Quantum Evolving Secret Sharing - revisited

Efrat Cohen, Ariel University, and
Anat Paskin-Cherniavsky, Ariel University

Abstract. In evolving secret sharing, introduced by Komargodski et al., an infinite set of parties share a secret according to an infinite access structure (where minimal qualified sets are finite). In such schemes, parties arrive one by one, and and are given a share by the dealer. There is no additional communication incurred to a given party until the time of reconstruction, where share holders who show up combine their shares to reconstruct the secret if they form a qualified set.

In this work, we revisit the notion of quantum evolving secret sharing schemes, we dub QESS, where a quantum secret is shared. Smoothly generalizing the above setting runs into difficulties due to the no-cloning theorem. In particular, values handed to previously arriving parties can not be copied by the dealer and used in the evaluation of future parties' shares, as often done in evolving secret sharing schemes from the literature. Indeed, attempts to formalize quantum evolving secret sharing, such as that on Chaudhury for the so called dynamic threshold setting and by Cohen et al. for general evolving access structures fell short from adhering to the minimally interactive communication pattern above.

In this paper, we take a different approach, and consider a setting where several (possibly infinitely many) copies of a secret (known to the dealer) are generated by need. This approach has been used by Cakan et al. for (finite) quantum secret sharing (QSSS), allowing to circumvent the impossibility of devising QSSS for monotone access structures which are not *no-cloning* - those that have disjoint pair of qualified sets. This setting is plausible in many applications, where the secret is known to the dealer at sharing time. Cakan et al. demonstrate that at most n copies of the secret prepared by the dealer, suffice to implement any monotone access structure. In the evolving setting, it is not clear how to devise QESS even for evolving *no-cloning* access structures. Introducing multiple copies of the secret allows to define QESS with a communication pattern similar to the classical setting, in which, as a bonus, arbitrary (not necessarily no cloning) evolving access structures can be implemented.

We study the copy number landscape for various finite and evolving access structures. In the finite setting, we prove copy number MCN is in the range $\omega(G_{\text{disj}}) \leq MCN \leq \chi(G_{\text{disj}})$ for a certain graph G_{disj} related to f. For (t, n)-threshold this graph coincides with the Kneser graph, for which χ is known. While this resolves the copy number for $(t, 2t)$-threshold at 2, gaps remain for values $t < n/2$, with the smallest remaining open question on MCN is thus $(2, 5)$-threshold. For evolving access structures, $c(t) \leq t$ copies of the secret suffice to generate the shares of the first t parties - similarly to the finite setting. On the lower bound side, the (generalized) no-cloning theorem implies $c(t) \geq t$ holds for some evolving access structures. We prove that every *no-cloning* evolving access structure has a QESS with a finite copy number $c(t) \leq C$, where the constant C depends on the particular access structure. The main question we leave open is whether a single copy suffices for no-cloning evolving access structures, while 1 is the exact number of the finite setting.

Our techniques generalize the hybrid technique of Cakan et al. abstracting their implicit approach of treating the access structure as a union of no-cloning access structures impelemnting some $f' \geq f$, and implementing each via exiting quantum erasure codes (QECC), which do not provide privacy. Then, a copy of the secret, masked by a classical random key (via QOTP) is encoded by each of these codes. The classical keys are then classically shared via a carefully selected access structure

to provide privacy (and maintain correctness).

Keywords: Quantum Evolving Secret Sharing, Minterms Hypergraph, Vertex Cover, No-cloning Theorem, Hybrid QESS.

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 $\mathcal{A}$. It follows from the above definition that access structures 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 [KNY16] defined *evolving secret-sharing schemes* with an unbounded number of parties. In a nutshell, evolving access structures are defined as a sequence of access structures $\mathcal{A}_1, \mathcal{A}_2, \ldots$ (equivalently, characteristic functions $f_1 : \{0,1\}^1 \to \{0,1\}, f_2 : \{0,1\}^2 \to \{0,1\}, \ldots$), where the individual access structures $\mathcal{A}_t = \{A \subseteq [t] | f^t(A) = 1\}$ 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 each $A \subseteq [min(t, t')]$. We refer to this property as *consistency*. A quantum secret sharing scheme (QSSS) in the standard n-party setting, shares a secret which 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 intensively studied in the past [HBB99, KKI99, CGL99, Got00, Smi00].

In this work, we revisit the notion of quantum evolving secret sharing schemes, we dub QESS, where a quantum secret is shared. Smoothly generalizing the above setting runs into difficulties due to the no-cloning theorem. In particular, values handed to previously arriving parties can not be copied by the dealer and used in the evaluation of future parties' shares, as often done in evolving secret sharing schemes from the literature. Indeed, attempts to formalize quantum evolving secret sharing, such as that in [Cha20] for the so called dynamic threshold setting and by [CP24] for general evolving access structures fell short from adhering to the minimally interactive communication pattern above. The main question we explore in this work is the following:

Question 1. Does there exist a meaningful notion of QESS which can (at least) be instantiated for any so called *no-cloning* evolving access structure.

The restriction to no cloning schemes is a minimal to capture the set of access structures not ruled out by the no-cloning theorem, which is the case in the finite setting. The definition does not need to exclude access structures which are not *no-cloning*. Jumping ahead, our solution in fact supports all evolving access structures.

1.1 Prior Work

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] the author explored QSS for general access structures. It devised a compiler converting linear classical secret-sharing schemes to quantum ones, for any so called *no-cloning* access structure - one for which no two disjoint sets can reconstruct the secret. We refer to such access structures as *no-cloning*, while [Smi00] refers to them as $Q2^*$. He also proves 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 access structures for which QSS is possible is due to the non-cloning theorem [MAN00]. The share complexity, in terms of a number of p-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 [ÇGLR23], the authors initiate a study of computational QSS, and similarly to the classical setting, obtain polynomial-time schemes for a large class of so-called *heavy* access structures under standard (post-quantum) assumptions. Most relevantly to our work, they obtain improved perfect QSS for so called *heavy* access structures - those where all minterms are of size $t > n/2$. They inherit the complexity of the best known classical schemes for worst-case access structures - $1.5^{n+o(n)}$ [AN21]. [1] This holds as the best-known classical linear schemes have worse complexity for certain access structures $2^{0.64n+o(n)}$ [AN21], and it can be demonstrated that every access structure $\mathcal{A}_f$ has a related *heavy* access structure $\mathcal{A}_{f'}$ with essentially the same share complexity.

Multi-copy QESS To handle all *no-cloning* access structures, and even all monotone access structures, which is beyond what is provably possible for QESS, they consider an extended notion of QESS by introducing a copy number parameter, which allows the dealer to enter multiple copies of the secret $\rho^{\otimes m}$, rather than a single copy. This notion was first introduced in [Chi20], and is applicable (and does not contradict the no-cloning theorem) if ρ is a fixed secret known to the dealer. This is an acceptable relaxation in many applications. We denote the minimal copy number of a QSSS for f by $MCN(f)$. They show in [ÇGLR23] that any monotone access structure can be implemented using at most n copies of the secret. The share complexity of the resulting scheme is also upper bounded by the best known classical share complexity.

Evolving secret sharing schemes. Komargodski, Naor, and Yogev [KNY16] 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 for an

[1] In fact these results may be generalized to a broader still class of functions, see [ÇGLR23] for more details.

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.[2]

Komargodski et al. [KNY16] 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 t'th 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 access structures 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* access structures. 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. Informally, as in the finite setting, this means that every share consists of finitely many linear combinations of a secret s and finitely many random elements $r_1, r_2, r_3, \ldots$, all coming from a certain finite field $\mathbb{F}_p$.

Quantum evolving secret sharing. Most relevant to our work are prior attempts of answering Question 1.

In [Cha20] the author initiates the study of QESS and considers so called dynamic threshold access structures. These access structures are defined by a monotone increasing function $0 \leq k(t) \geq t+1$, where t introduces a set of size $k(t)$ contained in $[t]$ as a minterm if it does not contain a minterm introduced a smaller t'. Although his construction is of value, his definition of general QESS is only implicit in the paper. Furthermore, it apparently falls short from allowing a full fledged evolving communication pattern, where dealt shares are never returned back to the dealer for evaluating future shares (and are only deployed for reconstruction). Working backwards from their construction, it appears that prior shares are reused at computing the share of the current party. Another indication that full fledged evolving quantum secret sharing can not be devised for dynamic threshold $k(t) > n_t/2$ as claimed there is the fact that such an access structure is not *no-cloning*, when restricted to a certain t (and thus can not be implemented). For instance, for $k(t) = 2/3t$, sets $[31, 90], [3]$ are qualified for this access structure, but they do not intersect. This does not allow the shares given to parties in [90] to implement the induced access structure f_{90} with a single secret copy.

In [CP24] the authors make another attempt at defining QESS for general access structures. Yet, their construction does not adhere to the evolving communication pattern either, and allows parties to send shares back and forth to the dealer. They define a certain notion of "consistency" between the share held by P_t at a given time. This notion is conceptually problematic in terms of justifying its sufficiency for applications, and cleanly recreating the desirable properties of the setting where parties receive their share only once. Furthermore, there appears to be a problem regarding feasibility of this notion, as it appears in the paper.

[2] 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.

1.2 Our Results

Although the definition of [CP24] could be corrected in various ways to fix the feasibility issue (and has been in a later version), we believe their notion is not well-motivated, as it requires previous parties to communicate with the dealer when the current party arrives and receives its share. Thus, in this work, we propose a definition of QESS that preserves the useful communication pattern for all evolving access structures, by allowing the introduction of multiple copies of the secret as new parties join, as considered in [ÇGLR23] for the finite setting. [3] That is, each party's share may depend on some finite (0 or more) copies of the secret generated upon its arrival. The different copies of the secret are not entangled, and the sequence of copy numbers $a_1 \leq a_2, \ldots$, where a_i marks the number of copies generated by the time party i arrives may or may not have a maximum. Similarly to the finite QSSS setting, we prove that $c(t) = t$ copies introduced by the time P_t arrives suffices. We also show this is tight for certain access structures. It is an easy observation that evolving access structures have QESS only if they are *no-cloning* - that is. no pair of minterms of f is disjoint. This holds as otherwise the induced access structure f_t for some t would have a QSSS. In the other direction, for *no-cloning* evolving access structures (where no pair of minterms are disjoint), we leave open the question whether a single copy suffices, but prove the following

Theorem 1 (Main result, informal)**.** *Every* no-cloning *evolving access structure f has a QESS with a finite copy number, where the constant depends on the particular f.*

For general evolving access structures, we obtain the following feasibility result.

Theorem 2 ((Informal))**.** *Every evolving access structure has a QESS where at most $c(t) \leq t$ copies are introduced by the time party t arrives. If f is a union of finitely many no-cloning evolving access structures, the share complexity of the QESS guaranteed is $O(b(t))$, where $b(t)$ is the best known classical evolving secret sharing complexity for f. Furthermore, there exists an access structure where $c(t) \geq t$ holds for all $t \geq 1$.*

In a nutshell, we extend the construction [ÇGLR23] to the evolving setting, by abstracting and generalizing their construction already for the finite setting. Although the concrete upper bounds of [ÇGLR23] do not result in a copy number of 1 for all *no-cloning* access structures - see Section 3, our generalization does not guaranty it either. We leave open the following question

Question 2. Do there exist no-cloning finite access structures for which our construction does not yield a copy number of 1, yet a standard QSSS (aka multi-copy QSSS with copy number 1) exists?

We do not know how to answer this question for evolving access structures, but we prove that QESS within our framework is not sufficient to close the gap.

Claim (Informal)**.** *There exists an evolving* no-cloning *access structure, for which our framework does not yield a QESS with copy number 1.*

1.3 Our Techniques

Let us first describe the simplest approach along the lines of our framework. Jumping ahead, it will result in QESS for only a subclass of evolving access structures (even when allowing multiple copies of the secret).

[3] It could be the case that the work of [Cha20] implicitly tries to make use of multiple copies of the secret, but it is a bit hard to understand from their construction. Additionally, it appears they do not take care of not using prior shares (that should not be available to the dealer, as they had been handed to a previous party at this point).

First attempt. Consider a specification of f via a hypergraph of its minterms $G(V = \mathbb{N}^+, E)$. Recall that all edges $e \in E$ are finite by definition of evolving access structures. Now, consider G as a union of finite e*no-cloning* access structures $G_1, G_2, \ldots, G_i, \ldots$ - $E = \bigcup_i E_i$. That is, access structures where the number of non-redundant parties in them is finite – in the paper, we refer to these access structures as access structures with finite support. The number of G_i's in the union may be finite or infinite. The simplest idea is to apply the construction of [Smi00] (we thereby refer to as Smith) to every G_i, sharing a separate copy of the secret ρ that we generate once the first party in the support of G_i arrives, and share it among the parties in the support of G_i. Every instance of Smith uses disjoint inputs - and there is thus no entanglement between the different instances. This black box approach results in a valid QESS scheme if every party is contained in a finite number of G_i's (supports). Otherwise, that party receives an infinite share, which is not allowed by the definition (and neither is it feasible). Thus, the above approach provably does not work for all evolving access structures. For example, consider an access structure where the minterms form an infinite star, where minterms are of size, say, 2 centered at a specific vertex. This access structure is a valid (even *no-cloning*) evolving access structure, but no sequence of G_i's as required above exists (by a simple pigeon-hole argument).

Second attempt. To extend the above construction to all *evolving* access structures, rather than relying on any QSSS for each G_i in a black-box manner, as the above simple construction, we use the hybrid approach of [ÇGLR23].

On a high level, [ÇGLR23] proceed as follows to implement QSSS for *no-cloning* (finite) access structures.

Construction 1.1.

1. ***Input:*** *Let ρ denote (a single copy) of the secret. For simplicity, here and through the paper we assume wlog. that ρ is a qbit. $f : \{0,1\}^n \to \{0,1\}$ is an n-party monotone access structure.*
2. ***Key Sampling:*** *Sample a classical key $k = (k_1, k_2) \leftarrow \{0,1\}^2$.*
3. ***Masking:*** *Encrypt ρ using a Quantum One-Time Pad (QOTP) with key k:*

$$E_\rho = OTPEnc(\rho, k) = X^{k_1} Z^{k_2} \rho (X^\dagger)^{k_1} (Z^\dagger)^{k_2}$$

   where X and Z are the Pauli gates.
4. ***Classical Sharing:*** *Share the classical key k using a classical (finite) secret sharing scheme.*
5. ***Quantum Encoding:*** *Encode the encrypted qubit E_ρ via a QECC - a quantum erasure correcting code some access structure $f' \geq f$.*

On a high level, masking via OTP (which uses classical keys!) and sharing the OTP keys via classical evolving secret sharing allows to replace the task of designing a QSSS for f into a a QECC for some $f' \geq f$. That is, the role of the QECC is to ensure that the secret is reconstructed by every qualified set in f. There is no need to make sure that unqualified sets do not manage to recover the secret (as it is protected by k it does not know by privacy of the classical secret sharing scheme). Thus, in our blueprint in attempt 1, we may replace $G_1, G_2, \ldots$ where $E = \bigcup_i E_i$ with the union of finite no-cloning access structures $G'_1, G'_2, \ldots$, the union of which cover some (evolving) $f' \geq f$. In the sequel we refer to such a sequence as a *no-cloning* cover as $\mathbf{f}$. Now, having decoupled privacy and recovery of the secret, out-sourcing it to a classical secret sharing scheme, we have much more freedom at choosing the sequence G'_1, G'_2. Indeed, the simple sequence of

singletons, where $G'_i = \{\{P_i\}, \{P_i\}\}$ is a cover of any evolving access structure f, resulting in t instances of the secret generated by the time P_t arrives.

In particular, an infinite star is covered by a single vertex containing the center of it. This way, an instantiation that uses this cover has the optimal copy number of 1.

It is interesting to note that moving to $f' \geq f$ is essential in the evolving setting, while in the finite setting [ÇGLR23], its goal is mostly to optimize total share complexity (but not copy number, which can not be reduced this way).

Our Construction. The above approach almost works, except for a single subtle remaining issue. One we use the same classical keys (k_1, k_2) for implementing all instances of QOTP creates an entanglement between the E_{ρ_i} instances for different Smith instances, so the construction does not satisfy the $|secret\rangle \otimes \psi$ output by a qualified A required by the definition of QSSS, after tracing out the other parties' system. To handle this issue, we sample an independent pair $(k_{i,1}, k_{i,2})$ for every Smith instance corresponding to H'_i. To make sure that every party P_t takes part in at most a finite number of Π_i instances, we devise an assignment h from minterms to elements of the cover CGH', where every party's minterms are assigned to at most a finite number of different H'_i. The assignment h only assigns a minterm M to i for which M is qualified in H'_i (note that M does not have to belong to $support(H'_i)$). The keys $(k_{i,1}, k_{i,2})$ are shares via a classical (generally) evolving scheme Π_i defined by the minterm graph G_i with $h^{-1}(i)$ as its edge set. We construct such a mapping in Section 5. Crucially only parties which are not redundant in Π_i receive any shares in it. Also, when the cover of f' H'_i finitely many H'_i, which just share each key k_i under f, as there is no risk of a party having to participate in infinitely many ESSS instances. Otherwise, we need to further restrict the set of covers used to make sure this number is finite for every party.

We sketch privacy and correctness (focusing on the combinatorial aspects of the construction - see Section 5 to make sure the entanglement issues are properly resolved). Also, in a formal proof we should consider $(Share^t, Rec^t)$ for a particular t, which we here ignore for simplicity. **Correctness.** Let A denote a qualified set for f, and fix some t. Then some minterm $M_A \subseteq A$ is assigned to some H'_i in CGH' it is qualified in. As A is qualified in H'_i, by Smith, we recover E_{ρ_i} from this instance. Also, by choice of i, $h(M_A) = i$, thus M_A is qualified in G_i, it recovers $(k_{i,1}, k_{i,2})$ in Π_i, which are then used to decrypt the QOTP and recover ρ. **Privacy** For an unqualified set B, in every Smith instance for H'_i, the key $(k_{i,1}, k_{i,2})$ is not known to B, which is not qualified even for f, and thus for $f_i \leq f$. The QOTP thus keeps the secret in that instances completely secret.

Implications to the finite setting. We observe that the construction in [ÇGLR23] for t-heavy (finite) access structures implicitly applies our scheme for a particular no-cloning cover of f. We show that finding the optimal cover number is exactly equivalent to classical graph coloring on a disjointness graph of the minterms. This connection allows us to prove that their bound of $n - 2t + 2$ copies is strictly tight for symmetric threshold structures. Conversely, for other structures, our no-cloning cover approach reveals massive improvements; for instance, we demonstrate a non-symmetric example with $t = 2$ where their scheme blindly requires $n - 2$ copies, while our framework needs only $c = 2$ secret copies.

1.4 Future work

The main question we leave open is understanding the minimal copy number corresponding to evolving *no-cloning* access structures.

More generally, the optimal copy number of various access structures is a more general open question. It is clear that the size m of the largest set of pairwise-disjoint minterms

in f's minterm graph G_f poses a lower bound on the copy number, but it is not clear in which cases this bound is tight.

Going back to the *no-cloning* case ($m = 1$), let us explore the difficulties arising for one natural research direction: attempting to directly generalize Smith's single-copy framework to the evolving setting. A naive attempt runs into difficulties we next outline. On a high level, Smith's construction for no-cloning access structures operates in two steps. Step (1) designs a QECC for f. The QECC happens to be a QSSS (that is, satisfy privacy as well) if f is self-dual. That is, both f and its dual are *no-cloning*. (2) For access structures that are only no-cloning, it is shown how to extend it into a *self dual* access structure, by adjoining a new "dummy" party with a new party 0, and defining a new access structure which agrees with the original access structure when restricted to the set $[n]$ of parties. However, as we demonstrate in Section A, it is not clear how to make step (2) go through in the evolving setting. Specifically, if the natural attempt to form an evolving self-dual access structure by adding one or more parties succeeds (in the sense that every restriction of it to $[n] \cup \{0\}$ is self dual) it means the original access structure was essentially finite (that is, it depends on a finite number of parties). This is another reason we initially used [ÇGLR23]'s hybrid technique.

Even when just trying to extend Smith to yield QECC for f (or even $f' \geq f$), one major difficulty is that party set $[t]$, for all $t \in \mathbb{N}^+$ party P_t's share depend on $s, r_1, \ldots, r_{\ell_t}$ as well - the secret and random elements used by earlier parties and handed out to them, and these registers are no longer available. Consider a concrete example that may arise as part of a common linear evolving scheme from the (classical) literature [KNY16] implementing the (finite) access structure defined by the minterms $\{1,2\},\{2,3\}$. Assume the dealer holds registers $|s\rangle, |r_1\rangle, |r_2\rangle$ and needs to compute shares $|s, r_1, r_2\rangle \to |r_1, r_1 \oplus r_2, s \oplus r_2\rangle$ (as defined on base elements). The first share register is sent to P_1 as its share, and the last two are given to P_2. This can be done in one step using Smith's scheme, and produce the required shares. Next, the dealer wishes to send $|r_3 \oplus r_1\rangle$ and $|r_3 \oplus s\rangle$ to P_3. To do this, access to the share registers received by parties P_1, P_2 is required, which is impossible since there are no copies of s, r_1, r_2 that the dealer holds at this point. This is not a problem for the finite setting, as it can just compute all required shares for all three parties in one step as done in step (1) in the construction of Smith. However, when infinitely many more parties (and shares) are ahead, it is not clear whether one can give a finite set of values W_t at the end of sharing to a finite subset $[t]$ of parties (in our case $t = 2$) to the dealer, that will suffice for generating all future shares. This requirement is further complicated by the constraint that W_t together with the original shares of $[t]$ do not form new qualified sets such that the resulting "effective" access structure formed by the shares given to $[t] \cup \{0\}$ remains no-cloning (otherwise [Smi00] does not work due to the no-cloning theorem). We leave mapping out when this is possible as an interesting open problem.

On the lower bound side, the existence of a hybrid scheme, allowing to clone basis vectors, demonstrates that an impossibility result would need to rely on the no-cloning theorem in subtle ways, that in particular accounts for the ability to copy basis vectors.

In the finite setting We prove copy number MCN is in the range $\omega(G_{\text{disj}}) \leq MCN \leq \chi(G_{\text{disj}})$ for a certain graph G_{disj} related to f. For (t,n)-threshold this graph coincides with the Kneser graph, for which χ is known. While this resolves the copy number for $(t,2t)$-threshold at 2, gaps remain for values $t < n/2$, with the smallest remaining open question on MCN is thus $(2,5)$-threshold. It is also interesting to better understand these combinatorial measures for new classes of access structures, such as weighted threshold structures.

Roadmap. Section 3 deals with a simple version of our framework applicable to the finite setting, explaining our basic generalization of the [ÇGLR23] hybrid construction and

presents cases where copy number improves by using a different isntance of this abstraction. In section 4 we put forward our new, multi-copy based, notion of quantum evolving secret sharing. In Section 5 we present our main quantum evolving construction for general evolving access structures.

2 Preliminaries

In section 2, we include the needed background on classical secret sharing, evolving secret sharing and quantum secret sharing. Whenever we consider random classical bits, we implement them as part of the quantum circuit via measuring $H(|0\rangle)$ in the standard basis. We assume familiarity with standard quantum information and computation, and use the satandard bra-ket notation, and density matrices to represent general qdits. See [MAN00] for details. We recall the standard notions of classical secret sharing, and classical evolving secret sharing. Then we recall the standard notions of quantum secret sharing - QSSS. The definition is via quantum erasure codes - QECC (in the finite setting), as well as useful feasibility results in these settings. We also need the newer extension of QSSS (and QECC) to the multi-copy setting, where the dealer inputs m copies ρ^m (along with a sufficient number of $|0\rangle$ bits) of a fixed secret into the QSSS sharing circuit. Finally, we also recall the construction of quamtum OTP (QOTP), which surprisingly uses classical bits to encrypt q qbit.

2.1 Classical Secret Sharing

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

Definition 1. (Access Structures) Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a set of parties. A collection $\mathcal{A} \subseteq 2^{\{P_1,\ldots,P_n\}}$ is monotone if $q \in \mathcal{A}$ and $q \subseteq C$ imply $C \in \Gamma$. An access structure $\mathcal{A} \subseteq 2^{\{P_1,\ldots,P_n\}}$ is a monotone collection of non-empty sets. Sets in $\mathcal{A}$ are called authorized, and sets not in $\mathcal{A}$ 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 ($f(P) = 0$).

Definition 2. (minterm) An authorized set A in the access structure $\mathcal{A}$ is called a minterm, if it is minimal in the sense that removing any party from A results in an unauthorized set.

We say a party P_i is redundant in an access structure $\mathcal{A}$ if it does not belong to any minterm of $\mathcal{A}$.

Definition 3. (Secret-Sharing Schemes). A secret-sharing scheme $\Sigma = \langle \mu, \Pi \rangle$ over a set of parties $\mathcal{P} = \{P_1, \ldots, P_n\}$ with a domain of secrets S is a pair where μ is a probability distribution on a finite set R (the set of random strings) and Π is a mapping from $S \times R$ to a set of n-tuples $S_1 \times \cdots \times S_n$ (where S_j is the domain of shares of P_j).

A dealer distributes a secret $s \in S$ by sampling $r \in R$ according to μ, computing the vector of shares $\Pi(s, r) = (sh_1, \ldots, sh_n)$, and privately communicating each share sh_j to party P_j.

For a set $A \subseteq \mathcal{P}$, let $\Pi_A(s, r)$ denote the restriction of $\Pi(s, r)$ to the entries corresponding to parties in A. A secret-sharing scheme realizes an access structure $\mathcal{A}$ if:

Correctness. For any authorized set $A \in \mathcal{A}$, there exists a reconstruction function $\text{Recon}_A : \prod_{P_j \in A} S_j \to S$ such that for every secret $s \in S$ and every random string $r \in R$:

$$\text{Recon}_A(\Pi_A(s, r)) = s$$

Security. For any unauthorized set $T \notin \mathcal{A}$, every two secrets $s_1, s_2 \in S$, and every possible vector of shares $\mathbf{sh}_T$:

$$\Pr[\Pi_T(s_1, r) = \mathbf{sh}_T] = \Pr[\Pi_T(s_2, r) = \mathbf{sh}_T]$$

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

A secret-sharing schemes can be defined using the notion of a monotone span program (MSP). We bring the definition of MSP below.

Definition 4 (Monotone Span Program [KW93])**.** A *monotone span program* is a triple $\mathcal{M} = (\mathbb{F}, M, \rho)$, where $\mathbb{F}$ is a field, M is an $m \times k$ matrix over $\mathbb{F}$, and a mapping $\rho : [m] \to [n]$ labels each row of M by a party's index. The size of $\mathcal{M}$ is the number of rows of M (i.e., m).

2.2 Evolving Secret Sharing

Definition 5. (Evolving Access Structure) [HS16] Let $\mathcal{P} = \{P_1, P_2, \dots\}$ be an infinite set of parties. An evolving access structure is an infinite sequence of access structures $\mathcal{A} = \{\mathcal{A}_n\}_{n\in\mathbb{N}}$ such that there exists a global monotone access structure $\Gamma \subseteq 2^{\mathcal{P}}$ where for every $n \in \mathbb{N}$:

$$\mathcal{A}_n = \{B \subseteq \{P_1, \dots, P_n\} \mid B \in \Gamma\}$$

Equivalently, the sequence satisfies:

1. **Monotonicity:** For every $n \in \mathbb{N}$, $\mathcal{A}_n$ is a monotone access structure over n parties.
2. **Consistency:** For every $n \in \mathbb{N}$, it holds that $\mathcal{A}_n \cap 2^{[n-1]} = \mathcal{A}_{n-1}$.

We identify an access structure $\mathcal{A}_n$ with its characteristic function $f_n : \{0,1\}^n \to \{0,1\}$. For any $n' \geq n$, a set $B \subseteq [n]$ can be interpreted as an input to $f_{n'}$ by padding its characteristic vector with $n' - n$ zeros. We say an evolving access structure Γ is finite if it has a finite number of non-redundant parties.

Definition 6 (Characteristic Function of an Access Structure)**.** An access structure Γ over a participant set P can be uniquely represented by its characteristic function $f : \{0,1\}^* \to \{0,1\}$, which maps a coalition's indicator vector to a binary predicate:

$$f(A) = \begin{cases} 1 & \text{if } A \in \Gamma \text{ (Authorized)} \\ 0 & \text{if } A \notin \Gamma \text{ (Unauthorized)} \end{cases} \tag{1}$$

For an evolving access structure, this generalizes to a sequence of functions $\{f_t\}_{t\geq 1}$ where $f_t : \{0,1\}^t \to \{0,1\}$ satisfies consistency: $f_t(x_1, \dots, x_{t-1}, 0) = f_{t-1}(x_1, \dots, x_{t-1})$.

Definition 7. (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 $(\text{SHARE}, \text{RECON})$. The sharing procedure SHARE and the reconstruction procedure RECON satisfy the following requirements:

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

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

   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 tth 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.

Theorem 3. *[KNY16] For every evolving access structure $\mathcal{A}$, there exists an evolving secret sharing scheme for $(\mathcal{A})$. Moreover, for a 1-bit secret, the share of the (t)-th party has size at most (2^{t-1}) bits [[KNY16], Theorem 1.1].*

Definition 8 (Dynamic thresholds [KPC17]:)**.** A dynamic threshold access structure has a sequence $k_1 \leq k_2 \leq ...$ 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, along with 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 access structure specified by $k(t)$. Then wlog., one may assume $k_t \leq k_{t-1} + 1, k_1 \leq 2$.*

2.3 Quantum Secret Sharing (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.[4] 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 (classical distributions over) quantum states $|s\rangle$ and their density matrices ρ interchangeably (adapting the operators accordingly).

See [MAN00] for a comprehensive reference on quantum information and computation.

We adapt the definition of the Quantum secret sharing from [ÇGLR23] which is based on Quantum erasure-correcting codes(QECC) [GBP97]. Such codes allow 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 9. (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 $\mathcal{H}_{inp}$ of dimension k qdits and output space $\mathcal{H}_{out} = \otimes_{i\in[n]}\mathcal{H}_i$ of n qdits 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

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

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

for some state σ, where the input ρ is implicitly padded via $|0\rangle^{\ell}$ to complement to n qdits as well as various ancilla bits. 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.

For a code over $\otimes_{i\in[n]}\mathcal{H}_i$, where each Hilbert space $\mathcal{H}_i$ is assigned to a party p_i, we denote by $tr_{\bar{P}}$ tracing out the subsystem corresponding to the party set $\bar{P}$.

The following QECC construction is implicit in [Smi00]'s paper.

Theorem 4 (Imported [Smi00])**.** *Let f be a no-cloning access structure with a classical MSP (monotone span program) of size d over $\mathbb{F}_2$ for qbit secrets. Then, there exists a QECC for f output input Hilbert space of d qbits.*

In the sequel, we refer to the above QECC construction as "Smith".

Multiple-copy QECC. Unlike classical erasure correcting codes where an encoder can freely replicate the input bits to introduce redundancy across different components, the quantum setting is fundamentally constrained by the *no-cloning theorem*. Specifically, a standard Quantum Erasure Correcting Code (QECC) cannot natively generate or operate on multiple independent copies of an arbitrary input state during the encoding process. Consequently, if a code requires the utilization of multiple copies of the target state to achieve better parameters or satisfy specific locality constraints, these copies must be explicitly provided as part of the initial quantum input. This physical limitation motivates the following formal generalization of the code's definition.

As in [ÇGLR23], we extend Definition 9 to use an m-copy quantum erasure correcting code (m-copy QECC), where the encoder is permitted to use m identical copies of the input state, while preserving k as the logical dimension of the code. It is known that the standard notion of QECC (with a single copy of the secret) .

Formally, an m-copy QECC over the input space $\mathcal{H}_{inp}$ and output space $\mathcal{H}_{out} = \bigotimes_{i\in[n]}\mathcal{H}_i$ is defined by a pair of trace-preserving quantum operations $QC = (QC.Enc, QC.Dec)$, where the encoder maps from the m-fold tensor product of the input space:

$$QC.Enc : \mathcal{H}_{inp}^{\otimes m} \to \mathcal{H}_{out} \tag{2}$$

[5] The pair QC is an m-copy QECC for a party set $P \subseteq [n]$ 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:

$$(QC.Dec \circ \Lambda \circ QC.Enc)(\rho^{\otimes m}) = \rho \otimes \sigma \tag{3}$$

for some state σ and a suitable workspace ℓ. In particular, the code (and induced QSS) precisely defines the locations of all copies of $\rho \in \mathcal{H}^m$, making them explicit among the input wires of $Q.Enc$ in the QECC (QESS). That is, when writing that $QC.ENC(\mathcal{H}_{inp}^m)$ maps to a space $\mathcal{H}_{out}$, we mean that it the input to $QC.ENC$ is from Hilbert space $\mathcal{H}_{inp,1} \otimes \mathcal{H}_{inp,2} \otimes \ldots \otimes \mathcal{H}_{inp,t}$ where exactly m of the $\mathcal{H}_{inp,i}$'s are $\mathcal{H}_{inp}$ and $2m-1 \le t \le 2m+1$. Although adding this generalization adds no expressive power in the finite setting, looking forward, it will be useful for cleanly defining the evolving setting based on it.

Definition 10. (No-cloning monotone function) 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 $f(\overline{P}) = 0$.

[5] As before, the input is padded by $|0\rangle^{\ell}$ as needed.

Remark 1. Alternatively, in terms of the access structure, a function with access structure $\mathcal{A}$ is no-cloning if and only if for any two minterms $P, Q \in \mathcal{A}$, it holds that $P \cap Q \neq \emptyset$.

Later (section 4), when we talk about no-cloning evolving access structure, the natural way to define it is to ensure, at any point, that no two minterms are disjoint.

Definition 11. (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 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 $\log_{dim(\mathcal{H}_0)}(dim(\mathcal{H}_i))$.[6]

Multiple-copy QSS. As for QECC, we extend Definition 11 to the m-copy setting. The generalization is straight-forward, as QSS is QECC with an added privacy requirement.

Remark 2. It is known that both QECC and QSS with a single copy allow to only implement no-cloning monotone functions / access structures. Thus, QECC and QSS was originally defined for no-cloning functions. One way to implement more general types of monotone functions, is applying the code to several copies of the secret, thus for this general setting, the no-cloning requirement is not necessary.

Furthermore, exploring the question of implementing QSS in the multi-copy setting, [ÇGLR23] study the minimal number of copies required to implenet a certain access structure f, which is not necessarily no-cloning. They define the notion of *t-heavy* functions, where a function f satisfies it if all minterms are of size at least t.

Theorem 5 ((Imported))**.** *Every t-heavy function has a QECC, $n - 2t + 2$ copies of the secret suffice for a QECC for f. In particular, n copies suffice for every monotone function (as all functions are 1-heavy).*

Using their Hybrid approach, they obtain a QSS for t-heavy functions.

Theorem 6 ((Imported))**.** *Every t-heavy access structure $f : \{0,1\}^n \to \{0,1\}$ has a QSS, using $n - 2t + 2$ copies of the secret. Total share size is (also) $n - 2t + 2$ qbits, as well as at most $2b(n) \cdot n$ classical bits, where $b(n)$ is the best known share complexity for sharing 1-bit secrets for f.*

Jumping ahead, in this paper we generalize this upper bound, improving copy numbers for certain functions even for the finite setting.

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

2.4 Quantum One-Time Pad (QOTP)

We recall the Quantum One-Time Pad (QOTP) encryption scheme [AMTdW00], which provides perfect secrecy for quantum states using a random classical key. While the construction is presented for qubits, it generalizes naturally to higher-dimensional systems (qudits).

The QOTP scheme is defined by a pair of quantum circuits $(\mathrm{OTPEnc}, \mathrm{OTPDec})$. For an n-qubit message state $\rho \in (\mathbb{C}^2)^{\otimes n}$ and a classical key $k \in \{0,1\}^{2n}$, the encryption and decryption operations are defined as follows:

$$\mathrm{OTPEnc}(\rho, k) = \left(X_1^{k_1} Z_1^{k_2} \otimes \cdots \otimes X_n^{k_{2n-1}} Z_n^{k_{2n}}\right) \rho \left(Z_n^{k_{2n}} X_n^{k_{2n-1}} \otimes \cdots \otimes Z_1^{k_2} X_1^{k_1}\right),$$
$$\mathrm{OTPDec}(\rho, k) = \left(Z_n^{k_{2n}} X_n^{k_{2n-1}} \otimes \cdots \otimes Z_1^{k_2} X_1^{k_1}\right) \rho \left(X_1^{k_1} Z_1^{k_2} \otimes \cdots \otimes X_n^{k_{2n-1}} Z_n^{k_{2n}}\right),$$

where X_i and Z_i denote the standard Pauli gates applied to the i-th qubit.

Lemma 1 ([AMTdW00])**.** *The quantum one-time pad encryption scheme is correct and perfectly secure for a uniformly chosen random key. Specifically:*

1. ***Correctness:*** *For any key $k \in \{0,1\}^{2n}$ and any state ρ, $OTPDec(OTPEnc(\rho, k), k) = \rho$.*
2. ***Perfect Secrecy:*** *For any two quantum states $\rho, \sigma \in (\mathbb{C}^2)^{\otimes n}$, the encrypted states are indistinguishable when averaged over all possible keys:*

$$\frac{1}{2^{2n}} \sum_{k \in \{0,1\}^{2n}} OTPEnc(\rho, k) = \frac{1}{2^{2n}} \sum_{k \in \{0,1\}^{2n}} OTPEnc(\sigma, k) = \frac{I}{2^n}.$$

3 Hybrid-Style Quantum Secret Sharing

We first recall the seminal hybrid approach of [ÇGLR23], as applied to finite *no-cloning* access structures. This results in a 1-copy QESS.

Construction 3.1 (The $G + 23$ Compiler (single-copy))**.** *Let $f : \{0,1\}^n \to \{0,1\}$ be a no-cloning monotone function. Let $\mathcal{SS} = (\mathcal{SS}.Share, (\mathcal{SS}.Rec_P)_{P \subseteq [n]})$ be a classical secret sharing scheme realizing f, and let $\mathcal{QC} = (\mathcal{QC}.Enc, \mathcal{QC}.Rec)$ be a Quantum Erasure-Correcting Code (QECC) with n components realizing a monotone no-cloning function f' such that $f'(x) \geq f(x)$ for all $x \in \{0,1\}^n$.*

The compiler constructs a hybrid quantum secret sharing scheme as follows:

1. ***Input:*** *An arbitrary qubit ρ.*
2. ***Key Sampling:*** *Sample a classical key $k = (k_1, k_2) \leftarrow \{0,1\}^2$.*
3. ***Quantum Encryption:*** *Encrypt ρ using a Quantum One-Time Pad (QOTP) with key k, yielding the perfectly encrypted qubit:*

$$E_\rho = OTPEnc(\rho, k) = X^{k_1} Z^{k_2} \rho (X^\dagger)^{k_1} (Z^\dagger)^{k_2}$$

   where X and Z are the Pauli gates.

4. ***Classical Sharing:*** *Share the classical key k using $\mathcal{SS}.Share$, yielding n classical shares $(S_1, \ldots, S_n)$.*
5. ***Quantum Encoding:*** *Encode the encrypted qubit E_ρ using $\mathcal{QC}.Enc$, yielding entangled quantum systems $(E_1, \ldots, E_n)$.*
6. ***Output Shares:*** *For each $i \in [n]$, set the pair (S_i, E_i) as the final share of the i-th party.*

In the sequel we refer to this construction as the G+23 compiler.

3.1 Multiple copy QSS

In [ÇGLR23], they formally define quantum secret sharing with multiple copies, analogously to the definitions in Section 2.3, with a minor change: it is required that the share function $QSS.Share$ takes as input $|\psi\rangle^{\otimes k}$ where $|\psi\rangle$ is the secret and k is the number of copies we have access to, and manage to devise QSS for any monotone function f, using at most n copies of the secret 5. Roughly, they proceed by a recursive construction, making a call to the (single-copy) G+23 compiler at every step.

In this work, we abstract their construction as using a so called no-cloning cover of f. The abstraction leads to a smaller copy number, which is arguably the most important complexity parameter in many applications. This is a contribution to QSSS already in the finite setting.

The following is an abstraction of the G+23 framework to the multi-copy setting [ÇGLR23].

Construction 3.2 (MC (multi-copy) Compiler)**.** *Let $f : \{0,1\}^n \to \{0,1\}$ be a monotone function. Let $\mathcal{SS} = (\mathcal{SS}.Share, (\mathcal{SS}.Rec_P)_{P\subseteq[n]})$ be a classical secret sharing scheme realizing f, and let $\mathcal{QC} = (\mathcal{QC}.Enc, \mathcal{QC}.Rec)$ be a Quantum Erasure-Correcting Code (QECC) with n components realizing a monotone function f' such that $f'(x) \geq f(x)$ for all $x \in \{0,1\}^n$.*

The compiler constructs a hybrid quantum secret sharing scheme as follows:

1. ***Input:*** *A tensor of $m \geq 1$ copies of a qubit $\rho^{\otimes m} = \rho_1 \otimes \ldots \otimes \rho_m$.*
2. *For each copy ρ_i:*
   (a) ***Key Sampling:*** *Sample a classical key $k_i = (k_{i,1}, k_{i,2}) \leftarrow \{0,1\}^2$.*
   (b) ***Quantum Encryption:*** *Encrypt each ρ_j using a Quantum One-Time Pad (QOTP) with key k:*
   $$E_{\rho_j} = OTPEnc(\rho, k) = X^{k_1} Z^{k_2} \rho_j (X^\dagger)^{k_1} (Z^\dagger)^{k_2}$$
   where X and Z are the Pauli gates.
   (c) ***Classical Sharing:*** *Share the classical key k_i using $\mathcal{SS}.Share$, yielding n classical shares $(S_{1,i}, \ldots, S_{n,i})$.*
3. ***Quantum Encoding:*** *Encode the encrypted qubits $E_{\rho_1} \otimes \ldots \otimes E_{\rho_m}$ using $\mathcal{QC}.Enc$, yielding entangled quantum systems $(E_1, \ldots, E_n)$.*
4. ***Output Shares:*** *For each $j \in [n]$, set the pair (S_j, E_j) as the final share of the j-th party.*

We instantiate item 3 with a QCC based on so called no-cloning covers of f, we describe next.

3.2 Upper bounding copy number via no-cloning covers of MH

Definition 12 (Minimum Copies Number (MCN))**.** Given an access structure Γ, the *Minimum Copies Number*, denoted as $MCN(\Gamma)$, is the minimum number of copies of the quantum secret state required to implement a corresponding Quantum Secret Sharing (QSS) scheme with perfect privacy. We ommit the Γ when clear from the context.

For example, as shown by Smith [Smi00], for any No-cloning access structure (s.t. no two authorized sets are disjoint) as defined in section 2.3, a single copy of the secret is sufficient, meaning $MCN(\Gamma) = 1$.

Definition 13 (Mintrems Hypergraph (MH))**.** Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be a set of parties, and $\Gamma \subseteq 2^{\mathcal{P}}$ be an access structure. We define the associated **access structure hypergraph** $MH(V, E)$ as follows:

1. The set of vertices V corresponds to the set of parties $\mathcal{P}$.
2. The set of hyperedges E is the collection of all **minterms** of Γ, denoted as Γ_{min}. That is, $E = \{A \in \Gamma \mid \forall B \subsetneq A, B \notin \Gamma\}$.

In this work, we often use the access structure Γ and its associated minterms hypergraph (MH) interchangeably. Notably, in the case of a no-cloning access structure, in the associated MH any two hyperedges intersect.

A notable example of a no-cloning access structure is the case where all minterms share a common party. This occurs, for example, when transforming a general access structure into a no-cloning structure by adding a single party to all original minterms. In this scenario, the associated hypergraph exhibits a non-empty global intersection $\bigcap_{e \in E} e \neq \emptyset$.

3.2.1 The general cover perspective

Definition 14. (no-cloning cover) Let f', f be functions that represent access structures on n parties, minterm hypergraphs HG, HG' respectively. Let CHG' be a union of m sub-hypergraphs $\{H'_i\}_{i=1}^m$ such that each of H'_i is a no-cloning access structure on the n parties (with some of the parties possibly being redundant). i.e.

$$HG' = H'_1 \cup H'_2 \ldots \cup H'_n.$$

If $f' \geq f$ ($HG' \geq HG$) we say that $CHG' = \{H'_1, \ldots, H'_m\}$ is a no-cloning cover of f (HG). We refer to the number of H'_i's in a smallest such CHG' as the no-cloning number of HG $NCCN(HG)$ (or of f). We refer to the set of non-redundant parties in H'_i as the support set of H'_i. We say that party j is contained in H'_i if it is contained in its support set. We refer to the number of H'_i's a party P_j belongs to in CHG' as the weight of P_j in CHG', note as $W_{CHG'}(i)$.

We instantiate Construction 3.2 via a no-cloning cover-based scheme. Namely

Construction 3.3 (Cover-based instantiation)**.**

- ***Input*** *Secret copies* $\rho^{\otimes m} = \rho_1 \otimes \ldots \otimes \rho_m$.
- *Instantiate Construction 3.2 so that*
  - *The keys* $(k_{i,1}, k_{i,2})$ *are shared according to a standard best known secret sharing scheme* Π *for* f *for 1-bit secrets (applied twice).*
  - *In item 5 we devise a no-cloning cover* $CHG' = \{H'_1, \ldots, H'_m\}$ *of* f*, and obtain our QCC by applying Smith's construction for finite non-cloning access structures with input secret* E_{ρ_j} *independently to each element* $H'_i \in CHG'$ *in the cover.*

Theorem 7. *Let* $f : \{0,1\}^n \to \{0,1\}$ *be a monotone function. Let* HG *denote a minterm graph for* f*, with* $m = NCCN(G)$ *with* $CHG' = \{H'_1, \ldots, H'_m\}$ *(of* $f' \geq f$*) a no-cloning cover of* f*. Then there exists a QSS for* f *with* m *copies of the secret.*

Proof. We prove that Construction 3.3 is indeed a valid QSS with the stated complexity parameters. The proof follows as a special case for our proof of the extended theorem in the evolving setting. In a nutshell, it relies on the privacy of the classical schemes for privacy, and the correctness of Smith for correctness. To prove recovered output of Rec^t has the proper structure $\phi \times \psi$, we rely on the distinct instances of Smith for the different H'_i's depending on mutually unentangled and disjoint input registers, except for the classical (k_1, k_2) bits reused by the different Smith instances, which do not create entanglement.

Complexity. The cover number is obvious from the construction, as we use a single copy per element in CHG'. □

3.3 A Disjointness-Graph based upper and lower bounds

The chromatic number of the Disjointness-Graph equals $NCCN(f)$ Theorem 7 establishes that the quantum copy complexity of the best (copy-number wise) construction in our hybrid framework is determined exactly by the minimal no-cloning cover number, $NCCN(f)$. To better understand this parameter, we prove it to be equal to the chromatic number of a certain graph related to f. This simplified from considering hypergraphs to graphs, as well as eliminate the dependence on f'. Furthermore, this connects copy number here to the chromatic number of a graph, which is a well studied parameter for various graph families.[7]

Let $f : \{0,1\}^n \to \{0,1\}$ be a finite monotone access structure, and let $HG(V, E)$ be its associated minterms hypergraph, where $E = \Gamma_{\min}$. We define the *disjointness graph* of f, denoted by $G_{\text{disj}} = (V_{\text{disj}}, E_{\text{disj}})$, as follows:

- The vertices correspond to the minimal qualified sets of f, i.e., $V_{\text{disj}} = \Gamma_{\min}$.
- A pair of vertices (M_1, M_2) forms an edge in E_{disj} if and only if the corresponding minterms are disjoint, i.e., $M_1 \cap M_2 = \emptyset$.

Theorem 8. *For any finite monotone access structure f, the minimal no-cloning cover number is exactly equal to the chromatic number of its disjointness graph, namely:*

$$NCCN(f) = \chi(G_{disj}) \tag{4}$$

Proof. We prove the theorem by establishing "$\leq$" in both directions:

1. **Upper Bound ($NCCN(f) \leq \chi(G_{\text{disj}})$):** Let $k = \chi(G_{\text{disj}})$ and consider a valid k-vertex coloring of G_{disj}. This coloring partitions the set of minterms $\Gamma_{\min}$ into k independent color classes, $C_1, C_2, \ldots, C_k$. By the definition of G_{disj}, no two vertices within the same color class share an edge, which implies that every pair of minterms assigned to the same class must intersect. Consequently, each color class C_i induces a valid no-cloning sub-hypergraph H'_i. The union of these sub-hypergraphs satisfies $\bigcup_{i=1}^{k} H'_i = HG$, thereby forming a valid no-cloning cover of size k. Thus, $NCCN(f) \leq \chi(G_{\text{disj}})$.

2. **Lower Bound ($\chi(G_{\text{disj}}) \leq NCCN(f)$):** Let $\mathcal{C} = \{H'_1, H'_2, \ldots, H'_m\}$ be a minimal no-cloning cover of f of size $m = NCCN(f)$. We define a vertex coloring (labeling) $\phi : \Gamma_{\min} \to [m]$ on G_{disj} by mapping each minterm $M \in \Gamma_{\min}$ to an index $i \in [m]$ such that M is qualified in the sub-hypergraph H'_i. If two distinct minterms M_1, M_2 receive the same color i, they must both be qualified in the same no-cloning access structure H'_i. By Definition A.12, any two qualified sets in a no-cloning structure must intersect, meaning $M_1 \cap M_2 \neq \emptyset$. Thus, $(M_1, M_2) \notin E_{\text{disj}}$, confirming that ϕ is a valid graph coloring. Therefore, $\chi(G_{\text{disj}}) \leq m = NCCN(f)$.

The two inequalities imply $NCCN(f) = \chi(G_{\text{disj}})$. □

Lower bound on MCN via a different measure of G_{disj} It turns out that the size of a maximal Clique in G_{disj} provides a lower bound on the copy number of f.

To summarize the lower and upper bounds of our framework, we obtain.

[7] We thank the anonymous Indocrypt referee of a previous version of this paper for pointing out this equivalence.

Theorem 9. *Let f denote an access structure, and let G_{disj} denote its disjointness graph. Then*

$$\omega(G_{disj}) \leq CN(f) \leq \chi(G_{disj})$$

The upper bound part is implied by instantiating Theorem 7 with a no-cloning cover of f of size $\chi(G_{\text{disj}})$. For the lower bound, we use a generalized variant of the no-cloning theorem, stating that no trace-preserving quantum operator transforms any $\rho^{\otimes m} \otimes |0\rangle^{\ell}$ into some $\rho^{\otimes n} \otimes |g\rangle$ and $n > m$. This claim can be proved by an extension of the standard no-cloning theorem (see [MAN00], Box 12.1) for unitary $Share^t$ operators, and general trace-preserving operators $Share^t$ in [DP09]. Consider a set of minterms $(M_1, \ldots, M_a)$ corresponding to a clique in G_{disj}, and assume for contradiction that we have a QSSS $\Pi(Share, Rec)$ for it with copy number $< \omega(G_{\text{disj}})$. Now, apply Rec to each set M_i of parties in parallel. Since Rec_{M_i} acts as the identity transformation on the other shares, and by correctness of Π, applying them all in parallel results in correct individual reconstructions, and outputs $\rho^{\otimes n} \otimes |g\rangle$ for some state ψ, contradicting the generalized no-cloning theorem.

3.4 Implications: Optimality and Structural Limits

Next, we cast some of the prior work as part of our graph-theoretic framework, and analyze share to copy number trade-offs that it provides for various access structures.

Optimality of [ÇGLR23] for Threshold Schemes. For a standard (t, n)-threshold access structure where all minimal qualified sets are of size exactly t, the defined disjointness graph G_{disj} is precisely isomorphic to the celebrated *Kneser graph* $KG(n, t)$. In a landmark result, Lovász [Lov78] determined that the chromatic number of Kneser graphs is exactly:

$$\chi(KG(n, t)) = n - 2t + 2 \tag{5}$$

By Theorem 8, this directly implies that $MCN(f) \leq NCCN(f) = n-2t+2$. In [ÇGLR23], the authors implicitly construct a hybrid scheme for general $t - heavy$ functions using a combination of $n - 2t + 1$ singletons and a majority access structure, achieving exactly $\max(n - 2t + 2, 1)$ copies (Theorem 3.7). Our graph coloring equivalence strictly proves that their bound is optimal within the no-cloning cover framework. The lower bound on MCN in Theorem 9 implies $\lfloor n/t \rfloor \leq CN$. These bounds establish that the copy number is precisely 2 for $(n/2, n)$-threshold, but leaves a gap for smaller values, including an exponential gap for $t = n/log(n)$, for instance.

The smallest interesting case for which there is a gap is $(2, 5)$-threshold, in which the gap is $2 \leq MCN(f) \leq 3$. Notably, here G_{disj} corresponds to the Petersen graph.

Vertex Covers as a Special Case of Graph Coloring. We observe that a minimal Vertex Cover (VC) of the minterms hypergraph HG provides a natural upper bound on the no-cloning cover number. Indeed, a vertex cover ensures that at least one participant from every minterm is included. In the language of our disjointness graph G_{disj}, a vertex cover corresponds to a specific type of coloring where the minterms are partitioned into color classes centered around individual vertices (singletons).

Let $VCN(f)$ denote the size of the smallest vertex cover of f. It follows immediately that $NCCN(f) \leq VCN(f)$. Implementing a QECC for $f' \geq f$ in [ÇGLR23] was done with the purpose of minimizing share complexity in the single-copy setting for some f. As a notable example, replacing a t-heavy access structure which may have an inefficient MSP with (t, n)-threshold for $t > n/2$, with a small MSP - leading to smaller quantum share complexity "for free". In our generalized multi-copy framework, Construction 3.3, a tradeoff between copy number and quantum share complexity appears. For example, using

f' with singleton-minterms (inducing a VC-type no-cloning cover of f), the $\leq$ singletons in get 1-qbit shares given to a single party each, while other covers may have fewer graphs, but some of them may have much higher complexities.

One example where VC-based no-cloning covers improve over [ÇGLR23]'s extension to the multi-copy setting, which implicitly uses a specific type of cover for (t, n) threshold, where f is t-heavy, is the following "Two-Flowers" example.

Example 1 (The Two-Flowers MH)**.** Consider an access structure where the minterms are partitioned into two "flowers," F_1 and F_2. In each flower F_i, there is a common center party p_i contained in all its minterms, which form distinct "petals" $F_{i,j}$ of size 2 each. This access structure is $t = 2$-heavy.

For this structure, the threshold-based construction of [ÇGLR23] requires $n - 2t + 2 = n - 2$ copies of the secret, as for (t, n)-threshold. However, the disjointness graph G_{disj} has a vertex cover (and thus a chromatic number) of exactly $\chi(G_{\text{disj}}) = 2$, centered around the two hub vertices $\{p_1, p_2\}$. This is an exponentially smaller number, by a deliberate choice of the no-cloning cover. In fact, we note that for this access structure, picking $(t, 2t - 1)$-thr as part of the cover does not help overall share complexity either.

4 Quantum Evolving Secret Sharing (QESS)

We would like to mirror the setting of evolving secret sharing for classical secrets as closely as possible for quantum secrets, so it is as suitable as possible for all applications where evolving secret sharing is used. Let us briefly recall the setting of evolving secret sharing, and examine the potential difficulties of constructing it in the quantum setting.

Motivation of our QESS notion. In the classical evolving setting, an infinite, finitary access structure is specified. Namely, the access structure is specified by a set of minterms $\{x \in \{0,1\}^* | f(x) = 1\}$, where each x is a characteristic vector of a (finite) subset of $\mathbb{N}^+$. The parties arrive one by one, and the dealer gives the share $Sh_i(s, r_1, \ldots, r_i)$ upon its arrival, where each r_i is sampled from a finite randomness domain R_i at time i in an i.i.d manner (and previously sampled randomness elements). When party P_i arrives to receive its share, the dealer samples r_i, and uses it along with previously sampled r_j's for $j < i$ to compute Sh_i. It then sends Sh_i to party i. Upon deciding to recover the secret, the parties come together and recover it.

To replicate this in the quantum setting, where the secret $|s\rangle$ is a qdit we should be more careful. In particular, the dealer can not naively send shares depending on $r_1, \ldots, r_t$ as well as the secret s, due to the no-cloning theorem. Our solution to this problem is to hand the dealer certain values it gets to keep after a party receives its share, to be used in the future, which are not a part of the current (or previous) shares.

There is no such issue in the finite setting, as the dealer can perform the entire quantum operation generating the shares of different parties all at once, assuming it is a unitary transformation. Indeed in [Smi00], it is demonstrated how to implement any no cloning access structure by implementing a quantum operator mapping $|s\rangle$ and a sequence of random inputs (implemented by a Hadamard gate applied to $|0\rangle$), and ancilla bits $|0\rangle$ to the output shares. The operator is based on a classical MSP sharing, properly extended into an invertible matrix (over $\mathbb{F}_2$).[8].

Trying to smoothly extend this construction to no-cloning evolving secret sharing runs into various issues, and we leave it as an open problem. See Section 1.4 for a concrete demonstration of this problem.

[8]The no-cloning property is required for reconstruction to work, rather than for the MPS-based encoding to be well defined.

A formal definition of QESS. We next formally define quantum evolving secret sharing to facilitate a communication pattern as in the finite setting. As discussed above, using copies of the secret is inherent even for no cloning evolving access structures (unlike finite evolving access structures, where it is not necessary). The particular number and location of copies is built into the definition. We assume that all Hilbert spaces $\mathcal{H}_*$ involved in the definition are of the form $\mathcal{B}^{\otimes m}$, where $\mathcal{B} = span(\{|0\rangle, |1\rangle\})$ is the space of qbits. We also assume that $\mathcal{H}_{inp} = \mathcal{B}$.[9] To be compatible with the evolving setting, it will be convenient to view $Share^t$ as quantum circuits with a certain structure and labels of input and output wires.

Definition 15. (Evolving Quantum secret sharing(QESS)) Let $\{f^t\}_{t>0}$ be an Evolving Access Structure with no redundant parties (not necessarily no-cloning). Let

$$\mathcal{H}_{inp}, \mathcal{H}_1, \mathcal{H}_{1,0}, \mathcal{H}_2, \mathcal{H}_{2,0} \dots$$

denote a sequence of finite, non-empty Hilbert spaces, where $\mathcal{H}_{inp}$ is a Hilbert space for the secret and $\mathcal{H}_i$ is a Hilbert space for the share of party i. Let $\mathcal{H}'_1, \mathcal{H}'_2, \dots$ where $\mathcal{H}'_t = \mathcal{H}'_{t-1} \otimes \mathcal{H}'^+_t$, where $\mathcal{H}'^+_t$ may be empty, which is of the same dimension as $\mathcal{H}_{t,0} \otimes \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_t$. $a_1, a_2, \dots$ is a sequence numbers, where $a_i \geq 0$ specifies the number of copies of the secrets expected to be received as part of $\mathcal{H}'^+_t$. Wlog., we let $\mathcal{H}'^+_t = \mathcal{H}^{\otimes a_t}_{inp} \otimes \mathcal{H}'_{t,rest}$, that is, the secret copies appear first. An evolving (multi-copy) quantum secret sharing (QESS) scheme with perfect privacy and correctness realizing f is an infinite sequence of tuples of quantum circuits of trace preserving operators.

$$Q = \{QESS_t = (\mathbf{Share^t}, (\mathbf{Rec^t}{}_P)_{P\subseteq[t], f^t(P)=1)}\}_{t\geq 1}$$

that satisfy the following properties for every $t > 1$:

- For each $t \geq 1$, $Share^t$ has input domain $\mathcal{H}'_t = \mathcal{H}_{t-1} \otimes \mathcal{H}'^+_t$ (the first component does not exist for $t = 1$). The output domain is of the form $\mathcal{H}_t = \mathcal{H}_{t,0} \otimes \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_t$ (and has the same dimension as the input domain). Note that the $\mathcal{H}_i$'s in the output do not necessarily appear as consecutive qbits in the circuit implementing the operator $Share^t$, but rather according to a wire labeling we describe.[10]
- Furthermore, for $t > 1$, the input domain to $Share^t$ operates in two steps.
  1. Apply $Share^t_1 = Share^{t-1}$ to the portion $\mathcal{H}'_{t-1}$ of the input (and an identity transformation to the rest) . Let $\mathcal{H}_{t-1} = \mathcal{H}_{t-1,0} \otimes \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_{t-1}$ denote the set of $Share^{t-1}$'s output wires.
  2. Compose the transformation from the previous item with $Share^t_2 = Share^t_{2,1} \otimes Share^t_{2,2}$, where $Share^t_{2,1} = I$ is applied to the $\mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_{t-1}$ output wires of $Share^{t-1}$. $Share^t_{2,2}$ is applied to the rest of the wires. That is $\mathcal{H}'^+_t \otimes \mathcal{H}_{t,0}$.[11]
  3. The output wires are relabeled as follows: for $i \in [t-1]$, each output wires of the $Share^t_{2,1}$ part inherit the labels $\mathcal{H}_i$ of its input corresponding input wires. Some of the output wires of $Share^t_{2,2}$ are labeled as $\mathcal{H}_{t,0}$, while the rest are labeled as $\mathcal{H}_t$.
- For every t, $QESS_t$ is a (multi-copy) QESS with secret domain $\mathcal{H}_{inp}$ and output domain $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_t$ and party set $[t]$. The copies of the secret are entered

[9] Both these assumptions are easy to get rid of, and are made only for simplicity of notation.

[10] Here and elsewhere, Hilbert spaces that may be empty are included in the notation, but are not assigned wires in the circuit if they do not exist.

[11] Intuitively, $\mathcal{H}_{t,0}$ are qbits "handed to the future", and can be modified by the dealer to obtain shares for future parties, while the $\mathcal{H}_i$'s are spaces of unchangeable bits, handed as shares to parties $1, \dots, t$ so far.

according to the $(a_i)_i$ sequence (as the first qbit of $\mathcal{H}'^{+}_t$). To account for 0-labels $\mathcal{H}_{t,0}$ here we consider $f^t(x_1,\ldots,x_n)$ as a function of $x_0,x_1,\ldots,x_n$, where $\mathcal{H}_{t,0}$ represents the value contributed by P_0.

Next, we define the evolving secret sharing protocol based on a QESS scheme $QESS_t$ as in Definition 15. While the induced communication protocol is obvious in the classical case, here it needs to be spelled out, due to the need to carefully monitor the parties' shares once they receive them, and not use them in the production of future shares. On a high level, the $\mathcal{H}_{t,0}$ is the part computed at step t, that we pass to the following iteration to be used, and is not part of the current share S_t or prior shares, which have already been handed out. To get some intuition on why this could be useful, consider Smith's construction [Smi00], where randomness and secret to generate a large set of shares is used to translate a linear classical scheme into a quantum one as long as the access structure is no-cloning. We show that in the quantum setting, this could be useful for essentially using early S_t for generating many (but a finite number) of future shares $S_{t+1},S_{t+2},\ldots,S_h$, and passing them through the 0-channel up to level h without doing additional evaluations, which would not be possible because S_t is no longer available starting step $t+1$.

Construction 4.1 (QESS Sharing protocol)**.**

Let Q denote a QESS for an evolving access structure $f:\{0,1\}^*\to\{0,1\}$.

When party $t=1$ arrives, construct the part of the circuit corresponding to $Share^1$. Generate a tensor $|0\rangle$'s and copies of ρ according to the structure of $\mathcal{H}'^{+}_1$ to heed to $Share^1$, send the $\mathcal{H}_1$ output wires to P_1, and save the $\mathcal{H}_{1,0}$ qbits in a register.

When party $t>1$ arrives, construct the part of circuit $Share^t$. Use use the registers corresponding to $\mathcal{H}_{t-1,0}$ from the circuit so far, together with the corresponding new copies of $|0\rangle$ and secret ρ^{a_t} as the $\mathcal{H}'^{+}_t$ part. Give P_t the its computed share, and store the resulting $H_{t,0}$'s.[12]

5 Hybrid-Style Quantum Evolving Secret Sharing

We generalize Construction 3.3 to the evolving setting. In particular, the notion of a no-cloning cover is generalized to infinite access structures in the natural way. That is, every H'_i has a finite support set (while the size of the cover may be infinite). Additionally, it is required that every party is contained in a finite number of H'_i's in the cover. Jumping ahead, we will need the latter requirement for our construction framework to work - see details in the following. Note that this requirement trivially holds for finite access structures defined in 14. Also, note that such a cover always exists. In particular, the set containing all vertices as singleton H'_i's always does the job, even with each j contained in a single H'_i. However, the total set of H'_i's may be larger. As in the finite case, the latter, will determine the copy complexity of our scheme.

Similarly to the finite setting, we let $b(t),c(t),q(t)$ denote the number of classical bits, secret copies and qbits used by $Share^t$ overall. In particular, $c(t)=\sum_{j\le t}a_j$. We say the copy number is finite, if there exists a constant C, such that for every $t\ge 1$, $c(t)\le C$. Note that the above construction need not have a finite copy number.

In our construction, we rely on the following simple observation.

Observation 5.1. *Let $f'\ge f$ denote evolving access structures, and let $CHG'=\{H'_i\}_i$ be a no-cloning cover of f'. Let M be a minterm of f, then M is qualified in H'_i iff. there exists a minterm $M'_i\neq\phi$ of H'_i for which $M'_i\subseteq M_i$.*

[12] In particular, some of the registers $H_{t-1,0}$ may be relabeled H_t and sent as part of P_t's share, as well some of the new registers.

In particular, since $f' \geq f$ it implies the following.

Corollary 1. *For f, f', CHG' as in Observation 5.1. Then every minterm M of f is qualified in some H'_i for which $M \cap support(H'_i) \neq \phi$.*

Also, we will restrict ourselves to no-cloning covers CGH' of f which are either finite, or where every vertex i such that $|\mathcal{M}_i = \{M \text{ is a minterm of f}|Min(M) = i\}| = \infty$ is included in CGH as some $G_j(V = \{i\}, \{i\})$.Also, without loss of generality (regarding optimizing $c(t)$), we require that every minterm of f' is contained in some $H'_i \in CGH'_i$, no M' for which $M \subseteq M$ is contained in some $H'_j \in CGH'_i$. The reason we make this restriction, is to obtain a sufficient condition that every party is involved in a finite number of ESSS scheme executions of recovering QOTP keys. We refer to such covers as *safe* covers of f. A safe cover exist for every $f \neq 0, 1$, for instance, taking $CGH' = \{H'_i\}_i$ where $H'_i = \{\{i\}, \{i\}\}$ satisfies these properties for every non-constant f. More general CGH''s could be used, and adapting the construction below to use such covers in a suitable way can lead to improved $c(t)$ - this is a topic for further research.

For an infinite *safe* no-cloning cover CGH' of f, and minterm M of f, let j be the smallest number such that there exist some $H'_a \in CGH$, and $M' \subseteq M$ which is a minterm of H'_a for which $j \in M'$. We denote the smallest index a of such a graph H'_a by $sG_{CGH'}(M)$, and the corresponding M' by $sj_{CGH}(M)$.[13]

Construction 5.1 (Hybrid cover-based QESS)**.** *Let f be an evolving access structure and $HG = (V, E)$ be its associated MH. Let ρ be the quantum secret. Let CGH' be a* safe *no-cloning cover of f.*

1. *If CGH' be is infinite, we construct an assignment $h : E \to \mathbb{N}^+$ of the minterms of f to new access structure indices. Minterm M of f is assigned to $a = sG_{CGH'}(M)$. Access structure f_a is defined by $G_a = (V_a = \bigcup_{M \in E_a} M, E_a)$, where $E_a = h^{-1}(a)$.*[14]
2. *If $CGH' = \{H'_i\}_{i \in [\ell]}$ is finite, define $G_a = HG$ for every $a \in [\ell]$.*[15]
3. ***The** $Share^t$ **circuit:** For each party P_t joining the system:*
   (a) *If there exist $m_t > 0$ H'_i's in CHG' in which P_t is the first party in $shpport(H'_i)$, run m parallel copies of Smith as follows.*
      i. *For each copy the dealer samples a fresh classical key $k = (k_{i,1}, k_{i,2}) \leftarrow \{0,1\}^2$, where $i - 1$ is the number of such copies generated so far, and produce a fresh copy ρ_i of the secret. Let $E_{\rho_i} = X^{k_{i,1}} Z^{k_{i,2}} \rho_i (X^\dagger)^{k_{i,1}} (Z^\dagger)^{k_{i,2}}$*
      ii. *For each copy, generate a separate Smith sharing circuit with secret E_{ρ_i} and give P_t its appropriate resulting smith shares. Also, generate fresh shares of $k_i = (k_{i,1}, k_{i,2})$ for the access structure defined by the minterm graph G_a via a (generally evolving) classical scheme Π_i. Give P_t its shares. Keep the rest of the shares as part of $\mathcal{H}_{t,0}$ for future use. Also generate shares for P_t in prior ESSS instances Π_j's (where $j < t$) where $t \in V_j$, using the proper (classical) bits stored in $\mathcal{H}_{t,0}$ (and new randomness as needed).*
   (b) *Give P_t every (Smith of Π_i) shares kept for it as part of previous $\mathcal{H}_{t',0}$ ($t' < 0$), formally relabeling it as part of $\mathcal{H}_t$ at the output of $Share^t$. What remains here are ongoing ESSS instances Π_j's (where $j < t$) where $t \in V_j$, using the proper (classical) bits stored in $\mathcal{H}_{t,0}$, as well as shares of ongoing sharings $E_{\rho_{i'}}$'s (for which some $t' < t$ was the first party).*

[13] A graph H'_a as in $sG_{CGH'}(M)$ exists by Corollary 1. Given such H'_a exists, since M is finite, the index j above is unique.

[14] Remove all H'_a's not useful in the sense of $a = sG_{CGH'}(M)$ for some minterm M.

[15] Jumping ahead, there are no complications in this case - we will just share H'_i's masking-keys under the original access structure f, with no risk of infinite ESSS shares.

Theorem 10. *Construction 5.1 is a QESS for f. In particular, it has a finite copy number iff. CHG' is finite. Furthermore, if CHG' if $|CGH'|$ is finite, then the share complexity of party t is $O(b(t))$, where $b(t)$ is a share complexity bound on some ESSS of f.*

Proof. First we prove that the construction is well defined, giving each party a finite share. This is obvious if CGH' is finite. Thus, consider the case it si infinite. Each party P_t gets a finite number of Smith shares, as it is contained in a finite number of H'_i's, by properties of CGH'. Also, it participates in a finite number of Π_j instances. To see this, we prove

Claim. *For every $i \geq 1$, $T_i = \{h(M) | M$ a minterm of $f, min(sj_{CGH'}(M)) = i\}$ is finite.*

We first prove how this implies the finiteness of every party's share, and then prove the claim by induction. Assuming the claim holds, for P_t, M's containing t with $sj_{CGH'}(M) \leq t$ introduce P_t into a finite number of f_i's supports (P_t does not get a share in an ESSS of f_i if it is not in its support). Minterms M containing t for which $sj_{CGH'}(M) > t$ contribute at most a finite number of new f_i's they have been assigned to. This is the case since if there is an infinite number of M's in which $t' \leq t$ is the smallest element, they have been assigned to the unique H'_a that contains $\{t'\}$ by safety of CGH'. Thus, its overall classical share size is finite, as required.

It remains to prove the claim by induction. In the base case, $i = 1$. Every M with $min(sj_{CGH'}(M)) = i$ maps to a graph $H'_a(V'_a, E'_a) \in CGH'$ containing a minterm $M' \in E'_a$ with $i \in M'$. If there are finitely many minterms of f satisfying $min(sj_{CGH'}(M)) = i$, we are done, as each contributes to T_i at most one value of $h(M)$. Otherwise, there are infinitely many M's with $min(sj_{CGH'}(M)) = i$. In this case, it must be that $Min(M) = 1$. Thus, $|\mathcal{M}_i| = \infty$, and by safety of CGH', both some $H'_a(\{i\}, \{i\})$ is in CGH', and not any other $H'_b(V_b, E_b)$ contains a minterm $M' \in E'_b$ with $\{i\} \subseteq E'_b$. Thus, $|T_i| = |\{a\}| = 1$. Step: let $i > 1$, and assume the claim holds for all $i' < i$. In case there are finitely many minterms of f satisfying $min(sj_{CGH'}(M)) = i$, we are done, as before. Otherwise, there are infinitely many M's with $min(sj_{CGH'}(M)) = i$, denote this set by A_i. Every $M \in A_i$ satisfies $Min(M) = i' \leq i$. $M \in A_i$'s with $min(M) < i$ contribute a finite number of values to T_i, by the induction hypothesis. For $M \in A_i$ with $min(M) = i$, there is either a finite number of them, and they thus contribute a finite number of $h(M)$'s to T_i. Otherwise, there is an infinite number of them - $|\mathcal{M}_i| = \infty$, which by safety of CGH' implies the existence of some $H'_a(\{i\}, \{i\})$ is in CGH', and that all these contribute only $\{a\}$, by the same argument as in the base case.

On a high level, the privacy and correctness proofs are a reduction to the single-copy finite case (G+23) in [ÇGLR23] (Thm 29 within), which relies on the fact that all Smith instances operate on their own independent instances of $(k_{i,1}, k_{i,2})$, sampled classical bits, quantum inputs and secret. As we only handle the sharing of the $(k_{i,1}, k_{i,2})$'s differently. Details follow.

Correctness. Let $A \subseteq [t]$, denote a qualified set in f, and t some integer, and let $M \subseteq A$ denote some minterm. As $h(M)$ assigns M to some $H'_a(V'_a, E'_a)$ for which it is qualified, by Observation 5.1, there also exists some $M' \subseteq M$ in E'_a qualified in H'_a. By construction, $M' \subseteq M$ recovers $E_{\rho_a} \times \psi_a$ from that Smith instance, tracing out $[t] \cup \{0\} \setminus A$ (that is, the dealer's part as well). Here ψ_a in particular includes the classical randomness for the Π_a instance). Indeed, this works as H'_i is no-cloning and Smith is QESS a for f'_a. Further recovering $(k_{1,i}, k_{2,i})$, as M is qualified in f_a implemented by Π_a results in $\rho \otimes \psi_a$.

Privacy. Let B denote an unqualified set of f out of $[t]$. As in Theorem 29 in [ÇGLR23] for consider a Smith instance such that $B \cap support(H'_i) \neq \emptyset$ (which is a QECC for H'_i). B is not qualified in f, so by construction, as every $f_i \leq f$, B is not qualified in f_i either, so by privacy of the ESSS Π_i, B receives no information on $(k_{1,i}, k_{2,i})$. Tracing out the shares of $[t] \sup\{0\} \setminus B$ results in a (mixed) state independent of ρ_i. Specifically, tracing

out every such $(k_{i,1}, k_{i,2})$, by the guarantee of QOTP; the density matrix of E_{ρ_j}, which is the input to this instance of Smith, is the maximally mixed state

$$\sigma = \sum_{k\in\{0,1\}^2} \frac{1}{4}\text{QOTPEnc}(\rho, k) \otimes r = \frac{I}{4} \otimes r.$$

where r is a mixed state corresponding to the classical bits (which are independent of (k_1, k_2)). This results in a state of the form $|o\rangle_i = \frac{I}{4} \otimes \psi_i$ for each Smith instance B receives shares in, and remains $|o'\rangle_i$ which is independent of ρ, after applying the Smith sharing circuit. Over the finite set I of such H'_i's and tracing out $[t] \setminus B$ we eventually obtain a state of the form $|o'\rangle = \otimes_{i\in I} |o'\rangle_i$, due to the independence of all classical inputs to the Smith instances, and the distinct, unentangled quantum registers input to each.

The claim on the copy complexity is obvious by construction - in particular, the number of secret copies required is $|CGH'|$, which is finite iff. CGH' is finite. Furthermore, if CGH' is finite, the parties participate in $|CGH'|$ instances of ESSS of f. The Smith instances contribute a constant number of qbits to (a finite subset) of the parties, which does not change the asymptotic complexity of $O(b(t))$, when instantiating Construction 5.1 with the proper ESSS for f. □

5.1 New upper bounds on the copy number of various evolving access structures

Next, we prove that for some evolving access structures, the copy number of our construction is tight. The upper bound is a simple extension of a similar upper bound for the finite setting in [ÇGLR23].

Theorem 11. *For every evolving access structure $f \neq 0$, there exists an instantiation of Construction 4, for which $c(t) \leq t$. Furthermore, there exists an access structure for which every QESS for it satisfied $c(t) \geq t$ for all $t \geq 1$.*

Proof. For the upper bound, fix f. Observe that $HG' = \{\{P_i | i \in \mathbb{N}^+\}\}$ induces f' satisfying $f' \geq f$ for every monotone $f \neq 0$. Applying Construction 5.1 to $CHG' = HG'$ as our no-cloning cover of f, every party P_i simply gets its separate copy E_{ρ_i}, leading to $c(t) = t$ for all $t \geq 1$.

For the lower bound, consider f where the minterms are all the singletons. Consider a quantum evolving secret sharing scheme $\Pi(Share, Rec)$ for it. For a given t, $(Share^t, \{Rec^t_P\}_{P\subseteq[t] \text{ is qualified}})$ is a secret sharing scheme for f^t. As G_{disj} for f^t has $\omega(G_{\text{disj}}) = t$, by Theorem 9, we conclude that at least t copies are required by $Share^t$. □

5.1.1 Some examples

As discussed before, arguably the most interesting and difficult setting is that of no-cloning access structures. First, we observe that for no-cloning evolving access structures, there exists a QESS with a finite copy number, which depends on the particular access structure. This construction may be obtained as a special case for our main Construction 5.1.

Theorem 12. *Let f denote a no-cloning evolving access structure, and let e denote its smallest minterm. Then, there exists a QESS for f with a finite copy number. More precisely, in this construction, $c(t) \leq |e|$. Furthermore, for $f = \bigcup_{i\in[a]} f_i$ where each f_i is no-cloning for some number a, f has a finite copy number.*

Proof. It suffices to specify an evolving access structure $f' \geq f$ and a no-cloning cover of f, and a safe CGH' induced by f' (via $HG' = \cup_i H'_i$ where each H'_i has finite support and is no-cloning). Indeed, let $e = \{v_1, \ldots, v_{|e|}\}$ denote the smallest minterm in HG, and let $HG' = \{H'_1 = \{v_1\}, \ldots, H'_{|e|} = \{v_{|e|}\}\}$ denote the MH of f'. Indeed, $f' \geq f$, since by the

no-cloning property of f, every minterm e_1 of f intersects e, and thus some vertex $v \in e$ is also in e_1. Thus, every minterm of f contains a minterm of f', which implies $f' \geq f$. Taking $CHG' = HG'$ (here the access structures in the cover are singletons), results in an evolving cover of size $|e|$. This cover is finite and thus safe. By Theorem 10, Construction 5.1 instantiated with this cover has $c(t) \leq |e|$ for all t. Finally, for $f = \bigcup_{i\in[a]} f_i$ as in the question, taking the union of the covers for the individual f_i's constructed as above, we obtain a finite cover. It is therefore safe, and the QESS follows by Construction 5.1, as in the $a = 1$ case. □

This leaves a gap in characterizing the share complexity of QESS for no-cloning evolving access structures. While the above implication indicates it must be finite, we do not know how to rule out a $c(t)$ of 1 via some other approach, and leave it as an interesting open question.

Finally, we prove a limitation of our technique, observing that some no-cloning evolving access structures have $c(t) > 1$ for some t for every instantiation of Construction 5.1 with a no-cloning cover. This is the case because every $f' \geq f$ which is finite is not no-cloning.

Theorem 13. *There exists a no-cloning evolving access structure f for which Construction 5.1 always yields a QESS with $c(t) > 1$ (for some t).*

Proof. We construct an explicit co-cloning evolving access structure f for which there exists no finite no-cloning function f' for which $f' \geq f$. This demonstrates that single-copy secret sharing schemes (such as Smith's construction) are insufficient for managing certain evolving structures, necessitating multi-copy approaches.

Defining f. The access structure f is iteratively defined by adding a minterm M_n at step n. The minterm M_n, is defined over the set of participants $\{1, 2, \ldots, 2n\}$, based of previously defined minterms as follows. For each $i \geq 1$, let

$$N_i = \{2i - 1, 2i\}$$

- **Base Case ($i = 1$):** The first minterm consists solely of the first two participants:

$$M_1 = N_1 = \{1, 2\}$$

- **Recursive Step ($i > 1$):** The minterm M_i initially contains its two new participants, N_i. For each $k = 1, \ldots, i - 1$, add $2k$ to M_i if i is even, and $2k - 1$ if i is odd.

Assume for the sake of contradiction that a finite no cloning $f' \geq f$ exists. As f' is finite, it is supported at party index set $[n']$ for some n'. Consider minterms $M_{n'+1}, M_{n'+2}$ of f. As $f' \geq f$, this implies the existence of two minterms M'_1, M'_2 of f' such that $M'_1 \subseteq M_{n'+1}$ and $M'_2 \subseteq M_{n'+2}$. As f' depends on parties $[2n']$ only, these minters are contained in $[n']$. Next, observe that the pair $M_{n'+1}, M_{n'+2}$ of minterms of f intersect at the single party $P_{2(n'+1)}$ if $n' + 2$ is even and $P_{2n'+1}$ if $n' + 2$ is odd. Thus, $M_{n'+1} \cap [2n']$ and $M_{n'+2} \cap [2n']$ are disjoint. Since $M'_1, M'_2 \subseteq [2n']$, $M'_1 \subseteq M_{n'+1}, M'_2 \subseteq M_{n'+2}$ together with the above observation implies that $M'_1 \cap M'_2 = \emptyset$, which contradicts the fact that f' is no-cloning. □

A Self-dual evolving access structures are finite

Theorem 14. *Consider an evolving access structure $f : \{0,1\}^* \to \{0,1\}$ which is self-dual. Then all but a finite number of parties are redundant in f.*

Proof. Consider a minterm M in f with the smallest maximal party index t among all minters (if no minterms exist, the theorem trivially holds). By self-duality, $[t] \setminus M$ is not qualified. We prove all parties with indices $i > t$ are redundant. We prove this by induction on i. In the base case, $i = t + 1$.

References

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009. URL: http://www.cambridge.org/catalogue/catalogue.asp?isbn=9780521424264.

[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. URL: https://eprint.iacr.org/2024/419.

[AMTdW00] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 547–553. IEEE, 2000.

[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. doi:10.1007/978-3-030-84252-9_21.

[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.

[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 of *LNCS*, pages 313–332. Springer, 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. doi:10.1007/978-3-030-45721-1_19.

[CGL99] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 83:648–651, Jul 1999. URL: https://link.aps.org/doi/10.1103/PhysRevLett.83.648, doi:10.1103/PhysRevLett.83.648.

[ÇGLR23] Alper Çakan, Vipul Goyal, Chen-Da Liu-Zhang, and João Ribeiro. Computational quantum secret sharing. In Omar Fawzi and Michael Walter, editors, *18th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2023, July 24-28, 2023, Aveiro, Portugal*, volume 266 of *LIPIcs*, pages 4:1–4:26. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023. URL: https://doi.org/10.4230/LIPIcs.TQC.2023.4, doi:10.4230/LIPICS.TQC.2023.4.

[Cha20] Shion Samadder Chaudhury. A quantum evolving secret sharing scheme. *International Journal of Theoretical Physics*, 59(3936–3950 (2020)), Nov 2020. URL: https://link.springer.com/article/10.1007/s10773-020-04644-5, doi:10.1007/s10773-020-04644-5.

[Chi20] Steven Chien. Augmented ((t, n))-threshold quantum secret sharing schemes. Senior thesis, Princeton University, 2020.

[CP24] Efrat Cohen and Anat Paskin-Cherniavsky. Quantum evolving secret sharing for general access structures. *IACR Cryptol. ePrint Arch.*, 2024:912, 2024. URL: https://eprint.iacr.org/2024/912.

[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. doi:10.1016/j.tcs.2021.01.019.

[DP09] Giacomo M. D'Ariano and Paolo Perinotti. Quantum no-stretching: A geometrical interpretation of the no-cloning theorem. *Physics Letters A*, 373(29):2416–2419, 2009. URL: https://www.sciencedirect.com/science/article/pii/S0375960109001832, doi:10.1016/j.physleta.2009.02.015.

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

[GBP97] M. Grassl, Th. Beth, and T. Pellizzari. Codes for the quantum erasure channel. *Phys. Rev. A*, 56:33–38, Jul 1997. URL: https://link.aps.org/doi/10.1103/PhysRevA.56.33, doi:10.1103/PhysRevA.56.33.

[Got00] Daniel Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61:042311, Mar 2000. URL: https://link.aps.org/doi/10.1103/PhysRevA.61.042311, doi:10.1103/PhysRevA.61.042311.

[HBB99] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. *Physical Review A*, 59(3):1829–1834, March 1999. URL: http://dx.doi.org/10.1103/PhysRevA.59.1829, doi:10.1103/physreva.59.1829.

[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. doi:10.1007/978-3-662-53644-5.

[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.

[KKI99] Anders Karlsson, Masato Koashi, and Nobuyuki Imoto. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A*, 59:162–168, Jan 1999. URL: https://link.aps.org/doi/10.1103/PhysRevA.59.162, doi:10.1103/PhysRevA.59.162.

[KNY16] Ilan Komargodski, Moni Naor, and Eylon Yogev. How to share a secret, infinitely. In *Theory of Cryptography - TCC 2016-B*, volume 9985 of *Lecture Notes in Computer Science*, pages 485–514. Springer, 2016. doi:10.1007/978-3-319-47471-7_19.

[KPC17] 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. doi:10.1007/978-3-319-70503-3_12.

[KW93] Mauricio Karchmer and Avi Wigderson. On span programs. *[1993] Proceedings of the Eigth Annual Structure in Complexity Theory Conference*, pages 102–111, 1993.

[Lov78] László Lovász. Kneser's conjecture, chromatic number, and homotopy. *Journal of Combinatorial Theory, Series A*, 25(3):319–324, 1978.

[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. doi:10.1145/3188745.3188936.

[MAN00] Isaac L Chuang Michael A Nielsen. *Quantum Information and Quantum Computation*. Cambridge University Press, 2000.

[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. URL: https://doi.org/10.4230/LIPIcs.ITC.2023.2, doi:10.4230/LIPICS.ITC.2023.2.

[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. doi:10.1007/978-3-031-49187-0_17.

[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. doi:10.1007/978-3-030-85987-9_5.

[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. *arXiv preprint quant-ph/0001087*, January 2000. URL: https://arxiv.org.

[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. doi:10.1109/TIT.2024.3379278.

[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. doi:10.1109/TCOMM.2023.3253720.