Secret-Sharing from Robust Conditional Disclosure of Secrets*

Amos Beimel and Naty Peter
Ben-Gurion University of the Negev, Be'er-Sheva, Israel
amos.beimel@gmail.com, naty@post.bgu.ac.il

May 18, 2019

Abstract

A secret-sharing scheme is a method by which a dealer, holding a secret string, distributes shares to parties such that only authorized subsets of parties can reconstruct the secret. The collection of authorized subsets is called an access structure. Secret-sharing schemes are an important tool in cryptography and they are used as a building box in many secure protocols. In the original constructions of secret-sharing schemes by Ito et al. [Globecom 1987], the share size of each party is $\tilde{O}(2^n)$ (where n is the number of parties in the access structure). New constructions of secret-sharing schemes followed; however, the share size in these schemes remains basically the same. Although much efforts have been devoted to this problem, no progress was made for more than 30 years. Recently, in a breakthrough paper, Liu and Vaikuntanathan [STOC 2018] constructed a secret-sharing scheme for a general access structure with share size $\tilde{O}(2^{0.994n})$. The construction is based on new protocols for conditional disclosure of secrets (CDS). This was improved by Applebaum et al. [EUROCRYPT 2019] to $\tilde{O}(2^{0.892n})$.

In this work, we construct improved secret-sharing schemes for a general access structure with share size $\tilde{O}(2^{0.762n})$. Our schemes are linear, that is, the shares are a linear function of the secret and some random elements from a finite field. Previously, the best linear secret-sharing scheme had shares of size $\tilde{O}(2^{0.942n})$. Most applications of secret-sharing require linearity. Our scheme is conceptually simpler than previous schemes, using a new reduction to two-party CDS protocols (previous schemes used a reduction to multi-party CDS protocols).

In a CDS protocol for a function f, there are k parties and a referee; each party holds a private input and a common secret, and sends one message to the referee (without seeing the other messages). On one hand, if the function f applied to the inputs returns 1, then it is required that the referee, which knows the inputs, can reconstruct the secret from the messages. On the other hand, if the function f applied to the inputs returns 0, then the referee should get no information on the secret from the messages. However, if the referee gets two messages from a party, corresponding to two different inputs (as happens in our reduction from secret-sharing to CDS), then the referee might be able to reconstruct the secret although it should not.

To overcome this problem, we define and construct t-robust CDS protocols, where the referee cannot get any information on the secret when it gets t messages for a set of zero-inputs of f. We show that if a function f has a two-party CDS protocol with message size c_f, then it has a two-party t-robust CDS protocol with normalized message size $\tilde{O}(tc_f)$. Furthermore, we show that every function $f : [N] \times [N] \to \{0,1\}$ has a *multi-linear* t-robust CDS protocol with normalized message size $\tilde{O}(t+\sqrt{N})$. We use a variant of this protocol (with t slightly larger than $\sqrt{N}$) to construct our improved linear secret-sharing schemes. Finally, we construct robust k-party CDS protocols for $k > 2$.

*The authors are supported by ISF grant 152/17, by a grant from the Cyber Security Research Center at Ben-Gurion University of the Negev, and by the Frankel center for computer science. The first author is supported by NSF grant no. 1565387, TWC: Large: Collaborative: Computing Over Distributed Sensitive Data. This work was done while the authors were visiting the Simons Institute for the Theory of Computing.

1 Introduction

A secret-sharing scheme is a method by which a dealer, holding a secret string, distributes strings (called shares) to parties such that authorized subsets of parties can reconstruct the secret, while unauthorized subsets get no information on the secret from their shares. Secret-sharing schemes are an important tool in cryptography and they are used as a building box in many secure protocols (in addition to their obvious usage for secure storage), e.g., they are used for secure multiparty computation protocols [18, 29], threshold cryptography [36], access control [51], attribute-based encryption [43, 60], and oblivious transfer [56, 58].

The original and most important secret-sharing schemes, introduced by Blakley [23] and Shamir [55], are threshold secret-sharing schemes, in which the authorized sets are all the sets whose size is larger than some threshold. Ito et al. [45] defined secret-sharing for an arbitrary (monotone) collection of authorized sets (such collection is called an access structure) and described two secret-sharing schemes realizing an arbitrary access structure. For most access structures, the share size in the schemes realizing them is $\tilde{O}(2^n)$ (where n is the number of parties in the access structure). New constructions of secret-sharing schemes followed, e.g., construction based on monotone formulas [20], construction based on monotone span programs [46], and multi-linear secret-sharing schemes [22]. However, the share size in these schemes remains basically the same as the schemes of [45] and no progress was made for more than 30 years. Recently, in a breakthrough paper, Liu and Vaikuntanathan [47] constructed a secret-sharing scheme for a general access structure in which the share size is $\tilde{O}(2^{0.994n})$. This was improved by Applebaum et al. [4] to $\tilde{O}(2^{0.892n})$; this scheme uses combinatorial covers to improve the scheme of [47].

A secret-sharing scheme is linear if the shares are a linear function of the secret and some random elements from a finite field. Alternatively, a secret-sharing scheme is linear if every share is a vector over the field, and for every authorized set, the secret is reconstructed by taking a linear combination of the coordinates of the vectors (i.e., the shares) of the parties in the set. Linearity enables, for example, to sum shares of two secrets s_1 and s_2, and get shares of the secret $s_1 + s_2$ [19]. This observation, together with a protocol that enables multiplication, was used in [18] to construct secure multiparty protocols computing arithmetic circuits. Most applications of secret-sharing require linearity, so it is important to construct linear secret-sharing schemes.

The construction of secret-sharing schemes of [47] is based on new conditional disclosure of secrets (CDS) protocols of [49]. CDS protocols are a cryptographic primitive introduced by Gertner et al. [42]. In a CDS protocol for a function f, there are k parties and a referee; each party holds a private input, a common secret, and a common random string, and sends one message to the referee (without seeing the other messages). The correctness requirement of the protocol is that if the function f applied to the inputs returns 1, then the referee, which knows the inputs, can reconstruct the secret from the messages. The security requirement of the protocol is that if the function f applied to the inputs returns 0, then the referee should get no information on the secret from the messages.

1.1 Our Contribution

Secret-Sharing Schemes for Arbitrary Access Structures. In this work, we construct improved linear secret-sharing schemes for arbitrary access structures:

Theorem. *Every access structure with n parties can be realized by a* linear *secret-sharing scheme with share size $\tilde{O}(2^{0.7616n})$.*

Previously, the best linear secret-sharing scheme for arbitrary access structures was the scheme that is given in [4] (improving on [47]) with shares of size $\tilde{O}(2^{0.942n})$. Furthermore, our secret-sharing scheme is

more efficient than the best known non-linear scheme for arbitrary access structures [47, 4]. Our scheme is conceptually simpler than previous schemes, using a new reduction to two-party CDS protocols (previous schemes used a reduction to multi-party CDS protocols). The share size in every linear secret-sharing scheme for arbitrary access structure is at least $\tilde{\Omega}(2^{n/2})$ (see, e.g., [4]). The share size of our linear scheme is getting closer to this size.

Robust CDS Protocols. In most previous CDS protocols, e.g., the protocols of [42, 41, 12, 11, 17], if the referee gets two messages from a party, corresponding to two different inputs (as happens in our reduction from secret-sharing to CDS), then the referee might be able to reconstruct the secret although it should not.

Example 1.1. Consider the following CDS protocol for the equality function EQ, where $\mathrm{EQ}(x, y) = 1$ if and only if $x = y$ for $x, y \in \{1, 2, 3\}$, which is a special case of a variant of the general linear CDS protocol of [41] (see also Figure 1). In the protocol, the secret is a bit s and the common random string contains three bits r_1, r_2, r_3. The message of the first party when holding $x = 1$ is r_2, r_3, its message when holding $x = 2$ is r_1, r_3, and its message when holding $x = 3$ is r_1, r_2. The message of the second party when holding $y = 1$ is $s \oplus r_2 \oplus r_3$, its message when holding $y = 2$ is $s \oplus r_1 \oplus r_3$, and its message when holding $y = 3$ is $s \oplus r_1 \oplus r_2$. The referee, when getting messages for inputs x, y such that $x = y$, can reconstruct the secret, since it gets two random bits from the first party and the secret masked by these bits from the second party. When the referee gets messages for inputs x, y such that $x \neq y$, it does not get any information on the secret, e.g., when it gets the message on $x = 1$ and $y = 2$, it misses the bit r_1 and cannot unmask s from the message $s \oplus r_1 \oplus r_3$. However, when getting two messages from the first party and one message from the second, the referee can always reconstruct the secret. For example when getting the messages of the first party on $x = 1$ and $x = 2$ and the message of the second party on $y = 3$, the referee can reconstruct the secret s, although $\mathrm{EQ}(1, 3) = \mathrm{EQ}(2, 3) = 0$.

To overcome this problem, we define and construct t-robust CDS protocols. In these protocols, the referee cannot get any information on the secret when it gets t messages for a zero-inputs set of f, that is, when it gets messages for a set of inputs S_i from party P_i (for every $i \in [k]$, where k is the number of parties) such that $f(x_1, \ldots, x_k) = 0$ for every $(x_1, \ldots, x_k) \in S_1 \times \cdots \times S_k$. We present a few constructions of robust CDS protocols: [1]

- We show that if a function f has a two-party CDS protocol for one-bit secrets with message size c_f, then it has a two-party t-robust CDS protocol for one-bit secrets with message size $\tilde{O}(t^2 c_f)$. Furthermore, under the same assumptions, it has a two-party t-robust CDS protocol for secrets of size $\tilde{\Theta}(t)$ with message size $\tilde{O}(t^2 c_f)$. That is, the normalized message size of this two-party t-robust CDS protocol (i.e., the message size per bit of the secret) is only $\tilde{O}(t c_f)$.

- We show that every function $f : [N] \times [N] \to \{0, 1\}$ has a *linear* two-party t-robust CDS protocol for one-bit secrets with message size $\tilde{O}\left((t + \sqrt{N})t\right)$ and has a *multi-linear* two-party t-robust CDS protocol for secrets of size $\tilde{\Theta}(t)$ with normalized message size $\tilde{O}(t + \sqrt{N})$. We use a variant of this protocol (with t slightly larger than $\sqrt{N}$) to construct our improved linear secret-sharing schemes.

- Finally, we construct robust k-party CDS protocols for a constant number of parties $k > 2$. We show that if a function f has a k-party CDS protocol for one-bit secrets with message size c_f, then it has a k-party t-robust CDS protocol for one-bit secrets with message size $\tilde{O}(t^k c_f)$. Furthermore, every function $f : [N] \times [N] \times [N] \to \{0, 1\}$ has a linear three-party t-robust CDS protocol for

[1] The order that we describe the results here is not the order we present them in the paper.

one-bit secrets with message size $\tilde{O}(t^2N)$ and has a multi-linear three-party t-robust CDS protocol for secrets of size $\tilde{\Theta}(t)$ with normalized message size $\tilde{O}(tN)$. We also present linear and multi-linear robust k-party CDS protocols for any constant $k > 3$.

Graph Secret-Sharing Schemes. Graph access structures are simple access structures that were studied in many papers [27, 57, 26, 25, 14, 35, 10, 12]. In a secret-sharing scheme for a graph, the parties are the vertices of the graph, and a subset of vertices can reconstruct the secret if and only if it contains an edge; alternatively, a subset of vertices is unauthorized if and only if it is an independent set. One can define a weaker requirement, of t-robust graph secret-sharing schemes, where we only require that a set is unauthorized if and only if it is an independent set of size at most t. By a simple reduction, t-robust graph secret-sharing schemes are equivalent to t-robust CDS protocols: For a bipartite graph $G = (U, V, E)$ we define the function $f : U \times V \to \{0, 1\}$, where $f(u, v) = 1$ if and only if $(u, v) \in E$. Thus, our results imply a linear t-robust graph secret-sharing scheme with normalized share size $\tilde{O}(t + \sqrt{N})$, where $N = |U| + |V|$. The best known graph secret-sharing scheme (i.e., N-robust graph secret-sharing scheme) has share size $O(N/\log N)$ [38, 28] and our results do not improve it.

1.2 Our Technique

Constructing Robust CDS Protocols. We start by explaining how to construct a CDS protocol for a function $f : A \times B \to \{0, 1\}$ that is secure when the first party, Alice, can send two messages (each one for a different input), and the second party, Bob, can send only one message. The idea is to start from a non-robust CDS protocol for f, partition the set of inputs A of Alice to two sets A_1 and A_2, and execute the non-robust CDS protocol for f twice, one for the restriction of f to $A_1 \times B$ and one for the restriction of f to $A_2 \times B$. Now, if Alice sends two messages on two inputs $x_1 \in A_1$ and $x_2 \in A_2$ then these messages are in different copies of the CDS protocols, and in each copy the referee gets one message from each party, so it does not get any information on the one-bit secret s (assuming that $f(x_1, y) = f(x_2, y) = 0$). However, if $x_1, x_2 \in A_1$, then there are no security guarantees.

Therefore, we consider ℓ partitions of A, denoted by $(A_1^1, A_2^1), \ldots, (A_1^\ell, A_2^\ell)$, such that for every $x_1, x_2 \in A$ there exists at least one partition (A_1^i, A_2^i) such that $x_1 \in A_1^i$ and $x_2 \in A_2^i$ (or vice versa). We choose ℓ random bits $s_1, \ldots, s_\ell$ such that $s = s_1 \oplus \cdots \oplus s_\ell$, and for every $i \in [\ell]$ we executed two CDS protocols with the secret s_i, one for the restriction of f to $A_1^i \times B$ and one for the restriction of f to $A_2^i \times B$. There are $\ell = \log |A|$ partitions satisfying the above requirement. We similarly use $\log |B|$ partitions of B and get a two-party 2-robust CDS protocol whose message size is $O(\log |A| \log |B|)$ times the message size of the original CDS protocol.

To construct a two-party t-robust CDS protocol we use partitions of A to $O(t^2)$ sets such that for every set T with t inputs, there exists at least one partition such that each input in T is in a different part. Such partitions are obtained using a family of perfect hash functions $H = \left\{h_i : A \to [t^2]\right\}$ [40]. We use a similar partition for the set B. The size of such family is $\ell = O(t \log N)$ (where $N = |A| = |B|$) and the message size in the resulting t-robust CDS protocol is $O(t^3 \log N)$ times the message size of the original CDS protocol.

To improve the message size we use two levels of hashing, similar to the tracing traitors protocol of [31]. We first use a family of hash functions with range of size $2t$. This ensures that for every set of inputs T of size at most t, there is at least one hash function such that there is no $\log t$-collusion on f. Thereafter, we can use the $\log t$-robust scheme described above.

To construct better linear robust-CDS protocols for arbitrary functions (i.e., "worst" functions), we start with a variant of the linear two-party CDS protocol of [41]. As discussed in Example 1.1, this CDS protocol

is not robust when Alice can send two messages. However, we show that it is robust when Alice sends one message and Bob sends many messages. Using this fact, we only need to partition the inputs of Alice; this results in a more efficient protocol. Again, to achieve an efficient t-robust CDS protocol, we use two levels of hashing to partition the inputs of Alice.

From Robust CDS Protocols to Secret-Sharing Schemes. We show how to construct a secret-sharing scheme for an access structure Γ from robust two-party CDS protocols. The basic idea is to partition the n parties $\{P_1, \ldots, P_n\}$ to two sets $B = \{P_1, \ldots, P_{n/2}\}$ and $\overline{B} = \{P_{n/2+1}, \ldots, P_n\}$, and define a function $f : 2^B \times 2^{\overline{B}} \to \{0, 1\}$, where $f(S_1, S_2) = 1$ if and only if $S_1 \cup S_2 \in \Gamma$. Notice that the number of inputs of each party in the CDS protocol is $2^{n/2}$. To share a one-bit secret s for the access structure Γ, we execute a CDS protocol for f, and for every $S \in 2^B \cup 2^{\overline{B}}$, we share the message of the CDS protocol on input S among the parties in S such that only all the parties in S can together reconstruct this message.

For the correctness of the scheme, observe that a set $S_1 \cup S_2 \in \Gamma$ can reconstruct the messages on inputs S_1 and S_2, and, hence, it can reconstruct s. For the security of the scheme, consider a set $S_1 \cup S_2 \notin \Gamma$. The parties in this set can reconstruct the messages of all sets contained in S_1 and all sets contained in S_2. If the CDS protocol is $(2^{n/2}, 2^{n/2})$-robust, we would get a secret-sharing scheme realizing Γ. Alas, the best known $(2^{n/2}, 2^{n/2})$-robust CDS protocol has messages of size $2^{n/2-o(n)}$, and the resulting scheme will have share size $2^{n-o(n)}$, since each party gets a share of $2^{n/2-1}$ messages of the CDS protocol.

Therefore, we need to be more careful in our reduction. First, using a method of [47], we can only consider minimal authorized sets of size between $(\frac{1}{2} - \delta)n$ and $(\frac{1}{2} + \delta)n$ for some small $\delta \in (0, \frac{1}{2})$, and assume that all sets of size larger than $(\frac{1}{2} + \delta)n$ are authorized (in our construction we take $\delta \approx 0.09$). Second, similar to [4], we show that we can only consider authorized sets S such that $|S \cap B| = |S \cap \bar{B}| = |S|/2$. Using these ideas, we can show that every unauthorized set can reconstruct messages of roughly $t = \tilde{O}(2^{0.2616n})$ inputs. Thus, we can use our t-robust CDS protocol with messages size $\tilde{O}(2^{0.2616n})$. The share size in the resulting scheme is $\tilde{O}(2^{n/2} \cdot 2^{0.2616n}) = \tilde{O}(2^{0.7616n})$, where the factor of $2^{n/2}$ is due to the sharing of the messages of the CDS protocol.

1.3 Related Work

Lower Bounds for Secret-Sharing Schemes. The best known lower bound on the share size of schemes realizing general access structures is $\Omega(n^2/\log n)$ [33, 34]. There is a huge gap between the lower and upper bounds. For linear secret-sharing schemes the lower bound is much better; by [54, 52, 53], there is a lower bound of $\Omega(2^{cn})$ on the share size of linear schemes, for a small constant $c < 1$. By counting arguments, one can obtain a lower bound of $\tilde{\Omega}(2^{n/2})$ on the share size of linear schemes for one-bit secrets (see, e.g., [4]).

The last lower bound for linear schemes is achieved as a special case for uniform access structures, which are access structure in which for some k, subsets of size less than k are unauthorized, subsets of size greater than k are authorized, and some subsets of size k can also be authorized. We say that such an access structure is k-uniform. In [4], it was shown that the lower bound on the share size of linear schemes realizing k-uniform access structures is $\tilde{\Omega}(2^{h(k/n)n/2})$. Moreover, this bound for k-uniform access structures is optimal (up to a small polynomial factor).

Conditional Disclosure of Secrets (CDS) Protocols. Conditional disclosure of secrets (CDS) protocols were first define by Gertner et al. [42]. The motivation for this definition was to construct private information

retrieval protocols. CDS protocols were used in many cryptographic applications, such as attribute based encryption [41, 7, 61], priced oblivious transfer [1], and secret-sharing schemes [47, 17, 4].

The original construction of multi-party CDS protocols for general functions $f : [N]^k \to \{0,1\}$, presented in [42], has message size $O(N^k)$ (where k is the number of parties and N is the input domain size of each party). This construction is linear, that is, each message is a vector in which each coordinate is a linear combination of the secret and random elements from some finite field.

Recently, better constructions of two-party CDS protocols for general functions (i.e., $k = 2$) were presented. Beimel et al. [15] have shown a non-linear CDS protocol for two parties with message size $O(N^{1/2})$. Gay et al. [41] constructed a linear CDS protocol for two parties with the same message size. By a lower bound of [11], this message size is optimal. Then, Liu et al. [48] showed a non-linear CDS protocol for two parties with message size $2^{O(\sqrt{\log N \log\log N})}$. Their CDS protocol is constructed by a reduction to a CDS protocol for the index function, and it uses ideas of the private information retrieval protocol of Dvir and Gopi [37]. Applebaum and Arkis [2] (improving on Applebaum et al. [3]) have shown that for long secrets, i.e., secrets of size $\Theta(2^{N^2})$, there is a CDS protocol for two parties with such long secrets in which the message size is 3 times the size of the secret.

There was also major improvement in the message size of multi-party CDS protocols for general functions. Liu et al. [49] constructed a CDS protocol (for one-bit secrets) with message size $2^{\tilde{O}(\sqrt{k \log N})}$. Beimel and Peter [17] and Liu et al. [49] constructed a linear CDS protocol (for one-bit secrets) with message size $O(N^{(k-1)/2})$; by [17], this bound is optimal (up to a factor of k). When we permit very long secrets, i.e., secrets of size $\Theta(2^{N^k})$, Applebaum and Arkis [2] showed that there is a CDS protocols with such long secrets in which the message size is 4 times the secret size.

Gay et al. [41] proved a lower bound of $\Omega(\log\log N)$ on the message size of CDS protocols for two parties and a lower bound of $\Omega(\sqrt{\log N})$ on the message size of linear CDS protocols for two parties. Applebaum et al. [3], Applebaum et al. [5], and Applebaum and Vasudevan [6] proved a lower bound of $\Omega(\log N)$ on the message size of CDS protocols for two parties.

CDS protocols are connected to secret-sharing schemes for uniform access structures; there are several transformations from CDS protocols to uniform access structures. A transformation from CDS protocols for two parties to secret-sharing schemes for two-uniform access is implied by the results of Beimel et al. [15]; the share size of the scheme is $O(\log n)$ times the message size of the CDS protocol. Beimel et al. [16] shows a transformation from n-party CDS protocols with binary inputs to secret-sharing schemes for k-uniform access structures with n parties in which the share size of the scheme is $O(n)$ times the message size of the CDS protocol. Applebaum and Arkis [2] and Beimel and Peter [17] showed a transformation from k-party CDS protocols to secret-sharing schemes for k-uniform access structures, where the share size of the scheme is $O(e^k)$ times the message size of the CDS protocol. This was improved recently by Applebaum et al. [4]; for one-bit secrets, they show a transformation in which the share size of the scheme is $O(kn)$ times the message size of the CDS protocol, and for long secrets, i.e., secrets of size $\tilde{\Theta}(2^{(n+1)^{k^2}} k)$, the share size of the scheme is $O(k^2)$ times the secret size (by using the efficient CDS protocol for long secrets of Applebaum and Arkis [2]). Moreover, the optimal linear secret-sharing scheme realizing k-uniform access structures of Applebaum et al. [4] for one-bit secrets, in which the share size is $\tilde{O}(2^{h(k/n)n/2})$, uses ideas of the optimal linear k-party CDS protocol of Beimel and Peter [17].

Private Simultaneous Messages (PSM) Protocols and Non-Interactive Secure Multi-Party Computation (NIMPC) Protocols. Private simultaneous messages (PSM) protocols, presented by Feige et al. [39] (see also [44]), is a primitive similar to CDS protocols. In a PSM protocol for a function $f : [N]^k \to \{0,1\}$ there are k parties, where each party holds a private input and a common random string, and sends one

message to the referee. In this case the referee does not know the inputs and should learn the value of f applied to the private inputs without learning any additional information on the inputs.

As in CDS protocols, the original definition of PSM protocols does not provide robustness for more than one message from each party. Beimel et al. [13] defined non-interactive secure multi-party computation (NIMPC) protocols, where some parties can collude with the referee and the referee can see the messages of all inputs of the colluding parties. Benhamouda et al. [21] presented efficient NIMPC protocols for a bounded number of parties colluding with the referee.

For Boolean functions, this notion of NIMPC protocols is equivalent to robust PSM protocols. However, for non-Boolean functions, in NIMPC protocols, if a party sends messages for two inputs, then the referee can learn the value of the function for all its inputs. Constructing efficient robust PSM protocols is an interesting open problem.

2 Preliminaries

2.1 Notations

We denote the logarithmic function with base 2 and base e by $\log$ and $\ln$, respectively. Additionally, we use the notation $[n]$ to denote the set $\{1, \ldots, n\}$. For $0 \leq \alpha \leq 1$, we denote the binary entropy of α by

$$h(\alpha) = -\alpha \log \alpha - (1-\alpha) \log(1-\alpha).$$

We define $\binom{[n]}{k}$ as the family of all subsets of $[n]$ of size k and $\binom{[n]}{\leq k}$ as the family of all subsets of $[n]$ of size at most k. That is, $\binom{[n]}{k} = \{A \subseteq [n] : |A| = k\}$ and $\binom{[n]}{\leq k} = \{A \subseteq [n] : |A| \leq k\}$. Next, we present an approximation of the binomial coefficients.

Claim 2.1. *Let n be an integer and let $k \in [n]$. Then, $\binom{n}{k} = \Theta(k^{-1/2} 2^{h(k/n)n})$.*

2.2 Secret-Sharing Schemes

We present the definition of secret-sharing schemes, similar to [9, 32].

Definition 2.2 (Access Structures)**.** *Let $P = \{P_1, \ldots, P_n\}$ be a set of parties. A collection $\Gamma \subseteq 2^P$ is* monotone *if $B \in \Gamma$ and $B \subseteq C$ imply that $C \in \Gamma$. An* access structure *is a monotone collection $\Gamma \subseteq 2^P$ of non-empty subsets of P. Sets in Γ are called* authorized*, and sets not in Γ are called* unauthorized*.*

Definition 2.3 (Secret-Sharing Schemes – Syntax)**.** *A* secret-sharing scheme *with domain of secrets S is a pair $\Sigma = \langle \Pi, \mu \rangle$, where μ is a probability distribution on some finite set R called the* set of random strings *and Π is a mapping from $S \times R$ to a set of n-tuples $S_1 \times \cdots \times S_n$, where S_i is called the* domain of shares *of party P_i. A dealer distributes a secret $s \in S$ according to Σ by first sampling a random string $r \in R$ according to μ, computing a vector of* shares *$\Pi(s, r) = (s_1, \ldots, s_n)$, and privately communicating each share s_i to party P_i. For a set $A \subseteq P$, we denote $\Pi_A(s, r)$ as the restriction of $\Pi(s, r)$ to its A-entries (i.e., the shares of the parties in A).*

Given a secret-sharing scheme Σ, define the secret size *as $\log |S|$ and the* share size *of the scheme Σ as the size of the largest share, i.e., $\max_{1 \leq i \leq n} \{\log |S_i|\}$.*

Definition 2.4 (Secret-Sharing Schemes – Correctness and Security)**.** *Let S be a finite set of secrets, where $|S| \geq 2$. A secret-sharing scheme $\Sigma = \langle \Pi, \mu \rangle$ with domain of secrets S realizes an access structure Γ if the following two requirements hold:*

CORRECTNESS. *The secret s can be reconstructed by any authorized set of parties. That is, for any set $B = \left\{P_{i_1}, \ldots, P_{i_{|B|}}\right\} \in \Gamma$ there exists a* reconstruction function $\mathrm{Recon}_B : S_{i_1} \times \cdots \times S_{i_{|B|}} \to S$ *such that for every secret $s \in S$ and every random string $r \in R$,*

$$\mathrm{Recon}_B\left(\Pi_B(s, r)\right) = s.$$

SECURITY. *Any unauthorized set cannot learn anything about the secret from its shares. Formally, there exists a randomized function* SIM*, called the* simulator*, such that for any set $T = \left\{P_{i_1}, \ldots, P_{i_{|T|}}\right\} \notin \Gamma$, every secret $s \in S$, and every vector of shares $(s_{i_1}, \ldots, s_{i_{|T|}}) \in S_{i_1} \times \cdots \times S_{i_{|T|}}$,*

$$\Pr[\,\mathrm{SIM}(T) = (s_{i_1}, \ldots, s_{i_{|T|}})\,] = \Pr[\,\Pi_T(s, r) = (s_{i_1}, \ldots, s_{i_{|T|}})\,],$$

where the first probability is over the randomness of the simulator SIM *and the second probability is over the choice of r from R at random according to μ.*

A scheme is linear if the mapping that the dealer uses to generate the shares that are given to the parties is linear, as we formalize at the following definition.

Definition 2.5 (Multi-Linear and Linear Secret-Sharing Schemes)**.** *Let $\Sigma = \langle \Pi, \mu \rangle$ be a secret-sharing scheme with domain of secrets S, where μ is a probability distribution on a set R and Π is a mapping from $S \times R$ to $S_1 \times \cdots \times S_n$. The scheme Σ is a* multi-linear secret-sharing scheme over a finite field $\mathbb{F}$ *if $S = \mathbb{F}^\ell$ for some integer $\ell \geq 1$, the sets $R, S_1, \ldots, S_n$ are vector spaces over $\mathbb{F}$, Π is an $\mathbb{F}$-linear mapping, and μ is the uniform probability distribution over R. The scheme Σ is a* linear secret-sharing scheme *if it is multi-linear and $S = \mathbb{F}$ (i.e., $\ell = 1$).*

Now, we define threshold secret-sharing schemes, and give known result for such schemes.

Definition 2.6 (Threshold Secret-Sharing Schemes)**.** *Let Σ be a secret-sharing scheme on a set of n parties P. We say that Σ is a k-*out-of-n secret-sharing scheme *if it realizes the access structure $\Gamma_{k,n} = \{A \subseteq P : |A| \geq k\}$.*

Claim 2.7 ([55])**.** *For every $k \in [n]$ there is a linear k-out-of-n secret-sharing scheme realizing $\Gamma_{k,n}$ for secrets of size m in which the share size is $\max\{m, \log n\}$.*

We define ramp secret-sharing schemes as in [24], and present the efficient ramp secret-sharing scheme implicit in [30].

Definition 2.8 (Ramp Secret-Sharing Schemes)**.** *Let Σ be a secret-sharing scheme on a set of n parties and let $0 \leq k_1 < k_2 \leq n$. The scheme Σ is a (k_1, k_2, n)-*ramp secret-sharing scheme *if each subset of parties of size at least k_2 can reconstruct the secret and each subset of parties of size at most k_1 cannot learn any information about the secret. There are no restrictions on other subsets of parties.*

Claim 2.9. *For every constants $0 \leq b < a \leq 1$ there is p_0 such that for every prime-power $q > p_0$, there is a linear (bn, an, n)-ramp secret-sharing scheme over the field $\mathbb{F}_q$ in which each share is a field element (where p_0 is independent of n).*

Finally, we present the following claim, dealing with decomposition of secret-sharing schemes.

Claim 2.10 ([20])**.** *Let $\Gamma_1, \ldots, \Gamma_t$ be access structures over the same set of n parties, and let $\Gamma = \Gamma_1 \cup \cdots \cup \Gamma_t$ and $\Gamma' = \Gamma_1 \cap \cdots \cap \Gamma_t$. If there exist secret-sharing schemes realizing $\Gamma_1, \ldots, \Gamma_t$ with share size at most c, then there exist secret-sharing schemes realizing Γ and Γ' with share size at most ct. Moreover, if the former schemes are linear over a finite field $\mathbb{F}$, then there exist linear secret-sharing schemes over $\mathbb{F}$ realizing Γ and Γ' with share size at most ct.*

2.3 Conditional Disclosure of Secrets Protocols

Next, we define k-party conditional disclosure of secrets (CDS) protocols, first presented in [42]. We consider a model where a set of k parties $P = \{P_1, \ldots, P_k\}$ hold a secret s and a common random string r. In addition, every party P_i holds an input x_i for some k-input function f. In a CDS protocol for f, for every $i \in [k]$, party P_i sends a message to a referee, based on r, s and x_i, such that the referee can reconstruct the secret s if $f(x_1, \ldots, x_k) = 1$, and it cannot learn any information about the secret s if $f(x_1, \ldots, x_k) = 0$.

Definition 2.11 (Conditional Disclosure of Secrets Protocols – Syntax and Correctness)**.** *Let $f : X_1 \times \cdots \times X_k \to \{0,1\}$ be a k-input function. A* k-party CDS protocol *$\mathcal{P}$ for f with domain of secrets S consists of:*

- *A finite domain of common random strings R, and k finite message domains $M_1, \ldots, M_k$.*
- *Deterministic message computation functions $\text{ENC}_1, \ldots, \text{ENC}_k$, where $\text{ENC}_i : X_i \times S \times R \to M_i$ for every $i \in [k]$.*
- *A deterministic reconstruction function $\text{DEC} : X_1 \times \cdots \times X_k \times M_1 \times \cdots \times M_k \to S$.*

We say that a CDS protocol $\mathcal{P}$ is correct (with respect to f) if for every inputs $(x_1, \ldots, x_k) \in X_1 \times \cdots \times X_k$ for which $f(x_1, \ldots, x_k) = 1$, every secret $s \in S$, and every common random string $r \in R$,

$$\text{DEC}(x_1, \ldots, x_k, \text{ENC}_1(x_1, s, r), \ldots, \text{ENC}_k(x_k, s, r)) = s.$$

The message size *of a CDS protocol $\mathcal{P}$ is defined as the size of the largest message sent by the parties, i.e.,* $\max_{1 \le i \le k} \{\log |M_i|\}$. *The* normalized message size *of a CDS protocol $\mathcal{P}$ is defined as* $\max_{1 \le i \le k} \{\log |M_i| / \log |S|\}$.

In 2-party CDS protocols we refer to the parties as Alice and Bob (instead of P_1, P_2).

We define the security of CDS protocols with a simulator, i.e., given $x_1, \ldots, x_k$ such that $f(x_1, \ldots, x_k) = 0$, we can simulate the messages sent by the parties by a simulator, which has access to $x_1, \ldots, x_k$ and does not know the secret, in such a way that one cannot distinguish between the messages sent by the parties and the messages generated by the simulator. That is, a CDS protocol is private if everything that can be learned from the messages on a zero-input $(x_1, \ldots, x_k)$ of f can be learned from the inputs $(x_1, \ldots, x_k)$ without knowing the secret.

Definition 2.12 (Conditional Disclosure of Secrets Protocols – Security)**.** *We say that a CDS protocol $\mathcal{P}$ is secure (with respect to f) if there exists a randomized function* SIM*, called the* simulator*, such that for every inputs $(x_1, \ldots, x_k) \in X_1 \times \cdots \times X_k$ for which $f(x_1, \ldots, x_k) = 0$, every secret $s \in S$, and every k messages $(m_1, \ldots, m_k) \in M_1 \times \cdots \times M_k$,*

$$\Pr[\, \text{SIM}(x_1, \ldots, x_k) = (m_1, \ldots, m_k) \,] = \Pr[\, (\text{ENC}_1(x_1, s, r), \ldots, \text{ENC}_k(x_k, s, r)) = (m_1, \ldots, m_k) \,],$$

where the first probability is over the randomness of the simulator SIM *and the second probability is over the choice of r from R with uniform distribution (the same r is chosen for all encryptions).*

In the definition of CDS protocols in [42], if a party sends messages for two inputs, then the security is not guaranteed and the referee can possibly learn the secret s. We generalize the notion of CDS protocols to robust CDS protocols, where the security holds even in the above scenario. That is, for subsets $(T_1, \ldots, T_k) \in 2^{X_1} \times \cdots \times 2^{X_k}$, in a $(T_1, \ldots, T_k)$-robust CDS protocols we require that if the referee gets messages for the of inputs of T_i from party P_i, such that $f(x_1, \ldots, x_k) = 0$ for every $x_1 \in T_1, \ldots, x_k \in T_k$, then it cannot learn any information about the secret. Next, we formally present our new definition of robustness of CDS protocols. In our definition, we consider a collection $\mathcal{T}$ of subsets of inputs $(T_1, \ldots, T_k)$ (e.g., $\mathcal{T}$ contains all subsets $(T_1, \ldots, T_k)$ such that $|T_1| + \cdots + |T_k| \le t$).

Definition 2.13 (Zero-inputs Sets)**.** *Let $f : X_1 \times \cdots \times X_k \to \{0,1\}$ be a k-input function. We say that $(x_1, \ldots, x_k) \in X_1 \times \cdots \times X_k$ is a* zero-input *of f if $f(x_1, \ldots, x_k) = 0$. We say that $(T_1, \ldots, T_k) \in 2^{X_1} \times \cdots \times 2^{X_k}$ is a* zero-inputs set *of f if every $(x_1, \ldots, x_k) \in T_1 \times \cdots \times T_k$ is a zero-input of f.*

Definition 2.14 (Conditional Disclosure of Secrets Protocols – Robustness)**.** *Let $\mathcal{T} \subseteq 2^{X_1} \times \cdots \times 2^{X_k}$. We say that a CDS protocol $\mathcal{P}$ is $\mathcal{T}$-robust (with respect to f) if there exists a randomized function* SIM*, called the* simulator*, such that for every zero-input set $(T_1, \ldots, T_k) \in \mathcal{T}$, every secret $s \in S$, and every subsets of messages $A_1 \subseteq M_1, \ldots, A_k \subseteq M_k$ such that $|A_i| = |T_i|$ for every $i \in [k]$,*

$$\Pr[\,\textsc{Sim}(T_1, \ldots, T_k) = (A_1, \ldots, A_k)\,] = \Pr[\,(\textsc{Enc}_1(T_1, s, r), \ldots, \textsc{Enc}_k(T_k, s, r)) = (A_1, \ldots, A_k)\,],$$

where $\textsc{Enc}_i(T_i, s, r)$ is the set of messages for the inputs in T_i, the first probability is over the randomness of the simulator SIM*, and the second probability is over the choice of r from R with uniform distribution (the same r is chosen for all encryptions). A CDS protocol $\mathcal{P}$ is $(t_1, \ldots, t_k)$-robust if it is $\mathcal{T}$-robust for $\mathcal{T} = \{(T_1, \ldots, T_k) : \forall i \in [k]\ T_i \subseteq X_i, |T_i| \leq t_i\}$ and it is t-robust if it is $(t_1, \ldots, t_k)$-robust for every $t_1, \ldots, t_k$ such that $t_1 + \cdots + t_k \leq t$. For every $j \in [k]$ and every $\mathcal{T}_1 \subseteq 2^{X_1}, \ldots, \mathcal{T}_j \subseteq 2^{X_j}$, a CDS protocol $\mathcal{P}$ is $(\mathcal{T}_1, \ldots, \mathcal{T}_j, |X_{j+1}|, \ldots, |X_k|)$-robust if it is $\mathcal{T}$-robust for $\mathcal{T} = \mathcal{T}_1 \times \cdots \times \mathcal{T}_j \times 2^{X_{j+1}} \times \cdots \times 2^{X_k} = \{(T_1, \ldots, T_k) : \forall i \in [j]\ T_i \in \mathcal{T}_i, \forall i \in \{j+1, \ldots, k\}\ T_i \subseteq X_i\}$.*

For example, the original (non-robust) definition of security of CDS protocols is $(1, \ldots, 1)$-robust using our terminology.

Informally, we say that a CDS protocol is linear if the reconstruction function of the referee is a linear function. We next present the formal definition of multi-linear and linear CDS protocols.

Definition 2.15 (Multi-Linear and Linear Conditional Disclosure of Secrets Protocols)**.** *We say that a CDS protocol $\mathcal{P}$ is multi-linear over a finite field $\mathbb{F}$ if:*

- *$S = \mathbb{F}^\ell$ for some integer $\ell \geq 1$.*
- *There exists constants $\ell_0, \ell_1, \ldots, \ell_k$ such that $R = \mathbb{F}^{\ell_0}$ and $M_i = \mathbb{F}^{\ell_i}$ for every $i \in [k]$.*
- *For every inputs $(x_1, \ldots, x_k) \in X_1 \times \cdots \times X_k$ for which $f(x_1, \ldots, x_k) = 1$, every secret $s \in S$, and every common random string $r \in R$, there exist field elements $(\alpha_{i,j_i})_{i \in [k], j_i \in [\ell_i]} \in \mathbb{F}$ such that*

$$\textsc{Dec}(x_1, \ldots, x_k, \textsc{Enc}_1(x_1, s, r), \ldots, \textsc{Enc}_k(x_k, s, r)) = \sum_{i \in [k], j_i \in [\ell_i]} \alpha_{i,j_i} m_{i,j_i},$$

where $\textsc{Enc}_i(x_i, s, r) = (m_{i,1}, \ldots, m_{i,\ell_i}) \in \mathbb{F}^{\ell_i}$ for every $i \in [k]$.

The protocol $\mathcal{P}$ is a linear CDS protocol if it is multi-linear and $S = \mathbb{F}$ (i.e., $\ell = 1$).

Equivalently, we could have required that for every $i \in [k]$ and every $x_i \in X_i$, the message $\textsc{Enc}_i(x_i, s, r)$ is a vector in which each coordinate is a linear combination over $\mathbb{F}$ of the field elements in the secret $s = (s_1, \ldots, s_\ell)$ and the field elements in $r = (r_1, \ldots, r_{\ell_0})$ (see [46, 8] for the equivalence).

In our CDS protocols presented in the following sections, we use the property that if we execute few copies of CDS protocols for a function f with the same secret s and with independent common random string in each copy, then the referee cannot learn any information about the secret s from the messages on zero-inputs of f, i.e., inputs for which f returns zero.

Claim 2.16. *Let $f : X_1 \times \cdots \times X_k \to \{0,1\}$ be a k-input function, and assume that there are ℓ k-party $(t_1, \ldots, t_k)$-robust CDS protocols for f, denoted by $\mathcal{P}_1, \ldots, \mathcal{P}_\ell$. Then, the CDS protocol $\mathcal{P} = (\mathcal{P}_1, \ldots, \mathcal{P}_\ell)$, in which each party sends its messages in all the ℓ protocols $\mathcal{P}_1, \ldots, \mathcal{P}_\ell$ (with independent common random string in each protocol), is a k-party $(t_1, \ldots, t_k)$-robust CDS protocol for f.*

To construct a CDS protocol for long secrets, we use a generalized decomposition technique [59] (generalizing [57]). For completeness, we supply the construction.

Proposition 2.17. *Let $f : X_1 \times \cdots \times X_k \to \{0,1\}$ be a k-input function, and assume that there are ℓ k-party CDS protocols $\mathcal{P}_1, \ldots, \mathcal{P}_\ell$ with the same set of secrets in which the message size of each of the protocols is $O(c)$, such that (1) for every $(x_1, \ldots, x_k) \in X_1 \times \cdots \times X_k$ for which $f(x_1, \ldots, x_k) = 1$, the referee can reconstruct the secret from the messages on the inputs $x_1, \ldots, x_k$ in each of the protocols, and (2) for every $(T_1, \ldots, T_k) \in 2^{X_1} \times \cdots \times 2^{X_k}$ that is a zero-inputs set of f such that $|T_1| \leq t_1, \ldots, |T_k| \leq t_k$, for at least $\ell/4$ of the protocols the referee cannot learn any information on the secret from the messages on the inputs of $T_1, \ldots, T_k$. Then, there is a k-party $(t_1, \ldots, t_k)$-robust CDS protocol $\mathcal{P}$ for f with secret size $\Theta(\ell)$ in which the normalized message size is $O(c)$.*

Proof. Let q be a prime-power guaranteed for $b = 3/4, a = 1$ in Claim 2.9 (the existence of ramp schemes) and let $s = (s'_1, \ldots, s'_{\ell/4}) \in \mathbb{F}_q^{\ell/4}$ be the secret. We use the $(3\ell/4, \ell, \ell)$-ramp secret-sharing scheme of Claim 2.9 to generate shares $s_1, \ldots, s_\ell \in \mathbb{F}_q$ of s. For every $i \in [\ell]$, we independently generate messages of the CDS protocol $\mathcal{P}_i$ with the secret s_i. In the protocol $\mathcal{P}$, the message of party P_j on input x_j contains the message of party P_j in the protocol $\mathcal{P}_i$ for every $i \in [\ell]$. Thus, for every $(T_1, \ldots, T_k) \in 2^{X_1} \times \cdots \times 2^{X_k}$ that is a zero-inputs set of f such that $|T_1| \leq t_1, \ldots, |T_k| \leq t_k$, the referee cannot get any information on at least $\ell/4$ values among $s_1, \ldots, s_\ell$ from the messages on the inputs of $T_1, \ldots, T_k$, and, hence, it cannot learn any information on the secret s. Moreover, for every $(x_1, \ldots, x_k) \in X_1 \times \cdots \times X_k$ for which $f(x_1, \ldots, x_k) = 1$, the referee can learn all the values $s_1, \ldots, s_\ell$ from the messages on the inputs $x_1, \ldots, x_k$, and, hence, it learns the secret s.

Therefore, the resulting protocol $\mathcal{P}$ is a k-party $(t_1, \ldots, t_k)$-robust CDS protocol for f with secret of size $\Theta(\ell)$ in which the normalized message size is $\frac{\ell \cdot O(c)}{\Theta(\ell)} = O(c)$. □

2.4 Probabilistic Claims

Following [40], we present the definition of a family of perfect hash functions.

Definition 2.18 (Families of Perfect Hash Functions)**.** *A set of functions $H_{n,t,m} = \{h_i : [n] \to [m] : i \in [\ell]\}$ is a family of perfect hash functions if for every set $T \subseteq [n]$ such that $|T| = t$ there exists at least one function $h \in H_{n,t,m}$ for which $|h(T)| = |\{h(a) : a \in T\}| = t$, that is, h restricted to T is one-to-one.*

It is known that using the probabilistic method, it can be proved that there exists a family of perfect hash functions $H_{n,t,t} = \{h_i : [n] \to [t] : i \in [\ell]\}$, where $\ell = \Theta(te^t \log n)$. Since we are interested in families of hash functions with additional properties, we give probabilistic proofs that such families of hash functions exist. We use the following Chernoff bound [50].

$$\Pr[\, X \leq (1-\delta)E(X)\,] \leq e^{-E(X)\delta^2/2} \text{ for any } 0 < \delta < 1. \tag{1}$$

Lemma 2.19. *Let n be an integer, $t \in [\sqrt{n}]$, and $\mathcal{T} \subseteq \binom{[n]}{\leq t}$. Then, there exists a family of hash functions $H_{n,t,t^2} = \{h_i : [n] \to [t^2] : i \in [\ell]\}$, where $\ell = 16 \ln |\mathcal{T}|$, such that for every $i \in [\ell]$ and every $b \in [t^2]$ it holds that $|\{a \in [n] : h_i(a) = b\}| \leq \lceil n/t^2 \rceil$, and for every subset $T \in \mathcal{T}$ there are at least $\ell/4$ functions $h \in H_{n,t,t^2}$ for which $|h(T)| = |T|$.*

Proof. We show that there exists a family of hash functions H_{n,t,t^2} as above with $\ell = 16 \ln |\mathcal{T}|$ functions using the probabilistic method. As a first step in the proof, we choose with uniform distribution a function $h : [n] \to [t^2]$ such that for every $b \in [t^2]$ it holds that $|\{a \in [n] : h(a) = b\}| \leq \lceil n/t^2 \rceil$, and fix a subset $T \in \mathcal{T}$ (recall that $|T| \leq t$). The probability that $|h(T)| < |T|$ is

$$\Pr[\,|h(T)| < |T|\,] = \Pr[\,\exists j_1 \neq j_2 \in T : h(j_1) = h(j_2)\,] \leq \sum_{j_1 \neq j_2 \in T} \Pr[\,h(j_1) = h(j_2)\,] < \binom{t}{2} \cdot \frac{1}{t^2} < \frac{1}{2}.$$

Next, we show that if we choose at random $\ell = 16 \ln |\mathcal{T}|$ functions as above, we can get the desired family $H_{n,t,t^2} = \{h_1, \ldots, h_\ell\}$. We bound the probability that for a given subset $T \in \mathcal{T}$ of size at most t, there exist at most $\ell/4$ functions $h \in H_{n,t,t^2}$ that we choose at random, such that $|h(T)| = |T|$. For every $i \in [\ell]$, let X_i be a boolean random variable such that $X_i = 1$ if $|h_i(T)| = |T|$ and $X_i = 0$ otherwise. Additionally, let $X = \sum_{i=1}^{\ell} X_i$, i.e., X is the number of hash functions h_i, for $i \in [\ell]$, such that $|h_i(T)| = |T|$. As we have shown above, $\Pr[\,X_i = 0\,] = \Pr[\,|h_i(T)| < |T|\,] < \frac{1}{2}$, so by linearity of expectation $E(X) = \sum_{i=1}^{\ell} E(X_i) = \sum_{i=1}^{\ell} \Pr[\,X_i = 1\,] > \frac{\ell}{2}$. By (1), we get that

$$\Pr[\,X \leq \ell/4\,] \leq \Pr[\,X \leq E(X)/2\,] \leq e^{-\frac{E(X)(1/2)^2}{2}} < e^{-\frac{\ell}{16}} = \frac{1}{e^{\ln |\mathcal{T}|}} = \frac{1}{|\mathcal{T}|}.$$

By the union bound, since there are $|\mathcal{T}|$ subsets in $\mathcal{T}$, the probability that there exists a subset $T \in \mathcal{T}$ with at most $\ell/4$ functions h_i, for $i \in [\ell]$, such that $|h_i(T)| = |T|$, is less than 1. This implies that there exists a family H_{n,t,t^2} with $\ell = 16 \ln |\mathcal{T}|$ hash functions as required. □

Next, we show a family of hash functions with logarithmic number of collisions. The existence of such family is known (e.g., [31]).

Lemma 2.20. *Let n be an integer, $t \in \{15, \ldots, n/2\}$, and $\mathcal{T} \subseteq \binom{[n]}{\leq t}$. Then, there exists a family of hash functions $H_{n,t,2t} = \{h_i : [n] \to [2t] : i \in [\ell]\}$, where $\ell = 16 \ln |\mathcal{T}|$, such that for every $i \in [\ell]$ and every $b \in [2t]$ it holds that $|\{a \in [n] : h_i(a) = b\}| \leq \lceil n/2t \rceil$, and for every subset $T \in \mathcal{T}$ there are at least $\ell/4$ functions $h \in H_{n,t,2t}$ such that for every $b \in [2t]$ it holds that $|\{a \in T : h(a) = b\}| < \log t$.*

Proof. Without loss of generality, we assume that t divides n (this can be achieved by increasing n by at most $t-1$). We show that there exists a family of hash function $H_{n,t,2t}$ as above with $\ell = 16 \ln |\mathcal{T}|$ functions using the probabilistic method. As a first step in the proof, we choose at random a function $h : [n] \to [2t]$ such that for every $b \in [2t]$ it holds that $|\{a \in [n] : h(a) = b\}| \leq \lceil n/2t \rceil$, and fix a subset $T \in \mathcal{T}$ (recall that $|T| \leq t$). The probability that for some $b \in [2t]$ it holds that $|\{a \in T : h(a) = b\}| \geq \log t$ is

$$\begin{aligned}
&\Pr[\,\exists b \in [2t] : |\{a \in T : h(a) = b\}| \geq \log t\,] \\
&\quad = \Pr[\,\exists j_1 \neq \cdots \neq j_{\log t} \in T : h(j_1) = \cdots = h(j_{\log t})\,] \\
&\quad \leq \sum_{j_1 \neq \cdots \neq j_{\log t} \in T} \Pr[\,h(j_1) = \cdots = h(j_{\log t})\,] < \binom{t}{\log t} \cdot \left(\frac{1}{2t}\right)^{\log t - 1} \\
&\quad \leq \left(\frac{et}{\log t}\right)^{\log t} \cdot \frac{1}{(2t)^{\log t - 1}} = \left(\frac{e}{2 \log t}\right)^{\log t} \cdot 2t < \frac{1}{2}
\end{aligned}$$

(where the last inequality holds since $t \geq 15$).

Next, we claim that if we choose at random $\ell = 16 \ln |\mathcal{T}|$ functions as above, we can get the desired family $H_{n,t,2t} = \{h_1, \ldots, h_\ell\}$. This implied by using the same arguments as in Lemma 2.19 (i.e., the Chernoff bound), so there exists a family $H_{n,t,2t}$ with $\ell = 16 \ln |\mathcal{T}|$ hash functions as required. □

Finally, we present a family of subsets such that every set of medium size is equally partitioned by one of the subsets in the family (a similar lemma appears in [4]).

Lemma 2.21. *Let P be a set of n parties for some even n and $\delta \in (0, \frac{1}{2})$. Then, there are $\ell = \Theta(n^{3/2})$ subsets $B_1, \ldots, B_\ell \subseteq P$, each of them of size $n/2$, such that for every subset $A \subseteq P$ for which $(\frac{1}{2} - \delta)n \leq |A| \leq (\frac{1}{2} + \delta)n$ it holds that $|A \cap B_i| = \lfloor |A|/2 \rfloor$ for at least one $i \in [\ell]$.*

Proof. We choose at random a subset $B \subseteq P$ of size $n/2$, and for a given subset of parties $A \subseteq P$ of size $k = |A|$, where $(\frac{1}{2} - \delta)n \leq k \leq (\frac{1}{2} + \delta)n$, we compute the probability that the size of $A \cap B$ is $\lfloor k/2 \rfloor$. The number of subsets B of size $n/2$ is $\binom{n}{n/2}$. The number of subsets B of size $n/2$ such that $|A \cap B| = \lfloor k/2 \rfloor$ is the number of options to choose $\lfloor k/2 \rfloor$ parties from the k parties of A times the number of options to choose $n/2 - \lfloor k/2 \rfloor$ parties from the $n - k$ parties of $\overline{A}$, which is $\binom{k}{\lfloor k/2 \rfloor} \cdot \binom{n-k}{n/2-\lfloor k/2 \rfloor}$. Thus,

$$\Pr[\, |A \cap B| = \lfloor |A|/2 \rfloor \,] = \frac{\binom{k}{\lfloor k/2 \rfloor} \cdot \binom{n-k}{n/2-\lfloor k/2 \rfloor}}{\binom{n}{n/2}} = \Theta\left(\frac{k^{-1/2}2^k \cdot n^{-1/2}2^{n-k}}{n^{-1/2}2^n}\right) = \Theta\left(\frac{1}{k^{1/2}}\right).$$

Hence, it holds that

$$\Pr[\, |A \cap B| \neq \lfloor |A|/2 \rfloor \,] = 1 - \Theta\left(\frac{1}{k^{1/2}}\right) \leq 1 - \Theta\left(\frac{1}{n^{1/2}}\right).$$

We repeat the above process $\ell = \Theta(n^{3/2})$ times, and get ℓ random subset of parties $B_1, \ldots, B_\ell$ of size $n/2$. By the union bound, we get that

$$\begin{aligned}
&\Pr[\, \exists A \subseteq [n], \left(\frac{1}{2} - \delta\right) n \leq |A| \leq \left(\frac{1}{2} + \delta\right) n, \forall i \in [\ell] : |A \cap B_i| \neq \lfloor |A|/2 \rfloor \,] \\
&\leq 2^n \left(\Pr[\, |A \cap B| \neq \lfloor |A|/2 \rfloor \,]\right)^\ell \leq 2^n \left(1 - \Theta\left(\frac{1}{n^{1/2}}\right)\right)^\ell \leq 2^n \cdot \frac{1}{e^n} < 1.
\end{aligned}$$

Thus, the probability of choosing the desired subsets $B_1, \ldots, B_\ell$ is greater than 0, and in particular such subsets exist. □

3 Linear Robust 2-Party CDS Protocols

In this section, we construct linear 2-party (t, N)-robust CDS protocols for arbitrary functions. For the "worst" functions, the message size in these protocols is smaller than the robust 2-party CDS protocols that can be constructed using the generic transformation of Theorem 5.2.

The construction has 3 stages. In the first stage, in Claim 3.1 and Claim 3.2, we show that a variant of a linear 2-party CDS protocol of [41] is $(1, N)$-robust. However, this protocol is not robust when Alice sends more than one message. To achieve robustness for the messages of Alice, we use hash functions. In the second stage of the construction, in Lemma 3.3, we use hash functions whose range is of size $O(t^2)$. This results with a (t, N)-robust CDS protocol; however, its message size is bigger than t^2. In the last stage, in Theorem 3.4, we use hash functions with range size $O(t)$; thus, only $\log t$ messages will collide, and then we use the protocol of Lemma 3.3 with $t' = \log t$.

3.1 Linear $(1, N)$-Robust CDS Protocols

The next robust CDS protocol is a variant of a protocol of [41], and it appears in [17]. The robustness property was not defined or proved in previous papers.

Claim 3.1. *Let $f : [M] \times [N] \to \{0, 1\}$ be a function. Then, for every finite field $\mathbb{F}$, protocol $\mathcal{P}_2^{(1,N)}$, described in Figure 1, is a linear 2-party $(1, N)$-robust CDS protocol for f with one-element secrets in which the message size of Alice is $O(M \log |\mathbb{F}|)$ and the message size of Bob is $O(\log |\mathbb{F}|)$.*

Proof. The protocol, denoted by $\mathcal{P}_2^{(1,N)}$, is described in Figure 1. In $\mathcal{P}_2^{(1,N)}$, Alice and Bob hold the inputs $x \in [M]$ and $y \in [N]$, respectively, and the common randomness is $M + 1$ uniformly distributed random elements $r_0, r_1, \ldots, r_M$. We denote the secret by $s \in \mathbb{F}$. Alice sends to the referee the elements $r_0, r_1, \ldots, r_{x-1}, r_{x+1}, \ldots, r_M$, and Bob sends the element $s + r_0 + \sum_{i \in [M], f(i,y)=0} r_i$. The message of Alice contains M field elements and the message of Bob contains one field element.

Protocol $\mathcal{P}_2^{(1,N)}$

The secret: An element $s \in \mathbb{F}$.
Inputs: Alice and Bob hold the inputs $x \in [M]$ and $y \in [N]$, respectively.
Common randomness: The two parties hold M uniformly distributed and independent random elements $r_0, r_1, \ldots, r_M \in \mathbb{F}$.
The protocol:

1. Alice sends to the referee the elements $m_A = (r_0, r_1, \ldots, r_{x-1}, r_{x+1}, \ldots, r_M)$.
2. Bob sends to the referee the element $m_B = s + r_0 + \sum_{i \in [M], f(i,y)=0} r_i$.
3. If $f(x, y) = 1$, the referee computes $m_B + r_0 + \sum_{i \in [M], f(i,y)=0} r_i$.

Figure 1: A linear 2-party CDS protocol $\mathcal{P}_2^{(1,N)}$ for a function $f : [M] \times [N] \to \{0, 1\}$.

For the correctness of the protocol, let $x \in [M], y \in [N]$ such that $f(x, y) = 1$. Thus, the random element r_x is not part of the sum in the message m_B, and the referee gets all the random elements $r_0, r_1, \ldots, r_M$ except for r_x, so it can unmask the secret s from the message m_B.

For the robustness of the protocol, assume that Alice sends the message of input $x \in [M]$, and Bob sends multiple messages for a subset of inputs $S_2 \subseteq [N]$ for which $f(x, y) = 0$ for every $y \in S_2$. Thus, the referee gets $r_0, r_1, \ldots, r_M$ except for r_x from Alice and $s + r_0 + \sum_{i \in [M], f(i,y)=0} r_i$ for every $y \in S_2$ from Bob; the element r_x is part of each sum since $f(x, y) = 0$ for every $y \in S_2$. Intuitively, r_x acts as one-time-pad protecting s. Formally, the messages are independent of s since $s + r_x$ is uniformly distributed, so a simulator for the protocol chooses uniformly distributed $r_0, r_1, \ldots, r_M$ for $s = 0$, and computes the messages as in the protocol $\mathcal{P}_2^{(1,N)}$.

Additionally, the referee cannot learn any information on the secret s from the messages of Bob on all the inputs $y \in [N]$, since these messages are masked by the element r_0. □

In the protocol of Claim 3.1, the message of Alice is long, while the message of Bob is short. The next protocol, originally appearing in [12], balances the sizes of messages of Alice and Bob. Its idea is to partition the set of inputs of Alice to disjoint sets and execute the protocol of Claim 3.1 independently for every set of inputs.

Claim 3.2 ([12]). *Let $f : [M] \times [N] \to \{0,1\}$ be a function. Then, for every finite field $\mathbb{F}$ and every $d \in [M]$, there is a linear 2-party $(1,N)$-robust CDS protocol $\mathcal{P}_2^{(1,N),\text{balanced}}$ for f with one-element secrets in which the message size of Alice is $O((M/d)\log|\mathbb{F}|)$ and the message size of Bob is $O(d\log|\mathbb{F}|)$.*

Proof. The description of the protocol $\mathcal{P}_2^{(1,N),\text{balanced}}$ is as follows: Let s be the secret, and partition the set $[M]$ to d disjoint sets $A_1, \ldots, A_d$ of size at most $\lceil M/d \rceil$, that is, every input $x \in [M]$ is in exactly one set A_i. For every $i \in [d]$, we execute the linear CDS protocol $\mathcal{P}_2^{(1,N)}$ independently for the restriction of f to the inputs of $A_i \times [N]$ with the secret s. Alice, when holding the input $x \in [M]$, only sends the message in the protocol for the restriction of f to the inputs of $A_i \times [N]$ for which $x \in A_i$. Bob, when holding the input $y \in [N]$, sends the messages in all the above independent protocols.

For the correctness of the protocol, if $f(x,y) = 1$ then the referee can reconstruct the secret from the messages of the CDS protocol for the restriction of f to the inputs of $A_i \times [N]$ for which $x \in A_i$. For the robustness of the protocol, let $x \in [M]$ and $S_2 \subseteq [N]$ such that $f(x,y) = 0$ for every $y \in S_2$. The referee cannot learn any information on the secret from the messages on x and the inputs of S_2 from each of the above independent protocols, which follows by the robustness of each of these protocols. By Claim 2.16, the resulting protocol $\mathcal{P}_2^{(1,N),\text{balanced}}$ is $(1,N)$-robust.

The message of Alice contains at most $\lceil M/d \rceil$ field elements (since it sends a message in one execution of $\mathcal{P}_2^{(1,N)}$ in which the input domain size of Alice is at most $\lceil M/d \rceil$) and the message of Bob contains d field elements. All together, the message size of the resulting CDS protocol $\mathcal{P}_2^{(1,N),\text{balanced}}$ is as in the claim. □

3.2 From $(1,N)$-Robust CDS Protocols to (t,N)-Robust CDS Protocols

We use the above linear CDS protocol $\mathcal{P}_2^{(1,N)}$ and a family of hash functions to construct the linear robust CDS protocol $\mathcal{P}_2^{(t,N)}$ (described in Figure 2). This protocol has specific parameters that are used in our protocol $\mathcal{P}_{\text{L2RCDS}}$ – the linear robust 2-party CDS protocol for arbitrary functions (other tradeoffs between the message size of Alice and Bob can be achieved by taking different parameters).

Lemma 3.3. *Let $f : [M] \times [N] \to \{0,1\}$ be a function and $t \leq \sqrt{M}$ be an integer. Then, for every finite field $\mathbb{F}$, there is a linear 2-party (t,N)-robust CDS protocol for f with one-element secrets in which the message size of Alice is $O(\sqrt{N}t\log M\log|\mathbb{F}|)$ and the message size of Bob is $O((t^3 + Mt/\sqrt{N})\log M\log|\mathbb{F}|)$. Furthermore, there is p_0 such that for every prime-power $q > p_0$, there is a multi-linear 2-party (t,N)-robust CDS protocol for f over $\mathbb{F}_q$ with secrets of size $\Theta(qt\log M)$ in which the normalized message size of Alice is $O(\sqrt{N})$ and the normalized message size of Bob is $O(t^2 + M/\sqrt{N})$.*

Proof. Let $H_{M,t,t^2} = \left\{h_i : [M] \to [t^2] : i \in [\ell]\right\}$, where $\ell = \Theta(t\log M)$, be the family of perfect hash functions promised by Lemma 2.19 for $\mathcal{T} = \binom{[M]}{\leq t}$ (that is, $|\mathcal{T}| = \Theta(M^t)$).

The desired CDS protocol $\mathcal{P}_2^{(t,N)}$ is described in Figure 2. For a fixed $h_i \in H_{M,t,t^2}$, the message of Alice contains $O(|A_{h_i(x)}|/d) = O\left(\frac{M/t^2}{\max\{1,M/(\sqrt{N}t^2)\}}\right) = O(\min\left\{M/t^2, \sqrt{N}\right\}) \leq O(\sqrt{N})$ field elements, and the message of Bob contains $t^2 d = t^2 \cdot \max\left\{1, M/(\sqrt{N}t^2)\right\} = O(t^2 + M/\sqrt{N})$ field elements. Since there are $\ell = \Theta(t\log M)$ hash functions, the sizes of the messages is as in the lemma.

For the correctness of the protocol, let $x \in [M]$ and $y \in [N]$ for which $f(x,y) = 1$. Then, for every $i \in [\ell]$, the input x is in $A_{h_i(x)}$, so the referee can reconstruct s_i using the messages on the inputs x, y in the CDS protocol $\mathcal{P}_2^{(1,N)}$ for the restriction of f to the inputs of $A_{h_i(x)} \times [N]$ with the secret s_i. Overall, the referee can learn all the elements $s_1, \ldots, s_\ell$, so it can reconstruct the secret s by summing these elements.

Protocol $\mathcal{P}_2^{(t,N)}$

The secret: An element $s \in \mathbb{F}$.
The protocol:

1. Choose ℓ random elements $s_1, \ldots, s_\ell \in \mathbb{F}$ such that $s = s_1 + \cdots + s_\ell$.
2. For every $i \in [\ell]$ do:
   - Let $A_j = \{x \in [M] : h_i(x) = j\}$, for every $j \in [t^2]$.
   - For every $j \in [t^2]$, independently execute the CDS protocol $\mathcal{P}_2^{(1,N),\text{balanced}}$ of Claim 3.2 for the restriction of f to $A_j \times [N]$ with the secret s_i and $d = \max\left\{1, M/(\sqrt{N}t^2)\right\}$. That is, Alice with input x sends a message only for the restriction of f to $A_{h_i(x)} \times [N]$, and Bob with input y sends a message for the restriction of f to $A_j \times [N]$, for every $j \in [t^2]$.

Figure 2: A linear 2-party (t, N)-robust CDS protocol $\mathcal{P}_2^{(t,N)}$ for a function $f : [M] \times [N] \to \{0, 1\}$.

For the robustness of the protocol, let (S_1, S_2) be a zero-inputs set of f such that $|S_1| \leq t$. By Lemma 2.19, there is at least one $i \in [\ell]$ for which $|h_i(S_1)| = |S_1|$. We prove that the referee cannot learn any information on s_i, and, thus, cannot learn the secret s.

Since h_i is one-to-one on S_1, each input of S_1 is in a different subset A_j in the partition induced by h_i, and the referee gets at most one message of Alice in each execution of the CDS protocol $\mathcal{P}_2^{(1,N)}$ for the restriction of f to $A_j \times [N]$. Since the CDS protocol $\mathcal{P}_2^{(1,N)}$ is $(1, N)$-robust and $f(x, y) = 0$ for every $(x, y) \in S_1 \times S_2$, the referee cannot learn any information about s_i from any execution of the CDS protocol $\mathcal{P}_2^{(1,N)}$ for the restriction of f to the inputs of $A_j \times [N]$ with the secret s_i, for every $j \in [t^2]$. Since each execution of $\mathcal{P}_2^{(1,N)}$ for each function h_i is done with independent common random strings, then by Claim 2.16, the referee cannot learn any information on s_i, and, hence, it cannot learn any information on the secret s.

To construct the desired protocol for long secrets, let $s = (s'_1, \ldots, s'_{\ell/4}) \in \mathbb{F}_q^{\ell/4}$ be the secret. We use the protocol of Proposition 2.17 with the above ℓ CDS protocols, one for every hash function $h_i \in H_{M,t,t^2}$. That is, we change step 1 in the protocol $\mathcal{P}_2^{(t,N)}$ (described in Figure 2) such that $s_1, \ldots, s_\ell \in \mathbb{F}_q$ are the shares of a $(3\ell/4, \ell, \ell)$-ramp secret-sharing scheme of the secret $s = (s'_1, \ldots, s'_{\ell/4}) \in \mathbb{F}_q^{\ell/4}$, where p_0 is the constant from Claim 2.9 and $q > p_0$.

As above, for every inputs $x \in [M], y \in [N]$ such that $f(x, y) = 1$, the referee can learn all the secrets in those ℓ protocols from the messages on the inputs x, y, so it can reconstruct the secret s using the reconstruction function of the ramp scheme. Moreover, for every (S_1, S_2) that is a zero-inputs set of f such that $|S_1| \leq t$, by Lemma 2.19, there are at least $\ell/4$ values of $i \in [\ell]$ for which $|h_i(S_1)| = |S_1|$. Thus, the referee cannot learn any information on at least $\ell/4$ of the shares $s_1, \ldots, s_\ell$ in the above ℓ protocols from the messages on the inputs of S_1, S_2. By the security of the ramp scheme, the referee cannot learn any information on the secret s. □

We improve our linear robust 2-party CDS protocol using the family of hash functions of Lemma 2.20.

Theorem 3.4. *Let $f : [N] \times [N] \to \{0, 1\}$ be a function. Then, for every finite field $\mathbb{F}$, every integer $t \leq N/(2\log^2 N)$, and every $\mathcal{T} \subseteq \binom{[N]}{\leq t}$, there is a linear 2-party $(\mathcal{T}, N)$-robust CDS protocol for f with one-*

element secrets in which the message size is $O((t\log^2 t+\sqrt{N})\log t\log N\log|\mathcal{T}|\log|\mathbb{F}|)$. *Furthermore, there is* p_0 *such that for every prime-power* $q>p_0$*, there is a multi-linear 2-party* $(\mathcal{T},N)$*-robust CDS protocol for* f *over* $\mathbb{F}_q$ *with secrets of size* $\Theta(q\log t\log N\log|\mathcal{T}|)$ *in which the normalized message size is* $O(t\log^2 t+\sqrt{N})$.

Proof. Let $H_{N,t,2t}=\{h_i:[N]\to[2t]:i\in[\ell]\}$, where $\ell=\Theta(\log|\mathcal{T}|)$, be the family of hash functions promised by Lemma 2.20 for $\mathcal{T}$ (that is, for every $T\in\mathcal{T}$, at least $\ell/4$ hash functions prevent a collision of $\log t$ elements of T).

Protocol $\mathcal{P}_{\mathrm{L2RCDS}}$

The secret: An element $s\in\mathbb{F}$.
The protocol:

1. Choose ℓ random elements $s_1,\ldots,s_\ell\in\mathbb{F}$ such that $s=s_1+\cdots+s_\ell$.
2. For every $i\in[\ell]$ do:
   - Let $A_j=\{x\in[N]:h_i(x)=j\}$, for every $j\in[2t]$.
   - For every $j\in[2t]$, independently execute the linear 2-party $(\log t,N)$-robust CDS protocol $\mathcal{P}_2^{(\log t,N)}$ of Lemma 3.3 for the restriction of f to $A_j\times[N]$ with the secret s_i. That is, Alice with input x sends a message only for the restriction of f to $A_{h_i(x)}\times[N]$, and Bob with input y sends a message for the restriction of f to $A_j\times[N]$, for every $j\in[2t]$.

Figure 3: A linear 2-party $(\mathcal{T},N)$-robust CDS protocol $\mathcal{P}_{\mathrm{L2RCDS}}$ for a function $f:[N]\times[N]\to\{0,1\}$.

The desired CDS protocol $\mathcal{P}_{\mathrm{L2RCDS}}$ is described in Figure 3. The protocol $\mathcal{P}_{\mathrm{L2RCDS}}$ contains $2t\ell=O(t\log|\mathcal{T}|)$ executions of the protocol $\mathcal{P}_2^{(t',N)}$ with $t'=\log t$ and $M=N/(2t)$ (since $t\le N/(2\log^2 N)$, we have that $\log t\le\sqrt{N/(2t)}$ as required). Since Alice sends only one message of $\mathcal{P}_2^{(t,N)}$ for every $h_i\in H_{N,t,2t}$, her message contains $O(\sqrt{N}\log t\log N\log|\mathcal{T}|)$ field elements. Since Bob sends $2t$ messages of $\mathcal{P}_2^{(t,N)}$ for every $h_i\in H_{N,t,2t}$, his message contains

$$O\left((\log^3 t+\frac{N\log t/(2t)}{\sqrt{N}})\log N\cdot 2t\log|\mathcal{T}|\right)=O((t\log^2 t+\sqrt{N})\log t\log N\log|\mathcal{T}|)$$

field elements.

For the correctness of the protocol, let $x,y\in[N]$ for which $f(x,y)=1$. Then, for every $i\in[\ell]$, the input x is in $A_{h_i(x)}$, so the referee can reconstruct s_i using the messages for the inputs x,y in the CDS protocol for the restriction of f to $A_{h_i(x)}\times[N]$. Overall, the referee can learn all the elements $s_1,\ldots,s_\ell$, so it can reconstruct the secret s by summing these elements.

For the robustness of the protocol, let (S_1,S_2) be a zero-inputs set of f such that $S_1\in\mathcal{T}$. By Lemma 2.20, there is at least one $i\in[\ell]$ such that for every $j\in[2t]$ it holds that $|\{a\in S_1:h_i(a)=j\}|<\log t$. Thus, each A_j contains less than $\log t$ inputs of S_1, and since the protocol $\mathcal{P}_2^{(t,N)}$ executed in the protocol $\mathcal{P}_{\mathrm{L2RCDS}}$ is $(\log t,N)$-robust, the referee cannot learn any information on s_i from each such protocol. By Claim 2.16, the referee cannot learn any information on s_i, and, hence, it cannot learn any information on the secret s.

To construct the desired protocol for long secrets, let $s=(s'_1,\ldots,s'_{\ell/4})\in(\mathbb{F}^{\ell'})^{\ell/4}$ be the secret, where $\ell'=\Theta(\log t\log N)$. Similarly to the multi-linear protocol of Lemma 3.3, we use the protocol

of Proposition 2.17 with the above ℓ CDS protocols, one for every hash function $h_i \in H_{N,t,2t}$. That is, we change step 1 in the protocol $\mathcal{P}_{\mathrm{L2RCDS}}$ such that $s_1, \ldots, s_\ell \in \mathbb{F}^{\ell'}$ are the shares of a $(3\ell/4, \ell, \ell)$-ramp secret-sharing scheme of the secret $s = (s'_1, \ldots, s'_{\ell/4}) \in (\mathbb{F}^{\ell'})^{\ell/4}$, but now in step 2 we execute the multi-linear 2-party $(\log t, N)$-robust CDS protocol of Lemma 3.3, instead of the linear protocol.

Overall, we results in a 2-party $(\mathcal{T}, N)$-robust CDS protocol for f with secrets of size $\Theta(\ell'\ell \log |\mathbb{F}|) = \Theta(\log t \log N \log |\mathcal{T}| \log |\mathbb{F}|)$ in which the normalized message size is $O(t \log^2 t + \sqrt{N})$. □

On the Optimality of Protocol $\mathcal{P}_{\mathrm{L2RCDS}}$. Assume that $\mathcal{T}$ is a subset such that $\mathcal{P}_{\mathrm{L2RCDS}}$ is a secure CDS protocol for f according to Definition 2.12. That is, for every x, y such that $f(x, y) = 0$, the referee should not learn any information of s from the messages on x and y (i.e., we assume that $\{x\} \in \mathcal{T}$ for every x). By[11], the message size in any linear 2-party CDS protocol for a general function is $\Omega(\sqrt{N})$. Thus, in any linear 2-party $(\mathcal{T}, N)$-robust CDS protocol, the message size is $\Omega(\sqrt{N})$. In Section 4, we use $\mathcal{P}_{\mathrm{L2RCDS}}$ with $|\mathcal{T}| = O(N)$. For this case, when $t < \sqrt{N}$, protocol $\mathcal{P}_{\mathrm{L2RCDS}}$ is optimal up to poly-logarithmic factors, that is, we achieve robustness with a very small cost. In Section 4, t is slightly larger than $\sqrt{N}$, and the cost for robustness is higher (however, it is less than $N^{0.02}$).

4 Secret-Sharing Schemes for General Access Structures

In this section we show a transformation from robust 2-party CDS protocols to secret-sharing schemes for general access structures.

As in [47], we decompose an access structure Γ to three parts: A bottom part Γ_{bot}, which handles small sets, a middle part Γ_{mid}, which handles medium-size sets, and a top part Γ_{top}, which handles large sets. This decomposition presented in the following proposition. In the sequence, we say that a secret-sharing scheme has an exponent c, where $0 \leq c \leq 1$, if the share size of the scheme is $2^{cn+o(n)}$ times the size of the secret.[2]

Proposition 4.1 ([47])**.** *Let Γ be an access structure over a set of n parties and $\delta \in (0, \frac{1}{2})$. Define the following access structures $\Gamma_{\mathrm{top}}, \Gamma_{\mathrm{bot}}$, and Γ_{mid}.*

$$A \notin \Gamma_{\mathrm{top}} \iff \exists A' \notin \Gamma, A \subseteq A' \text{ and } |A'| > \left(\frac{1}{2} + \delta\right) n,$$

$$A \in \Gamma_{\mathrm{bot}} \iff \exists A' \in \Gamma, A' \subseteq A \text{ and } |A'| < \left(\frac{1}{2} - \delta\right) n,$$

$$A \in \Gamma_{\mathrm{mid}} \iff A \in \Gamma \text{ and } \left(\frac{1}{2} - \delta\right) n \leq |A| \leq \left(\frac{1}{2} + \delta\right) n, \text{ or } |A| > \left(\frac{1}{2} + \delta\right) n.$$

Then, $\Gamma = \Gamma_{\mathrm{top}} \cap (\Gamma_{\mathrm{mid}} \cup \Gamma_{\mathrm{bot}})$. Therefore, if $\Gamma_{\mathrm{top}}, \Gamma_{\mathrm{bot}}$, and Γ_{mid} can be realized (respectively, linearly realized) by a secret-sharing scheme with an exponent of c then also Γ can be realized (respectively, linearly realized) by a secret-sharing scheme with an exponent of c.

As mentioned in Proposition 4.1, $\Gamma = \Gamma_{\mathrm{top}} \cap (\Gamma_{\mathrm{mid}} \cup \Gamma_{\mathrm{bot}})$. Thus, by standard closure properties of secret-sharing schemes (presented in Claim 2.10), realizing Γ can be reduced to realizing Γ_{top}, Γ_{bot}, and Γ_{mid}. In [47], the access structures Γ_{bot} was realized by sharing the secret independently for each minimal authorized set, resulting in a scheme realizing Γ_{bot} with share size $\binom{n}{(\frac{1}{2}-\delta)n} \leq O(2^{h(\frac{1}{2}-\delta)n})$ (a similar

[2] This notation is asymptotic; we consider a scheme that gets as its input an arbitrary access structure (with an arbitrary number of parties n) and realizes it.

construction was used for Γ_{top}). This was improved in [4], using covers and a recursive construction, resulting in the following lemma.

Lemma 4.2 ([4]). *Let Γ be an access structure and $\delta \in (0, \frac{1}{2})$. Assume that for every access structure Γ', the access structure Γ'_{mid} can be realized (respectively, linearly realized) by a secret-sharing scheme with an exponent of $M(\delta)$ (respectively, $M_\ell(\delta)$). Furthermore, let $X'(\delta) = h(\frac{1}{2} - \delta) - (\frac{1}{2} - \delta)\log(\frac{1+2\delta}{1-2\delta})$ and c be a constant such that $c > X'(\delta)$. Then, Γ can be realized (respectively, linearly realized) by a secret-sharing scheme with an exponent of $\max\{c, M(\delta)\}$ (respectively, $\max\{c, M_\ell(\delta)\}$).*

4.1 From (N, N)-Robust CDS Protocols to Secret-Sharing Schemes

As a warm-up, we first show how to construct secret-sharing schemes from 2-party (N, N)-robust CDS protocols (i.e., protocols that are secure against any zero-inputs set). For simplicity, we consider one-bit secrets. Assume that for every N and for every function $f : [N] \times [N] \to \{0, 1\}$ there is a 2-party (N, N)-robust CDS protocol for f with message size $c(N)$.

Given an access structure Γ over a set of n parties, let $B = \left\{P_1, \ldots, P_{n/2}\right\}$ and define the function $f : 2^B \times 2^{\overline{B}} \to \{0, 1\}$, where $f(S_1, S_2) = 1$ if and only if $S_1 \cup S_2 \in \Gamma$. To share the secret s, do as follows: (1) Execute a 2-party $(2^{n/2}, 2^{n/2})$-robust CDS protocol for the function f with the secret s. (2) For every subset $S_1 \subseteq B$, share the message of Alice when holding the input S_1 among the parties of S_1 using an $|S_1|$-out-of-$|S_1|$ threshold secret-sharing scheme, and (3) for every subset $S_2 \subseteq \overline{B}$, share the message of Bob when holding the input S_2 among the parties of S_2 using an $|S_2|$-out-of-$|S_2|$ threshold secret-sharing scheme.

To argue the correctness of the scheme, let $A \in \Gamma$, and define $S_1 = A \cap B$ and $S_2 = A \setminus B$. The parties in $A = S_1 \cup S_2$ can use the threshold schemes to reconstruct the messages of Alice and Bob when holding the inputs S_1 and S_2, respectively. Thus, since $f(S_1, S_2) = 1$, the parties in A can reconstruct the secret s using the reconstruction function of the CDS protocol.

To argue the security of the scheme, let $A \notin \Gamma$, and again define $S_1 = A \cap B$ and $S_2 = A \setminus B$. The parties in $A = S_1 \cup S_2$ can use the threshold schemes to reconstruct only the messages of Alice and Bob when holding the inputs S'_1 and S'_2, respectively, for every $S'_1 \subseteq S_1$ and every $S'_2 \subseteq S_2$. By the monotonicity property of access structures, $S'_1 \cup S'_2 \notin \Gamma$ for every $S'_1 \subseteq S_1, S'_2 \subseteq S_2$, so by the definition of f we get that $f(S'_1, S'_2) = 0$ for every $S'_1 \subseteq S_1, S'_2 \subseteq S_2$. Thus, the parties in A learn only the messages of a zero-inputs set of f, and since we use a 2-party $(2^{n/2}, 2^{n/2})$-robust CDS protocol for f, the parties in A cannot learn any information about the secret s.

Every party is contained in $2^{n/2-1}$ subsets of B (or $\overline{B}$), so it gets $2^{n/2-1}$ shares (of messages in the CDS protocol) of the threshold schemes, one for each such subset. Thus, the share size of each party in this scheme is $2^{n/2-1} \cdot c(2^{n/2})$. Unfortunately, in the best known (N, N)-robust CDS protocol for functions $f : [N] \times [N] \to \{0, 1\}$ the message size is $c(N) = O(N/\log N)$. Thus, the share size in the above scheme is $2^{n-o(n)}$. In our reduction from secret-sharing schemes to 2-party (t, N)-robust CDS protocols we will ensure that $t < N$ and save in the share size.

4.2 Secret-Sharing Schemes Realizing the Access Structure Γ_{mid}

Our main construction in this paper is an improved linear secret-sharing scheme realizing the middle access structure Γ_{mid}. That is, we show an improved expression for $M_\ell(\delta)$ (and also for $M(\delta)$). Towards this construction, we defined balanced access structures in Definition 4.3, represent Γ_{mid} as a union of a polynomial number of balanced access structures (this follows from Lemma 2.21), and show how to realize

each such access structure using a robust CDS protocol. By the closure properties of secret-sharing scheme (Claim 2.10), we can realize Γ_{mid} using the scheme for the balanced access structures, and, hence, we can realize Γ with a smaller share size.

Definition 4.3 (The Access Structure $\Gamma_{B,\mathrm{mid}}$)**.** *Let Γ be an access structure with n parties, $\delta \in (0, \frac{1}{2})$, and B be a subset of parties. The access structure $\Gamma_{B,\mathrm{mid}}$ is the access structure that contains all subsets of parties of size greater than $(\frac{1}{2}+\delta)n$, and all subsets of parties that contain authorized subsets $A' \in \Gamma$ of size between $(\frac{1}{2}-\delta)n$ and $(\frac{1}{2}+\delta)n$ that contain exactly $\lfloor |A'|/2 \rfloor$ of their parties from B. That is,*

$$\begin{aligned}\Gamma_{B,\mathrm{mid}} &= \left\{A : \exists A' \in \Gamma, A' \subseteq A, \left(\frac{1}{2}-\delta\right)n \leq |A'| \leq \left(\frac{1}{2}+\delta\right)n, \text{ and } |A' \cap B| = \lfloor |A'|/2 \rfloor\right\} \\ &\cup \left\{A : |A| > \left(\frac{1}{2}+\delta\right)n\right\}.\end{aligned}$$

Following the above definition, we present our main secret-sharing scheme, which realizes the access structure $\Gamma_{B,\mathrm{mid}}$.

Lemma 4.4. *Let Γ be a an access structure over a set of n parties, $\delta \in (0, \frac{1}{2})$, and B be a subset of parties such that $|B| = n/2$. Assume that for every integer N, every $t \in [N]$, every $\mathcal{T} \subseteq \binom{[N]}{\leq t}$, and every function $f : [N] \times [N] \to \{0,1\}$, there is a 2-party $(\mathcal{T}, N)$-robust CDS protocol for f with secrets of size m in which the message size is $c(t, |\mathcal{T}|, N, m)$, for some integer $m \geq 1$. Then, there is a secret-sharing scheme realizing $\Gamma_{B,\mathrm{mid}}$ for secrets of size m in which the share size is $O(2^{n/2} c(n 2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{4}+\frac{\delta}{2})n}, 2^{n/2}, 2^{n/2}, m))$ for $\delta < \frac{1}{6}$ and $O(2^{n/2} c(2^{(\frac{1}{4}+\frac{\delta}{2})n}, 2^{n/2}, 2^{n/2}, m))$ otherwise. Moreover, if the CDS protocol is linear then the resulting scheme is also linear.*

Proof. Assume without loss of generality that n is even (this can be done by adding dummy parties). Define $\mathcal{B}_1 = \left\{S_1 \subseteq B : (\frac{1}{4}-\frac{\delta}{2})n \leq |S_1| \leq (\frac{1}{4}+\frac{\delta}{2})n\right\}$ and $\mathcal{B}_2 = \left\{S_2 \subseteq \overline{B} : (\frac{1}{4}-\frac{\delta}{2})n \leq |S_2| \leq (\frac{1}{4}+\frac{\delta}{2})n\right\}$. Note that $N \stackrel{\Delta}{=} |\mathcal{B}_1| = |\mathcal{B}_2| < 2^{n/2}$. Moreover, define the function $f : \mathcal{B}_1 \times \mathcal{B}_2 \to \{0,1\}$, where $f(S_1, S_2) = 1$ if and only if $S_1 \cup S_2 \in \Gamma$, $(\frac{1}{2}-\delta)n \leq |S_1 \cup S_2| \leq (\frac{1}{2}+\delta)n$, and $|S_1| = |S_2|$ or $|S_1| = |S_2| - 1$. The scheme $\Sigma_{\mathrm{B,mid}}$ realizing $\Gamma_{\mathrm{B,mid}}$ is described in Figure 4.

For the correctness of the scheme, take a minimal authorized set $A \in \Gamma_{B,\mathrm{mid}}$, that is, $A = S_1 \cup S_2$ for some $S_1 \subseteq B, S_2 \subseteq \overline{B}$ such that $S_1 \cup S_2 \in \Gamma$, $(\frac{1}{2}-\delta)n \leq |S_1 \cup S_2| \leq (\frac{1}{2}+\delta)n$, and $|S_1| = |S_2|$ or $|S_1| = |S_2| - 1$. The parties in $A = S_1 \cup S_2$ can reconstruct the messages of Alice and Bob when holding the inputs S_1 and S_2, respectively, in the first CDS protocol (i.e., the protocol of step 3), and can reconstruct s_1 from these messages using the reconstruction function of this protocol (since $f(S_1, S_2) = 1$). By symmetric arguments, the parties in A can reconstruct s_2 (using the protocol of step 4), and, thus, the parties in A can reconstruct the secret s by summing s_1 and s_2. Authorized sets of size greater than $(\frac{1}{2}+\delta)n$ can reconstruct the secret s using the $((\frac{1}{2}+\delta)n+1)$-out-of-$n$ secret-sharing scheme (i.e., the scheme of step 1).

For the security of the scheme, take an unauthorized set $A \notin \Gamma_{B,\mathrm{mid}}$, that is, $A = S_1 \cup S_2$ such that $S_1 \subseteq B, S_2 \subseteq \overline{B}$ and $|S_1 \cup S_2| \leq (\frac{1}{2}+\delta)n$ (subsets of size greater than $(\frac{1}{2}+\delta)n$ are authorized), and assume without loss of generality that $|S_1| \leq (\frac{1}{4}+\frac{\delta}{2})n$ (otherwise, $|S_2| \leq (\frac{1}{4}+\frac{\delta}{2})n$ and we consider the second CDS protocol, i.e, the protocol of step 4). In the first CDS protocol (i.e, the protocol of step 3), the parties in S_1 know a message of Alice on an input $S_1' \in \mathcal{B}_1$ if and only if $S_1' \subseteq S_1$. That is, they can reconstruct the messages of the inputs (which are sets) in $\mathcal{B}_1$ for the set $T_{S_1} \stackrel{\Delta}{=} \left\{S_1' \in \mathcal{B}_1 : S_1' \subseteq S_1, |S_1'| \geq (\frac{1}{4}-\frac{\delta}{2})n\right\}$.

Scheme $\Sigma_{\mathrm{B,mid}}$

The secret: A string $s \in \{0,1\}^m$.
The scheme:

1. Share the secret s among the n parties using a $((\frac{1}{2}+\delta)n+1)$-out-of-$n$ secret-sharing scheme.
2. Choose a random string $s_1 \in \{0,1\}^m$ and define $s_2 = s - s_1$ (where the sum is in $\mathbb{Z}_2^m$).
3. Execute a 2-party $(\mathcal{T}_1, 2^{n/2})$-robust CDS protocol ($\mathcal{T}_1$ will be determined later) for the function f with the secret s_1, and share the message of Alice (respectively, Bob) when holding the input S_1 (respectively, S_2) among the parties of S_1 (respectively, S_2) using an $|S_1|$-out-of-$|S_1|$ (respectively, $|S_2|$-out-of-$|S_2|$) secret-sharing scheme, for every $S_1 \in \mathcal{B}_1$ (respectively, $S_2 \in \mathcal{B}_2$).
4. Execute a 2-party $(2^{n/2}, \mathcal{T}_2)$-robust CDS protocol ($\mathcal{T}_2$ will be determined later) for the function f with the secret s_2, and share the message of Alice (respectively, Bob) when holding the input S_1 (respectively, S_2) among the parties of S_1 (respectively, S_2) using an $|S_1|$-out-of-$|S_1|$ (respectively, $|S_2|$-out-of-$|S_2|$) secret-sharing scheme, for every $S_1 \in \mathcal{B}_1$ (respectively, $S_2 \in \mathcal{B}_2$).

Figure 4: A secret-sharing scheme $\Sigma_{\mathrm{B,mid}}$ realizing the access structure $\Gamma_{\mathrm{B,mid}}$.

The number of subsets in T_{S_1} is at most

$$t \triangleq \sum_{i=(\frac{1}{4}-\frac{\delta}{2})n}^{(\frac{1}{4}+\frac{\delta}{2})n} \binom{(\frac{1}{4}+\frac{\delta}{2})n}{i}.$$

When $\delta < \frac{1}{6}$, we have that

$$t = O(n \cdot \binom{(\frac{1}{4}+\frac{\delta}{2})n}{(\frac{1}{4}-\frac{\delta}{2})n}) = O(n 2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{4}+\frac{\delta}{2})n});$$

otherwise, the biggest summand is for $i = \frac{1}{2}(\frac{1}{4}+\frac{\delta}{2})n$, and $t = O(2^{(\frac{1}{4}+\frac{\delta}{2})n})$.

We define $\mathcal{T}_1 \subseteq \binom{\mathcal{B}_1}{\leq t}$ as $\mathcal{T}_1 \triangleq \left\{T_{S_1} : S_1 \subseteq B, |S_1| \leq (\frac{1}{4}+\frac{\delta}{2})n\right\}$. Thus,

$$|\mathcal{T}_1| = \sum_{i=0}^{(\frac{1}{4}+\frac{\delta}{2})n} \binom{n/2}{i} < 2^{n/2}.$$

We use this $\mathcal{T}_1$ in the 2-party $(\mathcal{T}_1, 2^{n/2})$-robust CDS protocol of step 3 of scheme $\Sigma_{\mathrm{B,mid}}$ (for the 2-party $(2^{n/2}, \mathcal{T}_2)$-robust CDS protocol of step 4 we define $\mathcal{T}_2$ symmetrically).

For every $S_1' \subseteq S_1$ and $S_2' \subseteq S_2$, we have that (S_1', S_2') is a zero-input of f, and the parties in $A = S_1 \cup S_2$ (which learn the messages on the inputs of T_{S_1} of Alice and possibly many messages of Bob) learn only messages of the zero-inputs set $T_{S_1} \times \{S_2' \in \mathcal{B}_2 : S_2' \subseteq S_2\}$ in the first CDS protocol. Thus, by the robustness of the CDS protocol, the parties in A cannot learn any information on s_1, and, hence, they cannot learn any information on the secret s.

Overall, in the resulting scheme each party P_i gets a share of size $\max\{m, \log n\}$ from the threshold scheme of step 1 and less than $N = |\mathcal{B}_1| = |\mathcal{B}_2| < 2^{n/2}$ shares from the threshold schemes of

step 3 (respectively, step 4), one for each message of the CDS protocol for f on an input S such that $P_i \in S$. Thus, the share size of each party in the scheme $\Sigma_{\mathrm{B,mid}}$ is $O(2^{n/2} \cdot c(t, |\mathcal{T}_1|, N, m))$, which is $O(2^{n/2} c(n2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{4}+\frac{\delta}{2})n}, 2^{n/2}, 2^{n/2}, m))$ for $\delta < \frac{1}{6}$, and $O(2^{n/2} c(2^{(\frac{1}{4}+\frac{\delta}{2})n}, 2^{n/2}, 2^{n/2}, m))$ otherwise. Additionally, this transformation preserves linearity. □

We use the above scheme and the family of "balancing" subsets of Lemma 2.21 to construct a scheme that realizes the access structure Γ_{mid}.

Theorem 4.5. *Let Γ be a an access structure over a set of n parties and $\delta \in (0, \frac{1}{2})$. Assume that for every integer N, every $t \in [N]$, every $\mathcal{T} \subseteq \binom{[N]}{\leq t}$, and every function $f : [N] \times [N] \to \{0,1\}$, there is a 2-party $(\mathcal{T}, N)$-robust CDS protocol for f with secrets of size m in which the message size is $c(t, |\mathcal{T}|, N, m)$, for some integer $m \geq 1$. Then, there is a secret-sharing scheme realizing Γ_{mid} for secrets of size m in which the share size is $O(n^{3/2} 2^{n/2} c(n2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{4}+\frac{\delta}{2})n}, 2^{n/2}, 2^{n/2}, m))$ for $\delta < \frac{1}{6}$ and $O(n^{3/2} 2^{n/2} c(2^{(\frac{1}{4}+\frac{\delta}{2})n}, 2^{n/2}, 2^{n/2}, m))$ otherwise. Moreover, if the CDS protocol is linear then the resulting scheme is also linear.*

Proof. As in Lemma 4.4, assume without loss of generality that n is even. By Lemma 2.21, there exist $\ell = \Theta(n^{3/2})$ subsets $B_1, \ldots, B_\ell \subseteq P$, where $|B_i| = n/2$ for every $i \in [\ell]$, such that for every subset A such that $(\frac{1}{2} - \delta)n \leq |A| \leq (\frac{1}{2} + \delta)n$, it holds that $|A \cap B_i| = \lfloor |A|/2 \rfloor$ for at least one $i \in [\ell]$. Thus, we get that $\Gamma_{\mathrm{mid}} = \cup_{i=1}^{\ell} \Gamma_{B_i,\mathrm{mid}}$. By Lemma 4.4, for every $i \in [\ell]$ there is a secret-sharing scheme $\Sigma_{B_i,\mathrm{mid}}$ realizing the access structure $\Gamma_{B_i,\mathrm{mid}}$ for secrets of size m in which the share size is $O(2^{n/2} c(n2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{4}+\frac{\delta}{2})n}, 2^{n/2}, 2^{n/2}, m))$ for $\delta < \frac{1}{6}$, and $O(2^{n/2} c(2^{(\frac{1}{4}+\frac{\delta}{2})n}, 2^{n/2}, 2^{n/2}, m))$ otherwise. As in Claim 2.10, for every $i \in [\ell]$ we independently share the secret s using $\Sigma_{B_i,\mathrm{mid}}$ realizing the access structure $\Gamma_{B_i,\mathrm{mid}}$. The combined scheme is a secret-sharing scheme realizing the access structure Γ_{mid} for secrets of size m in which the share size is $O(n^{3/2} 2^{n/2} c(n2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{4}+\frac{\delta}{2})n}, 2^{n/2}, 2^{n/2}, m))$ for $\delta < \frac{1}{6}$, and $O(n^{3/2} 2^{n/2} c(2^{(\frac{1}{4}+\frac{\delta}{2})n}, 2^{n/2}, 2^{n/2}, m))$ otherwise. □

Using the linear robust CDS protocol of Theorem 3.4 we get the following scheme.

Corollary 4.6. *Let Γ be a an access structure over a set of n parties and $\delta \in (0, \frac{1}{2})$. Then, for every finite field $\mathbb{F}$, there is a linear secret-sharing scheme realizing Γ_{mid} for one-element secrets in which the share size is $O(\mathrm{poly}(n) 2^{n/2} (2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{4}+\frac{\delta}{2})n} + 2^{n/4}) \log |\mathbb{F}|)$ for $\delta < \frac{1}{6}$ and $O(\mathrm{poly}(n) 2^{n/2} (2^{(\frac{1}{4}+\frac{\delta}{2})n} + 2^{n/4}) \log |\mathbb{F}|)$ otherwise, i.e., for $\delta \in (0, \frac{1}{6})$ the exponent of the scheme is $M_\ell(\delta) = \frac{1}{2} + \max\left\{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{4} + \frac{\delta}{2}), \frac{1}{4}\right\}$.*

Proof. By Theorem 3.4, for every finite field $\mathbb{F}$, every N, every $t \in [N]$, every $\mathcal{T} \subseteq \binom{[N]}{\leq t}$, and every function $f : [N] \times [N] \to \{0,1\}$, there is a linear 2-party $(\mathcal{T}, N)$-robust CDS protocol for f with one-element secrets in which the message size is $c(t, |\mathcal{T}|, N, \log |\mathbb{F}|) = O((t \log^2 t + \sqrt{N}) \log t \log N \log |\mathcal{T}| \log |\mathbb{F}|)$. Thus, by Theorem 4.5 we get that there is a linear secret-sharing scheme realizing Γ_{mid} for one-element secrets in which the share size is

$$\begin{aligned}
&O(n^{3/2} 2^{n/2} c(n2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{4}+\frac{\delta}{2})n}, 2^{n/2}, 2^{n/2}) \log |\mathbb{F}|) \\
&= O(n^{3/2} 2^{n/2} (n2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{4}+\frac{\delta}{2})n} + 2^{n/4}) \log^3 (n2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{4}+\frac{\delta}{2})n}) \log 2^{n/2} \log 2^{n/2} \log |\mathbb{F}|) \\
&= O(\mathrm{poly}(n) 2^{n/2} (2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{4}+\frac{\delta}{2})n} + 2^{n/4}) \log |\mathbb{F}|)
\end{aligned}$$

for $\delta < \frac{1}{6}$. The proof for $\delta \geq \frac{1}{6}$ is similar. □

4.3 Secret-sharing Schemes Realizing any Access Structure

By Lemma 4.2 and Corollary 4.6 we obtain the following corollary.

Corollary 4.7. *Let Γ be a an access structure over a set of n parties and $\delta \in (0, \frac{1}{6})$. Then, Γ can be linearly realized by a secret-sharing scheme with an exponent of*

$$\max\left\{h\left(\frac{1}{2}-\delta\right)-\left(\frac{1}{2}-\delta\right)\log\left(\frac{1+2\delta}{1-2\delta}\right), \frac{1}{2}+\max\left\{h\left(\frac{1-2\delta}{1+2\delta}\right)\left(\frac{1}{4}+\frac{\delta}{2}\right), \frac{1}{4}\right\}\right\}. \tag{2}$$

Define $\delta^\star \in (0, \frac{1}{6})$ as the value that satisfies

$$c^\star = h\left(\frac{1}{2}-\delta^\star\right)-\left(\frac{1}{2}-\delta^\star\right)\log\left(\frac{1+2\delta^\star}{1-2\delta^\star}\right) = \frac{1}{2}+\max\left\{h\left(\frac{1-2\delta^\star}{1+2\delta^\star}\right)\left(\frac{1}{4}+\frac{\delta^\star}{2}\right), \frac{1}{4}\right\},$$

That is, the minimal value of the exponent of the secret-sharing scheme of Corollary 4.7 realizing any access structure equals to $c^\star$. The value $\delta^\star \approx 0.0898524$ satisfies the above expression, and achieves an exponent of $c^\star = 0.761574$. The curves of the two functions in (2) and their intersection at $\delta^\star$ are described in Figure 5.

Theorem 4.8. *Let Γ be a an access structure over a set of n parties. Then, for every finite field $\mathbb{F}$, there is a linear secret-sharing scheme realizing Γ for one-element secrets in which the share size is $2^{0.7616n+o(n)} \log|\mathbb{F}|$.*

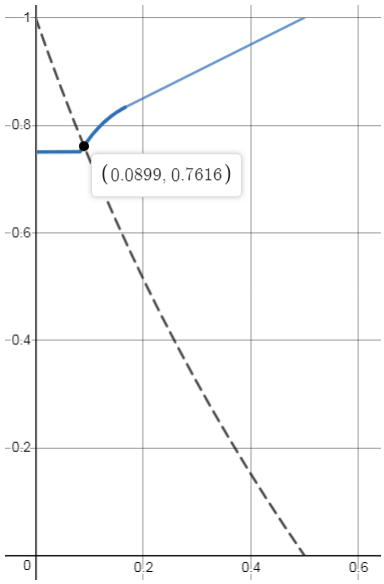

Figure 5: A description of the functions $M_\ell(\delta)$ and $X'(\delta)$. The x-axis represents δ and the y-axis represents the exponent. The dashed black curve represents the exponent $X'(\delta)$ of the scheme of [4] realizing the access structures Γ_{top} and Γ_{bot}, and the solid blue curve represents the exponent $M_\ell(\delta)$ of our scheme of Corollary 4.6 realizing the access structures Γ_{mid}. The exponent of our scheme of Theorem 4.8 realizing the access structures Γ appears as the y-coordinate of the intersection of the black and the blue curves.

4.4 From $(\mathcal{T}, N, N)$-Robust CDS Protocols to Secret-Sharing Schemes

We generalize our ideas and show how to transform a 3-party $(\mathcal{T}, N, N)$-robust CDS protocol to a secret-sharing scheme realizing the access structure Γ_{mid}. Thus, we get another scheme realizing any access structure Γ. Alas, the share size of this scheme is larger than the share size of the scheme in Section 4.3. We can use the same paradigm to construct a secret-sharing scheme realizing any access structure Γ from a k-party $(\mathcal{T}, N, \ldots, N)$-robust CDS protocol.

Assume that for every integer N, every $t \in [N]$, every $\mathcal{T} \subseteq \binom{[N]}{\leq t}$, and every function $f : [N] \times [N] \times [N] \to \{0,1\}$, there is a 3-party $(\mathcal{T}, N, N)$-robust CDS protocol for f with secrets of size m in which the message size is $c(t, |\mathcal{T}|, N, m)$, for some integer $m \geq 1$. Similarly to Definition 4.3, we first define the access structure $\Gamma_{(B_1,B_2,B_3),\mathrm{mid}}$, where (B_1, B_2, B_3) is a partition of $P = \{P_1, \ldots, P_n\}$ such that $|B_1| = |B_2| = |B_3| = n/3$ (assume without loss of generality that n is divided by 3). The access structure $\Gamma_{(B_1,B_2,B_3),\mathrm{mid}}$ contains all subsets of parties of size greater than $(\frac{1}{2} + \delta)n$, and all subsets of parties that contain authorized subsets $A' \in \Gamma$ of size between $(\frac{1}{2} - \delta)n$ and $(\frac{1}{2} + \delta)n$ that contain exactly $|A'|/3$ of their parties from B_i, for every $i \in [3]$. Then, similarly to Lemma 4.4, define $\mathcal{B}_i = \left\{S_i \subseteq B_i : (\frac{1}{6} - \frac{\delta}{3})n \leq |S_i| \leq (\frac{1}{6} + \frac{\delta}{3})n\right\}$ for every $i \in [3]$, and the function $f : \mathcal{B}_1 \times \mathcal{B}_2 \times \mathcal{B}_3 \to \{0,1\}$, where $f(S_1, S_2, S_3) = 1$ if and only if $S_1 \cup S_2 \cup S_3 \in \Gamma$, $(\frac{1}{2} - \delta)n \leq |S_1 \cup S_2 \cup S_3| \leq (\frac{1}{2} + \delta)n$, and $|S_1| = |S_2| = |S_3|$.

We construct a secret-sharing scheme realizing $\Gamma_{(B_1,B_2,B_3),\mathrm{mid}}$ as follows: (1) Share the secret $s \in \{0,1\}^m$ among the n parties using a $((\frac{1}{2} + \delta)n + 1)$-out-of-$n$ secret-sharing scheme. (2) Choose random strings $s_1, s_2, s_3 \in \{0,1\}^m$ such that $s = s_1 + s_2 + s_3$. (3) Execute a 3-party $(\mathcal{T}_1, 2^{n/3}, 2^{n/3})$-robust CDS protocol ($\mathcal{T}_1$ will be determined later) for the function f with the secret s_1, and share the message of P_1 (respectively, P_2 or P_3) when holding the input S_1 (respectively, S_2 or S_3) among the parties of S_1 (respectively, S_2 or S_3) using an $|S_1|$-out-of-$|S_1|$ (respectively, $|S_2|$-out-of-$|S_2|$ or $|S_3|$-out-of-$|S_3|$) secret-sharing scheme, for every $S_1 \in \mathcal{B}_1$ (respectively, $S_2 \in \mathcal{B}_2$ or $S_3 \in \mathcal{B}_3$). We do the same for a 3-party $(2^{n/3}, \mathcal{T}_2, 2^{n/3})$-robust and a 3-party $(2^{n/3}, 2^{n/3}, \mathcal{T}_3)$-robust CDS protocols for f.

The correctness of the scheme follows from the same arguments as in Lemma 4.4. For the security of the scheme, take an unauthorized set $A \notin \Gamma_{(B_1,B_2,B_3),\mathrm{mid}}$, and let $i \in [3]$ such that $|S_i| = |A \cap B_i| \leq (\frac{1}{6} + \frac{\delta}{3})n$. As in Lemma 4.4, we define the set $T_{S_i} = \left\{S'_i \in \mathcal{B}_i : S'_i \subseteq S_i, |S'_i| \geq (\frac{1}{6} - \frac{\delta}{3})n\right\}$, and get that $|T_{S_i}|$ is at most $t = \sum_{j=(\frac{1}{6}-\frac{\delta}{3})n}^{(\frac{1}{6}+\frac{\delta}{3})n} \binom{(\frac{1}{6}+\frac{\delta}{3})n}{j} \leq O(n \cdot \binom{(\frac{1}{6}+\frac{\delta}{3})n}{(\frac{1}{6}-\frac{\delta}{3})n}) = O(n 2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{6}+\frac{\delta}{3})n})$ for $\delta < \frac{1}{6}$. We define $\mathcal{T}_i \subseteq \binom{\mathcal{B}_i}{\leq t}$ as $\mathcal{T}_i = \left\{T_{S_i} : S_i \subseteq B_i, |S_i| \leq (\frac{1}{6} + \frac{\delta}{3})n\right\}$. Thus, $|\mathcal{T}_i| = \sum_{j=0}^{(\frac{1}{6}+\frac{\delta}{3})n} \binom{n/3}{j} < 2^{n/3}$.

Overall, in the resulting scheme each party gets less than $N = |\mathcal{B}_i| < 2^{n/3}$ shares from the threshold schemes, so the share size of each party in the scheme is $O(2^{n/3} \cdot c(t, |\mathcal{T}_i|, N, m))$, which is $O(2^{n/3} c(n 2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{6}+\frac{\delta}{3})n}, 2^{n/3}, 2^{n/3}, m))$ for $\delta < \frac{1}{6}$.

By using a family of "balancing" partitions of the n parties (similarly to Lemma 2.21) we get a scheme realizing Γ_{mid} with share size $O(\mathrm{poly}(n) 2^{n/3} c(n 2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{6}+\frac{\delta}{3})n}, 2^{n/3}, 2^{n/3}, m))$ for $\delta < \frac{1}{6}$ (similarly to Theorem 4.5). By Remark 6.6, we have a linear 3-party $(\mathcal{T}, N, N)$-robust CDS protocol with one-element secrets in which the message size is $\tilde{O}(tN \log|\mathcal{T}| \log|\mathbb{F}|)$. Hence, we get a linear scheme realizing Γ_{mid} for one-element secrets with share size $O(\mathrm{poly}(n) 2^{2n/3} 2^{h(\frac{1-2\delta}{1+2\delta})(\frac{1}{6}+\frac{\delta}{3})n} \log|\mathbb{F}|)$ for $\delta < \frac{1}{6}$, i.e., the exponent of the scheme is $M_\ell(\delta) = \frac{2}{3} + h(\frac{1-2\delta}{1+2\delta})(\frac{1}{6} + \frac{\delta}{3})$ for $\delta < \frac{1}{6}$. Thus, by Lemma 4.2, we obtain a linear scheme realizing any access structure Γ with an exponent of $\max\left\{h\left(\frac{1}{2} - \delta\right) - \left(\frac{1}{2} - \delta\right) \log\left(\frac{1+2\delta}{1-2\delta}\right), \frac{2}{3} + h(\frac{1-2\delta}{1+2\delta})(\frac{1}{6} + \frac{\delta}{3})\right\}$ for $\delta < \frac{1}{6}$. The minimal value of the exponent of this scheme is obtained by taking $\delta \approx 0.0677412$, which achieves an exponent of 0.816695.

5 Constructions of Robust k-Party CDS Protocols

In this section we show how to transform any k-party CDS protocol to a robust k-party CDS protocol. This is done using the families of hash functions of Lemma 2.19 and Lemma 2.20 (similar to the constructions of Section 3). This transformation can be applied to any CDS protocol. For $k = 2$, this results in a 2-party t-robust CDS protocol whose normalized message size is $\tilde{O}(t)$ times the message size of the original 2-party CDS protocol. For example, take a function that has a small branching program; then, it has an efficient CDS protocol [42]. Thus, using our transformation, we get that this function also has an efficient robust CDS protocol, when t is small. We describe the transformation in two stages. First, in Lemma 5.1, we describe a transformation which increase the normalized message size of the original protocol by a multiplicative factor of $O(t^{2k-2})$. Then, in Theorem 5.2, we show how to use this robust CDS protocol to construct a t-robust CDS protocol with multiplicative overhead of $\tilde{O}(k(2k^2t)^{k-1})$. This transformation is efficient when k is a small constant, e.g., when $k = 3$ the multiplicative overhead is $\tilde{O}(t^2)$.

Lemma 5.1. *Let $f : [N]^k \to \{0,1\}$ be a k-input function, for some integer $k > 1$, and $t \leq \sqrt{kN}$ be an integer. Assume that for some integer $m \geq 1$, there is a k-party CDS protocol $\mathcal{P}$ for f with secrets of size m in which the message size is $c_f(m)$. Then, there is a k-party t-robust CDS protocol for f with secrets of size m in which the message size is $O(t^{2k-1}c_f(m)\log(kN))$. If $\mathcal{P}$ is a linear protocol over $\mathbb{F}_{2^m}$, then the resulting protocol is also linear. Furthermore, there is a k-party t-robust CDS protocol for f with secrets of size $\Theta(mt\log(kN))$ in which the normalized message size is $O(t^{2k-2}c_f(m)/m)$.*

Proof. Let $H_{kN,t,t^2} = \left\{h_i : [k] \times [N] \to [t^2] : i \in [\ell]\right\}$, where $\ell = \Theta(t\log(kN))$, be the family of hash functions promised by Lemma 2.19 for $\mathcal{T} = \binom{[k]\times[N]}{\leq t}$ (that is, $|\mathcal{T}| = \Theta((kN)^t)$). We use the hash functions in H_{kN,t,t^2} to partition the inputs of the parties. For efficiency, we use one family of hash functions to partition all input domains.

The t-robust CDS protocol for f is as follows: Let $s \in \{0,1\}^m$ be the secret, and choose ℓ random strings $s_1, \ldots, s_\ell \in \{0,1\}^m$ such that $s = s_1 + \cdots + s_\ell$, where the sum is in $\mathbb{Z}_2^m$. For every $h_i \in H_{kN,t,t^2}$, we execute a CDS protocol for f as follows. For every $a \in [k]$ and every $j \in [t^2]$, let $A_{a,j} = \{x \in [N] : h_i(a,x) = j\}$. For every $j_1, \ldots, j_k \in [t^2]$, execute a CDS protocol (with an independent common random string) for the restriction of f to $A_{1,j_1} \times \cdots \times A_{k,j_k}$ with the secret s_i. That is, for every $a \in [k]$, party P_a on input x_a sends messages for the restriction of f to $A_{1,j_1} \times \cdots \times A_{a,h_i(a,x_a)} \times \cdots \times A_{k,j_k}$, for every $j_1, \ldots, j_{a-1}, j_{a+1}, \ldots j_k \in [t^2]$.

We first show the correctness of the CDS protocol for every $h_i \in H_{kN,t,t^2}$. For inputs $(x_1, \ldots, x_k) \in [N]^k$ such that $f(x_1, \ldots, x_k) = 1$, the referee can reconstruct s_i using the messages on the inputs $x_1, \ldots, x_k$ in the CDS protocol for the restriction of f to the inputs of $A_{1,h_i(1,x_1)} \times \cdots \times A_{k,h_i(k,x_k)}$ with the secret s_i. Overall, the referee can learn all the strings $s_1, \ldots, s_\ell$, so it can reconstruct the secret s by summing these strings.

For the robustness of the protocol, let $(S_1, \ldots, S_k)$ be a zero-inputs set of f such that $|S_1| + \cdots + |S_k| \leq t$. By Lemma 2.19, there is at least one $i \in [\ell]$ for which $|h_i(\{1\} \times S_1 \cup \cdots \cup \{k\} \times S_k)| = |S_1| + \cdots + |S_k|$. For every $a \in [k]$, since h_i is one-to-one on S_a, then each input of S_a is in a different subset $A_{a,j}$ in the partition induced by h_i, so the referee gets at most one message of each of the parties $P_1, \ldots, P_k$ in each execution of the (non-robust) CDS protocol. Thus, by the security of the CDS protocol for f, the referee cannot learn any information about s_i from any of the independent CDS protocols for the restriction of f to the inputs of $A_{1,j_1} \times \cdots \times A_{k,j_k}$. By Claim 2.16, the referee cannot learn any information on s_i, and, hence, it cannot learn any information on the secret s.

The message size of each party in the resulting protocol is $O(t^{2k-2}\ell c_f(m)) = O(t^{2k-1}c_f(m)\log(kN))$, since each party sends $(t^2)^{k-1} = t^{2k-2}$ messages of the CDS protocol for every $h_i \in H_{kN,t,t^2}$.

To construct the desired protocol for long secrets, let $s = (s'_1, \ldots, s'_{\ell/4}) \in \mathbb{F}_{2^m}^{\ell/4}$ be the secret. We use the protocol of Proposition 2.17 with the above ℓ CDS protocols, one for every hash function $h_i \in H_{kN,t,t^2}$. That is, now $s_1, \ldots, s_\ell \in \mathbb{F}_{2^m}$ are shares of a $(3\ell/4, \ell, \ell)$-ramp secret-sharing scheme of the secret $s = (s'_1, \ldots, s'_{\ell/4}) \in \mathbb{F}_{2^m}^{\ell/4}$. As above, for every inputs $(x_1, \ldots, x_k) \in [N]^k$ such that $f(x_1, \ldots, x_k) = 1$, the referee can learn each secret s_i in those ℓ protocols from the messages on the inputs $x_1, \ldots, x_k$, so it can reconstruct the secret s using the reconstruction function of the ramp scheme. Moreover, for every $(S_1, \ldots, S_k)$ that is a zero-inputs set of f such that $|S_1| + \cdots + |S_k| \leq t$, there are at least $\ell/4$ values of $i \in [\ell]$ for which $|h_i(\{1\} \times S_1 \cup \cdots \cup \{k\} \times S_k)| = |S_1| + \cdots + |S_k|$. Thus, the referee cannot learn any information on at least $\ell/4$ secrets in the above ℓ protocols from the messages on the inputs of $S_1, \ldots, S_k$, so by the security of the ramp scheme, the referee cannot learn any information on the secret s. □

Theorem 5.2. *Let $f : [N]^k \to \{0,1\}$ be a k-input function, for some integer $k > 1$, and $t \leq \min\left\{kN/2, 2\sqrt{N/k}\right\}$ be an integer. Assume that for some integer $m \geq 1$, there is a k-party CDS protocol $\mathcal{P}$ for f with secrets of size m in which the message size is $c_f(m)$. Then, there is a k-party t-robust CDS protocol for f with secrets of size m in which the message size is $O(k^{2k-1}2^k t^k c_f(m) \log^{2k-1} t \log^2(kN))$. If $\mathcal{P}$ is a linear protocol over $\mathbb{F}_{2^m}$, then the resulting protocol is also linear. Furthermore, there is a k-party t-robust CDS protocol for f with secrets of size $\Theta(mt \log t \log^2(kN))$ in which the normalized message size is $O(k^{2k-1}2^k t^{k-1} c_f(m)/m \cdot \log^{2k-2} t)$.*

Proof. Let $H_{kN,t,2t} = \{h_i : [k] \times [N] \to [2t] : i \in [\ell]\}$, where $\ell = \Theta(t \log(kN))$, be the family of perfect hash functions promised by Lemma 2.20 for $\mathcal{T} = \binom{[k]\times[N]}{\leq t}$ (that is, $|\mathcal{T}| = \Theta((kN)^t)$).

Protocol $\mathcal{P}_{\mathrm{kRCDS}}$

The secret: A string $s \in \{0,1\}^m$.
The protocol:

1. Choose ℓ random strings $s_1, \ldots, s_\ell \in \{0,1\}^m$ such that $s = s_1 + \cdots + s_\ell$.
2. For every $i \in [\ell]$ do:
   - Let $A_{a,j} = \{x \in [N] : h_i(a,x) = j\}$, for every $a \in [k]$ and every $j \in [2t]$.
   - For every $j_1, \ldots, j_k \in [2t]$, independently execute the k-party $k \log t$-robust CDS protocol of Lemma 5.1 for the restriction of f to $A_{1,j_1} \times \cdots \times A_{k,j_k}$ with the secret s_i. That is, for every $a \in [k]$, party P_a with input x_a sends a message for the restriction of f to $A_{1,j_1} \times \cdots \times A_{a-1,j_{a-1}} \times A_{a,h_i(a,x_a)} \times A_{a+1,j_{a+1}} \times \cdots \times A_{k,j_k}$ for every $j_1, \ldots, j_{a-1}, j_{a+1}, \ldots, j_k \in [2t]$.

Figure 6: A k-party t-robust CDS protocol $\mathcal{P}_{\mathrm{kRCDS}}$ for a function $f : [N]^k \to \{0,1\}$.

The desired CDS protocol $\mathcal{P}_{\mathrm{kRCDS}}$ for f is described in Figure 6. The protocol $\mathcal{P}_{\mathrm{kRCDS}}$ contains $(2t)^k \ell$ executions of the k-party $k \log t$-robust CDS protocol of Lemma 5.1 (since $t \leq \min\left\{kN/2, 2\sqrt{N/k}\right\}$, we have that $k \log t \leq \sqrt{kN}$ as required). For every $a \in [k]$, since party P_a sends $(2t)^{k-1}$ messages of the protocol of Lemma 5.1 for every $h_i \in H_{kN,t,2t}$, its message size is $O((k \log t)^{2k-1} c_f(m) \log(kN) \cdot (2t)^{k-1}\ell) = O(k^{2k-1}2^k t^k c_f(m) \log^{2k-1} t \log^2(kN))$.

For the correctness of the protocol, let $(x_1, \ldots, x_k) \in [N]^k$ such that $f(x_1, \ldots, x_k) = 1$. For every $i \in [\ell]$, the referee can reconstruct s_i using the messages on the inputs $x_1, \ldots, x_k$ in the CDS protocol for

the restriction of f to $A_{1,h_i(1,x_1)} \times \cdots \times A_{k,h_i(k,x_k)}$. Overall, the referee can learn all the strings $s_1, \ldots, s_\ell$, so it can reconstruct the secret s by summing these strings, where the sum is in $\mathbb{Z}_2^m$.

For the robustness of the protocol, let $(S_1, \ldots, S_k)$ be a zero-inputs set of f such that $|S_1|+\cdots+|S_k| \leq t$. By Lemma 2.20, there is at least one $i \in [\ell]$ such that for every $a \in [k]$ and every $j \in [2t]$, it holds that $|\{x_a \in S_a : h_i(a, x_a) = j\}| < \log t$. Thus, each $A_{a,j}$ contains less than $\log t$ input of S_a, and, hence, since each of the protocols of Lemma 5.1 executed in protocol $\mathcal{P}_{\mathrm{kRCDS}}$ is $k \log t$-robust, the referee cannot learn any information on s_i from each such protocol. By Claim 2.16, since each of the protocols of Lemma 5.1 is executed with independent common random string, the referee cannot learn any information on s_i from the $(2t)^k$ protocols (with the function h_i), and, hence, it cannot learn any information on the secret s.

The construction of the desired protocol for long secrets is similar to the construction in Lemma 5.1. □

6 Linear Robust k-Party CDS Protocols

In this section, we construct linear robust k-party CDS protocols for arbitrary functions. For an integer $k > 2$, we present linear k-party $(\mathbf{t}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})$-robust CDS protocols for k-input functions $f : [N]^k \to \{0,1\}$, that is, a CDS protocol that is secure when each of the first $\lfloor k/2 \rfloor$ parties sends at most t messages and each of the last $\lceil k/2 \rceil$ parties sends any number of messages (as long as these messages are for a zero-inputs set). As in the previous section, we think of k as a small constant, e.g., $k = 3$.

6.1 Linear $(\mathbf{1}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})$-Robust CDS Protocols

We start by showing that a variant of the k-party CDS protocol of [17] is $(\mathbf{1}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})$-robust.

Claim 6.1. *Let $f : [M] \times [N]^{k-1} \to \{0,1\}$ be a k-input function, for some integer $k > 2$. Then, for every finite field $\mathbb{F}$, protocol $\mathcal{P}_k^{(\mathbf{1}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})}$, described in Figure 7, is a linear k-party $(\mathbf{1}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})$-robust CDS protocol for f with one-element secrets in which the message size of party P_1 is $O(MN^{\lfloor k/2 \rfloor - 1} \log |\mathbb{F}|)$ and the message size of parties $P_2, \ldots, P_k$ is $O(N^{\lceil k/2 \rceil - 1} \log |\mathbb{F}|)$.*

Proof. In protocol $\mathcal{P}_k^{(\mathbf{1}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})}$, described in Figure 7, the first $\lfloor k/2 \rfloor$ parties simulate Alice in the 2-party CDS protocol $\mathcal{P}_2^{(1,N)}$ and the last $\lceil k/2 \rceil$ parties simulate Bob. The correctness of the protocol $\mathcal{P}_k^{(\mathbf{1}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})}$ is detailed in [17].

For the robustness of the protocol, recall that $k' = \lfloor k/2 \rfloor$ (that is, if k is even then $k' = k/2$ and if k is odd then $k' = (k-1)/2$). Assume without loss of generality that there exist $a_1 \in [M]$ such that $f(a_1, i_2, \ldots, i_k) = 0$ for every $i_2, \ldots, i_k \in [N]$ (this can be done by adding a dummy element to the input domain of the first party), and assume that parties $P_1, \ldots, P_{k'}$ send messages of inputs $x_1 \in [M]$ and $x_2 \ldots, x_{k'} \in [N]$, respectively, and parties $P_{k'+1}, \ldots, P_k$ send multiple messages for subsets of inputs $S_{k'+1}, \ldots, S_k \subseteq [N]$, respectively, such that $f(x_1, \ldots, x_{k'}, x_{k'+1}, \ldots, x_k) = 0$ for every $(x_{k'+1}, \ldots, x_k) \in S_{k'+1} \times \cdots \times S_k$. Thus, the referee learns the elements $r_{i_1,\ldots,i_{k'}}$ for every $i_1 \in [M]$ and every $i_2, \ldots, i_{k'} \in [N]$ except for $r_{x_1,\ldots,x_{k'}}$, the elements

$$s_{x_{k'+1},i_{k'+2},\ldots,i_k} = s + q_{i_{k'+2},\ldots,i_k} + \sum\nolimits_{i_1 \in [M], i_2,\ldots,i_{k'} \in [N], f(i_1,\ldots,i_{k'},x_{k'+1},i_{k'+2},\ldots,i_k)=0} r_{i_1,\ldots,i_{k'}}$$

for every $i_{k'+2}, \ldots, i_k \in [N]$ and every $x_{k'+1} \in S_{k'+1}$, and the elements $q_{x_{k'+2},\ldots,x_k}$ for every $(x_{k'+2}, \ldots, x_k) \in S_{k'+2} \times \cdots \times S_k$; for every $(x_{k'+1}, \ldots, x_k) \in S_{k'+1} \times \cdots \times S_k$, the element $r_{x_1,\ldots,x_{k'}}$ is part of each sum of $s_{x_{k'+1},x_{k'+2},\ldots,x_k}$. Intuitively, for every $(x_{k'+1}, \ldots, x_k) \in S_{k'+1} \times \cdots \times S_k$, the

Protocol $\mathcal{P}_k^{(\mathbf{1}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})}$

The secret: An element $s \in \mathbb{F}$.
Inputs: Parties $P_1, \ldots, P_k$ hold the inputs $x_1 \in [M]$ and $x_2, \ldots, x_k \in [N]$, respectively.
Common randomness: Let $k' = \lfloor k/2 \rfloor$. The k parties hold the following uniformly distributed and independent random elements.

- $r_{i_1,\ldots,i_{k'}} \in \mathbb{F}$, for every $i_1 \in [M]$ and every $i_2, \ldots, i_{k'} \in [N]$.
- $t_{i_j,\ldots,i_{k'}} \in \mathbb{F}$, for every $j \in \{2, \ldots, k'\}$ and every $i_j, \ldots, i_{k'} \in [N]$.
- $q^j_{i_j,\ldots,i_k} \in \mathbb{F}$, for every $j \in \{k'+2, \ldots, k\}$ and every $i_j, \ldots, i_k \in [N]$.

The protocol:

1. Define $q_{i_{k'+2},\ldots,i_k} = \sum_{j=k'+2}^{k} q^j_{i_j,\ldots,i_k}$ for every $i_{k'+2}, \ldots, i_k \in [N]$.
2. Party P_1 sends to the referee the elements $r_{i_1,\ldots,i_{k'}}$ for every $i_1 \in [M]$ such that $i_1 \neq x_1$ and every $i_2 \ldots, i_{k'} \in [N]$, and the elements $r_{x_1,i_2,\ldots,i_{k'}} + t_{i_2,\ldots,i_{k'}}$ for every $i_2, \ldots, i_{k'} \in [N]$.
3. For every $j \in \{2, \ldots, k'-1\}$, party P_j sends to the referee the elements $t_{i_j,\ldots,i_{k'}}$ for every $i_j, \ldots, i_{k'} \in [N]$ such that $i_j \neq x_j$, and the elements $t_{x_j,i_{j+1}\ldots,i_{k'}} + t_{i_{j+1},\ldots,i_{k'}}$ for every $i_{j+1}, \ldots, i_{k'} \in [N]$.
4. Party $P_{k'}$ sends to the referee the elements $t_{i_{k'}}$ for every $i_{k'} \in [N]$ such that $i_{k'} \neq x_{k'}$.
5. Party $P_{k'+1}$ sends to the referee the elements

$$s_{x_{k'+1},i_{k'+2},\ldots,i_k} = s + q_{i_{k'+2},\ldots,i_k} + \sum\nolimits_{i_1 \in [M], i_2,\ldots,i_{k'} \in [N], f(i_1,\ldots,i_{k'},x_{k'+1},i_{k'+2},\ldots,i_k)=0} r_{i_1,\ldots,i_{k'}}$$

   for every $i_{k'+2}, \ldots, i_k \in [N]$.
6. For every $j \in \{k'+2, \ldots, k\}$, party P_j sends to the referee the elements $q^j_{x_j,i_{j+1}\ldots,i_k}$ for every $i_{j+1} \ldots, i_k \in [N]$.
7. If $f(x_1, \ldots, x_k) = 1$, the referee computes

$$s_{x_{k'+1},x_{k'+2},\ldots,x_k} + q_{x_{k'+2},\ldots,x_k} + \sum\nolimits_{i_1 \in [M], i_2,\ldots,i_{k'} \in [N], f(i_1,\ldots,i_{k'},x_{k'+1},x_{k'+2},\ldots,x_k)=0} r_{i_1,\ldots,i_{k'}}.$$

Figure 7: A linear k-party CDS protocol $\mathcal{P}_k^{(\mathbf{1}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})}$ for a function $f : [M] \times [N]^{k-1} \to \{0, 1\}$.

element $r_{x_1,\ldots,x_{k'}}$ acts as one-time-pad protecting s in $s_{x_{k'+1},x_{k'+2},\ldots,x_k}$, and for every $x_{k'+1} \in S_{k'+1}$ and every $(i_{k'+2},\ldots,i_k) \notin S_{k'+2} \times \cdots \times S_k$, the element $q_{i_{k'+2},\ldots,i_k}$ acts as one-time-pad protecting s in $s_{x_{k'+1},i_{k'+2},\ldots,i_k}$. Formally, the messages are independent of s since $s + r_{x_1,\ldots,x_{k'}}$ and $s + q_{i_{k'+2},\ldots,i_k}$ for every $(i_{k'+2},\ldots,i_k) \notin S_{k'+2} \times \cdots \times S_k$ are uniformly distributed, so a simulator for the protocol chooses uniformly distributed random elements as in the protocol for $s = 0$, and computes the messages as in the protocol $\mathcal{P}_k^{(\mathbf{1}_{\lfloor k/2 \rfloor},\mathbf{N}_{\lceil k/2 \rceil})}$.

Additionally, the referee cannot learn any information on the secret s from the messages of party $P_{k'+1}$ on all the inputs $x_{k'+1} \in [N]$, since by our assumption (i.e., $f(a_1,i_2,\ldots,i_k) = 0$ for every $i_2,\ldots,i_k \in [N]$), these messages are masked by the elements $r_{a_1,i_2,\ldots,i_{k'}}$ for every $i_2,\ldots,i_{k'} \in [N]$.

The message of party P_1 contains $MN^{k'-1}$ field elements, the messages of parties $P_2,\ldots,P_{k'}$ contain $N^{k'-1}, N^{k'-2},\ldots,N^2, N-1$ field elements, respectively, the message of party $P_{k'+1}$ contains $N^{k-k'-1}$ field elements, and the messages of parties $P_{k'+2},\ldots,P_k$ contains $N^{k-k'-2}, N^{k-k'-3},\ldots,N,1$ field elements, respectively. □

Remark 6.2. In the 3-party $(1,N,N)$-robust CDS protocol $\mathcal{P}_3^{(1,N,N)}$ of Claim 6.1 we do not have the random elements $t_{i_j,\ldots,i_{k'}}$. Party P_1, when holding the input $x_1 \in [M]$, sends to the referee only the elements $r_1,\ldots,r_{x_1-1},r_{x_1+1},\ldots,r_M$, party P_2, when holding the input $x_2 \in [N]$, sends to the referee the elements $s_{x_2,i_3} = s + q_{i_3} + \sum_{i_1 \in [M], f(i_1,x_2,i_3)=0} r_{i_1}$ for every $i_3 \in [N]$, and party P_3, when holding the input $x_3 \in [N]$, sends to the referee the element q_{x_3}. The message size of party P_1 is $O(M \log |\mathbb{F}|)$ and the message size of parties P_2, P_3 is $O(N \log |\mathbb{F}|)$.

The next robust k-party CDS protocol is a k-party version of the protocol of Claim 3.2, balancing the sizes of the messages of the parties.

Lemma 6.3. *Let $f : [M] \times [N]^{k-1} \to \{0,1\}$ be a k-input function, for some integer $k > 2$. Then, for every finite field $\mathbb{F}$ and every $d \in [M]$, there is a linear k-party $(\mathbf{1}_{\lfloor k/2 \rfloor},\mathbf{N}_{\lceil k/2 \rceil})$-robust CDS protocol $\mathcal{P}_k^{(\mathbf{1}_{\lfloor k/2 \rfloor},\mathbf{N}_{\lceil k/2 \rceil}),\text{balanced}}$ for f with one-element secrets in which the message size of party P_1 is $O\left((M/d)N^{\lfloor k/2 \rfloor - 1} \log |\mathbb{F}|\right)$ and the message size of parties $P_2,\ldots,P_k$ is $O\left(dN^{\lceil k/2 \rceil - 1} \log |\mathbb{F}|\right)$.*

Proof. The proof is similar to the proof of Claim 3.2. The description of the protocol $\mathcal{P}_k^{(\mathbf{1}_{\lfloor k/2 \rfloor},\mathbf{N}_{\lceil k/2 \rceil}),\text{balanced}}$ is as follows: Let s be the secret, and partition the set $[M]$ to d disjoint sets $A_1,\ldots,A_d$ of size at most $\lceil M/d \rceil$. Every input of $[M]$ is in exactly one set A_i. For every $i \in [d]$, we execute the linear CDS protocol $\mathcal{P}_k^{(\mathbf{1}_{\lfloor k/2 \rfloor},\mathbf{N}_{\lceil k/2 \rceil})}$ independently for the restriction of f to the inputs of $A_i \times [N]^{k-1}$ with the secret s. Party P_1, when holding $x_1 \in [M]$, only sends the message in the protocol for the restriction of f to the inputs of $A_i \times [N]^{k-1}$ for which $x_1 \in A_i$. Parties $P_2 \ldots,P_k$, when holding $x_2,\ldots,x_k \in [N]$, respectively, send the messages in all the above independent protocols.

As in Claim 3.2, the correctness and robustness can be verified. The message of party P_1 contains $O((M/d)N^{\lfloor k/2 \rfloor - 1})$ field elements and the messages of parties $P_2,\ldots,P_k$ contain $O(dN^{\lceil k/2 \rceil - 1})$ field elements. Thus, the message size of the CDS protocol $\mathcal{P}_k^{(\mathbf{1}_{\lfloor k/2 \rfloor},\mathbf{N}_{\lceil k/2 \rceil}),\text{balanced}}$ is as in the lemma. □

6.2 From $(1_{\lfloor k/2 \rfloor},\mathbf{N}_{\lceil k/2 \rceil})$-Robust CDS Protocols to $(\mathbf{t}_{\lfloor k/2 \rfloor},\mathbf{N}_{\lceil k/2 \rceil})$-Robust CDS Protocols

As in our robust 2-party CDS protocol, we use the above linear CDS protocol $\mathcal{P}_k^{(\mathbf{1}_{\lfloor k/2 \rfloor},\mathbf{N}_{\lceil k/2 \rceil})}$ and a family of hash function to construct the following linear robust k-party CDS protocol $\mathcal{P}_k^{(\mathbf{t}_{\lfloor k/2 \rfloor},\mathbf{N}_{\lceil k/2 \rceil})}$, for an integer $k > 2$. This protocol is efficient for constant k, so we present its message size for such values of k.

Lemma 6.4. *Let $f : [M]^{\lfloor k/2 \rfloor} \times [N]^{\lceil k/2 \rceil} \to \{0,1\}$ be a k-input function, where $M \leq N$, for some constant integer $k > 2$, and $t \leq \sqrt{2M/k}$ be an integer. Then, for every finite field $\mathbb{F}$, there is a linear k-party $(\mathbf{t}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})$-robust CDS protocol for f with one-element secrets, in which for an odd k the message size of the protocol is $O\left(t^k N^{(k-1)/2} \log N \log |\mathbb{F}|\right)$, and for an even k the message size of party P_1 is $O\left(t^{k-1} N^{(k-1)/2} \log N \log |\mathbb{F}|\right)$ and the message size of parties $P_2, \ldots, P_k$ is $O\left(t^{k-1} N^{(k-3)/2} (t^2 \sqrt{N} + M) \log N \log |\mathbb{F}|\right)$.*

Proof. Let $k' = \lfloor k/2 \rfloor$ and $H_{k'M,k't,(k't)^2} = \left\{h_i : [k'] \times [M] \to [(k't)^2] : i \in [\ell]\right\}$, where $\ell = \Theta(k't \log(k'M)) = O(t \log N)$, be the family of hash functions promised by Lemma 2.19 for $\mathcal{T} = \binom{[k'] \times [M]}{\leq k't}$ (that is, $|\mathcal{T}| = \Theta((k'M)^{k't})$).

Protocol $\mathcal{P}_k^{(\mathbf{t}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})}$

The secret: An element $s \in \mathbb{F}$.
The protocol: Let $k' = \lfloor k/2 \rfloor$.

1. Choose ℓ random elements $s_1, \ldots, s_\ell \in \mathbb{F}$ such that $s = s_1 + \cdots + s_\ell$.
2. For every $i \in [\ell]$ do:
   - Let $A_{a,j} = \{x \in [M] : h_i(a,x) = j\}$, for every $a \in [k']$ and every $j \in [(k't)^2]$.
   - For every $j_1, \ldots, j_{k'} \in [(k't)^2]$, independently execute the CDS protocol $\mathcal{P}_k^{(\mathbf{1}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil}), \text{balanced}}$ of Lemma 6.3 for the restriction of f to $A_{1,j_1} \times \cdots \times A_{k',j_{k'}} \times [N]^{k-k'}$ with the secret s_i, and with $d = 1$ if k is odd or $d = \max\left\{1, M/(\sqrt{N}t^2)\right\}$ if k is even. That is, for every $a \in [k']$, party P_a with input x_a sends messages for the restriction of f to $A_{1,j_1} \times \cdots \times A_{a,h_i(a,x_a)} \times \cdots \times A_{k',j_{k'}} \times [N]^{k-k'}$ for every $j_1, \ldots, j_{a-1}, j_{a+1}, \ldots j_{k'} \in [(k't)^2]$, and parties $P_{k'+1}, \ldots, P_k$ with inputs $x_{k'+1}, \ldots, x_k$, respectively, send messages for the restriction of f to $A_{1,j_1} \times \cdots \times A_{k',j_{k'}} \times [N]^{k-k'}$ for every $j_1, \ldots, j_{k'} \in [(k't)^2]$.

Figure 8: A linear k-party $(\mathbf{t}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})$-robust CDS protocol $\mathcal{P}_k^{(\mathbf{t}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})}$ for a function $f : [M]^{\lfloor k/2 \rfloor} \times [N]^{\lceil k/2 \rceil} \to \{0,1\}$.

The desired CDS protocol $\mathcal{P}_k^{(\mathbf{t}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})}$ is described in Figure 8. For a fixed $h_i \in H_{k'M,k't,(k't)^2}$, the message of party P_1 contains $O\left((k't)^{2(k'-1)}(M/(t^2 d))N^{k'-1}\right)$ field elements. This expression equals to $O\left(t^{k-5} M N^{(k-3)/2}\right)$ for an odd k and to $O\left(\min\left\{t^{k-4} M N^{(k-2)/2}, t^{k-2} N^{(k-1)/2}\right\}\right) \leq O\left(t^{k-2} N^{(k-1)/2}\right)$ for an even k. For a fixed $h_i \in H_{k'M,k't,(k't)^2}$, the messages of the parties $P_2, \ldots, P_k$ contain $\left((k't)^{2k'} d N^{k-k'-1}\right)$ field elements. This expression equals to $O\left(t^{k-1} N^{(k-1)/2}\right)$ for an odd k and to $O\left(t^k N^{(k-2)/2} + t^{k-2} M N^{(k-3)/2}\right)$ for an even k. Since there are $\ell = O(t \log N)$ hash functions, the sizes of the messages is as in the lemma.

The correctness and robustness follow from the same arguments as in Lemma 3.3 and the details are omitted. □

As for our 2-party protocols, we improve our linear robust k-party CDS protocol using the family of hash functions of Lemma 2.20.

Theorem 6.5. *Let $f : [N]^k \to \{0,1\}$ be a k-input function, for some constant integer $k > 2$. Then, for every finite field $\mathbb{F}$ and every integer $t \leq N/(k \log^2 N)$, there is a linear k-party $(\mathbf{t}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})$-robust CDS protocol for f with one-element secrets in which the messages size is $\tilde{O}\left(t^{(k+1)/2} N^{(k-1)/2} \log |\mathbb{F}|\right)$ for an odd k and $\tilde{O}\left(t^{k/2} N^{(k-2)/2} (t + \sqrt{N}) \log |\mathbb{F}|\right)$ for an even k.*

Proof. Let $k' = \lfloor k/2 \rfloor$ and $H_{k'N,k't,2k't} = \{h_i : [k'] \times [N] \to [2k't] : i \in [\ell]\}$, where $\ell = \Theta(k't \log(k'N)) = O(t \log N)$, be the family of hash functions promised by Lemma 2.20 for $\mathcal{T} = \binom{[k'] \times [N]}{\leq k't}$ (that is, $|\mathcal{T}| = \Theta((k'N)^{k't})$).

Protocol $\mathcal{P}_{\mathrm{LkRCDS}}$

The secret: An element $s \in \mathbb{F}$.
The protocol: Let $k' = \lfloor k/2 \rfloor$

1. Choose ℓ random elements $s_1, \ldots, s_\ell \in \mathbb{F}$ such that $s = s_1 + \cdots + s_\ell$.
2. For every $i \in [\ell]$ do:
   - Let $A_{a,j} = \{x \in [N] : h_i(a,x) = j\}$, for every $a \in [k]$ and every $j \in [2k't]$.
   - For every $j_1, \ldots, j_{k'} \in [2k't]$, independently execute the linear k-party $(\log \mathbf{t}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})$-robust CDS protocol $\mathcal{P}_k^{(\log \mathbf{t}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})}$ of Lemma 6.4 for the restriction of f to $A_{1,j_1} \times \cdots \times A_{k',j_{k'}} \times [N]^{k-k'}$ with the secret s_i. That is, for every $a \in [k']$, party P_a with input x_a sends messages for the restriction of f to $A_{1,j_1} \times \cdots \times A_{a,h_i(a,x_a)} \times \cdots \times A_{k',j_{k'}} \times [N]^{k-k'}$ for every $j_1, \ldots, j_{a-1}, j_{a+1}, \ldots j_{k'} \in [2k't]$, and parties $P_{k'+1}, \ldots, P_k$ with inputs $x_{k'+1}, \ldots, x_k$, respectively, send messages for the restriction of f to $A_{1,j_1} \times \cdots \times A_{k',j_{k'}} \times [N]^{k-k'}$ for every $j_1, \ldots, j_{k'} \in [2k't]$.

Figure 9: A linear k-party $(\mathbf{t}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})$-robust CDS protocol $\mathcal{P}_{\mathrm{LkRCDS}}$ for a function $f : [N]^k \to \{0,1\}$.

The desired CDS protocol $\mathcal{P}_{\mathrm{LkRCDS}}$ is described in Figure 9. The protocol $\mathcal{P}_{\mathrm{LkRCDS}}$ contains $(2k't)^{k'} \ell = O(t^{\lfloor k/2 \rfloor + 1} \log N)$ executions of the protocol $\mathcal{P}_k^{(\mathbf{t}'_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})}$ of Lemma 6.4 with $t' = \log t$ and $M = N/(2t)$ (since $t \leq N/(k \log^2 N)$, we have that $\log t \leq \sqrt{N/(kt)}$ as required). In the protocol $\mathcal{P}_{\mathrm{LkRCDS}}$, the first party P_1 sends $(2k't)^{k'-1} \ell = O(t^{\lfloor k/2 \rfloor} \log N)$ messages and each of the last $k-1$ parties $P_2, \ldots, P_k$ sends at most $(2k't)^{k'} \ell = O(t^{\lfloor k/2 \rfloor + 1} \log N)$ messages. For an odd k, the number of field elements that each message of the protocol $\mathcal{P}_{\mathrm{LkRCDS}}$ contains is

$$O\left(\log^k t N^{(k-1)/2} \log N \cdot t^{\lfloor k/2 \rfloor + 1} \log N\right) = O\left(t^{(k+1)/2} N^{(k-1)/2} \log^k t \log^2 N\right).$$

For an even k, the number of field elements that each message of the protocol $\mathcal{P}_{\mathrm{LkRCDS}}$ contains is

$$\begin{aligned} O\Big((\log^{k-1} t \cdot N^{(k-1)/2} \cdot t^{\lfloor k/2 \rfloor} + \log^{k-1} t \cdot N^{(k-3)/2} (\log^2 t \cdot \sqrt{N} + N/(2t)) \cdot t^{\lfloor k/2 \rfloor + 1}) \cdot \log^2 N\Big) \\ = O\left(t^{k/2} N^{(k-2)/2} (t \log^2 t + \sqrt{N}) \log^{k-1} t \log^2 N\right) \end{aligned}$$

(where the first summand in the first row corresponds to the message size of party P_1 and the second summand in the first row corresponds to the messages size of parties $P_2, \ldots, P_k$). Overall, the message size of protocol $\mathcal{P}_{\mathrm{LkRCDS}}$ is as in the theorem.

The correctness and robustness follow from the same arguments as in Theorem 3.4; the details are omitted. □

Remark 6.6. As in the 2-party $(\mathcal{T}, N)$-robust CDS protocol of Theorem 3.4, we can construct a linear k-party $(\mathcal{T}_1, \ldots, \mathcal{T}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})$-robust CDS protocol for every $\mathcal{T}_1, \ldots, \mathcal{T}_{\lfloor k/2 \rfloor} \subseteq \binom{[N]}{\leq t}$. This results in a linear k-party $(\mathcal{T}_1, \ldots, \mathcal{T}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})$-robust CDS protocol with one-element secrets in which the message size is $\tilde{O}\left(t^{(k-1)/2} N^{(k-1)/2} \sum_{a=1}^{\lfloor k/2 \rfloor} \log |\mathcal{T}_a| \cdot \log |\mathbb{F}|\right)$ for an odd k and $\tilde{O}\left(t^{(k-2)/2} N^{(k-2)/2} (t + \sqrt{N}) \sum_{a=1}^{\lfloor k/2 \rfloor} \log |\mathcal{T}_a| \cdot \log |\mathbb{F}|\right)$ for an even k.

Additionally, we can also construct a multi-linear protocol with smaller normalized message size. This results in a multi-linear k-party $(\mathcal{T}_1, \ldots, \mathcal{T}_{\lfloor k/2 \rfloor}, \mathbf{N}_{\lceil k/2 \rceil})$-robust CDS protocol with secrets of size $\Theta(\log t \log N \cdot \sum_{a=1}^{\lfloor k/2 \rfloor} \log |\mathcal{T}_a| \cdot \log |\mathbb{F}|)$ in which the normalized message size is $\tilde{O}\left(t^{(k-1)/2} N^{(k-1)/2}\right)$ for an odd k and $\tilde{O}\left(t^{(k-2)/2} N^{(k-2)/2} (t + \sqrt{N})\right)$ for an even k.

For $t = \Theta(N/\log^2 N)$ and $\mathcal{T}_a = \binom{[N]}{\leq t}$ for every $a \in [\lfloor k/2 \rfloor]$, the normalized message size of this multi-linear protocol is $\tilde{O}(N^{k-1})$, which is the best known message size for such protocols in which $t = N$.

Acknowledgement. We thank Yuval Ishai and Eyal Kushilevitz for many discussions on secret-sharing schemes and CDS protocols. In particular, the notion of robust CDS protocols emerged in these discussions. We also thank Vinod Vaikuntanathan and Tianren Liu for useful discussions. Figure 5 is based on a similar figure from [4] drawn by Oded Nir.

References

[1] B. Aiello, Y. Ishai, and O. Reingold. Priced oblivious transfer: How to sell digital goods. In B. Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 118–134. Springer-Verlag, 2001.

[2] B. Applebaum and B. Arkis. On the power of amortization in secret sharing: d-uniform secret sharing and CDS with constant information rate. In A. Beimel and S. Dziembowski, editors, *TCC 2018*, volume 11239 of *LNCS*, pages 317–344. Springer, 2018.

[3] B. Applebaum, B. Arkis, P. Raykov, and P. N. Vasudevan. Conditional disclosure of secrets: Amplification, closure, amortization, lower-bounds, and separations. In J. Katz and H. Shacham, editors, *CRYPTO 2017*, volume 10401 of *LNCS*, pages 727–757. Springer, 2017.

[4] B. Applebaum, A. Beimel, O. Farràs, O. Nir, and N. Peter. Secret-sharing schemes for general and uniform access structures. Cryptology ePrint Archive, Report 2019/231, 2019. `https://eprint.iacr.org/2019/231`. To appear in EUROCRYPT 2019.

[5] B. Applebaum, T. Holenstein, M. Mishra, and O. Shayevitz. The communication complexity of private simultaneous messages, revisited. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018*, LNCS, pages 261–286. Springer-Verlag, 2018.

[6] B. Applebaum and P. N. Vasudevan. Placing conditional disclosure of secrets in the communication complexity universe. In *10th ITCS*, pages 4:1–4:14, 2019.

[7] N. Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 557–577. Springer-Verlag, 2014.

[8] A. Beimel. *Secure Schemes for Secret Sharing and Key Distribution*. PhD thesis, Technion, 1996. `www.cs.bgu.ac.il/~beimel/pub.html`.

[9] A. Beimel and B. Chor. Universally ideal secret-sharing schemes. *IEEE Trans. on Information Theory*, 40(3):786–794, 1994.

[10] A. Beimel, O. Farràs, and Y. Mintz. Secret-sharing schemes for very dense graphs. *J. of Cryptology*, 29(2):336–362, 2016.

[11] A. Beimel, O. Farràs, Y. Mintz, and N. Peter. Linear secret-sharing schemes for forbidden graph access structures. In Y. Kalai and L. Reyzin, editors, *TCC 2017*, volume 10678 of *LNCS*, pages 394–423. Springer-Verlag, 2017.

[12] A. Beimel, O. Farràs, and N. Peter. Secret sharing schemes for dense forbidden graphs. In V. Zikas and R. De Prisco, editors, *SCN 2016*, volume 9841 of *Lecture Notes in Computer Science*, pages 509–528, 2016.

[13] A. Beimel, A. Gabizon, Y. Ishai, E. Kushilevitz, S. Meldgaard, and A. Paskin-Cherniavsky. Non-interactive secure multiparty computation. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014*, volume 8617 of *LNCS*, pages 387–404. Springer-Verlag, 2014.

[14] A. Beimel, A. Gál, and M. Paterson. Lower bounds for monotone span programs. *Computational Complexity*, 6(1):29–45, 1997.

[15] A. Beimel, Y. Ishai, R. Kumaresan, and E. Kushilevitz. On the cryptographic complexity of the worst functions. In Y. Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 317–342. Springer-Verlag, 2014.

[16] A. Beimel, E. Kushilevitz, and P. Nissim. The complexity of multiparty PSM protocols and related models. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018*, volume 10821 of *LNCS*, pages 287–318. Springer-Verlag, 2018.

[17] A. Beimel and N. Peter. Optimal linear multiparty conditional disclosure of secrets protocols. In T. Peyrin and S. D. Galbraith, editors, *ASIACRYPT 2018*, volume 11274 of *LNCS*, pages 332–362. Springer, 2018.

[18] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for noncryptographic fault-tolerant distributed computations. In *20th STOC*, pages 1–10, 1988.

[19] J. C. Benaloh. Secret sharing homomorphisms: Keeping shares of A secret sharing. In A. M. Odlyzko, editor, *CRYPTO '86*, volume 263 of *LNCS*, pages 251–260. Springer-Verlag, 1986.

[20] J. C. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *CRYPTO '88*, volume 403 of *LNCS*, pages 27–35. Springer-Verlag, 1988.

[21] F. Benhamouda, H. Krawczyk, and T. Rabin. Robust non-interactive multiparty computation against constant-size collusion. In J. Katz and H. Shacham, editors, *CRYPTO 2017*, volume 10401 of *LNCS*, pages 391–419. Springer, 2017.

[22] M. Bertilsson and I. Ingemarsson. A construction of practical secret sharing schemes using linear block codes. In J. Seberry and Y. Zheng, editors, *AUSCRYPT '92*, volume 718 of *LNCS*, pages 67–79. Springer-Verlag, 1992.

[23] G. R. Blakley. Safeguarding cryptographic keys. In *Proc. of the 1979 AFIPS National Computer Conference*, volume 48 of *AFIPS Conference proceedings*, pages 313–317. AFIPS Press, 1979.

[24] G. R. Blakley and C. A. Meadows. Security of ramp schemes. In G. R. Blakley and D. Chaum, editors, *CRYPTO '84*, volume 196 of *LNCS*, pages 242–268. Springer-Verlag, 1984.

[25] C. Blundo, A. De Santis, R. de Simone, and U. Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Designs, Codes and Cryptography*, 11(2):107–122, 1997.

[26] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro. Graph decomposition and secret sharing schemes. *J. of Cryptology*, 8(1):39–64, 1995.

[27] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. of Cryptology*, 4(73):123–134, 1991.

[28] S. Bublitz. Decomposition of graphs and monotone formula size of homogeneous functions. *Acta Inf.*, 23(6):689–696, 1986.

[29] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols. In *20th STOC*, pages 11–19, 1988.

[30] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan. Secure computation from random error correcting codes. In M. Naor, editor, *EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 291–310. Springer-Verlag, 2007.

[31] B. Chor, A. Fiat, M. Naor, and B. Pinkas. Tracing traitors. *IEEE Trans. Information Theory*, 46(3):893–910, 2000.

[32] B. Chor and E. Kushilevitz. Secret sharing over infinite domains. *J. of Cryptology*, 6(2):87–96, 1993.

[33] L. Csirmaz. The size of a share must be large. In A. De Santis, editor, *AEUROCRYPT '94*, volume 950 of *LNCS*, pages 13–22. Springer-Verlag, 1994.

[34] L. Csirmaz. The dealer's random bits in perfect secret sharing schemes. *Studia Sci. Math. Hungar.*, 32(3–4):429–437, 1996.

[35] L. Csirmaz. Secret sharing schemes on graphs. Technical Report 2005/059, Cryptology ePrint Archive, 2005. `eprint.iacr.org/`.

[36] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures (extended abstract). In J. Feigenbaum, editor, *CRYPTO '91*, volume 576 of *LNCS*, pages 457–469. Springer-Verlag, 1991.

[37] Z. Dvir and S. Gopi. 2-server PIR with sub-polynomial communication. In *47th STOC*, pages 577–584, 2015.

[38] P. Erdös and L. Pyber. Covering a graph by complete bipartite graphs. *Discrete Mathematics*, 170(1–3):249–251, 1997.

[39] U. Feige, J. Kilian, and M. Naor. A minimal model for secure computation. In *26th STOC*, pages 554–563, 1994.

[40] M. L. Fredman, J. Komlós, and E. Szemerédi. Storing a sparse table with 0(1) worst case access time. *J. ACM*, 31(3):538–544, 1984.

[41] R. Gay, I. Kerenidis, and H. Wee. Communication complexity of conditional disclosure of secrets and attribute-based encryption. In R. Gennaro and M. Robshaw, editors, *CRYPTO 2015*, volume 9216 of *LNCS*, pages 485–502. Springer-Verlag, 2015.

[42] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin. Protecting data privacy in private information retrieval schemes. *J. of Computer and System Sciences*, 60(3):592–629, 2000.

[43] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *13th CCS*, pages 89–98, 2006.

[44] Y. Ishai and E. Kushilevitz. Private simultaneous messages protocols with applications. In *5th Israel Symp. on Theory of Computing and Systems*, pages 174–183, 1997.

[45] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In *Globecom 87*, pages 99–102, 1987. Journal version: Multiple assignment scheme for sharing secret. J. of Cryptology 6(1), 15-20, (1993).

[46] M. Karchmer and A. Wigderson. On span programs. In *8th Structure in Complexity Theory*, pages 102–111, 1993.

[47] T. Liu and V. Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. In *50th STOC*, pages 699–708, 2018.

[48] T. Liu, V. Vaikuntanathan, and H. Wee. Conditional disclosure of secrets via non-linear reconstruction. In J. Katz and H. Shacham, editors, *CRYPTO 2017*, volume 10401 of *LNCS*, pages 758–790. Springer-Verlag, 2017.

[49] T. Liu, V. Vaikuntanathan, and H. Wee. Towards breaking the exponential barrier for general secret sharing. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018*, volume 10820 of *LNCS*, pages 567–596. Springer-Verlag, 2018.

[50] M. Mitzenmacher and E. Upfal. *Probability and Computing*. Cambridge University Press, 2005.

[51] M. Naor and A. Wool. Access control and signatures via quorum secret sharing. In *3rd CCS*, pages 157–167, 1996.

[52] T. Pitassi and R. Robere. Strongly exponential lower bounds for monotone computation. In *49th STOC*, pages 1246–1255, 2017.

[53] T. Pitassi and R. Robere. Lifting nullstellensatz to monotone span programs over any field. In *50th STOC*, pages 1207–1219, 2018.

[54] R. Robere, T. Pitassi, B. Rossman, and S. A. Cook. Exponential lower bounds for monotone span programs. In *57th FOCS*, pages 406–415, 2016.

[55] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

[56] B. Shankar, K. Srinathan, and C. Pandu Rangan. Alternative protocols for generalized oblivious transfer. In S. Rao, M. Chatterjee, P. Jayanti, C. S. Ram Murthy, and S. K. Saha, editors, *9th ICDCN*, volume 4904 of *Lecture Notes in Computer Science*, pages 304–309. Springer-Verlag, 2008.

[57] D. R. Stinson. Decomposition construction for secret sharing schemes. *IEEE Trans. on Information Theory*, 40(1):118–125, 1994.

[58] T. Tassa. Generalized oblivious transfer by secret sharing. *Designs, Codes and Cryptography*, 58(1):11–21, 2011.

[59] M. van Dijk, W.-A. Jackson, and K. M. Martin. A general decomposition construction for incomplete secret sharing schemes. *Des. Codes Cryptography*, 15(3):301–321, 1998.

[60] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 53–70. Springer-Verlag, 2011.

[61] H. Wee. Dual system encryption via predicate encodings. In Y. Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 616–637. Springer-Verlag, 2014.