fault attacks and countermeasures

Subhadeep Banik
Email: `subb @ dtu.dk`

November 12, 2015

DTU Compute, Lyngby

table of contents

introduction

fault attack

- What is a **FAULT** ?
- ANS: Any external stimulus that causes a device to malfunction.
- Ex: Heat, High Voltage, Laser injection, Glitches etc.
- Can be used for cryptanalysis.

Figure 1: Diode Laser Station Courtesy (`www.riscure.com`)

a preliminary example: voltage fluctuation

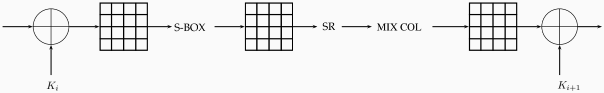
- **Car Protection System**.
- Both Car and Key fob have shared secret K.
- Car issues random challenge r and computes $s = E_K(r)$.
- Key fob calculates $s^* = E_K(r)$ and sends to Car.
- **If** $s = s^*$, Car accepts the Key.
- Supply voltage tampering during comparison.
- May cause Car to accept even if $s \neq s^*$ **!!!** (Watch at [1])

skorobogatov & anderson. [ches 2002]

- Modern CMOS circuits are built on Silicon Substrates.
- Behaves abnormally when exposed to light.
- Fault can be injected optically !!!
- Weapon of choice: a \$30 camera flash/ \$8 laser pointer.
- Target: Common micro-controller chip PIC16F84: state of flip-flop inverted.

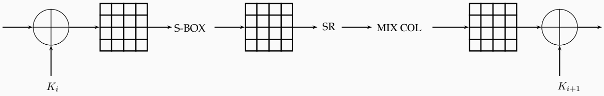
fault attack on aes

advanced encryption standard



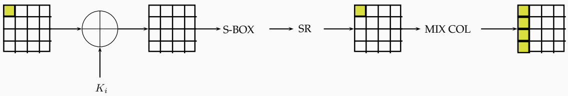
- Standard SPN Structure - 10 Rounds.
- 8-bit S-Box (Affine transform of the Inverse overs AES field)
- Shift Row - (*i*-th row rotated by *i* bytes)
- MDS matrix as Mix Column.

advanced encryption standard: fault model



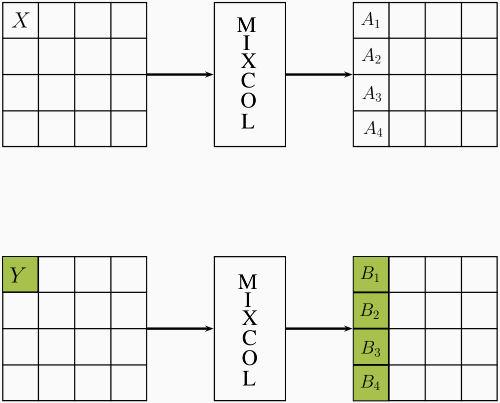
- More control vs Less Control.
- The lesser the control, the stronger the attack.
- Time synchronized faults: inject fault at precise moment.
- Space synchronized faults: inject fault at precise byte location.

advanced encryption standard: attack idea



- We will look at the differences between the correct/faulty Ciphertext.
- Corrupt the first byte at the beginning of a round.
- What is the difference between the correct and faulty Ciphertext after 1 round?
- How many differences are possible ?

advanced encryption standard: attack idea



Exercise 1

Let $X \oplus Y = \Delta$. Find $A_i \oplus B_i$.

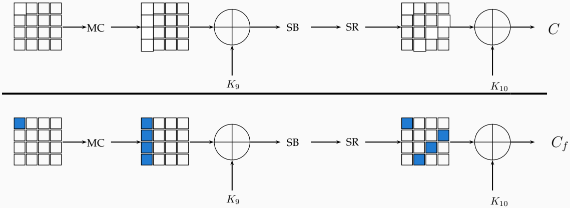
advanced encryption standard: attack idea

Solution 1

$$\begin{pmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \end{pmatrix} \oplus \begin{pmatrix} B_1 \\ B_2 \\ B_3 \\ B_4 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} X \oplus Y \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} \Delta \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2\Delta \\ \Delta \\ \Delta \\ 3\Delta \end{pmatrix}$$

advanced encryption standard: fault in 9th aes round

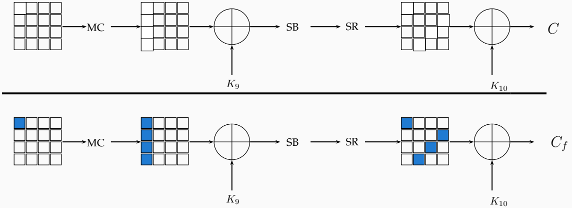


- Start by guessing four bytes of K_{10}

$$\Delta_i = SB^{-1}\left(C[i] \oplus K_{10}[i]\right) \oplus SB^{-1}\left(C_f[i] \oplus K_{10}[i]\right), i = 0, 7, 10, 13$$

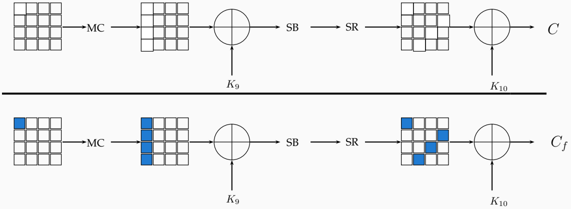
- For correct guess of the 4 bytes of $K_{10} \rightarrow \begin{pmatrix} \Delta_0 \\ \Delta_7 \\ \Delta_{10} \\ \Delta_{13} \end{pmatrix}$ is of form $\begin{pmatrix} 2\Delta \\ \Delta \\ \Delta \\ 3\Delta \end{pmatrix}$

advanced encryption standard: fault in 9th aes round



- We have 2^{32} guesses for four bytes.
- Repeat for each column : Time Complexity 2^{34}
- Once K_{10} is found completely: Invert Key Schedule $\rightarrow K_0$
- Key Schedule is invertible (Why ??)

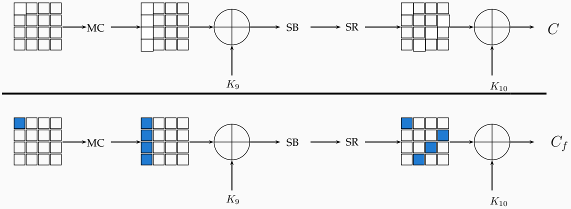
advanced encryption standard: fault in 9th aes round



THINK

What if fault is injected in 10th round ???

advanced encryption standard: fault in 9th aes round

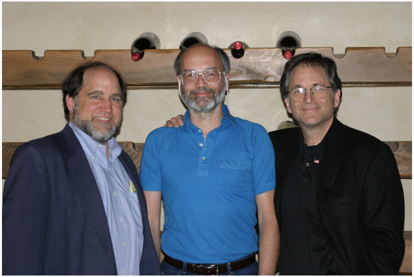


THINK

What if fault is injected in 8th round ???

fault attack on crt-rsa signatures

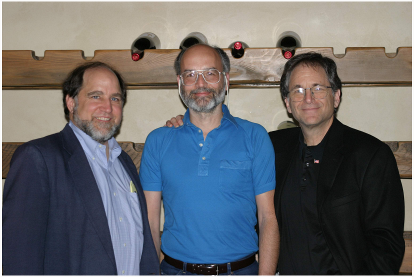
rsa public key cryptosystem



Asymmetric Keys

- Public Key Cryptosystem.
- Two Keys: Secret Key at one end / Public Key at another.
- Based on classically difficult problems in Computer Science.

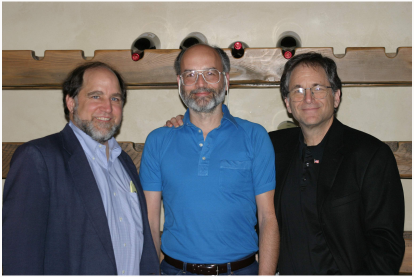
rsa public key cryptosystem



SETUP

- Based on the difficulty of factorization problem.
- Two large primes p, q and $n = pq$. $ed \equiv 1 \bmod (p-1)(q-1)$
- Secret Key: (p, q, d). Public Key (e, n)

rsa public key cryptosystem



Encryption/Decryption

- Encryption: $c = m^e \bmod n$.
- Decryption: $m = c^d \bmod n$.
- Correctness: $c^d = m^{de} \bmod n = (m^{\phi(n)})^k \cdot m \bmod n = m \bmod n$

rsa public key cryptosystem

Example

- $p = 37, q = 43$ and $n = 1591$. So $\phi(n) = 36 \cdot 42 = 1512$
- Select $e = 5$ and $d = 605$, so that $ed = 3125 = 2 * 1512 + 1$
- If $m = 57$: $c = m^e \bmod n = 57^5 \bmod 1591 = 1313$.
- Decryption: $m = c^d \bmod n = 1313^{605} \bmod 1591 = 57$.

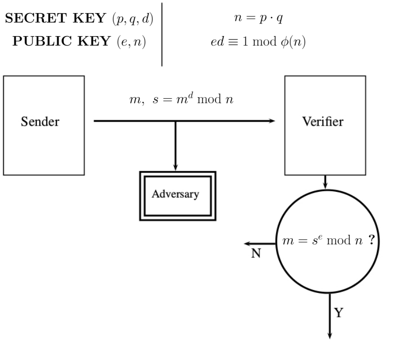
modular exponentiation: matlab code

```
 function result = modexp (x, y, n)
    %anything raised to 0th power = 1 so return 1
    if (y == 0)
        result = 1;
        return;
    end
    z = modexp(x, floor(y/2), n);

    if (mod(y, 2) == 0)
        result = mod(z*z, n);
        return;
    else
        result = mod(x*z*z, n);
        return;
    end
end
```

another example: crt-rsa signatures

- RSA based authentication scheme.
- $s = m^d$ mod n is too slow.



another example: crt-rsa signatures

- CRT-RSA to speed up (4 times faster).
- $d_p = d \bmod p-1$, $d_q = d \bmod q-1$.
- $s_p = m^{d_p} \bmod p$, $s_q = m^{d_q} \bmod q$
- Note that s is the solution to the above system.
- So calculate $s = CRT(s_p, s_q)$

$$= s_q \cdot p \cdot p^{-1} + s_p \cdot q \cdot q^{-1}$$

Example

- $p = 37, q = 43$ and $n = 1591$. So $\phi(n) = 36 \cdot 42 = 1512$
- Select $e = 5$ and $d = 605$, so that $ed = 3125 = 2 * 1512 + 1$
- $d_p = 605 \bmod 36 = 29$. $d_q = 605 \bmod 42 = 17$
- $s_p = 1313^{29} \bmod 37 = 20$. $s_q = 1313^{17} \bmod 43 = 14$
- $p^{-1} \bmod q = 7$. $q^{-1} \bmod p = 31$
- $s = 20 * 43 * 31 + 14 * 37 * 7 \bmod 1591 = 57$

fault attack: boneh-demillo-lipton 1997

- Corrupt any one of the modular exponentiation.
- $d_p = d \bmod p-1$, $d_q = d \bmod q-1$.
- $s_p = m^{d_p} \bmod p$, $s_q^* \neq m^{d_q} \bmod q \Leftarrow$ Faulty
- So calculate $s^* = CRT(s_p, s_q^*)$

$$= s_q^* \cdot p \cdot p^{-1} + s_p \cdot q \cdot q^{-1}$$

- Verify $[s^*]^e = [s_p]^e \bmod p = m \bmod p \Rightarrow p$ divides $[s^*]^e - m$

$$p = GCD([s^*]^e - m,\ n)$$

crt rsa signatures

Example

- $p = 37, q = 43$ and $n = 1591$. So $\phi(n) = 36 \cdot 42 = 1512$
- Select $e = 5$ and $d = 605$, so that $ed = 3125 = 2 * 1512 + 1$
- $d_p = 605 \bmod 36 = 29$. $d_q = 605 \bmod 42 = 17$
- $s_p = 1313^{29} \bmod 37 = 20$. $s_q = 1313^{17} \bmod 43 = 14 \neq 20$
- $p^{-1} \bmod q = 7$. $q^{-1} \bmod p = 31$
- $s^* = 20 * 43 * 31 + 20 * 37 * 7 \bmod 1591 = 20$

- $[s^*]^e = 20^5 \bmod 1591 = 499$
- GCD(499-1313,1591) = GCD(814,1591)=37

conclusion

summary

- Invasive Side Channel attack
- Pretty useful engineering tool.
- Fault protection is important research discipline.
- We will look at a few fault protection techniques in next class.

Questions?

references I

R. B. Carpi and R. Pareja.
Hacking chips on the (very) cheap. Availab;e at
`https://www.youtube.com/watch?v=yaMbxgayqco`.