A PROXY SIGNATURE SCHEME BASED ON NEW SECURE AUTHENTICATED KEY AGREEMENT PROTOCOL

H. Elkamchouchi[1], Heba G. Mohamed[2], Fatma Ahmed[3] and Dalia H. ElKamchouchi[4]

[1]Dept. of Electrical engineering, Faculty of Engineering, Alexandria University, helkamchouchi@ieee.org
[2]Dept. of Electrical engineering, Arab Academy for Science and Technology (AAST), heba.g.mohamed@gmail.com
[3]Dept. of Electrical engineering, Faculty of Engineering, Alexandria University, moonyally@yahoo.com
[4]Dept. of Electrical engineering, Faculty of Engineering, Alexandria University, Daliakamsh@yahoo.com

ABSTRACT

Proxy signature scheme permits an original signer to delegate his/her signing capability to a proxy signer and then the proxy signer generates a signing message on behalf of the original signer. So far, the proxy signature scheme is only applied in a special duration, when the original signer is not in his office or when he travels outside. The two parties must be able to authenticate one another and agree on a secret encryption key, in order to communicate securely over an unreliable public network. Authenticated key agreement protocols have an important role in building a secure communications network between the two parties. In this paper, we propose a secure proxy signature scheme over an efficient and secure authenticated key agreement protocol based on RSA cryptosystem.

KEYWORDS

Digital Signature, Proxy Signature, RSA, Key Agreement

1. INTRODUCTION

The cryptographic treatment of proxy signature scheme was first introduced by Mambo et Al.in 1996 [1]. Proxy signature is an important inquiry in the field of a digital signature. It permits an original signer to delegate his signing rights to a proxy signer, and then the proxy signer performs message signing on behalf of the original signer. For example, a director of a company wants to survive for a long trip. He would require a proxy agent, to whom he would delegate his signing capability, and thereafter the proxy agent would sign the documents on behalf of the director. The classification of the proxy signature is dependent on the basis of delegation, namely full delegation, partial delegation and delegation by warrant, and presents a well-organized strategy.

Natarajan Meghanathan et al. (Eds) : ICAIT, CRYPIS, NC, ITCSE-2016
pp. 25–33, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.60703

In full delegation, the proxy signer signs document using the same secret key of the original signer given by the original signer. The drawback of proxy signature with full delegation is the difficulty to distinct/differentiate between original signer and proxy signer. In partial delegation, the proxy key is derived from the secret key of the original signer and hands it over to the proxy signer as a delegation capability. Due to partial delegation cannot restrict the proxy signer's signing capability, he can misuse the delegation capability. The weaknesses of full delegation and partial delegation are eliminated by partial delegation with warrant. A warrant, explicitly states the signer's identity, delegation period and the qualification of messages on which the proxy signer can sign.

In 1997, Kim, et al., [2] proposed a scheme using the concept of partial delegation with a warrant to restrict proxy signer signing capability. In 1999, Okamoto, et al., [3], for the first time, proposed proxy unprotected signature scheme based on RSA scheme. A proxy-protected signature scheme based on the RSA assumption was proposed by Lee, et al., in 2001 [4, 5]. In 2002, Shum and Wei [6] proposed another proxy protected signature scheme. Shao proposed the first proxy signature scheme based on the factoring integer problem in 2003 [7]. In 2005, Zhou, et al., [8] proposed two efficient proxy-protected signature schemes. Their first system is based on RSA assumption and the second strategy was based on the integer factorization problem. Park, et al., [9] observed the defect of Zhou, et al., systems. The normal proxy signature scheme and multi-proxy signature scheme based on the difficulty of factoring of large integers was proposed by Xue, et al. in 2006. In 2009, Shao [10] proposed proxy-protected signature scheme based on RSA. Yong, et al., [11] pointed out provably secure proxy signature scheme from the factorization in 2012. Several variants of RSA-based proxy signature scheme were pointed in the sequel [12, 13, 14].

Key establishment protocols are applied at the beginning of a communication session in order to verify the parties' identities and build a common session key to communicate together securely over an unreliable public network. Authenticated key agreement protocols have an important role in establishing secure communications between any two parties over the open network. The most famous protocol for key agreement was proposed by Diffie and Hellman which is based on the concept of public-key cryptography (DL) [15]. There are two types of the Diffie-Hellman protocol namely static and ephemeral. In the first one, the parities exchange static public keys, and in the second, they exchange ephemeral public keys [16]. The important feature of the designed protocol is the established session key is formed as a combination of static and ephemeral private keys of two parties.

In this paper, we propose a secure proxy signature scheme over an efficient and secure authenticated key agreement protocol based on RSA cryptosystem. The designed protocol depends on the relation between two assumptions (RSA factoring and DLP). Moreover, it is efficient and provides authentication between original signer and proxy signer before exchanging the session keys. The remaining parts of this paper are organized as follows. In Section 2, we elaborate security properties of the proxy signature scheme. Next, we discuss the designed protocol in Section 3. In Section 4, we proposed our proxy signature scheme. We analyze the security properties and common attacks of our proposed scheme in Section 5. We analyze the performance analysis of our proposed scheme in Section 6. Finally, in Section 7, we give our conclusion.

2. SECURITY REQUIREMENTS OF PROXY SIGNATURE

Due to the security features of proxy signature scheme, it's become popular and widely. So, any proxy signature should satisfy several requirements. Therefore, a secure proxy signature scheme satisfies the following five requirements [17]:

1. Verifiability: A verifier can be confident of the original signer's agreement on the signed message from a proxy signature.
2. Strong unforgeability: Only the designated proxy signer can generate a valid proxy signature.
3. Strong identifiability: The identity of the proxy signer can be determined by any verifier from a proxy signature.
4. Strong undeniability: The proxy signer cannot repudiate the signature creation against anyone else, once he creates a valid proxy signature on behalf of an original signer.
5. Prevention of misuse: The responsibility of the proxy signer should be determined explicitly if he misuses the proxy key for the purposes other than generating a valid proxy signature.

3. THE NEW SECURE KEY AGREEMENT PROTOCOL

The used protocol for authenticated key agreement [18] provides authentication between the two parties A and B before exchanging the session keys. The protocol consists of three phases; The Registration Phase, The Transfer and Substantiation Phase, and The Key Generation Phase. Figure1 shows the overall operation of the new protocol.The system picks short-term private key r_A, r_B, they are random integers $2 \leq r_A, r_B < n1$ and $GCD(r, n1) = 1$ $n1 = (p-1)(q-1)$ where p, q are large safe prime numbers normally at least 512 bits. t_A, t_B are short-term public keys where $t_A = g^{r_A} \bmod n$ and $t_B = g^{r_B} \bmod n$, g is a generator of Z_p^* and $n = pq$ long term public key at least 1024 bits. Then the system picks long-term private keys x_A, x_B they are random integer where $2 \leq x_A, x_B < n1$ and $GCD(x, n1) = 1$ and compute long-term public key y_A , y_B where $y_A = g^{x_B} \bmod n$ and $y_B = g^{x_A} \bmod n$. K_{AB} is the shared secret key calculated by the new secure protocol between the two parties A and B.

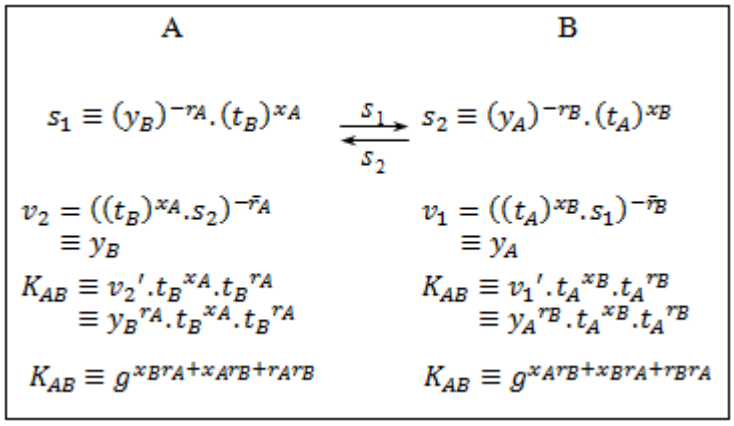

Fig. 1. Overall operation of the proposed protocol

4. PROPOSED PROXY SIGNATURE SCHEME

The proposed scheme is based on a proxy signature scheme with the new secure key agreement protocol and is divided into five phases: Initialization, Proxy key generation, Proxy key verification, Proxy signature generation and Proxy signature verification.

4.1 Initialization

The notation used in our scheme is included as follows:

A:	Original signer
B:	Proxy signer
p, q	Two large prime numbers
$(e_A; d_A)$:	Secret key of original signer
$(e_A; n_A)$:	Public key of original signer
$(e_B; d_B)$:	Secret key of proxy signer
$(e_B; n_B)$:	Public key of proxy signer
n_A , n_B:	The product of two large safe primes
$h(\ )$:	A secure one-way hash function
K_{AB} :	Shared secret key between A and B
m_w:	A warrant.

4.2 Proxy Key Generation

The original signer A does the following:

1. Computes $S_A = h(m_w \| e_B \| K_{AB})^{d_A} \ mod\ n_A$.
2. Sends (S_A, m_w) to the proxy signer over a public channel.

4.3 Proxy Key Verification

The proxy signer B checks whether $h(m_w \| e_B \| K_{AB}) = {S_A}^{e_A} \ mod \ n_A$. If it holds, the proxy signer accepts it as a valid proxy key; otherwise, rejects it.

4.4 Proxy Signature Generation

To sign message *m* on behalf of the original signer A, the proxy signer does the following:

1. Computes $S_B = (S_A \oplus h(m \| m_w \| e_B))^{\ d_B} \ mod\ n_B$ where $\oplus$ is an exclusive OR operation.
2. The proxy signature of message m is $(m, m_w, S_B, e_A, e_B, K_{AB})$.

4.5 Proxy Signature Verification

The verifier verifies whether $h(m_w \| e_B \| K_{AB}) = ({s_B}^{e_B} mod\ n_B \oplus h(m \| m_w \| e_B))^{e_A} \ mod\ n_A$. If it holds, he accepts it as a valid proxy signature; otherwise, rejects it.

5. SECURITY ANALYSIS

In the following, we show that the proposed schemes satisfy the security features, namely, verifiability, strong unforgeability, strong, undeniability, strong identifiability and prevention of misuse**.**

5.1 Verifiability

The verifier of proxy signature, can check whether verification equation $h(m_w \| e_B \| K_{AB}) = (s_B{}^{e_B} mod\ n_B \oplus h(m \| m_w \| e_B))^{e_A} mod\ n_A$ holds or not. We prove this as follows:

$$
\begin{aligned}
&(s_B{}^{e_B} mod\ n_B \oplus h(m \| m_w \| e_B))^{e_A} mod\ n_A \\
&\quad = \{(S_A \oplus h(m \| m_w \| e_B) mod n_B \oplus h(m \| m_w \| e_B)\}^{e_A} mod\ n_A \\
&\quad = \{(h(m_w \| e_B \| K_{AB})^{d_A} mod\ n_A mod\ n_B \oplus h(m \| m_w \| e_B) \oplus h(m \| m_w \| e_B)\}^{e_A} mod\ n_A \\
&= \ h(m_w \| e_B \| K_{AB}) \oplus h(m \| m_w \| e_B)^{e_A} mod\ n_B \oplus h(m \| m_w \| e_B)^{e_A} mod\ n_B \\
&= h(m_w \| e_B \| K_{AB})
\end{aligned}
$$

5.2 Strong Unforgeability

In this scheme, the proxy signature is created with the proxy signer's secret key d_B and delegated proxy key S_A. The proxy key is binding with the original signer's secret keyd_A and the session key K_{AB} where, $S_B = (S_A \oplus h(m \| m_w \| e_B))^{d_B} \ mod\ n_B$ and $S_A = h(m_w \| e_B \| K_{AB})^{d_A} mod\ n_A$. No one (including the original signer) can construct the proxy signature without having the knowledge of the secret keys d_B and d_A. Obtaining these secret keys by any other party is as difficult as breaking RSA. Moreover, the verification of $h(m_w \| e_B \| K_{AB})$ with the signed message prevents the dishonest party from the creation of forged proxy signatures. Therefore, any party, including the original signer cannot forge a valid proxy signature and thus the proposed scheme satisfies the unforgeability property.

5.3 Strong Identifiability

Any verifier can determine the identity of the proxy signer from the proxy signatures created by the proxy signer. Therefore, in the proposed scheme, any verifier can identify the identity of the proxy signer from the proxy signature generated by him, because the signed message is $S_B = (S_A \oplus h(m \| m_w \| e_B))^{d_B} mod n_B$, where S_A is the signed warrant by the original signer. Therefore, in the verification process any verifier can determine the identity of the proxy signer from m_w.

5.4 Strong Undeniability:

From the proposed scheme, the proxy signer and the original signer cannot deny their involvement in a valid proxy signature. In the proposed scheme, their involvements are determined by the warrant m_w , the connection of the public keys e_B and e_A and the common session key K_{AB} in the verification process.So the scheme satisfies the undeniability property.

5.5 Prevention of Misuse

In the proposed scheme, the proxy signer cannot forge the delegated rights. The responsibility of the proxy signer is determined from the warrant m_w in the case of the proxy signer's misuse. Therefore, the original signer's misuse is also prevented because he cannot compute a valid proxy signature against the proxy signer.

Next, we show that our scheme is heuristically secured by considering the following five most common attacks.

Known-Key Security (K-KS): In the proposed scheme, if an established session key between original signer and proxy signer is disclosed, the adversary is unable to learn other established session keys. In each run of the proposed scheme between the two parties should produce a unique session key K_{AB}which depends on r_A and r_B. Therefore, the opponent can't compute K_{AB} and the proposed scheme still achieves its goal in the face of the opponent.

(Perfect) Forward Secrecy: The secrecy of previous session keys established by honest entities is not affected if long-term private keys of one or more entities are compromised.The used protocol possesses a forward secrecy. Suppose that static private keys x_A and x_B of two parties are compromised. Even so, the secrecy of previous session keys established by honest parties is not affected, because an opponent who captured their private keys keys x_A or x_B should extract the ephemeral keys r_A or r_B from the exchanged values to know the previous or next session keys between them. However, this is RSA factorization problem and DLP (Discrete Logarithm Problem).

Key-Compromise Impersonation (K-CI): When A's static private key is compromised, it may be desirable that this event does not enable an adversary to impersonate other entities to A. Suppose A's long-term private key x_A , is disclosed. Now an opponent who knows this value can clearly impersonate A. But he can't impersonates B to A without knowing the B's long-term private keyx_B. For the success of the impersonation, the opponent must know A's ephemeral key r_A .So, in this case, the opponent should extract the value r_A from $t_A = g^{r_A} \ mod \ n$, then compute $r_A{}'$ from $r_A{}'r_A = 1 \ mod \ n1$ which is RSA factorization problem.

Unknown Key-Share (UK-S): Entity B cannot be coerced into sharing a key with entity A without B's knowledge, i.e., when B believes the key is shared with some entity C ≠ A, and A correctly believes the key is shared with B. The designed protocol prevents unknown key-share. Consequent to the assumption of this protocol that s_1 has verified that A possesses the private key x_A corresponding to his static public key y_A , an opponent can't register A's public key y_A as its own and subsequently deceive B into believing that A's messages are originated from the opponent. Therefore B cannot be coerced into sharing a key with entity A without B's knowledge

Subgroup Confinement Attack: Also small subgroup attack [9], the generator g is a primitive root of the prime p. If the selected prime p is such that p-1 has several small prime factors, then some values between 1 and p-1 do not generate groups of order p-1, but of subgroups of smaller orders. If the public parameter of either A or B lies within one of these small subgroups, so the shared secret key would be confined to that subgroup. The intruder may launch a brute force attack to determine the exact value of the shared secret key. The Solution to counter this kind of an attack is to choose a Safe Prime and use g that generates a large prime order subgroup or at the

very least make sure that composite order subgroup are not vulnerable for instance the order's prime number factorization contains only large primes, which we provided in our protocol, we choose two safe prime numbers and use generator of order p'q'

6. PERFORMANCE ANALYSIS

In order to analyze the performance of our scheme, we compare the computational complexity of our scheme with the existing RSA-based proxy signature schemes Lee, *et al.*, [2], Shao [11] and Sawati, *et al.* [17]. Our scheme and the existing schemes do not provide the proxy revocation mechanism. From this comparison, we show that our scheme and Sawati, *et al.* have the same performance analysis and they are efficient than the existing schemes; but our scheme provides extra security than the existing schemes by using new key agreement protocol to protect system fron any intruder . For simplicity, we neglect exclusive-OR operation ($\oplus$) time of the scheme.

Table1. Comparison of Computational Time with Previous Schemes

Phases	LKK schemes (2001)	Shao's scheme (2003)	Swati scheme (2013)	Our Scheme
Setup parameters	2Te + 2Tm + 2To	Te + Tm + To	2Te + 2Tm + 2To	2Te + 2Tm + 2To
Proxy key generation	Te + To + H	Te + To + H	Te + To + H	Te + To + H
Proxy key verification	Te + To + H	Te + To + Tm + H	Te + To + H	Te + To + H
Signature generation	3Te + 3To + 2H	2Te + 2Tm + 2To + H	Te + To + H	Te + To + H
Signature verification	3Te + 3To + 2H	2Te + Tm + To + 2H	2Te + 2Tm + 2To	2Te + 2Tm + 2To

The notations used in the Table 1 are as follows:

Te: computation time for an exponentiation operation
Tm: computation time for a multiplication operation
To: computation time for a modular operation
H: computation time for a hash operation.

The computation time of different phases of the schemes is given in Table 1. It is important to note that the computation time for a valid proxy signature falls into two parts. The first part consists of the time taken for the setup parameters, proxy key generation and proxy key verification process, which are a one-time computation and remain fixed for the entire delegation period. It is observed from Table 1 that for a proxy signature without revocation our scheme has the same performance as [17] in saving at least **Te** or **To** time unit in comparisons to others but it is more secure than the others.

7. CONCLUSION

In this paper, we proposed a new secure proxy signature scheme with a secure and efficient authentication key agreement protocol based on RSA cryptosystem. The used protocol depends

on the relation between two assumption (RSA factoring and DLP). Our scheme does not consider proxy revocation mechanism. The proposed scheme satisfies the necessary security requirements of proxy signature and has a secure channel to deliver the proxy key, through the designed new protocol. The system meets the security attributes and strong against most of potential attacks. So our system can be used to improve the security in an open Internet network.

REFERENCES

[1] M. Mambo, K. Usuda, E. Okamoto, Proxy signature: delegation of the power to sign the message, IEICE Trans. Fundamentals E79-A (9) (1996) PP. 1338 - 1353.

[2] S. Kim, S. Park and D. Won, "Proxy signatures", In: ICICS97, LNCS 1334, Springer-Verlag, (1997), pp. 223-232.

[3] T. Okamoto, M. Tada and E. Okamoto, "Extended proxy signatures for smart card", In: Proceedings of Information Security Workshop 99, LNCS 1729, Springer-Verlag, (1999), pp. 247-258.

[4] B. Lee, H. Kim and K. Kim, "Secure mobile agent using strong non-designated proxy signature", In: Information security and private (ACISP01), LNCS 2119, Springer-Verlag, (2001), pp. 474-486.

[5] B. Lee, H. Kim and K. Kim, "Strong proxy signature and its applications", In: Proceeding of the 2001 symposium on cryptography and information security (SCIS01), vol. 2, no. 2, (2001), pp. 603-608.

[6] K. Shum and V. K. Wei, "A strong proxy signature scheme with proxy signer privacy protection", In: Proceedings of IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE02), (2002).

[7] Z. Shao, "Proxy signature schemes based on factoring", Inform Process Lett., no. 85, (2003), pp. 137 143.

[8] Y. Zhou, Z. Cao and R. Lu, "Provably secure proxy-protected signature schemes based on factoring", Appl Math Comput., vol. 164, no. 1, (2005), pp. 83-98

[9] J. H. Park, B. G. Kang and J. W. Han, "Cryptanalysis of Zhou, et al., proxy-protected signature schemes", Appl. Math Comput., vol. 169, no. 1, (2005), pp. 192-197.

[10] Z. Shao, "Provably secure proxy-protected signature schemes based on RSA", Comput. Electr. Eng., vol. 35, (2009), pp. 497-505.

[11] Y. Yong, M. Yi, W. Susilo, Y. Sun and Y. Ji, "Provably secure proxy signature scheme from factorization", Mathematical and Computer Modelling, vol. 55, (2012), pp. 1160-1168.

[12] Y. Liu, H. Wen and C. Lin, "Proxy-protected signature secure against the un-delegated proxy signature attack", Comput Electron Eng., vol. 33, no. 3, (2007), pp. 177-185.

[13] R. Lu and Z. Cao, "Designated veri_er proxy signature scheme with message recovery", Appl Math Comput., vol. 169, no. 2, (2005), pp. 1237-1246.

[14] R. Lu, X. Dong and Z. Cao, "Designing e_cient proxy signature schemes for mobile communication", In: Science in China, vol. 51, no. 2, (2008), pp. 183-195.

[15] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. IT-l 22, no. 6, PP. 644-654, November, 1976.

[16] K. Chalkias, F. Mpaldimtsi, D. H. Varsakelis, and G. Stephanides, "On the Key-compromise impersonation vulnerability of one-pass key establishment protocols," in Proc. International Conference on Security and Cryptography (SECRYPT 2007), Barcelona, Spain, July 28-31, 2007.

[17] Swati Verma and Birendra Kumar Sharma," An Efficient Proxy Signature Scheme Based On RSA Cryptosystem," International Journal of Advanced Science and Technology Vol. 51, February, 2013,pp.121-126

[18] H. Elkamchouchi, M. R. M. Rizk, and Fatma Ahmed," A New Secure Protocol for Authenticated Key Agreement," IACSIT International Journal of Engineering and Technology, Vol. 5, No. 2, April 2013,pp.245-248

AUTHORS

H. Elkamchouchi obtained his B.Sc Electrical Communication Engineering - Excellent with First Class Honors - Faculty of Engineering – Alexandria University - June 1966, Master Communications Engineering (specialization accurate: antennas and propagation) Faculty of Engineering – Alexandria University - September 1969, B.Sc of Science in Applied Mathematics - Excellent with honors - Britain's Royal College of Science - University of London - England - August 1970, Doctor Communications Engineering (specialization accurate: antennas and propagation) - Faculty of Engineering - Alexandria University -March 1972. He work Professor Emeritus, Faculty of Engineering, Alexandria University from September 2003 until now.

Heba Gaber held a Masters' of science in Electrical Engineering from Faculty of Engineering, Arab Academy for Science and Technology. She works on Arab Academy for Science and Technology. She studies for Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University.

Fatma Ahmed held a Masters' of science in Electrical Engineering from Faculty of Engineering, Alexandria University. She works on Alexandria Higher Institute of Engineering and Technology. She Held a Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University.

Dalia ElKamchouchi held a Masters' of science in Electrical Engineering from Faculty of Engineering, Alexandria University. She works on Alexandria Higher Institute of Engineering and Technology. She Held a Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University.