A Novel Proxy Blind Signature Scheme for Mobile Devices

Daniyal M. Alghazzawi[1], Trigui Mohamed Salim, Syed Hamid Hasan[2]
[1,2]Faculty of Computing and Information Technology
Department of Information Systems
King Abdul Aziz University
Kingdom of Saudi Arabia
{shh786@hotmail.com, jayaprakashkar@yahoo.com}

ABSTRACT: *A proxy blind signature scheme is a special form of blind signature which allows a designated person called proxy signer to sign on behalf of two or more original signers without knowing the content of the message or document. It combines the advantages of proxy signature and blind signature scheme and satisfies the security properties of both proxy and blind signature scheme. This paper describes an effcient simple proxy blind signature scheme. The security of the scheme is based on Elliptic Curve Discrete Logarithm Problem(ECDLP). ECC offers security equivalent to RSA and DSA while using far smaller key sizes. The benefits of this higher-strength per-bit include higher speeds, lower power consumption, bandwidth savings, storage effciencies, and smaller certificates. This can be implemented in low power and small processor mobile devices such as smart card, PDA etc.*

Keywords: ECDLP, Blind signature, Proxy signature, Mobile devices

Received: 18 August 2010, Revised 16 September 2010, Accepted 21 September 2010

1. Introduction

Blind signature scheme was first introduced by Chaum [3]. It is a protocol for obtaining a signature from a signer on any message, without revealing any information about the meassage or its signature. In 1996, mamo et al proposed the concept of proxy signature [1]. In proxy signature scheme, the original signer delegates his signing capacity to a proxy signer who can sign a message submitted on behalf of the original signer. A verifier can validate its correctness and can distinguish between a normal signature and a proxy signature. In multi-proxy signature scheme, an original signer is allowed to authorize a group of proxy members to generate the multi signature on behalf of the original signer. In 2000, Hwang et al. proposed the first multi-proxy signature scheme [4]. A proxy blind signature scheme is a digital signature scheme that ensures the properties of proxy signature and blind signature. In a proxy blind signature, an original signer delegates his signing capacity to proxy signer.

2. Background

In this section we brief overview of prime field, Elliptic Curve over that field and Elliptic Curve Discrete Logarithm Problem.

2.1 The finite field *Fp*

Let p be a prime number. The finite field *Fp* is comprised of the set of integers 0, 1, 2....... *p* - 1 with the following arithmetic operations [5] [6] [7]:

- Addition: If $a ,b \in Fp$, then $a + b = r$, where r is the remainder when $a + b$ is divided by p and $0 \leq r \leq p - 1$. This is known as addition modulo p.

- Multiplication: If $a,b \in Fp$, then $a.b = s$, where s is the remainder when $a.b$ is divided by p and $0 \leq s \leq p -1$. This is known as multiplication modulo p.

Inversion: If a is a non - zero element in Fp, the inverse of a modulo p, denoted a^{-1}, is the unique integer $c \in Fp$ for which $a.c = 1$.

2.2 Elliptic Curve over *Fp*

Let $p \geq 3$ be a prime number. Let $a,b \in Fp$ be such that $4a3 + 27b2\ 6 \nvDash 0$ in Fp. An elliptic curve E over Fp defined by the parameters a and b is the set of all solutions $(x,y),x,y \varepsilon Fp$, to the equation $y2 = x3 + ax + b$, together with an extra point O, the point at in finity. The set of points $E(Fp)$ forms a Abelian group with the following addition rules [9]:

1. Identity : $P + O = O + P = P$, for all $P \in E(Fp)$

2. Negative : if $P(x,y) \in E(Fp)$ then $(x,y) + (x,-y) = O$, The point $(x,-y)$ is dented as -P called negative of P.

3. Point addition: Let $P((x1,y1),Q(x2,y2) \in E(Fp)$,then $P + Q = R \in E(Fp)$ and coordinate $(x3,y3)$of R is given by $x3 = \lambda_2 - x_1 - x_2$ and $y3 = \lambda(x1 - x3) - y1$ where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$

4.Point doubling : Let $P(x_1, y_1) \in E(K)$ where $P = -P$ then $2P \nvDash (x_3,y_3)$ where $x_3 = (\frac{3x_1^2 + a}{2y_1}) - 2x_1$ and $y_3 = (\frac{3x_1^2 + a}{2y_1})(x_3 - x_1) - y_1$

2.3 Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given an elliptic curve E defined over a finite field F_p,a point $P \in E(F_p)$ of order n, and a point $Q \in < P >$, find the integer $l \in [0, n - 1]$such that $Q = lP$. The integer l is called discrete logarithm of Q to base P, denoted $l = log_p Q$ [9].

3. Preliminaries

3.1 Notations

Common notations used in this paper as follows.

- p : the order of underlying finite field.
- F_p : the underlying finite field of order p
- E : elliptic curve defined on finite field F_p with large order.
- G : the group of elliptic curve points on E.
- P : a point in $E(F_p)$ with order n , where n is a large prime number.fs
- $H(.)$: a secure one-way hash function.
- d : the secret key of the original signer S to be choosen randomly from $[1, n - 1]$.
- Q is the public key of the original signer S, where $Q = d . Q$.
- || : Concatenation operation between two bit stings.

4. Proxy Signature and Proxy Blind Signature

A proxy blind signature is a digital signature scheme that ensures the properties of proxy signature and blind signature schemes. Proxy blind signature scheme is an extension of proxy blind signature, which allows a single designated proxy signer to generate a blind signature on behalf of group of original signers.A proxy blind signature scheme consists of the following three phases:

-Proxy key generation

-Proxy blind signature scheme

-Signature verification

5. Security propertiesm

The security properties described in [2] for a secure blind signature scheme are as follows:

-**Distinguishability :** The proxy blind signature must be distingushable from the ordinary signature.

-**Strong unforgeability:** Only the designated proxy signer can create the proxy blind signature for the original signer.

-**Non-repudiation:** The proxy signer can not claim that the proxy signer is disputed or illegally signed by the original signer.

-**Verifiability:** The proxy blind signature can be verified by everyone. After verification, the verifier can be convinced of the original signer's agreement on the signed message.

-**Stong undeniably:** Due to fact that the delegation information is signed by the original signer and the proxy signature are generated by the proxy signer's secret key. Both the signer can not deny their behavior.

-**Unlinkability:** When the signer is revealed, the proxy signer can not identify the association between the message and the blind signature he generated.

-**Secret key dependencies:** Proxy key or delegation pair can be computed only by the original signer's secret key.

-**Prevention of misuse :** The proxy signer cannot use the proxy secret key for purposes other than generating valid proxy signatures. In case of misuse, the responsibility of the proxy signer should be determined explicitly.

6. Proposed Protocol

The protocol involves three entities : Original signer S, Proxy signer P_s and verifier V. It is described as follows.

6.1 Proxy Phase

-Proxy generation : The original signer S selects random integer k in the interval $[1, n - 1]$. Computes $R = k \,.\, P = (x1 , y1)$ and $r = x_1 \bmod n$.Where x_1 is regarded as an integer between 0 and $q - 1$. Then computes $s = (d + k \,.\, r) \bmod n$ and computes $Q_p = s \,.\, P$.

-Proxy delivery : The original signer S sends (s,r) to the proxy signer P_s and make Q_p public.

- Proxy Verification: After receiving the secret key pairs (s, r), the proxy signer P_s checks the validity of the secret key pairs (s, r) with the following equation.

$$Q_p = s \,.\, P = Q + r \,.\, R \qquad (1)$$

6.2 Signing Phase

-The Proxy signer S_p chooses random integer $t\ 2\ [1, n - 1]$ and computes $U = t \,.\, P$ and sends it to the verifier V.

- After receiving the verifier $\sim$ chooses randomly $\alpha,\beta\ \varepsilon\ [1, n - 1]$ and computes the following

$$R= U + \alpha \,.\, P - \beta \,.\, Q_p \qquad (2)$$

$$\tilde{e} = H(\tilde{R} \,||\, M) \qquad (3)$$

$$e = (\tilde{e} + \beta) \bmod n \qquad (4)$$

and verifier V sends e to the proxy signer S_p .

- After receiving e, S_p computes the following

$$\tilde{s} = (t - s \,.e) \bmod n \qquad (5)$$

and sends it to V .

- Now V computes

$$s_p = (\tilde{s} + \alpha) \bmod n \qquad (6)$$

The tuples $(M, s_p , \tilde{e})$ is the proxy blind signature.

6.3 Verification Phase

The verifier V computes the following equation. (7)

$$\gamma = H((s_p \,.\, P + \tilde{e} \,.\, Q_p) \,||\, M)$$

and verifies the validity of proxy blind signature $(M, s_p , \tilde{e})$ with the equality $\gamma = \tilde{e}$.

6. Security Analysis

Theorem 1 : *It is infeasible for adversary A to derive signer's private key from all available public information.*

Proof : Assume that the adversary *A* wants to derive signer's private key *d* from his public key *Q*, he has to solve ECDLP problem which is computationally infeasible. Similarly, the adversary will encounter the same difficulty as she/he tries to obtain proxy signer's private key.

Theorem 2 : *Proxy signature is distinguishable from original signer's normal signature.*

Proof: Since proxy key is different from original signer's private key and proxy keys created by different proxy signers are different from each other, any proxy signature is distinguishable from original signer's normal signature and different proxy signer's signature are distinguishable.

Theorem 3: *The scheme satisfies Unlinkability security requirement*

Proof: In verification stage, the signer checks only whether $\gamma = H((s_p . P + \tilde{e} . Q_p) \,||\, M)$ holds. He does not know the original signer's private key and proxy signer's private key. Thus the signer knows neither the message nor the signature associated with the signature scheme.

7. Correctness

Theorem 4 : *The proxy blind signature (M, s_p, $\tilde{e}$) is universally verifiable by using the system public parameters*.

Proof: The of correctness of the signature is verified as follows We have to prove that

$$H((sp . P + \tilde{e} . Q_p) \,||\, M) = H(\tilde{R} \,||\, M)$$

$$\begin{aligned}
&i{:}e \text{ to show } s_p . P + \tilde{e} . Q_p = \tilde{R}\\
&= (\tilde{s} + \alpha) . P + \tilde{e} . Q_p\\
&= s . P + \alpha . P + \tilde{e} . Q_p\\
&= (t - s . e) . P + \alpha P + \tilde{e} . Q_p\\
&= t . P - e . Q_p + \alpha . P + \tilde{e} . Q_p\\
&= t . P - (\tilde{e} + \beta) . Q_p + \alpha P + \tilde{e} . Q_p\\
&= t . P - \tilde{e} . Q_p - \beta . Q_p + \alpha . P + \tilde{e} . Q_p\\
&= t . P - \beta . Q_p + \alpha . P\\
&= U - \beta . Q_p + \alpha . P\\
&= \tilde{R}
\end{aligned}$$

8. Conclusion

The security of the scheme is hardness of solving ECDLP. The primary reason for the attractiveness of ECC over systems such as RSA and DSA is that the best algorithm known for solving the underlying mathematical problem namely, the ECDLP takes fully exponential time. In contrast, sub-exponential time algorithms are known for underlying mathematical problems on which RSA and DSA are based, namely the integer factorization (IFP) and the discrete logarithm (DLP) problems. This means that the algorithms for solving the ECDLP become infeasible much more rapidly as the problem size increases more than those algorithms for the IFP and DLP. In this proposed scheme it is infeasible or adversary to derive signer's private key from all available public information. This protocol also achieves the security like requirements distinguishability,strong unforgeability, non-repudiation, stong undeniably and unlinkability.

References

[1] Mambo,M., Usda,K., Okamoto, E., Proxy signature: Delegation of power to sign messages *"IEICE Transaction on Fundamentals", E79-A(1996), pp.1338-1353,* 1996

[2] Kar, J, P., Proxy Blind multi-signature scheme using ECC for handheld devices, *ePrint Archive: Report 2011/043, available at: http://eprint.iacr.org/2011/43*

[3] Chaum, D., Blind Signature for Untraceable Payments, *In Crypto 82, New York, Plenum Press, pp.199-203*, 1983.

[4] Hwang, S, J., Shi, C, H. (2000). A Simple multi-signature scheme, “Proceeding of 10th National conference on Information Security, Taiwan.

[5] Koblitz, N. (1994). A course in Number Theory and Cryptography ,2nd edition Springer-Verlag-1994

[6] Rosen, K, H.(1986). Elementary Number Theory in Science and Communication, 2nd ed., *Springe*r-Verlag, Berlin.

[7] Menezes, A., Van Oorschot, P,C., Vanstone, S, A.(1997). Handbook of applied cryptog-raphy. CRC Press.

[8] Hankerson, D., Menezes, A., Vanstone,S.(2004) Guide to Elliptic Curve Cryptography, Springer Verlag.

[9] Certicom ECC Challenge and The Elliptic Curve Cryptosystem, available :http://www.certicom.com/index.php.

[10] Dwork C., Naor, M., Sahai, A. (1998). Concurrent zero-knowledge, in Proceedings of 30th ACM STOC’98, 409-418.

[11] Abdalla, M., Bellare, M., Rogaway, P.(2001). *T*he oracle Diffe-Hellman assumptions and an analysis of DHIES, *In*: Topics in Cryptology - CT-RSA 2001, LNCS, 2020,143-158.

[12] Aumann, Y., Rabin, M. (1998). Authentication, enhanced security and error correcting codes, *In*: Advances in Cryptology - Crypto’98, LNCS, 1462, 299-303.

[13] Diffe, W., Hellman, M,E. (1976). Directions in cryptography, *IEEE Transactions on Information Theory*, 22, 644-654.

[14] Shi, Y., Li, J., (2005), Identity-based deniable authentication protocol, *Electronics Letters*, 41,241-242.

[15] Shoup, V. (2004). Sequences of games: a tool for taming complexity in security proofs, in Cryptology ePrint Archive: Report 2004/332, available at: http://eprint.iacr.org/2004/332.