SECURE AND EFFICIENT DECENTRALIZED GROUP KEY ESTABLISHMENT REVISED ELGAMAL PROTOCOL FOR GROUP COMMUNICATION

Shailendra Singh Tanwar [#1], Dr. Suneet Chaudhary [#2]
[# 1] *M.Tech (CSE) Student, Dehradun Inst. of Technology, Dehradun*
[#2] *Associate Professor*, Department of Computer Science Engineering,
Dehradun Inst. of Technology, Dehradun
[1] *shailensingh9@gmail.com*, [2] *suneetcit81@gmail.com*

***Abstract*— in distributed systems it is sometimes necessary for users to share the power to use a cryptosystem. The system secret is divided up into shares and securely stored by the entities forming the distributed cryptosystem. We propose a new Multi signature scheme without a trusted third party (TTP), based on a round optimal, publicly verifiable distributed key generation (DKG) protocol. In this propose system, we define a new propose ElGamal algorithm, in that ElGamal algorithm has two random numbers. The original ElGamal algorithm is that, it has only one random number. In order to improve its security, the proposed scheme adds one more random number. The security of the proposed signature scheme is the same with the ElGamal signature scheme which is based on the difficult computable nature of discrete logarithm over finite fields. In this paper, the algorithm is proposed to enhance the security and usage of more random number to make algorithm more complicated, which can also make the link between the random number and the key more complicated. The scheme presented in this paper after analysis showed that the security level is kept high by using two random numbers and the time complexity is reduced.**

Keywords: Distributed key generation, Public Key Cryptography, ElGamal Algorithm, Discrete Algorithm.

I. INTRODUCTION

We all are familiar with the concept of signature. A person signs a document to show that it originated from him or was approved by him. In other words, signature is a method to authenticate any document. Thus the message, data, documents or any other materials in electronic format has to be signed electronically. The Multi signature scheme avoids conspiracy attacks without attaching a random secret to shares. The group public key is dependent on the number of group members, as the signature verifier needs the individual public values of all group members to compute the subgroup public key that is required to verifying the signature [1]. The main contribution to the communication overhead, post signature generation is made by the size of the group signature. The signature size of Multi signature schemes is bound to be dependent on the threshold parameter. Public-key cryptography refers to a cryptographic system requiring two separate parts, one private and one of which is public. Although different, the two parts of the key provide encryption using mathematical algorithms that scrambles the data when it is sent and decodes it once it is received. One key locks or encrypts the plaintext, and the other unlocks or decrypts the cipher text [2]. Neither key can perform both functions by itself. The public key can be distributed to those that you want to communicate with but only you can know the private key. Public-key cryptography is widely used. It is an approach used by many cryptographic algorithms and cryptosystems. It underpins such Internet standards as Transport Layer Security (TLS). There are three primary kinds of public key systems: public key distribution systems, digital signature systems, and public key cryptosystems, which can perform both public key distribution and digital signature services. Diffie–Hellman key exchange is the most widely used public key distribution system, while the Digital Signature Algorithm is the most widely used digital signature system [3]. The two main uses for public-key cryptography are: Public-key encryption: a message encrypted with a recipient's public key cannot be decrypted by anyone except a possessor of the matching private key – it is presumed that this will be the owner of that key and the person associated with the public key used. This is used to ensure confidentiality. Second one is Digital signatures: a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender had access to the private key and, therefore, is likely to be the person associated with the public key used [5]. The proposed discrete logarithm-based Multi signature scheme is also proactively secure, allowing for distribute key regeneration (DKR) to a new access structure and periodic

distributed key updating (DKU) to mitigate attacks from an active/mobile adversary. The proposed discrete logarithm-based Multi signature scheme is made proactively secure by periodically updating secret shares and facilitating changes in group membership by allowing an authorized subset of existing group members to redistribute secret shares to a new access structure. In this paper, we propose a ElGamal algorithm with variation that is useful in security purpose and also define multisignature scheme with signature generation and confirmation. Therefore, we explain all these in distributed key generation & confirmation scheme.

II ANALYSIS OF ELGAMAL ALGORITHM & MULTI SIGNATURE

The efficiency of Multi signature may be based on the following four criteria- Group Public Key Length, Group-Oriented Signature Size, Communication Cost of Signature Generation and Verification, Computational Cost of Signature Generation and Verification. In Group Public Key Length, The Multi signature scheme avoids conspiracy attacks without attaching a random secret to shares. The group public key is dependent on the number of group members, as the signature verifier needs the individual public values of all group members to compute the subgroup public key that is required to verifying the signature [4]. Difficulty will be experienced with this scheme when trying to eliminate the need for a trusted authority to distribute the initial group key shares. The proposed Multi signature scheme uses the long-term private keys of the members, provided by a public key infrastructure, to avoid conspiracy attacks even if colluding members derive or control the group secret. In second criteria, Group-Oriented Signature Size, the main contribution to the communication overhead, post signature generation, is made by the size of the group signature [6]. The signature size of Multi signature schemes is bound to be dependent on the threshold parameter. In third criteria, we define in terms of communication cost, the individual and threshold signature generation mechanisms of all the existing Multi signature schemes and the proposed scheme are almost equivalent. Multiparty signature schemes constructed from ElGamal type (discrete logarithm-based) signature variants are bound to be interactive. In Computational Cost of Signature Generation and Verification, it is assumed that the system parameters are chosen to yield the same time complexity for exponentiations, multiplications, and summations [7]. Although summations and, in some cases, multiplications contribute to an insignificant fraction of the overall time complexity, these operations are still included for the sake of completeness. The main problem with the ElGamal digital signature scheme was message recovery. The original ElGamal scheme does not contain message recovery techniques and some attacks are possible on it. As same as the ElGamal signature scheme, the improved signature scheme is also based on the difficulty in discrete logarithm finite field [11]. Eventually the improved signature scheme was analyzed on security and time complexity. The analysis shows that the security of the improved signature scheme is higher than original one, and has a relatively low time complexity. ElGamal signature scheme was first introduced in 1985. In this signature scheme the public key is used for encryption and signature verification [8]. ElGamal algorithm consists of three components- Key Generator, Encryption & Decryption. (i) Key Generation- A generates an efficient description of a multiplicative cyclic group G of order q with generator g. Then, A choose a random x from {1,2….q-1}. After that A compute $h=g^x$. At last A publishes h, along with description of G, q, g as his public key & remains x as his private key which must be secret. (ii) In encryption, we encrypt a message m to A under his public key (G, q, g, h). B choose a random y from {0, 1,…,q-1}, then calculates $C_1= g^y$. Then, B calculates the shared secret $S=h^y$. After this, B converts his secret message m into an element m□ of G. Now, B calculates C2= m□ .S, then B sends cipher text (C_1, C2) = (g^y, m□ .h^y) = (g^y, m□ .$(g^x)^y$) to A. (iii) Decryption is used to decrypt a cipher text (C_1, C2) with his private key x. then, A calculates the shared secret S= C_1x. After that, we compute m□ = $C_2.S^{-1}$, & convert back into plaintext message m.S^{-1} is C2.S^{-1}= m□ .h^y.$(g^{xy})^{-1}$ = m□ .g^{xy}.g^{-xy} = m□ . So, this is the procedure of original ElGamal algorithm [15].

III PROPOSED ALGORITHM

This section proposes a new ElGamal Algorithm. In original ElGamal Algorithm, we use only one random number, so for security purpose, we can say that to improve security one more random number is used due to which the difficulty of deciphering key increases. If we increase in signature generation equations like $R=g^x$ mod p, then the original algorithm will become complicated & more difficult to decipher [12]. So, we define a new algorithm as follow:

Step 1: A large prime number s is produced by system, b is generator of Z_s*, y ($1\leq y \leq s-1$) is the signer's private key, so signature public key $X = b^y$ mod s…..(1.1), So now public key is [s, b, x] and private key is [y].

Step 2: Define two different random numbers N and p are randomly selected by system where p, n, y must be co-prime (and $1 \leq p, N, \leq p-1$).

Step 3: Determine digital signature of the message M where $1 \leq M \leq s-1$.
$R = b^N \bmod s$……. …….. (1.2)

$T = (N + Ry) \bmod s-1$ …..(1.3)

$U = M * b^{-p} \bmod s$ …… (1.4)

$V = (p + TU) \bmod s-1$ …..(1.5)

So, now digital signature is [R, U, V].

Step 4: The signature of plain text M is [R, U, V] is sent to the specified users by system. The users use following equation to verify the correctness of plaintext M digital signatures.

1.) Recovery of the message M

$M = U * b^V * R^{-U} * X^{-RU} \bmod s$ …..(1.6)
Proof of message recovery
$M = U * b^V * R^{-U} * X^{-R\,U} = M * b^{-p}\ b^V * R^{-U}\ X^{-RU}$ by (1.4)

$= M * b^{-p}\ b^V * b^{-N\,U}\ X^{-R\,U}$ by (1.2)

$= M * b^{-p}\ b^V * b^{-N\,U} * b^{-y\,R\,U}$ by (1.1)

$= M * b^{-p}\ b^V * b^{-U(N+Ry)} = M * b^{-p}\ b^V * b^{-U\,(T)}$ by (1.3)

$= M * b^{-p}\ b^{(p+TU)} * b^{-U\,(T)}$ by (1.5)

$= M * b^{p+TU-TU-p} = M * b^0 = M$ original message

2.) Confirmation of Digital Signature
$C_1 = M^U \bmod s$ …… (1.7)

$C_2 = (U\,(b^V\,(R * X^R)^{-U}))^U \bmod s$ …. (1.8)

If $C_1 = C_2$, then signature is authentic and original message is recovered.

If $C_1 \neq C_2$, then signature is not authentic and original message is not recovered.
Proof of Confirmation equation:

$C_2 = (U\,(b^V\,(R * X^R)^{-U}))^U \bmod s$

$= U^U * (b^V\,(R * X^R)^{-U})^U \bmod s$

$= M^U * b^{-p\,U} * (b^V\,(R * X^R)^{-U})^U \bmod s$ by (1.4)

$= M^U * b^{-p\,U} * (b^V\,(R * X^{-U\,R}))^U \bmod s$

$= M^U * b^{-p\,U} * (b^V\,(b^{-NU} * b^{-y\,U\,R}))^U \bmod s$ by (1.1) & (1.2)

$= M^U * b^{-p\,U} * (b^{p+TU} * b^{-NU} * b^{-y\,U\,R})^U \bmod s$ by (1.5)

$= M^U * b^{-p\,U} * (b^{p+TU} * b^{-U(N\,+\,R\,y)})^U \bmod s$

$= M^U * b^{-p\,U} * (b^{p+TU} * b^{-U(T)})^U \bmod s$ by (1.3)

$= M^U * b^{-p\,U} * (b^{p+TU\,-UT})^U \bmod s$

$= M^U * b^{-p\,U} * (b^p)^U \bmod s = M^U * b^0 \bmod s = M^U \bmod s$

$= C_1$

In the beyond cited proposed algorithm, the similar message M corresponded to the different digital signature [R, U, V] for the different random number N, p [14]. After they can be all confirmed through the equations beyond and improves the uncertainty of the signature, because N & p are co-prime and in equations p, N, T and y are unknown values. So, from this we can improve the security.

In this proposed algorithm, we first define Signature Generation; in signature generation process we first define a prime number as define in above algorithm s, after that we calculate a private key that is calculated with the help of prime number s, generator b. So, when signature is generated, we determine it with the private key [13]. In figure 1, we define the signature generation process. When Signature generation is completed then digital signature [R. U. V] is generated, with this we confirm signature. In Figure 2, we explain the signature confirmation process.

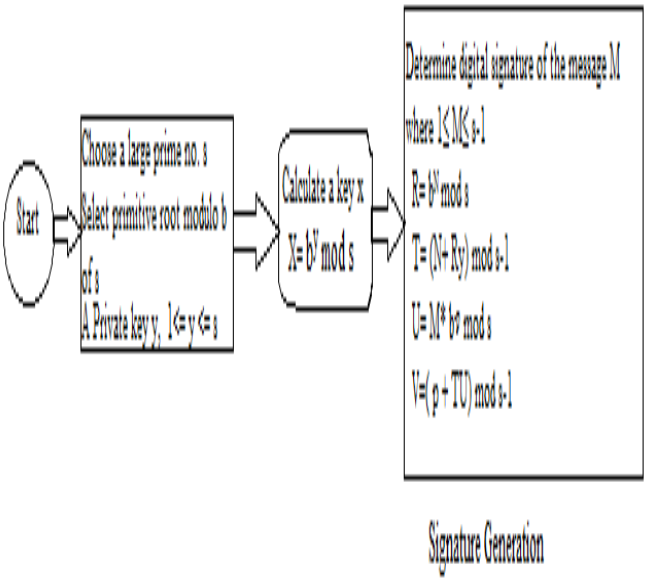

Figure 1: Signature Generation Process

Figure 2: Signature Confirmation

IV CONCLUSION

In this paper, we explained a new variant of algorithm. Our proposed scheme completely withstand with the message recovery technique. In this algorithm we have used two random numbers (N & p) that make the algorithm more secure. The values of p, y & N are used to generate the digital signature and randomly. T is unknown by the verifier and unknown value also dependant on p & y. There are various fields in which it helpful as Forgery attack as it is difficult to find y because T, N and y are all unknown in equation (1.3). If U and V both are known then also it is difficult to solve the equation (1.5) because there are two unknown values p and T in equation (1.5). Therefore, our algorithm is secure. The signature scheme proposed beyond can recover message from the signature itself and parameter reduction attack is not applicable on it. The method fully supports the message recovery feature, as message can easily recovered from the signature, so there is no need to send message along with the signature. Key generation use safe and large primes. We can also use this for signing large documents such as files etc. Hence the proposed signature scheme can be applicable in areas like e-banking, e-commerce etc.

VI REFERENCES

[1] An Efficient ID-based Digital Signature with Message Recovery Based on Pairing", Raylin Tso and Chunxiang Gu and Takeshi Okamoto and Eiji Okamoto, 2007, ISBN: 3-540-76968-4 978-3-540-76968-2.

[2] R. L. Rivest, A. Shamir, L. Adleman "A method for obtaining digital signatures and public-key cryptosystems", Comm. of the ACM, Vol. 21, (1978), S. 120-126.

[3] K. Nyberg, R. Rueppel, "Message recovery for signature schemes based on the discrete logarithmic problem ", Pre-proceedings of Eurocrypt '94, University of Perugia, Italy, (1994), pp. 175-190.

[4] J. M. Piveteau, "New signature scheme with message recovery" Electronics Letters, Vol. 29, No. 25, (1993), pp. 2185.

[5] Chenn Zhi-Ming. "An improved encryption algorithm on ElGamal algorithm" Computer Applications and Software, 2005, 22 (2): 82-85.

[6] Wang Li, Xing Wei, Xu Guang-zhong. "ElGamal public-key cryptosystem based on integral quaternions" Computer Applications, 2008, 28(5):1156-1157.

[7] Cao Tian-jie, Lin Dong-dai. "Security analysis of a signature scheme with message recovery" Journal of Zhejiang University (Science Edition), 2006, 33 (4): 396~ 397.

[8] William Stallings, "Cryptography and Network Security: Principles and Practice", Second Edition.

[9] T. EIGamal, "A public key cryptosystem and a signatures scheme based on discrete logarithms", IEEE Trans. Inform. Theory.

[10] J. He and T. Kiesler. Enhancing the security of ElGamal's signature scheme. In Computers and DigitalTechniques, IEE Proceedings-, volume 141, pages 249-252. IET, 1994.

[11] C.-M. Li, T. Hwang, and N.-Y. Lee, "Threshold-Multisignature Schemes where Suspected Forgery Implies Traceability of Adversarial Shareholders," Proc. Advances in Cryptology—EUROCRYPT '94, May 1994.

[12] S.F. Tzeng, C.Y. Yang, and M.S. Hwang. A new digital signature scheme based on factoring and discrete logarithms. International Journal of Computer Mathematics, 81(1):9-14, 2004.

[13] Wang Qing- ju, Kang Bao- yuan, Han Jin- guang "Several new ElGamal Type Digital Signature Schemes and Their Enhanced Schemes" [J] Journal of East China Jiaotong University, 2005, 22(5): 127-138.

[14] Zhang Hui-ying, Zhang Jun. "Research and Design of an Improved ElGamal Digital Signature Scheme" [J] Computer Engineering and Science, 2009, 31(12): 35-38.

[15] Omar Khadir, "New Variant of ElGamal Signature Scheme", Int. J. Contemp. Math. Sciences, Vol. 5, 2010, no. 34, 1653 – 1662.

ACKNOWLEDGEMENT

I acknowledge my sincere and profound gratitude to my guide, Dr. Suneet Chaudhary, for his valuable guidance, dedicated concentration and support throughout this work. I also acknowledge my sincere gratitude to authorities of Dehradun Institute of Technology, Dehradun and other teaching staff of Computer Science Engineering for their help and support. I am also thankful to my fellow research members for their cooperation.