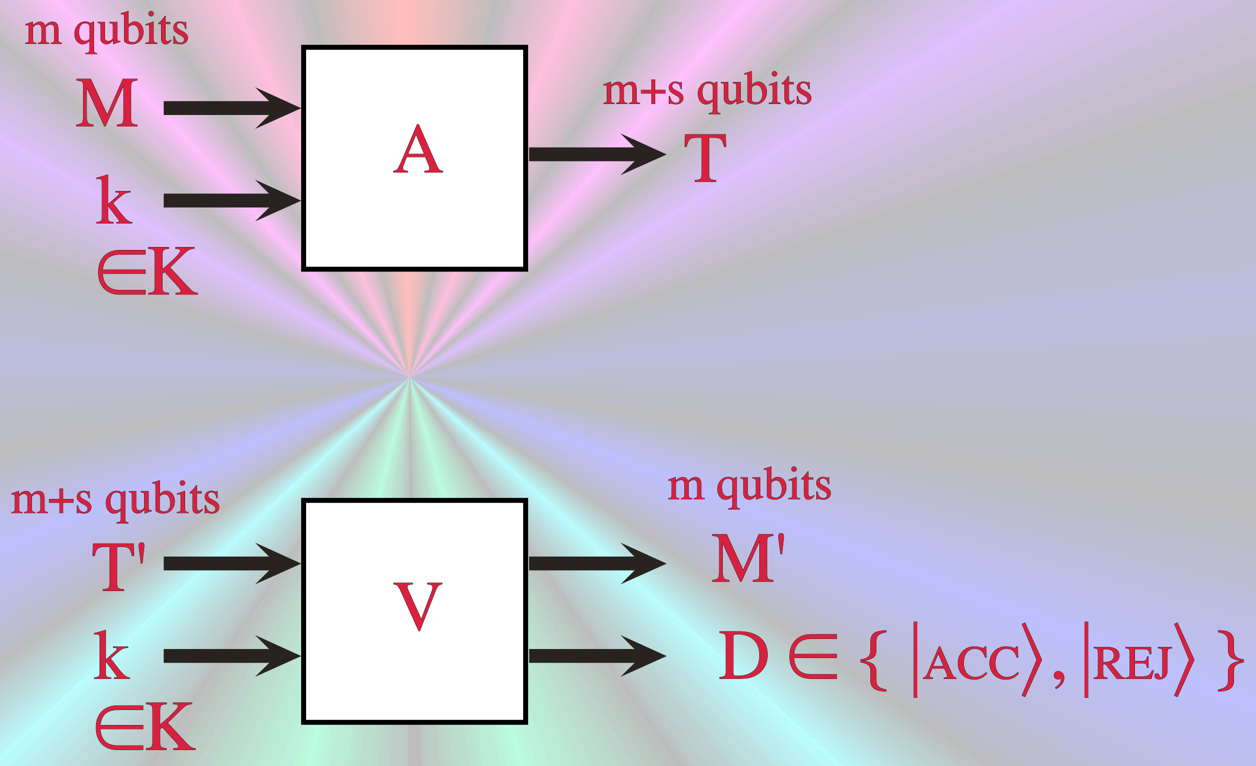
|B7Bασρδ3τδσΤτζφΥιλα⟩

symmetric authentication of Quantum Messages



Information Theoretical Security

One-time Q-Authentication



m qubits

M

k

$\in K$

A

m+s qubits

T

m+s qubits

T'

k

$\in K$

V

m qubits

M'

$D \in \{ |\text{ACC}\rangle, |\text{REJ}\rangle \}$

One-time Q-Authentication

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

- output <u>Right</u> if $M'=|\psi\rangle$ or if $D=|\text{REJ}\rangle$
- output <u>Wrong</u> otherwise

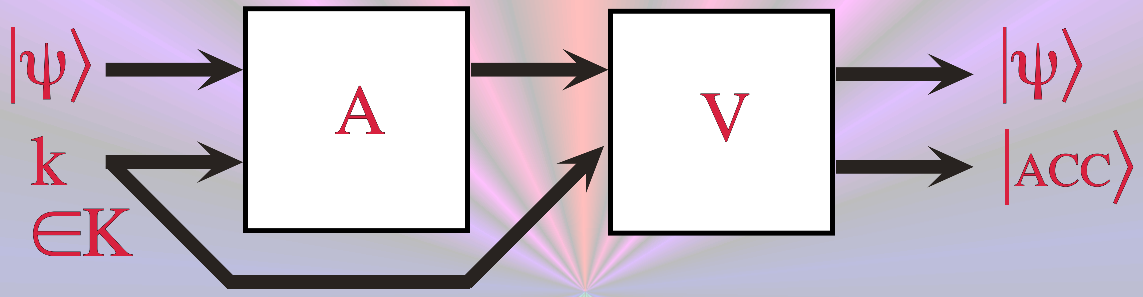
The corresponding projectors are

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

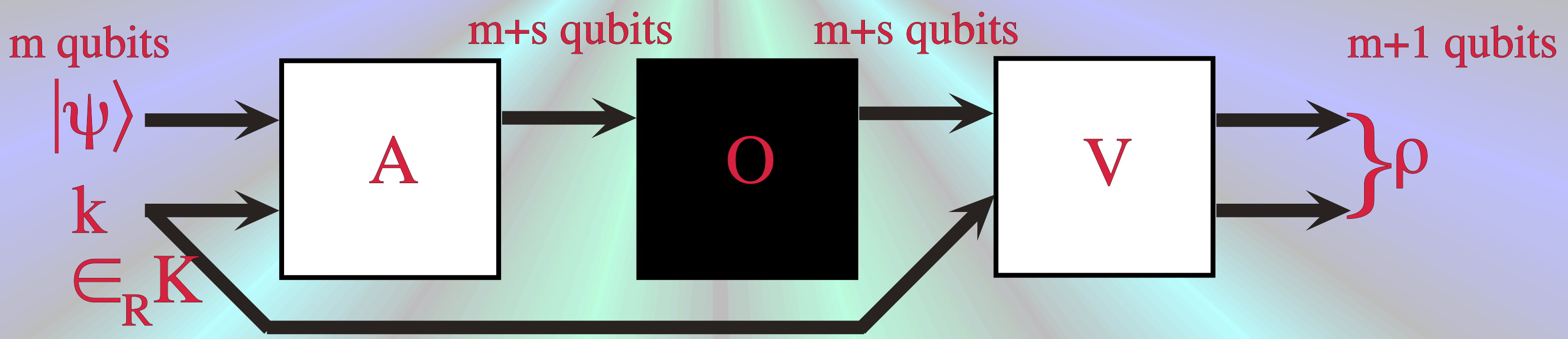
$$W_{|\psi\rangle}= (I_{M'} - |\psi\rangle\langle\psi|)\otimes|\text{ACC}\rangle\langle\text{ACC}|$$

One-time Q-Authentication

Completeness:

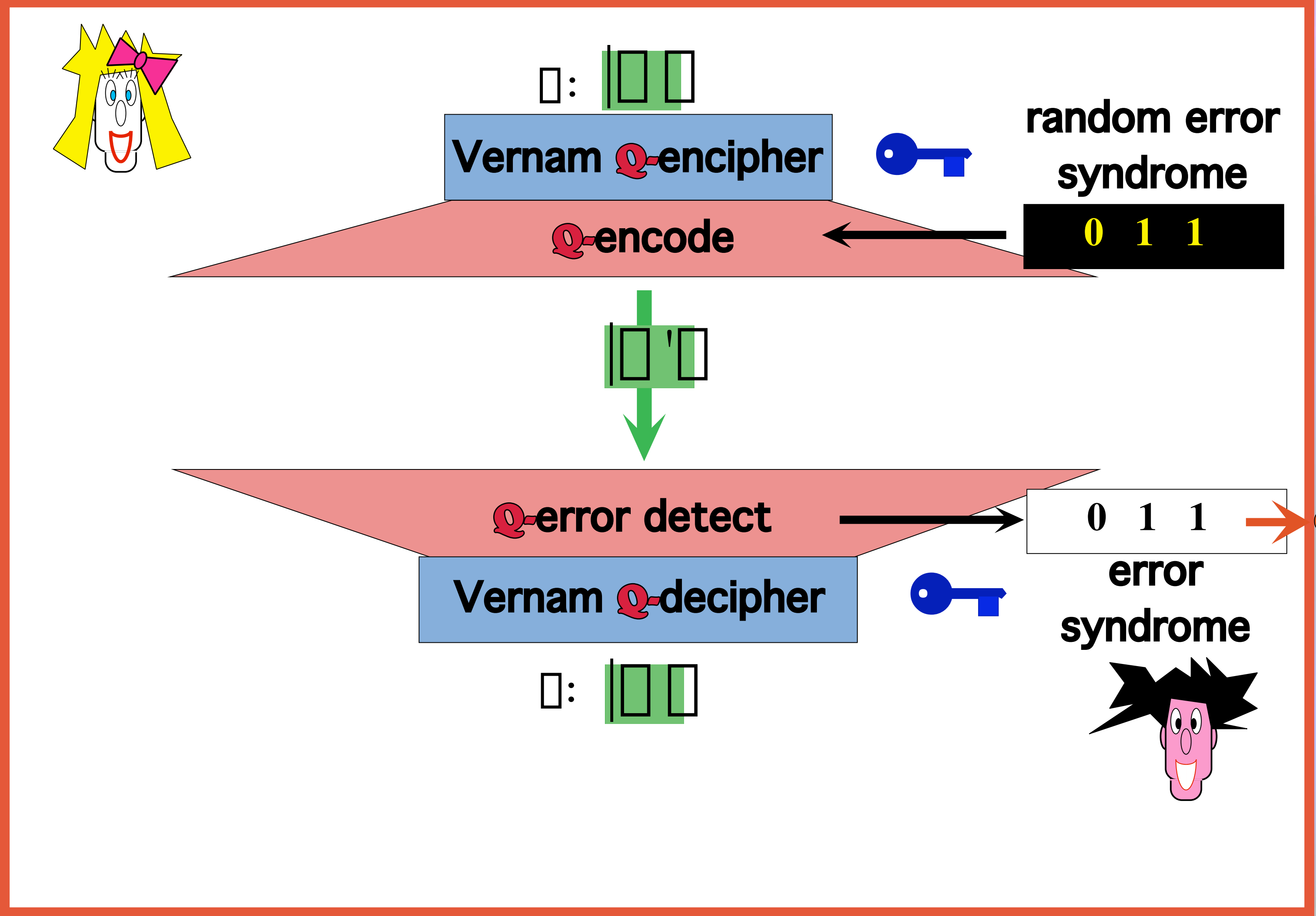


Soundness:



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

One-time Q-Authentication



□: |□ □

Vernam Q-encipher

Q-encode

random error syndrome

0 1 1

|□ '□

Q-error detect

Vernam Q-decipher

0 1 1

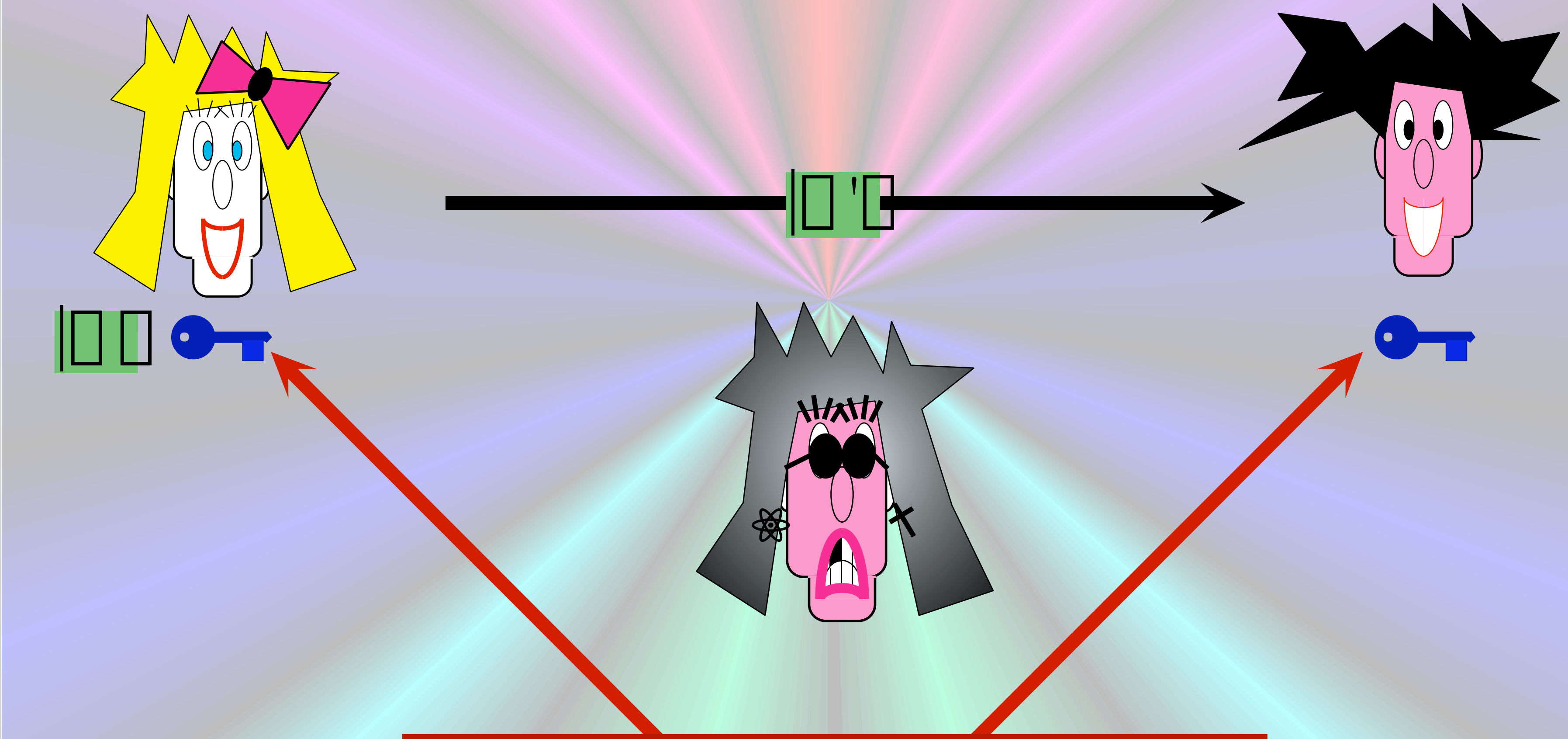
error?

error syndrome

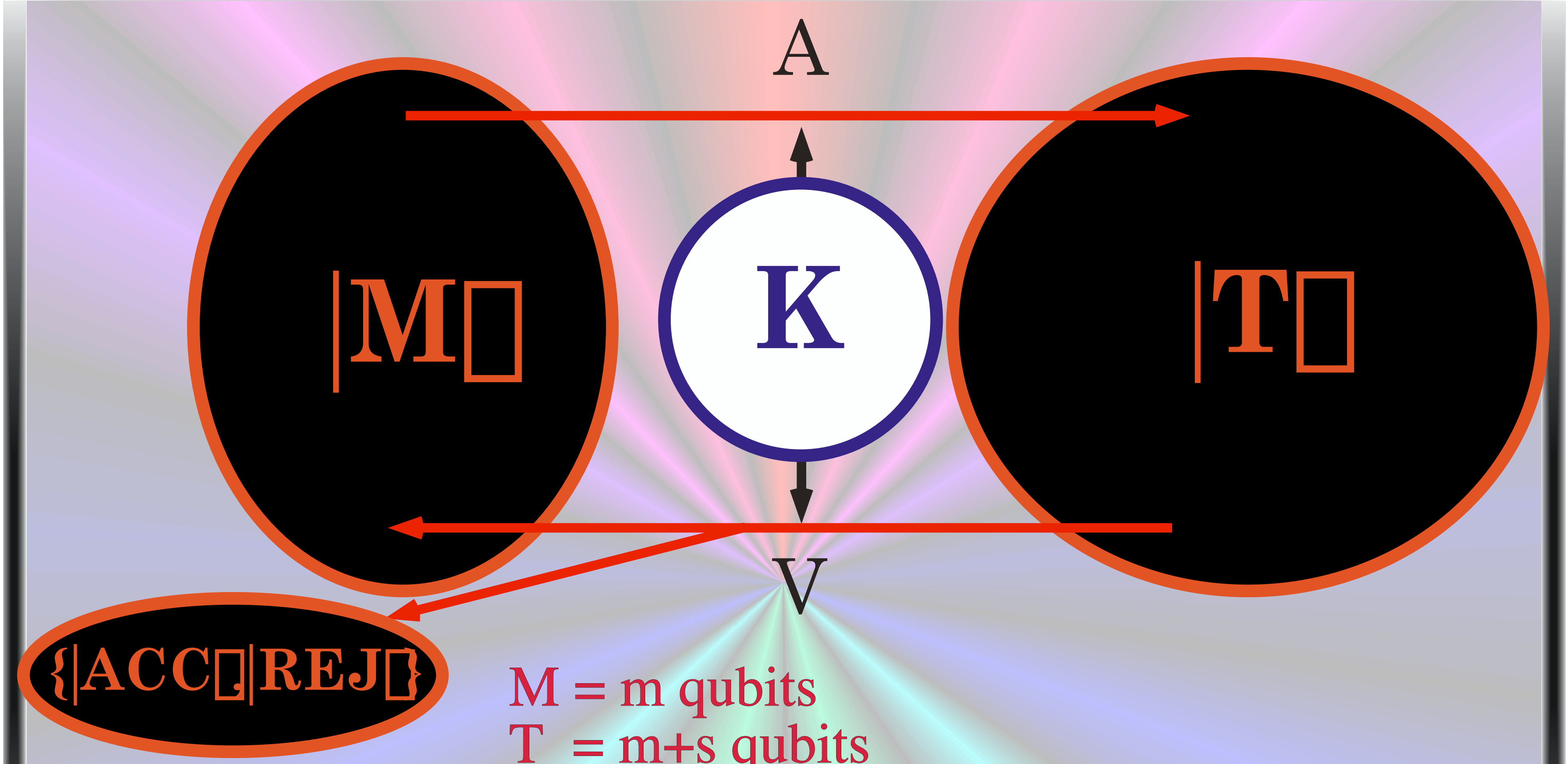
□: |□ □

Barnum-Crépeau-Gottesman-Smith-Tapp

One-time Q-Authentication



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



M = m qubits
T = m+s qubits
K = 2m + 2(lg(m)+5s) + 2s BITS
= 2(m+s + lg(m)+5s) BITS

2m = M's encryption key
2(lg(m)+5s) = code description
2s = syndrome randomizer

(4)
Quantum Codes Correcting* 1 Arbitrary Error out of 3 positions

*except with small probability

Q: (over GF(3))

$$\begin{array}{l}|0\rangle \to |000\rangle + |111\rangle + |222\rangle \\ |1\rangle \to |012\rangle + |120\rangle + |201\rangle \\ |2\rangle \to |021\rangle + |102\rangle + |210\rangle\end{array}$$

fixed

Q=[[3,1,2]] corrects one erasure.

$$Q|\psi\rangle = H_1 \otimes H_2 \otimes H_3$$

$\mathcal{Q}$: (over GF(q), q»3)

$$\mathcal{H}_1=\langle A_{K_1}(H_1),K_2,K_3\rangle$$
$$\mathcal{H}_2=\langle A_{K_2}(H_2),K_3,K_1\rangle$$
$$\mathcal{H}_3=\langle A_{K_3}(H_3),K_1,K_2\rangle$$

fixed

$\mathcal{Q}$=[[3,1,2]] correcting one arbitrary error!

$$\mathcal{Q}|\psi\rangle=\mathcal{H}_1\otimes\mathcal{H}_2\otimes\mathcal{H}_3$$

If zero/one error occurred (case 1)

but all keys K_1, K_2, K_3 **agree in** $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$

CASE 1)

$$\mathcal{H}_1 = \langle A_{K_1}(H_1), K_2, K_3 \rangle$$
$$\mathcal{H}_2 = \langle A_{K_2}(H_2), K_3, K_1 \rangle$$
$$\mathcal{H}_3 = \langle A_{K_3}(H_3), K_1, K_2 \rangle$$

If zero/one error occurred (case 1)

but all keys K_1, K_2, K_3 agree in $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$

CASE 1)

$$\mathcal{H}_1 = \langle A_{K_1}(H_1), K_2, K_3 \rangle$$
$$\mathcal{H}_2 = \langle A_{K_2}(H_2), K_3, K_1 \rangle$$
$$\mathcal{H}_3 = \langle A_{K_3}(H_3), K_1, K_2 \rangle$$

- using keys K_1, K_2, K_3

try to get H_1 from $\mathcal{H}_1$, H_2 from $\mathcal{H}_2$, H_3 from $\mathcal{H}_3$

If zero/one error occurred (case 1)

but all keys K_1, K_2, K_3 agree in $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$

CASE 1)

$$\mathcal{H}_1 = \langle A_{K_1}(H_1), K_2, K_3 \rangle$$
$$\mathcal{H}_2 = \langle A_{K_2}(H_2), K_3, K_1 \rangle$$
$$\mathcal{H}_3 = \langle A_{K_3}(H_3), K_1, K_2 \rangle$$

- using keys K_1, K_2, K_3

try to get H_1 from $\mathcal{H}_1$, H_2 from $\mathcal{H}_2$, H_3 from $\mathcal{H}_3$

- at most one quantum authentication may fail

If zero/one error occurred (case 1)

but all keys K_1, K_2, K_3 agree in $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$

CASE 1)

$$\mathcal{H}_1 = \langle A_{K_1}(H_1), K_2, K_3 \rangle$$
$$\mathcal{H}_2 = \langle A_{K_2}(H_2), K_3, K_1 \rangle$$
$$\mathcal{H}_3 = \langle A_{K_3}(H_3), K_1, K_2 \rangle$$

- using keys K_1, K_2, K_3

try to get H_1 from $\mathcal{H}_1$, H_2 from $\mathcal{H}_2$, H_3 from $\mathcal{H}_3$

- at most one quantum authentication may fail

- using Q's algorithm for correcting one erasure

get $|\psi\rangle$ from $\varnothing \otimes H_2 \otimes H_3$, $H_1 \otimes \varnothing \otimes H_3$ or $H_1 \otimes H_2 \otimes \varnothing$

CASE 1)

$\mathcal{H}_1=\langle A_{K_1}(H_1),K_2,K_3\rangle$

$\mathcal{H}_2=\langle A_{K_2}(H_2),K_3,K_1\rangle$

$\mathcal{H}_3=\langle A_{K_3}(H_3),K_1,K_2\rangle$

CASE 2)

$\mathcal{H}_\mathbf{a}=\langle A_{K_\mathbf{a}}(H_\mathbf{a}),K_\mathbf{i},K_\mathbf{b}\rangle$

~~$\mathcal{H}_\mathbf{i}=\langle A_{K_\mathbf{i}}(H_\mathbf{i}),K_\mathbf{b},K_\mathbf{a}\rangle$~~

$\mathcal{H}_\mathbf{b}=\langle A_{K_\mathbf{b}}(H_\mathbf{b}),K_\mathbf{a},K_\mathbf{i}\rangle$

CASE 3)

~~$\mathcal{H}_\mathbf{a}=\langle A_{K_\mathbf{a}}(H_\mathbf{a}),K_\mathbf{i},K_\mathbf{b}\rangle$~~

$\mathcal{H}_\mathbf{i}=\langle A_{K_\mathbf{i}}(H_\mathbf{i}),K_\mathbf{b},K_\mathbf{a}\rangle$

~~$\mathcal{H}_\mathbf{b}=\langle A_{K_\mathbf{b}}(H_\mathbf{b}),K_\mathbf{a},K_\mathbf{i}\rangle$~~

If one error occurred (case 2)

but for some *i* the keys K_a,K_b, $a \neq i \neq b$ disagree in $\mathcal{H}_b$ vs $\mathcal{H}_i$, and in $\mathcal{H}_a$ vs $\mathcal{H}_i$

($\mathcal{H}_i$ must be wrong)

CASE 2)

$$\mathcal{H}_a = \langle A_{K_a}(H_a), K_i, K_b \rangle$$
$$\mathcal{H}_i = \langle A_{K_i}(H_i), K_b, K_a \rangle$$
$$\mathcal{H}_b = \langle A_{K_b}(H_b), K_a, K_i \rangle$$

If one error occurred (case 2)

but for some *i* the keys K_a, K_b, $a \neq i \neq b$ disagree in $\mathcal{H}_b$ vs $\mathcal{H}_i$, and in $\mathcal{H}_a$ vs $\mathcal{H}_i$

($\mathcal{H}_i$ must be wrong)

- using keys K_a in $\mathcal{H}_b$, and K_b in $\mathcal{H}_a$ get H_a from $\mathcal{H}_a$, H_b from $\mathcal{H}_b$

CASE 2)

$$\begin{aligned}
\mathcal{H}_a &= \langle A_{K_a}(H_a), K_i, K_b \rangle \\
\mathcal{H}_i &= \langle A_{K_i}(H_i), K_b, K_a \rangle \\
\mathcal{H}_b &= \langle A_{K_b}(H_b), K_a, K_i \rangle
\end{aligned}$$

If one error occurred (case 2)

but for some i the keys K_a, K_b, $a\neq i\neq b$ disagree in $\mathcal{H}_b$ vs $\mathcal{H}_i$, and in $\mathcal{H}_a$ vs $\mathcal{H}_i$

($\mathcal{H}_i$ must be wrong)

- using keys K_a in $\mathcal{H}_b$, and K_b in $\mathcal{H}_a$ get H_a from $\mathcal{H}_a$, H_b from $\mathcal{H}_b$

- no Q-authentication may fail since error at i

If one error occurred (case 2)

but for some i the keys K_a, K_b, $a \neq i \neq b$ disagree in $\mathcal{H}_b$ vs $\mathcal{H}_i$, and in $\mathcal{H}_a$ vs $\mathcal{H}_i$

($\mathcal{H}_i$ must be wrong)

- using keys K_a in $\mathcal{H}_b$, and K_b in $\mathcal{H}_a$ get H_a from $\mathcal{H}_a$, H_b from $\mathcal{H}_b$

- no Q-authentication may fail since error at i

- using Q's algorithm for correcting one erasure get $|\psi\rangle$ from $\varnothing \otimes H_2 \otimes H_3$, $H_1 \otimes \varnothing \otimes H_3$ or $H_1 \otimes H_2 \otimes \varnothing$

If one error occurred (case 3)

but for some *i* only key K_i disagree in $\mathcal{H}_a$ vs $\mathcal{H}_b$, $a \neq i \neq b$. ($\mathcal{H}_i$ must be right)

CASE 3)

~~$\mathcal{H}_a = \langle A_{K_a}(H_a), K_i, K_b \rangle$~~

$\mathcal{H}_i = \langle A_{K_i}(H_i), K_b, K_a \rangle$

~~$\mathcal{H}_b = \langle A_{K_b}(H_b), K_a, K_i \rangle$~~

If one error occurred (case 3)

but for some i only key K_i disagree in $\mathcal{H}_a$ vs $\mathcal{H}_b$, $a{\neq}i{\neq}b$. ($\mathcal{H}_i$ must be right)

- using keys K_a in $\mathcal{H}_i$, and K_b in $\mathcal{H}_i$

try to get H_a from $\mathcal{H}_a$, H_b from $\mathcal{H}_b$

CASE 3)

$$\mathcal{H}_a = \langle A_{K_a}(H_a), K_i, K_b \rangle$$

$$\mathcal{H}_i = \langle A_{K_i}(H_i), K_b, K_a \rangle$$

$$\mathcal{H}_b = \langle A_{K_b}(H_b), K_a, K_i \rangle$$

If one error occurred (case 3)

but for some *i* only key K_i disagree in $\mathcal{H}_a$ vs $\mathcal{H}_b$, $a \neq i \neq b$. ($\mathcal{H}_i$ must be right)

- using keys K_a in $\mathcal{H}_i$, and K_b in $\mathcal{H}_i$ try to get H_a from $\mathcal{H}_a$, H_b from $\mathcal{H}_b$
- at most one quantum authentication may fail

CASE 3)

$$\mathcal{H}_a = \langle A_{K_a}(H_a), K_i, K_b \rangle$$
$$\mathcal{H}_i = \langle A_{K_i}(H_i), K_b, K_a \rangle$$
$$\mathcal{H}_b = \langle A_{K_b}(H_b), K_a, K_i \rangle$$

If one error occurred (case 3)

but for some i only key K_i disagree in $\mathcal{H}_a$ vs $\mathcal{H}_b$, $a \neq i \neq b$. ($\mathcal{H}_i$ must be right)

- using keys K_a in $\mathcal{H}_i$, and K_b in $\mathcal{H}_i$ try to get H_a from $\mathcal{H}_a$, H_b from $\mathcal{H}_b$

- at most one quantum authentication may fail

- if authentication fails at a (or b) then use key K_i in $\mathcal{H}_b$ ($\mathcal{H}_a$), and get H_i from $\mathcal{H}_i$

If one error occurred (case 3)

but for some i only key K_i disagree in $\mathcal{H}_a$ vs $\mathcal{H}_b$, $a \neq i \neq b$. ($\mathcal{H}_i$ must be right)

- using keys K_a in $\mathcal{H}_i$, and K_b in $\mathcal{H}_i$ try to get H_a from $\mathcal{H}_a$, H_b from $\mathcal{H}_b$
- at most one quantum authentication may fail
- if authentication fails at a (or b) then use key K_i in $\mathcal{H}_b$ ($\mathcal{H}_a$), and get H_i from $\mathcal{H}_i$
- using Q's algorithm for correcting one erasure get $|\psi\rangle$ from $\varnothing \otimes H_2 \otimes H_3$, $H_1 \otimes \varnothing \otimes H_3$ or $H_1 \otimes H_2 \otimes \varnothing$

(5)
Classical Secret Sharing

Classical Secret Sharing

$SS_{n,t}[K]$ = set of n-tuples of values s.t.

- any ≤t-1 values = no info about K
- any ≥t values = full info about K.

$$SS_{n,t}[K] =$$

$$\{ \langle p(1), p(2), \ldots, p(n) \rangle \mid$$

$$p(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \ldots + a_1 x + K,$$

$$a_{t-1}, a_{t-2}, \ldots, a_1 \in GF(q), q \geq n \}$$

(6)

Quantum Codes Correcting* up to (n-1)/2 Arbitrary Errors out of n positions

*except with small probability

Ingredients

Quantum Authentication Scheme:

$$|\psi\rangle, K \rightarrow A_K(|\psi\rangle)$$

Classical Authentication Scheme:

$$\mathbf{m}, \kappa \rightarrow (\mathbf{m}, \alpha_\kappa(\mathbf{m}))$$

Classical Secret Sharing Scheme:

$$\langle \mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_\mathbf{n} \rangle \in_\mathbf{R} \mathbf{SS}_{\mathbf{n,t}}[\mathbf{K}]$$

$\mathcal{Q}$: (over GF(q), q»3)

$$\mathcal{H}_1=\langle A_{K_1}(H_1),\mathbf{s}_1,\alpha_{\kappa_{\mathbf{21}}}(\mathbf{s}_1),\alpha_{\kappa_{\mathbf{31}}}(\mathbf{s}_1),\kappa_{12},\kappa_{13}\rangle$$
$$\mathcal{H}_2=\langle A_{K_2}(H_2),\mathbf{s}_2,\alpha_{\kappa_{\mathbf{32}}}(\mathbf{s}_2),\alpha_{\kappa_{\mathbf{12}}}(\mathbf{s}_2),\kappa_{23},\kappa_{21}\rangle$$
$$\mathcal{H}_3=\langle A_{K_3}(H_3),\mathbf{s}_3,\alpha_{\kappa_{\mathbf{13}}}(\mathbf{s}_3),\alpha_{\kappa_{\mathbf{23}}}(\mathbf{s}_3),\kappa_{31},\kappa_{32}\rangle$$

fixed

$\mathcal{Q}$=[[3,1,2]] **correcting one arbitrary error!**

$$\mathcal{Q}|\psi\rangle=\mathcal{H}_1\otimes\mathcal{H}_2\otimes\mathcal{H}_3$$

$$\langle \mathbf{s}_1,\mathbf{s}_2,\mathbf{s}_3\rangle \in_{\mathbf{R}} \mathbf{SS}_{\mathbf{3,2}}[\mathbf{K}_1:\mathbf{K}_2:\mathbf{K}_3]$$

def: s_i is valid if at most ONE classical authentication of it fails.

$$\mathcal{H}_1=\langle A_{K_1}(H_1),\mathbf{s}_1,\alpha_{\kappa_{21}}(\mathbf{s}_1),\alpha_{\kappa_{31}}(\mathbf{s}_1),\kappa_{12},\kappa_{13}\rangle$$
$$\mathcal{H}_2=\langle A_{K_2}(H_2),\mathbf{s}_2,\alpha_{\kappa_{32}}(\mathbf{s}_2),\alpha_{\kappa_{12}}(\mathbf{s}_2),\kappa_{23},\kappa_{21}\rangle$$
$$\mathcal{H}_3=\langle A_{K_3}(H_3),\mathbf{s}_3,\alpha_{\kappa_{13}}(\mathbf{s}_3),\alpha_{\kappa_{23}}(\mathbf{s}_3),\kappa_{31},\kappa_{32}\rangle$$

def: s_i is valid if at most ONE classical authentication of it fails.

claim: $\#\{\, i \mid s_i$ is valid $\} \geq 2$

$$\mathcal{H}_1=\langle A_{K_1}(H_1),s_1,\alpha_{\kappa_{21}}(s_1),\alpha_{\kappa_{31}}(s_1),\kappa_{12},\kappa_{13}\rangle$$
$$\mathcal{H}_2=\langle A_{K_2}(H_2),s_2,\alpha_{\kappa_{32}}(s_2),\alpha_{\kappa_{12}}(s_2),\kappa_{23},\kappa_{21}\rangle$$
$$\mathcal{H}_3=\langle A_{K_3}(H_3),s_3,\alpha_{\kappa_{13}}(s_3),\alpha_{\kappa_{23}}(s_3),\kappa_{31},\kappa_{32}\rangle$$

def: s_i is valid if at most ONE classical authentication of it fails.

claim: $\#\{\, i \mid s_i$ is valid $\} \geq 2$

$[K_1 \colon K_2 \colon K_3]$ is recovered from $\{\, s_i$ is valid $\}$

$$\mathcal{H}_1 = \langle A_{K_1}(H_1), s_1, \alpha_{\kappa_{21}}(s_1), \alpha_{\kappa_{31}}(s_1), \kappa_{12}, \kappa_{13} \rangle$$
$$\mathcal{H}_2 = \langle A_{K_2}(H_2), s_2, \alpha_{\kappa_{32}}(s_2), \alpha_{\kappa_{12}}(s_2), \kappa_{23}, \kappa_{21} \rangle$$
$$\mathcal{H}_3 = \langle A_{K_3}(H_3), s_3, \alpha_{\kappa_{13}}(s_3), \alpha_{\kappa_{23}}(s_3), \kappa_{31}, \kappa_{32} \rangle$$

def: s_i is valid if at most ONE classical authentication of it fails.

claim: #{ i | s_i is valid } ≥ 2

$[K_1:K_2:K_3]$ is recovered from { s_i is valid }

- using keys K_1, K_2, K_3 try to get H_1 from $\mathcal{H}_1$, H_2 from $\mathcal{H}_2$, H_3 from $\mathcal{H}_3$

- at most one quantum authentication may fail

- using Q's algorithm for correcting one erasure get $|\psi\rangle$ from $\emptyset \otimes H_2 \otimes H_3$, $H_1 \otimes \emptyset \otimes H_3$ or $H_1 \otimes H_2 \otimes \emptyset$

Generalization

Q: (over GF(q))

fixed

Q=[[n,k,d]] corrects d-1<$n/2$ erasures

$Q|\psi\rangle = H_1 \otimes H_2 \otimes H_3 \otimes \ldots \otimes H_n$

$\mathcal{Q}$: (over GF(q'), $q' \gg q$)

$\mathcal{H}_{\mathbf{1}},\ldots,\mathcal{H}_{\mathbf{i}},\ldots,\mathcal{H}_{\mathbf{n}}$

$$\mathcal{H}_{\mathbf{i}} = \langle A_{K_i}(H_{\mathbf{i}}), s_{\mathbf{i}},$$
$$\alpha_{K_{1i}}(s_{\mathbf{i}}),\ldots,\alpha_{K_{(i-1)i}}(s_{\mathbf{i}}),\alpha_{K_{(i+1)i}}(s_{\mathbf{i}}),\ldots,\alpha_{K_{ni}}(s_{\mathbf{i}}),$$
$$K_{\mathbf{i1}},\ldots,K_{\mathbf{i(i-1)}},K_{\mathbf{i(i+1)}},\ldots,K_{\mathbf{in}}\rangle$$

$\mathcal{Q}$=[[n,k,d]] correcting d-1arbitrary errors!

$$\mathcal{Q}|\psi\rangle = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_{\mathbf{n}}$$

$$\langle s_1, s_2, \ldots, s_{\mathbf{n}}\rangle \in_{\mathbf{R}} SS_{\mathbf{n,n-d}}[K_1:K_2:K_3:\ldots:K_{\mathbf{n}}]$$

def: S_i is valid if at most $\overset{\text{fixed}}{d\text{-}1}$ classical authentication of it fails.

claim: $\#\{\, i \mid S_i$ is valid $\} \geq n\text{-}\overset{\text{fixed}}{d\text{+}1} \geq n/2$

$[K_1:K_2:K_3:\ldots:K_n]$ is recovered from $\{\, S_i$ is valid $\}$

- using keys $K_1, K_2, K_3, \ldots, K_n$ try to get each H_i from $\mathcal{H}_i$

- at most d-1 quantum authentications may fail

- using Q's algorithm for correcting $\overset{\text{fixed}}{d\text{-}1}$ erasures get $|\psi\rangle$ from $H_1 \otimes H_2 \otimes \ldots \otimes H_n$, with $\underset{\text{fixed}}{d\text{-}1}$ ∅ parts.

Further Applications and Open Problems

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

● Length n QECC correcting d < n/2 arbitrary errors (with exponentially small probability)

— More natural constructions

— Constructions over smaller fields

Quantum Codes Correcting* up to $(n-1)/2$ arbitrary errors

*except with exponentially small probability

Claude Crépeau

School of Computer Science
McGill University

joint work with

D. Gottesman and A. Smith