A Provably Secure Short Signature Scheme from Coding Theory

Maryam Rajabzadeh Asaar*, Mahmoud Salmasizadeh*, Mohammad Reza Aref †
*Electronics Research Institute (Center), Sharif University of Technology, Tehran, Iran
† Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran
Email : asaar@ee.sharif.edu, salmasi@sharif.edu, aref@ee.sharif.edu

***Abstract*—Signatures with partially message recovery in which some parts of messages are not transmitted with signatures to make them shorter are useful where bandwidth is one of the crucial concern and especially in case of signing short messages in applications such as time stamping, certified email services and identity-based cryptosystems. In this paper, to have quantum-attack-resistant short signatures, a signature scheme with partially message recovery from coding theory is proposed. The security of the proposed scheme is proved under Goppa Parametrized Bounded Decoding and the Goppa Code Distinguishing assumptions in the random oracle model. Relying on the partially message recovery property, the proposal is shorter than the Dallot signature scheme, the only provably secure and practical code-based signature scheme. We should highlight that our scheme can be used as a building block of code-based signature schemes with additional properties since it compared to Dallot signature scheme not only improves its communication overhead but also it preserves its signature efficiency.**

Keywords: code-based signatures, signatures with message recovery, provable security, random oracle model.

I. Introduction

Digital signatures based on number theory are the most important achievements of modern cryptography, and widely deployed around the world. The progress in the quantum computing field leads serious threats to security of most widely used public key cryptosystems. In 1994, Shor has presented results to show that quantum computers can break security of cryptographic algorithms based on number theory [1]. To tackle this problem, it is necessary to have alternative constructions [2–4]. One of the few alternatives we have focus on is code-based cryptography.

CODE-BASED CRYPTOGRAPHY. McEliece [2] in 1978 introduced the concept of code-based cryptography, and also presented the first code-based public key encryption scheme from the general decoding problem.

McEliece [2] scheme cannot be used as a signature scheme since it is not invertible. In 1986, Niederreiter [5] modified McEliece code-based cryptosystem. Although Niederreiter security is as equivalent as that of McEliece scheme [6], its encryption is ten times faster than that of McEliece scheme, and it can be used for constructing of digital signature schemes. In 2001, Courtois, Finiasz and Sendrier [7] proposed the first practical code-based signature scheme called CFS scheme. They adapt the full domain hash approach of Bellare and Rogaway [8] to Niederreither encryption scheme [5] in a way that a message is concatenated with a counter before hashing to make hash values decodable. Although authors presented some security arguments, it does not support provable security. In 2008, Dallot [9] gave a slight modification to their signature scheme in a way the counter is replaced with a random value, this modified scheme is named modified CFS or Dallot scheme, and proved its security under Goppa Parameterized Bounded Decoding [10] and Goppa Code Distinguishing [11] assumptions in the random oracle model [8]. A few code-based signature schemes with special properties such as identity-based [12], one-time signatures [13], ring signatures [14], threshold ring [15–17], blind signatures [18], signcryption scheme [19] and undeniable signature [20] have been proposed, where the main core of most of these constructions is Dallot signature scheme [9].

SIGNATURES WITH MESSAGE RECOVERY. In signature schemes with message recovery, the signed message is not transmitted with the signature and can be retrieved from the signature by anyone. The main feature of this primitive is to shorten the signature size. Applications of this primitive are signing short messages, (e.g., including time, date and identifiers in certified email and time stamping services) and transmissions on small bandwidth.

There are two types of signature schemes with message recovery in the literature: RSA based and discrete logarithm (elliptic curve) based. PSS-R [21] and ISO/IEC 9796-1,9796-2 [22–24] are schemes of the first type, and the Nyberg-Rueppel signature schemes [25–27], Miyaji scheme [28] and Abe and Okamoto scheme [29] are instances of the second type. In 1991, ISO/IEC 9796-1 standard [22] was presented as the first international standard for digital signatures, and was believed to be secure till some attacks were proposed by Coron et al. [30] and by Coppersmith et al. [31]. Next this standard

was withdrawn, and standards ISO/IEC 9796-2-2002 and ISO/IEC 9796-2-2010 were proposed [23, 24], where all of them support message recovery feature. In 1993, the first discrete-logarithm based signature scheme giving message recovery was proposed by Nyberg and Rueppel [25], and in 1995 and 1996, Nyberg and Rueppel [26, 27] showed that all ElGamal-type signature schemes can be modified to support message recovery features, and this primitive is useful in various scenario such as identity-based cryptosystems and key agreement protocols. In 1998 and 1999, some security flaws of heuristically designed schemes [22] have been found [30, 32]. As a result, provable security even in the random oracle model [8] is necessary to assure the security of a scheme.

PSS-R scheme [21] and Abe and Okamoto scheme [29] are provably secure under RSA and discrete logarithm assumptions in the random oracle model, respectively. In fact, they are existentially unforgeable against adaptively chosen message attacks under number theory assumptions (the RSA and discrete logarithm assumption).

CONTRIBUTION. In one hand, in many applications such as identity-based cryptosystems where short messages need to be signed, message-recovery based signatures or short signatures are essential since they prevent message expansion; and on the other hand, code-based short signature schemes which are resistant against quantum attacks are important alternatives for number-theory based ones. As result, to have *code-based* signatures which are quantum-attack-resistant, to *minimize signature size* and *avoiding presenting heuristically designed* signature schemes, a provably secure code-based signature scheme with partially message recovery is proposed. To the best of our knowledge, this is the first *provably secure* signature scheme *with partially message recovery* from *coding theory*. To do so, the (partially) message recovery technique proposed in [29] is inserted to Dallot signature scheme [9], and it is possible due to the existence of a random number in the signature that makes hash values decodable. Then, we show that the proposal is secure under Goppa Parametrized Bounded Decoding and the Goppa Code Distinguishing assumptions in the random oracle model [8]. It should be emphasized that our scheme can be used as the base signature scheme on behalf of Dallot scheme [9] to construct code-based signatures with additional properties such as [12, 14, 17, 18] since it is as efficient as Dallot scheme, and also its signature size is improved.

A. Organization of the paper

The rest of this paper is organized as follows. Section II presents background and complexity assumptions employed as the signature foundation, the outline of signature schemes with message recovery and its security security model. Our proposed scheme and its formal security proof are presented in Section III. Section IV and V present the comparison and conclusion, respectively.

II. BACKGROUND

In this section, first the used notations in the paper are introduced, then, we review several fundamental backgrounds employed in this research, including Goppa Parametreized Bounded Decoding and Goppa Code Distinguishing assumptions.

A. Notations

In this subsection, the notations used in the paper are defined.

- $y||x$: a concatenation of two strings y and x such that from $y||x$, y and x are effectively recoverable.
- $\oplus$: X-OR operation.
- ${}_{l_2}|y|$: the first left l_2 bits of the string y.
- $|y|_{l_1}$: the first right l_1 bits of the string y.
- $|y|$: the number of bits of the string y.
- $w_H(y)$: the Hamming weight of a word y or the number of non-zero positions of y.
- y^T: transpose of a vector y.
- $\perp$: an empty string.
- $\theta \leftarrow B(y_1, ...)$: the operation of assigning the output of algorithm B on inputs $y_1, ...$ to θ.
- $y \xleftarrow{\$} Y$: the operation of assigning a uniformly random element of Y to y.

B. Coding Theory

Let $\mathbb{F}_2$ be the field with two elements and a binary code $\mathcal{C}(n,k)$ be a linear subspace of dimension k of $\mathbb{F}_2^n$, where k and $n \in mathbbN$. Elements of $\mathbb{F}_2^n$ and $\mathcal{C}$ are named words and codewords, respectively. Code $\mathcal{C}(n,k)$ is presented by a $(n-k) \times n$ binary parity check matrix H such that for a codeword $x \in \mathbb{F}_2^n$ belonged to $\mathcal{C}(n,k)$, we have $Hx^T = 0$ and the syndrome of a word $x \in \mathbb{F}_2^n$ is defined as $s = Hx^T$, where $s \in \mathbb{F}_2^{n-k}$. A syndrome s is said to be t-decodable if there exists a word $x \in \mathbb{F}_2^n$ such that $Hx^T = s$ and $w_H(x) \leq t$, where $t = \frac{n-k}{\log_2^n}$ is the error correcting capability of the code $\mathcal{C}(n,k)$.

Goppa codes are a subclass of alternant codes [33], and widely used in code-based cryptography. Goppa codes $G(n,k)$ of t error correcting capability are of length $n = 2^m$ and dimension $k = n - mt$, where m and $t \in \mathbb{N}$. It is assumed that $\mathcal{DEC}_H$ be the decoding algorithm of Goppa code $G(n,k)$ with the parity check matrix H.

C. Complexity assumptions

Hard problems and security assumptions are used in the paper are defined as follows [9, 11, 34].

Definition 1. Goppa Parameterized Bounded Decoding (GPBD) problem. Given a random $(n-k)\times n$ binary matrix H and a syndrome $s \in \mathbb{F}_2^{n-k}$, output a word $x \in \mathbb{F}_2^n$ such that $w_H(x) \leq \frac{n-k}{\log_2^n}$ and $Hx^T = s$.

Definition 2. Goppa Parametreized Bounded Decoding (GPBD) assumption. The GPBD problem is (τ, ϵ)-hard if there is no algorithm C which runs in time at most τ and with probability at least ϵ breaks the GPBD problem.

Definition 3. Goppa Code Distinguishing (GD) problem. Given a $(n-k)\times n$ binary parity check matrix H, output a bit $b \in \{0,1\}$ indicating if H is a random binary parity check matrix or a Goppa code random binary parity check matrix.

The advantage of the distinguisher C is defined as follows.

$$Adv_C^{GD}(n,k) = \Pr[1 \leftarrow C(H) \mid H \xleftarrow{\$} G(n,k)] - \Pr[1 \leftarrow C(H) \mid H \xleftarrow{\$} B(n,k)] \tag{1}$$

Definition 4. Goppa Code Distinguishing (GD) assumption. The GD problem is (τ, ϵ)-hard if there is no algorithm C which runs in time at most τ breaks the GD problem with probability $Adv_C^{GD}(n,k) \geq \epsilon$.

D. Dallot signature scheme

In this subsection, we review the modified CFS signature proposed by Dallot [9], Dallot scheme, whose security is based on the GD and GPBD assumptions in the random oracle model.

1) Setup: The system parameters are as follows. Let n, k, m and $t \in \mathbb{N}$ be parameters for a Goppa code of length $n = 2^m$, dimension k and error correcting capability $t = \frac{n-k}{\log_2^n}$ such that t-decoding has complexity at least 2^λ for a security parameter λ. Let $g : \{0,1\}^* \to \{0,1\}^{n-k}$ be a random oracle. It is assumed that $\tilde{H}$ be a $(n-k)\times n$ parity check matrix of a random binary Goppa code and $\mathcal{DEC}_{\tilde{H}}$ be its t-decoding algorithm. The public key is $pk = H = U\tilde{H}P$, and the secret key is $sk = (\mathcal{DEC}_{\tilde{H}}, U, P)$, where U is a random binary non-singular $(n-k)\times(n-k)$ matrix and P is a random $n \times n$ binary permutation matrix. Therefore, public parameters are $Para = \{n, k, m, t, g\}$.

2) Sign: To create a signature θ on the message M, the signer picks a number r randomly chosen from $\{1, ..., 2^{n-k}\}$, computes $\beta = g(r, M)$ and $x = \mathcal{DEC}_{\tilde{H}}(U^{-1}\beta)P$. If $x = \perp$, it chooses another r, and repeats the signing procedure. The signature θ on the message M is (r, x, M).

3) Ver: Given H, $Para$ and a signature $\theta = (r, x, M)$, if $Hx^T = g(r, M)$ and $w_H(x) \leq t$, the signature θ on the message M is valid and outputs 1; otherwise, it outputs 0 and the signature is invalid.

E. Outline of signature schemes with message recovery

A signer with the public key pk and a verifier are participants of a signature with message recovery, and the scheme consists of Setup, Sign and Ver/MR algorithms as follows [29].

- Setup: Given the system security parameter λ, it outputs system's parameters $Para$ and the users' key pair (sk, pk), i.e. $(Para, (sk, pk)) \leftarrow Setup(\lambda)$.
- Sign: Given the system's parameter $Para$, signer's secret key sk and the message M to be signed, it outputs the signature θ, i.e. $\theta \leftarrow Sign(Para, sk, M)$.
- Ver/MR: Given the system's parameter $Para$, the signer's public key pk and the signature θ, it first recovers the message M, and outputs 1 if θ is a valid signature of the message M and outputs 0 otherwise, i.e. $(M, \{0,1\}) \leftarrow Ver/MR(Para, pk, \theta)$.

F. Security model of signatures with message recovery

A signature scheme with message recovery should be secure against existential forgery under an adaptive-chosen-message attack [29].

To have a formal definition for existential unforgeability, the adversary A and a challenger C should interact through the following game[29].

1) Setup: Algorithm C runs the Setup algorithm with a security parameter λ to obtain system's parameter $Para$ and user's key pair (pk, sk), then it sends $(pk, Para)$ to A.

2) The adversary A in addition to making quires to random oracles adaptively issues a polynomially bounded number of questions to the Sign oracle as follows.
Sign: Adversary A can request a signature on the message M of its choice. Then, C returns $\theta \leftarrow Sign(Para, sk, M)$ to A.

3) Eventually, A returns a valid signature θ^* on the message M^* for the signer's public key pk, and wins the game if the message M^* has not been requested to the Sign algorithm.

The formal definition of existential unforgeability is expressed in Definition 5.

Definition 5. A signature is $(\tau, q_g, q_s, \epsilon)$-existentially unforgeable against adaptive chosen message attack if there is no adversary which runs in time at most τ, makes at most q_g random oracle queries, makes at most q_s Sign queries, and can win the aforementioned game with probability at least ϵ.

III. Our proposed signature scheme with message recovery

In this section, a short code-based signature scheme based on partially message recovery technique presented in [29] is proposed. Next, its security is proved under GPBD and GD assumptions in the random oracle model [8].

A. Details of the proposed signature scheme

In this section, we present the details of our signature scheme. There are two participants in the system, a signer with public key pk and a verifier. Our scheme consists of three algorithms as follows.

1) Setup: The system parameters are as follows. Let n, k, m and $t \in \mathbb{N}$ be parameters for a Goppa code of length $n = 2^m$, dimension k and error correcting capability $t = \frac{n-k}{\log_2^n}$ such that t-decoding has complexity at least 2^λ for a security parameter λ. Let $g_0 : \{0,1\}^{n-k} \to \{0,1\}^{n-k}$, $g_1 : \{0,1\}^{n-k} \times \{0,1\}^* \to \{0,1\}^{n-k}$, $F_1 : \{0,1\}^{l_2} \to \{0,1\}^{l_1}$, $F_2 : \{0,1\}^{l_1} \to \{0,1\}^{l_2}$ be random oracles, where l_1 and $l_2 \in \mathbb{N}$ and $l_1 + l_2 = n - k$.
It is assumed that $\tilde{H}$ be a $(n-k) \times n$ parity check matrix of a random binary Goppa code and $\mathcal{DEC}_{\tilde{H}}$ be its t-decoding algorithm. The public key is $pk = H = U\tilde{H}P$, and the secret key is $sk = (\mathcal{DEC}_{\tilde{H}}, U, P)$, where U is a random binary non-singular $(n-k) \times (n-k)$ matrix and P is a random $n \times n$ binary permutation matrix. Therefore, public parameters are $Para = \{n, k, m, t, g_0, g_1, F_1, F_2, l_1, l_2\}$.

2) Sign: To generate a signature θ on the message M, the signer chooses a random number r from $\{1, ..., 2^{n-k}\}$, parses the message M as $M_1||M_2$ such that $|M_2| = l_2$, and computes $M_2' = F_1(M_2)||F_2(F_1(M_2)) \oplus M_2$, $\alpha = M_2' \oplus g_0(r)$, $\beta = g_1(\alpha, M_1) \oplus g_0(r)$ and $x = \mathcal{DEC}_{\tilde{H}}(U^{-1}\beta)P$. If $x = \perp$, it chooses another r, and repeats the signing procedure. The signature θ on the message M is (α, x, M_1).

3) Ver/MR: Given H, $Para$ and a signature $\theta = (\alpha, x, M_1)$, a verifier computes $Hx^T \oplus g_1(\alpha, M_1) \oplus \alpha$ to attain $\hat{M}_2'$. Then, it obtains $\hat{M}_2 = |\hat{M}_2'|_{l_2} \oplus F_2({}_{l_1}|\hat{M}_2'|)$, and recovers the message M as $M_1||\hat{M}_2$. The signature θ on the message M is valid and outputs 1 if and only if ${}_{l_1}|\hat{M}_2'| = F_1(\hat{M}_2)$ and $w_H(x) \le t$; otherwise, it outputs 0 and the signature is invalid.

Remark 1. *However, it is possible to convert the proposed scheme to the one with full message recovery if the length of the message is considered to be constant; i.e. $|M| = l_2$ in the proposed scheme, we consider partial message recovery to make our construction flexible.*

B. Analysis of the proposed scheme

In this subsection, the correctness of the new scheme is verified and its existential unforgeability is proved in the random oracle model (see [8] for the background). In order to prove unforgeability of the proposed scheme, we need to show that it is unforgeable against adversary A (as defined in Section II-F).

To prove the security of our proposed scheme, and by contradiction, assuming an adversary A, we show that there is an algorithm C that can solve a random instance of the GPBD problem with a non-negligible probability. Our main result on the security of the proposed scheme is summarized in Theorem 1.

To start let us verify the correctness of the proposed scheme, and we use $\alpha = M_2' \oplus g_0(r)$ and $\beta = g_1(\alpha, M_1) \oplus g_0(r)$ in what follows.

$$\begin{aligned} & Hx^T \oplus g_1(\alpha, M_1) \oplus \alpha \\ &= (U\tilde{H}P)(\mathcal{DEC}_{\tilde{H}}(U^{-1}\beta)P)^T \oplus g_1(\alpha, M_1) \oplus \alpha \\ &= (U\tilde{H}P)P^T(\mathcal{DEC}_{\tilde{H}}U^{-1}\beta)^T \oplus g_1(\alpha, M_1) \oplus \alpha \\ &= UU^{-1}\beta \oplus g_1(\alpha, M_1) \oplus \alpha \\ &= g_1(\alpha, M_1) \oplus g_0(r) \oplus g_1(\alpha, M_1) \oplus M_2' \oplus g_0(r) \\ &= M_2' = F_1(M_2)||F_2(F_1(M_2)) \oplus M_2. \end{aligned} \tag{2}$$

If θ is a valid signature on the message M, $Hx^T \oplus g_1(\alpha, M_1) \oplus \alpha = M_2'$, and the message M_2 is recovered as $M_2 = |M_2'|_{l_2} \oplus F_2({}_{l_1}|M_2'|)$ and integrity of the message M_2 is checked by $F_1(M_2) = {}_{l_1}|M_2'|$.

Theorem 1. *If the GPBD problem is $(\tau_{GPBD}, \epsilon_{GPBD})$-hard and GD problem is $(\tau_{GD}, \epsilon_{GD})$-hard, then the proposed scheme is $(\tau, q_{g_0}, q_{g_1}, q_s, \epsilon)$-secure against the adversary A such that*

$$\epsilon_{GPBD} \geq \frac{\epsilon - \epsilon_{GD} - 2^{-(n-k+1)}}{q_{g_1} q_{g_0}}, \qquad \tau_{GPBD} \leq \tau + q_s(mt^2), \tag{3}$$

where n, k, t and m are systems's constants. In addition, q_{g_0}, q_{g_1} and q_s are the number of queries to oracles $g_0(.)$, $g_1(.,.)$ and Sign, respectively.

Proof:

It is supposed that there is an adversary A against unforgeability of the scheme with success probability ϵ. We construct another algorithm C to solve GPBD problem with success probability ϵ_{GPBD}. Given a random binary matrix H^* and a random vector s^*, algorithm C outputs x^* such that $H^*(x^*)^T = s^*$ and $w(x^*) \leq t$. Note that substituting the public key of the signer with a random binary matrix H^* changes the success probability of the simulator C with advantage at most ϵ_{BD} to solve the permuted Goppa code distinguishing.

The algorithm C runs Setup on a security parameter λ, and gets a random instance of the GPBD problem, (n, k, m, t, H^*, s^*), to set signer's public key, H, to H^* and generate the public parameters $Para = \{n, k, m, t, F_1, F_2, l_1, l_2\}$ and invokes the adversary A on $Para$ and $H = H^*$. The adversary A runs in time at most τ, makes q_{g_0} queries to the random oracle $g_0(.)$, q_{g_1} queries to the random oracle $g_1(.,.)$ and q_s queries to the Sign oracle, and can win the unforgeability game with probability at least $\epsilon_1 = \epsilon - \epsilon_{BD}$. Algorithm C maintains initially empty associative tables $T_0[.]$ and $T_1[.,.]$ to simulate random oracles $g_0(.)$ and $g_1(.,.)$, and answers A's oracle queries as described below (refer to Figure 1).

- $g_0(.)$ queries: If $T_0[.]$ is defined for the query r, then, C returns its value; otherwise, C chooses $T_0[r] \xleftarrow{\$} \{0,1\}^{n-k}$, and returns $g_0(r)$ to A (see Lines 4-11, Fig. 1).

- $g_1(.,.)$ queries: If $T_1[.,.]$ is defined for the query (M_1, α), then, C returns its value; otherwise, C chooses $T_1[M_1, \alpha] \xleftarrow{\$} \{0,1\}^{n-k}$, and returns $g_1(M_1, \alpha)$ to A (see Lines 12-19, Fig. 1).

- Sign queries: For a query M, C parses the message M as $M_1||M_2$ such that $|M_2| = l_2$, and computes $M_2' = F_1(M_2)||F_2(F_1(M_2)) \oplus M_2$, chooses a random r from $\{1, ..., 2^{n-k}\}$, makes $g_0(r)$ query to attain its value, computes $\alpha = M_2' \oplus g_0(r)$, and selects $x \xleftarrow{\$} \{0,1\}^{n-k}$ such that $w_H(x) \leq t$ and computes $Hx^T = \beta$. If $T_1[\alpha, M_1]$ has already been defined, then, C halts, returns $\perp$ and sets $bad \leftarrow true$; otherwise, it sets $T_1[\alpha, M_1] \leftarrow \beta \oplus g_0(r)$, and returns the signature $\theta = (\alpha, x, M_1)$ on the message M to A (see Lines 20-39, Fig. 1).

1: $Done = 0$.
2: $(Done, \xi_1 = (Question, Oracle), \xi_2) \leftarrow A(H, Para)$
3: **while** $\neg Done$ **do**
4: **if** $\xi_1 = (r, g_0)$ **and** $\xi_2 = \perp$ **then**
5: **if** $T_0[r]$ is defined **then**
6: **return** $g_0(r)$
7: **else**
8: Set $T_0[r] \xleftarrow{\$} \{0,1\}^{n-k}$ **and**
9: **return** $g_0(r)$
10: **end if**
11: **end if**
12: **if** $\xi_1 = ((\alpha, M_1), g_1)$ **and** $\xi_2 = \perp$ **then**
13: **if** $T_1[\alpha, M_1]$ is defined **then**
14: **return** $g_1(\alpha, M_1)$
15: **else**
16: Set $T_1[\alpha, M_1] \xleftarrow{\$} \{0,1\}^{n-k}$ **and**
17: **return** $g_1(\alpha, M_1)$
18: **end if**
19: **end if**
20: **if** $\xi_1 = (M, Sign)$ **and** $\xi_2 = \perp$ **then**
21: Parse the message M as $M_1||M_2$, where $|M_2| = l_2$
22: Compute $M_2' = F_1(M_2)||F_2(F_1(M_2)) \oplus M_2$
23: Choose $r \xleftarrow{\$} \{1, ..., 2^{n-k}\}$
24: **if** $T_0[r]$ is defined **then**
25: **return** $g_0(r)$
26: **else**
27: Set $T_0[r] \xleftarrow{\$} \{0,1\}^{n-k}$ **and**
28: **return** $g_0(r)$
29: **end if**
30: Compute $\alpha = M_2' \oplus g_0(r)$
31: Select $x \xleftarrow{\$} \{0,1\}^{n-k}$ such that $w_H(x) \leq t$ and compute $Hx^T = \beta$
32: **if** $T_1[\alpha, M_1]$ has already been defined **then**
33: Set $bad \leftarrow true$ **and**
34: **return** $\perp$
35: **else**
36: Set $T_1[\alpha, M_1] \leftarrow \beta \oplus g_0(r)$ **and**
37: **return** the signature $\theta = (\alpha, x, M_1)$ on the message M
38: **end if**
39: **end if**
40: **end while**
41: **if** Done **then**
42: A returns $(\xi_1 = \perp, \xi_2 = (g_0, g_1, \theta = (\alpha^*, x^*, M_1^*))$
43: **end if**

Fig. 1. Algorithm $C(H, s^*, Para)$

- Finally, A outputs a forged signature $\theta^* = (\alpha^*, x^*, M_1^*)$. The forgery is non-trivial if A has not made a Sign query on input M^* (see Lines 41-43, Fig. 1).

The probability of A in returning a forged signature θ^* is $\epsilon_2 = \Pr[E_1] \Pr[E_2|E_1]$ which is computed as follows. First of all, we define events E_1 and E_2.

- E_1 : Algorithm C does not abort as a result of signature simulation.
- E_2: Adversary A returns a non-trivial forgery.

To lower-bound the probability $\Pr[E_1]$, we need to compute the probability $\Pr[\neg bad]$, where event bad indicate that C aborts in signature simulation as a result of any of A's Sign queries. This probability is computed as follows.

Claim 1. $\Pr[E_1] = \Pr[\neg bad] \geq 1 - q_s((q_s + q_{g_1})2^{-(n-k)}) - {q_s}^2 2^{-(n-k)}$.

Proof. The probability of the event E_1,

$\Pr[\neg bad]$, is multiplication of the following probabilities.

- Case 1. If the pair (α, M_1) generated in a Sign simulation has been occurred by chance in a previous query to the oracle $g_1(.,.)$, we have $bad \leftarrow true$. Since there are at most $q_{g_1} + q_s$ entries in the table $T_1[.,.]$ and the number of α, uniformly distributed in $\mathbb{F}_2^{n-k}$, is 2^{n-k}, the probability of this event for one Sign query is at most $(q_{g_1}+q_s)2^{-(n-k)}$. Hence, the probability of this event for q_s queries is at most $q_s(q_{g_1} + q_s)2^{-(n-k)}$.

- Case 2. If C previously used the same randomness r, uniformly distributed in $\mathbb{F}_2^{n-k}$, in one Sign simulation, we have $bad \leftarrow true$. Since there are at most q_s Sign simulations, this probability is at most $q_s 2^{-(n-k)}$. Therefore, for q_s Sign queries the probability of this event is at most ${q_s}^2 2^{-(n-k)}$.

Claim 2. $\Pr[E_2|E_1] \geq \epsilon_1$.

Proof. The value of $\Pr[E_2|E_1]$ is the probability that A returns a valid forgery provided that C does not abort as a result of A's Sign queries. If C did not abort as a result of A's queries, all its responses to those queries are valid. Therefore, by hypothesis A will produce a non-trivial forgery with probability at least ϵ_1.

Therefore, the probability that A returns a tuple (θ^*, g_0, g_1) is at least

$$\epsilon_1 - q_s(2q_s + q_{g_1})2^{-(n-k)}.$$

Since $g_0(.)$ and $g_1(.,.)$ are random oracles, the probability of the event that $g_0 = g_0(r)$ and $g_1 = g_1(\alpha^*, M_1^*)$ is less than $2^{-(n-k+1)}$, unless they are asked during the attack. Hence, in what follows it is likely that queries r^* and (α^*, M_1^*) are asked during a successful attack. The lower bound of probability of producing a non-trivial forgery after making queries to $g_0(.)$ and $g_1(.,.)$ oracles is at least

$$\epsilon_1 - q_s(2q_s + q_{g_1})2^{-(n-k)} - 2^{-(n-k+1)}.$$

Algorithm C employs A, guesses fixed indices $1 \leq i \leq q_{g_1}$ and $1 \leq j \leq q_{g_0}$ and hopes that i be the index of the query (α^*, M_1^*) to oracle $g_1(.,.)$ and j be the index of the query r^* to oracle $g_0(.)$ for which A forges a signature. Algorithm C chooses $\tilde{s} \xleftarrow{\$} \{0,1\}^{n-k}$, and responses with $M_2' \oplus \tilde{s} \oplus s^*$ for ith query and responses with $\tilde{s}$ for jth query. The probability of the former is $\frac{1}{q_{g_1}}$ and the probability of the latter is $\frac{1}{q_{g_0}}$. Since the tuple $(\alpha^*, x^*, M_1^*, g_0, g_1)$ is a valid signature, the weight of x^* is less than t and we have

$$H{x^*}^T \oplus g_1(\alpha^*, M_1^*) \oplus \alpha^* = {M'}_2^*$$

.

With substituting the values of $g_1(\alpha^*, M_1^*)$ and $g_0(r^*)$, we have

$$H{x^*}^T = g_1(\alpha^*, M_1^*) \oplus \alpha^* \oplus {M'}_2^* =$$
$$\tilde{s} \oplus {M'}_2^* \oplus \tilde{s} \oplus s^* \oplus {M'}_2^* = s^*$$

with probability at least

$$\frac{\epsilon_1 - q_s(2q_s + q_{g_1})2^{-(n-k)} - 2^{-(n-k+1)}}{q_{g_1} q_{g_0}},$$

where $\epsilon_1 = \epsilon - \epsilon_{GD}$. As a consequence, x^* is a t-decodable of s^*.

Algorithm C's run-time τ_{GPBD} is A's run-time, τ, plus the time required to respond to hash queries and q_s Sign queries. Each Sign simulation takes one syndrome computation whose cost is mt^2. Therefore, C's run-time is $\tau_{GPBD} \leq \tau + q_s(mt^2)$. This completes the proof. ■

Schemes	Public key Size	Sign Cost	Ver Cost	Signature Size
Our Scheme	$mt2^m$	$t!t^2m^3$	mt^2	$\log_2 \binom{2^m}{t}$ $+mt+$ $\lvert M\rvert - l_2$
Dallot Scheme [9]	$mt2^m$	$t!t^2m^3$	mt^2	$\log_2 \binom{2^m}{t}$ $+mt$ $+\lvert M\rvert$

TABLE I
COMPARISON BETWEEN OUR SCHEME AND DALLOT SCHEME

IV. COMPARISON

The comparison of our scheme and Dallot scheme [9] is summarized in Table I. The comparison is in terms of Public key size, Sign-Cost, Ver-Cost and Signature Size which Sign-Cost and Ver-Cost are dominating computational cost in signature generation and signature verification, respectively.

As shown in Table I, the proposed scheme is as efficient as Dallot scheme since the public key of the signer is a $n \times (n-k)$-parity check matrix H, where $n = 2^m$ and $n - k = mt$, so the size of public key is $mt2^m$. In addition, the signature generation in our scheme needs one decoding whose cost is about $t!$ and each of them requires t^2m^3 operations, so the signature generation takes $t!t^2m^3$ operations, and the signature

Scheme	Actual Signature Size
Our Scheme	479
Dallot Scheme [9]	578

TABLE II
SIGNATURE-SIZE COMPARISON (IN BITS)

verification requires one syndrome computing whose cost is mt^2, so the verification cost is about mt^2 binary operations.

As shown in Table I, the signature size of ours is reduced by a l_2-bit factor compared to the Dallot scheme since the signature in our scheme is (α, x, M_1), where x is a $n = 2^m$-bit vector such that $w_H(x) \leq t$, $\log_2 \binom{2^m}{t}$ bits are required to present it, $|M_1| = |M| - l_2$ and $|\alpha| = mt$. Therefore, the signature length of the proposed scheme is $\log_2 \binom{2^m}{t} + mt + |M| - l_2$, while the signature size in Dallot scheme [9] is $\log_2 \binom{2^m}{t} + mt + |M|$.

To make it clearer, we write signature size of the schemes in terms of bits in Table II. In what follows, it is assumed that (m, t) be $(22, 9)$ for the security level of $2^{81.4}$, $|M| = 200$ for short messages and $l_2 = 99$. With these parameters, the schemes are resistant against generalized birthday attack [35].
As shown in Tables I and II, our scheme is shorter than Dallot scheme, the only provably secure code-based signature scheme, while it has the same efficiency.

V. CONCLUSION

In this paper, we proposed a short code-based signature scheme with employing message recovery feature. It is shown that it is secure under Goppa Parametrized Bounded Decoding and the Goppa Code Distinguishing assumptions in the random oracle model. As shown in the comparison, the size of our signature is reduced compared to Dallot signature scheme since some parts of the original message are not transmitted with the signature. In addition, it has the same efficiency as the only provably secure code-based signature scheme (Dallot scheme). We should emphasize that this post-quantum primitive is useful where bandwidth is one of the crucial concern and also in case of signing short messages, and can be used as the building block of code-based signatures with additional properties such as ring or threshold ring signature schemes.

REFERENCES

[1] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. of the 35th Annual Symposium on Foundations of Computer Science*. Santa Fe, New Mexico, USA: IEEE, 20-22 November 1994, pp. 124–134.

[2] R. McEliece, "A public-key cryptosystem based on algebraic coding theory," *DSN Progress Report 42-44*, no. 2, pp. 114–116, 1978.

[3] O. Regev, "Lattice-based cryptography," in *Proc. of 26th Annual Int. Cryptology Conf. on Advances in Cryptology-CRYPTO 2006*. Santa Barbara, California, USA: Springer-Verlag, Berlin, 20-24 August 2006, pp. 131–141.

[4] D. Bernstein, J. Buchmann, and E. Dahmen, *Post-quantum cryptography*. Springer-Verlag, Berlin, 2009.

[5] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory," *Problems of Control and Information Theory*, vol. 15, no. 2, pp. 159–166, 1986.

[6] Y. Li, R. Deng, and X. M. Wang, "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems," *IEEE Transactions on Information Theory*, vol. 40, no. 1, pp. 271–273, 1994.

[7] N. T. Courtois, M. Finiasz, and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," in *Proc. of the 7th Int. Conf. on the Theory and Application of Cryptology and Information Security-Advances in Cryptology-ASIACRYPT 2001*. Gold Coast, Australia: Springer-Verlag, Berlin, 9-13 December 2001, pp. 157–174.

[8] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. of the 1st ACM Conf. on Computer and Communications Security (CCS 1993)*. Fairfax, VA, USA: ACM, New York, NY, 3-5 November 1993, pp. 62–73.

[9] L. Dallot, "Towards a concrete security proof of Courtois, Finiasz and Sendrier signature scheme," in *Proc. of the 2nd Western European Workshop on Research in Cryptology-WEWoRC 2007*. Bochum, Germany: Springer-Verlag, Berlin, 4-6 July 2008, pp. 65–77.

[10] E. Berlekamp, R. McEliece, and H. V. Tilborg, "On the inherent intractability of certain coding problems," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 384–386, 1978.

[11] N. Sendrier, "Cryptosystmes cl publique bass sur les codes correcteurs derreurs," in *Habilitation diriger les recherches, Universit Pierre et Marie Curie*, Paris, France (in French), March 2002.

[12] P. L. Cayrel, P. Gaborit, and M. Girault, "Identity-based identification and signature schemes using correcting codes," in *Proc. of the Int. Workshop on Coding and Cryptology (WCC 2007)*. Versailles, France: Springer-Verlag, Berlin, 16-20 April 2007, pp. 69–78.

[13] P. Barreto, R. Misoczki, and M. A. S. Jr, "One-time signature scheme from syndrome decoding over

generic error-correcting codes," *Journal of Systems and Software*, vol. 84, no. 2, pp. 198–204, 2011.

[14] D. Zheng, X. Li, and K. Chen, "Code-based ring signature scheme," *International Journal of Network Security*, vol. 5, no. 2, pp. 154–157, 2007.

[15] D. Wong, K. Fung, J. K. Liu, and V. Wei, "On the RS-code construction of ring signature schemes and a threshold setting of RST," in *Proc. of the 5th Int. Conf. on Information and Communications Security- ICICS 2003*. Huhehaote, China: Springer-Verlag, Berlin, 10-13 October 2003, pp. 34–36.

[16] C. Melchor, P. Cayrel, P. Gaborit, and F. Laguillaumie, "A new efficient threshold ring signature scheme based on coding theory," *IEEE Transactions on Information Theory*, vol. 57, no. 7, pp. 4833–4842, 2011.

[17] L. Dallot and D. Vergnaud, "Provably secure code-based threshold ring signatures," in *Proc. of the 12th Int. Conf. on the Cryptography and Coding*. Cirencester, UK: Springer-Verlag, Berlin, 15-17 December 2009, pp. 222–235.

[18] R. Overbeck, "A step towards QC blind signatures," 2009, IACR Cryptology ePrint Archive.

[19] K. P. Mathew, S. Vasant, and C. P. Rangan, "A provably secure signature and signcryption scheme using the hardness assumption in coding theory," in *Proc. of the 16th Int. Conf. on Information Security and Cryptology-ICISC 2013*. Seoul, Korea: Springer-Verlag, Berlin, 27-99 November 2013, pp. 99–119.

[20] C. Aguilar-Melchor, S. Bettaieb, P. Gaborit, and J. Schrek, "A code-based undeniable signature scheme," in *Proc. of the 14th IMA Int. Conf. on Cryptography and Coding-IMACC 2013*. Oxford, UK: Springer-Verlag, Berlin, 17-19 December 2013, pp. 99–119.

[21] M. Bellare and P. Rogaway, "The exact security of digital signatures-how to sign with RSA and Rabin," in *Proc. of the 15th Annual Int. Conf. on Theory and Application of Cryptographic Techniques, Advances in Cryptology EUROCRYPT 1996*. Zaragoza, Spain: Springer-Verlag, Berlin, 12-16 May 1996, pp. 399–416.

[22] *ISO/IEC 9796-1, Information technology Security techniques Digital signature scheme giving message recovery, Part 1: Mechanisms using redundancy*.

[23] *ISO/IEC 9796-2:2002, Information technology Security techniques Digital signature scheme giving message recovery, Part 2: Integer factorization based mechanisms*.

[24] *ISO/IEC 9796-2:2010, Information technology Security techniques Digital signature scheme giving message recovery, Part 2: Integer factorization based mechanisms*.

[25] K. Nyberg and R. Rueppel, "a new signature scheme based on the DSA giving message recovery," in *Proc. of the 1st ACM Conf. on Computer and Communications Security (CCS 1993)*. Fairfax, VA, USA: Springer-Verlag, Berlin, 3-5 November 1993, pp. 58–61.

[26] ——, "Message recovery for signature schemes based on the discrete logarithm problem," in *Proc. of Workshop on the Theory and Application of Cryptographic Techniques, Advances in Cryptology - EUROCRYPT 1994*. Perugia, Italy: Springer-Verlag, Berlin, 9-12 May 1995, pp. 182–193.

[27] ——, "Message recovery for signature schemes based on the discrete logarithm problem," *Designs, Codes and Cryptography*, vol. 7, no. 1, pp. 61–81, 1996.

[28] A. Miyaji, "A message recovery signature scheme equivalent to DSA over elliptic curves," in *Proc. of the Int. Conf. on the Theory and Applications of Cryptology and Information Security, Advances in Cryptology ASIACRYPT 1996*. Kyongju, Korea: Springer-Verlag, Berlin, 3-7 November 1996, pp. 1–14.

[29] M. Abe and T. Okamoto, "A signature scheme with message recovery as secure as discrete logarithm," in *Proc. of the Int. Conf. on the Theory and Application of Cryptology and Information Security, Advances in Cryptology ASIACRYPT 1999*. Singapore, Singapore: Springer-Verlag, Berlin, 14-18 November 1999, pp. 378–389.

[30] J. Coron, D. Naccache, and J. Stern, "On the security of RSA padding," in *Proc. of 19th Annual Int. Cryptology Conf. on Advances in Cryptology-CRYPTO 1999*. Santa Barbara, California, USA: Springer-Verlag, Berlin, 15-19 August 1999, pp. 1–18.

[31] D. Coppersmith, J. S. Coron, F. Grieu, S. Halevi, C. Jutla, D. Naccache, and J. P. Stern, "Cryptanalysis of ISO/IEC 9796-1," *Journal of Cryptology*, vol. 21, no. 1, pp. 27–51, 2008.

[32] D. Bleichenbacher, "Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1," in *Proc. of 18th Annual Int. Cryptology Conf. on Advances in Cryptology-CRYPTO 1998*. Santa Barbara, California, USA: Springer-Verlag, Berlin, 23-27 August 1998, pp. 1–12.

[33] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[34] M. Finiasz, "Nouvelles constructions utilisant des codes correcteurs derreurs en cryptographie clef publique," in *These de doctorat, cole Polytechnique*, Paris, France (in French), October 2004.

[35] M. Finiasz and N. Sendrier, "Security bounds for the design of code-based cryptosystems," in *Proc. of the 15th Int. Conf. on the Theory and Application of Cryptology and Information Security-Advances in Cryptology-ASIACRYPT 2009*. Tokyo, Japan: Springer-Verlag, Berlin, 6-10 December 2009, pp. 88–105.

Maryam Rajabzadeh Asaar received her B.S. degree in Electrical Engineering from Shahid Bahonar University of Kerman, Kerman, Iran, in 2004, and received her M.S. and Ph.D. degrees in Electrical Engineering from Sharif University of Technology, Tehran, Iran in 2008 and 2014, respectively. She is currently a postdoctoral researcher at Electronics Research Institute of Sharif University of Technology. Her research interests include provable security, digital signatures, design and analysis of cryptographic protocols and network security and security in industrial control systems.

Mahmoud Salmasizadeh received the B.S. and M.S. degrees in electrical engineering from Sharif University of Technology, Tehran, Iran, in 1972 and 1989, respectively. He also received the Ph.D. degree in information technology from Queensland University of Technology, Australia, in 1997. Currently, he is an associate professor in the Electronics Research Institute and adjunct associate professor in the Electrical Engineering Department, Sharif University of Technology. His research interests include design and cryptanalysis of cryptographic algorithms and protocols, e-commerce security, and information theoretic secrecy. He is a founding member of Iranian Society of Cryptology

Mohhamd Reza Aref received the B.S. degree in 1975 from the University of Tehran, Iran, and the M.S. and Ph.D. degrees in 1976 and 1980, respectively, from Stanford University, Stanford, CA, USA, all in electrical engineering. He returned to Iran in 1980 and was actively engaged in academic affairs. He was a Faculty member of Isfahan University of Technology from 1982 to 1995. He has been a Professor of electrical engineering at Sharif University of Technology, Tehran, since 1995, and has published more than 230 technical papers in communication and information theory and cryptography in international journals and conferences proceedings. His current research interests include areas of communication theory, information theory, and cryptography.