Published in *Designs, Codes and Cryptography* **14(1):53–56, 1998.**

Reducing the elliptic curve cryptosystem of Meyer-Müller to the cryptosystem of Rabin-Williams

MARC JOYE joye@agel.ucl.ac.be
UCL Crypto Group, Dép. de Mathématique, Université de Louvain, Chemin du Cyclotron 2, B-1348 Louvain-la-Neuve, BELGIUM

JEAN-JACQUES QUISQUATER jjq@dice.ucl.ac.be
UCL Crypto Group, Dép. d'Électricité, Université de Louvain, Place du Levant 3, B-1348 Louvain-la-Neuve, BELGIUM

Abstract. At Eurocrypt '96, Meyer and Müller presented a new Rabin-type cryptosystem based on elliptic curves. In this paper, we will show that this cryptosystem may be reduced to the cryptosystem of Rabin-Williams.

Keywords: Cryptography, elliptic curves, Rabin-type cryptosystems

1. Introduction

In 1991, Koyama, Maurer, Okamoto and Vanstone [5] pointed out the existence of new one-way trapdoor functions similar to the RSA [10] on elliptic curves over a ring. At Eurocrypt '96, Meyer and Müller [7] presented another elliptic RSA-type cryptosystem with a public encryption exponent equal to 2. We will show that this cryptosystem may be reduced to the cryptosystem of Rabin-Williams [9, 11]. This has a lot of consequences. For example, Meyer and Müller claimed that 11 messages are required to mount successfully the so-called low exponent attack against their cryptosystem. However, since the system is reducible to the Rabin-Williams' one, only two messages [1] are required by using the algorithm of Coppersmith [2].

The remainder of the paper is organized as follows. Section 2 describes the cryptosystem of Meyer and Müller. In Section 3, we show how it may be reduced to the cryptosystem of Rabin-Williams. Finally, we conclude in Section 4.

2. Elliptic curve cryptosystem of Meyer-Müller

In this section, we describe succinctly the cryptosystem of Meyer and Müller. For a detailed description, we refer to the original paper (see [7]).

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 $\mathbf{Z}/n\mathbf{Z}$ given by the Weierstraß equation:

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

2.1. *Encryption procedure*

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

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

2.2. *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

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

If $\#I = 1$, then the message is given by $m = y(P_1)^3 x(P_1)^{-4} a^{-1}$.

3. Analysis

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

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

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

So, by cubing (1), and by replacing m^2 by X, we obtain the first polynomial

$$\begin{aligned} \mathcal{P}_1(X) &= \lambda^6 X^9 - (X^3 + aX + b)^3 \\ &= (a^2 - 1)X^9 - 3aX^7 - 3bX^6 - 3a^2X^5 - 6abX^4 - (a^3 + 3b^2)X^3 \\ &\quad -3a^2bX^2 - 3ab^2X - b^3. \end{aligned} \tag{2}$$

The second polynomial is constructed from the first coordinate of the point $Q = 2(m^2, \lambda m^3)$, which is given by

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

Hence, with equation (1), we have

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

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 [8, 3], a polynomial of degree 1. Thus, by solving this polynomial in X, we obtain the value of m^2.

4. Conclusion

We showed that the system of Meyer and Müller may be reduced to the cryptosystem of Rabin-Williams, because it enables to recover the value of m^2 from the Meyer-Müller's cryptogram corresponding to the message m.

Acknowledgments

We are grateful to Bernd Meyer and Volker Müller for providing us information about their cryptosystem. We are also grateful to Kenji Koyama for pointing out the existence of another Rabin-type cryptosystem based on elliptic curves [6]. We finally thank Richard Pinch for his careful reading of a preliminary version of this paper.

Appendix

Index to notations

Formal symbolism	Meaning
E	elliptic curve
$x(P)$	x-coordinate of point $P \in E$
$y(P)$	y-coordinate of point $P \in E$
$\mathrm{lsb}(a)$	least significant bit of a
$\left(\frac{a}{n}\right)$ or (a/n)	Jacobi's symbol of a modulo n
$\mathbf{Z}_n$	ring of integers modulo n

References

1. D. Bleichenbacher. Personal communication.
2. D. Coppersmith. Finding a small root of a univariate modular equation. In U. Maurer, editor, *Advances of Cryptology – Eurocrypt'96*, volume 1070 of *Lectures Notes in Computer Science*, pages 155–165. Springer-Verlag, 1996.
3. D. Coppersmith, M. Franklin, J. Patarin, and M. Reiter. Low-exponent RSA with related messages. In U. Maurer, editor, *Advances of Cryptology – Eurocrypt'96*, volume 1070 of *Lectures Notes in Computer Science*, pages 1–9. Springer-Verlag, 1996.
4. M. Joye and J.-J. Quisquater. On the cryptosystem of Chua and Ling. Technical Report CG-1997/4, UCL Crypto Group, April 1997.
5. K. Koyama, U. Maurer, T. Okamoto, and S. Vanstone. New public-key schemes based on elliptic curves over the ring $\mathbf{Z}_n$. In J. Feigenbaum, editor, *Advances of Cryptology – Crypto'91*, volume 576 of *Lectures Notes in Computer Science*, pages 252–256. Springer-Verlag, 1991.
6. H. Kuwakado and K. Koyama. A uniquely decipherable Rabin-type scheme over elliptic curves. Technical Report ISEC95-33 (in Japanese), IEICE, December 1995.
7. B. Meyer and V. Müller. A public key cryptosystem based on elliptic curves over $\mathbf{Z}/n\mathbf{Z}$ equivalent to factoring. In U. Maurer, editor, *Advances of Cryptology – Eurocrypt'96*, volume 1070 of *Lectures Notes in Computer Science*, pages 49–59. Springer-Verlag, 1996.
8. J. Patarin. Some serious protocol failures for RSA with exponent e of less than $\simeq 32$ bits. In *Proceedings of the Conference of Cryptography*, Luminy, France, September 1995.

9. M. O. Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical Report MIT/LCS/TR-212, MIT, Laboratory for Computer Science, January 1979.
10. R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
11. H. C. Williams. A modification of the RSA public-key encryption procedure. *IEEE Transactions on Information Theory*, IT-26(6):726–729, November 1980.