KEY AGREEMENT PROTOCOL USING ELLIPTIC CURVE MATRIX POWER FUNCTION*

Artūras Katvickis, Paulius Vitkus

***Abstract**: The key agreement protocol (KAP) using elliptic curve matrix power function is presented. This function pretends be a one-way function since its inversion is related with bilinear equation solution over elliptic curve group. The matrix of elliptic curve points is multiplied from left and right by two matrices with entries in Z_n. Some preliminary security considerations are presented.*

***Keywords**: key agreement protocol, elliptic curve cryptography, NP-complete problem.*

***ACM Classification Keywords**: E.3 Data Encryption, F.2.1 Numerical Algorithms and Problems.*

***Conference**: The paper is selected from Sixth International Conference on Information Research and Applications – i.Tech 2008, Varna, Bulgaria, June-July 2008*

Introduction

Key agreement protocols (KAP) is one of the basic cryptographic protocols. KAP allows two or more parties negotiate a common secret key using insecure communications.

First KAP was presented by Diffie-Hellman [Diffie, Hellman, 1976] which caused rapid development of asymmetric cryptography.

In 1993 new ideas appeared in asymmetric cryptography [Sidelnikov et al, 1993] – using known hard computational problems in infinite non- commutative groups instead of hard number theory problems such as discrete logarithm or integer factorization problems to construct one-way functions.

This idea was realized in [Anshel et al, 1999] where KAP was constructed using conjugator search problem and membership problem in Braid groups. The similar result was presented in [Ko et al, 2000].

Later, [Shpilrain, Ushakov, 2004] showed that conjugator search problem does not produce sufficient security level. The others hard problems were investigated to construct KAP and were based on triple decomposition problem [Kurt, 2006], subgroup membership problem [Shpilrain, Zapata, 2006] and elliptic curve pairing [Smart, 2002].

The idea to use non-commutative infinite group (e.g. braid group) representation was also used for the other kind of one-way functions construction as a background of both digital signature scheme and key agreement protocol [Sakalauskas, 2005], [Sakalauskas et al, 2007]. The (semi)group representation level allows us to avoid a significant problem of hiding the factors in the publicly available group word when using its presentation level. The hiding of factors in representation level occurs in a very natural way. However, the original hard problems, such as conjugator search or decomposition problems in (semi)group presentation level are considerably weakened when they are transformed into the representation level. Therefore using representation level these problems must be considerably strengthened by simultaneously adding the other additional hard problems.

In this paper we present KAP using elliptic curve matrix power function. This function pretends be a one-way function since its inversion is related with bilinear equation over elliptic curve group. The matrix of elliptic curve points is left and right side multiplied by two matrices with entries in Z_n.

* Work is partially supported by the Lithuanian State Science and Studies Foundation

Mathematical background

Let $p > 3$ be a prime integer. An elliptic curve $E_p(a, b)$ over GF(p) is defined by equation

$$y^2 = x^3 + ax + b, \quad (1)$$

where $a, b \in$ GF(p) and $4a^3 + 27b^2 \bmod p \neq 0$.

The addition operation between two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on elliptic curve is written in following algebraic formulas:

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \end{aligned} \quad (2)$$

where $\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & P \neq Q, \\ \dfrac{3x_1^2 + a}{2y_1}, & P = Q. \end{cases}$

A set of all points (x, y), $a, b \in$ GF(p), which satisfy (1) equation, together with special point O, called infinity point, and addition operation forms a finite cyclic group with O as its identity.

Another operation, defined on elliptic curve is multiplication of point P by integer k. This operation is defined straightforward, i.e. $4P = P + P + P + P$.

Elliptic curve group order $n = \#E_p(a, b)$ can be roughly estimated using Hasse theorem [York, 1992]:

Let $E_p(a, b)$ is a group on elliptic curve $y^2 = x^3 + ax + b$ and $t = p + 1 - \#E_p(a, b)$. Then

$$|t| \leq 2\sqrt{p}. \quad (3)$$

Equation (3) can be rewritten in more comfortable form:

$$p + 1 - 2\sqrt{p} \leq \#\mathrm{E}_p(a, b) \leq p + 1 + 2\sqrt{p}.$$

Since elliptic curve group is cyclic with order n, fixed point P multiplication by any integer k can be replaced with multiplication by number $\tilde{k} \in Z_n$, where $\tilde{k} = k \bmod n$ and $0P = O$, i.e. any point multiplied by zero is an infinity point.

Key agreement protocol (KAP)

Now we propose the following two parties key agreement protocol.

1. Parties agree on publicly available matrix Q over elliptic curve $E_p(a, b)$ and matrices L, R over Z_n.

2. Alice randomly generates two secret sequences $\{x_i\}$, $\{y_i\}$, $i = 0, 1, \ldots, k$ in Z_n and computes

$$X = \sum_{i=0}^{k} x_i L^i = x_0 I + x_1 L + \ldots + x_k L^k,$$

$$Y = \sum_{i=0}^{k} y_i R^i = y_0 I + y_1 R + \ldots + y_k R^k.$$

3. Bob randomly generates two secret sequences $\{u_i\}$, $\{v_i\}$, $i = 0, 1, \ldots, k$ in Z_n and computes

$$U = \sum_{i=0}^{k} u_i L^i = u_0 I + u_1 L + \ldots + u_k L^k,$$

$$V = \sum_{i=0}^{k} v_i R^i = v_0 I + v_1 R + \ldots + v_k R^k .$$

4. Alice computes intermediate value K_A and sends result to Bob.

$$K_A = XQY \quad (4)$$

5. Bob computes intermediate value K_B and sends result to Alice.

$$K_B = UQV \quad (5)$$

6. Since matrices X, U and Y, V are commutative, both parties compute common secret key

$$K = XK_BY = UK_AV = XUQVY. \quad (6)$$

Preliminary security analysis

The security parameters are matrix dimension m, elliptic curve group order n and secret sequences length k. They must be large enough to prevent brute force attack. To compromise the key K, the adversary must solve the (4), (5) matrix equations to find X, Y and U, V with known instances Q, K_A, K_B.

Let $X = \{x_{ij}\}$, $Y = \{y_{ij}\}$, $Q = \{Q_{ij}\}$, $A = \{A_{ij}\}$ are matrices of 2-nd order. Then matrix equation $XQY = K_A = A$ can be rewritten as system of bilinear equation over elliptic curve group:

$$\begin{cases} x_{11}y_{11}Q_{11} + x_{11}y_{21}Q_{12} + x_{12}y_{11}Q_{21} + x_{12}y_{21}Q_{22} = A_{11} \\ x_{11}y_{12}Q_{11} + x_{11}y_{22}Q_{12} + x_{12}y_{12}Q_{21} + x_{12}y_{22}Q_{22} = A_{12} \\ x_{21}y_{11}Q_{11} + x_{21}y_{21}Q_{12} + x_{22}y_{11}Q_{21} + x_{22}y_{21}Q_{22} = A_{21} \\ x_{21}y_{12}Q_{11} + x_{21}y_{22}Q_{12} + x_{22}y_{12}Q_{21} + x_{22}y_{22}Q_{22} = A_{22} \end{cases} \quad (7)$$

We do not know the actual complexity of such systems. It is known that solution of a system of polynomial equations over any field is NP-Complete [Garey, Jonson, 1979]. But in this case the obtained system is not over the field. This system can be interpreted also as a system of equations in vector space of elliptic curve points over Z_n. Thus, we can make a conjecture that solving a system of bilinear equations over elliptic curve points vector space is not easier than solving a system of bilinear polynomial equations over any field.

We can also refer to Schaefer Dixotomy theorem for a constraint satisfiability problem denoted by SAT(S) [Schaefer, 1978]. In general, the complexity of any computational problem can be estimated by reformulating this problem into the decisional problem and reducing some known NP-Complete problem into this decisional problem. Without proof we assert that there is a SAT(S) problem reducible in polynomial time to the decisional problem corresponding to (4), (5).

On the other hand, notice that proposed KAP is a generalized elliptic curve Diffie-Hellman KAP (ECDH). Indeed, if we set matrix dimension to $m = 1$ and secret sequence length to $k = 1$, we get algorithm similar to ECDH.

Further investigations are required to select the values of security parameters and estimate the security level.

Bibliography

[Anshel et al, 1999] Anshel I., Anshel M., Goldfeld D. An algebraic method for public key cryptography. Mathematical Research Letters 6, pp. 1–5, 1999.

[Diffie, Hellman, 1976] Diffe W., Hellman M.. New Directions in Cryptography. In IEEE Transaction on Information Theory, IT-22 (6, 644-654), 1976.

[Garey, Jonson, 1979] Garey M. R., Johnson D. S. Computers and Intractability: A Guide to the Theory of NP-Completeness, W. H. Freeman and Company, 1979.

[Ko et al, 2000] Ko K. H., Lee S. J., Cheon J. H., Han J. W., Kang J. S., Park C. New Public key Cryptosystem Using Braid Groups. Advances in Cryptology, Proc. Crypto 2000, LNCS 1880, Springer–Verlag, pp. 166–183, 2000.

[Kurt, 2006] Kurt Y. A New Key Exchange Primitive Based on the Triple Decomposition Problem. Available at: http://eprint.iacr.org/2006/377, 2006

[Sakalauskas, 2005] Sakalauskas E., One Digital Signature Scheme in Semimodule over Semiring, *Informatica*. ISSN: 0868-4952, vol. 16, no. 3(2005), pp. 383-394.

[Sakalauskas et al, 2007] Sakalauskas E., Tvarijonas P., Raulinaitis A., *Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problems in Group Representation Level,* Informatica, Vol. 18, No. 1, 2007, pp. 115-124.

[Sidelnikov et al, 1993] Sidelnikov V., Cherepnev M., Yaschenko V. Systems of open distribution of keys on the basis of non-commutative semigroups. Russian Acad. Sci. Dokl. Math., 48(2), pp. 566-567, 1993.

[Schaefer, 1978] Schaefer T.J., The Complexity of Satisfiability Problems. In Proceedings 10th ACM Symposium on Theory of Computing, 216-226, 1978.

[Shpilrain, Ushakov, 2004] Shpilrain V., Ushakov A., The conjugacy search problem in public key cryptography: unnecessary and insufficient, Available at: http://eprint.iacr.org/2004/321, 2004.

[Shpilrain, Zapata, 2006] Shpilrain V., Zapata G. Using the subgroup membership search problem in public key cryptography. Contemp. Math., Amer. Math. Soc. 418 (2006), 169–179

[Smart, 2002] Smart N. P. An Identity Based Authenticated Key Agreement Protocol Based on the Weil Pairing. Electronics Letters, 38 (13). ISSN 00135194, pp. 630–636. 2002.

[York, 1992] York E. Elliptic Curves Over Finite Fields. Aviable at: http://www.math.rochester.edu/people/grads/jdreibel/ref/yorkECC.pdf, 1992.

Authors' Information

Artūras Katvickis *– PhD student, Department of Applied Mathematics, Kaunas University of Technology, Studentu str. 50-324a, Kaunas, LT-51368, Lithuania, e-mail arturas.katvickis@ktu.lt*

Paulius Vitkus *– M.Sc. student, Department of Applied Mathematics, Kaunas University of Technology, Studentu str. 50-324a, Kaunas, LT-51368, Lithuania, e-mail paulius.vitkus@ktu.lt*