A New Type of Timing Attack: Application to GPS

Julien Cathalo*, François Koeune, Jean-Jacques Quisquater

UCL Crypto Group
Belgium

© UCL Crypto Group / CHES 2009

Main Result

- « Hamming Weight Cryptanalysis » of GPS

Hamming weight of several
(ephemeral) secret exponents

Long term secret = Private key

Outline

- Introduction
- GPS Identification Scheme
- Hamming Weight Cryptanalysis
- Timing Attack on GPS
- Countermeasures
- Conclusion

Introduction

- GPS: Identification Scheme, [Girault 91]
- Modification of [Schnorr 89]
- Designed for smart cards
- Efficient for the prover: $z = y + cx$
- Security proof [Poupard, Stern 98]: Statistical Zero-Knowledge
- Selected by Nessie in 2003

Outline

- Introduction
- GPS Identification Scheme
- Hamming Weight Cryptanalysis
- Timing Attack on GPS
- Countermeasures
- Conclusion

Basic GPS Parameters

- A modulus $n = pq$
- Integers A, B, S such that $A >> BS$
- An integer g ($g = 2$)
- Prover's private key: $x \in [0, S[$
- Prover's public key: $X = g^{-x} \bmod n$
- $E = A + (B-1)(S-1)$

Now $|A| = 240, |B| = 16, |S| = 160$

A Round of GPS

$X = g^{-x} \bmod n$

Commitment

$y \in_{rand} [0, A[$

$Y = g^{y} \bmod n$

Y

$c \in_{rand} [0, B[$

c

$\overset{?}{c} \in [0, B[$

$z = y + cx$

z

$\overset{?}{z} \in [0, E[$

$g^{z} X^{c} \overset{?}{\equiv} Y \pmod{n}$

$$g^{z} X^{c} \equiv g^{y+cx} (g^{-x})^{c} \equiv g^{y} \equiv Y \pmod{n}$$

The Commitment Step

- The commitment pairs $(y, Y = g^{y} \bmod n)$ can be computed:
  - Outside the card
    - Efficient
    - Limited number of identifications
  - Inside the card before the identification
    - Requires power
  - Inside the card during the identification
    - Requires a crypto-processor

Off-line variant

On-line variant

Outline

- Introduction
- GPS Identification Scheme
- Hamming Weight Cryptanalysis
- Timing Attack on GPS
- Countermeasures
- Conclusion

HWC Principle

- Input: a list $(Hw(y^{(i)}), z^{(i)} = y^{(i)} + x)_{i=1,\ldots,k}$
  where $y^{(i)} \in_{rand} [0, A[$
- Output: a candidate value $\tilde{x}$ that is close to the key (i.e. such that $Hd(\tilde{x}, x)$ is small)

Information on the lsb

- We have $z = y + x$:

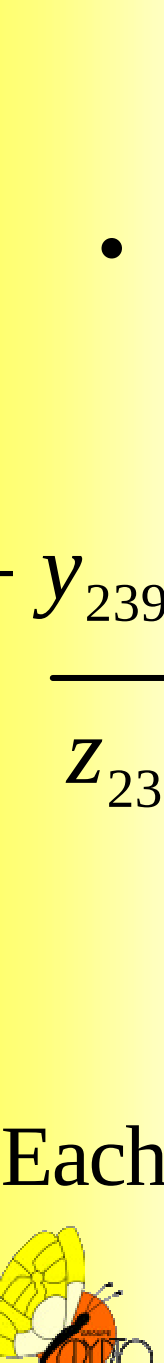
$$x_{159} \ominus x_1 x_0 \rightarrow P(x_0 = 1)$$

$$- \; y_{239} \ominus y_{160} y_{159} \ominus y_1 y_0 \rightarrow P(y_0 = 1) = \frac{Hw(y^{(i)})}{240}$$

$$z_{239} \ominus z_{160} z_{159} \ominus z_1 z_0 \rightarrow \text{known}$$

$$y_0^{(i)} \oplus x_0^{(i)} = z_0^{(i)}$$

Each $w^{(i)}, z^{(i)}$ couple leads to an estimation of $P(x_0 = 1)$



Combining these estimations

- M_0 = mean of the k estimations of $P(x_0 = 1)$
- `If` $M_0 > \frac{1}{2}$ `then` $\tilde{x}_0 = 1$
  `else` $\tilde{x}_0 = 0$
- Assuming that $\tilde{x}_0 = x_0$, compute $(y_0^{(i)})_{i=1,\ldots,k}$
- Update $(Hw(y^{(i)}))_{i=1,\ldots,k}$
- Guess the carries $carry_1^{(i)}{}_{i=1,\ldots k}$
- Now ready to guess x_1

$$y_1^{(i)} \oplus x_1^{(i)} \oplus carry_1^{(i)} = z_1^{(i)}$$

Guessing the next bit

- We have $z = y + x$:

$$
\begin{array}{r}
x_{159} \ominus x_1 x_0 \\
+\ y_{239} \ominus y_{160} y_{159} \ominus y_1 y_0 \\
\hline
z_{239} \ominus z_{160} z_{159} \ominus z_1 z_0
\end{array}
$$

$$y_1^{(i)} \oplus x_1^{(i)} y_0^{(i)} \oplus carry_0^{(i)} y_1^{(i)} = z_0^{(i)} z_1^{(i)}$$

Outline

- Introduction
- GPS Identification Scheme
- Hamming Weight Cryptanalysis
- Timing Attack on GPS
- Countermeasures
- Conclusion

Conditions of success

- For HWC to work, the attacker must:
  - Impersonate a honest verifier
  - Get Hamming weights
- A natural way to do it: Timing Attack
  - Commitment computed *on-line*
  - Square and Multiply algorithm (or similar)

Attack Summary

Impersonate the verifier

Collect timings and answers

Step 1

$(t^{(i)}, z^{(i)})_{i=1,\ldots,k}$

Deduce Hw

$(Hw(y^{(i)}), z^{(i)})_{i=1,\ldots,k}$

Hamming weight Cryptanalysis

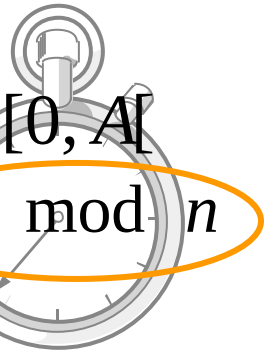
$\tilde{x}$ such that $Hd(\tilde{x}, x)$ is small

Exhaustive search

x private key !

Step 1

$X = g^{-x} \bmod n$



$y \in_{rand} [0, A[$

$Y = g^{y} \bmod n$

t

Y

$c = 1$ sent by

c

?

$c \in [0, B[$

$z = y + x$

z

$$\begin{cases} t^{(1)}, z^{(1)} \\ t^{(2)}, z^{(2)} \\ \vdots \\ t^{(k)}, z^{(k)} \end{cases}$$

Attack Summary

Impersonate the verifier

Collect timings and answers

$(t^{(i)}, z^{(i)})_{i=1,\ldots,k}$

$(Hw(y^{(i)}), z^{(i)})_{i=1,\ldots,k}$

Deduce Hw

Step 2

Hamming weight Cryptanalysis

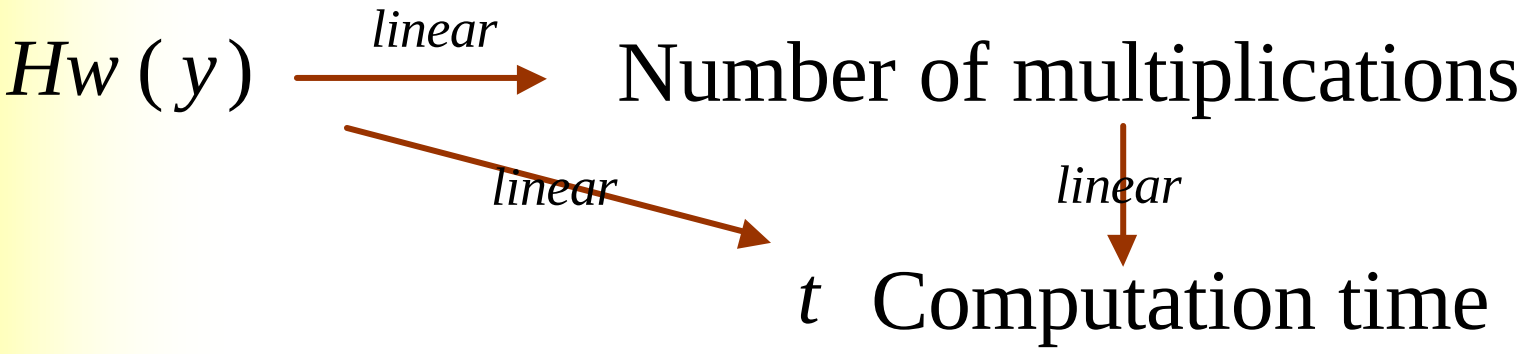
$\tilde{x}$ such that $Hd(\tilde{x}, x)$ is small

Exhaustive search

x private key !

Step 2

- When $g^y \bmod n$ is computed with Square and Multiply then



- With a linear regression

$$t^{(1)}, \text{😐}, t^{(k)} \longrightarrow Hw^{(1)}, \text{😐}, Hw^{(k)}$$

- Works whether CRT is used or not

Attack Summary

Impersonate the verifier

Collect timings and answers

$(t^{(i)}, z^{(i)})_{i=1,\ldots,k}$

Deduce Hw

$(Hw(y^{(i)}), z^{(i)})_{i=1,\ldots,k}$

Hamming weight Cryptanalysis

Step 3

$\tilde{x}$ such that $Hd(\tilde{x}, x)$ is small

Exhaustive search

x private key !

Attack Summary

Impersonate the verifier

Collect timings and answers

$$(t^{(i)}, z^{(i)})_{i=1,\ldots,k}$$

Deduce Hw

$$(Hw(y^{(i)}), z^{(i)})_{i=1,\ldots,k}$$

Hamming weight Cryptanalysis

$\tilde{x}$ such that $Hd(\tilde{x}, x)$ is small

Exhaustive search

x private key !

Step 4

Step 4: Experimental Results

k (number of samples)	200	400	600	800	1000
Immediate keys $\tilde{x} = x$	0%	2%	21%	52%	72%
seconds $Hd(\tilde{x}, x) \leq 2$	0%	3%	54%	80%	89%
hours $Hd(\tilde{x}, x) \leq 4$	0%	6%	72%	94%	97%
days $Hd(\tilde{x}, x) \leq 5$	0%	10%	77%	96%	98%
avg. distance $Hd(\tilde{x}, x)$	46	16.1	3.9	1.4	0.7

Outline

- Introduction
- GPS Identification Scheme
- Hamming Weight Cryptanalysis
- Timing Attack on GPS
- Countermeasures
- Conclusion

Countermeasures

- Message blinding (Kocher)
- Tweak Montgomery multiplication (Dhem, Walter)

} Unappropriate

- Exponent blinding

} Efficiency !!!

Exponent blinding

- Before blinding: $g^{y} \bmod n$

  where $|y| = 240$ to 300

- After blinding: $g^{y+t\times j\,(n)} \bmod n$

  where $|y + t \times j\,(n)| = |n|$

- It hides $Hw\,(y)$ but it's not efficient

Countermeasures

- Message blinding (Kocher)
- Tweak Montgomery multiplication (Dhem, Walter)

} Unappropriate

- Exponent blinding

} Efficiency !!!

- Square & Multiply always

} 33% overhead

- Division Chains (MIST)
- Use pre-computed commitments

} OK

Conclusion

- Hamming Weight Cryptanalysis is feasible
  - Short list of Hamming weights → 160 bit key !
  - A fast algorithm
  - Works with approximations of $Hw(y^{(i)})$
- Application of HWC: Timing Attack
  - An efficient side-channel attack on GPS

What if CRT is used ?

- Instead of $g^{y} \bmod n$, the prover computes $g^{y \bmod p-1} \bmod p$ then $g^{y \bmod q-1} \bmod q$
- Since $y << p, q$, we have $y \bmod p-1 = y$ and $y \bmod q-1 = y$
- The attack still works