Journal of Innovative Applied Mathematics and Computational Sciences

J. Innov. Appl. Math. Comput. Sci. **3**(1) (2023), 15–27. DOI: 10.58205/jiamcs.v3i1.129

http://jiamcs.centre-univ-mila.dz/

A new directed signature scheme on a general linear group over a group ring

Sassia Makhlouf [1]✉, Kenza Guenda [2] and Thomas Aaron Gulliver [3]

[1]Faculty of Economics, Commercial and Management Sciences, University of Batna 1, Batna, Algeria
[2]Faculty of Mathematics, University of Science and Technology Houari Boumediene, Algiers, Algeria
[3]Department of Electrical and Computer Engineering, University of Victoria, PO Box 1700, STN CSC, Victoria, BC, Canada V8W 2Y2

Received 29 March 2023, Accepted 5 May 2023, Published 6 May 2023

Abstract. In this work, we propose a new directed digital signature scheme over a group ring whose security relies on the hardness of the discrete logarithm problem and the factorization search problem. This scheme is efficient as it requires very few operations for both signing and verifying signatures. Furthermore, the security of the proposed scheme is examined.

Keywords: Directed signature, discrete logarithm problem, factorization search problem, group ring.
2020 Mathematics Subject Classification: 94A60, 15B33 , 20G35, 20G45.

1 Introduction

Digital signatures are among the most important applications in modern cryptography and information security as they provide data authentication and confidentiality. They were introduced by Diffie and Hellman in 1976 [3]. In this approach [6,16], a signer uses a private key to sign messages and their public key is used to verify the signatures. However, signed messages, such as business transactions and medical records, may be sensitive and thus should be protected against unauthorized access or alteration of the signature. To address this weakness, the concept of directed digital signatures was introduced [10]. With directed signatures, only the designated verifier can verify the signature. Furthermore, it is necessary that both the designated verifier and signer can prove to any third party that the signature is valid. The security of these signatures is based on the intractability of hard mathematical problems, such as the Discrete Logarithm Problem (DLP) and Integer Factorization Problem (IFP). Several directed signature schemes have been proposed using algebraic structures such as linear groups, non-abelian groups, and rings [1,2,8,18].

✉Corresponding author. Email: sassia.makhlouf@univ-batna.dz

ISSN (electronic): 2773-4196

In [14], the non-abelian group of matrices $GL_n(\mathbb{F}_q)$ was used for Diffie-Hellman key exchange. It was proven in [11] that the DLP over matrix groups can be reduced to the DLP over $\mathbb{F}_q^*$. Properties of matrices such as Cayley-Hamilton, and determinants and eigenvalues have been used to develop attacks against schemes that use $GL_n(\mathbb{F}_q)$ [4, 11, 12]. It was suggested in [4,9] to employ the group of invertible matrices over the group ring $GL_n(\mathbb{F}_q[S_r])$ and the semi-group of matrices over the group ring $M_{k\times k}(\mathbb{F}_q[S_r])$ to avoid such attacks. The security is based on the difficulty of the DL problem in the (semi-) group of matrices. A cryptanalysis of protocols based on the DL problem on (semi-) groups of matrices over group rings was given in [5]. In [8], the Factorization with Discrete Logarithm Problem (FDLP) over the non-abelian semi-group $M_{k\times k}(\mathbb{F}_q[S_r])$ was introduced. This scheme resists the above attacks. Using this new hard problem, we propose a new directed digital signature scheme whose security relies on the hardness of the FDLP on a group of invertible matrices over a group ring.

The rest of this paper is organized as follows. Section 2 gives some necessary definitions for the proposed signature scheme. In section 3, we describe the key exchange protocol based on FDLP proposed in [8] and then the new directed signature scheme is presented in section 4. The security of this scheme is examined in section 5. Finally, section 6 concludes the paper.

2 Preliminaries

In this section, we provide some useful definitions.

Definition 2.1 (Discrete Logarithm Problem (DLP) [11, 19])**.** Let G be a finite cyclic group of order n with generator g, and $y \in G$. Then the discrete logarithm problem is to find an integer k, $0 \leqslant k < n$, such that $g^k = y$.

Definition 2.2 (Factorization Search Problem (FSP) [13])**.** Given an element $x \in G$ and two subgroups A and B of G, the factorization search problem is to find $a \in A$ and $b \in B$ such that $ab = x$.

In [8], a combination of the above two problems was used to introduce the factorization with discrete logarithm problem.

Definition 2.3 (Factorization with Discrete Logarithm Problem (FDLP) [8])**.** Let G be a finite non-commutative group of order n. Given $x, y \in G$, the factorization with discrete logarithm problem is to find $z \in G$ and $t \in \mathbb{Z}$ such that $x = y^t z$.

If the secret parameter z is known, then the FDLP reduces to the DLP. The FDLP can also be considered as an FSP where the two unknown factors of x are $a = y^t$ and $b = z$.

The complexity of the FDLP and the security of cryptosystems based on the FDLP are discussed in [8]. The well-known determinant, eigenvalue [4], and Cayley-Hamilton [12] attacks are not applicable to the FDLP.

Definition 2.4 (Group rings)**.** Let G be a multiplicative group, not necessarily finite, and let $\mathbb{F}$ be a field. The group ring of G over $\mathbb{F}$, denoted $\mathbb{F}[G]$, is defined to be the set of all linear combinations

$$\alpha = \sum_{g\in G} a_g g,$$

where $a_g \in \mathbb{F}$.

We define the sum and product of two elements in $\mathbb{F}[G]$ by

$$\Big(\sum_{g\in G} a_g g\Big) + \Big(\sum_{g\in G} b_g g\Big) = \sum_{g\in G} \Big(a_g + b_g\Big) g,$$

and

$$\begin{array}{rcl} \left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} d_h h\right) & = & \sum_{g,h\in G} a_g d_h (gh) \\ & = & \sum_{u\in G} c_u u, \end{array}$$

where

$$gh = u,$$

and

$$c_u = \sum_{gh=u} a_g d_h.$$

For example, consider the group ring $\mathbb{F}_7[S_5]$ with identity e and let $a, b \in \mathbb{F}_7[S_5]$ such that

$$\begin{array}{rcl} a & = & 4(241) + 2(24)(35), \\ b & = & 6(241) + (21)(45) + 4(2435). \end{array}$$

Then

$$\begin{array}{rcl} a^2 & = & 2(142) + (12)(35) + (14)(35) + 4(1), \\ a+b & = & 3(241) + 2(24)(35) + (21)(45) + 4(2435), \\ ba & = & [4(241) + 2(24)(35)]\,[6(241) + (21)(45) + 4(2435)] \\ & = & 3(142) + 5(12)(35) + 4(254) + 2(12534) + 2(14)(235) + (23). \end{array}$$

Consider $M_{2\times 2}(\mathbb{F}_7[S_5])$, the semi-group of 2×2 matrices over the group ring $\mathbb{F}_7[S_5]$ under matrix multiplication. Let $A, B \in M_{2\times 2}(\mathbb{F}_7[S_5])$ such that

$$A = \begin{pmatrix} a & 0 \\ b & e \end{pmatrix},\ B = \begin{pmatrix} a & e \\ e & b \end{pmatrix}.$$

Then

$$\begin{array}{rcl} AB & = & \begin{pmatrix} a^2 & a \\ ba+e & 2b \end{pmatrix} \\ & = & \begin{pmatrix} a^2 & 4(241) + 2(24)(35) \\ ba+e & 5(241) + 2(21)(45) + (2435) \end{pmatrix}, \end{array}$$

where ba and a^2 are as given above. For more details concerning group rings, refer to [15].

3 A key exchange protocol based on the FDLP

In [8], a key exchange protocol was proposed based on the FDLP using matrices over the group ring $M_{k\times k}(\mathbb{F}_q[S_r])$. Let $G = M_{k\times k}(\mathbb{F}_q[S_r])$ be a finite non-abelian semi-group and H be an abelian sub-semi-group of G. Let $T \in G$, $C_G(T)$ the centralizer of T in G, and $\mathbb{F}_m = \{0, 1, \ldots, m-1\}$ where m is a large positive integer. The groups G, H, T, and m are publicly known. The protocol is as follows.

1. Alice chooses a random secret integer $a \in \mathbb{F}_m$ and a secret element $M_1 \in H \setminus C_G(T)$. She computes $A_1 = T^a M_1$ and sends it to Bob.

2. Bob chooses a random secret integer $b \in \mathbb{F}_m$ and a secret element $M_2 \in H \setminus C_G(T)$. He computes $A_2 = T^b M_2$ and sends it to Alice.

3. Alice computes $k_A = T^a A_2 M_1$.

4. Bob computes $k_B = T^b A_1 M_2$.

Since $M_1 M_2 = M_2 M_1$, then

$$\begin{aligned} k_A &= T^a A_2 M_1 = T^a T^b M_2 M_1 \\ &= T^b T^a M_1 M_2 = T^b A_1 M_2 = k_B. \end{aligned}$$

Thus, after Step 4, Alice and Bob share the same secret key $k = k_A = k_B$.

The security of this key exchange protocol is based on the hardness of the factorization with discrete logarithm problem over the non-commutative semi-group $M_{k\times k}\left(\mathbb{F}_q\left[S_r\right]\right)$. The complexity and security analysis of the protocol were given in [8]. The following attacks were considered: attacks using the properties of matrices [4, 12], attacks using the decomposition of group rings [5], and attacks on the DLP and linear algebra. It was shown in [8] that for small values of q and r, the complexity is high.

In this paper, this new hard problem is used to develop a new scheme that resists the above attacks. We consider the group of invertible matrices over the group ring $GL_2\left(\mathbb{F}_q\left[S_r\right]\right)$. From [4, Lemma 4.1.1], we have

$$|GL_2\left(\mathbb{F}_q\left[S_r\right]\right)| = q^8(q-1)^8(q+1)^4(q^2+1)(q^2+q+1),$$

so then

$$|GL_2\left(\mathbb{F}_q\left[S_r\right]\right)| > q^{16}.$$

Thus, even for small values of q and r, the security can be high as the complexity of the FDLP over $GL_2\left(\mathbb{F}_q\left[S_r\right]\right)$ is very high.

The main advantage of using $GL_n\left(\mathbb{F}_q\left[S_r\right]\right)$ is that matrix multiplication is very efficient [17] and the square and multiply algorithm can be used for exponentiation [9]. These groups are resistant to attacks, such as determinant and eigenvalue attacks [4]. This has been verified in [9].

4 Proposed directed signature scheme

In this section, a new directed signature scheme is proposed based on the group of invertible matrices over a group ring and the FDLP. This scheme involves the following steps.

4.1 Initialization

Suppose that Alice (A) wants to generate a signature on a message M and send it to Bob (B) for verification. Let $G = GL_n\left(\mathbb{F}_q\left[S_r\right]\right)$ be the group of $n \times n$ invertible matrices over the group ring $\mathbb{F}_q\left[S_r\right]$ and L an abelian subgroup of G. Let $X \in G$ which has large positive integer order m, $C_G(X)$ the centralizer of X in G, and H be a one-way hash function. The groups G, L, X, and m and H are publicly known.

4.2 Key generation

a. Alice chooses a secret integer $t \in \{2, 3, \ldots, m-1\}$ and a random matrix $U \in L \setminus C_G(X)$. She computes $Y_A = X^t U$ and then takes (t, U) as her private key and $Y_A = X^t U$ as her public key.

b. Bob chooses a secret integer $s \in \{2, 3, \ldots, m-1\}$ and a random matrix $P \in L \setminus C_G(X)$. He computes $Y_B = X^s P$ and then takes (s, P) as his private key and $Y_B = X^s P$ as his public key.

4.3 Signature generation

a. The signer (Alice) randomly selects another matrix $V \in L \setminus C_G(X)$ and a secret integer $r \in \{2, 3, \ldots, m-1\}$. She then computes

$$\begin{aligned} R &= X^r V, \\ S_A &= X^r Y_B V k^{-1}, \end{aligned}$$

where k denotes the shared secret key.

b. Using the one-way hash function H and message M, Alice computes

$$W_A = H(S_A, M),$$

and sends $\{W_A, R, M\}$ to Bob as her signature for M.

4.4 Signature verification

Once the signature $\{W_A, R, M\}$ is received from Alice, Bob computes

$$\begin{aligned} T &= R Y_A^{-1}, \\ S_B &= X^s T X^{-s}, \\ W_B &= H(S_B, M). \end{aligned}$$

Bob accepts the signature if and only if

$$W_A = W_B.$$

Otherwise, the signature is rejected.

4.5 Proof of validity to a third party (C)

In the proposed scheme, a third party (C) can verify the signature with the help of the designated verifier or signer. We describe below the protocol by which the designated verifier or signer can prove the validity of the signature.

4.5.1 Proof of validity by (A) to (C)

a. Alice selects a random secret matrix $D \in L \setminus C_G(X)$ and a secret integer $d \in \{2, 3, \ldots, m-1\}$, and computes $\sigma = X^d D$.

b. Alice computes $\lambda = X^d Y_C D S_A$ and sends (σ, λ) to (C) whose public key is $Y_C = X^z Q$.

c. (C) receives (σ, λ) and using their public key computes $S_C = (X^z \sigma Q)^{-1} \lambda$. Then, (C) checks $W_A = H(S_C, M)$, and if it holds accepts the validity of the signature.

The proof of Step c follows from

$$\begin{aligned}(X^z \sigma Q)^{-1} \lambda &= \left(X^z X^d D Q\right)^{-1} X^d Y_C D S_A \\ &= \left(X^{z+d} D Q\right)^{-1} X^d Y_C D S_A \\ &= \left(X^d Y_C D\right)^{-1} X^d Y_C D S_A = S_A.\end{aligned}$$

4.5.2 Proof of validity by (B) to (C)

a. Bob selects a random secret matrix $E \in L \setminus C_G(X)$ and a secret integer $g \in \{2, 3, \ldots, m-1\}$, and computes $\gamma = X^g E$.

b. Bob computes $\delta = X^g Y_C E S_B$ and sends (γ, δ) to (C).

c. (C) receives (γ, δ), and using their public key computes $S_C = (X^z \gamma Q)^{-1} \delta$. Then, (C) checks $W_A = H(S_C, M)$, and if it holds accepts the validity of the signature.

The proof of Step c follows from

$$\begin{aligned}(X^z \gamma Q)^{-1} \delta &= (X^z X^g E Q)^{-1} X^g Y_C E S_B \\ &= \left(X^{z+g} E Q\right)^{-1} X^g Y_C E S_B \\ &= (X^g Y_C E)^{-1} X^g Y_C E S_B = S_B.\end{aligned}$$

5 Example

5.1 Initialization

Consider $GL_2(\mathbb{F}_5[S_3])$ and $L = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbb{F}_5[S_3] \right\}$, and let $X = \begin{pmatrix} 3\alpha^2 & 0 \\ 0 & 1 \end{pmatrix}$ where $S_3 = \langle \alpha, \beta \mid \alpha^3 = 1, \beta^2 = 1 \rangle$, and $m = 12$.

5.2 Key generation

Alice randomly chooses $t = 2$ and $U = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$, and calculates

$$Y_A = X^2 U = \begin{pmatrix} 4\alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 4\alpha & 4\alpha\beta \\ 0 & 1 \end{pmatrix}.$$

Then $\left(2, \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}\right)$ is her private key and $Y_A = \begin{pmatrix} 4\alpha & 4\alpha\beta \\ 0 & 1 \end{pmatrix}$ is her public key.

Similarly, Bob randomly chooses $s = 3$ and $P = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, and calculates

$$Y_B = X^3 P = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2\alpha \\ 0 & 1 \end{pmatrix}.$$

Then $\left(3, \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}\right)$ is his private key and $Y_B = \begin{pmatrix} 2 & 2\alpha \\ 0 & 1 \end{pmatrix}$ is his public key.

The shared secret key is

$$k_A = X^2 Y_B U = \begin{pmatrix} 4\alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 2\alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3\alpha & 3\alpha\beta + 3\alpha^2 \\ 0 & 1 \end{pmatrix},$$

and

$$k_B = X^3 Y_A P = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 4\alpha & 4\alpha\beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3\alpha & 3\alpha^2 + 3\alpha\beta \\ 0 & 1 \end{pmatrix},$$

as $k = k_A = k_B$.

5.3 Signature generation

Alice also randomly chooses $r = 5$ and $V = \begin{pmatrix} 1 & \alpha\beta \\ 0 & 1 \end{pmatrix}$, and computes

$$\begin{aligned} R &= X^5 V \\ &= \begin{pmatrix} 3\alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha\beta \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 3\alpha & 3\alpha^2\beta \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

and

$$\begin{aligned} S_A &= X^r Y_B V k^{-1} \\ &= \begin{pmatrix} 3\alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 2\alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha\beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2\alpha^2 & 4\alpha + 4\beta \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 4\alpha\beta + \alpha^2\beta \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

where $k^{-1} = \begin{pmatrix} 2\alpha^2 & 4\alpha + 4\beta \\ 0 & 1 \end{pmatrix}$.

Let the hash function be

$$H\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}\right) = \begin{pmatrix} \sum a_{1i} & \sum b_{1i} \\ \sum a_{2i} & \sum b_{2i} \end{pmatrix},$$

and let $M = \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$ be the message. Then Alice computes

$$\begin{aligned} W_A &= H(S_A, M) \\ &= H\left(\begin{pmatrix} 2 & 4\alpha\beta + \alpha^2\beta \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}\right) \\ &= \begin{pmatrix} 2 + 4\alpha\beta + \alpha^2\beta & \alpha + \beta \\ 1 & 1 \end{pmatrix}, \end{aligned}$$

and sends $\{W_A, R, M\}$, i.e.

$$\left\{\begin{pmatrix} 2 + 4\alpha\beta + \alpha^2\beta & \alpha + \beta \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 3\alpha & 3\alpha^2\beta \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}\right\},$$

as her signature on the message M.

5.4 Signature verification

For verification, Bob computes

$$\begin{aligned} T &= R\,Y_A^{-1} \\ &= \begin{pmatrix} 3\alpha & 3\alpha^2\beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 4\alpha^2 & 4\beta \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 2\alpha\beta + 3\alpha^2\beta \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

and

$$\begin{aligned} S_B &= X^s\,T\,X^{-s} \\ &= \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 2\alpha\beta + 3\alpha^2\beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 4\alpha\beta + \alpha^2\beta \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

where $X^{-1} = \begin{pmatrix} 2\alpha & 0 \\ 0 & 1 \end{pmatrix}$ and

$$\begin{aligned} W_B &= H\,(S_B,\, M) \\ &= H\left(\begin{pmatrix} 2 & 4\alpha\beta + \alpha^2\beta \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \right) \\ &= \begin{pmatrix} 2 + 4\alpha\beta + \alpha^2\beta & \alpha + \beta \\ 1 & 1 \end{pmatrix}. \end{aligned}$$

Bob accepts the signature as

$$W_A = W_B.$$

5.5 Proof of validity by (A) to (C)

Alice randomly chooses $d = 6$ and $D = \begin{pmatrix} 1 & 2\beta \\ 0 & 1 \end{pmatrix}$, and calculates

$$\sigma = X^6 D = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2\beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 3\beta \\ 0 & 1 \end{pmatrix}.$$

(C) randomly chooses $z = 7$ and $Q = \begin{pmatrix} 1 & 3\alpha \\ 0 & 1 \end{pmatrix}$, and calculates

$$Y_C = X^7 Q = \begin{pmatrix} 2\alpha^2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3\alpha \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2\alpha^2 & 1 \\ 0 & 1 \end{pmatrix}.$$

Alice computes

$$\begin{aligned} \lambda &= X^d\,Y_C\,D\,S_A \\ &= \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2\alpha^2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2\beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 4\alpha\beta + \alpha^2\beta \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} \alpha^2 & 2\beta + 3\alpha\beta + \alpha^2\beta + 4 \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

and sends (σ, λ) to (C).

(C) receives (σ, λ) and computes

$$\begin{aligned} S_C &= (X^z \sigma Q)^{-1} \lambda \\ &= \begin{pmatrix} 2\alpha & 2\alpha + 3\beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha^2 & 2\beta + 3\alpha\beta + \alpha^2\beta + 4 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 4\alpha\beta + \alpha^2\beta \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

where $X^z \sigma Q = \begin{pmatrix} 3\alpha^2 & 4 + \alpha^2\beta \\ 0 & 1 \end{pmatrix}$. The validity of the signature is checked by computing

$$\begin{aligned} W_A &= H(S_C, M) \\ &= H\left(\begin{pmatrix} 2 & 4\alpha\beta + \alpha^2\beta \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}\right) \\ &= \begin{pmatrix} 2 + 4\alpha\beta + \alpha^2\beta & \alpha + \beta \\ 1 & 1 \end{pmatrix}. \end{aligned}$$

As this is true, (C) accepts the validity of the signature.

5.6 Proof of validity by (B) to (C)

Bob randomly chooses $g = 8$ and $E = \begin{pmatrix} 1 & 2\alpha \\ 0 & 1 \end{pmatrix}$, and calculates

$$\gamma = X^8 E = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2\alpha \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & 2\alpha^2 \\ 0 & 1 \end{pmatrix},$$

and

$$\begin{aligned} \delta &= X^g Y_C E S_B \\ &= \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2\alpha^2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2\alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 4\alpha\beta + \alpha^2\beta \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 4 & 3\alpha\beta + 2\alpha^2\beta \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Then, Bob sends (γ, δ) to (C).

(C) receives (γ, δ) and computes

$$\begin{aligned} S_C &= (X^z \gamma Q)^{-1} \delta \\ &= \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 4 & 3\alpha\beta + 2\alpha^2\beta \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 4\alpha\beta + \alpha^2\beta \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

where $X^z \gamma Q = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. The validity of the signature is checked by computing

$$\begin{aligned} W_A &= H(S_C, M) \\ &= H\left(\begin{pmatrix} 2 & 4\alpha\beta + \alpha^2\beta \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}\right) \\ &= \begin{pmatrix} 2 + 4\alpha\beta + \alpha^2\beta & \alpha + \beta \\ 1 & 1 \end{pmatrix}. \end{aligned}$$

As this is true, (C) accepts the validity of the signature.

6 Confirmation and security

6.1 Completeness

Theorem 6.1. *The verification protocol is complete if the verifier can always verify the equality* $W_A = W_B$.

Proof. Let $\{W_A, R, M\}$ be a valid signature generated by Alice. If she has followed the signature verification algorithm, then Bob will always accept $\{W_A, R, M\}$ as a valid signature. In verification, the parameters are R, M, and S_B.

Bob computes

$$\begin{aligned} T &= RY_A^{-1} \\ &= X^r V U^{-1} X^{-t}, \end{aligned}$$

and

$$\begin{aligned} S_B &= X^s T X^{-s} \\ &= X^s X^r V U^{-1} X^{-t} X^{-s} \\ &= X^{s+r} V U^{-1} X^{-s-t}. \end{aligned}$$

Since U, V, and P are commutative

$$\begin{aligned} S_B &= X^{s+r} V U^{-1} P P^{-1} X^{-s-t} \\ &= X^{s+r} P V U^{-1} P^{-1} X^{-s-t} \\ &= X^r X^s P V U^{-1} P^{-1} X^{-s} X^{-t} \\ &= X^r Y_B V k^{-1} \\ &= S_A, \end{aligned}$$

so $S_A = S_B$. Then, Bob computes $H(S_B, M)$, which is always equal to W_A and thus accepts $\{W_A, R, M\}$ as valid signature. Thus, if $\{W_A, R, M\}$ is a valid signature generated by Alice, and Alice and Bob have followed the protocol, then Bob can always authenticate the message M. □

Theorem 6.2. *The proposed signature scheme is a directed signature scheme.*

Proof. To verify the signature $\{W_A, R, M\}$ requires

$$S_B = X^s T X^{-s}.$$

Thus, verification requires the private key s of the verifier, so only Bob can verify the signature. □

6.2 Security analysis

In this subsection, we study the security of the proposed signature scheme. This security is based on the FDLP which is computationally hard. Assume that an adversary (E) can obtain, remove, forge, and retransmit any message sent by Alice to Bob. Any forged data is denoted by d^F. We consider the security against four well-known attacks.

6.2.1 Total break

This is as difficult as solving the FDLP on a non-commutative group of invertible matrices over a group ring. For example, using Alice's public key $Y_A = X^t U$, obtaining the private key (t, U) is intractable as the FDLP on a non-commutative group is very hard [8].

6.2.2 Data forging

Suppose that (E) replaces the original message M with a forged message M^F. Then Bob receives the signature $\{W_A, R, M^F\}$ and computes

$$W_B = H\left(S_B, M^F\right).$$

However, verification fails because

$$H\left(S_A, M\right) \neq H\left(S_B, M^F\right),$$

and $W_A = W_B$ is true only for the original message with high probability.

Another approach is to obtain M^F for a valid S_A. This is intractable because it is assumed that the hash function H is cryptographically secure, so finding S_A is very hard based on the FDLP. Thus, M^F cannot be signed to obtain a valid signature.

6.2.3 Signature repudiation

In the proposed scheme, Alice is the only one with the private key (t, U), thus she cannot deny having signed her signature. Assume that Alice intends to refute that she has signed a message M. Then it follows that the valid signature $\{W_A, R, M\}$ can be changed to $\{W_A^F, R^F, M\}$. The designated verifier Bob computes

$$T^F \;=\; R^F\, Y_A^{-1},$$

and

$$S_B^F \;=\; X^s\, T^F\, X^{-s}.$$

He then checks the validity of the signature using

$$W_B = H\left(S_B^F, M\right) \neq W_A^F,$$

this computation requires parameters based on the FDLP problem, so it is intractable for someone to find the private key (t, U). Thus, this signature scheme ensures the non-repudiation property.

6.2.4 Existential forgery

Existential forgery is defined in [7]. An attacker may try to impersonate the designated signer Bob by randomly selecting a matrix $V_1 \in L \setminus C_G(X)$ and an integer $r_1 \in \{2, 3, \ldots, m-1\}$, and then calculating

$$R = X^{r_1} V_1.$$

However, without knowing the secret key k, it is difficult to generate valid

$$S_A \;=\; X^{r_1} Y_B\, V_1\, k^{-1},$$

and

$$W_A \;=\; H\left(S_A, M\right),$$

for a message M such that the verification equation

$$W_A = W_B,$$

is satisfied. Thus, it is intractable to construct a valid signature without knowing the private key, so (E) is not able to calculate forged signatures.

7 Conclusion

In this paper, a new directed signature scheme based on FDLP was proposed using the group of invertible matrices over the group ring $\mathbb{F}_q[S_r]$ under the usual matrix multiplication. The security of the proposed scheme is based on the intractability of the FDLP. It was shown that this signature scheme is secure against data forgery, signature repudiation, and existential forgery. It is also secure against total break as the private and public keys are based on the FDLP.

References

[1] R. Alvarez, F-M. Martinez, J-F. Vicent and A. Zamora, *A new public key cryptosystem based on matrices*, in: Proc. WSEAS Int. Conf. on Inform. Security and Privacy, 2007, 36–39. URL

[2] J. J. Climent, P. R. Navarro and L. Tortosa, *Key exchange protocols over noncommutative rings The case of End$(Zp \times Zp2)$*, International Journal of Computer Mathematics, **89**(13-14) (2012), 1753–1763. DOI

[3] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory, **22**(6) (1976), 644–654. DOI

[4] M. Eftekhari, *A Diffie–Hellman key exchange protocol using matrices over non-commutative rings*, Journal of Groups, Complexity, Cryptology, **4**(1) (2012), 167–176. DOI

[5] M. Eftekhari, *Cryptanalysis of some protocols using matrices over group rings*, in: Proc. Int. Conf. on Cryptology in Africa, Lecture Notes in Computer Science, **10239** (2017), 223–229. DOI

[6] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory, **31**(4) (1985), 469–472. DOI

[7] S. Goldwasser, S. Micali and R. L. Rivest, *A digital signature scheme secure against adaptive chosen-message attacks*, SIAM Journal on Computing, **17**(2) (1988), 281–308. DOI

[8] I. Gupta, A. Pandey and M. K. Dubey, *A key exchange protocol using matrices over group ring*, Asian-European Journal of Mathematics, **12**(05) (2019), 1950075. DOI

[9] D. Kahrobaei, C. Koupparis and V. Shpilrain, *Public key exchange using matrices over group rings*, Journal of Groups, Complexity, Cryptology, **12**(1) (2013), 97–115. DOI

[10] C. H. Lim and P.J. Lee, *Modified Maurer-Yacobi's scheme and its applications*, in: Proc. Int. Workshop on the Theory and Application of Cryptographic Techniques, Lecture Notes in Computer Science, **718** (1982), 308–323. DOI

[11] A. J. Menezes and Y-H. Wu, *The discrete logarithm problem in $GL(n, q)$*, Ars Combinatoria, **47** (1997), 23–32. DOI

[12] G. Micheli, *Cryptanalysis of a non-commutative key exchange protocol*, Advances in Mathematics of Communications, **9**(2)(2015), 247–253. DOI

[13] A. Myasnikov, V. Shpilrain and A. Ushakov, *Non-commutative Cryptography and Complexity of Group-theoretic Problems*, Math. Surveys Monogr., Vol. 177, Am. Math. Soc., Providence, RI, USA, 2011. URL

[14] R. W. K. Odoni, V. Varadharajan and P. W. Sanders, *Public key distribution in matrix rings*, Electronics Letters , **20**(9) (1984), 386–387. DOI

[15] D. S. Passman, *The Algebraic Structure of Group Rings*, Wiley, New York, NY, USA, 1977. URL

[16] R. L. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, **21**(2) (1978), 120–126. DOI

[17] J. H. Silverman, *Fast multiplication in finite fields GF(2^N)*, in: Proc. Int. Workshop on Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, **1717** (1999), 122–134. DOI

[18] N. R. Wagner and M. R. Magyarik, *A public-key cryptosystem based on the word problem*, in: Proc. Workshop on the Theory and Application of Cryptographic Techniques, Lecture Notes in Computer Science, **196** (1984), 19–36. DOI

[19] S. Wei, *A new digital signature scheme based on factoring and discrete logarithms*, In: Chen, K. (eds) Progress on Cryptography. The International Series in Engineering and Computer Science, **769** (2004), 107–111. DOI