

CSE 509 class note (4/19)

Side Channel Attacks

- Timing
- Power
- Sound
- Light

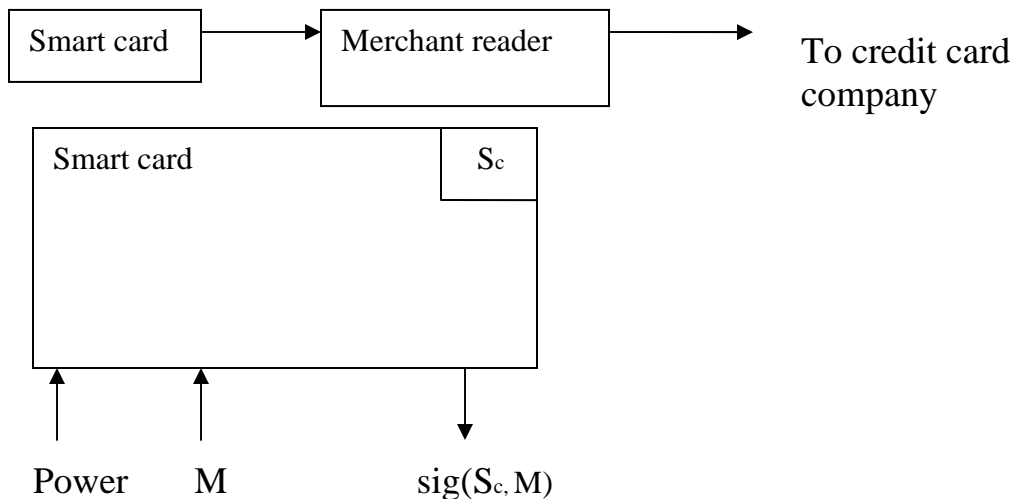
- Usability and Security
 - o Depending on Users
 - o Role playing

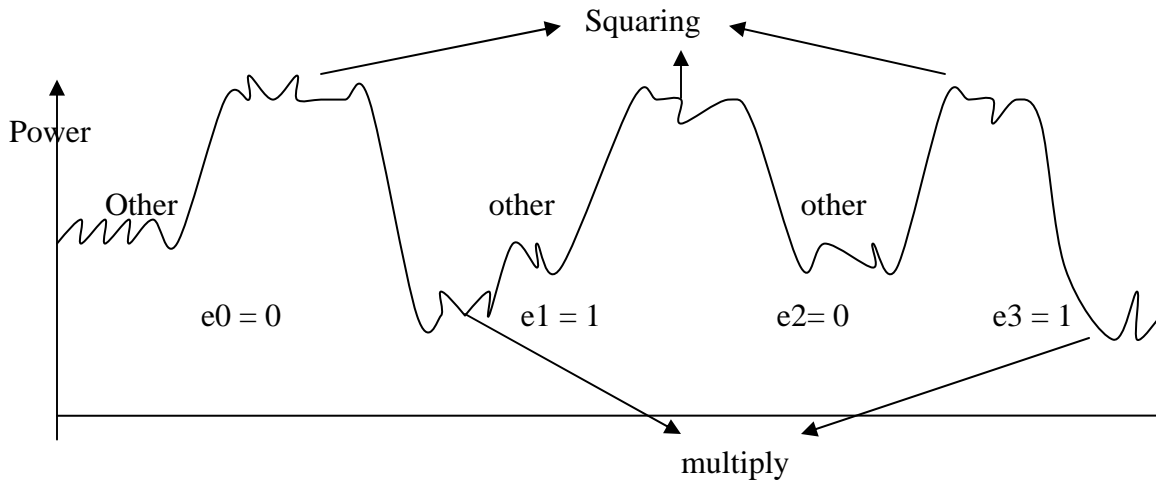
- Modular Exponentiation

```
ModExp(m,e,n)      // M^e mod n
  Let el ... e0=e  // the bits of e
  Let acc = 1
  For i=0 ... l
    if ei==1
      acc = acc*m mod n
      m = m^2 mod n
  return acc;
```

$$\begin{aligned} m^e \bmod n &= m^{(2^0 e_0 + 2^1 e_1 + 2^2 e_2 + \dots + 2^l e_l)} \bmod n \\ &= m^{e_0} * (m^2)^{e_1} * (m^4)^{e_2} * (m^{(2^l)})^{e_l} \bmod n \end{aligned}$$

- Power Analysis (smart cards)





- timing attack against square and multiply
 - o some reductions take longer than others
 - o fast reductions
 - o slow reductions
 - o if attackers knows $acc * m$, he can predict whether reduction is fast or slow

attacker input	m_0	m_1	m_2	m_3	...	m_k
time	t_0	t_1	t_2	t_3	...	t_k

suppose $e_0 = 1$

- can compute
 - o acc and m at end of round 0
- predict whether round 1 will be fast or slow for each message m_i
- let
 - o f = average time of "fast" messages
 - o s = average time of "slow" messages
- two cases
 - o $|s_1 - f_1|$ is small and $|s_0 - f_0|$ is small
 $\rightarrow e_1 = 0$
- suppose $|s_b - f_b|$ is large and $|s(\sim b) - f(\sim b)|$ is small
 $\rightarrow e_1 = 1$ and $e_0 = b$

repeat for round 2, ..., l

- defense
 - o for $i=0 \dots l$
 - if $e_i == 1$
 - $acc = acc * m \bmod n$
 - else
 - $tmp = acc * m \bmod n$
 - $m = m^2 \bmod n$

- RSA binding

to compute $m^e \bmod n$

- pick random r
- compute $x = (rm)^e \bmod n$
- compute $y = r^e \bmod n$
- return $x/y \bmod n$