

**from Quantum Coding**  
**to Quantum Authenticating,**  
**and back**

**Claude Crépeau**

School of Computer Science  
McGill University



joint work with  
**D. Gottesman and A. Smith**

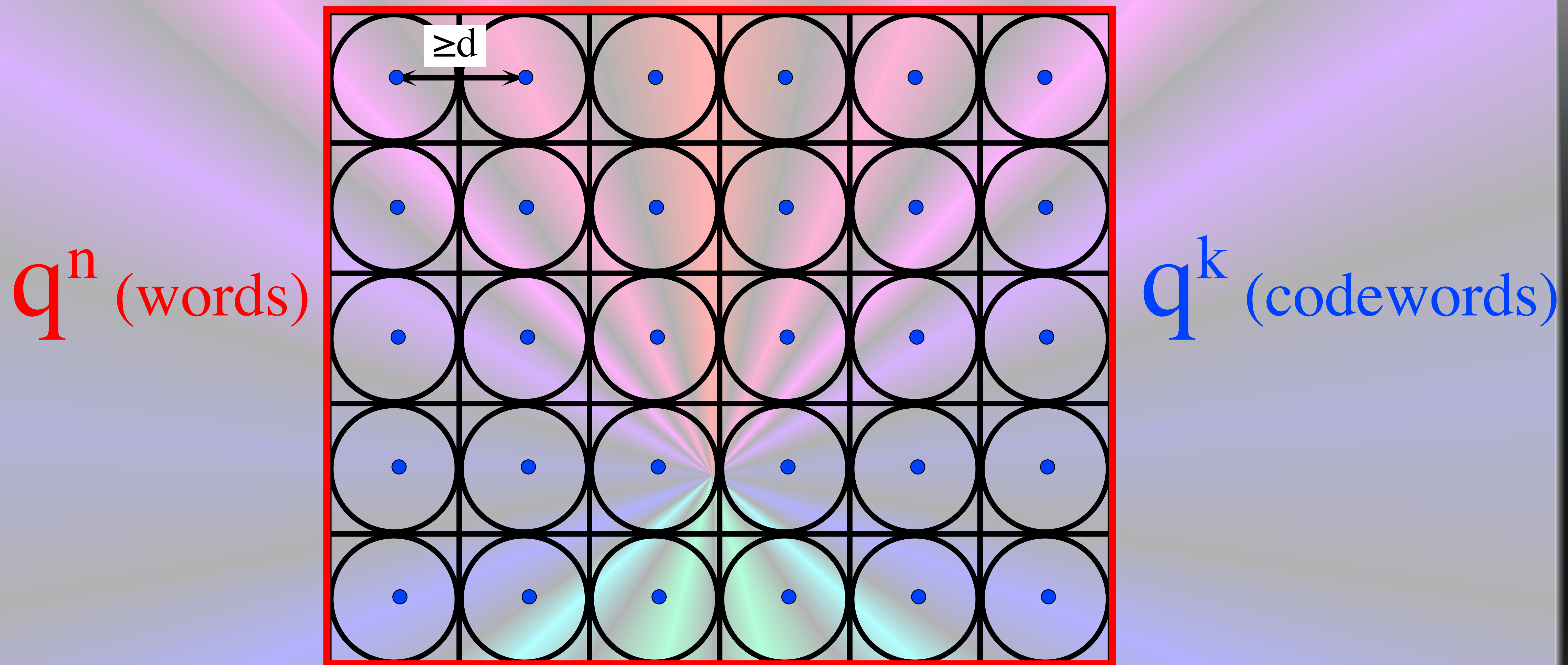


**(0)**

**Classical Error  
Correcting Codes**



# (classical) error-correcting codes



$[n, k, d]$  linear error-correcting code  
length  $n$ , dimension  $k$ ,  
corrects  $d-1$  erasures,  $(d-1)/2$  errors



**(1)**

**Quantum Error  
Correcting Codes**



**Q: (over GF(3))**

$$|0\rangle \rightarrow |000\rangle + |111\rangle + |222\rangle$$

$$|1\rangle \rightarrow |012\rangle + |120\rangle + |201\rangle$$

$$|2\rangle \rightarrow |021\rangle + |102\rangle + |210\rangle$$

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

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

$$|0\rangle \otimes H_2 \otimes H_3 \rightarrow (-H_2 - H_3 \bmod 3) \otimes H_2 \otimes H_3$$

$$H_1 \otimes |0\rangle \otimes H_3 \rightarrow H_1 \otimes (-H_3 - H_1 \bmod 3) \otimes H_3$$

$$H_1 \otimes H_2 \otimes |0\rangle \rightarrow H_1 \otimes H_2 \otimes (-H_1 - H_2 \bmod 3)$$



# Calderbank-Shor-Steane $Q$ -ECCs

Let  $C_1, C_2$  be two linear codes such that

$$\{0\} \subseteq C_2 \subseteq C_1 \subseteq \mathbb{F}^n$$

For  $v \in C_1$  define

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

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

$$\{0\} \subseteq C_1^\perp \subseteq C_2^\perp \subseteq \mathbb{F}^n$$

For  $v \in C_2^\perp$  define

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

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



## CSS Q-ECCs

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

$$\begin{aligned}\dim(Q) &= \dim(C_1) - \dim(C_2^\perp) \\ &= k_1 - k_2^\perp \\ &= \dim(C_2) - \dim(C_1) = \dim(Q^*)\end{aligned}$$

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

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



# CSS Q-ECCs

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

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

If small error probability is acceptable

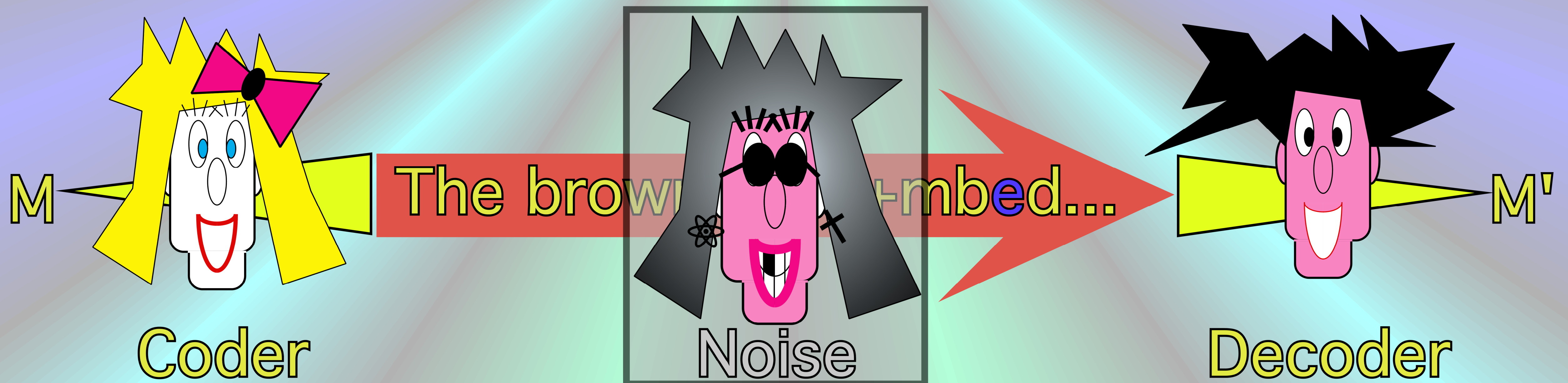


# Error probability of correcting

**is taken over choices\* of code  
but**

**NOT over distribution of errors**

\*All communications **MUST** go through the noisy channel.





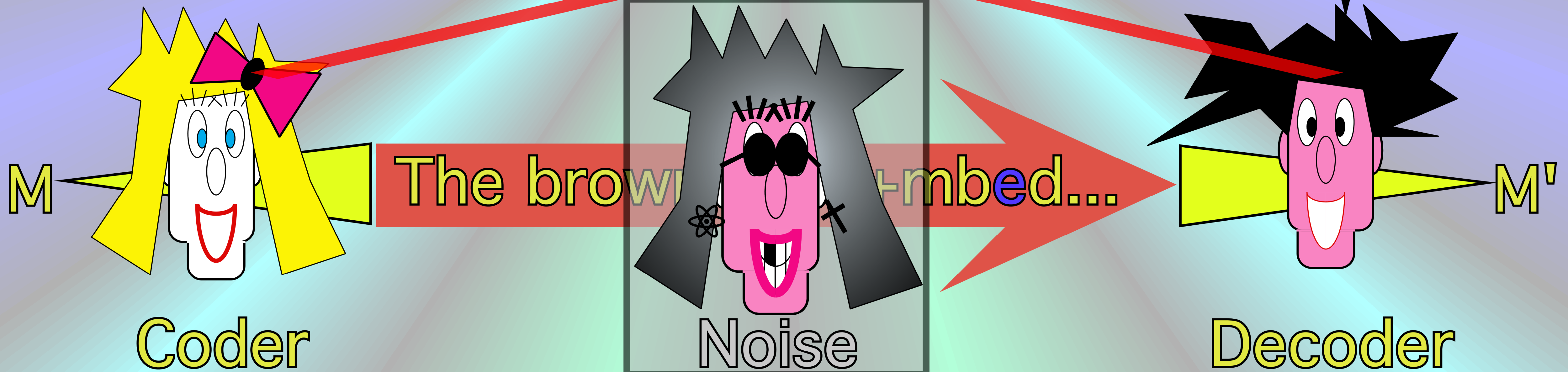
# Error probability of correcting

is taken over choices\* of code  
but

NOT over distribution of errors

\* All communications MUST go through the noisy channel.  
We disallow private channel between coder and decoder.

~~My new secret coding rule is ...~~





**(4)**

**Quantum Codes Correcting\***  
**1 Arbitrary Error out of 3**  
**positions**

**\*except with exponentially small probability**



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

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



$\mathcal{Q} : (\text{over GF}(q), q \gg 3)$

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

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

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

$\mathcal{Q} = [[3, 1, 2]]$  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)

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

- 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 fixing one erasure get  $|\psi\rangle$  from  $|0\rangle \otimes H_2 \otimes H_3$ ,  $H_1 \otimes |0\rangle \otimes H_3$  or  $H_1 \otimes H_2 \otimes |0\rangle$



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)

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

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

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

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 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)

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



# 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  $\mathcal{H}_b$

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 fixing one erasure get  $|\psi\rangle$  from  $|0\rangle \otimes H_2 \otimes H_3, H_1 \otimes |0\rangle \otimes H_3$  or  $H_1 \otimes H_2 \otimes |0\rangle$



# 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 )

CASE 3)

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



# If one error occurred (case 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)**

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



# If one error occurred (case 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)

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



# If one error occurred (case 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 fixing one erasure get  
 $|\psi\rangle$  from  $|0\rangle \otimes H_2 \otimes H_3$ ,  $H_1 \otimes |0\rangle \otimes H_3$  or  $H_1 \otimes H_2 \otimes |0\rangle$



**(5)**

# **Classical Secret Sharing**



# Classical Secret Sharing

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

- any  $\leq t-1$  values = no info about  $K$
- any  $\geq t$  values = full info about  $K$ .

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

$\{ \langle p(\omega_1), p(\omega_2), \dots, p(\omega_n) \rangle \mid$

$$p(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \dots + a_1x + K,$$

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



**(6)**

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

**\*except with exponentially small probability**



# Ingredients

**Quantum Authentication Scheme:**

$$|\psi\rangle, \mathcal{K} \rightarrow A_{\mathcal{K}}(|\psi\rangle)$$

**Classical Authentication Scheme:**

$$\mathbf{m}, \mathcal{K} \rightarrow (\mathbf{m}, \alpha_{\mathcal{K}}(\mathbf{m}))$$

**Classical Secret Sharing Scheme:**

$$\langle \mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_n \rangle \in_{\mathbf{R}} \mathbf{SS}_{n,t}[\mathbf{X}]$$



**$\mathcal{Q}$ : (over  $\text{GF}(q)$ ,  $q \gg 3$ )**

$$\begin{aligned}\mathcal{H}_1 &= \langle A_{\mathbf{K}_1}(\mathbf{H}_1), \mathbf{s}_1, \alpha_{\mathbf{K}_{21}}(\mathbf{s}_1), \alpha_{\mathbf{K}_{31}}(\mathbf{s}_1), \mathbf{K}_{12}, \mathbf{K}_{13} \rangle \\ \mathcal{H}_2 &= \langle A_{\mathbf{K}_2}(\mathbf{H}_2), \mathbf{s}_2, \alpha_{\mathbf{K}_{32}}(\mathbf{s}_2), \alpha_{\mathbf{K}_{12}}(\mathbf{s}_2), \mathbf{K}_{23}, \mathbf{K}_{21} \rangle \\ \mathcal{H}_3 &= \langle A_{\mathbf{K}_3}(\mathbf{H}_3), \mathbf{s}_3, \alpha_{\mathbf{K}_{13}}(\mathbf{s}_3), \alpha_{\mathbf{K}_{23}}(\mathbf{s}_3), \mathbf{K}_{31}, \mathbf{K}_{32} \rangle\end{aligned}$$

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

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

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



**def:  $S_i$  is valid if at most ONE classical authentication of it fails.**

$$\mathcal{H}_1 = \langle A_{K_1}(H_1), S_1, \alpha_{K_{21}}(S_1), \alpha_{K_{31}}(S_1), K_{12}, K_{13} \rangle$$
$$\mathcal{H}_2 = \langle A_{K_2}(H_2), S_2, \alpha_{K_{32}}(S_2), \alpha_{K_{12}}(S_2), K_{23}, K_{21} \rangle$$
$$\mathcal{H}_3 = \langle A_{K_3}(H_3), S_3, \alpha_{K_{13}}(S_3), \alpha_{K_{23}}(S_3), K_{31}, K_{32} \rangle$$



**def:  $S_i$  is valid if at most ONE classical authentication of it fails.**

**claim:  $\#\{ i \mid S_i \text{ is } \underline{\text{valid}} \} \geq 2$**

$$\begin{aligned}\mathcal{H}_1 &= \langle A_{K_1}(H_1), S_1, \alpha_{K_{21}}(S_1), \alpha_{K_{31}}(S_1), K_{12}, K_{13} \rangle \\ \mathcal{H}_2 &= \langle A_{K_2}(H_2), S_2, \alpha_{K_{32}}(S_2), \alpha_{K_{12}}(S_2), K_{23}, K_{21} \rangle \\ \mathcal{H}_3 &= \langle A_{K_3}(H_3), S_3, \alpha_{K_{13}}(S_3), \alpha_{K_{23}}(S_3), K_{31}, K_{32} \rangle\end{aligned}$$



**def:  $S_i$  is valid if at most ONE classical authentication of it fails.**

**claim:  $\#\{ i \mid S_i \text{ is } \underline{\text{valid}} \} \geq 2$**

**$[K_1 : K_2 : K_3]$  is recovered from  $\{ S_i \text{ is } \underline{\text{valid}} \}$**

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



**def:  $S_i$  is valid if at most ONE classical authentication of it fails.**

**claim:  $\#\{ i \mid S_i \text{ is } \underline{\text{valid}} \} \geq 2$**

**$[K_1:K_2:K_3]$  is recovered from  $\{ S_i \text{ is } \underline{\text{valid}} \}$**

**• 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 fixing one erasure get  $|\psi\rangle$  from  $|0\rangle \otimes H_2 \otimes H_3, H_1 \otimes |0\rangle \otimes H_3$  or  $H_1 \otimes H_2 \otimes |0\rangle$**



# Generalization

**Q: (over  $GF(q)$ )**

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

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



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

$\mathcal{H}_1, \dots, \mathcal{H}_i, \dots, \mathcal{H}_n$

$$\mathcal{H}_i = \langle A_{K_i}(H_i), s_i, \alpha_{K_{1i}}(s_i), \dots, \alpha_{K_{(i-1)i}}(s_i), \alpha_{K_{(i+1)i}}(s_i), \dots, \alpha_{K_{ni}}(s_i), K_{i1}, \dots, K_{i(i-1)}, K_{i(i+1)}, \dots, K_{in} \rangle$$

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

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

$$\langle s_1, s_2, \dots, s_n \rangle \in \mathbb{R} \text{SS}_{n, n-d} [K_1 : K_2 : K_3 : \dots : K_n]$$



**def:  $S_i$  is valid if at most  $d-1$  classical authentication of it fails.**

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

**$[K_1 : K_2 : K_3 : \dots : K_n]$  is recovered from  $\{ S_i \text{ is } \underline{\text{valid}} \}$**

- using keys  $K_1, K_2, K_3, \dots, K_n$   
try to get each  $H_i$  from  $\mathcal{H}_i$
- at most  $d-1$  quantum authentications may fail
- using Q's algorithm for fixing  $d-1$  erasures get  $|\psi\rangle$  from  $H_1 \otimes H_2 \otimes \dots \otimes H_n$ , where  $d-1$  parts are  $|0\rangle$ .



## 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**



**from Quantum Coding**  
**to Quantum Authenticating,**  
**and back**

**Claude Crépeau**

School of Computer Science  
McGill University



joint work with  
**D. Gottesman and A. Smith**