Commun. Combin., Cryptogr. & Computer Sci., 1 (2022), 62–70

ISSN:2783-5456

Communications in Combinatorics, Cryptography & Computer Science

Journal Homepage: http://cccs.sgh.ac.ir

A Secure Cryptosystem in Group Signature Scheme Based Over Group Ring

Nur Afiqah Suzelan Amir[a,*], Wan Ainun Mior Othman[a], Wong Kok Bin[a]

[a]Institute of Mathematical Sciences, Faculty of Science, University of Malaya 50603, Kuala Lumpur, Malaysia

Abstract

Due to its significant application in information security, cryptography is a mathematical field that is rapidly growing. To safeguard any transactions over an insecure medium, a secure protocol is essential. Secure file transfer protocols must protect the information via group signature in order to maintain data confidentiality and privacy during transmission. Under the group signature scheme, a member of the group signs a message on behalf of the group. Signatures can be checked with regard to a specific public key group, but does not disclose the identity of the signatory. However, it is challenging to preserve the privacy between two parties and maintain the reliability of the message broadcast. In our study, we construct an efficient group signature where the underlying work is based on generic linear group over group rings. The security evaluations show that our protocol improves performance efficiency.

Keywords: group ring, generic linear group, authentication, group signature.

2020 MSC: 20C05, 94A60, 94A62.

1. Introduction

David Chaum and Eugene van Heyst first introduced the idea of a group signature method in 1991 [34]. Group signatures enable each member to sign on the group's behalf. Even if they are unable to connect the signature to a specific signer, a verifier can determine that the signer is a member of a group. However, the user anonymity may be revoked by a trusted person (TP). When a group signature enables a TP to recognise the signature of a malicious user, the traceability feature is met. On the other side, if a trusted party colludes, all network users become susceptible to an adversary or malicious parties. The need to protect a user's anonymity causes a contradiction between accountability and privacy in this circumstance. Message reliability, privacy, and accountability are the security requirements conflict with group signatures even though they satisfy all security standards. In order to achieve higher performance efficiency in group signatures where the underlying work is based on group ring, we propose a well-balanced security and privacy requirement in light of the shortcomings conflicting security requirements. The Diffie-Hellman (DH) allow the exchange of a secret key via an insecure channel between two parties who have never met, the DH key agreement protocol, which was first conceptualised in 1976, offers a workable solution to the key distribution problem. It uses the cyclic group $\mathsf{F}_q^* = \mathsf{F}_q/0$, where F_q is the finite field with q elements. The complexity of the discrete logarithms problem (DLP) in the group F_q^* provides the foundation for the

*Corresponding author

Email addresses: nurafiqah@um.edu.my (Nur Afiqah Suzelan Amir), wanainun@um.edu.my (Wan Ainun Mior Othman), kbwong@um.edu.my (Wong Kok Bin)

Received: November 3, 2022 Revised: November 10, 2022 Accepted: November 21, 2022

security of this protocol. Numerous key exchange methods built on number theoretic issues, like the discrete logarithm problem (DLP) and the integer factorization problem (IFP), have since been presented. In these protocols, abelian groups are frequently the fundamental group structures [1]. This is due to the intractability of issues involving number theory serving as the basis for all of these hard problems [2], [3], [4], [5]. Nevertheless, Shor's and other quantum algorithms [6], [7], [8], [9], [10] can resolve the IFP and DLP over these abelian groups in polynomial time. In addition, these techniques based on number theory are not applicable in microelectronic devices, such as low-cost smart cards with limited processing capabilities. This motivates us to construct a safer and more effective number-theory-based key exchange protocols.

The non-commutative groups and rings have been used to propose a number of public key cryptosystems and key exchange protocols [11], [12], [13]. According to [14], [15], [16] certain matrices properties, such as determinant, eigenvalues, and Cayley–Hamilton theorem, can be used to develop attacks against protocols that use groups of invertible matrices over finite fields as their platform group. These approaches reduce the DLP on $GL_n(F_q)$ to a factoring issue or the DLP over finite fields [16]. The semigroup of matrices over group ring: $M_{(k\times k)}(F_q[S_r])$ under typical matrix multiplication operation [17] and group of invertible matrices over group ring: $GL_n(F_q[S_r]$ [14] have been proposed as the platform to prevent this reduction of DLP to the one over finite field.

Group ring applications in cryptography have received a significant amount of attention over the years. Rososhek et al. [18] [19] presented a cryptosystem based on group ring structure. A key exchange system based on matrices over a group ring was created in 2011 by Kahrobaei et al. [18]. Following that, a number of group ring-based systems were presented [19],[20], [21]. In [19], the author presented a number of key exchange protocols and public key encryption techniques based on group ring matrices, with the related intractable assumptions being DLP and factorization problem (FP) in group ring matrices, respectively. In 2016, S. Inam and R. Ali [20] developed a new El Gamal public key cryptosystem for which the underlying hard problem for their cryptosystem is the conjugacy search problem. In their study, they have substituted the conjugacy search problem (CSP) over group ring for the exponentiation of elements. The primary concept behind the use of group rings in cryptography is predicated on the assumptions that the cardinality of the finite ring R is fixed and that the cardinality of a group ring for a finite group is an exponent of the cardinality of a group G. Then, a reliable user can employ polynomial algorithms to conduct cryptographic transformations independently in the group G and in the ring R. In addition, the group ring will be extremely complicated for an unauthorised user.

Zhang et al. [22] introduced a key exchange protocol based on infinite non-abelian groups in 2022. They created a shared secret key that contained two difficult problems: the equivalent decomposition problem (EDP) and the discrete logarithm problem (DLP). Using semidirect products of finite groups, Lanel et al. [23] suggested a unique method for non-abelian group-based public-key cryptography protocols. The fundamental mathematical problem for the proposed protocols is given as an intractable problem of finding automorphisms and producing elements of a group. Then, they demonstrated how this insoluble task might be reduced to the challenging challenge of identifying the pathways and cycles of Cayley graphs, including Hamiltonian paths and cycles. In [24], [25], Gupta et al. developed a novel undeniable signature technique in a nonabelian group over group ring, whose security depends on the complexity of solving DLP and CSP. However, this approach needs regular connection with the signer in order to validate the message and credentials, and the signers may not always be available. Therefore, scheme in [24], [25] is impractical for business and confidential transactions. They claimed that while an undeniable signature is effective, a signer who has access to a private key may publish a publicly available message signature, which may compromise the confidentiality of the signer's identity. As a result, this scheme is unable to attain privacy-related properties. In [26], a new El Gamal public key cryptosystem based on matrices over a grouping was proposed. Although the platform of the group ring proposed is non commutative, the scheme may be inefficient because there is no explicit performance efficiency stated in [26]. In [27], Mittal et al. developed a robust ID-based encryp-

tion system whose security relies on the recently discovered significant problems in the algebraic structure of group rings. However, because the TP possesses the user's private keys, identity-based suffers from a key escrow problem. In [28], a new form of the group ring-based signature system was developed.

In considering the fact that group rings are often not commutative, $M(n, GR)$ and $GL(n, GR)$ do not make sense in general, therefore we must be very careful when choosing the ground structures of groups and rings [29], [31], [32]. In [33]. The platform that we are suggesting in our work is the matrices over the group ring $(F_q[S_r])$, where F_q is the finite field with q elements and S_r is the symmetric group of degree r.

Our contribution: In our work, we incorporate the two hard problems which are the CSP and DLP. We modify and extent the existing CSP and DLP to define a new problem, conjugacy search problem with DLP (CDL) where the underlying structure is based on group rings. We will also analyse the parameters that are suitable to design a secure and efficient CDL based on a group ring. We implement the new problem CDL to construct a secure and efficient group signature scheme. We provide an analysis that shows our protocol achieves efficient security level, system robustness and performance efficiency.

2. Pleliminaries

Here, we present some fundamental notions of general linear group, group ring and matrices over group ring.

Definition 1 (General Linear group) The general linear group is composed of $n \times n$ invertible matrices of degree n. The operation is identical to standard matrix multiplication. Since the product of two invertible matrices is also invertible and the inverse of an invertible matrix is equally invertible, this produces a group. For instance, given a ring R with identity, the general linear group $GL_n(R)$ is the group of $n \times n$ invertible matrices with elements in R.

Definition 2 (Group Ring) Let F be a field and G be a multiplicative group, finite or infinite. The group ring [18] is an associative F-algebra consisting of all finite sums of the form:

$$x = \sum_{g \in G} \alpha_g G$$

Where $\alpha_g \in F$ and we denote group ring as $F[G]$.

Let

$$y = \sum_{g \in G} \beta_g G$$

and

$$z = \sum_{h \in G} \gamma_h h$$

be elements of $F[G]$. Then, the addition and multiplication are defined as follows:

$$x + y = \sum_{g \in G} \alpha_g G + \sum_{g \in G} \beta_g G = \sum_{g \in G} \alpha_g G + \beta_g G$$

$$xz = \sum_{g \in G} \alpha_g G \times \sum_{h \in G} \gamma_h h = \sum_{g,h \in G} \alpha_g G \gamma_h h$$

Definition 3 (Matrices over group ring ($F_q[S_r]$)). Consider the field F_5 and the symmetric group S_5. Let e be the multiplicative identical element of $F_5[S_5]$ and $a, b \in F_5[S_5]$ such that:

$$a = 3(134) + 2(13)(25),$$
$$b = 4(134) + 2(1325) + (14)(35).$$

Then from the above definition,

$$a^2 = (14)(25) + 4(143) + (25)(34) + 4(1),$$
$$a + b = 2(134) + 2(13)(25) + 2(1325) + (14)(35),$$
$$ab = (4(134) + 2(1325) + (14)(35))(3(134) + 2(13)(25)) =$$
$$2(143) + 3(14)(25) + (125)(34) + 4(12) + 3(153) + 2(15234).$$

Hence, $M_{(2\times2)}(F_5[S_5])$is the semigroup of 2×2 matrices over the group ring $F_5[S_5]$ under conventional matrix multiplication. $LetA_1, A_2 \in M_(2 \times 2)(F_5[S_5])$ where:

$$A_1 = \begin{bmatrix} 0 & b \\ e & a \end{bmatrix}$$

,

$$A_2 = \begin{bmatrix} b & e \\ e & a \end{bmatrix}$$

Then,

$$A_1A_2 = \begin{bmatrix} b & ba \\ b+a & e+a^2 \end{bmatrix}$$

Where $ba, b + a$ and a^2 are calculated above.

2.1. Conjugacy Search Problem with Discrete Logarithm Problem (CDL)

This section presents a new hard problem known as the conjugacy search problem with discrete logarithm problem and examines its complexity and security.

Definition 1 (Conjugacy Search Problem) In a non-abelian group $(G, \dot{})$, the conjugacy search problem is formulated as follows: given $x, y \in G$ such that $x = a - 1 \cdot y \cdot a$, obtain $a \in G$.

Definition 2 (Discrete Logarithm Problem). Let p be a prime and given an element $\beta \in F_p^*$ where $F_p^*$is a cyclic group of order $p - 1$ generated by a, find an integer t, $0 \leqslant t \leqslant p - 2$ such that $a^t \equiv \beta \mod p$.

We combine the aforementioned two problems to formulate the new problem of conjugacy search problem with discrete logarithm problem (CDL), whose underlying structure is based on general linear group over group ring.

Definition 3 (Conjugacy Search Problem with Discrete Logarithm Problem). Let $(H, \dot{})$ be a finite non-abelian semigroup with v elements. Let x, y, z be arbitrary elements of H and a be a random element of F_p^*. Then for given $y, z \in H$, find $x \in H$ and $a \in F_p^*$ such that $y = xz^a x^{(-1)}$.

2.2. Security and complexity of CDL

Let $H = y_1, y_2, ..., y_n$ be a non-commutative semigroup of n elements and $Z_m = 0, 1, 2, 3, ..., m-1$, where m is large positive integer. Let $z \in G$ and $w \in Z_m \backslash 0, 1$ such that for given $x, y \in G$, $x = y^w z$. Since $x, y, z \in G$, they can be expressed as $x = y_i, y = y_j, z = y_k$ for some $i, j, k \in 1, 2, 3, ..., n$.

The elements z and w are chosen from G and $Z_m \backslash 0, 1$. There are n and m options for z and w, correspondingly. The total number of steps required to solve the CDL using a brute force approach is therefore $O(nm)$, which is exponential in the size of nm in bits and $d = log_e 2$ where:

$$e^{(\log_e^n m)} \tag{2.1}$$

$$e^{(\log_e 2 . \log_2 nm)} \tag{2.2}$$

$$e^{(d.size(nm))} \tag{2.3}$$

Example 1. For a certain non-abelian group, we evaluate the CDL's complexity. In the case when F_q is a field and S_r is a symmetric group, let $H = GL_n(F_q[S_r])$ be a non-abelian group of $n \times n$ matrices of order v over group ring $F_q[S_r]$. Assume X, Y, Z be three $n \times n$ matrices of H, with X being a non-degenerated matrix and $a \in F_p^*$ such that $Y = XZ^a X^{(-1)}$. Therefore, the number of operations needed to discover (X, a) is $O(vp)$ which is equivalent to $O(exp(\log_e vp))$.

Example 2. Let F_5 be a field and S_3 is a group on symmetric on 3 symbols. Then an arbitary element x of the group ring $F_5[S_3]$ can be expressed as:

$$x = \sum_{1}^{3} !u_i t_i$$

Where $u_i \in F_5$ and $t_i \in S_3$, that is all possible linear combinations of S_3. We note that the total number of elements in group ring $F_5[S_3]$ is $5^3!$. Hence the semigroup $G = GL_{(2\times 2)}(F_5[S_3])$ of 2×2 matrices have $(5^3!)^4 \approxeq 5^2 4$ elements in it. Therefore, we can conclude the complexity over $GL_{(2\times 2)}(F_5[S_3])$ is significantly large and robust against brute force attack as depicted in Table 1.

Table 1: The size of $GL_(k \times k)(F_q[S_r])$ for different values of k, q and r

Matrix Size $(k \times k)$	$q = 3r = 5$	$q = 3r = 7$	$q = 5r = 5$	$q = 5r = 7$
2×2	$(3^5!)^4 = 3^4 80$	$(3^7!)^4 = 3^2 0160$	$(5^5!)^4 = 5^4 80$	$(5^7!)^4 = 5^2 0160$
3×3	$(3^5!)^9 = 3^1 080$	$(3^7!)^9 = 3^4 5360$	$(5^5!)^9 = 5^1 080$	$(5^7!)^9 = 5^4 5360$

3. A Secure Group Signature Scheme Over Group Ring

In this section, we present our secure and efficient group signature scheme based on group ring where the security relies upon the complexity of CDL.

System setup: Consider the case where $H = GL_{(k\times k)}(F_q[S_r])$ is a commutative subsemigroup of G and N be an abelian subgroup of H. Let h be a cryptographic hash function from $\{0,1\}^*$ to H defined as $h\colon (0,1)^* \to H/N$. The system parameter is $\mu = \langle p, H_1, N, h, A, X, a\rangle$.

Key Generation: Consider, $A \in H/N$, then the public key is $(p_k = P)$ where $P = PXA^aX^{(-1)}$ for $X \in N$. Then, the private key $(s_k = X, a)$ for $a \in Z_p^*/(1)$.

Signature Phase: A signature on a message $m \in (0,1)^*$ is $S = Y(h(m))^aY^{(-1)} = XA^a(h(m))^aA^{(-a)}X^{(-1)}$, where $h(m) \in H/N$ and $Y = XA^a$. Generate a random p_k for a group member and produce a message link-identifier $\sigma = H_1(m)^{(s_k)}$.

Verification Phase: A verifier carries out the following steps to verify validity of the signature S:

Step 1. On receiving the signature S on the message m, the verifier picks a random matrix $R \in N$, a random integer $b \in Z_p^*\backslash 1$ and then computes $C = (RP^{(}-1)SPR^{(}-1))^b$ and sends C to the signer.
Step 2. The signer computes $Q = (X^{(-1)}CX)^{(a^{(}-1)})$ and sends Q to the verifier.
Step 3. The verifier now calculates $Q_1 = R((h(m))^bR^{(-1)}$ and checks whether $Q = Q_1$ or not.
Step 4. The signature is valid if and only if $Q = Q_1$.
Step 5. The verifier verifies messages that included the same σ as replay of σ demonstrates that the same messages were signed by the same signer more than once.

Revocation Phase: On receiving the S on the message m, the verifier calculates $C = (RP^{(-1)}SPR^{(-1)})^b$ and sends it to the signer, then the signer calculates $Q = (X^{(-1)}CX)^{(a^{(}-1)})$ using private key (X, a) and sends it to the verifier. The verifier then checks whether $Q = Q_1$ or not. The equality $Q = Q_1$ can be verified as follows:

$$\begin{aligned}
Q = (X^{-1}CX)^{(a^{-1})} &= X^{-1}C^{(a^{-1})}X \\
&= X^{-1}(RP^{-1}SPR^{-1})^{b^{(}a^{-1})X \\
= X^{-1}(R(XA^{-a}X^{-1})(XA^ah(m)^aA^{-a}X^{-1})(XA^aX^{-1})R^{-1})^{b^{(}a^{-1})X \\
&= X^{-1}(RX(h(m)^aX^{-1})R^{-1})^{b^{(}a^{-1})X \\
&= X^{-1}(RX(h(m)^{aba^{-1}})X^{-1})R^{-1}X \\
&= X^{-1}(XRh(m)^{(aa^{-1}b)}R^{-1}X^{-1})X \\
&= R(h(m))^bR^{-1} \\
&= Q_1.
\end{aligned}$$

Thus, on receiving Q, the verifier verifies the equality $Q = Q_1$ and if the equality holds the verifier accepts the signature.

4. Security and Performance Evaluation

In this section, we evaluate and discuss security issues and performance level of our proposed protocol. We compare our scheme with [24], [25] and [27] as both schemes proposed a secure cryptosystem where the underlying work is based over group ring. The following security requirements are critical concerns to be met towards a secure cryptosystem.

1) Reliability. The first two conditions of message reliability of are fulfilled in all aforementioned schemes. A secure digital signature technique is commonly used to achieve message authentication. Messages announced without modification is assured and the authenticity of the message is preserved.

Claim 1. The proposed protocol is robust against Sybil attack and achieves the third requirement of message reliability.

We consider a Sybil attack executed by an internal adversary. An external adversary is not considered, as they do not own a valid credential or direct access to the network thus pose less harms to other users in the network. Sybil attack occurs when an internal adversary generates multiple signatures and disguise as different signer in order to compromise the functionality of the cryptosystem.

Proof: Let an internal adversary be ψ. We consider a scenario where ψ generates two signatures on the same message and announce these messages. Upon receiving these messages, the verifier checks the message-link identifier, σ to ensure that a legitimate signer in the network generates each message once. However, ψ can be identified when the two signatures share the same component of $\sigma = H_1(m)^{(s_k)}$.

Hence, ψ can be computationally related by evaluating the component of σ on two messages reporting the same event. This enable ψ to be traceable when the replay of σ is recognized upon endorsing the same message more than once. Hence, the message will be discarded and thus, our protocol is robust against Sybil attack.

2) Privacy. We consider two elements of privacy, which are anonymity and unlinkability. with [24], [25] and [27] the requirement of privacy is achieved by the use of pseudonyms where it avoids linking the real identification of the signer to its source. Furthermore, different messages announced from an origin cannot be linked to each other. In our work, we satisfy the property of privacy.

Claim 2. Our protocol protects the privacy of the originators against an internal adversary.

Proof: Let an internal adversary be B. Consider the following anonymity game. We generate key pair as depicted in our work and obtaining n key pairs $(p_k)_(\nu_1), (s_k)_(\nu_1), ..., (p_k)_(\nu_n), (s_k)_(\nu_n)$. The system parameters μ is forwarded to adversary B upon request where:

$$\mu = \langle p, H_1, N, h, A, X, a \rangle. \tag{4.1}$$

We assume that the adversary B query the signer's secret key at index $i, 1 \leqslant i \leqslant n$. We respond with key pair $(p_k)_(\nu_i), (s_k)_(\nu_i)$. We produce a valid signature σ_i on m using $(s_k)_{(\nu_i)}$ and forward σ_i to B. The adversary B then generates a message m^*. We randomly choose a bit $b \in_R 0, 1$where b is unknown to us. We then compute a signature σ^* on m^* using $(s_k)_{(\nu_i)_b}$. We send σ^* to B. When B obtains the signature, B analyses the signature and outputs the guess of b' of bvwhere b' $\in_R$ 0, 1. We declare failure and B wins the game, provided that B can guess the value of b' = b. This anonymity game defines the advantage of adversary B winning the game as equation (4.2), where Pr[b' = b] represents the probability of b' = b.

$$Pr[b' = b] = 1/2 \tag{4.2}$$

The probability is taken over the coin tosses of adversary B. Consequently, the adversary B is unable to exploit the randomized key generation and signing algorithm to win the anonymity game in polynomial time with a non-negligible probability. Hence, our scheme satisfies the privacy requirement.

3) Accountability. An entity performing some unlawful actions is accountable by the authorised party. In our work we satisfy the accountability features.

Claim 3. Our protocol achieves all the accountability requirements.

Proof: We fulfil the accountability requirements of traceability, non-repudiation and revocation in our scheme. The property of traceability is satisfied where the group signature allows the verifier to reveal signature of a malicious vehicle. The identity of an adversary is traceable when the same component of σ is recognized upon verifying the same message more than once and the proof runs similar to the proof in Claim 1.

Table 2: Security Requirements in group ring

Security element	[24], [25]	[27]	Our work
Sender's authenticity	Yes	Yes	Yes
Data integrity	Yes	Yes	Yes
Message truthfulness	No	No	Yes
Anonymity	Yes	Yes	Yes
Unlinkability	Yes	Yes	Yes
Traceability	Yes	Yes	Yes
Non-repudiation	Yes	No	Yes
Revocation	No	No	Yes

5. Conclusion

In this study, we have introduced a new key exchange protocol where the underlying work is based upon a new conjugacy search problem with discrete logarithm problem with factorization (CDL) over group ring. As far as we are aware of, this is the first proposed protocol employing group ring exists in the literature. We employed the semigroup of matrices over the group ring with the standard matrix multiplication operation as the platform group for a new group signature scheme based on CDL. Robustness analysis of our work demonstrates the feasibility and applicability of our protocol in actual implementation.

References

[1] Koblitz, N. A course in number theory and cryptography. Springer Science and Business Media. 114, 1994. 1

[2] Landau, E. Elementary number theory. American Mathematical Society, 125, 2021. 1

[3] Yanlin, Q., and Xiaoping, W. New digital signature scheme based on both ECDLP and IFP. In 2009 2nd IEEE International Conference on Computer Science and Information Technology, 2009, pp. 348-351. 1

[4] Harn, L. Public-key cryptosystem design based on factoring and discrete logarithms. IEEE Proceedings-Computers and Digital Techniques, 141(3), 1994, pp. 193-195. 1

[5] Poulakis, D. A public key encryption scheme based on factoring and discrete logarithm. Journal of Discrete Mathematical Sciences and Cryptography, 12(6) ,2009, pp. 745 752. 1

[6] Grover, L. K. Quantum mechanics helps in searching for a needle in a haystack. Physical review letters, 79(2), 1997, pp. 325. 1

[7] Proos, J., and Zalka, C. Shor's discrete logarithm quantum algorithm for elliptic curves. 2003. arXiv preprint quant-ph/0301141. 1

[8] Manzoor, E., and Shah, N. B. Uncovering latent biases in text: Method and application to peer review. 2020. arXiv preprint arXiv:2010.15300. 1

[9] Rötteler, M. Quantum algorithms: A survey of some recent results". Informatik-Forschung und Entwicklung, 21(1), 2006, pp. 3-20. 1

[10] Greenwell, R. N. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. The College Mathematics Journal, 31(1), 2000, pp. 70. 1

[11] Alvarez, R., Martinez, F. M., Vicent, J. F., and Zamora, A. A new public key cryptosystem based on matrices. WSEAS Information Security and Privacy, 2007, pp. 36-39. 1

[12] Climent, J. J., Navarro, P. R., and Tortosa, L. Key exchange protocols over noncommutative rings. The case of. International Journal of Computer Mathematics, vol. 89(13-14), 2012, pp. 1753-1763. 1

[13] Stickel, E. A new public-key cryptosystem in non abelian groups. In Proceedings of the Thirteenth International Conference on Information Systems Development. Vilnius Technika, Vilnius, 2004, pp. 70-80. 1

[14] Ezhilmaran, D., and Muthukumaran, V. Key exchange protocol using decomposition problem in near-ring. Gazi University Journal of Science, 21(1), 2016, pp. 123-127. 1
[15] Menezes, A. J., and Wu, Y. H. The discrete logarithm problem in $\mathsf{GL}(n, q)$. Ars Combinatoria, 47, 1997, pp. 23-32. 1
[16] Cheng, Q., Zhang, J., and Zhuang, J. LWE from non-commutative group rings. Designs, Codes and Cryptography, 90(1), 2022, pp. 239-263. 1
[17] Kahrobaei, D., Koupparis, C., and Shpilrain, V. Public key exchange using matrices over group rings. Groups-Complexity-Cryptology, 5(1), 2013, pp. 97-115. 1
[18] S. K. Rososhek, Cryptosystems in automorphism groups of group rings of Abelian groups, J. of Math. Sci., 154, 2008, pp. 386-391. 1
[19] D. Kahrobaei, C. Koupparis, V. Shpilrain, A CCA secure cryptosystem using matrices over group rings. Contem. Math., 633, 2015,pp. 73-80. 1
[20] C. M. Koupparis, Non-commutative cryptography: Diffie-Hellman and CCA secure cryptosystems using matrices over group rings and digital signatures, City University of New York, 2012. 1
[21] S. Inam, R. Ali, A new ElGamal-like cryptosystem based on matrices over groupring, N. Comp. and App., 29, 2018, pp. 1279-1283. 1
[22] J., Zhang, Y.J. Yang, Y.P. Li, A New Key Exchange Protocol Based on Infinite Non-Abelian Groups, Sec. and Comm. Net., 2022. 1
[23] G.H.J., Lanel, T.M.K.K Jinasena, B.A.K., Welihinda, Cryptographic Protocols using Semidirect Products of Finite Groups, Inter. J. of Comp. Sci. and Net. Sec., 21, 2021,pp. 17-27. 1
[24] A. Pandey, I. Gupta, A new undeniable signature scheme on general linear group over group ring, J. of Disc. Math. Sci and Crypto., 2020, pp. 1-13. 1, 4, 2
[25] N. Goel, I. Gupta, M. K. Dubey, B. K Dass, Undeniable signature scheme based over group ring, App. Alg. in Engi. Comm. and Comp., 27, 2016, pp. 523-535. 1, 4, 2
[26] M. Rötteler, Quantum algorithms: A survey of some recent results, Informatik-Forsch. und Entwi., 21, 2006, pp. 3-20. 1
[27] G. Mittal, S. Kumar, S.Kumar, A quantum secure ID-based cryptographic encryption based on group rings. Sādhanā, 47, 2022, pp. 1-16. 1, 4, 2
[28] D. Pointcheval and J. Stern, Security arguments for digital signatures and blind signatures, J. of Crypto., 13, 2000, pp. 361-396. 1
[29] Xu, F., Wong, D., and Tian, F. Automorphism group of the intersection graph of ideals over a matrix ring. Linear and Multilinear Algebra,70(2), 2022. pp. 322-330. 1
[30] M. Eftekhari, Cryptanalysis of some protocols using matrices over group rings, in Int. Conf. on Cryptology in Africa: Progress in Cryptology — AFRICACRYPT 2017, Lecture Notes in Computer Science, 10239, 2017. 1
[31] G. Micheli, Cryptanalysis of a non-commutative key exchange protocol, Adv. Math. of Comm. 9(2), 2015, pp. 247–253. 1
[32] V. Shpilrain, Cryptanalysis of Stickels key exchange scheme, in Proc. of Computer Science in Russia, Lecture Notes in Computer Science, 5010, 2008, pp. 283–288. 1
[33] Chaum, David; van Heyst, Eugene. Group signatures. Advances in Cryptology — EUROCRYPT '91, Lecture Notes in Computer Science, 547, 1991, pp. 257–265. 1