FUJITSU THE POSSIBILITIES ARE INFINITE

www.fujitsu.com

Address-bit Differential Power Analysis of Cryptographic Schemes OK-ECDH and OK-ECDSA

Kouichi Itoh, Tetsuya Izu and Masahiko Takenaka

Fujitsu Laboratories LTD.

Contents

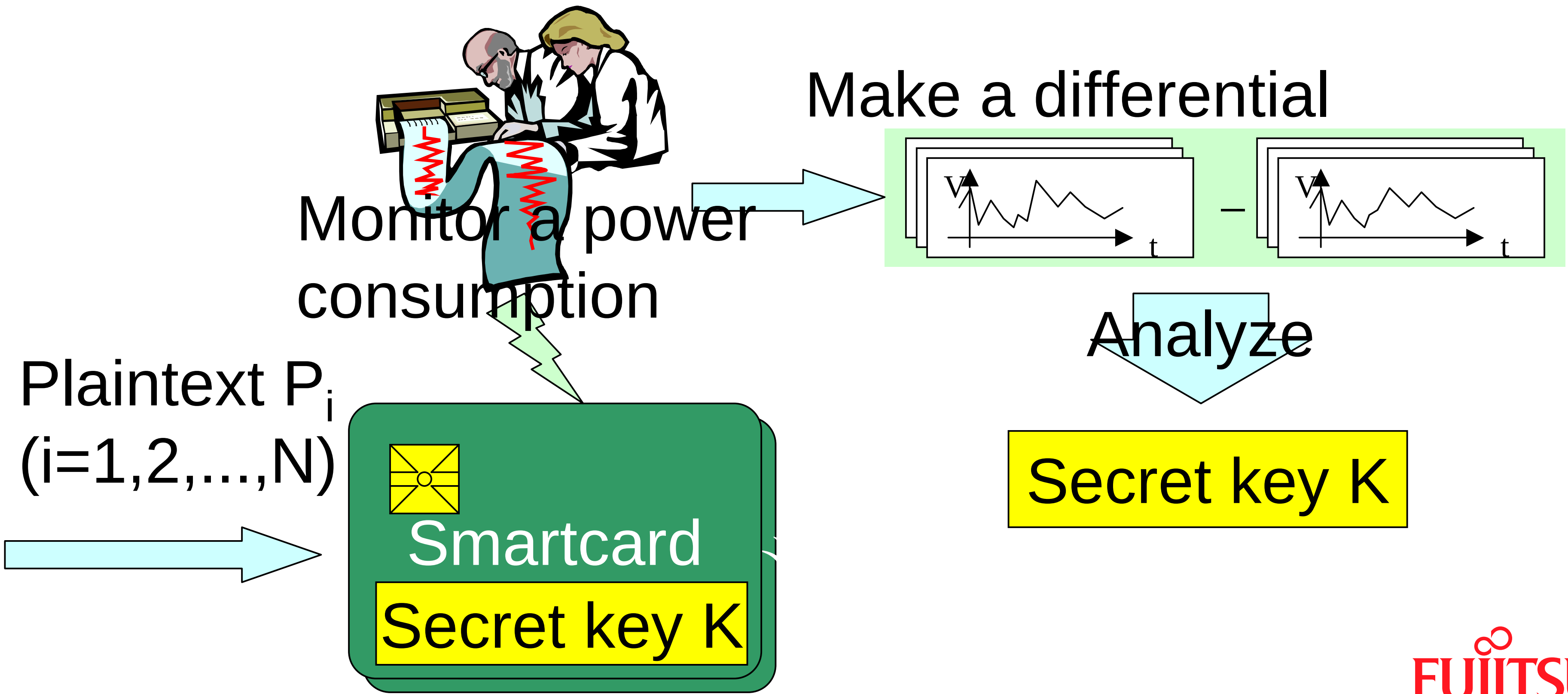
- What is DPA(Differential Power Analysis)?
- Data-bit DPA and Address-bit DPA
- Our Address-bit DPA Attack against OK-Schemes(OKS)
  - SE-attack
  - ZE-attack
- Our Experimental Result
- Countermeasures

FUJITSU

THE POSSIBILITIES ARE INFINITE

What is DPA? (Kocher, CRYPTO'99)

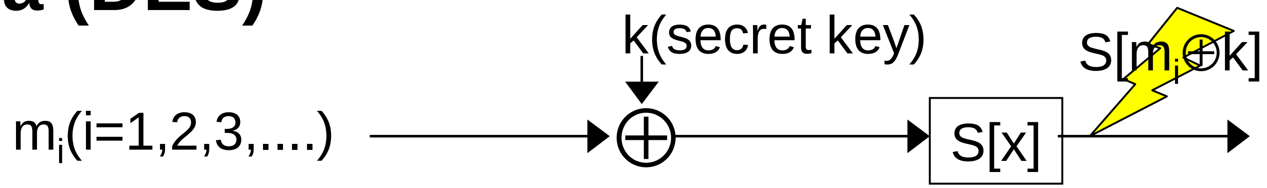
- **Analyze a secret key stored in the cryptographic device by monitoring its power consumption.**



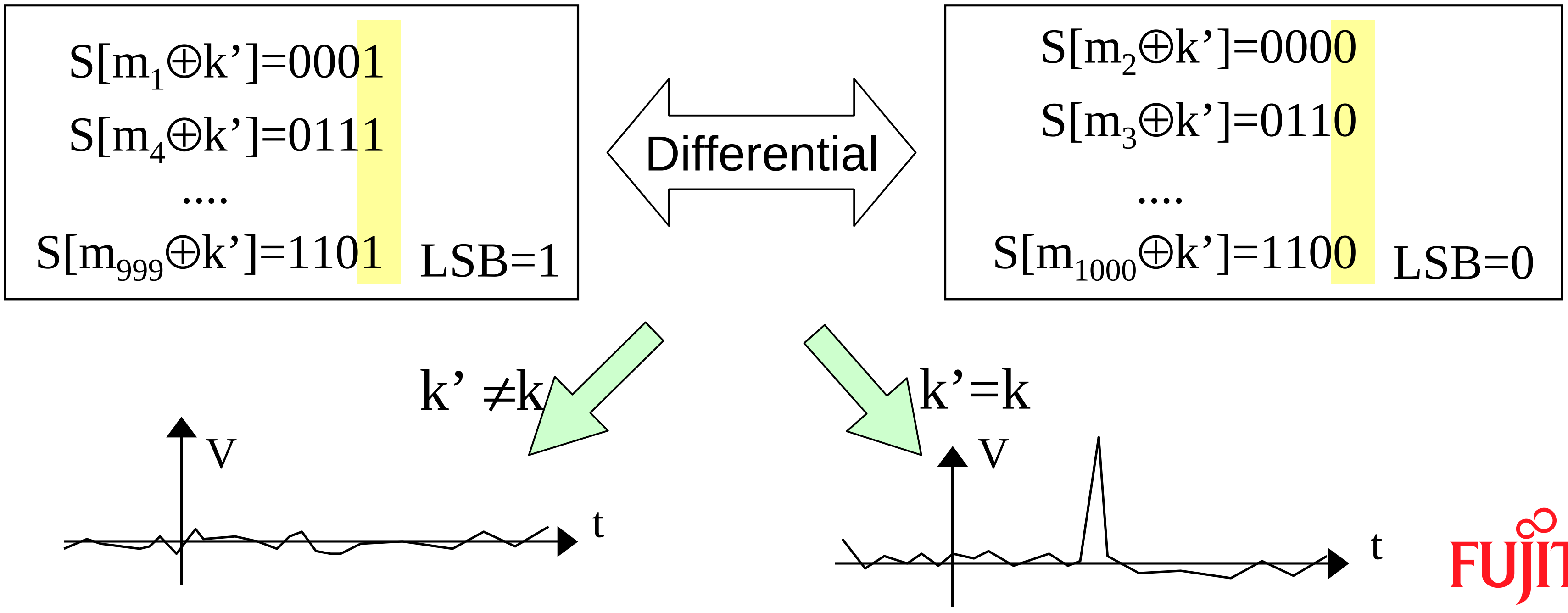
THE POSSIBILITIES ARE INFINITE

Data-bit DPA (Kocher, Crypto'99)

- Schema (DES)

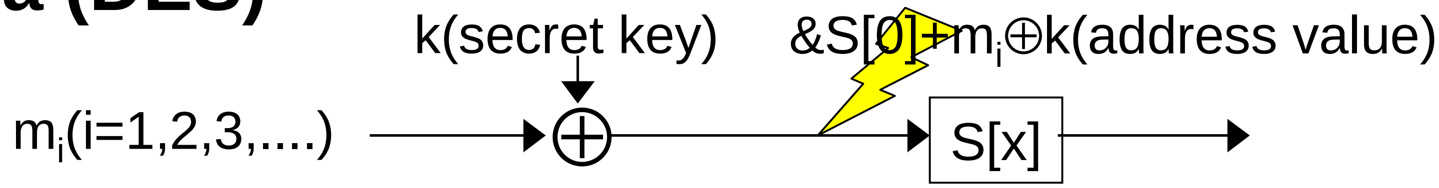


attacker guesses k'=k, then makes the differential for output value of Sbox



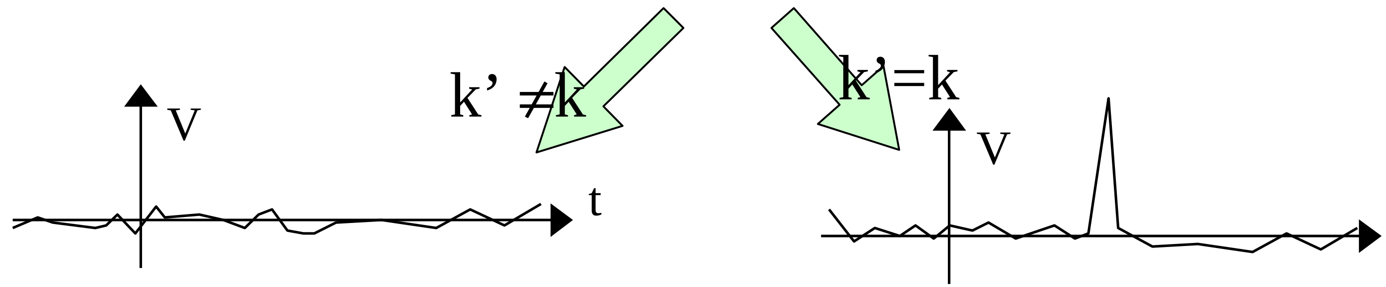
Address-bit DPA (Messerges, USENIX'99)

- Schema (DES)



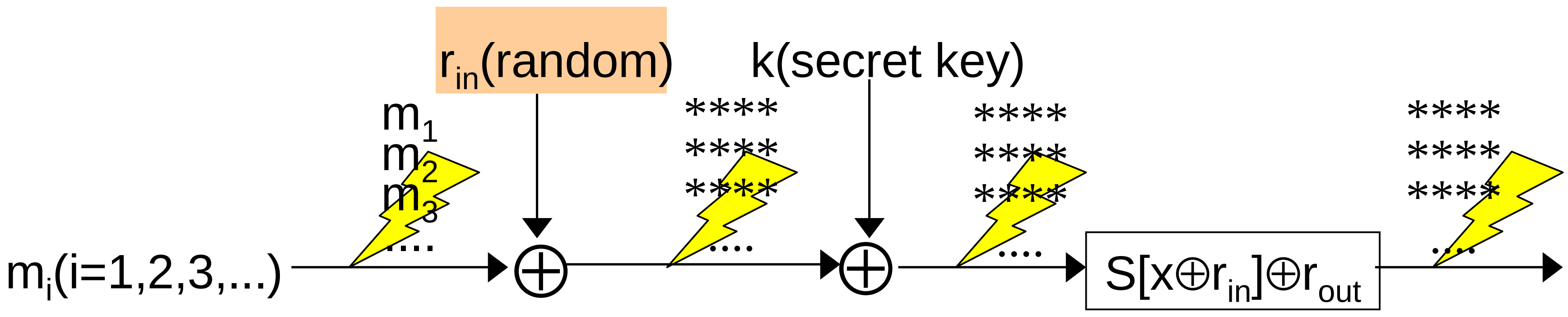
attacker guesses k'=k, then makes the differential for address value of Sbox

LSB=1		LSB=0
$\&S[0]+m_1 \oplus k' = 01010101$		$\&S[0]+m_2 \oplus k' = 01001100$
$\&S[0]+m_3 \oplus k' = 01111001$	Differential	$\&S[0]+m_4 \oplus k' = 01100110$
....		....
$\&S[0]+m_{999} \oplus k' = 01011101$		$\&S[0]+m_{1000} \oplus k' = 01110100$

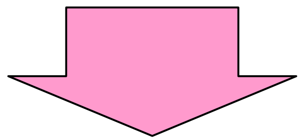


Masking Method on DES (Messerges, FSE 2000)

- **Countermeasure against DPA**



Data are blinded by the random number



DPA attack is prevented

THE POSSIBILITIES ARE INFINITE

Data-bit DPA vs Address-bit DPA in attacking DES

Normal

Sbox data S[x]

address	data
01101000	00110011
01101001	11011001
01101010	01011000

⇒ Data-bit DPA: ○
Address-bit DPA: ○

Masking Method

Sbox data
$S'[x]=S[x \oplus r_{in}] \oplus r_{out}$

address	data
********	********
********	********
********	********

⇒ Data-bit DPA: ×
Address-bit DPA: ×

Address-bit DPA is not more effective than data-bit DPA

FUJITSU
THE POSSIBILITIES ARE INFINITE

OKS (OK-ECDH/OK-ECDSA)

Cryptographic Schemes OKS

- Proposed by HITACHI
- Candidates of the CRYPTREC project in Japan
- Elliptic curve based schemes on Montgomery-form curves

Recommended Technology

- Montgomery ladder
- Randomized Projective Coordinate (RPC)

Scalar Multiplication in OKS(1)

- **Developer's claim :**
  - **Add-and-double-always chain**
    ⇒ Simple Power Analysis (SPA) protection
  - **Data are randomized by RPC**
    ⇒ DPA protection

```
Q[0] = P, Q[1] = ECDBL(P)
for i = n-2 downto 0 {
        Q[2] = ECDBL(Q[d_i])
        Q[1] = ECADD(Q[0], Q[1])
        Q[0] = Q[2–d_i], Q[1] = Q[1+d_i]
}
return Q[0]
```

⇒ "Secure against side channel attacks"

FUJITSU
THE POSSIBILITIES ARE INFINITE

Scalar Multiplication in OKS(2)

- Data are randomized by RPC

```
Q[0] = P, Q[1] = ECDBL(P)
for i = n-2 downto 0 {
        Q[2] = ECDBL(Q[d_i])
        Q[1] = ECADD(Q[0], Q[1])
        Q[0] = Q[2–d_i], Q[1] = Q[1+d_i]
}
return Q[0]
```

When d_i=0

	data
Q[0]	*********
Q[1]	*********
Q[2]	*********

When d_i=1

	data
Q[0]	*********
Q[1]	*********
Q[2]	*********

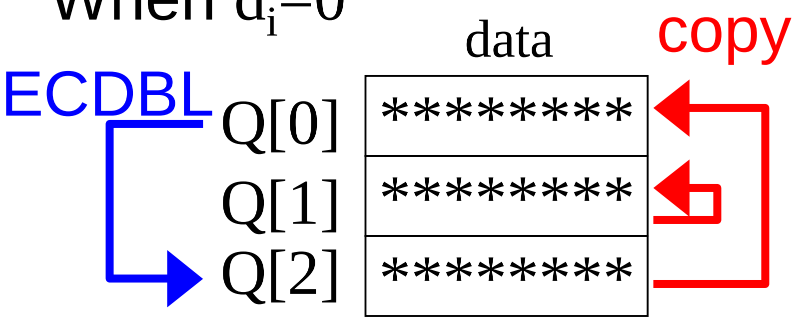
FUJITSU
THE POSSIBILITIES ARE INFINITE

Scalar Multiplication in OKS(2)

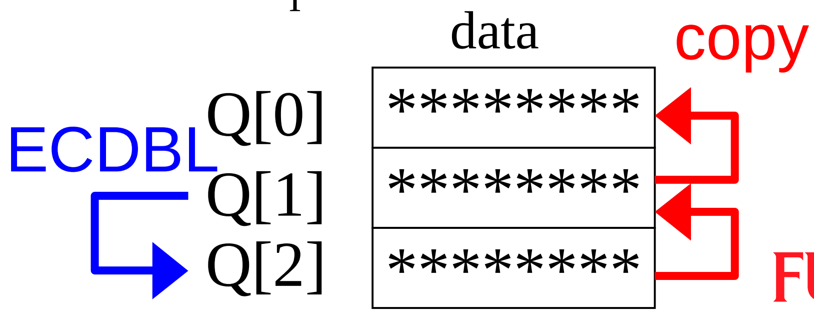
- **Data are randomized by RPC... but addresses are still correlated to the key bit d_i!**

```
Q[0] = P, Q[1] = ECDBL(P)
for i = n-2 downto 0 {
        Q[2] = ECDBL(Q[d_i])
        Q[1] = ECADD(Q[0], Q[1])
        Q[0] = Q[2–d_i], Q[1] = Q[1+d_i]
}
return Q[0]
```

When d_i=0



When d_i=1

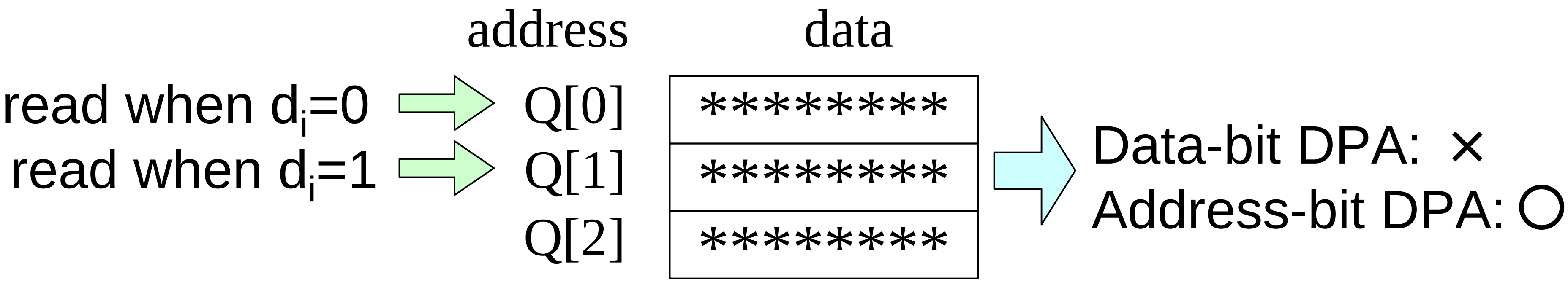


FUJITSU

THE POSSIBILITIES ARE INFINITE

Basic Idea of Our Attack

- **Analyze the correlation between address value and key bit d_i**



Address-bit DPA is effective!

Our Attack against OKS Scalar Multiplication

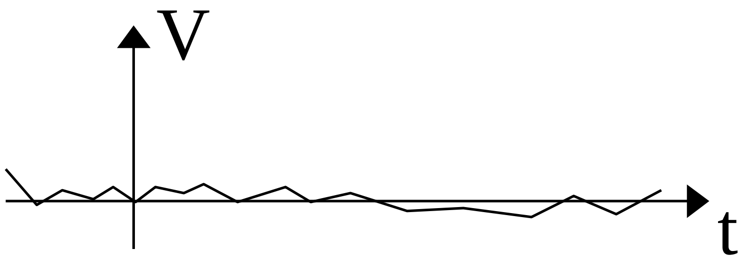
- **Basic strategy**

$Q[2] = ECDBL(Q[d_A])$
$Q[1] = ECADD(Q[0], Q[1])$
$Q[0] = Q[2-d_A], Q[1] = Q[1+d_A]$

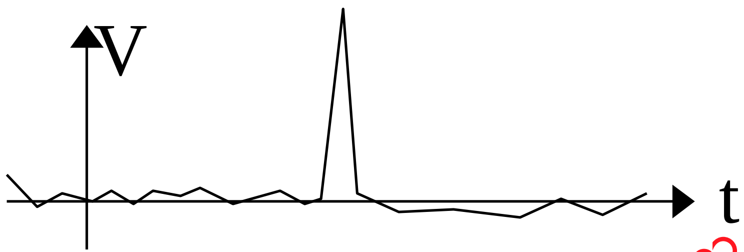
⇔ Differential

$Q[2] = ECDBL(Q[d_B])$
$Q[1] = ECADD(Q[0], Q[1])$
$Q[0] = Q[2-d_B], Q[1] = Q[1+d_B]$

If $d_A = d_B$



If $d_A \neq d_B$



THE POSSIBILITIES ARE INFINITE

Fundamental Experiment

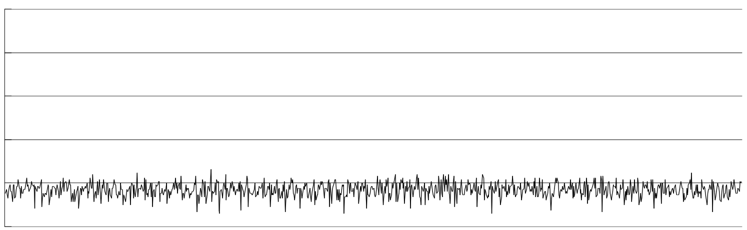
Validity of the attack

st [addr A], (random data)
....
ld A, [addr A]
....

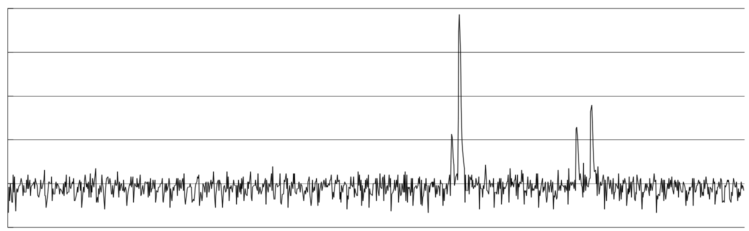
Differential

st [addr B], (random data)
....
ld A, [addr B]
....

Same address (A = B)



Different address (A ≠ B)



Average of loading 500 random data

THE POSSIBILITIES ARE INFINITE

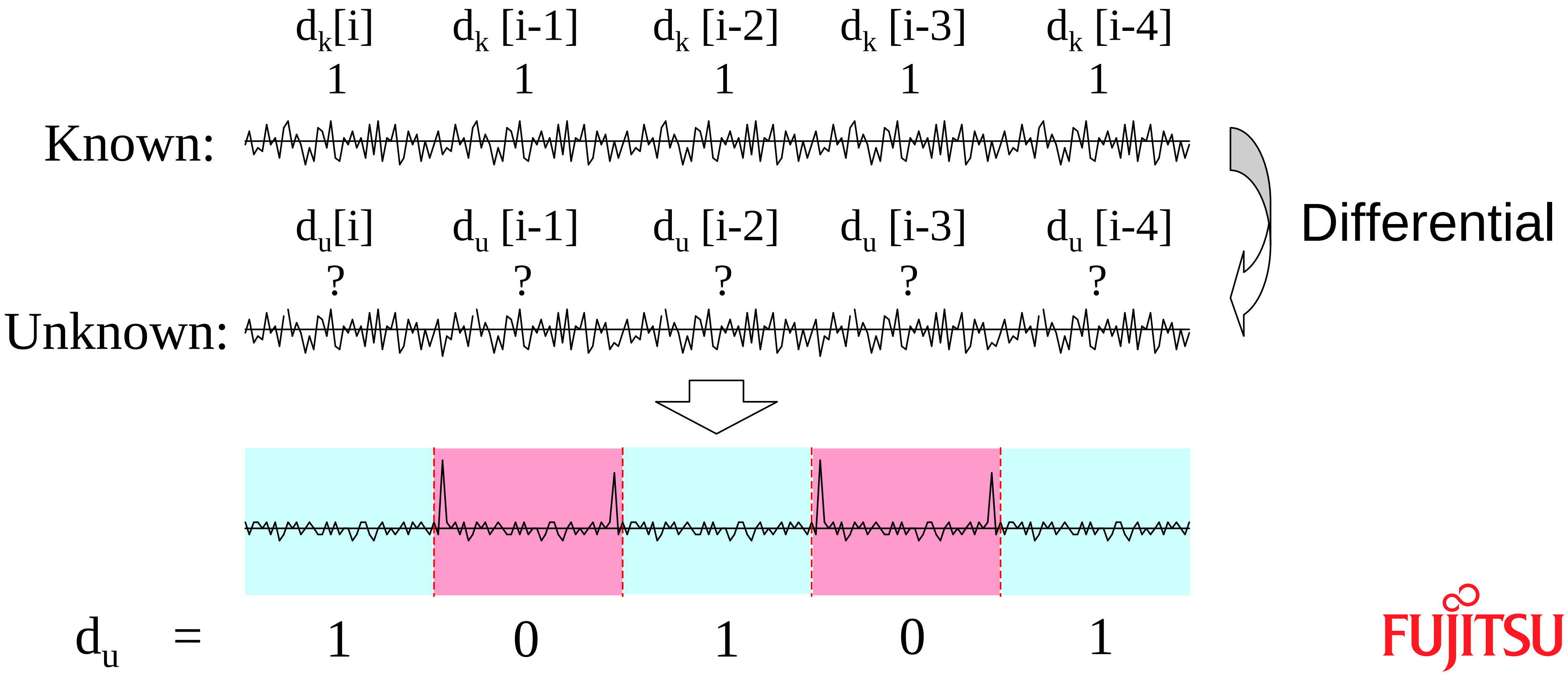
Our attack

- **Single-Exponent attack (SE-attack)**
  - Attacker has an averaged power trace for a known exponent, and collects that for an unknown exponent
- **Zero-Exponent attack (ZE-attack)**
  - Attacker collects an averaged power trace for an unknown exponent
  - Power trace should be segmented by each key bit operation

Attack (1): SE-attack

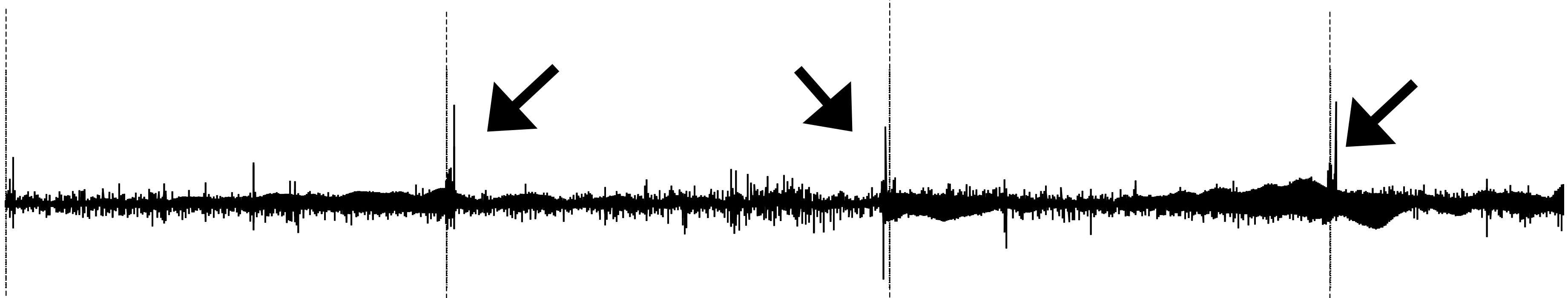
Schema

- Using an difference between a averaged power trace with known exponent and that with unknown exponent.



Experimental Result of SE-attack

- d_k: known exponent, d_u: unknown exponent



$d_u[n-1] = d_k[n-1]$ $d_u[n-2] \neq d_k[n-2]$ $d_u[n-3] = d_k[n-3]$

- We know d_k=1111… ⇒ We obtain d_u = 1010…

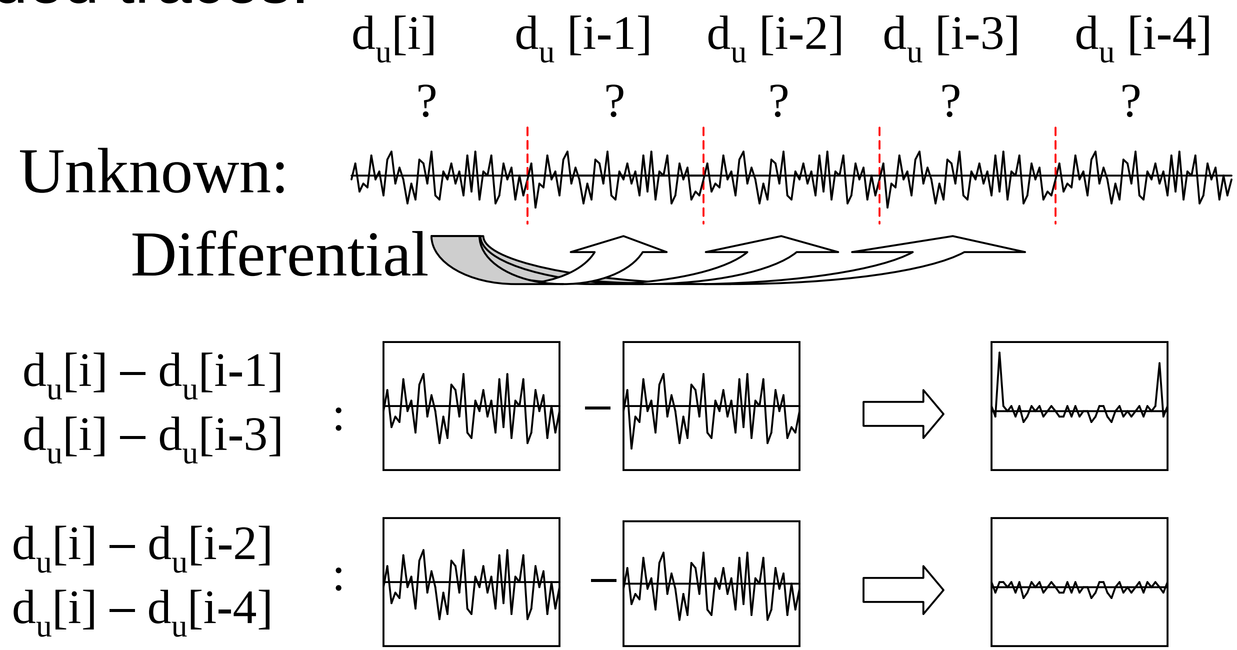
FUJITSU

THE POSSIBILITIES ARE INFINITE

Attack (2): ZE-attack

Schema

- Dividing an averaged power trace with unknown exponent at each processing of $d_u[i]$, and using a difference the divided traces.



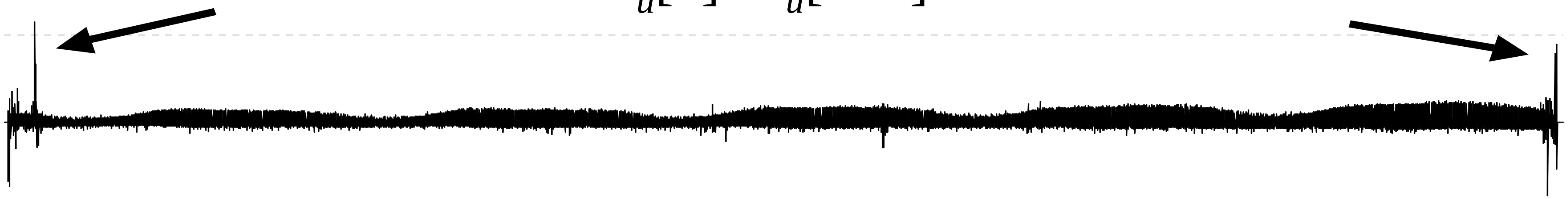
$d_U = 1\ 0\ 1\ 0\ 1\ \ldots$

THE POSSIBILITIES ARE INFINITE

Experimental Result of ZE-attack

$d_u[n] \neq d_u[n-1]$

$d_u[n] = d_u[n-2]$



$d_u[n] \neq d_u[n-3]$

We obtain d_u=1010...

Other Implementation

- **Address Swapping** ⇒ Enable (See our paper)

```
for i = n-2 downto 0 {
        Q[2] = ECDBL(Q[d_i])
        Q[1] = ECADD(Q[0], Q[1])
        Swap(&Q[0], &Q[2–d_i]), Swap(&Q[1], &Q[1+d_i])
}
```

- **Two Variables** ⇒ Easier (More spikes will appear)

```
for i = n-2 downto 0 {
        Q[1–d_i] = ECADD(Q[0], Q[1])
        Q[d_i] = ECDBL(Q[d_i])
}
```

FUJITSU

THE POSSIBILITIES ARE INFINITE

Countermeasures

- **Countermeasures against Proposed Attack**
  - Randomized Scalar
    - Scalar Blinding, Coron (CHES'99)

$$d \rightarrow d + r\phi$$

    - Scalar Splitting, Clavier-Joye (CHES'01)

$$d \rightarrow r + (d - r)$$

  - Overlapping Window, Itoh et al. (CHES'02)

d	1	0	1	1	0	1	1	1	0	1
w_0	1	0	1	0						
w_1			0	1	0	0				
w_2					0	1	1	0		

FUJITSU
THE POSSIBILITIES ARE INFINITE

Conclusion

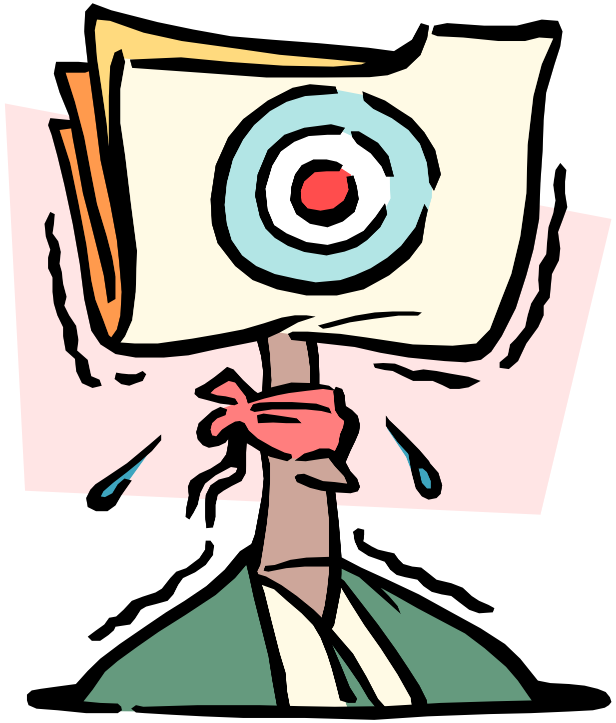
- **We proposed new address-bit DPA, and attacked against OKS**
- **We proved the validity of our attacks with experimental results**
- **OKS is not secure against address-bit DPA**
- **For securing against DPA, not only data value, but also data access procedure must be irrelevant to secret key value**

THE POSSIBILITIES ARE INFINITE

FUJITSU

THE POSSIBILITIES ARE INFINITE

Questions & Comments



THE POSSIBILITIES ARE INFINITE