STUDIA UNIV. "BABEŞ–BOLYAI", INFORMATICA, Volume **XLIV**, Number 2, 1999

BLIND SIGNATURE AND BLIND MULTISIGNATURE SCHEMES USING ELLIPTIC CURVES

CONSTANTIN POPESCU

Abstract. Blind signature schemes and blind multisignature schemes are useful in protocols that guarantee the anonymity of the participants. In this paper we propose an elliptic curve blind signature scheme and an elliptic curve blind multisignature scheme. The proposed schemes are described in the group of points on an elliptic curve because it offer equivalent security as the other groups but with smaller key size and faster computation times.

1. Introduction

The concept of blind signature schemes was introduced by Chaum in 1982 [2]. A blind signature scheme allows to realize secure electronic payment systems protecting customer's privacy [1], [3], [5]. Recent anonymous prepaid electronic payment systems, based on the blind signature technique, emulate physical cash. In these systems, the users withdraw electronic coins which consist of numbers, generated by users, and blindly signed by an electronic money issuer. Each signature represents a given amount. These coins are then spent in shops which can authenticate them by using the public signature key of the bank. The users retain anonymity in any transaction since the coins they use have been blindly signed.

In a blind multisignature scheme [8], [10] we have one owner Alice, who wants to obtain a digital signature from several signers, so that each signer doesn't know a relationship between the blinded and unblinded message and signature parameters. This means they cannot recognize the signature later, even if they all collude. A blind multisignature scheme can be used as a building block in cryptographic applications, e.g. in electronic voting schemes [4].

In this paper we propose an elliptic curve blind signature scheme and an elliptic curve blind multisignature scheme. The schemes proposed are described in the group of points on an elliptic curve defined over a finite field. Elliptic curve groups are advantageous because they offer equivalent security as the other groups but with smaller key size and faster computation times.

1991 *Mathematics Subject Classification.* 94A60.

1991 *CR Categories and Descriptors.* D.4.6 [**Operating Systems**]: Security and Protection – *Authentication Cryptographic controls.*

2. Elliptic Curves over Finite Fields

Many researchers have examined elliptic curve cryptosystems, which were firstly proposed by Miller [15] and Koblitz [12]. The elliptic curve cryptosystems which are based on the elliptic curve logarithm over a finite field have some advantages over other systems: the key size can be much smaller over the other schemes since only exponential-time attacks have been known so far if the curve is carefully chosen [13], and the elliptic curve discrete logarithms might be still intractable even if factoring and the multiplicative group discrete logarithm are broken.
Elliptic Curves over $GF(2^n)$: A non-supersingular elliptic curve E over $GF(2^n)$ can be written into the following standard form

$$E: \quad y^2 + xy = x^3 + ax^2 + b, \quad b \neq 0,\ a, b \in GF(2^n).$$

The points $P = (x, y)$, $x, y \in GF(2^n)$ that satisfy this equation, together with a "point at infinity" denoted O form an abelian group $(E, +, O)$ whose identity element is O.

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two different points on E and both P and Q are not equal to the infinity point. Addition law for E non-supersingular is as follow: For $2P = P + P = (x_3, y_3)$, if $x_1 \neq 0$

$$\begin{aligned} x_3 &= \delta^2 + \delta + a \\ y_3 &= (x_1 + x_3)\delta + x_3 + y_1, \quad \textit{where } \delta = x_1 + y_1/x_1. \end{aligned}$$

If $x_1 = 0$, $2P = O$. For $P + Q = (x_3, y_3)$, if $x_1 = x_2$, then $P + Q = O$. Otherwise,

$$\begin{aligned} x_3 &= \lambda^2 + \lambda + x_1 + x_2 + a \\ y_3 &= (x_1 + x_3)\lambda + x_3 + y_1, \quad \textit{where } \lambda = (y_1 + y_2)/(x_1 + x_2). \end{aligned}$$

Elliptic Curves over $GF(p^n)$: A non-supersingular elliptic curve E over $GF(p^n)$, $p > 2$ can be written into the following standard form

$$E: \quad y^2 = x^3 + ax + b, \quad 4a^3 + 27b^2 \neq 0,\ a, b \in GF(p^n).$$

For the addition law, for the elliptic curve E over $GF(p^n)$, see more details in [15].

3. Elliptic Curve Blind Signature Scheme

In this section we describe the elliptic curve blind version of the Harn's signature scheme [7]. We will use the same setup as suggested in IEEE P1363 standard form [11].

3.1. Key Generation.

Firstly, we choose elliptic curve domain parameters:

(1) Choose p a prime and n an integer. Let $f(x)$ be an irreducible polynomial over $GF(p)$ of degree n, generating finite field $GF(p^n)$ and assume that α is a root of $f(x)$ in $GF(p^n)$.

(2) Two field elements $a, b \in GF(p^n)$, which define the equation of the elliptic curve E over $GF(p^n)$ (i.e., $y^2 = x^3 + ax + b$ in the case $p > 3$), where $4a^3 + 27b^2 \neq 0$.
(3) Two field elements x_p and y_p in $GF(p^n)$, which define a finite point $P = (x_p, y_p)$ of prime order in $E(GF(p^n))$ ($P \neq O$, where O denotes the point at infinity).
(4) The order q of the point P.
(5) The converting function $c(x) : GF(p^n) \rightarrow Z_{p^n}$ which is given by

$$c(x) = \sum_{i=0}^{n-1} c_k p^i \in Z_{p^n}, \quad x = \sum_{i=0}^{n-1} c_k \alpha^i \in GF(p^n),\ 0 \leq c_i < p.$$

The operation of the key generation is as follows:

(1) Select a private key d, a random integer, from the interval $[1, q-1]$.
(2) Compute the public key Q, which is a point on E, such that $Q = dP$.

3.2. **Blind Signature Protocol.** The following protocol is a blind version of the Harn's elliptic curve signature scheme.

(1) Alice generates a one-time key pair $(\overline{k}, \overline{R})$ in the following way: randomly chooses $\overline{k} \in [1, q-1]$ and compute $\overline{R} = \overline{k}P = (x_{\overline{k}}, y_{\overline{k}})$. She computes $\overline{r}$ such that

$$\overline{r} = c(x_{\overline{k}}) = \sum_{i=0}^{n-1} c_{i\overline{k}} p^i, \quad where\ x_{\overline{k}} = \sum_{i=0}^{n-1} c_{i\overline{k}} \alpha^i,\ 0 \leq c_{i\overline{k}} < p.$$

and sends $\overline{r}$ and $\overline{R}$ to Bob.
(2) Bob chooses blind factors $a, b \in [1, q-1]$, computes the point R on E such that $R = a\overline{R} + bP = (x_k, y_k)$ and computes $r = c(x_k)$. He also computes $\overline{m} = (H(m) + r)a^{-1} - \overline{r}$, where $H(\cdot)$ is a hash function, and sends $\overline{m}$ to Alice.
(3) Alice computes $\overline{s} = d(\overline{m} + \overline{r}) + \overline{k}\ (mod\ q)$ and sends $\overline{s}$ to Bob.
(4) Bob computes $s = a\overline{s} + b$.

The pair (r, s) is an elliptic curve signature of the message m.

Theorem 3.1. *The pair (r, s) is a Harn elliptic curve signature of the message m and the above protocol is an elliptic curve blind signature scheme.*

Proof: The validity of the signature (r, s) of the message m follows from the next steps:

(1) Compute a point on E such that $sP - (H(m) + r)Q = (x_e, y_e)$.
(2) Use the converting function to compute the integer $c(x_e)$ and check if $r = c(x_e)(mod\ q)$. If this equation is true, then (r, s) is accepted as a valid signature of the message m. It is easy to verify that $sP - (H(m) + r)Q = R$.

To prove that the above protocol is blind we show that for every possible signer's view there exists a unique pair (a, b) of blind factors, with $a, b \in [1, q-1]$. Given any view consisting of $\overline{R}, \overline{k}, \overline{r}, \overline{m}, \overline{s}$ and any valid elliptic curve signature (r, s) of a message m, we consider

$$\begin{aligned} a &= (H(m)+r)(\overline{m}+\overline{r})^{-1}(mod\ q) \\ b &= s - a\overline{s}(mod\ q). \end{aligned}$$

We have to show that $R = a\overline{R} + bP$. We have $a\overline{R} + bP = a\overline{k}P + sP - a\overline{s}P = a\overline{k}P + sP - aP(d\overline{m} + d\overline{r} + \overline{k}) = sP - adP((H(m)+r)a^{-1} - \overline{r}) - ad\overline{r}P = sP - dH(m)P - drP = sP - (H(m)+r)Q = R.$ □

4. Elliptic Curve Blind Multisignature Scheme

In this section we describe the elliptic curve blind version of the Harn's multisignature scheme [8].

4.1. **Key Generation.** The elliptic curve domain parameters are the same as in Section 3. We assume there are t signers $U_i,\ i = 1, ..., t$. The operation of the key generation is as follows:

(1) Each signer U_i randomly selects his private key d_i, an integer, from the interval $[1, q-1]$.
(2) The public key of the signer U_i is the point
$$Q_i = d_iP = (x_{d_i}, y_{d_i}),\ i = 1, ..., t.$$
(3) The public key for all signers is
$$Q = Q_1 + ... + Q_t = dP = (x_d, y_d),$$
where $d = d_1 + ... + d_t(mod\ q)$.

4.2. **Blind Multisignature Protocol.** The following protocol is a blind version of the Harn's elliptic curve multisignature scheme.

(1) The user U_i generates a one-time key pair $(\overline{k}_i, \overline{R}_i)$ in the following way: randomly chooses $\overline{k}_i \in [1, q-1]$ and computes $\overline{R}_i = \overline{k}_iP = (x_{\overline{k}_i}, y_{\overline{k}_i})$. The user U_i computes $\overline{r}_i,\ i = 1, ..., t$, such that $\overline{r}_i = c(x_{\overline{k}_i})$ and sends $\overline{r}_i$ and $\overline{R}_i$ to the clerk.
(2) The clerk chooses the blind factors $a, b \in [1, q-1]$, computes the point R on E such that $R = a\overline{R} + bQ = (x_k, y_k)$, where $\overline{R} = \overline{R}_1 + ... + \overline{R}_t$ and $Q = Q_1 + ... + Q_t$. The clerk computes $r = c(x_k)(mod\ q)$ and $\overline{m} = (H(m) + r + b)a^{-1} - \overline{r}$, where $H(\cdot)$ is a hash function, and sends $\overline{m}$ and $\overline{r}$ to each signer U_i.
(3) The user U_i computes the signature $\overline{s}_i = d_i(\overline{m} + \overline{r}) + \overline{k}_i\ (mod\ q),\ i = 1, ..., t$ and sends $\overline{s}_i$ to the clerk.

(4) The clerk computes $\overline{s}_iP - (\overline{m}+\overline{r})Q_i = (x_{e_i}, y_{e_i})$ and check $\overline{r}_i = c(x_{e_i})$ $(mod\ q)$, $i = 1, ..., t$. The elliptic curve blind multisignature of the message m can be generated as (r, s), where $\overline{s} = \overline{s}_1 + ... + \overline{s}_t (mod\ q)$ and $s = \overline{s}a(mod\ q)$.

The pair (r, s) is a elliptic curve multisignature of the message m.

Theorem 4.1. *The pair (r, s) is a Harn elliptic curve multisignature of the message m and the above protocol is an elliptic curve blind multisignature scheme.*

Proof: The validity of the elliptic curve multisignature (r, s) of the message m follows from the next steps:

(1) Compute a point on E such that $sP - (H(m)+r)Q = (x_e, y_e)$.

(2) Use the converting function to compute the integer $c(x_e)$ and check if $r = c(x_e)(mod\ q)$. If this equality is true, then (r, s) is accepted as a valid elliptic curve multisignature of the message m. It is easy to verify that $sP - (H(m)+r)Q = R$.

To prove that the above protocol is blind we show that for every possible signer's view there exists a unique pair (a, b) of blind factors, with $a, b \in [1, q-1]$. Given any view consisting of $\overline{R}_i, \overline{k}_i, \overline{r}_i, \overline{s}_i, \overline{m}, \overline{r}$ and any valid elliptic curve multisignature (r, s) of a message m, we consider

$$\begin{aligned} a &= s\overline{s}^{-1}(mod\ q) \\ b &= (\overline{m}+\overline{r})a - H(m) - r(mod\ q). \end{aligned}$$

We have to show that $R = a\overline{R} + bQ$. We have $a\overline{R} + bQ = a(\overline{R}_1 + ... + \overline{R}_t) + ((\overline{m}+\overline{r})a - (H(m)+r))Q = a(\sum_{i=1}^{t} \overline{s}_iP - \sum_{i=1}^{t}(\overline{m}+\overline{r})Q_i)) + a(\overline{m}+\overline{r})Q - (H(m)+r)Q = a\overline{s}P - (H(m)+r)Q = sP - (H(m)+r)Q = R.$ □

5. Security Considerations

Our elliptic curve blind signature and multisignature schemes are as secure as the Harn schemes [7], [8]. But, our schemes is more efficient than Harn schemes because the group of points on an elliptic curve offer smaller key size and faster computation times. The signature schemes in [9] can provide similar elliptic curve blind signature schemes and elliptic curve blind multisignature schemes. In order to avoid the Pollard-rho [19] and Pohling-Hellman [18] algorithms for the elliptic curve discrete logarithm problem, it is necessary that the number of F_q-rational points on E, denoted $\#E(F_q)$, be divisible by a sufficiently large prime n. It is commonly recommended that $n > 2^{160}$. To avoid the reduction algorithms of Menezes, Okamoto and Vanstone [14] and Frey and Ruck [6], the curve should be non-supersingular. To avoid the attack of Semaev [20] on F_q-anomalous curves, the curve should not be F_q-anomalous (i.e., $\#E(F_q) \neq q$).

A prudent way to guard against these attacks, and similar attacks against special classes of curves that may be discovered in the future, is to select the elliptic curve E at random subject to the condition that $\#E(F_q)$ is divisible by a large prime - the probability that a random curve succumbs to these special purpose attacks is negligible. A curve can be selected verifiable at random by choosing the coefficients of the defining elliptic curve equation as the outputs of a one-way function such as SHA-1 according to some pre-specified procedure.

6. Conclusion

In this paper we proposed an elliptic curve blind signature scheme and an elliptic curve blind multisignature scheme. The proposed schemes are described in the setting of the group of points on an elliptic curve because it offer equivalent security as the other groups but with smaller key size and faster computation times. Our elliptic curve blind signature and multisignature schemes are as secure as the Harn schemes. These schemes are practical, requiring just a few exponentiations or integer multiplications over a group.

References

[1] S. Brands, Electronic Cash Systems Based on the Representation Problem in Groups of Prime Order, Advances in Cryptology-CRYPTO'93, Lecture Notes in Computer Sciences, Springer-Verlag, 1993.

[2] D. Chaum, Blind signature systems, Advances in Cryptology-CRYPTO'83, Plenum Press, 1984, pp. 153.

[3] D. Chaum, Privacy Protected Payment, SMART CARD 2000, Elsevier Science Publishers B.V., 1989, pp. 69-93.

[4] L. Chen, M. Burmester, A practical voting scheme with allows voters to abstain, Proceedings of Chinacrypt'94, 1994, pp. 100-107.

[5] N. Ferguson, Single Term Off-line Coins, Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Sciences, 765, Springer-Verlag, 1993, pp. 318-328.

[6] G. Frey, H. Ruck, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, Mathematics of Computation, 67, 1998, pp. 353-356.

[7] L. Harn, A New Digital Signature Based on the Discrete Logarithm, Electronics Letters, Vol. 30, No.5, 1994, pp. 193-195.

[8] L. Harn, Group-oriented (t, n) Threshold Signature and Multisignature, IEE Proceedings Computers and Digital Techniques, Vol. 141, No.5, 1994, pp. 307-313.

[9] L. Harn, On the design of generalized ElGamal type digital signature schemes based on the discrete logarithm, Electronics Letters, 1994.

[10] P. Horster, M. Michels, H. Petersen, Blind multisignature schemes and their relevance to electronic voting, Proc. 11th Annual Computer Security Applications Conference, New Orleans, IEEE Press, 1995, pp. 149 - 155.

[11] IEEE P1363, Standard Specifications for Public Key Cryptography, The Institute of Electrical and Electronics Engineers, 1998.

[12] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, 48, 1987, pp. 203-209.

[13] N. Koblitz, CM-Curves with Good Cryptographic Properties, Proceedings of Crypto'91, 1992.

[14] A. Menezes, T. Okamoto, S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Transactions on Information Theory, 39, 1993, pp. 1639-1646.

[15] A. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993.

[16] V. Miller, Uses of elliptic curves in cryptography, Advances in Cryptology, Proceedings of Crypto'85, Lecture Notes in Computer Sciences, 218, Springer-Verlag, 1986, pp. 417-426.

[17] T. Okamoto, K. Ohta, Universal Electronic Cash, Advances in Cryptology-CRYPTO'91, Lecture Notes in Computer Sciences, 576, Springer-Verlag, 1991, pp. 324-337.

[18] S. Pohling, M. Hellman, An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance, IEEE Transactions on Information Theory, 24, 1978, pp. 106-110.

[19] J. Pollard, Monte Carlo methods for index computation *mod* p, Mathematics of Computation, 32, 1978, pp. 918-924.

[20] I. Semaev, Evaluation of discrete logarithms in a group of p -torsion points of an elliptic curve in characteristic p, Mathematics of Computation, 67, 1998, pp. 353-356.

University of Oradea, Department of Mathematics, Str. Armatei Romane 5, Oradea, Romania

E-mail address: cpopescu@math.uoradea.ro