International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

A Variant of ElGamal Digital Signature Scheme

Mohammad Amir[1], **Brijesh Shukla**[2]

[1]Yuveraj Dutta PG College, Department of Mathematics, UP-242307, India
aamir329[at]gmail.com

[2]Yuveraj Dutta PG College, Department of Physics, UP-242307, India
brijeshshukla17[at]gmail.com

Abstract: ***Digital signature scheme is a fundamental cryptographic mechanism which allows one to sign an electronic message and later the produced signature can be verified by the owner of the message. This paper presents a variant of ElGamal digital signature scheme and discusses the security aspects of the proposed digital signature scheme. The security of the proposed digital scheme is based on the difficult problem of computing discrete logarithms over finite fields (e.g. DSA, Schnorr and ElGamal).***

Keywords: Digital Signature, hash function, discrete logarithms, security, message

1. Introduction

In general, a hand-written signature or a seal is attached to a document to indicate the owner's identity. As we move to the world where our decisions and agreements are communicated electronically, we need to develop cryptographic procedures. Public key cryptography (PKC) provides mathematical schemes for such procedures through digital signature scheme. A digital signature scheme is the most important cryptographic mechanism in PKC.

In order to prove the authenticity of transmitted electronic messages, the digital signature is often implemented. The digital signature schemes ensure the integrity of data and prove the authenticity of the users. Because of vital needs, many digital signature schemes [1], [3]-[8] have been proposed. A digital signature schemes consists of the following:

- A signature generation algorithm, which is a mathematical mechanism to produce a digital signature.
- A signature verification algorithm, which is a method for verifying a digital signature.

There are two general modes of digital signature schemes: appendix mode and message recovery mode.

A digital signature scheme with appendix depends upon cryptographic hash function and requires the original message as input at the time of verification process. DSA, ElGamal [7] and Schnorr signature scheme[6] are digital signature schemes with appendix mode.

In message recovery mode the signed message is recovered by the user from the received signature i.e., original message is not required at the time of verification process. The RSA, Nyberg Ruppel[4] and Rabin are digital signature schemes with message recovery.

This paper presents a digital signature scheme with appendix which is a variant of well-known ElGamal digital signature scheme.

2. ElGamal Digital Signature Scheme

The ElGamal signature scheme is a signature scheme whose security is based on solving difficult discrete logarithm problem. This scheme allow a receiver to verify the authenticity of a message sent by a signer over an insecure channel.[7]

2.1 System parameter

- All users of the signature scheme agree on Group G of prime order *(p-1)* with generator *g* in which the discrete log problem is assumed to be difficult.
- All user agree on cryptographic hash function $h:\{0,1\}^* \rightarrow Z_p^*$

2.2 Key Generation by signer

- Choose a secret key *x* with *1<x<p-1* .
- Compute $y = g^x \bmod p$
- Public key is (p, g, y).
- Secret key is *x*.

2.3 Signature Scheme

A signer performs following steps to sign a message m.

- Choose a random k such that $1 < k < p-1$, $\gcd(k, p-1)$.
- Compute $r = g^k \bmod p$
- Compute $s = \{h(m) - xr\}k^{-1} \bmod (p-1)$

Then (r, s)) is the digital signature on message m.

2.4 Verification

The signature (r, s) is verified as follows

- $0 < r < p$ *and* $1 < s < p-1$
- $g^{h(m)} = y^r.r^s \bmod p$

2.5 Signature Validation

- Compute $y^r.r^s = g^{xr}.g^{k\{h(m)-xr\}k^{-1}} = g^{h(m)}$. It implies the validity of signature scheme.

3. Proposed Digital Signature Scheme

3.1 System parameter

- All users of the signature scheme agree on Group G of prime order q with generator g in which the discrete log problem is assumed to be difficult.
- All user agree on cryptographic hash function $h:\{0,1\}^* \to Z_q^*$

3.2 Signature generation by signer

- Choose *p*,*q* such that $p = 1 \bmod q$
- Pick a random generators $g \in Z_p^*$ and $k \in Z_q^*$ such that $g^q = 1 \bmod p$
- Compute $r = g^k \bmod p$
- Compute $v = h(r \| m)$, where ‖ denotes concatenation and is represented as a bit string.
- Compute $s = \{h(m)\}^{-1}\{k - xv\} \bmod q$
- (r, s) is the digital signature on message m.

3.3 Verification by verifier

The signature (r, s) is verified as follows

- If $y^v g^{s.h(m)} = r \bmod p$ then signature is verified.

3.4 Validation of signature scheme

- Compute $s = \{h(m)\}^{-1}\{k - xv\} + tq$
- $L.H.S. \equiv y^v g^{s.h(m)}$

$$\begin{aligned} &= g^{xv}.g^{[h(m)^{-1}\{k-xv\}+tq]h(m)} \bmod p \\ &= g^{xv}.g^{\{k-xv\}+tq]} \bmod p \\ &= g^k.g^{tq} \bmod p \\ &= g^k \bmod p \\ &= r \equiv R.H.S. \end{aligned}$$

It implies the validity of signature scheme.

4. Security

Security aspect covered by above signature scheme as follows:

- A third party can forge the signature by finding the signer's private key *x*. But it is equivalent to solving discrete logarithm problem, which is believed to be very difficult.
- By finding collisions in the hash function $h(m) = h(M) \bmod q$ which is also supposed to be difficult.

5. Conclusion

This paper proposed a variant of ElGamal digital signature scheme whose security is also based on finding discrete logarithm over finite field. Hence security level of this scheme is similar to other discrete logarithm based schemes like ElGamal and DSA.

6. Future Research

To develop a Digital Signature Scheme , in which security is based on both the solving problem of factoring integer(RSA) and problem finding discrete logarithm over finite fields.

References

[1] Damgard I.B. (1987). Collision free hash function and public key signature scheme Advance in Cryptology - Eurocrypt - 87, Springer Verlag, p.p. 203-216.

[2] C.-G. Kang, "New digital multi signature scheme in electronic contract systems," in Proc. 1995 IEEE Int. Symp. on Information Theory, Whistler, BC, Canada, Sept. 1995, pp. 486–486.

[3] J. M. Piveteau, "New signature scheme with message recovery," Electron. Lett., vol. 29, no. 25, pp. 2185–2185, Dec. 1993

[4] L. Harn, "New digital signature scheme based on discrete logarithm," Electron. Lett., vol. 30, no. 5, pp. 296–298, Mar. 1994. NIST. (1994). Digital signature standard, U.S Department of Commerence, FIPS PUB, 186.

[5] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem," in Proc. Eurocrypt'94, Perugia, Italy, May 1994, pp. 182-193

[6] Schnorr C.P. (1991). Efficient signature generation by Smart cards, Journal of Cryptology -4(3), p.p. 161-174.

[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithm," IEEE Trans. Inform. Theory, vol. 31, pp. 469–472, July 1985

[8] Z. Shao, "Signature scheme based on discrete logarithm without using one-way hash function," Electron. Lett, vol. 34, no. 11, pp. 1079–1080, May 1998.

[9] M. Amir and J.Ahmed "Digital Signature Scheme Using Two Hash Functions" International Journal of Science and Research (IJSR), Vol.3, no. 4, pp. 126-128

Author Profile

Mohammad Amir received M.Sc. degree in Mathematics from M.J.P.R. University Bareilly in 2009 and M.Tech. degree in Computer Applications from Indian Institute of Technology Delhi in 2012. Currently working as an Assistant Professor in Y.D. PG College Lakhimpur-Kheri, UP

Brijesh Shukla received M.Sc. degree in Physics from University of Lucknow, Lucknow in 2003. Currently working as an Assistant Professor in Department of Physics Y.D. PG. College, Lakhimpur-Kheri, U.P.