Serdica
Mathematical Journal
Сердика
Математическо списание

Serdica Math. J. **47** (2021), 285–290

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

MODIFIED ELGAMAL SIGNATURE WITH SECRET KEY PAIR AND ADDITIONAL RANDOM NUMBER

Manoj Kumar Chande

Communicated by V. Drensky

Abstract. ElGamal digital signature has numerous applications in real time situations. Due to its utility and popularity, security threats and challenges are increasing day by day for this signature scheme. This paper introduces a variant of ElGamal signature scheme, mainly after analyzing the existing weaknesses of the scheme where the security depends on one private key only. To overcome this, our scheme consists of a private key pair and an additional random number which makes the relation between the secret key and the randomly chosen number used more complicated. The cryptographic security of the proposed scheme is relatively much higher than the existing ElGamal signature scheme in literature.

1. Introduction and preliminaries. In 1985, ElGamal [2] proposed a public key cryptosystem (PKC) and a digital signature scheme, where their safety relies on the Discrete Logarithm Problem (DLP). The ElGamal PKC is very efficient and safe to carry out private correspondence and to sign a document digitally on a network. This scheme is also the foundation of many of the important special-purpose schemes [6, 3]. There exist different signatures for a message because of the random selection of various parameters, messages and there is a

2020 *Mathematics Subject Classification:* 94A60.
Key words: ElGamal signature scheme, discrete logarithm problem, random number.

correspondence between every signature specifically chosen random number [8]. This is one of the threats against the security of the ElGamal Signature Scheme (ESS).

Let us consider a finite cyclic group G of order n. The element g is a generator of the group G and $y \in G$ another element. The discrete logarithm of y to the base g, denoted by $\log_g y$, is the unique integer $x \in \mathbb{Z}_n$, such that $y = g^x$. The ESS consists of two steps:

(i) Signing Step: The pair (a, b) is the signature for a specified message M. It can be obtained by a random selection of an integer k such that $GCD(k, p-1) = 1$.

$$a \equiv g^k \pmod{p},$$
$$b \equiv k^{-1}(M - xa) \pmod{(p-1)}.$$

(ii) Verification Step: To validate the signature $s = (a, b)$, verifier uses the equation given below

$$y^a a^b \equiv g^M \pmod{p},$$

where $y \equiv g^x \pmod{p}$.

In the ESS, the private key is the only entity which provides security to the scheme and if that is compromised due to some attack, then there is no security at all [4]. If an attacker finds a relation between the chosen random numbers, then he or she can comfortably target the secret key.

Let Alice be using the ESS to sign two different messages. Then she must choose two different values of k. If she chooses the same k for two different messages M_1, M_2, then the value of a will be the same for both the signatures and immediately Eve will notice that the same value for k is used repeatedly. Let b_1 and b_2 be two different values for b. Then Eve knows that

$$b_1 k - M_1 \equiv -xa \equiv b_2 k - M_2 \pmod{(p-1)}.$$

This implies

$$(b_1 - b_2)k \equiv (M_1 - M_2) \pmod{(p-1)}.$$

Now she can solve this for k. If $GCD((b_1 - b_2), p-1) = r$, then there will be a fair chance to solve this congruence relation because usually the number of solutions r is very small, so there are few feasible values for k.

Next, for every feasible value of k, Eve can compute g^k and find out the one which gives a. Finally Eve solves $xa \equiv (M_1 - kb_1) \pmod{(p-1)}$ for x, as she knows the specific value of k. There are $GCD(a, p-1)$ probable values of x.

Eve can compute g^x for every probable value of x, till she gets the required value of y. Ultimately Eve knows the secret key x, so she can do forgery by producing Alice's genuine signature.

Thus, the wrongly chosen public key or insecurely chosen random number will make scheme vulnerable. Therefore, the signer has to choose the random numbers very carefully [1]. The choices for random numbers are reduced greatly because of the restriction on its reusability, and this affects the algorithm very much because the random number k cannot be reused.

Nowadays, the flow of data is rigorously increased in any kind of communication network, so the need for digital signature is also increased. For the security concern, the signer has to change its private key value from time to time and the value of the public key too. To make this practice on a regular basis it is also required to communicate the new public key value to their customers as soon as it gets updated or else it will affect the business. Sometimes it is required to use the same signature later again, so the chosen number is required to be remembered and stored for a future use. As the number of signatures goes on increasing, the space to store the random number used has also to be increased.

Li, Shen, Chen [5] proposed an improved ESS, again by introducing an additional random number to the signature scheme. Here the additional random number is used to make deciphering of the key more difficult. They further claimed that the security of their scheme is better with reduced time complexity.

Motivated by the above works, in this work, an improved ESS is proposed. We introduce two random numbers, one random number to generate a private key pair and an additional random number to make the process of deciphering more difficult by giving strength to the relation between the secret key and the random number used.

Our paper is organized as follows: In the next section, we have given the improved ESS, In Section 3, security analysis of the proposed ESS is given, some conclusions are drawn in the last Section 4.

2. Proposed signature scheme. We use the basic ESS and implement the ideas of improvement.

(1) The process of the key generation is similar to the one which was used in the ElGamal PKC. Suppose a prime p is sufficiently large so that it is difficult to find the solution of DLP in $\mathbb{Z}_p^*$. Let $g \in \mathbb{Z}_p^*$ be a primitive element. The signer chooses a secret key $x < p - 1$. The public key of the individual signer is calculated by

$$y \equiv g^x \pmod{p}$$

and it is available publicly.

(2) Here we introduce the second secret key in the form of a random number d, which can be obtained by using an arbitrarily selected number e, such that

$$e\,d \equiv 1 \pmod{(p-1)}. \tag{2.1}$$

(3) Next, two different numbers t and k are randomly selected such that both are co-prime to x and there must exist their inverse modulo $(p-1)$. Further the values a and c are calculated by the equations

$$a \equiv g^k \pmod{p}, \tag{2.2}$$

$$c \equiv g^t \pmod{p}. \tag{2.3}$$

(4) The value b is computed on the basis of the previously obtained values as follows:

$$b \equiv (M - xa)k^{-1} \pmod{(p-1)}, \tag{2.4}$$

$$M\,d \equiv (xa + kc + tb) \pmod{(p-1)}. \tag{2.5}$$

Now the required private keys are (x, d), the public keys are (p, y, g, e) and the tuple (a, c, b) is the signature for the plain text M.

(5) The tuple (a, c, b), is sent to the respective client by the system. To verify the correctness of the digital signatures on the plain text M, the client uses the signature verification equation

$$g^{Md} \equiv (y^a a^c c^b)^e \pmod{p}. \tag{2.6}$$

The signature is the valid one, if the above equation (2.6) holds.

3. Analysis of the proposed scheme. In the original ESS, it is required that two different random numbers are used for two different signatures. If they are same, then it is easy for the adversary to mount a forgery attack. To enhance the resistance against the attacks is one of the objective to introduce random numbers. The attacker has no method to find the secret keys (x, d), which are used to generate the signature. The attacker have to encounter the difficulty of DLP and the intractability of the decomposition of randomly chosen prime numbers to attack on the secret keys directly in the proposed scheme in this paper.

Now we analyze the role of the additional random number in the proposed scheme. This improvement helps us to avoid the threats or attacks. Some of them are:

1. **Private Key Attack:** In the proposed ESS scheme an added random number is used to sign. Initially the attacker obtains a solution set of the secret key x and determines the secret key, but it is mathematically infeasible for him or her to find out k and t by the encrypting equation (2.5). Similarly, the attacker will not be able to use equations (2.2) and (2.3) to validate the secret key x which is already known to him or her. Therefore these types of attacks on the ESS are not going to succeed unless and until there exists an efficient algorithm for solving the DLP.
2. **Arbitrary Forged Signature Attack:** The signature verification equation is targeted in such a type of a forgery attack. It is computationally infeasible to find out b through the signature verification equation (2.6).
3. **Substitution Attack According to Known Signatures:** As more parameters are introduced in the improved algorithm, the possibility to adopt a message M can be reduced naturally. If a method is derived to forge the proposed signature, then still the computational and time complexity is more than that to forge the original ESS, while in the traditional digital signature algorithms, an attacker can still easily access signer's signature of the message or document M, and then forge a number of legitimate digital signatures [7]. To mount an attack on our scheme with additional random numbers is very difficult.

In our scheme an extra random number t is there, which is not there in the original ESS. So the calculation is also increased correspondingly. All the computations regarding k in the original ESS must be repeated for t. The calculation involved in the signature generation (2.5) and its verification (2.6) is a little bit complex. The computational load is obviously increased and therefore the efficiency will be decreased in comparison to the original ESS, but the primary goal is achieved by strengthening the security of the scheme.

4. Conclusion.

In the proposed scheme, the security of ESS is strengthened with the provision of an additional secret key, which closely associates to the signature and provides safety against attacks on the private key. This improvement also helps to remove the weakness that the random number cannot be reused. The signature scheme has also been improvised by introducing an additional random number, which makes the link more complex between the random number already used in the standard ESS and the private key. This improvement also results in the increase of difficulty for an attacker to attack on the random number used in the algorithm. The security and efficiency of the ESS is enhanced in two ways, without affecting the original algorithm. Therefore, the signature scheme proposed has a wider scope of applications.

REFERENCES

[1] Z. F. Cao, J. G. Li. A threshold key escrow scheme based on ElGamal public key cryptosystem. *Chinese J. Comput.* **25**, *4* (2002), 346–350 (in Chinese. English, Chinese summary).

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

[3] A. Ghodratabadi, H. M. Ziyabar, H. Bahramgiri. ElGamal signature for content distribution with network coding. *International Journal of Wireless & Mobile Networks*, **6**, *2* (2014), 61–66, DOI: 10.5121/ijwmn.2014.6206.

[4] B. C. Hu, D. S. Wong, Z. Zhang, X. Deng. Certificateless signature: a new security model and an improved generic construction. *Des. Codes Cryptogr.* **42**, *2* (2007), 109–126.

[5] Liao Xiao-fei, Shen Xuan-jing, Chen Hai-peng. An improved ElGamal digital signature algorithm based on adding a random number. In: 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, vol. 2, 2010, 236–240, DOI:10.1109/NSWCTC.2010.190.

[6] A. J. Ordonez, R. P. Medina, B. D. Gerardo. Modified El Gamal algorithm for multiple senders and single receiver encryption. 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), 28–29 April 2018, 201–205.

[7] H. Q. Wang, M. H. Xu, X. J. Guo. Cryptanalysis and improvement of several certificateless digital signature schemes. *Journal of Communications* **28**, *5* (2008), 88–92.

[8] L. Wang, W. Xing, G. Xu. ElGamal public-key cryptosystem based on integral quaternions. *J. Comput. Appl.* **28**, *5* (2008), 1156–1157 (in Chinese. English summary).

Shri Shankaracharya Institute of Professional Management and Technology
Raipur, 492015, Chhattisgarh, India
e-mail: `manojkumarchande@gmail.com`

Received September 4, 2021
Accepted November 1, 2022