Bul. Ştiinţ. Univ. Baia Mare, Ser. B,
Matematică-Informatică, Vol. XV(1999), Nr. 1-2, 145-150

Dedicated to Professor Ion PĂVĂLOIU on his 60th anniversary

PRACTICAL IDENTIFICATION SCHEME BASED ON THE ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM

Constantin POPESCU

Abstract

We present a practical three-move interactive identification scheme based on the elliptic curve discrete logarithm problem. Our identification scheme is almost as efficient as the elliptic curve version of Schnorr identification scheme. The scheme inherit almost all of the merits of the Schnorr identification scheme and the elliptic curve version of Schnorr identification scheme.

AMS classification: 94A60.

Keywords: identification scheme, elliptic curve, three move interactive protocol.

1 Introduction

Public key based identification schemes are very useful and fundamental tools in many applications such as electronic fund transfer and online systems for preventing data access by invalid users. Identification schemes are typical applications of zero-knowledge interactive proofs [5], and several practical zero-knowledge identification schemes have been proposed [1], [2], [3], [12].

Many researchers have examined elliptic curve cryptosystems, which were firstly proposed by Miller [9] and Koblitz [6]. The elliptic curve cryptosystems which are based on the elliptic curve logarithm over a finite field have some advantages than other systems: the key size can be much smaller than the other schemes since only exponential-time attacks have been known so far if the curve is carefully chosen [7], and the elliptic curve discrete logarithms might be still intractable even if factoring and the multiplicative group discrete logarithm are broken.

This contribution presents three-move identification scheme that is as efficient as the elliptic curve Schnorr identification scheme. The scheme inherit almost all of the merits of the Schnorr identification scheme [13] and the elliptic curve version of Schnorr identification scheme from all practical viewpoints such as communication overhead, interaction number, required memory size and processing speed..

2 Description of Identification Scheme

This section describes the proposed identification scheme, which is specified by the key generation and the three-move interactive protocol between A (prover) and B (verifier).

2.1 Key Generation

Firstly, we choose elliptic curve domain parameters:

- a field size q, where q is a prime power (in practice, either $q = p$, an odd prime, or $q = 2^m$).
- two field elements $a, b \in F_q$, which define the equation of the elliptic curve E over F_q (i.e., $y^2 = x^3 + ax + b$ in the case $p > 3$), where $4a^3 + 27b^2 \neq 0$.
- two field elements x_p and y_p in F_q, which define a finite point $P = (x_p, y_p)$ of prime order in $E(F_q)$ ($P \neq O$, where O denotes the point at infinity).
- the order n of the point P.

The operation of the key generation is as follows:

- Select a security parameter t, which is a positive integer (e.g., $t \geq 20$)
- Select P_1, P_2 of order n in the group $E(F_q)$
- Select random integers d_1, d_2 from the interval $[1, n-1]$. The pair (d_1, d_2) is the secret key
- Compute Q_1 and Q_2, points on E, such that

$$Q_1 = -d_1 \cdot P_1, \quad Q_2 = -d_2 \cdot P_2$$

- Compute the point V such that

$$V = Q_1 + Q_2$$

2.2 Interactive Protocol Between A and B

The three-move interactive protocol between A (prover) and B (verifier) is as follows:

- A select random numbers $r_1, r_2 \in [1, n-1]$, and computes the points R_1, R_2, such that
$$R_1 = r_1 \cdot P_1, \quad R_2 = r_2 \cdot P_2$$
- A computes X, point on E, such that
$$X = R_1 + R_2$$
and send X to B.
- B sends a random number $e \in Z_{2^t}$ to A
- A sends to B the pair (y_1, y_2) such that
$$y_1 = r_1 + ed_1, \quad y_2 = r_2 + ed_2$$
- B computes the points S_1, S_2 and U
$$S_1 = y_1 \cdot P_1, \quad S_2 = y_2 \cdot P_2, \quad U = e \cdot V$$
- B computes the point W on E
$$W = S_1 + S_2 + U = (x_0, y_0)$$
and checks that
$$x_1 = x_0$$
where x_1 is the x-coordinate of X and x_0 is the x-coordinate of W.

If it holds, B accepts, otherwise rejects.

3 Security Consideration

In order to avoid the Pollard-rho [11] and Pohling-Hellman [10] 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. To avoid the reduction algorithms of Menezes, Okamoto and Vanstone [8] and Frey and Ruck [4], the curve should be non-supersingular (i.e., p should not divide $(q+1-\#E(F_q))$). To avoid the attack of Semaev [14], Smart [15] 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 verifiably 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.

Our identification scheme is secure if and only if the elliptic curve discrete logarithm is intractable.

References

[1] T. Beth, Efficient Zero Knowledge Identification Scheme for Smart Cards, Proceedings of Eurocrypt'88, LNCS 330, Springer-Verlag, pp. 77-86 (1988).

[2] U. Feige, A. Fiat, A. Shamir, Zero Knowledge Proofs of Identity, Proceedings of STOC, pp. 210-217 (1987).

[3] A. Fiat, A. Shamir, How to Prove Yourself: Practical Solutions to Identification and Signature Problems, Proceedings of CRYPTO'86, LNCS 263, Springer-Verlag, pp. 186-194 (1987).

[4] 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), 353-356.

[5] S. Goldwasser, S. Micali, C. Rackoff, The Knowledge Complexity of Interactive Proofs, SIAM J. Comput., 18, 1, pp. 186-208 (1989).

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

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

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

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

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

[11] J. Pollard, Monte Carlo methods for index computation mod p, Mathematics of Computation, 32, (1978), 918-924.

[12] K. Ohta, T. Okamoto, A modification of the Fiat-Shamir Scheme, Proceedings of Crypto'88, Lecture Notes in Computer Sciences, 403, 1990, Springer-Verlag, pp. 232-243.

[13] C.P. Schnorr, Efficient Signature Generation by Smart Cards, Journal of Cryptology, Vol. 4, No. 3, pp. 161-174 (1991).

[14] 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), 353-356.

[15] N. Smart, The discrete logarithms problem on elliptic curves of trace one, preprint, 1997.

University of Oradea
Department of Mathematics
Str. Armatei Romane 5
Oradea, Romania
E-mail: cpopescu@math.uoradea.ro

Received: 5.08.1999