

# Homework Assignment 03

Machiry Aravind Kumar

UCSB

## 1 Problem 1

Consider the exponent  $d = 49 = (110001)$ . Show the steps and all intermediate powers in the computation of  $m^d$  for the algorithms

### 1.1 the left-to-right binary method

i	$e_i$	Step 2a	Step 2b
4	1	$(m)^2 = m^2$	$m^2.m = m^3$
3	0	$(m^3)^2 = m^6$	$m^6$
2	0	$(m^6)^2 = m^{12}$	$m^{12}$
1	0	$(m^{12})^2 = m^{24}$	$m^{24}$
0	1	$(m^{24})^2 = m^{48}$	$m^{48}.m = m^{49}$

### 1.2 the right-to-left binary method

$R_0 = 1, R_1 = m, i = 0$

i	$d_i$	$R_0$	$R_1$
0	1	$1.m$	$m^2$
1	0	$m$	$(m^2)^2$
2	0	$m$	$(m^4)^2$
3	0	$m$	$(m^8)^2$
4	1	$m.m^{16}$	$(m^{16})^2$
5	1	$m^{17}.m^{32}$	$(m^{32})^2$

$R_0 = m^{49}$

### 1.3 the square-and-multiply-always algorithm

$R_0 = 1, R_1 = 1$

i	$d_i$	b	$R_0$	$R_b$
5	1	0	$R_0 = 1^2$	$R_0 = 1.m$
4	1	0	$R_0 = m^2$	$R_0 = m^2.m$
3	0	1	$R_0 = (m^3)^2$	$R_1 = 1.m$
2	0	1	$R_0 = (m^6)^2$	$R_1 = m.m$
1	0	1	$R_0 = (m^{12})^2$	$R_1 = m^2.m$
0	1	0	$R_0 = (m^{24})^2$	$R_0 = m^{48}.m$

$R_0 = m^{49}$

#### 1.4 the Montgomery powering ladder

$$R_0 = 1, R_1 = m$$

i	$d_i$	b	$R_b$	$R_{d_i}$
5	1	0	$R_0 = 1.m$	$R_1 = m^2$
4	1	0	$R_0 = m.m^2$	$R_1 = (m^2)^2$
3	0	1	$R_1 = m^3.m^4$	$R_0 = (m^3)^2$
2	0	1	$R_1 = m^6.m^7$	$R_0 = (m^6)^2$
1	0	1	$R_1 = m^{12}.m^{13}$	$R_0 = (m^{12})^2$
0	1	0	$R_0 = m^{24}.m^{25}$	$R_1 = (m^{25})^2$

$$R_0 = m^{49}$$

#### 1.5 the Atomic square-and-multiply algorithm

$$R_0 = 1, R_1 = m$$

i	$d_i$	$b_{before}$	$R_b$	$R_0$	$b_{after}$
5	1	0	$R_0 = 1$	1.1	1
5	1	1	$R_1 = m$	1.m	0
4	1	0	$R_0 = m$	m.m	1
4	1	1	$R_1 = m$	$m^2.m$	0
3	0	0	$R_0 = m^3$	$m^3.m^3$	0
2	0	0	$R_0 = m^6$	$m^6.m^6$	0
1	0	0	$R_0 = m^{12}$	$m^{12}.m^{12}$	0
0	1	0	$R_0 = m^{24}$	$m^{24}.m^{24}$	1
0	1	1	$R_1 = m$	$m^{48}.m$	0

$$R_0 = m^{49}$$

#### 1.6 the Atomic right-to-left algorithm

$$R_0 = 1, R_1 = m, b = 1, i = 0$$

i	$d_i$	$b = b \oplus d_i$	$R_b$
0	1	0	$R_0 = 1.m$
0	1	1	$R_1 = m.m$
1	0	1	$R_1 = m^2.m^2$
2	0	1	$R_1 = m^4.m^4$
3	0	1	$R_1 = m^8.m^8$
4	1	0	$R_0 = m.m^{16}$
4	1	1	$R_1 = m^{16}.m^{16}$
5	1	0	$R_0 = m^{17}.m^{32}$
5	1	1	$R_1 = m^{32}.m^{49}$

$$R_0 = m^{49}$$

**2 Let an RSA key be determined by the parameters  $\{p,q,n,\phi(n),e,d\} = \{97,103,9991,9792,2015,8927\}$ . Compute  $S = M^d \pmod{n}$  for  $M = 25$  using each of these DPA-type countermeasure algorithms by selecting suitable random parameters:**

### 2.1 Randomizing m, where e is known

Picking random  $r = 17$ .

$$m^* = (17)^{2015} \cdot 25 \pmod{9991} = 7111.$$

$$S^* = (7111)^{8927} \pmod{9991} = 5681.$$

$$r^{-1} = 4114.$$

$$S = 5681 \cdot 4114 \pmod{9991} = \mathbf{2685}.$$

### 2.2 Randomizing m, where e is unknown

Picking random  $r = 17$ .

$$m^* = 17 \cdot 25 \pmod{9991} = 425.$$

$$S^* = (425)^{8927} \pmod{9991} = 4289.$$

$$r^{-1} = 4114.$$

$$S = 4289 \cdot 4114^{8927} \pmod{9991} = \mathbf{2685}.$$

### 2.3 Randomizing m, using a small r

Selecting  $l$  to be 5.  $2^l = 32$ .

Selecting  $r$  to be 17 ( $< 32$ ).

$$m^* = 25 + 17 \cdot 9991 = 169872.$$

$$N^* = 32 \cdot 9991 = 319712.$$

$$S^* = (169872)^{8927} \pmod{319712} = 52640.$$

$$S = 52640 \pmod{9991} = \mathbf{2685}.$$

### 2.4 Randomizing d, using a small r

Picking random  $r = 17$ .

$$d^* = 8927 + 17 \cdot 9792 = 175391.$$

$$S = (25)^{175391} \pmod{9991} = \mathbf{2685}.$$

### 2.5 Randomizing d, where $\phi(n)$ is unknown

Picking random  $r = 17$ .

$$d^* = 8927 + 17 \cdot (2015 \cdot 8927 - 1) = 305803295.$$

$$S = (25)^{305803295} \pmod{9991} = \mathbf{2685}.$$

### 2.6 Randomizing d, where e is unknown

Picking random  $r = 17$ .

$$d^* = 8927 - 17 = 8910.$$

$$S_1^* = (25)^{8910} \pmod{9991} = 7017.$$

$$S_2^* = (25)^{17} \pmod{9991} = 9120.$$

$$S = 7017 \cdot 9120 \pmod{9991} = \mathbf{2685}.$$

## 2.7 Randomizing n, using small random $r_1$ and $r_2$

Picking random  $r_1 = 17, r_2 = 29$ .

$$m^* = 25 + 17 \cdot 9991 = 169872.$$

$$N^* = 29 \cdot 9991 = 289739.$$

$$S^* = 169872^{8927} \bmod(289739) = 22667.$$

$$S = 22667 \bmod(9991) = \mathbf{2685}.$$