UCL Crypto Group Technical Report Series

Reducing Elliptic Curve Cryptosystem of Meyer-Müller

Marc Joye and Jean-Jacques Quisquater

http://www.dice.ucl.ac.be/crypto/

Technical Report
CG–1996/4

Place du Levant, 3
B-1348 Louvain-la-Neuve, Belgium

Phone: (+32) 10 472541
Fax: (+32) 10 478667

Reducing Elliptic Curve Cryptosystem of Meyer-Müller

Marc Joye[1)] and Jean-Jacques Quisquater[2)]

March 6, 1996

[1)] Département de Mathématique (AGEL), Université de Louvain
Chemin du Cyclotron, 2, B-1348 Louvain-la-Neuve, Belgium
E-mail: joye@agel.ucl.ac.be

[2)] Département d'Électricité (DICE), Université de Louvain
Place du Levant, 3, B-1348 Louvain-la-Neuve, Belgium
E-mail: jjq@dice.ucl.ac.be

Abstract. In [11], we showed the equivalence of the preliminary version of the Meyer-Müller's cryptosystem to the one of Rabin-Williams [15, 17]. In this paper, we proved that the second version of their cryptosystem is also equivalent to the cryptosystem of Rabin-Williams.

1 Meyer-Müller's public-key cryptosystem

Let n be the product of two large secret primes p and q, both congruent to 11 modulo 12. Consider the elliptic curve E over the ring $\mathbb{Z}/n\mathbb{Z}$ given by the Weierstraß equation:

$$E : y^2 = x^3 + ax + b.$$

1.1 Encryption procedure

Assume Alice wants to send the message m to Bob. First, she randomly chooses $\lambda \in \mathbb{Z}/n\mathbb{Z} - \{0\}$, and sets $P = (m^2, \lambda m^3)$. Next, she sets $a = \lambda^3$, and computes $b = (\lambda^2 - 1)m^6 - am^2$. Finally, she computes $Q = 2P$, and sends the corresponding ciphertext consisting of

$$a, b, x(Q), t = \left(\frac{y(Q)}{n}\right), l = \operatorname{lsb}\left(y(Q)\right).$$

1.2 Decryption procedure

Since Bob knows the factorization of n, he can recover the message m as follows. He first computes the unique square root $y(Q)$ of $x(Q)^3 + ax(Q) + b$, with type t and lsb l. Next, he computes the set

$$I = \Big\{1 \le i \le s \mid 2P_i = Q \text{ and } a^2 = y(P_i)^6 x(P_i)^{-9}\Big\}.$$

If $\#I = 1$, then the message is given by $m = y(P_I)^3 x(P_I)^{-4} a^{-1}$.

2 Analysis

We can easily determine two polynomials $\mathcal{P}_1$ and $\mathcal{P}_2 \in \mathbb{Z}/n\mathbb{Z}[x]$ for which m^2 is a root.

Since the point $P = (m^2, \lambda m^3)$ is on the curve, we have

$$\lambda^2 m^6 = m^6 + am^2 + b, \tag{1}$$

and we construct the first polynomial

$$\begin{aligned}\mathcal{P}_1(x) &= (\lambda^2 x^3)^3 - (x^3 + ax + b)^3 \\ &= (a^2-1)x^9 - 3ax^7 - 3bx^6 - 3a^2x^5 - 6abx^4 - (a^3+3b^2)x^3 \\ &\qquad -3a^2bx^2 - 3ab^2x - b^3. \end{aligned}\tag{2}$$

The second polynomial comes from the first coordinate of the point Q, which is given by

$$x(Q) = \frac{(3m^4 + a)^2}{4\lambda^2 m^6} - 2m^2.$$

Hence, with equation (1), we have

$$\begin{aligned}\mathcal{P}_2(x) &= \big(x(Q) + 2x\big)(4\lambda^2 x^3) - (3x^2 + a)^2 \\ &= \big(x(Q) + 2x\big)4(x^3 + ax + b) - (3x^2 + a)^2 \\ &= -x^4 + 4x(Q)x^3 + 2ax^2 + \big(8b + 4ax(Q)\big)x - a^2 + 4bx(Q). \end{aligned}\tag{3}$$

Since m^2 is a root of $\mathcal{P}_1$ and $\mathcal{P}_2$, m^2 will be a root of

$$\mathcal{R} = \gcd(\mathcal{P}_1, \mathcal{P}_2), \tag{4}$$

which is, with a very high probability [14, 7], a polynomial of degree 1. Thus, by solving this polynomial in x, we obtain the value of m^2.

3 Conclusion

In the scheme of Meyer and Müller [13], the decryption process involves the computation of 'square roots' on an elliptic curve. As showed in the previous section, the decryption process may be simplified as follows.

First, Bob computes the polynomial $\mathcal{R}$ and gets the value of m^2. Since m^2 has 4 square roots (modulo n), Bob finds the message m according to the y-coordinate of $Q = 2(m^2, \lambda m^3)$ has type t and lsb l.

Moreover, the system of Meyer and Müller is equivalent to the cryptosystem of Rabin-Williams [15, 17], because it enables to recover the value of m^2. Consequently, that implies the equivalence of their cryptosystem to factoring as proved in [15].

Acknowledgements

We are grateful to Daniel Veithen for some fruitful discussions. We are also grateful to Bernd Meyer and Volker Müller for providing us information about their cryptosystem.

References

[1] A. V. Aho, J. E. Hopcropft, and J D. Ullman: *The design and analysis of computer programming.* Addison-Wesley, 1974.

[2] C. Batut, D. Bernardi, H. Cohen, and M. Olivier: *User's guide to PARI-GP.* Available via anonymous ftp at megrez.math.u-bordeaux.fr, Jan. 1995.

[3] H. Cohen: *A course in computational algebraic number theory.* Number 138 in Graduate Texts in Mathematics. Springer-Verlag, 1993.

[4] D. Coppersmith: 'Finding a small root of a univariate modular equation', preprint, to appear in *Eurocrypt'96.*

[5] D. Coppersmith: 'Finding a small root of a bivariate integer equation: factoring with high bits known', preprint, to appear in *Eurocrypt'96.*

[6] D. Coppersmith: 'Small solutions to polynomial equations, and low exponent RSA vulnerabilities', submitted to *Journal of Cryptology.*

[7] D. Coppersmith, M. Franklin, J. Patarin, and M. Reiter: 'Low exponent RSA with related messages', preprint, to appear in *Eurocrypt'96*.

[8] M. K. Franklin, and M. K. Reiter:. 'A linear protocol failure for RSA with exponent three', preliminary note for *Crypto'95* rump session.

[9] L. Guillou, and J.-J. Quisquater: 'Efficient digital public-key signatures with shadow', in *Advances of Cryptology – Crypto '87, Lectures Notes on Computer Science*, Vol. 293, Springer-Verlag, 1988.

[10] L. Guillou, J.-J. Quisquater, and al.: *Information Technology – Security techniques – Digital signature scheme giving message recovery.* ISO/IEC 9796, 1991.

[11] M. Joye, and J.-J. Quisquater: 'Note on the preliminary version of the Meyer-Müller's cryptosystem', Technical report CG-1996/2, UCL Crypto Group, Université catholique de Louvain, Jan. 1996.

[12] M. Joye, and J.-J. Quisquater: 'Protocol failures for RSA-like functions using Lucas sequences and elliptic curves', presented at the *1996 Cambridge Workshop on Security Protocols*, Cambridge, 10–12 April 1996.

[13] B. Meyer, and V. Müller: 'A public key cryptosystem based on elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ equivalent to factoring', preprint, to appear in *Eurocrypt'96*.

[14] J. Patarin: 'Some serious protocol failures for RSA with exponent e of less than $\simeq$ 32 bits', presented at the *Conference of Cryptography*, CIRM Luminy, France, 25–29 Sept. 1995.

[15] M. O. Rabin: 'Digitalized signatures and public-key functions as intractable as factorization', Technical report MIT/LCS/TR-212, Laboratory for Computer Science, MIT, January 1979.

[16] R. Rivest, A. Shamir, and L. Adleman: 'A method for obtaining digital signatures and public-key cryptosystems', *Comm. ACM*, Vol. 21, 1978.

[17] H. C. Williams: 'A modification of the RSA public-key encryption procedure', *IEEE Transactions on Information Theory*, Vol. IT-26, No. 6, pp. 726–729, Nov. 1980.