Updated standards for validating elliptic curves.

Laura Hitt

Department of Mathematics
The University of Texas at Austin
Austin, TX 78712.
lhitt@math.utexas.edu

Abstract. We give a concise statement of a test for security of elliptic curves that should be inserted into the standards for elliptic curve cryptography. In particular, current validation for parameters related to the MOV condition that appears in the latest draft of the IEEE P1363 standard [3, Section A.12.1, Section A.16.8] should be replaced with our subfield-adjusted MOV condition. Similarly, the Standards for Efficient Cryptography Group's document SEC 1 [4] should make adjustments accordingly.

Keywords: elliptic curve cryptography, MOV condition, discrete logarithm, security.

1 Introduction

The security of an elliptic curve cryptosystem depends on the difficulty of solving the discrete logarithm problem (DLP) on the curve. There are standard specifications that elliptic curves used in cryptography are to meet in order to be accepted as secure. We are concerned with a particular test to be checked, known as the *MOV condition*, when validating parameters for elliptic curves over binary fields.

According to IEEE P1363 [3], the MOV condition "ensures that an elliptic curve is not vulnerable to the reduction attack of Menezes, Okamoto and Vanstone [2]." The MOV attack uses pairings to transport the DLP from the curve where it may be computationally difficult to solve, to a finite field where there are more efficient methods for solving the discrete logarithm.

We provide the conditions on the size of the finite field containing the MOV embedding required in order for the DLP in this field to be of comparable difficulty to the elliptic curve discrete logarithm over the field of definition. One may refer to [1] for mathematical justification of these parameters. The main idea is that if $q = p^m$ for a prime p and positive integer m, then the minimal embedding field is an extension of $\mathbb{F}_p$, not necessarily of $\mathbb{F}_q$, and hence the DLP may be embedded into a field of significantly smaller size than previously stated in the standards.

2 Suggested Text Modifications

We directly follow [3, Section A.12.1], with a few proposed corrections, emphasized by the boldfaced text.

> Before performing the algorithm to check the **subfield-adjusted** MOV condition, it is necessary to select an *MOV threshold*. This is a positive integer B such that taking discrete logarithms over $GF(q^B)$ is judged to be at least as difficult as taking elliptic discrete logarithms over $GF(q)$.

IEEE P1363 provides a suitable formula and table for determining the appropriate integer B. Next we offer the following correction.

> Once an appropriate B has been selected, the following algorithm checks the **subfield-adjusted** MOV condition for the choice of field size $\mathbf{q} = \mathbf{p^m}$ and base point order r by verifying that $\mathbf{p^i}$ is not congruent to 1 modulo r for any $i \leq \mathbf{mB}$.
>
> Input: an MOV threshold B, a prime-power q, and a prime r.
>
> Output: the message "True" if the **subfield-adjusted** MOV condition is satisfied for an elliptic curve over $GF(q)$ with a base point of order r; the message "False" otherwise.

```
1. Determine the prime p dividing q.
2. Set $t \leftarrow 1$.
3. For $i$ from 1 to $\mathbf{B} \log_{\mathbf{p}} \mathbf{q}$ do
   (a) Set $t \leftarrow t\mathbf{p} \bmod r$.
   (b) If $t = 1$ then output "False" and stop.
4. Output "True."
```

If the output of the above algorithm is "false," then the curve should be excluded, as it is vulnerable to the MOV reduction attack.

We recommend that other standards besides IEEE P1363 also make corrections with the sub-field adjusted MOV condition in consideration. The following are suggested corrections for SEC 1 [4, Section 3.1.2.1, bullet points under 3].

> – $b \neq 0$ in $\mathbb{F}_{2^m}$.
> – $\#E(\mathbb{F}_{2^m}) \neq 2^m$.
> – $\mathbf{2^B \not\equiv 1 \pmod{n}}$ **for any** $\mathbf{1 \leq B < 20m}$.
> – $h \leq 4$.

The suggested corrections for [4, Section 3.1.2.2.1, Actions] are as follows.

> 9. Check that $\mathbf{2^{B}} \not\equiv \mathbf{1} \pmod{\mathbf{n}}$ **for any** $\mathbf{1 \leq B < 20m}$**,** and that $nh \neq 2^m$.

The commentary in Appendix B.1 of [4, Page 60, line -8] should be modified, such as suggested below.

> These attacks efficiently reduce the ECDLP on these curves to the traditional discrete logarithm problem in a small degree extension of $\mathbb{F}_{\mathbf{p}}$.

3 Security Indicator

Let a be a positive integer and r be a prime, $r \nmid a$. The smallest positive integer x such that $a^x \equiv 1 \bmod r$ is called the *order of a modulo r*, and will be denoted by $\mathrm{ord}_r a$.

Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$, where $q = p^m$. If r divides the order of $E(\mathbb{F}_q)$, then pairings can embed a subgroup of $E(\mathbb{F}_q)$ of order r into the finite field $\mathbb{F}_{q^{\mathrm{ord}_r p/m}}$, as shown in [1]. We call this rational exponent of q the *security indicator* k'.

$$\boxed{k' = \tfrac{\mathrm{ord}_r p}{m}.}$$

One actually wants discrete logarithms in the minimal embedding field $\mathbb{F}_{q^{k'}}$ to be of approximate difficulty as elliptic curve discrete logarithms over $\mathbb{F}_q$. For example, if we have a (sub)group of order r, and r is a 160-bit prime, then one would like

$$\boxed{q^{k'} > 2^{1024}.}$$

This is equivalent to requiring $p^{\mathrm{ord}_r p} > 2^{1024}$.

Acknowledgments

Thanks to D. J. Bernstein and T. Lange for pointing out the need for revision in current elliptic-curve standards in light of [1].

References

1. L. Hitt. On the minimal embedding field. In *Pairing-Based Cryptography – Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, pages 294–301. Springer-Verlag, Berlin, 2007.

2. A. J. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions Information Theory*, 39(5):1639–1646, 1993.
3. IEEE P1363. *Standard Specifications for Public Key Cryptography.* IEEE, 2000.
4. SEC 1. *Elliptic Curve Cryptography.* Standards for Efficient Cryptography Group, 2000. Working Draft. Availabale from: http://www.secg.org/.