International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 8
ISSN: 2454-4248
56 – 59

A New Directed Digital Signature Scheme

Manoj Kumar
Department of Mathematics,
Rashtriya Kishan Postgraduate College Shamli
Utter Pradesh- India- 247776.
e-mail- yamu_balyan@yahoo.co.in

Abstract— In this modern age of electronic era, digital signature scheme is a latest and burning platform for researcher. A variety of digital signature schemes are available in the literature of cryptography. Different signature schemes are used according to the peculiar requirement/situations. A plenty of digital signature schemes have been proposed and discussed. This paper presents a directed signature scheme with the property that the signature can be verified only with the help of signer or signature receiver.

Keywords-*Cryptography, public key cryptography, public key, private key, digital signature scheme, hash function, discrete logarithm.*

*****

I. INTRODUCTION

To ensure confidentially and to prevent forgery of a signed message, there is a ancient method for centuries for the sender of the message to put an identification sign, the hand written signature at the end of the message and then sealed this letter in an envelope, before handing it over to a open channel/deliverer.

In this modern electronic-era of communication, hand written physical signature is not suitable. For this situation, digital signature is the cryptographic solution to the problems of information security and authenticity of the signed message. W. Diffie and M. Hellman [1] originally defined digital signatures. Practically, digital signature is in some sense similar to hands written signature. A hand written signature is verified by comparing it to others authentic signatures. The hand written signature does not depend upon the content of the message. In contrast to hand written signature, which is independent of message, digital signature depend on the message and must somehow reflect both the content of the message and the signer of the message .

In order to achieve these requirements of digital signature, a signer of the message who holds private/secret key, can generate digital signature by applying those secret information and a publicly known digital signature algorithm. To check the authenticity of the digital signature, the signature receiver uses the public key/information and a publicly known algorithm. In this way, a digital signature scheme allows a user with a public key and a corresponding private key to sign a document in such a way that everyone using his/her (signer) public key can verify the signature of the signed message/ document, but no one other than the original signer can forge or copy the signature. This property of digital signature is known as self-authenticity. This property of self authenticity is essentially requirement for practical applications of digital signatures. Some practical situations are the requirement of digital signature on a certificate or an official announcements issued by any competent/government authority.

On the other hands, there are many situations, where a signed message may be sensitive to the signature receiver. For example signature on sensitive medical records of the signature receiver/patient, tax information of a client and most personal/business transactions are such situations. For these situations, signature is generated in such a way that only the signature receiver can check the authenticity of the message and whenever it required, he/she is able to prove the authenticity of the message to any third party. Such signatures are called as directed signatures [11-14, 17-21]. In directed signature scheme, the signature receiver has full control over the signature verification process. Nobody can check the validity of signature without his cooperation.

The concept of directed signatures was first presented by C. H. Lim and P. J. Lee [6]. Since than, a plenty of such scheme have been proposed. This paper proposes a new directed signature scheme. In the proposed scheme, any third party can check the authenticity of the signature with the help of signature receiver or the signer as well. Both the signer and signature receiver have full control over the signature verification process. In other words, they are independent to prove the validity of the signature to any third party, whenever required and necessary. The paper is organized as follows

The section- II presents some basic tools. Section- III describes a new directed signature scheme. Proposed scheme is illustrated in section IV. The security of the proposed scheme is discussed in section- V. Finally, comes to a conclusion in the section VI.

II. PRELIMINARIES

A. *Preliminary Settings*

Throughout this paper we use the following system setting.

- A prime modulous *p*, where $2^{511} < p < 2^{512}$;
- A prime modulous *q*, where $2^{159} < q < 2^{160}$ and q is a divisor of $p - 1$;
- A number *g*, where $g \equiv k^{(p-1)/q} \bmod p$, *k* is random integer with $1 \leq k \leq p-1$ such that g >1; (g is a generator of order *q* in Zp^*).
- A collision free one-way hash function *h* [10];

The parameters *p*, *q*, *g* and *h* are common to all users. We assume that every user A chooses a random $x_A \in Zq$ and computes $y_A = g^{x_A} \bmod p$. Here x_A is the private key of A and y_A is the public key of A. For our purpose, we use Schnorr's signature scheme [8]. These basic tools are briefly described below.

B. *Schnorr's signature scheme*

In this scheme, the signature of A on message *m* are given by (r_A, S_A), where,

$$r_A = h(g^{k_A} \bmod p, m) \text{ and}$$

$$S_A = k_A - x_A . r_A \bmod p.$$

Here random $k_A \in Zq$ is private to A.

The signature are verified by checking the equality

$$r_A = h(g^{S_A} y_A^{r_A} \bmod p, m).$$

III. NEW DIRECTED SIGNATURE SCHEME

Suppose that signer A wants to generate a signature on message *m* so that only signature receiver B can directed verify the signature. The signature receiver B as well as signer A can independently prove the validity of signature to any third party C, whenever required. Our proposed directed signature scheme is based on Schnorr's signature scheme. The signing and verification processes are as follows.

A. *Signature generation by A*

- A picks random K_{a_1} and $K_{a_2} \in Zq$ and computes

$$W_B = g^{-K_{a_2}} \bmod p \text{ and}$$

$$V_B = g^{K_{a_1}} . y_B^{K_{a_2}} \bmod p.$$

Here y_B is the public key of the signature receiver B.

- Using a one- way hash function *h*, A computes a secret value

$$r_A = h(g^{K_{a_1}}, m).$$

- A computes $S_A = K_{a_1} + x_A . r_A \bmod q.$

Here x_A is the private key of the signer. $\{S_A, W_B, V_B, m\}$ is the signature of A on the message *m*.

B. *Signature verification by B*

- Using his private key x_B, B computes

$$R = V_B (W_B)^{x_B} \bmod p.$$

- B recovers $r_A = h(R, m)$.
- B checks the following congruence for a valid signature

$$g^{S_A} \stackrel{?}{\equiv} R . y_A^{r_A} \bmod p.$$

If hold then $\{S_A, W_B, V_B, m\}$ is a valid signature.

C. *Proof of validity to C*

In this scheme, both the signer and signature receiver can independently prove the validity of signature to any third party, whenever necessary. This sub-section describes the protocol using which the signer and the signature receiver can prove the validity of signature.

a) *Proof of validity by A to C*

- ✓ A computes $V_C = g^{K_{a_1}} . y_C^{K_{a_2}} \bmod p$ and sends to C.
- ✓ C uses V_C in place V_B to checks the validity of signature by using his secret key. The signature verification process will remain same as in sub-section *B*.

b) *Proof of validity by B to C*

- ✓ B picks random $K \in Zq$ and computes

$$W_C = g^{-K} \bmod p,$$

$$V_C = R . y_C^{K} \bmod ,$$

and sends to C.

- ✓ C uses (W_C, V_C) in place (W_B, V_B) to checks the validity of signature by using his secret key. The signature verification process will remain same as in sub-section *B*.

IV. ILLUSTRATION

We choose smaller parameters to illustrate the scheme. Taking $p = 23$, $q = 11$ and $g = 3$.The secret and public key of users is as follow.

 ISSN: 2454-4248
56 – 59

User	Secret Key	Public Key
A	4	12
B	7	2
C	6	16

A. Signature generation by A to B

- A picks random $K_{a_1} = 9$,and $K_{a_2} = 5$ and computes $W_B = 16$, $V_B = 1$.
- Using a one way hash function *h*, A computes $r_A = 10$, $S_A = 5$.
- A sends {5, 16, 1, *m*} to B as his/her signature on the message *m*.

B. Signature verification by B

- B computes R = 8, recovers $r_A = h(18,m) = 10$, let.
- B checks the following congruence for a valid signature $3^5 \overset{?}{\equiv} 18 \cdot 12^{10} \bmod 23$. This holds.

C. Proof of validity to C

a) Proof of validity by A to C

- ✓ A computes $V_C = 16$ and sends to C.
- ✓ C computes $R = 16 \cdot 16^6 \bmod 23 = 18$.
- ✓ C uses V_C in place V_B to checks the validity of signature by using his secret key.

b) Proof of validity by B to C

- ✓ B picks random $K = 8$ and computes $W_C = 4$, $V_C = 9$,and sends to C.
- ✓ C computes $R = 9 \cdot 4^6 \bmod 23 = 18$.
- ✓ C uses (W_C , V_C) in place (W_B , V_B) to checks the validity of signature by using his secret key.

V. Security Discussions

In this sub-section, we shall discuss the security of proposed Directed Signature Scheme.

- ❖ Can one retrieve the secret key x_A , integer K_{a_1} from the equation

$$S_A = K_{a_1} + x_A \cdot r_A \bmod q \, ?$$

Here the number of unknown parameters is two. The number of equation is one, so it is computationally infeasible for a forger to collect the secret x_A , integer K_1 from this equation. Obviously, this is also again computationally infeasible for a forger to collect any information.

- ❖ Can one impersonate the signer?

A forger may try to impersonate the signer by randomly selecting two integers K_1 and $K_2 \in Zq$ and calculate

$$W_B = g^{-K_2} \bmod p,$$
$$V_B = g^{K_1} \cdot y_B^{K_2} \bmod p,$$
$$r_A = h(g^{K_1}, m).$$

But without knowing the secret key x_A , it is difficult to generate a valid S_A to satisfy the verification equation

$$g^{S_A} \overset{?}{\equiv} [R \cdot y_A^{r_A}] \bmod p.$$

- ❖ Can one forge a signature { S_A , W_B , V_B , m} by the equation $g^{S_A} \overset{?}{\equiv} [R \cdot y_A^{r_A}] \bmod p$?

A forger may randomly select an integer R and then computes the hash value r_A such that

$$r_A = h(R, m) \bmod q.$$

Obviously, to compute the integer S_A is equivalent to solving the discrete logarithm problem. On the other hand, the forger can randomly select r_A and S_A first, then try to determine a value R^*, that satisfy the signature verification equation. Thus these attacks will not be successful.

VI. Conclusion

The new directed scheme has the following properties:

- This proposed directed scheme is based upon W. Diffie and M. Hellman's public key cryptosystem and Schnorr's signature scheme .
- This scheme is applicable, when the message is sensitive to the signature receiver
- Every user has a public key and private key pair.
- The public key is generated by using discrete logarithm problem.
- The signer is free to decide the security parameters and other secrets at the time of signing.
- The signer can use the security parameters and secrets as one-time secrets. There is no need to fix these security parameters.
- The signer can change the secret values to sign different documents.

REFERENCES

[1] W. Diffie and M. Hellman, New directions in Cryptography, IEEE Trans. Info.Theory.31.pp. 644 – 654, 1976

[2] J. Boyar, D. Chaum, I. Damgard and T. Pederson, Convertible undeniable signatures. Advances in Cryptology – Crypto, 90, LNCS # 537,p.p.189-205,1991.

[3] D. Chaum, Designated confirmer signatures, Advances in Cryptology Euro crypt, 94 LNCS # 950,p.p.86-91, 1995.

[4] D. Chaum, Zero- knowledge undeniable signatures. Advances in Cryptology –Eurocrypt, 90, LNCS # 473,p.p. 458-464, 1991.

[5] Y. Desmedt and Y. Frankel, Shared Generation of Authenticators and Signatures. In Advances in Cryptology – Crypto -91, Proceedings. p.p. 457-469. New York: Springer Verlag, 1991

[6] Lim C.H. and Lee P.J. (1993). Modified Maurer-Yacobi, scheme and its applications. Advance in cryptology –Auscrypt, LNCS # 718, p.p. 308 – 323.

[7] C. H. Lim and P. J. Lee,Security Protocol, In Proceedings of International Workshop, (Cambridge, United Kingdom), Springer-Verlag, LNCS # 1189,1996.

[8] C. P. Schnorr, Efficient signature generation by smart cards, Journal of Cryptology, 4(3), p.p.161-174,1994.

[9] A. Shamir, How to share a secret, communications of the ACM, 22: p.p. 612 – 613, 1979.

[10] Y. Zheng, T. Matsummoto and H. Imai, Structural properties of one – way hash functions. Advances in Cryptology – Crypto, 90, Proceedings, p.p. 285 – 302, Springer Verlag, 1990.

[11] J. Ku ,D. Yun, B. Zheng, S. Wei, An Efficient ID-Based Directed Signature Scheme from Optimal Eta Pairing. Communications in Computer and Information Science, vol 316,p.p. 440-448, 2012

[12] R. Lu, Z. Cao, A directed signature scheme based on RSA assumption, International Journal of Network Security 2 (3),p.p. 182– 186,2006.

[13] Q. Wei, J. He and H. Shao, "Directed Signature Scheme and its Application to Group Key Initial Distribution' in ICIS-2009, ACM, p.p. 24-26,2009.

[14] E. S. Ismail and Y. Abu- Hassan, A Directed Signature Scheme Based on Discrete Logarithm Problems, Jurnal Teknologi, 47(C), p.p . 37-44,2007.

[15] R. Lu and Z. Cao, A Directed Signature Scheme Based on RSA Assumption, International Journal of Network Security, 2, 153-157, 2006.

[16] S. S. M. Chow, C. Ma and J. Weng, Zero-knowledge Argument for Simultaneous Discrete Logarithms, Algorithmica, 64, 246-266,2011.

[17] M. Yang, W. Yu-min, Directed Proxy Signature in the Standard Model, J. Shanghai Jiaotong Univ. (Sci.) 16(6), p.p. 663-671,2011

[18] N. N. Ramlee and E. S. Ismail, A new highly secure directed signature scheme, AIP Conference doi: http://dx.doi.org/10.1063/1.4858783, 2013

[19] N. N. Ramlee, A New Directed Signature Scheme With Hybrid Problems, Applied Mathematical Sciences, Vol. 7, 125, p.p.6217 – 6225,2013.

[20] J. Y. Hwang, H. J. Kim, D. H.M Lee, B. Song, An enhanced (t,n) threshold directed signature scheme, Information Sciences,Volume 275,p.p. 284-292, 2014.

[21] Umaprasada. et. al., ID-Based Directed Blind Signature Scheme from Bilinear. Pairings, Int. J. Adv. Res. Sci. Technol. Volume 5, Issue 2, p.p. 571-576, 2016.

[22] Tejeshwari Thakurh "ID-Based Directed Multi Proxy Chameleon Signature Scheme with Bilinear Pairing". International Journal of Computer Trends and Technology 31(1) p. p. 35-41, January 2016.

About the Author:

Manoj Kumar is an Associate Professor Department of Mathematics, Rashtriya Kishan Post Graduate College Shamli, Choudhary Charan Singh University Meerut, India. He is a member of Indian Mathematical Society, Indian Society of Mathematics and Mathematical Science, Ramanujan Mathematical society, and Cryptography Research Society of India. He is working as a reviewer for various International peer review Journals: Journal of System and Software, Journal of Computer Security, International Journal of Network Security, The computer networks, computer and security, The Computer Journal and Applied Mathematics Journal of Chinese University etc. He is also working as a Technical Editor for some International peer review Journals- Asian Journal of Mathematics & Statistics, Asian Journal of Algebra, Trends in Applied Sciences Research, Journal of Applied Sciences. He is also the member of Technical Programme Committee of various national and international conferences. He has published his research works at national and international level. His current research interests include Cryptography and Applied Mathematics.