Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 12, December 2015, pg.119 – 124

Secure Proxy Digital Signature Scheme using Digital Signature Standard with Random Key Generation Process

Mohammad Amjad

Department of Computer Engineering, Jamia Millia Islamia, India
E-mail: mamjad@jmi.ac.in

Abstract- Now a days digital signature schemes stress on secure, authentication and verification mechanism of electronic signature used in electronic transaction system. In this sequence proxy digital signature may play an important role to achieve the security goals. Proxy Digital signature is the process of authorized signatory of the document by one person on behalf of other one. None of the proxy signature schemes which have been proposed up to now, are based on Digital Signature Standard (DSS) cryptosystem with changing random key values dynamically. Therefore, these proposals have unavoidably been considered infeasible because of obvious security weaknesses, so they suffer from new attacks. Consequently, I propose a new proxy signature scheme which combines the Digital Signature Standard (DSS) properties with random key generation. Finally, a DSS proxy digital signature system is implemented and its time complexity is analyzed.

Keywords: Digital signature, Digital Signature Standard, Random key generator, verification method, certificate Authority, Cryptography.

1. INTRODUCTION

Proxy signature allows user A i.e. sender of the message to delegate his signing capability to another user B called the proxy signer. Then the proxy signer B can sign original messages on behalf of the original signer A. Then the verifier, which knows the public keys of original signer and a proxy signer, can check a validity of a proxy signature issued by a proxy signer. In general three types of delegations are used: full delegation, partial delegation and delegation by warrant. Full delegation proxy signature scheme is analogous to giving the full authority to anybody for doing the signature and will have prior approval by the original signer. Proxy signature with all the set of keys used by other signer a proxy signer uses the same private key as an original signer and creates the proxy signature as an original signer does. Partial delegation is analogous to signing the original sign with the partial information given to proxy signer [3][4]. This means the proxy signer does not know all the detail of the original signer, even though he will be able to create the original sign. In the third type of proxy signature, the analogous of this signature is that the original signer may give a type of certificate called warrant and this warrant will be used as a proof of legal signature to be performed by the proxy signer. This means that whenever the proxy signature is done by the proxy signer, he must provide a warrant as a proof of legal signee of behalf of original signer. Proxy signatures can be used in a number of applications like e-cash, distributed systems, grid computing, mobile agent applications, distributed shared object systems, global distribution networks, communications and electronic commerce [5][7].

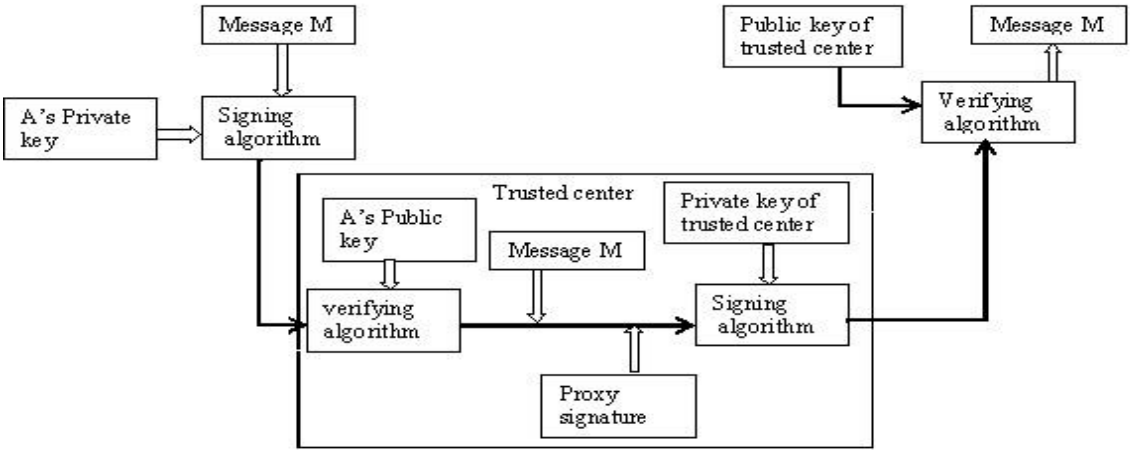

Figure 1: Proxy Digital Signature scheme

Desirable security properties of proxy signatures are as follows:
• Unforgeability: A designated proxy signer can create a valid proxy signature on behalf of the original signer. But the original signer and other third parties cannot create a valid proxy signature.
• Identifiability: Anyone can determine the identity of the corresponding proxy signer from the proxy signature.
• Verifiability: The verifier can be convinced of the original signer's agreement from the proxy signature.
• Distinguishability: Proxy signatures are distinguishable from normal signatures by everyone.
• Non- repudiation: Once a proxy signer creates a valid proxy signature, he cannot deny the signature creation.
• Prevention of misuse: The proxy signer cannot use the proxy key for other purposes than it is made for. That is, he cannot sign message with the proxy key that have not been defined in the warrant. If he does so, he will be identified explicitly from the warrant.

2. RELATED WORK

A number of new schemes and improvements have been proposed for the generation of proxy signature; however, most of them do not fully meet all the security requirements of a proxy signature scheme. Kim, Park proposed a threshold proxy signature, in which the original signing power is shared among a delegated group of *n* proxy signers such that only *t* or more of them can generate proxy signatures cooperatively [1][3]. Lee, Kim proposed non-designated proxy signature in which a warrant does not designate the identity of a proxy signer. So any possible proxy signer can respond this delegation and become a proxy signer. Furthermore, their scheme is used to design secure mobile agents in electronic commerce setting. One-time proxy signatures are suggested by N.-Y. Lee, T. Hwang, and C.-H.Wang. Lee, Cheon, and Kim investigated whether a secure channel for delivery of a signed warrant is necessary in existing schemes [3][7]. In contrast to the above mentioned schemes, which all are based on discrete logarithm cryptosystems, several RSA-based proxy signature schemes are proposed in B. Lee, H. Kim, and T. Okamoto, M. Tada, and E. Okamoto. The first work to formally define the model of proxy signatures is the recent work of Boldyreva, Palacio, and Warinschi [8][9]. These authors provide the first definition of fully hierarchical proxy signatures with warrants, supporting chains of several levels of delegation. Li et al. have proposed their generalization of proxy signature schemes. However, all of Li et al.'s schemes have a common security weakness. In Li et al.'s schemes, an adversary first intercepts a valid proxy signature generated by a proxy group [6][8]. From the intercepted proxy signature, the adversary can forge illegal proxy signatures being likely generated by the proxy group on behalf of an adversary. To overcome this weakness, an improvement is proposed. With the proxy key, the proxy signer can sign messages on behalf of the original signer. In cases where the proxy signer misuses the delegated rights, the original signer needs to revoke the proxy signer's signing capability. Currently, the proxy revocation protocols have four approaches.

i. One approach is to change the public key of the original signer. This approach is impractical because, once the public key of the original signer is changed; all signatures generated earlier by the original signer can no longer be verified.

ii. The other approach is to put proxy information on a public revocation list. Any verifier must ensure that the received signatures do not have proxy information on the list before verification.

iii. A proxy blind signature scheme based on Elliptic curve with proxy revocation is used. They achieve it by embedding non-blind time stamp in the signatures and thus the original signer can revoke delegation whenever necessary.

iv. When the original signer delegates his signing power to a proxy signer in the proxy warrant, it is included in a valid delegation period and other constrains on signing capability. Delegation period is the time allocation that must be done and will be terminated after the valid period expires. However, if the original signer wants to cancel the transactions before the time expires, the original signer then asks the allocated time slot in a public revocation list.

The information sent to the proxy signer is sent through a secure channel and it does not contain the identity information of the proxy signer. Here the original signer can play the role of the proxy signer as the key sent by the original signer is used as the proxy key. However, these approaches have two serious drawbacks. One is that, once the proxy information is posted, all valid proxy signatures generated using that information earlier can no longer be verified. The other drawback is that the size of the revocation list will grow unlimitedly. Also, there is no facility to send warrant messages to proxy signer and verifier, the verifier is unable to determine the time of proxy signature generation and also there is no provision for proxy signer revocation.

3. PROPOSED PROXY SIGNATURE SCHEME

a. Proxy Key Generation

1. User A selects a random $\Upsilon \in Z_q^*$, where gcd (Υ, p − 1) = 1 and computes $g' = (g * \Upsilon) \bmod p$.
Then, user A sends g′ to user B.
2. After receiving g′, B selects a random $k_B \in Z_q^*$, computes $r_B = g^{k}_B \bmod p$, and sets e = Hash $(g'^{k}_A) \bmod p$ and $s_B = (xe + k_A) \bmod q$. B then sends (r_B, s_B) to A. The pair (r_B, s_B) is a delegation proxy certification for proving that B delegates his signing capacity to A.
3. After the reception of the pair (r_B, s_B), A computes e'= Hash $(r^{\Upsilon}_B) \bmod p$ and verifies the validity by checking if $r_B = g^{s}_B * y^{-e'} \bmod p$.
4. If the equation $r_B = g^{s}_B y^{-e'} \bmod p$ holds, then A sets $s_A = (s_B * \Upsilon^{-1}) \bmod q$ as a proxy key, sets (s_A, $g^{s}_A \bmod p$) as public key pairs and sends the certificate request to the registration authority R_B.
5. According to certificate policy, R_B identifies user A and then forwards the certificate request to the certificate authority C_B for signing proxy certificate. The process of proxy key generating mechanism is shown in figure.

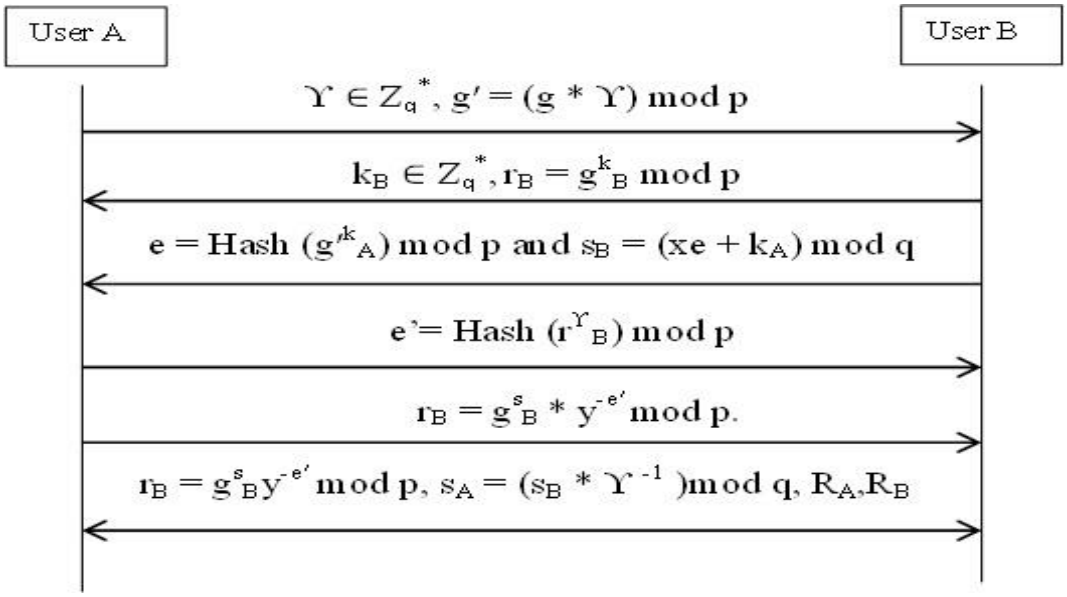

Figure 2: Proxy key generation and agreed upon by both the parties

3.2 Proxy Signature generation

Now to generate a proxy signature of a message m, user A should perform the following steps:
1. Select a random $k \in Z_q^*$.
2. Compute $r = (g'^{k} \bmod p) \bmod q$.
3. Set $s = k^{-1} (\text{Hash}(m) + (s_B * r)) \bmod q$.
4. $x_{i+1} = (ax_i + b) \bmod n$.
5. $s_1 = x_{i+1}$ XOR s
The proxy signature is the tuple (g′, r_B, e′, r, s_1).

In the above steps of proxy signature generation, the last step is used to generate the random number with the given function using variables a, b and n. The figure 3 for the proxy signature generation method is shown below.

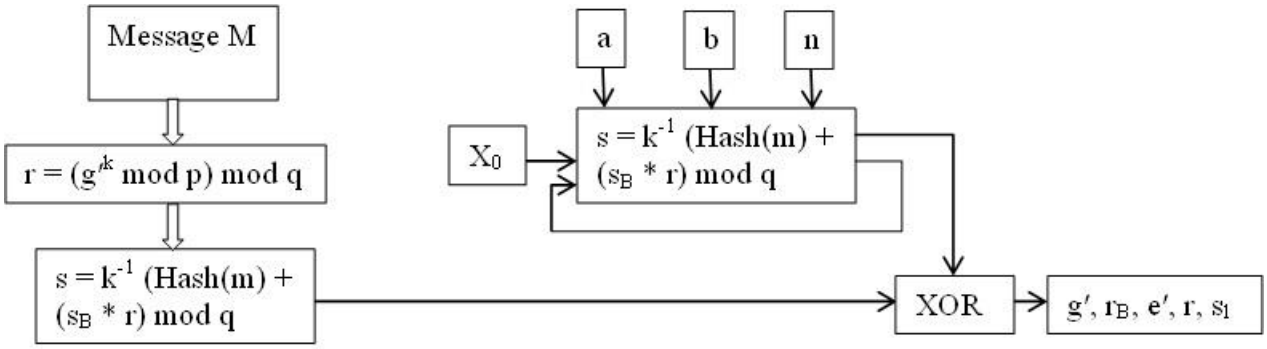

Figure 3: Proxy Signature generation

3.3 Proxy Signature Verification

The generated proxy signature is verified by the user B upon receiving the proxy signature tuple (g', r_B, e', r, s_1) on message m, then it is verified by using the following steps:

1. Certificate authority checks if the certificate of proxy key is valid.
2. Verify that $1 \leq r \leq q$ and $1 \leq s \leq q$; if not holds, reject the signature.
3. Compute $w = s^{-1} \bmod q$.
4. Compute $u_1 = w * \text{Hash}(m) \bmod q$, $u_2 = (r * w) \bmod q$, and $u_3 = (e' * u_2) \bmod q$.
5. Compute $v = (g'^{u1} * r^{u2}{}_A * Y^{u3}) \bmod q$.

The signature will only be accepted if v = r.

The process of proxy signature verification is shown in the following figure 4.

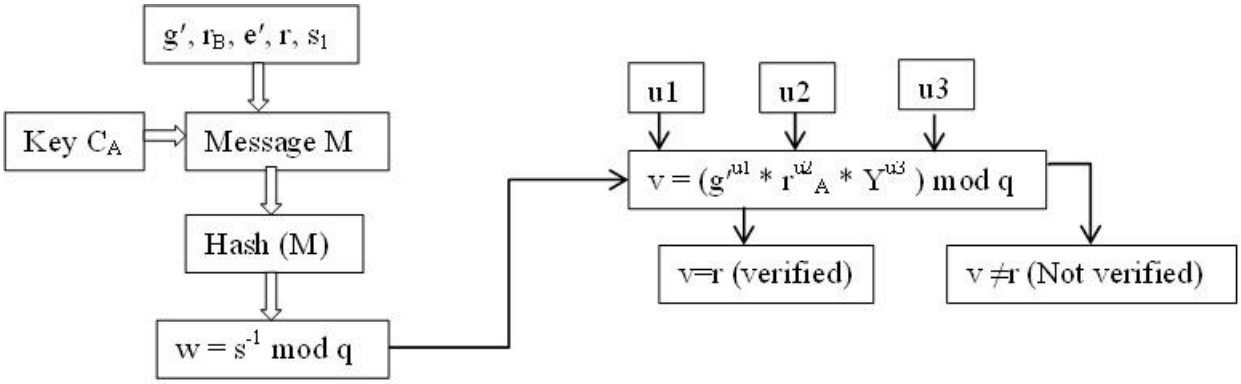

Figure 4: Proxy signature verification

4. Performance Analysis:

The proposed proxy digital signature scheme satisfies the basic requirements of a secure proxy signature scheme. We find that the scheme can be used to control delegation of any number of proxy signers for varying time periods. Any deceitful by the proxy signer is identified by the verifier i.e. the certificate authority. Though the original signer gives proxy information to all the proxy signers at the beginning of the method, the proxy signers will be able to generate proxy signatures only in their allotted time periods. Identity of the proxy signer is available in the information sent by original signer to proxy signer. There is a facility to send warrant messages to proxy signer and verifier. Proxy revocation is possible by which an original signer can revoke the signing capability given to proxy signer at his will and the verifier can also test whether the signature is from a revoked signer before verifying the proxy signature.

In the given Figure 5, we can observe the proxy signature generated by the user with the specified key generation. DSS validates and authenticates the message. This gives sufficient reason for the receiver to believe that the message is authentic and is sent by whom it appears to be sent from. If the signature is not verified by the competent authority, then the signature is simply discarded and shown in the list of not verified signature. Slight

tempering and changes with data makes the signature corrupt and message invalid. This cautions the receiver against believing in the contents of the message. Values of each variable used in the algorithm are shown separately. To assure functioning of the technique, the algorithm was run multiple times on different sets of data. The mean of five readings for each input set is tabulated. For representation of workload characteristics, six different sets of inputs of lengths in the range 10^3 to 10^{12} were taken. Table 1 lists the time required in seconds for hashing of inputs using SHA-1. For the smooth working of the proposed method we may use MD5 also, but the size of the generated proxy signature will be 64 bit long only. In our case using SHA-1 is used for message digest, it will be able to generate 160 bits long signature which guarantees more secure of the proposed method.
When we select the digital signature standard scheme in generating the proxy signature and on checking, a computing time is lesser in a proxy signature for warrant partial delegation than that by the warrant. Thus, a warrant delegation needs the time required for the signature generation and verification as shown in the figures 5 and 6 respectively.

Size of input (n characters)	Time (t in seconds)
10^3	$12.053*10^{-4}$
10^6	$4.032*10^{-3}$
10^7	$6.34*10^{-3}$
10^8	$6.72*10^{-2}$
10^{10}	5.340
10^{12}	18.481

Table 1: Time needed for proxy signature generation

Size of input (n characters)	Time (t in seconds)
10^3	$8.199*10^{-4}$
10^6	$10.201*10^{-4}$
10^7	$3.231*10^{-3}$
10^8	$12.924*10^{-3}$
10^{10}	$11.932*10^{-2}$
10^{12}	10.103

Table 2 : Time needed for proxy signature

```
C:\Users\Mohd. Amjad\Desktop\DSS>python
demonew.py
 Enter private key: 3
 PROXY SIGNATURE GENERATION
 Enter the file name : file1.txt
 Value of k= 11
 Value of x1= 19
 Value of y1= 17
 Value of r= 17
 Value of s= 23
 PROXY SIGNATURE VERIFICATION
 Value of w= 19
 Value of u1= 15
 Value of u2= 15
 Value of x0= 13
 Value of y0= 11
 Value of v= 17
 Since v=r, message verified and authentic.
--- 7.683542104 seconds ---
```

Figure 5: Proxy signature generation

```
C:\Users\Mohd. Amjad\Desktop\DSS>python
demonew.py
 Enter private key: 13
 PROXY SIGNATURE GENERATION
 Enter the file name : file1.txt
 Value of k= 7
 Value of x1= 15
 Value of y1= 11
 Value of r= 15
 Value of s= 11
 PROXY SIGNATURE VERIFICATION
 Value of w= 7
 Value of u1= 10
 Value of u2= 10
 Value of x0= 15
 Value of y0= 11
 Value of v= 15
 Since v=r, message verified and authentic.
--- 10.839400701 seconds ---
```

Figure 6: Proxy signature verification

5. CONCLUSION

The proxy signer may use the power of delegation of the signature even if we revoked the permission of generation of proxy signature. This causes the illegal use of the delegation by the proxy signer. To overcome this problem, here the concept of generation of a secret random number generation is introduced for each and every attempt of generation of proxy signature. In this procedure the random number generated by the original signer, is sent to the proxy signer who uses it in conjunction with its own signing key to produce proxy signatures. A proxy signature contains the warrant in the form of random number and the proxy signer's signature. The actual identity of the proxy signer is to be known even if the proxy signer is not identified by

traffic analysis. One of contribution of this paper is show that a direct implementation of this scheme is susceptible to a chosen plain text attack, since it is very difficult to guess about the randomly generated bits as well as for the text since it always generates a different bit pattern according to the chosen message.

REFERENCES

[1] L.,Buttyán, L.,Dóra, F.,Martinelli, M.,Petrocchi, 2010. Fast certificate-based authentication scheme in multi-operator maintained wireless mesh networks. Elsevier Computer Communications.

[2] Z.,Liu, Y.,Hu, X.,Zhang, H.,Ma, 2010. Provably secure multi-proxy signature scheme with revocation in the standard model. Elsevier journal of computer Communications.

[3] K. Shum and Victor K. Wei, "A strong proxy signature scheme with proxy signer privacy protection," in roceedings of 11th IEEE International Workshops on Enabling Technologies Infrastructure for Collaborative Enterprises, 2002, pp. 55-56.

[4] Sunder Lal, Awasthi A.: A scheme for obtaining a warrant message from the digital proxy signatures, cryptology e-print Archive Report 2005/073, (2005).

[5] Liu, Y., Wen H., and Lin C.: Proxy-Protected Signature Secure Against the Un-delegated Proxy Signature Attack, Computers and Electrical Engineering, Volume 33(3), pp. 177-185 (2007).

[6] Sunitha and Amberker: Proxy Signature Schemes for Controlled Delegation, Journal of Information Assurance and Security, 159- 174 (2008).

[7] Shao Z.: Provably secure proxy-protected signature schemes based on RSA, Computer Electronic engineering, 35, pp. 497-505 (2009).

[8] Cronin, E., Jamin, S., Malkin, T., McDaniel, P.: On the performance, feasibility, and use of forward-secure signatures. proceedings of the 10th ACM conference on Computer and communications security, 131–144 (2003).

[9] Zhou Y, Cao Z, and Lu R.: Provably secure proxy-protected signature schemes based on factoring, Application Math Computer164(1), pp. 83–98 (2005).

