General Quantum Evolving Secret Sharing

Anat Paskin-Cherniavsky and Efrat Cohen

June 7, 2024

Contents

Abstract **i**

1 Introduction **1**

1.1 Quantum Secret Sharing (QSS) Schemes 2

1.2 Evolving secret sharing schemes 2

1.3 QESS - prior work vs. our contribution 4

1.4 Our Techniques 4

2 Preliminaries **6**

2.1 Classical secret sharing 6

2.1.1 Linear Secret Sharing Scheme As Monotone Span Program (MSP) 8

2.2 Evolving Secret Sharing Scheme 8

2.2.1 Linear Evolving Secret Sharing Scheme As Infinite MSP 10

2.3 Quantum Secret Sharing Scheme (QSS) 12

3 Quantum Evolving Secret Sharing Scheme (QESS) **14**

3.1 Inherent limitation of No-Cloning for evolving access structures 16

4 A note on [Cha20] QESS for Dynamic Thresholds **16**

5 Quantum Evolving Secret Sharing Scheme (QESS) Based on MSP **17**

5.1 Quantum Secret Sharing (QSS) based on MSP [Smi00] . 17

5.2 Our construction 19

A Strong form of the no-cloning theorem **21**

Abstract

In the useful and well studied model of secret-sharing schemes [Bla79, Sha79, ISN89], there are n parties and a dealer, which holds a secret. The dealer applies some randomized algorithm to the secret, resulting in n strings, called shares; it gives the i'th share to the i'th party. There are two requirements. (1) correctness: some predefined subsets of the parties can jointly reconstruct the secret from their shares, and (2) security: any other set gets no information on the secret. The collection of predefined qualified sets is called an access structure (AS).

This model assumes that the number of parties is known when preparing the shares and giving the shares to the parties; furthermore, the sharing algorithm and the share size are determined by the number of parties, e.g. in the best-known secret-sharing scheme for an arbitrary n-party access structure the share size is 1.5^n [AN21].

The assumption that the number of parties is known in advance is problematic in many scenarios. Of course, one can take some upper bound on the number of parties. On one hand, if this bound is big, then the share size will be large even if only few parties actually participate in the scheme. On the other hand, if this bound is small, then there is a risk that too many parties will arrive and no further shares can be produced; this will require an expensive re-sharing of the secret and updating all shares (which can be impossible if some parties are temporally off-line). Thus, we need to consider models with an unbounded number of parties.

To address these concrens, Komargodski, Naor, and Yogev [KNY18] defined *evolving secret-sharing schemes* with an unbounded number of parties. In a nutshell, evolving AS's are defined as a monotone collection of finite qualified sets, such that at any time t a set $A \subseteq [t]$ is either qualified of not, depending only on A itself, and not on t (a 'global' monotonicity).

Quantum secret sharing (QSS) in the standard n-party setting, where the secret is an arbitrary quantum state (say, qbit), rather than classical data. In face of recent advancements in quantum computing, this is a natural notion to consider, and has been studied before.

In this work, we explore the natural notion of quantum evolving secret sharing (QESS). While this notion has been studied by [Samadder 20'], we make several new contributions. (1) The notion of QESS was only implicit in the above work. We formalize this notion (as well as AS's for which it is applicable), and in particular argue that the variant implied by the above work did not require 'global monotonicity' of the AS, which was the standard in the evolving secret sharing literature, and appears to be useful for QESS as well. (2) Discuss the applicability and limitations of the notion in the quantum setting that follow from the no-cloning theorem, and make its usability more limited. Yet, we argue that fundamental advantages of the evovling setting, such as keeping parties' shares independent of the total number of parties that arrive can be mantainted in the quantum setting. (3) We characterize the AS's ammenable to construction of QSSS - so called 'no cloning' evolving AS's, and point out that this class is not severly restricted relatively to the class of all evolving AS's. On the positive side, our construction combines the compiler of [Smith 00'] with ideas of hybrid secret sharing of [Goyal et. al 23'], to obtain a construction with share size comparable to the best classical linear share complexity of the scheme.

1 Introduction

In the model of secret-sharing schemes [Bla79, Sha79, ISN89], there are n parties and a dealer, which holds a secret. The dealer applies some randomized algorithm to the secret, resulting in n strings, called shares; it gives the i'th share to the i'th party. There are two requirements. (1) correctness: some predefined subsets of the parties can jointly reconstruct the secret from their shares, and (2) security: any other set gets no information on the secret. The collection of predefined qualified sets is called an access structure (AS). It follows from the above definition that AS's are monotone in the sense that all supersets of a qualified set are also qualified.

These schemes are well-studied and have many applications. This model assumes that the number of parties is known when preparing the shares and giving the shares to the parties; furthermore, the sharing algorithm and the share size are determined by the number of parties, e.g. in the best-known secret-sharing scheme for an arbitrary n-party access structure the share size is 1.5^n [AN21].

The assumption that the number of parties is known in advance is problematic in many scenarios. Of course, one can take some upper bound on the number of parties. On one hand, if this bound is big, then the share size will be large even if only a few parties actually participate in the scheme. On the other hand, if this bound is small, then there is a risk that too many parties will arrive and no further shares can be produced; this will require an expensive re-sharing of the secret and updating all shares (which can be impossible if some parties are temporally off-line). Thus, we need to consider models with an unbounded number of parties.

To address these concerns, Komargodski, Naor, and Yogev [KNY18] defined *evolving secret-sharing schemes* with an unbounded number of parties. In a nutshell, evolving AS's are defined as a sequence of AS's $f^1, f^2, \ldots$, where the individual AS's $\mathcal{A}_t = \{A[t] | f^t(A) = 1\}$ are monotone. Also, the authorization of a set A depends only on the set itself. Namely, $f^t(A) = f^{t'}(A)$ for all t, t' for which $A \subseteq [min(t, t')]$. We refer to this property as *consistency*.

Quantum secret sharing (QSS) in the standard n-party setting, where the secret is an arbitrary quantum state (say, qbit), rather than classical data. In the face of recent advancements in quantum computing, this is a natural notion to consider and has been studied before.

In this work, we explore the natural notion of quantum evolving secret sharing (QESS). We start with a definition of QESS, and discuss the applicability and limitations of this notion in the quantum setting, as follows from the no-cloning theorem. We characterize the evolving AS's for which a QESS exists and put forward a construction for all AS's amenable to a QESS construction. Next, we provide a short overview of related work on QSS and evolving secret sharing, as well as an overview of existing work on quantum evolving secret sharing.

1.1 Quantum Secret Sharing (QSS) Schemes

Quantum secret sharing (QSS) in the standard n-party setting, where the secret is an arbitrary quantum state (say, qbit), rather than classical data, was first studied in [HBB99] for the threshold 2-out-of-2 case, and generalized in [CGL99] to the general threshold $t > n/2$ setting. In [Smi00] they explored QSS for general AS's. They devised a compiler converting linear classical secret-sharing schemes to quantum ones, for any structure for which no two disjoint sets can reconstruct the secret. We refer to such AS's as *no-cloning*, while [Smi00] refer to them as $Q2^*$. They also prove that *no-cloning* is necessary for the existence of a QSS, which was also proved, somewhat differently, by D. Gottesman in [Got00]). In a nutshell, the limitations on the AS's for which QSS is possible is due to the non-cloning theorem. The share complexity, in terms of a number of qdits (over a basis of size p) in every party's state, in [Smi00]'s work is the same as the number of field elements in the underlying linear scheme over the field $\mathbb{F}_p$. In a recent advancement in terms of the share complexity of QSS, in [CGLZR23], the authors initiate a study of computational QSS, and similarly to the classical setting, obtain polynomial-time schemes for a large class of AS's under standard assumptions. Most relevantly to our work, they obtain improved perfect QSS for a rich class of so-called *heavy* AS's, inheriting the complexity of the best known classical schemes in for worst-case AS's - $1.5^{n+o(n)}$. This is an improvement over current instantiations of [Smi00], as the best-known classical linear schemes have worse complexity.

1.2 Evolving secret sharing schemes

Komargodski, Naor, and Yogev [KNY18] defined *evolving secret-sharing schemes* with an unbounded number of parties. In this model, parties arrive one after the other and the number of parties that will arrive is not known. At the beginning of the execution, the dealer holds a secret (as in the standard model). When a party arrives, the dealer computes a share and gives it to the party; this share cannot be updated in the future. Thus, when preparing the t'th share, the dealer cannot assume any bound on the number of parties that will eventually arrive; the size of the t'th share should be measured as a function of t. We require correctness and privacy with respect to an *evolving access structure*, where the parties are $p_{i i \in \mathbb{N}}$ and the evolving access structure is a collection of finite subsets of the parties that are authorized to reconstruct the secret.[1]

Komargodski et al. [KNY18] showed that every monotone evolving access structure can be realized by an evolving secret-sharing scheme; in this scheme the size of the t'th share is 2^{t-1}. Recently, Mazor [Maz23] proved that evolving secret-sharing schemes require exponentially long shares – there is an evolving access structure such that in any evolving secret-sharing scheme realizing it the size of the share of the party is $2^{t-o(t)}$ (for infinitely many t's). This is unlike the state of the art in standard secret sharing, where a seminal recent breakthrough [LV18] led to an improvement over $2^{t-o(t)}$ (long conjectured to be the best possible), with 1.5^n being the best known result for general AS's to date. On the positive side, Komargodski et al. and follow-up works [KPC17, BO18, BO20, DDD21, FV23, OK20, PSAM21, XY24, YLH23, Pet23, ABD+24] constructed efficient evolving secret-sharing schemes for natural access structures. In particular, [KPC17] construct QESS with polynomial share complexity $\tilde{O}(t^4)$ for a natural extension of threshold schemes, called *dynamic threshold* AS's. Such a scheme is defined by a threshold monotone threshold function $k(t)$, defining an AS where the qualified sets in $[t]$ are those qualified in $[t-1]$ or those of size at least $k(t)$. We also note that Komargodski's basic scheme, as well as many of the schemes in the above list are implicitly linear. On a high level, this means that every share consists of one or more linear combinations of a secret s and random elements $r_1, r_2, r_3, \ldots$, all coming from a certain finite field $\mathbb{F}_p$. We include a formal definition of linear evolving schemes below (in taken from an unpublished paper, soon to appear on eprint).

[1] We assume that the order that the parties arrive is known in advance, or, alternatively, the t'th party to arrive assumes the role of the t'th party.

1.3 QESS - prior work vs. our contribution

In [Cha20], the authors consider QSS in the evolving setting and devise a QESS for dynamic threshold AS's. In this work, our contribution beyond this work is twofold.

1. We identify the set of evolving AS's which are amenable to the construction of QSS. Namely, it suffices that they are *no-cloning*. These notions are not explicitly defined in [Cha20], but apparently, the evolving AS notion used there does not require *consistency*. As discussed in Section 2.7, we view this property as essential for evolving secret sharing in the quantum setting as well. In fact, we observe that once consistency is required, the only dynamic threshold AS's that have QESS constructions are effectively finite (in the sense that starting from some t_0, adding parties cannot turn a set from unqualified to qualified).
2. We put forward a QESS construction for all evolving AS's satisfying both consistency and no-cloning for every t for *general* evolving AS's.

1.4 Our Techniques

As mentioned above, we first observe that evolving AS's only have QESS only if they are no-cloning. To this end, we use a precise definition of the structure of inputs and outputs of a (standard, n-party) QSS, following [CGLZR23], extending to QESS. Then, we prove a construction always exists for no-cloning evolving AS's, generalizing [Smi00]'s construction for finite no-cloning AS's.

Their construction is two steps. In the first step, they provide a (pure) QSS for self-dual 2.12 AS's, and then provide a (mixed) scheme for no-cloning AS's by reduction to the former case. This reduction transforms the AS into a self-dual one, by adding a single party p_0 (whose shares parties will never get), which is consistent with the original AS on sets that do not contain p_0. Then, they apply the construction from step 1, and qualified sets of parties trace out p_0's share (along with other parties' shares), to learn the secret.

To implement step 1 (for the finite case), a method to convert an MSP to QSS for self-dual AS's is presented. Specifically, for any no-cloning AS, the resulting scheme is a QECC (Quantum erasure correcting code) for $\mathcal{A}$ which are no-cloning, handling erasures occurring at sets B, for which

$f(B) = 0, f(\overline{B}) = 1$. When $\mathcal{A}$ is self-dual, the scheme is also a QSS (for $\mathcal{A}$). The authors note that this privacy property comes essentially 'for free' from correctness, combined with a strong variant of the no-cloning theorem, stating that one can not only clone a general state but also, can not obtain an output $Q(|s\rangle \otimes |\mathbf{0}\rangle) = |s\rangle \otimes \psi$, where ψ depends on $|s\rangle$ is some way. The exact statement and proof of this theorem did not appear in the original paper. Although not very difficult, and although we will in fact not need it for our construction we include a statement of the relevant theorem in Appendix **??**.

Theorem 1.1 ([Smi00]). *Let (K, M, ρ) be a MSP for an n-party AS $\mathcal{A}$ which is no-cloning. Then Construction 5.1 is a QECC correcting erasures on all unqualified $B \notin \mathcal{A}$. In other words, it is a QSS, with the privacy requirement removed. Furthermore, if $\mathcal{A}$ is self-dual, then the construction is a full QSS for $\mathcal{A}$.*

We stress that [Smi00]'s compiler is defined already for non-cloning f, and relies on the fact that f is no-cloning to prove correctness for qualified sets. In particular, although the above construction is well-defined for arbitrary M, if a pair of qualified sets $A, [n] \setminus A$ existed, it would not be a correct QSS, please see the proof of Theorem 2 in [Smi00] for more details. The extra self-duality property is needed only for privacy.

Unfortunately, this elegant approach does not work for the evolving setting. Roughly, the reason is that self-dual evolving AS's are very limited (see Appendix B), and their particular type of reduction would only work for this very limited class of AS's. Namely, these AS's are essentially finite!

Fortunately, we are able to salvage this approach using an idea from [CGLZR23]. In more detail, we naturally extend the above step 1 construction to the evolving setting for no-cloning AS's (the best possible), and forgo the reduction used in [Smi00]. To add privacy to the construction, we use the beautiful hybrid scheme as used in [CGLZR23] for a different purpose of improving the share complexity of QSSS (in the standard setting).

1. Encrypt $|s\rangle$ under a classical key k, via quantum OTP, to obtain $|s'\rangle$.

2. Share k via a standard evolving scheme for f.

3. Share $|s'\rangle$ via [Smi00]'s scheme. Here, we no longer rely on the schemes' privacy, for which the full-blown self-duality for each t was

required. The parties could have gotten $|s'\rangle$ in the clear.[2]

Roadmap. In section 2, we include the needed background on secret classical sharing, evolving secret sharing and quantum secret sharing. In particular, it includes a yet unpublished formalization of linear evolving secret sharing schemes (from another paper). In section 3 we put forward our notion of quantum evolving secret sharing, and discuss the limitations of its applicability, and propose an alternative scenario for the application of quantum evolving secret sharing. In Section 5 we describe our main QESS construction for the so called no-cloning evolving access structures. In Section 3 we observe that this is indeed the most general class of evolving AS's for which QESS exists. In Appendix B, we prove that the full-fledged approach of [Smi00]. Finally, in Section A we state and prove a variant of the no-cloning theorem on which Smith's construction bases its privacy on (implicitly, without a proof or an explicit reference).

2 Preliminaries

2.1 Classical secret sharing

Let us first define an Access Structure and then proceed to define a standard secret-sharing.

Definition 2.1. *(Access Structures) Let $\mathcal{P} = \{P_1, \dots, P_n\}$ be a set of parties. A collection $A \subseteq 2^{\{P_1,\dots,P_n\}}$ is monotone if $q \in A$ and $q \subseteq C$ imply that $C \in \Gamma$. An access structure $A \subseteq 2^{\{P_1,\dots,P_n\}}$ is a collection of non-empty sets. Sets in A are called authorized, and sets not in A are called unauthorized.*

An alternative yet equivalent approach is to represent Access Structure as a function $f : \{0,1\}^n \to \{0,1\}$ from each set of parties to a predicate whether the set P is authorized ($f(P) = 1$) or unauthorized ($f(P) = 0$).

Given an *AS* $\mathcal{A}$ It is sometimes convenient to denote it by $(\mathcal{A}, \mathcal{B})$, where B is the set of unqualified subsets of $[n]$. Note that this representation is redundant, as $\mathcal{A}$ or B alone specify (the same) the same f. Nevertheless, this notation is convenient as Smith [Smi00] uses B for speficying f, and refers to it as an adversary structure and some of the notions he uses, that we dapot here, are stated in terms of $\mathcal{B}$.

[2] The reason we need step 1 as a method to distribute $|s'\rangle$ while maintaining recoverability by qualified sets. For instance, we couldn't just send each party a copy of $|s'\rangle$, because of no cloning

Definition 2.2. *(minterm) A minimal authorized set in the access structure $\mathcal{A}$ is called minterm.*

Definition 2.3. *(redundant party)[Bei11a]*

A party is redundant in an access structure $\mathcal{A}$ if the party do not belong to a minterm in the access structure $\mathcal{A}$.

A secret-sharing scheme realizes an access structure $\mathcal{A}$ if the unauthorized set of parties will learn nothing about the secret while the authorized set of parties can reconstruct the secret. The formal definition is given as follows.

Definition 2.4. *(Secret-Sharing Schemes). A secret-sharing $\Sigma = \langle \mu, \Pi \rangle$ over a set of parties $\mathcal{P} = \{P_1, \ldots, P_n\}$ with domain of secrets S is a pair, where μ is a probability distribution on some finite set R called the set of random strings and Π is a mapping from $S \times R$ to a set of n-tuples $S_1 \times S_2 \times \ldots \times S_n$ (the set S_j is called the domain of shares of p_j). We will usually assume that μ is a uniform distribution over R. A dealer distributes a secret $s \in S$ according to Σ by first sampling a random string $r \in R$ according to μ, computing a vector of shares $\Phi(s, r) = (sh_1, ..., sh_n)$, and privately communicating each share sh_j to party p_j .*

For a set $q \subseteq \{p_1, \ldots, p_n\}$, we denote $\Pi_A(s, r)$ as the restriction of $\Pi(s, r)$ to its q-entries (i.e., the shares of the parties in q). The size of the secret is defined as $log\ |S|$, the size of the share of party p_j is defined as $log|S_j|$, and the size of the share of Σ as max $log|S_j|$. A secret-sharing scheme $\langle \mu, \Pi \rangle$ with domain of secrets S realizes an access structure $\mathcal{A}$ if the following two requirements hold:

Correctness. *Any authorized set of parties can reconstruct the secret s. That is, for any set $q = \{p_{i_1}, \ldots, p_{i_{|B|}}\} \in A$, there exists a reconstruction function $Recon_q : S_{i_1} \times \ldots \times S_{i_{|Q|}} \to S$ such that for every secret $s \in S$ and every random string $r \in R$, $Recon_q(\Pi Q(s, r)) = s$.*

Security. *Every unauthorized set cannot learn anything about the secret from its shares. Formally, for any set $T \notin A$, every two secrets $s_1, s_2 \in S$, and every possible vector of shares $\langle sh_j \rangle p_j \in T$,*

$$Pr[\Pi_T(s_1, r) = \langle sh_j \rangle_{p_j \in T_i}] = Pr[\Pi_T(s_2, r) = \langle sh_j \rangle_{p_j \in T_i}],$$

where the probability is over the choice of r from R at random according to μ.

2.1.1 Linear Secret Sharing Scheme As Monotone Span Program (MSP)

We bring an explanation about linear secret sharing and MSP from Amos Beimel survey on secret sharing [Bei11a].

The construction of a secret sharing scheme is linear when the distribution scheme is linear mapping. More formally, in a linear secret-sharing scheme over a finite field $\mathbb{F}$, the secret is an element of the field, the randomness is a vector over the field, such that each coordinate of this vector is chosen independently with uniform distribution from the field. Every party's share is a vector over the field such that each coordinate of this vector is some fixed linear combination of the secret and the coordinates of the randomness.

To model a linear scheme, we use monotone span programs (MSP), which is, basically, the matrix describing the linear mapping of the linear scheme. The monotone span program also defines the access structure that the secret-sharing scheme realizes.

Definition 2.5. *(Monotone Span Program ([KW93a]) is a triple $\mathcal{M} = (\mathbb{F}, M, \rho)$, where $\mathbb{F}$ is a field, M is an $a \times b$ matrix over $\mathbb{F}$, and $\rho : \{1, ..., a\} \to \{p_1, ..., p_n\}$ labels each row of M by a party. The size of $\mathcal{M}$ is the number of rows of M (i.e., a). For any set $A \subseteq p_1, ..., p_n$, let M_A denote the sub-matrix obtained by restricting M to the rows labeled by parties in A. We say that $\mathcal{M}$ accepts B if the rows of M_B span the vector $\mathbf{e_1} = (1, 0, ..., 0)$. We say that $\mathcal{M}$ accepts an access structure $\mathcal{A}$ if M accepts a set B iff $B \in A$.*

A monotone span program implies a linear secret-sharing scheme for access structure containing all the sets accepted by the program as stated below. For more details see [KW93a].

2.2 Evolving Secret Sharing Scheme

Definition 2.6. *(Evolving access structure)[HS16]*

A (possibly infinite) sequence of access structures A_t for $t \in \mathbb{N}$ is called evolving if the following conditions hold:

1. *(monotonicity) For every $t \in \mathbb{N}$, it holds that A_t is an access structure over t parties.*

2. *(consistency) For every $t \in \mathbb{N}$, it holds that $A_t|t-1$ is equal to $A_{(t-1)}$.*

When considering the alternative presentation of access structure as a function $f : \{0,1\}^n \to \{0,1\}$ from any set P to a predicate whether the set is authorized or not, we look at evolving access structure as a family of functions $f(t)$ that when we decide on a specific time value t give a function $f^t : \{0,1\}^t \to \{0,1\}$. The functions f^t in the family $f(t)$ preserve legacy over time in the sense that for any set P once there exist t such that $f^t(P) = 1$ then for all $t' > t$ it must be that $f^{t'}(P) = 1$.

The notions of minterm and redundant party naturally extend to the evolving setting.

One type of evolving AS that is useful to us is that of a Dynamic threshold.

Definition 2.7 (Dynamic thresholds [KP17]:)**.** *A dynamic threshold access structure has a sequence $k_1 \leq k_2 \leq \ldots$ of positive integers. For any $t \in \mathbb{N}$, the set of qualified sets A with $f^t(A) = 1$ contains all subsets of $[t]$ of cardinality at least k_t (and those qualified according to f^{t-1}).*

Of particular interest is the sequence with $k_t = \gamma \cdot t$ where $\gamma \in (0,1)$ is a fixed constant, which also appears to be the hardest parameter setting (for classical constructions).

Observation 2.1. *[[APC24]] Let f denote a dynamic AS specified by $k(t)$. Then wlog., one may assume $k_t \leq k_{t-1} + 1, k_1 \leq 2$.*

Definition 2.8. *(Secret sharing for evolving access structures)[HS16]*

Let $\mathcal{A} = \{\mathcal{A}_t\}_{t \in \mathbb{N}}$ be an evolving access structure. Let S be a domain of secrets, where $|S| \geq 2$. A secret sharing scheme for $\mathcal{A}$ and S consists of a pair of algorithms $(SHARE, RECON)$. The sharing procedure $SHARE$ and the reconstruction procedure $RECON$ satisfy the following requirements:

1. *$SHARE(s, \Pi_1^{(s)}, \ldots, \Pi_{t-1}^{(s)})$ gets as input a secret $s \in S$ and the secret shares of parties $1, \ldots, t-1$. It outputs a share for the t^{th} party. For $t \in \mathbb{N}$ and secret shares $\Pi_1^{(s)}, \ldots, \Pi_{t-1}^{(s)}$ generated for parties $1, \ldots, t-1$, respectively, we let*

$$\Pi_t^{(s)} \leftarrow SHARE(s, \Pi_1^{(s)}, \ldots, \Pi_{t-1}^{(s)})$$

be the secret share of party t. We abuse notation and sometimes denote by $\Pi_t^{(s)}$ the random variable that corresponds to the secret share of party t generated as above.

2. *Correctness: For every secret $s \in S$ and every $t \in \mathbb{N}$, every qualified subset in $\mathcal{A}_t$ can reconstruct the secret. That is, for $s \in S$, $t \in \mathbb{N}$, and $B \in \mathcal{A}_t$, it holds that*

$$Pr[RECON(\Pi_i^{(s)}{}_{i\in B}, B) = s] = 1,$$

where the probability is over the randomness of the sharing and reconstruction procedures.

3. *Secrecy: For every $t \in \mathbb{N}$, every unqualified subset $B \notin \mathcal{A}_t$, and every two secret $s_1, s_2 \in S$, the distribution of the secret shares of parties in B generated with secret s_1 and the distribution of the shares of parties in B generated with secret s_2 are identical. Namely, the distributions $(\Pi_i^{(s_1)}{}_{i\in B})$ and $(\Pi_i^{(s_2)}{}_{i\in B})$ are identical. The share size of the t^{th} party in a scheme for an evolving access structure is max $|\Pi_t|$, namely the number of bits party t holds in the worst-case overall secrets and previous assignments.*

2.2.1 Linear Evolving Secret Sharing Scheme As Infinite MSP

Monotone span programs [KW93b] were used to construct linear secret-sharing schemes in [Bei11b]. In this section, we include a natural extension of MSP's to the evolving setting, capturing 'implicitly linear' constructions from the evolving secret sharing literature. This definition is part of [APC24] (will be happy to send as complementary material, if needed).

Notation. For IMSP's, we will deal with a certain type of infinite matrices over a finite field $\mathbb{F}$. The product of an infinite matrix $K \in \mathbb{F}^{[n]\times\mathbb{N}^+}$ by a finite vector $\mathbf{r} \in \mathbb{F}^{[m]}$ is defined as $K'r$, where K' is obtained by keeping the first m columns of K. Such products for matrices are typically used where all but the first m columns are 0. Generally, for a matrix M, we let $M[A, B]$ denote the submatrix of M restricted to row set A and column set B. $A = *$ $(B = *)$ stands for all rows (columns), and $A = i$ $(B = i)$ for a single index i, is a shorthand for $A = \{i\}$ $(B = \{i\})$.

Definition 2.9 (Infinite Monotone Span Program–IMSP)**.** *An IMSP is a triple $\mathcal{M} = (\mathrm{F}, M, \rho)$, where $\mathbb{F}$ is a finite field, $M \in \mathbb{F}^{\mathbb{N}\times\mathbb{N}}$ is an infinite* *matrix over $\mathbb{F}$, and $\rho : \mathbb{N}^+ \to \mathbb{N}^+$ labels each row of M by a party. There is a finite number of non-zero elements in each row in M, and $\rho^{-1}(x)$ is finite for every $x \in \mathbb{N}^+$, that is, each party gets a finite number of rows (shares). For any finite set $A \subseteq [n]$ of party indices, let M_A denote the sub-matrix obtained by restricting M to the rows i, with $\rho(i) \in A$. We say that $\mathcal{M}$ accepts B if the rows of M_B span the vector $\mathbf{e_1} = (1, 0, 0, \ldots)$. We say that $\mathcal{M}$ implements an evolving access structure Γ if $\mathcal{M}$ accepts a set B if and only if $B \in \Gamma$.*

For a finite set of parties A , denote by $C_A = \{j | \exists i, \rho^{-1}(i) \in A, M_{i,j} \neq 0\}$, the set of non-zero entries it holds.

Remark 2.1. *Note that in IMSP, it is only possible to use target vectors that have a finite number of non-zero entries, rather than any non-zero vector, as is the case in standard MSP. We make the simple choice of setting the target vector $\epsilon = (1, 0, 0, \ldots)$, and not make the target vector part of our definition. In particular because we do not need it, the more general definition is equivalent, though.*

We also denote by M_t the submatrix $M[\{i|\rho^{-1}(i) \in [t]\}, *]$. We let $Rows(M), Columns(M)$ denote the set of rows (columns) of a matrix M (both finite or infinite).

MSP-based linear secret sharing schemes can be easily generalized to the evolving setting, essentially giving each party the linear combinations of a randomness vector (that also defines the secret s), as specified by the IMSP. As in the finite case, every finite subset $A \subseteq \mathbb{N}^+$ either reconstructs the secret, or learns nothing about it.

Theorem 2.2. *[APC24] Let $\mathcal{M} = (\mathbb{F}, M, \rho)$ be an IMSP accepting an access structure Γ. Then, there exists an evolving secret sharing scheme (based on $\mathcal{M}$), that implements Γ for secret domain $S = \mathbb{F}$. The share of party t is comprised of $|Rows(M_t)| - |Rows(M_{t-1})|$ field elements.*

The following theorem states the basic feasibility of linear evolving secret sharing for all evolving AS's.

Theorem 2.3. *[KPC17] Let Γ denote an evolving access structure. Then there exists an IMSP $(\mathbb{F}_2, M, \rho)$ implementing it (for secret domain $S = \mathbb{F}_2$). Share size of the resulting scheme is at most 2^{t-1}.*

We note that for rich classes of AS's, the resulting share complexity is much better. For instance, for rich classes of evolving AS's, such as the infinite Branching Program (IBP) based constructions in [ABD+24], where the IBP width is relatively small, for which one could obtain much smaller share size. Although they are not explicitly stated as linear schemes, using linear schemes for the predicates at the edges of the resulting generalized tree (GIDT). A simple concrete example, capturing the most general case we are aware of casting previous schemes as IMSP's, we observe that in [KPC17]'s construction, each party p_t gets a finite number of independent Shamir sharings of secrets which are linear combinations of s and random elements in $\mathbb{F}_2$, for some finite number n_t of parties. To make this work, $\mathbb{F}_{2^\ell}$ used is some extension field of $\mathbb{F}_2$ (with different ℓ's used for different t's). However, one can interpret the results of linear combinations over the extension field as ℓ linear operations over the base field, resulting in an IMSP as above. See [APC24] for a detailed example.

2.3 Quantum Secret Sharing Scheme (QSS)

Notation. The state of an m-qubit vector is represented by a unit vector $v \in \mathbb{C}^{2^m}$ such that the state takes the value x with probability $|v_x|^2$ when measured. A valid quantum operator is any function $F : \mathbb{C}^{2^m} \to \mathbb{C}^{2^m}$ that is unitary, i.e., linear and norm-2 preserving.

That is, a quantum state[AB09] ϕ is in a Hilbert space overall 2^m tensor products of m "qubits" (the quantum parlance to bits), where each qubit is over the base $\{|0\rangle, |1\rangle\}$, and each qbit is normalized to have norm-2 that equals 1.[3] We denote by $\phi = \sum_{x\in\{0,1\}^m} \alpha_i |x\rangle$ for $\alpha_x \in \mathbb{C}$, where $|ab\rangle$ is a shorthand for $|a\rangle \otimes |b\rangle$. We often use quantum states $|s\rangle$ and their density matrices $|s\rangle\langle s|$ interchangeably (adapting the operators accordingly).

We denote by $tr_{\bar{P}}$ tracing out the subsystem computations corresponding to the party $\bar{P}$. See 2.7 for an in-depth overview of quantum computation.

We adopt definition of the Quantum secret sharing definition from [ÇGLR23] which is based on Quantum erasure-correcting codes(QECC) [GBP97], which allows to encode a quantum state into another quantum state of larger dimension, so that the original one can be retrieved perfectly even when there are erasures (arbitrary errors at known positions).

Definition 2.10. *(Quantum erasure correcting code[ÇGLR23]).*

A pair of trace-preserving quantum operations $QC = (QC.Enc, QC.Dec)$ is a quantum erasure correcting code (QECC) over the input space $\mathcal{H}_{inp}$

[3] This generalizes to qdits, which are over a basis of size $d \geq 2, |0\rangle, \ldots, |d-1\rangle$.

and output space $\mathcal{H}_{out} = \otimes_{i\in[n]}\mathcal{H}_i$ for $P \subseteq [n]$ if for any quantum operation Λ on $\mathcal{H}_{out}$ that acts as the identity on $\mathcal{H}_i$ for all $i \in P$, it holds for all states ρ on $\mathcal{H}_{inp}$ that

$$(QC.Dec \circ \Lambda \circ QC.Enc)(\rho) = \rho \otimes \sigma$$

for some state σ, and suitable ℓ.

If $(QC.Enc, QC.Dec_P)$ is a QECC for all sets $P \subseteq [n]$ such that $f(P) = 1$ for a monotone function $f : \{0,1\}^n \to \{0,1\}$, then we say that the family of functions $(QC.Enc, (QC.Dec_P)_{P\subseteq[n]})$ is a QECC realizing f. As a shorthand, we define $QC.RecP(\tau) = QC.Dec(\tau \otimes (|0\rangle\langle 0|)^{\otimes \overline{P}})$. A quantum code that encodes k q-ary qdits into n q-ary qudits and can correct any $d-1$ erasures is said to be an $[[n,k,d]]q$ code.

Definition 2.11. *(No-cloning AS) We say a monotone function $f : \{0,1\}^n \to \{0,1\}$ is no-cloning if for all $P \subseteq [n]$ $f(P) = 1$ implies $f(\overline{P}) = 0$.*

We refer to such AS's as *no-cloning*, while [Smi00] refer to them as $Q2^*$, because this is the limitations on the AS's for which QSS is possible due to the non-cloning theorem.

Definition 2.12. *(Self dual AS) We say a monotone function $f : \{0,1\}^n \to \{0,1\}$ is self-dual if for all $P \subseteq [n]$ $f(P) = 1$ iff. $f(\overline{P}) = 0$.*

Definition 2.13. *(Quantum secret sharing) Fix a number of parties $n \in \mathbb{Z}^+$, a Hilbert space $S = \mathcal{H}_0$ for the secret, and Hilbert spaces $H_1, \ldots, H_n$ for the shares. Let $f : \{0,1\}^n \to \{0,1\}$ be a no-cloning monotone function. A quantum secret sharing (QSS) scheme with perfect privacy realizing f is a tuple of quantum operations*

$$QSS = (\mathbf{Share}, (\mathbf{Rec}_P)_{P\subseteq[n]})$$

that satisfy the following properties for all $P \subseteq [n]$:

- *Correctness: If $f(P) = 1$, then $(\mathbf{Share}, \mathbf{Rec}_P)$ is a QECC for P, with $\mathcal{H}_{inp} = \mathcal{H}_0$ and $\mathcal{H}_{out} = \mathcal{H}_1 \otimes \ldots \otimes \ldots \otimes \mathcal{H}_n$.*
- *Perfect Privacy: If $f(P) = 0$, then for any $|\Psi_1\rangle, |\Psi_2\rangle \in S$ it holds that*

$$\mathbf{tr}_{\bar{P}}(\mathbf{Share}(|\Psi_1\rangle\langle\Psi_1|)) = \mathbf{tr}_{\bar{P}}(\mathbf{Share}(|\Psi_2\rangle\langle\Psi_2|)).$$

The share size of party p_i, $sc(i)$ is $\log_{dim(\mathcal{H}_0)}(dim(\mathcal{H}_i))$.[4]

[4] For example, $sc(i) = 3$ if $\mathcal{H}_i = \mathcal{H}_0 \times \mathcal{H}_0 \times \mathcal{H}_0$.

Observation 2.4. *An AS has QSS only if it is no-cloning. (def' 2.11)*

This was proved by [Smi00] and also by D. Gottesman in [Got00]). On a high level, this is a direct consequence of the no-cloning theorem, that roughly states that a general quantum state $|s\rangle$ can not be cloned. That is, no quntum operator maps $|s\rangle \otimes |\mathbf{0}\rangle$ to $|s\rangle \otimes |s\rangle \otimes |\psi\rangle$ for some ψ. This implies the observation as otherwise, sharing of s, and then reconstruction by each of the disjoint sets, would yield a circuit that clones the secret.

3 Quantum Evolving Secret Sharing Scheme (QESS)

Definition 3.1. *[No-cloning Evolving Access Structure] Let $f = \{f^t\}_{t\geq 1}$ denote an evolving AS. We say that f is no-cloning, if each f^t is no-cloning.*

Definition 3.2. *(Quantum secret sharing for evolving access structure (QESS)) Let $\{f^t\}_{t>0}$ be a No-cloning Evolving Access Structure. Let $\mathcal{H}_0, \mathcal{H}_1, \mathcal{H}_2 \ldots$ denote a sequence of (finite) Hilbert spaces, where H_0 is a Hilbert space for the secret and $\mathcal{H}_i$ is a Hilbert space for the share of party i. Let t_0 denote the smallest integer for which f^{t_0} is not identically 0.*

An evolving quantum secret sharing (QESS) scheme with perfect privacy and correctness realizing f is an infinite sequence of tuples of quantum operations

$$\{QESS_t = (\mathbf{Share^t}, (\mathbf{Rec^t}_P)_{P\subseteq[t]})\}_{t\geq t_0}$$

that satisfy the following properties for all $P \subseteq [t]$ and any $t \geq t_0$:

- *$QESS_t$ is a QESS with secret domain $\mathcal{H}_0$ and output domain $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_t$ and party set $[t]$.*
- *For any t, and any secret $|s\rangle$, we have*

$$\mathbf{Share^t}(|s\rangle \otimes |0^\ell\rangle) = \mathbf{tr}_{\{t+1\}}(\mathbf{Share^{t+1}}(|s\rangle \otimes \left|0^{\ell'}\right\rangle),$$

where $\ell \leq \ell'$ are suitable dimensions (as specified by $Share^t, Share^{t+1}$).[5]

The share size of a party p_i is its share size in $\mathbf{Share^i}$ *(and is the same for all subsequent t''s, by consistency)*

Observation 3.1. *An evolving AS has QESS only if it is non-cloning.*

[5] In the sequel, we often make the ancillas $|0^\ell\rangle, \left|0^{\ell'}\right\rangle$ implicit.

Application of an evolving QESS - inherently weaker than the classical setting! The dealer works in two phases. During phase 1 the dealer applies the above algorithms iteratively, computing the current time slot's $t+1$ $Share^{t+1}(|s\rangle)$ from the outputs $Share^{t}(|s\rangle)$ (combined with a few additional ancilla bits). Namely, it computes $(Sh^{t})^{-1}(sh_1^t \otimes \ldots \otimes sh_t^t) \otimes I(\left|0^{\ell'-\ell}\right\rangle) \otimes \left|0^{\ell'-\ell}\right\rangle) = |s\rangle \otimes \left|0^{\ell'}\right\rangle$. Then it applies Sh^{t+1} to the result, obtaining $sh^{t+1} = sh_1^{t+1} \otimes \ldots \otimes sh_t^{t+1} \otimes sh_{t+1}^{t+1}$. At the start of phase 2, which may potentially start at each time slot t, when the Dealer is notified whether a qualified set $A \subseteq [t]$ that arrived so far. The Dealer then sends the shares sh_i^t computed for each $i \in [t]$ that arrived, and keeps the shares in $[n] \setminus S$ to itself. At some point in the future, the parties in A may recover the secret, by applying Rec_A^t to their shares (and suitable ancilla bits).[6] [7] The reason we work in this manner is that to continue computing shares for larger and larger values of t, the dealer needs the previous shares, and can not generally give them away or give a copy (due to no cloning). Although parties can no longer asynchronously obtain their secret, but rather get it all at the same time and keep it unchanged until a later recovery time, consistency between the shares of p_i at different times is still important. We still maintain the advantage that earlier parties obtain smaller shares. Had we not had consistency, this could no longer hold. To remedy this, we could only require that the size of a share of p_i does not grow as the time t advances (aka, in $Share_t, Rec_r$). Furthermore, note that in the quantum setting the shares are always recomputed from $|s\rangle \otimes |\mathbf{0}\rangle$ in any case, so there is no concept of using "the same" randomness for p_i's share at all times, but rather the value of this share is the same vector of qbits (tensored with the other shares), which induces the same distributions on sh^i (when measured). Nevertheless, we stick with this requirement to be consistent with the more stringent classical notion of evolving secret sharing, which may be useful in a future application.

Remark 3.1. *Yet again, especially in the quantum setting, but also in the classical setting, for applications where a communication pattern as above is suitable, one could consider a relaxed evolving secret sharing notion, where shares may be recomputed, but p_i's share needs to be bounded by a small size $s(i)$ at all times.*

[6] In fact, the dealer could perform a single computation of Sh^t on $|s, \mathbf{0}\rangle$ when the initiator of phase 2 arrives. However, this could be useful if we want to have 0 latency at sending the shares at the correct time slot (which would be ready from the start).

[7] Note that we define and use $Share^t$'s only for t for which f_t is not the constant 0. Otherwise, information on $|s\rangle$ is lost. This way, the first t_0 parties necessarily obtain their share upon the arrival of P_t, for some $t \geq t_0$.

3.1 Inherent limitation of No-Cloning for evolving access structures

Intuitively, any quantum secret sharing for evolving access structure(QESS), by definition of the no-cloning evolving access structure is restricted by both the no-cloning theorem which is required for quantum operations, and also by the need to preserve legacy over time which is required for the correctness of an evolving protocol (that is, $f^t(A) = f^{t+1}(A)$ for all $A[t]$) . However, the no-cloning requirement means that for any pair of qualified sets P_i, P_j, $P_i \cap P_j \neq \phi$. This is the case, since otherwise for t where $P_i \cup P_j \subseteq [t]$, $[t] \setminus P_j$ would be qualified, breaking the non-cloning property of the finite AS f^t. We observe that in spite of these restrictions, a great richness of eligible AS's remains. Namely, we note that for any (unrestricted) evolving AS f, adding a single party to the set of parties, and letting defining f' over party set $\{0\} \cup \mathbb{N}^+$, and add the party 0 to every minterm.

Observation 3.2. *Let $\mathcal{A}$ be an evolving AS over party set $\mathbb{N}^+$. Then $\mathcal{A}'$ whose set of minterms is of the form $\{M' = M \cup \{0\} | M$ is a minterm of $f\}$, defined over party set $\mathbb{N}$ is a Non-cloning evolving AS.*

As mentioned above, although the set of AS's the above observation yields is very rich, one could add several parties, so that no single party is part of every minterm.

4 A note on [Cha20] QESS for Dynamic Thresholds

In [Cha20] Shion Samadder Chaudhury initiate the study of quantum evolving schemes to share a quantum secret and present a construction of an evolving quantum secret sharing scheme ($QESS$) which shares and protects a secret quantum state. Although their construction seems to be of value, their definition of the general QESS is apparently different, and does not take into account both requirements of every f^t being non-cloning, and *consistency* in the sense that $\mathcal{A}_t = \mathcal{A} \cap [t]$. Namely, they do account for the first requirement, and correctly observe that by the no-cloning theorem, each f^t must by no-cloning, which in this case implies that $k_t > t/2$ for all t. However, if consistency is also required, we observe that in that case $k(t)$ must be so large, that the AS becomes essentially finite.

Theorem 4.1. *Let f be a dynamic threshold evolving AS specified by*

$k(t)$. Then it is no-cloning only if

$$k(t_1) > n_{t_1} - t_0$$

for all $t_1 \geq 2t_0$, where t_0 is the smallest integer, for which $f^{t_0} \neq 0$. [8] *In particular, threshold AS's f which are non-cloning are effectively finite, in the sense that all parties $t' > N_f$ for a certain constant N_f are redundant.*

Proof. Assume $k(t) > n_t - t_0$ does not hold for some $t_1 \geq 2t_0$. we show there exist two disjoint qualified sets A, B, which contradicts no-cloning for f^t for all t's where $A, B \subseteq [t]$. Specifically, we set A to be a minterm in $[t_0]$, and $B = \{t_0 + 1 \leq i \leq t_1\}$. Since $k(t_1) \leq n_{t_1} - t_0$, or equivalently, $n_{t_1} - k(t_1) \geq t_0$, $f^{t_1}(B) = 1$. By consistency, and the fact that $f^{t_0}(A) = 1$, $1 = f^{t_1}(A)$. Also, by construction, $A \cap B = \phi$, contradicting the fact that f^{t_1} (and thus f) is no-cloning. For the "in particular" part, by the first part we have $k(t_1) > n_{t_1} - t_0$ for all $t_1 \geq 2t_0$. For a set A, if $A \cap [2t_0] \leq t_0$, it is not qualified according to f^{2t_0}, and is not qualified for any $t' > 2t_0$, since even if all the following parties in $[t']$ are in A, the difference $max_{t' \in A} t' - |A| \geq t_0$. Otherwise, if $A \cap [2t_0] > t_0$, then it is qualified according to f^{2t_0}, and the remains qualified for all $t > 2t_0$ by consistency. Thus, all parties in the AS but the first $2t_0$ are redundant (as $f(A) = f^t(A \cap [2t_0])$ for all $t \geq 2t_0$).

□

5 Quantum Evolving Secret Sharing Scheme (QESS) Based on MSP

5.1 Quantum Secret Sharing (QSS) based on MSP [Smi00]

In [Smi00], a characterization of (finite) AS's which have a QSS is put forward. Namely, these are exactly the AS's that are no-cloning. Their construction is two-step. In the first step, they provide a (pure) QSS for self-dual 2.12 AS's, and then provide a (mixed) scheme for no-cloning AS's by reduction to the former scheme. This reduction transforms the AS into a self-dual one, by adding a single party p_0 (whose shares parties will never get), which is consistent with the original AS on sets that do not contain p_0. Then, they apply the construction from step 1, and qualified sets of parties trace out p_0's share (along with other parties' shares), to learn the secret.

[8] In fact, by Observation 2.1, we have $t_0 = k(t_0)$ - that is, t_0 is the earliest instance when $t \geq k(t)$.

To implement step 1 (for the finite case), a method to convert an MSP to QSS for self-dual AS's is presented. Specifically, for any no-cloning AS, the resulting scheme is a QECC (Quantum erasure correcting code) for $\mathcal{A}$ which are no-cloning, handling erasures occurring at sets B, for which $f(B) = 0, f(\overline{B}) = 1$. When $\mathcal{A}$ is self-dual, the scheme is also a QSS (for $\mathcal{A}$). The authors note that this privacy property comes essentially 'for free' from correctness, combined with a strong variant of the no-cloning theorem, stating that one can not only clone a general state, but also, we can not obtain an output $Q(|s\rangle \otimes |\mathbf{0}\rangle) = |s\rangle \otimes \psi$, where ψ depends on $|s\rangle$ is some way. The exact statement and proof of this theorem did not appear in the original paper. Although not very difficult, and although we will in fact not need it for our construction we include a statement of the relevant theorem in Appendix A.

Let us spell [Smi00]'s construction for completeness, pointing out certain implementation and proof details that were omitted in the original paper.

Construction 5.1.

- *Consider an MPS (K, M, ρ) specifying a no-cloning access structure $f : P([n]) \to \{0, 1\}$, which is not identically 0.*
- *Extend M to an invertible $d \times d$ matrix M'. Notice that this is possible because wlog all $e \leq d$ columns* [9] *of M are linearly independent. Note also that the column vector corresponding to the secret's column, sc, is non-zero, and is included in every basis of the columns, as there exists $v \in Ker(cols(M))$, such that $< v, sc >= 1$ (e.g pick v as guaranteed to satisfy $v^T M = (1, 0, \ldots, 0)$, which exists as $[n]$ must be qualified).*
- *An input secret $|s\rangle$ is encoded as $|s\rangle \otimes \left|0^{d-1}\right\rangle$*
- *Construct a quantum operator $\tilde{M}$ implementing multiplication by M' and encode*[10] *a basis state $|s\rangle$, for $s \in K$ as follows*

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

This is a valid unitary operator, as mapping each basis state $|s\rangle \otimes |a_1 \ldots a_{e-1}\rangle \otimes |0 \ldots 0\rangle$ is mapped to $\left|M(s\Game)^T \otimes \left|0^{d-e}\right\rangle\right\rangle$, which defines

[9] In the original paper there was a typo: stating the rows are independent wlog.

[10] The code word for the quantum secret $|s\rangle$ in this QECC is computed in equation 1.

a partial permutation over basis vectors of the dim-K^d vector space, where the mapping of other vectors is complemented arbitrarily.

- *This scheme can be extended by linearity to arbitrary states* $|\phi\rangle = \sum_{s\in K} \alpha_s |s\rangle$ *(and density matrices). As usual, to obtain* $|s\rangle \otimes \sum_{a\in K^{e-1}} |a_1 \dots a_{e-1}\rangle \otimes |0\dots 0\rangle$ *from the encoded input, we apply* $I \otimes H \otimes H \otimes \dots \otimes H \otimes I \dots I$ *to it, where* H *is a Hadamard-like gate, mapping* $|0\rangle$ *to* $\sum_{i\in K} |i\rangle$.

Theorem 5.2 ([Smi00]). *Let* (K, M, ψ) *be a MSP for an* n*-party AS* $\mathcal{A}$ *which is no-cloning. Then Construction 5.1 is a QECC correcting erasures on all unqualified* $B \notin \mathcal{A}$*. In other words, it is a QSS, with the privacy requirement removed. Furthermore, if* $\mathcal{A}$ *is self-dual, then the construction is a full QSS for* $\mathcal{A}$.

As explained in the introduction, step 2 of [Smi00] does not work for the evolving setting. Instead, to add privacy to the construction, we use the beautiful hybrid scheme as used in [CGLZR23] for a different purpose of improving share complexity of QSSS (in the standard setting).

1. Encrypt $|s\rangle$ under a classical key k, via quantum OTP, to obtain $|s'\rangle$.
2. Share k via a standard evolving scheme for f.
3. Share $|s'\rangle$ via [Smi00]'s scheme. Here, we no longer rely on the schemes' privacy, for which the full-blown self-duality for each t was required. The parties could have gotten $|s'\rangle$ in the clear.[11]

5.2 Our construction

For convenience, we state our construction for $K = \mathbb{F}_2$. We use the following theorem on the existence of a quantum varianto of the OTP encryption, where an arbitrary quantum value is encrypted via a random classical key.

Theorem 5.3. *[QOT [?]] Let* $|s\rangle$ *denote an arbitrary qbit. Let* $OTPEnc(|s\rangle, k) = X^{k_1} Z^{k_2} |s\rangle \langle s| (X^*)^{k_1} (Z^*)^{k_2}$ *, where* X *and* Z *are Pauli gates.*[12] *Then*

$$\sum_{k\in\{0,1\}^2} OTPEnc(|s'\rangle, k) = \sum_{k\in\{0,1\}^2} OTPEnc(|s\rangle, k)$$

for all $|s\rangle, |s'\rangle$ *(privacy). Also, for every* k, $|s\rangle$ *we have that for all density matrices* s, $v = OTPEnc(s, k)$, $OTPDec(v, k) = (Z^*)^{k_2} (X^*)^{k_1} v Z^{k_1} X^{k_2} = |s\rangle \langle s| = s$.

[11] The reason we need step 1 as a method to distribute $|s'\rangle$ while maintaining recoverability by qualified sets. For instance, we couldn't just send each party a copy of $|s'\rangle$, because of no cloning

[12] $OTPEnc$ naturally extends to density matrices s over qbits.

Extending Smith's construction to the evolving setting, we proceed as follows.

Construction 5.4.

- *Input: a qbit $|s\rangle$.*
- *An evolving no-cloning AS f, where t_0 is the smallest integer for which $f^{t_0} \neq 0$ implemented by an evolving linear MSP (M, K, ψ) over $\mathbb{F}_2$.*
- *Initialization: Sample a pair of random classical bits (k_1, k_2). Let $\rho = OTPEnc(|s\rangle, k)$.*
- *Share k according to a standard evolving linear scheme for f (these shares are a classical part of every $Share^t$'s output).*
- *$Share^t : (|s\rangle, |0\rangle^\ell)$ (ℓ to be stated below), for $t \geq t_0$. Let M_t denote the (finite) submatrix of M corresponding to parties $[t]$. Recall zero-columns are removed, leaving us with a finite number c_t of columns. Let e_t denote the size of a set C_t of columns that constitute a basis for the column set of the $d_t \times c_t$ matrix M_t (recall that the column corresponding to s is necessarily among them). Apply Construction 5.1 to $|s\rangle$ and M_t.*
- *To reconstruct the secret from $Share^t$'s output (which also includes $OTPEnc$'s shares), reconstruct ρ, and k independently, and then apply $OTPDec$ to recover $|s\rangle$.*

Theorem 5.5. *Let f denote a no-cloning evolving AS, such that t_0 is the minimal integer for which $f^{t_0} \neq 0$. Construction 5.4 is a QESS for f, with share complexity of $|Rows(M_t)| - |Rows(M_{t-1})|$, where $(M, \mathbb{F}, \rho)$ is the IMSP used by this construction.*

Proof sketch. Correctness follows directly from correctness of Construction 5.1 for each $t > t_0$. Privacy follows from the fact that for an unqalified set's point of view, k_1, k_2 remain random, and thus ρ (even if fully reconstructed) appears to it as a quantum state which is independent of $|s\rangle$. Finally, by structure of M, $Sh^t(|s\rangle)$, derived from $Sh^{t+1}(|s\rangle)$ is the same as $Sh^{t+1}(|s\rangle)$ (with its added input qbits). To see that, recall that by structure of M, M_t is a submatrix of M_{t+1} covering the subset of d_t first rows. Thus, we have

$$\tilde{M}_{t+1}\left(|s\rangle \otimes \sum_{a \in K^{e_{t+1}-1}} \left|a_1 \dots a_{e_{t+1}-1}\right\rangle \otimes |0 \dots 0\rangle\right) = \qquad (2)$$

$$\sum_{a\in K^{e-1}} \left| M'_{t+1}[[d_t],*] \begin{pmatrix} s \\ a \\ 0^{d_{t+1}-e_{t+1}} \end{pmatrix} \right\rangle = \left| M_{t+1}[[d_t],*] \begin{pmatrix} s \\ a \end{pmatrix} \right\rangle \tag{3}$$

The latter equation yields a uniform distribution over the vectors in $colSpan(M_t)$, as is the case for the output of $Share^{t+1}$.

A Strong form of the no-cloning theorem

Definition A.1. *(information-theoretic privacy on QSS-based MSP) Given a quantum secret sharing-based MSP if the view of the unauthorized parties that consist of their shares of the secret s is constant and identical to their shares in the case of the secret s' where $s' \neq s$ then the scheme has information-theoretic privacy.*

Theorem A.1. *(Generalized form of the no-cloning theorem)*
For every quantum operator D s.t. for every $|s\rangle = \alpha|0\rangle + \beta|1\rangle$ $D(|s\rangle \otimes |0^l\rangle)$ is of the form $|s\rangle \otimes |B(s)\rangle$, it holds that for every $|s\rangle = \alpha|0\rangle + \beta|1\rangle, |s'\rangle = \alpha'|0\rangle + \beta'|1\rangle$ $|B(s)\rangle = |B(s')\rangle$. [13] *Furthermore, only no-cloning f's admit a QESS.*

Proof. Suppose, for contradiction, that there is quantum operator D s.t. given any quantum state

$$|s\rangle = \alpha|0\rangle + \beta|1\rangle$$

,

$$D(|s\rangle \otimes |0^l\rangle) = (|s\rangle \otimes B(s) =$$
$$(\alpha|0\rangle + \beta|1\rangle) \otimes (b^0_{(s)}|0^l\rangle + b^1_{(s)}|0^{l-1}1\rangle + \ldots + b^{2^{l-1}}|1^{l-1}0\rangle + b^{2^l-1}_{(s)}|1^l\rangle)$$

where $|B(s)\rangle = b^0_{(s)}|0^l\rangle + b^1_{(s)}|0^{l-1}1\rangle + \ldots + b^{2^{l-1}}|1^{l-1}0\rangle + b^{2^l-1}_{(s)}|1^l\rangle$ is a quantum state that its values and probabilities depend on $|s\rangle$.

On one hand, by the definition of D we get ,

$$D(|s\rangle \otimes |0^l\rangle) = (\alpha|0\rangle + \beta|1\rangle) \otimes (b^0_{(s)}|0^l\rangle + \ldots + b^{2^l-1}_{(s)}|1^l\rangle) =$$
$$\alpha b^0_{(s)}|00^l\rangle + \ldots + \alpha b^{2^l-1}_{(s)}|01^l\rangle + \beta b^0_{(s)}|10^l\rangle + \ldots + \beta b^{2^l-1}_{(s)}|11^l\rangle$$

I.e.

$$D(|s\rangle \otimes |0\rangle) = \alpha b^0_{(s)}|00^l\rangle + \ldots + \alpha b^{2^l-1}_{(s)}|01^l\rangle + \beta b^0_{(s)}|10^l\rangle + \ldots + \beta b^{2^l-1}_{(s)}|11^l\rangle \tag{4}$$

[13] The theorem can be easily generalized to any finite Hilbert space for s, using a similar proof.

On the other hand, $|s\rangle \otimes \left|0^l\right\rangle = (\alpha|0\rangle + \beta|1\rangle)\left|0^l\right\rangle = \alpha\left|00^l\right\rangle + \beta\left|10^l\right\rangle$ by this equality we know that

$$D(|s\rangle \otimes \left|0^l\right\rangle) = D(\alpha\left|00^l\right\rangle + \beta\left|10^l\right\rangle)$$

By the linearity of any quantum operator, we get :

$$D(\alpha\left|00^l\right\rangle + \beta\left|10^l\right\rangle) = \alpha \cdot D(\left|00^l\right\rangle) + \beta \cdot D(\left|10^l\right\rangle) =$$

$$\alpha|0\rangle(b^0_{(0)}\left|0^l\right\rangle + \ldots + b^{2^l-1}_{(0)}\left|1^l\right\rangle) + \beta|1\rangle(b^0_{(1)}\left|0^l\right\rangle + \ldots + b^{2^l-1}_{(1)}\left|1^l\right\rangle) =$$

$$\alpha b^0_{(0)}\left|00^l\right\rangle + \ldots + \alpha b^{2^l-1}_{(0)}\left|01^l\right\rangle) + \beta b^0_{(1)}\left|10^l\right\rangle + \ldots + \beta b^{2^l-1}_{(1)}\left|11^l\right\rangle$$

I.e.

$$D(\alpha\left|00^l\right\rangle+\beta\left|10^l\right\rangle) = \alpha b^0_{(0)}\left|00^l\right\rangle+\ldots+\alpha b^{2^l-1}_{(0)}\left|01^l\right\rangle)+\beta b^0_{(1)}\left|10^l\right\rangle+\ldots+\beta b^{2^l-1}_{(1)}\left|11^l\right\rangle \tag{5}$$

The operator D must have at least one input s s.t. both $\alpha \neq 0$,$\beta \neq 0$. Therefore we get: $\forall i : b^i_{|s\rangle} = b^i_{|0\rangle}$ along with: $\forall i : b^i_{|s\rangle} = b^i_{|1\rangle}$

Then, from the transitivity of an equation, we get:

$$\forall i : b^i_{|s\rangle} = b^i_{|0\rangle} = b^i_{|1\rangle} = b^i$$

Therefore from observing D operation on an s s.t. that both $\alpha \neq 0$,$\beta \neq 0$ we get that $\forall i : b^i$ are constants and so $|B(s)\rangle$ does not depend on $|s\rangle$.

Now let's show how it implies it for any input s not only when both $\alpha \neq 0$,$\beta \neq 0$.

First, because any quantum state belongs to a Hilbert space there will not be a quantum state where both $\alpha = \beta = 0$ because any quantum space is normalized to equal 1.

So, we can have an $|s\rangle$ s.t. $0 \neq \beta$ or $0 \neq \alpha$.

In the case $\beta \neq 0$ we learn form equations 4,5 that

$$\forall i : b^i_{(s)} = b^i_{(1)}$$

However, we already learn from the operation of D on a s s.t. both $\alpha \neq 0$,$\beta \neq 0$ that $\forall i : b^i_{(1)}$ are constants independent of $|s\rangle$ which is enough to complete the proof for this case (because we proved that $\forall i : b^i_{(s)}$ are constants independent of $|s\rangle$).

At last, in the case $\alpha \neq 0$ we learn from equation 4,5 that

$$\forall i : b^i_{(s)} = b^i_{(0)}$$

Which is, again, enough to complete the proof in this case, i.e. to show that in this case $\forall i : b^i_{(s)}$ are constants independent of $|s\rangle$, because we learn from the operation of D on a s s.t. both $\alpha \neq 0$,$\beta \neq 0$ that $\forall i : b^i_{(0)}$ are constants independent of $|s\rangle$.

Furthermore, □

B Self-dual evolving AS's are very limited

We state that a quantum secret sharing with a self-dual adversary structure [14] is determined fully by the first authorized set in the structure. We say an evolving AS $\mathcal{A}$ is *self-dual*, if $\mathcal{A}_n = \mathcal{A} \cap [n]$ is self-dual for every $n \geq n_0$ for some integer $n_0 > 0$.

It turns out that self-dual evolving AS's are effectively finite. That is,

Theorem B.1. *Every evolving self-dual evolving access structure satisfies $\exists n$ s.t all parties in $\mathbb{N} \setminus [n]$ are* redundant.

Proof. Fix an evolving $\mathcal{A}$ with $\mathcal{A}_n$ self dual for all $n > n_0$. There are two cases. Let $n > n_0$ be the smallest integer such that $\mathcal{A}_n$ contains a minterm A (possibly more). If none exists, this implies that all minterms are contained in $[n_0]$, and we are done. We prove that all minterms are contained in $[n]$. Suppose for contradiction that $\mathcal{A}_{n+i}$ for $i > 0$ a new minterm is added - let us call it Q. This term must contain at least one participant from $[n]$. Otherwise, Q could be complemented into $[n+i] \setminus A$, obtaining a pair of sets contradicting self-duality of $\mathcal{A}_{n+i}$.

Now, $Q \cap [n]$ must not be authorized in $[n]$ because Q is a minterm of $\mathcal{A}$ and $i > 0$. However, because the Access structure $\mathcal{A}_n$ is self-dual and $Q \cap [n]$ is unauthorized we get that $B = (Q \cap [n])^c = [n] \setminus (Q \cap [n]) = [n] - Q$ is authorized in $\mathcal{A}_n$. Since $\mathcal{A}$ is monotone, B is also authorized in $\mathcal{A}_{n+i}$ which is self-dual, therefore we get that compliment set of it $B^c = [n+i] - ([n] - Q)$ is unauthorized. This contradicts the assumption that Q is an authorized minterm because $Q \subseteq [n+i] - ([n] - Q)$, which we just concluded to be unauthorised.

□

[14] Which means also a self-dual access structure.

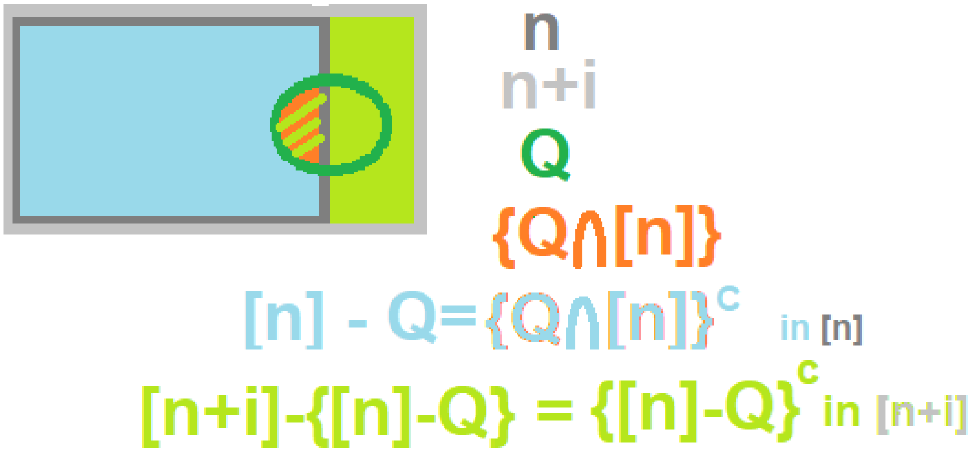

Figure 1: An illustration for the proof

References

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009.

[ABD$^+$24] Bar Alon, Amos Beimel, Tamar Ben David, Eran Omri, and Anat Paskin-Cherniavsky. New upper bounds for evolving secret sharing via infinite branching programs. Cryptology ePrint Archive, Paper 2024/419, 2024. https://eprint.iacr.org/2024/419.

[AN21] Benny Applebaum and Oded Nir. Upslices, downslices, and secret-sharing with complexity of 1.5^{n}. In *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part III*, pages 627–655, 2021.

[APC24] Tamar Ben David Anat Paskin-Cherniavsky, Varun Narayanan. New results in share conversion, with applications to evolving access structures. *submission to ITC 24, will be published also in eprint*, 2024.

[Bei11a] Amos Beimel. Secret-sharing schemes: A survey. pages 11–46, 05 2011.

[Bei11b] Amos Beimel. Secret-sharing schemes: A survey. In Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology*, pages 11–46, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[Bla79] George Rober Blakley. Safeguarding cryptographic keys. *1979 International Workshop on Managing Requirements Knowledge (MARK)*, pages 313–318, 1979.

[BO18] Amos Beimel and Hussien Othman. Evolving ramp secret-sharing schemes. In *SCN 2018*, volume 11035, pages 313–332, 2018.

[BO20] Amos Beimel and Hussien Othman. Evolving ramp secret sharing with a small gap. In *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part I*, pages 529–555, 2020.

[CGL99] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. How to share a quantum secret. *Physical Review Letters*, 83(3):648–651, jul 1999.

[ÇGLR23] Alper Çakan, Vipul Goyal, Chen-Da Liu-Zhang, and João Ribeiro. Computational quantum secret sharing. *CoRR*, abs/2305.00356, 2023.

[CGLZR23] Alper Cakan, Vipul Goyal, Chen-Da Liu-Zhang, and João Ribeiro. Computational quantum secret sharing. Cryptology ePrint Archive, Paper 2023/613, 2023. https://eprint.iacr.org/2023/613.

[Cha20] Shion Samadder Chaudhury. A quantum evolving secret sharing scheme. *International Journal of Theoretical Physics*, 59(3936–3950 (2020)), Nov 2020.

[DDD21] Paolo D'Arco, Roberto De Prisco, and Alfredo De Santis. Secret sharing schemes for infinite sets of participants: A new design technique. *Theor. Comput. Sci.*, 859:149–161, 2021.

[FV23] Danilo Francati and Daniele Venturi. Evolving secret sharing made short. Cryptology ePrint Archive, Paper 2023/1534, 2023. https://eprint.iacr.org/2023/1534.

[Got00] Daniel Gottesman. Theory of quantum secret sharing. *Physical Review A*, 61(4), mar 2000.

[HBB99] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. *Physical Review A*, 59(3):1829–1834, March 1999.

[HS16] Martin Hirt and Adam D. Smith, editors. *Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part II*, volume 9986 of *Lecture Notes in Computer Science*, 2016.

[ISN89] Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret sharing scheme realizing general access structure. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 72(9):56–64, 1989.

[KNY18] Ilan Komargodski, Moni Naor, and Eylon Yogev. How to share a secret, infinitely. *IEEE Trans. Inf. Theory*, 64(6):4179–4190, 2018.

[KP17] Ilan Komargodski and Anat Paskin-Cherniavsky. Evolving secret sharing: Dynamic thresholds and robustness. In *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part II*, pages 379–393, 2017.

[KPC17] Ilan Komargodski and Anat Paskin-Cherniavsky. Evolving secret sharing: Dynamic thresholds and robustness. In Yael Kalai and Leonid Reyzin, editors, *Theory of Cryptography*, pages 379–393, Cham, 2017. Springer International Publishing.

[KW93a] Mauricio Karchmer and Avi Wigderson. On span programs. In *Proceedings of the Eigth Annual Structure in Complexity Theory Conference, San Diego, CA, USA, May 18-21, 1993*, pages 102–111, 1993.

[KW93b] Mauricio Karchmer and Avi Wigderson. On span programs. *[1993] Proceedings of the Eigth Annual Structure in Complexity Theory Conference*, pages 102–111, 1993.

[LV18] Tianren Liu and Vinod Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 699–708, 2018.

[Maz23] Noam Mazor. A lower bound on the share size in evolving secret sharing. In *4th Conference on Information-Theoretic Cryptography, ITC 2023, June 6-8, 2023, Aarhus University, Aarhus, Denmark*, pages 2:1–2:9, 2023.

[OK20] Ryo Okamura and Hiroki Koga. New constructions of an evolving 2-threshold scheme based on binary or d-ary prefix codes. In *2020 International Symposium on Information Theory and Its Applications (ISITA)*, pages 432–436, 2020.

[Pet23] Naty Peter. Evolving conditional disclosure secrets. In *Information Security: 26th International Conference, ISC 2023, Groningen, The Netherlands, November 15–17, 2023, Proceedings*, page 327–347, Berlin, Heidelberg, 2023. Springer-Verlag.

[PSAM21] Kittiphop Phalakarn, Vorapong Suppakitpaisarn, Nuttapong Attrapadung, and Kanta Matsuura. Evolving homomorphic secret sharing for hierarchical access structures. In *Advances in Information and Computer Security: 16th International Workshop on Security, IWSEC 2021, Virtual Event, September 8–10, 2021, Proceedings*, page 77–96, Berlin, Heidelberg, 2021. Springer-Verlag.

[Sha79] Adi Shamir. How to share a secret. In *Communications of the ACM, 22*, pages 612–613, 1979.

[Smi00] Adam D. Smith. Quantum secret sharing for general access structures, 2000.

[XY24] Chaoping Xing and Chen Yuan. Evolving secret sharing schemes based on polynomial evaluations and algebraic geometry codes. *IEEE Transactions on Information Theory*, 70(5):3718–3728, 2024.

[YLH23] Wei Yan, Sian-Jheng Lin, and Yunghsiang S. Han. A new metric and the construction for evolving 2-threshold secret sharing schemes based on prefix coding of integers. *IEEE Transactions on Communications*, 71(5):2906–2915, 2023.