Sharing Secrets by Quantum Stabilizer Codes

Ryutaroh Matsumoto

Tokyo Tech., Japan and Aalborg University, Denmark
Send your comments to ryutaroh@ict.e.titech.ac.jp

January 2023
@ SecureCAT kick-off meeting

Copyright

Structure of this talk

1. Short Review to Secret Sharing and Quantum Information
2. Sharing Quantum Secrets by Quantum Stabilizer Codes
3. Sharing Classical Secrets by Quantum Stabilizer Codes

Most famous secret sharing scheme (Shamir-Blakley)

Goal: Share a secret s so that only qualified sets of participants know s.
$\mathbf{F}_q \ni s$: a secret
n: the number of participants
$\mathbf{F}_q \ni \alpha_1, ..., \alpha_n$: distinct nonzero elements

1. Choose a polynomial $f(x) = s + a_1 x + \cdots + a_{k-1} x^{k-1}$ at random.
2. Distribute $f(\alpha_i)$ to the i-th participant.

- $k-1$ or less participants has no information about s.
- k or more participants can reconstruct s (by solving linear equations).

A **share**: a piece of information distributed to a participant ($f(\alpha_i)$ in this example)

Access structure in secret sharing

Forbidden set: a set of participants who collectively have no information about the secret, that is, their shares are statistically independent of the secret, as random variables.
Example: A set of $k-1$ or less participants in the Shamir-Blakley scheme.

Qualified set: a set of participants who can collectively reconstruct the secret, that is, there exists a map from their shares to the secret.
Example: A set of k or more participants in the Shamir-Blakley scheme.

Intermediate set: a set of participants that is neither qualified nor forbidden.

Access structure: set of forbidden sets and set of qualified sets, that is, the structure of forbidden and qualified sets.

Secret sharing will be abbreviated as **SS**. **Ramp** SS allows intermediate sets, while **perfect** SS does not. Ramp SS enables higher **coding rate** (= size of secret / average size of shares).

Review of qubits

QUantum BIT: a unit of quantum information that can store 1 classical bit, and expressed by two-dimensional complex linear space $\mathbf{C}^2$. Its orthonormal basis is often written as $\left\{|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right\}$ (ket-zero and ket-one).

n qubits are expressed as a vector in $(\mathbf{C}^2)^{\otimes n}$ of dimension 2^n.
$|a\rangle \otimes |b\rangle$ is often abbreviated as $|ab\rangle$.

Example: Two typical orthonormal bases of 2 qubits are
$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ and
$\left\{ \frac{|0\ell\rangle + (-1)^m |1(1-\ell)\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1-\ell \\ \ell \\ \ell(-1)^m \\ (1-\ell)(-1)^m \end{pmatrix} \mid \ell, m = 0, 1 \right\}$ (the Bell basis).

Using Quantum Shares

In conventional SS, shares are bits (classical information).
Quantum shares

- enable sharing of **quantum secrets**, which will be useful for quantum internet (information network carrying quantum information), and
- realize higher efficiency (higher coding rate) with the same access structure, for **classical secrets**.

SS with quantum shares can be constructed by quantum stabilizer codes.

Review of the non-binary quantum stabilizer codes

For $(\vec{a}|\vec{b}) = (a_1, ..., a_n|b_1, ..., b_n)$, and $(\vec{c}|\vec{d}) = (c_1, ..., c_n|d_1, ..., d_n) \in \mathbf{F}_q^{2n}$, the symplectic inner product is defined as

$$\langle(\vec{a}|\vec{b}), (\vec{c}|\vec{d})\rangle_s = \langle \vec{a}, \vec{d}\rangle_E - \langle \vec{b}, \vec{c}\rangle_E,$$

where $\langle , \rangle_E$ denotes the Euclidean inner product.

A symplectic self-orthogonal space $C \subset C^{\perp s} \subset \mathbf{F}_q^{2n}$ with $\dim C = n - k$ gives an $[[n, k, d]]_q$ quantum stabilizer code, encoding k qudits $\in (\mathbf{C}^q)^{\otimes k}$ into n qudits $\in (\mathbf{C}^q)^{\otimes n}$, detecting $\leq d - 1$ quantum errors, and correcting $\leq d - 1$ quantum **erasures**.

Example of $[[4, 2, 2]]_2$ stabilizer code

Let $q = 2$, $n = 4$, $k = 1$, and $\mathbf{F}_2^8 \supset C$ be spanned by $(1, 1, 1, 1|0, 0, 0, 0)$ and $(0, 0, 0, 0|1, 1, 1, 1)$. This is a **CSS** code from $\{(1, 1, 1, 1), \vec{0}\} \subset \mathbf{F}_2^4$.

2-qubit quantum message can be written as
$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$. ($\alpha_{ij}$ are complex coefficients.)

The above message is encoded to 4-qubit quantum codeword (unnormalized)
$\alpha_{00}(|0000\rangle + |1111\rangle + |0110\rangle + |1001\rangle)$
$+\alpha_{01}(|0011\rangle + |1100\rangle + |1010\rangle + |0101\rangle)$
$+\alpha_{10}(|0000\rangle + |1111\rangle - |0110\rangle - |1001\rangle)$
$+\alpha_{11}(|0011\rangle - |1100\rangle - |1010\rangle + |0101\rangle)$.
This is a non-standard encoding for this CSS code.

Any single bit error, phase error, bit+phase error can be detected, and **any single erasure can be corrected**.

Quantum error-correcting code and SS

QECC encoder and erasure decoder are given. An SS can be obtained by

1. Encode a quantum secret by the given encoder. Then distribute each qubit in the quantum codeword to a participant.
2. Participants in a qualified set can reconstruct the quantum secret by the given erasure decoder.

R. Cleve, D. Gottesman and H.-K. Lo, “How to Share a Quantum Secret,” Phys. Rev. Lett., 1999.

There have been few papers on quantum **ramp** SS.

Access structure when quantum secret is shared

$\{1, ..., n\} \supset A$: a set of participants/shares.

A is qualified iff $\overline{A} = \{1, ..., n\} \setminus A$ is forbidden (Cleve et al, 1999 and Ogawa et al. 2005).

The speaker clarified (Quantum. Inf. Process 2017) that, for an SS defined by a stabilizer $C \subset \mathbf{F}_q^{2n}$,

A is qualified iff erasures in $\overline{A}$ is correctable iff $C^{\perp s} \cap \mathbf{F}_q^{\overline{A}} = C \cap \mathbf{F}_q^{\overline{A}}$, and
A is forbidden iff $C^{\perp s} \cap \mathbf{F}_q^{A} = C \cap \mathbf{F}_q^{A}$

where $\mathbf{F}_q^A = \{(a_1, b_1, ..., a_n, b_n) \in \mathbf{F}_q^{2n} \mid j \in \overline{A} \Rightarrow (a_j, b_j) = (0, 0)\}$. Observe $\dim \mathbf{F}_q^A = 2|A|$.

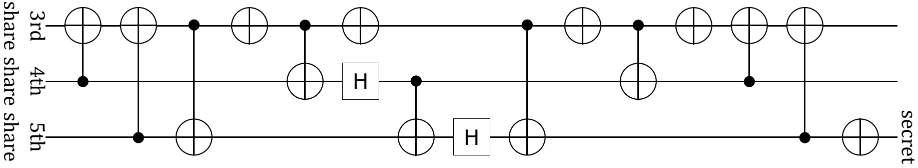
Unitary reconstruction of quantum secrets

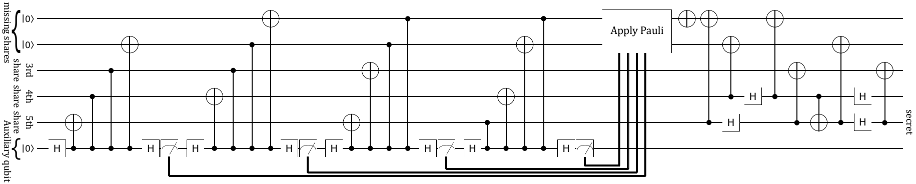
- Ogawa et al.'s quantum SS (2005) is constructed from the RS codes, and is a special case of stabilizer-based SS.
- Their reconstruction of secrets is a unitary procedure, whose quantum circuit operates on k qubits, while an erasure correction procedure operates on n qubits, for an $[[n, k]]$ code.

The speaker proposed a generic construction of unitary reconstruction procedure of quantum secrets (Quantum. Inf. Process 2017). An example next page.

Reconstruction circuits for the $[[5,1,3]]_2$ stabilizer code

Reconstruction circuits from 3 quantum shares (3 qubits in a codeword), constructed by my student Shogo Chiwaki.





From the **next slide**, we consider sharing **classical** secrets.

Gottesman's quantum secret sharing (PRA 2000)

Secret is 2 classical bits (ℓ, m).
There are 2 participants.
The 1st participant has the 1st qubit and
the 2nd one has the 2nd qubit of

$$\frac{|0\ell\rangle + (-1)^m |1(1-\ell)\rangle}{\sqrt{2}} \text{ (called a Bell state).}$$

- $\{1, 2\}$ is qualified.
- The (matrix expression of) quantum state (i.e. density matrix) of each share is $I_{2\times 2}/2$ and independent of values (ℓ, m), therefore $\emptyset$, $\{1\}$ and $\{2\}$ are forbidden.
- Coding rate = size of secret / average size of shares = 2, as 1 qubit can store at most 1 bit.
- The access structure is perfect, i.e., every set is either forbidden or qualified.
- When shares are classical and SS is perfect, coding rate must ≤ 1.
- This example shows high coding rate impossible by classical shares.

Sharing classical secrets by quantum stabilizer codes

- Show a general framework (Matsumoto, Quantum Inf. Processing, 2020) of quantum secret sharing based on quantum stabilizer codes that includes Gottesman's example as a special case.
- Compare stabilizer-based SS for classical secrets and quantum secrets.

Encoding **classical** secrets in quantum secret sharing

An $[[n,k]]_q$ quantum stabilizer code is a q^k-dimensional complex subspace Q of $(\mathbf{C}^q)^{\otimes n}$.
Q can encode $(k \log_2 q)$ **classical** bits to n qudits $\in (\mathbf{C}^q)^{\otimes n}$. Let $\{|\vec{v}\rangle \mid \vec{v} \in \mathbf{F}_q^k\}$ be an orthonormal basis of Q.
Classical secret $\vec{v} \in \mathbf{F}_q^k$ is encoded to $|\vec{v}\rangle \in Q$, then each participant has each qudit in the quantum codeword $|\vec{v}\rangle \in (\mathbf{C}^q)^{\otimes n}$.

The access structure depends on the choice of bases $\{|\vec{v}\rangle \mid \vec{v} \in \mathbf{F}_q^k\} \subset Q \subset (\mathbf{C}^q)^{\otimes n}$. So I will express choices of $\{|\vec{v}\rangle \mid \vec{v} \in \mathbf{F}_q^k\}$ in an algebraic coding theoretic way.

Proposed encoding in quantum secret sharing

For any $C \subset C^{\perp s} \subset \mathbf{F}_q^{2n}$ there always exists self-dual $C_{\max} = C_{\max}^{\perp s}$ such that

$$C \subset C_{\max} = C_{\max}^{\perp s} \subset C^{\perp s}.$$

$C_{\max} = C_{\max}^{\perp s}$ defines a commutative group S of complex Pauli matrices. Commutativity enables us to diagonalize all matrices in S by single common orthonormal basis.

Each complex vector in an orthonormal basis $\{|\vec{v}\rangle \mid \vec{v} \in \mathbf{F}_q^k\}$ of Q is chosen as a simultaneous eigenvector of all complex unitary matrices in S.

Example 1: Gottesman's example as a stabilizer code

Gottesman's secret sharing scheme by a quantum stabilizer. Let $p = 2$, $n = 2$ and C be the zero-dimensional linear space consisting of only the zero vector. Then $C^{\perp s} = \mathbf{F}_2^4$. We choose $C_{\max}$ as the space spanned by $(1, 1|0, 0)$ (corresponding to $X \otimes X$) and $(0, 0|1, 1)$ (corresponding to $Z \otimes Z$).

$X \otimes X$ and $Z \otimes Z$ decompose $\mathbf{C}_2^{\otimes 2}$ into 4 orthogonal spaces of dimension 1 whose bases are

$$\frac{|0\ell\rangle + (-1)^m |1(1-\ell)\rangle}{\sqrt{2}} \text{ (called a Bell state).}$$

2-bit classical secret (ℓ, m) is encoded into one of the above four quantum states.

Example 2: $[[4, 2, 2]]_2$ CSS code

Let $q = 2$, $n = 4$, $k = 2$, and $\mathbf{F}_2^8 \supset C$ be spanned by $(1, 1, 1, 1|0, 0, 0, 0)$ and $(0, 0, 0, 0|1, 1, 1, 1)$. This is a **CSS** code from $\{(1, 1, 1, 1), \vec{0}\} \subset \mathbf{F}_2^4$. C defines a $[[4, 2, 2]]_2$ code $Q \subset \mathbf{C}_2^{\otimes 4}$, shown earlier in page 9.

Let $C_{\max}$ be spanned by C and $(0, 1, 1, 0|0, 0, 0, 0)$ and $(0, 0, 0, 0|0, 1, 1, 0)$. $C_{\max}^{\perp s} = C_{\max}$ and $C_{\max}$ defines a $[[4, 0, 2]]_2$ CSS code.

Complex matrices corresponding to $C_{\max}$ decompose Q (the $[[4, 2, 2]]_2$ code shown above) into 4 orthogonal spaces of dimension 1 whose bases are
$|0000\rangle + |1111\rangle + |0110\rangle + |1001\rangle$,
$|0011\rangle + |1100\rangle + |1010\rangle + |0101\rangle$,
$|0000\rangle + |1111\rangle - |0110\rangle - |1001\rangle$,
$|0011\rangle - |1100\rangle - |1010\rangle + |0101\rangle$.

2-bit classical secret is encoded into one of the above four quantum states.

Access structure

$C \subset C_{\max} = C_{\max}^{\perp s} \subset C^{\perp s} \subset \mathbf{F}_q^{2n}$ with $\dim C = n - k$. Classical secrets have $(k \log_2 q)$ bits.

$\{1, ..., n\} \supset A$: a set of participants/shares.
$\mathbf{F}_q^A = \{(a_1, b_1, ..., a_n, b_n) \in \mathbf{F}_q^{2n} \mid j \in \overline{A} \Rightarrow (a_j, b_j) = (0, 0)\}$.

A is qualified iff $\dim C_{\max} \cap \mathbf{F}_q^A / C \cap \mathbf{F}_q^A = k$, and
A is forbidden iff $\dim C_{\max} \cap \mathbf{F}_q^A / C \cap \mathbf{F}_q^A = 0$.

More precisely, shares in A have $(\log_2 q \times \dim C_{\max} \cap \mathbf{F}_q^A / C \cap \mathbf{F}_q^A)$ bits of information about secret (measured by the Holevo information quantity).

Relation of access structures for classical/quantum secrets

A quantum stabilizer $C(\subset C_{\max} = C_{\max}^{\perp s} \subset C^{\perp s} \subset \mathbf{F}_q^{2n})$ with $\dim C = n - k$ can encode $k \log_2 q$-(qu)bit classical/quantum secrets into n quantum shares. For $A \subset \{1, ..., n\}$, we have the following relation of necessary and sufficient conditions of A being qualified/forbidden:

A is	for quantum secrets		for classical secrets
forbidden	$C^{\perp s} \cap \mathbf{F}_q^A = C \cap \mathbf{F}_q^A$	$\Rightarrow$	$\dim C_{\max} \cap \mathbf{F}_q^A / C \cap \mathbf{F}_q^A = 0$
qualified	$C^{\perp s} \cap \mathbf{F}_q^{\overline{A}} = C \cap \mathbf{F}_q^{\overline{A}}$	$\Rightarrow$	$\dim C_{\max} \cap \mathbf{F}_q^A / C \cap \mathbf{F}_q^A = k$

$\mathbf{F}_q^A = \{(a_1, b_1, ..., a_n, b_n) \in \mathbf{F}_q^{2n} \mid j \in \overline{A} \Rightarrow (a_j, b_j) = (0, 0)\}$.

Sufficient conditions in terms of symplectic weights will be given next.

Symplectic weights

For $\vec{x} = (\vec{a}|\vec{b}) = (a_1, b_1, \ldots, a_n, b_n) \in \mathbf{F}_q^{2n}$, the symplectic weight $w_s(\vec{x}) = |\{i \mid (a_i, b_i) \neq (0, 0)\}|$.

For a set $C \subset \mathbf{F}_q^{2n}$, $w_s(C)$ denotes $\min\{w_s(\vec{x}) \mid \vec{x} \in C \setminus \{\vec{0}\}\}$ in this talk.

Relation among weights and access structures

A quantum stabilizer $C(\subset C_{\max} = C_{\max}^{\perp s} \subset C^{\perp s} \subset \mathbf{F}_q^{2n})$ with $\dim C = n - k$ can encode $k \log_2 q$-(qu)bit classical/quantum secrets into n quantum shares. For $A \subset \{1, ..., n\}$, we have the following relation:

A is	for quantum secrets		for classical secrets
forbidden iff	$C^{\perp s} \cap \mathbf{F}_q^A = C \cap \mathbf{F}_q^A$	$\Rightarrow$	$\dim C_{\max} \cap \mathbf{F}_q^A / C \cap \mathbf{F}_q^A = 0$
	$\Uparrow$		$\Uparrow$
forbidden if	$\lvert A\rvert \le w_s(C^{\perp s} \setminus C) - 1$	$\Rightarrow$	$\lvert A\rvert \le w_s(C_{\max} \setminus C) - 1$
qualified iff	$C^{\perp s} \cap \mathbf{F}_q^{\overline{A}} = C \cap \mathbf{F}_q^{\overline{A}}$	$\Rightarrow$	$\dim C_{\max} \cap \mathbf{F}_q^A / C \cap \mathbf{F}_q^A = k$
	$\Uparrow$		$\Uparrow$
qualified if	$\lvert A\rvert \ge n + 1 - w_s(C^{\perp s} \setminus C)$	$\Rightarrow$	$\lvert A\rvert \ge n + 1 - w_s(C^{\perp s} \setminus C_{\max})$

where $\mathbf{F}_q^A = \{(a_1, b_1, ..., a_n, b_n) \in \mathbf{F}_q^{2n} \mid j \in \overline{A} \Rightarrow (a_j, b_j) = (0, 0)\}$. Note that $w_s(C_{\max} \setminus C)$ is often **much larger** than $w_s(C^{\perp s} \setminus C)$, as $C_{\max}$ is smaller than $C^{\perp s}$.

Relative generalied symplectic weights (added)

For linear spaces $V_2 \subset V_1 \subset \mathbf{F}_q^{2n}$, the i-th relative generalized symplectic weight is

$$d_s^i(V_1, V_2) = \min\{|A| : \dim \mathbf{F}_q^A \cap V_1 - \dim \mathbf{F}_q^A \cap V_2 \geq i\}.$$

We have $d_s^1(V_1, V_2) = w_s(V_1 \setminus V_2)$.

Recall that shares in A have $(\log_2 q \times \dim C_{\max} \cap \mathbf{F}_q^A / C \cap \mathbf{F}_q^A)$ bits of information about secret.

$$\Downarrow$$

If $|A| \leq d_s^i(C_{\max}, C) - 1$ then shars in A has at most $(i-1)\log_2 q$ bits of information, and
If $|A| \geq n + 1 - d_s^i(C^{\perp s}, C_{\max})$ then shares in A has at least $(k+1-i)\log_2 q$ bits of information.

From the next slide I will discuss randomness in encoding.

Randomization in encoding of classical secrets into classical shares

Classical shares are chosen randomly for a given classical secret in Shamir's scheme.

Suppose that a share X depends on the value of a classical secret S (which is almost always true), and that **encoding is deterministic**. Then X has nonzero information about S (the mutual information $I(S;X)$ is nonzero).

No randomness in encoding means that forbidden sets consist of only the empty set $\varnothing$.

Randomization is **indispensable** with encoding classical secrets into classical shares.

Randomization in encoding of quantum secrets

Quantum shares are deterministically encoded from a quantum secret by a QECC.

Suppose that we have a randomized encoder of a quantum secret into quantum shares. Then that randomized encoder can be realized by discarding some shares encoded by a deterministic encoder (Cleve et al, 1999 and Ogawa et al. 2005).

Randomization is **useless** in encoding quantum secrets into quantum shares.

Randomization in encoding of classical secrets into quantum shares

Quantum shares are deterministically encoded from a classical secret by a quantum stabilizer (in the speaker's proposal).

Randomness in encoding enables a wider class of access structures constructed from the same stabilizer (Matsumoto, Des. Codes. Crypt., 2020).

Randomization is **useful but dispensable** with encoding classical secrets into quantum shares.

Summary

- Secret sharing by quantum stabilizers
- Relations among the (relative generalized) minimum weights of codes and access structures
- Differences among classical/quantum secrets/shares in randomization of encoding

References (chronological order)

1. R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," Phys. Rev. Lett., vol.83, pp.648–651, 1999.
2. D. Gottesman, "Theory of quantum secret sharing,", Phys. Rev. A, vol.61, article 042311, 2000.
3. T. Ogawa et al., "Quantum secret sharing schemes and reversibility of quantum operations," Phys. Rev. A, vol.72, article 032318, 2005.
4. R. Matsumoto, "Unitary reconstruction of secret for stabilizer based quantum secret sharing," Quantum Inf. Process., vol.16, article 202, 2017.
5. R. Matsumoto, "Classical access structures of ramp secret sharing based on quantum stabilizer codes," Quantum Inf. Process., vol.19, article 9, 2020.
6. R. Matsumoto, "Message randomization and strong security in quantum stabilizer-based secret sharing for classical secrets," Des. Codes Crypto., vol.99, pp.1893–1907, 2020.