Fully Anonymous Perfect Secret-Sharing

Roni Con* Ray Li† Noam Mazor‡

Abstract

Fully anonymous secret-sharing schemes ensure two properties at once: for any fixed secret, the combined shares of every unauthorized set of participants are uniformly random, and every authorized set can reconstruct the secret exactly using only the share values, without needing to know which participant holds which share or in what order the shares appear. It was previously open whether such schemes exist for nontrivial exact-threshold parameters $2 < t < n$. For the smallest previously open threshold, $t = 3$, we give, for every $n \geq 4$, an explicit fully anonymous scheme for one-bit secrets, with $2\lceil \log n \rceil$-bit shares and a perfect reconstruction algorithm running in $\mathrm{poly}(\log n)$ time.

The next result, found by ChatGPT, shows that for every $1 \leq t \leq n$ there exists a fully anonymous perfect (t, n) threshold secret-sharing scheme for one-bit secrets, in which each share has length $O(t \log n)$ bits. The proof is purely existential and does not provide an efficient construction. Moreover, ChatGPT identified a simple construction of a fully anonymous perfect scheme for every access structure $\mathcal{A}$; if $\mathcal{A}$ contains ℓ authorized sets, then each share consists of ℓ^2 bits. The authors subsequently verified and streamlined the proofs on their own and take full responsibility for their correctness.

Contents

*School of Electrical & Computer Engineering, Tel Aviv University. Email: ronicon@tauex.tau.ac.il.

†Math & CS Department, Santa Clara University. Email: rli6@scu.edu. Research supported by NSF grant CCF-2347371.

‡New York University. Email: noammaz@gmail.com.

1 Introduction

Secret-sharing is a cryptographic primitive that enables a randomized dealer to distribute a secret among a set of participants by giving each participant a randomized share. The authorized subsets of participants, namely, those that can reconstruct the secret, form an *access structure*, whereas every unauthorized subset learns no information about the secret. Formally introduced independently by Shamir [Sha79] and Blakley [Bla79], secret-sharing schemes are used as a building block in many secure protocols including multiparty computation, Byzantine agreement, and threshold cryptography [Bei11].

A particularly important class of secret-sharing schemes is that of *threshold* secret-sharing schemes. In such schemes, a threshold value t is predetermined, and the following condition is satisfied: any set of fewer than t shares yields no information about the secret, while any set of t shares suffices to reconstruct the secret exactly.

Several recent works have studied stronger notions of secret-sharing in which an unauthorized collection of shares hides not only the secret but also information about the participants holding those shares [EBG+24, BGI+25, Con25]. Such schemes are referred to as *anonymous secret-sharing schemes*. One motivation for this additional requirement comes from abuse-resistant location tracking. Eldridge et al. [EBG+24] used anonymous secret-sharing to design protocols that balance the privacy of device owners with the need to detect location-tracking devices, such as AirTags, that have been covertly attached to a person. For further discussion of this application, we direct the reader to the introduction of [EBG+24].

Bishop et al. [BGI+25] introduced several notions of anonymity. We consider their strongest information-theoretic notion. Informally, for every fixed secret, the shares held by any unauthorized set of participants must be jointly uniform over the appropriate Cartesian power of the share domain. Moreover, every authorized set must be able to reconstruct the secret perfectly from the share values alone, without using the identities of the participants or the order of their shares. We refer to schemes satisfying both requirements as *fully anonymous perfect secret-sharing schemes*.

In the threshold setting, the shares in a fully anonymous scheme behave like unlabeled and unlinkable tokens. Any collection of fewer than t shares from distinct participants is distributed exactly as independent uniform samples from the share domain. Thus, the share values reveal neither the secret nor the identities of the participants holding them. Across independent executions of the sharing algorithm, they also cannot be used to determine whether two shares belong to the same participant. On the other hand, any t or more shares from the same execution determine the secret from their values alone,

regardless of their order. Full anonymity is therefore stronger than ordinary perfect secrecy: shares may hide the secret while still leaking identity or linkage information through participant-dependent formats, explicit labels, or persistent identifiers [BGI+25, Con25].

Eldridge et al. [EBG+24] presented a variant of Shamir's secret-sharing scheme such that the shares held by any unauthorized set are indeed uniformly distributed, however, the reconstruction algorithm may fail (albeit with negligible probability, assuming sufficiently large share sizes). Thus, their construction is fully anonymous but not perfect. In [BGI+25], Bishop et al. explicitly asked whether, aside from some simple instances, there exist fully anonymous schemes achieving perfect reconstruction for threshold access structures and, more generally, for arbitrary access structures. Subsequently, Con [Con25] made progress on this question for the *gap-threshold* setting by constructing a fully anonymous perfect secret-sharing scheme with privacy threshold ℓ and reconstruction threshold $2\ell + 1 \leq n$. That is, any set of ℓ shares, in any order, is distributed uniformly and any set of $2\ell + 1$ shares, in any order, can reconstruct the secret, without revealing the participants' identities.

We remark here that the cases where $t = 2$ or $t = n$ are simple. Namely, there are simple constructions that give fully anonymous secret-sharing schemes for these thresholds; see Section 2. Thus, the exact threshold case is unresolved for every $2 < t < n$.

In this paper, we resolve the exact-threshold case for $t = 3$ in the affirmative. Specifically, we prove that when the threshold is exactly three, there exists an explicit and efficient fully anonymous perfect secret-sharing scheme.

Additionally, we present a result found by Codex ChatGPT 5.6 Sol Ultra for the general threshold case. The proof establishes the existence of a fully anonymous threshold secret-sharing scheme for an arbitrary threshold t, with share length of $O(t \log n)$ bits. We verified and simplified the proofs and present them in this paper. The question to construct explicit and efficient fully anonymous threshold secret-sharing schemes for $4 \leq t < n$ remains open. Moreover, we present another simple construction, found by ChatGPT, which shows that for every access structure with ℓ authorized sets, there is a fully anonymous perfect secret-sharing scheme with ℓ^2-bit shares.

1.1 Setup and preliminaries

For an integer k, we denote $[k] = \{1, 2, \ldots, k\}$. Throughout, $\log(x)$ refers to the base-2 logarithm. For a prime power q, we denote by $\mathbb{F}_q$ the finite field with q elements. We call a sequence $I \in [n]^\ell$ a *distinct-element sequence* if all of its elements are pairwise distinct; that is, $I_i \neq I_j$ for all distinct $i, j \in [\ell]$. For a vector $v = (v_1, \ldots, v_n)$ and $I \in [n]^\ell$, we write $v_I := (v_{I_1}, \ldots, v_{I_\ell})$.

Fully anonymous secret-sharing. We begin with a brief reminder of threshold secret-sharing schemes. We refer the interested reader to Beimel's comprehensive survey [Bei11].

Suppose there are n players and a dealer $\mathcal{D}$ (distinct from the players) who chooses a secret $s \in \{0, 1\}$ and hands out the share $w_i \in \Omega$ to i-th participant for all $i \in [n]$. An *access structure* on $[n]$ is a nonempty family $\mathcal{A} \subseteq 2^{[n]}$ such that $\emptyset \notin \mathcal{A}$ and, whenever $A \in \mathcal{A}$ and $A \subseteq A' \subseteq [n]$, we have $A' \in \mathcal{A}$. Its members are called *authorized sets*, and all other subsets of $[n]$ are called *unauthorized sets*. A secret-sharing scheme is called a (t, n)

threshold secret-sharing scheme if $\mathcal{A} = \{A \subseteq [n] \mid |A| \geq t\}$. In other words, any group of at least t participants can recover the secret. Further, we want that for each $A \notin \mathcal{A}$, the respective parties cannot learn anything about the secret. We denote by `Share` a randomized algorithm that gets a secret s and produces a vector $\mathrm{sh} \in \Omega^n$ and we denote by `Recon` the reconstruction algorithm of the scheme.

Formally, let S be uniformly distributed over $\{0,1\}$. Conditioned on $S = s$, let $W_1, \ldots, W_n$ be the random variables corresponding to the n shares. We want

$$H(S|\mathcal{V}_A) = \begin{cases} 0, & |A| \geq t \\ 1, & |A| < t \end{cases}, \tag{1}$$

where $H(\cdot)$ denotes the entropy of a random variable and $\mathcal{V}_A = \{W_i \mid i \in A\}$. In words, (1) implies that any set of at least t parties can reconstruct the secret (there is no entropy in $H(S|\mathcal{V}_A)$) but any set of less than t parties cannot reveal any information about the secret.

Remark 1.1. *Throughout this paper, we restrict attention to one-bit secrets. By contrast, in the standard labeled Shamir scheme over $\mathbb{F}_q$, both the secret alphabet and each share alphabet have cardinality q; hence, its information rate is $\log q / \log q = 1$. Determining whether fully anonymous secret-sharing schemes can achieve an information rate bounded below by a positive constant independent of the scheme parameters (either by constructing schemes for longer secrets or by reducing the share length) is an interesting direction for future work.*

We now define the anonymity of a threshold secret-sharing scheme. Our definition adopts the strongest notion of anonymity from [BGI+25] in which any set of *unauthorized* shares is uniformly distributed over the domain of all possible shares.

Definition 1.2. *Given the definitions above, a* fully anonymous perfect (t, n) threshold secret-sharing scheme *with share alphabet Ω is a secret-sharing scheme such that the following two conditions are satisfied:*

1. *(Share anonymity) For every secret $s \in \{0,1\}$, every distinct-element sequence $I \in [n]^{t-1}$, and every $\mathbf{v} \in \Omega^{t-1}$, we have*

$$\Pr_{\mathrm{sh} \leftarrow \mathtt{Share}(s)}[\mathrm{sh}_I = \mathbf{v}] = |\Omega|^{-(t-1)} .$$

2. *(Perfect anonymous reconstruction) There exists a deterministic function* `Recon` *(possibly non-efficient) such that for every secret $s \in \{0,1\}$, every distinct-element sequence $I \in [n]^t$, and every* sh *in the support of* $\mathtt{Share}(s)$*, it holds that* $\mathtt{Recon}(\mathrm{sh}_I) = s$.

1.2 Results

The first result resolves the open question raised by Bishop et al. [BGI+25] for the smallest nontrivial threshold t for which existence of fully anonymous perfect (t, n) threshold secret-sharing scheme was previously unknown.

Theorem 1.3. *Let $n \geq 4$ be an integer. There exists an explicit fully anonymous $(3, n)$ secret-sharing scheme for one-bit secrets, where the share length is $2\lceil \log n \rceil$. The reconstruction algorithm runs in $\mathrm{poly}(\log n)$ time.*

We observe that this result not only establishes the existence of such schemes, but also yields an explicit and efficient construction, supporting both efficient sharing and reconstruction.

The remaining two results in this paper were discovered using Codex ChatGPT 5.6 Sol Ultra. We stress that the proofs of these results, after being simplified by the authors, were written by us, and we assume full responsibility for their correctness.

The following theorem settles the existence question for every threshold.

Theorem 1.4. *For every pair of integers $1 \leq t \leq n$, there exists a fully anonymous (t, n) threshold secret-sharing scheme one-bit secrets with share alphabet $\{0,1\}^m$, where $m = O(t \log n)$.*

This result merely shows existence and does not yield explicit and efficient schemes. The problem of designing efficient schemes for $4 \leq t < n$ with short shares remains a challenge for future research. However, the next theorem shows that if one allows long shares, an explicit construction exists. Moreover, there is such a construction of perfect, fully anonymous secret-sharing for *any* access structure.

Theorem 1.5. *Any access structure $\mathcal{A} \subseteq 2^{[n]}$ has a perfect, fully anonymous secret-sharing scheme for one-bit secrets. If the number of authorized sets in $\mathcal{A}$ is ℓ, then each participant receives an ℓ^2-bit share.*

In particular, for all integers $1 \leq t \leq n$, there is an explicit fully anonymous (t, n) secret-sharing scheme with share alphabet $\{0,1\}^m$, where $m = \binom{n}{t}^2$.

Previously, constructions for fully anonymous secret-sharing schemes (with a better share length) were known with either negligible deviation from uniform [PCO20] or with a negligible correctness error [BGI+25].

1.3 Prior work

Early work on anonymous secret sharing focused on *anonymous reconstruction*, where the reconstruction procedure takes only the share values and does not need to know which parties provided them [SV88, PP92, BS97, KOKO02]. Subsequent work advanced the notion of anonymity by additionally demanding that shares held by unauthorized sets hide identifying or linkability information, instead of limiting anonymity to the reconstruction phase. Guillermo, Martin, and O'Keefe [GMO03] analyzed a single-dealer form of share anonymity, which is weaker than full anonymity. Paskin-Cherniavsky and Olimid [PCO20] proposed *decisional share unpredictability*, a multi-instance concept connected to linkage anonymity, and presented an explicit scheme for arbitrary access structures with perfect reconstruction that is statistically close to fully anonymous. More recently, Eldridge et al. [EBG+24] examined a stronger unlinkability notion in the threshold setting, built a scheme that is also statistically close to fully anonymous, enables robust reconstruction for a constant number of dealers, and used it for abuse-resistant location tracking.

We briefly describe Construction 1 in [EBG+24]. Let t denote the threshold. Each time a dealer shares a secret, the dealer chooses independently and uniformly at random n points $\gamma_1, \ldots, \gamma_n \in \mathbb{F}_q \setminus \{0\}$, a random polynomial $f \in \mathbb{F}_q[x]_{\leq t-1}$ such that $f(0) = s$, and sets the i-th share to be $(\gamma_i, f(\gamma_i))$.[1] This scheme cannot guarantee perfect reconstruction, because two distinct shares may produce the same γ with probability $1/(q-1)$. Since reconstruction is based on polynomial interpolation and depends on having distinct evaluation points, there is always a nonzero chance that it fails.

Bishop et al. [BGI+25] subsequently carried out a systematic study of fully anonymous secret-sharing for general access structures. They defined a hierarchy of anonymity notions with progressively stronger guarantees, covering both the hiding of the participants' identities and the inability to link shares originating from the same dealer. In this paper, we adopt their strongest definition of share anonymity. They presented an explicit fully anonymous secret-sharing construction with smaller shares than [PCO20], at the cost of allowing imperfect reconstruction. In addition, they proved nearly tight lower bounds, showing that anonymity may require exponentially large shares even for access structures that admit succinct descriptions.

Their fully anonymous construction attains this strongest form of share anonymity; however, its reconstruction procedure succeeds with all but negligible probability and thus permits a negligible chance of reconstruction failure.

The constructions of Paskin-Cherniavsky and Olimid [PCO20], Eldridge et al. [EBG+24], and Bishop et al. [BGI+25] do not simultaneously achieve perfect share anonymity and perfect anonymous reconstruction. Con [Con25] achieved both properties in the gap-threshold setting. To state this result precisely, let p be the largest integer such that, for every $j \leq p$, every fixed secret s, and every distinct-element sequence $I \in [n]^j$, the vector sh_I, where $\mathrm{sh} \leftarrow \mathtt{Share}(s)$, is uniformly distributed over Ω^j. Let r be the smallest integer such that every collection of r shares held by distinct participants reconstructs the secret from the share values alone, without using the participants' identities. We call p the privacy threshold and r the reconstruction threshold. In an exact (t, n) threshold scheme, $p = t - 1$ and $r = t$, so there is no intermediate regime between privacy and reconstruction. For every k satisfying $2k - 1 \leq n$, Con constructed a fully anonymous $(k-1, 2k-1, n)$ gap-threshold scheme; thus, $p = k - 1$ and $r = 2k - 1$. The existential construction has $O(k \log n)$-bit shares and secret. Con also gave an explicit construction with $k^{O(k)} \log n$-bit shares and secret and, for $k = 2$, an explicit construction with privacy threshold 1, reconstruction threshold 3, and share size $3 \log n + O(1)$.

More recently, Zhang et al. [ZSZG26], building on the work [Con25] and [CGLZ25], showed the existence of fully anonymous $(k - 1, 2k - 1 + \varepsilon n, n)$ gap-threshold secret-sharing schemes with share and secret size of $O_\varepsilon(\log n)$ bits. Thus, in the regime where $k = \Theta(n)$, allowing an additive εn increase in the reconstruction threshold reduces the required share length from $O(n \log n)$ to $O_\varepsilon(\log n)$.

[1] Observe that this construction does not meet condition 1 (it is only statistically close to uniform). In Section 3.2.3 of [EBG+24], they suggest the following simple fix. The dealer records the γ values and, whenever a γ occurs again, replaces the polynomial evaluation by an independent uniform field element. This yields a fully anonymous secret-sharing scheme. Of course, this does not reduce the reconstruction failure probability. Alternatively, the dealer may select the γ_is so that they are pairwise distinct. In that setting, the scheme achieves perfect reconstruction, but condition 1 is not satisfied.

1.4 Open problems

This paper settles the problem posed by Bishop et al. [BGI+25] concerning the existence of fully anonymous threshold secret-sharing schemes. We conclude by highlighting two follow-up questions that we consider particularly interesting.

1. The main open problem is to design an explicit and efficient fully anonymous secret-sharing scheme in the threshold setting for every threshold value t. At present, explicit and efficient constructions are known only for $t \in \{1, 2, 3, n\}$, although it is known in principle that fully anonymous schemes exist for all other threshold values as well.

2. We define the rate of a fully anonymous threshold secret-sharing scheme as $\frac{\log |\Sigma|}{\log |\Omega|}$, where Σ denotes the alphabet of the secret and Ω denotes the alphabet of the shares. The existential construction underlying Theorem 1.4 has rate $\Theta(1/(t \log n))$, which tends to zero as $n \to \infty$. Is it possible to construct, or at least prove the existence of, a fully anonymous threshold secret-sharing scheme that achieves a constant rate?

2 Simple schemes

In this section, we outline two straightforward, fully anonymous threshold secret-sharing schemes, along with a fully anonymous scheme for arbitrary access structures. The two threshold schemes will serve as reference points for the subsequent sections. In particular, in the next section we will describe a $(3, n)$ scheme that can be viewed as a generalization of the $(2, n)$ scheme introduced below.

2.1 Simple perfect threshold schemes

A fully anonymous perfect $(2, n)$ scheme with $\log n + O(1)$-bit shares. Let $q \geq n$ be a prime power and assume that $\alpha_1, \ldots, \alpha_n$ are pairwise distinct points in $\mathbb{F}_q$. If the secret is 0, sample uniformly a random element $\beta \in \mathbb{F}_q$ and distribute to every player the symbol β. If the secret is 1, sample uniformly at random a line $P(x) = ax + b$ where $a \neq 0$ and distribute to the i-th player, the symbol $P(\alpha_i)$. The reconstruction is straightforward. Given two shares, x and y, if $x = y$ then output 0 and otherwise output 1. It is easy to see that for every secret $s \in \{0, 1\}$ and every $i \in [n]$, the probability that the i-th player is given the share $\beta \in \mathbb{F}_q$ is $1/q$.

A fully anonymous perfect (n, n) scheme with one-bit shares. Let $s \in \{0, 1\}$ be a secret. Choose uniformly at random a vector $v \in \{0, 1\}^n$ such that $\sum_{i=1}^{n} v_i \equiv s \pmod 2$ and distribute to the i-th player the symbol v_i. Reconstruction is obvious. Given $v_1, \ldots, v_n$, in any order, compute the sum of all the elements over $\mathbb{F}_q$. Also here, it is easy to see that the anonymity condition, i.e., Condition 1 of Definition 1.2 holds for any $n - 1$ shares in any order.

2.2 A simple scheme for arbitrary access structures

In this section, we focus on arbitrary access structures. We first give a formal definition, analogous to Definition 1.2, of fully anonymous secret sharing schemes for general access structures.

Definition 2.1. *Let $\mathcal{A} \subseteq 2^{[n]}$ be an access structure. A* fully anonymous secret sharing scheme for $\mathcal{A}$ *with share alphabet Ω has the following two properties:*

1. *(Share anonymity) For every secret $s \in \{0,1\}$, every unauthorized $U \notin \mathcal{A}$, every ordering of the elements of U, and every $\mathbf{v} \in \Omega^{|U|}$, we have*

$$\Pr_{\mathrm{sh} \leftarrow \mathtt{Share}(s)}[\mathrm{sh}_U = \mathbf{v}] = |\Omega|^{-|U|} .$$

2. *(Perfect anonymous reconstruction) There exists a deterministic function* `Recon` *(possibly non-efficient) such that for every secret $s \in \{0,1\}$, every $A \in \mathcal{A}$, every ordering of the elements of A, and every* sh *in the support of* $\mathtt{Share}(s)$*, it holds that* $\mathtt{Recon}(\mathrm{sh}_A) = s$.

We prove Theorem 1.5, which is restated next.

Theorem 1.5. *Any access structure $\mathcal{A} \subseteq 2^{[n]}$ has a perfect, fully anonymous secret-sharing scheme for one-bit secrets. If the number of authorized sets in $\mathcal{A}$ is ℓ, then each participant receives an ℓ^2-bit share.*

In particular, for all integers $1 \le t \le n$, there is an explicit fully anonymous (t,n) secret-sharing scheme with share alphabet $\{0,1\}^m$, where $m = \binom{n}{t}^2$.

Before describing the anonymous secret sharing scheme, let us describe a naive attempt. That is, using additive secret sharing. Let $\mathcal{A} \subseteq 2^{[n]}$ be an access structure. A simple secret sharing scheme for $\mathcal{A}$ is simply to share the secret independently for each authorized set $A \in \mathcal{A}$ using the (n,n) threshold scheme described above.

In more details, let $s \in \{0,1\}$ be the secret. Independently, for every authorized set $A \in \mathcal{A}$, sample the vector $(B_{A,i})_{i \in [n]}$ uniformly from the set

$$\Omega_{A,s} = \left\{ b \in \{0,1\}^n \;\middle|\; \bigoplus_{i \in A} b_i = s \right\} .$$

Equivalently, the bits indexed by A form a uniformly random additive sharing of s, while the remaining bits are independent and uniformly distributed. Next, for each $i \in [n]$, the share of participant i is simply the vector $S^i = (S^i_A)_{A \in \mathcal{A}}$ of length $|\mathcal{A}|$, defined by $S^i_A = B_{A,i}$. It is not hard to see that the joint distribution of shares of any unauthorized set is uniform.

For reconstruction, let $S^{i_1}, \ldots, S^{i_k}$ be k shares held by an authorized set $A = \{i_1, \ldots, i_k\}$ and let $S = S^{i_1} \oplus \cdots \oplus S^{i_k}$. It is not hard to see that $S_A = s$ is the secret. However, without knowing the identity of the authorized set A, the value of s is undetermined, as many entries of S may equal $1 - s$.

To reduce the error probability, one may consider parallel repetition. Let T be a large enough integer and, for each set $A \in \mathcal{A}$, sample T independent vectors $B^1_{A,i}, \ldots, B^T_{A,i}$.

Now, give each participant i a matrix S^i of size $|\mathcal{A}| \times T$, defined by $S^i_{A,j} = B^j_{A,i}$ for any $A \in \mathcal{A}$ and $j \in [T]$. The joint distribution of shares of any unauthorized set is still uniform as this is just T dependent samples from the same distribution as before.

As before, for authorized set $A = \{i_1, \ldots, i_k\}$, we let $S = S^{i_1} \oplus \cdots \oplus S^{i_k}$. Now, the *entire row* $S_{A,*}$ is equal to s^T. Moreover, the probability that there is another row A' for which $S_{A',*} = (1-s)^T$ is extremely unlikely ($\leq |\mathcal{A}| \cdot 2^{-T}$), and thus we can reconstruct s with overwhelming probability without knowing A. However, we want perfect reconstruction, which we do not achieve yet.

We observe that an error may occur only when the matrix S has both an all-zero row and an all-one row simultaneously, which can happen with positive probability. However, a matrix can never have both all-zero row and an all-one *column* at the same time. This is the main observation yielding the following scheme.

We now describe the scheme. Fix an access structure $\mathcal{A} \subseteq 2^{[n]}$.

Sharing the secret. Let $s \in \{0,1\}$ be the secret. Independently, for every ordered pair $(A_1, A_2) \in \mathcal{A}^2$, sample the vector $(B_{A_1,A_2,i})_{i\in[n]}$ uniformly from the set

$$\left\{ b \in \{0,1\}^n \;\middle|\; \bigoplus_{i \in A_1} b_i = s \right\}.$$

Equivalently, the bits indexed by A_1 form a uniformly random additive sharing of s, while the remaining bits are independent and uniformly distributed.

For each $i \in [n]$, let M_i be the $|\mathcal{A}| \times |\mathcal{A}|$ matrix whose rows and columns are indexed by sets in $\mathcal{A}$, and where $(M_i)_{A_1,A_2} = B_{A_1,A_2,i}$. The dealer gives participant i the share

$$\mathrm{sh}_i := \begin{cases} M_i, & \text{if } s = 0, \\ M_i^\top, & \text{if } s = 1. \end{cases}$$

Reconstructing the secret. Given shares $S^1, \ldots, S^k$ for an authorized set $A \in \mathcal{A}$, compute $S = S^1 \oplus \cdots \oplus S^k$. If S has an all-zero row, output 0 and otherwise, output 1.

Proof of theorem 1.5. We will show that this scheme satisfies the two properties of Definition 2.1.

Perfect reconstruction. Let $S^{i_1}, \ldots, S^{i_k}$ be k shares of an authorized set $A = \{i_1, \ldots, i_k\}$ and let $S = S^{i_1} \oplus \cdots \oplus S^{i_k}$. By construction, if $s = 0$, then the row corresponding to A in S is an all-zero row, and if $s = 1$, then the column corresponding to A is an all-one column. The claim follows by observing that one cannot have an all-zero row and an all-one column in the same matrix.

Full anonymity. Assume that $s = 0$. Let $S^{i_1}, \ldots, S^{i_k}$ be k shares of an unauthorized set $U = \{i_1, \ldots, i_k\}$. For every pair $A_1, A_2 \in \mathcal{A}$, we have that $(B_{A_1,A_2,i})_{i\in U}$ is uniformly distributed over $\{0,1\}^{|U|}$. This follows from the fact that $\mathcal{A}$ is monotone, which implies that $A_1 \not\subseteq U$, and thus for any fixed vector of values on U, there are exactly $2^{n-|U|-1}$ ways to complete the vector $(B_{A_1,A_2,i})_{i\in[n]}$ such that $\bigoplus_{i\in A_1} B_{A_1,A_2,i} = 0$. Also, recall that the sampling process acts independently for every pair $(A_1, A_2) \in \mathcal{A}^2$. Hence, the matrices $S^{i_1}, \ldots, S^{i_k}$ are independent, uniformly random matrices over $\{0,1\}^{|\mathcal{A}|\times|\mathcal{A}|}$. The claim for $s = 1$ is similar.

For the "in particular" part, observe that for the threshold access structure, it is enough to consider only minimal authorized sets (in contrast to any authorized set in the above construction). Also, note that in this case, once the reconstructor gets at least t shares, it chooses exactly t of them and reconstructs for these t shares. Now, the matrix M_i has dimensions $\binom{n}{t} \times \binom{n}{t}$. Thus, each share has length $\binom{n}{t}^2$ bits. □

3 Efficient fully anonymous $(3, n)$ scheme

In this section, we prove Theorem 1.3, restated next.

Theorem 1.3. *Let $n \geq 4$ be an integer. There exists an explicit fully anonymous $(3, n)$ secret-sharing scheme for one-bit secrets, where the share length is $2\lceil \log n \rceil$. The reconstruction algorithm runs in $\mathrm{poly}(\log n)$ time.*

We first reduce the proof to the case where the number of participants is a power of two. Given an arbitrary integer $n \geq 4$, let $N := 2^{\lceil \log n \rceil}$. Apply the construction below to N participants and discard the shares of any fixed $N - n$ participants. Every ordered pair of the remaining shares is still uniformly distributed, and every ordered triple still reconstructs the secret. Hence, the restricted scheme is a fully anonymous $(3, n)$ threshold secret-sharing scheme. Moreover, $2 \log N = 2\lceil \log n \rceil$ and $\mathrm{poly}(\log N) = \mathrm{poly}(\log n)$. Thus, it suffices to prove the theorem when n is a power of two. Throughout the remainder of this section, assume that n is a power of two and set $q := n$.

In Section 3.1, we prove two auxiliary claims. Then, in Section 3.2, we present the scheme, namely, the sharing and reconstruction algorithms. In Section 3.3, we prove the correctness of the scheme, i.e., that reconstruction always succeeds and that the properties given in Definition 1.2 hold.

Definition 3.1. *We say that the polynomials $P(x) = ax^2 + bx + e$ and $Q(x) = cx^2 + dx + f$ are* degenerate *if $ad - bc = 0$ and* non-degenerate *otherwise. Furthermore, we define*

$$\mathcal{S} := \{(P, Q) \in (\mathbb{F}_q[x]_{\leq 2})^2 \mid ad - bc \neq 0\}.$$

That is, $\mathcal{S}$ is the set of all non-degenerate pairs (P, Q).

3.1 Auxiliary claims about $\mathcal{S}$

Claim 3.2. *Let $\alpha, \beta \in \mathbb{F}_q$ be distinct and let $(P, Q) \in \mathcal{S}$. Then, $(P(\alpha), Q(\alpha)) \neq (P(\beta), Q(\beta))$.*

Proof. It holds that

$$\begin{pmatrix} P(\alpha) - P(\beta) \\ Q(\alpha) - Q(\beta) \end{pmatrix} = (\alpha - \beta) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \alpha + \beta \\ 1 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

since $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \neq 0$ and $\alpha \neq \beta$. □

Claim 3.3. *We have*

1. *For every $\alpha \in \mathbb{F}_q$ and every $v \in \mathbb{F}_q^2$, we have*

$$\Pr_{(P,Q)\sim_U \mathcal{S}}[(P(\alpha), Q(\alpha)) = v] = \frac{1}{q^2} .$$

2. *For $\alpha, \beta \in \mathbb{F}_q$ where $\alpha \neq \beta$ and for $u, v \in \mathbb{F}_q^2, u \neq v$, we have*

$$\Pr_{(P,Q)\sim_U \mathcal{S}}[(P(\alpha), Q(\alpha)) = v \text{ and } (P(\beta), Q(\beta)) = u] = \frac{1}{q^2(q^2-1)} .$$

Here, $X \sim_U T$ means that X is sampled uniformly from the finite set T.

Proof. First note that $|\mathcal{S}| = q^2(q^2-1)(q^2-q)$. Indeed, there are q^2 choices for (e, f), there are $q^2 - 1$ choices for $(a, b) \neq (0, 0)$, and there are $q^2 - q$ choices for (c, d) that are not a scalar multiple of (a, b).

For the first item, for every choice of (a, b, c, d) satisfying $ad - bc \neq 0$, the condition $(P(\alpha), Q(\alpha)) = v$ uniquely determines (e, f). Hence, there are exactly $(q^2-1)(q^2-q)$ pairs $(P, Q) \in \mathcal{S}$ satisfying $(P(\alpha), Q(\alpha)) = v$. Dividing by $|\mathcal{S}|$ gives the probability $1/q^2$.

For the second item, write $u = (u_1, u_2)$ and $v = (v_1, v_2)$. Since $\alpha \neq \beta$, for every choice of (a, c), the conditions $(P(\alpha), Q(\alpha)) = v$ and $(P(\beta), Q(\beta)) = u$ uniquely determine

$$b = \frac{u_1 - v_1}{\beta - \alpha} - a(\alpha + \beta) \qquad \text{and} \qquad d = \frac{u_2 - v_2}{\beta - \alpha} - c(\alpha + \beta),$$

and then uniquely determine (e, f) from the evaluation at α. Moreover,

$$ad - bc = \frac{a(u_2 - v_2) - c(u_1 - v_1)}{\beta - \alpha}.$$

Since $u \neq v$, the condition $ad - bc = 0$ is a nonzero linear equation in (a, c) and therefore has exactly q solutions. Thus, exactly $q^2 - q$ choices of (a, c) give a non-degenerate pair (P, Q). Dividing by $|\mathcal{S}|$ gives

$$\frac{q^2 - q}{q^2(q^2-1)(q^2-q)} = \frac{1}{q^2(q^2-1)}.$$

□

3.2 Scheme

Sharing the secret. Let $\alpha_1, \ldots, \alpha_n$ be any distinct points in $\mathbb{F}_q$. The randomized function `Share` takes a secret s as input and acts as follows.

- $s = 0$. Sample P, Q independently and uniformly from $\mathbb{F}_q[x]_{\leq 1}$, and set $\texttt{Share}_i = (P(\alpha_i), Q(\alpha_i))$ for every $i \in [n]$.
- $s = 1$. In this case, sample the ordered pair (P, Q) uniformly from $\mathcal{S}$. Now, independently of the chosen pair, sample $Y \sim \mathrm{Ber}((n-1)/q^2)$ and act as follows:
  1. $Y = 1$, the *matching option*. Independently sample a uniformly random perfect matching M of $[n]$; write every edge as (i, j) with $i < j$, and set $\texttt{Share}_i = \texttt{Share}_j = (P(\alpha_i), Q(\alpha_i))$.
  2. $Y = 0$, the *non-matching option*. Set $\texttt{Share}_i = (P(\alpha_i), Q(\alpha_i))$ for every $i \in [n]$.

Reconstructing the secret. Given an ordered sequence of at least three shares, apply the following rule to its first three entries $(x_1, y_1), (x_2, y_2), (x_3, y_3)$: output 0 if one of the following conditions holds:

1. All the points are equal.
2. All the points are distinct *and* the points reside on a line, namely, it holds that

$$(y_1 - y_2) \cdot (x_2 - x_3) = (x_1 - x_2) \cdot (y_2 - y_3) \ . \tag{2}$$

Otherwise, output 1.

3.3 Correctness

Proposition 3.4. *Reconstruction always succeeds.*

Proof. Assume the secret is zero and that $P(x) = ax + b, Q(x) = cx + d$ are two linear functions that are not both constant, i.e., $a \neq 0$ or $c \neq 0$. Then, given any three shares, in any order,

$$(P(\alpha), Q(\alpha)),\ (P(\beta), Q(\beta)),\ (P(\gamma), Q(\gamma)) \ .$$

One can easily verify that (2) holds. Here α, β, γ are distinct, and since $(a, c) \neq (0, 0)$, the identity $(P(u) - P(v), Q(u) - Q(v)) = (u - v)(a, c) \neq (0, 0)$ for $u \neq v$ shows that the three shares are pairwise distinct. If both P and Q are constant, then the first condition of the reconstruction holds.

Now, assume that the secret is 1. We will show that `Recon` cannot output 0. The claim will follow. Let $P(x) = ax^2 + bx + e$ and $Q(x) = cx^2 + dx + f$ be polynomials of degree at most 2 with $ad - bc \neq 0$. For three distinct participants, let α, β, γ denote the evaluation parameters actually used to generate their shares. In the non-matching option they are distinct, while in the matching option each parameter is used at most twice, so $|\{\alpha, \beta, \gamma\}| \in \{2, 3\}$. Consider the set

$$S = \{(P(\alpha), Q(\alpha)), (P(\beta), Q(\beta)), (P(\gamma), Q(\gamma))\} \ .$$

First assume that $|S| = 1$, i.e., all the points are equal. This implies that $P(\alpha) = P(\beta) = P(\gamma)$ and $Q(\alpha) = Q(\beta) = Q(\gamma)$. Clearly, if $|\{\alpha, \beta, \gamma\}| = 3$, then $P(x) = e$ is constant (also $Q(x)$ is constant) and this contradicts the condition that $ad - bc \neq 0$. If $|\{\alpha, \beta, \gamma\}| = 2$, then assume w.l.o.g. that $\alpha \neq \beta$ and since $|S| = 1$, we have $(P(\alpha), Q(\alpha)) = (P(\beta), Q(\beta))$. This contradicts Claim 3.2.

If $|S| = 2$, then `Recon` automatically outputs 1. Thus, we are left to check the case where $|S| = 3$. Note that this implies that $|\{\alpha, \beta, \gamma\}| = 3$. Assume that the points in S are collinear. Then,

$$(Q(\alpha) - Q(\beta))(P(\beta) - P(\gamma)) = (P(\alpha) - P(\beta))(Q(\beta) - Q(\gamma)) \ ,$$

which implies that

$$(\alpha - \beta)(\beta - \gamma)(\alpha - \gamma)(ad - bc) = 0 \ .$$

Thus, $ad - bc = 0$, in contradiction. □

Proposition 3.5. *For every $s \in \{0,1\}$, every distinct $i, j \in [n]$, and every $u, v \in \mathbb{F}_q^2$,*

$$\Pr[(\mathit{Share}_i, \mathit{Share}_j) = (u, v)] = q^{-4}.$$

Proof. First suppose that $s = 0$. Write $u = (u_1, u_2)$ and $v = (v_1, v_2)$. For $\alpha_i \neq \alpha_j$, the map $(a, b) \mapsto (P(\alpha_i), P(\alpha_j))$ where $P(x) = ax + b$ is a bijection from $\mathbb{F}_q^2$ to $\mathbb{F}_q^2$. Thus, $\Pr[(P(\alpha_i), P(\alpha_j)) = (u_1, v_1)] = q^{-2}$; independently, $\Pr[(Q(\alpha_i), Q(\alpha_j)) = (u_2, v_2)] = q^{-2}$. Hence

$$\Pr[(\mathtt{Share}_i, \mathtt{Share}_j) = (u, v)] = q^{-4}.$$

Now suppose that $s = 1$. First, consider $u = v$. By Claim 3.2, two shares can be equal only if (i) the matching option is selected and (ii) i is matched to j. Therefore, by the first item of Claim 3.3,

$$\Pr[(\mathtt{Share}_i, \mathtt{Share}_j) = (u, u)] = \frac{n-1}{q^2} \cdot \frac{1}{n-1} \cdot \frac{1}{q^2} = q^{-4}.$$

Now consider $u \neq v$. In the matching option, i and j must belong to different matching edges. Since different matching edges have distinct smaller endpoints, the two shares are evaluations at distinct field points. This occurs with probability $(n-2)/(n-1)$. Thus, by the second item of Claim 3.3,

$$\begin{aligned}
\Pr[(\mathtt{Share}_i, \mathtt{Share}_j) = (u, v)] &= \left(\frac{n-1}{q^2} \cdot \frac{n-2}{n-1} + \left(1 - \frac{n-1}{q^2}\right) \right) \frac{1}{q^2(q^2-1)} \\
&= \left(\frac{n-2}{q^2} + \frac{q^2 - n + 1}{q^2} \right) \frac{1}{q^2(q^2-1)} \\
&= q^{-4}.
\end{aligned}$$

□

We are now ready to prove the theorem of this section.

Proof of Theorem 1.3. We have to verify both conditions of Definition 1.2. Proposition 3.5 proves that every ordered pair of shares is uniform over $(\mathbb{F}_q^2)^2$. For every $i \in [n]$ and every $u \in \mathbb{F}_q^2$, choose $j \neq i$.

The reconstruction proposition, Proposition 3.4, shows that every valid triple reconstructs the secret. Since the reconstruction algorithm on longer inputs applies the three-share test to the first three entries, perfect reconstruction holds for every input of length at least 3.

Since $q = n$, each share in $\mathbb{F}_q^2$ contains exactly $2 \log n$ bits; reconstruction uses $O(1)$ field operations and therefore $\mathrm{poly}(\log n)$ bit operations. □

4 Existential proof for threshold access structures

In this section, we prove Theorem 1.4. Namely, we show that fully anonymous perfect (t, n) secret sharing schemes exists with $O(t \log n)$-bit shares.

Theorem 1.4. *For every pair of integers $1 \leq t \leq n$, there exists a fully anonymous (t, n) threshold secret-sharing scheme one-bit secrets with share alphabet $\{0,1\}^m$, where $m = O(t \log n)$.*

We begin by describing the construction. Let $[n]$ be the set of parties. In the following, we assume that $t \geq 2$ since otherwise there is a trivial scheme. Let $\mathbb{F}_q$ be a field of characteristic two and large enough size q (to be chosen later) with distinct points $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$.

Secret 0**:** Choose a uniformly random polynomial f of degree $\leq t-2$ and set the i-th share $\mathrm{sh}_i = f(\alpha_i)$.

Now, define

$$\mathcal{D}_0 := \left\{ (a_1, \ldots, a_t) : \begin{array}{l} \exists j_1 \neq \ldots \neq j_t \text{ and } f \in \mathbb{F}_q[x]_{\leq t-2} \\ \text{such that } (a_1, \ldots, a_t) = \big(f(\alpha_{j_1}), \ldots, f(\alpha_{j_t})\big) \end{array} \right\}.$$

Secret 1**:** Let $F \subseteq \mathbb{F}_q^n$ be the set of shares having *some* t-subset whose shares lies in $\mathcal{D}_0$. Namely,

$$F = \Big\{ y \in \mathbb{F}_q^n : \ \exists A \subseteq [n],\ |A| = t,\ y_A \in \mathcal{D}_0 \Big\}. \tag{3}$$

Let μ_1 be a distribution supported on $\mathbb{F}_q^n \setminus F$ whose marginals on any $t-1$ coordinates are uniform. Sample the shares from the distribution μ_1.

Decoding: given a tuple M of t field elements, output 0 if $M \in \mathcal{D}_0$ and 1 otherwise.

Assuming such a distribution μ_1 exists, the correctness of this scheme, as well as the anonymity, follows by construction. Indeed, the reconstruction procedure does not use the identity of the parties, and thus is anonymous. Moreover, the distribution of shares of any $t-1$ parties for $s = 0$ is uniform, and thus satisfying the share anonymity property for this case. Finally, the reconstruction procedure always outputs 0 for shares produced by the sharing protocol for $s = 0$, and 1 otherwise, and therefore correctness is also satisfied. The rest of this section is dedicated to proving the existence of such a distribution μ_1.

4.1 Cylinders and Anonymity

In order to construct the distribution μ_1, we will need the notion of cylinder. For a vector $x \in \mathbb{F}_q^n$ and a set $J \subseteq [n]$, the J-cylinder around x, denoted by $\Gamma(J, x)$, is the set of all $q^{n-|J|}$ vectors that agree with x on the set J, namely,

$$\Gamma(J, x) = \{ y \in \mathbb{F}_q^n \colon y_J = x_J \}.$$

Observe that to show that the marginal distribution of any $t-1$ shares in μ_1 is uniform, we need to show the following. For any shares $\mathrm{sh}_1, \ldots, \mathrm{sh}_n$, and any set of $t-1$ parties $J = \{j_1, \ldots, j_{t-1}\}$,

$$\sum_{\mathrm{sh}' \in \Gamma(J, \mathrm{sh})} \Pr_{\mu_1}[\mathrm{sh}'] = \Pr_{\mu_1}[\mathrm{sh}_{j_1}, \ldots \mathrm{sh}_{j_{t-1}}] = \frac{1}{q^{t-1}}$$

or equivalently,

$$\mathbb{E}_{\mathrm{sh}' \leftarrow \Gamma(J, \mathrm{sh})}[\Pr_{\mu_1}[\mathrm{sh}']] = 1/q^n.$$

To prove that such a distribution exists with support disjoint to F, we need the notion of sparsity. In the following, let $S = \mathbb{F}_q$ and $\mathcal{U} = \mathbb{F}_q^n$.

Definition 4.1 (Cylinder sparsity)**.** *$F \subseteq \mathcal{U}$ is (k, δ)-*cylinder-sparse *if for every $J \subseteq [n]$ with $|J| \leq k$ and every $x \in \mathcal{U}$,*

$$\frac{|F \cap \Gamma(J, x)|}{|\Gamma(J, x)|} \leq \delta.$$

The crux of our proof is the following theorem.

Theorem 4.2. *Let $k < n$, let $F \subseteq \mathcal{U}$ be $(k, (2n)^{-k-1})$-cylinder-sparse. Then there exists a probability distribution on $\mathcal{U}$, supported in $\mathcal{U} \setminus F$, all of whose marginals on at most k coordinates are uniform.*

We prove theorem 4.2 in section 4.2. But first let us use it to prove theorem 1.4. We will need the following lemma.

Lemma 4.3. *Assume $2 \leq t \leq n \leq q$ and $\alpha_1, \ldots, \alpha_n$ distinct. Let F be the set of vectors defined in (3). Then, F is $\left(t-1,\ n^{2t}/q\right)$-cylinder-sparse.*

Proof of lemma 4.3. Fix J with $|J| \leq t-1$ and let $x \in \mathbb{F}_q^n$ be any point. We will show that to specify any $y \in F \cap \Gamma(J, x)$, it is enough to specify $2t$ indices in $[n]$, together with $n - 1 - |J|$ field elements in $\mathbb{F}_q$. This implies that there are at most $n^{2t} q^{n-1-|J|}$ such y's, while the size of $\Gamma(J, x)$ is $q^{n-|J|}$. In other words, F is $(t-1, \frac{n^{2t}}{q})$ sparse.

Fix $y \in F \cap \Gamma(J, x)$. Since $y_J = x_J$, to specify y it is enough to specify the value of y_i for any $i \notin J$. However, by definition of F, there are indices $j_1 \neq \ldots \neq j_t$ and $i_1 \neq \ldots \neq i_t$, such that

$$(y_{i_1}, \ldots, y_{i_t}) = (f(\alpha_{j_1}), \ldots, f(\alpha_{j_t}))$$

for some $t-2$ degree polynomial f. Since $|J| \leq t-1$, there is an index $k \in [t]$ such that $i_k \notin J$. Finally, since f is a $t-2$ degree polynomial, it follows that the value of $f(\alpha_{j_k})$ is determined by $(f(\alpha_{j_1}), \ldots, f(\alpha_{j_{k-1}}), f(\alpha_{j_{k+1}}), \ldots f(\alpha_{j_t}))$, and thus the value of y_{i_k} is determined by $y_1, \ldots, y_{i_{k-1}}, y_{i_{k+1}}, \ldots, y_n$, together with the indices $j_1 \neq \ldots \neq j_t$ and $i_1 \neq \ldots \neq i_t$. It follows that we can specify y by specifying y_i for any $i \notin J \cup \{i_k\}$, together with $2t$ indices. □

Proving theorem 1.4. We are now ready to prove theorem 1.4

Proof of theorem 1.4. Let q be the smallest power of 2 with $q > (2n)^{3t+1}$. The correctness of the scheme is promised by construction, as well as the security when the secret is 0. By lemma 4.3 and theorem 4.2, there is a distribution μ_1 such that the scheme is secure for secret 1. Finally, observe that

$$\log q \leq (3t+1)\log(2n) + 1 = O(t \log n).$$

□

4.2 Proving theorem 4.2

Recall that to prove the theorem, it is enough to find a distribution with support disjoint from F, such that for any shares $\mathrm{sh}_1, \ldots, \mathrm{sh}_n$, and any set of $t-1$ parties $J = \{j_1, \ldots, j_{t-1}\}$,

$$\mathbb{E}_{\mathrm{sh}' \leftarrow \Gamma(J,\mathrm{sh})}[\Pr_{\mu_1}[\mathrm{sh}']] = 1/q^n.$$

The above implies that to find the desired distribution μ_1, it is enough to find a function $w \colon \mathbb{F}_q^n \to \mathbb{R}$, such that:

1. $w(\mathrm{sh}) \geq 0$ for every $\mathrm{sh} \in \mathbb{F}_q^n$,
2. $w(\mathrm{sh}) = 0$ for every $\mathrm{sh} \in F$, and
3. $\mathbb{E}_{\mathrm{sh}' \leftarrow \Gamma(J,\mathrm{sh})}[w(\mathrm{sh}')] = 1$ for any $|J| \leq t-1$ and $\mathrm{sh} \in \mathbb{F}_q^n$.

Such a function is enough to conclude the proof by choosing $\Pr_{\mu_1}[\mathrm{sh}] = w(\mathrm{sh})/q^n$. The crux of the proof is proving that such a function w exists for any set F which is sparse on every small cylinder. We prove the following lemma.

Lemma 4.4. *Let $k < n$, let $F \subseteq \mathcal{U}$ be (k, δ)-cylinder-sparse for $\delta = (2n)^{-k-1}$. Then there exists $w : \mathcal{U} \to \mathbb{Q}$ with*
(i) $w(x) = 0$ for any $x \in F$;
(ii) $w(x) \geq 0$ for any x;
(iii) $\mathbb{E}_{\mathrm{sh}' \leftarrow \Gamma(J,x)}[w(\mathrm{sh}')] = 1$ for every x and every J with $|J| \leq k$.

We note that the number of linear constraints (i) and (iii) introduce is $|F| + \binom{n}{\leq k}$ in total, which is, by our choice of parameters, much smaller than $|\mathcal{U}| = q^n$. Thus, we might have enough degrees of freedom for w to satisfy (ii). We prove lemma 4.4 below, but first let us use it to prove theorem 4.2.

Proof of theorem 4.2. Taking $J = \emptyset$ in (iii) gives $|S|^{-n} \sum_y w(y) = 1$, so $\mu = |S|^{-n} w$ is a valid probability distribution which vanishes on F by (i). For $|J| \leq k$, (iii) give $\sum_{y \in \Gamma(J,x)} w(y) = |S|^{n-|J|}$, i.e. $\sum_{y \in \Gamma(J,x)} \mu(y) = |S|^{-|J|}$: the marginal on the coordinates in J is exactly uniform. □

Before proving lemma 4.4 we will write item (iii) a bit differently. We will make use of *Efron–Stein decomposition* [ES81] (also known as Hoeffding decomposition, or ANOVA decomposition, see [O'D14]). We start with the definition of the conditional expectation operator E_J.

Definition 4.5 (Conditional expectation)**.** *For $J \subseteq [n]$ and $g : \mathcal{U} \to \mathbb{Q}$ define $E_J g : \mathcal{U} \to \mathbb{Q}$ by*

$$(E_J g)(x) \;=\; \frac{1}{|S|^{n-|J|}} \sum_{y \in \Gamma(J,x)} g(y) \;=\; \frac{1}{|\mathcal{U}|} \sum_{y \in \mathcal{U}} g\big((x_i)_{i \in J}, (y_i)_{i \notin J}\big),$$

where $((x_i)_{i \in J}, (y_i)_{i \notin J})$ denotes the word equal to x on J and to y off J.

We note that the operator E_J is linear and thus can be represented by an $|\mathcal{U}| \times |\mathcal{U}|$ matrix (where we identify a function $g\colon \mathcal{U} \to \mathbb{Q}$ with a vector $\mathbb{Q}^{\mathcal{U}}$).

For a set $T \subset [n]$, let Δ_T be the T-projection

$$\Delta_T = \sum_{I \subseteq T} (-1)^{|T|-|I|} E_I.$$

The Efron–Stein decomposition states that any function g can be written as

$$g = \sum_{T \subseteq [n]} \Delta_T g.$$

Using this notation, item (iii) in lemma 4.4 can be written simply as $E_J w \equiv 1$ for every $|J| \leq k$.

Remark 4.6. *[Hoeffding decomposition vs. Fourier Transform] $E_J g$ equivalently does the following: write g as a sum of Fourier characters $g = \sum_{a \in \mathbb{F}_q^n} \hat{g}(a)\chi_a$ (where $\chi_a : \mathcal{U} \to \mathbb{C}$). Then $E_J g$ filters for the Fourier characters with support in J: $E_J g = \sum_{a \in \mathbb{F}_q^n : supp(a) \subset J} \hat{g}(a)\chi_a$. By the Inclusion/Exclusion principle, Δ_T filters for terms with support* exactly *T: $\Delta_T g = \sum_{a \in \mathbb{F}_q^n : supp(a) = T} \hat{g}(a)\chi_a$. Under this interpretation, it is clear that $g = \sum_{T \subseteq [n]} \Delta_T g$. See [ES81, O'D14, KLLM24] for more details.*

The rest of this section is dedicated for proving lemma 4.4. In the following, write $w(x) = 1 - a'(x)$, where $w(x) = 1$ represents the uniform distribution over $\mathbb{F}_q^n$, and a' is the difference, or the residual of w from the uniform distribution. We want to find a' such that

- $a'(x) \leq 1$ for any sh (so that $w(\text{sh}) \geq 0$),
- $a'(x) = 1$ for any $x \in F$ (so that $w(x) = 0$), and
- $E_J a'(x) = 0$ for any x and any $|J| \leq k$.

We find such a function a by solving a linear equation system. In particular, we construct a matrix Z, such that for any function $a\colon \mathbb{F}_q^n \to \mathbb{R}$ (represented as a vector of dimension q^n), the function $a' = Za$ fulfills the third requirement above. Then we add the linear constraint that $a'(x) = 1$ for any $x \in F$ to find a solution $a' = Za$ that satisfies the second requirement. By bounding the norm of the matrix, we prove that any such solution satisfies also the first condition.

In more details, let $V = \mathbb{Q}^F$, a finite-dimensional $\mathbb{Q}$-vector space, let $X_F : V \to \mathbb{Q}^{\mathcal{U}}$ be extension by zero and $R_F : \mathbb{Q}^{\mathcal{U}} \to V$ be the restriction on F. That is, for $v \in V$, $X_F(v) \in \mathbb{Q}^{\mathcal{U}}$, where $X_F(v)_x = v_x$ if $x \in F$ or 0 otherwise. Similarly, for $u \in \mathbb{Q}^{\mathcal{U}}$, $R_F(u) \in V$ is the vector defined by $R_F(u)_x = u_x$ for all $x \in F$. Let $Q_k = \sum_{|T| \leq k} \Delta_T$.[2] We will need the following claim, proved in section 4.3.

Claim 4.7. *If $|J| \leq k$ then $E_J Q_k = E_J$.*

[2]Note that using remark 4.6, $Q_k g = \sum_{a \in \mathbb{F}_q^n : |supp(a)| \leq k} \hat{g}(a)\chi_a$. That is, Q_k filters the small Fourier coefficients. claim 4.7 easily follows by this interpretation.

Note that the above claim implies that for $Z = (I - Q_k)$, $E_J Z = 0$, and thus for every $a' = Za$ it holds that $E_J a' = E_J Z a = 0$. Finally, let

$$T := R_F \, Q_k \, X_F : V \to V.$$

Observe that T is a linear operator because X_F, Q_k and R_F are. Our goal is to show that there is a solution to the equation $(I - T)a = \mathbf{1}$. We will prove the following claim.

Claim 4.8. *For every $a \in V$ and every $M \geq 0$ with $\|a\|_\infty \leq M$ we have,*

$$\|Q_k X_F a\|_\infty \leq M/4, \qquad \textit{hence} \qquad \|Ta\|_\infty \leq 1/4 \cdot \|a\|_\infty.$$

In particular, the matrix $(I - T)$ has a full rank.

That is, claim 4.8 states that Q_k reduces the norm of any function $X_F a$ supported only on F, which follows by the fact that F is (k, δ)-cylinder sparse. We prove claim 4.8 next, but first let us use it to prove lemma 4.4.

Proof of lemma 4.4. By claim 4.8, there is a solution to the linear equation $(I - T)a = \mathbf{1}$. Let a be the solution, and let $M = \|a\|_\infty$. By definition we have that $a = Ta + \mathbf{1}$, and thus

$$M = \|a\|_\infty = \|Ta + \mathbf{1}\|_\infty \leq \|Ta\|_\infty + 1 \leq M/4 + 1,$$

where the last inequality holds by claim 4.8. We get that

$$M \leq 4/3. \tag{4}$$

Recall that by the definition of $T = R_F Q_k X_F$, and since $(I - T)a = \mathbf{1}$, we have that

$$a(y) - \big(Q_k X_F a\big)(y) = 1 \quad \text{for all } y \in F. \tag{5}$$

We now define the function w. Let

$$w := \mathbf{1} - Z X_F a = \mathbf{1} - (X_F - Q_k X_F)a.$$

(i). To see that the first property holds, observe that for $y \in F$, $X_F a(y) = a(y)$ and, by (5), $(Q_k X_F a)(y) = a(y) - 1$. Thus,

$$w(y) = 1 - a(y) + a(y) - 1 = 0.$$

(ii). To see the second property, observe that if $y \notin F$ then $X_F a(y) = 0$ and thus $w(y) = 1 + Q_k X_F a$. By claim 4.8 and (4), $(Q_k X_F a)(y) \geq -M/4 \geq -1/3$. Therefore

$$w(y) \geq \; 1 - 1/3 > \; 0.$$

(iii). Finally, for $|J| \leq k$, by the linearity of E_J we have that

$$E_J w = E_J \mathbf{1} - (E_J X_F - E_J Q_k X_F)a.$$

Since $E_J \mathbf{1} = \mathbf{1}$, and since by claim 4.7 $E_J Q_k = E_J$, we get that

$$E_J w = \mathbf{1} - (E_J X_F - E_J X_F)a = \mathbf{1}.$$

□

Proving claim 4.8. We now prove claim 4.8.

Proof of claim 4.8. First, notice that for any x, $|X_F a(x)| \leq M\mathbf{1}_F(x)$. By the definition of E_I and the triangular inequality, we get that for every J,

$$\left|(E_J X_F a)(x)\right| \leq E_J|(X_F a)|(x) \leq E_J(M\mathbf{1}_F)(x) \leq M(E_J\mathbf{1}_F)(x).$$

In particular, since every cylinder fixing at most k coordinates meets F in at most a δ-fraction, i.e. $(E_J\mathbf{1}_F)(x) \leq \delta$ for all $|J| \leq k$ and all x, then $|(E_J X_F a)(x)| \leq \delta M$.

By definition of Q_k,

$$Q_k(X_F a) = \sum_{|T|\leq k} \sum_{J\subseteq T} (-1)^{|T|-|J|} E_J(X_F a).$$

and thus by the triangular inequality,

$$\begin{aligned}
\|Q_k(X_F a)\|_\infty &\leq \sum_{|T|\leq k} \sum_{J\subseteq T} \|E_J(X_F a)\|_\infty \\
&\leq \sum_{|T|\leq k} \sum_{J\subseteq T} \delta M \\
&= \delta M \sum_{s=0}^{k} \binom{n}{s} 2^s \\
&\leq \delta M \cdot n^k \cdot 2^{k+1} = M/n.
\end{aligned}$$

Note that we can assume that $n \geq 4$ as for $n \leq 3$, we have already fully anonymous (t, n) secret sharing schemes for $t \in \{1, 2, 3\}$. Finally, to see that the matrix $(I - T)$ has a full rank, we will show that the kernel of $(I - T)$ is empty. Indeed, assume toward a contradiction this is not the case. That is, there is a vector $a \neq 0$ such that $(I - T)a = 0$. In other words, $a = Ta$. Let $M = \|a\|_\infty$. Then $M = \|a\|_\infty = \|Ta\|_\infty \leq M/4$, and therefore $M = 0$, and $a = 0$. □

4.3 Proving claim 4.7

To prove claim 4.7 we need to prove some basic properties of Δ_T.

Lemma 4.9. *The following hold.*

1. $E_J E_K = E_{J\cap K}$ *for all* $J, K \subseteq [n]$.
2. *For every* $J \subseteq [n]$, $\sum_{T\subseteq J} \Delta_T = E_J$.
3. *Let* $J, T \subseteq [n]$. *Then* $E_J\Delta_T = \Delta_T$ *if* $T \subseteq J$, *and* $E_J\Delta_T = 0$ *otherwise.*

Proof.

1. Write $\sigma_K(u,v)_i = u_i$ if $i \in K$ and v_i otherwise. Then

$$(E_J E_K g)(x) = \frac{1}{|\mathcal{U}|^2} \sum_{y \in \mathcal{U}} \sum_{z \in \mathcal{U}} g\big(\sigma_K(\,\sigma_J(x,y)\,, z)\big).$$

   Observe that $\sigma_K(\sigma_J(x,y),z)_i = x_i$ if $i \in J \cap K$, y_i if $i \in K \setminus J$, and z_i if $i \notin K$. Let $y' \in \mathcal{U}$ be defined by $y'_i = y_i$ if $i \in K \setminus J$ or z_i otherwise. Let $z' \in \mathcal{U}$ be defined similarly by $z'_i = z_i$ if $i \in K \setminus J$ or y_i otherwise. We can write

$$(E_J E_K g)(x) = \frac{1}{|\mathcal{U}|^2} \sum_{y' \in \mathcal{U}} \sum_{z' \in \mathcal{U}} g\big(\sigma_{J\cap K}(x,y')\big) = \frac{1}{|\mathcal{U}|} \sum_{y' \in \mathcal{U}} g\big(\sigma_{J\cap K}(x,y')\big) = (E_{J\cap K} g)(x).$$

2. Observe that

$$\sum_{T \subseteq J} \Delta_T = \sum_{T \subseteq J} \sum_{I \subseteq T} (-1)^{|T|-|I|} E_I = \sum_{I \subseteq J} \Big(\sum_{I \subseteq T \subseteq J} (-1)^{|T|-|I|} \Big) E_I.$$

   For fixed $I \subseteq T \subseteq J$, write $T = I \cup U$ for $U \subseteq J \setminus I$. Then

$$\sum_{I \subseteq J} \Big(\sum_{I \subseteq T \subseteq J} (-1)^{|T|-|I|} \Big) E_I = \sum_{I \subseteq J} \Big(\sum_{U \subseteq J \setminus I} (-1)^{|U|} \Big) E_I.$$

   Lastly, note that $\sum_{U \subseteq J\setminus I} (-1)^{|U|}$ equals 1 if $I = J$ and 0 otherwise.

3. By the first property, $E_J \Delta_T = \sum_{I \subseteq T} (-1)^{|T|-|I|} E_{J\cap I}$. If $T \subseteq J$ then $J \cap I = I$ for every $I \subseteq T$ and we recover Δ_T. Otherwise pick $p \in T \setminus J$ and pair each $I \subseteq T \setminus \{p\}$ with $I \cup \{p\}$. Since $p \notin J$ we have $J \cap (I \cup \{p\}) = J \cap I$, while the signs $(-1)^{|T|-|I|}$ and $(-1)^{|T|-|I|-1}$ are opposite; the two terms of each pair cancel.

□

We are now ready to prove claim 4.7.

Proof of claim 4.7. By the last item of lemma 4.9, $E_J \Delta_T$ vanishes unless $T \subseteq J$; and every $T \subseteq J$ satisfies $|T| \leq |J| \leq k$, so it occurs in Q_k. Hence $E_J Q_k = \sum_{T \subseteq J} E_J \Delta_T = \sum_{T \subseteq J} \Delta_T = E_J$ by the second property of lemma 4.9. □

AI Disclosure: As mentioned above, Theorems 1.5 and 1.4 were found by ChatGPT 5.6 Sol Ultra. Theorem 1.3 was found by the authors without use of AI. The authors verified and streamlined the proofs on their own and take full responsibility for their correctness.

References

[Bei11] Amos Beimel. Secret-sharing schemes: A survey. In *International conference on coding and cryptology*, pages 11–46. Springer, 2011.

[BGI+25] Allison Bishop, Matthew Green, Yuval Ishai, Abhishek Jain, and Paul Lou. Fully anonymous secret sharing. In *Annual International Cryptology Conference*, pages 356–389. Springer, 2025.

[Bla79] George Robert Blakley. Safeguarding cryptographic keys. In *Managing requirements knowledge, international workshop on*, pages 313–313. IEEE Computer Society, 1979.

[BS97] Carlo Blundo and Douglas R Stinson. Anonymous secret sharing schemes. *Discrete Applied Mathematics*, 77(1):13–28, 1997.

[CGLZ25] Roni Con, Zeyu Guo, Ray Li, and Zihan Zhang. Random Reed-Solomon Codes Achieve the Half-Singleton Bound for Insertions and Deletions over Linear-Sized Alphabets. In Keren Censor-Hillel, Fabrizio Grandoni, Joël Ouaknine, and Gabriele Puppis, editors, *52nd International Colloquium on Automata, Languages, and Programming (ICALP 2025)*, volume 334 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 60:1–60:21, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[Con25] Roni Con. Anonymous shamir's secret-sharing via reed-solomon codes against permutations, insertions, and deletions. *IEEE Transactions on Information Theory*, 2025.

[EBG+24] Harry Eldridge, Gabrielle Beck, Matthew Green, Nadia Heninger, and Abhishek Jain. {Abuse-Resistant} location tracking: Balancing privacy and safety in the offline finding ecosystem. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 5431–5448, 2024.

[ES81] Bradley Efron and Charles Stein. The jackknife estimate of variance. *The Annals of Statistics*, pages 586–596, 1981.

[GMO03] Mida Guillermo, Keith M Martin, and Christine M O'Keefe. Providing anonymity in unconditionally secure secret sharing schemes. *Designs, Codes and Cryptography*, 28:227–245, 2003.

[KLLM24] Peter Keevash, Noam Lifshitz, Eoin Long, and Dor Minzer. Hypercontractivity for global functions and sharp thresholds. *Journal of the American Mathematical Society*, 37(1):245–279, 2024.

[KOKO02] Wataru Kishimoto, Koji Okada, Kaoru Kurosawa, and Wakaha Ogata. On the bound for anonymous secret sharing schemes. *Discrete Applied Mathematics*, 121(1-3):193–202, 2002.

[O'D14] Ryan O'Donnell. *Analysis of boolean functions*, volume 2. Cambridge University Press Cambridge, 2014.

[PCO20] Anat Paskin-Cherniavsky and Ruxandra F Olimid. On cryptographic anonymity and unpredictability in secret sharing. *Information Processing Letters*, 161:105965, 2020.

[PP92] Steven J Phillips and Nicholas C Phillips. Strongly ideal secret sharing schemes. *Journal of Cryptology*, 5:185–191, 1992.

[Sha79] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[SV88] Douglas R Stinson and Scott A Vanstone. A combinatorial approach to threshold schemes. *SIAM Journal on Discrete Mathematics*, 1(2):230–236, 1988.

[ZSZG26] Yijun Zhang, Yubo Sun, Xiande Zhang, and Gennian Ge. Random reed–solomon codes correcting permutations, insertions, and deletions over polynomial-size alphabets. *arXiv preprint arXiv:2606.22344*, 2026.