FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2 | Pages 150-153 | e-ISSN: 2347-470X

A New Fail-Stop Group Signature over Elliptic Curves Secure against Computationally Unbounded Adversary

Namita Tiwari[1], **Mayur Rahul**[2], **Rati Shukla**[3], **Devvrat Tyagi**[4] **and Ayushi Prakash**[5]

[1]*Department of Mathematics, School of Sciences, C.S.J.M. University Kanpur, U.P. India*
[2]*Department of Computer Application, UIET, C.S.J.M. University Kanpur, U.P. India*
[3]*GIS Cell, MNNIT Prayagraj, U.P. India*
[4]*ABES Engineering College, Ghaziabad, U.P. India*
[5]*ABES Engineering College, Ghaziabad, U.P. India*

***Corresponding Author**: Namita Tiwari Email: namita.mnnit@gmail.com

ABSTRACT- If an adversary has unlimited computational power, then signer needs security against forgery. Fail Stop signature solves it. If the motive of the signature is to hide the identity of the signer who makes signature on behalf of the whole group then solution is Group signature. We combine these two features and propose “A new Fail Stop Group Signature scheme (FSGSS) over elliptic curves”. Security of our proposed FSGSS is based on “Elliptic curve discrete logarithm problem” (ECDLP). Use of elliptic curve makes our proposed FSGSS feasible to less bandwidth environment, Block chains etc. Due to security settings over elliptic curves, efficiency of proposed scheme increases in terms of computational complexity.

Keywords: ID based Public key cryptography, Group signature, Fail Stop Signature, Elliptic Curve Cryptography

ARTICLE INFORMATION

Author(s): Namita Tiwari, Mayur Rahul, Rati Shukla, Devvrat Tyagi and Ayushi Prakash;

Special Issue Editor: Dr. Vikash Yadav;
Received: 12/04/2022; **Accepted:** 04/05/2022; **Published:**22/05/2022;
E- ISSN: 2347-470X;
Paper Id;
Citation: 10.37391/IJEER.100217
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100217

crossref member
CROSSREF.ORG
THE CITATION LINKING BACKBONE

This article belongs to the Special Issue on **Recent Developments in Communication Technology using Machine Learning Techniques**.

Publisher’s Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

Nowadays, organizations are using e-documents instead of using paper documents. Paper-less work helps to maintain green environment. Due to use of electronic documents, digital signature's importance has been increased that ensures validity, authenticity and integrity of e-documents. Potential uses of Digital signature's technology introduced a technique called Group Signature in which only authorized group members can sign on behalf of whole group.

Receiver can verify its validity and if necessary, actual signer's identity could be revealed. David Cham firstly introduced the concept of GSS [15] in 1991. GSS can be used in many applications like electronic voting and electronic auctions etc. In the journey GSS, a lot of GSS [7-10] have been proposed in the literature. Ling et al. [7] proposed a new GSS by combining the properties of [9] and security features in [10]. In this proposal they made possible the revocation of group members efficiently as well as dynamic registration. Having inspired by Ling et al. [7], Sun et. al. proposed the first full dynamic GSS over ring [8]. They used the concept of Markel hash tree.

Besides these literatures, there is always a new thought in new direction that makes research more interesting. Literature tells us that security level of digital signatures could be enhanced if there is an algorithm to prove that signature has actually been forged. To meet this requirement, there is another type of digital signature called “Fail Stop digital Signature scheme” (FSSS) [16].

In an electronic cash payment system, customer can use FSS while signing for money with-drawl. In this setting, customer need not worry about the unbounded powered bank. A secure FSS scheme has at-least two security requirements [1]:

(i) FSS is secure against an adversary which has unbounded power computationally.
(ii) If security assumption based on mathematical equation has been broken, actual signer can prove that forged signature has been produced by an unbounded adversary.

Combining the features of GSS and FSSS, “Fail Stop Group Signature scheme” (FSGSS) has been proposed in the literature. Main goal of the FSGSS is to stop the repetition of signing key after the discovery of a forgery attack. Motivated by these features, we have raised one real-world scenario namely "Forgery done by Computationally Unbounded Adversary" discussed in Application section. Recently, block-chain technology has been widely used for verification of the original signature. Smart cards have been used in calculation of signature recognition and certificates which prevents the joint attack. "In Block-chain technology newly added signature node does not require center approval. It requires only the approval of the majority node [6]. However, the GS scheme, based on block-chain, requires heavy calculation and is more

expensive to implement. We noticed that several limitations and improvements are required to make existing schemes practically efficient and allowing less key sizes.
Motivated by above, We propose an Efficient FSGSS based on ECDLP.

Our proposed scheme is the first ever FSGSS whose security is based on ECDLP. It uses mathematics of elliptic curves given in section 2 that makes it much more efficient due to less key sizes [11-12].

LAYOUT: In *section 2*, mathematical foundation is given. Our proposed FSGSS is given in `*Section 3*`. Security issues of our FSGSS are demonstrated in`*Section 4*`. *Section 5* presents a detailed explanation of application related to FSGSS. At the end *Section 6* concludes our proposed scheme with some future directions.

2. PRELIMINARIES

2.1 Basics/Brief of Elliptic Curve Group (Tiwari et.al. [13])

Consider a prime field F_q, the symbol 'EC/F_q' means an elliptic curve EC over a prime finite field F_q s.t,

$z^2 = y^3 + ay + b, a, b \epsilon F_q$, and

$discriminant = 4a^3 + 27b^2 \neq 0$

The collection of points of EC/F_q with an extra point ∞ (point at infinity)
Make a group

$G' = \{(y,z): y,z \epsilon F_q, EC(y,z) = 0\} \text{U} \{\infty\}$.

Let G be the cyclic subgroup of G' under point addition $"+"$.
Let P be the generator of order n of group G. Readers can refer [13] for more details.

2.2 Complexity assumption

Given $x \epsilon R\ Z_n^*, P,$ such that $Q = xP$ "For any Q and generator P in elliptic curve group, to find **x** is assumed to be computationally intractable in polynomial time."
This mathematical problem is known as ECDLP.

3. PROPOSED SCHEME

Let $\{P_0, P_1, P_2, ..., P_n\}$ is signer's group. Any group member P*i* can make signature on behalf of whole group, where P_0 is group manager (GM).

3.1 KGC (Key Generating Center)

(1) KGC picks an elliptic curve such that
n = order of elliptic curve group
Eq(x; y) over finite field Fq.

(2) Chooses a point P in Eq(x; y) and d in Zn* calculates Q = dP, publishes $(E_q(x,y), q, P, Q, H, H_1)$.
Here $H : \{0,1\}^* \to Z_n^*$ and $H_1 : \{0,1\}^* \times G \to Z_n^*$
are hash functions.

Note: If n is not prime in above random selection of elliptic curve, discard the curve and repeat the process. Readers can refer for detail [14].

3.2 Key extract

This algorithm is conversation between group manager and group members.

Suppose P_i wishes to be an authorized group member, then
(a) P_i sends ID_i to P_0.
(b) P_0 computes ski = x Q_i mod n, where Q_i = xH (IDi) and sends sk_i to P_i via secure channel.
(c) Pi chooses b_1, b_2, b_3, b_4 randomly from Z_n* and Computes

$$ki_1 = b_1H_1 (ski, b_1, Q_i)$$
$$k_{i2} = b_2H_1(sK_i, b_2, Q_i)$$
$$k_{i3} = b_3H_1\ (sK_i, b_3, Q_i)$$
$$k_{i4} = b_4H_1\ (sK_i, b_4, Q_i)$$

Now P*i* computes its public keys as

$$\alpha_{i1} = k_{i3}P + k_{i1}Q \text{ and}$$
$$\alpha 2 = k4P + k2Q$$

Over elliptic curve Eq (a,b).
Here $(\alpha_{i1}, \alpha_{i2})$ is public key pair of P*i*.

3.3 Signing algorithm

Message owner request for signature on message M,
Pi computes

$$S_{i1} = k_i H_1(M, Q_i) + k_{i2} \bmod n$$
$$S_{i2} = k_{i3} H_1(M, Q_i) + k_{i4} \bmod n$$

and publishes (S_{i1}, S_{i2}) as signature on message M.

3.4 Verification algorithm

Recipient can verify the signature the signature (M, S_{i1}, S_{i2}) as:

$$S_{i2}P + S_{i1}Q = \alpha_{i1}H_1(m, Q_i) + \alpha_{i2}$$

4. SECURITY ANALYSIS

If a computationally unbounded adversary forges a valid signature (S'_{i1}, S'_{i2}) on same message M, that passes verification algorithm, the actual signer Pi provides a proof of forgery as follows:

4.1 Proof of forgery

Theorem: "If there is a forged signature that passes through verification test, the sender is able to solve the ECDL Problem."

Proof:
$S_{i2}P + S_{i1}Q = \alpha_{i1}H_1(m,Q_i) + \alpha_{i2}$
$S`_{i2}P + S`_{i1}Q = \alpha_{i1}H_1(m,Q_i) + \alpha_{i2}$
Thus
$S_{i2}P + S_{i1}Q = S`_{i2}P + S`_{i1}Q$
$(s_{i2} – si2')P = (si1' – si1)\ Q$
$(s_{i2} – si2')P = (si1'- si1)\ d\ P$

Hence d = $\frac{(s_{i2} - si2')}{(si1' - si1)}$

In addition our proposed FSGSS satisfies all of the following security concerns:

(1) CORRECTNESS: FSGSS using Signing Algorithm passes Verification algorithm as follows:

$$\begin{aligned} &S_{i2}P + S_{i1}Q \\ &= (k_{i3}H(M,Q_i) + k_{i4})P + (k_{i1}H_1(M,Q_i) + k_{i2})Q \\ &= (k_{i3}P + k_{i1}Q)H(M,Q_i) + (k_{i4}P + k_{i2}Q). \\ &= \alpha_{i1}H_1(M,Q_i) + \alpha_{i2} \end{aligned}$$

(2) UNFORGEABILITY: Only authorized group member can create signature on message M.

At the time of verification processes, verifier uses α_{i1} and α_{i2} that are linked with ski and $k_{i1}, k_{i2}, k_{i3}, k_{i4}$. So only authorized signer would be able to create sign on behalf of group.

(3) ANONYMITY: Only GM and Pi knows ski and ID*i* and nobody knows ID*i* so no one can determine ID*i* for given Q_i = H (ID*i*) So only GM can tell who is actual signer.

(4) UNLINKABILITY: If two valid message signature pair are given then it is infeasible to find whether two different valid signatures are created by the same signer.
In our scheme, clearly Q*i* disappears for given two different message signature pair.

(5) EXCULPABILITY: This property says that "neither a group member nor the group manager would be able to sign on behalf of other group members". In our scheme, one can see that at the time of signature generation,

$$S_{i1} = (k_i H_1(M,Q_i) + k_{i2}) \bmod n \quad \text{and}$$
$$S_{i2} = (k_{i3}H_1(M,Q_i) + k_{i4}) \bmod n$$

Every group member has its own secret
$k_{i1}, k_{i2}, k_{i3}, k_{i4}$,
So neither (GM) U0 nor any other member P*i* can sign on behalf of P_j where *i* is not equal to *j*.

(6) TRACEABILITY: It means that GM is always able to determine the actual signer. We show here how it meets in our scheme as follows:
As verification equation is

$$S_{i2}P + S_{i1}Q = \alpha_{i1}H_1(M,Q_i) + \alpha_{i2}$$

Here α_{i1}, α_{i2} are used in verification which involves ski.

Only GM knows ski, therefore he is the only person who can determine the actual signer on given message M.

5. APPLICATION

Let us consider the recruitment scenario in an organization. Vice Chancellor (VC) of university has unbounded Powers. Suppose he constitute a committee so that any committee member can put sign on documents on behalf of whole committee. Now if VC wants to forge a signature for his own interest, then he can do so because of unbounded computational power. Now both the signatures (signature by pre-assumed signer and by VC) passes verification process. So it is very difficult to find out whether pre- assumed signer has signed the document or VC has forged the signature. In digital world, FSGSS is the solution of this problem. In the setting of FSGSS, pre-assumed signer can give the proof of forgery.

So signature process can be stopped. That's why it is also known as FSGSS. Advantage of FSGSS is that if a computationally unbounded adversary forges a signature then proof of forgery shows that ECDLP is solved and so process must be stopped.

6. CONCLUSION

We propose the first FSGSS based on ECDLP, which is more efficient and secure due to use of Elliptic Curves and can be practically used in the situations if there is a need to hide identity of signers who can sign on behalf of Group. Our proposed scheme provides security to the actual signer against computationally unbounded adversary. It can also be used in Block-chain applications. In future, we will define a formal security model and will prove security against "adaptive chosen message attack in random oracle model". In addition, we are planning to propose its implementation/experiments in organizations.

REFERENCES

[1] Jonathan Jen-Rong Chen, Yi-Yuan Chiang, Wang-Hsin Hsu, and Wen-Yen Lin, Fail-Stop Group Signature Scheme, Security and Communication Networks, 2021, https://doi.org/10.1155/2021/6693726.

[2] M.Rahul, N.Kohli, R.Agarwal, Facial Expression Recognition using Local Multidirectional Score Pattern Descriptor and Modifid Hidden Markov Model International Journal of Advanced Intelligence Paradigm(Inderscience),Vol.18,No. 4, 2021.

[3] V.Yadav, M.Rahul, R.Shukla A New Improved Approach for Feature Generation and Selection in Multi- Relational Statistical Modelling using ML Journal of Scientific and Industrial Research, 79, 1095-1100, Dec 2020.

[4] Y. Cao, Decentralized group signature scheme based on block-chain, Proceedings of the 2019 International Conference on Communications, Information System And Computer Engineering (CISCE), Haikou, China, July 2019.

[5] Sun, Y., Liu, Y. & Wu, B. An efficient full dynamic group signature scheme over ring. *Cybersecurity* 2, 21 https://doi.org/10.1186/s42400-019-0037-8, 2019.

[6] Ling, S, Nguyen K, Wang H, Xu Y, Lattice-based group signatures: achieving full dynamicity with ease. In: Gollmann D, Miyaji A, Kikuchi H (eds) Proceedings of Conference ACNS: 10-12 July 2017; Kanazawa, 293–312. Springer, Beilin Heidelberg 2017.

[7] Libert, B, Ling S, Nguyen K, Wang H (2016b) Zero-knowledge arguments for lattice-based accumulators: logarithmic-size ring signatures and group signatures without trapdoors. In: Fischlin M Coron JS (eds) Proceedings of Conference EUROCRYPT: 8-12 May 2016; Vienna, 1–31, Springer, Beilin Heidelberg, 2016.

[8] Bootle, J, Cerulli A, Chaidos P, Ghadafi E, Groth J (2016) Foundations of fully dynamic group signatures. In: Manulis M, Sadeghi AR, Schneider S

(eds) Proceedings of Conference ACNS: 19-22 June 2016; Guildford, 117–136. Springer, Beilin Heidelberg, 2016.

[9] The Certicom Corporation, SEC 2: Recommended Elliptic Curve Domain Parameters, www:secg:org=collateral=sec2f inal:pdf.

[10] Shamus Software Ltd., Miracl library, http://www.shamus.ie/index.php?page=home.

[11] Tiwari N, Padhye S, Provable secure proxy signature scheme without bilinear pairings. Int. J. Commun. Syst. (2011), DOI: 10.1002/dac.1367.

[12] Neal Koblitz: A Course in Number Theory and Cryptography, Springer Verlag Berlin, 1994.

[13] David Chaum: Group Signatures, Advances in Cryptology-EUROCRYPT'91, LNCS 547, pp. 257-265, 1991. Q Springer-Verlag Berlin Heidelberg 1991

[14] Michael Waidner and Birgit P.: The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability, Advances in Cryptology EUROCRYPT '89, LNCS 434, Springer Verlag, p. 690, 1989.