Specialized Integer Factorization

Don Coppersmith

IBM Research
T.J. Watson Research Center
Yorktown Heights, NY 10598, USA

Abstract. Vanstone and Zuccherato [3] propose a cryptographic system based on an elliptic curve modulo a composite number. We show that the composite numbers so constructed are easily factored, rendering the system insecure.

1 Introduction

Vanstone and Zuccherato [3] propose a cryptographic system based on an elliptic curve modulo a composite number $N = pq$, whose factorization must remain secret. The primes p and q are constructed by a specific process, in order to make it easy to determine the size of the elliptic curve, and to enforce the property that this size be a "smooth" number (its prime factors should not exceed 10^{16}).

The specific construction, however, renders N easy to factor.

We give a straightforward method of factoring the sorts of integers that arise in the system. The effect is to give yet another warning to be careful with every stage of the production of RSA keys.

This note is organized as follows. In Section 2 we describe Vanstone and Zuccherato's scheme. Section 3 gives our method for factoring the integers that arise in this way. In Section 4 we speculate about possible extensions.

2 Basic Scheme

Vanstone and Zuccherato [3] propose a cryptographic system based on an elliptic curve modulo a composite number $N = pq$, whose factorization must remain secret. In section VII.C of [3], it is recommended to select 75-digit primes p and q with certain properties. Two methods are given for constructing such primes. The first constructs a 37- or 38-digit integer a (satisfying certain conditions which are irrelevant to the present discussion) and defines

$$p = a^2 + 4.$$

The second defines

$$p = a^2 - 3a + 9.$$

More generally, suppose we are given small integer coefficients A, B, C and told that, for some unknown large integer a, the prime p satisfies

$$p = Aa^2 + Ba + C.$$

Similarly we are told that q is of the form

$$q = Db^2 + Eb + F.$$

So A, B, C, D, E, F are small known integers, while p, q, a, b are large unknown integers. We are also given the product

$$N = pq.$$

(In practice, we may not actually know $A, B, \ldots, F$, but instead have to exhaustively search over possibilities.)

3 Factoring These Numbers

Let us begin by completing the square:

$$\begin{aligned} 4Ap &= 4A^2a^2 + 4ABa + 4AC \\ &= (2Aa + B)^2 - (B^2 - 4AC) \\ &= x^2 - \delta \end{aligned}$$

where $x = 2Aa + B$, and $\delta = B^2 - 4AC$ is the discriminant; δ may be positive or negative. Similarly

$$\begin{aligned} 4Dq &= y^2 - \epsilon \\ y &= 2Db + E \\ \epsilon &= E^2 - 4DF \end{aligned}$$

and

$$16ADN = (4Ap)(4Dq) = x^2y^2 - \delta y^2 - \epsilon x^2 + \delta\epsilon.$$

In this equation we know $A, D, N, \delta, \epsilon$, but not p, q, x, y.

The point is that $\sqrt{16ADN}$ gives us a good approximation to the quantity xy, and from that we can compute the rest of the factorization. That is,

$$\sqrt{16ADN} = xy - \frac{\delta y}{2x} - \frac{\epsilon x}{2y} + \text{smaller terms}$$

$$xy = \left\lfloor \sqrt{16ADN} \right\rfloor + O(\delta y/x) + O(\epsilon x/y)$$

Assume that Ap and Dq are roughly the same size, say

$$10^{-10} < \frac{Ap}{Dq} < 10^{10},$$

so that

$$\frac{x}{y} = \sqrt{\frac{Ap}{Dq}} + O(1) < 10^5,$$

and that δ and ϵ are reasonably small,

$$|\delta|,\ |\epsilon| < 10^5.$$

Then our uncertainty in the exact value of xy is bounded by about 10^{10}, and it will be feasible to exhaustively search in the neighborhood of $\lfloor\sqrt{N}\rfloor$ to find the exact value.

Given our guessed value of xy, we continue. Define τ by

$$\tau = (xy)^2 - 16ADN + \delta\epsilon = \delta y^2 + \epsilon x^2$$
$$\delta y^2 - \epsilon x^2 = \pm\sqrt{\tau^2 - 4\delta\epsilon(xy)^2}$$
$$y^2 = \frac{\tau \pm \sqrt{\tau^2 - 4\delta\epsilon(xy)^2}}{2\delta}$$

from which we can compute

$$q = \frac{y^2 - \epsilon}{4D}$$

and complete the factorization.

Remark: We can use a sieve to accomplish the task of trying various values of xy and seeing which ones yield integer values for y^2.

Remark: If B is even, the factor of 4 can be dispensed with. So in the case

$$N = (a^2 + 4)(b^2 + 4)$$

we can simply use $x = a$, $y = b$, and

$$xy = \left\lfloor\sqrt{N}\right\rfloor + O\left(\sqrt{\frac{p}{q}}\right).$$

4 Speculations

The present approach is not very robust. It does not work if p and q are of vastly different sizes:

$$p \ll q. \tag{1}$$

It does not work if N is the product of three specially constructed primes:

$$N = pqr = (a^2 + 4)(b^2 + 4)(c^2 + 4). \tag{2}$$

It does not work if N is the product of two primes, only one of which is known to be given by a quadratic formula:

$$N = pq = (a^2 + 4)(q). \tag{3}$$

These failures represent possible areas of further research.

This last problem (3) is reminiscent of the situation treated by the present author in [1]; see also [2]. That is, [1] considered the case $N = pq$ where we know half the bits of p (either the $(\log_2 p)/2 = (\log_2 N)/4$ most significant bits, or the $(\log_2 p)/2$ least significant bits, of p), and showed that we could discover the factorization of N using lattice basis reduction methods. The unknown part of p accounted for $(\log_2 N)/4$ bits.

In the present case (3), our knowledge of p is of a different sort: we know that p is of the form $a^2 + 4$, and again we have $\log_2 a = (\log_2 N)/4$ unknown bits. This is only a weak analogy; to our knowledge, the methods of [1] do not apply to the present problem. But they do encourage us to search for a factoring algorithm that could make use of the sort of information given in (3).

References

1. D. Coppersmith, "Finding a small root of a bivariate integer equation; factoring with high bits known," *Advances in Cryptology - EUROCRYPT '96*, Ueli Maurer (Ed.), Springer LNCS Volume 1070, 1996, pages 178-189.
2. D. Coppersmith, "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities," *Journal of Cryptology*, Volume 10 Number 4, Autumn 1997, pages 233-260.·
3. S. A. Vanstone and R. J. Zuccherato, "Elliptic curve cryptosystems using curves of smooth order over the ring $\mathbf{Z}_n$," *IEEE Trans. Inform. Theory*, Volume IT-43, 1997, pages 1231-1237.