Side Channel Attacks -- Randomized ME

Cybersecurity Specialization
-- Hardware Security

Randomized Modular Exponentiation

- Modular exponentiation: $y = x^d \pmod{N}$
- Attacker's goal: find the value of d
- Vulnerability in square and multiply algorithm
- Randomized modular exponentiation (gcd (x,N)=1)
  - Choose 3 random numbers r_1, r_2, r_3.
  - $x' = x + r_1 * N$
  - $d' = d + r_2 * \varphi(N)$
  - $N' = r_3 * N$
  - Compute $y' = (x')^{d'} \pmod{N'}$
  - Compute $y'' = y' \pmod{N}$

Claim:
$y'' = y = x^d \pmod{N}$

Square and Multiply for ME

- compute 15^{47} (mod 26)
  - $47_{10} = 101111_2$
  - 15^{47} (mod 26)
    - 1: 15
    - 0: $15^2 = 225 = -9$ (mod 26)
    - 1: $(-9)^2*15 = 81*15 = 3*15 = 45 = -7$ (mod 26)
    - 1: $(-7)^2*15 = 49*15 = (-3)*15 = -45 = 7$ (mod 26)
    - 1: $7^2*15 = 49*15 = 7$ (mod 26)
    - 1: $7^2*15 = 7$ (mod 26)
- Vulnerability: multiply only on 1, not on 0

47	÷	2	=	23	…	1
23	÷	2	=	11	…	1
11	÷	2	=	5	…	1
5	÷	2	=	2	…	1
2	÷	2	=	1	…	0
1	÷	2	=	0	…	1

Euler's φ-function

- $\varphi(n) = |\{k: 1 \le k \le n, \gcd(k,n) = 1\}|$ is the number of positive integers less than or equal to n and relatively prime to n.
- Examples:
  - $\varphi(2) = |\{1\}| = 1$
  - $\varphi(3) = |\{1, 2\}| = 2$
  - $\varphi(5) = |\{1, 2, 3, 4\}| = 4$
  - $\varphi(p) = |\{1, 2, \ldots, p-1\}| = p-1$ (if p is a prime)
  - $\varphi(10) = |\{1, 3, 7, 9\}| = 4 = \varphi(2)\,\varphi(5)$
  - $\varphi(15) = |\{1,2,4,7,8,11,13,14\}| = 8 = \varphi(3)\,\varphi(5)$

Euler's Product Formula

- $\varphi(m*n) = \varphi(m)\,\varphi(n)$ if $\gcd(m,n)=1$.
  - $(m-\varphi(m))*n + \varphi(m)*(n-\varphi(n)) = mn-\varphi(m)\varphi(n)$
  - $\varphi(2) = |\{1\}| = 1$, $\varphi(5) = |\{1, 2, 3, 4\}| = 4$
  - Not relatively prime to 10: $\{2,4,6,8,10\}\cup\{5\}$
  - $\varphi(10) = 10-6=4$
- Euler's product formula:
  - If $n = p_1^{k1} * p_2^{k2} * \ldots * p_m^{km}$, where p_i's are distinct primes, then

$$\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_m})$$

Euler's Theorem & An Application

- Euler's Theorem:
  - If $\gcd(a,n)=1$, $a^{\varphi(n)}=1 \pmod n$
- Find the modular multiplicative inverse
  - If $\gcd(a,n)=1$, $a^{-1} = a^{\varphi(n)-1} \pmod n$
  - Proof: $a*a^{\varphi(n)-1} = a^{\varphi(n)} = 1 \pmod n$
- Examples:
  - $\gcd(7,10) = 1$, $\varphi(10) = 4 \rightarrow$
  - $7^{-1} = 7^3 = 49*7 = 9*7 = 63 = 3 \pmod{10}$
  - Verify: $7*3 = 21 = 1 \pmod{10}$

Example of the Randomized ME

Choose 3 randoms r_1, r_2, r_3.
$x' = x + r_1 * N$
$d' = d + r_2 * \varphi(N)$
$N' = r_3 * N$
Compute $y' = (x')^{d'} \pmod{N'}$
Compute $y'' = y' \pmod N$

$15^{47} = 7 \pmod{26}$

- $r_1 = 4,\ r_2 = 7,\ r_3 = 5$
- $\varphi(26) = \varphi(2)\varphi(13) = 12$
- $x' = 15+4*26 = 119$
- $d' = 47+7*12 = 131$
- $N' = 5*26 = 130$
- $y' = 119^{131} \pmod{130}$
  - $131_{10} = 1000{,}0011_2$
  - $119^{131} = 59 \pmod{130}$
- $y'' = 59 = 7 \pmod{26}$

131	÷	2	=	65	…	1
65	÷	2	=	32	…	1
32	÷	2	=	16	…	0
16	÷	2	=	8	…	0
8	÷	2	=	4	…	0
4	÷	2	=	2	…	0
2	÷	2	=	1	…	0
1	÷	2	=	0	…	1

Proof the Randomized ME

Choose 3 randoms r_1, r_2, r_3.
$x' = x + r_1 * N$
$d' = d + r_2 * \varphi(N)$
$N' = r_3 * N$
Compute $y' = (x')^{d'} \pmod{N'}$
Compute $y'' = y' \pmod N$

- $a=c \pmod p \rightarrow a=c+pk_1$
- $b=d \pmod p \rightarrow b=d+pk_2$
- $ab = (c+pk_1)(d+pk_2) = cd \pmod p$
- $(x')^{d'}=(x+r_1N)^{d+r_2\varphi(N)} = (x+r_1N)^d\,(x+r_1N)^{r_2\varphi(N)}$
- Let $a = (x+r_1N)^d \pmod{N'}$
- $a = (x+r_1N)^d + r_3N\,k_1 \rightarrow a = x^d \pmod N$
- Let $b = (x+r_1N)^{r_2\varphi(N)} \pmod{N'}$
- $b = (x+r_1N)^{r_2\varphi(N)}+r_3N\,k_2 \rightarrow b=x^{r_2\varphi(N)}=1 \pmod N$
- $y'' = (x')')^{d'}=ab = x^d * 1 = x^d = y \pmod N$