Timing Attacks on Implementations of Di e Hellman RSA DSS and Other Systems

paul cryptography com

Abstract

Keywords

1 Introduction

2 Cryptanalysis of a Simple Modular Exponentiator

R

y^x n n y

x

y^x n y y n

x

y

R y^x n x w

```
Let s
For k     upto w
  If     k    x  is    then
    Let R_k    s_k  y       n
  Else
    Let R_k    s_k
  Let s_k      R_k       n
EndFor
Return  R_w
```

b b

b

b

b For s_b

R_b s_b y n

s_b y

R_b s_b y n

R_b s_b y n

b R_b s_b y n

b

s_b R_b n

3 Error Correction

b $R_{k\ b}$

4 The General Attack

j y y y_j
T T T_j x_b b

$$P\ x_b \quad \prod_i^j F\ T_i \quad t\ y_i\ x_b$$

$t\ y_i\ x_b$ b
y_i^x n x_b F
T $t\ y\ x_b$ y x_b F
T_i $t\ y_i\ x_b$ x_b
T_i $t\ y_i\ x_b$
s F
x_b x_b
x_b x_b'

$$\frac{\prod_i^j F\ T_i \quad t\ y_i\ x_b}{\prod_i^j F\ T_i \quad t\ y_i\ x_b \qquad \prod_i^j F\ T_i \quad t\ y_i\ x_b'}$$

F

5 Simplifying the Attack

F
T e $\sum_i^w t_i$ t_i
i e

x_b $\sum_i^b$ t_i y x_b

T e $\sum_i^w$ t_i $\sum_i^b$ t_i e $\sum_i^w{}_b$ t_i

e $\sum_i^w{}_b$ t_i

e w b t c b

e

w b c t

t

t

j

b w

c

$\sum_i^b$ t_i

t_i

e

P $\sum_i^j$ $\sqrt{w\ \ b}X_i$ $\sqrt{b\ \ c}Y_i$ $\sum_i^j$ $\sqrt{w\ \ b}X_i$

P $\sqrt{b\ \ c\ \ w\ \ b}\sum_i^j X_iY_i$ b c $\sum_i^j Y_i$

X Y j

$\sum_i^j$ Y_i j $\sum_i^j$ X_iY_i

$\sqrt{j}$

P $\sqrt{b\ \ c\ \ w\ \ b}\ \sqrt{j}Z$ b c j P Z $\frac{\sqrt{j\ b\ \ c}}{\sqrt{w\ \ b}}$

Z

$\sqrt{\frac{j\ b\ \ c}{w\ \ b}}$ x

∞ x j

w

6 Experimental Results

^{TM}

^{TM}

a b n

a b

n

y y n

s

$\sqrt{}$ s

s s

FIGURE 1: RSAREF Modular Multiplication Times

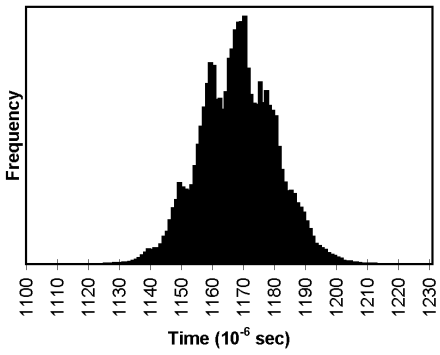
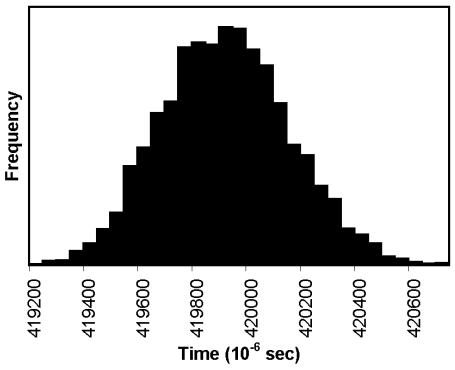


FIGURE 2: RSAREF Modular Exponentiation Times



$\sqrt{\frac{j\ b}{w}\frac{c}{b}}$

j b c w

$\sqrt{}$

b

7 Montgomery Multiplication and the CRT

n

t_b $\sum_i^w{}_b$ t_i

e

$\overline{}$

t_i

y p y q

y

y

p q

p q y

p y p y p

p y

p y p

y

p y p y p

y p

y p p

y

p

y

p

p

p

p

p q

8 Timing Cryptanalysis of DSS

s k H m x r q

r q k H m

x H m x r q

k q

x r q

H m H m q

x r

r

x

x

x x

x r

x k

9 Masking Timing Characteristics

R_i s_i y n

$\frac{ms}{ms}$ $mean$

10 Preventing the Attack

v_i v_f v_f $v_i{}^x$ n

v_i v_f $v_i{}^x$ n

v_f n

v_i $v_f{}^e$ n e

v_i n

v_f n

n

n

v_i v_f v_f $v_i{}^x$ n

v_i v_f

v_i v_f

v_i' v_i v_f' v_f

v_i v_f

v_i v_f

w

provably

n

n

11 Further Work

$$\sum_n \frac{\frac{56}{n}}{56} \qquad \frac{56}{\frac{56}{n}}$$

f

p q

12 Conclusions

13 Acknowledgements

References

Advances in Cryptology

Proceedings of Crypto 82

IEEE Transac

tions on Information Theory

On the Design and Security of Block Ciphers

Mathematics

of Computation

Fast Software Encryption Second

International Workshop Leuven Belgium December 1994 Proceedings

Communications of the ACM **21**

Fast Software Encryption Cambridge Security Workshop Cambridge

U K December 1993 Proceedings

`r`

Fast Software Encryption Second International Workshop Leuven

Belgium December 1994 Proceedings