A Second Pre-image Attack Against Elliptic Curve Only Hash (ECOH)

Michael A. Halcrow
mhalcrow@microsoft.com

Niels Ferguson
niels@microsoft.com

April 6, 2009

Abstract

We present a second pre-image attack on ECOH. Our attack requires 2^{143} time for ECOH-224 and ECOH-256, 2^{206} time for ECOH-384, and 2^{287} time for ECOH-512. The attack sets the checksum block to a fixed value and uses a collision search on the elliptic curve points.

1 An outline of ECOH

We first give a description of the essential elements of ECOH. We restrict ourselves to messages that are an integral number of blocks, which is what we use in our attack. For full details, please refer to the ECOH specifications [1].

ECOH divides the message into blocks, maps each block to an elliptic curve point, and adds these points together with two more points. One additional point contains the padding and depends only on the message length. The second additional point depends on the message length and the exclusive-or of all message blocks.

More formally, given n message blocks $M_0, \ldots, M_{n-1}$ we have

$$\begin{aligned} P_i &:= P(M_i, i) \qquad \text{for } i = 0, \ldots, n-1 \\ X_1 &:= P'(n) \\ X_2 &:= P''(\bigoplus_{i=0}^{n-1} M_i, n) \\ Q &:= \sum_{i=0}^{n-1} P_i + X_1 + X_2 \\ R &:= f(Q) \end{aligned}$$

Here, P is a function that maps a message block and an integer to an elliptic curve point. P' computes the padding point which depends only on the length of M. P'' computes the checksum point X_2 which depends on the exclusive-or of all the message blocks, and on the length of M. Finally, the $n+2$ elliptic curve points are added, and the result Q is passed through an output transformation function f to get the hash result R.

2 General form of the attack

For a second pre-image attack we are given a message M and try to find an M' that hashes to the same message. We will find an M' that results in the same value for Q that occurred in the hash computation of M. This lets us ignore the output transformation.

For this attack, we fix the message length to six blocks: $M' = (M_0,\ M_1,\ M_2,\ M_3,\ M_4,\ M_5)$. We choose K different random values for (M_0, M_1) and define M_2 by $M_2 := M_0 \oplus M_1$. We compute the K corresponding elliptic curve points $P(M_0, 0) + P(M_1, 1) + P(M_2, 2)$ and store them in a list. We then choose K different random values for (M_3, M_4), define $M_5 := M_3 \oplus M_4$, compute $Q - X_1 - X_2 - P(M_3, 3) - P(M_4, 4) - P(M_5, 5)$, and store them in a second list. Note that the target Q is known. X_1 only depends on the length of the message which we have fixed. X_2 depends on the length and the xor of all message blocks, but we choose the message blocks such that the xor is always zero. Thus, X_2 is fixed for all our tries.

If K is larger than the square root of the number of points on the elliptic curve then we expect one collision between the two lists. This gives us a message (M_0, M_1, M_2,

M_3, M_4, M_5) with

$$Q - X_1 - X_2 - \sum_{i=3}^{5} P(M_i, i) = \sum_{i=0}^{2} P(M_i, i)$$

and thus

$$Q = \sum_{i=0}^{5} P(M_i, i) + X_1 + X_2$$

which shows that this message leads to the target value Q and thus is a second pre-image.

The workload of this attack is $2K$ partial hash computations. As this is a direct collision search, well-known techniques can be used to convert this algorithm into one that uses only a limited amount of memory.

3 Actual parameters

ECOH-224 and ECOH-256 use the elliptic curve B-283 with approximately 2^{283} points on the curve. We choose $K = 2^{142}$ and get an attack with complexity 2^{143}.

ECOH-384 uses the elliptic curve B-409 with approximately 2^{409} points on the curve. Choosing $K = 2^{205}$ gives an attack with complexity 2^{206}.

ECOH-512 uses the elliptic curve B-571 with approximately 2^{571} points on the curve. Choosing $K = 2^{286}$ gives an attack with complexity 2^{287}.

4 Discussion

The ECOH authors discuss a possible second pre-image birthday attack in Section 6.2.2 of the ECOH paper. They claim that Wagner's Generalized Birthday Attack does not work because of the checksum block. Our method of choosing the message pieces effectively fixes the checksum block to zero, thereby circumventing this countermeasure.

5 Acknowledgements

We would like to thank Daniel Brown, the principal submitter of ECOH, for his helpful comments and suggestions.

References

[1] Daniel R. L. Brown, Adrian Antipa, Matt Campagna, Rene Struik, "ECOH: the Elliptic Curve Only Hash" `http://ehash.iaik.tugraz.at/uploads/a/a5/Ecoh.pdf`, Submission to NIST, 2008