A Timing Attack on Hyperelliptic Curve Cryptosystems

Asiacrypt 2003 rump session on Dec. 2nd, 2003

M. Katagi, I. Kitamura, T. Akishita, and T. Takagi(*)
Sony Corporation
(*) Technische Universitaet Darmstadt
Introduction

- Optimization of addition algorithm for HECC
  - Active area!
    - Harley Algorithm (Explicit Formulae)
- Side Channel Attacks (SCA) for HECC
  - Important, but not enough studied...
Experimental Results

- Timings of scalar multiplication
  - Detect the timing difference on PC!
    - Intel Xeon Processor 2.80GHz
    - Linux 2.4 (RedHat)
    - gcc3.3 and NTL5.3 with GMP4.0

<table>
<thead>
<tr>
<th>Addition Formulae</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Harley</td>
<td>15.12ms</td>
</tr>
<tr>
<td>Harley with one exceptional procedure</td>
<td>15.08ms</td>
</tr>
</tbody>
</table>

- Success to reveal 160bit key
  - about 10 hours on our environment
Timing Attack: Guessing 1 bit (genus two)

Addition Chain of $dD$, $d=(101\ldots)$

Input: randomly chosen divisor $D$

- $D \xrightarrow{\text{DBL}} 2D \xrightarrow{\text{ADD}} 3D$
- $3D \xrightarrow{\text{DBL}} 4D \xrightarrow{\text{ADD}} 5D$

Weight 2

Addition Chain of $dD$, $d=(101\ldots)$ with One Exceptional Procedure

Input: $D = 4^{-1} \mod (\#J_c)D_0$, $D_0$: weight 1 divisor, $\#J_c$: order of Jacobian

- $D \xrightarrow{\text{DBL}} 2D \xrightarrow{\text{ADD}} 3D$ (fast!)
- $3D \xrightarrow{\text{Ex DBL}} 4D \xrightarrow{\text{Ex ADD}} 5D$

Weight 1
Summary

- We demonstrated that scalar multiplication of HECC was vulnerable to chosen ciphertext attack
  - Exceptional procedure using low weight divisors
  - Easily attacked on regular PC

- We should investigate the security of HECC
  - This attack has not appeared in the standard ECC.

- Cryptology ePrint Archive