Single-Signature Key Recovery on the $\mathsf{SBC}_{\mathsf{VOLE}}$ Signature Scheme

MiniMax

November 2026

Abstract

Post-quantum signature schemes built from symmetric primitives in the Multi-Party Computation in the Head (MPCitH) and VOLE-in-the-Head (VOLEitH) paradigms rely on clean algebraic assumptions and idealised hash functions. At ASIACRYPT 2025, Huth and Joux proposed $\mathsf{SBC}_{\mathsf{VOLE}}$ and its MinMax commitment variant $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$ from the Subfield Bilinear Collision (SBC) problem (CRYPTO 2024), achieving a 48-byte public key and signatures as compact as 2,658 bytes at the 128-bit security level, backed by a formal EUF-CMA security reduction. Subsequent cryptanalysis confirmed that the underlying SBC instance retains at least 2^{128} hardness and identified only a sub-2^{128} key-only forgery against implicit global and MinMax tree commitments, leaving secret-key security and the explicit-commitment scheme $\mathsf{SBC}_{\mathsf{VOLE}}$ seemingly intact.

In this paper, we show that both $\mathsf{SBC}_{\mathsf{VOLE}}$ and $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$ are broken in practice by a passive single-signature secret-key recovery attack. Our key intuition is that, to save bandwidth, $\mathsf{SBC}_{\mathsf{VOLE}}$ transmits the linear slope of its quadratic verification polynomial without an independent multiplication mask, assuming that the unopened VOLE masks conceal the witness. Once verification opens the VOLE commitments at the challenge point, however, those hidden masks become affine functions of the secret key; substituting them back into the public slope causes all quadratic witness cross-terms to cancel pairwise in characteristic two, collapsing the slope into an unmasked binary linear system in the secret key bits. Passive observation of a single valid signature recovers the full 256-bit secret key in $2^{25.24}$ bit operations (0.06 s on a single CPU core) across all published parameter sets. We further show that the original EUF-CMA reduction overlooked the zero conditional entropy of this slope in its witness-free simulator, and we adapt standard VOLE multiplication masking into a minimal correlated-mask repair that restores zero-knowledge simulation at a signature-size overhead of 8.6%–15.1%.

1 Introduction

Post-quantum digital signatures constructed via the Fiat–Shamir transform [10] from zero-knowledge proofs of knowledge offer an attractive alternative to structured lattice schemes, resting solely on symmetric primitives and simple algebraic problems. Following the Multi-Party Computation in the Head (MPCitH) paradigm [15] and its VOLE-in-the-Head (VOLEitH) refinement [20, 19, 3], compact signatures can be obtained whenever the underlying hard relation has multiplicative depth one over a large extension field. At CRYPTO 2024, Huth and Joux [13] introduced an algebraic problem tailored to this setting: the *Subfield Bilinear Collision* (SBC) problem, motivated by bilinear descent steps in small-characteristic discrete logarithm algorithms [16].

Definition 1 (Subfield Bilinear Collision (SBC) and Normalised NSBC [13, 14])**.** Let q be a prime power, let $k, n \in \mathbb{Z}^+$, and consider the field extension $\mathbb{F}_{q^k}/\mathbb{F}_q$ under the canonical subfield embedding $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^k}$.

- **Instance:** Two $\mathbb{F}_{q^k}$-linearly independent vectors $\vec{u}, \vec{v} \in (\mathbb{F}_{q^k})^n$.

- **Solution ($\mathsf{SBC}[\vec{u},\vec{v}]$):** Two $\mathbb{F}_q$-linearly independent subfield vectors $\vec{x}',\vec{y}' \in \mathbb{F}_q^n$ satisfying

$$(\vec{u}\cdot\vec{x}')(\vec{v}\cdot\vec{y}') = (\vec{u}\cdot\vec{y}')(\vec{v}\cdot\vec{x}') \quad \text{in } \mathbb{F}_{q^k}, \tag{1}$$

  where $\vec{a}\cdot\vec{b} = \sum_{i=0}^{n-1} a_i b_i$.

- **Normalised Solution ($\mathsf{NSBC}[\vec{u},\vec{v}]$):** Up to an invertible $\mathbb{F}_q$-linear basis change, any solution can be normalised to the form

$$\vec{x}' = (\vec{x}, 1, 0) \in \mathbb{F}_q^n, \qquad \vec{y}' = (\vec{y}, 0, 1) \in \mathbb{F}_q^n \tag{2}$$

  for secret subfield vectors $\vec{x},\vec{y} \in \mathbb{F}_q^{n-2}$, in which case we write $(\vec{x}',\vec{y}') \in \mathsf{NSBC}[\vec{u},\vec{v}]$ (and, identifying $(\vec{x}',\vec{y}')$ with $(\vec{x},\vec{y})$, also $(\vec{x},\vec{y}) \in \mathsf{NSBC}[\vec{u},\vec{v}]$).

Using MPCitH with hypercube folding [1], the CRYPTO 2024 SBC signature scheme achieved 3,766-byte signatures at the $\lambda = 128$-bit security parameters $(q,k,n) = (2,257,130)$, where the secret key $(\vec{x},\vec{y}) \in \mathbb{F}_2^{128} \times \mathbb{F}_2^{128}$ comprises 256 bits. At ASIACRYPT 2025, Huth and Joux [14] migrated SBC to a streamlined VOLEitH architecture, introducing a two-layer correlated GGM forest ($\mathsf{SBC}_{\mathsf{VOLE}}$) and an optional extremal tree commitment ($\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$). Together with a 48-byte public key and ≈ 2.2 ms signing and verification times (90% faster than [13]), $\mathsf{SBC}_{\mathsf{VOLE}}$ (2,978 B) undercut FAEST v2 (4,506 B) and FAEST-EM v2 (3,906 B) [2], ReSolveD (3,916 B) [8], VOLEitH-PKP (3,686 B) [4], and VOLEitH-MQ (3.1–3.6 kB) [7], while $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$ (2,658 B) further improved upon Dual-SDitH (2,813–2,851 B) [5] to reach the smallest signature size among comparable $\lambda = 128$-bit VOLEitH designs.

Existing Analyses. Subsequent studies examined three orthogonal aspects of the $\mathsf{SBC}_{\mathsf{VOLE}}$ family: its underlying algebraic problem, its tree-commitment binding, and its cGGM root-seed reduction. Briaud and Neveu [6] analysed pure SBC instances via linear rank-metric decoding over $\mathbb{F}_{q^k}$ and Plücker maximal-minor systems, confirming a complexity of at least 2^{128} operations at $(q,k,n) = (2,257,130)$. Independently, Kim, Lee, and Son [17] showed that condensing per-leaf commitments into an implicit global summary—as in the initial preprint of [14] (which prompted the explicit 2λ-bit tree commitments $(X_j)_{j\in[\tau]}$ of $\mathsf{SBC}_{\mathsf{VOLE}}$ [14, Section 4]) and in the MinMax variant $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$—sacrifices leaf-level binding and admits a sub-2^{128} key-only existential forgery; however, commitment-layer attacks require exponential offline search, do not recover the secret key, and leave $\mathsf{SBC}_{\mathsf{VOLE}}$ unaffected. Separately, Kosuge and Xagawa [18] and Feneuil and Rivain [9] identified a reduction circularity in secret-key-rooted cGGM trees, showing that tight EUF-CMA reductions require guessing the λ-bit tree-root prefix (here $\vec{x} \in \mathbb{F}_2^{128}$) to retain 2^λ hardness, a condition still consistent with 2^{128} security at $(q,k,n) = (2,257,130)$.

All of these external analyses [17, 6, 18, 9] and the EUF-CMA proof of Huth and Joux [14, Theorem 2] rely on a shared, untested assumption about the algebraic verification layer. To compress signatures from 3,766 bytes down to 2,658–2,978 bytes, $\mathsf{SBC}_{\mathsf{VOLE}}$ omits the per-party multiplication masks used in [13] and transmits the raw degree-1 slope of the quadratic NSBC verification polynomial in every signature, assuming that the unopened VOLE masks inside this slope suffice to hide $(\vec{x},\vec{y})$. If that assumption fails once the VOLE commitments are opened during verification, then neither the 2^{128} hardness of SBC nor a binding tree commitment can protect the secret key, and the witness-free simulator underlying the EUF-CMA reduction breaks down.

Our Intuition and Main Results. In this paper, we refute this masking assumption and show that a single passive signature exposes the entire secret key of both $\mathsf{SBC}_{\mathsf{VOLE}}$ and $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$. The core intuition is straightforward: although the signer's VOLE masks are hidden prior to opening, verification reconstructs single-point VOLE evaluations that lock each hidden mask to an affine function of the secret key $(\vec{x},\vec{y})$. When this affine relation is substituted into the

Table 1: Cryptanalytic results on $\mathsf{SBC}_{\mathsf{VOLE}}$ and $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$ at $\lambda = 128$ ($q = 2, k = 257, n = 130$).

Work	Target	Attack Goal	Data (sigs)	Complexity (ops)
Briaud–Neveu [6]	Underlying SBC	Key recovery	0	$\geq 2^{128.00}$
Kim–Lee–Son [17]	$\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$	Key-only forgery	0	$< 2^{128.00}$
This Work	$\mathsf{SBC}_{\mathsf{VOLE}}, \mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$	**Full key recovery**	**1**	$\mathbf{2^{25.24}}$

transmitted degree-1 verification slope, the bilinear symmetry of (1) causes every quadratic term in $(\vec{x}, \vec{y})$ to appear twice and vanish identically in characteristic 2. What remains is an exact, noiseless $\mathbb{F}_2$-linear map from the $2(n-2)$ secret key bits into $\mathbb{F}_{2^k}$, yielding our main cryptanalytic result (proved formally as Theorem 1 in Section 4):

Theorem 1 (Single-Signature Key Recovery, Informal). *For $q = 2$ and any tree parameters (D, τ), given a public key $\mathsf{pk} = (\vec{u}, \vec{v}) \in (\mathbb{F}_{2^k})^n \times (\mathbb{F}_{2^k})^n$ and a single valid signature σ of either $\mathsf{SBC}_{\mathsf{VOLE}}$ or $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$, a passive observer can construct a deterministic system of k linear equations over $\mathbb{F}_2$ in the $2(n-2)$ secret key bits.*

As summarised in Table 1, our contributions are threefold:

1. **Single-Signature Secret-Key Recovery:** We prove the characteristic-2 quadratic cancellation in the public verification slope and derive a closed-form $k \times 2(n-2)$ binary linear system whose complexity depends only on (n, k) and is independent of (D, τ), breaking all parameter sets of both $\mathsf{SBC}_{\mathsf{VOLE}}$ and $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$ in $2^{25.24}$ bit operations (and generalising to honest signatures over any odd characteristic $q > 2$).

2. **Security-Proof Diagnosis and Simulator Distinguisher:** We trace why the EUF-CMA proof [14, Appendix A, full version] missed this attack: its witness-free simulator treats the verification slope as conditionally uniform given single-point acceptance, whereas in honest signatures its conditional entropy given the opened transcript is zero, yielding a single-query distinguisher with advantage at least $1 - \varepsilon_{\mathsf{SBC}}$ (exceeding $1 - 2^{-254}$ against the explicit simulation strategies of [14]).

3. **Soundness-Preserving VOLE-Masking Repair:** Adapting standard VOLEitH multiplication masking [20, 3] to $\mathsf{SBC}_{\mathsf{VOLE}}$'s cross-tree offset architecture, we prove that no existing leaf share can conceal the leaked slope, construct a minimal repair using one correlated field mask, prove that it preserves identification soundness and restores Game 2 simulation, and establish an exact size overhead of 257–450 bytes (+289 B at $(D, \tau) = (13, 10)$, while shifting the size-optimal repaired $\mathsf{SBC}_{\mathsf{VOLE}}$ set to $(15, 9)$ at 3,235 B).

We also implement our key-recovery attack and validate it across all published parameter sets of $\mathsf{SBC}_{\mathsf{VOLE}}$ and $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$.

Organisation. Section 2 establishes field notation, sharing primitives, and security definitions. Section 3 specifies the $\mathsf{SBC}_{\mathsf{VOLE}}$ architecture, five-pass protocol, and Fiat–Shamir signature. Section 4 derives the algebraic collapse and proves our key-recovery theorem. Section 5 analyses the failure of the original EUF-CMA simulator. Section 6 presents and evaluates our correlated VOLE-masking repair, Section 7 reports experimental results, and Section 8 concludes.

2 Preliminaries

2.1 Notation and Binary Extension Fields

We denote the target security parameter by $\lambda \in \mathbb{Z}^+$. For any integer $m \geq 1$, write $[m] := \{0, \ldots, m-1\}$, and for $m > 1$, write $[m]^* := \{1, \ldots, m-1\}$. For an integer $\ell \geq 0$, $\mathsf{bit}_i(\ell) \in \{0, 1\}$

denotes bit i in the binary expansion $\ell = \sum_{i\geq 0} \mathsf{bit}_i(\ell)2^i$. Sampling an element s uniformly at random from a finite set S is written $s \xleftarrow{\$} S$. Vectors are written with arrows, e.g., $\vec{a} = (a_0, \ldots, a_{m-1})$, with 0-based indexing; $(\vec{a}, \vec{b})$ denotes vector concatenation, and $\vec{a} \cdot \vec{b} = \sum_{i=0}^{m-1} a_i b_i$ denotes the standard inner product.

Throughout our analysis of $\mathsf{SBC}_{\mathsf{VOLE}}$, we work over the binary ground field $\mathbb{F}_2 = \{0, 1\}$ and its degree-k extension $\mathbb{F}_{2^k} = \mathbb{F}_2[\theta]/(p(\theta))$ generated by an irreducible polynomial $p(\theta) \in \mathbb{F}_2[\theta]$ of degree k. Since $\mathrm{char}(\mathbb{F}_{2^k}) = 2$, addition and subtraction in $\mathbb{F}_2$, $\mathbb{F}_{2^k}$, and their vector spaces coincide with bitwise XOR ($\oplus$), and every element $Z \in \mathbb{F}_{2^k}$ satisfies $Z \oplus Z = 0$. Under the canonical subfield embedding $\mathbb{F}_2 \hookrightarrow \mathbb{F}_{2^k}$, multiplying a field element $\beta \in \mathbb{F}_{2^k}$ by a bit $x \in \mathbb{F}_2$ coincides with scalar selection ($0 \cdot \beta = 0$, $1 \cdot \beta = \beta$).

Let $\mathrm{vec} : \mathbb{F}_{2^k} \xrightarrow{\sim} \mathbb{F}_2^k$ denote the $\mathbb{F}_2$-vector space isomorphism mapping each element $\beta = \bigoplus_{r=0}^{k-1} \beta_r \theta^r \in \mathbb{F}_{2^k}$ to its column vector of polynomial-basis coordinates $(\beta_0, \ldots, \beta_{k-1})^\top \in \mathbb{F}_2^k$. Because vec is $\mathbb{F}_2$-linear, any $\mathbb{F}_{2^k}$-linear combination with binary scalars $x_0, \ldots, x_{m-1} \in \mathbb{F}_2$ satisfies

$$\mathrm{vec}\left(\bigoplus_{i=0}^{m-1} x_i\, \beta_i\right) = \bigoplus_{i=0}^{m-1} x_i\ \mathrm{vec}(\beta_i) \in \mathbb{F}_2^k \qquad (\forall \beta_0, \ldots, \beta_{m-1} \in \mathbb{F}_{2^k}). \tag{3}$$

For $\lambda = 128$-bit security, Huth and Joux [13, 14] fix $(q, k, n) = (2, 257, 130)$, instantiated with $p(\theta) = \theta^{257} + \theta^{12} + 1$ in the official reference implementation. Key generation samples $\mathsf{sk} = (\vec{x}, \vec{y}) \xleftarrow{\$} \mathbb{F}_2^{n-2} \times \mathbb{F}_2^{n-2}$ (256 bits) and a seed $\mathsf{seed}_{\mathsf{pk}} \xleftarrow{\$} \{0,1\}^\lambda$, expands $\mathsf{seed}_{\mathsf{pk}}$ via a pseudorandom generator (PRG) into $\vec{u} \in (\mathbb{F}_{2^k})^n$ and $(v_0, \ldots, v_{n-2}) \in (\mathbb{F}_{2^k})^{n-1}$, and solves (1) for the final coordinate

$$v_{n-1} = (\vec{u} \cdot \vec{x}')^{-1} \left((\vec{u} \cdot \vec{y}') \bigoplus_{i=0}^{n-2} v_i x'_i \ \oplus\ (\vec{u} \cdot \vec{x}') \bigoplus_{i=0}^{n-2} v_i y'_i \right), \tag{4}$$

restarting if $\vec{u} \cdot \vec{x}' = 0$ or if $\vec{u}, \vec{v}$ are $\mathbb{F}_{2^k}$-linearly dependent. The public key $\mathsf{pk} = (\mathsf{seed}_{\mathsf{pk}}, v_{n-1})$ occupies $\lambda + k = 385$ bits (≈ 48 bytes). Hash functions H_0, H_1, H_2, H_3 are modelled as independent random oracles, and pseudorandom generators PRG are assumed to be $(t, \varepsilon_{\mathsf{PRG}})$-indistinguishable from uniform bitstrings.

2.2 Additive Sharings, Hypercube Folding, and Correlated GGM Trees

An N-party additive sharing of x over an $\mathbb{F}_2$-vector space $\mathcal{V}$ is a tuple $[\![x]\!] = (x^{[\![0]\!]}, \ldots, x^{[\![N-1]\!]}) \in \mathcal{V}^N$ such that $\bigoplus_{\ell=0}^{N-1} x^{[\![\ell]\!]} = x$. When shares $(x^{[\![\ell]\!]})_{\ell \in [N]}$ are derived pseudorandomly, their sum equals a random value; to share a prescribed target $x \in \mathcal{V}$, the prover publishes an *offset* $\delta_x := x \oplus \bigoplus_{\ell=0}^{N-1} x^{[\![\ell]\!]}$, allowing reconstruction via $x = \delta_x \oplus \bigoplus_{\ell=0}^{N-1} x^{[\![\ell]\!]}$.

Hypercube Folding [1, 13]. For $N = 2^D$, hypercube folding maps a 2^D-party sharing $[\![x]\!] = (x^{[\![0]\!]}, \ldots, x^{[\![N-1]\!]})$ via $\mathsf{Folding}([\![x]\!])$ into D independent 2-party sharings $(x^{[\![0]\!]_i}, x^{[\![1]\!]_i})_{i \in [D]}$, defined along each bit axis $i \in [D]$ by

$$x^{[\![b]\!]_i} := \bigoplus_{\substack{\ell \in [2^D] \\ \mathsf{bit}_i(\ell) = b}} x^{[\![\ell]\!]} \quad (b \in \{0,1\}), \qquad \text{so that} \qquad x^{[\![0]\!]_i} \oplus x^{[\![1]\!]_i} = \bigoplus_{\ell=0}^{2^D-1} x^{[\![\ell]\!]}. \tag{5}$$

Revealing all $2^D - 1$ shares except a single missing leaf $i^* \in [2^D]$ hides $x^{[\![\mathsf{bit}_i(i^*)]\!]_i}$ on every axis $i \in [D]$, while allowing the verifier to compute the complementary share $x^{[\![b_i]\!]_i}$ indexed by the *known branch bit* $b_i := 1 \oplus \mathsf{bit}_i(i^*) \in \{0, 1\}$.

GGM Puncturable PRFs and Correlated GGM (cGGM) Trees [11, 12, 14]. In a depth-D Goldreich–Goldwasser–Micali (GGM) binary tree [11], each internal node $P \in \mathbb{F}_2^\lambda$ is expanded into left and right children (L, R) via a length-doubling PRG or salted hash, yielding $N = 2^D$ leaves. To reveal all leaves except $i^* \in [2^D]$, the prover outputs the *punctured key* K_{i^*} consisting of the D sibling nodes along the path from the root to leaf i^* ($D\lambda$ bits in total). In an *XOR-preserving correlated GGM* (cGGM) tree [12, 14], the child derivation at tree j and node position pos is modified to

$$L \leftarrow H_2(\mathsf{salt} \parallel j \parallel \mathsf{pos} \parallel P), \qquad R \leftarrow P \oplus L,$$

ensuring $L \oplus R = P$ at every internal split. Initialising level 1 of a depth-D tree with a pair $(S_0, S_1) \in \mathbb{F}_2^\lambda \times \mathbb{F}_2^\lambda$, denoted $\mathsf{cGGM}_{\mathsf{salt}}(S_0, S_1, 2^D)$, guarantees that the XOR of all 2^D leaves equals $S_0 \oplus S_1$ without transmitting an external offset.

2.3 VOLE-in-the-Head, Consistency Bounds, and Security Notions

From Bit-OLEs to Extension-Field VOLE [20, 19, 3]. Given $M = \tau D$ binary 2-sharings $(\vec{x}_m^{[\![0]\!]}, \vec{x}_m^{[\![1]\!]})_{m\in[M]}$ of a common vector $\vec{x} \in \mathbb{F}_2^{n-2}$ (so $\vec{x}_m^{[\![0]\!]} \oplus \vec{x}_m^{[\![1]\!]} = \vec{x}$), knowing one share $\vec{x}_m^{[\![b_m]\!]}$ for a bit $b_m \in \mathbb{F}_2$ is equivalent to evaluating the affine function $f_m(b_m) = \vec{x}_m^{[\![0]\!]} \oplus b_m\vec{x} \in \mathbb{F}_2^{n-2}$. Weighting these M bit-level evaluations by public coefficients $(\alpha_m)_{m\in[M]} \in (\mathbb{F}_{2^k})^M$ produces a single *Vector Oblivious Linear Evaluation* (VOLE) over $\mathbb{F}_{2^k}$:

$$\vec{F}_x(\Delta) := \bigoplus_{m=0}^{M-1} \alpha_m f_m(b_m) = \vec{A}_{F_x} \oplus \Delta \cdot \vec{x} \in (\mathbb{F}_{2^k})^{n-2},$$

where $\vec{A}_{F_x} := \bigoplus_{m=0}^{M-1} \alpha_m \vec{x}_m^{[\![0]\!]}$ is known to the prover, and the verifier learns $(\Delta, \vec{F}_x(\Delta))$ at the scalar evaluation point $\Delta := \bigoplus_{m=0}^{M-1} b_m\alpha_m \in \mathbb{F}_{2^k}$.

Cross-Tree Consistency and Identification Soundness. When uncorrelated leaf expansions are aligned across τ trees via per-tree offsets, $\mathsf{SBC}_{\mathsf{VOLE}}$ checks cross-tree equality of $(\vec{y}_j, z_j) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_{2^k}$ using a simplified SoftSpokenOT batch check [19, 14]: for any distinct pairs $(\vec{y}, z) \neq (\vec{y}', z')$ in $\mathbb{F}_2^{n-2} \times \mathbb{F}_{2^k}$ and a uniform challenge vector $\vec{\mu} \xleftarrow{\$} (\mathbb{F}_{2^k})^{n-2}$, the collision probability $\Pr_{\vec{\mu}}[z \oplus \vec{\mu} \cdot \vec{y} = z' \oplus \vec{\mu} \cdot \vec{y}']$ is at most 2^{-k} [14, Lemma 1]. Union-bounding this test across τ trees and applying a degree-2 polynomial root-counting bound over $2^{\tau D}$ evaluation points shows that the five-pass $\mathsf{SBC}_{\mathsf{VOLE}}$ identification protocol has soundness error at most $\varepsilon = \tau^2 2^{-k} + 2^{1-\tau D}$ [14, Theorem 1], requiring $\tau D > \lambda$ for λ-bit security.

HVZK Simulation and Signature Security. An interactive identification protocol is *Honest-Verifier Zero-Knowledge* (HVZK) if there exists a probabilistic polynomial-time simulator $\mathcal{S}(\mathsf{pk})$, given pk without sk, whose output transcripts are indistinguishable from honest executions between $\mathcal{P}(\mathsf{pk}, \mathsf{sk})$ and an honest verifier $\mathcal{V}(\mathsf{pk})$. For the Fiat–Shamir signature scheme $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$, *Existential Unforgeability under Chosen-Message Attacks* (EUF-CMA) requires that no adversary $\mathcal{A}$ running in time t, making q_s signing queries to $\mathcal{O}(\mathsf{sk}, \mathsf{pk})$ and q_i random-oracle queries to H_i, can output a valid pair $(\mathsf{msg}^*, \sigma^*)$ on a fresh message msg^* except with negligible probability (*key-only* attacks, EUF-KO, correspond to $q_s = 0$). Standard Fiat–Shamir EUF-CMA reductions [13, 14] replace $\mathcal{O}(\mathsf{sk}, \mathsf{pk})$ by the witness-free HVZK simulator $\mathcal{S}(\mathsf{pk})$ to reduce EUF-CMA to EUF-KO and thence to the underlying hard problem.

3 The $\mathsf{SBC}_{\mathsf{VOLE}}$ Signature Scheme

Equipped with the primitives from Section 2, we now specify the $\mathsf{SBC}_{\mathsf{VOLE}}$ and $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$ protocols of Huth and Joux [14, Sections 3–6].

3.1 Correlated Forest and VOLE Architecture

Let $\mathsf{sk} = (\vec{x}, \vec{y}) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_2^{n-2}$ be the secret key with normalised vectors $\vec{x}' = (\vec{x}, 1, 0)$ and $\vec{y}' = (\vec{y}, 0, 1)$ satisfying $(\vec{x}', \vec{y}') \in \mathsf{NSBC}[\vec{u}, \vec{v}]$. As illustrated in Figure 1, the signer prepares τD correlated sharings of $\vec{x}$ and $\vec{y}$ across three stages:

1. **Pre-Tree Derivation (Figure 1a):** The signer samples $R_{\vec{x}} \xleftarrow{\$} \mathbb{F}_2^{n-2}$ and $\mathsf{salt} \xleftarrow{\$} \{0,1\}^{2\lambda}$, computes the depth-$\tau$ pre-tree $T_{\vec{x}}^{\mathrm{pre}} \leftarrow \mathsf{cGGM}_{\mathsf{salt}}(R_{\vec{x}}, R_{\vec{x}} \oplus \vec{x}, 2^\tau)$, and folds its 2^τ leaves via (5) into τ binary root sharings $(\vec{x}^{[\![0]\!]_j}, \vec{x}^{[\![1]\!]_j})_{j\in[\tau]}$ satisfying $\vec{x}^{[\![0]\!]_j} \oplus \vec{x}^{[\![1]\!]_j} = \vec{x}$.

2. **Second-Layer Forest and Leaf Expansion (Figure 1b):** For each $j \in [\tau]$, the signer generates $T_{\vec{x}_j} \leftarrow \mathsf{cGGM}_{\mathsf{salt}}(\vec{x}^{[\![0]\!]_j}, \vec{x}^{[\![1]\!]_j}, 2^D)$ with $N = 2^D$ leaves $(\vec{x}_j^{[\![0]\!]}, \ldots, \vec{x}_j^{[\![2^D-1]\!]})$, and expands each leaf $\vec{x}_j^{[\![\ell]\!]}$ $(\ell \in [2^D])$ into $(\vec{y}_j^{[\![\ell]\!]}, z_j^{[\![\ell]\!]}, \mathsf{com}_j^{[\![\ell]\!]}) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_{2^k} \times \{0,1\}^{2\lambda}$. Applying $\mathsf{Folding}$ to tree $T_{\vec{x}_j}$ produces D binary sharings $(\vec{x}_j^{[\![0]\!]_i}, \vec{x}_j^{[\![1]\!]_i})$, $(\vec{y}_j^{[\![0]\!]_i}, \vec{y}_j^{[\![1]\!]_i})$, $(z_j^{[\![0]\!]_i}, z_j^{[\![1]\!]_i})$, and $(\mathsf{com}_j^{[\![0]\!]_i}, \mathsf{com}_j^{[\![1]\!]_i})$ for $i \in [D]$. Setting the global consistency pad $z \leftarrow z_0^{[\![0]\!]_0} \oplus z_0^{[\![1]\!]_0} \in \mathbb{F}_{2^k}$, the signer computes the cross-tree alignment offsets:

$$\delta_{\vec{y}_j} \leftarrow \vec{y} \oplus \vec{y}_j^{[\![0]\!]_0} \oplus \vec{y}_j^{[\![1]\!]_0} \in \mathbb{F}_2^{n-2} \quad (j \in [\tau]), \qquad \delta_{z_j} \leftarrow z \oplus z_j^{[\![0]\!]_0} \oplus z_j^{[\![1]\!]_0} \in \mathbb{F}_{2^k} \quad (j \in [\tau]^*), \tag{6}$$

   with $\delta_{z_0} := 0$ omitted. In $\mathsf{SBC}_{\mathsf{VOLE}}$, the signer sets $X_j \leftarrow \bigoplus_{\ell=0}^{2^D-1} \mathsf{com}_j^{[\![\ell]\!]}$ and $h_{\mathsf{com}} \leftarrow H_3(\mathsf{salt}, (\mathsf{com}_j^{[\![0]\!]_i}, \mathsf{com}_j^{[\![1]\!]_i})_{(i,j)\in[D]\times[\tau]}, (X_j)_{j\in[\tau]})$; in $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$, $(X_j)_{j\in[\tau]}$ is replaced by hashing the global minimum and maximum $(M^{\min}, M^{\max})$ of $\{\mathsf{com}_j^{[\![\ell]\!]}\}$ into h_{com}, aborting if a punctured leaf hits an extremum.

3. **VOLE Lifting (Figure 1c):** Indexing $m = jD + i \in [\tau D]$ and absorbing $\delta_{\vec{y}_j}$ into the 1-branch of $\vec{y}_j$, puncturing each tree $T_{\vec{x}_j}$ at leaf $i_j^* \in [2^D]$ (with pre-tree leaf $i_{\mathrm{p}}^* \in [2^\tau]$ determined by $\mathsf{bit}_j(i_{\mathrm{p}}^*) = \mathsf{bit}_{D-1}(i_j^*)$, opened via punctured keys $K_{i_{\mathrm{p}}^*}$ and $K_{i_0^*,\ldots,i_{\tau-1}^*}$) reveals the known branch $b_m = 1 \oplus \mathsf{bit}_i(i_j^*)$ on every coordinate $m \in [\tau D]$, lifting under challenge weights $(\alpha_m)_{m\in[\tau D]} \in (\mathbb{F}_{2^k})^{\tau D}$ to the VOLE evaluations $\vec{F}_x(\Delta^*)$ and $\vec{F}_y(\Delta^*)$.

3.2 Verification Polynomial and Cross-Tree Consistency

Using the first-challenge weights $(\alpha_m)_{m\in[\tau D]} \in (\mathbb{F}_{2^k})^{\tau D}$, the signer forms the constant VOLE mask vectors $\vec{A}_{F_x}, \vec{A}_{F_y} \in (\mathbb{F}_{2^k})^{n-2}$ from the 0-side hypercube shares [14]:

$$\vec{A}_{F_x} \leftarrow \bigoplus_{j=0}^{\tau-1} \bigoplus_{i=jD}^{(j+1)D-1} \alpha_i \, \vec{x}_j^{[\![0]\!]_{i-jD}}, \qquad \vec{A}_{F_y} \leftarrow \bigoplus_{j=0}^{\tau-1} \bigoplus_{i=jD}^{(j+1)D-1} \alpha_i \, \vec{y}_j^{[\![0]\!]_{i-jD}}. \tag{7}$$

For any formal evaluation point $\Delta \in \mathbb{F}_{2^k}$, the underlying VOLE vector polynomials are the degree-1 affine functions

$$\vec{F}_x(\Delta) = \vec{A}_{F_x} \oplus \Delta \cdot \vec{x} \in (\mathbb{F}_{2^k})^{n-2}, \qquad \vec{F}_y(\Delta) = \vec{A}_{F_y} \oplus \Delta \cdot \vec{y} \in (\mathbb{F}_{2^k})^{n-2}. \tag{8}$$

To verify that $(\vec{x}', \vec{y}') = ((\vec{x}, 1, 0), (\vec{y}, 0, 1))$ satisfies the normalised bilinear collision relation (1), the protocol embeds $\vec{F}_x(\Delta)$ and $\vec{F}_y(\Delta)$ into length-n vectors and evaluates the bilinear determinant polynomial $\Phi(\Delta) = A \oplus B\Delta \oplus C\Delta^2 \in \mathbb{F}_{2^k}[\Delta]$, whose quadratic coefficient is

$$C = \left(\vec{u} \cdot \begin{pmatrix} \vec{x} \\ 1 \\ 0 \end{pmatrix}\right)\left(\vec{v} \cdot \begin{pmatrix} \vec{y} \\ 0 \\ 1 \end{pmatrix}\right) \oplus \left(\vec{u} \cdot \begin{pmatrix} \vec{y} \\ 0 \\ 1 \end{pmatrix}\right)\left(\vec{v} \cdot \begin{pmatrix} \vec{x} \\ 1 \\ 0 \end{pmatrix}\right). \tag{9}$$

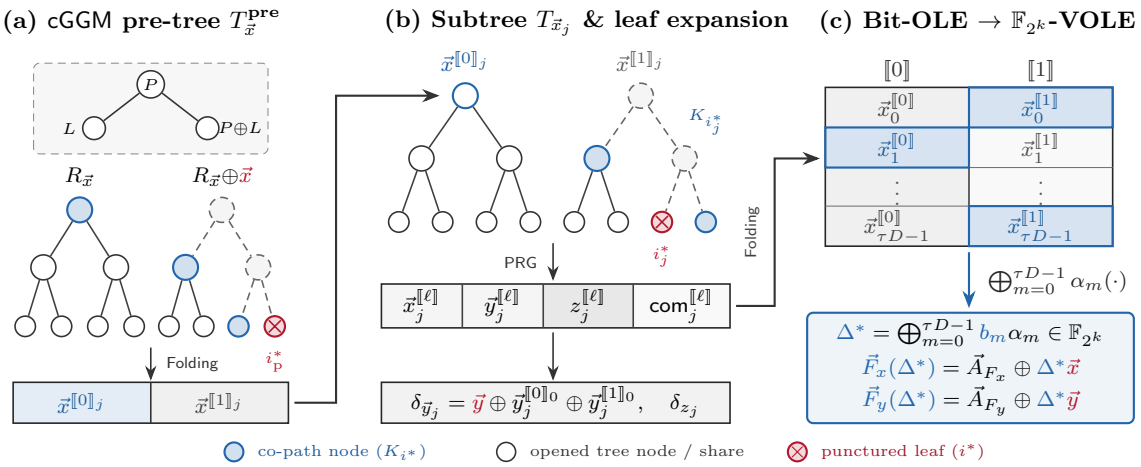


Figure 1: VOLE-in-the-Head architecture of $\mathsf{SBC}_{\mathsf{VOLE}}$ [14]. **(a)** An XOR-preserving cGGM pre-tree $T_{\vec{x}}^{\text{pre}}$ splits $(R_{\vec{x}}, R_{\vec{x}} \oplus \vec{x})$ into 2^τ leaves and folds them into τ binary root sharings $(\vec{x}^{[\![0]\!]_j}, \vec{x}^{[\![1]\!]_j})$ of $\vec{x}$. **(b)** Each second-layer tree $T_{\vec{x}_j}$ ($N = 2^D$ leaves) expands every leaf into $(\vec{x}_j^{[\![\ell]\!]}, \vec{y}_j^{[\![\ell]\!]}, z_j^{[\![\ell]\!]}, \mathsf{com}_j^{[\![\ell]\!]})$, using public offsets $(\delta_{\vec{y}_j}, \delta_{z_j})$ to align $(\vec{y}, z)$ across trees; revealing the sibling co-path $K_{i_j^*}$ (blue) opens $2^D - 1$ leaves while hiding leaf i_j^* (red). **(c)** Hypercube folding turns the opened half-cubes $b_m = 1 \oplus \mathsf{bit}_i(i_j^*)$ into τD bit-level OLEs $f_m(b_m) = \vec{x}_m^{[\![0]\!]} \oplus b_m \vec{x}$, whose α_m-weighted sum yields the $\mathbb{F}_{2^k}$-VOLE evaluations $\vec{F}_x(\Delta^*)$ and $\vec{F}_y(\Delta^*)$.

By Definition 1, $C = 0$ if and only if $(\vec{x}', \vec{y}') \in \mathsf{NSBC}[\vec{u}, \vec{v}]$, in which case $\Phi(\Delta)$ reduces to the degree-1 affine polynomial $\Phi(\Delta) = A \oplus B\Delta$. Writing $\eta \in \{0, 1\}$ for the normalisation-coordinate mask padding indicator, the constant term $A \in \mathbb{F}_{2^k}$ and linear slope $B \in \mathbb{F}_{2^k}$ are given by [14]:

$$A \leftarrow \left(\vec{u} \cdot \begin{pmatrix} \vec{A}_{F_x} \\ \eta \\ 0 \end{pmatrix}\right)\left(\vec{v} \cdot \begin{pmatrix} \vec{A}_{F_y} \\ 0 \\ \eta \end{pmatrix}\right) \oplus \left(\vec{u} \cdot \begin{pmatrix} \vec{A}_{F_y} \\ 0 \\ \eta \end{pmatrix}\right)\left(\vec{v} \cdot \begin{pmatrix} \vec{A}_{F_x} \\ \eta \\ 0 \end{pmatrix}\right), \tag{10}$$

$$\begin{aligned} B \leftarrow &\left(\vec{v} \cdot \begin{pmatrix} \vec{A}_{F_y} \\ 0 \\ \eta \end{pmatrix}\right)\left(\vec{u} \cdot \begin{pmatrix} \vec{x} \\ 1 \\ 0 \end{pmatrix}\right) \oplus \left(\vec{u} \cdot \begin{pmatrix} \vec{A}_{F_x} \\ \eta \\ 0 \end{pmatrix}\right)\left(\vec{v} \cdot \begin{pmatrix} \vec{y} \\ 0 \\ 1 \end{pmatrix}\right) \\ &\oplus \left(\vec{u} \cdot \begin{pmatrix} \vec{A}_{F_y} \\ 0 \\ \eta \end{pmatrix}\right)\left(\vec{v} \cdot \begin{pmatrix} \vec{x} \\ 1 \\ 0 \end{pmatrix}\right) \oplus \left(\vec{v} \cdot \begin{pmatrix} \vec{A}_{F_x} \\ \eta \\ 0 \end{pmatrix}\right)\left(\vec{u} \cdot \begin{pmatrix} \vec{y} \\ 0 \\ 1 \end{pmatrix}\right). \end{aligned} \tag{11}$$

Normalisation-Coordinate Padding ($\eta \in \{0, 1\}$). Setting $\eta = 1$ in (10)–(11) places $(1, 0)$ and $(0, 1)$ in the last two coordinates of $\vec{A}_{F_x}, \vec{A}_{F_y}$ as printed in [14, Figure 5], whereas setting $\eta = 0$ shares the fixed coordinates homogeneously as $0 \oplus 1 \cdot \Delta$ (so $(\vec{F}_x(\Delta), \Delta, 0)$ and $(\vec{F}_y(\Delta), 0, \Delta)$ scale uniformly with Δ), as implemented in the authors' official reference artifact. Carrying $\eta \in \{0, 1\}$ throughout Section 4 covers both conventions simultaneously; η shifts only a known public constant in the linear coefficients and has no effect on the quadratic cancellation.

In addition to A and B, the signer computes the cross-tree consistency responses [14]:

$$b \leftarrow z \oplus \vec{y} \cdot \vec{\mu} \in \mathbb{F}_{2^k}, \qquad a^{(j)} \leftarrow \vec{A}_{F_y}^{(j)} \cdot \vec{\mu} \oplus A_{F_z}^{(j)} \in \mathbb{F}_{2^k} \quad (j \in [\tau]), \tag{12}$$

where $\vec{A}_{F_y}^{(j)} = \bigoplus_{i=jD}^{(j+1)D-1} \alpha_i \vec{y}_j^{[\![0]\!]_{i-jD}}$ and $A_{F_z}^{(j)} = \bigoplus_{i=jD}^{(j+1)D-1} \alpha_i z_j^{[\![0]\!]_{i-jD}}$, corresponding to the per-tree VOLE polynomials $\vec{F}_y^{(j)}(\Delta_j) = \vec{A}_{F_y}^{(j)} \oplus \Delta_j \vec{y}$ and $Z^{(j)}(\Delta_j) = A_{F_z}^{(j)} \oplus \Delta_j z$ at $\Delta_j = \bigoplus_{i=jD}^{(j+1)D-1} b_i \alpha_i$.

3.3 Five-Pass Identification Protocol and Fiat–Shamir Signature

Figure 2 illustrates the five-pass interactive identification protocol between Prover $\mathcal{P}(\mathsf{pk}, \mathsf{sk})$ and Verifier $\mathcal{V}(\mathsf{pk})$, together with its compilation into a non-interactive signature σ [14, Sections 4–5].

Interactive Five-Pass Identification Protocol (Figure 2a, Left). The interactive proof of knowledge of $(\vec{x}', \vec{y}') \in \mathsf{NSBC}[\vec{u}, \vec{v}]$ proceeds across five passes:

- **Pass 1 (Commitment, $\mathcal{P} \to \mathcal{V}$):** $\mathcal{P}$ samples $R_{\vec{x}} \xleftarrow{\$} \mathbb{F}_2^{n-2}$ and $\mathsf{salt} \xleftarrow{\$} \{0,1\}^{2\lambda}$, generates the correlated cGGM forest $(T_{\vec{x}}^{\mathrm{pre}}, T_{\vec{x}_0}, \ldots, T_{\vec{x}_{\tau-1}})$, expands and folds all leaf shares, computes the alignment offsets $(\delta_{\vec{y}_j})_{j\in[\tau]}$ and $(\delta_{z_j})_{j\in[\tau]^*}$ via (6) as well as the global commitment digest h_{com}, and sends $\big(h_{\mathsf{com}}, \mathsf{salt}, (\delta_{\vec{y}_j})_{j\in[\tau]}, (\delta_{z_j})_{j\in[\tau]^*}, (X_j)_{j\in[\tau]}\big)$ to $\mathcal{V}$ (with $(X_j)_{j\in[\tau]}$ omitted in $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$).
- **Pass 2 (First Challenge, $\mathcal{V} \to \mathcal{P}$):** $\mathcal{V}$ samples the cross-tree consistency vector $\vec{\mu} \xleftarrow{\$} (\mathbb{F}_{2^k})^{n-2}$ and the VOLE lifting weights $(\alpha_m)_{m\in[\tau D]} \xleftarrow{\$} (\mathbb{F}_{2^k})^{\tau D}$, and sends $\big(\vec{\mu}, (\alpha_m)_{m\in[\tau D]}\big)$ to $\mathcal{P}$.
- **Pass 3 (First Response, $\mathcal{P} \to \mathcal{V}$):** From the 0-side hypercube shares and the Pass 2 challenges, $\mathcal{P}$ computes the VOLE mask vectors $(\vec{A}_{F_x}, \vec{A}_{F_y})$ via (7), evaluates the verification coefficients $(A, B) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ via (10)–(11) and the consistency responses $b \in \mathbb{F}_{2^k}$ and $(a^{(j)})_{j\in[\tau]} \in (\mathbb{F}_{2^k})^{\tau}$ via (12), and sends $\big(A, B, (a^{(j)})_{j\in[\tau]}, b\big)$ to $\mathcal{V}$.
- **Pass 4 (Second Challenge, $\mathcal{V} \to \mathcal{P}$):** $\mathcal{V}$ samples one punctured leaf index $i_j^* \xleftarrow{\$} [2^D]$ for each tree $j \in [\tau]$, implicitly fixing the complementary branch bits $b_m = 1 \oplus \mathsf{bit}_i(i_j^*)$ and the evaluation points $(\Delta_j^*)_{j\in[\tau]}$ and $\Delta^* = \bigoplus_{j=0}^{\tau-1} \Delta_j^*$, and sends $(i_j^*)_{j\in[\tau]}$ to $\mathcal{P}$.
- **Pass 5 (Second Response and Verification, $\mathcal{P} \to \mathcal{V}$):** $\mathcal{P}$ forms the pre-tree index $i_{\mathrm{p}}^* = \sum_{j=0}^{\tau-1} \mathsf{bit}_{D-1}(i_j^*) 2^j$ and sends the punctured forest keys $(K_{i_{\mathrm{p}}^*}, K_{i_0^*,\ldots,i_{\tau-1}^*})$ to $\mathcal{V}$ (aborting and restarting in $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$ if any i_j^* hits a commitment extremum). Using the opened leaves and Pass 1 offsets, $\mathcal{V}$ recomputes h'_{com}, $(\vec{F}_y^{(j)}(\Delta_j^*), Z^{(j)}(\Delta_j^*))_{j\in[\tau]}$, and $(\vec{F}_x(\Delta^*), \vec{F}_y(\Delta^*))$, and accepts if and only if $h'_{\mathsf{com}} = h_{\mathsf{com}}$, $Z^{(j)}(\Delta_j^*) \oplus \vec{F}_y^{(j)}(\Delta_j^*) \cdot \vec{\mu} = a^{(j)} \oplus b\Delta_j^*$ for all $j \in [\tau]$, and $\Phi(\Delta^*) = A \oplus B\Delta^*$.

Non-Interactive Fiat–Shamir Signature (Figure 2a, Right & 2b). Applying the five-pass Fiat–Shamir transform [10] to sign a message $\mathsf{msg} \in \{0,1\}^*$ replaces $\mathcal{V}$'s two interactive challenges with random-oracle digests expanded via PRGs:

- **First Challenge Digest ($H_0 \to \mathsf{PRG}_0$):** After running Pass 1, the signer hashes msg and the commitment transcript into

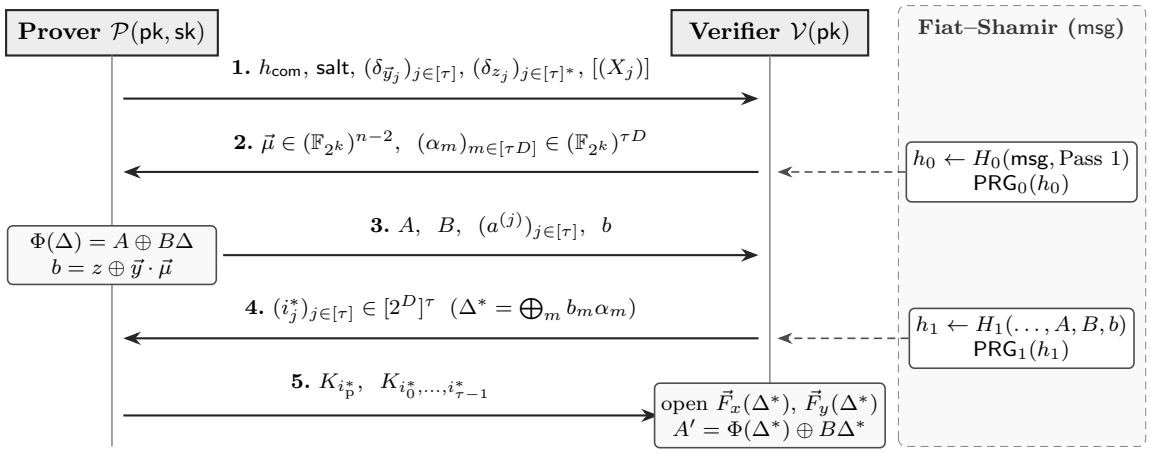
$$h_0 \leftarrow H_0\big(\mathsf{msg}, h_{\mathsf{com}}, \mathsf{salt}, (\delta_{\vec{y}_j}, \delta_{z_j})_{j\in[\tau]}, (X_j)_{j\in[\tau]}\big), \tag{13}$$

  and expands $\big(\vec{\mu}, (\alpha_m)_{m\in[\tau D]}\big) \leftarrow \mathsf{PRG}_0(h_0)$ locally in place of Pass 2.
- **Second Challenge Digest ($H_1 \to \mathsf{PRG}_1$):** After computing the Pass 3 responses $\big(A, B, (a^{(j)})_{j\in[\tau]}, b\big)$, the signer hashes them together with h_0 into

$$h_1 \leftarrow H_1\Big(\mathsf{msg}, h_{\mathsf{com}}, \mathsf{salt}, (\delta_{\vec{y}_j}, \delta_{z_j})_{j\in[\tau]}, h_0, A, B, (a^{(j)})_{j\in[\tau]}, b\Big), \tag{14}$$

  and derives the punctured leaf indices $(i_j^*)_{j\in[\tau]} \leftarrow \mathsf{PRG}_1(h_1)$ in place of Pass 4.

(a) Five-pass identification protocol and Fiat–Shamir transform:



(b) Non-interactive signature σ layout:

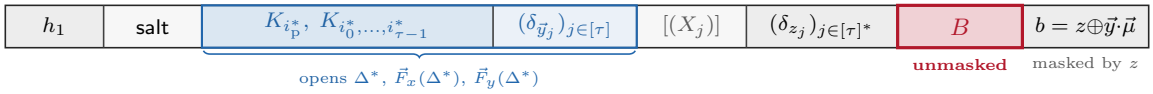


Figure 2: Protocol flow and vulnerability location in $\mathsf{SBC}_{\mathsf{VOLE}}$ and $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$. **(a)** Five-pass identification protocol between $\mathcal{P}$ and $\mathcal{V}$ with Fiat–Shamir hashes H_0, H_1. While A and $(a^{(j)})_{j\in[\tau]}$ are absorbed into h_1 and $b=z\oplus\vec{y}\cdot\vec{\mu}$ is one-time-pad masked by z, the degree-1 slope $B\in\mathbb{F}_{2^k}$ in Pass 3 is transmitted unmasked so that $\mathcal{V}$ can reconstruct $A'=\Phi(\Delta^*)\oplus B\Delta^*$. **(b)** Resulting signature σ, exposing unmasked B (red) alongside the punctured keys and $\vec{y}$-offsets (blue) that open $\vec{F}_x(\Delta^*)$ and $\vec{F}_y(\Delta^*)$.

- **Transcript Compression and Signature Format:** During verification, $\mathcal{V}$ derives $(i^*_j)_{j\in[\tau]}\leftarrow\mathsf{PRG}_1(h_1)$, opens the punctured forest to recover h'_{com}, h'_0, and the VOLE evaluations, reconstructs $A'\leftarrow\Phi(\Delta^*)\oplus B\Delta^*$ and $a'^{(j)}\leftarrow Z^{(j)}(\Delta^*_j)\oplus\vec{F}^{(j)}_y(\Delta^*_j)\cdot\vec{\mu}\oplus b\Delta^*_j$ $(j\in[\tau])$, and checks $h'_1=h_1$. Because h_0, A, and $(a^{(j)})_{j\in[\tau]}$ are deterministically recomputed by $\mathcal{V}$, they are omitted from transmission, yielding the signature tuple

$$\sigma=\Big(h_1,\ \mathsf{salt},\ (\delta_{\vec{y}_j})_{j\in[\tau]},\ (\delta_{z_j})_{j\in[\tau]^*},\ B,\ b,\ K_{i^*_{\mathrm{p}}},\ K_{i^*_0,\ldots,i^*_{\tau-1}},\ (X_j)_{j\in[\tau]}\Big), \tag{15}$$

  where $(X_j)_{j\in[\tau]}$ is omitted in the MinMax variant $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$.

Forced Exposure of B by Protocol Design. Notice the fundamental asymmetry highlighted in Figure 2 between $b=z\oplus\vec{y}\cdot\vec{\mu}$ and B in (15):

- In (12), the linear combination $\vec{y}\cdot\vec{\mu}$ is explicitly masked by the random field element $z\in\mathbb{F}_{2^k}$. Indeed, the authors state in Remark 4 [14, p. 14, full version]: *"Note that the goal of z is to act as a one-time-pad and hide the value $\vec{\mu}\cdot\vec{y}$ which would, if revealed, leak the secret $\vec{y}$."*
- By contrast, the coefficient $B\in\mathbb{F}_{2^k}$ in (11) is placed directly into σ without any additive mask. This omission is an intentional bandwidth-saving design choice rather than a typographical slip or implementation oversight: the published signature-size formulas $\lambda^2+5\tau\lambda+7\lambda$ bits for $\mathsf{SBC}_{\mathsf{VOLE}}$ and $\lambda^2+3\tau\lambda+7\lambda$ bits for $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$ [14, Sections 5.2 and 6.1] budget strictly $\tau+1$ elements of $\mathbb{F}_{2^k}$, namely $(\delta_{z_j})_{j\in[\tau]^*}$, B, and b, leaving zero room for the $(\tau-1)$ per-tree alignment offsets that a second VOLE mask would require, and both the EUF-CMA proof [14, Appendix A, full version] and the official reference implementation follow this unmasked specification verbatim.

Furthermore, transmitting B (or an equivalent unmasked value) is structurally forced by verification. Because A and $(a^{(j)})_{j\in[\tau]}$ are omitted from σ to save $(1+\tau)k$ bits of bandwidth, the verifier must reconstruct A' after learning the second-round challenge point Δ^* via

$$A' \leftarrow \Phi(\Delta^*) \oplus B\Delta^* \tag{16}$$

and check that $H_1(\mathsf{msg}, h'_{\mathsf{com}}, \mathsf{salt}, (\delta_{\vec{y}_j}, \delta_{z_j})_{j\in[\tau]}, h'_0, A', B, (a'^{(j)})_{j\in[\tau]}, b) = h_1$. Since h_1 commits to A before Δ^* is derived from $\mathsf{PRG}_1(h_1)$, $B = (\Phi(\Delta^*) \oplus A) \cdot (\Delta^*)^{-1}$ is the unique field element allowing A' to match A. Even if σ transmitted A instead of B, any observer would compute $B = (\Phi(\Delta^*) \oplus A) \cdot (\Delta^*)^{-1}$ whenever $\Delta^* \neq 0$ (probability $1 - 2^{-k}$).

3.4 Public Transcript Reconstructed by Verification

Given only the public key $\mathsf{pk} = (\vec{u}, \vec{v})$, a message msg, and a valid signature σ, the deterministic verification algorithm [14, Section 5] computes the following public quantities:

1. **Opened Branch Bits and First-Round Challenges:** From $(i^*_j)_{j\in[\tau]} \leftarrow \mathsf{PRG}_1(h_1)$, the verifier expands all punctured trees using $K_{i^*_{\mathrm{p}}}, K_{i^*_0,\ldots,i^*_{\tau-1}}$ and salt. For each tree $j \in [\tau]$ and bit axis $i \in [D]$, $b_{i,j} = 1 \oplus \mathsf{bit}_i(i^*_j) \in \{0,1\}$ indexes the known hypercube share $\vec{x}_j^{[\![b_{i,j}]\!]_i}$. Recomputing the leaf commitments yields h'_{com}, $h'_0 \leftarrow H_0(\ldots)$, and $(\vec{\mu}, (\alpha_m)_{m\in[\tau D]}) \leftarrow \mathsf{PRG}_0(h'_0)$.

2. **Global Evaluation Point Δ^*:** Writing $b_m = b_{m-jD,j}$ for $m = jD + i \in [\tau D]$, the verifier computes the per-tree and global evaluation points:

$$\Delta^*_j \leftarrow \bigoplus_{i=jD}^{(j+1)D-1} b_{i-jD,j}\,\alpha_i, \qquad \Delta^* \leftarrow \bigoplus_{j=0}^{\tau-1} \Delta^*_j = \bigoplus_{m=0}^{\tau D-1} b_m\,\alpha_m \in \mathbb{F}_{2^k}. \tag{17}$$

3. **Punctured VOLE Evaluations $\vec{F}_x(\Delta^*)$ and $\vec{F}_y(\Delta^*)$:** Using the known b_m-side shares and the transmitted offsets $(\delta_{\vec{y}_j})_{j\in[\tau]}$, the verifier reconstructs:

$$\vec{F}_x(\Delta^*) \leftarrow \bigoplus_{m=0}^{\tau D-1} \alpha_m\,\vec{x}_m^{[\![b_m]\!]} \in (\mathbb{F}_{2^k})^{n-2}, \tag{18}$$

$$\vec{F}_y(\Delta^*) \leftarrow \bigoplus_{j=0}^{\tau-1} \bigoplus_{i=jD}^{(j+1)D-1} \alpha_i \left(\vec{y}_j^{[\![b_{i-jD,j}]\!]_{i-jD}} \oplus b_{i-jD,j}\,\delta_{\vec{y}_j}\right) \in (\mathbb{F}_{2^k})^{n-2}. \tag{19}$$

Because every quantity in (17)–(19) is computed publicly from $(\mathsf{pk}, \mathsf{msg}, \sigma)$, any passive observer holding a single valid signature knows the tuple $\big(\vec{u}, \vec{v}, B, \Delta^*, \vec{F}_x(\Delta^*), \vec{F}_y(\Delta^*)\big)$.

4 Single-Signature Secret-Key Recovery

We now prove that combining the transmitted coefficient $B \in \mathbb{F}_{2^k}$ with the verifier's reconstructed VOLE evaluations $(\vec{F}_x(\Delta^*), \vec{F}_y(\Delta^*))$ reduces key recovery to solving a single binary linear system.

4.1 Mask Elimination via Public VOLE Evaluations

Although B in (11) is formed from the signer's unopened 0-side VOLE masks $\vec{A}_{F_x}, \vec{A}_{F_y} \in (\mathbb{F}_{2^k})^{n-2}$, evaluating the VOLE affine relation (8) at $\Delta = \Delta^*$ expresses both hidden masks in terms of the public openings and the secret key:

$$\vec{A}_{F_x} = \vec{F}_x(\Delta^*) \oplus \Delta^*\vec{x}, \qquad \vec{A}_{F_y} = \vec{F}_y(\Delta^*) \oplus \Delta^*\vec{y}. \tag{20}$$

That is, conditioned on $\vec{F}_x(\Delta^*)$ and $\vec{F}_y(\Delta^*)$, the masks $\vec{A}_{F_x}$ and $\vec{A}_{F_y}$ retain no secret randomness independent of $(\vec{x}, \vec{y})$.

To substitute (20) into (11), partition $\vec{u}, \vec{v} \in (\mathbb{F}_{2^k})^n$ into their prefix vectors $\bar{u} = (u_0, \ldots, u_{n-3})$ and $\bar{v} = (v_0, \ldots, v_{n-3})$ in $(\mathbb{F}_{2^k})^{n-2}$, together with their final two coordinates

$$c := u_{n-2}, \qquad e := v_{n-2}, \qquad f := u_{n-1}, \qquad g := v_{n-1}.$$

Define the four unknown $\mathbb{F}_2$-linear witness projections

$$P(\vec{x}) := \bigoplus_{i=0}^{n-3} u_i x_i, \quad Q(\vec{x}) := \bigoplus_{i=0}^{n-3} v_i x_i, \quad R(\vec{y}) := \bigoplus_{i=0}^{n-3} u_i y_i, \quad S(\vec{y}) := \bigoplus_{i=0}^{n-3} v_i y_i, \tag{21}$$

and the four publicly computable inner products of $\bar{u}, \bar{v}$ with $\vec{F}_x(\Delta^*), \vec{F}_y(\Delta^*)$:

$$U_x^* := \bar{u} \cdot \vec{F}_x(\Delta^*), \quad V_x^* := \bar{v} \cdot \vec{F}_x(\Delta^*), \quad U_y^* := \bar{u} \cdot \vec{F}_y(\Delta^*), \quad V_y^* := \bar{v} \cdot \vec{F}_y(\Delta^*). \tag{22}$$

By (21), the four witness inner products in (11) take the form

$$\begin{aligned} \vec{u} \cdot (\vec{x}, 1, 0) &= P(\vec{x}) \oplus c, & \vec{v} \cdot (\vec{x}, 1, 0) &= Q(\vec{x}) \oplus e, \\ \vec{u} \cdot (\vec{y}, 0, 1) &= R(\vec{y}) \oplus f, & \vec{v} \cdot (\vec{y}, 0, 1) &= S(\vec{y}) \oplus g, \end{aligned} \tag{23}$$

while substituting (20) into the four mask inner products in (11) gives

$$\begin{aligned} \vec{u} \cdot (\vec{A}_{F_x}, \eta, 0) &= U_x^* \oplus \Delta^* P(\vec{x}) \oplus \eta c, & \vec{v} \cdot (\vec{A}_{F_x}, \eta, 0) &= V_x^* \oplus \Delta^* Q(\vec{x}) \oplus \eta e, \\ \vec{u} \cdot (\vec{A}_{F_y}, 0, \eta) &= U_y^* \oplus \Delta^* R(\vec{y}) \oplus \eta f, & \vec{v} \cdot (\vec{A}_{F_y}, 0, \eta) &= V_y^* \oplus \Delta^* S(\vec{y}) \oplus \eta g, \end{aligned} \tag{24}$$

where $\eta \in \{0, 1\}$ denotes the normalisation-coordinate padding indicator defined in Section 3.

4.2 Pairwise Quadratic Cancellation in Characteristic Two

To keep the proof of our main key-recovery theorem modular, we first isolate the algebraic collapse of the verification slope B into an exact $\mathbb{F}_2$-affine functional of the secret key $(\vec{x}, \vec{y})$.

Lemma 1 (Closed-Form $\mathbb{F}_2$-Affine Structure of B)**.** *In both* $\mathsf{SBC}_{\mathsf{VOLE}}$ *and* $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$*, for any public key* $\mathsf{pk} = (\vec{u}, \vec{v})$ *and any signature transcript with reconstructed evaluation point* Δ^* *and punctured VOLE evaluations* $\vec{F}_x(\Delta^*), \vec{F}_y(\Delta^*)$*, the transmitted coefficient* $B \in \mathbb{F}_{2^k}$ *is an exact* $\mathbb{F}_2$*-affine functional of the secret key* $(\vec{x}, \vec{y}) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_2^{n-2}$*:*

$$B = c_P P(\vec{x}) \oplus c_Q Q(\vec{x}) \oplus c_R R(\vec{y}) \oplus c_S S(\vec{y}) \oplus \gamma_\sigma = \bigoplus_{i=0}^{n-3} x_i \, \beta_i^{(x)} \oplus \bigoplus_{i=0}^{n-3} y_i \, \beta_i^{(y)} \oplus \gamma_\sigma, \tag{25}$$

where the public scalar coefficients $c_P, c_Q, c_R, c_S, \gamma_\sigma \in \mathbb{F}_{2^k}$ *are given by*

$$\begin{aligned} c_P &= V_y^* \oplus (\eta \oplus \Delta^*) g, & c_Q &= U_y^* \oplus (\eta \oplus \Delta^*) f, \\ c_R &= V_x^* \oplus (\eta \oplus \Delta^*) e, & c_S &= U_x^* \oplus (\eta \oplus \Delta^*) c, \\ \gamma_\sigma &= c V_y^* \oplus g U_x^* \oplus e U_y^* \oplus f V_x^*, \end{aligned} \tag{26}$$

and for each coordinate $i \in [n-2]$*, the column field elements* $\beta_i^{(x)}, \beta_i^{(y)} \in \mathbb{F}_{2^k}$ *are*

$$\beta_i^{(x)} = c_P u_i \oplus c_Q v_i, \qquad \beta_i^{(y)} = c_R u_i \oplus c_S v_i. \tag{27}$$

Proof. In (11), the unknown witness $(\vec{x}, \vec{y})$ is multiplied against the prover's unopened 0-side VOLE masks $(\vec{A}_{F_x}, \vec{A}_{F_y})$. Once verification opens the punctured trees at the challenge point Δ^*, however, the affine VOLE relations (20) express both hidden masks as public evaluations shifted by $\Delta^*\vec{x}$ and $\Delta^*\vec{y}$. Substituting an affine function of $(\vec{x}, \vec{y})$ into a bilinear form generically produces degree-2 cross-terms in $(\vec{x}, \vec{y})$; the core mechanism is that the skew-symmetric determinant structure of SBC pairs every quadratic cross-term with an identical counterpart, and in characteristic 2 these paired quadratic terms cancel identically. We proceed in three steps: (1) expanding the four bilinear summands T_1, T_2, T_3, T_4 of B under (23)–(24); (2) establishing the pairwise characteristic-2 cancellation of all degree-2 witness terms and η-dependent constants; and (3) collecting the surviving degree-1 projections over the binary coordinates $(x_i, y_i) \in \mathbb{F}_2$.

Step 1: Bilinear expansion under VOLE mask substitution. Write $B = T_1 \oplus T_2 \oplus T_3 \oplus T_4$ for the four bilinear summands in (11). Substituting the witness inner products (23) and the mask inner products (24) into each summand and expanding by distributivity over $\mathbb{F}_{2^k}$ yields:

$$\begin{aligned} T_1 &= \big(V_y^* \oplus \Delta^* S(\vec{y}) \oplus \eta g\big)\big(P(\vec{x}) \oplus c\big) \\ &= \underline{\Delta^* S(\vec{y})P(\vec{x})} \oplus (V_y^* \oplus \eta g)P(\vec{x}) \oplus \Delta^* c\, S(\vec{y}) \oplus c(V_y^* \oplus \eta g), \end{aligned} \tag{28}$$

$$\begin{aligned} T_2 &= \big(U_x^* \oplus \Delta^* P(\vec{x}) \oplus \eta c\big)\big(S(\vec{y}) \oplus g\big) \\ &= \underline{\Delta^* P(\vec{x})S(\vec{y})} \oplus \Delta^* g\, P(\vec{x}) \oplus (U_x^* \oplus \eta c)S(\vec{y}) \oplus g(U_x^* \oplus \eta c), \end{aligned} \tag{29}$$

$$\begin{aligned} T_3 &= \big(U_y^* \oplus \Delta^* R(\vec{y}) \oplus \eta f\big)\big(Q(\vec{x}) \oplus e\big) \\ &= \underline{\underline{\Delta^* R(\vec{y})Q(\vec{x})}} \oplus (U_y^* \oplus \eta f)Q(\vec{x}) \oplus \Delta^* e\, R(\vec{y}) \oplus e(U_y^* \oplus \eta f), \end{aligned} \tag{30}$$

$$\begin{aligned} T_4 &= \big(V_x^* \oplus \Delta^* Q(\vec{x}) \oplus \eta e\big)\big(R(\vec{y}) \oplus f\big) \\ &= \underline{\underline{\Delta^* Q(\vec{x})R(\vec{y})}} \oplus \Delta^* f\, Q(\vec{x}) \oplus (V_x^* \oplus \eta e)R(\vec{y}) \oplus f(V_x^* \oplus \eta e). \end{aligned} \tag{31}$$

Step 2: Pairwise quadratic cancellation in characteristic two. Summing (28)–(29) and (30)–(31), commutativity of multiplication in $\mathbb{F}_{2^k}$ together with the characteristic-2 identity $Z \oplus Z = 0$ cancels the underlined degree-2 witness cross-terms pairwise (Figure 3a):

$$\Delta^* S(\vec{y})P(\vec{x}) \oplus \Delta^* P(\vec{x})S(\vec{y}) = 0, \qquad \Delta^* R(\vec{y})Q(\vec{x}) \oplus \Delta^* Q(\vec{x})R(\vec{y}) = 0. \tag{32}$$

Similarly, in the degree-0 constant terms of $T_1 \oplus T_2$ and $T_3 \oplus T_4$, the η-dependent products cancel via $c(\eta g) \oplus g(\eta c) = 0$ and $e(\eta f) \oplus f(\eta e) = 0$. Equation (32) holds identically as a polynomial identity over $\mathbb{F}_{2^k}$ without invoking the NSBC constraint (1).

Step 3: Grouping of $\mathbb{F}_2$-linear projections and coordinate columns. Collecting the surviving degree-1 coefficients of $P(\vec{x})$ and $S(\vec{y})$ in $T_1 \oplus T_2$, those of $Q(\vec{x})$ and $R(\vec{y})$ in $T_3 \oplus T_4$, and the remaining degree-0 terms produces the first equality in (25) with public scalars $c_P, c_Q, c_R, c_S, \gamma_\sigma$ given by (26). Finally, substituting the linear definitions of $P(\vec{x}), Q(\vec{x}), R(\vec{y}), S(\vec{y})$ from (21) gives

$$c_P P(\vec{x}) \oplus c_Q Q(\vec{x}) = \bigoplus_{i=0}^{n-3} x_i(c_P u_i \oplus c_Q v_i), \qquad c_R R(\vec{y}) \oplus c_S S(\vec{y}) = \bigoplus_{i=0}^{n-3} y_i(c_R u_i \oplus c_S v_i),$$

which establishes the second equality in (25) with column elements $\beta_i^{(x)}, \beta_i^{(y)}$ defined by (27). □

Generalisation to Odd Characteristic ($q > 2$). Although Lemma 1 uses characteristic 2 to cancel the quadratic terms identically for arbitrary pairs $(\vec{x}, \vec{y})$, honest signatures collapse linearly over *every* finite field extension $\mathbb{F}_{q^k}/\mathbb{F}_q$ ($q \geq 2$). Writing $\Phi(\Delta) = (\vec{u} \cdot \vec{F}'_x(\Delta))(\vec{v} \cdot \vec{F}'_y(\Delta)) - (\vec{u} \cdot \vec{F}'_y(\Delta))(\vec{v} \cdot \vec{F}'_x(\Delta)) = A + B\Delta + C\Delta^2$ with $\vec{F}'_x(\Delta) = \vec{A}'_{F_x} + \Delta\vec{x}'$ and $\vec{F}'_y(\Delta) = \vec{A}'_{F_y} + \Delta\vec{y}'$, Taylor-expanding around Δ^* gives $B = \Phi'(\Delta^*) - 2\Delta^* C$, where the formal derivative $\Phi'(\Delta^*) =$

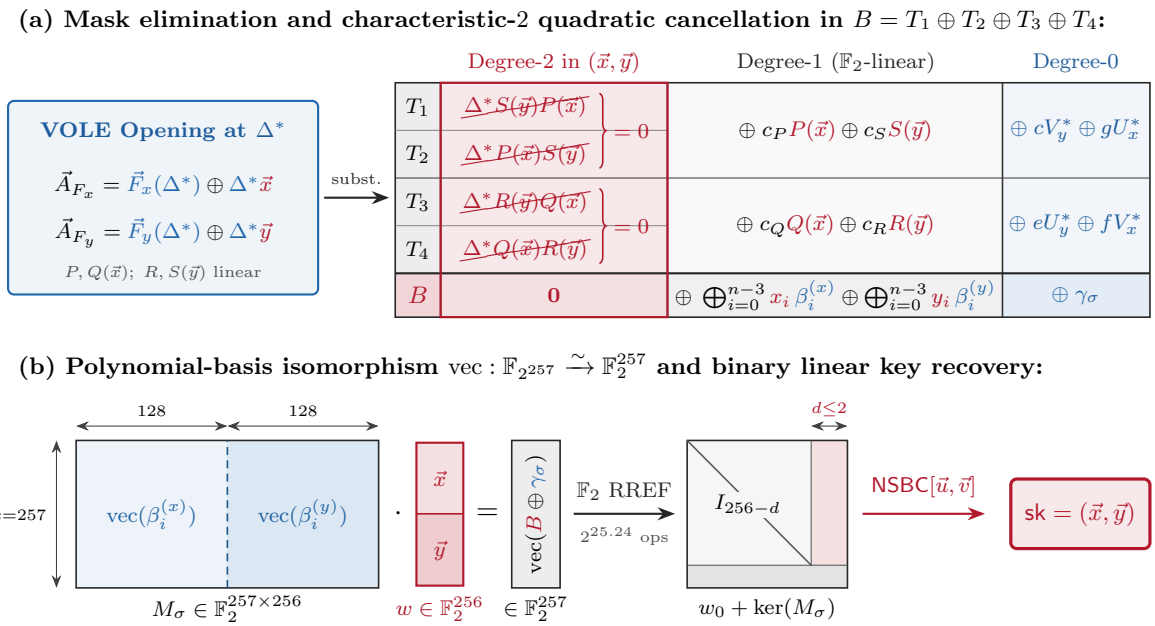


Figure 3: Visualisation of single-signature secret-key recovery (Lemma 1, Theorem 1, and Algorithm 1). **(a)** Substituting the public VOLE evaluations $\vec{A}_{F_x} = \vec{F}_x(\Delta^*) \oplus \Delta^* \vec{x}$ and $\vec{A}_{F_y} = \vec{F}_y(\Delta^*) \oplus \Delta^* \vec{y}$ (blue) into $B = T_1 \oplus T_2 \oplus T_3 \oplus T_4$ cancels every quadratic cross-term in $(\vec{x}, \vec{y})$ pairwise in characteristic 2, collapsing B to a noiseless $\mathbb{F}_2$-affine functional. **(b)** Expanding over the polynomial basis of $\mathbb{F}_{2^{257}}$ yields a 257×256 binary system $M_\sigma w = \mathrm{vec}(B \oplus \gamma_\sigma)$ with kernel dimension $d \le 2$, uniquely solved via Gaussian elimination and the public NSBC test.

$(\vec{u} \cdot \vec{x}')(\vec{v} \cdot \vec{F}_y'(\Delta^*)) + (\vec{u} \cdot \vec{F}_x'(\Delta^*))(\vec{v} \cdot \vec{y}') - (\vec{u} \cdot \vec{y}')(\vec{v} \cdot \vec{F}_x'(\Delta^*)) - (\vec{u} \cdot \vec{F}_y'(\Delta^*))(\vec{v} \cdot \vec{x}')$ is $\mathbb{F}_q$-affine in $(\vec{x}, \vec{y})$ with publicly computable coefficients. Characteristic 2 forces $2\Delta^* C \equiv 0$ everywhere (even on invalid dummy witnesses in Section 5), whereas for $q > 2$ the residual $-2\Delta^* C$ vanishes on every honest witness because $C = 0$ by (1), again yielding k noiseless $\mathbb{F}_q$-linear equations in the $2(n-2)$ secret $\mathbb{F}_q$-coordinates whenever $k \ge 2(n-2)$.

4.3 Binary Linear System and Complexity Analysis

Applying the polynomial-basis isomorphism $\mathrm{vec} : \mathbb{F}_{2^k} \xrightarrow{\sim} \mathbb{F}_2^k$ from (3) to both sides of (25) (Figure 3b) converts a single equation in $\mathbb{F}_{2^k}$ into k linear equations over $\mathbb{F}_2$ in the $2(n-2)$ secret key bits $w = (x_0, \ldots, x_{n-3}, y_0, \ldots, y_{n-3})^\top \in \mathbb{F}_2^{2(n-2)}$:

$$M_\sigma \cdot w = \mathrm{vec}(B \oplus \gamma_\sigma), \tag{33}$$

where $M_\sigma \in \mathbb{F}_2^{k \times 2(n-2)}$ is the public binary matrix

$$M_\sigma = \Big[\mathrm{vec}(\beta_0^{(x)}) \ \cdots \ \mathrm{vec}(\beta_{n-3}^{(x)}) \ \Big| \ \mathrm{vec}(\beta_0^{(y)}) \ \cdots \ \mathrm{vec}(\beta_{n-3}^{(y)}) \Big]. \tag{34}$$

Theorem 1 (Single-Signature Secret-Key Recovery)**.** *Let* $(\mathsf{pk}, \mathsf{sk})$ *be any key pair of* $\mathsf{SBC}_{\mathsf{VOLE}}$ *or* $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$ *over* $\mathbb{F}_{2^k}/\mathbb{F}_2$*, and let* σ *be any honestly generated signature on a message* msg *inducing a linear system* (33) *of kernel dimension* $d = 2(n-2) - \mathrm{rank}(M_\sigma)$*. Then Algorithm 1 returns a non-empty witness set* $\mathcal{W}_\sigma \subseteq \mathsf{NSBC}[\vec{u}, \vec{v}]$ *of size at most* 2^d *that contains the signer's secret key* $\mathsf{sk} = (\vec{x}, \vec{y})$*, using (to leading order in Gaussian elimination)*

$$T(n,k) = \underbrace{4(n-2)k^2}_{\text{forming } \beta_i^{(x)}, \beta_i^{(y)}} + \underbrace{\frac{1}{3}k\big(2(n-2)\big)^2}_{\text{GF(2) elimination}} + \underbrace{2^d\big(4(n-2)k + 2k^2\big)}_{\text{NSBC candidate check}} \tag{35}$$

Algorithm 1: Single-Signature Secret-Key Recovery against $\mathsf{SBC}_{\mathsf{VOLE}}$ and $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$

Input: Public key $\mathsf{pk} = (\vec{u}, \vec{v}) \in (\mathbb{F}_{2^k})^n \times (\mathbb{F}_{2^k})^n$, message msg, valid signature σ.
Output: Candidate witness set $\mathcal{W}_\sigma \subseteq \mathsf{NSBC}[\vec{u}, \vec{v}]$ containing $\mathsf{sk} = (\vec{x}, \vec{y})$.

1. Run the public verification reconstruction (Section 3.4) on $(\mathsf{pk}, \mathsf{msg}, \sigma)$ to obtain $\Delta^* \in \mathbb{F}_{2^k}$ and $\vec{F}_x(\Delta^*), \vec{F}_y(\Delta^*) \in (\mathbb{F}_{2^k})^{n-2}$.
2. Compute $U_x^*, V_x^*, U_y^*, V_y^* \in \mathbb{F}_{2^k}$ via (22) and $c_P, c_Q, c_R, c_S, \gamma_\sigma \in \mathbb{F}_{2^k}$ via (26).
3. for $i = 0$ **to** $n-3$ **do**
  Compute $\beta_i^{(x)} \leftarrow c_P u_i \oplus c_Q v_i$ and $\beta_i^{(y)} \leftarrow c_R u_i \oplus c_S v_i$ in $\mathbb{F}_{2^k}$.
  Set column i of M_σ to $\mathrm{vec}(\beta_i^{(x)})$ and column $(n-2+i)$ of M_σ to $\mathrm{vec}(\beta_i^{(y)})$.
4. Solve the $k \times 2(n-2)$ binary linear system $M_\sigma w = \mathrm{vec}(B \oplus \gamma_\sigma)$ over $\mathbb{F}_2$ via Gaussian elimination to obtain a particular solution w_0 and a basis of $\ker(M_\sigma)$, where $d = 2(n-2) - \mathrm{rank}(M_\sigma)$.
5. Return $\mathcal{W}_\sigma \leftarrow \{(\tilde{\vec{x}}, \tilde{\vec{y}}) : (\tilde{\vec{x}}, \tilde{\vec{y}})^\top \in w_0 + \ker(M_\sigma) \text{ and } ((\tilde{\vec{x}}, 1, 0), (\tilde{\vec{y}}, 0, 1)) \in \mathsf{NSBC}[\vec{u}, \vec{v}]\}$.

elementary bit operations beyond a single signature verification.

Proof. Lemma 1 reduces the verification slope B to a single scalar equation over $\mathbb{F}_{2^k}$ in the binary coordinates of $(\vec{x}, \vec{y}) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_2^{n-2}$. Following the classical subfield-basis expansion (Weil restriction) used by Huth and Joux [13, Section 2.2] to expand (1) into k bilinear equations over $\mathbb{F}_2$ in $2(n-2)$ binary unknowns—where the $\lambda = 128$-bit parameters $(k, n) = (257, 130)$ from collision resistance and prime-extension selection [13, Sections 2.2 and 4.1] satisfy $k = 257 > 2(n-2) = 256$—we apply the polynomial-basis isomorphism $\mathrm{vec} : \mathbb{F}_{2^k} \xrightarrow{\sim} \mathbb{F}_2^k$ from (3) to (25). Because scalar multiplication by $x_i, y_i \in \mathbb{F}_2$ commutes with vec, a single $\mathbb{F}_{2^k}$-affine equation decomposes into k linear equations over $\mathbb{F}_2$ in the $2(n-2)$ secret bits, reducing the candidate space to a low-dimensional affine coset $w_0 + \ker(M_\sigma)$ that is filtered against (1). We establish the theorem in three steps: (1) proving completeness of the binary linear reduction; (2) bounding the affine solution space and proving exactness of the NSBC filter; and (3) accounting for the bit-operation complexity.

Step 1: Completeness of the $\mathbb{F}_2$-linear reduction. Let σ be an honestly generated signature under $\mathsf{sk} = (\vec{x}, \vec{y})$ with normalised witness $(\vec{x}', \vec{y}') = ((\vec{x}, 1, 0), (\vec{y}, 0, 1)) \in \mathsf{NSBC}[\vec{u}, \vec{v}]$. By Lemma 1, the transmitted field element $B \in \mathbb{F}_{2^k}$ satisfies

$$\bigoplus_{i=0}^{n-3} x_i \, \beta_i^{(x)} \oplus \bigoplus_{i=0}^{n-3} y_i \, \beta_i^{(y)} = B \oplus \gamma_\sigma \quad \text{in } \mathbb{F}_{2^k}.$$

Applying $\mathrm{vec} : \mathbb{F}_{2^k} \xrightarrow{\sim} \mathbb{F}_2^k$ to both sides and using the $\mathbb{F}_2$-linearity identity (3) yields

$$\bigoplus_{i=0}^{n-3} x_i \, \mathrm{vec}(\beta_i^{(x)}) \oplus \bigoplus_{i=0}^{n-3} y_i \, \mathrm{vec}(\beta_i^{(y)}) = \mathrm{vec}(B \oplus \gamma_\sigma) \quad \text{in } \mathbb{F}_2^k.$$

By definition of M_σ in (34), the left-hand side equals the matrix-vector product $M_\sigma w^*$ for the true secret key vector $w^* = (\vec{x}, \vec{y})^\top \in \mathbb{F}_2^{2(n-2)}$. Hence $M_\sigma w^* = \mathrm{vec}(B \oplus \gamma_\sigma)$, so the linear system in Step 4 of Algorithm 1 is always consistent.

Step 2: Solution-space cardinality and NSBC candidate filtering. Since $M_\sigma w = \mathrm{vec}(B \oplus \gamma_\sigma)$ is consistent and $\dim_{\mathbb{F}_2} \ker(M_\sigma) = 2(n-2) - \mathrm{rank}(M_\sigma) = d$, Gaussian elimination in Step 4 returns an affine solution space $w_0 + \ker(M_\sigma) \subseteq \mathbb{F}_2^{2(n-2)}$ of exact cardinality 2^d containing w^*. In Step 5, each candidate $(\tilde{\vec{x}}, \tilde{\vec{y}})^\top \in w_0 + \ker(M_\sigma)$ is tested against $((\tilde{\vec{x}}, 1, 0), (\tilde{\vec{y}}, 0, 1)) \in \mathsf{NSBC}[\vec{u}, \vec{v}]$. Because $(\vec{x}', \vec{y}') \in \mathsf{NSBC}[\vec{u}, \vec{v}]$, the true key $\mathsf{sk} = (\vec{x}, \vec{y})$ survives this filter, while every surviving candidate is by construction a valid normalised $\mathsf{NSBC}[\vec{u}, \vec{v}]$ witness. Thus $\mathsf{sk} \in \mathcal{W}_\sigma \subseteq \mathsf{NSBC}[\vec{u}, \vec{v}]$ and $1 \le |\mathcal{W}_\sigma| \le 2^d$.

Step 3: Bit-operation complexity. Beyond the public verification reconstruction of Section 3.4, Step 3 evaluates $2(n-2)$ linear combinations $\beta_i^{(x)} = c_P u_i \oplus c_Q v_i$ and $\beta_i^{(y)} = c_R u_i \oplus c_S v_i$, requiring

$4(n-2)$ multiplications in $\mathbb{F}_{2^k}$, or $4(n-2)k^2$ elementary bit operations under schoolbook polynomial arithmetic. Step 4 performs Gaussian elimination on $M_\sigma \in \mathbb{F}_2^{k\times 2(n-2)}$, requiring $\frac{1}{3}k(2(n-2))^2$ bit operations to leading order. Finally, Step 5 evaluates the four subfield-to-extension inner products $\vec{u}\cdot\tilde{\vec{x}}', \vec{v}\cdot\tilde{\vec{x}}', \vec{u}\cdot\tilde{\vec{y}}', \vec{v}\cdot\tilde{\vec{y}}'$ ($4(n-2)k$ bit operations via subset XORs) and two $\mathbb{F}_{2^k}$ multiplications ($2k^2$ bit operations) for each of the 2^d candidates, summing to (35). □

Rank Deficiency and Concrete Complexity at $\lambda = 128$. At the $\lambda = 128$-bit parameters $(q, k, n) = (2, 257, 130)$, the unknown secret key has $2(n-2) = 256$ bits while (33) provides $k = 257$ binary equations ($M_\sigma \in \mathbb{F}_2^{257\times 256}$). A uniformly random 257×256 matrix over $\mathbb{F}_2$ has kernel dimension $d = 256 - \mathrm{rank}(M_\sigma)$ concentrated on $\{0, 1, 2\}$ ($\Pr[d = 0] \approx 0.578$, $\Pr[d = 1] \approx 0.385$, $\Pr[d = 2] \approx 0.037$), leaving at most $2^d \le 4$ affine candidates with probability above 99.9%; any false candidate fails the 257-bit field identity (1) with probability $1 - 2^{-257}$, uniquely identifying sk. Evaluating (35) at $(n, k) = (130, 257)$ and $d = 0$ gives 33,817,088 + 5,614,251 + 263,682 = 39,695,021 $\approx 2^{25.24}$ bit operations (9,258,690 $\approx 2^{23.14}$ with Karatsuba multiplication, or 74,040,501 $\approx 2^{26.14}$ if $U_x^*, V_x^*, U_y^*, V_y^*$, c_P, c_Q, c_R, c_S, and γ_σ are also charged as full k^2 multiplications) and $257 \times 256 = 65{,}792$ bits (8.0 kB) of memory from 1 signature. Neither D nor τ enters (35): every parameter set of both $\mathsf{SBC}_{\mathsf{VOLE}}$ and $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$ is broken with identical algebraic complexity, more than 101 bits below the claimed 128-bit security level.

5 Conditional Entropy of B and Security Proof Analysis

Given that Huth and Joux provided an explicit EUF-CMA security reduction in Theorem 2 and Appendix A of [14], we now pinpoint the exact step in their reduction where this leakage went undetected.

5.1 The Witness-Free Simulator in Game 2

In Section 5 of [14, p. 18, full version], $\mathsf{SBC}_{\mathsf{VOLE}}$ is obtained by applying the Fiat–Shamir transform to the five-pass identification protocol of Section 3. In Appendix A [14, pp. 33–35, full version], the proof of EUF-CMA security proceeds via a hybrid game sequence from the real signing game (**Game 1**, which answers signing queries via the real oracle $\mathcal{O}(\mathsf{sk}, \mathsf{pk})$) to a simulated signing game (**Game 2**, which replaces $\mathcal{O}(\mathsf{sk}, \mathsf{pk})$ by a witness-free simulator $\mathcal{S}(\mathsf{pk})$ that chooses random oracle outputs h_0, h_1 in advance).

To argue that $\mathcal{S}(\mathsf{pk})$ reproduces the honest signature distribution without knowing sk, the proof states verbatim [14, Appendix A, p. 35, full version]:

> *"The simulator then proceeds to derive the shares of $\vec{x}$ and $\vec{y}$ as in the original Signing algorithm, with the difference that $\vec{x}$ and the offset values $(\delta_{\vec{y}_j})_{j\in[\tau]}$ are picked at random. Therefore, $\vec{x}$ and the derived $\vec{y} = \sum_{i=0}^{N-1} \vec{y}_j^{[\![i]\!]} + \delta_{\vec{y}_j}$ solve the SBC problem only with negligible probability. The simulator can then use the Verification algorithm to compute the expected values of A, B, b and $(\delta_{z_j})_{j\in[\tau]^*}$. Using this simulator, the shares revealed in the signature are uniformly distributed under the condition that $\Phi(\Delta^*) = A + B\Delta^*$, i.e., they have the same distribution as the shares obtained from an honest signature execution. If the algorithms do not abort, the obtained signatures from $\mathcal{S}(\mathsf{pk})$ and $\mathcal{O}(\mathsf{sk}, \mathsf{pk})$ are therefore identically distributed."*

From this claim, the proof concludes that $|\varepsilon_{\text{Game 2}} - \varepsilon_{\text{Game 1}}| \le Q^2/2^{2\lambda}$ (accounting only for salt collisions).

5.2 Zero Conditional Entropy and Simulator Distinguisher

Inspection of the Game 2 transition reveals both an operational contradiction and an algebraic error:

1. Verification Takes B as Input Rather Than Output. In the verification algorithm [14, Section 5], B, b, and $(\delta_{z_j})_{j\in[\tau]^*}$ are *inputs* parsed from σ, not outputs computed by verification. Verification computes $\Phi(\Delta^*)$ from the opened VOLE evaluations and evaluates $A' \leftarrow \Phi(\Delta^*) \oplus B\Delta^*$, imposing only one scalar constraint $A' \oplus B\Delta^* = \Phi(\Delta^*)$ on the pair (A', B) while leaving B undetermined.

2. Zero Conditional Entropy of B Given the Opened Transcript. In the predecessor CRYPTO 2024 MPCitH scheme [13], each virtual party $i \in [N]$ generated fresh random masks $R_A^{[\![i]\!]}, R_B^{[\![i]\!]} \in \mathbb{F}_{q^k}$, and the unopened party's mask $R_B^{[\![i^*]\!]}$ genuinely acted as a one-time pad on the transmitted offset δ_B. When migrating to VOLEitH in [14], the per-party masks $R_A^{[\![i]\!]}, R_B^{[\![i]\!]}$ were removed under the implicit assumption that the unopened VOLE masks $\vec{A}_{F_x}, \vec{A}_{F_y}$ inside (11) would still randomise B. However, once the punctured keys and $(\delta_{\vec{y}_j})_{j\in[\tau]}$ are revealed in σ, the evaluations $\vec{F}_x(\Delta^*)$ and $\vec{F}_y(\Delta^*)$ are fixed, locking $\vec{A}_{F_x} = \vec{F}_x(\Delta^*) \oplus \Delta^*\vec{x}$ and $\vec{A}_{F_y} = \vec{F}_y(\Delta^*) \oplus \Delta^*\vec{y}$ deterministically to the witness. By Lemma 1, in an honest signature under sk, the coordinate vector $\mathrm{vec}(B)$ is a deterministic point mass on $M_\sigma w \oplus \mathrm{vec}(\gamma_\sigma)$:

$$H\Big(B \;\Big|\; \mathsf{pk},\, \mathsf{sk},\, \mathsf{salt},\, K_{i_{\mathrm{p}}^*},\, K_{i_0^*,\ldots,i_{\tau-1}^*},\, (\delta_{\vec{y}_j})_{j\in[\tau]},\, h_0,\, h_1\Big) = 0. \tag{36}$$

More generally, any VOLEitH reduction that omits an explicit multiplication-gate mask must verify that transmitted polynomial coefficients retain full conditional entropy *after* conditioning on the punctured VOLE evaluations, rather than inspecting mask entropy prior to opening.

Theorem 2 (Refutation of HVZK Simulation and Game 2 Indistinguishability)**.** *Let $\mathcal{D}$ be the polynomial-time distinguisher that, given $\mathsf{pk} = (\vec{u}, \vec{v})$ and one signature σ (or interactive transcript), runs Algorithm 1 and outputs 1 if and only if $\mathcal{W}_\sigma \neq \emptyset$. Then $\mathcal{D}$ outputs 1 with probability 1 on honest signatures from $\mathcal{O}(\mathsf{sk}, \mathsf{pk})$ (Game 1), whereas for any simulator $\mathcal{S}(\mathsf{pk})$ running without knowledge of an $\mathsf{NSBC}[\vec{u}, \vec{v}]$ witness (Game 2),*

$$\left|\varepsilon_{\text{Game 2}} - \varepsilon_{\text{Game 1}}\right| \geq 1 - \varepsilon_{\mathsf{SBC}}$$

after a single signing query ($q_s = 1$). In particular, at $(q, k, n) = (2, 257, 130)$, where $\mathsf{pk} \leftarrow \mathsf{KeyGen}(1^\lambda)$ plants $\mathsf{sk} \in \mathsf{NSBC}[\vec{u}, \vec{v}]$ so that $\mathbb{E}_{\mathsf{pk}}\big[|\mathsf{NSBC}[\vec{u}, \vec{v}]|\big] = 1 + (2^{2(n-2)} - 1)2^{-k} \approx 3/2$:

1. *If $\mathcal{S}(\mathsf{pk})$ samples $B \xleftarrow{\$} \mathbb{F}_{2^k}$ uniformly and sets $A \leftarrow \Phi(\Delta^*) \oplus B\Delta^*$ (Strategy $\mathcal{S}_1$), then $\mathrm{vec}(B \oplus \gamma_\sigma) \notin \mathrm{im}(M_\sigma)$ with probability $1 - 2^{\mathrm{rank}(M_\sigma)-k} \geq 1/2$, and $\mathcal{W}_\sigma \neq \emptyset$ holds with probability at most $|\mathsf{NSBC}[\vec{u}, \vec{v}]|/2^k$ ($\approx 3 \cdot 2^{-258} < 2^{-256}$ in expectation over KeyGen).*

2. *If $\mathcal{S}(\mathsf{pk})$ samples a random dummy pair $(\tilde{\vec{x}}, \tilde{\vec{y}}) \xleftarrow{\$} \mathbb{F}_2^{n-2} \times \mathbb{F}_2^{n-2}$ as described in [14, p. 35, full version], computes B via (11), and sets $A \leftarrow \Phi(\Delta^*) \oplus B\Delta^*$ (Strategy $\mathcal{S}_2$), then $M_\sigma w = \mathrm{vec}(B \oplus \gamma_\sigma)$ recovers $(\tilde{\vec{x}}, \tilde{\vec{y}})^\top \in w_0 + \ker(M_\sigma)$, which fails (1) with probability $1 - |\mathsf{NSBC}[\vec{u}, \vec{v}]|/2^{2(n-2)}$, and $\mathcal{W}_\sigma \neq \emptyset$ holds with probability at most $2^d|\mathsf{NSBC}[\vec{u}, \vec{v}]|/2^{2(n-2)}$ ($< 2^{-254}$ in expectation).*

Proof. The breakdown of the Game 1 → Game 2 transition stems from an incompatibility between zero conditional entropy and witness-free simulation. Because B has zero conditional entropy given the opened transcript and sk, Algorithm 1 functions as a deterministic algebraic extractor whenever $\mathrm{vec}(B)$ lies in the image of $\mathsf{NSBC}[\vec{u}, \vec{v}]$ under the affine map $w \mapsto M_\sigma w \oplus \mathrm{vec}(\gamma_\sigma)$. Consequently, any witness-free simulator $\mathcal{S}(\mathsf{pk})$ that causes $\mathcal{D}$ to accept with probability p immediately yields an algorithm that solves $\mathsf{SBC}[\vec{u}, \vec{v}]$ from pk alone with probability p. We first establish the general reduction bound $|\varepsilon_{\text{Game 2}} - \varepsilon_{\text{Game 1}}| \geq 1 - \varepsilon_{\mathsf{SBC}}$, and then derive the explicit acceptance probabilities of Strategies $\mathcal{S}_1$ and $\mathcal{S}_2$.

Step 1: General reduction to $\mathsf{SBC}[\vec{u}, \vec{v}]$. When σ is generated by the real signing oracle $\mathcal{O}(\mathsf{sk}, \mathsf{pk})$ in Game 1, Theorem 1 guarantees $\mathsf{sk} \in \mathcal{W}_\sigma$, so $\mathcal{W}_\sigma \neq \emptyset$ and $\Pr[\mathcal{D}(\mathsf{pk}, \mathcal{O}(\mathsf{sk}, \mathsf{pk})) = 1] = 1$.

Suppose now that in Game 2 a witness-free simulator $\mathcal{S}(\mathsf{pk})$ produces a transcript $\sigma_{\mathcal{S}} \leftarrow \mathcal{S}(\mathsf{pk})$ satisfying $\Pr[\mathcal{D}(\mathsf{pk}, \sigma_{\mathcal{S}}) = 1] = p$. By Step 5 of Algorithm 1, every element of $\mathcal{W}_{\sigma_{\mathcal{S}}}$ is a valid solution in $\mathsf{NSBC}[\vec{u}, \vec{v}]$. Hence running $\mathcal{S}(\mathsf{pk})$ once followed by Algorithm 1 solves the instance $\mathsf{SBC}[\vec{u}, \vec{v}]$ without access to sk with success probability $p \leq \varepsilon_{\mathsf{SBC}}$, yielding $|\varepsilon_{\text{Game 2}} - \varepsilon_{\text{Game 1}}| = 1 - p \geq 1 - \varepsilon_{\mathsf{SBC}}$.

Step 2: Analysis of Strategy $\mathcal{S}_1$ (uniform B) and Strategy $\mathcal{S}_2$ (dummy witness). Under Strategy $\mathcal{S}_1$, B is chosen uniformly from $\mathbb{F}_{2^k}$, so $\mathrm{vec}(B \oplus \gamma_\sigma)$ is uniform over $\mathbb{F}_2^k$. Since $\mathrm{im}(M_\sigma) \subseteq \mathbb{F}_2^k$ is a subspace of dimension $\mathrm{rank}(M_\sigma) \leq 2(n-2) < k$, the linear system $M_\sigma w = \mathrm{vec}(B \oplus \gamma_\sigma)$ has no solution with probability $1 - 2^{\mathrm{rank}(M_\sigma)-k} \geq 1 - 2^{2(n-2)-k} = 1/2$ at $(k, n) = (257, 130)$. Moreover, $\mathcal{W}_\sigma \neq \emptyset$ holds only if $\mathrm{vec}(B \oplus \gamma_\sigma)$ falls into $\{M_\sigma w : w \in \mathsf{NSBC}[\vec{u}, \vec{v}]\}$, which has cardinality at most $|\mathsf{NSBC}[\vec{u}, \vec{v}]|$, bounding the acceptance probability by $|\mathsf{NSBC}[\vec{u}, \vec{v}]|/2^k$; since KeyGen plants sk and each remaining pair satisfies (1) with probability 2^{-k}, $\mathbb{E}_{\mathsf{pk}}[|\mathsf{NSBC}[\vec{u}, \vec{v}]|] = 1 + (2^{256} - 1)2^{-257} \approx 3/2$, giving expectation $\approx 3 \cdot 2^{-258} < 2^{-256}$. Under Strategy $\mathcal{S}_2$, Lemma 1 applies identically to the dummy vector $\tilde{w} = (\tilde{\vec{x}}, \tilde{\vec{y}})^\top \xleftarrow{\$} \mathbb{F}_2^{2(n-2)}$, so Step 4 of Algorithm 1 recovers $w_0 + \ker(M_\sigma) = \tilde{w} + \ker(M_\sigma)$. For any fixed coset offset $z \in \ker(M_\sigma)$, $\tilde{w} \oplus z$ is uniform over $\mathbb{F}_2^{2(n-2)}$ and lands in $\mathsf{NSBC}[\vec{u}, \vec{v}]$ with probability $|\mathsf{NSBC}[\vec{u}, \vec{v}]|/2^{2(n-2)}$; union-bounding over the 2^d coset elements gives acceptance probability at most $2^d|\mathsf{NSBC}[\vec{u}, \vec{v}]|/2^{2(n-2)}$ (and $\approx \frac{9}{4} \cdot 2^{-256} < 2^{-254}$ in expectation for uniform M_σ, where $\mathbb{E}[2^d] \approx 3/2$). □

6 Protocol Repair via Correlated VOLE Masking

Theorem 1 and Theorem 2 show that both the key-recovery vulnerability and the Game 2 simulation failure stem from the zero conditional entropy of B in (36). Restoring security therefore requires reinstating an independent degree-1 multiplication mask on (A, B), following the standard VOLEitH multiplication-check paradigm of QuickSilver [20], Baum et al. [3], and FAEST [2] (and playing the VOLE analogue of the per-party masks $(R_A^{[\![i]\!]}, R_B^{[\![i]\!]})$ in [13]).

6.1 Insufficiency of Existing Leaf Shares

None of the three existing leaf-expanded share families in $T_{\vec{x}_j}$ ($\vec{y}_j^{[\![\ell]\!]} \in \mathbb{F}_2^{n-2}$, $z_j^{[\![\ell]\!]} \in \mathbb{F}_{2^k}$, or $\mathsf{com}_j^{[\![\ell]\!]} \in \{0,1\}^{2\lambda}$) can mask B without adding fresh randomness:

1. **Secret row $\vec{y}_j^{[\![\ell]\!]}$:** Aligned via $\delta_{\vec{y}_j}$ to sum to the secret $\vec{y}$ itself.
2. **Consistency pad $z_j^{[\![\ell]\!]}$:** Already consumed by $b = z \oplus \vec{y} \cdot \vec{\mu}$ in (12); masking B by z (sending $\tilde{B} = B \oplus z$) leaves $\tilde{B} \oplus b = B \oplus \vec{y} \cdot \vec{\mu}$, which remains an unmasked $\mathbb{F}_2$-affine functional of $(\vec{x}, \vec{y})$.
3. **Commitment row $\mathsf{com}_j^{[\![\ell]\!]}$:** Completely revealed in $\mathsf{SBC}_{\mathsf{VOLE}}$ via $\mathsf{com}_j^{[\![1-b_{i,j}]\!]_i} = X_j \oplus \mathsf{com}_j^{[\![b_{i,j}]\!]_i}$, carrying zero conditional entropy in the verifier's view.

6.2 Correlated VOLE Masking Construction

To integrate VOLE multiplication masking into $\mathsf{SBC}_{\mathsf{VOLE}}$ and $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$, we introduce one correlated field mask $\rho \in \mathbb{F}_{2^k}$ aligned across all τ trees via the same offset-and-H_0-binding mechanism that [14] already uses for z in (6) and (13):

1. **Leaf Expansion:** Expand each leaf $\ell \in [2^D]$ of tree $T_{\vec{x}_j}$ ($j \in [\tau]$) into an additional share $\rho_j^{[\![\ell]\!]} \in \mathbb{F}_{2^k}$ and fold via (5) into $(\rho_j^{[\![0]\!]_i}, \rho_j^{[\![1]\!]_i})_{i \in [D]}$.

2. **Global Mask and Offsets:** Set $\rho \leftarrow \rho_0^{[\![0]\!]_0} \oplus \rho_0^{[\![1]\!]_0} \in \mathbb{F}_{2^k}$ from tree $T_{\vec{x}_0}$, and for each $j \in [\tau]^*$ compute

$$\delta_{\rho_j} \leftarrow \rho \oplus \rho_j^{[\![0]\!]_0} \oplus \rho_j^{[\![1]\!]_0} \in \mathbb{F}_{2^k} \qquad \text{(with } \delta_{\rho_0} := 0 \text{ omitted)}.$$

3. **Pre-Challenge Hash Binding:** Bind $(\delta_{\rho_j})_{j\in[\tau]^*}$ inside the first Fiat–Shamir hash:

$$h_0 \leftarrow H_0\Big(\mathsf{msg}, h_{\mathsf{com}}, \mathsf{salt}, (\delta_{\vec{y}_j}, \delta_{z_j}, \delta_{\rho_j})_{j\in[\tau]}, (X_j)_{j\in[\tau]}\Big). \tag{37}$$

4. **Masked Coefficients:** Compute $A_{F_\rho} \leftarrow \bigoplus_{j=0}^{\tau-1} \bigoplus_{i=jD}^{(j+1)D-1} \alpha_i \, \rho_j^{[\![0]\!]_{i-jD}} \in \mathbb{F}_{2^k}$ and set

$$\tilde{A} \leftarrow A \oplus A_{F_\rho} \in \mathbb{F}_{2^k}, \qquad \tilde{B} \leftarrow B \oplus \rho \in \mathbb{F}_{2^k}. \tag{38}$$

   Hash $(\tilde{A}, \tilde{B})$ in place of (A, B) into h_1, and transmit $\tilde{B}$ and $(\delta_{\rho_j})_{j\in[\tau]^*}$ in σ.

5. **Verification Unmasking:** The verifier reconstructs the opened mask VOLE evaluation

$$F_\rho(\Delta^*) \leftarrow \bigoplus_{j=0}^{\tau-1} \bigoplus_{i=jD}^{(j+1)D-1} \alpha_i \left(\rho_j^{[\![b_{i-jD,j}]\!]_{i-jD}} \oplus b_{i-jD,j}\, \delta_{\rho_j}\right) = A_{F_\rho} \oplus \Delta^* \rho, \tag{39}$$

   computes $\tilde{A}' \leftarrow \Phi(\Delta^*) \oplus F_\rho(\Delta^*) \oplus \tilde{B}\Delta^*$, and verifies that the recomputed digest h_1' matches h_1.

6.3 Soundness Neutrality and Restored Simulation

Theorem 3 (Soundness Neutrality and Restored Simulation)**.** *The repaired* $\mathsf{SBC}_{\mathsf{VOLE}}$ *and* $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$ *protocols satisfy:*

1. ***Exact Soundness Preservation:*** *The five-pass identification protocol retains the exact soundness error bound* $\varepsilon = \tau^2 2^{-k} + 2^{1-\tau D}$ *[14, Theorem 1].*

2. ***Restored Game 2 Simulation:*** *There exists a polynomial-time witness-free simulator* $\mathcal{S}_{\text{repaired}}(\mathsf{pk})$ *in Game 2 whose output distribution on the masked verification transcript is indistinguishable from* $\mathcal{O}(\mathsf{sk}, \mathsf{pk})$ *up to PRG and random-oracle collision bounds (orthogonal to commitment-binding [17] and* cGGM *root-prefix reduction bounds [18, 9]).*

3. ***Multi-Signature Linear Security:*** *Across any* $m \geq 1$ *signatures under* sk*, the joint linear system in* $(\vec{x}, \vec{y})$ *and the per-signature masks* $(\rho^{(0)}, \ldots, \rho^{(m-1)})$ *maintains constant rank deficiency* $2(n-2)$*, leaking zero linear information about* $(\vec{x}, \vec{y})$*.*

Proof. Masking B without disturbing the degree-1 verification check relies on lifting the folded shares of $\rho \in \mathbb{F}_{2^k}$ into the auxiliary VOLE evaluation $F_\rho(\Delta^*) = A_{F_\rho} \oplus \Delta^*\rho$. In the verifier's linear combination $\Phi(\Delta^*) \oplus F_\rho(\Delta^*) \oplus \tilde{B}\Delta^*$, the $\Delta^*\rho$ term cancels the shift in $\tilde{B} = B \oplus \rho$, translating the reconstructed constant term from A to $\tilde{A} = A \oplus A_{F_\rho}$. We prove the three claims sequentially: (1) algebraic equivalence of the verification check at every challenge point Δ^*; (2) conditional independence and uniformity of $\tilde{B}$ and $(\delta_{\rho_j})_{j\in[\tau]^*}$ given the punctured keys, which restores Game 2 simulation; and (3) rank-deficiency invariance across m signatures.

Step 1: Exact soundness equivalence. When $(\delta_{\rho_j})_{j\in[\tau]^*}$ is bound in h_0 via (37) before $(\alpha_m)_{m\in[\tau D]}$ are derived, the prover commits to a fixed sequence of tree masks $\rho_j = \rho_j^{[\![0]\!]_0} \oplus \rho_j^{[\![1]\!]_0} \oplus \delta_{\rho_j}$. Substituting (38) and (39) into the verifier's reconstructed constant $\tilde{A}'$ yields

$$\tilde{A}' = \Phi(\Delta^*) \oplus (A_{F_\rho} \oplus \Delta^*\rho) \oplus (B \oplus \rho)\Delta^* = \big(\Phi(\Delta^*) \oplus B\Delta^*\big) \oplus A_{F_\rho}.$$

Table 2: Signature sizes before and after the correlated VOLE-masking repair at $\lambda = 128$ ($q = 2, k = 257, n = 130$).

Params		**Basic Scheme** $\mathsf{SBC_{VOLE}}$			**MinMax Scheme** $\mathsf{SBC^{M}_{VOLE}}$			**Added**
D	τ	Original	Repaired	Overhead	Original	Repaired	Overhead	Offsets
9	15	3,458 B	3,908 B	+13.0%	2,978 B	3,428 B	+15.1%	14
10	13	3,218 B	3,604 B	+12.0%	2,802 B	3,188 B	+13.8%	12
11	12	3,170 B	3,523 B	+11.1%	2,786 B	3,139 B	+12.7%	11
12	11	3,090 B	3,411 B	+10.4%	2,738 B	3,059 B	+11.7%	10
13	**10**	**2,978 B**	**3,267 B**	**+9.7%**	**2,658 B**	**2,947 B**	**+10.9%**	**9**
15	9	2,978 B	3,235 B	+8.6%	2,690 B	2,947 B	+9.6%	8

Since $\tilde{A} = A \oplus A_{F_\rho}$, the equality $\tilde{A}' = \tilde{A}$ holds if and only if $\Phi(\Delta^*) \oplus B\Delta^* = A$. Hence the set of accepting second-round challenges $(i_j^*)_{j\in[\tau]}$ for any cheating prover is identical to that of the original protocol, preserving $\varepsilon = \tau^2 2^{-k} + 2^{1-\tau D}$.

Step 2: Restored witness-free simulation. Conditioned on the punctured keys $(K_{i_{\mathrm{p}}^*}, K_{i_0^*,\ldots,i_{\tau-1}^*})$ and PRG security, the unopened leaf share $\rho_0^{[\![i_0^*]\!]} \in \mathbb{F}_{2^k}$ in tree $T_{\vec{x}_0}$ is pseudorandom and appears in no opened branch share $\rho_0^{[\![b_{i,0}]\!]_i}$. Thus $\rho = \rho_0^{[\![0]\!]_0} \oplus \rho_0^{[\![1]\!]_0}$ acts as an independent one-time pad on $\tilde{B} = B \oplus \rho$, while each unopened leaf share $\rho_j^{[\![i_j^*]\!]}$ ($j \in [\tau]^*$) independently masks $\delta_{\rho_j} = \rho \oplus \rho_j^{[\![0]\!]_0} \oplus \rho_j^{[\![1]\!]_0}$. Consequently, a witness-free simulator $\mathcal{S}_{\mathrm{repaired}}(\mathsf{pk})$ that samples $\tilde{B} \xleftarrow{\$} \mathbb{F}_{2^k}$ and $(\delta_{\rho_j})_{j\in[\tau]^*} \xleftarrow{\$} (\mathbb{F}_{2^k})^{\tau-1}$ uniformly at random and sets $\tilde{A} \leftarrow \Phi(\Delta^*) \oplus F_\rho(\Delta^*) \oplus \tilde{B}\Delta^*$ produces transcripts whose distribution matches $\mathcal{O}(\mathsf{sk}, \mathsf{pk})$ up to $\varepsilon_{\mathsf{PRG}}$ and random-oracle collision bounds.

Step 3: Multi-signature linear security. In signature $r \in [m]$, expanding $\tilde{B}^{(r)} = B^{(r)} \oplus \rho^{(r)}$ over $\mathbb{F}_2^k$ yields the k-row linear equation $M_{\sigma^{(r)}} w \oplus \mathrm{vec}(\rho^{(r)}) = \mathrm{vec}(\tilde{B}^{(r)} \oplus \gamma_{\sigma^{(r)}})$. Stacking m signatures produces an $mk \times (2(n-2) + mk)$ binary system whose matrix is $\left[\, M \;\middle|\; I_{mk} \,\right]$, which has full row rank mk and constant kernel dimension $2(n-2)$ for every $m \geq 1$. □

Necessity of Pre-Challenge Hash Binding. Including $(\delta_{\rho_j})_{j\in[\tau]^*}$ inside H_0 in (37) is essential for soundness. Because δ_{ρ_j} enters $F_\rho(\Delta^*)$ linearly as $\bigoplus_{j=1}^{\tau-1} \Delta_j^* \delta_{\rho_j}$, omitting $(\delta_{\rho_j})_{j\in[\tau]^*}$ from H_0 would let a keyless attacker commit to dummy vectors $(\tilde{\vec{x}}, \tilde{\vec{y}})$, obtain $(\Delta_j^*)_{j\in[\tau]}$, and solve a linear equation in $\mathbb{F}_{2^k}$ for δ_{ρ_j} whenever $\Delta_j^* \neq 0$ for some $j \geq 1$ (probability $1 - 2^{-D(\tau-1)}$) to force $\tilde{A}' = \tilde{A}$.

6.4 Signature-Size Overhead and Post-Repair Standing

Replacing B by $\tilde{B}$ adds zero bits, while appending $(\delta_{\rho_1}, \ldots, \delta_{\rho_{\tau-1}}) \in (\mathbb{F}_{2^k})^{\tau-1}$ adds $\tau - 1$ elements of $\mathbb{F}_{2^k}$. Under the bit-packing rule of [14] for $k = 257$ (each $\mathbb{F}_{2^{257}}$ element occupies 32 bytes plus 1 bit packed 8-per-byte across all transmitted $\mathbb{F}_{2^{257}}$ elements, increasing the packed element count from $\tau + 1$ to 2τ), the exact byte overhead is

$$\Delta|\sigma|(\tau) = 32(\tau - 1) + \left\lceil \frac{2\tau}{8} \right\rceil - \left\lceil \frac{\tau + 1}{8} \right\rceil \quad \text{bytes.} \tag{40}$$

Table 2 lists the resulting sizes across all six published (D, τ) pairs. Because $\Delta|\sigma|(\tau)$ grows with $\tau - 1$, $(D, \tau) = (15, 9)$ (3,235 B, ≈ 5.1 ms signing and verification [14]) overtakes the headline $(13, 10)$ set (3,267 B, +289 B or +9.7%, ≈ 2.2 ms) as the smallest repaired $\mathsf{SBC_{VOLE}}$ configuration. At 3,235–3,267 B, repaired $\mathsf{SBC_{VOLE}}$ exceeds Dual-SDitH (2,813–2,851 B) [5] and the smallest VOLEitH-MQ instantiation (3.1–3.6 kB) [7], confirming that the sub-3 kB headline size of $\mathsf{SBC_{VOLE}}$ depended on omitting a mandatory multiplication mask. Even so,

Table 3: Single-signature key recovery and kernel-dimension distribution of $M_\sigma \in \mathbb{F}_2^{257\times256}$ across 1,200 random instances (100 keys per cell).

Params		**Basic Scheme** $\mathsf{SBC}_{\mathsf{VOLE}}$					**MinMax Scheme** $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$				
D	τ	Recov.	$d=0$	$d=1$	$d=2$	Mean d	Recov.	$d=0$	$d=1$	$d=2$	Mean d
9	15	100/100	56	41	3	0.470	100/100	51	46	3	0.520
10	13	100/100	63	33	4	0.410	100/100	59	37	4	0.450
11	12	100/100	58	36	6	0.480	100/100	62	35	3	0.410
12	11	100/100	56	41	3	0.470	100/100	57	40	3	0.460
13	10	100/100	54	39	7	0.530	100/100	59	41	0	0.410
15	9	100/100	60	38	2	0.420	100/100	48	47	5	0.570
Pooled		**600/600**	**347**	**228**	**25**	**0.463**	**600/600**	**336**	**246**	**18**	**0.470**

repaired $\mathsf{SBC}_{\mathsf{VOLE}}$ still saves 499–531 bytes and roughly 90% runtime over CRYPTO 2024 SBC (3,766 B) [13], and remains more compact than VOLEitH-PKP (3,686 B) [4], FAEST-EM v2 (3,906 B) [2], ReSolveD (3,916 B) [8], and FAEST v2 (4,506 B) [2] while keeping a 48-byte public key. Although repaired $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$ reaches 2,947 B at both $(13, 10)$ and $(15, 9)$, our ρ-masking repair addresses only the algebraic verification layer and does not harden the implicit MinMax commitment against [17].

7 Experimental Verification

We implemented Algorithm 1 and evaluated single-signature secret-key recovery across all published parameter sets of $\mathsf{SBC}_{\mathsf{VOLE}}$ and $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$ [14].

First, at $(q, k, n) = (2, 257, 130)$, we verified that the second difference $B(w_1) \oplus B(w_2) \oplus B(w_1 \oplus w_2) \oplus B(0)$ vanished across 200/200 random trials, and that the closed-form identity (25)–(26) matched the four-term formula (11) with zero mismatches under both padding conventions ($\eta \in \{0, 1\}$).

Second, we ran Algorithm 1 end-to-end across all six published (D, τ) parameter sets and both variants ($\mathsf{SBC}_{\mathsf{VOLE}}$ and $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$), testing 100 independent random key pairs per configuration (1,200 instances in total). Given only pk and a single valid signature σ, the solver forms and reduces $M_\sigma \in \mathbb{F}_2^{257\times256}$, recovers sk, and produces a valid signature on a fresh message.

As reported in Table 3, Algorithm 1 recovered the exact 256-bit secret key on 1,200/1,200 (100%) of tested instances, producing valid signatures on fresh messages in every case, while all negative controls (bit-flipped key, modified message, and replayed signature) were rejected (0/51). Pooled kernel dimensions were $\{d = 0 : 683, d = 1 : 474, d = 2 : 43\}$ ($\bar{d} = 0.467$, $d_{\max} = 2$), matching the theoretical distribution of a uniform 257×256 binary matrix, and single-core execution required 0.06 s per signature.

8 Conclusion

This work demonstrates that the 2^{128} algebraic hardness of the Subfield Bilinear Collision problem does not prevent passive single-signature key recovery when its VOLEitH verification polynomial omits an independent multiplication mask. Once punctured VOLE evaluations are opened during verification, substituting the resulting affine mask relations into the unmasked slope B cancels all quadratic witness cross-terms in characteristic 2 (and vanishes on every honest witness in odd characteristic $q > 2$), exposing the 256-bit secret key of both $\mathsf{SBC}_{\mathsf{VOLE}}$ and $\mathsf{SBC}^{\mathsf{M}}_{\mathsf{VOLE}}$ in $2^{25.24}$ bit operations. Beyond repairing $\mathsf{SBC}_{\mathsf{VOLE}}$ via a correlated VOLE field mask at a +8.6%–15.1% size overhead, our analysis illustrates a general verification principle for VOLE-in-the-Head security proofs: zero-knowledge simulators cannot treat polynomial

verification coefficients as conditionally uniform without verifying positive conditional entropy *after* conditioning on the opened VOLE evaluations.

Use of AI. The cryptanalytic results and artifacts were initially developed through an autonomous agent system powered by a MiniMax internal model. We validated the key technical claims and refined the presentation of the manuscript.

References

[1] C. Aguilar-Melchor, N. Gama, J. Howe, A. Hülsing, D. Joseph, and D. Yue, "The return of the SDitH," in *Advances in Cryptology – EUROCRYPT 2023*, Part V, LNCS, vol. 14008, pp. 564–596, Springer, 2023.

[2] C. Baum, W. Beullens, L. Braun, C. Delpech de Saint Guilhem, M. Klooß, C. Majenz, S. Mukherjee, E. Orsini, S. Ramacher, C. Rechberger, L. Roy, and P. Scholl, "FAEST v2: Algorithm Specifications," Version 2.0, NIST Post-Quantum Cryptography Additional Digital Signatures Round 2 Submission, 2025. Available at https://faest.info/faest-spec-v2.0.pdf.

[3] C. Baum, L. Braun, C. Delpech de Saint Guilhem, M. Klooß, E. Orsini, L. Roy, and P. Scholl, "Publicly verifiable zero-knowledge and post-quantum signatures from VOLE-in-the-head," in *Advances in Cryptology – CRYPTO 2023*, Part V, LNCS, vol. 14085, pp. 581–615, Springer, 2023. (Full version: IACR ePrint 2023/996.)

[4] S. Bettaieb, L. Bidoux, P. Gaborit, and M. Kulkarni, "Modelings for generic PoK and applications: Shorter SD and PKP based signatures," Cryptology ePrint Archive, Paper 2024/1668, 2024.

[5] L. Bidoux, T. Feneuil, P. Gaborit, R. Neveu, and M. Rivain, "Dual support decomposition in the head: Shorter signatures from rank SD and MinRank," in *Advances in Cryptology – ASIACRYPT 2024*, Part II, LNCS, vol. 15485, pp. 38–69, Springer, 2024.

[6] P. Briaud and R. Neveu, "Cryptanalysis of the Subfield Bilinear Collision Problem," *IACR Communications in Cryptology*, vol. 3, no. 3, 2026, doi:10.62056/a0l2ip10. (Preprint: IACR ePrint 2026/916.)

[7] D. Bui, "Shorter VOLEitH signature from multivariate quadratic," Cryptology ePrint Archive, Paper 2024/465, 2024. (Revised version published as "Efficient multi-instance vector commitment and application to post-quantum signatures" in *Information Security and Privacy – ACISP 2025*, Part II, LNCS, vol. 15659, pp. 23–41, Springer, 2025.)

[8] H. Cui, H. Liu, D. Yan, K. Yang, Y. Yu, and K. Zhang, "ReSolveD: Shorter signatures from regular syndrome decoding and VOLE-in-the-head," in *Public-Key Cryptography – PKC 2024*, Part I, LNCS, vol. 14601, pp. 229–258, Springer, 2024.

[9] T. Feneuil and M. Rivain, "On the security of MPC-in-the-head signatures with correlated GGM trees," Cryptology ePrint Archive, Paper 2026/615, 2026.

[10] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Advances in Cryptology – CRYPTO '86*, LNCS, vol. 263, pp. 186–194, Springer, 1987.

[11] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," *Journal of the ACM*, vol. 33, no. 4, pp. 792–807, 1986.

[12] X. Guo, K. Yang, X. Wang, W. Zhang, X. Xie, J. Zhang, and Z. Liu, "Half-tree: Halving the cost of tree expansion in COT and DPF," in *Advances in Cryptology – EUROCRYPT 2023*, Part I, LNCS, vol. 14004, pp. 330–362, Springer, 2023.

[13] J. Huth and A. Joux, "MPC in the head using the subfield bilinear collision problem," in *Advances in Cryptology – CRYPTO 2024*, Part I, LNCS, vol. 14920, pp. 39–70, Springer, 2024. (Full version: IACR ePrint 2023/1685.)

[14] J. Huth and A. Joux, "VOLE-in-the-Head Signatures from Subfield Bilinear Collisions," in *Advances in Cryptology – ASIACRYPT 2025*, Part IV, LNCS, vol. 16248, pp. 3–34, Springer, 2025. (Full version: IACR ePrint 2024/1537.)

[15] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, "Zero-knowledge from secure multiparty computation," in *Proceedings of the 39th Annual ACM Symposium on Theory of Computing (STOC 2007)*, pp. 21–30, ACM, 2007.

[16] A. Joux and C. Pierrot, "Algorithmic aspects of elliptic bases in finite field discrete logarithm algorithms," *Advances in Mathematics of Communications*, vol. 18, no. 5, pp. 1266–1302, 2024.

[17] S. Kim, B. Lee, and M. Son, "Shorter VOLE-in-the-Head-based Signatures from Vector Semi-Commitment," Cryptology ePrint Archive, Paper 2025/1077, 2025. (Also in *Proceedings of the 2026 ACM SIGSAC Conference on Computer and Communications Security (CCS 2026)*.)

[18] H. Kosuge and K. Xagawa, "New security proofs of TC-in-the-head signatures in the quantum random oracle model," *IACR Communications in Cryptology*, vol. 3, no. 3, 2026, doi:10.62056/akmpxruc2.

[19] L. Roy, "SoftSpokenOT: Quieter OT extension from small-field silent VOLE in the minicrypt model," in *Advances in Cryptology – CRYPTO 2022*, Part I, LNCS, vol. 13507, pp. 657–687, Springer, 2022.

[20] K. Yang, P. Sarkar, C. Weng, and X. Wang, "QuickSilver: Efficient and affordable zero-knowledge proofs for circuits and polynomials over any field," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS 2021)*, pp. 2986–3001, ACM, 2021. (Full version: IACR ePrint 2021/076.)