Side Channel Attacks -- More Attacks and Countermeasures

Cybersecurity Specialization
-- Hardware Security

RSA Algorithm

- Key generation:
  - Generate large (say, 2048-bit) primes p, q
  - Compute n=pq
  - Choose small e, relatively prime to (p-1)(q-1)
  - Compute the unique d such that ed = 1 mod (p-1)(q-1)
  - Public key = (e,n); private key = d
    - Security relies on the assumption that it is difficult to factor n into p and q
- Encryption of m: $c = m^e \bmod n$
- Decryption of c: $c^d \pmod n = (m^e)^d \bmod n = m$
- Square and multiply for "$y^x \bmod n$".

Kocher's Timing Attack on RSA

- Guess some bits of the exponent and predict how long decryption will take.
- Run decryption and compare the run time with the prediction.
  - if the guess is correct, correlation in execution time can be observed
  - otherwise, the prediction will look random
- Start by guessing a few top bits, look at correlations for each guess, pick the most promising candidate and continue.

Montgomery Reduction

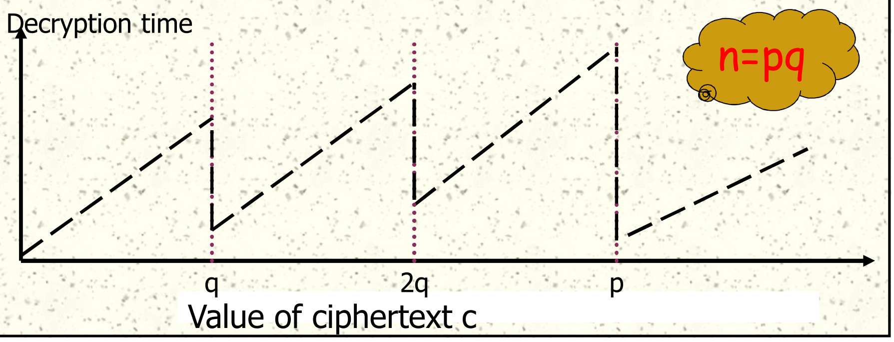
- Let R>N be two integers and gcd(N,R)=1. For $0 \le T < NR$, the *Montgomery reduction* of T modulo N w.r.t. R is defined as TR^{-1} (mod N).
- Montgomery reduction algorithm
  - $m = T \times (-N^{-1}) \pmod R$
  - $t = (T + mN)/R$
  - if ($N \le t$)
  - $t = t - N$
- Claim: $t = TR^{-1} \pmod N$
  - $tR = T \pmod N$
  - $0 \le t < N$

Montgomery reduction can be used to compute modular multiplication efficiently

for larger T, multiple subtractions will be needed to have t<N

Schindler's Observation

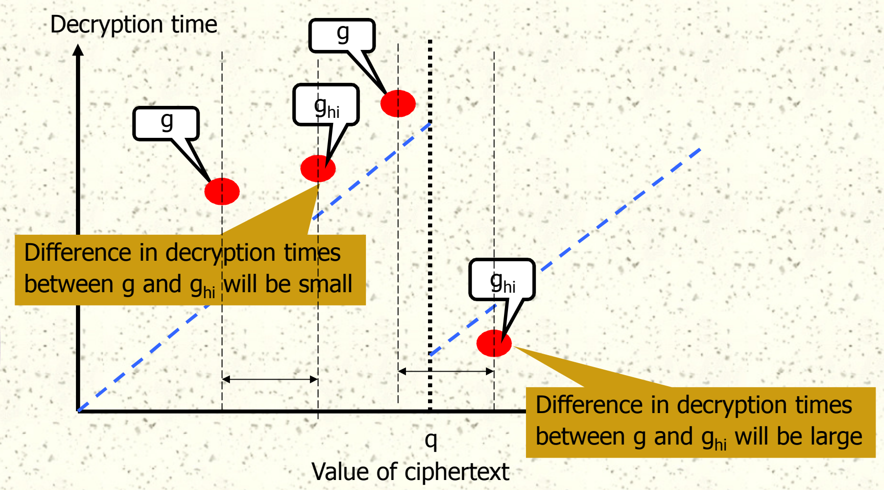
- Probability of the subtraction step ∝ c mod q
  - If c is close to q, a lot of subtractions will be needed
  - If c mod q = 0, very few subtractions
- An attacker can guess q by observing the decryption time with different values of c.



Attack Overview

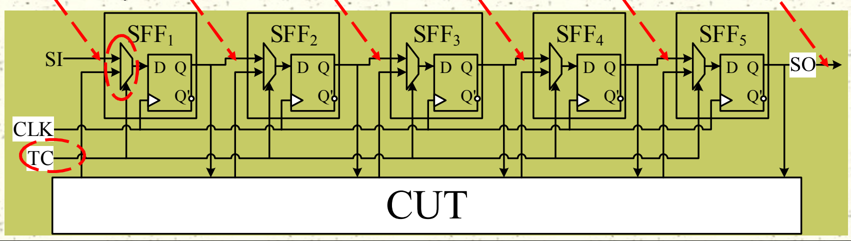
- Initial guess g for q between 2^{511} and 2^{512} (for 1024-bit RSA)
- Try all possible guesses for the top few bits
- Suppose we know that top i-1bits of q are 101001, to guess the i^{th} bit
  - Set g = 101001000…000
  - Set g_{hi}= 101001100…000
  - If $g<q<g_{hi}$ then the i^{th} bit of q is 0
  - If $g<g_{hi}<q$ then the i^{th} bit of q is 1

Determine the Next Bit for q



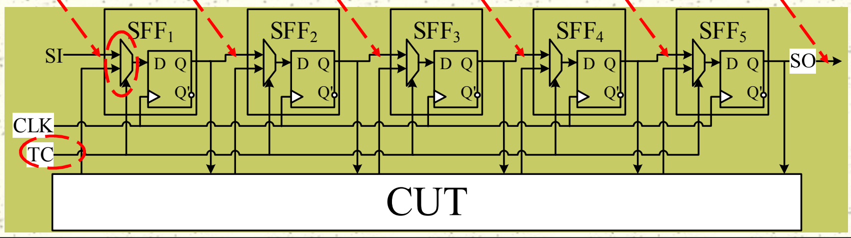
Scan Chain Attacks

- Attacks based on observability
  - TC=0, provide primary input to the system
  - TC=0, run for one or more clock cycles
  - TC=1, test mode to capture internal state from scan out
  - Repeat to collect more information



Scan Chain Attacks

- Attacks based on controllability
  - TC=1, test mode to set the system state
  - TC=0, run for one or more clock cycles
  - TC=1, test mode to capture internal state from scan out
  - Repeat to collect more information



Countermeasures to SCA

- Hiding

  Make it more challenging for the attackers to extract information from side channels
  - Noise generator
    - Use extra circuits to draw current randomly or add random delay to certain paths or logic units
    - Keep the total power consumption constant
    - Add EM noise
  - Balanced logic styles
    - Make logic unit's power/delay independent of input data (and the key)

Countermeasures to SCA

- Hiding
  - Asynchronous logic
    - No clock and global synchronization, so many side channel attacks will fail
  - Low power design

    Reduce total power weakens the signals from most of the side channels.
  - Shielding

    Physically shield or filter the side channel leakage
    - Use the upper level metal layer (EM emission)
    - Use sound dampening materials (acoustic)

Countermeasures to SCA

- Hiding
- Masking/blinding

  Remove the correlation between input data and side channel emissions.
  - Gate level: XOR the output of a logic unit with pre-selected data values to mask the real values
  - Word level: randomize input data, might be hard because the operation needs to be modified as well to generate the correct output

Countermeasures to SCA

- Hiding
- Masking/blinding
- Design partitioning/separation
  - Memory: RED (plain text) vs. BLACK (cipher text)
  - On-chip infrastructure: power supply, clock network, testing
  - Fabrication: 3D stacking, split fabrication
- Physical security

  Denial of proximity, access, and possession
  - Acoustic shielding of the target devices
  - Secure zone (against EM emission attacks)