On Round-Optimal Computational VSS

Karim Baghery[1], Navid Ghaedi Bardeh[2], Shahram Khazaei[3] and Mahdi Rahimi[1]

[1] COSIC, KU Leuven, Leuven, Belgium
[2] University of Klagenfurt, Klagenfurt, Austria
[3] Sharif University of Technology, Tehran, Iran

Abstract. In ASIACRYPT 2011, Backes, Kate, and Patra (BKP) introduced two computationally secure round-optimal (2-round) Verifiable Secret Sharing (VSS) schemes in the honest-majority setting, one based on non-homomorphic commitments and the other on homomorphic ones. Their scheme based on non-homomorphic commitments has $O(n^2)$ computational complexity and necessitates $O(n^2\lambda)$ public and private communication for the dealer, where n denotes the number of parties and λ is the security parameter. They showed that these costs are n times higher compared to their round-optimal VSS scheme employing homomorphic commitments and posed a research question regarding the inevitability of this gap. In this paper, we fill this gap by introducing a new variant of the recently proposed unified framework $\mathbf{\Pi}$ by Baghery at PKC 2025, designed to enable the construction of more efficient round-optimal VSS schemes in the honest-majority setting. Compared to the original framework, our variant reduces the required rounds by one while maintaining compatibility with any commitments and achieving comparable efficiency. Leveraging this new general construction, we develop several round-optimal VSS schemes that surpass state-of-the-art alternatives. Particularly noteworthy is the new round-optimal VSS scheme based on non-homomorphic commitments, which improves the BKP scheme by a factor of n across all efficiency metrics. Compared to their schemes based on homomorphic commitments, our schemes demonstrate significantly expedited verification and reconstruction. Implementation results further validate the practicality of these new VSS schemes. For example, for $(n, t) = (256, 127)$, where t represents the threshold, compared to the hash-based BKP VSS scheme, our proposed scheme showcases speed-ups exceeding $120,000\times$ (and $50\times$) for the dealer (and parties, respectively), while also requiring $365\times$ (and $512\times$) less communication.

Keywords: Verifiable Secret Sharing · Round-Optimal Verifiable Secret Sharing · Shamir Secret Sharing · $\mathbf{\Pi}$ framework

1 Introduction

Threshold cryptography has gained considerable traction in recent years, particularly due to its application in safeguarding cryptocurrency wallets, enabling secure access control mechanisms, and facilitating distributed protocol design. At its core, threshold cryptography ensures that cryptographic operations can be performed only when a specified threshold of participants collaborates, thereby thwarting the efforts of malicious entities attempting to compromise the system.

E-mail: karim.baghery@kuleuven.be (Karim Baghery), navid.ghaedibardeh@gmail.com (Navid Ghaedi Bardeh), shahram.khazaei@sharif.ir (Shahram Khazaei), mahdi.rahimi@kuleuven.be (Mahdi Rahimi)

Central to the functionality of threshold cryptography are secret sharing schemes, which enable the secure distribution of sensitive information among multiple parties. While traditional secret-sharing schemes like Shamir's protocol [Sha79] lay the groundwork, the need for enhanced security against malicious actors has led to the development of Verifiable Secret Sharing (VSS) schemes [CGMA85, Fel87, BGW88, Ped92, GRR98, BKP11, ABCP23, SS24, CCG24, Bag25]. These VSS schemes not only ensure correct share distribution but also provide mechanisms for parties to verify the validity of their shares, improving the overall security posture of the system. Verifiability in secret sharing schemes often necessitates interaction between the dealer and shareholders, depending on the communication model employed.

Our studied VSS schemes are constructed in the synchronous and honest-majority settings. In this setting, in the context of the Discrete Logarithm (DL), research has demonstrated the feasibility of constructing one-round VSS schemes using Public Key Infrastructure (PKI). These schemes, commonly referred to as Publicly Verifiable Secret Sharing (PVSS) [Sch99, CD17, Gro21, GHL22, Bag25] or Pre-Constructed PVSS (PPVSS) schemes [Sch99, BKNR25], leverage pre-registered public keys of parties to enable efficient and verifiable secret sharing operations. PVSS and PPVSS schemes have found widespread applications across domains such as e-voting, random beacon generation, and numerous others [Sch99, CD17, CD20, BKNR25]. Well-established and practical computational VSS schemes in the synchronous setting, such as those proposed by Pedersen [Ped92], Feldman [Fel87], Atapoor, Baghery, Cozzo, and Pedersen [ABCP23], and Baghery [Bag25], typically operate under the assumption of a secure communication channel between the dealer and shareholders, as well as access to a broadcast channel for both the dealer and parties. In scenarios where conflicts arise between parties, these protocols may necessitate three rounds of communication between the dealer and parties. However, it is important to note that under optimal conditions, such as when there are no complaints from shareholders, these protocols can often be executed with just a single round of communication. In practice, due to using lightweight operations, such as polynomial evaluation and hashing, hash-based VSS schemes, such as those proposed by Atapoor, Baghery, Cozzo, and Pedersen [ABCP23], Cascudo, Cozzo, and Giunta [CCG24], and Baghery [Bag25], are considerably more efficient.

In the synchronous communication model featuring a broadcast channel, Backes, Kate, and Patra (BKP) [BKP11] studied the round complexity of computational VSS schemes employing both homomorphic and non-homomorphic commitments. As a key negative result, they showed the impossibility of constructing 1-round computational VSS protocol in the standard communication model, i.e., without relying on PKI. They then tighten the lower-bound result by presenting a 2-round computational VSS scheme using any (non-homomorphic) commitments in the honest-majority setting, i.e., $n \geq 2t + 1$, where n represents the number of parties and t denotes the threshold parameter, which defines the maximum number of malicious parties that the scheme can tolerate while still ensuring the integrity of the secret-sharing process.. Their construction, based on non-homomorphic commitments, leveraged bivariate polynomials [BGW88] to ensure verifiability but imposes $O(n^2)$ computational complexity in the sharing phase and necessitates $O(n^2\lambda)$ bits of broadcast, $O(n^2\lambda)$ bits of private communication in the sharing phase, as well as $O(n^2\lambda)$ broadcasts in the reconstruction phase. Additionally, BKP [BKP11] presented a 2-round computational VSS scheme using homomorphic commitments, which demonstrated comparable computation and communication complexities to 3-round schemes proposed by Pedersen [Ped92] (or Feldman [Fel87]), albeit requiring one fewer round of communication. In a similar setting, namely synchronous communication with an honest majority, lately, Atapoor, Baghery, Cozzo, and Pedersen [ABCP23] introduced the first practical hash-based 3-round VSS scheme within the Quantum Random Oracle Model (QROM). More recently, Baghery [Bag25] proposed a unified framework, dubbed $\mathbf{\Pi}$, enabling the construction

of 3-round Shamir-based computational VSS schemes utilizing both homomorphic and non-homomorphic commitment schemes. Notably, instantiation of **Π** with different commitment schemes has yielded various practical 3-round VSS schemes [Bag25], that in general outperform earlier constructions proposed in [Fel87, Ped92, ABCP23].

1.1 Our Contributions

We summarize the contributions of paper as follows:

Round-Optimal Variant of Unified Framework Π. As the main contribution of this paper, we introduce **2R-Π**, a new variant of the unified framework **Π** [Bag25]. Distinguishing itself from the original construction, **2R-Π** is round-optimal and reduces the required number of rounds by one while maintaining compatibility with any commitment scheme and achieving comparable efficiency. To achieve this reduction in round complexity, we employ a novel modification based on commitments and a one-time pad encryption scheme, inspired by techniques used in earlier unconditionally secure [GIKR01] and computationally secure (albeit less efficient) [BKP11] VSS schemes. More specifically, unlike the original construction, **2R-Π** eliminates the need for interaction in the *unhappy* path. Instead, shareholders privately send a secret key s_i (for one-time pad encryption) to the dealer while also publishing a public commitment C_i to their secret key s_i. In the second round, the dealer broadcasts the encryption of each party's share using the corresponding secret key s_i hidden within commitment C_i. This approach allows parties to resolve conflicts within the same round, avoiding additional interactions. In case of a complaint, the complaining party can open their commitment C_i by revealing the secret key s_i. Other parties can then verify its validity and use it to decrypt the ciphertext published by the dealer, enabling them to identify the malicious party, disqualify them, and determine the final qualified set –or abort the protocol if necessary. In contrast, the constructions proposed in [Bag25] and other three-round VSS schemes, such as [Fel87, Ped92, ABCP23, CCG24], require two additional rounds to resolve conflicts. Specifically, in the second round, parties submit complaints, and in the third round, the dealer responds. Then the parties locally decide who is malicious, disqualify them, and determine the final qualified set or abort the protocol.

In terms of efficiency, our approach introduces only minimal (i.e., constant) overhead in both communication and computational costs for the parties. For example, in the hash-based three-round VSS scheme of [Bag25], in the optimistic case, each party computes two hashes and performs one polynomial evaluation. In our scheme, this increases to three hashes and one polynomial evaluation. In the pessimistic case, these costs rise to $2t$ hashes and t polynomial evaluations in [Bag25], compared to $3t$ hashes and t polynomial evaluations in our scheme. For the dealer, the computational cost in [Bag25] consists of n hash computations and $2n$ polynomial evaluations. In our hash-based round-optimal VSS scheme, this increases to $2n$ hash computations and $2n$ polynomial evaluations.

More Efficient Round-Optimal Computational VSS Schemes. Leveraging the resulting general construction **2R-Π** and employing various commitment schemes, we have developed several round-optimal VSS schemes that outperform the state-of-the-art alternatives proposed by BKP [BKP11]. Our approach builds upon the same instantiations used in the original 3-round **Π** framework [Bag25], wherein commitment scheme is instantiated using DL-based [Ped92] and hash-based commitments. Consequently, we obtain round-optimal variant of each 3-round VSS scheme proposed in [Bag25, Sec. 4], originally built using the original **Π** framework.

In assessing the efficiency of the newly introduced round-optimal VSS schemes, it is noteworthy that the VSS scheme based on non-homomorphic (e.g., hash-based) commitments outperforms the alternative construction presented by BKP [BKP11, Sec. 3.2] by a factor of n in terms of computational cost, as well as broadcast and private communications

during the sharing and reconstruction phases. Notably, to the best of our knowledge, this represents the first practical, hash-based (plausibly post-quantum secure), round-optimal, and computational VSS scheme based on Shamir secret sharing. Regarding the new round-optimal VSS schemes based on homomorphic commitments, our schemes require $O(1)$ (and $O(t)$, respectively) exponentiations in the verification (and reconstruction) process, as opposed to $O(t)$ (and $O(t^2)$) in the alternative constructions proposed in [BKP11, Sec. 3.5]. However, this improvement comes with a trade-off, as the sharing phase experiences a constant-time (i.e., $< 3\times$) slowdown and increased communication.

Table 1 presents a comprehensive summary of key features and performance metrics for our proposed round-optimal VSS schemes, comparing them with state-of-the-art schemes from the literature [BKP11].

Table 1: A comparison of new 2-round VSS schemes with those of Backes, Kate, and Patra [BKP11]. DL: Discrete Logarithm, IT-S: Information Theoretical Secrecy, RO: Random Oracle, Plain: Plain Model, BC: Broadcast, PV: Private, Recons.: Reconstruction, n: Number of parties, t: threshold parameter ($t \approx n/2$), $E_{\mathbb{G}}$: Exponentiation in group $\mathbb{G}$, $M_{\mathbb{G}}$: Multiplication in group $\mathbb{G}$, $\mathcal{PE}$: degree-t Polynomial Evaluation, $\mathcal{BPE}$: degree-t (Symmetric) Bivariate Polynomial Evaluation, $\mathcal{H}$: Hashing, $|\mathbb{G}|$: $\mathbb{G}$ element size, $|\mathbb{Z}_q|$: $\mathbb{Z}_q$ element size, $|\mathcal{H}|$: Output size of $\mathcal{H}$, R1 & R2: Rounds 1 and 2.

VSS Scheme, Security	Computation Cost		Communication Cost		Recons. (with $t+1$ parties)
	Dealer (R1 & R2)	Party P_i (R1 & R2)	Dealer	Party P_i	
Section 4.3 RO, DL	$2n\ \mathcal{PE} + 1\mathcal{H} + 3n\ E_{\mathbb{G}}$	$1\ \mathcal{PE} + 1\mathcal{H} + 3\ E_{\mathbb{G}}$	Private: $n\|\mathbb{Z}_q\|$ BC: $1.5n\|\mathbb{Z}_q\| + n\|\mathbb{G}\|$	PV: $1\ \|\mathbb{Z}_q\|$ BC: $1\ \|\mathbb{G}\|$	$O(t)\mathcal{PE} + O(t)\mathcal{H} + O(t)\ E_{\mathbb{G}}$
[BKP11, Sec. 3.5] Plain, DL, IT-S	$\approx 2n\ \mathcal{PE} + 5n\ E_{\mathbb{G}}$	$\approx 0.5n\ M_{\mathbb{G}} + 0.5n\ E_{\mathbb{G}}$	Private: $2n\ \|\mathbb{Z}_q\|$ BC: $2n\|\mathbb{Z}_q\| + 0.5n\|\mathbb{G}\|$	PV: $4\ \|\mathbb{Z}_q\|$ BC: $2\ \|\mathbb{G}\|$	$O(t^2)\ M_{\mathbb{G}} + O(t^2)\ E_{\mathbb{G}}$
Section 4.1 RO, DL, IT-S	$2n\ \mathcal{PE} + 1\mathcal{H} + 7n\ E_{\mathbb{G}}$	$1\ \mathcal{PE} + 1\ \mathcal{H} + 7\ E_{\mathbb{G}}$	Private: $2n\ \|\mathbb{Z}_q\|$ BC: $2.5n\|\mathbb{Z}_q\| + n\|\mathbb{G}\|$	PV: $4\ \|\mathbb{Z}_q\|$ BC: $2\ \|\mathbb{G}\|$	$O(t)\mathcal{PE} + O(t)\mathcal{H} + O(t)\ E_{\mathbb{G}}$
[BKP11, Sec. 3.2] Plain*, Hash	$\approx n^2\ \mathcal{BPE} + 3n^2\ \mathcal{H}$	$3n\ \mathcal{H} + n\ \mathcal{PE}$	Private: $2n^2\ \|\mathbb{Z}_q\|$ BC: $2n^2\|\mathbb{Z}_q\| + n^2\|\mathcal{H}\|$	PV: $4n\ \|\mathbb{Z}_q\|$ BC: $2n\ \|\mathcal{H}\|$	$O(t^2)\ \mathcal{PE} + O(t^2)\ \mathcal{H}$
Section 4.2 RO, Hash	$2n\ \mathcal{PE} + 2n\ \mathcal{H}$	$3\ \mathcal{H} + 1\ \mathcal{PE}$	Private: $n\ \|\mathbb{Z}_q\|$ BC: $1.5n\|\mathbb{Z}_q\| + n\|\mathcal{H}\|$	PV: $2\ \|\mathbb{Z}_q\|$ BC: $1\ \|\mathcal{H}\|$	$O(t)\ \mathcal{PE} + O(t)\ \mathcal{H}$

* Note that achieving the hiding property in a hash-based commitment scheme $\mathcal{H}$ inherently assumes that the underlying hash function behaves as a random oracle.

As shown in the table, our round-optimal VSS schemes are built in the random oracle model. Notably, achieving the hiding property in a hash-based commitment inherently assumes that the underlying hash function behaves as a random oracle. Consequently, both our hash-based round-optimal VSS schemes from Sec. 4.2 and those from [BKP11] rely on a random oracle, yet our construction is asymptotically more efficient across all metrics. On the other hand, our proposed VSS schemes from Sec. 4.3 and 4.1 also require a random oracle, whereas the Pedersen-based alternative from [BKP11] operates in the plain model. While the latter may seem preferable in terms of assumptions when considered in isolation, our proposed schemes offer better efficiency overall. Moreover, VSS schemes are typically used as building blocks for larger cryptographic protocols, such as threshold signatures and distributed key generation protocols. In many cases, these protocols already require a random oracle due to the need for a proof of knowledge. As a result, the use of a random oracle is often a necessity in the final threshold protocol, rather than an additional requirement introduced by the VSS scheme itself.

Benchmarking New VSS Schemes. To evaluate the empirical performance of the new round-optimal VSS schemes, we implemented a prototype using SageMath. Additionally, we implemented the alternative constructions proposed by BKP [BKP11, Sections 3.2 and 3.5] and compared their efficiency, as detailed in Sec. 5. Our implementation results underscore the impracticality of the 2-round VSS scheme proposed by BKP for large-scale applications, as its efficiency metrics scale quadratically with the number of parties. Conversely, our proposed hash-based 2-round VSS scheme exhibits remarkable efficiency, making it suitable even for large-scale deployments. Employing the new hash-based 2-round VSS scheme allows a dealer to share a secret with $n = 256$ parties in approximately 60 milliseconds, with each shareholder needing around 0.7 milliseconds to commit and validate their received shares. In terms of communication, during the sharing phase for the same number of parties, the dealer broadcasts messages of approximately 20 KB and privately sends less than 8 KB to each shareholder. Conversely, each party broadcasts 32 bytes messages and privately sends 32 bytes to the dealer. The efficiency gains of the new hash-based 2-round VSS scheme are significant in the sharing phase, achieving speedups of approximately 385× and 121000× compared to the hash-based BKP scheme [BKP11, Sec. 3.2] for (n, t) values of $(64, 31)$ and $(256, 127)$, respectively. Correspondingly, for the same parameter sets, the dealer (and each party) in our new hash-based VSS scheme requires respectively 91× (and 128×, respectively) and 182× (and 512×) less communication compared to the alternative scheme proposed by BKP [BKP11, Sec. 3.2]. Regarding the empirical performance of the round-optimal VSS scheme discussed in Sec. 4.1 and BKP [BKP11, Sec. 3.5], that both satisfy Information Theoretical (IT) secrecy, the implementation results demonstrate that our proposed scheme can achieve verification times more than 75× faster than the BKP scheme, for parameter pairs $(n, t) = (2048, 1023)$. However, this improvement comes with a trade-off: the sharing phase is slower by a constant factor of less than 2×, and the dealer's broadcast communication increases by less than 1.5×.

1.2 Outline

In Sec. 2, we provide an overview of some preliminary concepts. In Sec. 3, we present **2R-Π** as the round-reduced version of unified framework **Π**. In Sec. 4, we use the **2R-Π** and present several 2-round VSS schemes. In Sec. 5, we assess the empirical performance of new round-optimal VSS schemes and compare them with the state-of-the-art constructions. Finally, in Sec. 6, we conclude the paper.

2 Preliminaries

We let λ denote a security parameter. A function is called *negligible in* X, written $\mathsf{negl}(X)$, if for any constant c, there exists some X_0, such that $f(X) < X^{-c}$ for $X > X_0$. A function that is negligible in the security parameter λ is simply called negligible. We use the assignment operator $\leftarrow$ to denote uniform sampling from a set Ξ, e.g. $x \leftarrow \Xi$.

Throughout this paper p and q denote two large primes such that q divides $p-1$, $\mathbb{G}$ is the unique subgroup of $\mathbb{Z}_p^\star$ of order q, and g is a generator of cyclic group $\mathbb{G}$ of prime order q. One can test if an element $a \in \mathbb{Z}_p^\star$ is in $\mathbb{G}$, by checking if $a^q = 1$. The group $\mathbb{G}$ is chosen such that computing Discrete Logarithms (DL) of $h \in \mathbb{G}$, i.e., $\log_g h$, is hard in this group. When we refer to groups we assume they have known prime order and efficient algorithms to compute group operations. It will be assumed that all parties know p, q and g. We write $\mathbb{Z}_q[X]_t$ for polynomials of degree$t$ in the variable X and with coefficients in the finite field $\mathbb{Z}_q$. For $n \in \mathbb{N}$, we write $[n] = \{1, \ldots, n\}$. Finally all logarithms are in base 2.

2.1 Zero-Knowledge Proofs on Secret Shared Data

The unified framework $\mathbf{\Pi}$ can be considered as an optimized and generalized version of Atapoor, Baghery, Cozzo and Pedersen's construction [ABCP23], both of which employ threshold Zero Knowledge (ZK) proofs on secret shared data [BBC+19]. Next, we recall recall the definition of Non-Interactive Threshold ZK (NI-TZK) proofs [BBC+19, ABCP23], which are also utilized in our proposed round-reduced variant of $\mathbf{\Pi}$.

In a Threshold ZK proof a single prover interacts with several verifiers $\{V_i\}_{i=1}^n$ over a network that includes secure point-to-point channels, and each verifier V_j holds a share $x^{(j)} \in \mathbb{F}^{l_j}$ of the main statement x. The single prover aims to convince multiple verifiers that the main input x is in some language $L \subseteq \mathbb{F}^l$. Next, we recall the formal definition for distributed inputs (or statements), languages, relations, and threshold ZK proofs that are given by Boneh et al. [BBC+19].

Definition 1 (Distributed Inputs, Languages, and Relations [BBC+19])**.** Let n be a number of parties, $\mathbb{F}$ be a finite field, and $l, l_1, l_2, \cdots, l_n \in \mathbb{N}$ be length parameters, where $l = l_1 + l_2 + \cdots + l_n$. An n-distributed input over $\mathbb{F}$ (or just distributed input/statement) is a vector $x = x^{(1)} \parallel x^{(2)} \parallel \cdots \parallel x^{(n)} \in \mathbb{F}^l$ where $x^{(i)} \in \mathbb{F}^{l_i}$, and it refers to a piece (or share) of x. An n-distributed language L is a set of n-distributed inputs. A distributed NP relation with witness length h is a binary relation $R(x, w)$ where x is an n-distributed input and $w \in \mathbb{F}^h$. We assume that all x in L and $(x, w) \in R$ share the same length parameters. Finally, we let $L_R = \{x : \exists w (x, w) \in R\}$.

Definition 2 (n-Verifier Interactive Proofs [BBC+19])**.** An *n-Verifier Interactive Proof* scheme over $\mathbb{F}$ is an interactive protocol $\Gamma = (P, V_1, V_2, \cdots, V_n)$ involving a prover P and n verifiers $\{V_i\}_{i=1}^n$. The protocol proceeds as follows.

- The prover P holds an n-distributed input $x = x^{(1)} \parallel x^{(2)} \parallel \cdots \parallel x^{(n)} \in \mathbb{F}^l$, a witness $w \in \mathbb{F}^h$, and each verifier V_j holds an input share $x^{(j)}$.
- Parties can communicate in synchronous rounds over secure point-to-point channels. While honest parties follow the protocol, malicious parties (i.e., adversary) can send arbitrary messages.
- At the end, each verifier outputs either 1 (accept) or 0 (reject) based on its view, where the view of V_j consists of its input piece $x^{(j)}$, random input $r^{(j)}$, and messages it received during the execution of Γ.

$\Gamma(x, w)$ denotes running Γ on secret shared input x and witness w, and says that $\Gamma(x, w)$ accepts (respectively, rejects) if at the end all verifiers output 1 (resp., 0). $View_{\Gamma,T}(x, w)$ denotes the (joint distribution of) views of verifiers $\{V_j\}_{j \in T}$ in the execution of Γ on the distributed statement x and witness w. Let $R(x, w)$ be a k-distributed relation over finite field $\mathbb{F}$. We say that an n-verifier interactive proof scheme $\Gamma = (P, V_1, \cdots, V_n)$ is a distributed threshold ZK proof protocol for R with t-security against malicious prover *and* malicious verifiers, and with soundness error ϵ, if Γ satisfies the following properties [BBC+19, ABCP23]:

Definition 3 (Completeness)**.** For every n-distributed input $x = x^{(1)} \parallel x^{(2)} \parallel \cdots \parallel x^{(n)} \in \mathbb{F}^l$, and witness $w \in \mathbb{F}^h$, such that $(x, w) \in R$, the execution of $\Gamma(x^{(1)} \parallel x^{(2)} \parallel \cdots \parallel x^{(n)}, w)$ accepts with probability 1.

Definition 4 (Soundness Against Prover and t Verifiers.)**.** For every $T \subseteq [n]$ of size $|T| \leq t$, an $\mathcal{A}$ controlling the prover P and verifiers $\{V_j\}_{j \in T}$, n-distributed input $x = x^{(1)} \parallel x^{(2)} \parallel \cdots \parallel x^{(n)} \in \mathbb{F}^l$, and witness $w \in \mathbb{F}^h$ the following holds. If there is no n-distributed input $x' \in L_R$ such that $x'_H = x_H$, where $H = [n]/T$, the execution of $\Gamma^\star(x, w)$ rejects except with at most ϵ probability, where here $\Gamma^\star$ denotes the interaction of $\mathcal{A}$ with the honest verifiers.

Definition 5 (Threshold ZK)**.** For every $T \subseteq [n]$ of size $|T| \leq t$ and an $\mathcal{A}$ controlling $\{V_j\}_{j\in T}$, there exists a simulator $\mathcal{S}$ such that for every n-distributed input $x = x^{(1)} \parallel x^{(2)} \parallel \cdots \parallel x^{(n)} \in \mathbb{F}^l$, and witness $w \in \mathbb{F}^h$ such that $(x, w) \in R$, we have $\mathcal{S}((x^{(j)})_{j\in T}) \equiv View_{\Gamma^\star,T}(x, w)$. Here, $\Gamma^\star$ denotes the interaction of adversary $\mathcal{A}$ with the honest prover P and the honest verifiers $\{V_j\}_{j\in T}$.

Remark 1 (Threshold Honest-Verifier ZK). In the context of Threshold ZK, one may consider a relaxed definition, Threshold *Honest-Verifier* ZK, that retains the same properties as the original definition, with the added requirement that the subset of verifiers, $\{V_j\}_{j\in T}$, is stipulated to follow the protocol honestly.

2.2 Commitment Schemes

In this section, we recall the definition of commitment schemes, which are used in both the general construction $\mathbf{\Pi}$ and our proposed variant.

Definition 6 (Commitment Scheme)**.** A commitment scheme consists of three polynomial-time algorithms $(\mathsf{KGen}, \mathcal{C}, \mathsf{Open})$, each taking an implicit input 1^λ, where λ is the security parameter. These algorithms are defined as follows:

- $\mathsf{KGen}(1^\lambda) \to pp$: A probabilistic polynomial-time algorithm that, given the security parameter 1^λ, outputs the public parameters pp and defines the message space.

- $\mathcal{C}(pp, m, r) \to c$: A probabilistic polynomial-time algorithm that, given the public parameters pp, a message m in the message space, and a random string $r \in \{0,1\}^\lambda$, outputs a commitment c to m.

- $\mathsf{Open}(pp, m, r, c) \to \{0, 1\}$: A deterministic polynomial-time algorithm that, given the public parameters pp, a message m, randomness r, and a commitment c, outputs 1 if (m, r) is a valid opening of c, and 0 otherwise.

A secure commitment scheme must satisfy two essential properties: *hiding* and *binding*. Informally, the hiding property ensures that the commitment c does not reveal any information about m, while the binding property guarantees that it is infeasible to open c to two distinct messages.

Definition 7 (Hiding)**.** A commitment scheme $\mathcal{C}$ satisfies the hiding property if, for a security parameter λ and any polynomial-time adversary $\mathcal{A}$, it holds that:

$$\left|\Pr\begin{bmatrix} pp \leftarrow \mathsf{KGen}(1^\lambda), (m_0, m_1) \leftarrow \mathcal{A}(pp), b \leftarrow\!\$\ \{0,1\}, \\ r \leftarrow\!\$\ \{0,1\}^\lambda, c \leftarrow \mathcal{C}(pp, m_b, r), b' \leftarrow \mathcal{A}(c) : b = b' \end{bmatrix} - \frac{1}{2}\right| = \mathsf{negl}(\lambda).$$

Definition 8 (Binding)**.** A commitment scheme $\mathcal{C}$ satisfies the binding property if, for a security parameter λ and any polynomial-time adversary $\mathcal{A}$, it holds that:

$$\Pr\begin{bmatrix} pp \leftarrow \mathsf{KGen}(1^\lambda), (m_0, r_0, m_1, r_1, c) \leftarrow \mathcal{A}(pp) : \\ m_0 \neq m_1 \wedge \mathsf{Open}(pp, m_0, r_0, c) = \mathsf{Open}(pp, m_1, r_1, c) = 1 \end{bmatrix} = \mathsf{negl}(\lambda).$$

2.3 Verifiable Secret Sharing

Our studied protocols utilize Shamir secret sharing [Sha79] for securely sharing a secret, a concept we review below.

2.3.1 Shamir Secret Sharing

A $(t+1, n)$-Shamir secret sharing scheme [Sha79] allows n parties to individually hold a share f_i of a common secret f_0, such that any subset of t parties or less is not able to learn any information about the secret f_0, while any subset of at least $t+1$ parties are able to efficiently reconstruct the common secret f_0. In more detail, this is achieved via polynomial interpolation over the field $\mathbb{Z}_q$. A common polynomial $f(X) \in \mathbb{Z}_q[X]_t$ is chosen, such that the secret f_0 is set to be its constant term, namely $f_0 = f(0)$. Each party P_i for $i \in \{1, \cdots, n\}$ is assigned the secret share $f_i = f(i)$. Then any subset $Q \subseteq \{1, \ldots, n\}$ of at least t parties can reconstruct the secret f_0 via Lagrange interpolation by computing $f_0 = f(0) = \sum_{i \in Q} f_i \cdot L_{0,i}^Q$, where

$$L_{0,i}^Q := \prod_{j \in Q \setminus \{i\}} \frac{j}{j-i} \pmod q.$$

are the Lagrange basis polynomials evaluated at 0. Any unqualified set of parties are not able to find $f_0 = f(0)$, as this is information theoretically hidden from the other shares.

2.3.2 Round-Optimal Verifiable Secret Sharing

A typical secret sharing scheme is designed to withstand passive attacks. However, in numerous scenarios, it's imperative for a secret sharing scheme to also be resilient against malicious actors or parties employing active attacks. This enhanced security is achieved through VSS schemes, first introduced in 1985 [CGMA85].

Next, we summarize our definition of round-optimal VSS schemes, which can be viewed as a formalized version of those presented in [GIKR01, BKP11]. Following the foundational work of [GIKR01], and to enable a fair comparison with the state-of-the-art round-optimal VSS scheme [BKP11], we adopt a property-based analysis in our paper.

Definition 9. An (n, t)-VSS scheme consists of two polynomial time algorithms (Sharing, Reconstruction), defined as follows:

1. Sharing: A stateful dealer D (also denoted as Sharing.D) holds an input f_0, referred to as the secret, and each party $P_i \in \mathcal{P}$ (also denoted as Sharing.P$_i$) holds independent random inputs (s_i, t_i), and publishes a public commitment c_i to them. The sharing phase may consist of several rounds of interaction between the dealer Sharing.D and each party Sharing.P$_i$ for $i \in [n]$. In each round, parties may privately send messages to each other and may also broadcast messages. In particular, the dealer broadcasts the threshold proof π_{share} and $\{\alpha_i\}_{i \in [n]}$, representing the encryptions of the individual shares. Each message sent or broadcast by P_i (or Sharing.P$_i$) is determined by its input, its random coins, and the messages received from other parties in previous rounds. At the end of this stage, the parties either abort the sharing phase or return Happy and each receives a valid share of the secret f_0.

2. Reconstruction: Let $V \subseteq [n]$ be a qualified set of parties, and let π_{share} be the proof generated by the dealer during the sharing phase. To reconstruct the secret, each party P_i for $i \in V$ provides its share f_i from the sharing phase. The shares are then verified using π_{share}, and if at least $t+1$ valid shares are obtained, they are used to reconstruct the secret f_0. If fewer than $t+1$ valid shares are collected, the protocol returns $\perp$.

A t-adversary may choose any set of t parties to be corrupted during the entire execution of the protocol (including both phases). For simplicity, a two-phase, n-parties protocol as above is called a (perfect) (n, t)-VSS protocol if, for any t-adversary, the following requirements hold:

- Correctness: If the dealer is honest, then the reconstructed value is always equal to the secret f_0 (i.e., for any choice of the uncorrupted parties' random inputs and adversary's randomness). More formally, for any integers $n > 1$ and $t < n$, a two-round VSS satisfies correctness if for all λ, and a secret f_0, we have:

$$\Pr\begin{bmatrix}(\{f_i\}_{i=1}^n, \pi_{share}) \leftarrow \mathsf{Sharing.D}(n,t,f_0); (c_i,s_i,t_i) \leftarrow \mathsf{Sharing.P_i}(n,t,f_i);\\ i \in [n]; \{\alpha_i\}_{i\in[n]} \leftarrow \mathsf{Sharing.D}(\{c_i,s_i,t_i\}_{i\in[n]}) : i \in [n],\\ \mathsf{Happy} \leftarrow \mathsf{Sharing.P_i}(f_i,s_i,t_i,\{c_j,\alpha_j\}_{j\in[n]},\pi_{share}) \wedge\\ \forall V \in [n], |V| > t, f_0 \leftarrow \mathsf{Reconstruciton}(\{f_i\}_{i\in Q},\pi_{share})\end{bmatrix} = 1\ .$$

where V is a set of qualified honest parties.

- Commitment: Even if the dealer is dishonest, any execution of the sharing phase determines a unique value f_0 which will be reconstructed at the reconstruction phase. That is, the same value f_0 will be reconstructed by any qualified set of honest parties, regardless of the inputs provided by the adversary to Reconstruction. More formally, for any integers $t \geq 0$ and $2t+1 \leq n$, a two-round VSS satisfies commitment if for all PPT (stateful) adversaries $\mathcal{A}$, for all λ, we have:

$$\Pr\begin{bmatrix}Q \subset [n]; |Q| \leq t; (\{f_i\}_{i=1}^n, \{c_i,s_i,t_i\}_{i\in Q}, \pi_{share}) \leftarrow \mathsf{Sharing.}\mathcal{A}(n,t);\\ j \in [n] \setminus Q, (c_j,s_j,t_j) \leftarrow \mathsf{Sharing.P_j}(n,t,f_j),\\ \{\alpha_i\}_{i\in[n]} \leftarrow \mathsf{Sharing.}\mathcal{A}(\{c_i,s_i,t_i\}_{i\in[n]}),\\ \forall k \in [n], \mathsf{Happy} \leftarrow \mathsf{Sharing.P_k}(f_k,s_k,t_k,\{c_j,\alpha_j\}_{j\in[n]},\pi_{share}) :\\ \exists f_0, \forall V \in [n], |V| > t, f_0 \leftarrow \mathsf{Reconstruciton}(\{f_i\}_{i\in V},\pi_{share})\end{bmatrix} \geq 1-\mathsf{negl}(\lambda)\ ,$$

where Q is the set of corrupted parties and V denotes a qualified set of honest parties.

- Unpredictability: If the dealer is honest, then any polynomial time (stateful) adversary who controls up to t parties, cannot recover (or predict) the secret f_0 with a significant advantage. More formally, for any integers $n > 1$ and $t < n$, a two-round VSS is called unpredictable if for all PPT adversaries $\mathcal{A}$ who has non-adaptively corrupted up to t parties, for all λ, and a random secret f_0, we have:

$$\Pr\begin{bmatrix}(\{f_i\}_{i=1}^n, \pi_{share}) \leftarrow \mathsf{Sharing.D}(n,t,f_0); Q \subset [n]; |Q| \leq t;\\ \{c_i,s_i,t_i\}_{i\in Q} \leftarrow \mathsf{Sharing.}\mathcal{A}(n,t,\{f_i\}_{i\in Q}), \{c_i,s_i,t_i\}_{i\in[n]\setminus Q} \leftarrow \{0,1\}^\lambda,\\ \{\alpha_i\}_{i\in[n]} \leftarrow \mathsf{Sharing.D}(\{c_i,s_i,t_i\}_{i\in[n]}),\\ f_0' \leftarrow \mathsf{Sharing.}\mathcal{A}(\{f_i,s_i,t_i\}_{i\in Q},\{c_i,\alpha_i\}_{i\in[n]},\pi_{share}) : f_0' = f_0\end{bmatrix} \leq \mathsf{negl}(\lambda)\ .$$

- Secrecy: In some cases, the definition of Unpredictability can be strengthened by requiring that the view of adversary who corrupted t parties can be simulated. Namely, if the dealer is honest, then the t-adversary's view during the sharing phase is simulatable and reveals no information on f_0. More formally, the t-adversary's view is identically distributed under all different values of f_0. In the case of *perfect* secrecy, the adversary is assumed to have *unbounded* computational power.

3 A Unified Framework for Ronud-Optimal VSS

In this section, we introduce **2R-Π** as a new variant of the recently proposed unified framework **Π**, allowing the construction of 3-round Shamir-based VSS schemes in the honest-majority setting [Bag25]. In comparison to the original construction, the new variant reduces the number of required rounds by one while maintaining similar efficiency.

The resulting protocol enables the creation of round-optimal VSS schemes with superior performance when compared to state-of-the-art constructions proposed by Backes, Kate, and Patra [BKP11].

Fig. 1 describes the procedure of our proposed construction for building round-optimal VSS schemes.

Sharing: Two Rounds

Round 1: Given the public parameters pp, a secret f_0, dealer D

1. Chooses a random polynomial $f(X)$ and $r(X)$ of degree-t such that $f(0) = f_0$
2. For $i = 1, 2, \ldots, n$: set $f_i := f(i)$ and $r_i := r(i)$.
3. For $i = 1, 2, \ldots, n$: set $c_i = \mathcal{C}(pp, (f_i, r_i), \gamma_i)$, where γ_i are random values sampled from $\mathbb{Z}_q$. In some cases, the randomizer γ_i can be omitted.
4. Compute the challenge value $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$.
5. Set $z(X) = r(X) + df(X)$ and $\pi_{share} := (c_1, \ldots, c_n, z(X))$.
6. Send the shares (f_i, γ_i) (or just f_i) securely to party P_i and broadcast π_{share}.

Given the public parameters pp, every other party P_i

1. Chooses two random pairs (s_i, t_i) and (u_i, v_i)) (or just a random pair (s_i, t_i)) and computes $c_{s_i} = \mathcal{C}(pp, s_i, t_i)$ and $c_{u_i} = \mathcal{C}(pp, u_i, v_i)$ (or just $c_{s_i} = \mathcal{C}(pp, s_i, t_i)$).
2. Send (s_i, t_i) and (u_i, v_i) (or just (s_i, t_i)) to dealer, and broadcast commitments c_{s_i} and c_{u_i} (or just c_{s_i}).

Round 2: Dealer D, for every party P_i

1. Using the algorithm Open of the commitment scheme, checks if commitments c_{s_i} and c_{u_i} are (or just c_{s_i} is) consistent with the received pairs (s_i, t_i) and (u_i, v_i) (or just (s_i, t_i)).
2. Broadcast $\alpha_i = f_i + s_i$ and $\beta_i = \gamma_i + u_i$ (or just $\alpha_i = f_i + s_i$) if the verification succeeds, and broadcast f_i and γ_i (or just f_i) otherwise.

Party P_i

1. First verify if $\deg(z(X)) = t$ and, then using his/her share f_i and γ_i (or just f_i) checks if $c_i = \mathcal{C}(pp, (f_i, z(i) - df_i), \gamma_i)$ (or $c_i = \mathcal{C}(pp, f_i, z(i) - df_i)$), where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$ and $\mathcal{H}$ is an instantiation for the random oracle.
2. Broadcasts nothing if the verification succeeds, and broadcasts pairs (s_i, t_i) and (u_i, v_i) (or just (s_i, t_i)) otherwise. Party P_i is considered happy in the former case, while he/she is unhappy in the later case.

Local Computation: Every party P_k

1. discards D and halts the execution of the protocol, if
   (a) D broadcasts f_i and γ_i (or just f_i) such that $c_i \neq \mathcal{C}(pp, (f_i, z(i) - df_i), \gamma_i)$ (or $c_i \neq \mathcal{C}(pp, f_i, z(i) - df_i)$), where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$.
   (b) D broadcasts α_i and β_i (or just α_i); and P_i broadcasts (s_i, t_i) and (u_i, v_i) (or just (s_i, t_i)) such that $\mathsf{Open}(pp, s_i, t_i, c_{s_i}) = 1$ and $\mathsf{Open}(pp, u_i, v_i, c_{u_i}) = 1$ (or just $\mathsf{Open}(pp, s_i, t_i, c_{s_i}) = 1$) and $c_i \neq \mathcal{C}(pp, (f'_i, z(i) - df'_i), \gamma'_i)$ (or $c_i \neq \mathcal{C}(pp, f'_i, z(i) - df'_i)$), where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$ and $f'_i = \alpha_i - s_i$ and $\gamma'_i = \beta_i - u_i$ (or just $f'_i = \alpha_i - s_i$).
2. Discards an unhappy party P_i, if he/she broadcasts (s_i, t_i) and (u_i, v_i) (or just (s_i, t_i)) such that $\mathsf{Open}(pp, s_i, t_i, c_{s_i}) = 0$ and $\mathsf{Open}(pp, u_i, v_i, c_{u_i}) = 0$ (or just $\mathsf{Open}(pp, s_i, t_i, c_{s_i}) = 0$). Let $\mathbb{Q}$ be the set of non-discarded parties.
3. Outputs f_k and γ_k (or f_k) as received in Round 1, if P_k is happy and in $\mathbb{Q}$. If he/she is unhappy and belongs to $\mathbb{Q}$, then he/she outputs f_k and γ_k (or f_k) if they are directly broadcasted by D in Round 2. Otherwise, P_k computes f_k and γ_k (or just f_k) as $f_k = \alpha_k - s_k$ and $\gamma_k = \beta_k - u_k$ (or just $f_k = \alpha_k - s_k$).

Reconstruction: One Round

1. Party $P_i \in \mathbb{Q}$ broadcast f'_i and γ'_i (or f'_i).

Local Computation: For every party P_k,

1. Party $P_i \in \mathbb{Q}$ is said to be *confirmed* if $c_i = \mathcal{C}(pp, (f'_i, z(i) - df'_i), \gamma'_i)$ (or $c_i = \mathcal{C}(pp, f'_i, z(i) - df'_i)$) where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$.
2. Consider f'_i values of any $t+1$ *confirmed* parties and interpolate $f'(X)$. Output $f'_0 = f'(0)$.

Figure 1: 2R-Π: the proposed general 2-round computational VSS scheme for $n \geq 2t + 1$. In the protocol, $\mathcal{H}$ represents an instantiation for the Random Oracle, and $\mathcal{C}$ is a perfectly (resp. computationally) binding and computationally (resp. perfectly) hiding commitment.

Overview. As in the original $\mathbf{\Pi}$ protocol [Bag25], the dealer utilizes a NI-TZK proof scheme for the Shamir relation and proves the validity and consistency of the distributed shares. Specifically, when given the secret f_0, the dealer initiates a standard Shamir secret sharing by selecting a random t-degree polynomial $f(X)$ with $f(0) = f_0$. Subsequently, the dealer privately sends the shares $f_i = f(i)$ for $i = 1, \ldots, n$ to the parties and utilizes the NI-TZK proof scheme from the $\mathbf{\Pi}$ protocol, generating an NI-TZK argument π_{share} and broadcasting it. The NI-TZK proof scheme enables the share-holders to verify if the degree of the shared univariate polynomial $f(X)$ is (at most) t without learning the main secret. In the general construction of **2R-$\mathbf{\Pi}$**, $\mathcal{H}$ represents an instantiation for the Random Oracle, and $\mathcal{C}$ is committing algorithm of a perfectly (resp. computationally) hiding and computationally (resp. perfectly) binding commitment scheme. We highlight that, in practice, to build a 2-round VSS scheme that satisfies IT secrecy, one must commit to $m_i := (f_i, r_i)$ using a perfectly hiding commitment scheme.

To reduce the number of rounds in framework $\mathbf{\Pi}$, we incorporate a modification which is based on commitments and one-time pad encryption, inspired by the technique used in the earlier unconditionally secure [GIKR01] and computationally secure [BKP11] VSS schemes. This modification requires shareholders to engage in some computation and communication during the first round. Specifically, in the first round, each party is required to publicly commit to one (or two) randomness and send the randomness to the dealer. Subsequently, in the second round, the dealer uses these randomness values as a blinding pad and broadcasts the (one-time pad encryption of) shares.

At the beginning of the second round, each party verifies a portion of the NI-TZK proof π_{share} using their received shares. Simultaneously, the dealer checks the consistency of his received values with the corresponding commitments made by individual parties. In case of a failed verification of π_{share} or any inconsistency between the public commitments and private values, these issues are addressed in the second round through broadcast communication. At the conclusion of the second round, following local computations, an agreement is reached among the honest parties. Specifically, if the dealer is disqualified, all honest parties become aware of it, resulting in an identical copy of the set $\mathbb{Q}$, which represents the set of qualified parties.

In the reconstruction phase, each shareholder broadcasts their shares. Subsequently, the disclosed shares are verified with respect to the public NI-TZK proof generated during the sharing phase. Following verification, $t+1$ valid shares are employed for the reconstruction of the secret polynomial $f(X)$ and, consequently, the main secret $s = f(0)$.

Efficiency. In terms of computational cost, to share a secret among n parties with a threshold of t, the dealer's computational cost is dominated with the computation of $2n$ evaluations of degree-t polynomials $f(X)$ and $r(X)$ along with $2n$ (or $3n$) commitments for computing c_i and checking c_{s_i} (and c_{u_i} if applicable). In the sharing phase which also includes the verification, each party is required to generate 2 (or 3) commitments, make a single query to the random oracle, and perform a one-time evaluation of a t-degree polynomial $z(X)$.

In terms of communication, during the sharing phase, the dealer requires $O(n\lambda)$ bits of broadcast and $O(n\lambda)$ bits of private communication. Conversely, each party only requires $O(1)$ bits of broadcast and $O(1)$ bits of private communication with the dealer. In the reconstruction phase, the protocol demands $O(n\lambda)$ bits for broadcast. This communication complexity is at least a linear factor lower than the state-of-the-art 2-round VSS scheme based on non-homomorphic commitments, as proposed in [BKP11, Section 3.2]. On the other hand, it is asymptotically comparable to the communication complexity of 3-round VSS schemes [Fel87, Ped92, ABCP23, Bag25].

We prove the security of new general round-optimal VSS scheme in the following theorem.

Theorem 1 (Round-Optimal Synchronous VSS Schemes)**.** *If the (vector) commitment scheme $\mathcal{C}$ is computationally (resp. perfectly) binding and perfectly (resp. computationally) hiding and $\mathcal{H}$ is a random oracle, then the generic construction given in Fig. 1 is a secure 2-round VSS scheme in the honest-majority setting, that satisfies perfect (resp. computational) Secrecy, Correctness, and Commitment (Defined in Sec. 2.3.2). Namely, (i) the Reconstruction protocol results in a unique secret distributed by the dealer for any qualified set of shareholders, (ii) any non-qualified set of computationally unbounded (resp. bounded) shareholders cannot gain any information about the secret.*

Proof. We prove the security properties of **2R-Π** for the scenario where the commitment scheme $\mathcal{C}$ is perfectly hiding and computationally binding, resulting in a VSS scheme that achieves perfect secrecy. The reverse case can be addressed similarly, leading to a VSS scheme that achieves computational secrecy.
Perfect Secrecy: We show that a simulator can perfectly simulate the view of an unbounded t-adversary $\mathcal{A}$, a computationally unbounded adversary who controls up to t parties. Let $\mathcal{A}$ be an unbounded t-adversary against the VSS scheme described in Fig. 2, which w.l.o.g., has corrupted first t parties and knows the public values and the secret inputs for all of the corrupted parties, i.e., $(f_i, \gamma_i, s_i, t_i, u_i, v_i)$ for $i = 1, \ldots, t$. Assuming the dealer acts honestly, the adversary's view involves observing t points on a polynomial of degree t (denoted as $f(X)$), alongside a masked degree-t polynomial $z(X) := r(X) + d \cdot f(X)$, and all commitment values $c_i := \mathcal{C}(pp, (f_i, r_i); \gamma_i)$ for $i = 1, \ldots, n$ in Round 1. Additionally, in Round 1, the adversary observes t values of (s_i, t_i, u_i, v_i). Subsequently, in Round 2, the adversary receives $2n$ values: $\alpha_i = f_i + s_i$ and $\beta_i = \gamma_i + u_i$ or f_i and γ_i while he has information only on t values of s_i and u_i (he already knows f_i and γ_i for those t parties so this round does not give him any more information!). Regarding the information obtained by the attacker in the first round, we note that given perfectly hiding commitments c_1, c_{s_1}, c_{u_1}, $\ldots$, c_n, c_{s_n}, c_{u_n}, the random challenge value d and $z_i = r_i + d \cdot f_i$ learning any information (or obtaining in some cases) f_i, r_i, γ_i is infeasible. Namely, from commitments $\{c_i, c_{s_i}, c_{u_i}\}_{i=1}^n$ and the masked degree-t polynomial $z(X)$, obtaining the values of $f(X)$ and $r(X)$ in other points is infeasible. Concerning the second round, it is obvious that the attacker does not gain any additional information, since s_i and u_i are used to hide f_i and γ_i, respectively, and s_i and u_i themselves are randomly chosen. We highlight two points. Firstly, in Round 1, we emphasize that t evaluations of a degree-t polynomial, information theoretically does not reveal any information about the polynomial. Hence, the adversary learn any information about (or cannot recover) other points, including the secret value $f(0)$, from the transcript of the protocol. Secondly, note that (s_i, t_i) and (u_i, v_i) are randomly chosen, and they remain perfectly secure, even if the commitments c_{s_i} and c_{u_i} are made public, due to the perfect hiding property of the commitment scheme.

With this knowledge, given the inputs (i.e., individual shares) of t corrupted parties, we can formally show that the view of $\mathcal{A}$ is simulatable and the simulation is perfect. To this end, given the public parameters and the random oracle $\mathcal{H}$, the simulator acts as follows:

- Given the public parameters pp, the shares $\{f_i, \gamma_i\}_{i=1}^t$, it samples two random degree-t polynomials $f'(X)$ and $r'(X)$, such that $f'(i) = f_i$ and $\gamma'_i = \gamma_i$ for $i = 1, \ldots, t$.
- The simulator sets $c'_i = \mathcal{C}(pp, (f'(i), r'(i)); \gamma'_i)$ for $i = 1, \ldots, n$, then it programs the random oracle to $d = \mathcal{H}(c'_1, \ldots, c'_n)$ and sets $z'(X) := r'(X) + d \cdot f'(X)$, where γ'_i are sampled randomly for $i = t+1, \ldots, n$. Note that, in this case, the simulator can also sample $c'_{t+1}, \ldots, c'_n$ at random, which will result in a more efficient simulation.
- Then, given the values $\{s_i, t_i, u_i, v_i\}_{i=1}^t$ for corrupted parties, the simulator samples the rest of $\{s_i, t_i, u_i, v_i\}_{t+1}^n$ at random and sets $c'_{s_i} := \mathcal{C}(pp, s_i, t_i)$ and $c'_{u_i} := \mathcal{C}(pp, u_i, v_i)$ for $i = 1, 2, \ldots, n$.
- Next, the simulator sets $\alpha'_i = f'(i) + s_i$ and $\beta'_i = \gamma'_i + u_i$ for $i = 1, 2. \ldots, n$.
- At the end, the simulator returns $(d, z'(X), c'_i, c'_{s_i}, c'_{u_i}, \alpha'_i, \beta'_i)$ for $i = 1, \ldots, n$ as the simulated transcript.

We can observe that the simulated transcript is perfectly indistinguishable from a real transcript of the protocol, as the commitments are perfectly hiding and encryptions of α'_i and β'_i are done using one-time pad encryption via secret keys that are hidden in the perfectly hiding commitments (c'_{s_i}, c'_{u_i}). Therefore, the VSS scheme satisfies perfect secrecy (a.k.a., IT secrecy) against an unbounded adversary who controls up to t parties.

Correctness: If the dealer is honest, then each party receives a unique evaluation of a degree-t polynomial with constant term f_0. Therefore, in the reconstruction phase, any set of (at least) $t+1$ honest parties can use Lagrange interpolation and recover a unique degree-t polynomial, and a unique secret value f_0.

Commitment: To achieve the commitment property and to prove the validity of the distributed shares, the dealer uses a special-sound sigma protocol with distributed and designated verifiers. Then, the protocol is made non-interactive in the random oracle model, using a variant of the Fiat-Shamir transform proposed in [BBC+19]. In the interactive version of the underlying sigma protocol, given two acceptable transcripts $(c_1, \ldots, c_n, d, z(X))$ and $(c_1, \ldots, c_n, d' \neq d, z'(X))$ obtained by rewiring the dealer, the verification equation allows us to express:

$$\mathcal{C}(pp, (f_i, z(i) - d \cdot f_i), \gamma_i) = \mathcal{C}(pp, (f_i, z'(i) - d' \cdot f_i), \gamma_i)$$

for $i = 1, \ldots, n$, where $n \geq 2t+1$. Based on the above equation and the computational binding property of commitment scheme $\mathcal{C}$ we can deduce that for $i = 1, \ldots, n$, with overwhelming probability,

$$z(i) - d \cdot f_i = z'(i) - d' \cdot f_i.$$

As a result, $f_i = \frac{z(i)-z'(i)}{d-d'}$ for $i = 1, \ldots, n$. Assuming that $d - d'$ is invertible modulo q, given any set of $t+1$ valid shares, an extractor can extract a *unique* degree-t polynomial $f(X)$ from the dealer with overwhelming probability. This polynomial satisfies $f(i) = f_i$ for $i \in Q$, where Q represents the set of valid shares with $|Q| \geq t+1$.

Note that we have considered the case that $\mathcal{C}$ satisfies computationally binding. Assume by contradiction that in the reconstruction phase parties reconstruct $f'_0 \neq f_0 := f(0)$ by choosing $t+1$ values $f'_1, \ldots, f'_{t+1}$ and $\gamma'_1, \ldots, \gamma'_{t+1}$, such that $c_i = \mathcal{C}(pp, (f'_i, z(i) - d \cdot f'_i); \gamma'_i)$. This means that the t-degree polynomials $f'(X)$ and $r'(X)$ interpolated by the points f'_i and $z(i) - d \cdot f'_i$ have the property that $\mathcal{C}(pp, (f'_i, z(i) - d \cdot f'(i)); \gamma'_i) = \mathcal{C}(pp, (f'_i, r'(i)), \gamma'_i) = c_i$ for $i = 1, \ldots, t+1$, but $f'(X) \neq f(X)$ (as they differ in the free term), thus there must be an index j such that $f'(j) \neq f(j)$. Since each degree-t polynomial gets unique with its $t+1$ distinct evaluations, then the values $(z(j) - d \cdot f'(j))$ and $(z(j) - d \cdot f(j))$ are a double opening for the commitment, which is known to either the dealer or P_j, which contradicts the hypothesis, the computational binding property of $\mathcal{C}$.

Therefore, at the end of the *Reconstruction* phase, any set of $t+1$ honest parties, can use their valid shares and reconstruct a unique degree-t polynomial $f(X)$, and determine a unique secret value $f_0 := f(0)$. □

4 More Efficient Round-Optimal VSS Schemes

The strength of **2R-Π** (illustrated in Fig. 1) lies in its generality. It only requires a random oracle $\mathcal{H}$ and a commitment scheme $\mathcal{C}$, which does not necessarily have to be homomorphic. Therefore, it can be instantiated similar to the original version of **Π** protocol. In practice, random oracles (with some estimations) are instantiated using secure cryptographic hash functions, and commitments can be constructed using various cryptographic primitives and relying on different cryptographic assumptions.

In this section, we employ different commitment schemes based on discrete logarithms and hash functions and instantiate **2R-Π** from Sec. 3 to build new VSS schemes in the

honest-majority setting. These new round-optimal VSS schemes demonstrate considerably better efficiency compared to the state-of-the-art alternatives proposed in [BKP11, Sections 3.2, 3.5]. From a different perspective, the proposed VSS schemes can be viewed as round-reduced (i.e., 2-round) variants of the 3-round VSS schemes built using the original **Π** protocol [Bag25].

4.1 2-Round IT-Secure VSS Scheme from Pedersen Commitment

By instantiating the general construction **2R-Π** from Sec. 4 with a (vector) variant of the Pedersen commitment scheme from [BG18], specifically by employing *three* randomly chosen group generators $(g_1, g_2, g_3) \in \mathbb{G}$, we obtain a novel DL-based 2-round VSS scheme. The new VSS scheme can satisfy IT secrecy, as in the 3-round VSS schemes Pedersen[Ped92] and $\mathbf{\Pi_P}$ [Bag25], and can be considered as an efficient alternative to the 2-round VSS scheme proposed in [BKP11, Sec. 3.5].

In this scheme, commitments c_i are computed as $c_i = g_1^{f_i} g_2^{r_i} g_3^{\gamma_i}$ for $i = 1, \ldots, n$, where as in **2R-Π**, γ_i are randomizers sampled from $\mathbb{Z}_q$. Inherent for the **Π** protocol, in the resulting VSS scheme, before computing the value $z(X) = r(X) + d \cdot f(X)$, the dealer additionally checks if $g_1 \neq g_2^d$ and continues if the check passes. This check is necessary to achieve IT-security against up to t shareholders. On the other side, in first round, the party P_i chooses two random pairs (s_i, t_i) and (u_i, v_i), and then publishes two Pedersen commitments c_{s_i} and c_{u_i}. The description of new VSS scheme is summarized in Fig. 2.

The resulting round-optimal VSS scheme is a direct instantiation of the general construction **2R-Π** with a perfectly hiding and computationally binding commitment scheme. Under the DL assumption, Theorem 1 can be adapted for this particular instantiation, resulting in the following corollary.

Corollary 1 (Round-Optimal IT-secure VSS Scheme)**.** *Let, $(g_1, g_2, g_3) \in \mathbb{G}$ be three random group generators for $\mathbb{G}$ and $\mathcal{H}$ be a random oracle. Then, under discrete logarithm assumption, the construction given in Fig. 2 is a secure 2-round VSS scheme that satisfies perfect* Secrecy, Correctness, *and (computational)* Commitment *(Defined in Sec. 2.3.2) in the random oracle model. Namely, (i) the Reconstruction protocol results in a unique secret distributed by the dealer for any qualified set of shareholders, (ii) any non-qualified set of computationally unbounded shareholders learns nothing about the secret.*

The resulting IT secure round-optimal VSS scheme surpasses the alternative scheme proposed in [BKP11, Sec 3.5], and has more efficient verification and reconstruction phases.

4.2 2-Round VSS Scheme from Hash Functions

The instantiation from Sec. 4.1 uses the Pedersen commitment which is homomorphic and relies on the DL assumption. In this section, we instantiate **2R-Π** with a hash-based commitment scheme which is non-homomorphic and plausibly have post-quantum security. A description of the new 2-round VSS scheme based on a hash-based commitment scheme is summarized in Fig. 3. The instantiation results in the first practical round-optimal hash-based VSS scheme, requiring $O(n)$ computation and $O(n\lambda)$ communication. In the general case of new VSS scheme, when the secret f_0 lacks sufficient entropy, commitments c_i are computed as $c_i = \mathsf{H}(f_i, r_i, \gamma_i)$, where H is a well-defined secure hash function and γ_i are randomly sampled for $i = 1, \ldots, n$. However, when sharing a high-entropy secret, the randomizer γ_i used be the dealer, and the randomizers (u_i, v_i) used by P_i are no longer needed and can be omitted from the protocol.

The new round-optimal hash-based VSS scheme is a direct instantiation of **2R-Π** with a computationally hiding and perfectly binding commitment scheme $\mathcal{C}(.,.;.)$. Under the assumption that $\mathcal{C}$ is a secure scheme, which is established in the RO model, Theorem 1 can be adapted for this particular instantiation, resulting in the following corollary.

Sharing: Two Rounds

Round 1: Given the group generators $pp := (g_1, g_2, g_3)$, public parameters, a secret f_0, dealer D

1. Chooses a random polynomial $f(X)$ and $r(X)$ of degree-t such that $f(0) = f_0$
2. For $i = 1, 2, \ldots, n$: set $f_i := f(i)$ and $r_i := r(i)$.
3. For $i = 1, 2, \ldots, n$: set $c_i = g_1^{f_i} g_2^{r_i} g_3^{\gamma_i}$, where γ_i are sampled randomly from $\mathbb{Z}_q$.
4. Compute the challenge value $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$, where $\mathcal{H}$ is a Random Oracle.
5. Set $z(X) = r(X) + df(X)$ and $\pi_{share} := (c_1, \ldots, c_n, z(X))$.
6. Send shares f_i and γ_i securely to party P_i and broadcast π_{share}.

Given group generators $pp := (g_1, g_2)$, every other party P_i

1. Chooses two random pairs (s_i, t_i) and (u_i, v_i) and computes $c_{s_i} = g_1^{s_i} g_2^{t_i}$ and $c_{u_i} = g_1^{u_i} g_2^{v_i}$.
2. Send (s_i, t_i) and (u_i, v_i) to dealer, and broadcast commitments c_{s_i} and c_{u_i}.

Round 2: Dealer D, for every party P_i

1. Using the algorithm Open of the commitment scheme, checks if commitments c_{s_i} and c_{u_i} are consistent with the received pairs (s_i, t_i) and (u_i, v_i).
2. Broadcast $\alpha_i = f_i + s_i$ and $\beta_i = \gamma_i + u_i$ if the verification succeeds, and broadcast f_i and γ_i otherwise.

Party P_i

1. First verify if $\deg(z(X)) = t$ and, then using his/her shares f_i and γ_i checks if $c_i = g_1^{f_i} g_2^{z(i) - df_i} g_3^{\gamma_i}$, where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$ and $\mathcal{H}$ is a Random Oracle.
2. Broadcasts nothing if the verification succeeds, and broadcasts pairs (s_i, t_i) and (u_i, v_i) otherwise. Party P_i is considered happy in the former case, while he/she is unhappy in the later case.

Local Computation: Every party P_k

1. discards D and halts the execution of the protocol, if
   (a) D broadcasts f_i and γ_i such that $c_i \neq g_1^{f_i} g_2^{z(i) - df_i} g_3^{\gamma_i}$, where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$.
   (b) D broadcasts α_i and β_i; and P_i broadcasts (s_i, t_i) and (u_i, v_i) such that $c_{s_i} = g_1^{s_i} g_2^{t_i}$ and $c_{u_i} = g_1^{u_i} g_2^{v_i}$ and $c_i \neq g_1^{f_i'} g_2^{z(i) - df_i'} g_3^{\gamma_i'}$, where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$ and $f_i' = \alpha_i - s_i$ and $\gamma_i' = \beta_i - u_i$.
2. Discards an unhappy party P_i, if he/she broadcasts (s_i, t_i) and (u_i, v_i) such that $c_{s_i} \neq g_1^{s_i} g_2^{t_i}$ and $c_{u_i} \neq g_1^{u_i} g_2^{v_i}$. Let $\mathbb{Q}$ be the set of non-discarded parties.
3. Outputs f_k and γ_k as received in Round 1, if P_k is happy and in $\mathbb{Q}$. If he/she is unhappy and belongs to $\mathbb{Q}$, then he/she outputs f_k and γ_k if they are directly broadcasted by D in Round 2. Otherwise, P_k computes f_k and γ_k as $f_k = \alpha_k - s_k$ and $\gamma_k = \beta_k - u_k$.

Reconstruction: One Round

1. Party $P_i \in \mathbb{Q}$ broadcast f_i' and γ_i'.

Local Computation: For every party P_k,

1. Party $P_i \in \mathbb{Q}$ is said to be *confirmed* if $c_i = g_1^{f_i'} g_2^{z(i) - df_i'} g_3^{\gamma_i'}$ where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$.
2. Consider f_i' values of any $t+1$ *confirmed* parties and interpolate $f'(X)$. Output $f_0' = f'(0)$.

Figure 2: A novel 2-round IT-secure VSS scheme from Pedersen's commitment.

Corollary 2 (Round-Optimal Hash-based VSS Scheme)**.** *Let,* H *and* $\mathcal{H}$ *be two properly defined secure hash functions that are modeled as random oracle. Then, the construction given in Fig. 3 is a secure 2-round VSS scheme that satisfies computational* Secrecy*,* Correctness*, and* Commitment *(Defined in Sec. 2.3.2) in the random oracle model. Specifically, (i) the Reconstruction protocol results in a unique secret distributed by the dealer for any qualified set of shareholders, (ii) any non-qualified set of computationally bounded shareholders learns nothing about the secret.*

4.3 2-Round VSS Scheme from Pedersen Commitment

Our instantiations from Sections 4.1 and 4.2 were direct instantiations of the general construction **2R-Π**. In this section, by employing a random oracle $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_q$ and

Sharing: Two Rounds

Round 1: Given the hash functions $pp := (\mathsf{H}, \mathcal{H})$, a (low-entropy) secret f_0, dealer D

1. Chooses two random polynomials $f(X)$ and $r(X)$ of degree-t such that $f(0) = f_0$
2. For $i = 1, 2, ..., n$: set $f_i := f(i)$ and $r_i := r(i)$.
3. For $i = 1, 2, ..., n$: set $c_i = \mathsf{H}(f_i, r_i, \gamma_i)$, where γ_i are sampled randomly from $\mathbb{Z}_q$.
4. Compute the challenge value $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$, where $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_q$ is an instantiation for the random oracle.
5. Set $z(X) = r(X) + df(X)$ and $\pi_{share} := (c_1, \ldots, c_n, z(X))$.
6. Send share (f_i, γ_i) securely to party P_i and broadcast π_{share}.

Given $pp := (\mathsf{H}, \mathcal{H})$, every other party P_i

1. Chooses two random pairs (s_i, t_i) and (u_i, v_i), and computes $c_{s_i} = \mathsf{H}(s_i, t_i)$ and $c_{u_i} = \mathsf{H}(u_i, v_i)$.
2. Send (s_i, t_i) and (u_i, v_i) to dealer, and broadcast commitments c_{s_i} and c_{u_i}.

Round 2: Dealer D, for every party P_i

1. Using the algorithm Open of the commitment scheme, checks if c_{s_i} and c_{u_i} are consistent with the received pairs (s_i, t_i) and (u_i, v_i).
2. Broadcast $\alpha_i = f_i + s_i$ and $\beta_i = \gamma_i + u_i$ if the verification succeeds, and broadcast f_i and γ_i otherwise.

Party P_i

1. First verify if $\deg(z(X)) = t$ and, then using his/her share (f_i, γ_i) checks if $c_i = \mathsf{H}(f_i, z(i) - df_i; \gamma_i)$, where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$.
2. Broadcasts nothing if the verification succeeds, and broadcasts pairs (s_i, t_i) and (u_i, v_i) otherwise. Party P_i is considered happy in the former case, while he/she is unhappy in the later case.

Local Computation: Every party P_k

1. discards D and halts the execution of the protocol, if
   (a) D broadcasts f_i and γ_i such that $c_i \neq \mathsf{H}(f_i, z(i) - df_i; \gamma_i)$, where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$.
   (b) D broadcasts α_i and β_i; and P_i broadcasts (s_i, t_i) and (u_i, v_i) such that $c_{s_i} = \mathsf{H}(s_i, t_i)$ and $c_{u_i} = \mathsf{H}(u_i, v_i)$ and $c_i \neq \mathsf{H}(f_i', z(i) - df_i'; \gamma_i')$, where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$ and $f_i' = \alpha_i - s_i$ and $\gamma_i' = \beta_i - u_i$.
2. Discards an unhappy party P_i, if he/she broadcasts (s_i, t_i) and (u_i, v_i) such that $c_{s_i} \neq \mathsf{H}(s_i, t_i)$ and $c_{u_i} \neq \mathsf{H}(u_i, v_i)$. Let $\mathbb{Q}$ be the set of non-discarded parties.
3. Outputs f_k and γ_k as received in Round 1, if P_k is happy and in $\mathbb{Q}$. If he/she is unhappy and belongs to $\mathbb{Q}$, then he/she outputs f_k and γ_k if they are directly broadcasted by D in Round 2. Otherwise, P_k computes f_k and γ_k as $f_k = \alpha_k - s_k$ and $\gamma_k = \beta_k - u_k$.

Reconstruction: One Round

1. Party $P_i \in \mathbb{Q}$ broadcast f_i' and γ_i'.

Local Computation: For every party P_k,

1. Party $P_i \in \mathbb{Q}$ is said to be *confirmed* if $c_i = \mathsf{H}(f_i', z(i) - df_i'; \gamma_i')$ where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$.
2. Consider f_i' values of any $t+1$ *confirmed* parties and interpolate $f'(X)$. Output $f_0' = f'(0)$.

Figure 3: A practical 2-round VSS scheme based on non-homomorphic (hash-based) commitments. If the secret f_0 has sufficient entropy, the highlighted parts (e.g., randomizers γ_i for $i = 1, \ldots, n$) can be omitted.

the standard form of Pedersen commitment scheme [Ped92] within **2R-Π**, we obtain a novel round-optimal VSS scheme which uses homomorphic commitments, requires high-entropy secret, and achieves a weaker notion of security compared to the construction from Fig. 2. We believe that this scheme should be sufficient for the construction of various protocols, such as distributed key generation protocols. Let, $(g_1, g_2) \in \mathbb{G}$ be two random group generators for the Pedersen commitment scheme. Then, in the new VSS scheme the commitments are computed as $c_i := g_1^{f_i} g_2^{r_i}$. Fig. 4 describes the procedure of resulting

Sharing: Two Rounds

Round 1: Given the group generators $pp := (g_1, g_2)$, a secret f_0, dealer D

1. Chooses a random polynomial $f(X)$ and $r(X)$ of degree-t such that $f(0) = f_0$
2. For $i = 1, 2, ..., n$: set $f_i := f(i)$ and $r_i := r(i)$.
3. For $i = 1, 2, ..., n$: set $c_i = g_1^{f_i} g_2^{r_i}$.
4. Compute the challenge value $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$, where $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_q$ is an instantiation for the Random Oracle.
5. Set $z(X) = r(X) + df(X)$ and $\pi_{share} := (c_1, \ldots, c_n, z(X))$.
6. Send share f_i securely to party P_i and broadcast π_{share}.

Given the group generator g_1, every other party P_i

1. Chooses a random value s_i and compute $c_{s_i} = g_1^{s_i}$. Note that, in this case we can omit the randomizer t_i mentioned in the general construction.
2. Send s_i to dealer, and broadcast commitment c_{s_i}.

Round 2: Dealer D, for every party P_i

1. Using the algorithm Open of the commitment scheme, checks if commitment c_{s_i} is consistent with the received value s_i.
2. Broadcast $\alpha_i = f_i + s_i$ if the verification succeeds, and broadcast f_i otherwise.

Party P_i

1. First verify if $\deg(z(X)) = t$ and, then using his/her share f_i checks if $c_i = g_1^{f_i} g_2^{z(i) - df_i}$, where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$.
2. Broadcasts nothing if the verification succeeds, and broadcasts s_i otherwise. Party P_i is considered happy in the former case, while he/she is unhappy in the later case.

Local Computation: Every party P_k

1. discards D and halts the execution of the protocol, if
   (a) D broadcasts f_i such that $c_i \neq g_1^{f_i} g_2^{z(i) - df_i}$, where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$.
   (b) D broadcasts α_i; and P_i broadcasts s_i such that $c_{s_i} = g_1^{s_i}$ and $c_i \neq g_1^{f'_i} g_2^{z(i) - df'_i}$, where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$ and $f'_i = \alpha_i - s_i$.
2. Discards an unhappy party P_i, if he/she broadcasts (s_i, t_i) such that $c_{s_i} \neq g_1^{s_i} g_2^{t_i}$. Let $\mathbb{Q}$ be the set of non-discarded parties.
3. Outputs f_k as received in Round 1, if P_k is happy and in $\mathbb{Q}$. If he/she is unhappy and belongs to $\mathbb{Q}$, then he/she outputs f_k if they are directly broadcastebd by D in Round 2. Otherwise, P_k computes f_k as $f_k = \alpha_k - s_k$.

Reconstruction: One Round

1. Party $P_i \in \mathbb{Q}$ broadcast f'_i.

Local Computation: For every party P_k,

1. Party $P_i \in \mathbb{Q}$ is said to be *confirmed* if $c_i = g_1^{f'_i} g_2^{z(i) - df'_i}$ where $d = \mathcal{H}(c_1, c_2, \ldots, c_n)$.
2. Consider f'_i values of any $t+1$ *confirmed* parties and interpolate $f'(X)$. Output $f'_0 = f'(0)$.

Figure 4: A novel 2-round VSS scheme based on discrete logarithm.

2-round VSS scheme. Next, we show that under the DL assumption, the resulting 2-round VSS scheme satisfies the properties of *Unpredictability*, *Correctness* and *Commitment*.

Theorem 2 (2-Round VSS Scheme Based on DL)**.** *Let, $(g_1, g_2) \in \mathbb{G}$ be two random group generators for $\mathbb{G}$ and $\mathcal{H}$ be a random oracle. Then, under DL assumption, the scheme given in Fig. 4 is a secure 2-round VSS scheme that satisfies Unpredictability, Correctness, and Commitment (Defined in Sec. 2.3.2) in the random oracle model. Namely, (i) the Reconstruction protocol results in a unique secret distributed by the dealer for any qualified set of shareholders, (ii) any non-qualified set of shareholders is unable to recover the secret.*

Proof. Unpredictability: We show that if a t-adversary $\mathcal{A}$, a polynomial time adversary who controls up to t parties, can recover the secret f_0, then we can use $\mathcal{A}$ and build an adversary $\mathcal{B}$ that can break DL assumption with the same advantage. We write the reduction for the case $n = t + 1$, but it can be written for the general case as well. Let $\mathcal{A}$

be a t-adversary against the VSS scheme described in Fig. 4, which w.l.o.g., has corrupted first t parties and knows the public values and the secret inputs for all of the corrupted parties, i.e., (f_i, s_i) for $i = 1, \ldots, t$. Let, $\mathcal{B}$ be a polynomial time adversary which given $y = g_1^x$ and group generator g_1, aims to break DL assumption and recover x. To this end, the adversary $\mathcal{B}$ acts as follows:

- It samples a random x' and sets $g_2 = g_1^{x'}$ as the second generator of $\mathbb{G}$.
- Given, the public challenge value d and the secret values $f_1, ..., f_t$ it samples a degree-t polynomial $z(X)$ and sets $c_i = g_1^{f_i} g_2^{z(i)-df_i}$ for $i = 1, ..., t$.
- Then, given the value $y = g_1^x$ and the sampled value x', it sets the commitment value c_{t+1} as $c_{t+1} = y g_2^{z(t+1)} y^{-dx'}$. Note that this will imply that $c_{t+1} = g_1^x g_2^{z(t+1)} g_1^{x(-dx')} = g_1^x g_2^{z(t+1)} g_1^{x'(-dx)} = g_1^x g_2^{z(t+1)-dx}$, which is the commitment to the share of party $t+1$.
- Given $s_1, \ldots, s_t$, it sets $\alpha_i = f_i + s_i$ and $c_{s_i} = g_1^{s_i}$ for $i = 1, \ldots, t$.
- Sample a random value α_{t+1} and compute $c_{s_{t+1}} = \frac{g_1^{\alpha_{t+1}}}{y}$.
- Then it sends the simulated elements $(c_1, \ldots, c_{t+1}, d, z(X), c_{s_1}, \ldots, c_{s_{t+1}})$ to adversary $\mathcal{A}$ and receives f_0.
- Then it uses $f_0, f_1, ..., f_t$, and compute f_{t+1} by Lagrange interpolation and returns $x = f_{t+1}$ as the solution for $y = g^x$.

We observe that the advantage of $\mathcal{B}$ and $\mathcal{A}$ are equal. This implies that the protocol satisfies unpredictability under the DL assumption.

Correctness: If the dealer is honest, then each party gets a unique evaluation of a degree-t polynomial with constant term f_0. Therefore, in the reconstruction phase, any set of qualified parties can collectively reconstruct a unique degree-t polynomial, and consequently the same secret value of f_0.

Commitment: In order to achieve the commitment property and to prove the validity of the distributed shares, the dealer uses a special-sound sigma protocol with distributed and designated verifiers. This protocol is subsequently transformed into a non-interactive form in the random oracle model, employing a variant of the Fiat-Shamir transform [BBC+19]. In the interactive version of the underlying sigma protocol, given two acceptable transcripts $(c_1, \ldots, c_n, d, z(X))$ and $(c_1, \ldots, c_n, d' \neq d, z'(X))$ obtained by rewiring the dealer, the verification equation allows us to express:

$$g_1^{f_i} g_2^{z(i)-d\cdot f_i} = g_1^{f_i} g_2^{z'(i)-d'\cdot f_i}$$

for $i = 1, \ldots, n$, where $n \geq 2t+1$. Based on the above equation (and the binding property of Pedersen commitment scheme), we can deduce that with overwhelming probability,

$$z(i) - d \cdot f_i = z'(i) - d' \cdot f_i.$$

Consequently, $f_i = \frac{z(i)-z'(i)}{d-d'}$ for $i = 1, \ldots, n$. Assuming that $d - d'$ is invertible modulo q, an extractor can extract a *unique* degree-t polynomial $f(X)$ from the dealer given any set of $t+1$ valid shares. This polynomial satisfies $f(i) = f_i$ for $i \in Q$, where Q represents the set of valid shares with $|Q| \geq t+1$.

Therefore, at the end of the *Reconstruction* phase, any set of $t+1$ honest parties, can use their valid shares and reconstruct a unique degree-t polynomial $f(X)$, and determine a unique secret value $f_0 = f(0)$. □

Note that as in 3-round Feldman [Fel87] and $\mathbf{\Pi_F}$ VSS schemes [Bag25], in the new 2-round VSS scheme the secret f_0 should contain sufficient entropy.

5 Performance of New 2-Round VSS Schemes

To summarize the asymptotic performance of new proposed 2-round VSS schemes and compare them with alternative constructions from the literature [BKP11], we refer to Table 1. Additionally, in this section, we evaluate the empirical performance of the proposed 2-round VSS schemes from Sections 4.1 and 4.2 through a prototype implementation in SageMath.[1] Furthermore, we conduct an efficiency comparison with the state-of-the-art alternatives proposed by Backes, Kate, and Patra in [BKP11, Sections 3.2 and 3.5].

We conducted our experiments using the SHA256 hash function for both commitment and random oracle, on a MacBook Pro. The laptop features an 8-Core Intel Core i9 processor with a base frequency of 2.30GHz and 16GB of memory. All protocol rounds were executed in single-thread mode. Our implementation results for various parameter sets are summarized in Table 2.

Table 2: Implementation results of 2-round VSS schemes of Backes, Kate, and Patra [BKP11], and our constructions from Sections 4.1 and 4.2. n: Number of parties, t: Threshold value, R1: Round 1, R2: Round 2, D: Dealer, P_i: Party i, BC: Broadcast Communication, PVC: Private Communication, $|\mathbb{Z}_q| = |\mathcal{H}| = 256$ bits.

(n, t)	Metrics	[BKP11, Fig. 3]		Section 4.1		[BKP11, Fig. 1]		Section 4.2	
		R1	R2	R1	R2	R1	R2	R1	R2
(32, 15)	D's Time	0.1 s	0.42 s	0.58 s	0.42 s	1.49 s	0.01 s	2.0 ms	0.2 ms
	P_i's Time	13 ms	14 ms	13 ms	11 ms	1.0 ms	1.0 ms	0.03 ms	0.1 ms
	D's BC	2.46 KB		3.45 KB		95 KB		2.47 KB	
	D's PVC	1.96 KB		1.96 KB		63 KB		0.98 KB	
	P_i's BC	63.78 B		63.75 B		2 KB		32 B	
	P_i's PVC	126 B		126 B		3.93 KB		63 B	
(64, 31)	D's Time	0.21 s	0.84 s	0.63 s	0.82 s	19.27 s	50 ms	5 ms	0.6 ms
	P_i's Time	13 ms	21 ms	13 ms	10 ms	2 ms	2.6 ms	0.03 ms	0.1 ms
	D's BC	4.88 KB		6.84 KB		377 KB		4.91 KB	
	D's PVC	3.89 KB		3.89 KB		249 KB		1.94 KB	
	P_i's BC	63.5 B		63.5 B		4 KB		32 B	
	P_i's PVC	124.5 B		124.5 B		7.78 KB		62.25 B	
(128, 63)	D's Time	0.43 s	1.69 s	1.32 s	1.66 s	352 s	190 ms	0.016 s	1 ms
	P_i's Time	13 ms	49 ms	13 ms	12 ms	4.5 ms	8.7 ms	0.03 ms	0.2 ms
	D's BC	9.79 KB		13.73 KB		1512 KB		9.85 KB	
	D's PVC	7.81 KB		7.81 KB		1000 KB		3.9 KB	
	P_i's BC	63.5 B		63.5 B		8 KB		32 B	
	P_i's PVC	125 B		125 B		15.62 KB		62.5 B	
(256, 127)	D's Time	0.92 s	3.43 s	2.66 s	3.36 s	7176 s	3 ms	59 ms	2 ms
	P_i's Time	13 ms	0.14 s	13 ms	0.014 s	8.5 ms	27.1 ms	0.3 ms	0.4 ms
	D's BC	19.57 KB		27.42 KB		6048 KB		19.71 KB	
	D's PVC	15.62 KB		15.62 KB		4000 KB		7.81 KB	
	P_i's BC	63.1 B		63.1 B		16 KB		32 B	
	P_i's PVC	125 B		125 B		31.25 KB		62.5 B	
(2048, 1023)	D's Time	9.85 s	28.08 s	23.97 s	27.74 s	− s	− s	2.99 s	19 ms
	P_i's Time	13 ms	3.09 s	13 ms	0.04 s	− s	− s	0.4 ms	3 ms
	D's BC	157.81 KB		221.12 KB		389120 KB		158.5 KB	
	D's PVC	126 KB		126 KB		258048 KB		63 KB	
	P_i's BC	63.62 B		63.62 B		128 KB		32 B	
	P_i's PVC	126 B		126 B		252 KB		63 B	

Upon comparing the implementation outcomes of the protocols, it is evident that the new hash-based 2-round VSS scheme demonstrates a significant acceleration across all metrics. Notably, it achieves running times that are more than 120000× faster compared to the alternative scheme of BKP [BKP11] for $(n, t) = (256, 127)$. Similarly, regarding

[1] Our implementation code is publicly available on https://github.com/KULeuven-COSIC/2R-Pi-VSS and https://github.com/Baghery/VSS-2Round-Pi.

communication costs, the new scheme requires considerably shorter broadcast and private communications from the dealer and the parties. Specifically, the new scheme demands significantly less data broadcast and private communication from the dealer and parties, amounting to respectively 182× and 512× less compared to 1× in the BKP scheme [BKP11, Section 3.2], again for $(n, t) = (256, 127)$.

By comparing the implementation outcomes of the VSS schemes from Sec. 4.1 and BKP [BKP11, Fig. 3], we see that our scheme has considerably more efficient verification. Notably, it achieves verification times that are 10× and 77× faster in comparison to the BKP [BKP11, Fig. 3] scheme for the parameter pairs (n, t) equal to $(256, 127)$ and $(2048, 1023)$, respectively. In terms of communication costs, the scheme from Sec. 4.1 demands a slightly larger data broadcast from the dealer, amounting to 1.4× compared to 1× in BKP [BKP11, Fig. 3] scheme.

6 Conclusion

We introduced **2R-Π**, a novel variant of the recently proposed unified framework **Π** [Bag25], facilitating the construction of round-optimal and practical computational VSS schemes based on Shamir secret sharing in the honest-majority setting.

Using this new framework, we addressed a crucial gap in constructing round-optimal computational VSS schemes, initially highlighted by Backes, Kate, and Patra (BKP) in ASIACRYPT 2011 [BKP11]. Specifically, we presented the first round-optimal VSS scheme based on any (non-homomorphic) commitment scheme, boasting $O(n)$ computational cost and $O(n\lambda)$ broadcast and private communications. Compared to the state-of-the-art alternative construction [BKP11, Sec. 3.2], our scheme demonstrates a factor of n improvement in both computation and communication costs.

Additionally, we introduced a novel 2-round VSS scheme based on homomorphic commitment schemes, surpassing the alternative scheme proposed in [BKP11, Sec. 3.5] notably in verification and reconstruction phases. Practical implementation results corroborate the effectiveness of these new round-optimal VSS schemes, showcasing significant speed-ups and communication reductions compared to existing hash-based round-optimal VSS schemes.

In conclusion, our contributions propel the state-of-the-art in round-optimal computational VSS schemes, providing more efficient solutions. The efficiency and simplicity of these new round-optimal VSS schemes render them invaluable tools for various classic and post-quantum secure threshold protocols, such as distributed key generation protocols and threshold signature schemes.

Acknowledgments

We thank the anonymous reviewers for their helpful comments and suggestions that improved the quality of this paper. This work was supported by the Flemish Government through the Cybersecurity Research Program with grant number VOEWICS02.

References

[ABCP23] Shahla Atapoor, Karim Baghery, Daniele Cozzo, and Robi Pedersen. VSS from distributed ZK proofs and applications. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part I*, volume 14438 of *LNCS*, pages 405–440. Springer, Singapore, December 2023. doi:10.1007/978-981-99-8721-4_13.

[Bag25] Karim Baghery. Π: A unified framework for computational verifiable secret sharing. In Tibor Jager and Jiaxin Pan, editors, *PKC 2025, Part IV*, volume

15677 of *LNCS*, pages 110–142. Springer, Cham, May 2025. doi:10.1007/978-3-031-91829-2_4.

[BBC+19] Dan Boneh, Elette Boyle, Henry Corrigan-Gibbs, Niv Gilboa, and Yuval Ishai. Zero-knowledge proofs on secret-shared data via fully linear PCPs. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part III*, volume 11694 of *LNCS*, pages 67–97. Springer, Cham, August 2019. doi:10.1007/978-3-030-26954-8_3.

[BG18] Jonathan Bootle and Jens Groth. Efficient batch zero-knowledge arguments for low degree polynomials. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018, Part II*, volume 10770 of *LNCS*, pages 561–588. Springer, Cham, March 2018. doi:10.1007/978-3-319-76581-5_19.

[BGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *20th ACM STOC*, pages 1–10. ACM Press, May 1988. doi:10.1145/62212.62213.

[BKNR25] Karim Baghery, Noah Knapen, Georgio Nicolas, and Mahdi Rahimi. Preconstructed publicly verifiable secret sharing and applications. In Marc Fischlin and Veelasha Moonsamy, editors, *Applied Cryptography and Network Security - 23st International Conference, ACNS 2025, Munich, Germany, June 23-27, 2025, Proceedings*, volume 13906 of *Lecture Notes in Computer Science*, pages 89–119. Springer, 2025. doi:10.1007/978-3-031-95761-1_4.

[BKP11] Michael Backes, Aniket Kate, and Arpita Patra. Computational verifiable secret sharing revisited. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 590–609. Springer, Berlin, Heidelberg, December 2011. doi:10.1007/978-3-642-25385-0_32.

[CCG24] Ignacio Cascudo, Daniele Cozzo, and Emanuele Giunta. Verifiable secret sharing from symmetric key cryptography with improved optimistic complexity. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part VII*, volume 15490 of *LNCS*, pages 100–128. Springer, Singapore, December 2024. doi:10.1007/978-981-96-0941-3_4.

[CD17] Ignacio Cascudo and Bernardo David. SCRAPE: Scalable randomness attested by public entities. In Dieter Gollmann, Atsuko Miyaji, and Hiroaki Kikuchi, editors, *ACNS 2017*, volume 10355 of *LNCS*, pages 537–556. Springer, Cham, July 2017. doi:10.1007/978-3-319-61204-1_27.

[CD20] Ignacio Cascudo and Bernardo David. ALBATROSS: Publicly AttestabLe BATched Randomness based On Secret Sharing. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part III*, volume 12493 of *LNCS*, pages 311–341. Springer, Cham, December 2020. doi:10.1007/978-3-030-64840-4_11.

[CGMA85] Benny Chor, Shafi Goldwasser, Silvio Micali, and Baruch Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults (extended abstract). In *26th FOCS*, pages 383–395. IEEE Computer Society Press, October 1985. doi:10.1109/SFCS.1985.64.

[Fel87] Paul Feldman. A practical scheme for non-interactive verifiable secret sharing. In *28th FOCS*, pages 427–437. IEEE Computer Society Press, October 1987. doi:10.1109/SFCS.1987.4.

[GHL22] Craig Gentry, Shai Halevi, and Vadim Lyubashevsky. Practical non-interactive publicly verifiable secret sharing with thousands of parties. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part I*, volume 13275 of *LNCS*, pages 458–487. Springer, Cham, May / June 2022. doi:10.1007/978-3-031-06944-4_16.

[GIKR01] Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. The round complexity of verifiable secret sharing and secure multicast. In *33rd ACM STOC*, pages 580–589. ACM Press, July 2001. doi:10.1145/380752.380853.

[Gro21] Jens Groth. Non-interactive distributed key generation and key resharing. Cryptology ePrint Archive, Report 2021/339, 2021. URL: https://eprint.iacr.org/2021/339.

[GRR98] Rosario Gennaro, Michael O. Rabin, and Tal Rabin. Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. In Brian A. Coan and Yehuda Afek, editors, *17th ACM PODC*, pages 101–111. ACM, June / July 1998. doi:10.1145/277697.277716.

[Ped92] Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 129–140. Springer, Berlin, Heidelberg, August 1992. doi:10.1007/3-540-46766-1_9.

[Sch99] Berry Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 148–164. Springer, Berlin, Heidelberg, August 1999. doi:10.1007/3-540-48405-1_10.

[Sha79] Adi Shamir. How to share a secret. *Communications of the Association for Computing Machinery*, 22(11):612–613, November 1979. doi:10.1145/359168.359176.

[SS24] Victor Shoup and Nigel P. Smart. Lightweight asynchronous verifiable secret sharing with optimal resilience. *J. Cryptol.*, 37(3):27, 2024. doi:10.1007/S00145-024-09505-6.