A SECURITY WEAKNESS IN COMPOSITE-ORDER PAIRING-BASED PROTOCOLS WITH IMBEDDING DEGREE $k > 2$

NEAL KOBLITZ

Abstract. In this note we describe a security weakness in pairing-based protocols when the group order is composite and the imbedding degree k is greater than 2.

In pairing-based protocols, as in elliptic curve cryptography more generally, one usually works in a prime-order subgroup of an elliptic curve $E(\mathbb{F}_q)$. However, starting in 2005 with work of Boneh, Goh, and Nissim [1], composite-order groups have been used in pairing-based protocols to achieve certain cryptographic objectives in such areas as traitor tracing [3] and group signatures [4, 5].

Let $N = \prod_{i=1}^{r} p_i^{\alpha_i}$ be an odd composite number whose factorization needs to be kept secret. Suppose that N is the order of the group $\mathbb{G}$ in a pairing-based protocol with imbedding degree $k > 2$, and let E be the elliptic curve over $\mathbb{F}_q$ that is being used to implement the protocol. With no loss of generality we suppose that g.c.d.$(q, N) = 1$. It is well-known (see, for example, Remark 4.5 of [2]) that one needs q to have exact multiplicative order k not only modulo N, but also modulo $p_i^{\alpha_i}$ for each i in order to avoid a simple attack that factors N; in particular, this means that $p_i \equiv 1 \pmod{k}$ for $i = 1, 2, \ldots, r$.

Theorem 1. *In the above setting, an attacker who observes two independent implementations (with the same N and k but different E and q) has probability at least $1 - \phi(k)^{1-r} \geq 1 - 2^{1-r}$ of factoring N, where $r \geq 2$ is the number of distinct prime factors of N.*

Proof. Let $\mathbb{F}_{q_1}$ and $\mathbb{F}_{q_2}$ be the finite fields in the two implementations. Because each q_j must have exact order k modulo $p_i^{\alpha_i}$ for each $i = 1, \ldots, r$, it follows from the Chinese Remainder Theorem that, given q_1, there are $\phi(k)^r$ possible values of q_2 mod N. Of the $\phi(k)^r$ possible values of q_2 mod N, there are $\phi(k)$ that are in the multiplicative group mod N generated by q_1. Suppose that q_2 mod N is *not* in the group generated by q_1. Then there is some value of j, $1 \leq j < k$ with g.c.d.$(j, k) = 1$, such that q_2 agrees with q_1^j mod $p_1^{\alpha_1}$ (because q_1 and q_2 generate the same group mod $p_1^{\alpha_1}$) but

Date: April 22, 2010.

Key words and phrases. public key cryptography, pairing-based protocol, imbedding degree.

not mod N. Thus, one can factor N by computing g.c.d.$(N, q_2 - q_1^j)$ for $1 \le j < k$ for which g.c.d.$(j, k) = 1$. Hence, the probability of factoring N is at least $(\phi(k)^r - \phi(k))/\phi(k)^r = 1 - \phi(k)^{1-r}$, as claimed.

Example 1. *Suppose that $N = p_1p_2$ is an RSA-modulus and $k = 3$. Then, given q_1, there are 4 possibilities for q_2 mod N. In two cases q_1 and q_2 are either equal or the squares of one another mod N. In the other two cases g.c.d.$(N, q_1 - q_2)$ is either p_1 or p_2.*

Remark 1. *Since k is always quite small, the number of g.c.d.'s the attacker needs to compute is also small.*

Remark 2. *The same argument shows that, more generally, if the two implementations have different imbedding degrees k_1 and k_2, and if $k_0 =$ g.c.d.$(k_1, k_2) > 2$, then the attacker has probability at least $1 - \phi(k_0)^{1-r}$ of factoring N.*

Remark 3. *In pairing-based protocols with prime-order group $\mathbb{G}$ it would be very undesirable to have to restrict to imbedding degree $k = 1$ or 2. The reason is that one usually wants to choose k so that the running time for squareroot discrete log algorithms in $\mathbb{G}$ is comparable to the running time for the number field or function field sieve in $\mathbb{F}_{q^k}^{\times}$, and this certainly means that $k > 2$. However, if $\mathbb{G}$ has composite order N and one needs to protect the factorization of N, then one wants the running time for the number field sieve for factoring N to be comparable to the running time for the number field or function field sieve in $\mathbb{F}_{q^k}^{\times}$. Since N has roughly the same order as q, it is thus reasonable to choose $k = 1$ (or $k = 2$).*

In conclusion, it is prudent to use imbedding degree 1 or 2 when a pairing-based protocol needs to hide the factorization of a composite group order.

References

[1] D. Boneh, E.-J. Goh, and K. Nissim, Evaluating 2-DNF formulas on ciphertexts, in J. Kilian, ed., *Proc. Second Theory of Cryptography Conference, TCC 2005*, LNCS 3378, Springer-Verlag, 2005, 325-341.

[2] D. Boneh, K. Rubin, and A. Silverberg, Finding composite order ordinary elliptic curves using the Cocks-Pinch method, ro appear in *J. Number Theory*, available at http://eprint.iacr.org/2009/533.pdf

[3] D. Boneh, A. Sahai, and B. Waters, Full collusion resistant traitor tracing with short ciphertexts and private keys, in S. Vaudenay, ed., *Advances in Cryptology – Eurocrypt 2006*, LNCS 4004, Springer-Verlag, 2006, 573-592.

[4] X. Boyen and B. Waters, Compact group signatures without random oracles, in S. Vaudenay, ed., *Advances in Cryptology – Eurocrypt 2006*, LNCS 4004, Springer-Verlag, 2006, 427-444.

[5] X. Boyen and B. Waters, Full-domain subgroup hiding and constant-size group signatures, in T. Okamoto and X. Wang, eds., *Public Key Cryptography, PKC 2007*, LNCS 4450, Springer-Verlag, 2007, 1-15.

Department of Mathematics, Box 354350, University of Washington, Seattle, WA 98195 U.S.A.

E-mail address: koblitz@math.washington.edu