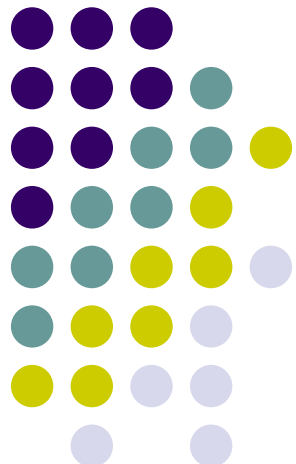
A Timing Attack on Hyperelliptic Curve Cryptosystems

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

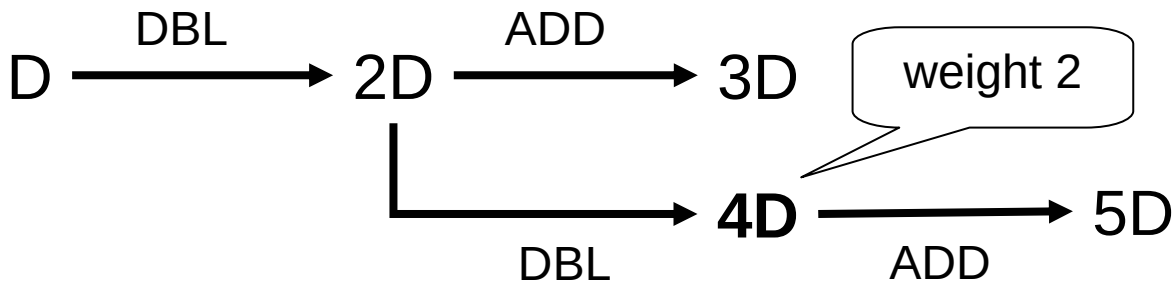
Addition Formulae	Timing
Harley	15.12ms
Harley with one exceptional procedure	15.08ms

- Success to reveal 160bit key
  - about 10 hours on our environment

Timing Attack : Guessing 1bit (genus two)

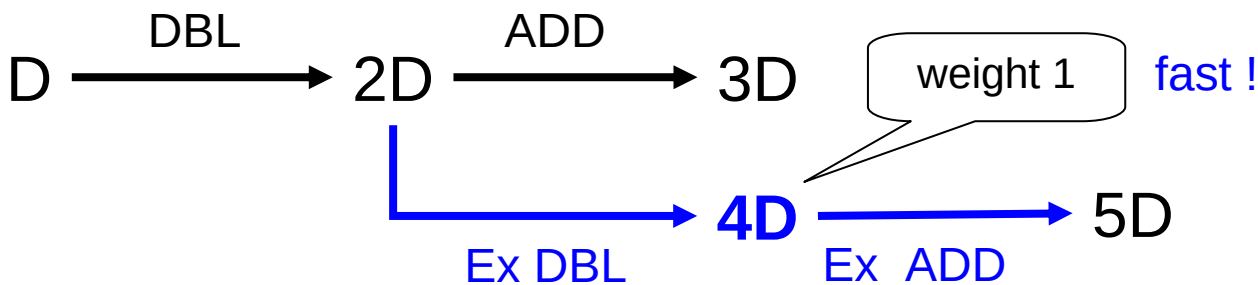
Addition Chain of dD, d=(101.....)

Input: randomly chosen divisor D



Addition Chain of dD, d=(101.....) with One Exceptional Procedure

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



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
  - http://eprint.iacr.org/2003/203/