

A Plausible Attack on the Adaptive Security of Threshold Schnorr Signatures

Elizabeth Crites and Alistair Stewart

Web3 Foundation
firstname@web3.foundation

Abstract. The standard notion of security for threshold signature schemes is static security, where the set of corrupt parties is assumed to be fixed before protocol execution. In this model, the adversary may corrupt up to $t - 1$ out of a threshold of t parties. A stronger notion of security for threshold signatures considers an adaptive adversary, who may corrupt parties dynamically based on its view of the protocol execution, learning the corrupted parties' secret keys as well as their states. Adaptive security of threshold signatures has become an active area of research recently due to ongoing standardization efforts. Of particular interest is *full* adaptive security, the analogue of static security, where the adversary may adaptively corrupt a full $t - 1$ parties.

We present a plausible attack on the full adaptive security of threshold Schnorr signature schemes with public key shares of the form $pk_i = g^{sk_i}$, where all secret keys sk_i lie on a polynomial. We show that a wide range of threshold Schnorr signature schemes, including all variants of FROST, Sparkle, and Lindell'22, cannot be proven fully adaptively secure without modifications or assuming the hardness of a search problem that we define in this work. We then prove a generalization that extends below $t - 1$ adaptive corruptions.

1 Introduction

Some of the most destructive attacks in threshold cryptography in recent years were the so-called ROS attacks [11, 25] (Random inhomogeneities in a Overdetermined Solvable system of linear equations). The ROS problem was first stated in the original paper on Schnorr signatures [47]. The attacks fundamentally rely on concurrency, where an adversary may gain an advantage in forging a signature by opening many signing sessions in parallel and interleaving protocol messages from different sessions. A wide range of threshold, blind, and multi-signature schemes were broken in the concurrent setting by ROS attacks [41, 31, 48, 44, 2, 52, 54, 32].

The ROS_ℓ problem, parameterized by an integer ℓ , is a search problem to find $\ell + 1$ vectors $\boldsymbol{\rho}_i = (\rho_{i,j})_{j=1}^\ell$ such that the following system of $\ell + 1$ linear equations in unknowns c_1, \dots, c_ℓ in \mathbb{Z}_p has a solution, where $H_{\text{ROS}} : (\mathbb{Z}_p)^\ell \rightarrow \mathbb{Z}_p$ is a random oracle: $\sum_{j=1}^\ell \rho_{i,j} c_j = H_{\text{ROS}}(\boldsymbol{\rho}_i)$, $i \in \{1, \dots, \ell + 1\}$. In the context of multi-party

Schnorr signatures,¹ ROS attacks amount to an adversary searching for a solution to the ROS problem and outputting a forgery that is a linear combination of the other parties' signature contributions. Many increasingly effective ROS attacks have been demonstrated since the original cryptanalysis of Schnorr [47, 53, 43, 25, 11, 35], with the most recent [35] showing a polynomial-time attack for ℓ greater than $0.725 \log(p)$ (e.g., ≈ 190) concurrent sessions, rendering the aforementioned schemes insecure for a modest number of concurrent sessions easily mounted by a real-world attacker.

The Problem P. In this work, we define a search problem P and show a concrete, efficient attack if P is easy to solve.

Definition 1. *P is the following search problem. Given $\mathbf{v} \in \mathbb{Z}_p^t$ and $\mathbf{k}_1, \dots, \mathbf{k}_n \in \mathbb{Z}_p^t$, find a set $F \subset \{1, \dots, n\}$ with $|F| = f$ such that $\mathbf{v} \in \text{span}(\{\mathbf{k}_i\}_{i \in F})$ if one exists.*

In the context of threshold signatures, p is the prime order of the group, n is the number of parties, t is the threshold required to issue a signature, and f is the corruption threshold, up to $f = t - 1$. As in cryptographic assumptions like the discrete logarithm problem, the problem P will not be hard for some parameters, for example small p .

Similar to the ROS problem, the problem P does not rely on group elements or operations; it relies on field elements alone. The ROS problem, however, relies on a random oracle. The problem P is not stated in terms of, for example, a group with hard discrete logarithm, or with random oracles.

We give an attack against a large class of threshold Schnorr signature schemes, given access to an oracle to solve P that, for an arbitrary vector $\mathbf{v} \in \mathbb{Z}_p^t$, returns a subset $F \subset \{1, \dots, n\}$ of size f such that $\mathbf{v} \in \text{span}(\{\mathbf{k}_i\}_{i \in F})$, if such a subset exists. Our attack demonstrates that any proof of full adaptive security ($f = t - 1$) must imply that P is not solvable in polynomial time. We then prove a generalization that extends below $f = t - 1$ adaptive corruptions.

The Attack. Similar to ROS, we demonstrate an attack where the forgery amounts to a linear combination of parties' public values. Uniquely, our attack allows a forgery *based on public key shares alone* - no partial signatures are required. Unlike ROS attacks, the attack works even for a single signing session.

Our attack applies to any scheme satisfying the following three properties:

1. Public key shares pk_1, \dots, pk_n are public.
2. Public keys are $pk = g^{q(0)}, pk_1 = g^{q(1)}, \dots, pk_n = g^{q(n)}$, where q is a degree $t - 1$ polynomial with coefficients in \mathbb{Z}_p .
3. The threshold signature is compatible with Schnorr verification (Definition 2).

Condition 1 does not require public key shares to be output as a result of key generation. Concealing public key shares naively is not a viable solution to avoid

¹ Recall that a (single-party) Schnorr signature, defined over a prime-order group, is a pair (R, z) such that $g^z = R \cdot pk^c$, where $c = \text{Hash}(R, pk, m)$.

assuming the problem P is hard for many natural schemes [38, 24, 39], which reveal the public key share of a signer through a single partial signature issued by them. Thus, modifications to the protocol itself would need to be made to avoid this assumption.

Condition 2 is not overly restrictive and applies to many protocols, especially those implemented in practice (e.g., BLS [12, 5] and ECDSA [30, 17]). Public keys of this form are used to efficiently verify the correctness of each party’s contribution to the signature, so that a misbehaving party can be identified and removed (i.e., to achieve identifiable abort [38, 46]).

Condition 3 is not specific to Schnorr signatures. EdDSA signatures, a deterministic version of Schnorr signatures, are not verifiably deterministic, so our results apply. Any scheme compatible with the single-party Schnorr verification algorithm is susceptible to our attack.

We now give an overview of the core ideas in the attack. To issue a Schnorr signature, it is necessary to provide the discrete logarithm of $R \cdot pk^c$. If the adversary is able to express this as a combination of f public key shares, then it can corrupt those f parties, and obtain the discrete logarithm with the combination of f secret key shares. First, pk is a combination of public key shares. The adversary chooses R as a random combination of public key shares and uses this fact to get $R \cdot pk^c$ as a combination of public key shares. The chance that this is a combination of a particular f parties’ keys is small, since the protocol is secure against static corruption, indeed $1/p$ or less. But there are many, $\binom{n}{f}$ combinations of parties to corrupt, which means that the probability that there is some sparse combination of shares that gives $R \cdot pk^c$ can be significant. However, the large number of combinations means that the adversary cannot brute force the set to corrupt even if one would work. An oracle for the problem P would allow them to find the sparse combination when one exists and thus the set of parties to corrupt, resulting in a successful forgery.

Impact of Our Results. Our results have far-reaching implications for threshold cryptography, both theoretically and practically.

Consider that, until recently, there were only three digital signature schemes standardized by NIST: RSA, ECDSA, and EdDSA. NIST recently published a draft Call for Multi-Party Threshold Schemes [13, 14], emphasizing a strong preference for schemes achieving provable adaptive security. The Call specifies two categories of schemes; Class N is the main category of interest, which considers schemes that are compatible with single-party verification of NIST-standardized signatures. This important design goal has motivated an extensive line of work on multi-party signatures achieving compatibility with single-party EdDSA/Schnorr verification [3, 42, 38, 24, 39, 40, 9, 46, 10, 6, 37]. Many have seen widespread adoption in practice, and some, e.g., FROST, are already the subject of standardization efforts [20].

Now consider that most threshold signature schemes are proven in the static corruption model, where an adversary is assumed to control up to $t - 1$ out of a threshold of t parties, but does not corrupt any parties during protocol execution. In the adaptive corruption model, an adversary has the added capability of

corrupting parties based on observing some of the protocol execution. *Full* adaptive security is of particular interest, as it matches the corruption profile of static security, allowing an adversary to corrupt $t - 1$ parties dynamically. There is sometimes a presumption that the lack of an adaptive security proof does not imply complete failure of basic security properties in the presence of an adaptive adversary. However, any such failure could have catastrophic consequences, for example, a complete loss of funds in cryptocurrency wallets. NIST [13] states, “Given the possibility of adaptive corruptions in the real world, it is important to consider for any proposed threshold signature scheme whether the major safety properties of interest (such as unforgeability) are safeguarded against such an adversary.”

Our results have two striking implications:

1. If the problem P is easy, all of the schemes meeting the stated conditions are statically secure but not adaptively secure. This would be the first such separation for any natural protocol, solving a long-standing open problem in multi-party computation.² Moreover, it would apply to a large class of schemes and would hold even in the strongest idealized models (e.g., the algebraic group model (AGM) and the generic group model (GGM)).
2. The full adaptive security of these schemes cannot be proven without an assumption that implies the hardness of some instances of P . Such an assumption would likely go beyond assumptions about the group and random oracles since P is not defined in terms of them.³ Moreover, this extends to corruption thresholds below $f = t - 1$.

One natural question is: Why not assume the problem P is hard for showing *security*? As in ROS, it is dangerous to assume this problem is hard.

The NIST Call specifies several parameter regimes of interest, with $n = 1024$ and $f = t - 1$ being the highest level of security. Considering modest to large n is important in practical applications where identifiable abort falls short, and guaranteed output delivery is required [46, 10, 6]. Moreover, for small n , there are straightforward ways to turn statically secure schemes into adaptively secure ones via a simple guessing argument.

Quantitatively, we show the impact of our attack in Table 1, giving the probability of the attack succeeding for different parameter regimes with $p \approx 2^{252}$ (e.g., Ed25519). An entry of 0.0 indicates that our attack succeeds with probability $2^{-0} = 1$. For probabilities under 2^{-126} , it would be better to attack the discrete logarithm problem. These probabilities are for one call to an oracle to solve P and for one random oracle query. So, for example, without assuming P is hard and

² Protocols have been concocted for the express purpose of demonstrating a separation, cf. [16, 15], but, to the best of our knowledge, no separation has been shown for a natural protocol.

³ This is true even if P is NP-hard, as the instances of P in the average case that are used in the attack would need to be NP-hard. See Section 7 for a discussion of the hardness of P .

(n, t)	$f = t - 1$	$f = t - 2$	$f = t - 3$	$f = t - 4$
(64,43)	195.84	446.97	698.2	949.52
(128,86)	137.87	388.92	640.02	891.17
(196,131)	75.41	326.45	577.53	828.64
(512,342)	0.0	37.25	288.28	539.32
(768,513)	0.0	0.0	53.8	304.82
(1024,683)	0.0	0.0	0.0	69.29

Table 1. The probability that our attack succeeds is 2^{-x} for x given in the table, with $p \approx 2^{252}$, where x is computed as in Theorem 2. Here, n is the total number of potential signers, t is the threshold, and f is the corruption threshold.

only assuming a bound on the number of random oracle queries, a modest 131 out of 196 parties and a $2^{-75.41}$ probability of attack is insecure, corresponding to the number of hashes all the Bitcoin miners in the world can compute in roughly one minute.

2 Impact of the Attack

2.1 Schemes Affected by the Attack

The following schemes are susceptible to our attack.

FROST, FROST2, FROST3. FROST [38, 7] and its variants FROST2 [24, 7] and FROST3 [46, 19] are state-of-the-art protocols for threshold Schnorr signing that are currently undergoing standardization efforts, including a recent RFC through the IETF [20]. All three variants are two-round protocols consisting of one online signing round and one preprocessing round. All three are secure in the static corruption setting under the one-more-discrete logarithm assumption (OMDL)⁴ in the ROM.

SimpleTSig. SimpleTSig [24] is a three-round threshold Schnorr signature scheme that follows a commit-reveal approach and allows for one round of preprocessing. Its static security holds under the security of the (single-party) Schnorr signature scheme, which itself holds under the discrete logarithm assumption (DL) in the ROM [44, 27].

Sparkle, Sparkle+. Sparkle and Sparkle+ [23] are adaptations of SimpleTSig that are secure against adaptive corruptions. Sparkle is fully three rounds, and Sparkle+ allows preprocessing, but requires an additional plain signature (or authenticated channels). Static security holds under the DL assumption in the

⁴ The OMDL assumption states: Given $q + 1$ challenge group elements (X_0, \dots, X_q) (in addition to the generator g) and q -time access to a discrete logarithm solution oracle, compute x_i such that $X_i = g^{x_i}$ for all $i \in [0..q]$.

ROM. Adaptive security for up to $(t-1)/2$ corruptions has been proven under the algebraic one-more discrete logarithm assumption (AOMDL)⁵ in the ROM. Our results show that the full adaptive security of Sparkle and Sparkle+ [24], claimed under AOMDL in the AGM and ROM, cannot hold without an assumption that implies the hardness of some instances of the problem P.

Lindell’22. Lindell’22 [39] is a three-round, commit-reveal protocol that is proven to UC-realize a Schnorr signing functionality in the hybrid model where the following functionalities exist: a multiparty broadcast commitment functionality and a zero-knowledge functionality. Security is proven in the static corruption model.

Classic S. Classic Schnorr [40] is a three-round, commit-reveal protocol that is proven to UC-realize the threshold signature functionality in [17] in the global random oracle model, assuming the hardness of the DL problem. Adaptive security is shown using the guessing argument.

ROAST. ROAST [46] is a wrapper protocol for FROST, which has $\mathcal{O}(n)$ round complexity and achieves robustness (i.e., guaranteed output delivery). FROST has the property of identifiable abort, where a party issuing malformed protocol messages can be identified and removed, and the protocol rerun. However, such a procedure is impractical beyond small numbers of parties. ROAST, therefore, offers an alternative to FROST for large n . Its static security has been shown under the OMDL assumption in the ROM.

SPRINT. SPRINT [10] is another robust threshold Schnorr signature scheme, with 3 broadcast rounds, which is proven statically secure under the DL assumption in the ROM. Its security is argued with a restriction on concurrency, but results in [50] suggest general concurrency does hold.

HARTS. HARTS [6] is a robust threshold Schnorr scheme with $\mathcal{O}(1)$ round complexity that has been proven adaptively secure for up to $(t-1)/2$ corruptions under the OMDL assumption in the AGM and ROM. It requires secure erasure of secret state for its zero-knowledge proofs. Our results apply even to schemes relying on secure erasures.

GJKR. GJKR [31] is a robust threshold Schnorr signing protocol, with 3 broadcast rounds, proven statically secure assuming the security of single-party Schnorr signatures. It is insecure in the concurrent setting due to ROS attacks.

Stinson-Strobl. Stinson-Strobl [51] is, to the best of our knowledge, the first threshold Schnorr signature scheme proposed in the literature. It achieves robustness, and its static security reduces to the security of single-party Schnorr signatures.

⁵ The AOMDL assumption is the same as OMDL, except any discrete logarithm solution oracle query must include an algebraic representation in terms of the challenge group elements and generator g . This makes the oracle polynomial time and therefore AOMDL a falsifiable assumption.

Arctic. Arctic [37] is a two-round deterministic threshold Schnorr signature scheme proven statically secure under the DL assumption in the ROM.

GKMN. GKMN [29] is a three-round deterministic Schnorr signature scheme proven to UC-realize an n -party Schnorr signing functionality, in the presence of an adversary statically corrupting up to $n - 1$ parties, in the hybrid model where the following functionalities exist: a deterministic nonce derivation functionality and a committed zero-knowledge proof-of-knowledge for discrete logarithm functionality.

Remark 1 (Key Generation). Our results hold for the above schemes when implemented with trusted key generation or any distributed key generation (DKG) protocol revealing public key shares of the appropriate form. However, even if public key shares are suppressed at the key generation phase, most of the above protocols anyway expose public key shares during signing. All of these combinations are susceptible to our attack.

2.2 Schemes Unaffected by the Attack

Non-Schnorr Threshold Signatures. Our results do not immediately apply to schemes not compatible with single-party Schnorr verification. However, it is an interesting open question whether a similar search problem could be defined, and shown necessary, for adaptive security of schemes with a similar structure, for example those derived by applying the Fiat-Shamir transform [26] to other identification schemes.

Crackle & Snap, FROST-Mask. Crackle & Snap [36] are five-round stateless and four-round stateful threshold Schnorr protocols, respectively, which are obtained by applying a masking technique to Sparkle. Both schemes are proven fully adaptively secure under the DL assumption in the ROM. Uniquely, the security of these protocols critically relies on public key shares never being revealed, even through signing, and therefore they do not achieve identifiable abort. As we will see, this is precisely what is needed to avoid our attack. However, without identifiable abort, Crackle & Snap are impractical except for small numbers of parties. FROST-Mask [18] takes the same technical approach, applying the masking technique of [36] to FROST to obtain 3-round stateless and 2-round stateful schemes.

Abe-Fehr, Zero S., Glacius. One general approach for achieving adaptive security is to output public key shares that are not perfectly binding commitments to secret keys, allowing the reduction to equivocate on the secret keys as needed. Abe-Fehr [1], Zero S. [40], and Glacius [4] all follow this line of reasoning. Indeed, our attack does not work if public key shares, for example, are Pedersen commitments $pk_i = g^{sk_i} h^{r_i}$.

3 Related Work

Prior work [22] proves a series of impossibility results on the adaptive security of threshold signature schemes, including those compatible with Schnorr signature verification. Specifically, one result rules out adaptive security for more than $t/2$ corruptions for threshold Schnorr signatures that satisfy a property called key-uniqueness. An example of a key-unique scheme is one for which public keys are perfectly binding commitments to secret keys, e.g., $pk_i = g^{sk_i}$ as in our work. This result rules out adaptive security above $t/2$ corruptions under the OMDL and AOMDL assumptions in the programmable ROM, following the standard rewinding argument for Schnorr signatures. In the case that the problem P is easy, our results rule out t adaptive corruptions as well some values below $t - 1$, with rewinding and programming or not, under any hardness assumption. Furthermore, if P is easy, our work rules out adaptive security in strong idealized models: in the AGM and even in the GGM. However, we emphasize that whether P is easy or not remains an open question. Interestingly, the metareductions in [22] and our attack are based on public key shares alone - not even one partial signature is needed. The results in [22] extend beyond threshold Schnorr signatures, ruling out adaptive security for more than $t/2$ corruptions under any non-interactive computational assumption for a wide range of threshold signature schemes and a natural class of reductions.

Follow-up work [21] shows a positive result about the adaptive security of FROST (and its variants), and builds on the techniques of our work. FROST is proven adaptively secure for up to $t/2$ corruptions in the ROM only under the AOMDL assumption, and adaptively secure above $t/2$ corruptions additionally in the AGM and assuming the hardness of the low-dimensional vector representation (LDVR) problem. The LDVR problem specializes the problem P, and is proven to be both sufficient and necessary for proving the adaptive security of FROST. The hardness of P and LDVR remains an intriguing open question.

4 Preliminaries

Let $\lambda \in \mathbb{N}$ denote the security parameter and 1^λ its unary representation. A function $\nu : \mathbb{N} \rightarrow \mathbb{R}$ is called *negligible* if for all $c \in \mathbb{R}, c > 0$, there exists $k_0 \in \mathbb{N}$ such that $|\nu(k)| < \frac{1}{k^c}$ for all $k \in \mathbb{N}, k \geq k_0$. For a non-empty set S , let $x \leftarrow^s S$ denote sampling an element of S uniformly at random and assigning it to x . We use $[n]$ to represent the set $\{1, \dots, n\}$ and $[0..n]$ to represent the set $\{0, \dots, n\}$. We represent vectors as $\mathbf{a} = (a_1, \dots)$.

Let PPT denote probabilistic polynomial time. Algorithms are randomized unless explicitly noted otherwise. Let $y \leftarrow A(x; \rho)$ denote running algorithm A on input x and randomness ρ and assigning its output to y . Let $y \leftarrow^s A(x)$ denote $y \leftarrow A(x; \rho)$ for a uniformly random ρ . The set of values that have non-zero probability of being output by A on input x is denoted by $[A(x)]$.

Group Generation. Let GROUPGEN be a polynomial-time algorithm that takes as input a security parameter 1^λ and outputs a group description (\mathbb{G}, p, g)

consisting of a group \mathbb{G} of order p , where p is a λ -bit prime, and a generator g of \mathbb{G} .

Random Oracle Model (ROM) [8]. The random oracle model is an idealized model that treats a hash function Hash as an oracle in the following way. When queried on an input in the domain of Hash , the oracle first checks if it has an entry stored in its table for this input. If so, it returns this value. If not, it samples an output in the codomain of Hash uniformly at random, stores the input-output pair in its table, and returns the output.

Definition 2 (Schnorr Signatures [47]). *The Schnorr signature scheme consists of efficient algorithms (SETUP, KEYGEN, SIGN, VERIFY), defined as follows:*

- $\text{SETUP}(1^\lambda) \rightarrow \text{par}$: On input a security parameter 1^λ , run $(\mathbb{G}, p, g) \leftarrow \text{GROUPGEN}(1^\lambda)$ and select a hash function $\text{Hash} : \{0, 1\}^* \rightarrow \mathbb{Z}_p$. Output public parameters $\text{par} \leftarrow ((\mathbb{G}, p, g), \text{Hash})$ (which are given implicitly as input to all other algorithms).
- $\text{KEYGEN}() \rightarrow (pk, sk)$: Sample a secret key $sk \leftarrow_{\$} \mathbb{Z}_p$ and compute the public key as $pk \leftarrow g^{sk}$. Output key pair (pk, sk) .
- $\text{SIGN}(sk, m) \rightarrow \sigma$: On input a secret key sk and a message m , sample a nonce $r \leftarrow_{\$} \mathbb{Z}_p$. Then, compute a nonce commitment $R \leftarrow g^r$, $c \leftarrow \text{Hash}(R, pk, m)$, and $z \leftarrow r + csk$. Output a signature $\sigma \leftarrow (R, z)$.
- $\text{VERIFY}(pk, m, \sigma) \rightarrow 0/1$: On input a public key pk , a message m , and a purported signature $\sigma = (R, z)$, compute $c \leftarrow \text{Hash}(R, pk, m)$ and output 1 (accept) if $R \cdot pk^c = g^z$; else, output 0 (reject).

Schnorr signatures have been proven secure under the discrete logarithm (DL) assumption in the ROM [44]. Their tight security has been proven under DL in the AGM and ROM [27].

Remark 2. Our attack also applies the variant of Schnorr signatures where the signature is (c, z) .

Polynomial Interpolation. A polynomial $q(Z) = x_0 + x_1Z + x_2Z^2 + \dots + x_{t-1}Z^{t-1}$ of degree $t-1$ over a field \mathbb{F} can be interpolated by t points. Let $\eta \subseteq [n]$ be the list of t distinct indices corresponding to the x -coordinates $z_i \in \mathbb{F}, i \in \eta$, of these points. Then the Lagrange polynomial $L_i(Z)$ has the form:

$$L_i(Z) = \prod_{j \in \eta; j \neq i} \frac{Z - z_j}{z_i - z_j}$$

Given a set of t points $(z_i, q(z_i))_{i \in [t]}$, any point $q(z_\ell)$ on the polynomial f can be determined by Lagrange interpolation as follows:

$$q(z_\ell) = \sum_{k \in \eta} q(z_k) \cdot L_k(z_\ell)$$

Definition 3 (Shamir Secret Sharing [49]). *Shamir secret sharing is a t -out-of- n secret sharing scheme over a field \mathbb{F} that consists of efficient algorithms (SS.SHARE, SS.RECOVER), defined as follows:*

- SS.SHARE(sk, n, t) $\rightarrow \{(z_i, sk_i), \dots, (z_n, sk_n)\}$: *On input a secret sk , number of participants n , and threshold t , sample coefficients $x_1, \dots, x_{t-1} \leftarrow^* \mathbb{F}$ and define the polynomial $q(Z) = sk + x_1 Z + x_2 Z^2 + \dots + x_{t-1} Z^{t-1}$. Choose arbitrary non-zero points z_1, \dots, z_n in \mathbb{F} . (These could, for example, be participant indices $1, \dots, n$.) For $i \in [n]$, compute $sk_i = q(z_i)$. Output shares $\{(z_i, sk_i)\}_{i \in [n]}$.*
- SS.RECOVER($t, \{(z_i, sk_i)\}_{i \in \mathcal{S}}$) $\rightarrow \perp / sk$: *On input threshold t and a set of shares $\{(z_i, sk_i)\}_{i \in \mathcal{S}}$, output \perp if $\mathcal{S} \not\subseteq [n]$ or $|\mathcal{S}| < t$. Otherwise, recover sk by polynomial interpolation:*

$$sk \leftarrow \sum_{i \in \mathcal{S}} \lambda_i^{\mathcal{S}} sk_i$$

where the Lagrange coefficient for the set \mathcal{S} is:

$$\lambda_i^{\mathcal{S}} = L_i(0) = \prod_{j \in \mathcal{S}, j \neq i} \frac{-z_j}{z_i - z_j}$$

Definition 4 (Vandermonde Matrix). *We define the Vandermonde matrix $V(z_1, \dots, z_t)$ for the $t \geq 1$ numbers $z_1, \dots, z_t \in \mathbb{Z}_p$ as:*

$$V(z_1, \dots, z_t) := \begin{pmatrix} 1 & z_1 & z_1^2 & \dots & z_1^{t-1} \\ 1 & z_2 & z_2^2 & \dots & z_2^{t-1} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 1 & z_t & z_t^2 & \dots & z_t^{t-1} \end{pmatrix}$$

which is invertible if and only if the z_i are pairwise distinct.

Definition 5 (Cantelli's Inequality). *Let X be a real-valued random variable. Let $a > 0$ and let $\text{Var}(X)$ be the variance of X . Then:*

$$\Pr[X - E(X) \geq a] \leq \frac{\text{Var}[X]}{\text{Var}[X] + a^2}$$

where $E(X)$ is the expected value of X . Applying the above to $-X$ gives:

$$\Pr[X - E(X) \leq -a] \leq \frac{\text{Var}[X]}{\text{Var}[X] + a^2}.$$

4.1 Threshold Signatures

We begin with the definition of a threshold signature scheme given in [23]. The definition is for a generic signing protocol with r rounds, as threshold Schnorr signature schemes in the literature consist of two or more signing rounds. Key generation is given as an algorithm, but may be replaced by a distributed key generation (DKG) protocol.

Definition 6 (Threshold signature scheme). A threshold signature scheme TS whose signing protocol consists of r rounds is a tuple of the following algorithms $\text{TS} = (\text{SETUP}, \text{KEYGEN}, (\text{SIGN}_1, \dots, \text{SIGN}_r), \text{COMBINE}, \text{VERIFY})$, defined as follows:

- $\text{SETUP}(1^\lambda) \rightarrow \text{par}$: Takes as input a security parameter and outputs public parameters par (which are given implicitly as input to all other algorithms).
- $\text{KEYGEN}(n, t) \rightarrow (pk, \{sk_i\}_{i \in [n]})$: A probabilistic algorithm that takes as input the number of signers n and the threshold t and outputs the public key pk and secret key shares $\{sk_i\}_{i \in [n]}$, which are sent to each party privately.
- $(\text{SIGN}_1, \dots, \text{SIGN}_r) \rightarrow \{pm_{1,i}, \dots, pm_{r,i}\}_{i \in \mathcal{S}}$: A set of signing algorithms executed by each party in a signing set $\mathcal{S} \subseteq [n], |\mathcal{S}| \geq t$, on a message m :

$$\begin{aligned} (pm_{1,i}, st_{1,i}) &\leftarrow \text{SIGN}_1(i, sk_i, \mathcal{S}, m) \\ (pm_{2,i}, st_{2,i}) &\leftarrow \text{SIGN}_2(st_{1,i}, \mathcal{PM}_1) \\ &\dots \\ pm_{r,i} &\leftarrow \text{SIGN}_r(st_{r-1,i}, \mathcal{PM}_{r-1}) \end{aligned}$$

Here, $pm_{j,i}$ is the protocol message sent by party $i \in \mathcal{S}$ in round j , $st_{j,i}$ is the state of party i in round j , and $\mathcal{PM}_j = \{pm_{j,i}\}_{i \in \mathcal{S}}$ is a set of protocol messages sent in round j .

- $\text{COMBINE}(\mathcal{S}, m, \mathcal{PM}_1, \mathcal{PM}_2, \dots, \mathcal{PM}_r) \rightarrow (m, \sigma)$: A deterministic algorithm that takes as input the signing set \mathcal{S} , the message m , and a set of protocol messages $\mathcal{PM}_1, \mathcal{PM}_2, \dots, \mathcal{PM}_r$ and outputs a signature σ .
- $\text{VERIFY}(pk, m, \sigma) \rightarrow 0/1$: A deterministic algorithm that takes as input the public key pk , a message m , and a purported signature σ and outputs 1 (accept), or 0 (reject).

Correctness of TS. A threshold signature scheme is *correct* if for all security parameters $\lambda \in \mathbb{N}$, all $\text{par} \in [\text{SETUP}(1^\lambda)]$, all $(pk, \{sk_i\}_{i \in [n]}) \in [\text{KEYGEN}(n, t)]$, all $\mathcal{S} \subseteq [n]$ such that $|\mathcal{S}| \geq t$, and all messages m , we have:

$$\Pr[\text{VERIFY}(pk, m, \sigma) = 1 \mid \sigma \leftarrow \text{TSIGNHON}(pk, \{sk_i\}_{i \in [n]}, \mathcal{S}, m)] = 1$$

where the algorithm TSIGNHON is as defined in Fig. 1.

Remark 3. The COMBINE algorithm may be executed by one of the signers or an external party, typically a coordinator.

Remark 4. The signing set \mathcal{S} , message m , and secret key share sk_i are given as input in the first round of signing; however, for some schemes, this is deferred until the second round to allow preprocessing [38, 24, 7, 46, 19].

$\text{TSIGNHON}(pk, \{sk_i\}_{i \in [S]}, \mathcal{S}, m)$
return \perp if $\mathcal{S} \not\subseteq [n] \wedge \mathcal{S} < t$ for $k \in \mathcal{S}$ do $(pm_{1,k}, st_{1,k}) \leftarrow \text{SIGN}_1(k, sk_k, \mathcal{S}, m)$ for $k \in \mathcal{S}$ do $(pm_{2,k}, st_{2,k}) \leftarrow \text{SIGN}_2(st_{1,k}, \{pm_{1,i}\}_{i \in \mathcal{S}})$ \dots for $k \in \mathcal{S}$ do $pm_{r,k} \leftarrow \text{SIGN}_r(st_{r-1,k}, \{pm_{r-1,i}\}_{i \in \mathcal{S}})$ $\sigma \leftarrow \text{COMBINE}(\mathcal{S}, m, \{pm_{1,i}, \dots, pm_{r,i}\}_{i \in \mathcal{S}})$ return σ

Fig. 1. An algorithm TSIGNHON modeling an honest execution of the signing protocol.

4.2 Static and Adaptive Security

We next define static and adaptive security for threshold signatures, as specified by [23], in Fig. 2.

The adaptive unforgeability game takes as input the security parameter λ , the number of parties n , the threshold t , and the allowed number of corruptions f ($t - 1$ in the static and full adaptive settings). The challenger generates public parameters par and returns all parameters to the adversary \mathcal{A} . The adversary returns an initial set of corrupt parties \mathcal{C} (or the full set, in the case of static corruption), which must not exceed f , and the challenger sets the honest parties $\mathcal{H} \leftarrow [n] \setminus \mathcal{C}$. The challenger runs KEYGEN and returns pk and the set of corrupt secret keys $\{sk_j\}_{j \in \mathcal{C}}$ to \mathcal{A} . The adversary can then query signing oracles $\mathcal{O}^{\text{SIGN}_1, \dots, \text{SIGN}_r}$ for honest parties, and the challenger performs various checks to ensure each query is valid. The adversary may open concurrent signing sessions; each session is managed with a session ID sid . The adaptive unforgeability game includes a corruption oracle $\mathcal{O}^{\text{CORRUPT}}$, which returns the secret key and state of the selected party across all signing sessions. The adversary wins the game if it can produce a valid forgery $\sigma^* = (R^*, z^*)$ with respect to public key pk on a message m^* that has not been queried to a signing oracle.

Definition 7 (Static Security). *Let the advantage of an adversary \mathcal{A} playing the static security game $\text{Game}_{\mathcal{A}, \text{TS}}^{UF}(\lambda, n, t, f)$ for $f = t - 1$, as defined in Figure 2, be as follows:*

$$\text{Adv}_{\mathcal{A}, \text{TS}}^{UF}(\lambda, n, t, f) = \Pr[\text{Game}_{\mathcal{A}, \text{TS}}^{UF}(\lambda, n, t, f) = 1]$$

A threshold signature scheme TS is statically secure if for all PPT adversaries \mathcal{A} , $\text{Adv}_{\mathcal{A}}^{UF}(\lambda, n, t, f)$ is negligible.

Definition 8 (Adaptive Security). *Let the advantage of an adversary \mathcal{A} playing the adaptive security game $\text{Game}_{\mathcal{A}, \text{TS}}^{adp-UF}(\lambda, n, t, f)$ for $f \leq t - 1$, as defined in Figure 2, be as follows:*

$$\text{Adv}_{\mathcal{A}, \text{TS}}^{adp-UF}(\lambda, n, t, f) = \Pr[\text{Game}_{\mathcal{A}, \text{TS}}^{adp-UF}(\lambda, n, t, f) = 1]$$

$\text{MAIN Game}_{\mathcal{A}, \text{TS}}^{\text{[adp]-UF}}(\lambda, n, t, f)$ <hr/> $\mathcal{ID}, Q_m \leftarrow \emptyset$ $par \leftarrow \text{SETUP}(1^\lambda)$ $(\mathcal{C}, \text{st}_{\mathcal{A}}) \leftarrow \mathcal{A}(par, n, t, f)$ return \perp if $\mathcal{C} \not\subseteq [n] \vee \mathcal{C} > f$ $\mathcal{H} \leftarrow [n] \setminus \mathcal{C}$ $(pk, \{sk_i\}_{i \in [n]}) \leftarrow \text{KEYGEN}(n, t)$ $\text{input} \leftarrow (pk, \{sk_j\}_{j \in \mathcal{C}}, \text{st}_{\mathcal{A}})$ $(m^*, \sigma^*) \leftarrow \mathcal{A}^{\text{SIGN}_1, \dots, \text{SIGN}_r, \text{[CORRUPT]}}(\text{input})$ return 1 if $m^* \notin Q_m$ $\wedge \text{VERIFY}(pk, m^*, \sigma^*) = 1$ return 0 $\text{Init}(sid, k, \mathcal{S}, m)$ <hr/> if $sid \notin \mathcal{ID}$ return \perp if $\mathcal{S} \not\subseteq [n] \vee \mathcal{S} < t$ $\vee k \notin \mathcal{H} \cap \mathcal{S}$ $\mathcal{ID} \leftarrow \mathcal{ID} \cup \{sid\}$ $\mathcal{S}[sid] \leftarrow \mathcal{S}; m[sid] \leftarrow m$ $Q_m \leftarrow Q_m \cup \{m[sid]\}$ return \perp if $k \notin \mathcal{H} \cap \mathcal{S}[sid]$ $\vee \text{rnd}[sid, k] \neq \perp$ return 1 <div style="border: 1px dashed black; padding: 5px;"> $\text{O}^{\text{CORRUPT}}(k)$ <hr/> return \perp if $k \notin \mathcal{H} \vee \mathcal{C} \geq f$ $\mathcal{C} \leftarrow \mathcal{C} \cup \{k\}$ $\mathcal{H} \leftarrow \mathcal{H} \setminus \{k\}$ return $(sk_k, \{\text{st}[sid', k]\}_{sid' \in \mathcal{ID}})$ </div>	$\text{O}^{\text{SIGN}_1}(sid, k, \mathcal{S}, m)$ <hr/> return \perp if $\perp \leftarrow \text{Init}(sid, k, \mathcal{S}, m)$ $(pm_1[sid, k], \text{st}_1[sid, k])$ $\leftarrow \text{SIGN}_1(k, sk_k, \mathcal{S}[sid], m[sid])$ $pm_{1,k} \leftarrow pm_1[sid, k]; \text{rnd}[sid, k] \leftarrow 1$ return $pm_{1,k}$ $\text{O}^{\text{SIGN}_2}(sid, k, \mathcal{PM}_1)$ <hr/> return \perp if $sid \notin \mathcal{ID}$ $\vee k \notin \mathcal{H} \cap \mathcal{S}[sid] \vee \text{rnd}[sid, k] \neq 1$ parse $\{pm_{1,i}\}_{i \in \mathcal{S}} \leftarrow \mathcal{PM}_1$ return \perp if $pm_{1,k} \neq pm_1[sid, k]$ $(pm_2[sid, k], \text{st}_2[sid, k])$ $\leftarrow \text{SIGN}_2(\text{st}_1[sid, k], \mathcal{PM}_1)$ $pm_{2,k} \leftarrow pm_2[sid, k]; \text{rnd}[sid, k] \leftarrow 2$ return $pm_{2,k}$ \vdots $\text{O}^{\text{SIGN}_r}(sid, k, \mathcal{PM}_{r-1})$ <hr/> return \perp if $sid \notin \mathcal{ID}$ $\vee k \notin \mathcal{H} \cap \mathcal{S}[sid] \vee \text{rnd}[sid, k] \neq r - 1$ parse $\{pm_{r-1,i}\}_{i \in \mathcal{S}} \leftarrow \mathcal{PM}_{r-1}$ return \perp if $pm_{r-1,k} \neq pm_{r-1}[sid, k]$ $pm_r[sid, k] \leftarrow \text{SIGN}_r(\text{st}_{r-1}[sid, k], \mathcal{PM}_{r-1})$ $pm_{r,k} \leftarrow pm_r[sid, k]; \text{rnd}[sid, k] \leftarrow r$ return $pm_{r,k}$
---	--

Fig. 2. Games defining the static and adaptive unforgeability of a threshold signature scheme with r signing rounds [23]. The static game contains all but the dashed boxes, and the adaptive game adds the dashed boxes. The public parameters par are implicitly given as input to all algorithms.

A threshold signature scheme TS is adaptively secure if for all PPT adversaries \mathcal{A} , $\text{Adv}_{\mathcal{A}, \text{TS}}^{\text{adp-UF}}(\lambda, n, t, f)$ is negligible.

Definition 9 (Full Adaptive Security). A threshold signature scheme TS achieves full adaptive security if the corruption threshold f in $\text{Game}_{\mathcal{A}, \text{TS}}^{\text{adp-UF}}(\lambda, n, t, f)$ is $f = t - 1$.

5 The Attack

We now present the main result of this work.

Our attack applies to protocols where the secret shares are generated as follows.

Definition 10 (Threshold Schnorr signature protocol with Shamir secret-shared key). We say a protocol is a threshold Schnorr signature protocol with Shamir secret-shared key if signature verification is compatible with Schnorr verification (Definition 2) and there exists a polynomial $q(Z)$ with coefficients in \mathbb{Z}_p such that:

- the public key for the threshold Schnorr signatures is $pk = g^{q(0)}$,
- each honest party i knows $sk_i = q(z_i)$ for some $z_i \in \mathbb{Z}_p$, and
- the points z_1, \dots, z_n are public.

Theorem 1. There is an adversary with an oracle to solve P that can forge using just the public key shares for any threshold Schnorr signature protocol with Shamir secret-shared key where the elements $pk_1 = g^{q(z_1)}, \dots, pk_n = g^{q(z_n)}$ are public. The adversary, which makes one random oracle query (or hash computation) and calls the oracle for P once, succeeds with probability at least $\frac{\binom{n}{t-1}}{p + \binom{n}{t-1}}$. In particular, it succeeds with probability at least $1/2$ when $\binom{n}{t-1} \geq p$.

If P is solvable in polynomial time, this rules out the full adaptive security of such schemes. Any proof of full adaptive security must imply that P is not solvable in polynomial time. Could there be a proof that only involves the hardness of group problems (e.g., DL, AOMDL), idealized models of groups (e.g., AGM, GGM), or a bound on the random oracle queries?

Note that the description of P does not involve the group or random oracles. For, say, an elliptic curve, the instance of P uses a different field than the arithmetic of the elliptic curve is defined and so we would not expect the hardness of P to be related to that of problems involving the specific group. However, if P is NP-hard, then its hardness would be implied by hardness of any NP problem, such as the discrete logarithm problem in a group with efficient operations. Even in this case, to prove full adaptive security without additional assumptions would require showing that the instances used in the attack are hard and that they are hard for a uniformly random \mathbf{v} . We discuss this further in Section 7.

Now, consider the points $X_0 = g^{x_0}, \dots, X_{t-1} = g^{x_{t-1}}$ where

$$q(Z) = x_0 + x_1 Z + x_2 Z^2 + \dots + x_{t-1} Z^{t-1}.$$

These points would be the Feldman VSS commitments for a trusted party who uses q . If each dealer in the DKG uses the Feldman VSS or a related VSS protocol that uses these commitments, then these could be computed from their commitments. Even if not, our assumptions suffice to compute them. While introducing the linear algebra needed to describe the setting, we will show below that:

Claim. Given pk_1, \dots, pk_n , it is possible to compute X_0, \dots, X_{t-1} and vice versa.

Schemes using the Feldman VSS commitments operate in the reverse direction to the claim. The dealer or DKG outputs $X_0 = g^{x_0}, \dots, X_{t-1} = g^{x_{t-1}}$. Any party $i \in \{1, \dots, n\}$ can verify their public key share as:

$$pk_i = \mathbf{K}_i^\top \mathbf{X}$$

where $\mathbf{X}^\top = (X_0, X_1, \dots, X_{t-1})$ and $\mathbf{K}_i^\top = (1, z_i, z_i^2, \dots, z_i^{t-1})$. In other words,

$$pk_i = X_0 X_1^{z_i} X_2^{z_i^2} \dots X_{t-1}^{z_i^{t-1}}$$

We will also take $pk = X_0$. We can define $\mathbf{K}_0^\top = (1, 0, \dots, 0)$ so that $pk = g^{q(0)} = \mathbf{K}_0^\top \mathbf{X}$.

Any set of t distinct indices $i_1, \dots, i_t \in \{0, 1, \dots, n\}$ have that $\mathbf{K}_{i_1}, \dots, \mathbf{K}_{i_t}$ form a basis of \mathbb{Z}_p^n . This is because they are the rows of the Vandermonde matrix of z_{i_1}, \dots, z_{i_t} (with the convention that $z_0 = 0$), which is non-singular when z_{i_1}, \dots, z_{i_t} are distinct (see Definition 4).

As a result of this, if X_0, X_1, \dots, X_{t-1} are not public, but $pk, pk_1, pk_2, \dots, pk_n$ are, then the former can be computed from any t of the latter by solving a non-singular linear system of equations. We have now shown both directions of the claim.

Proof. (of Theorem 1) Consider the following attack. The adversary's goal in the adaptive security game (Fig. 2) is to adaptively corrupt, based on its view of the protocol execution, a maximum of $f = t - 1$ honest parties, receiving their secret keys sk_i , and to produce a forgery. In particular, the forgery $(m^*, \sigma^* = (R^*, z^*))$ must be such that no honest party has ever signed m^* , and σ^* must pass Schnorr signature verification (see Definition 2):

$$R^* \cdot pk^{c^*} = g^{z^*}$$

where $c^* = \text{Hash}(R^*, pk, m^*)$. In order to forge, the adversary sets R^* as:

$$R^* = \boldsymbol{\alpha}^\top \mathbf{X} = X_0^{\alpha_0} X_1^{\alpha_1} \dots X_t^{\alpha_t} \quad (1)$$

for some uniformly random $\alpha_0, \alpha_1, \dots, \alpha_t \leftarrow \mathbb{Z}_p$. Then, since $X_0 = pk$, we have:

$$R^* \cdot pk^{c^*} = X_0^{\alpha_0 + c^*} X_1^{\alpha_1} \dots X_t^{\alpha_t} = (\boldsymbol{\alpha} + c^* \mathbf{K}_0)^\top \mathbf{X}$$

The adversary tries to find $t - 1$ public keys $pk_{j_1}, pk_{j_2}, \dots, pk_{j_{t-1}}$ and some $\mu_{j_1}, \mu_{j_2}, \dots, \mu_{j_{t-1}} \in \mathbb{Z}_p$ such that:

$$\alpha + c^* K_0 = \sum_{i=1}^{t-1} \mu_{j_i} K_{j_i}$$

and so

$$R^* \cdot pk^{c^*} = pk_{j_1}^{\mu_{j_1}} pk_{j_2}^{\mu_{j_2}} \dots pk_{j_{t-1}}^{\mu_{j_{t-1}}}.$$

Given j_1, \dots, j_{t-1} for which there is a solution to the above, it is possible to compute $\mu_{j_1}, \mu_{j_2}, \dots, \mu_{j_{t-1}}$ as follows: since $K_{j_1}, \dots, K_{j_f}, K_0$ is a basis, using the Vandermonde matrix, it is possible to compute $\mu_{j_1}, \mu_{j_2}, \dots, \mu_{j_{t-1}}, \mu_0$ with

$$\alpha + c^* K_0 = \mu_0 K_0 + \sum_{i=1}^{t-1} \mu_{j_i} K_{j_i}.$$

Since this is a basis, $\mu_{j_1}, \mu_{j_2}, \dots, \mu_{j_{t-1}}, \mu_0$ is unique. If $\mu_0 \neq 0$, then there is no solution; otherwise, the equation above holds.

There are $\binom{n}{t-1}$ possible sets of $t - 1$ parties. If the adversary can find such a set F of $t - 1$ signers, then they can corrupt j_1, j_2, \dots, j_{t-1} to obtain $sk_{j_1}, sk_{j_2}, \dots, sk_{j_{t-1}}$ and set $z^* = \mu_{j_1} sk_{j_1} + \mu_{j_2} sk_{j_2} + \dots + \mu_{j_{t-1}} sk_{j_{t-1}}$.

First, we need to show under what circumstances such an F of $f = t - 1$ signers exists. For any set of $t - 1$ signers F , we define $H_F = span(\{K_j\}_{j \in F})$. We need that:

Lemma 1. H_F is a $t - 1$ dimensional subspace of \mathbb{Z}_p^t . For any distinct sets of $t - 1$ signers F, F' , $H_F \cap H_{F'}$ is a $t - 2$ dimensional subspace of \mathbb{Z}_p^t .

Proof. (of Lemma 1) $\{K_j\}_{j \in F}$ are linearly independent, as $\{K_j\}_{j \in F} \cup K_{j'}$ forms a basis for any $j' \notin F$. So $\dim H_F = |\{K_j\}_{j \in F}| = t - 1$.

Given $F' \neq F$, there is a $j' \in F' \setminus F$, and $\{K_j\}_{j \in F} \cup K_{j'}$ forms a basis and so is linearly independent. So $K_{j'} \notin span(\{K_j\}_{j \in F}) = H_F$. Thus H_F and $H_{F'}$ are distinct hyperplanes and so their intersection has $t - 2$ dimensions. \square

Now, note that $\alpha + c^* K_0$ is distributed uniformly at random from the p^t points in \mathbb{Z}_p^t . Thus, we have that $\Pr[\alpha + c^* K_0 \in H_F] = p^{t-1}/p^t = 1/p$ and $\Pr[\alpha + c^* K_0 \in H_F \cap H_{F'}] = p^{t-2}/p^t = 1/p^2$.

Now let X_F be the indicator variable that is 1 when $\alpha + c^* K_0 \in H_F$ and 0 otherwise. Then X_F is distributed as *Bernoulli*($1/p$) and for distinct F, F' ,

$$\begin{aligned} Cov(X_F, X_{F'}) &= E[(X_F - E[X_F])(X_{F'} - E[X_{F'}])] \\ &= E[X_F X_{F'} - E[X_F]E[X_{F'}]] = 1/p^2 - 1/p^2 = 0. \end{aligned}$$

Let \mathcal{F} be the set of all sets of f signers. Now let $X = \sum_{F \in \mathcal{F}} X_F$.

$$E[X] = \sum_{F \in \mathcal{F}} E[X_F] = \binom{n}{t-1} / p.$$

$$\begin{aligned}
\text{Var}[X] &= \sum_{F \in \mathcal{F}} \text{Var}[X_F] + \sum_{F, F' \in \mathcal{F}, F \neq F'} 2\text{Cov}(X_F, X_{F'}) \\
&= \binom{n}{t-1} (1/p)(1-1/p) + 0 \leq E[X].
\end{aligned}$$

Now if there is an $F \in \mathcal{F}$ with $\alpha + c^* \mathbf{K}_0 \in H_F$, then $X_F = 1$ and so $X > 0$. Conversely, if $X > 0$ then such an F must exist. Now we can use Cantelli's inequality (Definition 5) to obtain:

$$\Pr[X = 0] = \Pr[X \leq 0] = \Pr[X - E[X] \leq -E[X]] \leq \frac{\text{Var}[X]}{\text{Var}[X] + E[X]^2}$$

And so we have:

$$\begin{aligned}
\Pr[\exists F \in \mathcal{F} : \alpha + c^* \mathbf{K}_0 \in H_F] &= \Pr[X > 0] \\
&\geq 1 - \frac{\text{Var}[X]}{\text{Var}[X] + E[X]^2} \\
&= \frac{E[X]^2}{\text{Var}[X] + E[X]^2} \\
&\geq \frac{E[X]^2}{E[X] + E[X]^2} \\
&= \frac{E[X]}{1 + E[X]} \\
&= \frac{\binom{n}{t-1}}{p + \binom{n}{t-1}}
\end{aligned}$$

This is at least $1/2$ for $\binom{n}{t-1} \geq p$.

With an oracle for solving P, the adversary can find a set F of $t-1$ parties to corrupt to create a forgery with probability at least $\frac{\binom{n}{t-1}}{p + \binom{n}{t-1}}$ as required. \square

Remark 5. We note that there are additional assumptions that we could have added to Definition 1 that might make it easier to solve but which were omitted for a clean statement. For example, we could require that any t of the \mathbf{k}_i are linearly independent. Indeed, we explore this particular assumption in Section 7.

Remark 6. In Equation 1, we only considered a random α to simplify the analysis. It may be possible that an adversary that does not choose α at random can achieve a higher probability of success or obtain an instance of P that has a special form for which there is an efficient algorithm to solve.

6 Extension to when f is smaller than $t-1$

In the previous section, we considered the case where the adversary is allowed to adaptively corrupt a full $f = t-1$ out of a threshold of t parties. We now show a generalization of this result to lower corruption thresholds.

Theorem 2. *There is an adversary with an oracle to solve P that can forge using just the public key shares for any threshold Schnorr signature protocol with Shamir secret-shared key where the elements $pk_1 = g^{q(z_1)}, \dots, pk_n = g^{q(z_n)}$ are public. Assuming that for some security parameter λ , $nt \leq 2^\lambda$ and $p \geq 2^{2\lambda}$, the adversary, who makes one random oracle query and one call to the oracle for P, succeeds with probability at least $\frac{\binom{n}{f}}{p^{t-f}(1+O(2^{-\lambda})) + \binom{n}{f}}$. If additionally, we assume $\binom{n}{f} \geq p^{t-f}(1+O(2^{-\lambda}))$, then the adversary succeeds with probability at least $1/2$.*

The two assumptions $nt \leq 2^\lambda$ and $p \geq 2^{2\lambda}$ are made to simplify the statement where $O(2^{-\lambda})$ hides terms which are negligible. We note that many protocols have time complexity $\Omega(nt)$, such as DKGs where all parties secret share or identifiably abort, and 2^λ is unfeasible complexity. The choice $p \geq 2^{2\lambda}$ is required because of attacks on the discrete logarithm problem in groups of order p that have time complexity \sqrt{p} , such as Pollard's rho algorithm.

Following the same line of reasoning as in the proof of Theorem 1, we can consider α as living in the vector space that is the dual to the space of polynomials of degree at most $t-1$. For any polynomial of degree at most $t-1$, $p(x)$, we write \mathbf{p} for its vector of coefficients in \mathbb{Z}_p^t . For any set $S \subset \{0, 1, \dots, n\}$ of signers (and possibly 0), we define the vanishing polynomial $v_S(x)$ as $v_S(x) = \prod_{i \in S} x - z_i$.

Lemma 2. *H_F is an f -dimensional subspace of \mathbb{Z}_p^t . Its annihilator, the subspace H_F^\perp of degree at most $t-1$ polynomials $p(x)$ with $\mathbf{X}^T \mathbf{p} = 0$ for all $X \in H_F$, $p \in H_F^\perp$, consists of the span of $v_F(x), xv_F(x), \dots, x^{t-1-f}v_F(x)$. For any distinct sets of $t-1$ signers F, F' , $H_F \cap H_{F'}$ is a $2f - \min\{t, |F \cup F'|\}$ -dimensional subspace of \mathbb{Z}_p^t .*

Proof. (of Lemma 2) H_F is the span of \mathbf{K}_i for $i \in F$. A polynomial p has $\mathbf{X}^T \mathbf{p}$ for all $X \in H_F$ if and only if $\mathbf{K}_i^T \mathbf{p} = p(z_i)$ is 0 for all $i \in F$. Thus, $p(x) = q(x)v_F(x)$ for some polynomial $q(x)$ of degree at most $t-1 - \deg v_F = t-1-f$. This subspace of polynomials H_F^\perp is spanned by $v_F(x), xv_F(x), \dots, x^{t-1-f}v_F(x)$, which has dimension $t-f$.

Now $H_F \cap H_{F'}$ is a subspace whose annihilator is $H_F^\perp + H_{F'}^\perp$, which is the span of $v_F(x), xv_F(x), \dots, x^{t-1-f}v_F(x), v_{F'}(x), xv_{F'}(x), \dots, x^{t-1-f}v_{F'}(x)$. This set need not be linearly independent. If they are, then $\dim H_F^\perp + H_{F'}^\perp = 2f$ and so $\dim H_F \cap H_{F'} = 2f - t$. Otherwise, the dimension of $H_F^\perp + H_{F'}^\perp$ is reduced by the dimension of the space of linear combinations of $v_F(x), xv_F(x), \dots, x^{t-1-f}v_F(x), v_{F'}(x), xv_{F'}(x), \dots, x^{t-1-f}v_{F'}(x)$ that give the zero polynomial. Such a linear combination can be written as $q(x)v_F(x) + r(x)v_{F'}(x)$ for polynomials q, r of degree at most $t-1-f$.

If $q(x)v_F(x) + r(x)v_{F'}(x) = 0$, then $q(z_i)v_F(z_i) + r(z_i)v_{F'}(z_i) = 0$ for all $i \in F \cup F'$. Thus $q(z_i) = 0$ for all $i \in F' \setminus F$ and so $v_{F' \setminus F}(x)$ divides $q(x)$. Similarly, $v_{F \setminus F'}(x)$ divides $r(x)$. Now both terms $q(z_i)v_F(z_i)$ and $r(z_i)v_{F'}(z_i) = 0$ divide $v_{F \cup F'}(x) = v_{F' \setminus F}(x)v_F(x) = v_{F \setminus F'}(x)v_{F'}(x)$ and so the linear combination is of the form $s(x)v_{F' \setminus F}(x)v_F(x) - s(x)v_{F \setminus F'}(x)v_{F'}(x)$ for some polynomial $s(x)$ of degree at most $t-1 - \deg v_{F \setminus F'}(x) = t-1 - |F \cup F'|$.

If $t - 1 - |F \cup F'| < 0$, then there are no such linear combinations. In this case, $\dim H_F^\perp + H_{F'}^\perp = 2f$. Otherwise, the space of linear combinations has the same dimension as that of polynomials of degree at most $t - 1 - |F \cup F'|$, that is $t - |F \cup F'|$. In this case, $\dim H_F^\perp + H_{F'}^\perp = 2f - t + |F \cup F'|$. Thus, the dimension of the subspace for which this is the annihilator $H_F \cap H_{F'}$ is $2f - \min\{t, |F \cup F'|\}$. \square

Again, let X_F be the indicator variable that is 1 when $\alpha + c^* \mathbf{K}_0 \in H_F$ and 0 otherwise. $\alpha + c^* \mathbf{K}_0$ is a uniformly random point and so $\Pr[X_F = 1] = 1/p^{t - \dim H_F} = 1/p^{t-f}$, i.e., X_F is distributed as *Bernoulli*($1/p^{t-f}$).

Now for $F, F' \in \mathcal{F}$,

$$E[X_F X_{F'}] = \Pr[X_F = 1 \wedge X_{F'} = 1] = 1/p^{t - \dim H_F \cap H_{F'}} = 1/p^{t + \min\{t, |F \cup F'|\} - 2f}.$$

For any F , how many F' have $E[X_F X_{F'}] = 1/p^{t-f-k}$? For $k = 0$, there is just one F' , $F' = F$ because that needs $|F \cup F'| = f = |F|$. For $0 < k < t - f$, $|F \cup F'| = f + k$ and so $|F \setminus F'| = |F' \setminus F| = k$. There are $\binom{f}{k}$ possible sets of k parties to remove from F and then $\binom{n-f}{k}$ possible sets of k parties to add to get F' . This results in $\binom{f}{k} \binom{n-f}{k}$ values of F' . Finally, for $k = t - f$, $|F \setminus F'| \geq k$, which is all other F' that have $E[X_F X_{F'}] = p^{2(t-f)}$.

So for $X = \sum_{F \in \mathcal{F}} X_F$, we have $E[X] = \binom{n}{f} 1/p^{t-f}$,

$$\begin{aligned} \text{Var}[X] &= E[X^2 - E[X]^2] = \sum_{F, F'} E[X_F X_{F'} - 1/p^{2(t-f)}] \\ &= \binom{n}{f} \sum_{k=0}^{t-f-1} \binom{f}{k} \binom{n-f}{k} (1/p^{t-f-k} - 1/p^{2(t-f)}) \end{aligned}$$

Here the $k = t - f$ term is a multiple of $1/p^{2(t-f)} - 1/p^{2(t-f)} = 0$. Note that the ratio of the k term to the $k + 1$ term is $(f - k)(n - f - k)/p(k + 1)^2 \leq nt/p$. Now in our regime, this is negligibly small. Concretely, in terms of a security parameter λ , we will assume that $nt \leq 2^\lambda$ and $p \geq 2^{2\lambda}$. Now we have $nt/p \leq 2^{-\lambda}$ and so the expression of $\text{Var}[X]$ is dominated by the $k = 0$ term $\binom{n}{f}/p^{t-f} = E[X]$. So we have $\text{Var}[X] = E[X](1 + O(2^{-\lambda}))$.

Using Cantelli's inequality (Definition 5), we have

$$\begin{aligned} \Pr[\exists F \in \mathcal{F} : \alpha + c^* \mathbf{K}_0 \in H_F] &= \Pr[X > 0] \\ &\geq 1 - \frac{\text{Var}[X]}{\text{Var}[X] + E[X]^2} \\ &= \frac{E[X]^2}{\text{Var}[X] + E[X]^2} \\ &\geq \frac{E[X]^2}{E[X](1 + O(2^{-\lambda})) + E[X]^2} \\ &= \frac{E[X]}{1 + O(2^{-\lambda}) + E[X]} \end{aligned}$$

$$= \frac{\binom{n}{f}}{p^{t-f}(1 + O(2^{-\lambda})) + \binom{n}{f}}$$

So when $\binom{n}{f} \geq (1 + O(2^{-\lambda}))p^{t-f}$, we have $E[X] \geq 1$ and that $\Pr[X > 0] \geq 1/2$.

So we have that if α is chosen at uniformly at random from \mathbb{Z}_p^t , the probability that $\alpha + c^* \mathbf{K}_0 \in H_F$ for some $F \in \mathcal{F}$ is at least $1/(2 - O(2^{-\lambda}))$. Now the adversary proceeds in a similar way to the one from Theorem 1. They choose α uniformly at random, then compute R^* as in Equation 1, query or compute $c^* = \text{Hash}(R^*, pk, m^*)$ and query their oracle for P to find F with $|F| = f$ and $\alpha + c^* \mathbf{K}_0 \in H_F$. If the oracle returns such an F , the adversary corrupts parties in F to learn sk_i for $i \in F$. Then, it solves a linear system to find $\mu_{j_1}, \mu_{j_2}, \dots, \mu_{j_f}$ with $\alpha + c^* \mathbf{K}_0 = \sum_{i=1}^f \mu_{j_i} \mathbf{K}_{j_i}$, so (R^*, z^*) with $z^* = \sum_{i=0}^f \mu_{j_i} sk_{j_i}$ satisfies $R^* \cdot pk^{c^*} = g^{z^*}$ and is a forgery. This occurs with probability at least $\frac{\binom{n}{f}}{p^{t-f}(1 + O(2^{-\lambda})) + \binom{n}{f}}$, as required. \square

7 Is the Problem P Hard?

We show in Theorem 3 that the instances of the problem P the attack uses are related to the bounded distance decoding of Reed-Solomon codes [45] (Section 7.1). Decoding of Reed-Solomon codes is a classical, well-studied problem. It is therefore perhaps surprising that, in the parameter ranges for which the attack applies, we do not know whether the corresponding Reed-Solomon code problem, and therefore P, is hard or whether the instances the attack uses are easy. Here, we state what is known about this problem and speculate about what this means for the hardness of P.

The relevant Reed-Solomon codes have length n and dimension $k = n - t$, i.e., they are evaluations of polynomials of degree $n - t - 1$. We consider f errors for f corruptions. This Reed-Solomon code would be uniquely decodable up to $k/2$ errors, corresponding to the $f \leq (t - 1)/2$ corruption regime. With more errors than this, Reed-Solomon codes are list-decodable, where an algorithm can output a list of all words in the code with at most f differences. However, the region where our attack applies with $\binom{n}{f} \geq p^{t-f} = p^{n-k-f}$ corresponds roughly to the list decoding capacity bound (cf. Theorem 7.4.1 of [33]), above which the average list size (which appears as $E[X]$ in the proof above) becomes exponentially large. Consequently, in this region, list decoding cannot be polynomial time, as the output is not polynomial sized. However, the problem of bounded distance decoding – returning one out of the possibly many codewords within f if one exists – might still be feasible in this region. Bounded distance decoding, indeed list decoding, is known to be feasible up the Johnson bound of $n(n-f) \geq kn = n(n-t)$. It is an open question whether it is feasible beyond this bound. (Open Question 12.2.1 of [33] is this for list decoding.)

So, might bounded distance decoding of Reed-Solomon codes, and therefore the problem P, be hard in our parameter region? Indeed, there are hardness results in the literature for our parameters n, k, f . The bounded distance decoding

is shown to be NP-hard in [34] for $n - k - f = 1$, corresponding to $f = t - 1$, which was extended to slightly lower f in [28]. It has also been shown to be hard for discrete log in an extension field for the region of our attack $\binom{n}{f} \geq p^{n-k-f}$. However, none of these results apply to the fields typically used in Schnorr signatures, i.e. cryptographically large prime fields, but not exponentially large in n for which the attack would not apply. The reduction in [34] applies to binary fields. [28] used fields which are exponentially large in n . The bounded distance decoding result in [28] only applies to the domain being the entire field, which requires a smaller field. It is possible that some modification of these results applies.

However, these hardness reductions use a structured codeword for the input to the problem. Our attack actually uses an input vector \mathbf{v} chosen uniformly at random. This can be translated to a uniformly random input codeword for Reed-Solomon decoding. So, even if P is hard, including NP-hard, it is possible that this average case is easy.

Even if the average case is not easy, we do not know of a reduction strategy from the literature that is likely to apply to a random input. Without such a reduction, a new assumption, beyond group-related assumptions and the ROM, would still be required to show full adaptive security of threshold Schnorr signature schemes.

7.1 Connection to Reed-Solomon Codes

A linear code C of length n and dimension k over an alphabet of size q , where q is a prime power, is a k -dimensional subspace of \mathbb{Z}_q^n . The Hamming distance $d_H(\mathbf{u}, \mathbf{v})$ between two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_q^n$ is defined as the number of non-zero coordinates of the vector $\mathbf{u} - \mathbf{v}$.

Definition 11 (Bounded Distance Decoding). *Bounded distance decoding for a code C and distance f is the following problem: Given $\mathbf{u} \in \mathbb{Z}_q^n$, find $\mathbf{v} \in C$ such that $d_H(\mathbf{u}, \mathbf{v}) \leq f$ provided such a \mathbf{v} exists.*

The linear codes we are particularly interested in are Reed-Solomon codes. For an enumerated domain $\mathbf{z} \in \mathbb{Z}_q^n$ with no duplicate coordinates, i.e., $z_i \neq z_j$ for $i \neq j$, we define $RS(\mathbb{Z}_q, \mathbf{z}, k)$ containing codewords \mathbf{v} of the form $v_i = v(z_i)$ for some polynomial $v(x)$ of degree at most $k - 1$.

Theorem 3. *For any $\mathbf{K}_1, \dots, \mathbf{K}_n \in \mathbb{Z}_p^t$ such that any t are linearly independent, instances of P with these \mathbf{K}_i are equivalent to bounded distance decoding in a linear code C of length n and dimension $n - t$. For the special case $\mathbf{K}_i = (1, z_i, z_i^2, \dots, z_i^{t-1})$, P is equivalent to bounded distance decoding of $RS(\mathbb{Z}_p, \mathbf{z}, n - t)$.*

Proof. A parity-check matrix for a linear code C of length n and dimension k is an $(n - k) \times n$ matrix H such that the subspace C is the kernel of the linear transformation given by H , i.e., $H\mathbf{u} = \mathbf{0}$ if and only if $\mathbf{u} \in C$. For a codeword $\mathbf{u} \in \mathbb{Z}_q^n$, $H\mathbf{u} \in \mathbb{Z}_q^{n-k}$ is called the *syndrome* of \mathbf{u} .

Given an instance of P such that any t of the \mathbf{K}_i are linearly independent, we take H to be the $t \times n$ matrix whose i^{th} column is \mathbf{K}_i . Because any t of the \mathbf{K}_i are linearly independent, any $t \times t$ submatrix of H is non-singular and so H has rank t . Let C be the kernel of H , i.e., the subspace of \mathbb{Z}_p^n such that $H\mathbf{u} = 0$ if and only if $\mathbf{u} = 0$. By the rank-nullity theorem, this subspace has dimension $n - t$.

Lemma 3. *If $\mathbf{v} = H\mathbf{u}$, then for any $\mathbf{a} \in \mathbb{Z}_p^n$, the following are equivalent:*

- (i) $\mathbf{u} - \mathbf{a} \in C$,
- (ii) $\mathbf{v} = \sum_i a_i \mathbf{K}_i$.

Proof. (ii) is $\mathbf{v} = H\mathbf{a}$ and (i) is $H(\mathbf{u} - \mathbf{a}) = 0$ and so both are equivalent to $H\mathbf{u} = H\mathbf{a}$. \square

Such an \mathbf{a} that has at most f non-zero coordinates provides a solution to the bounded distance decoding problem for \mathbf{u} via (i) and a solution to P for \mathbf{v} via (ii).

Corollary 1. *If $\mathbf{v} = H\mathbf{u}$, then P has a solution for \mathbf{v} if and only if the bounded distance decoding problem has a solution for \mathbf{u} .*

Proof. If there exists an \mathbf{a} that has at most f non-zero coordinates that satisfies Lemma 3, then both have a solution; otherwise, neither have a solution. \square

Given an input vector $\mathbf{v} \in \mathbb{Z}_p^t$ for P , we can solve P using an oracle for bounded distance decoding for C as follows. First, find $\mathbf{u} \in \mathbb{Z}_p^n$ with $H\mathbf{u} = \mathbf{v}$. This is an overdetermined linear system, but for any subset $T \subset \{1, \dots, n\}$ with $|T| = t$, the submatrix of H , H_T , of columns with indices from T is non-singular; indeed, its columns are \mathbf{K}_i for $i \in T$, which were assumed to be linearly independent. Then, using $H_T^{-1}\mathbf{v}$, we can find a vector \mathbf{u} with non-zero entries only in T with $H\mathbf{u} = \mathbf{v}$. Now apply the oracle for bounded distance decoding to \mathbf{u} . If it returns \mathbf{c} , then let $F \subset \{1, \dots, n\}$ be the set of non-zero entries in $\mathbf{u} - \mathbf{c}$, and so there are a_i such that $\mathbf{u} - \mathbf{c} = \sum_i a_i \mathbf{e}_i$. By Lemma 3, $\mathbf{v} = \sum_i a_i \mathbf{K}_i$ and we return this solution. If there were no solutions, then by Corollary 1, we can return that there are no solutions.

Given an input vector $\mathbf{u} \in \mathbb{Z}_p^t$ for the bounded distance decoding problem for C , we can solve bounded distance decoding using an oracle for P . Use the oracle for P on $H\mathbf{u}$. If it succeeds and outputs F, a_i with $\mathbf{v} = \sum_{i \in F} a_i \mathbf{K}_i$, then output $\mathbf{c} = \mathbf{u} - \sum_{i \in F} a_i \mathbf{e}_i \in C$ as a solution to bounded distance decoding. If P has no solutions for $H\mathbf{u}$, then by Corollary 1, the bounded distance decoding problem has no solutions.

This completes the proof for general \mathbf{K}_i such that any t are linearly independent. Now we consider $\mathbf{K}_i = (1, z_i, z_i^2, \dots, z_i^{t-1})$ for \mathbf{z} with distinct coordinates. As mentioned previously, any t of these are linearly independent. Indeed, for any $T \subset \{1, \dots, n\}$ of size $|T| = t$, the submatrix H_T of columns with indices from T and so columns \mathbf{K}_i is a Vandermonde matrix and therefore non-singular.

The code C obtained as above for these \mathbf{K}_i is not quite a Reed-Solomon code. In fact it is a *generalized Reed-Solomon code* obtained by scaling Reed-Solomon codewords pointwise.

We will first give explicitly the vector $\mathbf{w} \in \mathbb{Z}_p^n$ of scaling and its key property and then show how this is related to our codes.

Lemma 4. *Let $\mathbf{w} \in \mathbb{Z}_p^n$ be defined by $w_i = 1/v'_z(z_i)$, where $v'_z(z)$ is the formal derivative of the vanishing polynomial $v_z(z) = \prod_i (z - z_i)$. Then, for any polynomial $p(x)$ of degree at most $n - 1$, the coefficient of x^{n-1} in $p(x)$ is $\sum_i w_i p(z_i)$.*

Proof. Consider the Lagrange interpolation formula for any polynomial $p(x)$ (see Section 4): $p(x) = \sum_i p(z_i) v_z(x)/v'_z(z_i)(x - z_i) = \sum_i w_i p(z_i) v_z(x)/(x - z_i)$. Now, the x^{n-1} coefficient of $v_z(x)/(x - z_i)$ is 1 and so taking the x^{n-1} coefficient of this expression for $p(x)$ gives $\sum_i w_i p(z_i)$. \square

Next, we show how this vector relates to the Reed-Solomon code.

Lemma 5. *$\mathbf{u} \in RS(\mathbb{Z}_p, \mathbf{z}, n - t)$ if and only if $\sum_i u_i w_i z_i^j = 0$ for all $0 \leq j \leq t - 1$.*

Proof. Let $u(x)$ be the polynomial of degree at most $n - 1$ with $u_i = u(z_i)$ for all $1 \leq i \leq n$. By Lemma 4, if $u(x)$ has degree at most $n - j - 1$, then $\sum_i u_i w_i z_i^j$ is the x^{n-1} coefficient of $u(x)x^j$ and so also the coefficient of x^{n-j-1} in $u(x)$.

Suppose that $\mathbf{u} \in RS(\mathbb{Z}_p, \mathbf{z}, n - t)$. Then $\deg u(x) \leq n - t$. For each $0 \leq j \leq t - 1$, $u(x)$ has degree at most $n - j - 1$ and x^{n-j-1} coefficient 0 and so $\sum_i u_i w_i z_i^j = 0$.

Now, suppose that $\sum_i u_i w_i z_i^j = 0$ for all $0 \leq j \leq t - 1$. If $u(x)$ has degree at most $n - j - 1$, then the coefficient of x^{n-j-1} in $u(x)$ is 0 and so it has degree at most $n - j - 2$. It has degree at most $n - 1$, so by induction, it has degree at most $n - t - 1$. Thus, we have $\mathbf{u} \in RS(\mathbb{Z}_p, \mathbf{z}, n - t)$. \square

Now consider the rows of H . The j^{th} column of H is $\mathbf{K}_j = \{1, z_j, \dots, z_j^n\}$. So, we have $H_{ij} = z_j^i$ and that the i^{th} row of H is $(z_1^{i-1}, z_2^{i-1}, \dots, z_n^{i-1})$. Thus, we have the following corollary.

Corollary 2. *$\mathbf{u} \in RS(\mathbb{Z}_p, \mathbf{z}, n - t)$ if and only if \mathbf{u}' with $u'_i = u_i w_i$ has $\mathbf{u}' \in C$.*

Proof. $\mathbf{u}' \in C$ is equivalent to $H\mathbf{u}' = \mathbf{0}$ and so $\sum_i u'_i z_i^j = 0$ for all $0 \leq j \leq t - 1$. By Lemma 5, this is equivalent to $\mathbf{u} \in RS(\mathbb{Z}_p, \mathbf{z}, n - t)$. \square

The equivalence between bounded distance decoding in the two codes is obtained by multiplying or dividing the inputs by \mathbf{w} pointwise. Concretely, we have shown the correctness of this reduction from P to bounded distance decoding of $RS(\mathbb{Z}_p, \mathbf{z}, n - t)$:

1. Find \mathbf{u} with $\mathbf{v} = H\mathbf{u}$ by taking any $T \subset [n]$ with $|T| = t$ and letting $\mathbf{u}_T = (V(\mathbf{z}_T)^T)^{-1}\mathbf{v}$ and $v_i = 0$ for $i \notin T$. Here, V is the Vandermonde matrix and $\mathbf{u}_T, \mathbf{z}_T$ refer to the vectors \mathbf{u}, \mathbf{z} , respectively, which have coordinates in T .

2. Compute \mathbf{w}' , \mathbf{w} with $w'_i = v'_z(z_i) = \prod_{j \neq i} (z_i - z_j)$ and $w_i = 1/w'_i$.
3. Use the bounded distance to Reed-Solomon decoding oracle on $Diag(\mathbf{w}')\mathbf{u}$, where $Diag$ is the diagonal matrix operator, with $RS(\mathbb{Z}_p, \mathbf{z}, n-t)$ and distance f .
4. If the oracle returns $c \in RS(\mathbb{Z}_p, \mathbf{z}, n-t)$ with $d_H(Diag(\mathbf{w}')\mathbf{u}, \mathbf{c}) \leq f$, then return $\mathbf{u} - Diag(\mathbf{w})\mathbf{c}$.

This concludes the proof of Theorem 3. \square

References

- [1] M. Abe and S. Fehr. “Adaptively Secure Feldman VSS and Applications to Universally-Composable Threshold Cryptography”. In: *Advances in Cryptology - CRYPTO 2004, 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*. Ed. by M. K. Franklin. Vol. 3152. Lecture Notes in Computer Science. Springer, 2004, pp. 317–334. DOI: 10.1007/978-3-540-28628-8_20. URL: https://doi.org/10.1007/978-3-540-28628-8_20.
- [2] M. Abe and T. Okamoto. “Provably Secure Partially Blind Signatures”. In: *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*. Ed. by M. Bellare. Vol. 1880. Lecture Notes in Computer Science. Springer, 2000, pp. 271–286. DOI: 10.1007/3-540-44598-6_17. URL: https://doi.org/10.1007/3-540-44598-6_17.
- [3] H. K. Alper and J. Burdges. “Two-Round Trip Schnorr Multi-signatures via Delinearized Witnesses”. In: *CRYPTO 2021, Virtual Event, August 16-20, 2021*. Ed. by T. Malkin and C. Peikert. Vol. 12825. LNCS. Springer, 2021, pp. 157–188.
- [4] R. Bacho, S. Das, J. Loss, and L. Ren. “Glacius: Threshold Schnorr Signatures from DDH with Full Adaptive Security”. In: *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part II*. Ed. by S. Fehr and P. Fouque. Vol. 15602. Lecture Notes in Computer Science. Springer, 2025, pp. 304–334. DOI: 10.1007/978-3-031-91124-8_11. URL: https://doi.org/10.1007/978-3-031-91124-8_11.
- [5] R. Bacho and J. Loss. “On the Adaptive Security of the Threshold BLS Signature Scheme”. In: *IACR Cryptol. ePrint Arch.* (2022), p. 534. URL: <https://eprint.iacr.org/2022/534>.
- [6] R. Bacho, J. Loss, G. Stern, and B. Wagner. “HARTS: High-Threshold, Adaptively Secure, and Robust Threshold Schnorr Signatures”. In: *IACR Cryptol. ePrint Arch.* (2024), p. 280. URL: <https://eprint.iacr.org/2024/280>.
- [7] M. Bellare, E. Crites, C. Komlo, M. Maller, S. Tessaro, and C. Zhu. *Better than advertised security for non-interactive threshold signatures*. CRYPTO 2022. To appear. 2022.
- [8] M. Bellare and P. Rogaway. “Random Oracles are Practical: A Paradigm for Designing Efficient Protocols”. In: *CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993*. Ed. by D. E. Denning, R. Pyle, R. Ganesan, R. S. Sandhu, and V. Ashby. ACM, 1993, pp. 62–73. DOI: 10.1145/168588.168596. URL: <https://doi.org/10.1145/168588.168596>.

- [9] M. Bellare, S. Tessaro, and C. Zhu. “Stronger Security for Non-Interactive Threshold Signatures”. In: *IACR Cryptol. ePrint Arch.* (2022), p. 833. URL: <https://eprint.iacr.org/2022/833>.
- [10] F. Benhamouda, S. Halevi, H. Krawczyk, Y. Ma, and T. Rabin. “SPRINT: High-Throughput Robust Distributed Schnorr Signatures”. In: *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part V*. Ed. by M. Joye and G. Leander. Vol. 14655. Lecture Notes in Computer Science. Springer, 2024, pp. 62–91. DOI: 10.1007/978-3-031-58740-5_3. URL: https://doi.org/10.1007/978-3-031-58740-5_3.
- [11] F. Benhamouda, T. Lepoint, J. Loss, M. Orrù, and M. Raykova. “On the (in)Security of ROS”. In: *J. Cryptol.* 35.4 (2022), p. 25. DOI: 10.1007/S00145-022-09436-0. URL: <https://doi.org/10.1007/s00145-022-09436-0>.
- [12] A. Boldyreva. “Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme”. In: *PKC 2003, Miami, FL, USA, January 6-8, 2003*. Ed. by Y. Desmedt. Vol. 2567. LNCS. Springer, 2003, pp. 31–46.
- [13] L. Brandão and M. Davidson. *Notes on Threshold EdDSA/Schnorr Signatures*. <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8214B.ipd.pdf>. 2022.
- [14] L. Brandão and R. Peralta. *NIST First Call for Multi-Party Threshold Schemes*. <https://doi.org/10.6028/NIST.IR.8214C.2pd>. 2025.
- [15] R. Canetti, I. Damgård, S. Dziembowski, Y. Ishai, and T. Malkin. “On Adaptive vs. Non-adaptive Security of Multiparty Protocols”. In: *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*. Ed. by B. Pfitzmann. Vol. 2045. Lecture Notes in Computer Science. Springer, 2001, pp. 262–279. DOI: 10.1007/3-540-44987-6_17. URL: https://doi.org/10.1007/3-540-44987-6_17.
- [16] R. Canetti, U. Feige, O. Goldreich, and M. Naor. “Adaptively Secure Multi-Party Computation”. In: *STOC '96, Philadelphia, Pennsylvania, USA, May 22-24, 1996*. Ed. by G. L. Miller. ACM, 1996, pp. 639–648.
- [17] R. Canetti, R. Gennaro, S. Goldfeder, N. Makriyannis, and U. Peled. “UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts”. In: *CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020*. Ed. by J. Ligatti, X. Ou, J. Katz, and G. Vigna. ACM, 2020, pp. 1769–1787. DOI: 10.1145/3372297.3423367. URL: <https://doi.org/10.1145/3372297.3423367>.
- [18] Y. Chen. “Round-Efficient Adaptively Secure Threshold Signatures with Rewinding”. In: *IACR Cryptol. ePrint Arch.* (2025), p. 638. URL: <https://eprint.iacr.org/2025/638>.
- [19] H. Chu, P. Gerhart, T. Ruffing, and D. Schröder. “Practical Schnorr Threshold Signatures Without the Algebraic Group Model”. In: *CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023*. Ed. by H. Handschuh and A. Lysyanskaya. Vol. 14081. LNCS. Springer, 2023, pp. 743–773. DOI: 10.1007/978-3-031-38557-5_24. URL: https://doi.org/10.1007/978-3-031-38557-5_24.
- [20] D. Connolly, C. Komlo, I. Goldberg, and C. Wood. *Two-Round Threshold Schnorr Signatures with FROST*. 2022. URL: <https://datatracker.ietf.org/doc/draft-irtf-cfrg-frost/>.

- [21] E. Crites, J. Katz, C. Komlo, S. Tessaro, and C. Zhu. *On the Adaptive Security of FROST*. To appear in CRYPTO 2025. 2025.
- [22] E. Crites, C. Komlo, and M. Maller. *On the Adaptive Security of Key-Unique Threshold Signatures*. Cryptology ePrint Archive, Paper 2025/943. 2025. URL: <https://eprint.iacr.org/2025/943>.
- [23] E. C. Crites, C. Komlo, and M. Maller. “Fully Adaptive Schnorr Threshold Signatures”. In: *CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023*. Ed. by H. Handschuh and A. Lysyanskaya. Vol. 14081. LNCS. Springer, 2023, pp. 678–709. DOI: 10.1007/978-3-031-38557-5_22. URL: https://doi.org/10.1007/978-3-031-38557-5_22.
- [24] E. C. Crites, C. Komlo, and M. Maller. “How to Prove Schnorr Assuming Schnorr: Security of Multi- and Threshold Signatures”. In: *IACR Cryptol. ePrint Arch.* (2021), p. 1375. URL: <https://eprint.iacr.org/2021/1375>.
- [25] M. Drijvers et al. “On the Security of Two-Round Multi-Signatures”. In: *SP 2019, San Francisco, CA, USA, May 19-23, 2019*. IEEE, 2019, pp. 1084–1101.
- [26] A. Fiat and A. Shamir. “How to Prove Yourself: Practical Solutions to Identification and Signature Problems”. In: *CRYPTO 1986, Santa Barbara, California, USA, 1986*. Ed. by A. M. Odlyzko. Vol. 263. LNCS. Springer, 1986, pp. 186–194.
- [27] G. Fuchsbauer, A. Plouviez, and Y. Seurin. “Blind Schnorr Signatures and Signed ElGamal Encryption in the Algebraic Group Model”. In: *EUROCRYPT 2020, Zagreb, Croatia, May 10-14, 2020*. Ed. by A. Canteaut and Y. Ishai. Vol. 12106. LNCS. Springer, 2020, pp. 63–95.
- [28] V. Gandikota, B. Ghazi, and E. Grigorescu. “NP-Hardness of Reed-Solomon Decoding, and the Prouhet-Tarry-Escott Problem”. In: *SIAM J. Comput.* 47.4 (2018), pp. 1547–1584. DOI: 10.1137/16M110349X. URL: <https://doi.org/10.1137/16M110349X>.
- [29] F. Garillot, Y. Kondi, P. Mohassel, and V. Nikolaenko. “Threshold Schnorr with Stateless Deterministic Signing from Standard Assumptions”. In: *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*. Ed. by T. Malkin and C. Peikert. Vol. 12825. Lecture Notes in Computer Science. Springer, 2021, pp. 127–156. DOI: 10.1007/978-3-030-84242-0_6. URL: https://doi.org/10.1007/978-3-030-84242-0_6.
- [30] R. Gennaro and S. Goldfeder. “Fast Multiparty Threshold ECDSA with Fast Trustless Setup”. In: *CCS 2018, Toronto, ON, Canada, October 15-19, 2018*. Ed. by D. Lie, M. Mannan, M. Backes, and X. Wang. ACM, 2018, pp. 1179–1194.
- [31] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. “Secure Distributed Key Generation for Discrete-Log Based Cryptosystems”. In: *J. Cryptol.* 20.1 (2007), pp. 51–83.
- [32] P. Grontas, A. Pagourtzis, A. Zacharakis, and B. Zhang. “Towards everlasting privacy and efficient coercion resistance in remote electronic voting”. In: *IACR Cryptol. ePrint Arch.* (2018), p. 215. URL: <http://eprint.iacr.org/2018/215>.
- [33] V. Guruswami, A. Rudra, and M. Sudan. *Essential Coding Theory*. 2023. URL: <https://cse.buffalo.edu/faculty/atri/courses/coding-theory/book/web-coding-book.pdf>.
- [34] V. Guruswami and A. Vardy. “Maximum-likelihood decoding of Reed-Solomon codes is NP-hard”. In: *Proceedings of the Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2005, Vancouver, British Columbia, Canada,*

- January 23-25, 2005. SIAM, 2005, pp. 470–478. URL: <http://dl.acm.org/citation.cfm?id=1070432.1070497>.
- [35] A. Joux, J. Loss, and G. Santato. “Dimensional eROSion: Improving the ROS Attack with Decomposition in Higher Bases”. In: *IACR Cryptol. ePrint Arch.* (2025), p. 306. URL: <https://eprint.iacr.org/2025/306>.
 - [36] S. Katsumata, K. Takemure, and M. Reichle. “Adaptively Secure 5 Round Threshold Signatures from MLWE/MSIS and DL with Rewinding”. In: *CRYPTO 2024*. To appear. 2024.
 - [37] C. Komlo and I. Goldberg. “Arctic: Lightweight and Stateless Threshold Schnorr Signatures”. In: *IACR Cryptol. ePrint Arch.* (2024), p. 466. URL: <https://eprint.iacr.org/2024/466>.
 - [38] C. Komlo and I. Goldberg. “FROST: Flexible Round-Optimized Schnorr Threshold Signatures”. In: *SAC 2020, Halifax, NS, Canada (Virtual Event), October 21-23, 2020*. Ed. by O. Dunkelman, M. J. J. Jr., and C. O’Flynn. Vol. 12804. LNCS. Springer, 2020, pp. 34–65. DOI: 10.1007/978-3-030-81652-0_2.
 - [39] Y. Lindell. “Simple Three-Round Multiparty Schnorr Signing with Full Simulatability”. In: *IACR Cryptol. ePrint Arch.* (2022), p. 374. URL: <https://eprint.iacr.org/2022/374>.
 - [40] N. Makriyannis. *On the Classic Protocol for MPC Schnorr Signatures*. Cryptology ePrint Archive, Paper 2022/1332. <https://eprint.iacr.org/2022/1332>. 2022. URL: <https://eprint.iacr.org/2022/1332>.
 - [41] G. Maxwell, A. Poelstra, Y. Seurin, and P. Wuille. “Simple Schnorr multi-signatures with applications to Bitcoin”. In: *Des. Codes Cryptogr.* 87.9 (2019), pp. 2139–2164.
 - [42] J. Nick, T. Ruffing, and Y. Seurin. “MuSig2: Simple Two-Round Schnorr Multi-signatures”. In: *CRYPTO 2021, Virtual Event, August 16-20, 2021*. Ed. by T. Malkin and C. Peikert. Vol. 12825. LNCS. Springer, 2021, pp. 189–221.
 - [43] A. Nicolosi, M. N. Krohn, Y. Dodis, and D. Mazières. “Proactive Two-Party Signatures for User Authentication”. In: *Proceedings of the Network and Distributed System Security Symposium, NDSS 2003, San Diego, California, USA*. The Internet Society, 2003. URL: <https://www.ndss-symposium.org/ndss2003/proactive-two-party-signatures-user-authentication/>.
 - [44] D. Pointcheval and J. Stern. “Security Arguments for Digital Signatures and Blind Signatures”. In: *J. Cryptol.* 13.3 (2000), pp. 361–396.
 - [45] I. S. Reed and G. Solomon. “Polynomial Codes Over Certain Finite Fields”. In: *Journal of the Society for Industrial and Applied Mathematics* 8.2 (1960), pp. 300–304. DOI: 10.1137/0108018. eprint: <https://doi.org/10.1137/0108018>. URL: <https://doi.org/10.1137/0108018>.
 - [46] T. Ruffing, V. Ronge, E. Jin, J. Schneider-Bensch, and D. Schröder. “ROAST: Robust Asynchronous Schnorr Threshold Signatures”. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*. Ed. by H. Yin, A. Stavrou, C. Cremers, and E. Shi. ACM, 2022, pp. 2551–2564. DOI: 10.1145/3548606.3560583. URL: <https://doi.org/10.1145/3548606.3560583>.
 - [47] C. Schnorr. “Efficient Signature Generation by Smart Cards”. In: *J. Cryptol.* 4.3 (1991), pp. 161–174.
 - [48] C. Schnorr. “Security of Blind Discrete Log Signatures against Interactive Attacks”. In: *Information and Communications Security, Third International Conference, ICICS 2001, Xian, China, November 13-16, 2001*. Ed. by S. Qing, T. Okamoto, and J. Zhou. Vol. 2229. Lecture Notes in Computer Science. Springer, 2001,

- pp. 1–12. DOI: 10.1007/3-540-45600-7_1. URL: https://doi.org/10.1007/3-540-45600-7_1.
- [49] A. Shamir. “How to Share a Secret”. In: *Commun. ACM* 22.11 (1979), pp. 612–613.
 - [50] V. Shoup. “The many faces of Schnorr”. In: *IACR Cryptol. ePrint Arch.* (2023), p. 1019. URL: <https://eprint.iacr.org/2023/1019>.
 - [51] D. R. Stinson and R. Strobl. “Provably Secure Distributed Schnorr Signatures and a (t, n) Threshold Scheme for Implicit Certificates”. In: *ACISP 2001, Sydney, Australia, July 11-13, 2001*. Ed. by V. Varadharajan and Y. Mu. Vol. 2119. LNCS. Springer, 2001, pp. 417–434.
 - [52] E. Syta et al. “Keeping Authorities ”Honest or Bust” with Decentralized Witness Cosigning”. In: *IEEE Symposium on Security and Privacy, SP 2016, San Jose, CA, USA, May 22-26, 2016*. IEEE Computer Society, 2016, pp. 526–545. DOI: 10.1109/SP.2016.38. URL: <https://doi.org/10.1109/SP.2016.38>.
 - [53] D. A. Wagner. “A Generalized Birthday Problem”. In: *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*. Ed. by M. Yung. Vol. 2442. Lecture Notes in Computer Science. Springer, 2002, pp. 288–303. DOI: 10.1007/3-540-45708-9_19. URL: https://doi.org/10.1007/3-540-45708-9_19.
 - [54] A. Zacharakis, P. Grontas, and A. Pagourtzis. “Conditional Blind Signatures”. In: *IACR Cryptol. ePrint Arch.* (2017), p. 682. URL: <http://eprint.iacr.org/2017/682>.