Evolving Ramp Secret-Sharing Schemes

Amos Beimel and Hussien Othman(✉)

Department of Computer Science, Ben Gurion University, Beer Sheva, Israel
amos.beimel@gmail.com, hussien.othman@gmail.com

Abstract. Evolving secret-sharing schemes, introduced by Komargodski, Naor, and Yogev (TCC 2016b), are secret-sharing schemes in which the dealer does not know the number of parties that will participate. The parties arrive one by one and when a party arrives the dealer gives it a share; the dealer cannot update this share when other parties arrive. Komargodski and Paskin-Cherniavsky (TCC 2017) constructed evolving $a \cdot i$-threshold secret-sharing schemes (for every $0 < a < 1$), where any set of parties whose maximum party is the i-th party and contains at least ai parties can reconstruct the secret; any set such that all its prefixes are not an a-fraction of the parties should not get any information on the secret. The length of the share of the i-th party in their scheme is $O(i^4 \log i)$. As the number of parties is unbounded, this share size can be quite large.

In this work we suggest studying a relaxation of evolving threshold secret-sharing schemes; we consider evolving (a, b)-ramp secret-sharing schemes for $0 < b < a < 1$. Again, we require that any set of parties whose maximum party is the i-th party and contains at least ai parties can reconstruct the secret; however, we only require that any set such that all its prefixes are not a b-fraction of the parties should not get any information on the secret. For all constants $0 < b < a < 1$, we construct an evolving (a, b)-ramp secret-sharing scheme where the length of the share of the i-th party is $O(1)$. Thus, we show that evolving ramp secret-sharing schemes offer a big improvement compared to the known constructions of evolving $a \cdot i$-threshold secret-sharing schemes.

1 Introduction

Evolving secret-sharing schemes, introduced by Komargodski, Naor, and Yogev [11], are a secret-sharing scheme in which the dealer does not know the number of parties that will participate and has no upper bound on their number. The parties arrive one after the other and when a party arrives the dealer gives it a share; the dealer cannot update this share when other parties arrive. The motivation for studying such schemes is that updates can be the very costly (e.g., the Y2K problem). On the other hand, if the system designer would take cautious upper bound on the number of parties, then the scheme will not be efficient (specifically, if a small number of parties participate).

Research supported by ISF grant 152/17, the BGU Cyber Security Research Center, and by the Frankel center for computer science.

D. Catalano and R. De Prisco (Eds.): SCN 2018, LNCS 11035, pp. 313–332, 2018.
https://doi.org/10.1007/978-3-319-98113-0_17

Komargodski, Naor and Yogev [11] constructed evolving k-threshold secret-sharing schemes for any constant k (where any k parties can reconstruct the secret). The size of the share of the i-th party in their scheme is $O(k \log i)$. Komargodski and Paskin-Cherniavsky [12] constructed evolving dynamic a-threshold secret-sharing schemes (for every $0 < a < 1$), where any set of parties whose maximum party is the i-th party and contains at least ai parties (i.e., the set contains an a-fraction of the firtst i parties) can reconstruct the secret; any set such that all its prefixes are not an a-fraction of the parties should not get any information on the secret. The length of the share of the i-th party in their scheme is $O(i^4 \log i)$. As the number of parties is unbounded, this share size can be quite large.

We consider a relaxation of evolving a-threshold secret-sharing schemes motivated by ramp secret-sharing schemes. Ramp secret-sharing schemes were first presented by Blakley and Meadows [2], and were used to construct efficient secure multiparty computation (MPC) protocols, starting in the work of Franklin and Yung [8]. We consider evolving (a, b)-ramp secret-sharing schemes (where $0 < b < a < 1$), in which any set of parties whose maximum party is the i-th party and contains at least ai parties can reconstruct the secret, however we only require that any set such that all its prefixes are not a b-fraction of the parties should not get any information on the secret. For all constants $0 < b < a < 1$, we construct an evolving (a, b)-ramp secret-sharing scheme where the length of the share of the i-th party is $O(1)$. Thus, we show that evolving ramp secret-sharing schemes offer a big improvement compared to the known constructions of evolving $a \cdot i$-threshold secret-sharing schemes. We note that all our schemes are linear.

Our Technique. We demonstrate the basic idea of our schemes by describing a simple construction of an evolving (1/2,1/8)-ramp secret-sharing scheme. Following [11], we partition the parties to sets, called generations, according to the order they arrive. The first generation contains the first two parties, the second generation contains the next 2^2 parties, and so on, where the g-th generation contains 2^g parties. When the first party of the g-th generation arrives, the dealer prepares shares of a $2^g/4$-out-of-2^g threshold secret-sharing scheme (e.g., Shamir's scheme [14]); when a party in generation g arrives the dealer gives it a share of this scheme. On one hand, if a set whose maximum party is the i-th party contains at least $i/2$ parties, then in some generation it contains at least $1/4$ of the parties (even if it ends at the beginning of a generation), thus it can reconstruct the secret. On the other hand, if a set can reconstruct the secret from the shares of some generation g, then it contains at least $1/4$ of the parties in that generation, hence it contains at least $1/8$ of the parties that have arrived until the end of the generation.

Using a more complicated analysis, we show how to construct evolving (1/2,b)-ramp secret-sharing schemes with small share size for every $b < 1/6$ by sharing the secret using one threshold secret-sharing scheme in each generation (with an appropriate threshold). To construct evolving (a, b)-ramp secret-sharing schemes for every constants $0 < b < a < 1$, we need to share the secret more

than once in each generation. However, we share the secret only $O(1)$ times in each generation, resulting in a scheme in which the share size of the i-th party is $O(\log i)$ (where $O(\log i)$ is the share size in the threshold secret-sharing scheme). To reduce the share size to $O(1)$, we use (non-evolving) ramp secret-sharing schemes of Chen et al. [6] instead of the threshold secret-sharing schemes. As Chen et al. only provide an existential proof of their ramp schemes with share size $O(1)$, we only obtain that there exist evolving (a, b)-ramp secret-sharing schemes with share size $O(1)$. In contrast, our evolving (a, b)-ramp secret-sharing schemes with share size $O(\log i)$ for party p_i are explicit.

1.1 Previous Works

Secret-sharing schemes were introduced by Shamir [14] and Blakley [1] for threshold access structures, and by Ito, Saito, and Nishizeki for the general case [9]. Shamir's [14] and Blakley's [1] constructions are efficient both in the size of the shares and in the computation required for sharing and reconstruction. The size of the share in Shamir's scheme for sharing an ℓ-bits secret among n parties is $\max\{\ell, \log n\}$. Blakley's scheme requires larger share size, but it can be optimized by using finite fields to get a scheme that is equivalent to Shamir's scheme. Kilian and Nisan [10] proved a $\log(n - k + 2)$ lower bound on the share size for sharing a 1-bit secret for the k-out-of-n threshold access structure. This lower bound implies that $\Omega(\log n)$ bits are necessary when k is not too close to n. Bogdanov, Guo, and Komargodski [3] proved that the lower bound of $\Omega(\log n)$ bits applies to any secret-sharing scheme realizing k-out-of-n threshold access structures for *every* $1 < k < n$. When $k = 1$ or $k = n$, schemes with share size of 1 are known.

Ramp secret-sharing schemes are a generalization of threshold secret-sharing schemes that allow for a gap between the privacy and reconstruction thresholds. Ramp secret-sharing schemes were first presented by Blakley and Meadows [2], and were used to construct efficient secure multiparty computation (MPC) protocols, starting in the work of Franklin and Yung [8]. Ramp schemes have found numerous other applications in cryptography, including broadcast encryption [15] and error decodable secret sharing [13]. Cascudo, Cramer, and Xing [5] proved lower bounds on the share size in ramp secret-sharing schemes: If every set of size at least an can reconstruct the secret while every set of size at most bn cannot learn any information on the secret, then the length of the shares is at least $\log((1 - b)/(a - b))$. Bogdanov et al. [3] showed that for all $0 < b < a < 1$, in any ramp secret sharing the length of the shares is at least $\log(a/(a - b))$. On the positive side, Chen et al. [6] proved that for every $\epsilon > 0$ there is a ramp secret-sharing scheme with share size $O(1)$ in which every set of size at least $(1/2 + \epsilon)n$ can reconstruct the secret while every set of size at most $(1/2 - \epsilon)n$ cannot learn any information on the secret.

Evolving Secret-Sharing Schemes. Evolving secret-sharing schemes were introduced by Komargodski, Naor, and Yogev [11]. They showed that for every evolving access structure there is a secret-sharing scheme that realizes it in which the

share size of party i is 2^{i-1} (even if the dealer does not know the access structure in advance). The main result of their work is providing schemes for evolving threshold access structures. They showed a scheme for the evolving 2-threshold access structure where the share size of party i is $\log i + O(\log \log i)$. Furthermore, they proved a matching lower bound on the share size in any evolving secret-sharing scheme realizing the evolving 2-threshold access structure, that is, their scheme is almost optimal. They generalized the scheme for the evolving 2-threshold access structure to a scheme for the evolving k-threshold access structure for any constant $k \in \mathbb{N}$. In their scheme, the size of the share of the i-th party is $(k-1)\log i + O(\log \log i)$.

Komargodski and Paskin-Cherniavsky [12] considered evolving $\alpha(i)$-threshold access structures, where a set A is authorized if for some $p_i \in A$ the set A contains at least $\alpha(i)$ parties from the set $\{p_1, \ldots, p_i\}$. For example, for the function $\alpha(i) = i/2$ this is the evolving $1/2 \cdot i$-threshold access structure. For every monotone function $\alpha : \mathbb{N} \to \mathbb{N}$, they constructed an evolving secret-sharing scheme realizing the evolving $\alpha(i)$-threshold access structure in which the share size of the i-th party is $O(i^4 \log i)$. Furthermore, they showed how to transform any evolving secret-sharing scheme to a *robust* schme, where a shared secret can be recovered even if some parties hand-in incorrect shares.

Cachin [4] and Csirmaz and Tardos [7] considered online secret sharing, which is similar to evolving secret-sharing schemes. As in evolving secret-sharing scheme, in on-line secret-sharing, parties can enroll in any time after the initialization, and the number of parties is unbounded. However, in the works on online secret-sharing, the number of authorized sets a party can join is bounded.

2 Preliminaries

In this section we present formal definitions of secret-sharing schemes and evolving secret-sharing schemes.

Notations. We denote the logarithmic function with base 2 by log. We use the notation $[n]$ to denote the set $\{1, 2, \ldots, n\}$. When we refer to a set of parties $A = \{p_{i_1}, p_{i_2}, \ldots, p_{i_t}\}$, we assume that $i_1 < i_2 < \cdots < i_t$.

2.1 Secret-Sharing Schemes

We next present the definition of secret-sharing schemes.

Definition 2.1 (Access structures). *Let $\mathcal{P} = \{p_1, \ldots, p_n\}$ be a set of parties. A collection $\Gamma \subseteq 2^{\{p_1,\ldots,p_n\}}$ is* monotone *if $B \in \Gamma$ and $B \subseteq C$ imply that $C \in \Gamma$. An* access structure *$\Gamma = (\Gamma_{\mathrm{YES}}, \Gamma_{\mathrm{NO}})$ is a pair of collections of sets such that $\Gamma_{\mathrm{YES}}, \Gamma_{\mathrm{NO}} \subseteq 2^{\{p_1,\ldots,p_n\}}$, the collections Γ_{YES} and $2^{\{p_1,\ldots,p_n\}} \setminus \Gamma_{\mathrm{NO}}$ are monotone, and $\Gamma_{\mathrm{YES}} \cap \Gamma_{\mathrm{NO}} = \emptyset$. Sets in Γ_{YES} are called* authorized, *and sets in Γ_{NO} are called* unauthorized. *The access structure is called an* incomplete access structure *if there is a subset of parties $A \subseteq \mathcal{P}$ such that $A \notin \Gamma_{\mathrm{YES}} \cup \Gamma_{\mathrm{NO}}$. Otherwise, it is called a* complete access structure.

Definition 2.2 (Secret-sharing schemes). *A* secret-sharing $\Sigma = \langle \Pi, \mu \rangle$ *over a set of parties* $\mathcal{P} = \{p_1, \ldots, p_n\}$ *with domain of secrets* K *is a pair, where* μ *is a probability distribution on some finite set* R *called the set of random strings and* Π *is a mapping from* $K \times R$ *to a set of* n*-tuples* $K_1 \times K_2 \times \cdots \times K_n$ *(the set* K_j *is called the* domain of shares *of* p_j*). A dealer distributes a secret* $k \in K$ *according to* Σ *by first sampling a random string* $r \in R$ *according to* μ*, computing a vector of* shares $\Pi(k, r) = (s_1, \ldots, s_n)$*, and privately communicating each share* s_j *to party* p_j*. For a set* $A \subseteq \{p_1, \ldots, p_n\}$*, we denote* $\Pi_A(k, r)$ *as the restriction of* $\Pi(k, r)$ *to its* A*-entries (i.e., the shares of the parties in* A*). The* size *of the secret is defined as* $\log |K|$ *and the size of the share of party* p_j *is defined as* $\log |K_j|$.

A secret-sharing scheme $\langle \Pi, \mu \rangle$ *with domain of secrets* K *realizes an access structure* $\Gamma = (\Gamma_{\text{YES}}, \Gamma_{\text{NO}})$ *if the following two requirements hold:*

Correctness. *The secret* k *can be reconstructed by any authorized set of parties. That is, for any set* $B = \{p_{i_1}, \ldots, p_{i_{|B|}}\} \in \Gamma_{\text{YES}}$*, there exists a* reconstruction function $\text{Recon}_B : K_{i_1} \times \cdots \times K_{i_{|B|}} \to K$ *such that for every secret* $k \in K$ *and every random string* $r \in R$*,* $\text{Recon}_B\Big(\Pi_B(k, r)\Big) = k$.

Security. *Every unauthorized set cannot learn anything about the secret from its shares. Formally, for any set* $T \in \Gamma_{\text{NO}}$*, every two secrets* $a, b \in K$*, and every possible vector of shares* $\langle s_j \rangle_{p_j \in T}$*,* $\Pr[\, \Pi_T(a, r) = \langle s_j \rangle_{p_j \in T}\,] = \Pr[\, \Pi_T(b, r) = \langle s_j \rangle_{p_j \in T}\,]$*, where the probability is over the choice of* r *from* R *at random according to* μ.

Remark 2.3. For sets of parties $A \in 2^{\mathcal{P}}$ such that $A \notin \Gamma_{\text{YES}} \cup \Gamma_{\text{NO}}$ there are no requirements, i.e., they might be able to reconstruct the secret, they may have some partial information on the secret, or they may have no information on the secret.

Definition 2.4 (Threshold access structures). *Let* $1 \leq k \leq n$*. A* k*-out-of-*n *threshold access structure* Γ *over a set of parties* $\mathcal{P} = \{p_1, \ldots, p_n\}$ *is the complete access structure accepting all subsets of size at least* k*, that is,* $\Gamma_{\text{YES}} = \{A \subseteq \mathcal{P} : |A| \geq k\}$ *and* $\Gamma_{\text{NO}} = \{A \subseteq \mathcal{P} : |A| < k\}$.

The well known scheme of Shamir [14] for the k-out-of-n threshold access structure (based on polynomial interpolation) satisfies the following.

Claim 2.5 (Shamir [14]). *For every* $n \in N$ *and* $1 \leq k \leq n$*, there is a secret-sharing scheme for secrets of length* m *realizing the* k*-out-of-*n *threshold access structure in which the share size is* ℓ*, where* $\ell = \max\{m, \lceil \log(n+1) \rceil\}$.

Definition 2.6 (Ramp secret-sharing schemes [2]). *Let* $0 \leq b \leq a \leq 1$*. An* (a, b)-ramp access structure *over a set of parties* $\mathcal{P} = \{p_1, \ldots, p_n\}$ *is the incomplete access structure* $\Gamma^n_{a,b} = (\Gamma_{\text{YES}}, \Gamma_{\text{NO}})$*, where* $\Gamma_{\text{YES}} = \{A \subseteq \mathcal{P} : |A| \geq an\}$ *and* $\Gamma_{\text{NO}} = \{A \subseteq \mathcal{P} : |A| < bn\}$. An (a, b)-ramp scheme *with* n *parties is a secret-sharing scheme realizing* $\Gamma^n_{a,b}$.

Chen et al. [6] showed the existence of ramp secret-sharing schemes with share size $O(1)$.

Claim 2.7 (Chen et al. [6]). *For every constant $0 < \epsilon < 1/2$ there are integers ℓ and n_0 such that for every $n \geq n_0$ there is a $(1/2 + \epsilon, 1/2 - \epsilon)$-ramp secret-sharing scheme with n parties and share size ℓ.*

2.2 Secret Sharing for Evolving Access Structures

We proceed with the definition of an evolving access structure, introduced in [11].

Definition 2.8 (Evolving access structures). *Let $\mathcal{P} = \{p_i\}_{i\in\mathbb{N}}$ be an infinite set of parties. An evolving access structure $\Gamma = (\Gamma_{\text{YES}}, \Gamma_{\text{NO}})$ is a pair of collections of sets $\Gamma_{\text{YES}}, \Gamma_{\text{NO}} \subset 2^{\mathcal{P}}$, where each set in $\Gamma_{\text{YES}} \cup \Gamma_{\text{NO}}$ is finite and for every $t \in \mathbb{N}$ the collections $\Gamma^t \triangleq (\Gamma_{\text{YES}} \cap 2^{\{p_1,\ldots,p_t\}}, \Gamma_{\text{NO}} \cap 2^{\{p_1,\ldots,p_t\}})$ is an access structure as defined in Definition 2.1.*

Definition 2.9 (Evolving secret-sharing schemes). *Let Γ be an evolving access structure, K be a domain of secrets, where $|K| \geq 2$, and $\{R^t\}_{t\in\mathbb{N}}, \{K^t\}_{t\in\mathbb{N}}$ be two sequences of finite sets. An evolving secret-sharing scheme with domain of secrets K is a pair $\Sigma = \langle\{\Pi^t\}_{t\in\mathbb{N}}, \{\mu^t\}_{t\in\mathbb{N}}\rangle$, where, for every $t \in \mathbb{N}$, μ^t is a probability distribution on R_t and Π^t is a mapping $\Pi^t : K \times R_1 \times \cdots \times R_t \to K_t$ (this mapping returns the share of p_j).*

An evolving secret-sharing scheme $\Sigma = \langle\{\Pi^t\}_{t\in\mathbb{N}}, \{\mu^t\}_{t\in\mathbb{N}}\rangle$ realizes Γ if for every $t \in \mathbb{N}$ the secret-sharing scheme $\langle\mu^1 \times \cdots \times \mu^t, \Pi_t\rangle$, where $\Pi_t(k, (r_1, \ldots, r_k)) = \langle\Pi^1(k, r_1), \ldots, \Pi^t(k, r_1, \ldots, r_t)\rangle$, is a secret-sharing scheme realizing Γ^t according to Definition 2.2.

Definition 2.10 (Evolving threshold access structures [11]). *For every $k \in \mathbb{N}$, the evolving k-threshold access structure is the evolving access structure Γ, where Γ^t is the k-out-of-t threshold access structure.*

Definition 2.11 ($\alpha(t)$-threshold access structures [12]). *Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a monotone function. The $\alpha(t)$-threshold access structure is the evolving access structure Γ, where Γ^t is the $\alpha(t)$-out-of-t threshold access structure.*

Similar to the above definition of the $\alpha(t)$-threshold access structure, we define the evolving *ramp* access structure as follows.

Definition 2.12 (Evolving ramp access structures). *For every $0 \leq b < a \leq 1$, the evolving (a, b)-ramp incomplete access structure is the evolving incomplete access structure $\Gamma_{a,b}$, where $\Gamma^t_{a,b}$ is the (a, b)-ramp access structure.*

Let $A = \{p_{i_1}, p_{i_2}, \ldots, p_{i_t}\}$. Notice that the set A is authorized in $\Gamma_{a,b}$ if $a \cdot i_j < j$ for some $1 \leq j \leq t$. Furthermore, the set A is unauthorized in $\Gamma_{a,b}$ if $b \cdot i_j \geq j$ for every $1 \leq j \leq t$. There are no requirements on sets where $j < a \cdot i_j$ for every j and $b \cdot i_j < j$ for at least one j.

We next prove two lemmas that are used to prove the security and correctness of the schemes we construct in this paper.

Lemma 2.13. *Assume that we share a secret s using a k-out-of-n secret-sharing scheme among the parties $p_{\ell+1}, \ldots, p_{\ell+t}$ and*

$$k \geq b\,(\ell + t)\,. \tag{1}$$

If a set $A = \{p_{i_1}, p_{i_2}, \ldots, p_{i_t}\}$, where $i_t \leq \ell + t$, can learn information on the secret then $|A| \geq b \cdot i_t$, i.e., A is not unauthorized in $\Gamma_{a,b}$.

Proof. If A can learn information on the secret, by the security of the threshold secret-sharing scheme, it must contain at least k parties from the parties $p_{\ell+1}, p_{\ell+2}, \ldots, p_{\ell+n}$. Since $i_t \leq \ell + t$ parties, by (1), $|A| \geq k \geq b(\ell + t) \geq b \cdot i_t$. This implies that A contains at least a fraction b of the parties $p_1, p_{\ell+2}, \ldots, p_{i_t}$, i.e., A is not unauthorized in $\Gamma_{a,b}$. □

The above lemma remains true if we replace the k-out-of-n secret-sharing scheme with any secret-sharing scheme in which each set of size $k - 1$ has no information on the secret.

Lemma 2.14. *Let $A = \{p_{i_1}, p_{i_2}, \ldots, p_{i_t}\}$ be a minimal authorized set in $\Gamma_{a,b}$ for $a < 1$. If for some $j < i_t$ there are at most D parties in $A \cap \{p_1, \ldots, p_j\}$, then $i_t \cdot a \geq \frac{a}{1-a}(j - D)$.*

Proof. We first give an upper bound on the size of A, $|A| = |A \cap \{p_1, \ldots, p_j\}| + |A \cap \{p_{j+1}, \ldots, p_{i_t}\}| \leq D + i_t - j$. Since A is a minimal authorized set, the number of parties in A is at least $i_t \cdot a$, hence, $D + i_t - j \geq i_t \cdot a$, and the lemma follows. □

3 Two Warmup Evolving Ramp Schemes

3.1 A Simple Scheme Realizing $\Gamma_{1/2,1/8}$

As a warm up, we start with a secret-sharing scheme realizing $\Gamma_{1/2,1/8}$. We partition the parties into sets, called generations; the size of generation g is 2^g, that is, generation g contains the parties $p_{2^g-1}, \ldots, p_{2^{g+1}-2}$. We define the scheme Π^0 as follows.

Input: a secret $s \in \{0, 1\}$.

1. For every g, share the secret s among the parties in generation g using a $\frac{2^g}{4}$-out-of-2^g threshold secret-sharing scheme.

Remark 3.1. In the above scheme and in the rest of the paper, when we instruct the dealer to share the secret among the parties in generation g, we mean that when the first party of generation g arrives, the dealer shares the secret using Shamir's threshold scheme; when the i-th party in generation g arrives, the dealer gives it the i-th share of the scheme. Since we use Shamir's scheme, the dealer does not need to prepare all shares of Shamir's scheme in advance; instead it samples the appropriate polynomial Q; when the i-th party in generation g arrives, the dealer gives it the share $Q(i)$.

In order to prove the correctness of Π^0, it suffices to prove that a minimal authorized set of parties A, that is, a set that contains the majority of the parties that have arrived, can reconstruct the secret. Let $A = \{p_{i_1}, p_{i_2}, \ldots, p_{i_t}\}$ be a minimal authorized set; in particular $t \geq i_t/2$. Let g be the generation of party p_{i_t}. Then, $i_t \geq 2^g - 1$ and

$$|A| \geq \left\lceil \frac{i_t}{2} \right\rceil \geq \left\lceil \frac{2^g - 1}{2} \right\rceil = 2^{g-1}. \tag{2}$$

There are two cases:

1. For some $j < g$ the number of parties in A from generation j is at least $\frac{1}{4} \cdot 2^j$. In this case A can reconstruct the secret using the shares of generation j.
2. For each $j < g$, there are less than $\frac{1}{4} \cdot 2^j$ parties from generation j. Thus, the number of parties in A from generations $1, \ldots, g-1$ is less than $\sum_{j=1}^{g-1} \frac{1}{4} \cdot 2^j = (2^g - 2)/4$. Thus, by (2), the number of parties in A from generation g is at least $|A| - (2^g - 2)/4 \geq 2^{g-1} - (2^g - 2)/4 > 2^g/4$, so the parties in A from generation g can reconstruct the secret using the shares of generation g.

Next we prove the security of the scheme. We show that if the parties in A can learn some information on the secret, then there is a prefix of A that contains at least a $1/8$ fraction of the parties, i.e., the set A is not unauthorized. As the dealer shares the secret independently in each generation, if a set A can learn some information on the secret, then it can learn information on the secret from the shares of some generation g. In generation g, the secret is shared by a $\frac{2^g}{4}$-out-of-2^g secret-sharing scheme among the parties $p_{2^g-1}, \ldots, p_{2^{g+1}-2}$. It holds that $2^g/4 \geq \left(2^{g+1} - 2\right)/8$. Therefore, by Lemma 2.13, the set of parties in A from generations $1, \ldots, g$ is not unauthorized in $\Gamma_{1/2,1/8}$, hence, A is not unauthorized.

3.2 A Scheme Realizing $\Gamma_{1/2,b}$ for $b < \frac{1}{6}$

We next generalize the scheme Π^0 to a scheme realizing $\Gamma_{1/2,b}$ provided that $b < \frac{1}{6}$. We denote the scheme by Π^1. We partition the parties to generations, where the size of generation g is m^g for some integer m that will be fixed later. That is, generation g contains the parties $p_{\frac{m^g - m}{m-1}+1}, \ldots, p_{\frac{m^{g+1}-m}{m-1}}$. We define the scheme Π^1 below; in this scheme, $c < 1$ and g_0 are constants that will be chosen such that correctness and security hold.

Input: a secret $s \in \{0, 1\}$.

1. For every g, share the secret s among the parties in generation g using a $\lceil c \cdot m^g \rceil$-out-of-$m^g$ secret-sharing scheme.
2. For all the parties in the first $g_0 - 1$ generations, share the secret using a (non-evolving) secret-sharing scheme realizing the (a, b)-ramp access structure restricted to the parties in the first $g_0 - 1$ generations.

For security, we require that

$$c \geq \frac{bm}{m-1}. \tag{3}$$

Thus, $\lceil c \cdot m^g \rceil \geq c \cdot m^g \geq \frac{bm^{g+1}}{m-1} > b \cdot \frac{m^{g+1}-m}{m-1}$, and, by Lemma 2.13, every set that can learn information on the secret is not unauthorized, thus, the scheme is secure.

For correctness, let $A = \{p_{i_1}, p_{i_2}, \ldots, p_{i_t}\}$ be a minimal authorized set in $\Gamma_{1/2,b}$; in particular, $t \geq i_t/2$. Let g be the generation of party p_{i_t}. There are two cases.

First Case. For some $j < g$, the number of parties in A from generation j is at least $\lceil c \cdot m^j \rceil$. In this case A can reconstruct the secret using the shares of generation j.

Second Case. For every $j < g$, the number of parties in A from generation j is less than $\lceil c \cdot m^j \rceil$, thus is less than $c \cdot m^j$. In this case, we show a condition on the parameters m and c that implies that the number of parties from generation g in A must be at least $\lceil c \cdot m^g \rceil$, and therefore they can reconstruct the secret.

We first show that, since the first case does not hold, the index i_t cannot be in the beginning of generation g. Since for $1 \leq j \leq g-1$ the number of parties from generation j is less than $c \cdot m^j$,

The number of parties in A from the first $g-1$ generations is less than

$$\sum_{j=1}^{g-1} c \cdot m^j = c \cdot \frac{m^g - m}{m-1}. \tag{4}$$

Thus, since the first party in generation g is $p_{\frac{m^g-m}{m-1}+1}$, by Lemma 2.14 it holds that $\frac{i_t}{2} \geq \frac{m^g-m}{m-1}(1-c)$.

Since $t = |A| \geq \frac{i_t}{2}$, by (4), the number of parties from generation g is at least

$$\frac{i_t}{2} - c \cdot \frac{m^g - m}{m-1} \geq \frac{(m^g - m)(1-2c)}{m-1}. \tag{5}$$

For correctness, we want that the parties in generation g can reconstruct the secret. Therefore, it suffices to require $\frac{(m^g-m)(1-2c)}{m-1} \geq c \cdot m^g + 1$. That is, $m^g \left(\frac{1-2c}{m-1} - c\right) \geq 1 + \frac{m(1-2c)}{m-1}$. If $\frac{1-2c}{m-1} - c > 0$, then there is a g_0 such that for every $g \geq g_0$ the condition holds. For the parties in the first $g_0 - 1$ generations we share the secret using a (non-evolving) secret-sharing scheme realizing the (a, b)-ramp access structure restricted to the parties in the first $g_0 - 1$ generations. Therefore, it suffices to require $\frac{1-2c}{m-1} - c > 0$. That is,

$$c < \frac{1}{m+1}. \tag{6}$$

By (3) and (6),

$$b \leq \frac{c(m-1)}{m} \leq \frac{m-1}{m} \cdot \frac{1}{m+1} = \frac{m-1}{m^2+m}. \tag{7}$$

The maximum value of the right hand side of (7) is maximized when $m = 3$ (recall that m is an integer); in this case (7) holds when $b < \frac{1}{6}$. In this case, we take $c = \frac{bm}{m-1} = 1.5b < 1/4$ and (3) and (6) hold.

Lemma 3.2. *For every $b < \frac{1}{6}$, there exists an integer g_0 such that the scheme Π^1 realizes $\Gamma_{1/2,b}$.*

Proof. The correctness and security of the Π^1 for parties in generations $g \geq g_0$ follows from the discussion above. A traditional secret-sharing scheme is used in Step 3.2 of Π^1 to share the secret for parties in the first $g_0 - 1$ generations is correct and secure. Since the shares given to parties in generations $g \geq g_0$ are independent of the shares given to the parties in the first $g_0 - 1$ generations, the combination of both secret-sharing schemes is correct and secure as well. □

Example 3.3. If we take $m = 3$ and $b = 1/7$. Then, $c = 3/14$ and $\frac{1-2c}{m-1} - c = (1 - 3/7)/2 - 3/14 = 1/14$. Thus, for (5) to hold, we can take $g_0 = 3$, therefore we need to share the secret among the parties in the first 2 generations using a (non-evolving) secret-sharing scheme.

4 Evolving Ramp Schemes Realizing $\Gamma_{a,b}$ for Every $a < 1$ and $b < a$

In the scheme Π^1, in each generation we shared the secret using one threshold secret-sharing scheme; Π^1 can realize $\Gamma_{1/2,b}$ only when $b < 1/6$. To realize $\Gamma_{a,b}$ for every $a < 1$ and $b < a$, we generalize the previous method and in each generation we share the secret using r threshold secret-sharing schemes, for a constant r.

As in our previous schemes, we partition the parties into generations, where the size of generation g is m^g. That is, generation g contains the parties

$$p_{\frac{m^g-m}{m-1}+1}, \ldots, p_{\frac{m^{g+1}-m}{m-1}}.$$

We define the scheme Π^2 below; in this scheme, $k_r = m - 1$ and the other parameters will be chosen later such that the security and correctness hold.

Input: a secret $s \in \{0,1\}$.

1. For every g, share the secret s among the parties in generation g using a $\lceil c_0 m^g \rceil$-out-of-m^g secret-sharing scheme (denote this scheme by Π_{c_0}).
2. For every $1 \leq \ell \leq r$ and for every $g \geq 2$, share the secret s among the parties in generation $g-1$ and the first $\left\lceil \frac{k_\ell}{m-1} \cdot m^g \right\rceil$ parties in generation g using a $\left(\lceil c_\ell \cdot m^{g-1} \rceil\right)$-out-of-$\left(m^{g-1} + \left\lceil \frac{k_\ell}{m-1} \cdot m^g \right\rceil\right)$ secret-sharing scheme (denote this scheme by Π_{c_ℓ}).
3. For all the parties in the first $g_0 - 1$ generations, share the secret s using a (non-evolving) secret-sharing scheme realizing the (a,b)-ramp access structure restricted to the parties in the first $g_0 - 1$ generations.

We will choose our parameters such that $c_0 \leq 1$ and $\lceil c_\ell \cdot m^{g-1} \rceil \leq m^{g-1} + \left\lceil \frac{k_\ell}{m-1} \cdot m^g \right\rceil$ for $1 \leq \ell \leq r$, thus, all threshold schemes used in Π^2 are properly defined. For security of Π_{c_0}, by Lemma 2.13, it suffices to require

$$c_0 \geq \frac{b \cdot m}{m-1}. \tag{8}$$

For security of Π_{c_ℓ} for each $1 \leq \ell \leq r$, we require

$$c_\ell \geq \frac{b \cdot m}{m-1} \cdot (1 + k_\ell). \tag{9}$$

Thus, $\lceil c_\ell \cdot m^{g-1} \rceil \geq c_\ell \cdot m^{g-1} \geq \frac{b \cdot m}{m-1} \cdot (1 + k_\ell) \cdot m^{g-1} \geq b \cdot \left(\frac{m^g}{m-1} + \frac{k_\ell}{m-1} m^g \right) > b \cdot \left(\frac{m^g - m}{m-1} + \frac{k_\ell}{m-1} m^g + 1 \right)$, and by Lemma 2.13 (observing that the maximal index of a party that gets a share in Π_{c_ℓ} is $\frac{m^g - m}{m-1} + \left\lceil \frac{k_\ell}{m-1} \cdot m^g \right\rceil$), the scheme is secure.

Next we consider the correctness. Let $A = \{p_{i_1}, p_{i_2}, \ldots, p_{i_t}\}$ be a minimal authorized set in $\Gamma_{a,b}$; in particular, $t \geq i_t \cdot a$. Let g be the generation of party p_{i_t}. There are a few cases, for which we define $r-1$ segments for every $g \geq 2$.

– Segment 1 contains the parties with indexes

$$\left\{ \frac{m^g - m}{m-1} + 1, \ldots, \frac{m^g - m}{m-1} + \left\lceil \frac{k_1}{m-1} \cdot m^g \right\rceil \right\}.$$

– Segment ℓ where $2 \leq \ell \leq r-1$ contains the parties with indexes

$$\left\{ \frac{m^g - m}{m-1} + \left\lceil \frac{k_{\ell-1}}{m-1} \cdot m^g \right\rceil + 1, \ldots, \frac{m^g - m}{m-1} + \left\lceil \frac{k_\ell}{m-1} \cdot m^g \right\rceil \right\}.$$

We defined $k_r = m-1$; thus, these $r-1$ segments are a partition of generation g.

First Case. For some $j < g$, the number of parties in A from generation j is at least $\lceil c_0 \cdot m^j \rceil$. In this case A can reconstruct the secret from the scheme Π_{c_0} for generation j.

Observation 4.1. *If case 1 does not hold, then for every $j < g$ the number of parties in A from generations $1, \ldots, j$ is less than $\sum_{i=1}^{j} c_0 \cdot m^j = c_0 \cdot \frac{m^{j+1}-m}{m-1}$.*

Second Case. Case 1 does not hold and party p_{i_t} is in the first segment in generation g, that is $\frac{m^g-m}{m-1} + 1 \leq i_t \leq \frac{m^g-m}{m-1} + \left\lceil \frac{k_1}{m-1} \cdot m^g \right\rceil$. In this case we show a condition on the parameters implying that the number of parties in A from generations $g-1$ and the first segment of generation g must be at least $c_1 \cdot m^{g-1}$, therefore they can reconstruct the secret.

We start with a lower bound on i_t. By Observation 4.1 and Lemma 2.14 (with $j = \frac{m^g-m}{m-1}$ – the index of last party in generation $g-1$)

$$i_t \cdot a \geq \frac{a}{1-a} \left(\frac{m^g - m}{m-1}(1-c_0) \right). \tag{10}$$

The shares of Π_{c_1} are given to the parties in generation $g-1$ and the parties in the first segment in generation g. As the number of parties in A from generations $1, \ldots, g-2$ is less than $c_0 \cdot \frac{m^{g-1}-m}{m-1}$ (by Observation 4.1), the number of parties in A from generation $g-1$ and the parties in the first segment in generation g is at least

$$i_t \cdot a - c_0 \cdot \frac{m^{g-1} - m}{m-1}. \tag{11}$$

In order to reconstruct the secret from the scheme Π_{c_1} of generation g, the number of parties from generation $g-1$ and the parties in Segment 1 in generation g must be at least $\lceil c_1 \cdot m^{g-1} \rceil$. Therefore, by (11), it suffices to require $i_t \cdot a - c_0 \cdot \frac{m^{g-1}-m}{m-1} \geq c_1 \cdot m^{g-1} + 1$. Thus, by (10), it suffices to require $\frac{a}{1-a} \left(\frac{m^g-m}{m-1}(1-c_0) \right) - c_0 \cdot \frac{m^{g-1}-m}{m-1} \geq c_1 \cdot m^{g-1} + 1$, that is,

$$m^{g-1} \left(\frac{\frac{am}{1-a}(1-c_0) - c_0}{m-1} - c_1 \right) \geq \frac{\frac{am}{1-a}(1-c_0) - c_0 \cdot m}{m-1} + 1. \tag{12}$$

If $\left(\frac{\frac{am}{1-a}(1-c_0)-c_0}{m-1} - c_1 \right) > 0$, then there exists g_1 such that for every $g \geq g_1$ inequality (12) holds. Therefore, it suffices to require that

$$\frac{\frac{a}{1-a}m - c_1 \cdot (m-1)}{\frac{a}{1-a}m + 1} > c_0. \tag{13}$$

Third Case. For each $2 \leq \ell \leq r$ we define Case 3.ℓ as:

The number of parties in A from generation $g-1$ and the first $\left\lceil \frac{k_\ell \cdot m^g}{m-1} \right\rceil$ parties from generation g is at least $\lceil c_\ell \cdot m^g \rceil$. In this case A can reconstruct the secret from the scheme Π_{c_ℓ} for generation g.

Fourth Case. For each $2 \leq \ell \leq r$ we define the Case 4.ℓ as:

Cases 1 and Case 3.$\ell - 1$ do not hold and p_{i_t} is in the ℓ-th segment in generation g, that is $\frac{m^g-m}{m-1} + \left\lceil \frac{k_{\ell-1}}{m-1} \cdot m^g \right\rceil + 1 \leq i_t \leq \frac{m^g-m}{m-1} + \left\lceil \frac{k_\ell}{m-1} \cdot m^g \right\rceil$. In this case we show a condition on the parameters implying that the number of parties in A from generation $g-1$ and the first ℓ segments of generation g must be at least $c_\ell \cdot m^{g-1}$, therefore they can reconstruct the secret.

The number of parties in A from generations $1, \ldots, g-1$ and the parties in the first $\ell - 1$ segments in generation g is less than $c_0 \cdot \frac{m^{g-1}-m}{m-1} + c_{\ell-1} \cdot m^{g-1}$, by Observation 4.1 and since there are less than $c_{\ell-1} \cdot m^{g-1}$ parties in A from generation $g-1$ and the parties in the first $\ell - 1$ segments in generation g (since Case 3.$\ell - 1$ does not hold). By Lemma 2.14 (with $j = \frac{m^g-m}{m-1} + \left\lceil \frac{k_{\ell-1}}{m-1} \cdot m^g \right\rceil$ – the index of last party in segment $\ell - 1$)

$$i_t \cdot a \geq \frac{a}{1-a} \left(\frac{m^g - m}{m-1} + \frac{k_{\ell-1}}{m-1} \cdot m^g - c_0 \cdot \frac{m^{g-1} - m}{m-1} - c_{\ell-1} \cdot m^{g-1} \right). \quad (14)$$

The shares of the scheme Π_{c_ℓ} of generation g are given to the parties in generation $g-1$ and the parties in the first ℓ segments in generation g. As the number of parties in A from generations $1, \ldots, g-2$ is less than $c_0 \cdot \frac{m^{g-1}-m}{m-1}$ (by Observation 4.1), the number of parties in A from generation $g-1$ and the parties in the first ℓ segments in generation g is at least

$$i_t \cdot a - c_0 \cdot \frac{m^{g-1} - m}{m-1}. \quad (15)$$

For correctness, we require that the parties in A from generation $g-1$ and the parties in the first ℓ segments in generation g can reconstruct the secret from the scheme Π_{c_ℓ} of generation $g-1$. Therefore, by (15), it suffices to require $i_t \cdot a - c_0 \cdot \frac{m^{g-1}-m}{m-1} \geq c_\ell \cdot m^{g-1} + 1 > \lceil c_\ell \cdot m^{g-1} \rceil$. Thus, by (14), it suffices to require

$$\frac{a}{1-a} \left(\frac{m^g - m}{m-1} + \frac{k_{\ell-1}}{m-1} \cdot m^g - c_0 \cdot \frac{m^{g-1} - m}{m-1} - c_{\ell-1} \cdot m^{g-1} \right) - c_0 \cdot \frac{m^{g-1} - m}{m-1} \quad \geq \quad c_\ell \cdot m^{g-1} + 1. \quad (16)$$

That is,

$$m^{g-1} \left(\frac{\frac{am}{1-a}(1 + k_{\ell-1}) - c_0(1 + \frac{a}{1-a})}{m-1} - \frac{a}{1-a} c_{\ell-1} - c_\ell \right) \geq 1 + \frac{m(\frac{a}{1-a} - c_0 \frac{a}{1-a} - c_0)}{m-1}. \quad (17)$$

If $\frac{\frac{am}{1-a}(1+k_{\ell-1})-c_0(1+\frac{a}{1-a})}{m-1} - \frac{a}{1-a}c_{\ell-1} - c_\ell > 0$, then there exist g_ℓ such that for every $g \geq g_\ell$ inequality (17) holds. Therefore, it suffices to require that

$$\frac{a}{1-a}m + \frac{a}{1-a}k_{\ell-1} \cdot m - \frac{a}{1-a}c_{\ell-1}(m-1) - c_\ell(m-1) > \frac{c_0}{1-a}. \quad (18)$$

4.1 Finding the Values of the Parameters for Realizing $\Gamma_{a,b}$ for Every $b < a$

In order to build a scheme for $\Gamma_{a,b}$ for $0 < b < a < 1$, we have to find constants $m, r, k_1, \ldots, k_{r-2}$, and $c_0, c_1, \ldots, c_r$ that satisfy (8), (9), (13), and (18). In Theorem 4.7 we prove that such constants exist for every $b < a$. To find the values of the parameters, we first prove that we can choose the values of $c_0, \ldots, c_r$ as the minimal values required by the security requirements (i.e., (8) and (9)). We then prove that for large enough m there is a value of k_1 that satisfies inequality (13). Then, we prove that there exists a constant $\beta < 1$ such that for every k_ℓ if we can take $k_{\ell-1} = \beta k_\ell$, then we satisfy inequality (18). Thus, if we start with $k_r = m - 1$ and with a large enough r and apply the last step iteratively, then k_1 is small enough to satisfy (13).

Example 4.2. As an example, for the scheme $\Gamma_{1/2,0.25}$ we take $r = 2$ and $m = 5$. We start with $k_2 = m-1 = 4$ and take $\beta = 1/3$, thus, $k_1 = \beta k_2 = 4/3$. We choose the values of c_0, c_1, and c_2 as the minimal values required by (8) and (9), that is, $c_0 = \frac{mb}{m-1} = 5/16$, $c_1 = \frac{mb}{m-1}(1+k_1) = 35/48$, and $c_2 = \frac{mb}{m-1}(1+k_2) = 25/16$. Note that for $a = 1/2$ and $m = 5$, inequality (13) requires that $c_1 < (5 - 6c_0)/4$ and c_0, c_1 satisfy this inequality (if this inequality would not hold, we would have taken a larger r). It can be checked that (18) also holds.

Lemma 4.3. *Let $0 < b < a < 1$. If Π^2 realizes the access structure $\Gamma_{a,b}$ with the parameters $r, m, k_1, \ldots, k_r$ and $c_0, c_1, \ldots, c_r$, then Π^2 realizes it with $r, m, k_1, \ldots, k_r$, $c_0 = \frac{m \cdot b}{m-1}$, and $c_\ell = \frac{(1+k_\ell)b \cdot m}{m-1}$ for every $1 \leq \ell \leq r$.*

Proof. By (13), if we decrease c_1 then the left side of the inequality increases, and thus the inequality still holds. By (18), if we decrease $c_{\ell-1}$ and c_ℓ, the left side increases and, thus, the inequality still holds. In all the inequalities, if we decrease c_0, they still hold. Therefore, we can decrease each c_ℓ to its minimum value which is $c_\ell = \frac{(1+k_\ell)b \cdot m}{m-1}$ and keep the inequalities. □

In all our proofs in this section, we take the minimum value of $c_0, c_1, \ldots, c_r$, that is, $c_0 = \frac{m \cdot b}{m-1}$, and $c_\ell = \frac{(1+k_\ell)b \cdot m}{m-1}$ for every $1 \leq \ell \leq r$.

Lemma 4.4. *Let $b < a$. Every $m \geq \frac{2b}{a-b}$ and every $k_1 \leq \frac{a-b}{2b(1-a)}$ satisfy (13).*

Proof. We set $c_0 = \frac{m}{m-1}b$ and $c_1 = (1+k_1)\frac{m}{m-1}b$ in (13). Next we prove that for any $b < a$ for every $0 < k_1 < \frac{a-b}{2b(1-a)}$ inequality (13) holds. By substituting the above c_0, c_1 in (13) we obtain the inequality $\frac{\frac{a}{1-a}m-(1+k_1)\frac{m}{m-1}b\cdot(m-1)}{\frac{a}{1-a}m+1} > \frac{m}{m-1}b$.

That is,

$$k_1 < \frac{\frac{a}{1-a} - b - \frac{b}{m-1} - \frac{ba}{(1-a)(m-1)}}{b} = \frac{\frac{a-b}{1-a} - \frac{b}{(m-1)(1-a)}}{b}. \tag{19}$$

Thus, every $m > \frac{2b}{a-b} + 1$ and $k_1 \leq \frac{a-b}{(1-a)2b}$ satisfy inequality (19). □

Lemma 4.5. *For every $b < a$, every $m > \frac{a}{a-b}$, and every k_ℓ inequality (18) is satisfied when $k_{\ell-1} = \frac{(1-a)b}{a(1-b)}k_\ell$.*

Proof. We substitute $c_0 = \frac{mb}{m-1}$, $c_{\ell-1} = (1+k_{\ell-1})\frac{mb}{m-1}$, and $c_\ell = (1+k_\ell)\frac{mb}{m-1}$ in (18) and obtain the following requirement.

$$\frac{a}{1-a}m + \frac{a}{1-a}k_{\ell-1}m - \frac{a}{1-a}(1+k_{\ell-1})\frac{mb}{m-1}(m-1) - (1+k_\ell)\frac{mb}{m-1}(m-1) > \left(1+\frac{a}{1-a}\right)\frac{mb}{m-1}.$$

That is,

$$\frac{a-b}{1-a} + \frac{a}{1-a}(1-b)k_{\ell-1} - bk_\ell > \frac{b}{(1-a)(m-1)}. \tag{20}$$

Taking $k_{\ell-1} = \frac{(1-a)b}{a(1-b)}k_\ell$, we conclude that (20) holds if and only if $m > \frac{b}{a-b}+1 = \frac{a}{a-b}$. □

Next we show that the schemes $\Pi_{c_0}, \ldots, \Pi_{c_r}$ are all legal threshold secret-sharing schemes, that is, the number of parties needed to reconstruct the secret is at most the number of parties in the scheme.

Lemma 4.6. *Assume that $m \geq \frac{2}{1-b}$. The thresholds in the schemes Π_{c_ℓ} for $0 \leq \ell \leq r$ are at most the number of parties in the schemes for every $g \geq 2$, that is, $\lceil c_0 \cdot m^g \rceil \leq m^g$ and $\lceil c_\ell \cdot m^{g-1} \rceil \leq m^{g-1} + \left\lceil \frac{k_\ell}{m-1} \cdot m^g \right\rceil$ for $1 \leq \ell \leq r$.*

Proof. For Π_{c_0}, note that $c_0 = \frac{mb}{m-1} = b + \frac{b}{m-1}$. Thus, if $m \geq \frac{b}{1-b} + 1$, then $c_0 \leq 1$ and $\lceil c_0 \cdot m^g \rceil \leq \lceil m^g \rceil = m^g$ as required.

For Π_{c_ℓ} (where $1 \leq \ell \leq r$), the threshold is $\lceil c_\ell \cdot m^{g-1} \rceil < c_\ell \cdot m^{g-1} + 1$ and the number of parties is $m^{g-1} + \left\lceil \frac{k_\ell}{m-1} \cdot m^g \right\rceil \geq m^{g-1} + \frac{k_\ell}{m-1} \cdot m^g$. Recall that $c_\ell = \frac{(1+k_\ell)b\cdot m}{m-1}$. Thus, it suffices to show that $\frac{(1+k_\ell)bm}{m-1} \cdot m^{g-1} + 1 \leq m^{g-1} + \frac{k_\ell}{m-1} \cdot m^g$.

As $b < 1$ and $g \geq 2$, it suffices to choose m such that

$$\left(1 - \frac{bm}{m-1}\right) m \geq 1. \tag{21}$$

Taking $m \geq \frac{2}{1-b}$ satisfies (21). □

Theorem 4.7. *For every $b < a$ there is a choice of the parameters such that Π^2 realizes $\Gamma_{a,b}$ with share size of $O(\log i)$ for party p_i.*

Proof. In order to prove the theorem, we need to show that for every $b < a$ there is a choice of the parameters that satisfies (8), (9), (13), and (18). We take $c_0 = \frac{mb}{m-1}$ and $c_\ell = (1 + k_\ell)\frac{mb}{m-1}$ for $1 \leq \ell \leq r$, thus, inequalities (8) and (9) are satisfied and the scheme is secure.

We take $m = \left\lceil \frac{2}{a-b} \right\rceil \geq \max\{\frac{2b}{a-b}, \frac{a}{a-b}, \frac{2}{1-b}\}$, thus, we can apply Lemmas 4.4 to 4.6. We still need to find r. In order to find it, we apply Lemma 4.5 iteratively starting from $k_r = m - 1$ and taking $k_{\ell-1} = \frac{(1-a)bk_\ell}{a(1-b)} = \left(\frac{(1-a)b}{a(1-b)}\right)^{r-\ell}(m-1)$ for $2 \leq \ell \leq r$. By Lemma 4.5, inequality (18) is satisfied for every ℓ. Note that $\frac{(1-a)b}{a(1-b)} < 1$ (as $b < a$), thus, $k_1 < k_2 < \cdots < k_r$. We take $r = \left\lceil 2 + \log_{\frac{a(1-b)}{(1-a)b}} \frac{2(1-a)b \cdot m}{a-b} \right\rceil$. Thus, we get $k_1 \leq \left(\frac{(1-a)b}{a(1-b)}\right)^{\log_{\frac{a(1-b)}{(1-a)b}} \frac{2(1-a)b \cdot m}{a-b}} (m-1) = \frac{a-b}{2(1-a)b \cdot m}(m-1) < \frac{a-b}{2(1-a)b}$; by Lemma 4.4, inequality (13) is satisfied.
If we take $g_0 = \max\{2, g_1, \ldots, g_r\}$ (where $g_1, \ldots, g_r$ are the constants required for (13) and (18)), then the scheme is correct.

We next analyze the length of the share of p_i in Π^2. Let g be the generation of p_i. It suffices to consider only parties in generations $g \geq g_0$. Recall that the generation g of p_i is the maximal g such that $(m^g - m)/(m-1) < i$; in particular, $m^g \leq (m-1)i$. Every party p_i gets $O(r)$ shares in Shamir's scheme with $O(m^g) = O(mi)$ parties. The length of the share in Shamir's scheme with n parties and a one bit secret is $O(\log n)$. Thus, the size of the share of each party p_i is $O(\log i)$ (since m and r are constants as $b < a$ are constants). □

4.2 An Optimized Scheme with Share Size $O(1)$

Next we show an optimization of the previous scheme such that each party's share size is $O(1)$. In the optimized scheme we use ramp secret-sharing schemes instead of threshold secret sharing schemes. We next describe the optimized scheme, denoted as Π^3, in which the share size is $O(1)$.

Input: a secret $s \in \{0,1\}$.

1. For every g, share s among the m^g parties in generation g using a $(c_0, c_0 - \epsilon)$-ramp secret-sharing scheme for some constant $\epsilon > 0$ to be fixed later (denote this scheme by Π'_{c_0}).
2. For every $1 \leq \ell \leq r$ and for every $g \geq 2$, share the secret s among the parties in generation $g-1$ and the first $\left\lceil \frac{k_\ell}{m-1} \cdot m^g \right\rceil$ parties in generation g using a $(c_\ell \cdot m^{g-1} \cdot \frac{1}{n}, (c_\ell - \epsilon) \cdot m^{g-1} \cdot \frac{1}{n})$-ramp secret-sharing scheme for some constant $\epsilon > 0$ to be fixed later, where $n = m^{g-1} + \left\lceil \frac{k_\ell}{m-1} \cdot m^g \right\rceil$ is the number of parties (denote this scheme by Π'_{c_ℓ}).
3. For all the parties in the first $g_0 - 1$ generations, share the secret s using a (non-evolving) secret-sharing scheme realizing the (a,b)-ramp access structure restricted to the parties in the first $g_0 - 1$ generations.

Chen et al. [6] showed that there exist $(1/2+\epsilon, 1/2-\epsilon)$-ramp secret-sharing schemes with share size $O(1)$ for every constant $\epsilon > 0$ (see Claim 2.7). In Appendix A, we prove the following claim that shows that Chen et al.'s result implies the existence of (a,b)-ramp secret-sharing schemes with share size $O(1)$ for every constants $b < a$.

Claim 4.8. *For every constants $0 < b < a < 1$ there are integers ℓ and n_0 such that for every $n \geq n_0$ there is an (a,b)-ramp secret-sharing scheme with n parties and share size ℓ.*

Theorem 4.9. *For every $b < a$ there is a choice of the parameters such that Π^3 realizes $\Gamma_{a,b}$ with share size $O(1)$.*

Proof. We modify the proof of Π^2 to prove the security and correctness of Π^3. For the security of Π'_{c_0}, we now have the following requirement.

$$c_0 \geq \frac{bm}{m-1} + \epsilon. \tag{22}$$

For security of Π'_{c_ℓ} for each $1 \leq \ell \leq r$, we require

$$c_\ell \geq \frac{b \cdot m}{m-1} \cdot (1 + k_\ell) + \epsilon. \tag{23}$$

Thus, it holds that $\lceil (c_\ell - \epsilon) m^{g-1} \rceil \geq (c_\ell - \epsilon) m^{g-1} \geq \frac{b \cdot m}{m-1} \cdot (1 + k_\ell) \cdot m^{g-1} \geq b \cdot \left(\frac{m^g}{m-1} + \frac{k_\ell}{m-1} m^g \right) > b \cdot \left(\frac{m^g - m}{m-1} + \frac{k_\ell}{m-1} m^g + 1 \right)$, and by Lemma 2.13 (observing that the party with the maximal index which gets a share for Π_{c_ℓ} is $\frac{m^g - m}{m-1} + \left\lceil \frac{k_\ell}{m-1} \cdot m^g \right\rceil$), the scheme is secure.

The correctness conditions remain the same. Therefore, we need to prove that inequalities (13) and (18) hold under the new security conditions. Let $m, r, c_0, c_1, \ldots, c_r, k_1, \ldots, k_r$ be the parameters used to construct Π^2 for some a and b. We show that there exists ϵ such that the parameters $m, r, c'_0 = c_0+\epsilon, c'_1 = c_1 + \epsilon, \ldots, c'_r = c_r + \epsilon, k_1, \ldots, k_r$ satisfy the security and correctness conditions for Π^3. It is easy to see that the security conditions hold, since $c_0 \geq b\frac{m}{m-1}$ and increasing it by $\epsilon > 0$ will satisfy the security condition (22) for Π^3 (the same for the other conditions).

For the correctness, in inequality (13) the right-hand side is increased by ϵ, and the left-hand side is decreased by $\frac{\epsilon(m+1)(1-a)}{am+1-a}$. In (13), it is required that the left-hand side is strictly greater than the right-hand side. Thus, for the constants defined in the proof of the correctness of Π^2, there is a constant $\delta_1 > 0$ (which is a function of a and b) such that the left side of inequality (13) equals to $c_0 + \delta_1$. Therefore, the left side in inequality (13) with $c'_0, \ldots, c'_r$ equals to $c_0 + \delta_1 - \frac{\epsilon(m-1)(1-a)}{am+1-a}$. For the inequality to hold, we require that $c_0 + \delta_1 - \frac{\epsilon(m-1)(1-a)}{am+1-a} > c_0 + \epsilon$. Taking ϵ such that $\epsilon + \frac{\epsilon(m-1)(1-a)}{am+1-a} < \delta_1$ will satisfy the inequality. Thus, we take $\epsilon < \min\{c_0, \frac{\delta_1(am+1-a)}{m}\}$.

In inequality (18), the right hand side is increased by $\frac{\epsilon}{1-a}$, and the left hand side is decreased by $\frac{\epsilon(m-1)}{1-a}$. In (18), it is required that the left-hand side is strictly greater than the right-hand side. Thus, for the constants defined in the proof of the correctness of Π^2, there is a constant $\delta_2 > 0$ (which is a function of a and b) such that the left side of inequality (18) equals to $\frac{c_0}{1-a} + \delta_2$, Therefore, the left hand side in inequality (18) with $c'_0, \ldots, c'_r$ equals to $\frac{c_0}{1-a} + \delta_2 - \frac{\epsilon(m-1)}{1-a}$. For the inequality to hold, we require that $\frac{c_0}{1-a} + \delta_2 - \frac{\epsilon(m-1)}{1-a} > \frac{c_0+\epsilon}{1-a}$. Taking $\epsilon < \frac{\delta_2(1-a)}{m}$ satisfies the inequality.

Taking $\epsilon < \min\{c_0, \ldots, c_r, \frac{\delta_1(am+1-a)}{m}, \frac{\delta_2(1-a)}{m}\}$ satisfies both inequalities and guarantees that all ramp secret-sharing schemes are properly defined.

The share size each party consists of $r = O(1)$ shares of ramp secret-sharing schemes, each is of size $O(1)$. Therefore, the share size of each party is $O(1)$. □

A Proof of Claim 4.8

We next prove Claim 4.8, i.e., we prove that for every constants $b < a$ there exists a ramp secret-sharing scheme with share size $O(1)$.

Proof. Chen et al. [6] proved the claim for the case when $a = 1/2 + \epsilon$ and $b = 1/2 - \epsilon$ for every $\epsilon > 0$, see Claim 2.7. We use two standard transformations to prove it for every $b < a$. Let $\Pi^N_{1/2+\epsilon,1/2-\epsilon}$, for some $\epsilon < 1/2$, be a ramp secret-sharing scheme with share size ℓ with N parties. If $a > 1/2$ and $b < 1/2$, the scheme $\Pi^n_{1/2+\epsilon,1/2-\epsilon}$, where $\epsilon = \min\{a - 1/2, 1/2 - b\}$, is an (a, b)-ramp secret-sharing with share size $O(1)$. Otherwise, there are two cases; in each case we show the existence of an (a, b)-ramp secret-sharing scheme with n parties, denoted $\Pi^n_{a,b}$, with share size ℓ.

The case $b \geq 1/2$. We use the scheme $\Pi^N_{1/2+\epsilon,1/2-\epsilon}$, where $N = \alpha n$ for some constants $\alpha > 1$ and $\epsilon < 1/2$ to be fixed later. We only use the shares of the first n parties of $\Pi^N_{1/2+\epsilon,1/2-\epsilon}$. In $\Pi^N_{1/2+\epsilon,1/2-\epsilon}$, a set of size $N(1/2+\epsilon) = \alpha n(1/2+\epsilon)$ can reconstruct the secret. In $\Pi^n_{a,b}$, we require that an parties can reconstruct the secret, thus, we take α such that $\alpha n(1/2+\epsilon) = an$, i.e., $\alpha = \frac{2a}{1+2\epsilon}$. By the security of $\Pi^N_{1/2+\epsilon,1/2-\epsilon}$, any set of parties of size less than $N(1/2-\epsilon) = \alpha n(1/2-\epsilon) = \frac{2a}{1+2\epsilon} n(1/2-\epsilon)$ cannot learn any information on the secret. In $\Pi^n_{a,b}$, we require that bn parties cannot learn any information on the secret, thus, we require that $\frac{2a}{1+2\epsilon}(1/2-\epsilon) = b$, i.e., $\epsilon = \frac{a-b}{2(a+b)}$. Notice that $\alpha = \frac{2a}{1+2\epsilon} = \frac{2a}{1+\frac{a-b}{a+b}} = a+b > 1$ (since $a > b \geq 1/2$), thus, we have enough shares in $\Pi^{\alpha n}_{1/2+\epsilon,1/2-\epsilon}$ to give to the n parties. Furthermore, $\epsilon < 1/2$ as required by Claim 2.7.

The case $a \leq 1/2$. Again, we use the scheme $\Pi^N_{1/2+\epsilon,1/2-\epsilon}$, where $N = \alpha n$ for some constants $\alpha > 1$ and $\epsilon < 1/2$ to be fixed later. We use the shares of the first n parties of $\Pi^N_{1/2+\epsilon,1/2-\epsilon}$ as the shares in $\Pi^n_{a,b}$. However, in this case we publish $N - n = (\alpha - 1)n$ shares on a public blackboard (we later explain how to get rid of this public blackboard). In $\Pi^n_{a,b}$, we require that an parties can reconstruct the secret. As the number of shares of $\Pi^N_{1/2+\epsilon,1/2-\epsilon}$ that an parties in $\Pi^n_{a,b}$ have is $an + (\alpha-1)n$, we require that $an + (\alpha-1)n = N(1/2+\epsilon) = \alpha n(1/2+\epsilon)$, i.e., $\alpha = (2-2a)/(1-2\epsilon)$. In $\Pi^n_{a,b}$, we require that bn parties cannot learn any information on the secret. As the number of shares of $\Pi^N_{1/2+\epsilon,1/2-\epsilon}$ that bn parties in $\Pi^n_{a,b}$ have is $bn+(\alpha-1)n$, we require that $bn+(\alpha-1)n = \alpha n(1/2-\epsilon)$, i.e., $\alpha(1+2\epsilon) = 2-b$. Solving the requirements on α, we get that $\epsilon = \frac{a-b}{2(2-a-b)}$ and $\alpha = 2-a-b$. Note that $\alpha > 1$ since $b < a \leq 1/2$ and $\epsilon < 1/2$.

To get rid of the shares published on the blackboard, we fix possible shares $s_{n+1}, \ldots, s_{\alpha n}$ of the last $(\alpha-1)n$ parties in $\Pi^N_{1/2+\epsilon,1/2-\epsilon}$ (e.g., in the scheme of Chen et al. [6], we can fix $s_{n+1} = \cdots = s_{\alpha n} = 0$). To share the secret, the dealer chooses only vectors of shares of $\Pi^N_{1/2+\epsilon,1/2-\epsilon}$ such that the shares of the last $(\alpha-1)n$ parties are the fixed shares $s_{n+1}, \ldots, s_{\alpha n}$. □

References

1. Blakley, G.R.: Safeguarding cryptographic keys. In: AFIPS, p. 313 (1979)
2. Blakley, G.R., Meadows, C.: Security of ramp schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 242–268. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_20
3. Bogdanov, A., Guo, S., Komargodski, I.: Threshold secret sharing requires a linear size alphabet. In: Hirt, M., Smith, A. (eds.) TCC 2016. LNCS, vol. 9986, pp. 471–484. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53644-5_18
4. Cachin, C.: On-line secret sharing. In: Boyd, C. (ed.) Cryptography and Coding 1995. LNCS, vol. 1025, pp. 190–198. Springer, Heidelberg (1995). https://doi.org/10.1007/3-540-60693-9_22
5. Cascudo Pueyo, I., Cramer, R., Xing, C.: Bounds on the threshold gap in secret sharing and its applications. IEEE Trans. Inf. Theory 5600–5612 (2013)

6. Chen, H., Cramer, R., Goldwasser, S., de Haan, R., Vaikuntanathan, V.: Secure computation from random error correcting codes. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 291–310. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-72540-4_17
7. Csirmaz, L., Tardos, G.: On-line secret sharing. Des. Codes Crypt. **63**(1), 127–147 (2012)
8. Franklin, M.K., Yung, M.: Communication complexity of secure computation. In: STOC 1992, pp. 699–710 (1992)
9. Ito, M., Saito, A., Nishizeki, T.: Secret sharing schemes realizing general access structure. In: Proceedings of Globecom 1987, pp. 56–64 (1987)
10. Kilian, J., Nisan, N.: Private communication (1990)
11. Komargodski, I., Naor, M., Yogev, E.: How to share a secret, infinitely. In: Hirt, M., Smith, A. (eds.) TCC 2016. LNCS, vol. 9986, pp. 485–514. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53644-5_19
12. Komargodski, I., Paskin-Cherniavsky, A.: Evolving secret sharing: dynamic thresholds and robustness. In: Kalai, Y., Reyzin, L. (eds.) TCC 2017. LNCS, vol. 10678, pp. 379–393. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70503-3_12
13. Martin, K.M., Paterson, M.B., Stinson, D.R.: Error decodable secret sharing and one-round perfectly secure message transmission for general adversary structures. Cryptography Commun. 65–86 (2011)
14. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
15. Stinson, D.R., Wei, R.: An application of ramp schemes to broadcast encryption. Inform. Process. Lett. 131–135 (1999)