How Many Feet Are Best for A Football Game With AES?

Ye Yuan, Liji Wu

Institute of Microelectronics, Tsinghua University

Introduction of the Football Game

Competition

- Multiple-bits collision side channel attack on AES

How many feet are best?

- How many bits are best for the attack method?

Scoring

- Detecting multiple-bits collision successfully

Referee

- Attacking Efficiency

How to Train
——the procedure of the attack strategy

Tsinghua University

Algorithm1: multiple-bits side-channel collision attack

Step 1 ,2,3 are based on multiple-bits attack model

1:$\{P(n)|n = 1,2,3,\cdots,16N\} \leftarrow \boldsymbol{ChoosePlaintexts}()$

2:$\{T^{mj}(n)|n = 0,1,2,3,\cdots,N\}_{j=0}^{15} \leftarrow \boldsymbol{AcquireTrace}(\{P(n)\}_{n=1}^{16N})$

3:$\{\bar{t}_i^{mj}|1 \le i \le 16\}_{j=0}^{15} \leftarrow \boldsymbol{PreProcessTrace}(\{T^{mj}(n)|0 \le n \le N\}_{j=0}^{15})$

4: **for** each $(\{(i_1, i_2)|1 \le i_1 < i_2 \le 16\})$

5: $\Delta k_{i_1,i_2} \leftarrow$ DDVD$(\{\bar{t}_{i_1}^{mj}\}_{j=0}^{15}, \{\bar{t}_{i_2}^{mj}\}_{j=0}^{15})$

6: **end for**

7: **Recoverkey**$(\Delta_{i_1,i_2}(1 \le i_1 < i_2 \le 16))$

Algorithm2: *ChoosePlaintexts*

Input: the total number of plaintexts 16N

Output: 16N plaintexts: $\{\boldsymbol{P^n}\}$ $(1 \le n \le 16N)$

1: **for** $j = 0{:}15$

2: **for** $i = 1{:}N$

3: $P^{16j+i} = \{p_k|p_k^m = j, p_k^l = random(16)\}$

($random(n)$ is to generate an integer ranging from 0 to n-1)

4: **end for**

5: **end for**

6: **return** $\{P^n\}$ $(1 \le n \le 16N)$

Algorithm 3: AcquireTrace

Input: 16N plaintexts: $\{\boldsymbol{P^n}\}$ $(1 \le n \le 16N)$

Output: 16 sets of traces consisting of N single power traces:

$\{T^{mj}(n)|n = 0,1,2,3,\cdots,N\}_{j=0}^{15}$

1: **for** $j = 0{:}15$

2: **for** $i = 1{:}N$

3: $T^{mj}(i) = Powertraces\ of\ first\ round\ encryption(P^{16j+i})$

4: **end for**

5: **end for**

6: **return** $\{T^{mj}(n)|n = 0,1,2,3,\cdots,N\}_{j=0}^{15}$

Algorithm 4: *PreProcessTrace*

Input: 16 sets of power traces:$\{\boldsymbol{T^{mj}(n)|n = 0,1,2,3,\cdots,N}\}_{j=0}^{15}$

Output: 16 averaged power traces:$\{\bar{T}^{mj}\}_{j=0}^{15} = \{\bar{t}_i^{mj}|i = 1,2,3,\cdots,16\}_{j=0}^{15}$

1: **for** $j = 0{:}15$

2: $\bar{T}^{mj} = \frac{1}{N}\sum_{n=0}^{N} T^{mj}(n)$

3: Cut $\bar{T}^{mj}$ into 16 sub-traces: $\bar{T}^{mj} = \{\bar{t}_i^{mj}|i = 1,2,3,\cdots,16\}$

4: **end for**

5: **return** $\{\bar{T}^{mj}\}_{j=0}^{15} = \{\bar{t}_i^{mj}|i = 1,2,3,\cdots,16\}_{j=0}^{15}$

How to Score

——the procedure of the attack strategy

Algorithm 5: Double Distance Voting Detection

Input: 2 sets of sub-traces: $\{\bar{t}_{i_1}^{mj_1}\}_{j_1=0}^{15}$, $\{\bar{t}_{i_2}^{mj_2}\}_{j_2=0}^{15}$

Output: the 4 most significant bits of $\Delta k_{i_1,i_2}$: $\Delta k_{i_1,i_2}^{m}$

Distance Stage:

```
for (0 ≤ j1 ≤ 15)
    for (0 ≤ j2 ≤ 15)
        Distance(j1 ⊕ j2) = Σ_{l=1}^{L} (t̄_{i1,l}^{mj1} − t̄_{i2,l}^{mj2})^2
    end for
    Δ_{j1} = arg min_{j1⊕j2} Distance(j1 ⊕ j2)
end for
```

Voting Stage:

```
num_n = 0 (0 ≤ n ≤ 15)
for (0 ≤ j ≤ 15)
    for (0 ≤ n ≤ 15)
        if (Δ_j = n)
            num_n = num_n + 1
        else
            num_n = num_n
        end if
    end for
end for
Δk_{i1,i2}^m = arg max_n num_n
return Δk_{i1,i2}^m
```

- For each sub-traces of S-box i_1, calculate the distance between each of S-box i_2 and it;
- Choose the minimum one and get Δ;
- Choose Δ as the result, whose number is maximum.

➢ Improved:

maybe the top three as the results, and check them by

$$\Delta k_{i_1,i_2} \oplus \Delta k_{i_2,i_3} = \Delta k_{i_1,i_3}$$

Probability of Scoring
——the probability of successful detection

the probability of two traces corresponding to the collision n bit has the least distance:

$$Pro = 1 - \frac{C_{2^n}^{m} \times C_{2^n-m}^{m}}{C_{2^n}^{m} \times C_{2^n}^{m}}$$

the probability of successful detection for the method:

$$Pro\_dete = 1 - \sum_{i=2^{n-1}}^{2^n} C_{2^n}^{i} \times (1 - Pro)^{i} \times Pro^{2^n - i}$$

the probability of successful detection for the improved method:

$$Pro\_dete\_impro = 1 - \sum_{i=2^n-2^{n-2}}^{2^n} C_{2^n}^{i} \times (1 - Pro)^{i} \times Pro^{2^n - i}$$

So, How Many feet?
——how many bits collision are best for the number of necessary traces?

To reach a 90% success rate for the original attack schedule:

n-bits	1	2	3	4	5	6	7	8
number of traces	288	160	168	128	192	256	512	256

To reach a 90% success rate for the improved attack schedule:

n-bits	1	2	3	4	5	6	7	8
number of traces	non	128	120	96	140	256	256	256

So, maybe when playing football game with AES or other block cipher, two hands and two feet are enough for you to be a best scorer!

清華大學
Tsinghua University