Representations of Elementary Vectors in VOLE-in-the-head-based Schemes

Tung Chou

Academia Sinica, Taiwan
blueprint@crypto.tw

Abstract. This paper presents a family of representations of elementary vectors, which covers existing representations as special cases. We make use of the family of representations to reduce signature size of existing signature schemes based on the VOLE-in-the-head framework. In particular, we use new representations to build modelings for the regular syndrome decoding problem in $\mathbb{F}_2$, which is used in the post-quantum signature scheme SDith, and for the permuted kernel problem in characteristic-2 fields, which is used in a post-quantum signature scheme recently proposed by Bettaieb, Bidoux, Gaborit, and Kulkarni. For the "short" parameter sets of SDith, which are designed for minimizing signature size, we achieve a size reduction of 3.6% to 4.2%. For parameter sets of the Bettaieb-Bidoux-Gaborit-Kulkarni signature scheme, we achieve a size reduction of 9% to 12%.

Keywords: post-quantum signature schemes, VOLE-in-the-head, regular syndrome decoding, permuted kernel problem

1 Introduction

In the future, large-scale quantum computers are expected to break traditional public-key schemes such as RSA [9] and schemes based on the elliptic curve discrete log problem (ECDLP). In order to collect, evaluate, and standardize existing post-quantum cryptographic schemes, a competition was initialized by NIST in 2017, which is known as the NIST post-quantum cryptography standardization process. In 2022, NIST selected 3 signature schemes along with 1 key encapsulation mechanism for standardization. In 2025, NIST selected another key encapsulation mechanism for standardization.

In 2023, NIST initilaized another branch of the competition, which is dedicated for post-quantum signature schemes. Since there are already some standardized signature schemes, candidates in this branch are considered as "additional signatures" by NIST. A promising class of candidates in the competition for additional signatures is the "MPC-in-the-head" schemes. The second-round MPC-in-the-head candidates are Mirath [2], MQOM [5], PERK [1], RYDE [3], and SDith [8]. These schemes feature pretty compact public keys. Their signatures, however, are not as compact as public keys. For example, the parameter set `SDitH2-L1-gf2-short` of SDith has public key size of only 70 bytes and signature size of 3705 bytes.

In MPC-in-the-head schemes, some existing frameworks are used to turn the hard problems into zero-knowledge proofs. In the zero-knowledge proofs, each witness is divided into multiple shares. The prover runs a multi-party-computation-like process "in the head", where each party holds one of the shares. Once the zero-knowledge proof is constructed, the Fiat-Shamir transform [7] is applied to turn the zero-knowledge proofs to signature schemes.

VOLE-in-the-head (VOLEith) [4], introduced in 2023, is one of these frameworks. Compared to other frameworks, VOLEith often allows pretty competitive signature size, so it has been adopted by several signature schemes including SDith. To make use of VOLEith, an instance of the hard problem is usually expressed as a system of polynomial equations over $\mathbb{F}_2$, such that knowledge of a solution of the polynomial system implies knowledge of a solution to the problem, and vise versa. The polynomial system is often called the "modeling". Different modelings can often lead to different signature size. Thus, it is natural to consider whether/how signature size can be improved by using better modelings.

1.1 The Regular Syndrome Decoding and Permuted Pernel Problems

The regular syndrome decoding problem (RSD) is defined as follows.

Problem 1 (RSD). Given a parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$ and $s \in \mathbb{F}_q^{n-k}$, find $e \in \mathbb{F}_q^n$ such that

- $s = He$, and
- e is the result of concatenating w elementary vectors of length n/w.

The permuted kernel problem (PKP) is defined as follows.

Problem 2 (PKP). Given $H \in \mathbb{F}_q^{m\times n}$ and $x \in \mathbb{F}_q^n$, find permutation matrix $P \in \mathbb{F}_q^{n\times n}$ such that $0 = HPx$.

The RSD problem with $q = 2$ is used in the post-quantum signature scheme SDith [8], which is a candidate in NIST's competition for additional signatures. PKP is used in

- PERK [1], which is another candidate in NIST's competition for additional signature schemes, and
- a post-quantum signature scheme described in [6], which we call "PKPith" in this paper for convenience. [1]

Signature size of PKPith is much smaller than that of PERK. In PKPith, $\mathbb{F}_q$ is always a characteristic-2 field, while in PERK q is an odd prime. Both SDith (the 2nd-round version) and PKPith are constructed by using the VOLEith framework. The current version of PERK, however, is not constructed by using VOLEith.

[1] The authors of [6] did not give a name to the scheme.

In either SDith or PKPith, signature size increases if any of the two parameters increases: The witness size $|\texttt{wit}|$, which is essentially the number of variables, and the degree d of polynomial equations in the modeling. To be more precice, the formula for signature size is of the form $X \cdot |\texttt{wit}| + Y \cdot d + Z$, where X and Y are positive values. The values of X, Y, and Z only depend on other parameters such as the number of rounds, which can be chosen independently of $|\texttt{wit}|$ and d.

A solution e of an instance of RSD consists of w elementary vectors of length n/w. Similarly, each row in a solution P of an instance of PKP is an elementary vector of length n. The modelings of SDith and PKPith highly depend on how these elementary vectors are represented. This paper discusses how to improve the modelings by using new representations of elementary vectors. As the result, we manage to reduce signature size of both SDith and PKPith. For SDith, the size reduction is achieved by reducing $|\texttt{wit}|$ while keeping the same d. For PKPith, the size reduction is achieved by reducing d by a large factor while increasing $|\texttt{wit}|$ by a relatively small factor.

1.2 Limitation

Different modelings can also lead to different computation costs. This paper focuses solely on reducing signature size with new modelings. Their impact on computation cost is considered out of scope.

1.3 Organization

Section 2 introduces notations used in this paper. Section 3 reviews how RSD is modeled in SDith. Section 4 reviews how PKP is modeled in PKPith. Section 5 presents the main ideas of the paper, including a family of representations of elementary vectors, and how to use new representations to reduce signature size of SDith and PKPith. Section 6 compares signature size under different modelings.

2 Notations

For any positive integer n, $[n]$ denotes the set $\{1, 2, \ldots, n\}$. By default, vectors are considered as column vectors. For any vector v, $\texttt{wt}(v)$ denotes the Hamming weight of v. $\texttt{reg}_q(w, \ell)$ denotes the set of vectors in $\mathbb{F}_q^{w\ell}$ that can be obtained by concatenating w elementary vectors of length ℓ. For any $v \in \texttt{reg}_q(w, \ell)$, $v^{(i)}$ denotes the vector

$$(v_{(i-1)\ell+1}, \ldots, v_{i\ell}) \in \mathbb{F}_q^{\ell}.$$

$\mathcal{E}(\ell)$ denotes the set of all elementary vectors in $\mathbb{F}_2^{\ell}$. $\mathcal{E}_d(\ell)$ denotes the set of all weight-d vectors in $\mathbb{F}_2^{\ell}$. For any matrix H, $H[i]$ denotes column i of H.

Let $(\ell : d)$ denote $\binom{\ell}{d}$. Given $S = (S_1, \ldots, S_{(\ell:d)})$ satisfying

- $S_i \subseteq \{1, \ldots, \ell\}$ and $|S_i| = d$ for each i, and

– $i \neq i' \implies S_i \neq S_{i'}$,

and a length-ℓ vector v, $\mathtt{prod}_d^S(v)$ is defined as

$$(\prod_{j \in S_1} v_j, \prod_{j \in S_2} v_j \ldots, \prod_{j \in S_{(\ell:d)}} v_j).$$

In the remainder of this paper, how S is defined exactly does not really matter, so it will be omitted from the notation.

3 How RSD is modeled in SDith

Let $e \in \mathtt{reg}_2(w, n/w)$ be a solution of an instance defined by (s, H) of RSD. In SDith, each $e^{(\alpha)}$ is considered as a tensor product of t elementary vectors. [2] That is, given $\mu_1, \ldots, \mu_t$ such that $n/w = \prod_i \mu_i$,

$$e^{(\alpha)} = v^{(\alpha,1)} \otimes v^{(\alpha,2)} \otimes \cdots \otimes v^{(\alpha,t)},$$

where $(v^{(\alpha,1)}, \ldots, v^{(\alpha,t)}) \in \mathcal{E}(\mu_1) \times \cdots \times \mathcal{E}(\mu_t)$. We define $v^{(\alpha)}$ as $v^{(\alpha,1)} \| \cdots \| v^{(\alpha,t)}$. Each entry of $e^{(\alpha)}$ can be written as $\prod_i v^{(i)}_{j_i}$, where $(j_1, \ldots, j_t) \in [\mu_1] \times \cdots \times [\mu_t]$. In this way, any vector in $\mathcal{E}(n/w)$ can be represented by a unique element in $\mathcal{E}(\mu_1) \times \cdots \times \mathcal{E}(\mu_t)$, and any element in $\mathcal{E}(\mu_1) \times \cdots \times \mathcal{E}(\mu_t)$ represents a unique vector in $\mathcal{E}(n/w)$.

When $e^{(\alpha)}$ is not known, it can be written naturally as

$$\epsilon^{(\alpha)} \coloneqq \nu^{(\alpha,1)} \otimes \nu^{(\alpha,2)} \otimes \cdots \otimes \nu^{(\alpha,t)},$$

where each $\nu^{(\alpha,i)}$ is a length-μ_i vector in which entries are variables in a multivariate polynomial ring over $\mathbb{F}_2$. We define $\nu^{(\alpha)}$ as $\nu^{(\alpha,1)} \| \cdots \| \nu^{(\alpha,t)}$. If there are w vectors $\epsilon^{(1)}, \ldots, \epsilon^{(w)}$, there will be $w \sum_i \mu_i$ variables.

Let $\epsilon = \epsilon^{(1)} \| \epsilon^{(2)} \| \cdots \| \epsilon^{(w)}$. Now, $s = H\epsilon$ immediately gives $n - k$ degree-t polynomial equations in the variables:

$$s_i = \sum_{j=1}^{n} H_{i,j} \cdot \epsilon_j, \ i = 1, \ldots, n-k. \tag{1}$$

We call these equations the *instance-dependent equations*, as they depend on the RSD instance (s, H). Knowledge of a vector $e \in \mathtt{reg}_2(w, n/w)$ such that $s = He$ implies knowledge of a solution $v = v^{(1,1)} \| \cdots \| v^{(w,t)}$ of the instance-dependent equations. However, a solution $v = v^{(1,1)} \| \cdots \| v^{(w,t)}$ of the instance-dependent equations can contain $v^{(\alpha,i)} \notin \mathcal{E}(\mu_i)$. To make use of VOLEith, we need a system of equations, such that knowledge of a solution $v = v^{(1,1)} \| \cdots \| v^{(w,t)}$ to the system

[2] [8] simply uses d to indicate the number of vectors $v^{(\alpha,i)}$'s for each α, which is reasonable as the number happens to be the same as the degree d in the modeling. We use t here because the remainder of the paper shows modelings where the number of vectors $v^{(\alpha,i)}$'s can be different from the degree d.

also implies knowledge of a vector $e \in \mathtt{reg}_2(w, n/w)$ such that $s = He$. In order to achieve this, in addition to the instance-dependent equations, some *instance-independent* equations are included in [8], such that the solution space of the instance-independent equations is basically $(\mathcal{E}(\mu_1) \times \cdots \times \mathcal{E}(\mu_t))^w$.

To ensure that $\mathtt{wt}(v^{(\alpha,i)}) \leq 1$ for any (α, i), all polynomials equations of the form $\nu_j^{(\alpha,i)} \cdot \nu_{j'}^{(\alpha,i)} = 0, j < j'$ are included in the set of instance-independent equations. To ensure that each $v^{(\alpha,i)}$ has weight 1 instead of 0, one can add linear equations of the form $\sum_j \nu_j^{(\alpha,i)} = 1$ to the system of equations. In SDith, the linear equations are not included. Instead, each $\nu_{\mu_i}^{(\alpha,i)}$ is replaced by $\sum_{j=1}^{\mu_i - 1} \nu_j^{(\alpha,i)} + 1$, which is equivalent to adding the linear equations.

The modeling above gives $|\mathtt{wit}| = w \cdot \sum_i (\mu_i - 1)$ and $d = t$. As a concrete example, in `SDitH2-L1-gf2`, $n/w = 185$ and $d = t = 4$. $(\mu_1, \mu_2, \mu_3, \mu_4)$ is set to $(4, 4, 4, 3)$, so $|\mathtt{wit}| = ((4 + 4 + 4 + 3) - 4)w = 11w$.

Remark 1. The reader might have noticed that $n/w < \prod_i \mu_i$ in `SDitH2-L1-gf2` (and actually in all other parameter sets of SDith), so the modeling above does not directly apply. We did not find how this issue is handled exactly in the specification. Our understanding is that [8, Section 2.2], which describes the modeling of SDith, is written under the assumption that $\prod_i \mu_i = n/w$. To derive the signature size, however, [8, Section 4.2] clearly uses $d = t$ and $|\mathtt{wit}| = w \cdot \sum_i (\mu_i - 1)$, so it is reasonable to believe that the modeling above is tweaked in a way that does not affect the witness size and d. The framework described in Section 5 covers the modeling above as a special case, and it works when $n/w < \prod_i \mu_i$.

4 How PKP is Modeled in PKPith

To understand how PKP is modeled in [6], consider the following two problems.

Problem 3. Given $H \in \mathbb{F}_q^{m \times n}$ and $x \in \mathbb{F}_q^n$, find $e \in \mathtt{reg}_q(n, n)$ such that $i \neq i' \implies e^{(i)} \neq e^{(i')}$ and $(\underbrace{0, \ldots, 0}_{m})^\top = \tilde{H}e$, where $\tilde{H} \in \mathbb{F}_q^{m \times n^2}$ is the matrix

$$\big(x_1 H[1] \cdots \; x_n H[1] \;\; x_1 H[2] \cdots \; x_n H[2] \;\; \cdots\cdots \;\; x_1 H[n] \cdots \; x_n H[n]\big).$$

Problem 4. Given $H \in \mathbb{F}_q^{m \times n}$ and $x \in \mathbb{F}_q^n$ and let

$$\hat{H} = \begin{pmatrix} \tilde{H} \\ I_n \cdots I_n \end{pmatrix} \in \mathbb{F}_q^{(m+n) \times n^2},$$

find $e = e^{(1)} \parallel \cdots \parallel e^{(n)}$ such that each $e^{(i)} \in \mathbb{F}_q^n$ is either an elementary vector or a zero vector, and

$$s \coloneqq (\underbrace{0, \ldots, 0}_{m}, \underbrace{1, \ldots, 1}_{n})^\top = \hat{H}e. \tag{2}$$

We show that PKP is equivalent to each of the two problems by proving the following theorems.

Theorem 1. *PKP is equivalent to Problem 3.*

Proof. Let $P \in \mathbb{F}_q^{n\times n}$ be a solution of a PKP instance defined by (H, x). Let $e \in \mathtt{reg}_q(n, n)$ be the vector obtained by setting each $e_j^{(i)}$ to $P_{i,j}$. Since P is a permutation matrix, $i \neq i' \implies e^{(i)} \neq e^{(i')}$. For $i = 1, \ldots, n$, let j_i be the integer such that $e_{j_i}^{(i)} = 1$ (or equivalently, $P_{i,j_i} = 1$). Then

$$\tilde{H}e = \sum_{i=1}^{n} x_{j_i} H[i] = HPx = (\underbrace{0, \ldots, 0}_{m})^\top,$$

which shows that e is a solution of the instance defined by (H, x) of Problem 3.

A very similar proof can be written to show that if e is a solution of an instance defined by (H, x) of Problem 3, then P, obtained by setting $P_{i,j} = e_j^{(i)}$, is a solution of the PKP instance defined by (H, x). □

Theorem 2. *Problem 3 is equivalent to Problem 4.*

Proof. Let e be a solution of an instance (H, x) of Problem 3. That is, $e \in \mathtt{reg}_q(n, n)$, $i \neq i' \implies e^{(i)} \neq e^{(i')}$, and $(0, \ldots, 0)^\top = \tilde{H}e$. To verify that e is also a solution of the instance (H, x) of Problem 4, it suffices to verify that

$$(\underbrace{1, \ldots, 1}_{n})^\top = \left(I_n \cdots I_n\right) e = \sum_{i=1}^{n} e^{(i)}, \tag{3}$$

which holds as $e \in \mathtt{reg}_q(n, n)$ and $i \neq i' \implies e^{(i)} \neq e^{(i')}$.

Now let e be a solution of an instance (H, x) of Problem 4. That is,

$$(\underbrace{0, \ldots, 0}_{m}, \underbrace{1, \ldots, 1}_{n})^\top = \hat{H} \cdot e,$$

and each $e^{(i)}$ is either an elementary vector or a zero vector. To verify the e is a solution to the instance (H, e) of Problem 3, it suffices to verify that $e \in \mathtt{reg}_q(n, n)$ and $i \neq i' \implies e^{(i)} \neq e^{(i')}$. Suppose there exists i such that $\mathtt{wt}(e^{(i)}) = 0$, we must have $\mathtt{wt}(\sum_i e^{(i)}) < n$, which implies that Equation 3 does not hold. Suppose there exist i, i' such that $i \neq i'$ and $e^{(i)} = e^{(i')}$, we must also have $\mathtt{wt}(\sum_i e^{(i)}) < n$. Therefore, by contradiction, $e \in \mathtt{reg}_q(n, n)$ and $i \neq i' \implies e^{(i)} \neq e^{(i')}$. □

Let q be a power of 2 as in [6]. When entries in s and H are viewed as column vectors over $\mathbb{F}_2$, and when entries of e are viewed as elements in $\mathbb{F}_2$, Equation 2 becomes a linear system over $\mathbb{F}_2$ of $(m+n)\log_2 q$ equations, which can be reduced to $m \log_2 q + n$ linear equations if redundant equations of the form $0 = 0$ are

removed. Now it is clear that an instance of PKP can be transformed into an instance of RSD.

The modeling for PKP in PKPith is similar to the result of applying the modeling in Section 3 to Problem 4. The difference is that in PKPith, each elementary vector is represented as a truncated tensor product. That is,

$$e^{(\alpha)} = M \cdot (v^{(\alpha,1)} \otimes v^{(\alpha,2)} \otimes \cdots \otimes v^{(\alpha,t)}),$$

where $M = (I_n\ 0) \in \mathbb{F}_2^{n \times \prod_i \mu_i}$ and $(v^{(\alpha,1)}, \ldots, v^{(\alpha,t)}) \in \mathcal{E}(\mu_1) \times \cdots \times \mathcal{E}(\mu_t)$. In this way, each vector in $\mathcal{E}(n)$ is represented by a unique element in $\mathcal{E}(\mu_1) \times \cdots \times \mathcal{E}(\mu_t)$. PKPith also sets the following rules on parameters:

- $d = t = \lceil \log_2 n \rceil$, and
- $\mu_i = 2$ for each i.

In this way, $|\mathtt{wit}| = n \cdot \lceil \log_2 n \rceil (2-1) = n \lceil \log_2 n \rceil$.

When $n = \prod_i \mu_i$, given any $(v^{(\alpha,1)}, \ldots, v^{(\alpha,t)}) \in \mathcal{E}(\mu_1) \times \cdots \times \mathcal{E}(\mu_t)$, the truncated tensor product will always be an elementary vector. However, when $n < \prod_i \mu_i$, there exists $(v^{(\alpha,1)}, \ldots, v^{(\alpha,t)}) \in \mathcal{E}(\mu_1) \times \cdots \times \mathcal{E}(\mu_t)$ such that the truncated tensor product becomes a zero vector. The proof of Theorem 2 has implicitly shown that it is impossible to have a solution v (of the system consisting of instance-dependent and instance-independent equations) which contains $v^{(\alpha)}$ such that the truncated tensor product is a zero vector. Each solution v will lead to $\mathtt{wt}(e^{(\alpha)}) = 1$ for all α.

As a concrete example, the NIST-I parameter set in [6, Table 5] has $n = 64$. As the result, $d = t = \lceil \log_2 64 \rceil = 6$, and $|\mathtt{wit}| = n \lceil \log_2 n \rceil = 6n$. In this case, $n = \prod_i \mu_i$, so there is no need to truncate tensor products (we have $M = I_n$). However, the NIST-V parameter set has $n = 109$, in which case truncation is required.

Remark 2. [6] does not use Problem 4 to explain its modeling. We use Problem 4 to explain the modeling because this allows us to consider an instance of PKP as an instance of RSD, which make it easier to present our main ideas in the remainder of the paper.

5 A Family of Representations of Elementary Vectors

The ways elementary vectors are represented in Section 3 and Section 4 can be considered as special cases of a family of representations. Let ℓ, δ, μ be positive integers satisfying $\ell \leq \binom{\mu}{\delta}$. In this family of modelings, an elementary vector $u \in \mathcal{E}(\ell)$ is represented by vectors $v \in \mathcal{E}_\delta(\mu)$ such that

$$u = M \cdot \mathtt{prod}_\delta(v), \tag{4}$$

where $M \in \mathbb{F}_2^{\ell \times \binom{\mu}{\delta}}$ is chosen under the constraints

- $\mathtt{wt}(M[i]) \in \{0, 1\}$ for all i, and

– M has no zero rows (or equivalently, the rank of M is ℓ).

Each entry u_i is thus

$$\sum_{M[i,j]=1} (\mathtt{prod}_\delta(v))_j.$$

In this way, any $u \in \mathcal{E}(\ell)$ can be represented by one or more vectors $v \in \mathcal{E}_\delta(\mu)$ such that $u = M \cdot \mathtt{prod}_\delta(v)$. A vector $v \in \mathcal{E}_\delta(\mu)$, however, might lead to $0 = M \cdot \mathtt{prod}_\delta(v)$. If necessary, v can be partitioned into t vectors $v^{(1)} \in \mathcal{E}(\mu_1), \ldots, v^{(t)} \in \mathcal{E}(\mu_t)$.

The matrix M indicates the set of vectors $v \in \mathcal{E}_\delta(\mu)$ such that $M \cdot \mathtt{prod}_\delta(v) = u \in \mathcal{E}(\ell)$: Let i be the integer such that $u_i = 1$; The set can be written as

$$\mathcal{V}_i = \Big\{ v \in \mathcal{E}_\delta(\mu) \mid (\mathtt{prod}_\delta(v))_j = 1, M[i,j] = 1 \}.$$

The matrix M also indicates the set of vector $v \in \mathcal{E}_\delta(\mu)$ such that $0 = M \cdot \mathtt{prod}_\delta(v)$, which can be written as

$$\Big\{ v \in \mathcal{E}_\delta(\mu) \mid (\mathtt{prod}_\delta(v))_j = 1, \mathtt{wt}(M[j]) = 0 \Big\}.$$

Following the discussion in Section 3, to model RSD, for each α we need a set of instance-independent equations such that the solution space is $\bigcup_i \mathcal{V}_i$. This can be translated into two constraints on v:

– $\mathtt{wt}(v) = \delta$ and
– $\mathtt{wt}(M \cdot \mathtt{prod}_\delta(v)) = 1$.

We call the two constraints the *default constraint* and the *additional constraint*, respectively. Note that the additional constraint is only meaningful when there is at least one zero column in M. If there are no zero columns, the default constraint implies the additional constraint.

To model PKP using problem 4, it is fine if the solution space contains weight-δ vectors v's such that $\mathtt{wt}(M \cdot \mathtt{prod}_\delta(v)) = 0$, for reasons discussed in Section 4. The important thing is that the solution space is a superset of $\bigcup_i \mathcal{V}_i$ and a subset of $\mathcal{E}_\delta(\mu)$. Therefore, each of the following three cases will lead to a valid modeling.

– Adopting both constraints, under which the solution space is $\bigcup_i \mathcal{V}_i$.
– Adopting only the default constraint, under which the solution space is $\mathcal{E}_\delta(\mu)$.
– Something in between.

The three cases can lead to modelings that differ in $|\mathtt{wit}|$ and d. In the remainder of this section, we always choose the first case.

Similar to that in Section 3, a variable ν_j is introduced for each entry v_j of v. If necessary, ν can be partitioned into t vectors $\nu^{(1)} \in \mathcal{E}(\mu_1), \ldots, \nu^{(t)} \in \mathcal{E}(\mu_t)$. The default constraint $\mathtt{wt}(v) = \delta$ can be ensured by all polynomial equations of the form

$$\nu_{j_1} \cdots \nu_{j_{\delta+1}} = 0,\ j_1 < \cdots < j_{\delta+1}, \tag{5}$$

along with

$$\sum_{j_1<\cdots<j_\delta} \nu_{j_1} \cdots \nu_{j_\delta} = 1.$$

The additional constraint, under the default constraint, can be expressed as

$$\mathtt{wt}(M[j]) = 0 \implies (\mathtt{prod}_\delta(v))_j = 0,$$

which turns out to be equivalent to

$$\sum_{\mathtt{wt}(M[j])=0} (\mathtt{prod}_\delta(v))_j = 0.$$

Therefore, the additional constraint can be ensured by adding the polynomial equation

$$\sum_{\mathtt{wt}(M[j])=0} (\mathtt{prod}_\delta(\nu))_j = 0.$$

The default constraint $\mathtt{wt}(v) = \delta$ implies that $\sum_i v_i = \delta$ (δ should be considered as an element in $\mathbb{F}_2$). Therefore, a simple optimization is to replace ν_μ by $\sum_{i=1}^{\mu-1} \nu_i + \delta$, which is equivalent to adding the equation $\sum_i \nu_i = \delta$.

The discussion above shows a generic way to design instance-independent equations when each elementary vector is represented in the way shown in Equation 4. The complete modeling for RSD/PKP has $d = \delta + 1$, as Equations 5 are of degree $\delta + 1$. Note that the instance-dependent equations are of degree only δ.

Interestingly, as we will show in the remainder of this section, by choosing M and $\mathtt{prod}_\delta(\cdot)$ in a clever way, it is possible to reduce the degree d to δ. This can be achieved if the default and additional constraints together can be represented as a set of polynomial equations of degree at most δ. A good choice of $(M, \mathtt{prod}_\delta(\cdot))$ can also lead to linear equations other than $\sum_i \nu_i = \delta$, allowing further reduction in the number of variables.

Finally, we show that the representations of Section 3 and Section 4 fall into the family of representations. For both sections, v is considered as the result of concatenating t vectors $v^{(1)} \in \mathcal{E}(\mu_1)$, $\ldots$, $v^{(t)} \in \mathcal{E}(\mu_t)$, and δ is set to t. For the representation of Section 3, M and $\mathtt{prod}_\delta(\cdot)$ are chosen such that

$$\mathtt{wt}(M[j]) = 1 \iff \exists (j_1, \ldots, j_t) \in [\mu_1] \times \cdots \times [\mu_t] \text{ such that } (\mathtt{prod}_\delta(\nu))_j = \nu_{j_1}^{(1)} \nu_{j_2}^{(2)} \cdots \nu_{j_t}^{(t)},$$

so M has exactly $n/w = \prod_i \mu_i$ non-zero columns. For the representation of Section 4, M and $\mathtt{prod}_\delta(\cdot)$ are chosen such that

$$\mathtt{wt}(M[j]) = 1 \implies \exists (j_1, \ldots, j_t) \in [\mu_1] \times \cdots \times [\mu_t] \text{ such that } (\mathtt{prod}_\delta(\nu))_j = \nu_{j_1}^{(1)} \nu_{j_2}^{(2)} \cdots \nu_{j_t}^{(t)},$$

and M has exactly $n \leq \prod_i \mu_i$ non-zero columns.

Remark 3. To be more precise, we briefly discuss how the complete modeling for RSD looks like. Let $\epsilon^{(\alpha)} \coloneqq M \cdot \mathtt{prod}_\delta(\nu^{(\alpha)})$, where $\nu^{(\alpha)}$ is a length-μ vector of variables. Let $\epsilon \coloneqq \epsilon^{(1)} \| \cdots \| \epsilon^{(w)}$. Then the instance-dependent equations can be written as Equations 1. For each α there will be a set of instance-independent equations, of which the solution space is $\bigcup_i \mathcal{V}_i$.

Remark 4. The complete modeling for PKP also includes a set of instance-independent equations for each α, of which the solution space is $\bigcup_i \mathcal{V}_i$. Following the previous remark, there will be another $m \log_2 q + n$ equations, which come from Equation 2. From the point of view of RSD, these $m \log_2 q + n$ equations are all instance-dependent equations. However, from the point of view of PKP, it can be seen that only the first $m \log_2 q$ equations depend on the PKP instance, while the last n equations (which come from Equations 3) are independent of the PKP instance.

5.1 A New Modeling for `SDitH2-L1-gf2`

Let $t = 2$, $\mu_1 = \mu_2 = 6$ (so $\mu = \mu_1 + \mu_2 = 12$), and $\delta = 4$. In this modeling, each $e^{(\alpha)} \in \mathcal{E}(n/w)$ is represented by one or more vectors $v^{(\alpha)} \in \mathcal{E}_\delta(\mu)$ such that $\mathtt{wt}(v^{(\alpha,1)}) = \mathtt{wt}(v^{(\alpha,2)}) = 2$, and any vector $v^{(\alpha)} \in \mathcal{E}_\delta(\mu)$ such that $\mathtt{wt}(v^{(\alpha,1)}) = \mathtt{wt}(v^{(\alpha,2)}) = 2$ represents a unique element in $\mathcal{E}(n/w)$. To achieve this, M and $\mathtt{prod}_\delta(\cdot)$ are chosen such that

$$\mathtt{wt}(M[j]) = 1 \iff (\mathtt{prod}_\delta(\nu^{(\alpha)}))_j \in \mathcal{T},$$

$$\mathcal{T} = \left\{ \nu_{j_1}^{(\alpha,1)} \nu_{j_1'}^{(\alpha,1)} \nu_{j_2}^{(\alpha,2)} \nu_{j_2'}^{(\alpha,2)} \mid 1 \le j_1 < j_1' \le \mu_1, 1 \le j_2 < j_2' \le \mu_2 \right\}.$$

As a sanity check, $|\mathcal{T}| = \binom{6}{2}^2 = 225 > 185 = n/w$, so it is possible to choose such an M. Now it remains to show a set of instance-indenpendent polynomial equations w.r.t. any specific α, such that its solution space is

$$\mathcal{P}^{(\alpha)} = \left\{ v^{(\alpha)} \in \mathcal{E}_\delta(\mu) \mid \mathtt{wt}(v^{(\alpha,1)}) = \mathtt{wt}(v^{(\alpha,2)}) = 2 \right\}.$$

We propose to include all polynomial equations of the form

$$\nu_{j_1}^{(\alpha,i)} \cdot \nu_{j_2}^{(\alpha,i)} \cdot \nu_{j_3}^{(\alpha,i)} = 0, \ 1 \le j_1 < j_2 < j_3 \le \mu_i, \ i \in \{1, 2\} \tag{6}$$

along with two equations

$$\sum_{j_1 < j_2} \nu_{j_1}^{(\alpha,i)} \cdot \nu_{j_2}^{(\alpha,i)} = 1, \ i = 1, 2. \tag{7}$$

The first type of equations ensures that $\mathtt{wt}(v^{(\alpha,i)}) < 3$. The second type of equations then ensures that $\mathtt{wt}(v^{(\alpha,i)}) = 2$. In conclusion, the solution space of the polynomial system consisting of Equations 6 and 7 is exactly $\mathcal{P}^{(\alpha)}$.

The instance-indenpendent equations above for $\alpha = 1, \ldots, w$ are of degrees at most 3. Since the instance-dependent equations have degree $\delta = 4$, we have

$d = \delta = 4$. In order to reduce the number of variables, each $\nu_{\mu_i}^{(\alpha,i)}$ is replaced by $\sum_{j=1}^{\mu_i - 1} \nu_{\mu_i}^{(\alpha,i)}$, which is allowed because $\sum_j v_j^{(\alpha,i)} = 2 = 0 \in \mathbb{F}_2$. In this way, the witness size can be reduced to $(6 + 6 - 2)w = 10w < 11w$, which leads to reduction in signature size.

5.2 Another New Modeling for `SDitH2-L1-gf2`

Now let $t = 2$, $\mu_1 = \mu_2 = 5$ (so $\mu = \mu_1 + \mu_2 = 10$), and $\delta = 4$. In this modeling, each $e^{(\alpha)} \in \mathcal{E}(n/w)$ is represented by one or more vectors $v^{(\alpha)} \in \mathcal{E}_\delta(\mu)$ such that $(\mathtt{wt}(v^{(\alpha,1)}), \mathtt{wt}(v^{(\alpha,2)})) \in \{(1,3),(2,2),(3,1)\}$, and any vector $v^{(\alpha)} \in \mathcal{E}_\delta(\mu)$ such that $(\mathtt{wt}(v^{(\alpha,1)}), \mathtt{wt}(v^{(\alpha,2)})) \in \{(1,3),(2,2),(3,1)\}$ represents a unique vector in $\mathcal{E}(n/w)$. To achieve this, M and $\mathtt{prod}_\delta(\cdot)$ are chosen such that

$$\mathtt{wt}(M[j]) = 1 \iff (\mathtt{prod}_\delta(\nu^{(\alpha)}))_j \in \mathcal{T},$$

$$\begin{aligned}\mathcal{T} = &\left\{\nu_{j_1}^{(\alpha,1)}\nu_{j_1'}^{(\alpha,1)}\nu_{j_2}^{(\alpha,2)}\nu_{j_2'}^{(\alpha,2)} \mid 1 \le j_1 < j_1' \le \mu_1, 1 \le j_2 < j_2' \le \mu_2\right\} \cup \\ &\left\{\nu_{j_1}^{(\alpha,1)}\nu_{j_1'}^{(\alpha,1)}\nu_{j_1''}^{(\alpha,1)}\nu_{j_2}^{(\alpha,2)} \mid 1 \le j_1 < j_1' < j_1'' \le \mu_1, 1 \le j_2 \le \mu_2\right\} \cup \\ &\left\{\nu_{j_1}^{(\alpha,1)}\nu_{j_2}^{(\alpha,2)}\nu_{j_2'}^{(\alpha,2)}\nu_{j_2''}^{(\alpha,2)} \mid 1 \le j_1 \le \mu_1, 1 \le j_2 < j_2' < j_2'' \le \mu_2\right\}.\end{aligned}$$

As a sanity check, $|\mathcal{T}| = \binom{5}{2}^2 + 2 \cdot \binom{5}{3}\binom{5}{1} = 200 > 185 = n/w$, so it is possible to choose such an M. Now it remains to show a set of instance-indenpendent polynomial equations w.r.t. any specific α, such that the solution space is

$$\mathcal{P}^{(\alpha)} = \left\{v^{(\alpha)} \in \mathcal{E}_\delta(\mu) \mid (\mathtt{wt}(v^{(1)}), \mathtt{wt}(v^{(2)})) \in \{(1,3),(2,2),(3,1)\}\right\}.$$

We propose to first include all polynomial equations of the form

$$\nu_{j_1}^{(\alpha,i)} \cdot \nu_{j_2}^{(\alpha,i)} \cdot \nu_{j_3}^{(\alpha,i)} \cdot \nu_{j_4}^{(\alpha,i)} = 0,\ 1 \le j_1 < j_2 < j_3 < j_4 \le \mu_i,\ i \in \{1,2\}, \tag{8}$$

equations

$$\sum_{j_1<j_2<j_3} (\nu_{j_1}^{(\alpha,i)} \cdot \nu_{j_2}^{(\alpha,i)} \cdot \nu_{j_3}^{(\alpha,i)}) + \sum_{j_1<j_2} (\nu_{j_1}^{(\alpha,i)} \cdot \nu_{j_2}^{(\alpha,i)}) + \sum_j \nu_j^{(\alpha,i)} = 1,\ i = 1,2, \tag{9}$$

equation

$$\sum_j \nu_j^{(\alpha,1)} + \sum_j \nu_j^{(\alpha,2)} = \delta = 0, \tag{10}$$

and equation

$$\sum_{i \ne i', j_1 < j_2} ((\nu_{j_1}^{(\alpha,i)} \cdot \nu_{j_2}^{(\alpha,i)}) \cdot \nu_{j_3}^{(\alpha,i')}) = \sum_j \nu_j^{(1)}. \tag{11}$$

Equations 8 ensure that $\mathtt{wt}(v^{(\alpha,i)}) < 4$ for each i. Equations 9 ensure that $\mathtt{wt}(v^{(\alpha,i)}) \in \{1,2,3\}$ for each i. Equation 10 then ensures that

$$\{\mathtt{wt}(v^{(\alpha,1)}), \mathtt{wt}(v^{(\alpha,2)})\} \in \left\{\{1,1\},\{1,3\},\{2,2\},\{3,3\}\right\}.$$

It might be hard to see the effect of Equations 11. It turns out that whether the left-hand side is equal to the right-hand side depends on what $\{\mathtt{wt}(v^{(\alpha,1)}), \mathtt{wt}(v^{(\alpha,2)})\}$ is, as summarized in the following table.

$\{\mathtt{wt}(v^{(\alpha,1)}), \mathtt{wt}(v^{(\alpha,2)})\}$	LHS	RHS
{1,1}	0	1
{1,3}	1	1
{2,2}	0	0
{3,3}	0	1

Therefore, Equation 11 further ensures that

$$\{\mathtt{wt}(v^{(\alpha,1)}), \mathtt{wt}(v^{(\alpha,2)})\} \in \big\{\{1,3\},\{2,2\}\big\}.$$

In conclusion, the solution space of the polynomial system consisting of Equations 8, 9, 10, 11 is exactly $\mathcal{P}^{(\alpha)}$.

The instance-indenpendent equations above for $\alpha = 1, \ldots, w$ are of degrees at most 4. Since the instance-dependent equations also have degree $\delta = 4$, we have $d = \delta = 4$. In order to reduce the number of variables, each $\nu_{\mu_2}^{(\alpha,2)}$ is replaced by $\sum_{j=1}^{\mu_1} \nu_j^{(\alpha,1)} + \sum_{j=1}^{\mu_2-1} \nu_j^{(\alpha,2)}$, which is allowed because of Equation 10. In this way, the witness size can be reduced to $(5+5-1)w = 9w < 11w$, which leads to even more reduction in signature size.

5.3 A New Modeling for the NIST-I Parameter Set of PKPith

Recall that in the parameter set, n is set to 64. Let $t = 2$, $(\mu_1, \mu_2) = (4, 5)$, and $\delta = 3$. In this modeling, each $e^{(\alpha)} \in \mathcal{E}(n)$ is represented by one or more vectors $v^{(\alpha)} \in \mathcal{E}_\delta(\mu)$ such that $\{\mathtt{wt}(v^{(\alpha,1)}), \mathtt{wt}(v^{(\alpha,2)})\} = \{1,2\}$, and any vector $v^{(\alpha)} \in \mathcal{E}_\delta(\mu)$ such that $\{\mathtt{wt}(v^{(\alpha,1)}), \mathtt{wt}(v^{(\alpha,2)})\} = \{1,2\}$ represents a unique element in $\mathcal{E}(n)$. To achieve this, M and $\mathtt{prod}_\delta(\cdot)$ are chosen such that

$$\mathtt{wt}(M[j]) = 1 \iff (\mathtt{prod}_\delta(\nu^{(\alpha)}))_j \in \mathcal{T},$$

$$\begin{aligned}\mathcal{T} = &\big\{\nu_{j_1}^{(\alpha,1)}\nu_{j_1'}^{(\alpha,1)}\nu_{j_2}^{(\alpha,2)} \mid 1 \le j_1 < j_1' \le \mu_1, 1 \le j_2 \le \mu_2\big\} \cup \\ &\big\{\nu_{j_1}^{(\alpha,1)}\nu_{j_2}^{(\alpha,2)}\nu_{j_2'}^{(\alpha,2)} \mid 1 \le j_1 \le \mu_1, 1 \le j_2 < j_2' \le \mu_2\big\}.\end{aligned}$$

As a sanity check, $|\mathcal{T}| = \binom{4}{1}\binom{5}{2} + \binom{4}{2}\binom{5}{1} = 70 > 64 = n$, so such a martix M exists. Now it remains to show a set of instance-independent polynomial equations w.r.t. any specific α, such that the solution space is

$$\mathcal{P}^{(\alpha)} = \Big\{v^{(\alpha)} \in \mathcal{E}_\delta(\mu) \mid \{\mathtt{wt}(v^{(\alpha,1)}), \mathtt{wt}(v^{(\alpha,2)})\} = \{1,2\}\Big\}.$$

We propose to include all equations of the form

$$\nu_{j_1}^{(\alpha,i)} \cdot \nu_{j_2}^{(\alpha,i)} \cdot \nu_{j_3}^{(\alpha,i)} = 0,\ 1 \le j_1 < j_2 < j_3 \le \mu_i,\ i \in \{1,2\}, \tag{12}$$

equations

$$\sum_{j_1<j_2} (\nu_{j_1}^{(\alpha,i)} \cdot \nu_{j_2}^{(\alpha,i)}) + \sum_j \nu_j^{(\alpha,i)} = 1,\ i = 1,2, \tag{13}$$

and equation

$$\sum_j \nu_j^{(\alpha,1)} + \sum_j \nu_j^{(\alpha,2)} = \delta = 1. \tag{14}$$

Equations 12 ensure that $\mathtt{wt}(v^{(\alpha,i)}) < 3$ for each α. Equations 13 ensure that $\mathtt{wt}(v^{(\alpha,i)}) \in \{1,2\}$ for each α. Equation 14 ensures that $\{\mathtt{wt}(v^{(\alpha,1)}), \mathtt{wt}(v^{(\alpha,2)})\} = \{1,2\}$. In conclusion, the solution space of the polynomial system consisting of Equations 12, 13, and 14 is exactly $\mathcal{P}^{(\alpha)}$.

Let $\mathcal{F}^{(\alpha)}$ be the set consisting of Equations 12, 13 and 14 for a specific α. As mentioned in Remark 4, equations in $\bigcup_\alpha \mathcal{F}^{(\alpha)}$ are not the only equations that are indenpendent of the PKP instance. There will be another n instance-indenpendent equations

$$1 = \sum_\alpha (M \cdot \mathtt{prod}_\delta(\nu^{(\alpha)}))_j,\ j = 1, \ldots, n,$$

which come from Equations 3. The polynomial system consisting of all instance-independent equations has a solution space

$$\Big\{ v^{(1)} \parallel \cdots \parallel v^{(n)} \ \mid v^{(\alpha)} \in \mathcal{P}^{(\alpha)}\ \forall \alpha, \\ \alpha \neq \alpha' \implies M \cdot \mathtt{prod}_\delta(v^{(\alpha)}) \neq M \cdot \mathtt{prod}_\delta(v^{(\alpha')}) \Big\}.$$

The instance-indenpendent equations above are of degrees at most 3. Since the instance-dependent equations also have degree $\delta = 3$, degree d is reduced from 6 to 3. In order to reduce the number of variables, each $\nu_{\mu_2}^{(\alpha,2)}$ is replaced by $\sum_{j=1}^{\mu_1} \nu_j^{(\alpha,1)} + \sum_{j=1}^{\mu_2-1} \nu_j^{(\alpha,2)} + 1$, which is allowed because of Equation 14. In this way, the witness size becomes $(4+5-1)n = 8n > 6n$.

Even though d is reduced from 6 to 3, as $|\mathtt{wit}|$ increases from $6n$ to $8n$, it is not obvious whether the signature size can be reduced. Recall that the formula for signature size is of the form $X \cdot |\mathtt{wit}| + Y \cdot d + Z$. It turns out $X \cdot 6n < Y \cdot 6$ for the parameter set, which leads to

$$(X \cdot 8n) + (Y \cdot 3) + Z < (X \cdot 6n) + (Y \cdot 6) + Z.$$

The exact values of X,Y, and Z can be derived from numbers shown in the next section.

6 Comparisons of Signature Size

Table 1 summarizes signature size (in bytes) of `SDitH2-L1-gf2`, `SDitH2-L3-gf2` and `SDitH2-L5-gf2` when different modelings are used. The numbers of bytes

are derived using the formula for the number of bits

$$\begin{aligned}
&3\lambda \\
&+ (\tau - 1) \cdot \big(|\texttt{wit}|_2 + (d-1)\lambda + (\lambda + B)\big) \\
&+ (\lambda + B) \\
&+ |\texttt{wit}|_2 \\
&+ d \cdot \lambda \\
&+ \lambda \cdot T_{\text{open}} + \tau \cdot (2\lambda) + 32,
\end{aligned}$$

which can be found in [8, page 37]. In the formula, $|\texttt{wit}|_2$ is defined as

$$8 \cdot \lceil |\texttt{wit}|/8 \rceil = 8 \cdot \lceil (w \cdot \sum_i (\mu_i - 1))/8 \rceil.$$

In Table 1, $|\sigma|$ is the signature size when the modeling of SDith is used. SDith always sets $d = 4$ regardless of the parameter set, and $(\mu_1, \ldots, \mu_4)$ is set to $(4, 4, 4, 3)$, $(4, 4, 4, 4)$, and $(4, 4, 4, 3)$ for `SDitH2-L1-gf2`, `SDitH2-L3-gf2`, and `SDitH2-L5-gf2`, respectively. For `SDitH2-L1-gf2` and `SDitH2-L5-gf2`, $|\sigma'|$ is the signature when the modeling in Section 5.1 is used, while $|\sigma''|$ is the signature size when the modeling in Section 5.2 is used. Similar modelings are also used for `SDitH2-L3-gf2`: The modeling used for $|\sigma'|$ is essentially the same as the one in Section 5.1 except that (μ_1, μ_2) is set to $(6, 7)$, while the modeling used for $|\sigma''|$ is essentially the same as the one in Section 5.2 except that (μ_1, μ_2) is set to $(5, 6)$.

parameter set	n/w	w	λ	τ	T_{open}	B	$\lvert\sigma\rvert$	$\lvert\sigma'\rvert$	$\lvert\sigma''\rvert$
`SDitH2-L1-gf2-short`	185	56	128	11	107	16	3 705	3 628	3 551
`SDitH2-L1-gf2-fast`				16	101	16	4 484	4 372	4 260
`SDitH2-L3-gf2-short`	252	73	192	16	157	16	7 964	7 820	7 676
`SDitH2-L3-gf2-fast`				24	153	16	9 916	9 700	9 484
`SDitH2-L5-gf2-short`	191	104	256	21	216	16	14 121	13 848	13 575
`SDitH2-L5-gf2-fast`				32	207	16	17 540	17 124	16 708

Table 1. Signature size in bytes of parameter sets of SDith under different modelings.

Table 2 summarizes signature size (in bytes) of the parameter sets in [6, Table 5], when different modelings are used. The numbers of bytes are derived using the formula for the number of bits

$$\begin{aligned}
4\lambda + (\tau - 1) \cdot \big(|\texttt{wit}| + (d-1) \cdot \kappa\tau + (\kappa\tau + B)\big) + (\kappa\tau + B) \\
+ |\texttt{wit}| + d \cdot \kappa\tau + \lambda \cdot T_{\text{open}} + \tau \cdot 2\lambda,
\end{aligned}$$

which can be found in [6, page 18]. $|\sigma|$ is the signature size when modeling of PKPith (described in Section 4) is used. For NIST-I, $|\sigma'|$ is the signature size

when the modeling in Section 5.3 is used. For NIST-V, the modeling used for $|\sigma'|$ is essentially the same as the one in Section 5.3 except that (μ_1, μ_2) is set to $(5, 6)$.

parameter set	n	λ	τ	κ	T_{open}	B	$\lvert\sigma\rvert$	$\lvert\sigma'\rvert$
`NIST-I`	64	128	11	11	100	16	3 580	3 257
`NIST-V`	109	256	23	11	214	16	15 811	13 842

Table 2. Signature size in bytes of parameter sets (shown in [6, Table 5]) of PKPith under different modelings.

References

1. Aaraj, N., Bettaieb, S., Bidoux, L., Budroni, A., Dyseryn, V., Esser, A., Feneuil, T., Gaborit, P., Kulkarni, M., Mateu, V., Palumbi, M., Perin, L., Rivain, M., Tillich, J.P., Xagawa, K.: Perk (2025), https://pqc-perk.org/assets/downloads/perk-v2.0.pdf
2. Adj, G., Aragon, N., Barbero, S., Bardet, M., Bellini, E., Bidoux, L., Chi-Domínguez, J.J., Dyseryn, V., Esser, A., Feneuil, T., Gaborit, P., Neveu, R., Rivain, M., Rivera-Zamarripa, L., Sanna, C., Tillich, J.P., Verbel, J., Zweydinger, F.: Mirath signature scheme (2025), https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/mirath-spec-round2-web.pdf
3. Aragon, N., Bardet, M., Bidoux, L., Chi-Domínguez, J.J., Dyseryn, V., Feneuil, T., Gaborit, P., Joux, A., Neveu, R., Rivain, M., Tillich, J.P., Vinçotte, A.: RYDE signature scheme (2025), https://pqc-ryde.org/assets/downloads/ryde_specification_v2.0.1.pdf
4. Baum, C., Braun, L., de Saint Guilhem, C.D., Klooß, M., Orsini, E., Roy, L., Scholl, P.: Publicly verifiable zero-knowledge and post-quantum signatures from VOLE-in-the-head. In: Annual international cryptology conference. pp. 581–615. Springer (2023)
5. Benadjila, R., Bouillaguet, C., Feneuil, T., Rivain, M.: MQOM: MQ on my mind (2025), https://mqom.org/docs/mqom-v2.0.pdf
6. Bettaieb, S., amd Philippe Gaborit, L.B., Kulkarni, M.: Modelings for generic PoK and applications: Shorter SD and PKP based signatures (2024), https://eprint.iacr.org/2024/1668.pdf
7. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Conference on the theory and application of cryptographic techniques. pp. 186–194. Springer (1986)
8. Melchor, C.A., Bidoux, S.B.L., Feneuil, T., Gaborit, P., Gama, N., Gueron, S., Howe, J., Hülsing, A., Joseph, D., Joux, A., Kulkarni, M., Persichetti, E., Randrianarisoa, T.H., Yue, M.R.D.: The syndrome decoding in the head (SD-in-the-head) signature scheme (2025), https://sdith.org/docs/sdith-v2.0.pdf
9. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM **21**(2), 120–126 (1978)