Evolving Ramp Secret Sharing with a Small Gap

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 there is no a-priory upper bound on 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. Motivated by the fact that when the number of parties is known, ramp secret-sharing schemes are more efficient than threshold secret-sharing schemes, we study evolving ramp secret-sharing schemes. Specifically, we study evolving $(b(j), g(j))$-ramp secret-sharing schemes, where $g, b : \mathbb{N} \rightarrow \mathbb{N}$ are non-decreasing functions. In such schemes, any set of parties that for some j contains $g(j)$ parties from the first parties that arrive can reconstruct the secret, and any set such that for every j contains less than $b(j)$ parties from the first j parties that arrive cannot learn any information about the secret.

We focus on the case that the gap is small, namely $g(j) - b(j) = j^{\beta}$ for $0 < \beta < 1$. We show that there is an evolving ramp secret-sharing scheme with gap t^{β}, in which the share size of the j-th party is $\tilde{O}(j^{4-\frac{1}{\log^2 1/\beta}})$. Furthermore, we show that our construction results in much better share size for fixed values of β, i.e., there is an evolving ramp secret-sharing scheme with gap $\sqrt{j}$, in which the share size of the j-th party is $\tilde{O}(j)$. Our construction should be compared to the best known evolving $g(j)$-threshold secret-sharing schemes (i.e., when $b(j) = g(j) - 1$) in which the share size of the j-th party is $\tilde{O}(j^4)$. Thus, our construction offers a significant improvement for every constant β, showing that allowing a gap between the sizes of the authorized and unauthorized sets can reduce the share size.

In addition, we present an evolving $(k/2, k)$-ramp secret-sharing scheme for a constant k (which can be very big), where any set of parties of size at least k can reconstruct the secret and any set of parties of size at most $k/2$ cannot learn any information about the secret. The share size of the j-th party in our construction is $O(\log k \log j)$. This is

This work was done while the first author was visiting Georgetown university, supported by NSF grant no. 1565387, TWC: Large: Collaborative: Computing Over Distributed Sensitive Data. The authors are also supported by ISF grant 152/17, by a grant from the Cyber Security Research Center at Ben-Gurion University of the Negev, and by the Frankel center for computer science. The second author is also supported by a scholarship from the Israeli Council For Higher Education.

A. Canteaut and Y. Ishai (Eds.): EUROCRYPT 2020, LNCS 12105, pp. 529–555, 2020.
https://doi.org/10.1007/978-3-030-45721-1_19

an improvement over the best known evolving k-threshold secret-sharing schemes in which the share size of the j-th party is $O(k \log j)$.

1 Introduction

In secret-sharing schemes (as in many cryptographic primitives) the number of parties is known in advance. If the number of parties is not known in advance, the dealer can assume an upper bound on this number. On one hand, if this upper bound is too pessimistic (e.g., very few parties are active), then the shares are unnecessarily large. On the other hand, if the upper bound is too optimistic and the number of parties exceeds the upper bound, then either new parties cannot join the system or the dealer needs to refresh the shares of all existing parties, which is very costly. Komargodski, Naor, and Yogev [14] suggested evolving secret-sharing schemes as a solution to this problem. In such schemes, there is no upper bound on the number of parties and the parties arrive one after the other. When a party arrives the dealer gives it a share; the dealer cannot update this share when other parties arrive.

Continuing our previous work [1], we consider evolving ramp secret-sharing schemes. In a traditional (b, g)-ramp secret-sharing schemes (with a fixed number of parties n, where $b < g \leq n$), sets of parties of size at least g should be able to reconstruct the secret, while sets of parties of size at most b should get no information on the secret.[1] There are no requirements on sets with more than b parties but less than g parties. Allowing a gap between b and g results in schemes that are more efficient than threshold secret-sharing schemes. Ramp secret-sharing schemes were first presented by Blakley and Meadows [4], and were used to construct efficient secure multiparty computation (MPC) protocols, starting in the work of Franklin and Yung [11]. In evolving (b, g)-ramp secret-sharing schemes (without an upper bound on the number of parties), g and b are non-decreasing functions $g, b : \mathbb{N} \rightarrow \mathbb{N}$ such that $b(j) < g(j)$ for every $j \in \mathbb{N}$, sets of parties that for some j contain at least $g(j)$ parties from the first j parties that arrive are authorized (i.e., should be able to reconstruct the secret), while sets of parties that for every j contain at most $b(j)$ parties from the first j parties that arrive are unauthorized (i.e., should get no information on the secret). Again, there are no requirements on sets that do not satisfy either of the requirements. In this work we investigate evolving ramp secret-sharing schemes, where the gap between g and b is small, e.g., $g(j) - b(j) = j^{\beta}$ for some constant β or $b(j) = k/2$ and $g(j) = k$ for some constant k.

Before presenting our results, we describe several results on evolving secret-sharing schemes. Komargodski, Naor, and Yogev [14] showed that every evolving access structure (i.e., collection of authorized sets) can be realized by a secret-sharing scheme, where the size of the share of the j-th party is 2^{j-1} (even if the dealer does not know the access structure in advance). They also

[1] The letters b and g stand for "bad" parties (that should not learn information about the secret) and "good" parties (that can reconstruct the secret).

showed evolving k-threshold secret-sharing schemes (where any set of k parties can reconstruct the secret), in which the share size of the j-th party is $(k-1)\log j + O(\log\log j)$. Komargodski and Paskin-Cherniavsky [15] considered evolving dynamic-threshold secret-sharing schemes in which the threshold is defined by a function $g : \mathbb{N} \rightarrow \mathbb{N}$; in such a scheme a set of parties is authorized if for some j the set contains at least $g(j)$ parties from the first j parties that arrive; all other parties are unauthorized. For every non-decreasing function $1 \leq g(j) \leq j$, they constructed an evolving $g(j)$-threshold secret-sharing scheme in which the share size of the j-th party is $O(j^4 \log j)$. As the number of parties is unbounded, this share size can be quite large. Beimel and Othman [1] constructed for any constants $0 < \alpha < \gamma < 1$ an evolving $(b(j) = \alpha j, g(j) = \gamma j)$-ramp secret-sharing scheme (i.e., the gap is a constant fraction of the parties) where the size of the share of the j-th party is $O(1)$.

Evolving ramp secret-sharing schemes with small gap are motivated due two reasons. First, they are step towards understanding the evolving dynamic threshold schemes, i.e., when the gap is 1. Second, it is a very interesting theoretical question to understand how the evolving ramp schemes behave as a function of the size of the gap. Namely, we know that when the gap is a constant fraction then the share size is O(1) and when the gap is 1 the best share size of the j-th party is $\tilde{O}(j^4)$; understanding what the share size is in between these two extremes is a natural question.

1.1 Our Results

In this work we continue the investigation of evolving ramp secret-sharing schemes. We study the share size in ramp evolving secret-sharing schemes when the gap between $g(j)$ and $b(j)$ is small, i.e., $o(j)$. Can the share size be smaller than j^4 – the share size in the evolving threshold secret-sharing schemes of [15]? We give positive results when $g(j) - b(j) \leq j^\beta$ for some constant β. We prove the following theorem:

Theorem 1.1. *For every constants $0 < \beta < 1$ and $0 < \gamma < 1$, there exists an evolving $(b(j) = \gamma j - j^\beta, g(j) = \gamma j)$-ramp secret-sharing scheme, where the share size of party p_j, for $j \in \mathbb{N}$, is*

$$O\left(j^{4-O(\frac{1}{\log^2(1/\beta)})} \log^2 j\right).$$

For $\beta \geq 1/2$, we prove the following better result.

Theorem 1.2. *Let $\beta > 0$ and $0 < \gamma \leq 1$. There exists an evolving $(\gamma t - t^\beta, \gamma t)$-ramp secret-sharing scheme in which for every $j \in \mathbb{N}$ the share size of p_j is $O(j^{(1-\beta)/\beta} \log j)$.*

As instantiations of Theorem 1.2 we get:

- When $g(j) - b(j) = \frac{j}{\text{polylog}(j)}$, the share size in our scheme is polylog(j) (Theorem 1.2 with $\beta = 1 - \Theta(\frac{\log\log j}{\log j})$).

- When $g(j) - b(j) = \sqrt{j}$, the share size in our scheme is $\tilde{O}(j)$ (Theorem 1.2 with $\beta = 1/2$).

Thus, our constructions offer a significant improvement for a constant β compared to [15], showing that allowing a gap between $g(j)$ and $b(j)$ can reduce the share size in known evolving secret-sharing schemes compared to schemes in which there is no gap (i.e., $g(j) - b(j) = 1$).

In addition, we present a construction of evolving $(k/2, k)$-ramp secret-sharing schemes for a constant k (where any set of parties of size at least k can reconstruct the secret and any set of parties of size at most $k/2$ cannot learn any information about the secret). The share size of the j-th party in our construction is $O(\log k \log j)$. We prove the following theorem:

Theorem 1.3. *For every constant $k \in \mathbb{N}$, there exists an evolving $(k, k/2)$-ramp secret-sharing scheme, where the share size of party p_j, for $j \in \mathbb{N}$, is $O(\log k \log j)$.*

This is an improvement over the evolving k-threshold secret-sharing schemes of [14] in which the share size of the j-th party is $O(k \log j)$. Our result can be either seen as a first step in constructing improved evolving k-threshold secret-sharing schemes or as showing that for constant k evolving $(k/2, k)$-ramp secret-sharing schemes are more efficient.

1.2 Our Techniques

We next describe the ideas of our construction for an evolving $(b(j) = j/2 - j^\beta, g(j) = j/2)$-ramp secret-sharing scheme. We start in Sect. 3 by reducing the problem of realizing an evolving ramp secret-sharing scheme with an infinite number of parties to a problem of constructing secret-sharing realizing access structures with a finite number of parties. Specifically, for a given $t \in \mathbb{N}$, we define an access structure Γ_t containing the parties $\{p_{t^\beta}, \dots, p_{2t}\}$. A set A whose maximal party is p_k should be able to reconstruct the secret in Γ_t if $k > t$ and $|A| \geq k/2 - t^\beta/2$. A set that should not learn any information on the secret in the evolving $(j/2 - j^\beta, j/2)$-ramp secret-sharing scheme, should not get any information on the secret in Γ_t. Given secret-sharing schemes realizing Γ_t, we construct an evolving $(j/2 - j^\beta, j/2)$-ramp secret-sharing scheme by executing a secret-sharing scheme realizing Γ_t for every t that is a power of 2. That is, for every $\ell \in \mathbb{N}$, when party p_{t^β} for $t = 2^\ell$ arrives, we share the secret by a secret-sharing scheme realizing Γ_t with parties $\{p_{t^\beta}, \dots, p_{2t}\}$. When party p_j for $t^\beta \leq j \leq 2t$ arrives, we give p_j the share of p_j in the scheme realizing Γ_t (notice that p_j gets shares in the scheme for Γ_t for many values of t). The correctness of the scheme is explained by the fact that we "lose" at most t^β parties from the beginning; since we allow a gap of at most t^β parties, we will not miss any authorized set.

We present two constructions of secret-sharing schemes realizing the above access structure Γ_t. The first construction, described in Sect. 4, uses the so-called segments technique, where we have a sequence $n_0, n_1, \dots, n_r$ of integers, where $t < n_0 < n_1 < \cdots < n_r \leq 2t$ and we share the secret among the parties $\{p_{t^\beta}, \ldots, p_{n_i}\}$ for every $0 \leq i \leq r$ using a threshold secret-sharing scheme, with an appropriate threshold. We choose the sequence of number of parties and thresholds so the correctness and security hold. This construction yields our best result when $\beta \geq 1/2$. For $\beta = 1/2$ we get an evolving secret-sharing scheme in which the share size of the j-th party is $O(j \log j)$.

Our second construction, described in Sect. 6, uses the so called tree technique (which also uses the segments technique). The tree technique was introduced in [15] (generalizing ideas of [14]). In the tree technique, we construct a tree, where for every edge in the tree we assign a set of consecutive parties and a weight. We define an access structure for this tree, where a set of parties A should be able to reconstruct the secret if there is a path from the root to a leaf such that for every edge in the path whose weight w the set A contains at least w parties from the set of parties assigned to the edge. In [15], an infinite tree is constructed with appropriate sets and weights such that the resulting scheme is an evolving $g(n)$-threshold secret-sharing scheme; in this scheme the share size of the j-th party is $\tilde{O}(j^4)$. Using the fact that we have a gap between b and g and our reduction to finite access structures, we can construct finite trees resulting in more efficient evolving secret-sharing schemes. For example, we optimize our construction for the evolving $(j/2 - j^{1/8}, j/2)$-ramp secret-sharing scheme, resulting in share size $\tilde{O}(j^{2.32})$ for the j-th party. For every $\beta < 1/2$ the share size of the j-th party in our evolving $(t/2 - t^\beta, t/2)$-ramp secret-sharing scheme is $O(j^{4-\frac{1}{\log^2 1/\beta}} \log^2 j)$.

The results in Sect. 4 proves Theorem 1.2 only for a constant $\gamma \leq 1/2$. In Sect. 7, we prove Theorem 1.2 for any constant $\gamma > 0$. This is done by a reduction, where we use an evolving $(j/d - ((j/d\gamma)^\beta - 1), j/d)$-ramp secret-sharing scheme Π for any constant d to construct an evolving $(\gamma j - j^\beta, \gamma j)$-ramp secret-sharing scheme Π'. The reduction is simple, the share of the j-th party in Π' is the share of the $\lfloor \gamma dt \rfloor$-th party in Π. Verifying that the reduction is correct is quite easy (see proof of Theorem 7.1).

In Sect. 8, we construct an evolving $(k/2, k)$-ramp secret-sharing scheme in which the share size of the j-th party is $O(\log k \log j)$. The idea of the construction is as follows. We use the evolving k-threshold secret-sharing scheme of [14] as a building box. The secret-sharing scheme of [14] is recursive and its bottleneck is a procedure that shares k secrets $v_1, \ldots, v_k$ among a set of parties of size j, where each secret v_i is independently shared using an i-out-of-j threshold secret-sharing scheme. Since each sharing results in a share of size $\log j$, the total share of the j-th party is $k \log j$. For the ramp scheme, we use a similar procedure, however we use only $\log k$ threshold secret-sharing schemes, where for every $\ell \in \{0, \ldots, \log k\}$ we share $v_{2^\ell}, \ldots, v_{2^{\ell+1}-1}$ using a 2^ℓ-out-of-j threshold secret-sharing scheme. For the security of the scheme we observe that a set of size $k/2$ obtains less than k shares of the evolving k-threshold secret-sharing scheme, thus learns nothing about the secret. Since sharing k short secrets in a 2^ℓ-out-of-j threshold secret-sharing scheme requires only shares of size $\log j$, the share size in our scheme is $O(\log k \log j)$.

In Sect. 9, we analyze the share size in the schemes $\Pi_{\rm seg}$ and $\Pi_{\rm tree}$ – our schemes from Sect. 4 and Sect. 6 respectively. We prove that for $\beta > 1/2$ the share size in the scheme $\Pi_{\rm seg}$ is better than the share size in every implementation of $\Pi_{\rm tree}$, that is, for $\beta > 1/2$ the best share size achievable using our schemes is $j^{(1-\beta)/\beta}$. Furthermore, we prove a weak lower bound of $\Omega(j)$ on the best share size in $\Pi_{\rm seg}$ and $\Pi_{\rm tree}$ for $\beta \leq 1/2$.

1.3 Previous Works

Secret-sharing schemes were introduced by Shamir [17] and Blakley [3] for threshold access structures, and by Ito, Saito, and Nishizeki for the general case [12]. Shamir's [17] and Blakley's [3] 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-bit secret among n parties is $\max\{\ell, \log n\}$. Kilian and Nisan [13] 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 (see [7]). This lower bound implies that $\Omega(\log n)$ bits are necessary when k is not too close to n. Bogdanov, Guo, and Komargodski [5] 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. Ramp secret-sharing schemes were presented by Blakley and Meadows [4]. For long enough secrets, they constructed a (b, g)-ramp secret-sharing scheme with share size $1/(g-b)$ times the size of the secret. Ramp schemes have found numerous applications in cryptography, including efficient secure multiparty computation (MPC) protocols (Franklin and Yung [11] and many follow-up works), broadcast encryption (Stinson and Wei [18]) and error decodable secret sharing (Martin, Paterson, and Stinson [16]). Cascudo, Cramer, and Xing [7] 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. [5] showed that for all $0 < b < a < 1$, in any ramp secret sharing the size of the shares is at least $\log(a/(a-b))$. On the positive side, Chen et al. [8] 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 and online secret-sharing schemes. D'Arco et al. [10] constructed evolving k-threshold secret-sharing schemes, where the secret is reconstructed only with probability $p < 1$, however the share size is $O(1)$. Komargodski and Paskin-Cherniavsky [15] showed how to transform any evolving secret-sharing scheme to a *robust* scheme, where a shared secret can be recovered even if some parties hand-in incorrect shares. Cachin [6] and Csirmaz and Tardos [9] 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. Our definition is of non-perfect secret-sharing schemes, where some sets of parties can reconstruct the secret, some sets should not get any information on the secret, and there are no requirements on all other sets.

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

Definition 2.2 (Secret-sharing schemes). *A* secret-sharing *$\varSigma = \langle \varPi, \mu \rangle$ 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 $\varPi$ 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 $\varSigma$ by first sampling a random string $r \in R$ according to μ, computing a vector of* shares *$\varPi(k, r) = (s_1, \ldots, s_n)$, and privately communicating each share s_j to party p_j. For a set $A \subseteq \{p_1, \ldots, p_n\}$, we denote $\varPi_A(k, r)$ as the restriction of $\varPi(k, r)$ 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 $\langle \varPi, \mu \rangle$ with domain of secrets K realizes an access structure $\varGamma = (\varGamma_{\mathrm{YES}}, \varGamma_{\mathrm{NO}})$ if the following two requirements hold:

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

Security. *Every unauthorized set cannot learn anything about the secret from its shares. Formally, for any set $T \in \mathit{\Gamma}_{\mathrm{NO}}$, every two secrets $a, b \in K$, and every possible vector of shares $\langle s_j \rangle_{p_j \in T}$,*

$$\Pr[\,\mathit{\Pi}_T(a,r) = \langle s_j \rangle_{p_j \in T}\,] = \Pr[\,\mathit{\Pi}_T(b,r) = \langle s_j \rangle_{p_j \in T}\,],$$

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

Remark 2.3. For sets of parties $A \subseteq \mathcal{P}$ such that $A \notin \mathit{\Gamma}_{\mathrm{YES}} \cup \mathit{\Gamma}_{\mathrm{NO}}$ 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 $\mathit{\Gamma}$ 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, $\mathit{\Gamma}_{\mathrm{YES}} = \{A \subseteq \mathcal{P} : |A| \geq k\}$ and $\mathit{\Gamma}_{\mathrm{NO}} = \{A \subseteq \mathcal{P} : |A| < k\}$.*

The well known scheme of Shamir [17] for the k-out-of-n threshold access structure (based on polynomial interpolation) is an efficient threshold secret-sharing scheme, whose properties are summarized in the following claim.

Claim 2.5 (Shamir [17]). *For every $n \in N$ and $1 \leq k \leq n$, there is a secret-sharing scheme for secrets of size 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 [4]). *Let $0 \leq b < g \leq n$. The* (b, g)-ramp access structure *over a set of parties $\mathcal{P} = \{p_1, \ldots, p_n\}$ is the incomplete access structure $\mathit{\Gamma}_{b,g} = (\mathit{\Gamma}_{\mathrm{YES}}, \mathit{\Gamma}_{\mathrm{NO}})$, where $\mathit{\Gamma}_{\mathrm{YES}} = \{A \subseteq \mathcal{P} : |A| \geq g\}$ and $\mathit{\Gamma}_{\mathrm{NO}} = \{A \subseteq \mathcal{P} : |A| \leq b\}$. A* (b, g)-ramp scheme *with n parties is a secret-sharing scheme realizing $\mathit{\Gamma}_{b,g}$.*

Chen et al. [8] showed the existence of ramp secret-sharing schemes with share size $O(1)$.

Claim 2.7 (Chen et al. [8]). *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 $((1/2 - \epsilon)n, (1/2 + \epsilon)n)$-ramp secret-sharing scheme with n parties and share size ℓ.*

The next corollary, which can be found in [1], shows the existence of ramp secret-sharing schemes for any gap of $\mathit{\Theta}(n)$.

Corollary 2.8. *For every constants $0 < b < g < 1$ there are integers ℓ and n_0 such that for every $n \geq n_0$ there is a (b, g)-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 [14].

Definition 2.9. (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 $\Gamma^t \triangleq (\Gamma_{\text{YES}} \cap 2^{\{p_1,\dots,p_t\}}, \Gamma_{\text{NO}} \cap 2^{\{p_1,\dots,p_t\}})$ is an access structure as defined in Definition 2.1.*

Definition 2.10. (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 $\Pi_t(k, (r_1, \dots, r_k)) = \langle \Pi^1(k, r_1), \dots, \Pi^t(k, r_1, \dots, r_t) \rangle$, is a secret-sharing scheme realizing Γ^t according to Definition 2.2.

Definition 2.11. (Evolving ramp access structures). *For two non-decreasing functions $b, g : \mathbb{N} \to \mathbb{N}$ such that $0 \leq b(t) < g(t) \leq t$ for every $t \in \mathbb{N}$, the evolving $(b(t), g(t))$-ramp incomplete access structure is the evolving incomplete access structure $\Gamma_{b(t),g(t)}$, where for a set A whose maximum party is p_t:*

- *A is authorized if $|A \cap \{p_1, \dots, p_j\}| \geq g(j)$ for some $1 \leq j \leq t$,*
- *A is unauthorized if $|A \cap \{p_1, \dots, p_j\}| \leq b(j)$ for every $1 \leq j \leq t$.*

In other words, A is authorized in $\Gamma_{b(t),g(t)}$ if it is authorized in the $(b(j), g(j))$-ramp incomplete access structure for some $j \leq t$ and it is unauthorized in $\Gamma_{b(t),g(t)}$ if it is unauthorized in the $(b(j), g(j))$-ramp incomplete access structure for every $j \leq t$. In the above definition, there are no requirements on sets where $|A \cap \{p_1, \dots, p_j\}| < g(j)$ for every j and $|A \cap \{p_1, \dots, p_j\}| > b(j)$ for at least one j. We abuse notation and consider $g, b : \mathbb{N} \to \mathbb{R}$ (e.g., $g(t) = t/2$); in this case, we actually consider $\lceil g(t) \rceil$ and $\lfloor b(t) \rfloor$.

In the rest of the paper, the secret is taken from $\{0, 1\}$.

3 Reduction to an Access Structure with a Finite Number of Parties

Our goal is to construct an evolving $(\gamma t - f(t), \gamma t)$-ramp secret-sharing scheme for any constant $0 < \gamma < 1$ and some function $0 < f(t) \leq \gamma t$ such that $\gamma t - f(t)$ is non-decreasing. We show that to construct a ramp evolving secret-sharing scheme (with an unbounded number of parties) it suffices to construct a secret-sharing scheme for an access structure $\Gamma^f_{t,\rho,\gamma}$ with a finite number of parties.

The ramp evolving secret-sharing schemes we construct will use many copies of a scheme realizing $\Gamma^{f}_{t,\rho,\gamma}$ (for every t that is a power of 2). In the definition of $\Gamma^{f}_{t,\rho,\gamma}$, there is a parameter $0 < \rho \leq 1$. This parameter adds flexibility to our reductions and we use different values of ρ in our two constructions.

Definition 3.1. (The access structure $\Gamma^{f}_{t,\rho,\gamma}$). *Let $0 < \gamma < 1$ be a constant and $f : \mathbb{N} \to \mathbb{N}$ be a function such that $0 < f(j) < \gamma j$ for every $j \in \mathbb{N}$ and $\gamma t - f(t)$ is non-decreasing, let t be an integer, and let $0 < \rho \leq 1$. The incomplete access structure $\Gamma^{f}_{t,\rho,\gamma}$ over the set of parties $\{p_{\rho \cdot f(t)}, p_{\rho \cdot f(t)+1}, \dots, p_{2t}\}$ is the following access structure, where for a set $A = \{p_{i_1}, \dots, p_{i_k}\} \subseteq \{p_{\rho \cdot f(t)}, \dots, p_{2t}\}$:*

- *if $i_j > t$ and $j \geq \gamma i_j - \gamma\rho \cdot f(t)$ for some $j \in [k]$, then A is authorized.*
- *If $j \leq \gamma i_j - f(i_j)$ for every $j \in [k]$, then A is unauthorized.*

Example 3.2. Consider the function $f(t) = \sqrt{t}$ and the access structure $\Gamma^{\sqrt{j}}_{t,1,1/2}$ whose parties are $\{p_{\sqrt{t}}, \dots, p_{2t}\}$. Next we show examples of authorized and unauthorized subsets. The subset $A = \{p_{(t+\sqrt{t}+3)/2}, \dots, p_{t+1}\}$ is authorized since it contains $(t+1)/2 - \sqrt{t}/2$ parties. The subset $B = \{p_{3t/2+1}, \dots, p_{2t}\}$ is unauthorized for $t > 32$ since for every p_{i_j} in the set it holds that $i_j/2 - \sqrt{i_j} > 3t/4 - \sqrt{2t} \geq t/2 \geq j$. Notice that the unauthorized set B is bigger than the authorized set A. Such sets imply that realizing $\Gamma^{f}_{t,\rho,\gamma}$ is non-trivial.

Theorem 3.3. *Let $0 < \rho \leq 1$. If for every t there is a secret-sharing scheme $\Pi^{f}_{t,\rho,\gamma}$ realizing the access structure $\Gamma^{f}_{t,\rho,\gamma}$, where, for $\rho \cdot f(t) \leq j \leq t$, the size of the share of party p_j is $c_t(j)$, then the scheme $\Pi_{reduction}$, described in Fig. 1, realizes the evolving access structure $\Gamma_{\gamma t - f(t), \gamma t}$, where the size of the share of p_j is $\sum_{t\,:\,\exists_{i \in \mathbb{N}} t = 2^i \wedge \rho \cdot f(t) \leq j \leq 2t} c_t(j)$.*

The Scheme $\Pi_{\text{reduction}}$

- For every $\ell \in \mathbb{N}$ do:
  - Let $t = 2^{\ell}$
  - When party $p_{\rho \cdot f(t)}$ arrives, prepare the shares of $\Pi^{f}_{t,\rho,\gamma}$, denote these shares by $s_{t,\rho \cdot f(t)}, \dots, s_{t,2t}$.
- The share of party p_j is $(s_{t,j})_{\{\,t\,:\,\exists_{i \in \mathbb{N}} t = 2^i \wedge \rho \cdot f(t) \leq j \leq 2t\,\}}$.

Fig. 1. The scheme $\Pi_{\text{reduction}}$ that realizes the evolving ramp access structure $\Gamma_{\gamma t - f(t), \gamma t}$, assuming a scheme $\Pi^{f}_{t,\rho,\gamma}$ realizing $\Gamma^{f}_{t,\rho,\gamma}$.

Proof. We first prove the correctness of the scheme $\Pi_{\text{reduction}}$. Consider a minimal authorized set $A = \{p_{i_1}, \dots, p_{i_k}\}$ of $\Gamma_{\gamma t - f(t), \gamma t}$, thus, $k \geq \gamma i_k$. Let $\ell \in \mathbb{N}$ be the index such that $2^{\ell} < i_k \leq 2^{\ell+1}$ and let $t = 2^{\ell}$, thus, $t < i_k \leq 2t$.

As A is a minimal authorized set, it contains less than $\gamma\rho \cdot f(t)$ parties among the parties $\{p_1, \dots, p_{\rho \cdot f(t)-1}\}$, i.e., it contains at least $\gamma i_k - \gamma\rho \cdot f(t)$ parties from $\{p_{\rho \cdot f(t)}, \dots, p_{2t}\}$. This implies that A is authorized in $\Gamma^f_{t,\rho,\gamma}$ and the parties in A can reconstruct the secret from their shares in $\Pi^f_{t,\rho,\gamma}$.

We now prove the security of the scheme. Consider a set A that is unauthorized in $\Gamma_{\gamma t - f(t),\gamma t}$. By definition, it is unauthorized in all $\Gamma^f_{t,\rho,\gamma}$, thus, the parties in A have no information on the secret.

The share of p_j contains shares of $\Pi^f_{t,\rho,\gamma}$ for every value t such that t is a power of 2 and $\rho \cdot f(t) \leq j \leq 2t$, that is, the size of p_j's share is

$$\sum_{t\,:\,\exists_{i \in \mathbb{N}} t = 2^i \wedge \rho \cdot f(t) \leq j \leq 2t} c_t(j).$$

□

For the case that $f(t) = t^\beta$ for some $0 < \beta < 1$, the reduction in Theorem 3.3 yields the following result.

Corollary 3.4. *Let $0 < \beta < 1$ be a constant and $c : \mathbb{N} \to \mathbb{N}$ be a function. If for every t there exists a scheme realizing $\Gamma^{f(t)=t^\beta}_{t,\rho,\gamma}$ where the size of the share of each party p_j, for $\rho t^\beta < j \leq 2t$, is $c(j)$, then there exists a scheme realizing $\Gamma_{\gamma t - t^\beta,\gamma t}$ in which the size of the share of each party p_j, for $j \in \mathbb{N}$, is $c(j)\log j$.*

Our main challenge in Sects. 4 to 6 is to construct efficient schemes realizing the access structure $\Gamma^f_{t,\rho,\gamma}$ for some parameter ρ.

Example 3.5. Consider the evolving $(t/4, t/2)$-ramp access structure, i.e., $f(t) = t/4$. In this case, $\Gamma^{f(t)=t/4}_{t,1,1/2}$ is an access structure over the parties $\{p_{t/4}, \dots, p_{2t}\}$. A first attempt to realize $\Gamma^{f(t)=t/4}_{t,1,1/2}$ is to use one threshold secret-sharing scheme. This attempt fails since the set $\{p_{5t/8+1}, \dots, p_{t+1}\}$ is an authorized set of size $\approx 3t/8$, while $\{p_{3t/2}, \dots, p_{2t}\}$ is an unauthorized set of size $2t/4 = t/2$. To solve this problem, we use 4 threshold schemes. That is, to realize $\Gamma^{f(t)=t/4}_{t,1,1/2}$, for every $\alpha = 1, 2, 3, 4$, we share the secret s using a $(2+\alpha)t/8$-out-of-$(4+\alpha-1)t/4$ among the parties $\{p_{t/4}, \dots, p_{t+\alpha t/4}\}$. In the next two paragraphs we prove that this scheme realizes $\Gamma^{f(t)=t/4}_{t,1,1/2}$.

Consider a minimal authorized set $A = \{p_{i_1}, \dots, p_{i_k}\}$ of $\Gamma^{f(t)=t/4}_{t,1,1/2}$ and let α be such that $t + (\alpha-1)t/4 < i_k \leq t + \alpha t/4$. This set contains at least $i_k/2 - t/8 \geq (1 + (\alpha-1)/4)t/2 - t/8 = (2+\alpha)t/8$ parties from the set $\{p_{t/4}, \dots, p_{t+\alpha t/4}\}$, thus it can reconstruct the secret.

Consider an unauthorized set A of $\Gamma^{f(t)=t/4}_{t,1,1/2}$. For every $\alpha = 1, 2, 3, 4$, it contains at most $(1+\alpha/4)t/4$ parties among the parties $\{p_{t/4}, \dots, p_{t+\alpha t/4}\}$ (as such set contains at most a quarter of the parties ending at party $(1+\alpha/4)t$). Since $(1+\alpha/4)t/4 < (2+\alpha)t/8$, the parties in A cannot learn any information on the secret from each of the 4 schemes, thus, cannot learn any information on the secret.

The size of the share of party p_j in this scheme for $\Gamma^{f(t)=t/4}_{t,1,1/2}$ is $O(\log t) = O(\log j)$ (as this is the share size in Shamir's scheme). If instead of sharing the secret using a threshold secret-sharing scheme, we share the secret using a (non-evolving) $((1+\alpha/4)t/4, (2+\alpha)t/8)$-ramp secret-sharing scheme, the size of the share will be reduced to $O(1)$, by [8] (see Corollary 2.8). By Theorem 3.3, the size of the share of p_j in the evolving scheme realizing $\Gamma_{t/4,t/2}$ is the sum of the shares in the schemes realizing $\Gamma^{f(t)=t/4}_{t,1,1/2}$, where t is a power of two such that $t/4 < j < 2t$. Thus, the share size of p_j is $O(1)$.

4 First Scheme Realizing $\Gamma^{f(t)}_{t,1,\gamma}$: The Segments Technique

In this section we construct a simple scheme Π_{seg} realizing $\Gamma^{f}_{t,1,\gamma}$ for $0 < \gamma \leq 1/2$, proving Theorem 1.2 for $0 < \gamma \leq 1/2$. We analyze the share size of the evolving ramp scheme resulting by using Π_{seg} in $\Pi_{\text{reduction}}$ for a function $f(t) = t^{\beta}$ for some $\beta < 1$. For $\beta \geq 1/2$ this is our best scheme. For smaller values of β, the scheme presented in Sect. 6 is more efficient.

The scheme Π_{seg} is a generalization of the scheme presented in Example 3.5; we realize $\Gamma^{f}_{t,1,\gamma}$ using several threshold secret-sharing schemes on increasing segments of parties, where for larger segments we use larger thresholds. The scheme is described in Fig. 2.

The Scheme Π_{seg}

- For $\alpha = 1$ to $\lceil t/f(t) \rceil$,
  - Share s using Shamir's $(\lfloor \gamma(t+(\alpha-2)f(t)) \rfloor + 1)$-out-of-$(t+(\alpha-1)f(t))$ secret-sharing scheme among the parties $\{p_{f(t)}, \ldots, p_{t+\alpha f(t)}\}$; let $s_{\alpha,f(t)}, s_{\alpha,f(t)+1}, \ldots, s_{\alpha,t+\alpha f(t)}$ be the shares in this scheme.
- The share of p_j is $(s_{\alpha,j})_{\{\alpha:\alpha \geq \max\{1,(j-t)/f(t)\}\}}$.

Fig. 2. A scheme Π_{seg} realizing the access structure $\Gamma^{f}_{t,1,\gamma}$.

Lemma 4.1. *Let $0 < \gamma \leq 1/2$. The secret-sharing scheme Π_{seg}, described in Fig. 2, realizes the access structure $\Gamma^{f}_{t,1,\gamma}$ with share size $O(t/f(t)\log t)$.*

Proof. We start by proving the correctness of the scheme Π_{seg}. Consider a minimal authorized set $A = \{p_{i_1}, p_{i_2}, \ldots, p_{i_k}\}$ of $\Gamma^{f}_{t,1,\gamma}$ and let α be such that $t+(\alpha-1)f(t) < i_k \leq t+\alpha f(t)$. Since A is a minimal authorized set,

$$|A| = k \geq \gamma i_k - \gamma f(t) > \gamma(t+(\alpha-1)f(t)) - \gamma f(t) = \gamma(t+(\alpha-2)f(t)).$$

Since $|A|$ is an integer,

$$|A| \geq \lfloor \gamma(t + (\alpha - 2)f(t)) \rfloor + 1.$$

By the construction, the parties in A can reconstruct the secret from the threshold scheme for the parties $\{p_{f(t)}, \dots, p_{t+\alpha f(t)}\}$.

We continue by proving the security of the scheme. Consider an unauthorized set A. We show that for every α, the parties in A cannot learn any information about the secret from the threshold scheme for $\{p_{f(t)}, \dots, p_{t+\alpha f(t)}\}$. Note that $f(t + \alpha f(t)) \geq f(t) \geq 2\gamma f(t)$. Since A is unauthorized, the number of parties in $A \cap \{p_{f(t)}, \dots, p_{t+\alpha f(t)}\}$ is at most

$$\gamma(t + \alpha f(t)) - f(t + \alpha f(t)) \leq \gamma(t + \alpha f(t)) - 2\gamma f(t) = \gamma(t + (\alpha - 2)f(t)).$$

Thus, the parties in A cannot learn any information about the secret from the shares of each threshold scheme. As these schemes are executed with independent randomness, the parties in A cannot learn any information about the secret.

Finally, we analyze the share size of each party in the scheme. Each party gets at most $O(t/f(t))$ shares of Shamir's secret-sharing scheme with $O(t)$ parties; the size of each such share is $O(\log t)$. Thus, the total share size is $O(t/f(t) \log t)$. □

We next present two conclusions of Lemma 4.1.

Theorem 4.2. *For every constants $0 < \delta < \gamma \leq 1/2$, the evolving $(\delta t, \gamma t)$-ramp access structure can be realized by an evolving secret-sharing scheme with share size $O(1)$ for every party.*

Proof. Let $b = \gamma - \delta$. In this case $f(t) = bt$ and $\Gamma_{t,1,\gamma}^{f(t)=bt}$ is an access structure whose parties are $\{p_{bt}, \dots, p_{2t}\}$. By Lemma 4.1, Π_{seg} realizes $\Gamma_{t,1,\gamma}^{f(t)=bt}$ with share size $O(\log t)$ (since b is constant). We next show how to reduce the share size to $O(1)$. By the construction, the secret is shared among the parties $\{p_{bt}, \dots, p_{t+bt\alpha}\}$ for every $\alpha = 1$ to $\lceil 1/b \rceil$ by a $(\lfloor \gamma t(1 + b\alpha - 2b) \rfloor + 1)$-out-of-$(t + (\alpha - 1)bt)$ threshold secret-sharing scheme. However, in an unauthorized set there are at most $\delta(t + bt\alpha) = (\gamma - b)(t + bt\alpha) = \gamma t(1 + b\alpha - b/\gamma - b^2\alpha/\gamma) < \gamma t(1 + b\alpha - 2b)$ parties. Therefore, we can share the secret by a $(\gamma t(1 + b\alpha - b/\gamma - b^2\alpha/\gamma), \gamma t(1 + b\alpha - 2b) + 1)$-ramp secret-sharing scheme. By Corollary 2.8, we realize $\Gamma_{t,1,\gamma}^{f(t)=bt}$ with share size $O(1)$ for every party. By Theorem 3.3, the size of the share of p_j in the evolving scheme realizing $\Gamma_{\delta t,\gamma t}$ is the sum of the shares in the schemes realizing $\Gamma_{t,1,\gamma}^{f(t)=bt}$, where t is a power of two such that $\delta t < j < 2t$. There are $O(1)$ schemes. Thus, the share size of p_j is $O(1)$. □

The same result was proved in [1]. However, the analysis of the new scheme is much simpler than the one in [1]. We next prove Theorem 1.2 for $\gamma \leq 1/2$ (the case of $1/2 < \gamma \leq 1$ is obtained from the following lemma in Sect. 7).

Lemma 4.3. *For every $\beta > 0$ and $0 < \gamma \leq 1/2$, there exists an evolving $(\gamma t - t^{\beta}, \gamma t)$-ramp secret-sharing scheme in which for every $j \in \mathbb{N}$ the share size of p_j is $O(j^{(1-\beta)/\beta} \log j)$.*

Proof. Consider the scheme $\Pi_{\text{reduction}}$ with Π_{seg} as the scheme realizing $\Gamma_{t,1,\gamma}^{f(t)=t^{\beta}}$. By Lemma 4.1, the scheme Π_{seg} realizes $\Gamma_{t,1,\gamma}^{f(t)=t^{\beta}}$, where the share size of p_j is $c_t(j) = O(t^{1-\beta} \log t)$. Thus, by Theorem 3.3, $\Pi_{\text{reduction}}$ realizes the evolving ramp access structure $\Gamma_{\gamma t - t^{\beta}, \gamma t}$, where the share size of the party p_j is

$$\sum_{t\,:\,\exists_{i \in \mathbb{N}} t=2^i \wedge t^{\beta} \leq j \leq 2t} c_t(j) = \sum_{t\,:\,\exists_{i \in \mathbb{N}} t=2^i \wedge j/2 \leq t \leq j^{1/\beta}} c_t(j).$$

The largest value of t in the above sum is $j^{1/\beta}$ and $c_{j^{1/\beta}}(j) = O(j^{(1-\beta)/\beta} \log j)$; the second largest value of t in the above sum is $j^{1/\beta}/2$ and $c_{j^{1/\beta}/2}(j) = O(j^{(1-\beta)/\beta}/2^{1-\beta} \log j)$ and so on. Thus, the share size of p_j is a sum of a geometric sequence and is $O(j^{(1-\beta)/\beta} \log j)$. □

5 Realizing Weighted Trees Access Structures

In this section, we review and generalize the tree technique introduced in [15] (generalizing ideas of [14]) in order to construct a scheme for the evolving majority access structure.

Next we overview and generalize the tree technique. In Sect. 6, we construct a specific tree that we use in our constructions.

5.1 A Secret Sharing Scheme Realizing Finite Trees

In this section, we define a complete access structure from a tree and show how to realize it. This scheme is a special case of the scheme realizing the connectivity access structure [2].

For a directed tree $T = (V, E)$, we define the following access structure. The edges in the tree represent the parties in the access structure. A set of edges is authorized if it contains a path from the root to a leaf, otherwise it is an unauthorized and should not learn any information on the secret.

We next describe a simple scheme Π_{T} realizing this tree. Let $k \in \{0, 1\}$ be the secret. The share of each edge (u, v) is a bit $r_{u,v}$ computed as follows: if v is not a leaf, then it is a uniformly distributed random bit. Otherwise, if v is a leaf and $P = (v_0, v_1, \ldots, v_{n-1} = u, v_n = v)$ is the path from the root to v, then $r_{u,v} = \oplus_{i=0}^{n-2} r_{v_i, v_{i+1}} \oplus k$. To see that this scheme is correct, observe that the edges on a path can reconstruct the secret by computing the exclusive-or of the shares given to the parties (edges) of the path.

To see that this scheme is secure consider an unauthorized set, that is, a set of edges F not containing a path from s to a leaf. Define the set of nodes V_1 such that $v_i \in V_1$ if there exists a path from the root to v_i in (V, F). By definition,

$s \in V_1$ and V_1 does not contain leaves. Furthermore, for every $(v_i, v_j) \in F$ either both nodes v_i, v_j are in V_1 or both of them are not in V_1. Let $\{r_{i,j}\}_{(v_i,v_j)\in F}$ be a set of shares generated for the parties in F with a secret $k \in \{0,1\}$, where $r_{i,j}$ is the share given to party (v_i, v_j). We next show that the same set of shares can be used to share the secret $k \oplus 1$. Complete the shares $\{r_{i,j}\}_{(v_i,v_j)\in F}$ of the parties in F to shares $\{r_{i,j}\}_{(v_i,v_j)\in E}$ of all the parties in the tree for the secret k. Consider the shares $r'_{i,j}$ such that $r'_{i,j} = r_{i,j} \oplus 1$ if $v_i \in V_1$ and $v_j \notin V_1$ and $r'_{i,j} = r_{i,j}$ otherwise. Notice that $r'_{i,j} = r_{i,j}$ for every $(v_i, v_j) \in F$. We claim that the shares $\{r'_{i,j}\}_{(v_i,v_j)\in E}$ are shares for the secret $k \oplus 1$. This is true since for any simple path $s = v_0, v_1, \ldots, v_{n-1}, v_n = v$ from the root to a leaf contains exactly one edge (v_i, v_{i+1}) such that $v_i \in V_1$ and $v_{i+1} \notin V_1$ and the exclusive or of the shares given to the parties (edges) on the path is $k \oplus 1$. As we describe a bijection between the shares of k and $k \oplus 1$, the probabilities of $\{r_{i,j}\}_{(v_i,v_j)\in F}$ given k and $k \oplus 1$ are equal, thus the security holds.

5.2 Secret-Sharing Schemes Realizing Finite Weighted Trees

Following [15], we describe an access structure for a finite directed weighted tree $T = (V, E)$, where each edge (u, v) has weight $w_{u,v}$. In addition, for each edge we assign a set of parties; informally, any set of at least $w_{u,v}$ parties among the parties assigned to an edge can reconstruct "the bit of the edge".

We remark that the tree used in [15] is infinite. However, since we allow a gap between the sizes of authorized and unauthorized sets, we can use a scheme realizing a finite tree.

Terminology: We use the following notations in our constructions.

- The i-th layer of the tree contains nodes of distance exactly i from the root.
- A node in the i-th layer is identified by the sequence of weights assigned to the edges along the path from the root to that node; the node is denoted by $u_{w_1,w_2,\ldots,w_i}$, where $w_1, \ldots, w_i$ are the weights of the edges from the root to the node. That is, the root is u_ϵ and for every nodes $u_{w_1,w_2,\ldots,w_{i-1}}$ and $u_{w_1,w_2,\ldots,w_{i-1},w_i}$ in the $(i-1)$-th and i-th layers respectively there is an edge with weight w_i connecting them. We assume that for every node in the tree the weights of its outgoing edges are distinct, thus, the notation $u_{w_1,\ldots,w_i}$ uniquely identifies a node.
- We assign parties to each edge of the tree. That is, we consider a function $q : V \to \mathbb{N}$ such that $q(u_\epsilon)$ is the index of the first party in the scheme and for every $(u, v) \in E$ it holds that $q(v) > q(u)$, the parties $\{p_{q(u)+1}, \ldots, p_{q(v)}\}$ are assigned to the edge (u, v).

Definition 5.1. *Given a finite weighted tree $T = (V, E)$ with a weight function $w : E \to \mathbb{N}$ and a function $q : V \to \mathbb{N}$, let $u_{\max} = \max_{v\in V}\{q(v)\}$. We define the complete access structure $\Gamma_{T,w,q}$ with parties $\{p_{q(u_\epsilon)}, \ldots, p_{q(u_{\max})}\}$, where a set A is authorized in the access structure if and only if there exists a leaf $u_{w_1,\ldots,w_i}$ in the tree and a path*

$$(u_\epsilon, u_{w_1}), (u_{w_1}, u_{w_1,w_2}), \ldots, (u_{w_1,\ldots,w_{i-1}}, u_{w_1,\ldots,w_i})$$

such that $|A \cap \{p_{q(u_{w_1,\ldots,w_{j-1}})+1}, \ldots, p_{q(u_{w_1,\ldots,w_j})}\}| \geq w_j$ for every $1 \leq j \leq i$.

Given a finite weighted tree T, we construct a secret-sharing scheme, denoted by Π_{wt}, realizing $\Gamma_{T,w,q}$. We next informally describe Π_{wt}: we first share the secret using the scheme of Sect. 5.1. Then for every edge (u,v) we share the bit given to (u,v) by a threshold secret-sharing scheme among the parties assigned to the edge; the threshold used is the weight of the edge. The formal description of Π_{wt} appears in Fig. 3.

The Scheme Π_{wt}

– Run Π_{T} on the tree T. Denote the share given to an edge (u,v) by $r_{u,v}$, where if $w(e)=0$ then $r_e=0$ (instead of a random bit).
– For every edge $(v_{w_1,w_2,\ldots,w_{i-1}}, v_{w_1,w_2,\ldots,w_{i-1},w_i})$ such that $w_i > 0$, share the bit $r_{v_{w_1,w_2,\ldots,w_{i-1}},v_{w_1,w_2,\ldots,w_{i-1},w_i}}$ among the parties $\{p_{q(v_{w_1,w_2,\ldots,w_{i-1}})+1},\ldots,p_{q(v_{w_1,w_2,\ldots,w_{i-1},w_i})}\}$ by a w_i-out-of-$\big(q(v_{w_1,w_2,\ldots,w_{i-1},w_i}) - q(v_{w_1,w_2,\ldots,w_{i-1}})\big)$ threshold secret-sharing scheme.

Fig. 3. The scheme Π_{wt} that realizes the access structure $\Gamma_{T,w,q}$.

Lemma 5.2. *The scheme Π_{wt} realizes $\Gamma_{T,w,q}$.*

Proof. Since we share the secret using Π_{T}, a set A can reconstruct the secret iff it can reconstruct the bits $r_{v_\epsilon,v_1}, r_{v_1,v_2},\ldots,r_{v_{c-1},v_c}$ for some path $(v_\epsilon,\ldots,v_c)$ from the root to a leaf. Let $w_1,\ldots,w_c$ be the weights of the edges on this path. The bit r_{v_{j-1},v_j} is shared by a w_j-out-of-$(q(v_j)-q(v_{j-1}))$ threshold secret-sharing scheme among the parties $\{p_{q(v_{j-1})+1},\ldots,p_{q(v_j)}\}$ and A can learn the bit r_{v_{j-1},v_j} if and only if $|A \cap \{p_{q(v_{j-1})+1},\ldots,p_{q(v_j)}\}| \geq w_j$. □

6 The Second Scheme Realizing $\Gamma^f_{t,1/2,\gamma}$: The Tree Technique

In this section, we prove Theorem 1.1. We show how to use the secret sharing for weighted trees described in Sect. 5 to realize $\Gamma^f_{t,1/2,\gamma}$, thus, to construct evolving ramp secret-sharing schemes. Our scheme Π_{tree} can be used for arbitrary functions $f(t)$, however to simplify the analysis of the share size, we only consider functions $f(t)=t^\beta$ for some constant $0<\beta<1$. In Fig. 4, we define a weighted tree T_{ramp}. The tree contains $n+1$ layers for some constant n. The first n layers partition the parties $p_{f(t)/2},\ldots,p_{t^\alpha}$ (for some $\alpha \leq 1$ as will be defined later) to n sets of consecutive parties, and the parties corresponding to edges from the $(i-1)$-th layer to the i-th layer are the parties from the i-th set. The $(n+1)$-th layer adds, for every node of layer n, edges as in the segment construction in Sect. 4 for the set of parties $p_{t^\alpha+1},\ldots,p_{2t}$. We construct a scheme Π_{tree}:

– Execute Π_{wt} on T_{ramp}.

1. Parameters:
   - n: the number of layers in the tree (to be fixed later).
   - $q_0, q_1, q_2, \ldots, q_n$: $q_0 = \frac{f(t)}{2}$, $q_n \leq t, q_{n+1} = 2t$, where $q_1, q_2, \ldots, q_n$ will be chosen later.
   - Let $d_i = t + if(t)$ for $0 \leq i < \frac{t}{f(t)}$; $m = \lceil \frac{t}{f(t)} \rceil$ and $d_m = 2t$.
   - Let $W_i = \{0, \frac{\gamma f(t)}{2n}, \frac{2\gamma f(t)}{2n}, \ldots, \lfloor \frac{2nq_i}{\gamma f(t)} \rfloor \cdot \frac{\gamma f(t)}{2n}\}$ for $0 \leq i \leq n$.
2. Layer V_0 contains the root u_ϵ with $q(u_\epsilon) = q_0$.
3. For every $1 \leq i \leq n$, for each $u_{w_1,w_2,\ldots,w_{i-1}} \in V_{i-1}$ and $w_i \in W_i \cup \{\sum_{j=1}^{i-1} w_j\}$ such that $w_i \geq \sum_{j=1}^{i-1} w_j$, add the node $u_{w_1,w_2,\ldots,w_{i-1},w_i-\sum_{j=1}^{i-1} w_j}$ in layer V_i, add the edge $(u_{w_1,w_2,\ldots,w_{i-1}}, u_{w_1,w_2,\ldots,w_{i-1},w_i-\sum_{j=1}^{i-1} w_j})$ (with weight $w_i - \sum_{j=1}^{i-1} w_j$), and define $q(u_{w_1,\ldots,w_{i-1},w_i}) = q_i$.
4. Add an additional layer V_{n+1}: For every $0 \leq i \leq \frac{t}{f(t)}$, for every $u_{w_1,w_2,\ldots,w_n} \in V_n$, add the node $u_{w_1,w_2,\ldots,w_n,w}$ to V_{n+1}, where $w = \lceil \gamma d_i - \sum_{i=1}^{n} w_i - \gamma f(t) \rceil$, add the edge $(u_{w_1,w_2,\ldots,w_n}, u_{w_1,w_2,\ldots,w_n,w})$, and define $q(u_{w_1,w_2,\ldots,w_n,w}) = d_{i+1}$.

Fig. 4. The weighted tree T_{ramp} used for realizing $\Gamma^f_{t,1/2,\gamma}$.

Lemma 6.1. *Let f be a function such that $f(t+f(t)) > f(t)$. The scheme Π_{tree} realizes the access structure $\Gamma^f_{t,1/2,\gamma}$.*

Proof. We start by proving the correctness of the scheme, that is, if $A = \{p_{i_1}, p_{i_2}, \ldots, p_{i_k}\}$ such that $t < i_k \leq 2t$ and $k \geq \gamma i_k - \frac{\gamma f(t)}{2}$, then A can reconstruct the secret. By Lemma 5.2, we need to prove that there is a path from the root to a leaf $u_{w_1,\ldots,w_{n+1}}$ such that

$$|A \cap \{p_{q(u_{w_1,\ldots,w_{i-1}})+1}, \ldots, p_{q(u_{w_1,\ldots,w_i})}\}| \geq w_i \tag{1}$$

for every $1 \leq i \leq n+1$. Let $z_i = |A \cap \{p_{q_{i-1}+1}, \ldots, p_{q_i}\}|$ for $1 \leq i \leq n$. We define the weights inductively. Assume that we defined $w_1, \ldots, w_{i-1}$ such that (1) holds for them. Let $w_i = \max\{w - \sum_{j=1}^{i-1} w_j : w \in W_i, w \leq \sum_{j=1}^{i-1} w_j + z_i\}$. By the construction of W_i, $w_i \geq z_i - \frac{\gamma}{2n} f(t)$. The path from the root to $u_{w_1,\ldots,w_n}$ satisfies (1) for every $1 \leq i \leq n$ and

$$\sum_{i=1}^{n} w_i \geq |A \cap \{p_{f(t)/2}, \ldots, p_{t^{\alpha_n}}\}| - \frac{\gamma f(t)}{2}. \tag{2}$$

Let j be the index such that $d_j < i_k \leq d_j + f(t)$ and let $w_{n+1} = \lceil \gamma d_j - \sum_{i=1}^{n} w_i - \gamma f(t) \rceil$. By the construction of T_{ramp} there is an edge between $u_{w_1,\ldots,w_n}$ and $u_{w_1,\ldots,w_n,w_{n+1}}$. To complete the proof of the correctness, we need to show that $|A \cap \{p_{t^{\alpha_n}+1}, \ldots, p_{d_j+f(t)}\}| \geq w_{n+1}$:

$$\begin{aligned}|A \cap \{p_{t^{\alpha_n}+1}, \ldots, p_{d_j+f(t)}\}| &= |A| - |A \cap \{p_{f(t)/2}, \ldots, p_{t^{\alpha_n}}\}| \\ &\geq \gamma i_k - \frac{\gamma f(t)}{2} - \left(\sum_{i=1}^{n} w_i + \frac{\gamma f(t)}{2} \right) \\ &\geq \gamma d_j - \sum_{i=1}^{n} w_i - \gamma f(t).\end{aligned}$$

Since $|A \cap \{p_{t^{\alpha_n}+1}, \ldots, p_{d_j+f(t)}\}|$ is an integer, $|A \cap \{p_{t^{\alpha_n}+1}, \ldots, p_{d_j+f(t)}\}| \geq \lceil \gamma d_j - \sum_{i=1}^{n} w_i - \gamma f(t) \rceil = w_{n+1}$.

We next prove the security of the scheme. Let A be an unauthorized set of $\Gamma^{f}_{t,1/2,\gamma}$. By Lemma 5.2, we need to prove that there is no path from the root to a leaf $u_{w_1,\ldots,w_{n+1}}$ such that

$$|A \cap \{p_{q_{w_1,\ldots,w_{i-1}}+1}, \ldots, p_{q_{w_1,\ldots,w_i}}\}| \geq w_i$$

for every $i = 1, \ldots, n+1$. Fix such a leaf $u_{w_1,\ldots,w_{n+1}}$ and let j be the index such that $w_{n+1} = \lceil \gamma d_j - \sum_{i=1}^{n} w_i - \gamma f(t) \rceil$ and $q(u_{w_1,\ldots,w_{n+1}}) = d_{j+1}$. Since A is unauthorized,

$$|A \cap \{p_{f(t)/2}, \ldots, p_{d_{j+1}}\}| \leq \gamma d_{j+1} - f(d_{j+1}) < \gamma d_{j+1} - f(t), \qquad (3)$$

where the last inequality is implied by the assumption that $f(t + (j+1)f(t)) \geq f(t + f(t)) > f(t)$ for every t. If $|A \cap \{p_{q_{w_1,\ldots,w_{i-1}}+1}, \ldots, p_{q_{w_1,\ldots,w_i}}\}| < w_i$ for some $i = 1, \ldots, n$, then we are done. Otherwise,

$$\begin{aligned}|A \cap \{p_{t^{\alpha_n}+1}, \ldots, p_{d_{j+1}}\}| &= |A \cap \{p_{f(t)/2}, \ldots, p_{d_{j+1}}\}| - |A \cap \{p_{f(t)/2}, \ldots, p_{t^{\alpha_n}}\}| \\ &< (\gamma d_{j+1} - f(t)) - \sum_{i=1}^{n} w_i \quad \leq \quad w_{n+1}.\end{aligned}$$

□

6.1 Analysis of the Share Size

We next analyze the share size of the scheme Π_{tree} for a function $f(t) = t^{\beta}$ for some $0 < \beta < 1$. In this case, it would be convenient to write $q_0 = t^{\alpha_0}, q_1 = t^{\alpha_1}, \ldots, q_n = t^{\alpha_n}, q_{n+1} = 2t^{\alpha_{n+1}} = 2t$ (where $\alpha_{n+1} = 1$) and express the share size as a function of $\alpha_0, \ldots, \alpha_n, \alpha_{n+1}$.

Lemma 6.2. *Let $q_0 = t^{\beta}/2$, $\alpha_0 = \beta, \alpha_{n+1} = 1, q_{n+1} = 2t$, and let n and $\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_n$ be constants such that $\beta < \alpha_1 < \alpha_2 < \cdots < \alpha_n \leq \alpha_{n+1} = 1$. Denote $q_i = t^{\alpha_i}$ for $i = 1, \ldots, n$. For every $1 \leq i \leq n+1$ and $q_{i-1} < j \leq q_i$, the share size of the party p_j in Π_{tree} is $O\left(j^{\frac{\sum_{\ell=1}^{i} \alpha_\ell - i\beta}{\alpha_{i-1}}} \log j \right)$.*

Proof. The share of party p_j is composed of many shares of Shamir's threshold secret-sharing scheme with $O(t)$ parties; the size of each such share is $O(\log t)$. The number of shares of a threshold secret-sharing that party p_j gets is the number of edges between layer $i-1$ and layer i in T_{ramp}, i.e., the number of nodes in layer i in T_{ramp}; this number is bounded from above by

$$\prod_{\ell=1}^{i} |W_\ell| = \prod_{\ell=1}^{i} \frac{2nq_\ell}{\gamma f(t)} = \prod_{\ell=1}^{i} \frac{2n}{\gamma} t^{\alpha_\ell - \beta} = \left(\frac{2n}{\gamma}\right)^i \cdot t^{(\sum_{\ell=1}^{i} \alpha_\ell) - i\beta}.$$

This holds also for parties $p_{t^{\alpha_n}+1}, \dots, p_{2t}$ by taking $\alpha_{n+1} = 1$ and $|W_{n+1}| = t^{1-\beta}$. As $n, i, \alpha_i = O(1)$, the total share size of p_j is $O\left(j^{\frac{\sum_{\ell=1}^{i} \alpha_\ell - i\beta}{\alpha_{i-1}}} \log j\right)$. □

By Theorem 3.3 and Lemma 6.2 we get the following lemma.

Lemma 6.3. *Let n and $\alpha_0, \alpha_1, \dots, \alpha_n, \alpha_{n+1}$ be constants such that $\beta = \alpha_0 < \alpha_1 < \alpha_2 < \dots < \alpha_n \leq \alpha_{n+1} = 1$. Define*

$$C = \max\left\{ \frac{\sum_{\ell=1}^{i} \alpha_\ell - i\beta}{\alpha_{i-1}} : 1 \leq i \leq n+1 \right\}.$$

Then, there is a secret-sharing scheme realizing $\Gamma_{t,1/2,\gamma}^{f(t)=t^\beta}$, where the size of the share of p_j, for $t^\beta/2 < j \leq 2t$, is $O(j^C \log j)$ and there is an evolving secret-sharing scheme realizing $\Gamma_{\gamma t - t^\beta, \gamma t}$, where the size of the share of p_j, for $j \in \mathbb{N}$, is $O(j^C \log^2 j)$.

In order to find the best share size, we should find the number of layers n and the values of $\alpha_1, \dots, \alpha_n$ that minimize the above value C.

Example 6.4. Take $\alpha_0 = \beta$ and $\alpha_i = 2\alpha_{i-1}$ for $0 \leq i \leq \log 1/\beta$ and let i, j be such that $t^{\alpha_{i-1}} < j \leq t^{\alpha_i}$. In this case $n = \log(1/\beta)$. The share size of party p_j in the scheme realizing $\Gamma_{t,1/2,\gamma}^{f(t)=t^\beta}$ is $O(j^C \log j)$, where

$$C = \frac{\sum_{\ell=1}^{i} \alpha_\ell - i\beta}{\alpha_{i-1}} = \frac{\sum_{\ell=1}^{i} 2^\ell \beta - i\beta}{2^{i-1}\beta} = \frac{2^{i+1} - 1 - i}{2^{i-1}} \leq 4 - 2\beta \log(1/\beta),$$

where the last inequality is implied by the fact that $i \leq \log(1/\beta)$. By Corollary 3.4, this implies a scheme realizing the evolving access structure $\Gamma_{\gamma t - t^\beta, \gamma t}$ with share size $O(j^{4-\beta\log(1/\beta)} \log^2 j)$. This should be compared to the secret-sharing scheme of [15], which realizes the dynamic majority access structure (i.e., $\Gamma_{t/2-1,t/2}$) with share size $\tilde{O}(j^4)$. Thus, our scheme improves on the scheme of [15] for every constant $\beta > 0$, showing that allowing a gap between the sizes of the authorized and unauthorized sets reduces the share size, in the best known schemes.

Our goal in the rest of the section is to find better choices of $\alpha_1, \ldots, \alpha_n, \alpha_n$ that will reduce the share size. For $\beta = 1/8$ this is done in Example 6.6; similar optimization can be done for every fixed β. For general values of β this is done in Claim 6.8, where we care about the asymptotic dependency of the exponent in the share size on β.

Example 6.5. We next analyze the optimal share size that we can get by our scheme using one layer. We need to choose $\beta < \alpha_1 \leq 1$. By Lemma 6.2, the share size of the parties p_j where $t^{\beta}/2 \leq j \leq t^{\alpha_1}$ is $O(j^{\frac{\alpha_1 - \beta}{\beta}} \log j)$, and the share size of the parties p_j where $t^{\alpha_1} < j \leq 2t$ is $O(j^{\frac{\alpha_1 + 1 - 2\beta}{\alpha_1}} \log j)$. We need to find α such that $\max\{\frac{\alpha_1 - \beta}{\beta}, \frac{\alpha_1 + 1 - 2\beta}{\alpha_1}\}$ is minimized. The solution of this problem is when $\frac{\alpha_1 - \beta}{\beta} = \frac{\alpha_1 + 1 - 2\beta}{\alpha_1}$ (since increasing α_1 will increase $\frac{\alpha_1 - \beta}{\beta}$ and decrease $\frac{\alpha_1 + 1 - 2\beta}{\alpha_1}$), therefore, $\alpha_1 = \beta + \sqrt{\beta - \beta^2}$ and the exponent in the share size is $\sqrt{1/\beta - 1}$. Note that by using zero layers, the exponent in share size is $1/\beta - 1$. When $\beta > 1/2$ it holds that $1/\beta - 1 < \sqrt{1/\beta - 1}$, and zero layers are better in this case than one layer. When $\beta < 1/2$, one layer is better than zero layers.

Example 6.6. We present an upper bound for the share size that can be achieved by our construction for $\beta = \frac{1}{8}$. We get this upper bound for $n = 2$, that is, when $q_0 = \frac{t^{1/8}}{2}, q_1 = t^{\alpha_1}, q_2 = t^{\alpha_2}, q_3 = 2t$. We need to find α_1 and α_2. By Lemma 6.2, the share size of the parties p_j, where $t^{1/8}/2 \leq j \leq t^{\alpha_1}$, is $O(j^{\frac{\alpha_1 - 1/8}{1/8}} \log j)$, the share size of the parties p_j, where $t^{\alpha_1} < j \leq t^{\alpha_2}$, is $O(j^{\frac{\alpha_1 + \alpha_2 - 2/8}{\alpha_1}} \log j)$, and the share size of the parties p_j, where $t^{\alpha_2} < j \leq 2t$, is $O(j^{\frac{\alpha_1 + \alpha_2 + 1 - 3/8}{\alpha_2}} \log j)$. In order to find the an upper bound, we solve the following non-linear program.

Minimize C subject to:

$$\begin{aligned} \alpha_1 - 1/8 &\leq C/8 \\ \alpha_2 + \alpha_1 - 2/8 &\leq C\alpha_1 \\ 1 + \alpha_1 + \alpha_2 - 3/8 &\leq C\alpha_2 \\ 1/8 < \alpha_1 < \alpha_2 &\leq 1 \end{aligned}$$

A possible solution for this problem is $\alpha_1 = 0.413857, \alpha_2 = 0.792505$. In this case, $C = 2.310852$. However, we do not know if this solution is optimal.

Theorem 6.7. *There is an evolving secret-sharing scheme realizing the evolving access structure $\Gamma_{\gamma t - t^{1/8}, \gamma t}$, where the share size of party p_j is $O(j^{2.32} \log^2 j)$.*

Choosing the Parameters for the General case. In this subsection, we show how to choose good parameters for a general $0 < \beta < 1/2$. To minimize the share size, we need to minimize $\frac{\sum_{\ell=1}^{i} \alpha_\ell - i\beta}{\alpha_{i-1}}$. As the saving we aim to is bigger than $i\beta$, we will ignore this term and minimize $\frac{\sum_{\ell=1}^{i}\alpha_\ell}{\alpha_{i-1}} = \frac{\sum_{\ell=1}^{i-2}\alpha_\ell}{\alpha_{i-1}} + 1 + \frac{\alpha_i}{\alpha_{i-1}}$. In Example 6.4, we saw that if we take the values of α_i as a geometric sequence with common ratio 2, then we get an exponent slightly smaller than 4. If α_ℓ is much smaller than $2\alpha_{\ell-1}$ for many values on ℓ, then $\sum_{\ell=1}^{i-2}\alpha_\ell$ will be greater than α_{i-1} and the exponent in the share size will be larger than 4. On the other hand, if α_i is bigger than $2\alpha_{i-1}$, then $\frac{\alpha_{i-1}}{\alpha_i} > 2$ and, also in this case, the share size will be larger than 4. Thus, we take a sequence that is close to geometric sequence with common ratio 2.

Claim 6.8. *Let $\alpha_0 = \beta$ and $\alpha_i = (2+\frac{1}{2i})\cdot\alpha_{i-1}$ until the first n such that $\alpha_n \geq 1$ (and define $\alpha_n = 1$). Then, for every i*

$$\frac{\sum_{i=1}^{i}\alpha_\ell - i\beta}{\alpha_{i-1}} \leq \left(4 - O\left(\frac{1}{\log^2(1/\beta)}\right)\right).$$

Proof. Note that $\alpha_i > 2\alpha_{i-1}$, so $n \leq \log(1/\beta)$. Furthermore, for every $\ell \leq i$

$$\alpha_\ell = \frac{\alpha_i}{\left(2+\frac{1}{2(\ell+1)}\right)\cdot\ldots\cdot(2+\frac{1}{2i})} \leq \frac{\alpha_i}{(2+\frac{1}{2i})^{i-\ell}}.$$

Thus,

$$\begin{aligned}\sum_{\ell=1}^{i}\alpha_j &\leq \sum_{\ell=1}^{i}\frac{\alpha_i}{\left(2+\frac{1}{2i}\right)^{i-\ell}}\\ &= \frac{\alpha_i}{\left(2+\frac{1}{2i}\right)^{i}}\frac{\left(2+\frac{1}{2i}\right)^{i+1} - \left(2+\frac{1}{2i}\right)}{\left(1+\frac{1}{2i}\right)}\\ &\leq \alpha_i\left(2+\frac{1}{2i}\right)\left(1-\frac{1}{2i+1}\right).\end{aligned}$$

For every $2 \leq i \leq n$,

$$\begin{aligned}\frac{\sum_{\ell=1}^{i}\alpha_\ell - i\beta}{\alpha_{i-1}} &\leq \frac{\sum_{\ell=1}^{i-1}\alpha_\ell + \alpha_i}{\alpha_{i-1}}\\ &\leq \left(2+\frac{1}{2(i-1)}\right)\left(1-\frac{1}{2(i-1)+1}\right) + \frac{\alpha_i}{\alpha_{i-1}}\\ &\leq 4 - \frac{1}{2i(2i-1)}\\ &\leq 4 - O\left(\frac{1}{\log^2(1/\beta)}\right),\end{aligned}$$

where the last inequality is implied by the fact that $i \leq n \leq \log(1/\beta)$. Note that for $i = n+1$ it holds that $\frac{\alpha_n}{\alpha_{n-1}} = 1$ and therefore the inequality holds. □

For example, for $\beta = 2^{-20}$ the exponent is less than $4 - 1/(40\cdot 39) < 3.9994$. This should be compared to the simpler solution given in Example 6.4, where the exponent is $4 - 40/2^{20} > 3.99996$.

By Lemma 6.3 and Claim 6.8, we obtain our evolving ramp secret-sharing scheme, proving Theorem 1.1.

Remark 6.9. In our analysis in Sect. 6.1 we ignore the factor of $i\beta$ in the exponent in the share size. This implies that in our construction of T_{ramp} we can take $W_i = \{0, 1, \ldots, q_i\}$. The saving in this case, compared to the scheme of [15], stems from the fact that we take a collection of finite trees, where in each tree we ignore the first $f(t)/2$ parties.

7 Reduction Between Evolving Ramp Secret-Sharing Schemes

In this section we show how to construct an evolving secret-sharing scheme realizing $\Gamma_{\gamma t - t^\beta, \gamma t}$ for some constants γ, β from an evolving secret-sharing scheme realizing $\Gamma_{t/d-((t/d\gamma)^\beta-1),t/d}$ for a constant d such that $\gamma > 1/d$. This construction is used to prove Theorem 1.2 from Lemma 4.3.

Theorem 7.1. *Let $0 < \beta < 1$, $d \in \mathbb{N}$, and $1/d < \gamma < 1$ be constants, and let Π be a scheme that realizes the evolving ramp access structure $\Gamma_{t/d-((\frac{t}{\gamma d})^\beta-1),t/d}$ such that the length of the share of party p_j is $c(j)$. Then there is a scheme realizing the evolving ramp access structure $\Gamma_{\gamma t - t^\beta, \gamma t}$ such that the size of the share of party p_j is $c(\lfloor \gamma d j \rfloor)$.*

Proof. In Fig. 5 we describe the scheme Π' that realizes the evolving access structure $\Gamma_{\gamma t - t^\beta, \gamma t}$. Next we prove the correctness and security of this scheme as well as analyzing its share size.

The Scheme Π'

For every $j \in \mathbb{N}$:

1. Give party p_j the share of party $p_{\lfloor \gamma d j \rfloor}$ in Π.

Fig. 5. The scheme Π' that realizes the evolving access structure $\Gamma_{\gamma t - t^\beta, \gamma t}$.

First we observe that, as $\gamma d > 1$, for every $j > j'$, parties p_j and $p_{j'}$ in Π' get shares of parties $p_{\lfloor \gamma d j \rfloor}$ and $p_{\lfloor \gamma d j' \rfloor}$ in Π, respectively, such that $\lfloor \gamma d j \rfloor \geq \lfloor \gamma d (j'+1) \rfloor \geq \lfloor (\gamma d j') + 1 \rfloor > \lfloor \gamma d j' \rfloor$, thus, the parties in Π' get shares of different parties in Π.

Correctness: Let $A = \{p_{i_1}, \ldots, p_{i_k}\}$ be a minimal authorized set, i.e., $|A| = k \geq \gamma i_k$. The parties in A get shares of parties in the set $\{p_1, \ldots, p_{\lfloor \gamma d i_k \rfloor}\}$ in Π and $|A| \geq \lfloor \gamma d i_k \rfloor / d$, thus they can reconstruct the secret.

Security: Let $A = \{p_{i_1}, \ldots, p_{i_k}\}$ be an unauthorized set. Thus, for every $1 \leq j \leq k$, parties $p_{i_1}, \ldots, p_{i_j}$ in Π' get shares of parties in the set $\{p_1, \ldots, p_{\lfloor \gamma d i_j \rfloor}\}$, and

$$j \leq \gamma i_j - (i_j)^\beta \leq \frac{\lfloor \gamma d i_j \rfloor + 1}{d} - \left(\frac{\lfloor \gamma d i_j \rfloor}{\gamma d}\right)^\beta \leq \frac{\lfloor \gamma d i_j \rfloor}{d} - \left(\left(\frac{\lfloor \gamma d i_j \rfloor}{\gamma d}\right)^\beta - 1\right).$$

Thus, for every $1 \leq j \leq k$, parties $p_{i_1}, \ldots, p_{i_j}$ in Π' get shares of an unauthorized set in $\Gamma_{t/d-((\frac{t}{\gamma d})^\beta - 1), t/d}$, and the parties $p_{i_1}, \ldots, p_{i_k}$ get no information about the secret.

Share size: Party p_j gets the share of party $p_{\lfloor \gamma d j \rfloor}$ in Π. Therefore, the share size of party p_j is $c(\lfloor \gamma d j \rfloor)$. □

By applying the reduction of Theorem 7.1 to the scheme of Lemma 4.3, we obtain Theorem 1.2.

8 An Evolving $(k/2, k)$-Ramp Secret-Sharing Scheme

Komargodski et al. [14] presented an evolving secret-sharing scheme for the evolving k-threshold access structure for a constant k (i.e., the complete access structure containing all sets of size at least k). In their construction, the j-th party's share size is $O(k \log j)$, we denote this construction by Π_0. An interesting open question is whether the dependency on k can be improved. We study a relaxation of the problem, namely evolving $(k/2, k)$-ramp secret-sharing for constant k; where every set that contains at least k parties can reconstruct the secret, and any set of size at most $k/2$ cannot learn any information about the secret. We require nothing regarding the sets of size greater than $k/2$ but smaller than k. We construct an evolving $(k/2, k)$-ramp secret-sharing scheme with share size $O(\log k \log j)$. In our construction, we use the scheme Π_0 of [14] as a building box.

In Fig. 6 we describe the scheme $\Pi_{k/2,k}$ that realizes the evolving $(k/2, k)$-threshold access structure. As in [14], we first partition the parties into sets, called generations, according to the order they arrive, where the i-th generation contains the parties $p_{2^{ki}}, \ldots, p_{2^{k(i+1)}-1}$.

We use the following observation in order to analyze the share size in $\Pi_{k/2,k}$.

Observation 8.1. *Shamir's t-out-of-n secret-sharing scheme shares m different secrets $s_1, s_2, \ldots, s_m$ with sizes $\ell_1, \ldots, \ell_m$ among n parties using share size* $\max\{\lceil \log(n+1) \rceil, \ell_1 + \ell_2 + \cdots + \ell_m\}$.

Proof. We simply share the secret $s = s_0 \circ s_1 \circ \cdots \circ s_m$ by Shamir's secret-sharing scheme (where $\circ$ is the concatenation of string). □

The Scheme $\Pi_{k/2,k}$

Let Π_0 be the evolving k-threshold scheme of [14].
When party $p_{2^{ki}}$ arrives, the dealer prepares shares for all the parties $\{p_{2^{ki}}, \ldots, p_{2^{k(i+1)}-1}\}$.

1. Generate the next k shares from the scheme Π_0. Denote these shares by $v^i_1, v^i_2, \ldots, v^i_k$.
2. For $\ell \in \{0, 1, \ldots, \log k\}$, share $v^i_{2^\ell}, \ldots, v^i_{2^{\ell+1}-1}$ by a 2^ℓ-out-of-$(2^{k(i+1)}-2^{ki})$ secret-sharing scheme among the parties $\{p_{2^{ki}}, \ldots, p_{2^{k(i+1)}-1}\}$. Denote this scheme by Π^i_ℓ. That is, the share v^i_1 is shared with threshold 1 using Π^i_1, the shares v^i_2, v^i_3 are shared with threshold 2 using Π^i_2, the shares $v^i_4, \ldots, v^i_7$ are shared with threshold 4 using Π^i_3, etc.

Fig. 6. The scheme $\Pi_{k/2,k}$ realizing the evolving $(k/2, k)$-access structure.

Theorem 8.2. *The scheme $\Pi_{k/2,k}$ realizes the evolving ramp access structure $\Gamma_{k/2,k}$ with share size $O(\log k \log j)$ for party p_j.*

Proof. Correctness: we show that any set of size at least k can reconstruct the secret. Let $A = \{p_{i_1}, p_{i_2}, \ldots, p_{i_k}\}$ be a minimal authorized set such that p_{i_k} is in the g-th generation, that is, $2^{kg} \le i_k \le 2^{k(g+1)} - 1$. For $1 \le j \le g$, let c_j be the number of of parties in A from the j-th generation. By the construction, c_j parties in generation j can reconstruct at least c_j shares from generation j (this is true since every v^j_ℓ is shared by threshold of at most ℓ). Therefore, the set A can reconstruct at least $\sum_{j=1}^{k} c_j = k$ shares of Π_0, thus, by the correctness of Π_0, the set A can reconstruct the secret.

Security: Let A be an unauthorized set of size at most $k/2$ ending in generation g. By the construction, c_j parties from the j-th generation can reconstruct at most $2c_j - 1$ shares from generation j (this is true since every v^j_ℓ is shared by threshold of at least $\lceil \ell/2 \rceil$), thus the set A can reconstruct at most $\sum_{j=1}^{g}(2c_j - 1) < k$ shares of Π_0. By the security of Π_0, the set A cannot learn any information about the secret.

Share size analysis: the share of party p_j in generation g is composed of the shares from the schemes Π^i_ℓ for every $\ell \in \{0, 1, \ldots, \log k\}$. The size of generation g is $2^{k(g+1)} - 2^{kg} \le 2^{kg} \cdot 2^k$. Party p_j is in the $\lfloor \frac{\log j}{k} \rfloor$-th generation. The log of the generation size of the generation of p_j is less than $kg + k \le \frac{k \log j}{k} + k = \log j + k$. The scheme Π^i_ℓ for every $0 \le \ell \le \log k$ requires share size $\max\{\log j + k, |v^g_{2^\ell}| + \cdots + |v^g_{2^{\ell+1}-1}|\}$ (by Observation 8.1). The shares $v^g_1, \ldots, v^g_k$ are generated from Π_0; recall that the share size of the n-th party in Π_0 is $k \log n$. By the construction, $k(g-1)$ shares from Π_0 were generated for the previous generations. Therefore,

$$|v^g_\ell| \le |v^g_k| \le k \log kg \le k \log k \frac{\log j}{k} = k \log \log j.$$

Thus, the share size in Π_ℓ^g is at most

$$\max\{\log j + k, 2^\ell \cdot k \log\log j\}.$$

The total share size is:

$$\sum_{\ell=0}^{\log k} \max\{\log j + k, 2^\ell \cdot k \log\log j\} \leq (\log k + 1)(\log j + k) + 2k^2 \log\log j.$$

□

When $j > 2^{2k^2}$, the share size of p_j is $O(\log k \log j)$.

9 Properties of Optimal Choices of Parameters for the Tree Technique

In this section we show the limitations of the tree technique for $\beta \geq 1/2$. We also give an upper bound on the number of layers minimizing the share size in our scheme for general β.

9.1 The Share Size in Π_{tree}

In this subsection, we analyze the share size in Π_{tree} and prove that for $1/2 \leq \beta < 1$ the optimal share size is obtained when $n = 0$, i.e., it is $\Theta(j^{\frac{1-\beta}{\beta}})$.

Claim 9.1. *For every $\beta \geq 1/2$, the share size in Π_{tree} is $\Omega(j^{\frac{1-\beta}{\beta}})$ for at least one party p_j.*

Proof. Let $j = t^{\alpha_n} + 1$. By Lemma 6.2, the share size of the party p_j is $\Omega(j^C)$, where $C = \frac{1+\sum_{\ell=1}^{n-1} \alpha_\ell + \alpha_n - \beta(n+1)}{\alpha_n}$. It holds that,

$$\begin{aligned}\sum_{\ell=1}^{n-1} \alpha_\ell &= \alpha_n(C - \frac{1-\beta}{\beta}) + (n+1)\beta - \frac{2\beta-1}{\beta}\alpha_n - 1 \\ &\leq \alpha_n(C - \frac{1-\beta}{\beta}) + (n+1)\beta - (2\beta - 1) - n - 1 \\ &= \alpha_n(C - \frac{1-\beta}{\beta}) + (n-1)\beta,\end{aligned}$$

where the inequality follows from the fact that $\alpha_n > \beta$ and $2\beta - 1 \geq 0$. As $\alpha_\ell > \beta$ for every $1 \leq \ell \leq n-1$, we get that $\alpha_n(C - \frac{1-\beta}{\beta}) \geq \sum_{\ell=1}^{n-1} \alpha_\ell - (n-1)\beta \geq 0$, i.e., $C \geq \frac{1-\beta}{\beta}$. □

Remark 9.2. For every $n > 0$ and $\beta > 1/2$, Π_{tree} with n layers has shares greater than Π_{seg} (since, $\frac{2\beta-1}{\beta}\alpha_n > 2\beta - 1$ as $\alpha_n > \beta$).

Claim 9.3. *For every $\beta < 1/2$ there is at least one party p_j such that the share size of p_j in Π_{tree} is $\Omega(j)$.*

Proof. Let $j = t^{\alpha_n} + 1$. The share size of party p_j is $\Omega(j^{C'})$ where $C' = \frac{1+\sum_{\ell=1}^{n-1} \alpha_\ell + \alpha_n - \beta(n+1)}{\alpha_n} \geq \frac{\alpha_n}{\alpha_n} = 1$ (since $\alpha_\ell \geq \beta$ for every $1 \leq \ell \leq n-1$). □

9.2 Upper Bound on the Number of Layers in the Optimal Solution for $\Pi_{\textbf{tree}}$

In this section, we show that, for every $\beta < 1/2$, there exists a choice of the parameters $n, \alpha_1, \ldots, \alpha_n$ that minimizes the share size of Π_{tree} and the number of layers n is at most $O(\log(1/\beta))$.

Claim 9.4. *Let $n, \alpha_1, \ldots, \alpha_n$ be parameters for Π_{tree}. If the share size of party p_j, for every $j \in \mathbb{N}$, in Π_{tree} is less than j^4 and there exist indices $1 \le i_1 < i_2 \le n-2$ such that $\alpha_{i_2} < 2\alpha_{i_1}$ and $\alpha_{i_1} \ge 2\beta$, then $i_2 \le i_1 + 15$.*

Proof. By the assumption of the lemma, $\alpha_{i_1} - \beta \ge \alpha_{i_1} - 0.5\alpha_{i_1} = 0.5\alpha_{i_1}$. Recall that the the share size of party p_j where $j = t^{\alpha_{i_2}} + 1$ is greater than j^C, where $C = \frac{\sum_{\ell=1}^{i_2+1} \alpha_\ell - (i_2+1)\beta}{\alpha_{i_2}}$. We next analyze this expression, using the fact that $\alpha_\ell > \beta$ for $1 \le \ell \le i_1 - 1$ and $\alpha_\ell \ge \alpha_{i_1}$ for $\ell \ge i_1$.

$$\begin{aligned}\frac{\sum_{\ell=1}^{i_2+1} \alpha_\ell - (i_2+1)\beta}{\alpha_{i_2}} &\ge \frac{\sum_{\ell=i_1}^{i_2+1} (\alpha_{i_1} - \beta)}{\alpha_{i_2}} \\ &\ge \frac{\sum_{\ell=i_1}^{i_2+1} 0.5\alpha_{i_1}}{2\alpha_{i_i}} \\ &\ge \frac{i_2 + 1 - i_1}{4}.\end{aligned}$$

Since we assume that the exponent is at most 4, we obtain that $i_2 \le i_1 + 15$. □

Lemma 9.5. *For every $\beta < 1/2$, there exists a choice of the parameters $n, \beta < \alpha_1 < \cdots < \alpha_n \le 1$ that minimizes the share size in Π_{tree} and the number of layers n is at most* $15\log(1/\beta) + 2$.

Proof. First, let i be the largest index such that $\alpha_i \le 2\beta$. If $i \ge 2$, we consider the parameters $n-i+1, \alpha_i, \ldots, \alpha_n$ with $n-i+1$ layers. This choice of parameters can only decrease the share size of parties $p_{t^{\alpha_i}+1}, \ldots, p_{2t}$ (since $\alpha_1, \ldots, \alpha_{i-1} > \beta$). The share size of party p_j, where $t^\beta/2 \le j \le t^{\alpha_i}$, is $\tilde{O}(j^C)$ where $C = (\alpha_i - \beta)/\beta \le 1$. By Claim 9.3, for every $\beta \le 1/2$, the exponent of the share size is at least 1. Thus, $n - i + 1, \alpha_i, \ldots, \alpha_n$ is also optimal.[2]

Second, the optimal solution has exponent less than 4 (by our construction in Sect. 6.1). Thus, by Claim 9.4, for every $1 \le \log(1/\beta)$, in the interval $2^d\beta + 1, \ldots, 2^{d+1}\beta$ there are at most 15 layers. Thus, the total number of layers is as most $15\log(1/\beta) + 2$. □

References

1. Beimel, A., Othman, H.: Evolving ramp secret-sharing schemes. In: Catalano, D., De Prisco, R. (eds.) SCN 2018. LNCS, vol. 11035, pp. 313–332. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98113-0_17

[2] In fact, for every $\beta < 1/2$, it must hold that $\alpha_2 > \beta$, as the exponent in this case is greater than 1.

2. Benaloh, J., Rudich, S.: Private communication (1989)
3. Blakley, G.R.: Safeguarding cryptographic keys. In: AFIPS, p. 313 (1979)
4. 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
5. 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
6. 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
7. Cascudo Pueyo, I., Cramer, R., Xing, C.: Bounds on the threshold gap in secret sharing and its applications. IEEE Trans. Inf. Theory **59**, 5600–5612 (2013)
8. 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
9. Csirmaz, L., Tardos, G.: On-line secret sharing. Des. Codes Cryptogr. **63**(1), 127–147 (2012)
10. D'Arco, P., De Prisco, R., De Santis, A., Pérez del Pozo, A., Vaccaro, U.: Probabilistic secret sharing. In: 43rd International Symposium on Mathematical Foundations of Computer Science (MFCS 2018). Leibniz International Proceedings in Informatics (LIPIcs), vol. 117, pp. 64:1–64:16 (2018)
11. Franklin, M.K., Yung, M.: Communication complexity of secure computation. In: STOC 1992, pp. 699–710 (1992)
12. Ito, M., Saito, A., Nishizeki, T.: Secret sharing schemes realizing general access structure. In: Proceedings of the Globecom 1987, pp. 56–64 (1987)
13. Kilian, J., Nisan, N.: Private communication (1990)
14. 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
15. 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
16. Martin, K.M., Paterson, M.B., Stinson, D.R.: Error decodable secret sharing and one-round perfectly secure message transmission for general adversary structures. Cryptogr. Commun. **3**, 65–86 (2011)
17. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
18. Stinson, D.R., Wei, R.: An application of ramp schemes to broadcast encryption. Inform. Process. Lett. **69**, 131–135 (1999)