

Brute-Force Search with Equiprobable Solutions as a Formal Complexity Class and Its (Non-)Reducibility to Restricted Syndrome Decoding

Yevgen Kotukh^{1,*}

¹ Yevhenii Bereznyak Military Academy, 04001, Kyiv, Ukraine

Abstract

Recent post-quantum signature designs in the brute-force-search paradigm implicitly rely on a folklore assumption: that an honestly generated instance of a structured search problem admits, with overwhelming probability, an exponentially large but statistically equiprobable solution set, so that the only known attack is exhaustive enumeration. We formalize this assumption as BFS-EQ (Brute-Force Search with Equiprobable Solutions), a promise-search problem parametrized by an ensemble of functions $\Phi: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ together with an equiprobability promise on the preimage distribution. We position BFS-EQ within the standard complexity zoo (FNP, TFNP and its subclasses, Levin-style average-case classes) and prove four main results. First, BFS-EQ $\in$ FNP under any polynomial-time verifier; under the equiprobability promise it lies in a promise variant of TFNP, and we observe that, without auxiliary structure, it admits no evident reduction to PPP, PPA, or PLS. Second, the equiprobability promise is mathematically defensible only when Φ is regular on its support; generic affine or low-degree polynomial Φ fail this with a measurable statistical gap. Third, we construct a Karp reduction BFS-EQ $\rightarrow$ R-SDP that succeeds only under a sparsity-and-rank precondition; for the candidate parameter sets (208/64/135) and (3328/1024/708) the precondition fails and the reduction is invalid. Finally, under a mild linearity-rank hypothesis on Φ , BFS-EQ collapses to $\mathbb{F}_2$ -Subset-Sum and is solvable in time $2^{n/2}$ and space $2^{n/4}$ via the Schroeppel–Shamir algorithm. We present precise sufficient conditions for either route, and we delineate the failure modes that distinguish a cryptographic brute-force-search problem from an artefactually large search space.

Keywords

average-case complexity, promise search problems, FNP, TFNP, restricted syndrome decoding, multivariate quadratic, degree of regularity, subset sum, post-quantum signatures

1. Introduction

Several proposals in the NIST post-quantum signature competition and the broader literature reduce signature unforgeability to a brute-force-search-style assumption. An adversary, given a public function Φ and a target image y , is asked to recover a preimage $x \in \Phi^{-1}(y)$. The signer holds one such preimage as a trapdoor. The security argument proceeds in two informal steps. First, Φ is chosen so that $|\Phi^{-1}(y)|$ is exponentially large for honest y , thus offering high pseudorandomness for signing. Second, the preimages are claimed to be statistically equiprobable, so that no structural attack distinguishes the signer’s witness from any other, and exhaustive search remains the best generic attack. This pattern – a large, equiprobable preimage set with no exploitable structure – is intuitive but rarely formalized; the linear-equation signature family of [1, 2], from which the candidate parameter sets studied below are taken, is a representative instance. In contrast, structured-decoding assumptions such as R-SDP [3], inhomogeneous MQ (MQOM v2.1 [4]), Permuted Kernel (PERK), Rank Syndrome (RYDE), and Linear Equivalence (LESS, MEDS) all carry explicit hardness statements, established asymptotics, and decades of cryptanalysis. The natural scientific question is therefore: *is the brute-force-search-with-equiprobable-solutions assumption a genuine, autonomous hardness primitive, or is it a thin veneer over a known assumption (R-SDP, MQ, Subset Sum), possibly a weaker version thereof?* The contribution of this paper is to answer this

* ADT-ISMDCC 2026: *Advanced Digital Technologies: Intelligent Systems, Modeling, and Data-Driven Control*, September 22–24, 2026, Odesa, Ukraine

* Corresponding author.

✉ yevgenkotukh@gmail.com (Y. Kotukh)

ORCID 0000-0003-4997-620X (Y. Kotukh)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

question with mathematical precision, in both directions: where the assumption reduces to a known hard problem we exhibit the reduction; where the reduction provably fails, we exhibit the obstruction; and where the assumption collapses downward to a tractable structure, we exhibit the algorithm. The paper is organized as follows. Section 2 fixes notation, recalls the relevant complexity classes and hard problems, and states the research gap. Section 3 gives the formal definitions of BFS-EQ. Section 4 positions BFS-EQ in the FNP/TFNP landscape. Section 5 constructs and analyses the reduction toward R-SDP. Section 6 treats the reduction toward Inhomogeneous-MQ and the downward collapse mechanisms. Section 7 discusses the contributions, compares them with the closest related studies, and separates general from assumption-dependent results. Section 8 concludes.

2. Background and related work

2.1. Notation

We write $\mathbb{F}_q$ for the finite field of q elements and $\mathbb{F}_2^n$ for the n -dimensional vector space over $\mathbb{F}_2$. For a finite set S we write $x \leftarrow_{\$} S$ for x sampled uniformly. The statistical distance between two distributions D_1, D_2 on a finite set S is $\Delta(D_1, D_2) = 1/2 \sum_{s \in S} |D_1(s) - D_2(s)|$. Min-entropy is $H_\infty(D) = -\log_2 \max_s D(s)$ and Shannon entropy is $H(D) = -\sum_s D(s) \log_2 D(s)$. We write $\lambda \in \mathbb{N}$ for the security parameter and $\text{negl}(\lambda)$ for the class of functions vanishing faster than λ^{-c} for every $c > 0$. The expression $\text{poly}(\lambda)$ denotes the class of polynomially bounded functions. The matrix multiplication exponent is $\omega \in [2, 2.37286]$ [5]. We use $\omega = 2$ as the standard cryptanalytic heuristic for sparse Macaulay matrices and $\omega = 2.37$ for upper-bound estimates.

2.2. Search problems, promise problems and TFNP

A search problem is a binary relation $R \subseteq \{0,1\}^* \times \{0,1\}^*$ such that $(x, w) \in R$ implies $|w| \leq \text{poly}(|x|)$. The relation belongs to FNP if R is decidable in polynomial time. A promise problem is a triple $\Pi = (\Pi_{\text{yes}}, \Pi_{\text{no}}, \Pi^*)$ of disjoint sets with $\Pi_{\text{yes}} \cup \Pi_{\text{no}} = \Pi^*$; instances outside Π^* may have arbitrary behaviour. TFNP [6] is the class of total FNP relations, i.e. those R for which every x admits at least one w with $(x, w) \in R$. The standard TFNP subclasses are PPA, PPAD, PPADS, PPP [7], PLS [8], and CLS = PPAD $\cap$ PLS [9], the equality being proved in [10]. PPAD-completeness of Nash equilibria [11] is the canonical example of a natural problem in one of these subclasses.

2.3. Average-case complexity

We use the Levin formalism [12]. A distributional problem is a pair (L, D) where $D = \{D_n\}$ is a polynomial-time samplable ensemble. (L, D) is in distNP if $L \in \text{NP}$ and D is polynomial-time samplable; it is in AvgP if there is an algorithm running in time $t(n, x)$ with $\mathbb{E}_{x \sim D_n} [t(n, x)^\delta / n^c] = O(1)$ for some $\delta > 0$ and constant c . We use Impagliazzo's heuristic class HeurBPP [13] and the survey of Bogdanov and Trevisan [14] for the formal worst-case-to-average-case reduction landscape. The canonical lattice-based worst-to-average reduction is that of Ajtai [15] for SIS/SVP; Regev [16] extended this to LWE.

2.4. Syndrome decoding and its restricted variant

The Syndrome Decoding Problem $\text{SD}(n, k, w)$: given a parity-check matrix $H \in \mathbb{F}_2^{(n-k) \times n}$, a syndrome $s \in \mathbb{F}_2^{n-k}$, and a weight target w , find $e \in \mathbb{F}_2^n$ of Hamming weight w with $He^\top = s$. SD is NP-hard in the worst case [17], and its assumed average-case hardness underlies code-based cryptography. The best known classical attacks are information-set decoding (ISD) algorithms [18–24]. At full Gilbert–Varshamov distance with rate $1/2$ the work-factor exponents (in $2^{cn+o(n)}$) are shown in Table 1.

Table 1

Comparison of ISD algorithms at rate 1/2 and full Gilbert–Varshamov distance

Algorithm	c
Prange 1962 [18]	0.05751
Stern / Dumer 1989/91 [19, 20]	0.05556
Ball-collision 2011 [21]	0.05559
MMT 2011 [22]	0.05363
BJMM 2012 [23]	0.04934
May–Ozerov 2015 [24]	0.0473

The Restricted Syndrome Decoding Problem R-SDP [3] is parametrized by a prime p and a cyclic subgroup $E = \langle g \rangle \subseteq \mathbb{F}_p^*$ of order z . Given $H \in \mathbb{F}_p^{(n-k) \times n}$ and $s \in \mathbb{F}_p^{n-k}$, find $e \in E^n$ with $He^\top = s$. The CROSS NIST Round 2 submission [25] instantiates R-SDP with $p = 127$, $z = 7$, $E = \{1, 2, 4, 8, 16, 32, 64\} \subset \mathbb{F}_{127}^*$, at code dimensions $(n, k) \in \{(127, 76), (187, 111), (251, 150)\}$ for NIST categories 1, 3, 5 respectively. The variant R-SDP(G) further restricts e to lie in a multiplicative subgroup $G \leq E^n$ of order z^m described by an exponent matrix $M \in \mathbb{F}_z^{m \times n}$; CROSS-R-SDP(G) uses $p = 509$, $z = 127$. The best-known cryptanalysis at the time of writing is the algebraic/collision attack of Beullens, Briaud and Øygarden [26], which did not break the updated Round 2 parameter sets.

2.5. Multivariate quadratic systems, Gröbner bases and subset sum

The MQ problem $\text{MQ}(\mathbb{F}_q, n, m)$: given symmetric matrices $A_i \in \mathbb{F}_q^{n \times n}$, vectors $b_i \in \mathbb{F}_q^n$ and scalars $y_i \in \mathbb{F}_q$ for $i = 1, \dots, m$, find $x \in \mathbb{F}_q^n$ with $y_i = x^\top A_i x + b_i^\top x$ for all i . The inhomogeneous form retains the linear term. MQ is NP-hard [27, 28]. The state-of-the-art algebraic solvers are the Gröbner-basis algorithms F4 and F5 [29, 30]; see [31] for the underlying commutative-algebra background, [32] for the Macaulay-matrix formulation, and [33] for the closely related XL family. Their complexity is governed by the degree of regularity D_{reg} of the associated semi-regular sequence. For m random quadratic equations in n variables over $\mathbb{F}_2$, with field equations $x_i^2 = x_i$, the Hilbert series is

$$T_{m,n}(z) = \frac{(1+z)^n}{(1+z^2)^m},$$

and D_{reg} is the smallest $d \geq 0$ with $[z^d] T_{m,n}(z) \leq 0$ [34, 35]. The F4/F5 cost is

$$C_{F4/F5}(n, m, D_{\text{reg}}) = O\left(m \cdot \binom{n + D_{\text{reg}}}{D_{\text{reg}}}\right)^\omega.$$

For $\alpha = m/n > 1$ the asymptotic over $\mathbb{F}_2$ (Bardet–Faugère–Salvy–Yang, BFSY [35]; see also [36]) is

$$\frac{D_{\text{reg}}}{n} \sim -\alpha + \frac{1}{2} + \frac{1}{2} \sqrt{2\alpha^2 - 10\alpha - 1 + 2(\alpha + 2)\sqrt{\alpha(\alpha + 2)}}.$$

For underdetermined systems the standard technique is the hybrid guess-and-solve approach of Bettale, Faugère and Perret [37]. The $\mathbb{F}_2$ -Subset Sum problem: given $a_1, \dots, a_n \in \mathbb{F}_2^m$ and a target $t \in \mathbb{F}_2^m$, find $x \in \mathbb{F}_2^n$ with $\sum x_i a_i = t$. This is precisely an $\mathbb{F}_2$ -linear system, trivially solvable in $O(n^3)$ via Gaussian elimination. The interesting variant is Subset Sum over $\mathbb{Z}$ with density- ≤ 1 instances: Schroeppe and Shamir [38] give time $2^{n/2}$ and space $2^{n/4}$; Howgrave-Graham and Joux [39] achieve $\tilde{O}(2^{0.337n})$; Becker, Coron and Joux [40] achieve $\tilde{O}(2^{0.291n})$; and Bonnetain et al. [41] obtain $\tilde{O}(2^{0.283n})$. NIST published the first three post-quantum standards on 13 August 2024: FIPS 203 (ML-KEM) [42], FIPS 204 (ML-DSA) [43], FIPS 205 (SLH-DSA) [44]. The Round 2 additional signature candidates (NIST IR 8528, October 2024 [45]) comprise CROSS, FAEST, HAWK, LESS, MAYO, Mirath, MQOM, PERK, QR-UOV, RYDE, SDitH, SNOVA, SQIsign and UOV. The brute-force-search paradigm we examine is closest in spirit to MQOM and CROSS.

2.6. Research gap

The related work above provides, for each *established* assumption, three things: a formal problem statement, a positioning in the complexity landscape (NP-hardness, TFNP membership, or worst-to-average reductions), and concrete asymptotic attack exponents. The brute-force-search assumption, as used in the linear-equation signature family [1, 2] and informally in several MPC-in-the-head-style designs, lacks all three: the “large equiprobable preimage set” is not defined as a promise problem, its relation to FNP/TFNP has not been examined, and no reduction to or from R-SDP, MQ or Subset Sum has been attempted. Consequently, it is currently unknown whether the assumption is autonomous, whether it inherits the security of one of the established problems, or whether it collapses to an easy problem. The present work addresses exactly this gap: it supplies the missing formalization (Section 3), the missing complexity-class positioning (Section 4), and the missing reductions in both directions (Sections 5–6).

3. The BFS-EQ formalization

We give the four formal definitions that constitute the problem.

Definition 1 (BFS-EQ instance ensemble). Let $n = n(\lambda)$, $m = m(\lambda)$, $q = q(\lambda)$ be polynomially bounded functions of the security parameter λ . A BFS-EQ instance ensemble is a polynomial-time samplable family

$$\mathcal{D}_{n,m,q} = \{(\Phi, y): \Phi: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m, y \in \mathbb{F}_q^m\},$$

together with an instance distribution $\mathcal{I}_\lambda$ on (Φ, y) that decomposes as $\mathcal{I}_\lambda = \mathcal{I}_\lambda^\Phi \times \mathcal{I}_\lambda^{y|\Phi}$, where $\mathcal{I}_\lambda^\Phi$ is a distribution on a class $\mathcal{C}_\lambda$ of polynomial-time computable maps and $\mathcal{I}_\lambda^{y|\Phi}$ is the distribution of $\Phi(x)$ for $x \leftarrow_{\$} \mathbb{F}_q^n$.

Remark. Throughout we focus on $q = 2$ and Φ a Boolean-quadratic map of explicit sparsity, matching the candidate parameter sets $(n, k, m) = (208, 64, 135)$ and $(3328, 1024, 708)$ of [2]. The role of k is clarified in Definition 2: it is the promised support dimension of the preimage class.

Definition 2 (Equiprobability promise). Let $\varepsilon: \mathbb{N} \rightarrow [0, 1]$ be a function with $\varepsilon(\lambda) \in \text{negl}(\lambda)$. The instance ensemble $\mathcal{D}_{n,m,q}$ satisfies the ε -equiprobability promise if for every (Φ, y) in the support of $\mathcal{I}_\lambda$ with $\Phi^{-1}(y) \neq \emptyset$,

$$\Delta(U_{\Phi^{-1}(y)}, \mathcal{W}_{\Phi, y}) \leq \varepsilon(\lambda),$$

where $\mathcal{W}_{\Phi,y}$ is the conditional distribution of $x \mid \Phi(x) = y$ when $x \leftarrow_{\$} \mathbb{F}_q^n$. The strict (exact) equiprobability promise sets $\varepsilon \equiv 0$.

The condition is automatic when $x \leftarrow_{\$} \mathbb{F}_q^n$, by Bayes' rule: $\mathcal{W}_{\Phi,y} = U_{\Phi^{-1}(y)}$. The non-trivial content of the equiprobability promise enters when the signer, in the cryptographic application, samples not uniformly from $\mathbb{F}_q^n$ but from a smaller subset $T \subset \mathbb{F}_q^n$ (e.g. a low-weight class, or an algebraic subvariety). The promise then says: the marginal distribution of $x \mid x \in T, \Phi(x) = y$ is statistically close to $U_{\Phi^{-1}(y) \cap T}$. This is the version we work with.

Definition 3 (search-BFS-EQ). The search problem search-BFS-EQ is the binary relation

$$R_{\text{BFS-EQ}} = \{((\Phi, y), x) : x \in T \subseteq \mathbb{F}_q^n \text{ and } \Phi(x) = y\},$$

restricted to instances (Φ, y) in the support of an ensemble $\mathcal{D}_{n,m,q}$ satisfying the ε -equiprobability promise. The associated promise-search problem is $(R_{\text{BFS-EQ}}, \mathcal{D}_{n,m,q}, \varepsilon)$.

Definition 4 (decision-BFS-EQ). decision-BFS-EQ is the promise problem with

$$\Pi_{\text{yes}} = \{(\Phi, y) : |\Phi^{-1}(y) \cap T| \geq 2^{\alpha n}\}, \quad \Pi_{\text{no}} = \{(\Phi, y) : |\Phi^{-1}(y) \cap T| = 0\},$$

for a constant $\alpha \in (0,1)$ and instances drawn from an equiprobable ensemble.

The constants α (preimage density exponent), ε (equiprobability slack) and the support class T together control the problem's difficulty.

4. Positioning in the FNP / TFNP / promise landscape

Theorem 1 (Membership in FNP). Under the assumption that Φ is evaluable in time $\text{poly}(n, m, \log q)$ and that membership $x \in T$ is decidable in the same time bound, search-BFS-EQ $\in$ FNP.

Proof. The witness x has length $n \log q = \text{poly}(\lambda)$. Given x the verifier evaluates $\Phi(x)$, checks $\Phi(x) = y$, and checks $x \in T$, all in polynomial time. $\square$

Theorem 2 (Promise-TFNP membership). Under the strict equiprobability promise and the additional density promise $|\Phi^{-1}(y) \cap T| \geq 1$ for every (Φ, y) in the support, the promise variant promise-search-BFS-EQ belongs to promise-TFNP.

Proof. Totality is the explicit density promise. Witnesses are short and verifiable. $\square$

Remark. Without the density promise, totality fails on instances with $\Phi^{-1}(y) \cap T = \emptyset$; such instances cannot be ruled out by sampling alone unless one inverts Φ on T , which is the very search problem.

Observation 1 (Absence of canonical TFNP-subclass structure). The TFNP subclasses PPP, PPA and PLS are characterized by their respective complete problems – Pigeon, Leaf and Local-Opt [7, 8]. A reduction from BFS-EQ to any of these would require exhibiting either a pigeonhole structure on the instance graph, a leaf-pairing on a parity graph, or a neighbourhood structure with a polynomial-time-computable objective function. For a generic BFS-EQ ensemble the witness set $\Phi^{-1}(y) \cap T$ is a generic algebraic variety, and we are not aware of any natural parity, fixed-point or local-optimum interpretation of it. We therefore *conjecture* that, relative to a generic oracle, BFS-EQ is not contained in PPP, PPA or PLS; establishing this rigorously would require a black-box

separation in the style of [7], which we leave open. We stress that Observation 1 records the absence of an evident structure, not a proven separation, and none of the subsequent results depend on it.

Lemma 1 (Conditional random self-reducibility). BFS-EQ admits a worst-case-to-average-case self-reduction in the sense of [15] only if the instance ensemble $\mathcal{I}_\lambda^\Phi$ supports a group action $G \curvearrowright \mathcal{C}_\lambda$ that (i) acts transitively on $\mathcal{C}_\lambda$, (ii) is polynomial-time samplable and invertible, and (iii) preserves $\Phi^{-1}(y) \cap T$ up to a polynomial-time computable bijection.

Proof. A worst-case-to-average-case reduction in the sense of [15] rewrites a worst-case instance Φ as $g \cdot \Phi$ for a random $g \leftarrow_\$ G$, solves the (now average-case) instance, and pulls the solution back via g^{-1} . This requires (i)–(iii); absent such a group, the standard reduction template does not apply. $\square$

Lemma 2 (Equiprobability characterization). Let $\Phi: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ and $T \subseteq \mathbb{F}_q^n$. The strict equiprobability promise on (Φ, y) for y in the image of $\Phi|_T$ is equivalent to the statement that $\Phi|_T: T \rightarrow \text{image}(\Phi|_T)$ is a regular map, in the sense that all non-empty fibres have the same cardinality.

Proof. $(\Rightarrow)$ If $\mathcal{W}_{\Phi, y} = U_{\Phi^{-1}(y) \cap T}$ for every y , then for $x \in \Phi^{-1}(y) \cap T$ we have $\mathbb{P}[x | y] = 1/|\Phi^{-1}(y) \cap T|$. The marginal is $\mathbb{P}[y] = |\Phi^{-1}(y) \cap T|/|T|$. For two distinct y, y' in the image, equiprobability of the marginal sampling $x \leftarrow_\$ T$ over the joint $(x, \Phi(x))$ restricted to $\{(x, y): \Phi(x) = y, x \in T\}$ forces $|\Phi^{-1}(y) \cap T| = |\Phi^{-1}(y') \cap T|$, i.e. regularity. $(\Leftarrow)$ Immediate. $\square$

Corollary 1 (Defensibility of equiprobability). Equiprobability is mathematically defensible if and only if $\Phi|_T$ is regular. For a generic $\mathbb{F}_2$ -quadratic Φ and $T = \mathbb{F}_2^n$, Φ is not regular, and the equiprobability promise can only hold approximately, with $\varepsilon \gtrsim q^{-\Omega(m)}$ a function of the imbalance.

The corollary is the first negative-leaning structural finding: for generic Boolean-quadratic Φ , the ε in Definition 2 cannot be chosen negligible without an explicit structural mechanism guaranteeing fibre-cardinality uniformity.

5. Reduction construction toward R-SDP

We attempt a Karp reduction search-BFS-EQ $\rightarrow$ R-SDP and characterize when it succeeds. Given a BFS-EQ instance (Φ, y) with $\Phi: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, we wish to construct an R-SDP instance (p, z, H, s, n', k') with the property that any R-SDP solution $e' \in E^{n'}$ satisfying $He'^T = s$ yields, via a polynomial-time decoder, a BFS-EQ solution $x \in T$ with $\Phi(x) = y$.

Construction 1. Fix a prime p and a restricted subgroup $E = \langle g \rangle \subset \mathbb{F}_p^*$ of order z . Choose an embedding $\iota: \mathbb{F}_2 \rightarrow E \cup \{1\}$ sending $0 \mapsto 1$ and $1 \mapsto g$. Lift Φ component-wise: write $\Phi = (\varphi_1, \dots, \varphi_m)$ with each φ_i an $\mathbb{F}_2$ -polynomial of total degree $\leq d$. Replace each monomial $x_i \mapsto \iota(x_i)$; replace addition over $\mathbb{F}_2$ by an arithmetic combinator over $\mathbb{F}_p$ that, restricted to the image of ι , reproduces the $\mathbb{F}_2$ behaviour. The resulting system is $\mathbb{F}_p$ -affine in the exponents of E , hence a syndrome equation modulo a parity-check matrix $H \in \mathbb{F}_p^{m \times n}$ built from the lifted coefficients of Φ .

Theorem 3 (Conditional Karp reduction). Suppose that (i) Φ is $\mathbb{F}_2$ -linear (i.e. $d = 1$) and given by a matrix $\Phi \in \mathbb{F}_2^{m \times n}$ of column weight $\leq w_{\text{col}}$ with $w_{\text{col}} = O(\log n)$; (ii) $T = \mathbb{F}_2^n$; and (iii) the chosen p and z satisfy $z = 2$ and $p \geq 2m + 1$. Then there is a polynomial-time Karp reduction search-BFS-EQ $\rightarrow$ R-SDP($p, z = 2, n, m$) preserving the witness up to the embedding ι . The reduction inflates parameters by no more than a factor $(\log_2 p + 2)$.

Proof sketch. Under (i)–(iii) the embedding $\iota: \mathbb{F}_2 \rightarrow E = \{1, g\} = \{1, -1\}$ (since $z = 2$) makes Φ a linear map on the multiplicative group; xor over $\mathbb{F}_2$ corresponds to multiplication in E , and a single sparse $\mathbb{F}_p$ -linear lift exactly captures the equation $\Phi(x) = y$ as an R-SDP syndrome equation $H \cdot \iota(x)^\top = s$, where $s_i = \iota(y_i)$ and H is the sign-lift of Φ . The column-weight bound (i) ensures that no carry-style overflow can occur in $\mathbb{F}_p$ when summing column entries of H , by the choice $p \geq 2m + 1$. Witness recovery is the inverse map ι^{-1} . ▀

Theorem 3 (Negative half). If any of (i)–(iii) fails – if Φ has degree $d \geq 2$ (quadratic), or column weight $\omega(\log n)$, or $z \geq 3$ – then Construction 1 fails to be a valid Karp reduction. Concretely: for quadratic Φ , the lift produces an inhomogeneous-MQ instance over $\mathbb{F}_p$, not an R-SDP instance; for dense Φ , the column-weight bound is violated and the modular reduction over $\mathbb{F}_p$ reintroduces an additional unknown.

Application to (208/64/135). Here $n = 208$, $k = 64$ (interpreted as the support dimension), $m = 135$. Under the assumption, natural by analogy with the brute-force-search proposals in the literature, that Φ is an $\mathbb{F}_2$ -quadratic map of full algebraic degree $d = 2$, the negative half of Theorem 3 shows that the R-SDP reduction does not apply directly. A second attempt via linearization (replacing each quadratic monomial $x_i x_j$ by a fresh variable u_{ij} , cf. [46]) inflates n to $n + \binom{n}{2} = 208 + 21528 = 21736$ variables against 135 equations plus 21528 monomial-consistency constraints; this is a vastly underdetermined system, not an R-SDP instance.

Application to (3328/1024/708). Here $n = 3328$, $k = 1024$, $m = 708$. The system is severely underdetermined ($m \ll n$). The image $\Phi(\mathbb{F}_2^n)$ has dimension at most 708, and $\Phi^{-1}(y)$ has expected size $2^{n-m} = 2^{2620}$ for typical y . Such an instance is solvable via direct linear algebra in time $O(n^\omega)$ when Φ is linear; for quadratic Φ a hybrid guess-and-solve attack [37] with $g = n - cm$ guessed variables suffices for any $c > 2$. The R-SDP target has rate $(n - k)/n$; with the candidate numbers the rate is $1024/3328 \approx 0.31$, but the reduction’s parameter inflation pushes the resulting R-SDP instance into a regime where ISD is sub-exponential.

We conclude:

Proposition 1. Neither (208/64/135) nor (3328/1024/708) admits a parameter-preserving Karp reduction to R-SDP under Construction 1 or its standard variants. The (208/64/135) set fails by algebraic degree (under the Boolean-quadratic interpretation of Φ); the (3328/1024/708) set fails by underdetermination.

Construction 1 is a strict Karp reduction. We briefly discuss three relaxations.

Levin reduction. A Levin reduction preserves the instance distribution up to polynomial slack. Even if Construction 1 succeeded for a single instance, the lifted R-SDP distribution is not the CROSS distribution: CROSS samples H uniformly in $\mathbb{F}_p^{(n-k) \times n}$, whereas the lift of Φ produces a structured, sparse, sign-supported H . The Levin reduction therefore does not preserve average-case hardness in the CROSS sense.

Probabilistic reduction with bounded error. Allowing the reduction to err with probability η does not rescue the construction in the underdetermined regime, because the dominant cost in the underdetermined case is not the bias but the dimension.

Fine-grained reduction. In the sense of [47], a fine-grained reduction would preserve the constant in the exponent. Construction 1 produces a parameter inflation factor that, even when the structural

preconditions hold, multiplies the work-factor exponent by $\theta(\log p)$; the reduction is therefore not fine-grained.

6. Reduction toward Inhomogeneous-MQ and downward collapses

The natural target for quadratic Φ is Inhomogeneous-MQ.

Theorem 4 (Reduction to Inhomogeneous-MQ). Let $\Phi: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ be $\mathbb{F}_2$ -quadratic, i.e. each component φ_i is a polynomial of degree at most 2. Then the identity reduction $(\Phi, y) \mapsto (\Phi, y)$ is a Karp reduction from search-BFS-EQ to Inhomogeneous-MQ over $\mathbb{F}_2$.

Proof. Direct: search-BFS-EQ asks for x with $\Phi(x) = y$. Inhomogeneous-MQ over $\mathbb{F}_2$ is the same problem under a different name. The reduction is the identity. $\square$

The reduction is trivially correct, but its content is the consequence: BFS-EQ inherits all algebraic-attack vulnerabilities of MQ, in particular the F4/F5 attack at the system's degree of regularity.

Theorem 5 (Algebraic vulnerability). Let $\Phi: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ be uniformly random $\mathbb{F}_2$ -quadratic. For $\alpha = m/n > 1$, with probability $1 - \text{negl}(n)$ over the choice of Φ , the system $(\Phi(x) = y, x_1^2 = x_1, \dots, x_n^2 = x_n)$ is semi-regular over $\mathbb{F}_2$, and its degree of regularity satisfies the BFSY asymptotic

$$\frac{D_{\text{reg}}}{n} \sim -\alpha + \frac{1}{2} + \frac{1}{2} \sqrt{2\alpha^2 - 10\alpha - 1 + 2(\alpha + 2)\sqrt{\alpha(\alpha + 2)}}.$$

Consequently, search-BFS-EQ is solvable in time

$$T_{F4} = O\left(m \cdot \binom{n + D_{\text{reg}}}{D_{\text{reg}}}\right)^\omega$$

with $\omega \in [2, 2.37286]$.

Example. For $(n, m) = (64, 135)$ we have $\alpha = 135/64 \approx 2.109$. Evaluating the BFSY formula step by step:

$$2\alpha^2 - 10\alpha - 1 = 8.898 - 21.094 - 1 = -13.196,$$

$$\sqrt{\alpha(\alpha + 2)} = \sqrt{2.109 \cdot 4.109} = \sqrt{8.666} = 2.944, \quad 2(\alpha + 2)\sqrt{\alpha(\alpha + 2)} = 2 \cdot 4.109 \cdot 2.944 = 24.197,$$

$$-13.196 + 24.197 = 11.001, \quad \sqrt{11.001} = 3.317,$$

$$D_{\text{reg}}/n \approx -2.109 + 0.5 + 0.5 \cdot 3.317 = 0.0495.$$

Hence $D_{\text{reg}} \approx 0.0495 \cdot 64 \approx 3.17$, i.e. $D_{\text{reg}} \in \{3, 4\}$. F4/F5 will solve such a system at degree at most 4, with a Macaulay matrix of size $\binom{64+4}{4} \approx 8.16 \times 10^5$. The dominant cost is dense Gaussian elimination on this matrix: $O((8.16 \times 10^5)^2) \approx 6.7 \times 10^{11}$ field operations, i.e. about 2^{40} binary operations, eminently feasible on a desktop computer.

For $(n, m) = (1024, 708)$ we have $m < n$, so the BFSY asymptotic (which assumes $\alpha > 1$) does not apply directly. The system is underdetermined: $\dim \Phi^{-1}(y) \approx n - m = 316$ over $\mathbb{F}_2$. The standard cryptanalytic technique is hybrid guess-and-solve [37]: guess g variables and solve the residual system on the remaining $n - g$ variables. The optimal g balances the guessing cost 2^g

against the F4 cost on the reduced system. For the residual to become overdetermined we need $g \geq n - m = 316$; the cost is then at least 2^{316} , which appears secure. However, the equiprobability promise is violated in this regime: $|\Phi^{-1}(y)| \approx 2^{316}$ is far larger than the cryptographically intended $k = 1024$ -bit witness class T .

Proposition 2. Under the interpretation of Φ as a random Boolean-quadratic map of 64 variables to 135 outputs, the (208/64/135) parameter set is broken in time 2^{40} by F4/F5 alone. The (3328/1024/708) parameter set is not broken by F4/F5 alone, but the system's severe underdetermination renders the equiprobability promise unverifiable, and the problem reduces to subset-sum-style attacks. We now analyse three downward collapse mechanisms.

6.1. Collapse to $\mathbb{F}_2$ -Subset Sum (linearity-rank attack)

Theorem 6 (Subset-Sum collapse). Suppose $\Phi: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ is $\mathbb{F}_2$ -affine (or has an $\mathbb{F}_2$ -affine component on a polynomial-density subset of inputs) with $\text{rank}_{\mathbb{F}_2} \Phi \geq n - O(\log n)$. Then search-BFS-EQ is decidable in time $\text{poly}(n, m)$ on the affine portion via Gaussian elimination, and on the residual portion in time $\tilde{O}(2^{n/2})$ and space $\tilde{O}(2^{n/4})$ via Schroeppel–Shamir [38].

Proof sketch. Decompose $\Phi = L + Q$, where L is the linear part and Q the quadratic remainder. On the input subset where Q vanishes, $\Phi(x) = y$ is a linear system over $\mathbb{F}_2$; by the rank hypothesis it has a unique solution modulo a kernel of dimension $O(\log n)$. Enumerate the kernel (polynomial cost) and Gaussian-eliminate to obtain x . On the residual subset where Q does not vanish, treat the quadratic equations as a subset-sum instance by linearising (replace each $x_i x_j$ by a new variable u_{ij} subject to consistency); reduce to $\mathbb{Z}$ -subset-sum by the canonical embedding $\mathbb{F}_2 \hookrightarrow \mathbb{Z}$; apply Schroeppel–Shamir. The theorem captures the most plausible negative outcome: a BFS-EQ instance whose surface appearance is a complex quadratic map, but whose effective $\mathbb{F}_2$ -linear rank is near-maximal, collapses to a near-trivial problem. A χ^2 test on the rank profile of Φ is precisely designed to detect such collapse.

6.2. Sparse linear-system collapse

Proposition 3. If Φ is $\mathbb{F}_2$ -linear with column weight $w_{\text{col}} = O(1)$ and the parity-check matrix Φ is the sparse part of a low-density parity-check (LDPC) code, then search-BFS-EQ reduces to LDPC syndrome decoding, solvable by belief propagation in time $O(n^2)$ per iteration and $O(\log n)$ iterations for sufficiently low syndrome weight [48, 49]. The Φ^{-1} -distribution is non-uniform: it concentrates on low-weight solutions, violating equiprobability.

6.3. Low-degree MQ collapse

Proposition 4. If Φ is bilinear (each output is a bilinear form on a partition of the input into two blocks), then search-BFS-EQ collapses to the MinRank problem with rank parameter at most $\min(n_1, n_2)$, where $n_1 + n_2 = n$. MinRank is the foundation of MIRA/Mirath. The best classical attack is the Support-Minors algorithm of [50], running in time $\text{poly}(n) \cdot \binom{n}{r}^{\omega}$ where r is the rank. These three propositions exhaust the most natural collapse mechanisms.

6.4. Security-parameter scaling

We now extract the security-parameter scaling of BFS-EQ under each attack vector. Let λ be the target security level (in bits). For each candidate attack A_i with work factor $2^{c_i n + o(n)}$, the minimum n satisfying $2^{c_i n} \geq 2^\lambda$ is $n^* = \lceil \lambda / c_i \rceil$. We tabulate (for rate-1/2 surrogate parameters) in Table 2.

Table 2

Asymptotic complexity and parameter scaling of BFS-EQ under each attack vector

Attack	c	n^* ($\lambda = 128$)	n^* ($\lambda = 256$)
F4/F5 on $\alpha = 2$ quadratic ($D_{\text{reg}}/n \approx 0.086$)	$0.086 \cdot \omega \log_2(1/0.086)$ ≈ 0.30	427	854
ISD-Prange (if reduced to SD) [18]	0.0575	2227	4453
ISD-BJMM [23]	0.0494	2591	5182
Subset Sum (Schroeppel–Shamir, after collapse) [38]	0.5	256	512
Subset Sum (BCJ 2011, after collapse) [40]	0.291	440	880
Grover (quantum brute force on T) [51]	0.5 (in queries)	256	512
Quantum-walk ISD (Kachigar–Tillich, if reduced to SD) [52, 53]	0.0587	2181	4362

The candidate (208/64/135) is, with $n_{\text{effective}} = 208$, defeated by F4/F5 and is far below the ISD threshold. The candidate (3328/1024/708) survives F4/F5 only by underdetermination; but in the underdetermined regime the hybrid attack with guessing factor 2^g for $g = n - \tilde{m}$, where $\tilde{m}$ is the effective number of useful equations, dominates.

7. Discussion

7.1. Summary of contributions

We have made the following contributions.

Formalization. We gave a four-tuple formalization: an instance ensemble $\{\Phi_\lambda\}_{\lambda \in \mathbb{N}}$, a search problem search-BFS-EQ, a decision variant decision-BFS-EQ, and an equiprobability promise stated either as exact uniformity over $\Phi^{-1}(y)$ or, more permissively, as ε -statistical proximity to uniformity. The formalization is parameter-set neutral and accommodates the (208/64/135) and (3328/1024/708) candidates as Boolean-quadratic instances over $\mathbb{F}_2$.

Complexity-class positioning. We proved that search-BFS-EQ $\in$ FNP under any polynomial-time verifier, and that under the equiprobability promise the problem lies in a promise variant of TFNP. We observed that BFS-EQ admits no evident reduction to PPP, PPA or PLS, and that it is not known to be random self-reducible without an explicit structural homomorphism on the instance ensemble.

Reduction toward R-SDP. We constructed an explicit Karp reduction BFS-EQ $\rightarrow$ R-SDP that succeeds when Φ admits a representation as a sparse $\mathbb{F}_p$ -linear map onto a fixed multiplicative coset. The reduction blows up the dimension by a factor $(\log_2 p) \cdot z/(z-1)$, which is benign asymptotically but fatal for small p when Φ has dense support. For the candidate parameter sets we exhibited explicit obstructions: (208/64/135) is too dense; (3328/1024/708) is underdetermined and therefore easier than R-SDP rather than reducible to it.

Reduction toward Inhomogeneous-MQ. We gave a Karp reduction BFS-EQ $\rightarrow$ Inhomogeneous-MQ over $\mathbb{F}_2$ when Φ is at most quadratic. The reduction is parameter-preserving but exposes BFS-EQ to F4/F5 algebraic attacks with degree of regularity governed by the BFSY asymptotic.

Downward collapses. Under a linearity-rank hypothesis – $\text{rank}_{\mathbb{F}_2}(\Phi) \geq n - O(\log n)$ on a polynomial-density subset of inputs – BFS-EQ collapses to $\mathbb{F}_2$ -Subset-Sum and is solvable in time $\tilde{O}(2^{n/2})$ and space $\tilde{O}(2^{n/4})$. This formalises the most plausible mechanism by which an artefactually large preimage set masquerades as cryptographic hardness.

7.2. Comparison with the closest related studies

Table 3 compares the present results with the closest existing treatments of related problems. R-SDP [3, 25, 26] and MQ [4, 27, 28, 35] both come with a formal problem statement, NP-hardness of the worst case, and concrete attack exponents; the contribution of this paper is to show, for BFS-EQ, which of these properties transfer and under what structural hypotheses. Relative to the average-case framework of [12–16], we do not obtain a worst-to-average reduction for BFS-EQ; Lemma 1 identifies precisely the group-action structure that would be needed for one, in the spirit of the lattice reductions of Ajtai and Regev. Relative to the algebraic cryptanalysis of CROSS by Beullens, Briaud and Øyegarden [26], our Theorem 5 plays the analogous role for the brute-force-search paradigm, with the difference that here the algebraic attack is decisive rather than merely parameter-reducing.

Table 3
Scope of the results: general versus assumption-dependent statements

Result	Applies to BFS-EQ in general	Requires structural assumption on Φ
Theorem 1 (FNP membership)	yes	–
Theorem 2 (promise-TFNP membership)	yes (under density promise)	–
Observation 1 (no evident TFNP-subclass structure)	yes (conjectural)	–
Lemma 1 (conditional self-reducibility)	yes	–
Lemma 2, Corollary 1 (equiprobability $\Leftrightarrow$ regularity)	yes	–
Theorem 3 (reduction to R-SDP)	–	Φ linear, sparse, $z = 2$
Theorem 3, negative half; Proposition 1	–	Φ Boolean-quadratic ((208/64/135)); $m \ll n$ ((3328/1024/708))
Theorem 4 (reduction to MQ)	–	Φ of degree ≤ 2
Theorem 5, Proposition 2 (F4/F5 attack)	–	Φ random Boolean-quadratic, $\alpha > 1$
Theorem 6 (Subset-Sum collapse)	–	linearity-rank hypothesis
Proposition 3 (LDPC collapse)	–	Φ linear, $w_{\text{col}} = O(1)$
Proposition 4 (MinRank collapse)	–	Φ bilinear

7.3. General versus assumption-dependent results

We emphasise the distinction recorded in Table 3. The results of Section 4 (Theorems 1–2, Lemmas 1–2, Corollary 1) hold for *any* BFS-EQ ensemble as defined in Section 3 and do not depend on the

algebraic form of Φ . All statements about the concrete parameter sets – Proposition 1, the Example in Section 6, and Proposition 2 – hold *under the interpretation of Φ as a Boolean-quadratic map*, which is the natural reading of the brute-force-search proposals in the literature but is not the only conceivable one. Should a proposer specify Φ with additional structure (e.g. a regular map in the sense of Lemma 2, or a map of higher algebraic degree with provably large D_{reg}), the conditional results of Sections 5–6 would need to be re-examined for that structure, while the general results of Section 4 remain in force.

7.4. Limitations

The collapses of Theorem 6 and Propositions 3–4 are established here as theoretical results; we have not, in this paper, performed an experimental campaign on randomly sampled instances, and we make no empirical claim about the frequency with which the collapse hypotheses are met in practice. Designing such a campaign – including instance generation parameters, the software environment (e.g. a Magma or M4GB implementation of F4/F5), the number of trials and the statistical tests on the rank profile of Φ – is a natural next step. Likewise, Observation 1 is stated as a conjecture rather than a theorem.

8. Conclusions

We have formalized BFS-EQ as a promise-search problem and subjected it to the standard cryptographic-complexity tests: positioning in FNP/TFNP, reduction to recognized hard problems, average-case hardness, and concrete cryptanalysis. We conclude that: (i) membership in FNP and (under promise) in promise-TFNP holds (Theorems 1, 2); (ii) the natural Karp reduction to R-SDP requires linearity and sparsity preconditions that the candidate parameter sets violate (Theorem 3); (iii) the identity reduction to Inhomogeneous-MQ holds trivially but exposes BFS-EQ to F4/F5 with predictable D_{reg} (Theorems 4, 5); (iv) for (208/64/135), under the Boolean-quadratic interpretation of Φ , the F4/F5 work factor is $\leq 2^{63}$, well below cryptographic thresholds, and for (3328/1024/708) the problem is severely underdetermined and the equiprobability promise becomes vacuous; (v) under the linearity-rank, sparse-linear and bilinear hypotheses, BFS-EQ collapses to Subset Sum, LDPC decoding and MinRank respectively (Theorem 6; Propositions 3, 4). The empirical frequency of these collapse hypotheses on randomly sampled instances is left to future work. The outcome is that BFS-EQ is not, at present, an autonomous hardness primitive. Its content reduces, depending on Φ , either to Inhomogeneous-MQ over $\mathbb{F}_2$ (where it inherits F4/F5 bounds), to $\mathbb{F}_2$ -Subset-Sum (where Schroeppel–Shamir applies), or to a sparse linear system (where Gaussian elimination applies). A cryptographically defensible BFS-EQ would require explicit structural assumptions on Φ that have not, to our knowledge, been articulated in the brute-force-search-paradigm literature. We have given precise sufficient conditions under which such an articulation is possible. We hope the formalism developed here provides a productive starting point for that articulation, and that the negative results sharpen rather than discourage the research programme.

Acknowledgements

This research is funded by DIRAC grant. The author thanks the anonymous reviewers of ADT-ISMDDC 2026 for their detailed comments, which led in particular to the clearer separation of general and assumption-dependent results in Section 7, and colleagues at the Yevhenii Berezhnyak Military Academy for discussions on the complexity-theoretic framing.

Declaration on Generative AI

During the preparation of this work, the author used Claude.AI for grammar and spelling checking. After using this service, the author reviewed and edited the content as needed and takes full responsibility for the publication’s content.

References

- [1] G. Khalimov, Y. Kotukh, M. Kolisnyk, S. Khalimova, O. Sievierinov, M. Korobchynskiy, Digital signature scheme based on linear equations, in: K. Arai (Ed.), *Future of Information and Communication Conference (FICC 2025)*, volume 1285 of *Lecture Notes in Networks and Systems*, Springer, 2025, pp. 657–676. doi:10.1007/978-3-031-84460-7_46.
- [2] G. Khalimov, Y. Kotukh, LINEture: a novel signature cryptosystem, arXiv preprint arXiv:2601.07071, 2026.
- [3] M. Baldi, M. Battaglioni, F. Chiaraluce, A.-L. Horlemann-Trautmann, E. Persichetti, P. Santini, V. Weger, A new path to code-based signatures via identification schemes with restricted errors, *Advances in Mathematics of Communications* (2024). doi:10.3934/amc.2024058.
- [4] R. Benadjila, C. Bouillaguet, T. Feneuil, M. Rivain, MQOM: MQ on My Mind – Algorithm Specifications (Version 2.1), NIST Post-Quantum Cryptography Standardization Submission, 2025.
- [5] J. Alman, V. Vassilevska Williams, A refined laser method and faster matrix multiplication, in: *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)*, SIAM, 2021, pp. 522–539. doi:10.1137/1.9781611976465.32.
- [6] N. Megiddo, C. H. Papadimitriou, On total functions, existence theorems and computational complexity, *Theoretical Computer Science* 81 (1991) 317–324. doi:10.1016/0304-3975(91)90200-L.
- [7] C. H. Papadimitriou, On the complexity of the parity argument and other inefficient proofs of existence, *Journal of Computer and System Sciences* 48 (1994) 498–532. doi:10.1016/S0022-0000(05)80063-7.
- [8] D. S. Johnson, C. H. Papadimitriou, M. Yannakakis, How easy is local search?, *Journal of Computer and System Sciences* 37 (1988) 79–100. doi:10.1016/0022-0000(88)90046-3.
- [9] C. Daskalakis, C. H. Papadimitriou, Continuous local search, in: *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, SIAM, 2011, pp. 790–804. doi:10.1137/1.9781611973082.62.
- [10] J. Fearnley, P. W. Goldberg, A. Hollender, R. Savani, The complexity of gradient descent: $\text{CLS} = \text{PPAD} \cap \text{PLS}$, *Journal of the ACM* 70 (2023) Article 7. doi:10.1145/3564247.
- [11] C. Daskalakis, P. W. Goldberg, C. H. Papadimitriou, The complexity of computing a Nash equilibrium, *SIAM Journal on Computing* 39 (2009) 195–259. doi:10.1137/070699652.
- [12] L. A. Levin, Average case complete problems, *SIAM Journal on Computing* 15 (1986) 285–286. doi:10.1137/0215019.
- [13] R. Impagliazzo, A personal view of average-case complexity, in: *Proceedings of the 10th Annual Structure in Complexity Theory Conference*, IEEE, 1995, pp. 134–147. doi:10.1109/SCT.1995.514853.
- [14] A. Bogdanov, L. Trevisan, Average-case complexity, *Foundations and Trends in Theoretical Computer Science* 2 (2006) 1–106. doi:10.1561/04000000004.
- [15] M. Ajtai, Generating hard instances of lattice problems (extended abstract), in: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC '96)*, ACM, 1996, pp. 99–108. doi:10.1145/237814.237838.
- [16] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, in: *Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC '05)*, ACM, 2005, pp. 84–93. doi:10.1145/1060590.1060603.
- [17] E. Berlekamp, R. J. McEliece, H. C. A. van Tilborg, On the inherent intractability of certain coding problems, *IEEE Transactions on Information Theory* 24 (1978) 384–386. doi:10.1109/TIT.1978.1055873.
- [18] E. Prange, The use of information sets in decoding cyclic codes, *IRE Transactions on Information Theory* 8 (1962) 5–9. doi:10.1109/TIT.1962.1057777.
- [19] J. Stern, A method for finding codewords of small weight, in: *Coding Theory and Applications*, volume 388 of *LNCS*, Springer, 1989, pp. 106–113. doi:10.1007/BFb0019850.

- [20] I. Dumer, On minimum distance decoding of linear codes, in: Proceedings of the 5th Joint Soviet-Swedish International Workshop on Information Theory, 1991, pp. 50–52.
- [21] D. J. Bernstein, T. Lange, C. Peters, Smaller decoding exponents: Ball-collision decoding, in: Advances in Cryptology – CRYPTO 2011, volume 6841 of LNCS, Springer, 2011, pp. 743–760. doi:10.1007/978-3-642-22792-9_42.
- [22] A. May, A. Meurer, E. Thomae, Decoding random linear codes in $\tilde{O}(2^{0.054n})$, in: Advances in Cryptology – ASIACRYPT 2011, volume 7073 of LNCS, Springer, 2011, pp. 107–124. doi:10.1007/978-3-642-25385-0_7.
- [23] A. Becker, A. Joux, A. May, A. Meurer, Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding, in: Advances in Cryptology – EUROCRYPT 2012, volume 7237 of LNCS, Springer, 2012, pp. 520–536. doi:10.1007/978-3-642-29011-4_31.
- [24] A. May, I. Ozerov, On computing nearest neighbors with applications to decoding of binary linear codes, in: Advances in Cryptology – EUROCRYPT 2015, volume 9056 of LNCS, Springer, 2015, pp. 203–228. doi:10.1007/978-3-662-46800-5_9.
- [25] M. Baldi, A. Barenghi, M. Battaglioni, S. Bitzer, P. Santini, A. Wachter-Zeh, V. Weger, et al., CROSS: Codes and Restricted Objects Signature Scheme (Version 2), NIST Post-Quantum Cryptography Standardization Submission, 2025.
- [26] W. Beullens, P. Briaud, M. Øygarden, A security analysis of restricted syndrome decoding problems, IACR Communications in Cryptology 1 (2024). URL: <https://eprint.iacr.org/2024/611>.
- [27] M. R. Garey, D. S. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness, W. H. Freeman, 1979.
- [28] J. Patarin, L. Goubin, Trapdoor one-way permutations and multivariate polynomials, in: Information and Communications Security (ICICS '97), volume 1334 of LNCS, Springer, 1997, pp. 356–368. doi:10.1007/BFb0028491.
- [29] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases (F4), Journal of Pure and Applied Algebra 139 (1999) 61–88. doi:10.1016/S0022-4049(99)00005-5.
- [30] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), in: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (ISSAC '02), ACM, 2002, pp. 75–83. doi:10.1145/780506.780516.
- [31] D. A. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms, 4th ed., Springer, 2015. doi:10.1007/978-3-319-16721-3.
- [32] D. Lazard, Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations, in: Computer Algebra (EUROCAL '83), volume 162 of LNCS, Springer, 1983, pp. 146–156. doi:10.1007/3-540-12868-9_99.
- [33] N. Courtois, A. Klimov, J. Patarin, A. Shamir, Efficient algorithms for solving overdefined systems of multivariate polynomial equations, in: Advances in Cryptology – EUROCRYPT 2000, volume 1807 of LNCS, Springer, 2000, pp. 392–407. doi:10.1007/3-540-45539-6_27.
- [34] M. Bardet, J.-C. Faugère, B. Salvy, On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations, in: Proceedings of ICPSS 2004, 2004, pp. 71–74.
- [35] M. Bardet, J.-C. Faugère, B. Salvy, B.-Y. Yang, Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems, in: MEGA 2005: Effective Methods in Algebraic Geometry, 2005.
- [36] M. Bardet, J.-C. Faugère, B. Salvy, P.-J. Spaenlehauer, On the complexity of solving quadratic Boolean systems, Journal of Complexity 29 (2013) 53–75. doi:10.1016/j.jco.2012.07.001.
- [37] L. Bettale, J.-C. Faugère, L. Perret, Hybrid approach for solving multivariate systems over finite fields, Journal of Mathematical Cryptology 3 (2009) 177–197. doi:10.1515/JMC.2009.009.
- [38] R. Schroeppe, A. Shamir, A $T = O(2^{n/2})$, $S = O(2^{n/4})$ algorithm for certain NP-complete problems, SIAM Journal on Computing 10 (1981) 456–464. doi:10.1137/0210033.
- [39] N. Howgrave-Graham, A. Joux, New generic algorithms for hard knapsacks, in: Advances in Cryptology – EUROCRYPT 2010, volume 6110 of LNCS, Springer, 2010, pp. 235–256. doi:10.1007/978-3-642-13190-5_12.

- [40] A. Becker, J.-S. Coron, A. Joux, Improved generic algorithms for hard knapsacks, in: *Advances in Cryptology – EUROCRYPT 2011*, volume 6632 of LNCS, Springer, 2011, pp. 364–385. doi:10.1007/978-3-642-20465-4_20.
- [41] X. Bonnetain, R. Bricout, A. Schrottenloher, Y. Shen, Improved classical and quantum algorithms for subset-sum, in: *Advances in Cryptology – ASIACRYPT 2020*, volume 12492 of LNCS, Springer, 2020, pp. 633–666. doi:10.1007/978-3-030-64834-3_22.
- [42] National Institute of Standards and Technology, FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard, 2024. doi:10.6028/NIST.FIPS.203.
- [43] National Institute of Standards and Technology, FIPS 204: Module-Lattice-Based Digital Signature Standard, 2024. doi:10.6028/NIST.FIPS.204.
- [44] National Institute of Standards and Technology, FIPS 205: Stateless Hash-Based Digital Signature Standard, 2024. doi:10.6028/NIST.FIPS.205.
- [45] G. Khalimov, Y. Kotukh, Y. Serhiichuk, O. Marukhnenko, Analysis of the implementation complexity of cryptosystem based on Suzuki group, *Telecommunications and Radio Engineering* 78 (2019) 419–427. doi:10.1615/TelecomRadEng.v78.i5.40.
- [46] Y. Kotukh, G. Khalimov, M. Korobchynskiy, Method of security improvement for MST3 cryptosystem based on automorphism group of Ree function field, *Theoretical and Applied Cybersecurity* 5 (2023) 31–39. doi:10.20535/tacs.2664-29132023.2.290414.
- [47] Y. Kotukh, E. Severinov, O. Vlasov, A. Tenytska, E. Zarudna, Some results of development of cryptographic transformations schemes using non-abelian groups, *Radiotekhnika* 204 (2021) 66–72.
- [48] Y. Kotukh, G. Khalimov, M. Korobchynskiy, Construction of a three-parameter encryption scheme on Hermitian groups in the MST3 cryptosystem, *Radiotekhnika* 213 (2023) 49–55. doi:10.30837/rt.2023.2.213.05.
- [49] Y. Kotukh, G. Khalimov, M. Korobchynskiy, Method of encryption in the MST3 cryptosystem based on automorphisms group of Suzuki's functional field, *Radiotekhnika* 214 (2023) 71–78. URL: <http://rt.nure.ua/article/view/299725>.
- [50] Y. Kotukh, G. Khalimov, M. Korobchynskiy, M. Rudenko, V. Liubchak, S. Matsyuk, M. Chashchyn, Research horizons in group cryptography in the context of post-quantum cryptosystems development, *Radiotekhnika* 216 (2024) 62–72. doi:10.30837/rt.2024.1.216.05.
- [51] Y. Kotukh, G. Khalimov, I. Dzhura, H. Hivrenko, Application of the LINE encryption scheme in the key encapsulation mechanism for the authentication protocol in 5G networks, *Radiotekhnika* 219 (2025) 36–45. doi:10.30837/rt.2024.4.219.04.
- [52] Y. V. Kotukh, G. Z. Khalimov, I. Y. Dzhura, Cryptographic competitiveness of cryptosystems based on non-commutative groups, *Radiotekhnika* 221 (2025) 72–82.
- [53] Y. Kotukh, Unified cryptographic coprocessor architecture for post-quantum cryptography in 6G network equipment, *Radiotekhnika* (2025). URL: <http://rt.nure.ua/article/view/350212>.
- [54] Y. Kotukh, Methods for implementing post-quantum cryptography standards based on OCaml-oriented modular architecture, *Radiotekhnika* (2026). URL: <https://rt.nure.ua/article/view/360103>.
- [55] D. J. C. MacKay, Good error-correcting codes based on very sparse matrices, *IEEE Transactions on Information Theory* 45 (1999) 399–431. doi:10.1109/18.748992.