Quantum secret sharing for general access structures

Adam Smith
MIT*
asmith@theory.lcs.mit.edu

May 1999; revised January 2000

Abstract

We explore the conversion of classical secret sharing schemes to quantum ones, and how this can be used to give efficient QSS schemes for general adversary structures. Our first result is that quantum secret-sharing is possible for any structure for which no two disjoint sets can reconstruct the secret (this was also proved, somewhat differently, in [7]). To obtain this we show that a large class of *linear* classical SS schemes can be converted into quantum schemes of the same efficiency.

We also give a necessary and sufficient condiion for the direct conversion of classical schemes into quantum ones, and show that all group homomorphic schemes satisfy it.

1 Introduction

A classical secret sharing scheme is a (usually) randomized encoding of a secret s into a n-tuple, the coordinates of which are each given to different players in the player set P. The encoding is a secret sharing scheme if there exists a collection $\mathcal{A}$ of subsets of P (called the *adversary structure*) such that no set of players in $\mathcal{A}$ gets any information about s from their shares, but any set of players not in $\mathcal{A}$ will be able to compute s. The classic example of this is due to Shamir [11]. He gives a construction based on polynomials over a finite field of a *threshold* secret-sharing scheme for any threshold t and any number of players (in such a scheme, $\mathcal{A} = \{B \subseteq P : |B| \leq t\}$).

The idea of sharing *quantum* secrets was first described and solved for the case $t = 1, n = 2$ by Hillery *et al.* in [8][1]. A more general solution, for all $t > \frac{n}{2} - 1$, was recently given by Cleve *et al.* (CGL, [4]). Their scheme is a direct generalization of the well-known Shamir scheme [11], with all calculations done unitarily and "at the quantum level", *i. e.* replacing random choices with equal superpositions over those choices.

In next section we give definitions and background. In section 3, we then prove that classical *linear* secret-sharing schemes, with an appropriate adversary structure, can be converted into quantum schemes with the same complexity, both in terms of share size and encoding/reconstruction. This gives another proof of theorem 8 from [7]. In the last section, we give a necessary and sufficient condition for (not necessarily linear) classical SS schemes to become quantum ones when run at the quantum level, and observe that all group homomorphic schemes obey this condition.

2 Preliminaries

2.1 Adversary structures

Given a set of players P, an adversary structure $\mathcal{A}$ over P is a set of subsets of players which is downward-closed under inclusion:

$$(B \in \mathcal{A} \text{ and } B' \subseteq B) \Longrightarrow B' \in \mathcal{A}.$$

Normally such a structure is used to represent the collection of all coalitions of players which a given protocol can tolerate without losing security: as long as the set of cheating players is in $\mathcal{A}$, the cheaters cannot breach the security of the protocol.

Secret-sharing schemes usually tolerate *threshold structures*, which are of the form $\mathcal{A} = \{B \subseteq P : |B| \leq t\}$ for some t. However, when working with more general structures, the following definitions prove useful.

Definition 1 *An adversary structure $\mathcal{A} \subseteq 2^P$ is $\mathcal{Q}^2$ if no two sets in $\mathcal{A}$ cover P, that is*

$$\nexists B_1, B_2 \in \mathcal{A} : \quad B_1 \cup B_2 = P.$$

*Work done while author was at McGill University, Montreal. Supported by an NSERC undergraduate research grant.

[1] In fact, [8] shows how efficency can be gained in the insecure channels model by combining the key distribution and secret-sharing layers of the protocol. An even more efficient protocol was suggested in [10].

Definition 2 *The* dual *of an adversary structure $\mathcal{A}$ over P is the collection*

$$\mathcal{A}^* = \{B \subseteq P : B^c \notin \mathcal{A}\}$$

where B^c denotes the complement $P - B$.

Definition 3 *A structure $\mathcal{A}$ over P is $\mathcal{Q}^{2*}$ if its dual $\mathcal{A}^*$ is $\mathcal{Q}^2$. This means that any two sets not in $\mathcal{A}$ will have a non-empty intersection.*

It is interesting to note that $\mathcal{A}$ is $\mathcal{Q}^2$ iff $\mathcal{A} \subseteq \mathcal{A}^*$. Dually, $\mathcal{A}$ is $\mathcal{Q}^{2*}$ iff $\mathcal{A} \supseteq \mathcal{A}^*$. Consequently, a collection is *self-dual* iff it is both $\mathcal{Q}^2$ and $\mathcal{Q}^{2*}$.

2.1.1 Monotone functions

We can define a partial order on $\{0,1\}^n$ by the rule "$\mathbf{x} \leq \mathbf{y}$ iff each coordinate of $\mathbf{x}$ is smaller than the corresponding coordinate of $\mathbf{y}$."

By identifying $\{0,1\}^n$ with $2^{\{1,\ldots,n\}}$, the relation $\leq$ on $\{0,1\}^n$ corresponds to inclusion ($\subseteq$) in $2^{\{1,\ldots,n\}}$. Then a monotone function f corresponds to a function from $2^{\{1,\ldots,n\}}$ to $\{0,1\}$ such that $A \subseteq B \implies f(A) \leq f(B)$.

Such a monotone function f naturally defines an adversary structure $\mathcal{A}_f = f^{-1}(\{0\}) = \{B \subseteq P : f(B) = 0\}$. Moreover, f is called $\mathcal{Q}^2$ (resp. $\mathcal{Q}^{2*}$) iff $\mathcal{A}_f$ is $\mathcal{Q}^2$ (or $\mathcal{Q}^{2*}$).

2.2 Monotone span programs

Span programs were introduced as a model of computation in [9]. They were first used for multiparty protocols in [5] under this name, although a similar construction, attributed to Brickell, already existed ([12]). In this section we define some concepts related to monotone span programs.

Definition 4 ***A monotone span program*** *(MSP) over a set P is a triple (K, M, ψ) where K is a finite field, M is a $d \times e$ matrix over K and $\psi : \{1,\ldots,d\} \to P$ is a function which effectively labels each row of M by a member of P.*

The MSP associates to each subset $B \subseteq P$ a subset of the rows of M: the set of rows l such that $\psi(l) \in B$. This corresponds to a linear subspace of K^e (the span of those rows). The monotone function $f : 2^P \to \{0,1\}$ defined by a MSP is given by the rule "$f(B) = 1$ if and only if the target vector $\epsilon = (1,0,0,\ldots,0)$ is in the subspace associated with B". If we denote by M_B the submatrix of M formed of the rows l such that $\psi(l) \in B$ then we get that

$$f(B) = 1 \iff \epsilon \in Im(M_B^T).$$

In fact, given any monotone function f, we can construct a MSP which computes it. The size of the MSP will be at most proportional to the size of the smallest monotone threshold formula for f, but may in some cases be exponentially smaller [1, 5].

The proof uses the following fact from linear algebra. Here the dual of a vector subspace W is denoted $W^\perp = \{\mathbf{u} : \mathbf{u}^\top \mathbf{w} = 0 \quad \forall \mathbf{w} \in W\}$.

Remark: Denote the dual of a vector subspace W by $W^\perp = \{\mathbf{u} : \mathbf{u}^\top \mathbf{w} = 0 \quad \forall \mathbf{w} \in W\}$. For any matrix M we have $Im(M^\top) = ker(M)^\perp$. Thus, $f(B) = 0$ iff $\exists \mathbf{v} : M_B \mathbf{v} = \mathbf{0}$ and $\epsilon^\top \mathbf{v} \neq 0$.

2.2.1 Secret-sharing from MSP's

Given a MSP (K, M, ψ), we can define a classical secret sharing scheme which tolerates the adversary structure $\mathcal{A}_f$ induced by the MSP. Say the dealer has a secret $s \in K$. He extends it to an e-rowed vector by adding random field elements $a_2, \ldots, a_e$ to make a vector $\mathbf{s}_* = (s, a_2, \ldots, a_e)$. The dealer gives the lth component of $\hat{\mathbf{s}} = M\mathbf{s}_*$ to player $P_{\psi(l)}$. If $\hat{\mathbf{s}}_A$ denotes the elements of $\hat{\mathbf{s}}$ with indices in A where $A \subseteq \{1,\ldots,d\}$, then each P_i receives $\hat{\mathbf{s}}_{\psi^{-1}(i)}$.

The SS scheme thus defined tolerates exactly the adversary structure $\mathcal{A}_f$.

Note that the concept of MSP's is very general: any linear secret-sharing scheme (i.e. one in which the encoding of the secret is given by a linear map over a field) can be formulated as a MSP-based scheme [5]. The Shamir scheme is a special case, where M is a $n \times (k+1)$ Vandermonde matrix, $e = k+1$, $d = n$, and ψ is the identity on $\{1,\ldots,n\}$.

2.3 Secret sharing with general access structures

With classical data, secret sharing is possible for any access structure. Given a monotone threshold formula for a function f, Benaloh and Leichter [2] gave a construction for $\mathcal{A}_f$ with efficency proportional to the size of the formula. This is improved on by constructions based on monotone span programs (section 2.2.1), which are always at least as efficient as the Benaloh-Leichter scheme but can be superpolynomially more so.

When sharing quantum data, the situation is slightly different. Because of the no-cloning theorem, it is impossible to share secrets with an adversary structure which is not $\mathcal{Q}^{2*}$ (since then one can

find two disjoint sets which can reconstruct the secret based on their shares). Because a pure-state QSS scheme is also a quantum code correcting erasures on the sets described by its adversary structure, we also get that any pure-state QSS scheme has an adversary structure which is in fact self-dual [4]. The natural converse to this is

Theorem 1 *Given any $\mathcal{Q}^{2*}$ structure $\mathcal{A}$, we can find a QSS scheme for $\mathcal{A}$. If $\mathcal{A}$ is self-dual, then the scheme can be a pure-state one.*

This was proved for the case of threshold structures in [4]: their construction works when the number of cheaters t is more than $\frac{n}{2} - 1$ (*i. e.* it takes more than $\frac{n}{2}$ players to reconstruct the secret). Moreover, theirs is a pure-state scheme when $n = 2t + 1$ (these correspond to the $\mathcal{Q}^{2*}$ and self-dual conditions, respectively).

The full theorem was stated but not proved in [4]. We give a proof here, based on monotone span programs. Another proof, due to Daniel Gottesman and based on purification of quantum superoperators, appeared in [7].

3 Quantum secret-sharing from classical linear schemes

We assume that the reader is familiar with the notation and basic concepts of quantum computing. For clarity, we will ignore normalization factors.

3.1 Pure-state linear QSS

Cramer *et al.* [5] pointed out that any linear secret-sharing scheme can be realized as a MSP-based scheme. In this section, I show that any MSP with adversary structure $\mathcal{A}$ gives rise to a quantum erasure-correcting code for erasures occuring on any set of positions in $\mathcal{A} \cap \mathcal{A}^*$. In the case where $\mathcal{A}$ is self-dual, this yields a pure-state quantum secret-sharing scheme for $\mathcal{A}$.

The idea is the same as that for the CGL scheme [4]. First choose a MSP, say (K, M, ψ). Note that WLOG all e rows of M are linearly independent and so we can extend M to an invertible $d \times d$ matrix M'. We can construct a quantum circuit $\tilde{M}$ implementing multiplication by M' and thus encode a basis state $|s\rangle$, for $s \in K$, as

$$\tilde{M}\left(|s\rangle \otimes \sum_{\mathbf{a} \in K^{e-1}} |a_1 \cdots a_{e-1}\rangle \otimes |0 \cdots 0\rangle\right) = \sum_{\mathbf{a} \in K^{e-1}} \left| M \begin{pmatrix} s \\ \mathbf{a} \end{pmatrix} \right\rangle$$

(The expression $\binom{s}{\mathbf{a}}$ denotes the column vector obtained by adjoining s to the beginning of the vector $\mathbf{a}$).

This scheme can be extended by linearity to arbitrary states $|\phi\rangle = \sum_{s \in K} \alpha_s |s\rangle$. The pieces of the encoded state are then distributed according to the function ψ. We have:

Theorem 2 *Let (K, M, ψ) be a MSP with a.s. $\mathcal{A}$. Then the encoding above is corrects erasures on any set of positions in $\mathcal{A} \cap \mathcal{A}^*$.*

To prove this, we need to show for any set B which is in $\mathcal{A}$ but whose complement is not, the players in A can reconstruct the encoded data. We give a reconstruction procedure. The proof consists of the two following lemmas.

First we show the existence of certain vectors used in the reconstruction process.

Lemma 3 *Let (K, M, ψ) be a MSP with a.s. $\mathcal{A}$. Suppose $B \in \mathcal{A} \cap \mathcal{A}^*$ (i.e. $A = P - B$ is in $\mathcal{A}$). Then there exists an invertible linear transformation U on the shares of A such that after the transformation,*

1. *the first share contains the secret s;*
2. *all remaining shares, including those of players in B, are distributed independently of s when the $e - 1$ other components of $\mathbf{s}_*$ are chosen at random.*

Proof: Say A contains m shares. Then we must construct m linearly independent vectors $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m$ such that

1. $\mathbf{u}_1^\top M_A \binom{s}{\mathbf{a}} = s$;
2. If U' is the matrix with rows given by $\mathbf{u}_2, \ldots, \mathbf{u}_m$, then the value

$$\begin{pmatrix} U' M_A \\ M_B \end{pmatrix} \begin{pmatrix} s \\ \mathbf{a} \end{pmatrix}$$

is distributed independently of s.

To satisfy the first condition, pick any $\mathbf{u}_1$ such that $\mathbf{u}_1^\top M_A = \epsilon^\top$. Such a vector must exist since by hypothesis the players in A can reconstruct the secret.

To satisfy the second condition, it's enough to ensure there exists $\mathbf{v}$ such that $\binom{U' M_A}{M_B}\mathbf{v} = \mathbf{0}$ and $\epsilon^\top \mathbf{v} \neq 0$ (see section 2.2).

Since $B \in \mathcal{A}$, we know that there is a $\mathbf{v}$ such that $\epsilon^\top \mathbf{v} \neq 0$ and $M_B \mathbf{v} = \mathbf{0}$. Furthermore, the subspace $W = \{\mathbf{u} \in K^m : \mathbf{u}^\top M_A \mathbf{v} = 0\}$ has dimension $m-1$, and $\mathbf{u}_1$ is not in that space since $\mathbf{u}_1^\top M_A \mathbf{v} = \epsilon^\top \mathbf{v} \neq 0$. Hence any basis $\{\mathbf{u}_2, \ldots, \mathbf{u}_m\}$ of W will do.

The matrix U whose rows are given by the $\mathbf{u}_i$'s gives the desired transformation. Note that the U doesn't depend on $\mathbf{a}$. □

Finally we show that the reconstruction process works:

Lemma 4 *Let (K, M, ψ) be a MSP and let $B \in \mathcal{A} \cap \mathcal{A}^*$, $A = P - B$. Suppose a quantum state $|\phi\rangle = \sum_{s \in K} \alpha_s |s\rangle$ is encoded as described at the beginning of this section. Then the shares in A can be used to reconstruct $|\phi\rangle$. Consequently, no information on $|\phi\rangle$ can be obtained from the shares in B.*

Proof: Consider the case when $|\phi\rangle = |s\rangle$ for some $s \in K$. Then the encoded state can be written

$$\sum_{\mathbf{a} \in K^{e-1}} \left| M_A \begin{pmatrix} s \\ \mathbf{a} \end{pmatrix} \right\rangle \left| M_B \begin{pmatrix} s \\ \mathbf{a} \end{pmatrix} \right\rangle$$

Construct a quantum circuit for the map $\mathbf{b} \longmapsto U\mathbf{b}$, where U is constructed as in lemma 3. Denote by U' the matrix obtained by removing the first row of U. Applying the circuit for U only to the components of the encoded state corresponding to A, we get

$$\sum_{\mathbf{a} \in K^{e-1}} \left| U M_A \begin{pmatrix} s \\ \mathbf{a} \end{pmatrix} \right\rangle \left| M_B \begin{pmatrix} s \\ \mathbf{a} \end{pmatrix} \right\rangle = |s\rangle \otimes \sum_{\mathbf{a} \in K^{e-1}} \left| U' M_A \begin{pmatrix} s \\ \mathbf{a} \end{pmatrix} \right\rangle \left| M_B \begin{pmatrix} s \\ \mathbf{a} \end{pmatrix} \right\rangle$$

However, by construction the joint distribution of $U' M_A \binom{s}{\mathbf{a}}$ and $M_B \binom{s}{\mathbf{a}}$ is independent of s when $\mathbf{a}$ is chosen uniformly at random (lemma 3). Hence, for an arbitrary state $|\phi\rangle$ this procedure yields

$$|\phi\rangle \otimes \sum_{\mathbf{a} \in K^{e-1}} \left| U' M_A \begin{pmatrix} 0 \\ \mathbf{a} \end{pmatrix} \right\rangle \left| M_B \begin{pmatrix} 0 \\ \mathbf{a} \end{pmatrix} \right\rangle$$

By a strong form of the no cloning theorem, the correctness of the reconstruction implies that the shares of B give no information at all on $|\phi\rangle$. □

(This completes the proof of theorem 2).

When the adversary structure $\mathcal{A}$ defined by a MSP is $\mathcal{Q}^2$, we have $\mathcal{A} \subseteq \mathcal{A}^*$. Hence, the previous theorem shows that erasures on any set of coordinates in $\mathcal{A}$ can be corrected. In addition, if $\mathcal{A}$ is self-dual (*i. e.* both $\mathcal{Q}^2$ and $\mathcal{Q}^{2*}$) then the qualified sets are precisely the complements of sets in $\mathcal{A}$ and hence every qualified set can reconstruct the secret but no unqualified set gets any information on it. Thus we have shown theorem 1 for the case of self-dual structures.

3.2 Mixed-state linear QSS

To handle structures which are simply $\mathcal{Q}^{2*}$, we follow the strategy of [4]: first extend to a self-dual structure and then "trace-out" the new share(s).

To extend a structure $\mathcal{A}$ over a player set P, add a new player to P (say τ):

Lemma 5 *For any $\mathcal{Q}^{2*}$ adversary structure $\mathcal{A}$ over a player set P, the structure $\mathcal{A}'$ over the set $P' = P \cup \{\tau\}$ given by*

$$\mathcal{A}' = \mathcal{A} \cup \left\{B \cup \{\tau\} : B \in \mathcal{A}^*\right\}$$

is self-dual and its restriction to P yields $\mathcal{A}$.

Proof: Elementary, using the fact that $\mathcal{A}$ is $\mathcal{Q}^{2*} \iff \mathcal{A}^* \subseteq \mathcal{A}$. □

Thus, a pure-state QSS scheme for $\mathcal{A}'$ will yield a mixed-state scheme for $\mathcal{A}$ by throwing out the share corresponding to τ. For the construction to be efficient, we need the following:

Lemma 6 *Given a MSP for $\mathcal{A}$, an MSP for $\mathcal{A}'$ can be efficiently constructed.*

Proof: Note that the new access structure is $\Gamma' = \Gamma \cup \{B \cup \{\tau\} : B \in \Gamma^*\}$ (here $\Gamma, \Gamma^*, \Gamma'$ are the complements of $\mathcal{A}, \mathcal{A}^*, \mathcal{A}'$ resp.). Thus if f, f^*, f' are functions detecting membership in $\mathcal{A}, \mathcal{A}^*, \mathcal{A}'$ respectectively, and if f_τ detects the presence of τ in a set, then $f' = f \vee (f^* \wedge f_\tau)$.

Now to construct the desired MSP, first obtain an MSP for $\mathcal{A}^*$ according to [6]. The MSP for A' can then be constructed by composition from MSP's calculating AND and OR. □

The resulting MSP is at most a constant times the size of the original.

4 QSS from classical SS

A natural conjecture given the results of the previous section is that *any* classical secret-sharing scheme for an adversary structure will give a quantum erasure-coorecting for erasures in $\mathcal{A} \cap \mathcal{A}^*$. I show here a condition on the scheme for this to be the case. Not all schemes satisfy the condition, though a large class of them does, in particular group-homomorphic ones.

The corollary to this, as before, is that when $\mathcal{A}$ is self-dual, the resulting quantum scheme is a QSS scheme for $\mathcal{A}$. Note that the main difference between the proof we give here and that of the preivous section is that here we don't guarantee that the reconstructon procedure is efficient, only that it exists and is unitary.

4.1 A general condition

A classical secret sharing scheme can be thought of as a probabilistic map E from a secret space $\mathcal{S}$ into n "share spaces" $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$. The random input can be modeled as a choice from some set $\mathcal{R}$ with a given probability distribution. Now consider some set $U \in \mathcal{A} \cap \mathcal{A}^*$ and let $Q = U^c$ be its complement (Q is qualified). Let S be the random variable corresponding to the secret and let Y_u and Y_q be those corresponding to the shares in U and Q respectively. Denote their concatenation $E(S) = Y = Y_u Y_q$. Finally, let $\mathcal{Y}_u, \mathcal{Y}_q$ be the share spaces for U and Q and let $\mathcal{Y} = \mathcal{Y}_u \times \mathcal{Y}_q$ be the global share space.

Note that for the SS scheme to be perfect we must have

Correctness: $H(S|Y_q) = 0$. Equivalently, $S = f(Y_q)$ for some deterministic function f.

Secrecy: $I(S; Y_u) = 0$. Equivalently, $P(Y_u = y_u | S = s) = P(Y_u = y_u | S = s') = P(Y_u = y_u) \quad \forall s, s' \in \mathcal{S}$.

Suppose now we have a quantum secret which is a linear superposition of shares in $\mathcal{S}$ and a unitary map $\tilde{E}$ such that for $s \in \mathcal{S}$:

$$\tilde{E}\,|s\rangle = \sum_{y \in \mathcal{Y}} \sqrt{P(Y = y | S = s)}\,|y\rangle$$

This can in fact be rewritten as

$$\sum_{y_q : f(y_q) = s} \sqrt{P(Y_q = y_q | S = s)}\,|y_q\rangle \quad \cdot \quad \sum_{y_u \in \mathcal{Y}_u} \sqrt{P(Y_u = y_u | Y_q = y_q)}\,|y_u\rangle$$

We want to decide if this is can correct erasures on U. To do so requires showing that the density matrix of the U component is independent of the secret's state. Note that it is not sufficient to show that the density matrix is the same for all $|s\rangle$. We have to show this for all choices of the α_s's in $\sum_{s \in \mathcal{S}} \alpha_s |s\rangle$. We can compute the density matrix explicitly by imagining that a measure is made on the Q component of the code and the secret. We can then consider $P(S = s)$ to be $|\alpha_s|^2$. In what follows $\boldsymbol{\rho_{U|y_q}}$ is the density matrix of U given $Y_q = y_q$.

$$\begin{aligned}
&\rho_u \\
&= \sum_{s \in \mathcal{S}} |\alpha_s|^2 \sum_{y_q \in \mathcal{Y}_q} P(Y_q = y_q | S = s) \boldsymbol{\rho_{U|y_q}} \\
&= \sum_{y_q \in \mathcal{Y}_q} P(Y_q = y_q) \boldsymbol{\rho_{U|y_q}} \\
&= \sum_{y_q \in \mathcal{Y}_q} P(Y_q = y_q) \cdot \\
&\quad \left(\sum_{y_u^{(1)} \in \mathcal{Y}_u} \sqrt{P(Y_u = y_u^{(1)} | Y_q = y_q)} \left| y_u^{(1)} \right\rangle \right) \cdot \\
&\quad \left(\sum_{y_u^{(2)} \in \mathcal{Y}_u} \sqrt{P(Y_u = y_u^{(2)} | Y_q = y_q)} \left\langle y_u^{(2)} \right| \right) \\
&= \sum_{y_u^{(1)}, y_u^{(2)} \in \mathcal{Y}_u} \sum_{y_q \in \mathcal{Y}_q} \sqrt{P(Y_u = y_u^{(1)}, Y_q = y_q)} \cdot \\
&\qquad \sqrt{P(Y_u = y_u^{(2)}, Y_q = y_q)} \left| y_u^{(1)} \right\rangle \left\langle y_u^{(2)} \right|
\end{aligned}$$

The matrices in the set

$$\left\{ \left| y_u^{(1)} \right\rangle \left\langle y_u^{(2)} \right| : y_u^{(1)}, y_u^{(2)} \in \mathcal{Y}_u \right\}$$

are linearly independent. Their coefficients are

$$\begin{aligned}
&\sum_{y_q \in \mathcal{Y}_q} \sqrt{P(Y_u = y_u^{(1)}, Y_q = y_q) P(Y_u = y_u^{(2)}, Y_q = y_q)} \\
&= \sum_{s \in \mathcal{S}} |\alpha_s|^2 \sum_{y_q : f(y_q) = s} \sqrt{P(Y_u = y_u^{(1)}, Y_q = y_q | S = s)} \\
&\qquad \sqrt{P(Y_u = y_u^{(2)}, Y_q = y_q | S = s)}
\end{aligned}$$

For ρ_u to be independent of the choice of α_s we must therefore have

$$\sum_{y_q : f(y_q) = s} \sqrt{P(Y_u = y_u^{(1)}, Y_q = y_q | S = s)} \sqrt{P(Y_u = y_u^{(2)}, Y_q = y_q | S = s)} \quad (1)$$

independent of s for all $y_u^{(1)}, y_u^{(2)} \in \mathcal{Y}_u$. Thus

Theorem 7 *Given a classical SS scheme for an adversary structure $\mathcal{A}$, the correspnding quantum scheme corects erasures on $U \in \mathcal{A} \cap \mathcal{A}^*$, iff Equation (1) is independent of s for all $y_u^{(1)}, y_u^{(2)} \in \mathcal{Y}_u$.*

As unnatural as this condition seems, it is nonetheless satisfied by many SS schemes:

- If Y_u is a function of Y_q (as is the case in the Shamir scheme) then we have the expression (1) equal to 0 whenever $y_u^{(1)} \neq y_u^{(2)}$. Furthermore, when $y_u^{(1)} = y_u^{(2)} = y_u$ the expression reduces to $\sum_{y_q : f(y_q)=s} P(Y_u = y_u, Y_q = y_q | S = s)$, which sums to $P(Y_u = y_u | S = s)$. This is independent of s by the secrecy assumption above. Thus this type of scheme yields a secure QSS.

- A group homomorphic secret sharing scheme is based on an injective homomorphism $h : G \times G^m \longrightarrow G^n$ for some group G. The secret s is an element of G and the n shares are obtained by picking $\mathbf{v} \in_R G^m$ and calculating $h(s, \mathbf{v})$.

  In this case, the independence of expression (1) from s is guaranteed by the following fact: in any homomorphic SS scheme, either two words $y_u^{(1)}, y_u^{(2)}$ never appear with the same word y_q (that is

  $$P(Y_u = y_u^{(1)} | Y_q = y_q) P(Y_u = y_u^{(2)} | Y_q = y_q) = 0$$

  for all y_q) or they always appear with the same probability:

  $$\sqrt{P(Y_u = y_u^{(1)} | Y_q = y_q) P(Y_u = y_u^{(2)} | Y_q = y_q)} = P(Y_u = y_u^{(1)} | Y_q = y_q).$$

  The same analysis as before applies: QSS schemes constructed from homomorphic schemes are secure. Interestingly, there seem to be no cases where non-homomorphic schemes provide any advantage over homomorphic ones [13].

Thus, it seems that although not all classical SS schemes yield a QSS scheme directly, the most important ones do. However, the proof given does not give the reconstruction procedure; it only proves its existence. It is not *a priori* clear that all classical SS schemes which yield a secure QSS scheme will have efficient (quantum) reconstruction procedures.

Acknowledgements

I would like to thank Richard Cleve, Claude Crépeau, Daniel Gottesman and Paul Dumais for helpful discussions.

References

[1] L. Babai, A. Gál, J. Kollár, L. Rónyai, T. Szabó, and A. Wigderson. Extremal bipartite graphs and superpolynomial lower bounds for monotone span programs. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 603–611, Philadelphia, Pennsylvania, 22–24 May 1996.

[2] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *Advances in Cryptology—CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer-Verlag, 1990, 21–25 Aug. 1988.

[3] N. J. Cerf and R. Cleve. Information-theoretic interpretation of quantum error-correcting codes. *Physical Review A*, 56(3):1721–1732, Sept. 1997. Preprint at quant-ph/9702031.

[4] R. Cleve, D. Gottesman, and H.-K. Lo. How to share a quantum secret. quant-ph/9901025, Jan. 1999.

[5] R. Cramer, I. Damgård, and U. Maurer. General secure multi-party computation from any linear secret-sharing scheme. Most recent version available from Ronald Cramer at http://www.inf.ethz.ch/personal/cramer, 1998.

[6] S. Fehr. Efficient construction of the dual span program. Manuscript available from author at http://www.inf.ethz.ch/personal/fehr/, Jan. 1999.

[7] D. Gottesman. On the theory of quantum secret sharing. Preprint at quant-ph/9910067, Oct. 1999.

[8] M. Hillery, V. Buzek, and A. Berthiaume. Quantum secret sharing. *Physical Review A*, 59(3):1829–1834, Mar. 1999. Preprint at quant-ph/9806063.

[9] M. Karchmer and A. Wigderson. On span programs. In *Proceedings of the Eighth Annual Structure in Complexity Theory Conference*, pages 102–111, San Diego, California, 18–21 May 1993. IEEE Computer Society Press.

[10] A. Karlsson, M. Koashi, and N. Imoto. Quantum entanglement for secret sharing and secret splitting. *Physical Review A*, 59(1):162–168, Jan. 1999.

[11] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

[12] D. Stinson. *Cryptography: Theory and Practice*, chapter 11. CRC Press, fourth edition, 1996.

[13] D. Stinson. Personal communication. May 1999.