International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 11 | Nov -2016 www.irjet.net p-ISSN: 2395-0072

A Secure ElGamal Cryptosystem Using Zero Knowledge Protocol

M. Ranjithkumar

Department of Mathematics, Jeppiaar Institute of Technology,
Chennai – 631 604, Tamil Nadu, India.
mranjithkumar@jeppiaarinstitute.org

Abstract - This paper describes the ElGamal digital signature where the identification protocol is converted into a digital signature scheme. This scheme is based on the zero knowledge proof and so it is more secure than the usual ElGamal digital signature scheme.

Key Words: discrete logarithmic problem, ElGamal digital signature scheme and zero knowledge proof.

1. INTRODUCTION

A digital signature is a cryptographic code which when attached to an electronically transmitted message helps to uniquely identify the sender and ensures that the message has not been tampered by any adversary. The digital signature is content-bound in the sense that any later changes of the content are impossible without invalidating the signature.

Digital signatures rely on public cryptography. Public key cryptography has two keys namely public and private key. The public key is used by others to send a secured e-mail. With the help of it, the message is encrypted and it can be decrypted with the private key only. Not even the sender of the message is able to reopen it. With the digital signature the message is protected against forgery and any alteration in the message if any, will be noticed by the recipient immediately.

For practical reasons, when digital signatures are used, people don't actually sign the original message with their private key. Instead, they apply a hash function to the message called a message digest or hash value. The message digest is usually shorter than the original message. Infact the hash function is to convert a message of arbitrary length into a fixed length. This saves a considerable amount of time. The sender signs the message digest with his private key. Anyone can decrypt the signed message digest, by using the sender's known public key. Thus the digital signature has the following properties:

i. Message authentication – the receiver has to be sure of sender's identity.

ii. Integrity – the data must arrive exactly as it was sent.

iii. Non-repudiation – a receiver must be able to prove that a particular message came from a specific sender.

The idea of discrete logarithm by Diffie and Hellman in 1976 [1] resulted in the realization of signatures schemes. The famous digital signature schemes are the RSA [7], ElGamal [2], Schnorr[8] and the Fiat-Shamir scheme [3]. In this paper a zero knowledge proof is applied to ElGamal digital signature scheme to improve the security.

2. ELGAMAL DIGITAL SIGNATURE SCHEME

The ElGamal signature scheme [6] is a randomized signature mechanism. It generates digital signature with the binary messages of arbitrary length and uses a hash function $h:\{0;1\}^* \to z_p$ where p is large prime number, to reduce the length of a message of arbitrary length into a fixed length.

2.1. Algorithm

Each entity say A, creates a public key, the corresponding private key and perform the following operation.

a. Generate a large random prime p and a generator α of the multiplicative group Z_p^* .

b. Select a random integer a , $1 \le a \le p-2$.

c. Compute $y = \alpha^a \mod p$.

d. A's private key is a and public key is (p, α, y).

2.2. Signature generation

Entity A does the following:

a. Represent the message as an integer m in the range $\{0,1,2,\cdots, p-1\}$.

b. Select a random secret integer k, $1 \le k \le p-2$.

c. Compute $r \equiv \alpha^k \mod p$

d. Compute $k^{-1} \mod (p-1)$

e. Find $s \equiv k^{-1}\{h(m) - ar\} \mod (p-1)$

f. A's signature for message m is the pair (r, s)

2.3. Verification

To verify A's signature (r, s) on m, B does the following:

a. Obtain A's authentic public key (p, α, y).

b. Verify that $1 \le r \le p-1$; If not the signature is rejected.

c. Compute $v_1 \equiv y^r r^s \mod p$

d. Find h(m) and $v_2 \equiv \alpha^{h(m)} \mod p$

e. Accept the signature if and only if $v_1 = v_2$.

2.4. Security of ElGamal digital signature scheme

a. An adversary might attempt to forge A's signature on m by selecting a random integer k and computing $r \equiv \alpha^k \mod p$. The adversary must then determine $y = k^{-1}\{h(m) - sr\} \mod (p-1)$. Since the discrete logarithm problem is computationally infeasible.

b. The ElGamal cryptosystem is as secure as the discrete logarithm problem, given no weak random exponents or primes. It further prevents a chosen plaintext attack. As this k is chosen uniformly before encryption, the same plaintext can result in p-1 different ciphertexts, one of which is chosen uniformly by choosing a k.

c. This scheme requires that the signer generate a unique secret key for each message. If the same secret key is used for two different messages, it would expose the signer's private key and vice versa. For example, suppose the same k is used to encrypt two messages m_1, m_2 and the resulting ciphertext pairs are (r_1, α_1) and (r_2, α_2). Then $\alpha_1 / \alpha_2 = m_1 / m_2$ where m_2 could be easily computed if m_1 were known. For this purpose, use different random integer k to encrypt different message.

d. If no hash function h is used, the signing equation is $y = k^{-1}\{h(m) - sr\} \mod (p-1)$ now it is easy for an adversary to mount an existential forgery attack.

e. There is a message expansion by a factor of 2. That is the ciphertext is twice as long as the corresponding plaintext, which means the message m is between $1 \le m \le p-1$ and the random integer k, lies between $1 \le k \le p-2$. This comes from choosing a new random k for each block of the plaintext message m_i. The public key derived from this k has to be sent together with the c_i as the pair (c_i, g^k), the set of all these pairs giving the ciphertext C.

f. The ElGamal digital signature scheme is secure against passive attack [8].

g. Signature generation is relatively fast, requiring one modular exponentiation $(\alpha^k \mod p)$, the extended Euclidean algorithm (for computing $(k-1) \mod (p-1)$), and two modular multiplications. This can be done off-line, in which case the possible pre-computation requires only two on-line modular multiplications.

3. ZERO KNOWLEDGE PROOF IN IDENTIFICATION PROTOCOL

For application areas like contract or document or authorization or payment signing through online problems like invalidation of public key, expose or revoke of public key may arise. To avoid such problems, a public key certificates can be used where the signature is put by Certification Authority(CA), to validate the public key. Certificates are similar to the passport or driving licenses, which bind a public key to a name or other attributes of key holder. The certificates are signed by a trusted party, the certificate is also signed by the user with his private key, which will make them immutable and protect them against forgery. Even the smallest alteration made, makes the ID invalid. This procedure makes the receiving party to validate name, attributes and identity of key owner. Zero knowledge protocol is an efficient tool in identification cases like the above.

In this paper, we present the ElGamal digital signature scheme where the identification protocol is converted into a digital signature scheme. This scheme is based on the zero knowledge proof and so it is more secure than the usual ElGamal digital signature scheme. This technique of converting an honest-verifier three-pass identification protocol into a digital signature algorithm is usually called the Fiat-Shamir heuristics.

The working of this scheme is that the receiver Bob challenge Alice with questions and assesses the answers until he is satisfied that Alice is who she claims to be. In one such scheme, Bob generates a random number and transmits it to Alice. Alice generates a new random number and then digitally signs a message containing both her random number and Bob's. She then sends the signed message, together with her random number, to Bob. Bob verifies the signature to ensure that he is communicating with Alice. This scheme is secure against an eavesdropper and it also prevents Bob form impersonating Alice.

Thus, a zero knowledge proof is an interactive proof, which allows one person to convince another person of some fact without revealing the information about the proof. The main features of zero knowledge protocols are,

a. The verifier cannot learn anything from the protocol
b. The prover cannot cheat the verifier
c. The verifier cannot cheat the prover
d. The verifier could be convinced of any true statement.
e. The verifier cannot pretend to be the prover to any third party

3.1 Zero Knowledge proof of ElGamal digital signature scheme

The ElGamal protocol involves an entity identifying itself by proving knowledge of a secret using a Zero-Knowledge proof [4]; the protocol reveals no partial information whatsoever regarding the secret identification value(s) of Alice. Here, Alice proves her identity to Bob in t executions of a 3-pass protocol.

A trusted center Tom selects a large prime number p and a generator α of multiplicative group Z_P^* for all users. The method also requires a hash function $h:\{0;1\}^* \to Z_p$. Here $\{0;1\}$ denotes the set of strings of arbitrary bit lengths. This method is a randomized mechanism.

3.2 Algorithm

Alice proves her identity to Bob in a 3-pass protocol.

3.2.1 Selection of system parameters

A trusted authority Tom, chooses the following parameters:

a. Select a large prime p and a generator α of the multiplicative group Z_p^* such that the discrete logarithm problem in Z_p^* is intractable.

b. A security parameter t such that $p \geq 2^t$. For most applications, t=40 provides adequate security.

c. Tom also establishes a secure signature scheme with a secret signing algorithm sig_{Tom} and a public verification algorithm ver_{Tom} .

d. A secure hash function is specified which is used to hash the message before it is signed.

3.2.2 Issuing a certificate to Alice

a. Tom establishes Alice's identity by means of conventional forms of identification such as birth certificate or passport. Then Tom forms a string ID(Alice) that contains her identity information.

b. Alice secretly chooses a random exponent a, where $0 \leq a \leq p-2$. She then computes $v \equiv \alpha^{-a} \bmod p$ and gives v to Tom.

c. Tom generates a signature $s = sig_{Tom}\left(ID(Alice), v\right)$ and gives the certificate $cert_{Alice} = \left(ID(Alice), v, s\right)$ to Alice.

3.2.3. Protocol message and actions

Alice identifies herself to verifier Bob as follows:

a. Alice chooses a random r (the commitment), $0 \leq r \leq p-2$, and $\gcd(r,\ p-1)=1$ computes (the witness) $x \equiv \alpha^r \bmod p$, and sends her

certificate $cert_{Alice} = (ID(Alice), v, s)$ and x to Bob.

b. Bob verifies the signature of Tom by checking that, $ver_{Tom} - (ID(Alice), v, s)$ is true and then he chooses a random number e(the challenge), $1 \le e \le 2^t$ and sends it to Alice.
c. Alice computes $y \equiv ae + r \mod(p-1)$ and sends y(response) to Alice.
d. Bob computes $z \equiv \alpha^y v^e \mod p$, and accepts Alice's identity provided z=x.

4. SECURITY OF THE PROPOSED CRYPTOSYSTEM

To identify a protocol Tom proves the validity of Alice's certificate by affixing his signature. So, Bob verifies the signature of Tom on Alice's certificate to convince himself that the certificate is authentic. Secondly the value a, functions like a PIN and convinces Bob that the person carrying out the protocol is indeed Alice. The following congruence's show that Alice will be able to prove her identity to Bob:

$$\alpha^y v^e \equiv \alpha^{r+ae} v^e \mod p \equiv \alpha^{r+ae} \alpha^{-ae} \mod p$$

$$\equiv \alpha^r \mod p$$

$$\equiv x \mod p$$

So Bob will accept Alice's proof of identity. While an adversary, Oscar, will not gain any information about a when Alice proves her identity(zero-knowledge protocol).

Although an adversary, Oscar, could gain access to Alice's correct certificate (since the information on a certificate is revealed each time the identification is run), he will not able to impersonate Alice unless he knows the value of a. Oscar would have to compute y for each round, but y is a function of a. The computation of a from v involves a discrete logarithm problem, which we assume is intractable. The computations performed by Alice require the modular exponentiation, $x \equiv \alpha^r \mod p$ which although computationally intensive can be performed offline. The computation of $y \equiv ae + r \mod p - 1$ comprises one modular addition and one modular multiplication, which is not computationally intensive. On the other hand, Bob's calculations are computationally intensive, since he has to verify Tom's signature on Alice's certificate and also verify that $z \equiv \alpha^y v^e \mod p = x$. A hash function is applied to produce a message digest of the entire message. The ElGamal digital signature scheme, which applies zero knowledge proof is more secure than the original ElGamal digital signature scheme. This scheme is secure against active and passive attack. This scheme is designed to be very fast and efficient both from a computational point of view and the amount of information that can be exchanged in the protocol. It is also designed to minimize the amount of computation done by Alice.

5. CONCLUSIONS

In this paper the focus is on the identification schemes that are based on zero knowledge protocols. In particular, we examine the ElGamal protocols that are based on zero-knowledge proof. The idea of digital signature schemes is likely to grow in its importance as one seek new ways to negotiate the conflicting needs of privacy on the one hand and that of proving its identify to another.

REFERENCES

[1] W. Diffie, M. Hellman, New directions in cryptography. IEEE Transactions on Information Theory, Vol.22, 6, 644-654, 1976.

[2] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, Vol.IT-30, 4, 469-472, 1985.

[3] A. Fiat, A. Shamir, How to prove yourself: Practical solutions to identification and signature problems. Lecture Notes in Computer Science 263, Advanced in Cryptology: Proc. Crypto '86, 1987.

[4] U. Feige, A. Fiat and A. Shamir, Zero Knowledge proofs of Identity, Proceedings of STOC, pp.210-217, 1987.

[5] S. Goldwasser and S. Micali, Probabilistic Encryption, J.Computer and System Sciences, 28, pp.270-299, 1984.

[6] A.J. Menezes , P.C. Van Oorchot and S.A. Vanstone, Handbook of Applied Cryptography. CRC Press, 2000.

[7] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol.21, No.2, pp.120-126, 1978.

[8] C.P. Schnorr, Efficient identification and signatures for smart card. Lecture Notes in Computer Science 435, Advances in Cryptology: Proc. Crypto '89, Springer Verlag, 120-126, 1990.

[9] M.K. Viswanath and M. Ranjithkumar, A secure cryptosystem using the decimal expansion of an Irrational number. Applied Mathematical Sciences, Vol. 9, pages 5293-5303, 2015.