J. Cryptology (1997) 10: 71–72

Journal of
CRYPTOLOGY

A Chosen Message Attack on Demytko's Elliptic Curve Cryptosystem

Burton S. Kaliski, Jr.
RSA Laboratories, 100 Marine Parkway, Suite 500,
Redwood City, CA 94065, U.S.A.
burt@rsa.com

Communicated by Ueli M. Maurer.

Received 7 September 1995 and revised 2 December 1995

Abstract. One of the purported advantages of the elliptic curve cryptosystem proposed by Demytko in 1993 is resistance to signature forgery under a chosen message attack. Based on a similar result by Bleichenbacher *et al.* on the LUC cryptosystem, this purported advantage is shown not to hold.

Key words. Elliptic curves, Chosen message attack, Demytko's cryptosystem, Signature forgery.

1. Introduction

In response to concerns about the multiplicative structure of the RSA cryptosystem [8], elliptic curve cryptosystems with a composite modulus have been developed by Koyama *et al.* [4] and Demytko [2].

Demytko's cryptosystem has the property that only x-coordinates of points on the curve are processed, and, as a result, it is difficult to compute the composition of two arbitrary points. This would be required in signature forgery under a straightforward adaptation of the multiplicative chosen message attack on RSA.

2. The Attack

While arbitrary composition indeed seems difficult, a well-known construction relating x-coordinates (see, for instance, [7]) does yield a successful attack:

$$x_{i+j} = \frac{4b + 2(a + x_i x_j)(x_i + x_j)}{(x_i - x_j)^2} - x_{i-j}. \tag{1}$$

The construction is also implicit in the derivation of Demytko's equation (34).

Let x_1 be a message whose signature is to be forged, and let u and v be chosen such that $u + v = 1$. Define $i = du$ and $j = dv$, where d is the private exponent for signing the message x_1 and its elliptic curve multiples. Then x_i is the signature of x_u; x_j is the signature of x_v; x_{i-j} is the signature of x_{u-v}; and $x_{i+j} = x_d$ is the signature of $x_{u+v} = x_1$.

A chosen message attack follows directly: given x_1 the opponent obtains the signatures of its multiples x_u, x_v, and x_{u-v}, and computes the signature of x_1 by (1).

The attack is basically just an adaptation of Bleichenbacher *et al.*'s attack on the LUC cryptosystem [1]; their variations of the attack apply here as well.

3. Conclusions

The Demytko cryptosystem, like RSA and the Koyama *et al.* cryptosystem [4], is vulnerable to signature forgery under a chosen message attack. The chosen message attack can also be viewed as a chosen ciphertext attack. It is worth noting, however, that these attacks are not as general as so-called homomorphism attacks on RSA where the opponent manipulates arbitrary combinations of messages.

Another purported advantage of elliptic curve cryptosystems based on a composite modulus—resistance to "low exponent" attacks—has also been recently shown not to hold [5]. Thus, the present benefits of elliptic curve cryptosystems based on a composite modulus do not seem significiant.

Elliptic curve cryptosystems based on the discrete logarithm problem [6], [3] are not affected by any of the attacks just described, and their benefits, especially the shorter key size, remain significant. Further research will establish more accurately the appropriate level of confidence in those systems.

Acknowledgments

I am grateful to Matt Robshaw for reviewing this note, and to the authors of reference [1] for providing early drafts of their work. The anonymous referees and the editors were very helpful in encouraging me to publish this result as a short note. I am also thankful to God (Col. 3:17).

References

[1] D. Bleichenbacher, W. Bosma, and A. K. Lenstra, Some remarks on Lucas-based cryptosystems, in D. Coppersmith, editor, *Advances in Cryptology—Crypto* '95, Springer-Verlag, New York, 1995, pp. 386–396.

[2] N. Demytko, A new elliptic curve based analogue of RSA, in T. Helleseth, editor, *Advances in Cryptology—Eurocrypt* '93, Springer-Verlag, New York, 1994, pp. 40–49.

[3] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, vol. 48 (1987), pp. 203–209.

[4] K. Koyama, U. M. Maurer, T. Okamoto, and S. A. Vanstone, New public-key schemes based on elliptic curves over the ring $\mathbf{Z}_n$, in J. Feigenbaum, editor, *Advances in Cryptology—Crypto* '91, Springer-Verlag, New York, 1994, pp. 252–266.

[5] K. Kurosawa, K. Okada, and S. Tsujii, Low exponent attack against elliptic curve RSA, in J. Pieprzyk and R. Safavi-Naini, editors, *Advances in Cryptology—Asiacrypt* '94, Springer-Verlag, New York, 1995, pp. 376–383.

[6] V. S. Miller, Use of elliptic curves in cryptography, in H. C. Williams, editor, *Advances in Cryptology—Crypto* '85, Springer-Verlag, New York, 1986, pp. 417–426.

[7] P. L. Montgomery, Speeding the Pollard and elliptic curve methods of factorization, *Mathematics of Computation*, vol. 48, no. 177 (1987), pp. 243–264.

[8] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, vol. 21, no. 2 (1978), pp. 120–126.