

Access Structure Hiding Secret Sharing from Novel Set Systems and Vector Families[†]

Vipin Singh Sehrawat^{1‡§} and Yvo Desmedt^{2,3§}

¹ Seagate Technology, Singapore
{vipin.sehrawat.cs@gmail.com}

² The University of Texas at Dallas, Richardson, USA

³ University College London, London, UK

Abstract. Secret sharing provides a means to distribute shares of a secret such that any authorized subset of shares, specified by an access structure, can be pooled together to recompute the secret. The standard secret sharing model requires public access structures, which violates privacy and facilitates the adversary by revealing high-value targets. In this paper, we address this shortcoming by introducing *hidden access structures*, which remain secret until some authorized subset of parties collaborate. The central piece of this work is the construction of a set-system \mathcal{H} with strictly greater than $\exp\left(c \frac{1.5(\log h)^2}{\log \log h}\right)$ subsets of a set of h elements. Our set-system \mathcal{H} is defined over \mathbb{Z}_m , where m is a non-prime-power, such that the size of each set in \mathcal{H} is divisible by m but the sizes of their pairwise intersections are not divisible by m , unless one set is a subset of another. We derive a vector family \mathcal{V} from \mathcal{H} such that superset-subset relationships in \mathcal{H} are represented by inner products in \mathcal{V} . We use \mathcal{V} to “encode” the access structures and thereby develop the first *access structure hiding* secret sharing scheme. For a setting with ℓ parties, our scheme supports $2^{\binom{\ell}{2}+1}$ out of the $2^{2^{\ell}-O(\log \ell)}$ total monotone access structures, and its maximum share size for any access structures is $(1 + o(1)) \frac{2^{\ell+1}}{\sqrt{\pi \ell/2}}$. The scheme assumes semi-honest polynomial-time parties, and its security relies on the Generalized Diffie-Hellman assumption.

Keywords: Computational Secret Sharing · Hidden Access Structures · Computational Hiding · Computational Secrecy · Extremal Set Theory.

[†] This is the full version of the paper that appears in D. Kim et al. (Eds.): COCOON 2020, LNCS 12273, pp. 246-261. DOI: 10.1007/978-3-030-58150-3_20. This version contains tighter bounds on the (maximum) share size, and the total number of access structures supported.

[‡] Work done while the author was a PhD candidate at The University of Texas at Dallas, USA.

[§] Research partially supported by NPRP award NPRP8-2158-1-423 from the Qatar National Research Fund (a member of The Qatar Foundation). The statements made herein are solely the responsibility of the authors.

1 Introduction

A secret sharing scheme [58, 8, 36] is a method by which a dealer, holding a secret string, distributes strings, called shares, to parties such that authorized subsets of parties, specified by a public access structure, can reconstruct the secret. Secret sharing is the foundation of multiple cryptographic tools (in addition to its obvious use in secure storage), including threshold cryptography [23], (secure) multiparty computation [48], attribute-based encryption [32], generalized oblivious transfer [63], perfectly secure message transmission [25], anonymous communications [57], e-voting [56, 39] and e-auctions [35, 11]. The extensive survey by Beimel [5] gives a review of the notable results in the area.

The maximum share size in the original secret sharing schemes for general/arbitrary access structures [36] is $2^{\ell-1}$, where ℓ is the total number of parties. While for specific access structures, the share size of the later schemes [12, 38, 59] is less than the share size for the scheme from [36], the share size of all schemes for general access structures remained $2^{\ell-o(\ell)}$ until 2018. In 2018, Liu and Vaikuntanathan [45] (using results from [47]) constructed a secret sharing scheme for general access structures with share size $2^{0.944\ell}$. Applebaum et al. [2] (using results of [1, 47]) improved those results, and constructed a secret sharing scheme for general access structures with share size $2^{0.637\ell+o(\ell)}$. Whether the share size can be improved to $2^{o(\ell)}$ (or even smaller) remains an important open problem. On the other hand, multiple works [9, 14, 19, 20, 66] have proved various lower bounds for secret sharing with the best being $\Omega(\ell^2/\log \ell)$ from Csirmaz [19].

1.1 Motivation

Existing secret sharing model requires the access structure to be known to the parties. Since secret reconstruction requires shares of any authorized subset, from the access structure, having a public access structure reveals the high-value targets, which can lead to compromised security in the presence of malicious parties. Having a public access structure also implies that some parties must publicly consent to the fact that they themselves are not trusted.

Need for Hidden Access Structures: Consider a scenario where Alice dictates her will/testament and instructs her lawyer that each of her 15 family members should receive a valid “share” of the will. In addition, the shares should be indistinguishable from each other in terms of size and entropy. She also insists that in order to reconstruct her will, {Bob, Tom, Catherine} or {Bob, Cristine, Keri, Roger} or {Rob, Eve} must be part of the collaborating set. But, Alice does not want to be in the bad books of her other, less trusted family members. So, she demands that the shares of her will and the procedure to reconstruct it back from the shares must not reveal her “trust structures”, until after the will is successfully reconstructed. This problem can be generalized to secret sharing, but with *hidden access structures*, which remain secret until some authorized subset of parties collaborate.

Superpolynomial Size Set-Systems and Efficient Cryptography: In this paper, we demonstrate that set-systems with specific intersections can be used to enhance existing cryptographic protocols, particularly the ones

meant for distributed security. In order to minimize the computational cost of cryptographic protocols, it is desirable that parameters such as exponents, moduli and dimensions do not grow too big. For a set-system whose size is superpolynomial in the number of elements over which it is defined, achieving a large enough size requires smaller modulus and fewer number of elements, which translates into smaller dimensions, exponents and moduli for its cryptographic applications.

1.2 Related Work

A limited number of attempts have been made to introduce privacy-preserving features to secret sharing. The first solution that focused on bolstering privacy in secret sharing was called anonymous secret sharing [62], wherein the secret can be reconstructed without the knowledge of which participants hold which shares. In such schemes, secret reconstruction can be carried out by giving the shares to a black box that does not know the identities of the participants holding those shares. However, anonymous secret sharing completely discards parties' identities, which limits its applicability as an extension of secret sharing. Another issue is that the known anonymous secret sharing schemes [62, 51, 10, 40, 53] operate in very restricted settings (e.g. n -out-of- n threshold, 2-out-of- n threshold) or use hard to generate underlying primitives. For instance, the constructions from [62, 10] use resolvable Steiner systems [60]. However, in design theory, resolvable Steiner systems are non-trivial to achieve with a few known results in restricted settings [13, 64, 15, 22, 43, 49, 52, 54, 29, 41, 68, 69]. There are also known impossibility results concerning existence of certain desirable Steiner systems [50]. Other attempts made to realize anonymous secret sharing avoided the hard to generate primitives and instead employed combinatorics [40]. But, they also lead to very restricted and specific thresholds.

Remark 1. Steiner systems have strong connections to a wide range of topics, including statistics, finite group theory, finite geometry, combinatorial design, experimental design, storage systems design, wireless communication, low-density parity-check code design, distributed storage, batch codes, and low-redundancy private information retrieval. For an introduction to the subject, we refer the interested reader to [17, 16].

1.3 Our Contributions

We bolster the privacy guarantees of secret sharing by introducing *hidden access structures*, which remain unknown until some authorized subset of parties collaborate. We develop the first access structure hiding (computational) secret sharing scheme. As the basis of our scheme, we construct a novel set-system, which is defined by the following theorem.

Theorem 1. *Let $\{\alpha_i\}_{i=1}^r$ be $r > 1$ positive integers and $m = \prod_{i=1}^r p_i^{\alpha_i}$ be a positive integer with r different prime divisors: p_1, \dots, p_r . Then there exists $c = c(m) > 0$, such that for every integer $h > 0$, there exists an explicitly constructible non-uniform[¶] set-system \mathcal{H} over a universe of h elements such that the following conditions hold:*

[¶] all member sets do not have equal size

1. $|\mathcal{H}| > \exp\left(c \frac{1.5(\log h)^r}{(\log \log h)^{r-1}}\right),$
2. $\forall H \in \mathcal{H} : |H| = 0 \bmod m,$
3. $\forall G, H \in \mathcal{H}, \text{ where } G \neq H : \text{if } H \subset G \text{ or } G \subset H, \text{ then } |G \cap H| = 0 \bmod m, \text{ else } |G \cap H| \neq 0 \bmod m,$
4. $\forall G, H \in \mathcal{H}, \text{ where } G \neq H \text{ and } \forall i \in \{1, \dots, r\} : |G \cap H| \in \{0, 1\} \bmod p_i^{\alpha_i}.$

(Recall that $a \bmod m$ denotes the smallest non-negative $b = a \bmod m$.) In secret sharing, the family of minimal authorized subsets $\Gamma_0 \in \Gamma$, corresponding to an access structure Γ , is defined as the collection of the minimal sets in Γ . Therefore, Γ_0 forms the *basis* of Γ . Note that Conditions 2 and 3 of Theorem 1 define the superset-subset relations in the set-system \mathcal{H} . We derive a family of vectors $\mathcal{V} \in (\mathbb{Z}_m)^h$ from our set-system \mathcal{H} , that captures the superset-subset relations in \mathcal{H} as (vector) inner products in \mathcal{V} . This capability allows us to capture “information” about any minimal authorized subset $\mathcal{A} \in \Gamma_0$ in the form of an inner product, enabling efficient testing of whether a given subset of parties \mathcal{B} is a superset of \mathcal{A} or not. Since Γ is monotone, $\mathcal{B} \supseteq \mathcal{A}$, for some $\mathcal{A} \in \Gamma_0$, implies that $\mathcal{B} \in \Gamma$, i.e., \mathcal{B} is an authorized subset of parties. Similarly, $\mathcal{B} \not\supseteq \mathcal{A}$, for all $\mathcal{A} \in \Gamma_0$, implies that $\mathcal{B} \notin \Gamma$, i.e., \mathcal{B} is not an authorized subset of parties. We use our novel set-system and vector family to construct the first access structure hiding (computational) secret sharing scheme. We assume semi-honest polynomial-time parties, and reduce the security and privacy guarantees of our scheme to the Generalized Diffie-Hellman assumption [61]. For a setting with ℓ parties, our scheme supports $2^{\binom{\ell}{\ell/2+1}}$ out of the $2^{2^{\ell} - O(\log \ell)}$ total monotone access structures, and its maximum share size for any of those $2^{\binom{\ell}{\ell/2+1}}$ monotone access structures is $(1 + o(1)) \frac{2^{\ell+1}}{\sqrt{\pi \ell/2}}$. Hence, the maximum share size for our access structure hiding secret sharing scheme is greater than the current upper bound of $2^{0.637\ell + o(\ell)}$ [2] on the share size for secret sharing schemes for general access structures.

1.4 Organization

The rest of this paper is organized as follows: we recall the pertinent background and results in Section 2. Section 3 formally defines access structure hiding computational secret sharing. We present the construction of our set-systems and vector families in Section 4, and use them to develop the first access structure hiding computational secret sharing scheme in Section 5. We conclude by describing two open problems.

2 Preliminaries

We begin by recalling an informal definition of the Generalized Diffie-Hellman (GDH) assumption [61]. For a formal definition, see [7]. For a positive integer n , we define $[n] := \{1, \dots, n\}$.

Definition 1 (GDH Assumption: Informal). Let $\{a_1, a_2, \dots, a_n\}$ be a set of n different integers. Given a group G and an element $g \in G$, it is hard to compute $g^{\prod_{i \in [n]} a_i}$ for an algorithm that can query $g^{\prod_{i \in I} a_i}$ for any proper subset $I \subsetneq [n]$.

Definition 2 (Dirichlet's Theorem [24]). For all coprime integers a and q , there are infinitely many primes, p , of the form $p = a \bmod q$.

Definition 3 (Euler's Theorem). Let y be a positive integer and \mathbb{Z}_y^* denote the multiplicative group mod y . Then for every integer c that is coprime to y , it holds that: $c^{\varphi(y)} = 1 \bmod y$, where $\varphi(y) = |\mathbb{Z}_y^*|$ denotes Euler's totient function.

Definition 4 (Hadamard/Schur product). Hadamard/Schur product of two vectors $\mathbf{u}, \mathbf{v} \in \mathcal{R}^n$, denoted by $\mathbf{u} \circ \mathbf{v}$, is a vector in the same linear space whose i -th element is defined as: $(\mathbf{u} \circ \mathbf{v})[i] = \mathbf{u}[i] \cdot \mathbf{v}[i]$, for all $i \in [n]$.

Definition 5 (Negligible Function). For security parameter ω , a function $\epsilon(\omega)$ is called *negligible* if for all $c > 0$ there exists a ω_0 such that $\epsilon(\omega) < 1/\omega^c$ for all $\omega > \omega_0$.

Definition 6 (Computational Indistinguishability [31]). Let $X = \{X_\omega\}_{\omega \in \mathbb{N}}$ and $Y = \{Y_\omega\}_{\omega \in \mathbb{N}}$ be ensembles, where X_ω 's and Y_ω 's are probability distributions over $\{0, 1\}^{\kappa(\omega)}$ for some polynomial $\kappa(\omega)$. We say that $\{X_\omega\}_{\omega \in \mathbb{N}}$ and $\{Y_\omega\}_{\omega \in \mathbb{N}}$ are polynomially/computationally indistinguishable if the following holds for every (probabilistic) polynomial-time algorithm \mathcal{D} and all $\omega \in \mathbb{N}$:

$$\left| \Pr[t \leftarrow X_\omega : \mathcal{D}(t) = 1] - \Pr[t \leftarrow Y_\omega : \mathcal{D}(t) = 1] \right| \leq \epsilon(\omega),$$

where ϵ is a negligible function.

Definition 7 (Access Structure). Let $\mathcal{P} = \{P_1, \dots, P_\ell\}$ be a set of parties. A collection $\Gamma \subseteq 2^{\mathcal{P}}$ is monotone if $\mathcal{A} \in \Gamma$ and $\mathcal{A} \subseteq \mathcal{B}$ imply that $\mathcal{B} \in \Gamma$. An access structure $\Gamma \subseteq 2^{\mathcal{P}}$ is a monotone collection of non-empty subsets of \mathcal{P} . Sets in Γ are called authorized, and sets not in Γ are called unauthorized.

If Γ consists of all subsets of \mathcal{P} with size greater than or equal to a fixed threshold t ($1 \leq t \leq \ell$), then Γ is called a t -threshold access structure.

Definition 8 (Minimal Authorized Subset). For an access structure Γ , a family of minimal authorized subsets $\Gamma_0 \in \Gamma$ is defined as:

$$\Gamma_0 = \{\mathcal{A} \in \Gamma : \mathcal{B} \not\subseteq \mathcal{A} \text{ for all } \mathcal{B} \in \Gamma \setminus \{\mathcal{A}\}\}.$$

Definition 9 (Computational Secret Sharing [42]). A computational secret sharing scheme with respect to an access structure Γ , security parameter ω , a set of ℓ polynomial-time parties $\mathcal{P} = \{P_1, \dots, P_\ell\}$, and a set of secrets \mathcal{K} , consists of a pair of polynomial-time algorithms, **(Share, Recon)**, where:

- **Share** is a randomized algorithm that gets a secret $k \in \mathcal{K}$ and access structure Γ as inputs, and outputs ℓ shares, $\{\Pi_1^{(k)}, \dots, \Pi_\ell^{(k)}\}$, of k ,

- **Recon** is a deterministic algorithm that gets as input the shares of a subset $\mathcal{A} \subseteq \mathcal{P}$, denoted by $\{\Pi_i^{(k)}\}_{i \in \mathcal{A}}$, and outputs a string in \mathcal{K} ,

such that, the following two requirements are satisfied:

1. *Perfect Correctness*: for all secrets $k \in \mathcal{K}$ and every authorized subset $\mathcal{A} \in \Gamma$, it holds that:
 $\Pr[\text{Recon}(\{\Pi_i^{(k)}\}_{i \in \mathcal{A}}, \mathcal{A}) = k] = 1$,
2. *Computational Secrecy*: for every unauthorized subset $\mathcal{B} \notin \Gamma$ and all different secrets $k_1, k_2 \in \mathcal{K}$, it holds that the distributions $\{\Pi_i^{(k_1)}\}_{i \in \mathcal{B}}$ and $\{\Pi_i^{(k_2)}\}_{i \in \mathcal{B}}$ are computationally indistinguishable (with respect to ω).

Remark 2 (Perfect Secrecy). If $\forall k_1, k_2 \in \mathcal{K}$ with $k_1 \neq k_2$, the distributions $\{\Pi_i^{(k_1)}\}_{i \in \mathcal{B}}$ and $\{\Pi_i^{(k_2)}\}_{i \in \mathcal{B}}$ are identical, then the scheme is called a perfect secret sharing scheme.

2.1 Set Systems with Restricted Intersections

The problem of constructing set systems under certain intersection restrictions and bounding their size has a central place in Extremal Set Theory. We shall not give a full account of such problems, but only touch upon the results that are particularly relevant to our set-system and its construction. For a broader account, we refer the interested reader to the survey by Frankl and Tokushige [30].

Lemma 1 ([34]). *Let $m = \prod_{i=1}^r p_i^{\alpha_i}$ be a positive integer with $r > 1$ different prime divisors. Then there exists an explicitly constructible polynomial Q with n variables and degree $O(n^{1/r})$, which is equal to 0 on $z = (1, 1, \dots, 1) \in \{0, 1\}^n$ but is nonzero mod m on all other $z \in \{0, 1\}^n$. Furthermore, $\forall z \in \{0, 1\}^n$ and $\forall i \in \{1, \dots, r\}$, it holds that: $Q(z) \in \{0, 1\} \pmod{p_i^{\alpha_i}}$.*

Theorem 2 ([34]). *Let m be a positive integer, and suppose that m has $r > 1$ different prime divisors: $m = \prod_{i=1}^r p_i^{\alpha_i}$. Then there exists $c = c(m) > 0$, such that for every integer $h > 0$, there exists an explicitly constructible uniform set-system \mathcal{H} over a universe of h elements such that:*

1. $|\mathcal{H}| \geq \exp\left(c \frac{(\log h)^r}{(\log \log h)^{r-1}}\right)$,
2. $\forall H \in \mathcal{H} : |H| \equiv 0 \pmod{m}$,
3. $\forall G, H \in \mathcal{H}, G \neq H : |G \cap H| \not\equiv 0 \pmod{m}$.

Matching Vectors. A matching vector family is a combinatorial object that is defined as:

Definition 10 ([26]). Let $S \subseteq \mathbb{Z}_m \setminus \{0\}$, and $\langle \cdot, \cdot \rangle$ denote the inner product. We say that subsets $\mathcal{U} = \{\mathbf{u}_i\}_{i=1}^N$ and $\mathcal{V} = \{\mathbf{v}_i\}_{i=1}^N$ of vectors in $(\mathbb{Z}_m)^h$ form an S -matching family if the following two conditions are satisfied:

- $\forall i \in [N]$, it holds that: $\langle \mathbf{u}_i, \mathbf{v}_i \rangle \equiv 0 \pmod{m}$,

– $\forall i, j \in [N]$ such that $i \neq j$, it holds that: $\langle \mathbf{u}_i, \mathbf{v}_j \rangle \bmod m \in S$.

The question of bounding the size of matching vector families is closely related to the well-known Extremal Set Theory problem of constructing set systems with restricted modular intersections. Matching vectors have found applications in the context of private information retrieval [6, 4, 27, 26, 28, 67, 46], conditional disclosure of secrets [46], secret sharing [47] and coding theory [26]. The first super-polynomial size matching vector family follows directly from the set-system constructed by Grolmusz [34]. If each set H in the set-system \mathcal{H} defined by Theorem 2 is represented by a vector $\mathbf{u} \in (\mathbb{Z}_m)^h$, then it leads to the following family of S -matching vectors:

Corollary 1 ([26] to Theorem 2). *Let $h, m > 0$, and suppose that $m = \prod_{i=1}^r p_i^{\alpha_i}$ has $r > 1$ different prime divisors. Then, there exists a set S of size 2^{r-1} and a family of S -matching vectors $\{\mathbf{u}\}_{i=1}^N$, $\mathbf{u}_i \in (\mathbb{Z}_m)^h$, such that, $N \geq \exp\left(c \frac{(\log h)^r}{(\log \log h)^{r-1}}\right)$.*

3 Access Structure Hiding Computational Secret Sharing: Definition

In this section, we give a formal definition of an access structure hiding computational secret sharing scheme.

Definition 11. An access structure hiding computational secret sharing scheme with respect to an access structure Γ , a set of ℓ polynomial-time parties $\mathcal{P} = \{P_1, \dots, P_\ell\}$, a set of secrets \mathcal{K} and a security parameter ω , consists of two pairs of polynomial-time algorithms, $(\text{HsGen}, \text{HsVer})$ and $(\text{Share}, \text{Recon})$, where $(\text{Share}, \text{Recon})$ are the same as defined in the definition of computational secret sharing (see Definition 9), and $(\text{HsGen}, \text{HsVer})$ are defined as:

- **HsGen** is a randomized algorithm that gets \mathcal{P} and Γ as inputs, and outputs ℓ *access structure tokens* $\{\mathcal{U}_1^{(\Gamma)}, \dots, \mathcal{U}_\ell^{(\Gamma)}\}$,
- **HsVer** is a deterministic algorithm that gets as input the *access structure tokens* of a subset $\mathcal{A} \subseteq \mathcal{P}$, denoted by $\{\mathcal{U}_i^{(\Gamma)}\}_{i \in \mathcal{A}}$, and outputs $b \in \{0, 1\}$,

such that, the following three requirements are satisfied:

1. *Perfect Completeness*: every authorized subset of parties $\mathcal{A} \in \Gamma$ can identify itself to be a member of the access structure Γ , i.e., formally, it holds that: $\Pr[\text{HsVer}(\{\mathcal{U}_i^{(\Gamma)}\}_{i \in \mathcal{A}}) = 1] = 1$,
2. *Perfect Soundness*: every unauthorized subset of parties $\mathcal{B} \notin \Gamma$ can identify itself to be outside of the access structure Γ , i.e., formally, it holds that: $\Pr[\text{HsVer}(\{\mathcal{U}_i^{(\Gamma)}\}_{i \in \mathcal{B}}) = 0] = 1$,
3. *Computational Hiding*: for all access structures $\Gamma, \Gamma' \subseteq 2^{\mathcal{P}}$, where $\Gamma \neq \Gamma'$, and each subset of parties $\mathcal{B} \notin \Gamma, \Gamma'$ that is unauthorized in both Γ and Γ' , it holds that:

$$\left| \Pr[\Gamma \mid \{\mathcal{U}_i^{(\Gamma)}\}_{i \in \mathcal{B}}, \{\Pi_i^{(k)}\}_{i \in \mathcal{B}}] - \Pr[\Gamma' \mid \{\mathcal{U}_i^{(\Gamma)}\}_{i \in \mathcal{B}}, \{\Pi_i^{(k)}\}_{i \in \mathcal{B}}] \right| \leq \epsilon(\omega),$$

where ϵ is a negligible function and $\{\Pi_i^{(k)}\}_{i \in \mathcal{B}}$ denotes the subset of shares of a secret k , that belong to the parties in \mathcal{B} , and are generated by **Share** with respect to the access structure Γ .

4 Novel Set-Systems and Vector Families

In this section, we construct our novel set-systems and vector families. The following notations are frequently used throughout this section.

- We denote the coefficient of x^k in the power series for $f(x)$ by $[x^k] : f(x)$,
- Let L be an ordered list of a finite number of different symbols, and $u \in L^e$ be a string comprised of $e \in \mathbb{N}$ different symbols from L . We define \triangleright to represent *string membership*, i.e., $j \triangleright u$ denotes that the string u contains the j^{th} symbol from the ordered list L .

4.1 Set System Construction

In this section, we provide the proof for Theorem 1 by giving an explicit construction of the set-system \mathcal{H} defined in it. Our construction is inspired by that of Grolmusz [34].

Proof (Theorem 1). We use the polynomial Q defined in Lemma 1 to construct our set-system. We begin by recalling the following property of Q :

$$Q(z) = 0 \bmod m \iff z_1 = z_2 = \dots = z_n = 1, \quad (4.1)$$

where $z = (z_1, z_2, \dots, z_n) \in \{0, 1\}^n$. We know from Lemma 1 that Q has degree $d = O(n^{1/r})$, and can be written as:

$$Q(z_1, z_2, \dots, z_n) = \sum_{i_1, i_2, \dots, i_l} a_{i_1, i_2, \dots, i_l} z_{i_1} z_{i_2} \dots z_{i_l},$$

where $0 \leq l \leq d$, and $a_{i_1, i_2, \dots, i_l} \in \mathbb{Z}$ with $1 \leq i_1 < i_2 < \dots < i_l \leq n$. Reducing that modulo m , we get:

$$\tilde{Q}(z_1, z_2, \dots, z_n) = \sum_{i_1, i_2, \dots, i_l} \tilde{a}_{i_1, i_2, \dots, i_l} z_{i_1} z_{i_2} \dots z_{i_l}, \quad (4.2)$$

where $\tilde{a}_{i_1, i_2, \dots, i_l} = a_{i_1, i_2, \dots, i_l} \bmod m$. Let $L = (0, 1, \dots, n-1)$ be an ordered list of n symbols. Define a characteristic function $\psi : \{0, 1, \dots, n-1\}^n \rightarrow \{0, 1\}^n$ as:

$$\psi(u)[j] := \begin{cases} 1 & \text{if } j \triangleright u \\ 0 & \text{otherwise,} \end{cases} \quad (4.3)$$

where $1 \leq j \leq n$ and $\psi(u)[j]$ denotes the j^{th} bit of $\psi(u) \in \{0, 1\}^n$. If a string $u \in \{0, 1, \dots, n-1\}^n$, defined over the symbols in L , contains the j^{th} symbol from the ordered list L , then $\psi(u)[j] = 1$, else $\psi(u)[j] = 0$. Define a comparison function $\delta(x, y) : \{0, 1\} \times \{0, 1\} \rightarrow \{0, 1\}$ as:

$$\delta(u, v) := \neg(u \oplus v), \quad (4.4)$$

where \neg and \oplus denote negation and XOR, respectively. Hence, $\delta(u, v) = 1$ if $u = v$, else $\delta(u, v) = 0$. Let $\mathbf{A} = (a_{x,y})$ be a $n^n \times n^n$ matrix ($x, y \in \{0, 1, \dots, n-1\}^n$). For $x' = \psi(x)$ and $y' = \psi(y)$, define each entry $a_{x,y}$ as:

$$a_{x,y} = \tilde{Q}(\delta(x'_1, y'_1), \delta(x'_2, y'_2), \dots, \delta(x'_n, y'_n)) \bmod m, \quad (4.5)$$

where $\tilde{Q}(\cdot)$ is the polynomial defined in Equation 4.2, and x'_j, y'_j denote the j^{th} bit of the binary bit strings $x', y' \in \{0, 1\}^n$. It follows from Equation 4.3, Equation 4.4 and Equation 4.5 that if $a_{x,y} = \tilde{Q}(1, 1, \dots, 1) = 0 \bmod m$, then either $x = y$ or $\forall j \in [n]$ it holds that $y'_j = x'_j$, i.e., x and y are comprised of the same symbols. In both cases, we say that x and y “cover” each other, and denote it by $x \Upsilon y$. We know from Equation 4.2 that the polynomial $\tilde{Q}(z)$ can be defined as a sum of monomials $z_{i_1} z_{i_2} \dots z_{i_l}$ ($l \leq d$), where each monomial $z_{i_1} z_{i_2} \dots z_{i_l}$ occurs with multiplicity $\tilde{a}_{i_1, i_2, \dots, i_l}$ in the sum. Therefore, since matrix \mathbf{A} is generated via \tilde{Q} , it follows from Equation 4.2 that \mathbf{A} can be defined as the sum of matrices $\mathbf{B}_{i_1, i_2, \dots, i_l}$, whose entries are defined as:

$$b_{x,y}^{i_1, i_2, \dots, i_l} = \delta(x'_{i_1}, y'_{i_1}) \delta(x'_{i_2}, y'_{i_2}) \dots \delta(x'_{i_l}, y'_{i_l}). \quad (4.6)$$

Hence, it follows from Equation 4.2, Equation 4.5 and Equation 4.6, that \mathbf{A} can be written as:

$$\mathbf{A} = \sum_{i_1, i_2, \dots, i_l} \tilde{a}_{i_1, i_2, \dots, i_l} \mathbf{B}_{i_1, i_2, \dots, i_l}, \quad (4.7)$$

where $\tilde{a}_{i_1, i_2, \dots, i_l}$ is the multiplicity with which the matrix $\mathbf{B}_{i_1, i_2, \dots, i_l}$ occurs in the sum. Next, we analyze the matrices \mathbf{A} and $\mathbf{B}_{i_1, i_2, \dots, i_l}$. In particular, we count the number of 0 entries in \mathbf{A} and the number of 1 entries in $\mathbf{B}_{i_1, i_2, \dots, i_l}$.

Analysis of the Matrices. We begin by counting the total number of entries $a_{x,y} \in \mathbf{A}$ that are equal to 0, which translates into counting the number of $x, y \in \{0, 1, \dots, n-1\}^n$ such that $x \Upsilon y$.

Let \mathcal{S} be a set of n different symbols. Let *unique symbol weight* (USW) denote the number of different symbols in a string, i.e., $\text{USW}(x) = w(\psi(x))$, where $w(\cdot)$ denotes the Hamming weight. To form a string x of length n such that $\text{USW}(x) = k$, for a fixed $k \leq n$, the first step is to select k distinct symbols $s_{i_1}, s_{i_2}, \dots, s_{i_k}$ from \mathcal{S} . We know from Rosen [55] (Section 2.4.2), that the number of onto functions from a set of n elements to a set of k elements is given by $k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$, where $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ denotes Stirling number of the second kind (see Graham et al. [33], p. 257). Hence, $k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ is the total number of strings of length n , that contain exactly the selected k -out-of- n symbols: $s_{i_1}, s_{i_2}, \dots, s_{i_k}$.

Let N_k denote the total number of different $x \in \{0, 1, \dots, n-1\}^n$ such that $\text{USW}(x) = k$. We know that for a fixed set of k -out-of- n symbols, the number strings $x \in \{0, 1, \dots, n-1\}^n$ satisfying $\text{USW}(x) = k$ is $k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$. Accounting for the number of ways one can choose k -out-of- n symbols, we get:

$$N_k = \binom{n}{k} k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}.$$

We know that for each k , there are N_k rows in matrix \mathbf{A} that “cover” exactly $k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ entries. Hence, from Equation 4.5, the number of $a_{x,y} = 0 \bmod m$ entries in \mathbf{A} is:

$$S(n) = \sum_{k=1}^n N_k \cdot k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} = \sum_{k=1}^n \binom{n}{k} k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}. \quad (4.8)$$

We recall the following well known identities involving the first-order Eulerian numbers (see Graham et al. [33], p. 267) and Stirling numbers of the second kind:

$$\ell! \left\{ \begin{smallmatrix} n \\ \ell \end{smallmatrix} \right\} = \sum_{k=0}^n \left\langle \begin{smallmatrix} n \\ k \end{smallmatrix} \right\rangle \binom{k}{n-\ell}; \quad (n-\ell)! \left\{ \begin{smallmatrix} n \\ n-\ell \end{smallmatrix} \right\} = \sum_{k=0}^n \left\langle \begin{smallmatrix} n \\ k \end{smallmatrix} \right\rangle \binom{k}{\ell},$$

where $\left\langle \begin{smallmatrix} n \\ k \end{smallmatrix} \right\rangle$ denotes the first-order Eulerian number, which gives the total number of permutations $\pi_1, \pi_2, \dots, \pi_n$ with k *ascents*, i.e., k places where $\pi_t < \pi_{t+1}$. Therefore, Equation 4.8 can be rewritten as:

$$\begin{aligned} S(n) &= \sum_{k=0}^n \binom{n}{k} k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} \\ &= \sum_{k=0}^n \binom{n}{k} k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} \sum_{j=0}^n \left\langle \begin{smallmatrix} n \\ j \end{smallmatrix} \right\rangle \binom{j}{n-k} \\ &= n! \sum_{k=0}^n \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} \left(\sum_{j=0}^n \left\langle \begin{smallmatrix} n \\ j \end{smallmatrix} \right\rangle \binom{j}{n-k} \right) \frac{1}{(n-k)!}. \end{aligned}$$

Thus, the exponential generating function for $S(n)$ comes out to be:

$$\sum_{n \geq 0} S(n) \frac{x^n}{n!} = \sum_{n \geq 0} \sum_{k=0}^n \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} x^k \left(\sum_{j=0}^n \left\langle \begin{smallmatrix} n \\ j \end{smallmatrix} \right\rangle \binom{j}{n-k} \right) \frac{x^{n-k}}{(n-k)!}.$$

Recall the following definition of Touchard polynomial (Jacques Touchard [65]):

$$T_n(x) = \sum_{k=0}^n \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} x^k.$$

We write $S(n)$ as:

$$S(n) = n! [x^n] : (T_n(x) P_n(x)), \quad (4.9)$$

where the second polynomial, $P_n(x)$, is defined via convolution as:

$$P_n(x) = \sum_{k=0}^n \left(\sum_{j=0}^n \left\langle \begin{smallmatrix} n \\ j \end{smallmatrix} \right\rangle \binom{j}{k} \right) \frac{x^k}{k!} = \sum_{k=0}^n \frac{(n-k)!}{k!} \left\{ \begin{smallmatrix} n \\ n-k \end{smallmatrix} \right\} x^k.$$

Observe that all diagonal entries $a_{x,x}$ in matrix \mathbf{A} are 0, and \mathbf{A} is symmetric across its diagonal.

Lemma 2. *Let the term B-entries denote the entries $b_{x,y}^{i_1,i_2,\dots,i_l} \in \mathbf{B}_{i_1,i_2,\dots,i_l}$ that are equal to 1. Then the following holds for B-entries:*

1. $\forall x \in \{0, 1, \dots, n-1\}^n$, each entry $a_{x,x} \in \mathbf{A}$ has the same number of B-entries, $b_{x,x}^{i_1,i_2,\dots,i_l} = 1$, and this number is divisible by m ,
2. for each pair x, y ($x, y \in \{0, 1, \dots, n-1\}^n$), the total number of B-entries, $b_{x,y}^{i_1,i_2,\dots,i_l} = 1$, corresponding to $a_{x,y} \in \mathbf{A}$, is divisible by m iff $x \Upsilon y$, else not.

Proof. We know from Equation 4.6 that except for the B-entries, all other entries in matrices $\mathbf{B}_{i_1,i_2,\dots,i_l}$ are equal to 0. Hence, it follows from Equation 4.7 that each entry $a_{x,y} \in \mathbf{A}$ is simply the total number of B-entries, $b_{x,y}^{i_1,i_2,\dots,i_l} = 1$. It further follows from Equation 4.5 and Equation 4.1 that for all x , we get $a_{x,x} = \tilde{Q}(1, 1, \dots, 1) = 0 \bmod m$, i.e., for all x , the total number of B-entries, $b_{x,x}^{i_1,i_2,\dots,i_l} = 1$, is divisible by m . Furthermore, it follows from Equation 4.6 that because $x = x$, all entries $b_{x,x}^{i_1,i_2,\dots,i_l}$ are indeed B-entries and all cells $a_{x,x}$ have the same number of corresponding B-entries, $b_{x,x}^{i_1,i_2,\dots,i_l} = 1$. Finally, it follows from Equation 4.5 and Equation 4.1 that for all pairs (x, y) , where $x \neq y$, the total number of B-entries, $b_{x,y}^{i_1,i_2,\dots,i_l} = 1$, is: $a_{x,y} = \tilde{Q}(1, 1, \dots, 1) = 0 \bmod m$ if $x \Upsilon y$, and $a_{x,y} \neq 0 \bmod m$ otherwise. ■

By taking all $a_{x,y} = 0 \bmod m$ ($\forall x, y \in \{0, 1, \dots, n-1\}^n$) entries of \mathbf{A} to denote sets with the corresponding B-entries, $b_{x,y}^{i_1,i_2,\dots,i_l} = 1$, as the elements in those sets leads to a set-system \mathcal{H} , that satisfies Conditions 2 and 3 of Theorem 1. The number of elements, h , over which \mathcal{H} is defined is:

$$\begin{aligned} h = \tilde{Q}(n, n, \dots, n) &= \sum_{l \leq d} \sum \tilde{a}_{i_1,i_2,\dots,i_l} n^l \leq (m-1) \sum_{l \leq d} \binom{n}{l} n^l \\ &< (m-1) \sum_{l \leq d} n^{2l}/l! < 2(m-1)n^{2d}/d!, \end{aligned}$$

assuming $n \geq 2d$. Since $d > 2$, we get: $n > 4$. From Equation 4.9, it is easy to verify that the following holds for $n > 2$:

$$|\mathcal{H}| = S(n) > n^{1.5n}. \quad (4.10)$$

We know from [34] that for $r > 1, m = \prod_{i=1}^r p_i^{\alpha_i}, d = O(n^{1/r}), c = c(m) > 0$ and $h < 2(m-1)n^{2d}/d!$, the following relation holds:

$$n^n \geq \exp \left(c \frac{(\log h)^r}{(\log \log h)^{r-1}} \right).$$

Therefore, the following can be derived from Equation 4.10 and elementary estimations for binomial coefficients:

$$|\mathcal{H}| > \exp \left(c \frac{1.5(\log h)^r}{(\log \log h)^{r-1}} \right).$$

A tighter bound can be derived by using Lambert \mathcal{W} function [44] and the results from Corless et al. [18] on the principal branch of Lambert \mathcal{W} function, but the bound derived above suffices for our purpose. Since

$m \geq 6$ and $r \geq 2$, the size of our set-system \mathcal{H} is strictly greater than $\exp\left(c \frac{1.5(\log h)^2}{\log \log h}\right)$. Condition 4 of Theorem 1 follows directly from Lemma 1. It is easy to verify that the total number of B-entries corresponding to each cell (x, y) , where $x \neq y$ and for which $a_{x,y} = 0 \pmod m$, is not same. Moreover, since all $b_{x,x}^{i_1, i_2, \dots, i_l}$ entries are indeed B-entries, it holds that $a_{x,y} < a_{x,x}$ for all $x \neq y$. Hence, the sets in \mathcal{H} do not have the same size, making \mathcal{H} a non-uniform set-system. This completes the proof of Theorem 1. \blacksquare

4.2 Covering Vector Families

Definition 12 (Covering Vectors). Let $m, h > 0$ be positive integers, $S \subseteq \mathbb{Z}_m \setminus \{0\}$, and $w(\cdot)$ and $\langle \cdot, \cdot \rangle$ denote Hamming weight and inner product, respectively. We say that a subset $\mathcal{V} = \{\mathbf{v}_i\}_{i=1}^N$ of vectors in $(\mathbb{Z}_m)^h$ forms an S -covering family of vectors if the following two conditions are satisfied:

- $\forall i \in [N]$, it holds that: $\langle \mathbf{v}_i, \mathbf{v}_i \rangle = 0 \pmod m$,
- $\forall i, j \in [N]$, where $i \neq j$, it holds that:

$$\langle \mathbf{v}_i, \mathbf{v}_j \rangle \pmod m = \begin{cases} 0 & \text{if } w(\mathbf{v}_i \circ \mathbf{v}_j \pmod m) = 0 \pmod m \\ \in S & \text{otherwise,} \end{cases}$$

where \circ denotes Hadamard/Schur product (see Definition 4).

Recall from Theorem 1 that h, m are positive integers, with $m = \prod_{i=1}^r p_i^{\alpha_i}$ having $r > 1$ different prime divisors. Further, recall Condition 4 of Theorem 1, which implies that the sizes of the pairwise intersections of the sets in \mathcal{H} occupy at most $2^r - 1$ residue classes modulo m . If each set $H_i \in \mathcal{H}$ is represented by a representative vector $\mathbf{v}_i \in (\mathbb{Z}_m)^h$, then for the resulting subset \mathcal{V} of vectors in $(\mathbb{Z}_m)^h$, the following result follows from Theorem 1.

Corollary 2 (to Theorem 1). *For the set-system \mathcal{H} defined in Theorem 1, if each set $H_i \in \mathcal{H}$ is represented by a unique vector $\mathbf{v}_i \in (\mathbb{Z}_m)^h$, then for a set S of size $2^r - 1$, the set of vectors $\mathcal{V} = \{\mathbf{v}_i\}_{i=1}^N$, formed by the representative vectors of all sets in \mathcal{H} , forms an S -covering family such that $N > \exp\left(c \frac{1.5(\log h)^r}{(\log \log h)^{r-1}}\right)$ and $\forall i, j \in [N]$ it holds that $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = |H_i \cap H_j| \pmod m$.*

5 Our Scheme

In Section 5.1, we introduce an algorithm to encode and identify hidden access structures, that remain unknown unless some authorized subset of parties collaborate. Followed by that, in Section 5.2, we extend that algorithm into an access structure hiding computational secret sharing scheme. We assume semi-honest polynomial-time parties, which try to gain additional information while correctly following the protocols. The following notations are frequently used from hereon.

- If each party P_i holds a value x_i , then for any subset of parties \mathcal{A} , $\{x_i\}_{i \in \mathcal{A}}$ denotes the set of all x_i values that belong to the parties $P_i \in \mathcal{A}$,
- $\prod_{i \in \mathcal{A}} x_i$ and $\sum_{i \in \mathcal{A}} x_i$ respectively denote the product and sum of all values from the set $\{x_i\}_{i \in \mathcal{A}}$,
- large prime: refers to a prime number of size equal to or greater than the minimum size recommended by NIST for primes [3].

5.1 Access Structure Encoding Scheme (ASES)

In this section, we describe our scheme to encode and identify hidden access structures. Let $\mathcal{P} = \{P_1, \dots, P_\ell\}$ be a set of ℓ polynomial-time parties and $\Omega \in \Gamma_0$ be any minimal authorized subset (see Definition 8). Hence, each party $P_i \in \mathcal{P}$ can be identified as $P_i \in \Omega$ or $P_i \in \mathcal{P} \setminus \Omega$.

Setup. The scheme is initialized as follows:

1. For $\eta \geq \ell$, generate a set of distinct large primes, $\{p_1, p_2, \dots, p_\eta\}$. Generate a prime $q = u \prod_{i=1}^{\eta} p_i + 1$, where u is an integer. We know from Dirichlet's Theorem (see Definition 2) that there are infinitely many such primes q . Generating q in this manner ensures hardness of the discrete log problem in \mathbb{Z}_q [37] which, by extension, translates into hardness of the Generalized Diffie-Hellman assumption in \mathbb{Z}_q .
2. Let $w = \prod_{i=1}^{\eta} p_i$ and $m = \varphi(q)$. Then, it follows from $q = u \prod_{i=1}^{\eta} p_i + 1$ that $w | \varphi(q)$, where φ denotes Euler's totient function (see Definition 3). Hence, the following holds for $d \geq 1$ primes β_d and positive integers α_d :

$$m = w \cdot \prod_{d \geq 1} \beta_d^{\alpha_d} = \prod_{i=1}^{\eta} p_i \cdot \prod_{d \geq 1} \beta_d^{\alpha_d}.$$

Let $r = d + \eta > \ell$ denote the total number of prime factors of m .

3. Construct a set-system \mathcal{H} modulo m (as defined by Theorem 1). Let $\mathcal{V} \in (\mathbb{Z}_m)^h$ denote the covering vectors family (as defined by Corollary 2) representing \mathcal{H} such that each vector $\mathbf{v}_i \in \mathcal{V}$ represents a unique set $H_i \in \mathcal{H}$.
4. Randomly sample $H \in \mathcal{H}$. Let $\mathbf{v} \in \mathcal{V}$ be the representative vector for H . We call \mathbf{v} and H the *access structure vector* and *access structure set*, respectively.

Distributing Access Structures. Following procedure “encodes” the access structure Γ that originates from Ω , and outputs ℓ *access structure tokens*.

1. For each party $P_i \in \Omega$, randomly select a unique vector $\mathbf{v}_i \xleftarrow{\$} \mathcal{V}$, such that, $\langle \mathbf{v}, \mathbf{v}_i \rangle \neq 0 \pmod m$ (i.e., $H \not\subseteq H_i$ and $H_i \not\subseteq H$) and $\mathbf{v} = \sum_{i \in \Omega} \mathbf{v}_i \pmod m$. Compute the identifier for party P_i as: $x_i = \langle \mathbf{v}, \mathbf{v}_i \rangle \pmod m$.
2. For each party $P_e \in \mathcal{P} \setminus \Omega$, select a unique *covering party* $P_i \in \Omega$. Let $H_i \in \mathcal{H}$ be the set represented by P_i 's covering vector, $\mathbf{v}_i \in \mathcal{V}$. Randomly sample $H_j \in \mathcal{H}$, such that, $H_i \subset H_j$. Let $\mathbf{v}_j \in \mathcal{V}$ be the covering vector representing H_j .
3. Compute $\mathbf{v}_e \in \mathcal{V}$ such that: $\mathbf{v}_e + \mathbf{v}_i = \mathbf{v}_j \pmod m$. Verify that $\langle \mathbf{v}, \mathbf{v}_e \rangle \neq 0 \pmod m$, which translates into $H \not\subseteq H_e, H_e \not\subseteq H$, for $H_e \in \mathcal{H}$ represented by \mathbf{v}_e . If these requirements do not hold, go back to Step 2.

4. Compute the identifier for party P_e as: $x_e = \langle \mathbf{v}, \mathbf{v}_e \rangle \bmod m$. Generating identifiers in this manner for parties $P_e \in \mathcal{P} \setminus \Omega$ ensures that they are “covered” by the identifiers of parties in Ω . Since each party $P_i \in \Omega$ can “cover” at most one party $P_e \in \mathcal{P} \setminus \Omega$, our scheme requires that $|\mathcal{P}| \leq 2 \cdot |\Omega|$.
5. Each party $P_z \in \mathcal{P}$ receives an *access structure token* $t_z^{(\Gamma)} = \mu^{x_z} \bmod q$, where $\mu \xleftarrow{\$} \mathbb{Z}_q^* \setminus \{1\}$.

In case of an identifier collision, i.e., $x_i = x_j$, where x_j is the identifier of another party $P_j \in \mathcal{P}$, re-generate the identifier for either P_i or P_j . Recall from Corollary 2 that $\langle \mathbf{v}, \mathbf{v}_i \rangle$ occupies $\leq 2^r - 1$ residue classes modulo m . Therefore, the probability of an identifier collision is $\approx 1/(2^r - 1)^2 < 1/(2^\ell - 1)^2$, which may be non-negligible. Since our scheme works with minimal authorized subsets Ω such that $|\Omega| \geq \lceil \ell/2 \rceil$, it supports $2^{\binom{\ell}{\ell/2+1}}$ out of the $2^{2^\ell - O(\log \ell)}$ total monotone access structures over a set of size ℓ .

Access Structure Identification. Theorem 3 proves that any authorized subset of parties $\mathcal{A} \in \Gamma$ can use its set of access structure tokens, $\{t_i^{(\Gamma)}\}_{i \in \mathcal{A}}$, to identify itself as a member of the access structure Γ .

Theorem 3. *Every authorized subset $\mathcal{A} \in \Gamma$ can identify itself as a member of the access structure Γ by verifying that: $\prod_{i \in \mathcal{A}} t_i^{(\Gamma)} = 1 \bmod q$.*

Proof. Recall that for any authorized subset $\mathcal{A} \in \Gamma$, it holds that the set $H_{\mathcal{A}} \in \mathcal{H}$, represented by $\sum_{i \in \mathcal{A}} \mathbf{v}_i = \mathbf{v}_{\mathcal{A}}$, is a superset of the *access structure set* $H \in \mathcal{H}$, i.e., $H \subseteq H_{\mathcal{A}}$. Hence, from Theorem 1 and Corollary 2, it follows that: $\langle \mathbf{v}, \mathbf{v}_{\mathcal{A}} \rangle = 0 \bmod m = y \cdot m = y \cdot \varphi(q)$, where y is a positive integer. This translates into $\mu^{\langle \mathbf{v}, \mathbf{v}_{\mathcal{A}} \rangle} = 1 \bmod q$ (using Euler’s theorem). Hence, the following holds for all authorized subsets $\mathcal{A} \in \Gamma$:

$$\prod_{i \in \mathcal{A}} t_i^{(\Gamma)} = \prod_{i \in \mathcal{A}} \mu^{x_i} = \mu^{\left\langle \mathbf{v}, \sum_{i \in \mathcal{A}} \mathbf{v}_i \right\rangle} = \mu^{\langle \mathbf{v}, \mathbf{v}_{\mathcal{A}} \rangle} = \mu^{y \cdot \varphi(q)} = 1 \bmod q. \quad \blacksquare$$

Perfect Soundness and Computational Hiding.

Theorem 4. *Every unauthorized subset $\mathcal{B} \notin \Gamma$ can identify itself to be outside Γ by using its set of access structure tokens, $\{t_i^{(\Gamma)}\}_{i \in \mathcal{B}}$, to verify that: $\prod_{i \in \mathcal{B}} t_i^{(\Gamma)} \neq 1 \bmod q$. Given that the Generalized Diffie-Hellman problem is hard, the following holds for all unauthorized subsets $\mathcal{B} \notin \Gamma$ and all access structures $\Gamma' \subseteq 2^{\mathcal{P}}$, where $\Gamma \neq \Gamma'$ and $\mathcal{B} \notin \Gamma'$:*

$$\left| \Pr[\Gamma \mid \{t_i^{(\Gamma)}\}_{i \in \mathcal{B}}] - \Pr[\Gamma' \mid \{t_i^{(\Gamma)}\}_{i \in \mathcal{B}}] \right| \leq \epsilon(\omega),$$

where $\omega = |\mathcal{P} \setminus \mathcal{B}|$ is the security parameter and ϵ is a negligible function.

Proof. It follows from the ASES procedure that for all unauthorized subsets $\mathcal{B} \notin \Gamma$, it holds that the set $H_{\mathcal{B}} \in \mathcal{H}$, represented by $\sum_{i \in \mathcal{B}} \mathbf{v}_i = \mathbf{v}_{\mathcal{B}}$, cannot be a superset or subset of the *access structure set* $H \in \mathcal{H}$. Hence, it follows from Theorem 1 and Corollary 2 that: $\langle \mathbf{v}, \mathbf{v}_{\mathcal{B}} \rangle \neq 0 \bmod m$, which translates into the following relation by Euler’s theorem (since $m = \varphi(q)$ and $\mu \xleftarrow{\$} \mathbb{Z}_q^* \setminus \{1\}$):

$$\prod_{i \in \mathcal{B}} t_i^{(\Gamma)} = \prod_{i \in \mathcal{B}} \mu^{x_i} = \mu^{\left\langle \mathbf{v}, \sum_{i \in \mathcal{B}} \mathbf{v}_i \right\rangle} = \mu^{\langle \mathbf{v}, \mathbf{v}_{\mathcal{B}} \rangle} \neq 1 \bmod q.$$

Hence, any unauthorized subset $\mathcal{B} \notin \Gamma$ can identify itself as not being a part of the access structure Γ by simply multiplying its *access structure tokens*, $\{t_i^{(\Gamma)}\}_{i \in \mathcal{B}}$. The security parameter $\omega = |\mathcal{P} \setminus \mathcal{B}|$ accounts for this minimum information that is available to any unauthorized subset $\mathcal{B} \notin \Gamma$.

If some unauthorized subset $\mathcal{B} \notin \Gamma$ has non-negligible advantage in distinguishing access structure Γ from any other $\Gamma' \subseteq 2^{\mathcal{P}}$, where $\Gamma \neq \Gamma'$ and $\mathcal{B} \notin \Gamma'$, then the following must hold for some non-negligible function χ :

$$\left| \Pr[\Gamma \mid \{t_i^{(\Gamma)}\}_{i \in \mathcal{B}}] - \Pr[\Gamma' \mid \{t_i^{(\Gamma)}\}_{i \in \mathcal{B}}] \right| \geq \chi(\omega), \quad (5.1)$$

Let $g \in \mathbb{Z}_q^*$ be a generator of \mathbb{Z}_q^* (recall that \mathbb{Z}_q^* is a cyclic group). We know that the setup procedure used to generate q ensures that: $|\mathbb{Z}_q^*| = \varphi(q) \gg |\mathcal{P}|$. Hence, given that g is a generator of \mathbb{Z}_q^* , it follows that for each identifier x_i , there exists some $a_i \in \mathbb{Z}$ such that: $\mu^{x_i} = g^{a_i} \bmod q$. Therefore, by extension, it follows that for all sets \mathcal{B} , there exists set(s) of n different integers $I_{\mathcal{B}} = \{a_1, \dots, a_n\}$, where $n = |\mathcal{B}|$, such that $\mu^{\sum_{i \in \mathcal{B}} x_i} = g^{\prod_{i=1}^n a_i} \bmod q$. Hence, it holds that: $\prod_{i \in \mathcal{B}} \mu^{x_i} = g^{\prod_{i=1}^n a_i} \bmod q$.

We know that each unauthorized subset $\mathcal{B} \notin \Gamma$ has at least one proper superset $\mathcal{A} \supsetneq \mathcal{B}$, such that $\mathcal{A} \in \Gamma$. Since g is a generator of \mathbb{Z}_q^* , there exists set(s) of n' different integers $I_{\mathcal{A}} = I_{\mathcal{B}} \cup \{a_{n+1}, \dots, a_{n'}\}$, where $n' = |\mathcal{A}|$, such that the following holds: $\prod_{i \in \mathcal{A}} \mu^{x_i} = g^{\prod_{i=1}^{n'} a_i} \bmod q$.

We know that in order to satisfy Equation 5.1, \mathcal{B} must gain some non-negligible information about $g^{\prod_{i=1}^{n'} a_i}$ in \mathbb{Z}_q^* . We also know that \mathcal{B} can compute $g^{\prod_{i=1}^n a_i} \bmod q$. Hence, it follows directly from Definition 1 that gaining any non-negligible information about $g^{\prod_{i=1}^{n'} a_i}$ from $g^{\prod_{i=1}^n a_i}$ in \mathbb{Z}_q^* requires solving the Generalized Diffie-Hellman (GDH) problem. Therefore, Equation 5.1 cannot hold given that the GDH assumption holds. Hence, the advantage of $\mathcal{B} \notin \Gamma$ must be negligible in the security parameter ω . ■

5.2 Building the Full Scheme

The following procedure allows an honest dealer to employ the ASES scheme and realize an access structure hiding computational secret sharing scheme.

1. Perform ASES to generate *access structure tokens* $t_z^{(\Gamma)} = \mu^{x_z} \bmod q$, for each party $P_z \in \mathcal{P}$.
2. Follow Step 1 of the setup procedure of ASES to generate a suitable prime q' .
3. Generate a set-system \mathcal{H}' modulo m' (as defined by Theorem 1), where $m' = \varphi(q')$. Let \mathcal{V}' denote the covering vector family (as defined by Corollary 2) that is formed by the representative vectors $\mathbf{v}_i \in \mathcal{V}$ for the sets $H_i \in \mathcal{H}$.
4. Generate the secret that needs to be shared: $k \xleftarrow{\$} \mathbb{Z}_{q'}^*$, and randomly sample $|\Omega|$ integers, $\{b_i\}_{i=1}^{|\Omega|}$, such that: $\prod_{i=1}^{|\Omega|} b_i = k \bmod q'$.
5. Generate $\gamma \xleftarrow{\$} \mathbb{Z}_{q'}^* \setminus \{1\}$. For each party $P_j \in \mathcal{P} \setminus \Omega$, employ ASES with parameters $\{m', q', \mathcal{H}', \mathcal{V}', \gamma\}$ to generate identifier $y_j \in \mathbb{Z}_m$, and access structure token: $s_j^{(k)} = \gamma^{y_j} \bmod q'$. Party P_j receives $s_j^{(k)}$ as its share.

6. The share for each party $P_i \in \Omega$ is generated as: $s_i^{(k)} = (b_i \cdot \gamma^{y_i}) \bmod q'$. Each party $P_z \in \mathcal{P}$ receives $\langle \text{access structure token, share} \rangle$ pair: $(t_z^{(\Gamma)}, s_z^{(k)})$.

Completeness, Soundness, Correctness, Secrecy and Hiding: We prove that our access structure hiding computational secret sharing scheme satisfies the completeness, soundness, correctness, hiding and secrecy requirements outlined by the definition of Access Structure Hiding Computational Secret Sharing (see Definition 11). Since independent iterations of ASES are used to generate the access structure tokens and shares, perfect completeness follows directly from Theorem 3. Similarly, perfect soundness and computational hiding follow directly from Theorem 4. Hence, we move on to proving perfect correctness and computational secrecy.

Perfect Correctness: It follows directly from Theorem 3 that for all authorized subsets $\mathcal{A} \in \Gamma$, it holds that: $\prod_{i \in \mathcal{A}} \gamma^{y_i} = 1 \bmod q'$. Hence, any $\mathcal{A} \in \Gamma$ can reconstruct the secret, k , by combining its shares as:

$$\prod_{i \in \mathcal{A}} s_i^{(k)} \bmod q' = 1 \cdot \prod_{y \in \Omega} b_y \bmod q' = k, \quad \left(\text{using } \prod_{i \in \mathcal{A}} \gamma^{y_i} = 1 \bmod q' \right).$$

Theorem 5. *The maximum share size of our access structure hiding secret sharing scheme for any access structure is $(1 + o(1)) \frac{2^{\ell+1}}{\sqrt{\pi \ell / 2}}$.*

Proof. Our access structure hiding secret sharing scheme is designed to “encode” minimal authorized subsets. It is easy to verify that the maximum number of unique minimal authorized subsets in any access structure is $\binom{\ell}{\ell/2}$. For each minimal authorized subset, each party $P_z \in \mathcal{P}$ receives two elements, $s_z^{(k)}$ and $t_z^{(\Gamma)}$, both of which have (almost) the same size as the secret. Hence, it follows that the maximum share size for any (supported) access structure is:

$$\begin{aligned} \max \left(\Pi^{(k)} \right) &\approx \binom{\ell}{\ell/2} 2|k| \\ &= (1 + o(1)) \frac{2^{\ell+1}}{\sqrt{\pi \ell / 2}} |k|, \quad \left(\text{using results from [21]} \right). \end{aligned}$$

Hence, the maximum share size with respect to the secret size $|k|$ is: $(1 + o(1)) \frac{2^{\ell+1}}{\sqrt{\pi \ell / 2}}$. ■

Computational Secrecy: Since independent iterations of ASES are used to generate the sets $\{t_z^{(\Gamma)}\}_{z \in \mathcal{P}}$ and $\{s_z^{(k)}\}_{z \in \mathcal{P}}$, computational indistinguishability (w.r.t. security parameter $\omega = |\mathcal{P} \setminus \mathcal{B}|$) of all different access structures $\Gamma, \Gamma' \subseteq 2^{\mathcal{P}}$, for all unauthorized subsets $\mathcal{B} \notin \Gamma, \Gamma'$ follows directly from Theorem 4, i.e., it holds that:

$$\left| Pr[\Gamma \mid \{t_i^{(\Gamma)}\}_{i \in \mathcal{B}}, \{s_i^{(k)}\}_{i \in \mathcal{B}}] - Pr[\Gamma' \mid \{t_i^{(\Gamma)}\}_{i \in \mathcal{B}}, \{s_i^{(k)}\}_{i \in \mathcal{B}}] \right| \leq \epsilon(\omega).$$

Theorem 6. *Given that GDH problem is hard, it holds for every unauthorized subset $\mathcal{B} \notin \Gamma$ and all different secrets $k_1, k_2 \in \mathcal{K}$ that the distributions $\{s_i^{(k_1)}\}_{i \in \mathcal{B}}$ and $\{s_i^{(k_2)}\}_{i \in \mathcal{B}}$ are computationally indistinguishable w.r.t. the security parameter $\omega = |\mathcal{P} \setminus \mathcal{B}|$.*

Proof. Since the set $\{b_i\}_{i=1}^{|\Omega|}$ is generated randomly, secrecy of the b_i values follows from one-time pad. Moving on to the secrecy of γ^{y_i} values: since $\gamma (\neq 1)$ is a random element from $\mathbb{Z}_{q'}^*$, there exists a generator g of $\mathbb{Z}_{q'}^*$ (note that $\mathbb{Z}_{q'}^*$ is a cyclic group) such that for each identifier, y_i , generated by the ASES procedure, there exists an $a_i \in \mathbb{Z}$ such that: $\gamma^{y_i} = g^{a_i} \bmod q'$. By extension, there exists set(s) of n different integers $I_{\mathcal{B}} = \{a_1, \dots, a_n\}$, where $n = |\mathcal{B}|$, such that: $\prod_{i \in \mathcal{B}} \gamma^{y_i} = g^{\prod_{i=1}^n a_i} \bmod q'$. We know that each unauthorized subset $\mathcal{B} \notin \Gamma$ has at least one proper superset $\mathcal{A} \supsetneq \mathcal{B}$, such that $\mathcal{A} \in \Gamma$. Since g is a generator of $\mathbb{Z}_{q'}^*$, there exists set(s) of n' different integers $I_{\mathcal{A}} = I_{\mathcal{B}} \cup \{a_{n+1}, \dots, a_{n'}\}$, where $n' = |\mathcal{A}|$, such that: $\prod_{i \in \mathcal{A}} \gamma^{y_i} = g^{\prod_{i=1}^{n'} a_i} \bmod q'$. It follows from Definition 1 that in order to gain any non-negligible information about $g^{\prod_{i=1}^{n'} a_i}$ from $g^{\prod_{i=1}^n a_i}$, in $\mathbb{Z}_{q'}^*$, \mathcal{B} must solve the GDH problem. Therefore, for every unauthorized subset $\mathcal{B} \notin \Gamma$, computational indistinguishability of $\{s_i^{(k_1)}\}_{i \in \mathcal{B}}$ and $\{s_i^{(k_2)}\}_{i \in \mathcal{B}}$ w.r.t. the security parameter ω follows directly from the GDH assumption. ■

Open Problems

Our access structure hiding secret sharing scheme requires that $|\mathcal{P}| \leq 2|\Omega|$, where $\Omega \in \Gamma_0$ is any minimal authorized subset. It is worth exploring whether this restriction can be further relaxed, or removed. Another interesting problem is defining and constructing set-systems and vector families that can support simultaneous encoding of multiple minimal authorized subsets.

References

1. Benny Applebaum, Amos Beimel, Oriol Farràs, Oded Nir, and Naty Peter. Secret-sharing schemes for general and uniform access structures. In *EUROCRYPT*, pages 441–471, 2019.
2. Benny Applebaum, Amos Beimel, Oded Nir, and Naty Peter. Better secret sharing via robust conditional disclosure of secrets. In *ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 280–293, 2020.
3. Elaine B. Barker, Lidong Chen, Allen L. Roginsky, Apostol T. Vassilev, and Richard Davis. Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography. Special Publication (NIST SP) - 800-56Ar3, 2018.
4. A. Beimel, Y. Ishai, E. Kushilevitz, and I. Orlov. Share conversion and private information retrieval. In *IEEE 27th Conference on Computational Complexity*, pages 258–268, 2012.
5. Amos Beimel. Secret-sharing schemes: A survey. *Coding and Cryptology, Third International Workshop, IWCC*, pages 11–46, 2011.
6. Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. In *TCC*, pages 317–342, 2014. Full Version (2017) available at: <https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/BIKK.pdf>.
7. Eli Biham, D. Boneh, and Omer Reingold. Breaking generalized Diffie-Hellman modulo a composite is no easier than factoring. *Information Processing Letters*, 70(2):83–87, 1999.

8. G.R. Blakley. Safeguarding cryptographic keys. *American Federation of Information Processing*, 48:313–318, 1979.
9. C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro. On the information rate of secret sharing schemes. In *CRYPTO*, pages 149–169, 1992.
10. C. Blundo and D. R. Stinson. Anonymous secret sharing schemes. *Designs, Codes and Cryptography*, 2:357–390, 1996.
11. Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas Jakobsen, Mikkel Kroigaard, Janus Dam Nielsen, Jesper Buus Nielsen, Kurt Nielsen, Jakob Pagter, Michael Schwartzbach, and Tomas Toft. Secure multiparty computation goes live. In *Financial Cryptography and Data Security*, pages 325–343, 2009.
12. Ernest F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.
13. Darryn Bryant and Daniel Horsley. Steiner triple systems without parallel classes. *SIAM J. Discrete Math*, 31(4):693–696, 2017.
14. Renato M. Capocelli, Alfredo De Santis, Luisa Gargano, and Ugo Vaccaro. On the size of shares for secret sharing schemes. *Journal of Cryptology*, 6(3):157–168, 1993.
15. Charles Colbourn, Spyros S. Magliveras, and Rudolf A. Mathon. Transitive steiner and kirkman triple systems of order 27. *Mathematics of Computation*, 58(197):441–450, 1992.
16. Charles J. Colbourn and Jeffrey H. Dinitz. *Handbook of Combinatorial Designs*. Discrete Mathematics and Its Applications. Chapman and Hall/CRC, 2006.
17. Charles J. Colbourn and Alex Rosa. *Triple Systems*. Oxford Mathematical Monographs. Clarendon Press and Oxford University Press, 1999.
18. R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth. On the LambertW function. *Adv. Comput. Math.*, 5:329–359, 1996.
19. László Csirmaz. The dealer’s random bits in perfect secret sharing schemes. *Studia Sci. Math. Hungar.*, 32(3-4):429–437, 1996.
20. László Csirmaz. The size of a share must be large. *Journal of Cryptology*, 10(4):223–231, 1997.
21. Shagnik Das. A brief note on estimates of binomial coefficients. URL: <http://page.mi.fu-berlin.de/shagnik/notes/binomials.pdf>.
22. Louis DeBiasio and Michael Tait. Large monochromatic components in 3-edge-colored steiner triple systems. *Mathematics of Computation*, 28(6):428–444, 2020.
23. Yvo G. Desmedt and Yair Frankel. Shared generation of authenticators and signatures (extended abstract). In *CRYPTO*, pages 457–469, 1991.
24. Peter Gustav Lejeune Dirichlet. Beweis des satzes, dass jede unbegrenzte arithmetische progression, deren erstes glied und differenz ganze zahlen ohne gemeinschaftlichen factor sind, unendlich viele primzahlen enthält [proof of the theorem that every unbounded arithmetic progression, whose first term and common difference are integers without common factors, contains infinitely many prime numbers]. *Abhandlungen der Königlich PreuBischen Akademie der Wissenschaften zu Berlin*, 48:45–71, 1837.
25. Danny Dolev, Cynthia Dwork, Orli Waarts, and Moti Yung. Perfectly secure message transmission. *Journal of the ACM (JACM)*, pages 17–47, 1993.
26. Zeev Dvir, Parikshit Gopalan, and Sergey Yekhanin. Matching vector codes. *SIAM Journal on Computing*, 40(4):1154–1178, 2011.
27. Zeev Dvir and Sivakanth Gopi. 2-server pir with sub-polynomial communication. In *STOC*, pages 577–584, 2015.
28. Klim Efremenko. 3-query locally decodable codes of subexponential length. In *STOC*, pages 39–44, 2009.
29. Asaf Ferber and Matthew Kwan. Almost all Steiner triple systems are almost resolvable. *arXiv: preprint, arXiv:1907.06744*, 2019. **arXiv:1907.06744**.
30. Peter Frankl and Norihide Tokushige. Invitation to intersection problems for finite sets. *J. Combinatorial Theory Series A*, 144, 2016.
31. Shafi Goldwasser and Silvio M Micali. Probabilistic encryption & how to play mental poker keeping secret all partial information. In *STOC*, pages 365–377, 1982.

32. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *13th ACM conference on Computer and Communications Security*, pages 89–98, 2006.
33. Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics, Second Edition*. Addison-Wesley Professional, 1994.
34. Vince Grolmusz. Superpolynomial size set-systems with restricted intersections mod 6 and explicit ramsey graphs. *Combinatorica*, 20:71–86, 2000.
35. Michael Harkavy, J. Doug Tygar, and Hiroaki Kikuchi. Electronic auctions with private bids. In *Proceedings of the 3rd conference on USENIX Workshop on Electronic Commerce*, pages 6–6, 1998.
36. Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret sharing scheme realizing general access structure. In *Globecom*, pages 99–102, 1987.
37. Antoine Joux, Andrew Odlyzko, and Cécile Pierrot. The past, evolving present, and future of the discrete logarithm. *Open Problems in Mathematics and Computational Science*, pages 5–36, 2014.
38. M. Karchmer and A. Wigderson. On span programs. In *Structure in Complexity Theory Conference*, pages 102–111, 1993.
39. Aggelos Kiayias and Moti Yung. The vector-ballot e-voting approach. In *International Conference on Financial Cryptography*, pages 72–89, 2004.
40. Wataru Kishimoto, Koji Okada, Kaoru Kurosawa, and Wakaha Ogata. On the bound for anonymous secret sharing schemes. *Discrete Applied Mathematics*, 121:193–202, 2002.
41. E.S. Kramer and R. Mathon. Proper $S(t, \mathcal{K}, v)$'s for $t \geq 3, v \leq 16, |\mathcal{K}| > 1$ and their extensions. *J. Combin. Des.*, pages 411–425, 1995.
42. Hugo Krawczyk. Secret sharing made short. In *CRYPTO*, pages 136–146, 1993.
43. Matthew Kwan. Almost all Steiner triple systems have perfect matchings. *Proceedings of the London Mathematical Society*, 121(6):1468–1495, 2020.
44. Johann Heinrich Lambert. Observationes variae in mathesin puram. *Acta Helv. Phys. Math. Anat. Bot. Med.*, 3(5), 1758.
45. Tianren Liu and Vinod Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. In *ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 699–708, 2018.
46. Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In *CRYPTO*, pages 758–790, 2017.
47. Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Towards breaking the exponential barrier for general secret sharing. In *EUROCRYPT*, pages 567–596, 2018.
48. Silvio Micali and Phillip Rogaway. Secure computation. In *CRYPTO*, pages 392–404, 1991.
49. Patrick Morris. Random Steiner triple systems. Master's thesis, Freie Universität Berlin, 2017.
50. Patric R.J. Östergård and Olli Pottonen. There exists no Steiner system $S(4,5,17)$. *Journal of Combinatorial Theory, Series A*, 115(8):1570–1573, 2008.
51. Steven J. Phillips and Nicholas C. Phillips. Strongly ideal secret sharing schemes. *Journal of Cryptology*, 5:185–191, Oct. 1992.
52. Nicholar Pippenger and Joel Spencer. Asymptotic behavior of the chromatic index for hypergraphs. *J. Combin. Theory Ser. A*, 51(1):24–42, 1989.
53. Ying pu Deng, Li feng Guo, and Mu lan Liu. Constructions for anonymous secret sharing schemes using combinatorial designs. *Acta Mathematicae Applicatae Sinica*, 23:67–78, January 2007.
54. D. K. Ray-Chaudhuri and R. M. Wilson. Solution of Kirkman's schoolgirl problem. *Combinatorics (Proc. Sympos. Pure Math., Vol. XIX, Univ. California, Los Angeles, Calif., 1968)*, *Amer. Math.Soc., Providence, R.I.*, pages 187–203, 1971.
55. Kenneth H. Rosen. *Handbook of Discrete and Combinatorial Mathematics, Second Edition*. Chapman & Hall/CRC, 2010.
56. Berry Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting. In *CRYPTO*, pages 148–164, 1999.
57. Vipin Singh Sehrawat, Yogendra Shah, Vinod Kumar Choyi, Alec Brusilovsky, and Samir Ferdi. Certificate and signature free anonymity for V2V communications. In *IEEE Vehicular Networking Conference (VNC)*, pages 139–146, 2017.

- 58. Adi Shamir. How to share a secret. *Commun. ACM*, 22:612–613, 1979.
- 59. Gustavus J. Simmons. How to (really) share a secret. In *CRYPTO*, pages 390–448, 1988.
- 60. Jakob Steiner. Combinatorische aufgaben. *J. Reine Angew. Math.*, 45:181–182, 1853.
- 61. Michael Steiner, Gene Tsudik, and Michael Waidner. Diffie-hellman key distribution extended to group communication. In *3rd ACM conference on Computer and Communications Security*, pages 31–37, 1996.
- 62. D. R. Stinson and S. A. Vanstone. A combinatorial approach to threshold schemes. In *CRYPTO*, pages 330–339, 1987.
- 63. Tamir Tassa. Generalized oblivious transfer by secret sharing. *Designs, Codes and Cryptography*, 58:11–21, 2011.
- 64. Luc Teirlinck. Some new 2-resolvable steiner quadruple systems. *Designs, Codes and Cryptography*, pages 5–10, 1994.
- 65. Jacques Touchard. Sur les cycles des substitutions. *Acta Math*, 70(1):243–297, 1939.
- 66. Marten van Dijk. On the information rate of perfect secret sharing schemes. *Des. Codes Cryptography*, 6(2):143–169, 1995.
- 67. Sergey Yekhanin. Towards 3-query locally decodable codes of subexponential length. *Journal of the ACM (JACM)*, 55(1):1–16, 2008.
- 68. J.L. Yucas. Extending $AG(4, 2)$ to $S(4, \{5, 6\}, 17)$. *J. Combin. Des.*, pages 113–117, 1999.
- 69. J.L. Yucas. Extensions of $PG(3, 2)$ with bases. *Australas. J. Combin.*, pages 125–131, 2002.