FUJITSU THE POSSIBILITIES ARE INFINITE

www.fujitsu.com

DPA Countermeasures by Improving the Window Method

Kouichi Itoh, Jun Yajima, Masahiko Takenaka and Naoya Torii

Fujitsu Laboratories LTD.

Contents

- What is DPA?
- Previous DPA countermeasures
- Our DPA countermeasures
- Security of our countermeasures
- Performance comparison with other countermeasures

FUJITSU

THE POSSIBILITIES ARE INFINITE

Overview

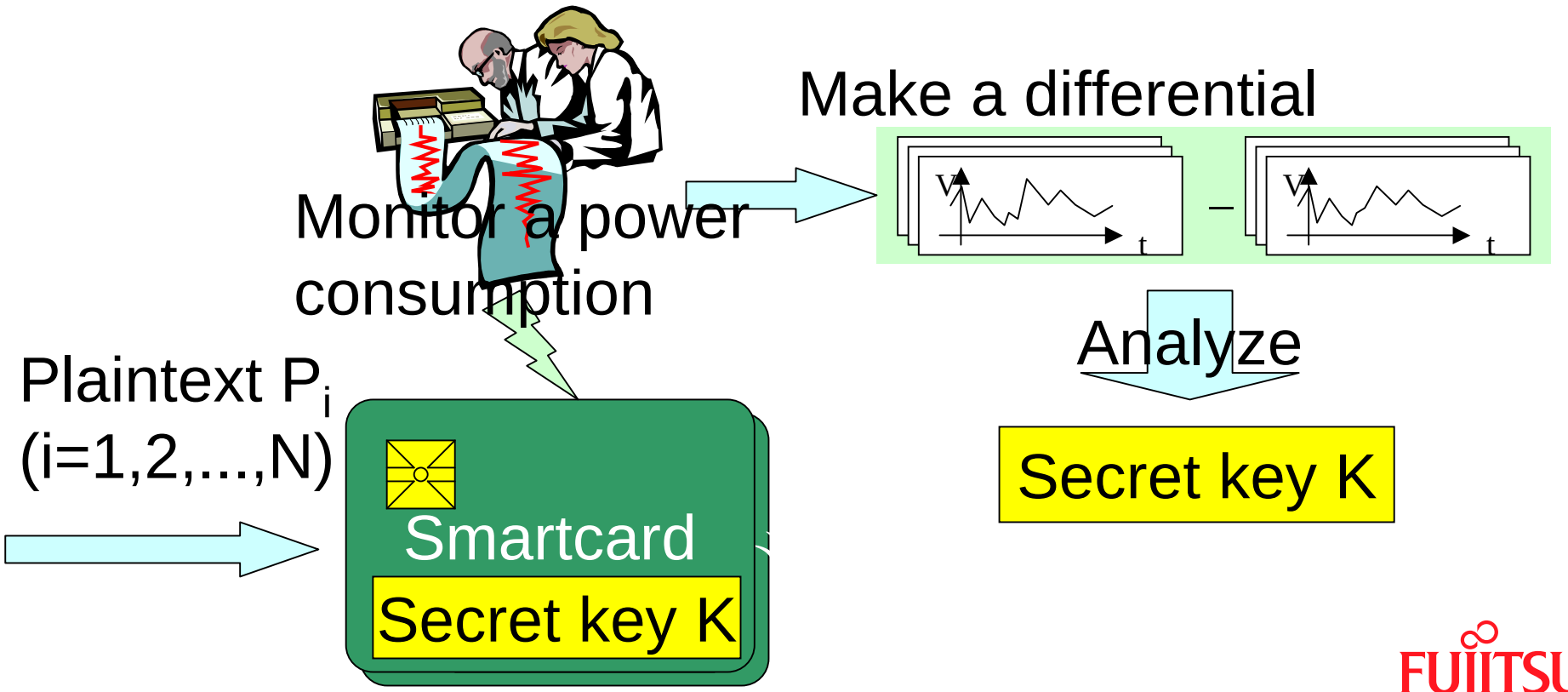
- Objectives
  - Proposal of new effective DPA countermeasure(s) for public key cryptosystems
- Characteristics
  - Fast encryption speed
  - No additional parameter
  - Applicable in both RSA and ECC

FUJITSU

THE POSSIBILITIES ARE INFINITE

What is DPA? (Differential Power Analysis)

- Analyze a secret key stored in the cryptographic device by monitoring its power consumption. (Kocher, CRYPTO'99)



Previous DPA Countermeasures for public key Cryptosystems

- Randomization of the private exponent (Coron, CHES'99)
  - $d \Rightarrow d' = d + r \times \phi$ (r:random, ϕ:order)
- Randomized binary-method (Messerges-Dabbish-Sloan, CHES'99)
  - $d =$ 1 0 1 0 0 0 1 1 0 1 0 1 1 1 0 1 1 1 0 1 0 1 0

    LSB-to-MSB binary-method ← | → MSB-to-LSB binary-method

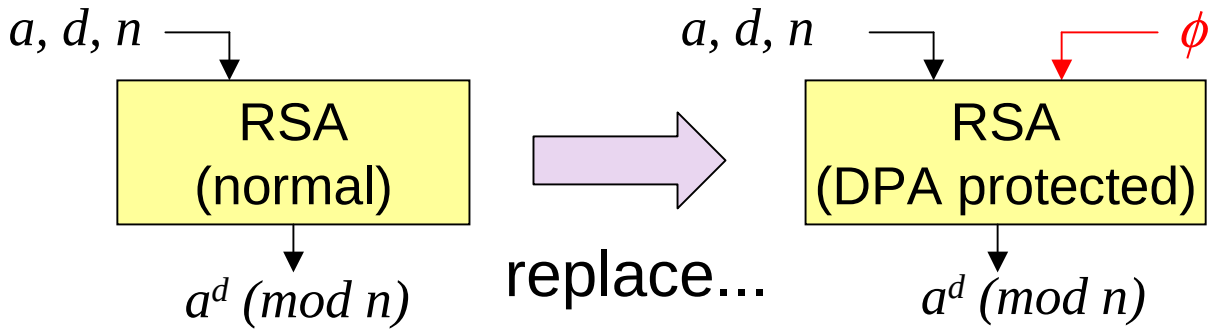
    randomly choose
- Exponent splitting (Clavier-Joye, CHES2001)
  - $d = d_1 + d_2$, $a^d = a^{d_1} \times a^{d_2} \pmod{n}$, ($d_1, d_2$:random)
- Randomized projective coordinates (Coron, CHES'99)
  - $(x,y) \Rightarrow (x \times r, y \times r, z \times r)$ (r:random)

FUJITSU

THE POSSIBILITIES ARE INFINITE

Demerits of Previous DPA Countermeasures

- Slow encryption speed (Clavier-Joye, Messerges)
  - Exponent splitting technique takes 2 times computation.
- Additional parameter is required(Coron)
  - When randomizing the private exponent, parameter ϕ is used.



- Not applicable to both RSA and ECC(Coron)
  - Randomized projective coordinates technique is available only in ECC.

FUJITSU

THE POSSIBILITIES ARE INFINITE

Merits of Our Countermeasures

- Fast encryption speed (Overhead is low)
  - In comparison with k-ary method, computational complexity is 105% in 1024-bit RSA, and is 119% in 160-bit ECC
- No additional parameter
  - Vulnerable encrypt engine is easily replaced to secure one
- Applicable to both RSA and ECC
  - All countermeasures are based on the window method

FUJITSU

THE POSSIBILITIES ARE INFINITE

Our DPA Countermeasures

- We propose 3 countermeasures:
  - Overlapping Window Method(O-WM)
  - Randomized Table Window Method(RT-WM)
  - Hybrid Randomizing Window Method(HR-WM)
- Each has unique characteristics (speed, security)

  ⇒ A suitable countermeasure can be chosen according to the environment (encryption algorithm, key length...)

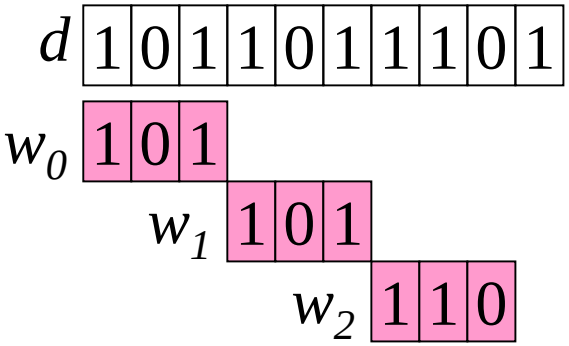
FUJITSU

THE POSSIBILITIES ARE INFINITE

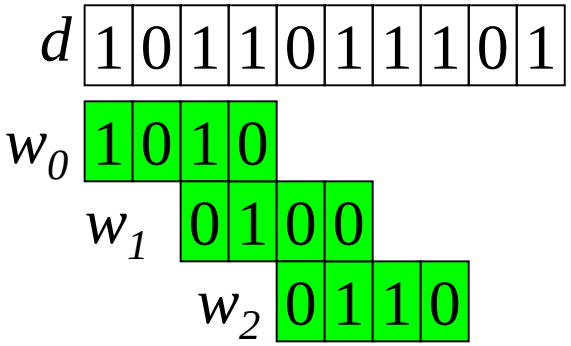
Overlapping Window Method(O-WM)

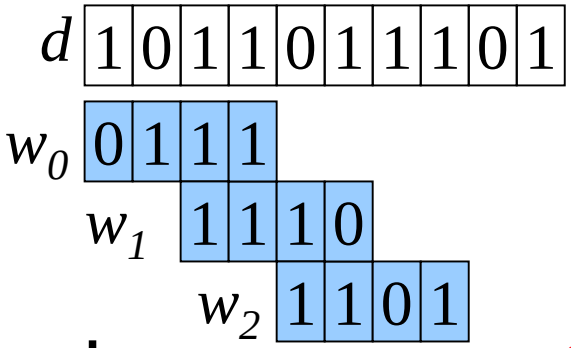
Basic idea

Traditional WM



By overlapping w_i and w_{i+1}, various expressions are possible.





Data is randomized.

Randomized Table Window Method (RT-WM)

Basic idea

Traditional WM

d 1 0 1 1 0 1 1 1 0 1

w_0 1 0 1

w_1 1 0 1

w_2 1 1 0

Table lookup: $tab[i] = a^i \ (mod\ n)$

a^{000}	a^{100}
a^{001}	a^{101}
a^{010}	a^{110}
a^{011}	a^{111}

Randomize

RT-WM

d 1 0 1 1 0 1 1 1 0 1

r: 0 1 1 (random)

w_0 1 0 1 0 1 1

w_1 0 1 0 0 1 1

w_2 0 1 1 0 1 1

Table lookup : $tab[i] = a^{i \times 2^3 + r} \ (mod\ n)$

$a^{000000+r}$	$a^{100000+r}$
$a^{001000+r}$	$a^{101000+r}$
$a^{010000+r}$	$a^{110000+r}$
$a^{011000+r}$	$a^{111000+r}$

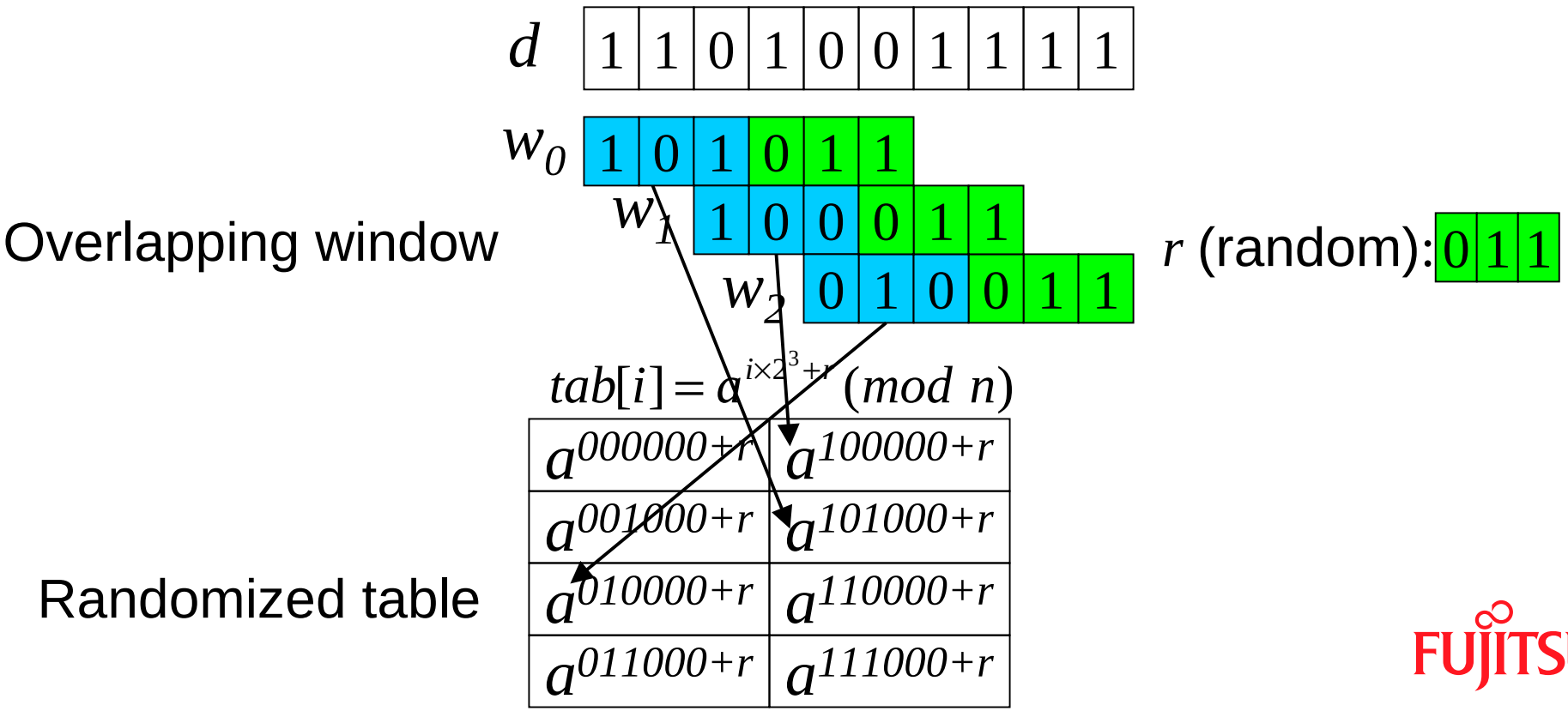
Data is randomized.

FUJITSU

THE POSSIBILITIES ARE INFINITE

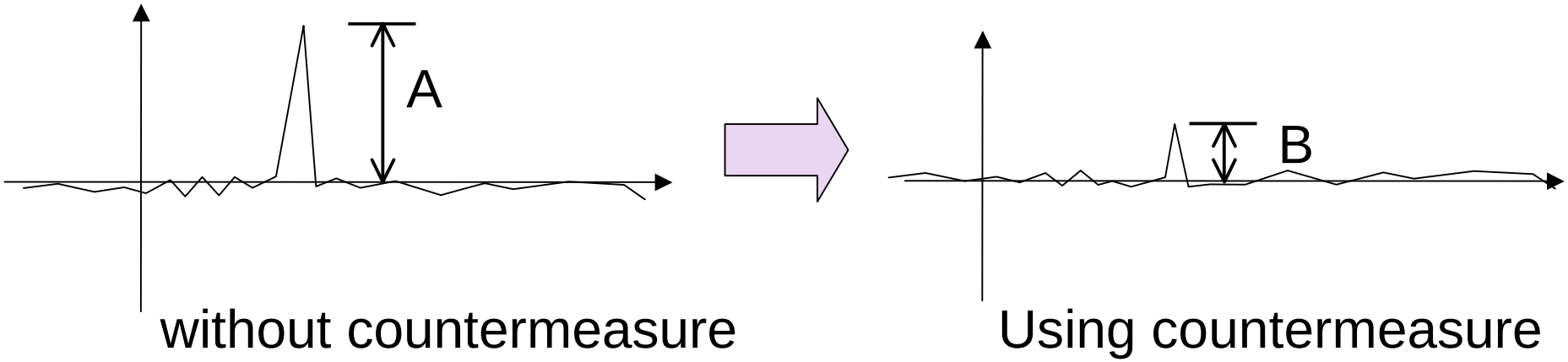
Hybrid Randomizing Window Method (HR-WM)

- HR-WM = O-WM + RT-WM
  = (Overlapping) + (Randomized Table)



Security Evaluation of Our Countermeasures

- Basic idea



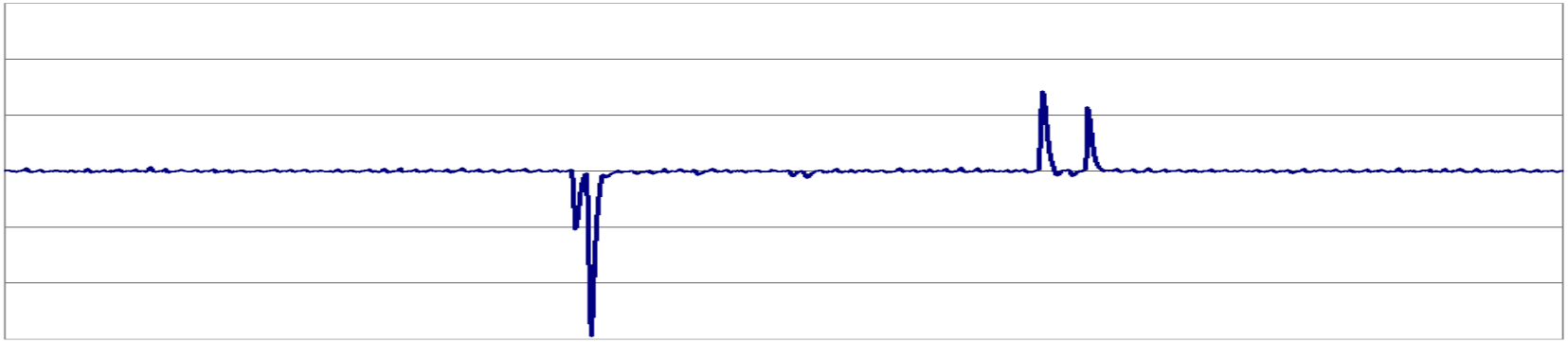
Size of the spike will be smaller by the countermeasure

Security is evaluated by the ratio of the sizes.
(attenuation ratio = B/A)

FUJITSU
THE POSSIBILITIES ARE INFINITE

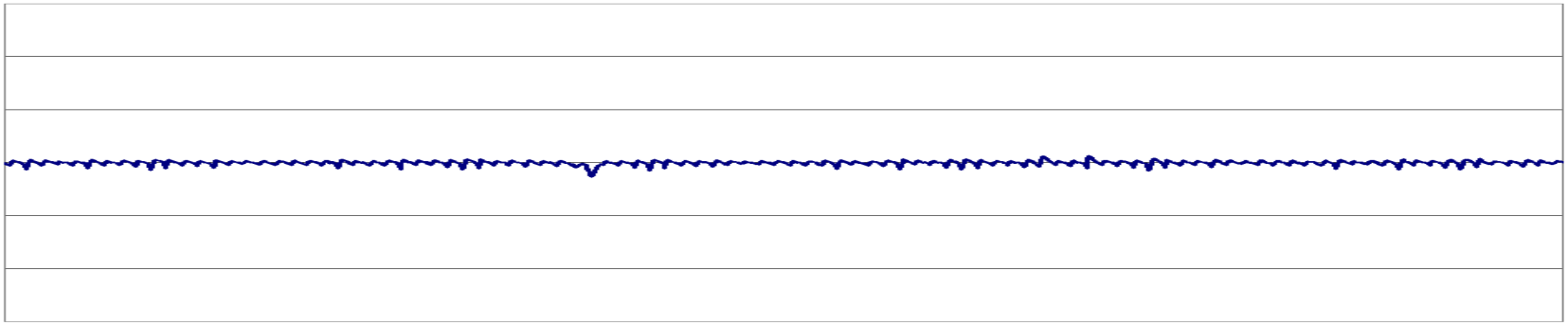
DPA Attack Experiment

- RSA(Normal)



- RSA(O-WM)

attenuation ratio=1/10



FUJITSU

THE POSSIBILITIES ARE INFINITE

Security Evaluation Result

Attenuation Ratio(AR) for a fixed parameter

	RSA ECC(2D)	ECC(3D)
O-WM	$2^{-2.6}$~$2^{-7.2}$(*)	$2^{-2.6}$~2^{-80}(*)
RT-WM	2^{-20}	2^{-20}
HR-WM	2^{-11}	2^{-11}~2^{-61} (*)

ECC(2D) : An implementation using affine coordinates
ECC(3D) : An implementation using projective or Jacobian coordinates

(*) : The reason why AR varies, is described in the paper

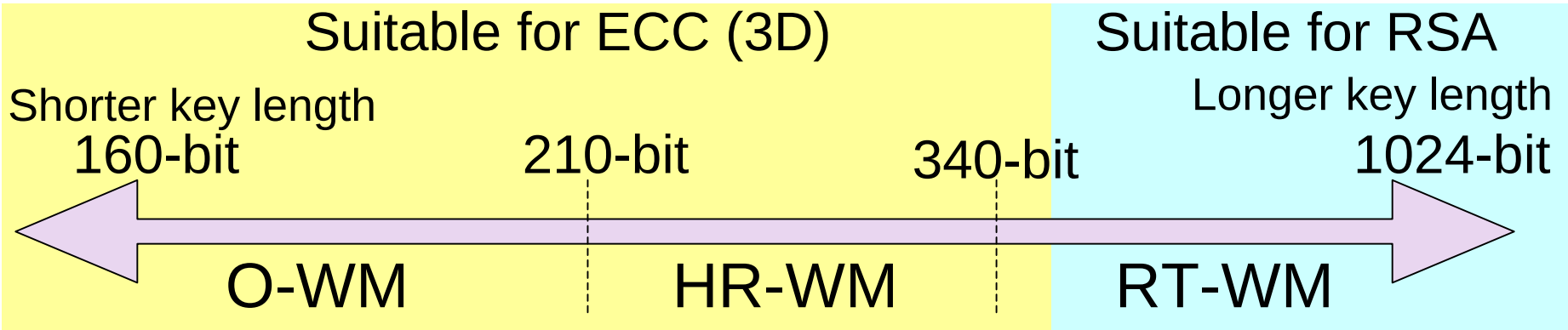
FUJITSU

THE POSSIBILITIES ARE INFINITE

Performance Comparison among Our Countermeasures

		O-WM	HR-WM	RT-WM
ECC(3D) (160-bit)	TIME	256	264	279
	AR	$\sim 2^{-80}$	$\sim 2^{-61}$	2^{-20}
RSA (1024-bit)	TIME	1552	1416	1359
	AR	$\sim 2^{-7.2}$	2^{-11}	2^{-20}

TIME:number of addition/doubling(ECC) or multiplication/squaring(RSA)



FUJITSU

THE POSSIBILITIES ARE INFINITE

Comparison with Other Countermeasures

		O-WM	HR-WM	RT-WM	Coron	Messerges
ECC(3D) (160-bit)	TIME	256	264	279	241	214
	AR	$\sim 2^{-80}$	$\sim 2^{-61}$	2^{-20}	2^{-20}	$2^{-7.3}$
RSA (1024-bit)	TIME	1552	1416	1359	1321	1536
	AR	$\sim 2^{-7.2}$	2^{-11}	2^{-20}	2^{-20}	2^{-10}
Additional Parameter		**No**	**No**	**No**	**Yes**	**No**

TIME:number of addition/doubling(ECC) or multiplication/squaring(RSA)

Proposed and Coron : 4-bit window, Messerges : binary-method(RSA) or signed-binary(ECC)

vs Coron : Additional parameter is unnecessary

vs Messerges : Much higher security in ECC,

higher security and 13% faster in RSA

FUJITSU

THE POSSIBILITIES ARE INFINITE

Conclusion

- We proposed new DPA countermeasures, O-WM, RT-WM and HR-WM
  - Fast encryption speed
  - No Additional parameter
  - Applicable to both RSA and ECC
- We evaluated the security by attenuation ratio
  - ECC : All countermeasures provide enough security
  - RSA : RT-WM and HR-WM provide enough security

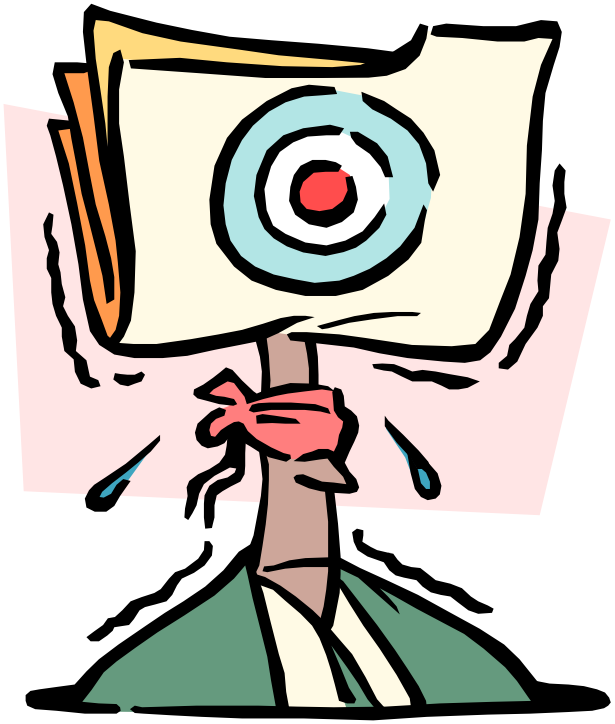
FUJITSU

THE POSSIBILITIES ARE INFINITE

FUJITSU

THE POSSIBILITIES ARE INFINITE

Questions & Comments



FUJITSU

THE POSSIBILITIES ARE INFINITE