A Secured Digital Signature Using Conjugacy and DLP on Non-commutative Group over Finite Field

L. Narendra Mohan and G.S.G.N. Anjaneyulu

Abstract In the present paper, we propose a secured scheme of digital signature connecting both conjugacy problem and discrete logarithm problem based on non-commutative group generated over a finite field. For this, we define a non-commutative group over matrices with the elements of finite field such that conjugacy and discrete logarithm problems can be executed together proficiently. By doing so, we can formulate the signature structures using conjugacy and discrete logarithm through non commutative group. In some domains, the above combination reduces to completely in discrete logarithm problem. This digital signature scheme more elemental over $F^{*}q(x) = G\ L_n\ (F_q)$. Here the security of the signature protocol depending on complexity of the problems associated with conjugacy and discrete logarithm. The security analysis and intermission of proposed protocol of digital signature is presented with the aid of order of complexity, existential forgery and signature repudiation.

Keywords Digital signature · Public key cryptography · Conjugacy problem · Discrete logarithm problem · Quasideterminant and non commutative ring

1 Introduction

A digital signature scheme is a scientific approach for demonstrating the legitimacy of an advanced message or record. A substantial digital signature delivers for a beneficiary reason to have confidence that those message might have been made by an known sender, such and such the sender cannot rebuff hosting sent those message (authentication and non-repudiation). Also note that those messages might have been not modified, when the message being transmitted(integrity). In the

L. Narendra Mohan · G.S.G.N. Anjaneyulu (✉)
Department of Mathematics, SAS, VIT University, Vellore 632014, Tamil Nadu, India
e-mail: anjaneyulu.gsgn@vit.ac.in

L. Narendra Mohan
e-mail: mohannarendra3@gmail.com

S.C. Satapathy et al. (eds.), *Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications*, Advances in Intelligent Systems and Computing 516, DOI 10.1007/978-981-10-3156-4_47

present scenario, Digital signatures are essential and regularly utilized to programming distribution, economic transactions, what's more to other situations the place, where it is imperative should recognize falsification or damaging. Diffie and Hellman principally presented the basic notion about advanced signature scheme along with the first introduced the concept of Digital signature scheme using cryptography. This piece of information of a "digital signature" at first disclosed in Diffie and Hellman's inspiring paper, "New Directions in Cryptography" [1]. They suggested that each client must distribute an "open key"(used for validating/Confirming signatures), and at the same time keeping mystery "secret key" (used for producing signatures). At the inception, in their protocol, Entity A's signature for a message M is a worth which relies on upon M and on A's private key, so that any individual may be ensured those one can check the legitimacy of A's signature with A's open key. Be that as it may, in the meantime knowing A's open key is important to support and one to authenticate A's signatures, it doesn't concede one to just distort A's signatures.

In this proposed article, we make some components over non-commutative group/ring/field. Here we utilize digital signature scheme in cyclic group F_q^*, the place F_q will be the finite field for q components. The strength and security of this scheme in light of the challenge depending on the strain of calculating discrete logarithms in the cyclic group F_q^*. Here discrete logarithm issue is a hard-hitting experience. Let $F_q^* = GL_1(F_q)$, particular case could wonder if the group $GL_2(F_q)$ for two-by-two invertible matrices or all the more for the most part of the group $GL_n(F_q)$, which conceals natural typical form, might be a chance to utilize in Digital Signature and also there may be some preference previously, utilizing them.

Let us detect a non-singular matrix $X \in GL_n(F_q)$. Realizing X and a power X^a, it is very hard to compute a. The initial side of the point will be that having X, one can calculate det(X) $\in F_q^*$ (the determinant of X), furthermore det $(X^a) = (\det(X))^a$. In this way, such DL problem in matrix groups tempers to the DL problem done in F_q^*. Person could halt away from this struggle by picking a matrix X such that det(X) as unity, at the same time then by calculating characteristic values from X and from X^a and utilizing the reality that those last are those previous in the power of a, particular case diminishes once more those DL problem of the particular case in some development about $F*$, So there will be no improvement in view of the DL problem in the pool of non-singular matrices over a finite field, what's new additional for the most part through a finite commutative ring. In this problem, including non-commutative (semi) groups in digital signatures suggested a stage involving braid groups and the same notion was proposed in [2]. Also another platform using matrix algebra was conferred in [3]. It employs conjugation and exponential powers together to its security. A stage to this protocol utilizing braid groups might have been initially proposed in [4] also an alternate one utilizing an F_q-algebra to [5].

We might provide for a digital signature scheme of these two platforms in the area described in the Sect. 2.3, by dropping the issue to the DL problem over certain finite field. Those semi group generated on matrices in a commutative ring might have been acknowledged in [5] to an verification protocol, be that its security is in light of the strain of the conjugacy search problem, but not depending on the discrete logarithm tool. Certainly, the creators consider about matrices through some way or another convoluted ring, to be specific those ring of polynomials for k variables would create the conjugacy search problem infeasible.

1.1 Phases of Digital Signature Protocol

Another fundamental public key cryptographic scheme is a Digital signature, whose concept was first designed by Diffie–Hellman (DH76-17). The ability to build a digital signature scheme is a great lead of public cryptography over symmetric key cryptography. The present article is based on digital signature. So we discuss different primal stages of digital signature scheme. A digital signature algorithm can be designated as follows. A digital signature is an authentication mechanism that facilitates the creator to attach a code that acts as a Digital signature. The signature is molded by taking the hash of the message and encrypting the message with the creators' private key. The Digital signature guarantees that the source and integrity of the message [6, 7].

A **Digital signature** is a structure having five components (F, C, I, L, O), whether the following conditions are satisfied.

1. F is a finite set of manageable keys.
2. C is a finite set of manageable signatures.
3. I, the key space and is a finite set of manageable keys.
4. For each $k \in I$, there is a signing algorithm $sig_k \in L$ and an associated verification algorithm $Ver_k \in O$. Each $Sig_k: F \rightarrow C$ and $Ver_k: FXC$ {True, False} are functions such that the accompanying condition is fulfilled for each message $x \in F$ and for each signature $y \in C$. Ver (x, y) = {True if y = sig(x) and False if $y \neq$ sig(x)}

For every $k \in I$, the functions Sig_k and Ver_k should be polynomial time functions. Ver_k will be a public function and Sig_k will be a secret. Thereafter, a signature must be not forgeable. This means that, it must be infeasible to calculate a signature of a message, with respect to a public key without the information of the corresponding secret key [8–12].

2 Computational Primitives for Proposed Signature Scheme

2.1 Discrete Logarithm Problem

Most widely used computational problem in security protocols is discrete logarithm problem. More details can be seen [13, 14].

Definition If G be a finite cyclic group of order n and g be a generator of G and y $\in$G then discrete logarithm of y to the base h, denoted by $\log_h^y$ is the unique integer x,

$0 \le x \le$ n-1, such that y = g ^{x}. This is called as DLP [15, 16].

2.2 Conjugacy Problem

The Conjugacy problem in non-commutative group G contains two components u, v in G are mutually conjugate each other, composed u $\sim$ v where v = a^{-1}u a for some element a$\in$ G. Here the elements a or its inverse is known as a conjugator and the couple (u, v) is understood to be conjugate. More details can be seen [13, 14]. Obviously '$\sim$' is an equivalence relation. The conjugacy relation has the following properties

(i) u = e^{-1}u e for e$\in$ G and u $\in$ G (Reflexive).
(ii) v = a^{-1}u a $\rightarrow$ u = $(a^{-1})^{-1}$v a $\rightarrow$ u $\sim$ v (Symmetric).
(iii) v = a^{-1}u a, w = b^{-1}u b then w = $(ab)^{-1}$ u ab $\rightarrow$ w $\sim$ u (Transitive).

So that conjugacy relation is clearly an equivalence relation and the following are the types of conjugacy problems, which have been used in cryptography [17, 18].

(a) **The conjugacy decision problem (CDP):** The CDP inquire to find out, whether u, v are used for a particular occasion (u, v) $\in$ G x G
(b) **The conjugator search problem (CSP):** The CSP solicits to discover a $\in$ G, satisfying v = a^{-1}u a for a specified case (u, v) $\in$ G x G such that u $\sim$ v.

2.3 Matrices—Quasideterminents

Let L be a square matrix of order n, with elements of a non commutative ring R, we reminder $L^{ij,}$ the matrix attain from square matrix L by removing the ith row and the jth column. We like wise reminder by the ith row of matrix with jth place excepted, and with the jth column of L by the ith place excepted. Here every position (i, j), the quasideterminant [19] of d is defined by $|L|_{ij} := d_{ij} - r_i^j(L_{ij})^{-1}c_i^j$ We have $|L|_{ij} \in$ R and, obviously, this quasideterminant occurs if the (n − 1)-by-(n − 1) matrix L_{ij} is invertible. Thus, for a matrix of order n, there will be a n^2quasideterminants.

Example $L = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$ for n = 2

$|L|_{11} = c_{11} - c_{12}c_{22}^{-1}\, c_{21,}|L|_{12} = c_{12} - c_{11}c_{21}^{-1}\, c_{22,}$
$|L|_{21} = c_{21} - c_{22}c_{12}^{-1}\, c_{11}, |L|_{22} = c_{22} - c_{21}c_{11}^{-1}c_{12.}$

Remark Where in the abelian case, a quasideterminant is not equivalent to a det, but rather additionally the proportion of two dets, to be specific,

$$|\mathrm{L}|_{\mathrm{ij}} = (-1)^{\mathrm{i+j}} \frac{\det(D)}{\det(D_{ij})}$$

Here with signature perspective, we just need to ensure that there is no scheme decreasing the DL problem in the group of matrices with non-commutative elements to the Discrete Logarithm problem in the ring of coefficients. More details can be seen [20].

3 Proposed Digital Signature

Here we elucidate a digital signature scheme based on group of matrices over a finite field. This digital signature scheme has the following stages.

3.1 Initial Setup

We select a nonsingular matrix X $\in$ G $L_n(F_q)$, and calculate power X^a. The Next step det(X) $\in$ F_q^* (the determinant of X), furthermore det(X^a) = $(\det(X))^{a.}$. Here Alice needs to produce a signature for a message M. At the last step, the recipient Bob should confirm the signature, which is valid and also demonstrate the legitimacy to reveal the message [21].

Construct a square matrix L of order n, with elements over some finite field F with non commutative property. We note L^{ij} is the sub matrix derived commencing L by neglecting those ith row and the jth column. We furthermore reminder through the ith row of L with jth position excepted, and through the jth column of L with the ith position excepted [22].

3.2 Key Generation

We now combine the discrete logarithm problem and the conjugacy search problem collectively to generate the public key. So that extracting the private key from public key is not feasible as the discrete logarithm problem and the conjugacy search problem are intractable over the fundamental work structure. Suppose G may be non-commutative group generated over field elements of F and K_1, K_2 are two subgroups of G such that each component of K_1 commutes with each component K_2. We define G, K_1, K_2, also a component X $\in$ G of various higher powers of n, would be public information [23].

A picks on arbitrary a secret integer a $\in$ {2, 3, … , n − 1} and a secret matrix U $\in$ K_1 (UX $\neq$ XU), V $\in$ K_2; She computes a public key $\alpha = U^{-1}X^aU$.

Let us suppose that $K = K_1 = K_2 = \left\{ \begin{bmatrix} x & y \\ y & x \end{bmatrix} \right.$ $\in$ GL_2 (F_q), x, y $\in$ F_q, $x^2 - y^2 \neq 0\}$,

which is commutative subgroup of $GL_2(F_q)$.

3.3 Signature Generation

Let a group G = GL_2 (F_q) be the fundamental work infrastructure and X $\in$ $GL_2(F_q)$ of order n, Alice performs the following simultaneously. Alice selects a secret integer '**a**' $\in$ {2, 3, … , n − 1} as her private key and a secret matrix U $\in$ K and $\alpha = U^{-1}X^aU$ as her public key. Alice calculates as follows

$\beta = V^{-1}X^aU$ and also computes
$\gamma = (V^{-1}X^aV)$
$\delta = U^{-1}X^aV$

Here Alice forms a code (β, γ, δ, M) as her signature and send it to Bob as her signature on the message M for confirmation and acceptance.

3.4 Verification

After receiving the signature (β, γ, δ, M) from Alice and to verify this signature as authenticated, Bob will do as follows.

First he computes $\theta = \alpha\ \beta^{-1}$. If $\delta = \theta\gamma$ then he accepts the signature, otherwise it will be rejected automatically.

3.5 Confirmation Theorem

Theorem If $\theta = \alpha\ \beta^{-1}$ then $\delta = \theta\gamma$
Completeness: A's signature is (β, γ, δ, M). If Alice monitors signature verification, and then Bob always approves it, as an authenticated signature and the message.

Proof We know that $\alpha = U^{-1}X^aU$ is Alice's public key and Bob accepts the signature

(β, γ, δ, M) and are parameters of the signature
Then we prove the signature as follows
Since $\theta = \alpha\ \beta^{-1}$

$\beta = V^{-1}X^{a}U$
$\gamma = (V^{-1}X^{a}V)$ and $\delta = U^{-1}X^{a}V$
$\theta = U^{-1}X^{a}UU^{-1}X^{-a}V = U^{-1}X^{a}X^{-a}V$
$\theta = U^{-1}V$

Then conformation will be done as follows in final

$$\begin{aligned}\theta\gamma &= U^{-1}VV^{-1}X^{a}V\\ &= U^{-1}X^{a}V = \delta\end{aligned}$$

Here Bob computes the message, when Alice follows his algorithm. Then B accepts signature algorithm.

Hence completes the proof.

4 Security Analysis

We explain the security for the digital signature scheme of matrices over non commutative group over a finite field is given below. Here n be the index of X and $\alpha = U^{-1}X^{a}$ U, we have to calculate the secret key '**a**' and exchanged key $U^{-1}V^{-1}$ X^{ab} UV is difficult [24–27]

(i) **Existential Forgery**: No hash function will be utilized within the elgamal signature system, at that point the existential falsification may believable under direct attack. Without hash function, existential forgery is not applicable in this signature.

(ii) **Signature Repudiation**: Assume Alice intentionally refuse her signature on some valid information. Substantial signature might be changed by eve and furthermore she could sign the message M, with the forged signature ($\beta_{e,}$ γ_d, δ_e, M_d) instead of original. That moment conformation technique and verification will be failed as

$$\theta_e\gamma_e = (U^{-1}V)_e(V^{-1}X^{a}V)_e \neq \delta.$$

Then this identifies non repudiation property.

(iii) **Total Break**: The security of the private key in this digital signature is additional, as we develop the secret signature key on non-commutative structure, where the problem is not tractable. These days' signatures need aid of utilizing this property. Here the problem is dependent upon unmanageability from claiming conjugacy and discrete logarithm problem.

(iv) **Selective Forgery**: Even an assailant has the ability to make a signature by selecting identified with specific message M, this contradicts with the equation $\delta_e \neq \theta_e\gamma_d$. The Making the signatures like this is not beneficial for the attacker under the selective forgery.

5 Conclusions

In this article, we effectively utilized conjugacy problem and discrete logarithm together to enhance security of signature scheme. We have designed digital signature scheme over non-commutative matrix group with elements of field. The key thought behind our plan is that we constructed non-commutative group of matrices over the field. We make them as the underlying field structure for constructing signature. We demonstrated the strength and soundness for signature scheme by proving confirmation theorem. We enlightened the security analysis of the signature scheme by proving, it is secure against data forgery, signature repudiation and existential forgery. This is secure against total break as public key and private keys are connected with conjugacy problem and discrete logarithm.

References

1. W. Diffie, M. Hellman, New directions in cryptography. IEEE Trans. Inf. Theory **IT-2.2**(6), 644–654 (1976)
2. J. Kang, J.W. Han, J.H. Cheon, S.J. Lee, K.H. Ko, S.J. Lee, C. Park, New public key crypto system using braid groups. Lect. Notes Comput. Sci. **1880**, 166–183 (2000)
3. D. Moon, K.C. Ha, S. Cho, Y.-O. Kim, Key exchange protocol using matrix algebras and its analysis. J. Korean Math. Soc.
4. A. Raulynaitis, E. Sakalauskas, P. Tvarijonas, key agreement protocol using conjugacy and discrete logarithm problems in group representation level. Informatica **18**(1), 115–124 (2007)
5. Los Alamitos, Network and System Security. IEEE Computer Society, CA, USA (2009), pp. 443–446
6. Text Book: Cryptography and network security by MR. AtulKahate
7. http://www.iacr.org (International Association for Cryptographic Research—website)
8. D. Poulakis, A Variant of Digital Signature Algorithm Designs, Codes and Cryptography, vol. 51(1) (2009), pp. 99–104
9. N.M.F. Tahat, E.S. Ismail, R.R. Ahmad, A new digital signature scheme based on factoring and Discrete logarithms. J. Math. Stat. **4**(4), 222–225 (2008)
10. C.Y. Yang, M.S. Hwang, S.F. Tzeng, A new digital signature scheme based on factoring and discrete logarithm. IJCM **81**(1), 9–14 (2004)
11. Z. Shao, Security of a new digital signature scheme based on factoring and discrete logarithms. IJCM **82**(10), 1215–1219 (2005)
12. Z. Shao, Signature schemes based on factoring and discrete logarithms, in *Computers and Digital Techniques, IEEE Proceedings-*, vol. 145. IET (2002), pp. 33–36
13. G.S.G.N. Anjaneyulu, P.V. Reddy, U.M. Reddy, Secured digital signature scheme using polynomials over non-commutative division semi ring. IJCSNS **8**(8), (2008)
14. G.S.G.N. Anjaneyulu, U.M. Reddy Secured directed digital signature over non-commutative division semirings and allocation of experimental registration number. IJCSI **9**(5), 3 (2012)
15. A.J. Menezes, Y.-H. Wu, The discrete logarithm problem in G Ln (Fq); ARS Combinatorica **47**, 23–32 (1997)
16. S. Wei, A new digital signature scheme based on factoring and discrete logarithms, in *Progress on Cryptography* (2004), pp. 107–111
17. S. Alam, A. Jamil, A. Saldhi, M. Ahamad, Digital image authentication and encryption using digital signature, in *ICACEA* (2015), pp. 332–336

18. N.A. Moldovyan, D.N. Moldovyan, A new hard problem over non commutative finite groups for cryptographic protocols. Lect. Notes Comput. Sci. **6258**, 183–194 (2010)
19. D. Boneh, A. Joux, P.Q. Nguyen, Why textbook Elgamal and RSA encryption are insecure, in *Lecture Notes in Computer Science,* vol. 1976 (2000), pp. 30–44
20. V. Retakh, S. Gelfand, I. Gelfand, R. Wilson, Quasideterminants. Adv. Math. **193**, 56–141 (2005)
21. M. Eftekhari, A Diffie-Hellman key exchange protocol using matrices over non abelian ring. http://arXiv1209.6144v1[cs.CR] (2012)
22. B. Leclerc, V. Retakh, J.-Y. Thibon, A. Lascoux, D. Krob, I. Gelfand, Non commutative symmetric functions. Adv. Math. **112**(2), 218–348 (1995)
23. V. Shpilrain, D. Grigoriev, Authentication from matrix conjugation, groups, complexity, cryptology, vol. 1, pp. 199–205 (2009)
24. B. Lynn, D. Boneh, H. Shacham, Short signatures from the Weil pairing, in *Proceedings of Asia Crypt 2001*, LNCS, vol. 2248 (Springer, 2001), pp. 533–551
25. D. Pointcheval, T. Okamoto, The gap-problems: a new class of problems for the security of cryptographic schemes, in *Proceedings of PKC 2001*, LNCS, vol. 1992 (Springer, 2001), pp. 104–118
26. A. Lincoln, Electronic signature laws and the need for uniformity in the global market, 8 J. Small & Emerging Bus. L. 67 (2004)
27. T.J. Smedinghoff, R.H. Bro, Moving with change: electronic signature legislation as a vehicle for advancing e-commerce. 17 J. Marshall J. Computer & Info. L. 723, 199