Published in *Electronics Letters* **33(23):1938, 1997.**

Cryptosystem of Chua and Ling

M. Joye and J.-J. Quisquater

Indexing terms: Cryptography

The authors show that the cubic curve cryptosystem proposed by Chua and Ling can easily be reduced to the cryptosystem of Rabin-Williams.

Introduction: At Eurocrypt '96, Meyer and Müller [1] presented a new Rabin-type scheme based on elliptic curves. In [2], this system was reduced to the system of Rabin-Williams [3, 4]. Using the same technique, we show that the system of Chua and Ling [5] can also be reduced.

Chua-Ling's cryptosystem: This cryptosystem is based on a singular cubic curve of the form

$$C_n(b) : y^2 \equiv x^3 + bx^2 \pmod{n}.$$

To setup the system, each user chooses two large primes p and q both congruent to 11 modulo 12. Then, he publishes the value of $n = pq$.

Suppose Alice wants to send a message m to Bob. Then she chooses $\lambda \in \mathbb{Z}/n\mathbb{Z} - \{0, \pm 1\}$ and sets $\mathbf{P} = (m^2, \lambda m^3)$. Next, she computes $c = \lambda^3 \bmod n$ and $b = (\lambda^2 - 1)m^2 \bmod n$, and sends the ciphertext consisting of c, b, $x_Q = x([2]\mathbf{P})$, $t = \left(\frac{y([2]\mathbf{P})}{n}\right)$ and $u = \mathrm{lsb}\,(y([2]\mathbf{P}))$.

To recover the plaintext m, Bob computes the unique y_Q satisfying $y_Q^2 \equiv x_Q^3 + bx_Q^2 \pmod{n}$ with Jacobi symbol t and lsb u. He sets $\mathbf{Q} = (x_Q, y_Q)$. Letting $\mathbf{Q}_p = \mathbf{Q} \bmod p$ and $\mathbf{Q}_q = \mathbf{Q} \bmod q$, he computes $\mathbf{P}_{i,p} = (x_{i,p}, y_{i,p})$ $(i = 1, 2)$ such that $[2]\mathbf{P}_{i,p} = \mathbf{Q}_p$ on $C_p(b)$ and similarly $\mathbf{P}_{i,q}$. Next, he computes $I_p = \left\{i \,:\, c^2 \equiv y_{i,p}^6 x_{i,p}^{-9} \pmod{p}\right\}$. He does the same for the prime q. Finally, he computes $m_p = y_{i,p}^3 x_{i,p}^{-4} c^{-1} \bmod p$ $(i \in I_p)$ and m_q. So, Bob obtains m using the Chinese Remainder Theorem such that $m \equiv m_p \pmod{p}$ and $m \equiv m_q \pmod{q}$.

Reduction to Rabin-Williams: Since $\mathbf{P} = (m^2, \lambda m^3) \in C_n(b)$, it follows that:

$$x_Q = x([2]\mathbf{P}) \equiv \frac{(3m^2 + 2b)^2}{4\lambda^2 m^2} - 2m^2 - b \pmod{n}, \quad (1)$$

and

$$\lambda^2 m^2 \equiv m^2 + b \pmod{n}. \quad (2)$$

From eqns. 1 and 2, we construct the polynomials $\mathcal{P}_1, \mathcal{P}_2 \in (\mathbb{Z}/n\mathbb{Z})[X]$ given by

$$\mathcal{P}_1(X) = 4(x_Q + 2X + b)(X + b) - (3X + 2b)^2,$$
$$\mathcal{P}_2(X) = c^2 X^3 - (X + b)^3.$$

Since m^2 is a root of $\mathcal{P}_1$ and $\mathcal{P}_2$, m^2 will be a root of $\mathcal{R} = \gcd(\mathcal{P}_1, \mathcal{P}_2)$. The polynomial $\mathcal{R}$ is very likely to be of degree 1 [6]. Solving this polynomial in X gives the value of m^2.

Conclusion: We have shown that we can easily recover the value of m^2 from the ciphertext corresponding to a plaintext m. Therefore, the Chua-Ling scheme is reduced to the Rabin-Williams cryptosystem.

Acknowledgements: We are grateful to S.-K. Chua and S. Ling for sending a preprint of their paper.

5 September 1997

M. Joye (*UCL Crypto Group, Département de Mathématique (AGEL), Université catholique de Louvain, Chemin du Cyclotron 2, B-1348 Louvain-la-Neuve, Belgium*)

J.-J. Quisquater (*UCL Crypto Group, Département d'Électricité (DICE), Université catholique de Louvain, Place de Levant 3, B-1348 Louvain-la-Neuve, Belgium*)

E-mail: joye@agel.ucl.ac.be / jjq@dice.ucl.ac.be

References

1 MEYER, B., and MÜLLER, V.: 'A public key cryptosystem based on elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ equivalent to factoring', in *Advances in Cryptology – EUROCRYPT '96* (1996), U. Maurer, Ed., vol. 1070 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 49–59

2 JOYE, M., and QUISQUATER, J.-J.: 'Reducing the elliptic curve cryptosystem of Meyer-Müller to the cryptosystem of Rabin-Williams', *Designs, Codes and Cryptography*, to appear

3 RABIN, M. O.: 'Digitalized signatures and public-key functions as intractable as factorization', Tech. Rep. MIT/LCS/TR-212, MIT, Laboratory for Computer Science, Jan. 1979

4 WILLIAMS, H. C.:'A modification of the RSA public-key encryption procedure', *IEEE Transactions on Information Theory*, 1980, **IT-26**, (6), 726–729

5 CHUA, S. K., and LING, S.: 'A Rabin-type scheme on $y^2 \equiv x^3 + bx^2 \bmod n$', in *Third Annual International Computing and Combinatorics Conference (COCOON '97)*, T. Jiang and D.T. Lee, Eds, vol. 1276 of *Lectures Notes in Computer Science*, Springer-Verlag, to appear

6 COPPERSMITH, D., FRANKLIN, M., PATARIN, J., and REITER, M.: 'Low exponent RSA with related messages', in *Advances in Cryptology – EUROCRYPT '96* (1996), U. Maurer, Ed., vol. 1070 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 1-9