Cryptanalysis and Improvement of Yanlin and Xiaoping's Signature Scheme based on ECDLP and Factoring

Hemlal Sahu
School of Studies in Mathematics
Pt. RavishankarShukla University Raipur (C.G.)
India 492010

B. K. Sharma
School of Studies in Mathematics
Pt. RavishankarShukla University Raipur (C.G.)
India 492010

ABSTRACT
Qin Yanlin and Wu Xiaoping proposed a digital signature scheme based on elliptic curve discrete logarithm problem and factoring a composite integer. They claimed that the security of their scheme depends on solving ECDLP and factoring both. In this paper, it is shown that if anyone can solve ECDLP then he can generate a valid signature without knowledge of private keys. An improved scheme is also proposed in this paper. The proposed scheme requires minimal operations in encryption and decryption algorithms which makes it more efficient.

General Terms
2000 AMS Subject Classification No. 94A60

Keywords
Cryptanalysis; elliptic curve discrete logarithm; factoring

1. INTRODUCTION
Since the invention of public-key cryptography in 1976 by Whitfield Diffie and Martin Hellman [1] numerous public-key cryptographic systems and signature schemes have been proposed. The security of all of these systems was based on the difficulty of solving a mathematical problem. Many of them public-key cryptographic systems have been broken and many others have been demonstrated to be impractical. Today, three types of systems are considered secure and efficient. The mathematical problem on which their security is based, are

1. Integer factorization problem (IFP) (RSA [8])
2. Discrete logarithm problem (DLP) (ElGamal[2])
3. Elliptic curve discrete logarithm problem (ECDLP)(elliptic curve analogue of ElGamal [4][7]

Several public-key cryptosystems are based on solving just one hard problem. If these cryptographic assumptions are made easy to solve, the corresponding cryptosystems will no longer be secure. Thus several cryptographic systems try to base their security on solving multiple hard problems simultaneously. Although only few of them achieved their goal Li et.al. [6], L Harn [3], Laih and Kuo [5] are some digital signature schemes based on multiple problems. Qin Yanlin and Wu Xiaoping [9] gave a digital Signature Scheme Based on both ECDLP and IFP. They claimed that the security of their scheme depends on solving both the problems ECDLP and IFP. Now in this paper we shown that their claim is incorrect .That is security of their scheme can be broken by solving only one problem ECDLP. So security of digital signature scheme proposed by Qin Yanlin et.al [9] depends on solving only one problem not two. An improvement of Yanlin and Wu Xiaoping scheme is also proposed which is more secure and efficient. The main advantage of Elliptic Curve Cryptography (ECC) is that its cipher key is much shorter than other cryptographies on the premise of same security. Shorter key means less management time and smaller storage which supplies convenience to realization of software and hardware. ECC hasn't been attacked by sub exponent algorithm till now.

The rest of this paper is as follows: In next sections, Yanlin and Wu Xiaoping's scheme and its cryptanalysis are discussed. In section 4, we give improved digital signature scheme and in sections 5, 6 efficiency and security analysis of proposed scheme are analyzed. Last section is conclusion.

2. REVIEW OF QIN YANLIN ' S DIGITAL SIGNATURE SCHEME

2.1. System Parameter of the Digital Signature Scheme.
Let p be a large prime number and $p-1$ has two prime factors p_1 andq_1, Let $n = p_1q_1$, so that $n \mid (p-1).a, b \in GF(p)$, and confirm the Elliptic Curve. The root points of Elliptic Curve construct a circulating subgroup. P is a generating element for the subgroup and its rank equals to n. $h()$ is a secure hash function. The public parameters are p, n, P and the secret parameters are $p_1$and q_1.

2.2. Creation of User's Secret Key and Public Key
Alice chooses a random integer $d \in [1, n-1]$ and computes $Q = d^2P$, then she chooses t, random integers $u_1, u_2, \ldots\ldots, u_t$, where $u_i \in [1, n-1]$ and $(u_i^2 mod n, n) = 1$. Next she computes l_i from

$$l_i u_i^2 = -1 mod n \ (i = 1, 2, \ldots\ldots, t)$$

$(d, u_1, u_2, \ldots\ldots, u_t)$ is protected as secret key of Alice and $Q, l_1, l_2, \ldots\ldots, l_i$ are the corresponding public keys.

2.3. Creation of Signature
Alice performs the following steps to sign message m :-

1) Compute hash value $h(m)$ of m;
2) Choose random integer $k \in [1, n-1], (k, n) = 1$ and compute point $R(x_R, y_R) = k^2P$. Introduce the notation r, where $r \equiv x_R mod n$. If $r = 0$, turn to the first step:
3) Compute $k^{-1} mod n$.
4) Compute $S_1 \equiv (h(m) - rd)k^{-1} mod n$ and $S_2 \equiv (h(m)d + r)k^{-1} mod n$.
5) Choose v which satisfies $(v, n) = 1$. Compute $\alpha \equiv \frac{1}{2}\left(v - \frac{s_1^2 + s_2^2}{v}\right) mod n$ and $h(\alpha) = (e_1, e_2, \ldots\ldots, e_t)$, where $e_i \in \{0, 1\}$. If the number of 1 in $e_1, e_2, \ldots\ldots, e_t$ is an even number, we have to choose another v until that the number of 1 in $e_1, e_2, \ldots\ldots, e_t$ is an odd number.
6) Compute

$$\beta = \frac{1}{2}\prod_{i=1}^{t} u_i^{e_i}\left(v - \frac{s_1^2 + s_2^2}{v}\right) mod n$$

At last, Alice lets $(R,\ \alpha,\ \beta)$ be the signature of m and sends the signed message $(m;\ (R,\ \alpha,\ \beta)$ to the authenticator Bob.

2.4. Authenticator of Signature

The receiver of signature Bob gets the signed message $(m;\ (R,\ \alpha,\ \beta)$, he will take the following steps to authenticate the signature:

1) Compute $h(m)$ from the received m;
2) Compute $h(\alpha) = (e_1, e_2, \ldots\ldots, e_t)$;
3) Authenticate the equation $(\alpha^2 + \beta^2 \prod_{i=1}^{t} l_i^{e_i})R = (h(m)^2 + r^2)Q + (h(m)^2 + r^2)P$

3. CRYPTANALYSIS

Now suppose an adversary attempts to forge a valid signature $(R,\ \alpha,\ \beta)$for a given message m. Adversary does not know secret keys and valid signature of the signer. He sets two variables of $(R,\ \alpha,\ \beta)$ to be the fixed integers and find the other variable from the equation

$$(\alpha^2 + \beta^2 \prod_{i=1}^{t} l_i^{e_i})R = (h(m)^2 + r^2)Q + (h(m)^2 + r^2)P$$

Adversary randomly selects $(\alpha,\ \beta)$. He reduces above equation as

$$\left(\alpha^2 + \beta^2 \prod_{i=1}^{t} l_i^{e_i} k^2\right) = (h(m)^2 + r^2)(d^2 + 1) mod n$$

Suppose Adversary is able to solve ECDLP, then Adversary can find d^2 from $Q = d^2 P$. From above equation

$$\beta^2 \prod_{i=1}^{t} l_i^{e_i} k^2 = ((h(m)^2 + r^2)(d^2 + 1) - \alpha^2) mod n$$

If gcd $\left(\beta^2 \prod_{i=1}^{t} l_i^{e_i}, n\right) \neq 1$then Adversary can factor n. So he can find secret keys.

If$\gcd\left(\beta^2 \prod_{i=1}^{t} l_i^{e_i}, n\right) = 1$, then inverse of $(\beta^2 \prod_{i=1}^{t} l_i^{e_i})$ exists and Adversary can find k^2 by

$$k^2 = (\beta^2 \prod_{i=1}^{t} l_i^{e_i})^{-1} ((h(m)^2 + r^2)(d^2 + 1) - \alpha^2) mod n$$

Therefore $(R = k^2 P,\ \alpha,\ \beta)$ becomes a valid signature for message m, and Adversary thus get success in his attempts to generate a valid signature.

4. IMPROVED DIGITAL SIGNATURE SCHEME

Now describe our new digital signature scheme based on intractability of multiple problems.

4.1. System initialization

In the system initialization phase, the following commonly required parameters are generated to initialize the scheme.

1) Let p be a large prime number and $p - 1$ has two large primefactors $p_1, q_1, n = p_1 q_1$, so that $n | p - 1$
2) Two parameters $a, b \in G(F_p)$ that define the equation of ellipticcurve E over $F_p(y^2 = x^3 + ax + b\ (mod\ q)$ in the case $p > 3$,where $4a^3 + 27b^2 \neq 0)$
3) A point P of elliptic curve E whose rank is equal to n.
4) $h(,)$ a secure hash function.

4.2. Key generation

In our scheme each user has two pairs of secret keys and public keys. One of the pairs is (u, Q) satisfying $ku^2 = -1 mod\ n$ and $Q = kP$. Other pair is (u_1, k_1) satisfying $k_1 u_1^2 = 1 mod\ n$.

4.3. Signature generation

Signer executes the following steps.

1) Randomly select a number b such that $b^2 = a\ mod n$ and compute $R = aP$.
2) Select a random number r such that $gcd(r, n) = 1$.
3) Calculate $x = \frac{1}{2}(r + \frac{a}{r}) mod\ n$.
4) Calculate $y = \frac{1}{2} u u_1^{h(M,x)} (r - \frac{a}{r}) mod\ n$.
5) Calculate $t = bu\ mod\ n$.

Then (R, x, y, t) is a signature of M signed by signer.

4.4. Signature verification

After receiving the signature (R, x, y, t) for M, the verifier verifies the validity of the signature through the following equation

$$x^2 P + y^2 k_1^{h(M,x)} Q = -t^2 Q = R \qquad (4.1)$$

If it holds, the message M is authenticated and the signature (R, x, y, t) is valid.

Theorem 4.1. The signature is considered to be valid if the signer and verifier confirm to the applied protocols.

Proof . $x^2 P + y^2 k_1^{h(M,x)} Q$

$$= \frac{1}{4}(r + \frac{a}{r})^2 P + \frac{1}{4} u^2 u_1^{2h(M,x)} (r - \frac{a}{r})^2 k_1^{h(M,x)} Q$$

$$= \frac{1}{4}(r^2 + (\frac{a}{r})^2 + 2a)P + \frac{1}{4}(r^2 + \left(\frac{a}{r}\right)^2 - 2a\Big) u^2 u_1^{2h(M,x)} k k_1^{h(M,x)} P$$

$$= \frac{1}{4}(r^2 + (\frac{a}{r})^2 + 2a)P + \frac{1}{4}(r^2 + \left(\frac{a}{r}\right)^2 - 2a\Big) (ku^2)(k_1 u_1^2)^{h(M,x)} P$$

$$= {}^1/_4\,(4a)P$$

$$= R$$

and

$$-t^2 Q = -b^2 u^2 kP = aP = R$$

5. SECURITY ANALYSIS

The security with elliptic curve based discrete logarithm is more reliable in public key cryptosystems as compare to others. To find solution x of quadratic equation $x^2 = a\ mod\ n$ is as difficult as factoring n. Security of proposed scheme depends on solving both the problems. Some possible attacks by which an adversary may try to take down the proposed scheme will be analyzed as follows.

Attack1−Assume an adversary attempts to obtain the secret key from the public key of any user. In this attack, the adversary must solve the ECDL problem to derive k from

public key Q. In addition the adversary needs to solve the IFP to recover u from $ku^2 = -1 mod n$. Similarly, the adversary must solve the IFP of n to obtain u_1 from $k_1 u_1^2 = 1 mod n$.

Attack2−Assume an adversary attempts to forge a valid signature (R, x, y, t) for a given message M. Adversary does not know secret key and valid signature of the signer. The adversary sets two variables to be fixed integers and find solutions to the other variable from equation (4.1). Then the adversary has to randomly select (x, y) and find t and R to satisfy equation (4.1), which is as difficult as solving ECDLP and IFP simultaneously. In another similar approach, given (R, y), finding x and t to satisfy equation (4.1) is also as difficult as solving ECDLP, IFP and one way hash function,simultaneously.

Attack3− An adversary may also try collecting l valid signatures (R_j, x_j, y_j, t_j) on message M_j , signed by signer, $j = 1, 2, 3, . l$.Adversary, attempts to obtain the secret key u and u_1 from the following equations

$$x_1^2 + y_1^2 k k_1^{h(M,x)} = a_1 = -k t_1^2 mod n$$

$$x_2^2 + y_2^2 k k_1^{h(M,x)} = a_2 = -k t_2^2 mod n$$

……
……
……..

$$x_l^2 + y_l^2 k k_l^{h(M,x)} = a_l = -k t_l^2 mod n$$

In the above l equations, there are $(2l + 1)$ variables, k, a_j and $t_j . j = 1, 2, 3, l$ which are not known by the adversary. On the other hand, the adversary first solves ECDLP to obtain k and a_j . Then adversary still has to face the problem of IFP to find u andu_1.

Attack4− Assume an adversary is able to solve the ECDL problem, adversary can obtain integer k from $Q = kP$. In this attack, adversary tries to forge the signature for any message. The adversary can reduce equation (2.1) as

$$x^2 + y^2 k_1^{h(M,x)} k = -k t^2 = a \, mod n$$

from above equation to find t is as difficult as factoring composite number.

Attack5− Assume an adversary is able to solve the factoring problem, then adversary has to face ECDL problem to find secret keys**.**

6. EFFICIENCY ANALYSIS

Efficiency of our scheme is compared with Yanlin and Xiaoping's [9] new digital signature scheme based on both ECDLP and factoring. Following parameters are used to compare

1) T_{MUL} →Time of Executing the Modular Multiplication.
2) T_{EXP} →Time of Executing the Exponentiation.
3) T_{INV} →Time of Executing the Inversion.
4) T_{ADD} →Time of Executing the Addition.
5) T_{EC-MUL} →Time of Executing the Elliptic Curve Multiplication.
6) T_{EC-ADD} →Time of Executing the Elliptic Curve Addition.
7) T_{HASH} →Time of Executing the Hash function.

Modular addition and subtraction are ignored here

Efficiency of proposed scheme is analyzed below.

Phases	Yanlin and Xiaoping's scheme	Our scheme
Key generation	$(t+1)T_{MUL} + tT_{INV} + 1T_{EC-MUL}$	$2T_{MUL} + 2T_{INV} + 1T_{EC-MUL}$
Signature generation	$(t+8)T_{MUL} + 2T_{INV} + tT_{EXP} + 2T_{HASH} + 1T_{EC-MUL}$	$5T_{MUL} + 1T_{INV} + 1T_{EXP} + 1T_{HASH} + 1T_{EC-MUL}$
Signature verification	$(t+4)T_{MUL} + tT_{EXP} + 2T_{HASH} + 3T_{EC-MUL} + 1T_{EC-ADD}$	$4T_{MUL} + 1T_{EXP} + 1T_{HASH} + 3T_{EC-MUL} + 1T_{EC-ADD}$

7. CONCLUSION

Security of digital signature scheme proposed by Qin Yanlin et.al. depends only on solving ECDLP. Security of our scheme depends on solving ECDLP and factoring both. The proposed scheme also requires minimal operations in encryption and decryption algorithms thus it is more efficient. Some possible attacks have also been considered and showed that the scheme is secure from those attacks.

8. REFERENCES

[1] Diffie W, Hellman M. 1976, "New directions in cryptography" IEEE trans. Inf. Theory

[2] E1Gamal T. 1985, "A public key cryptosystem and a signature scheme based on discrete logarithms" IEEE Trans. Inf. Theory.

[3] HarnL 1994, "Public key cryptosystem design based on factoring and discrete logarithms" IEE proc. Comp. Digital Tech .

[4] Koblitz, Neal 1987 " Elliptic curve cryptosystems" Mathematics of Computation.

[5] Laih C-S; Kuo W-c, 1997 " New signature scheme based on factoring and discrete logarithms",IEICE Transactions on cryptography and information security.

[6] Li Li-Hua, Tzeng Shiang-Feng;Hwang Min-Shiang, 2005 " Improvement of signature scheme based on factoring and discrete logarithms" ,Applied mathematics and computation 161 (2005)45-49.

[7] Miller, V.S. 1986 "Uses of elliptic curves in cryptography" in: Advances in Cryptology-Crypto'85, Lecture Notes in Computer Science, 218, Springer-Verlag, Berlin.

[8] Rivest R.L.; Shamir A.; Adleman L., 1978 "A method for obtaining digital signatures and public key cryptosystems", Communication of the ACM.

[9] Yanlin,Qin;Xiaoping,Wu 2009 "New Digital Signature Scheme Based on both ECDLP and IFP" ,2nd IEEE International Conference 2009. ICCSIT Computer Science and Information Technology.