Quasi-Cyclic Stern Proof of Knowledge

Loïc Bidoux, Philippe Gaborit, Mukul Kulkarni, Nicolas Sendrier

Quasi-Cyclic Stern Proof of Knowledge

Loïc Bidoux
Technology Innovation Institute
UAE
loic.bidoux@tii.ae

Philippe Gaborit
University of Limoges
France
gaborit@unilim.fr

Mukul Kulkarni
Technology Innovation Institute
UAE
mukul.kulkarni@tii.ae

Nicolas Sendrier
Inria
Paris, France
nicolas.sendrier@inria.fr

***Abstract*—The ongoing NIST standardization process has shown that Proof of Knowledge (PoK) based signatures have become an important type of possible post-quantum signatures. Regarding code-based cryptography, the main original approach for PoK based signatures is the Stern protocol which allows to prove the knowledge of a small weight vector solving a given instance of the Syndrome Decoding (SD) problem over $\mathbb{F}_2$. It features a soundness error equal to $2/3$. This protocol was improved a few years later by Véron who proposed a variation of the scheme based on the General Syndrome Decoding (GSD) problem which leads to better results in terms of communication. A few years later, the AGS protocol introduced a variation of the Véron protocol based on Quasi-Cyclic (QC) matrices. The AGS protocol permits to obtain an asymptotic soundness error of $1/2$ and an improvement in terms of communications.**

In the present paper, we introduce the Quasi-Cyclic Stern PoK which constitutes an adaptation of the AGS scheme in a SD context, as well as several new optimizations for code-based PoK. Our main optimization on the size of the signature cannot be applied to GSD based protocols such as AGS and therefore motivated the design of our new protocol. In addition, we also provide a special soundness proof that is compatible with the use of the Fiat-Shamir transform for 5-round protocols. This approach is valid for our protocol but also for the AGS protocol which was lacking such a proof. We compare our results with existing signatures including the recent code-based signatures based on PoK leveraging the MPC in the head paradigm. In practice, our new protocol is as fast as AGS while reducing its associated signature length by 20%. As a consequence, it constitutes an interesting trade-off between signature length and execution time for the design of a code-based signature relying only on the difficulty of the SD problem.

***Index Terms*—Code-based Signature, PoK, Stern Protocol**

I. Introduction

Since its introduction in 1978 by McEliece [34], code-based cryptography has been one of the main alternatives to classical cryptography. This is illustrated by the ongoing NIST Post-Quantum Cryptography standardization process whose round 3 features three code-based Key Encapsulation Mechanisms (KEM) [3], [4], [6]. Additional KEM [2], [5], [9] were also considered during the round 2 of the competition. Although there exists satisfactory code-based KEM, designing signatures from coding theory has historically been challenging. Two approaches have been used in the literature namely signatures from the hash-and-sign paradigm and signatures based on identification. In the first category, a construction was proposed in 2001 [21] although it is rather inefficient. The recent Wave construction [23] provides an efficient solution following the same paradigm and features small signature sizes. In the second category, two constructions have been proposed in the past few years namely LESS [10] and Durandal [7]. Hereafter, we focus on signatures constructed from the Fiat-Shamir paradigm [22], [26], [35] along with Zero-Knowledge Proofs of Knowledge (ZK PoK) for the Syndrome Decoding (SD) problem.

The first PoK for the SD problem was introduced by Stern in 1993 [38]. In 1997, Véron showed that using the general decoding problem (GSD), one can design a protocol that is more efficient than the initial Stern proposal [42]. The SD and GSD problems are equivalent and differ only in the way used to represent the underlying code namely using a parity-check matrix in the former and using a generator matrix in the latter. Both protocols require 3 rounds to be executed and feature a soundness error equal to 2/3. In 2011, the CVE [17] and AGS [1] PoK respectively improved the Stern and Véron protocols by lowering their soundness error to 1/2 (asymptotically close to 1/2 for AGS) using 5 rounds of execution. The CVE protocol is based on the SD problem over $\mathbb{F}_q$ while the AGS protocol relies on the QCGSD problem namely the GSD problem instantiated with a Quasi-Cyclic (QC) matrix. An issue with respect to the zero-knowledge property of GSD based protocols (Véron and AGS) has been identified in [31] and has been fixed in [13]. Some of these protocols have also been adapted in the rank metric setting, see [12], [19], [27] for instance. Recently, several proposals have used the MPC in the head paradigm in order to achieve a negligible soundness error of $1/N$ for some parameter N. The GPS [28] construction achieves such a small soundness error by relying on the SD problem over $\mathbb{F}_q$ while the FJR [25] and BGKM [15] proposals rely on the SD problem over $\mathbb{F}_2$. However, these constructions induce a performance overhead with respect to previous approaches.

Thanks to these new results, the research problem associated to these protocols has shifted from minimizing the signature size to finding the best trade-off between expected performances and signature size. Amongst existing constructions, AGS features the smallest expected performance cost while FJR is the best approach to get small signature sizes. In this paper, we propose a new PoK that has the same cost as AGS while featuring a signature size that is 20% smaller. As such, our new protocol provides a new interesting trade-off for the design of signatures based on PoK for the SD problem.

Contributions. We introduce the Quasi-Cyclic Stern protocol which is a new PoK for SD problem as well as several new optimizations for code-based PoK. Our main optimization on the size of the signature cannot be applied to GSD based protocols such as AGS which motivates the design of our new protocol. In addition, we also provide a special soundness proof that is compatible with the use of the Fiat-Shamir transform for 5-round protocols which was lacking in the AGS protocol. In practice, our new protocol is as fast as AGS while reducing its communication length by 20% therefore providing an interesting trade-off for the design of a code-based signature relying only on the difficulty of the SD problem.

II. Preliminaries

We denote by $w_H(\mathbf{x})$ the Hamming weight of $\mathbf{x}$ and by S_n the symmetric group of all permutations of n elements. If X is a finite set, then $x \xleftarrow{\$} X$ denotes that x is sampled uniformly at random from X and $x \xleftarrow{\$,\psi} X$ denotes that x is sampled uniformly at random from X using the seed ψ.

A. Coding Theory and Cryptography

Let n and k be positive integers such that $k < n$. A binary linear $\mathcal{C}$ code is a k-dimensional subspace of $\mathbb{F}_2^n$. $\mathcal{C}$ can be represented by a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$ such that $\mathcal{C} = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{H}\mathbf{x}^\top = 0\}$. A QC code of index 2 is a code whose parity-check matrix $\mathbf{H}$ is the concatenation of two $k \times k$ circulant matrices which is denoted by $\mathbf{H} \in \mathcal{QC}(\mathbb{F}_2^{k\times 2k})$. Given $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$ (respectively $\mathbf{H} \in \mathcal{QC}(\mathbb{F}_2^{k\times 2k})$) and a syndrome $\mathbf{y}^\top = \mathbf{H}\mathbf{x}^\top$ of a vector of small weight $w_H(\mathbf{x}) = \omega$, the SD (respectively QCSD) problem asks to find $\mathbf{x}$.

B. Proof of Knowledge and Commitment Schemes

A commitment scheme $\mathsf{COM} = (\mathsf{Commit}, \mathsf{Open})$ allows a sender to produce a commitment c to a message m of their choice. COM is said to be *hiding* if c does not reveal any information about m. The sender can convince any receiver that m is the underlying message used to generate c using the Open algorithm. The *binding* property of COM guarantees that a cheating sender cannot produce a valid opening for any message except m after sending c to the receiver. In this paper, we instantiate the commitment scheme using collapse-binding hash functions (quantum-secure analogue of collision-resistant hash functions, see [24], [39]–[41] for formal definition and further details) with appropriate salt values and the opening information simply reveals the salt.

An interactive proof system is a protocol between two parties (P and V) used to establish the validity of some statement x by proving the existence of a witness w such that $R(x, w) = 1$ for some public relation R. A PoK system additionally proves that P actually *knows* a valid witness w (as opposed to its existence earlier). A PoK system is (1) *complete* if a proof corresponding to a valid statement ($x \in L$) is always accepted by the honest verifier, (2) *sound* if a malicious prover cannot prove a false statement, (3) *special sound* if repeated interactions with a malicious prover (with a fixed false statement) allow for efficient recovery of a valid witness, and (4) *zero-knowledge* (ZK) if V does not learn any information about the witness w after interacting with P.

III. Quasi-Cyclic Stern Proof of Knowledge

Our new PoK is based on the Stern protocol along with quasi-cyclicity and shares similarities with AGS [1]. It seems plausible that Véron based protocols such as AGS would inherently be more efficient than Stern based ones, however this work contradicts such intuition. We introduce the non optimized QC Stern protocol in Section III-A. Then, we recall some optimizations from the literature and present new ones in Section III-B. Finally, we describe the optimized QC Stern protocol and discuss its security in Section III-C.

A. Quasi-Cyclic Stern Protocol

Our new protocol (see Figure 1) is a ZK PoK for the Quasi-Cyclic Syndrome Decoding (QCSD) problem. Given inputs $(\mathbf{H}, \mathbf{y}) \xleftarrow{\$} \mathcal{QC}(\mathbb{F}_2^{k\times 2k}) \times \mathbb{F}_2^k$, it allows a prover to convince a verifier that he knows $\mathbf{x} \in \mathbb{F}_2^{2k}$ such that $\mathbf{H}\mathbf{x}^\top = \mathbf{y}^\top$ and $w_H(\mathbf{x}) = w$ without revealing anything on the secret. Let $\mathbf{a} = (a_0, a_1, \cdots, a_{k-1}) \in \mathbb{F}_2^k$, we define the $\mathbf{rot}()$ operator as $\mathbf{rot}_r(\mathbf{a}) := (a_{k-r+1}, a_{k-r+2}, \cdots, a_{k-r})$. For $\mathbf{b} = (\mathbf{b}_1, \mathbf{b}_2) \in \mathbb{F}_2^{2k}$, we slightly abuse notations and define $\mathbf{rot}_r(\mathbf{b}) := (\mathbf{rot}_r(\mathbf{b}_1), \mathbf{rot}_r(\mathbf{b}_2))$. As we are considering QC matrices, one can see that $\mathbf{y}^\top = \mathbf{H}\mathbf{x}^\top \Leftrightarrow \mathbf{rot}_r(\mathbf{y})^\top = \mathbf{H}\,\mathbf{rot}_r(\mathbf{x})^\top$ hence one can prove the knowledge of the secret $\mathbf{x}$ associated to the public value $\mathbf{y}$ using any of k different equations arising from the k possible rotations. This property allows to introduce a new kind of challenge that permits to reduce the soundness error to $1/2$ asymptotically.

B. Existing Improvements and New Optimizations

Reducing the number of commitments [1]**.** We recall that code-based proofs of knowledge generally feature a soundness error of $2/3$ or $1/2$ therefore one needs to perform δ iterations of these protocols to get a negligible soundness error. Using Figure 1 as an illustrative example, the idea is to compress the commitments over all the iterations so that only two initial commitments $\text{CMT}_1 = (c_{1,1}||c_{1,2}||\cdots||c_{\delta,1}||c_{\delta,2})$ and $\text{CMT}_2 = (c_{1,3}||\cdots||c_{\delta,3})$ need to be sent. As the verifier is only able to reconstruct 2 out of 3 commitments himself, the prover must send him the missing commitment at the end of each iteration. Overall, this reduces the number of commitments to be sent from 3δ to $2 + \delta$.

Small weight vector compression [1]**.** The prover must reveal a permutation $\pi[\mathbf{z}]$ of a small weight vector $\mathbf{z}$ to answer some challenges. Leveraging the small weight of $\mathbf{z}$, one can compress $\pi[\mathbf{z}]$ before sending it thus reducing the cost of sending small weight vectors from n to approximately $n/2$.

Mitigation of an attack against 5-rounds protocols [13]**.** The attack against 5-rounds PoK from [32] is relevant for our construction. The key idea of this attack is to split the attacker's work in two steps by first trying to guess the first challenge for several repetitions and then guess the second challenge for the remaining repetitions. One has to increase

$\underline{\mathsf{Setup}(1^\lambda)\ \&\ \mathsf{Keygen}(\mathsf{param})}$

$\mathsf{param} = (k, w) \longleftarrow \mathsf{Setup}(1^\lambda)$

$\mathbf{x} \xleftarrow{\$} \mathbb{F}_2^{2k}$ such that $w_H(\mathbf{x}) = w$

$\mathbf{H} \xleftarrow{\$} \mathcal{QC}(\mathbb{F}_2^{k\times 2k}),\ \mathbf{y}^\top = \mathbf{H}\mathbf{x}^\top$

$(\mathsf{sk}, \mathsf{pk}) = (\mathbf{x}, (\mathbf{H}, \mathbf{y}))$

$\underline{\mathsf{P}_1(\mathsf{param}, \mathsf{sk}, \mathsf{pk})}$

$\pi \xleftarrow{\$} S_{2k},\ \mathbf{u} \xleftarrow{\$} \mathbb{F}_2^{2k}$

$c_1 = \mathsf{Commit}(\pi \,||\, \mathbf{H}\mathbf{u}^\top),\ c_2 = \mathsf{Commit}(\pi[\mathbf{u}])$

$\mathrm{CMT}_1 = (c_1, c_2)$

$\underline{\mathsf{V}_1(\mathsf{param}, \mathsf{pk}, \mathrm{CMT}_1)}$

$r \xleftarrow{\$} [0, k-1]$

$\mathrm{CH}_1 = r$

$\underline{\mathsf{P}_2(\mathsf{param}, \mathsf{sk}, \mathsf{pk}, \mathrm{CMT}_1, \mathrm{CH}_1)}$

$\mathbf{x}_r = \mathbf{rot}_r(\mathbf{x}),\ c_3 = \mathsf{Commit}(\pi[\mathbf{u} + \mathbf{x}_r])$

$\mathrm{CMT}_2 = c_3$

$\underline{\mathsf{V}_2(\mathsf{param}, \mathsf{pk}, \mathrm{CMT}_1, \mathrm{CH}_1, \mathrm{CMT}_2)}$

$\mathrm{CH}_2 \xleftarrow{\$} \{0, 1\}$

$\underline{\mathsf{P}_3(\mathsf{param}, \mathsf{sk}, \mathsf{pk}, \mathrm{CMT}_1, \mathrm{CH}_1, \mathrm{CMT}_2, \mathrm{CH}_2)}$

if $\mathrm{CH}_2 = 0$ **then**

  $\mathrm{RSP} = (\pi,\ \mathbf{u} + \mathbf{x}_r)$

if $\mathrm{CH}_2 = 1$ **then**

  $\mathrm{RSP} = (\pi[\mathbf{u}],\ \pi[\mathbf{x}_r])$

$\underline{\mathsf{V}_3(\mathsf{param}, \mathsf{pk}, \mathrm{CMT}_1, \mathrm{CH}_1, \mathrm{CMT}_2, \mathrm{CH}_2, \mathrm{RSP})}$

if $\mathrm{CH}_2 = 0$ **then**

  $\bar{c}_1 = \mathsf{Commit}(\pi \,||\, \mathbf{H}(\mathbf{u} + \mathbf{x}_r)^\top - \mathbf{rot}_r(\mathbf{y})^\top)$

  $\bar{c}_3 = \mathsf{Commit}(\pi[\mathbf{u} + \mathbf{x}_r])$

  if $c_1 \neq \bar{c}_1$ **or** $c_3 \neq \bar{c}_3$ **then**

    return reject

if $\mathrm{CH}_2 = 1$ **then**

  $\bar{c}_2 = \mathsf{Commit}(\pi[\mathbf{u}])$

  $\bar{c}_3 = \mathsf{Commit}(\pi[\mathbf{u}] + \pi[\mathbf{x}_r])$

  if $c_2 \neq \bar{c}_2$ **or** $c_3 \neq \bar{c}_3$ **or** $w_H(\pi[\mathbf{x}_r]) \neq w$ **then**

    return reject

return accept

Fig. 1: Quasi-Cyclic Stern Protocol (one iteration)

the number of iterations δ of the underlying PoK to ensure that the resulting signature remains secure, which increases its size. One way to mitigate this attack is to consider s instances of the SD problem within the keypair namely using $\mathsf{sk} = (\mathbf{x}^i)_{i\in[1,s]}$ and $\mathsf{pk} = (\mathbf{H}, (\mathbf{y}^i)^\top = \mathbf{H}(\mathbf{x}^i)^\top)_{i\in[1,s]}$. Doing so, the first challenge space size is increased from k to $s \times k$ which makes the attack less efficient so that δ would not need to be increased as much as initially expected. In practice, this introduces a trade-off between key size and signature size.

Additional vector compression from seeds. Starting from the initial Stern proposal, all constructions suggest to use seeds to reduce communication costs. Using Figure 1 for illustrative purposes, one can use a seed θ to compute π and then substitute π by θ in the prover's response. We now introduce an additional vector compression that is only applicable to SD based protocols. One can go one step further and use a seed ξ to generate a random value $\mathbf{v} \xleftarrow{\$,\xi} \mathbb{F}_2^n$ and then compute the value $\mathbf{u} = \pi^{-1}[\mathbf{v}]$. When the prover is required to send $\pi[\mathbf{u}]$, he now needs to send $\mathbf{v}$ which can be substituted by ξ. Instead of sending a vector of size n, the prover only sends a seed which greatly reduces the communication cost. We now explain why this optimization cannot be applied to the AGS protocol. Under the GSD representation, the prover needs to send $\pi[\mathbf{u}\mathbf{G}]$ rather than $\pi[\mathbf{u}]$ whenever $\mathrm{CH}_2 = 1$. But the quantity $\pi[\mathbf{u}\mathbf{G}]$ cannot be replaced by a seed generating it as $\mathbf{u}\mathbf{G}$ is a codeword hence the optimization can not be applied.

Seed and commitment compression. Using the previous optimization, one can see that the prover sends one seed during each iteration either θ from which π can be recomputed or ξ from which $\pi[\mathbf{u}]$ can be recomputed. Let us consider two consecutive iterations of the protocol, the prover will have to send one of the following tuple of seeds: $(\theta_1, \theta_2), (\theta_1, \xi_2), (\xi_1, \theta_2), (\xi_1, \xi_2)$. If master seeds θ (respectively ξ) are used to generate θ_1 and θ_2 (respectively ξ_1 and ξ_2), then the prover will have to send one of the following values: $\theta, (\theta_1, \xi_2), (\xi_1, \theta_2), \xi$. By using such a technique, one reduces the average communication cost associated to seeds by 25%. This optimization can be seen as a variation of the seed compression optimization from [33] in which the (unique) binary tree used is replaced by several binary trees of depth 1. Similarly, one can also group commitments using binary trees of depth 1 (from bottom to top contrarily to the previous case) which reduces the cost associated to commitments from $(2+\delta)\cdot|\mathsf{com}|$ to $(2+0.75\delta)\cdot|\mathsf{com}|$, where $|\mathsf{com}|$ denotes the size of a single commitment in bits. For further explanation and details about seed and commitment compression using binary trees please refer [15], [16], [33].

C. Optimized Quasi-Cyclic Stern Protocol

Figure 2 describes the optimized version of QC Stern protocol and includes the δ iterations required to reduce the soundness bellow $2^{-\lambda}$ where λ is the security parameter. As it is usually done, we do not include binary tree related optimizations nor small weight vector related optimizations as this simplifies the description of the protocol while not being related to its security. We discuss the soundness and zero-knowledge properties of our PoK giving only sketches of proof and defer the reader to the full version of the paper for additional details [16]. The soundness relies on a reduction from the QCSD problem to the DiffSD problem.

Definition 1 (DiffSD *problem):* Given positive integers ($n = 2k$), k, w, α, a parity-check matrix of a quasi-cyclic code $\mathbf{H} \xleftarrow{\$} \mathcal{QC}(\mathbb{F}_2^{k\times 2k})$ and $\mathbf{y} \in \mathbb{F}_2^k$ such that $\mathbf{H}\mathbf{x}^\top = \mathbf{y}^\top$ where $\mathbf{x} \in \mathbb{F}_2^{2k}$ and $w_H(\mathbf{x}) = w$. The Differential Syndrome Decoding problem $\mathsf{DiffSD}(n, k, w, \alpha)$ asks to find a set of

$\underline{\mathsf{Setup}(1^\lambda)\ \&\ \mathsf{Keygen}(\mathsf{param})}$

$\mathsf{param} = (k, w, \delta, s, |\mathsf{seed}|) \longleftarrow \mathsf{Setup}(1^\lambda)$

$\phi_1 \xleftarrow{\$} \{0,1\}^{|\mathsf{seed}|}, \phi_2 \xleftarrow{\$} \{0,1\}^{|\mathsf{seed}|}, \mathbf{H} \xleftarrow{\$,\phi_2} \mathcal{QC}(\mathbb{F}_2^{k\times 2k})$

for $i \in [1\,..\,s]$ **do** $\{\ \mathbf{x}^i \xleftarrow{\$,\phi_1} \mathbb{F}_2^{2k},\ (\mathbf{y}^i)^\top = \mathbf{H}(\mathbf{x}^i)^\top\ \}$

$(\mathsf{sk}, \mathsf{pk}) = (\phi_1, (\phi_2, \mathbf{y}^1, \cdots, \mathbf{y}^s))$

$\underline{\mathsf{P}_1(\mathsf{param}, \mathsf{sk}, \mathsf{pk})}$

for $i \in [1\,..\,\delta]$ **do**

$\theta_i \xleftarrow{\$} \{0,1\}^{|\mathsf{seed}|},\ \pi_i \xleftarrow{\$,\theta_i} S_{2k}$

$\xi_i \xleftarrow{\$} \{0,1\}^{|\mathsf{seed}|},\ \mathbf{v}_i \xleftarrow{\$,\xi_i} \mathbb{F}_2^{2k},\ \mathbf{u}_i = \pi^{-1}[\mathbf{v}_i]$

$c_{i,1} = \mathsf{Commit}(\pi_i \,||\, \mathbf{H}\mathbf{u}_i^\top),\ c_{i,2} = \mathsf{Commit}(\pi_i[\mathbf{u}_i])$

$\mathrm{CMT}_1 = \mathsf{Commit}(c_{1,1}||c_{1,2}||\cdots||c_{\delta,1}||c_{\delta,2})$

$\underline{\mathsf{V}_1(\mathsf{param}, \mathsf{pk}, \mathrm{CMT}_1)}$

for $i \in [1\,..\,\delta]$ **do** $\{\ s_i \xleftarrow{\$} [0, s-1],\ r_i \xleftarrow{\$} [0, k-1]\ \}$

$\mathrm{CH}_1 = ((s_1, r_1), \cdots, (s_\delta, r_\delta))$

$\underline{\mathsf{P}_2(\mathsf{param}, \mathsf{sk}, \mathsf{pk}, \mathrm{CMT}_1, \mathrm{CH}_1)}$

for $i \in [1\,..\,\delta]$ **do**

$\mathbf{x}_{r_i}^{s_i} = \mathbf{rot}_{r_i}(\mathbf{x}^{s_i}),\ c_{i,3} = \mathsf{Commit}(\pi_i[\mathbf{u}_i + \mathbf{x}_{r_i}^{s_i}])$

$\mathrm{CMT}_2 = \mathsf{Commit}(c_{1,3}||\cdots||c_{\delta,3})$

$\underline{\mathsf{V}_2(\mathsf{param}, \mathsf{pk}, \mathrm{CMT}_1, \mathrm{CH}_1, \mathrm{CMT}_2)}$

for $i \in [1\,..\,\delta]$ **do** $\{\ b_i \xleftarrow{\$} \{0,1\}\ \}$

$\mathrm{CH}_2 = (b_1, \cdots, b_\delta)$

$\underline{\mathsf{P}_3(\mathsf{param}, \mathsf{sk}, \mathsf{pk}, \mathrm{CMT}_1, \mathrm{CH}_1, \mathrm{CMT}_2, \mathrm{CH}_2)}$

for $i \in [1\,..\,\delta]$ **do**

if $b_i = 0$ **then** $d_i = \big(\theta_i,\ \mathbf{u}_i + \mathbf{x}_{r_i}^{s_i},\ c_{i,2}\big)$

if $b_i = 1$ **then** $d_i = \big(\xi_i,\ \pi_i[\mathbf{x}_{r_i}^{s_i}],\ c_{i,1}\big)$

$\mathrm{RSP} = (d_1, \cdots, d_\delta)$

$\underline{\mathsf{V}_3(\mathsf{param}, \mathsf{pk}, \mathrm{CMT}_1, \mathrm{CH}_1, \mathrm{CMT}_2, \mathrm{CH}_2, \mathrm{RSP})}$

for $i \in [1\,..\,\delta]$ **do**

if $b_i = 0$ **then**

$\pi_i \xleftarrow{\$,\theta_i} S_{2k},\ \bar{c}_{i,2} = c_{i,2}$

$\bar{c}_{i,1} = \mathsf{Commit}(\pi_i \,||\, \mathbf{H}(\mathbf{u}_i + \mathbf{x}_{r_i}^{s_i})^\top - \mathbf{rot}_{r_i}(\mathbf{y}^{s_i})^\top)$

$\bar{c}_{i,3} = \mathsf{Commit}(\pi_i[\mathbf{u}_i + \mathbf{x}_{r_i}^{s_i}])$

if $b_i = 1$ **then**

$\mathbf{v}_i \xleftarrow{\$,\xi_i} \mathbb{F}_2^{2k},\ \bar{c}_{i,1} = c_{i,1}$

$\bar{c}_{i,2} = \mathsf{Commit}(\mathbf{v}_i),\ \bar{c}_{i,3} = \mathsf{Commit}(\mathbf{v}_i + \pi_i[\mathbf{x}_{r_i}^{s_i}])$

if $w_H\big(\pi_i[\mathbf{x}_{r_i}^{s_i}]\big) \neq w$ **then return** reject

if $\mathsf{Open}(\mathrm{CMT}_1,\ \bar{c}_{1,1}||\bar{c}_{1,2}||\cdots||\bar{c}_{\delta,1}||\bar{c}_{\delta,2}) \neq 1$ **then**

return reject

if $\mathsf{Open}(\mathrm{CMT}_2,\ \bar{c}_{1,3}||\cdots||\bar{c}_{\delta,3}) \neq 1$ **then**

return reject

return accept

Fig. 2: Quasi-Cyclic Stern Protocol (with optimizations)

vectors $(\mathbf{c}, (\mathbf{z}_1, \cdots, \mathbf{z}_\alpha)) \in \mathbb{F}_2^k \times (\mathbb{F}_2^{2k})^\alpha$ such that for each $i \in [1, \alpha]$, $\mathbf{H}\mathbf{z}_i^\top + \mathbf{c} = \mathbf{rot}_i(\mathbf{y}^\top)$ with $w_H\big(\mathbf{z}_i\big) = w$.

*Theorem 1 (*QCSD ***to*** DiffSD ***reduction** [1], [36]):* If there exists a Probabilistic Polynomial-Time (PPT) algorithm solving the $\mathsf{DiffSD}(n, k, w, \alpha)$ problem with success probability p, then there exists a PPT algorithm solving the $\mathsf{QCSD}(n, k, w)$ problem with success probability $(1 - \frac{\binom{n}{w}^{\alpha-1}}{2^{(n-k)(\alpha-2)}}) \cdot p$.

The security of the multi-round Fiat-Shamir transform has been analyzed in [8]. Following their definitions, we provide a soundness proof compatible with 5-round protocols. Such a proof was lacking in previous quasi-cyclic based proposals. A $(q, 2)$-tree of transcripts for a 5-round (public coin) protocol is a set of $2q$ transcripts arranged in a tree structure. The nodes in the tree represent the prover's messages and the edges between the nodes correspond to the verifier's challenges. Each transcript is represented by a path from the three root to a leaf node. We say that the protocol is $(q, 2)$ special-sound if there exists a PPT algorithm that on an input statement and a $(q, 2)$-tree of accepting transcripts outputs a witness.

*Theorem 2 (**(sk, 2)-Special Soundness**):* Let k and δ be public parameters denoting the dimension of a $[n = 2k, k]$ QC code and the number of iterations within the protocol. If COM is a binding commitment scheme, then the PoK depicted in Figure 2 is sound with soundness error $(\frac{sk+\alpha-1}{2sk})^\delta$ for some parameters α and s assuming that the QCSD problem is computationally hard.

Proof: Informally, one can show that if an adversary is able to cheat with probability greater than $(\frac{sk+\alpha-1}{2sk})^\delta$, then he is able to cheat in at least one iteration of the protocol. For that particular iteration of the protocol, one can prove that if an adversary can successfully answer at least $sk + \alpha$ challenges over the $2sk$ possible ones, then he is able to solve the $\mathsf{DiffSD}(n, k, w, \alpha)$ problem. Indeed, this means that given a fixed first commitment CMT_1, there exists α first challenges CH_1 for which the adversary is able to answer both second challenges $\mathrm{CH}_2 = 0$ and $\mathrm{CH}_2 = 1$. Each pair of accepting transcript associated to a challenge α allows to retrieve one unknown $(\mathbf{z}_i)_{i\in[1,\alpha]}$ of the $\mathsf{DiffSD}(n, k, w, \alpha)$ hence the adversary can solve it. Formally, one can extract the aforementioned 2α accepting transcripts from the given $(sk, 2)$-tree of transcripts and build a knowledge extractor for the $\mathsf{DiffSD}(n, k, w, \alpha)$ problem. One completes the proof using Theorem 1, we defer the reader to [16] for the full proof. □

*Theorem 3 (**Honest Verifier Zero-Knowledge**):* If COM is a hiding commitment scheme, then the PoK depicted in Figure 2 satisfies the Honest-Verifier Zero-Knowledge property.

Proof: Informally, the transcript contains commitments and tuples of the form $(\pi_i, \mathbf{u}_i + \mathbf{x}_{r_i}^{s_i})$ for $b_i = 0$ or $(\pi_i[\mathbf{u}_i], \pi_i[\mathbf{x}_{r_i}^{s_i}])$ for $b_i = 1$ (but not both tuples for a given index i). If the commitment used are hiding, they do not leak anything on the secret. When $b_i = 0$ the secret $\mathbf{x}_{r_i}^{s_i}$ is masked by the random value $\mathbf{u}_i$ and when $b_i = 1$ the secret $\mathbf{x}_{r_i}^{s_i}$ is masked by the random permutation π_i. Formally, one can build a simulator that generates the view of an honest verifier with access to the public key only, we defer the reader to [16] for details. □

IV. Parameters and Resulting Sizes

The protocol described in Figure 2 can be turned into a signature using the Fiat-Shamir transform [8], [22], [26], [30], [35]. Hereafter, we discuss the choice of our parameters and compare our protocol with existing schemes.

Decoding attack. We consider the BJMM generic decoder [11] with estimates from [29]. The parameters (n, k, w) are chosen such that decoding w errors in a binary quasi-cyclic $[n, k]$ code costs at least 2^λ. The attacker has access to $N = sk$ syndromes (k rotations of s public keys) and is successful by decoding one of them. As shown in [37], this multiple targets attack reduces the complexity by a factor of at most $\sqrt{N}$.

Soundness error. Following [1], for given (n, k, w), solving $\mathsf{DiffSD}(n, k, w, \alpha)$ provides a solution to $\mathsf{QCSD}(n, k, w)$ with probability $1 - \varepsilon(\alpha)$ where $\varepsilon(\alpha) \approx \binom{n}{w}^{\alpha-1} / 2^{(n-k)(\alpha-2)}$. The soundness error for one iteration cannot exceed $\rho^* = \frac{sk+\alpha^*-1}{2sk}$ where α^* is the largest integer such that $\varepsilon(\alpha^*) \leq 2^{-\lambda}$. The soundness error for δ iterations is $(\rho^*)^\delta$ and it is lower than $2^{-\lambda}$ if $\delta \geq \frac{-\lambda}{\log_2 \rho^*}$.

Attack against 5-rounds protocols. The attack of [32] can be used against our protocol. For δ iterations of the protocol, the attacker will find the value of τ^* (the number of second challenges to guess) which minimizes the attack cost $P^{-1} + 2^{\delta-\tau^*}$ where $P = \sum_{\tau \geq \tau^*} \binom{\delta}{\tau} \left(\frac{1}{sk}\right)^\tau \left(\frac{sk-1}{sk}\right)^{\delta-\tau}$. The choice of δ must be such that this cost is $\geq 2^\lambda$.

Signature length and scalability. The signature consists of the outputs of $\mathsf{P}_1, \mathsf{P}_2, \mathsf{P}_3$ namely two commitments and a seed along with all the d_i (see Figure 2). Each response d_i consists of a seed, a commitment, and a word of $\mathbb{F}_2^n$ with no particular structure if $b_i = 0$ and of weight w if $b_i = 1$. The seeds and commitments are taken of length λ and 2λ respectively. The words of weight w can be compressed to $n - k$ bits. Finally the seeds and commitments can be structured pairwise as explained in Section III-B, allowing to save one seed and one commitment every 4 iterations on average. For codes of rate $1/2$ ($k = n/2$) the average length of the signature is $|\sigma| = 5\lambda + \delta(0.75n + 2.25\lambda)$. Both δ and n will grow linearly with the security parameters λ and thus the signature length grows as λ^2, roughly we have here $|\sigma| \approx 11\lambda^2$.

TABLE I: Parameters and signature sizes in bytes for $\lambda = 128$

n	k	w	δ	s	sk size	pk size	σ size
1306	653	137	151	1	16 B	0.1 kB	24.1 kB
			145	4	16 B	0.4 kB	23.1 kB
			141	20	16 B	1.7 kB	22.5 kB

Comparison with code-based schemes. We compare our proposal to code-based signatures constructed from PoK for the SD problem in Table II. We consider both size and expected performances as criteria. Since there is no implementation available for most of these schemes yet, we provide an estimate of their expected relative performances. For all these schemes, the first step (every operations executed by the prover before he outputs its first commitment) is likely to dominate the overall performance cost. This step can be seen as repeating μ times the computation of ν operations whose cost is approximated to be equal amongst schemes. We refer the reader to the full version of this paper for a discussion about the relevance and limits of this metric [16]. Overall, one can see that our proposal offers an interesting trade-off between cost and sizes as it has the smallest expected cost while still featuring competitive sizes. In addition, we also present in Table III the sizes of other code-based signatures. Wave [23] is based on the SD problem over $\mathbb{F}_3$ (with secrets of large weights) and the Generalized $(U, U + V)$-codes indistinguishability, LESS [10] relies on the permutation code equivalence problem and Durandal [7] is based on the rank SD problem and the product spaces subspaces indistinguishability.

TABLE II: Signatures from PoK for the SD problem ($\lambda = 128$)

	Performance			Size	
	μ	ν	Cost	pk	σ
Stern [38]	219	2	438	0.1 kB	36.2 kB
Véron [13], [42]	219	2	438	0.2 kB	30.8 kB
CVE [17]	156	2	312	0.3 kB	31.4 KB
AGS [1]	151	2	302	0.2 kB	29.3 kB
	145	2	290	0.7 kB	28.2 kB
	141	2	282	3.3 kB	27.4 kB
GPS [28]	512	128	65 536	0.2 kB	27.1 kB
	4096	1024	4 194 304	0.2 kB	19.8 kB
FJR [25]	187	8	1496	0.1 kB	24.4 kB
	389	32	12 448	0.1 kB	17.6 kB
BGKM (Sig. 1) [15]	256	2	512	0.1 kB	24.3 kB
This Paper	151	2	302	0.1 kB	24.1 kB
	145	2	290	0.4 kB	23.1 kB
	141	2	282	1.7 kB	22.5 kB

TABLE III: Other code-based signatures ($\lambda = 128$)

	pk	σ	pk + σ
Wave [23]	3.2 MB	0.93 kB	3.3 MB
LESS [10]	11.6 kB	10.4 kB	22.0 kB
Durandal [7]	15.3 kB	4.1 kB	19.4 kB

Comparison with other schemes. Outside of code-based cryptography, there exist many other signatures based on the Fiat-Shamir transform. Some of them were submitted to the NIST standardization process [18], [20] while other have been published recently [14]. All these schemes reduce to a given difficult problem like for instance the MQ or PKP problems. For 128 bits of security, depending on these different post-quantum ZK signature schemes, the size of the signature may vary (also depending on chosen trade-offs) between 12kB for [14] and 40kB for MQDSS [20]. A strong feature of the SD problem is that the problem has been used for a long time, the attacks are well understood, and thus significant speedups in the attacks are unlikely to occur.

Generalization to additional metrics. Our protocol can be generalized to other weights as explained in the full version of the paper [16].

References

[1] Aguilar, C., Gaborit, P., Schrek, J.: A new zero-knowledge code based identification scheme with reduced communication. In: IEEE IT Workshop (2011)

[2] Aguilar Melchor, C., Aragon, N., Bardet, M., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Hauteville, A., Otmani, A., Ruatta, O., Tillich, J.P., Zémor, G.: ROLLO - Rank-Ouroboros, LAKE & LOCKER. NIST Post-Quantum Cryptography Standardization Project (Round 2) (2020)

[3] Aguilar Melchor, C., Aragon, N., Barreto, P., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Ghosh, S., Gueron, S., Güneysu, T., Misoczki, R., Persichetti, E., Sendrier, N., Tillich, J.P., Vasseur, V., Zémor, G.: BIKE: Bit Flipping Key Encapsulation. NIST Post-Quantum Cryptography Standardization Project (Round 3) (2020)

[4] Aguilar Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Bos, J., Deneuville, J.C., Dion, A., Gaborit, P., Lacan, J., Persichetti, E., Robert, J.M., Véron, P., Zémor, G.: Hamming Quasi-Cyclic (HQC). NIST Post-Quantum Cryptography Standardization Project (Round 3) (2020)

[5] Aguilar Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Bros, M., Couvreur, A., Deneuville, J.C., Gaborit, P., Hauteville, A., Zémor, G.: Rank Quasi-Cyclic (RQC). NIST Post-Quantum Cryptography Standardization Project (Round 2) (2020)

[6] Albrecht, M.R., Bernstein, D.J., Chou, T., Cid, C., Gilcher, J., Lange, T., Maram, V., von Maurich, I., Misoczki, R., Niederhagen, R., Patterson, K.G., Persichetti, E., Peters, C., Schwabe, P., Sendrier, N., Szefer, J., Tjhai, C.J., Tomlinson, M., Wang, W.: Classic McEliece. NIST Post-Quantum Cryptography Standardization Project (Round 3) (2020)

[7] Aragon, N., Blazy, O., Gaborit, P., Hauteville, A., Zémor, G.: Durandal: a rank metric based signature scheme. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) (2019)

[8] Attema, T., Fehr, S., Klooß, M.: Fiat-Shamir Transformation of Multi-Round Interactive Proofs. Cryptology ePrint Archive, Report 2021/1377 (2021), https://ia.cr/2021/1377

[9] Baldi, M., Barenghi, A., Chiaraluce, F., Pelosi, G., Santini, P.: LEDAcrypt. NIST Post-Quantum Cryptography Standardization Project (Round 2) (2020)

[10] Barenghi, A., Biasse, J.F., Persichetti, E., Santini, P.: LESS-FM: Fine-tuning Signatures from a Code-based Cryptographic Group Action. In: International Workshop on Post-Quantum Cryptography (PQCrypto) (2021)

[11] Becker, A., Joux, A., May, A., Meurer, A.: Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding. In: Pointcheval, D., Johansson, T. (eds.) Eurocrypt 2012. LNCS, vol. 7237, pp. 520–536. Springer (2012)

[12] Bellini, E., Caullery, F., Gaborit, P., Manzano, M., Mateu, V.: Improved Véron Identification and Signature Schemes in the rank metric. In: IEEE International Symposium on Information Theory (ISIT) (2019)

[13] Bettaieb, S., Bidoux, L., Blazy, O., Gaborit, P.: Zero-Knowledge Reparation of the Véron and AGS Code-based Identification Schemes. In: IEEE International Symposium on Information Theory (ISIT) (2021)

[14] Beullens, W.: Sigma Protocols for MQ, PKP and SIS, and Fishy Signature Schemes. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) (2020)

[15] Bidoux, L., Gaborit, P., Kulkarni, M., Mateu, V.: Code-based Signatures from New Proofs of Knowledge for the Syndrome Decoding Problem. arXiv preprint arXiv:2201.05403 (2022)

[16] Bidoux, L., Gaborit, P., Kulkarni, M., Sendrier, N.: Quasi-Cyclic Stern Proof of Knowledge. arXiv preprint arXiv:2110.05005 (2021)

[17] Cayrel, P.L., Véron, P., El Yousfi Alaoui, S.M.: A Zero-Knowledge Identification Scheme Based on the q-ary Syndrome Decoding Problem. In: International Conference on Selected Areas in Cryptography (SAC) (2011)

[18] Chase, M., Derler, D., Goldfeder, S., Kales, D., Katz, J., Kolesnikov, V., Orlandi, C., Ramacher, S., Rechberger, C., Slamanig, D., Xiao, W., Zaverucha, G.: The Picnic Signature Algorithm. NIST Post-Quantum Cryptography Standardization Project (Round 3), https://microsoft.github.io/Picnic/ (2020)

[19] Chen, K.: A new identification algorithm. In: International Conference on Cryptography: Policy and Algorithms (1995)

[20] Chen, M.S., Hülsing, A., Rijneveld, J., Samardjiska, S., Schwabe, P.: MQDSS specifications. NIST Post-Quantum Cryptography Standardization Project (Round 2), http://mqdss.org (2020)

[21] Courtois, N., Finiasz, M., Sendrier, N.: How to achieve a McEliece-based digital signature scheme. In: International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT) (2001)

[22] Dagdelen, Ö., Galindo, D., Véron, P., Alaoui, S.M.E.Y., Cayrel, P.L.: Extended security arguments for signature schemes. Designs, Codes and Cryptography **78**(2) (2016)

[23] Debris-Alazard, T., Sendrier, N., Tillich, J.P.: Wave: A new family of trapdoor one-way preimage sampleable functions based on codes. In: International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT) (2019)

[24] Don, J., Fehr, S., Majenz, C.: The measure-and-reprogram technique 2.0: multi-round Fiat-Shamir and more. In: Annual International Cryptology Conference. pp. 602–631. Springer (2020)

[25] Feneuil, T., Joux, A., Rivain, M.: Shared Permutation for Syndrome Decoding: New Zero-Knowledge Protocol and Code-Based Signature. Cryptology ePrint Archive, Report 2021/1576 (2021)

[26] Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Advances in Cryptology (CRYPTO) (1986)

[27] Gaborit, P., Schrek, J., Zémor, G.: Full cryptanalysis of the Chen identification protocol. In: International Workshop on Post-Quantum Cryptography (PQCrypto) (2011)

[28] Gueron, S., Persichetti, E., Santini, P.: Designing a Practical Code-based Signature Scheme from Zero-Knowledge Proofs with Trusted Setup. Cryptology ePrint Archive, Report 2021/1020 (2021)

[29] Hamdaoui, Y., Sendrier, N.: A non asymptotic analysis of information set decoding. Cryptology ePrint Archive, Report 2013/162 (2013)

[30] Hülsing, A., Rijneveld, J., Samardjiska, S., Schwabe, P.: From 5-pass MQ-based identification to MQ-based signatures. Cryptology ePrint Archive, Report 2016/708 (2016)

[31] Jain, A., Krenn, S., Pietrzak, K., Tentes, A.: Commitments and Efficient Zero-Knowledge Proofs from Learning Parity with Noise. In: International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT) (2012)

[32] Kales, D., Zaverucha, G.: An Attack on Some Signature Schemes Constructed From Five-Pass Identification Schemes. In: International Conference on Cryptology and Network Security (CANS) (2020)

[33] Katz, J., Kolesnikov, V., Wang, X.: Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures. In: Proceedings of the 2018 ACM Conference on Computer and Communications Security (CCS) (2018)

[34] McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. Coding Thv **4244** (1978)

[35] Pointcheval, D., Stern, J.: Security proofs for signature schemes. In: International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) (1996)

[36] Schrek, J.: Signatures et authentications pour les cryptosystèmes basés sur les codes correcteurs en métrique de Hamming et en métrique rang. Ph.D. thesis, University of Limoges (2013)

[37] Sendrier, N.: Decoding One Out of Many. In: Yang, B.Y. (ed.) PQCrypto 2011. LNCS, vol. 7071, pp. 51–67 (2011)

[38] Stern, J.: A new identification scheme based on syndrome decoding. In: Annual International Cryptology Conference (CRYPTO) (1993)

[39] Unruh, D.: Quantum Proofs of Knowledge. In: Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology – EUROCRYPT 2012. pp. 135–152. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)

[40] Unruh, D.: Computationally Binding Quantum Commitments. In: Fischlin, M., Coron, J.S. (eds.) Advances in Cryptology – EUROCRYPT 2016. pp. 497–527. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)

[41] Unruh, D.: Post-quantum Security of Fiat-Shamir. In: ASIACRYPT (1). pp. 65–95. Springer (2017)

[42] Véron, P.: Improved identification schemes based on error-correcting codes. Applicable Algebra in Engineering, Communication and Computing (1997)