A More Flexible Countermeasure against Side Channel Attacks using Window Method

Hitachi Ltd.

TU Darmstadt
Germany

Abstract

Motivation	- Cryptography is a key technology for ubiquitous computing. - It requires memory-constraint devices.
Problem	Side channel attacks are able to break the implementation of cryptography on memory-constraint devices.
Result	We introduce a new computation of ECC, in which we can freely choose the table size without losing its security.

Contents

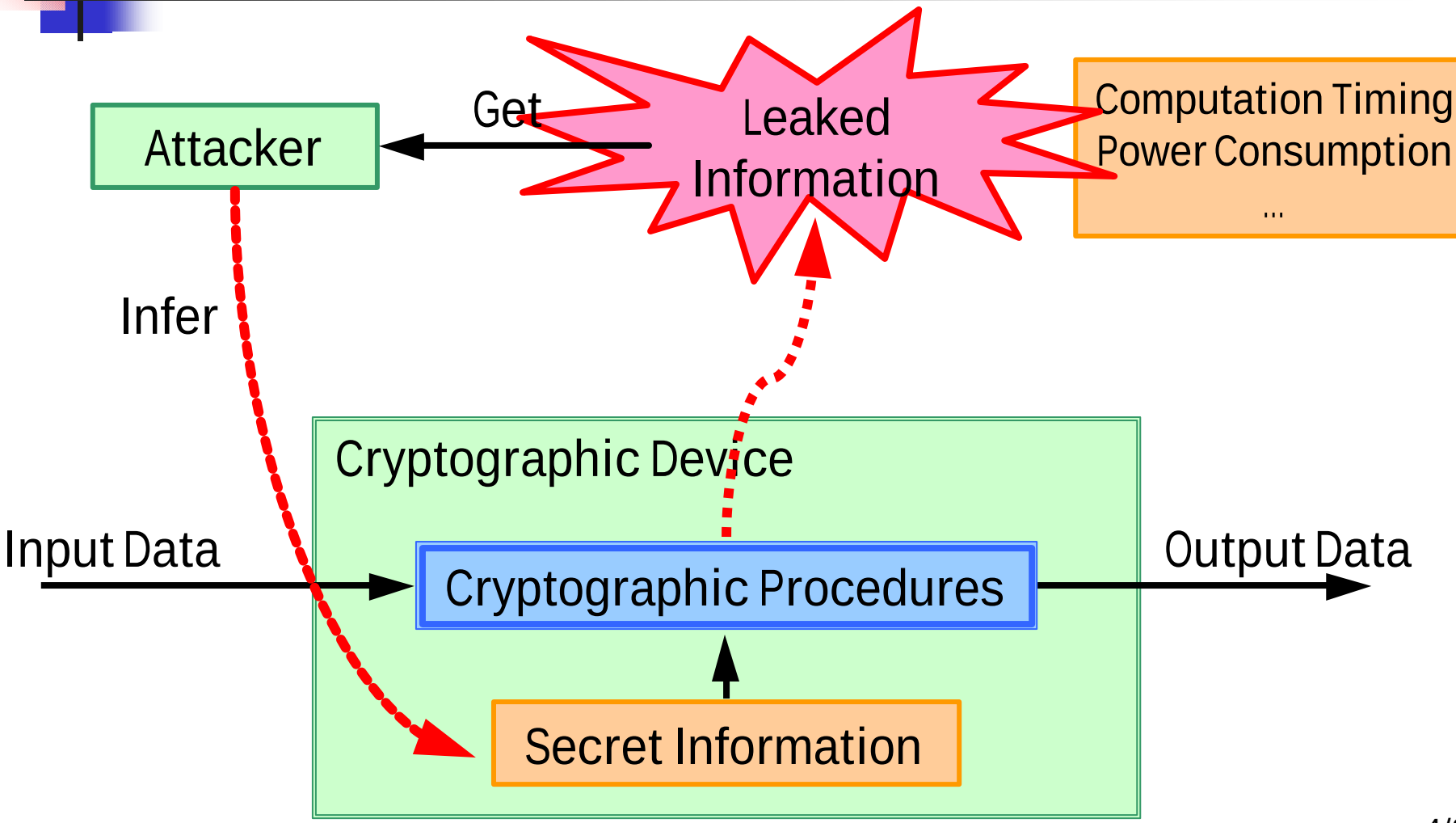
Side Channel Attacks

Known Countermeasures

Proposed Countermeasure

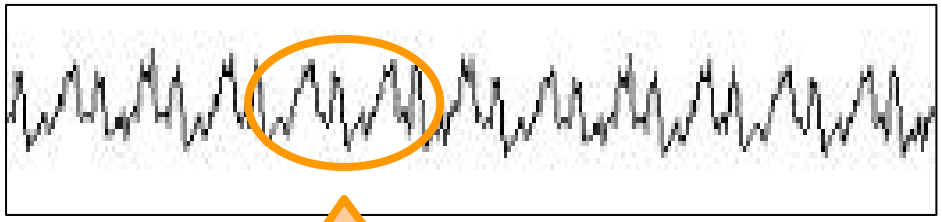
Side Channel Attacks

[Koc96,KJJ99]



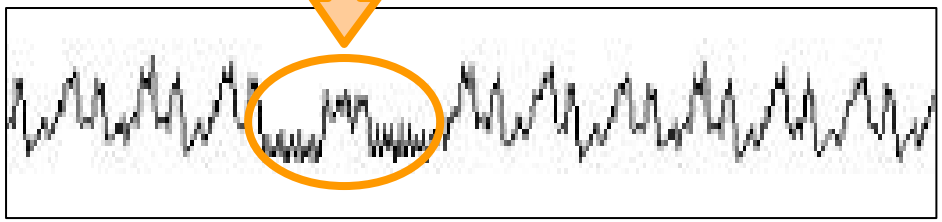
How to Infer the Secret Information

Power consumption that a specific bit of secret information is 1



Different

Power consumption that a specific bit of secret information is 0



SPA: Directly distinguish the cases using (single) measurement

DPA: Distinguish the cases using averaging trick of noise elimination

SPA against Binary Method

Binary Method

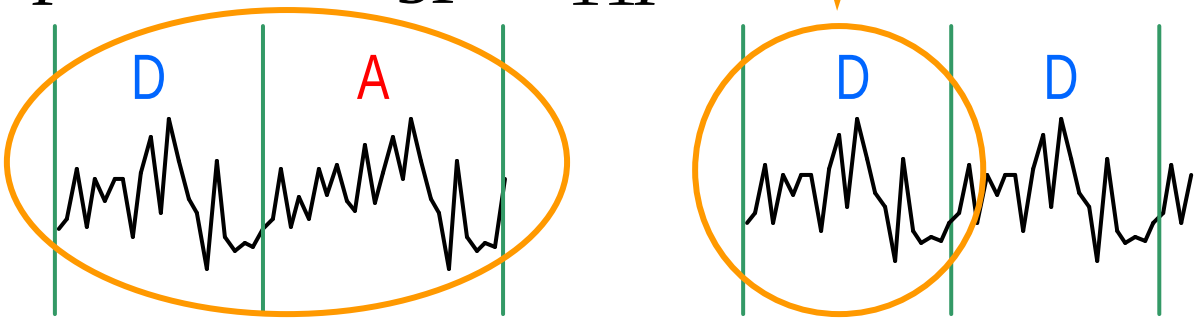
$d = 89 = (1011001)_2$

Q → Q+P Addition Q+P

Q → 2Q Doubling 2Q

Secret

d	1	0	1	1	0	0	1
O	O	$2P$	$4P$	$10P$	$22P$	$44P$	$88P$
P	P		$5P$	$11P$			$89P$



Binary method is vulnerable to SPA

Coron's SPA Countermeasure [Cor99]

Binary + Dummy operations

$d = 89 = (1011001)_2$

Q → Q+P Addition Q+P

Q → 2Q Doubling 2Q

d	1	0	1	1	0	0	1
O	O	$2P$	$4P$	$10P$	$22P$	$44P$	$88P$
P	P	$3P$	$5P$	$11P$	$23P$	$45P$	$89P$

D A D A D A D A D A D A

Always add and double per bit, the result is discarded if the bit is 0 → SPA immune

Contents

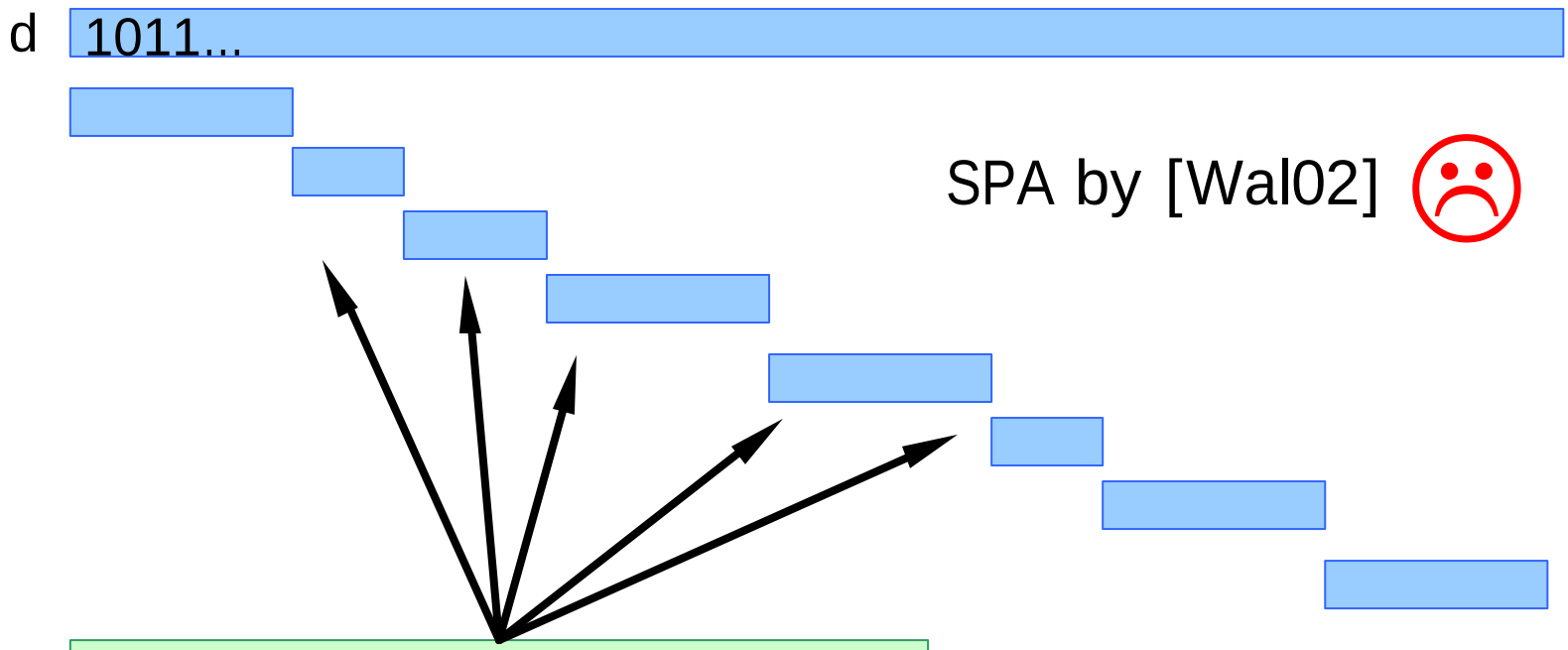
Known Countermeasures

- Window Method based Countermeasures -

(1) Randomized Window Method
(2) Overlapping Window Method
(3) Window Method with Dummy Addition
(4) Parallelizable Window Method
(5) Non-Zero Window Method
(6) wNAF Method

Randomized Window Method

[LS01]

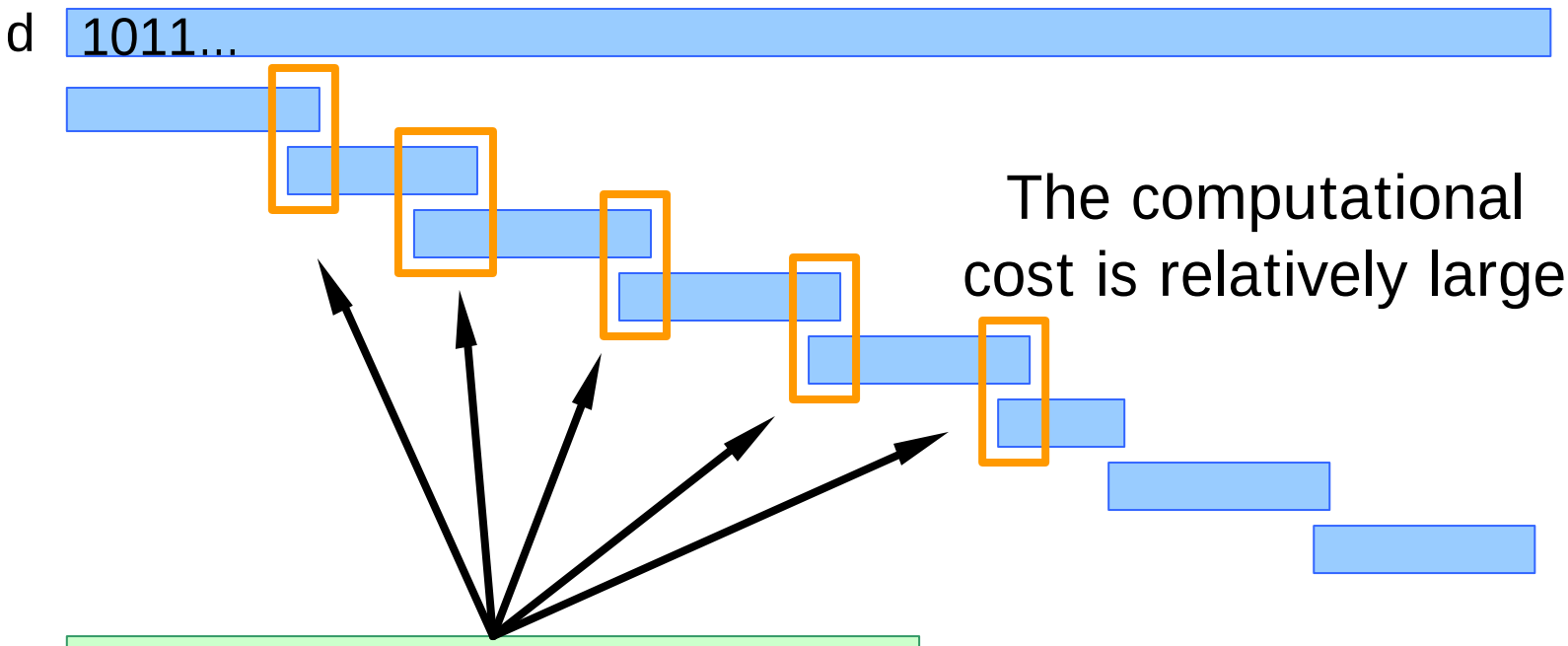


SPA by [Wal02] ☹

The length of the target window is randomly chosen

Overlapping Window Method

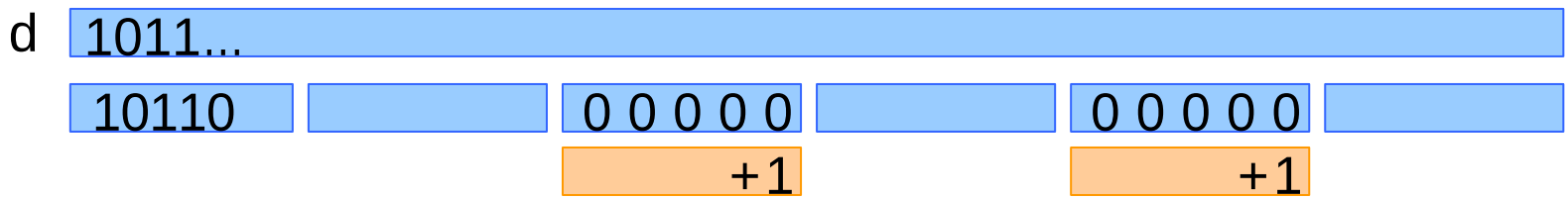
[IYTTO



The computational cost is relatively large

Windows are overlapped with random mask

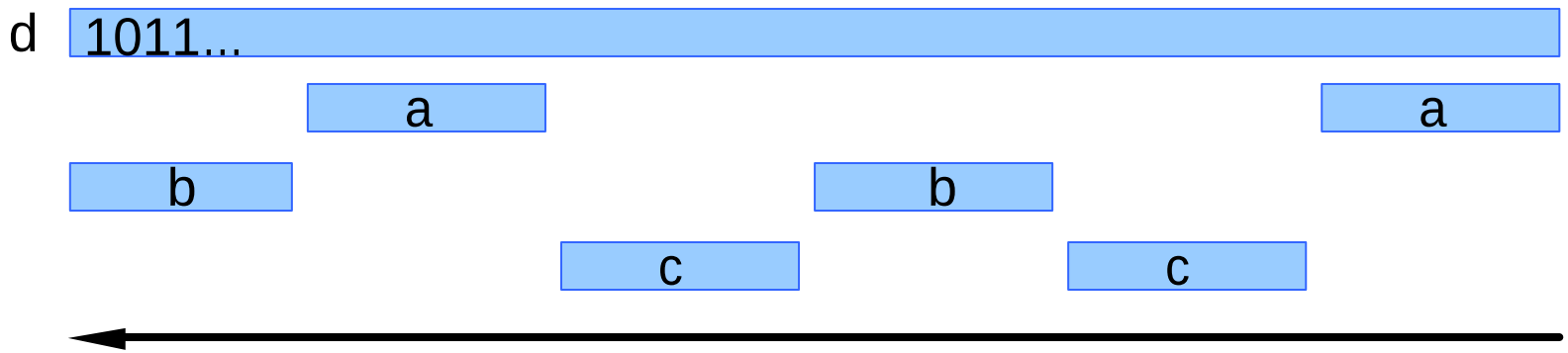
Window Method with Dummy Addition



Safe error attack
[YKLM01]

Dummy addition is performed if the value of window is 0

Parallelizable Window Method [Möl02

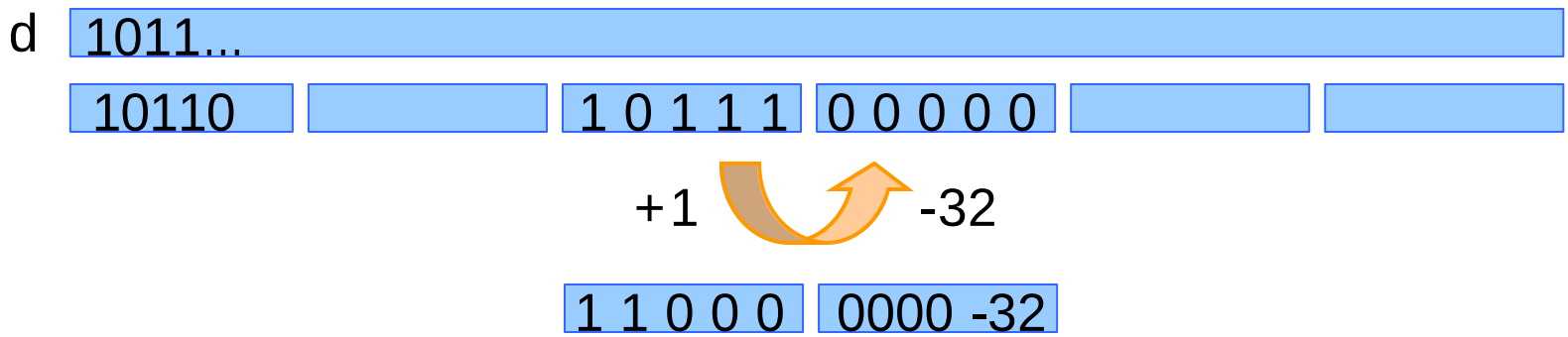


Total computational cost increases

Computation is parallel and right-to-left

Non-Zero Window Method

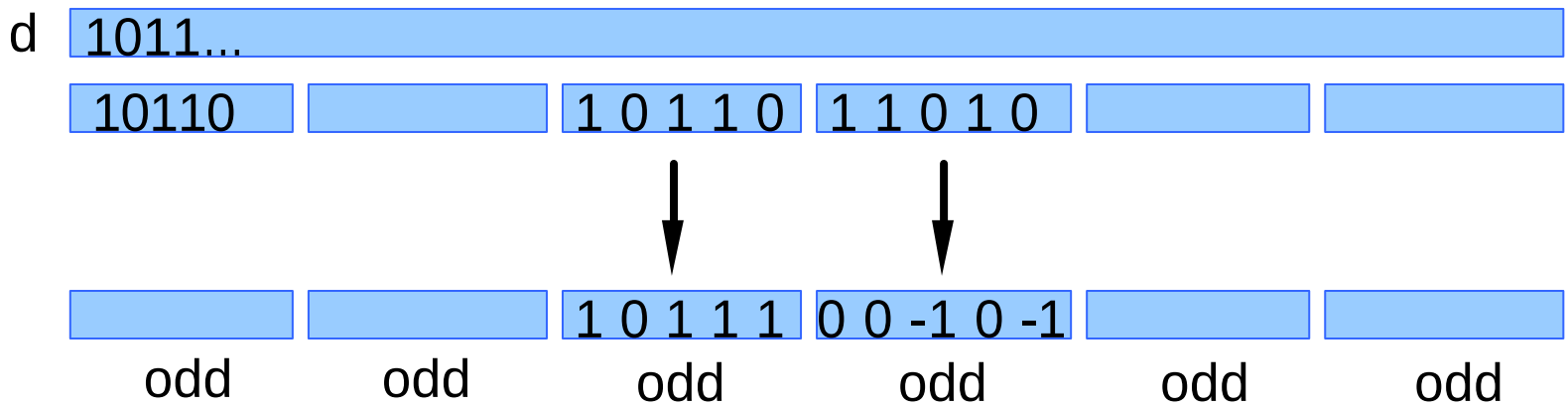
[Möl0



Speed is optimal ☺

0-value window is converted to non-zero window

wNAF Method



[OT03a

Memory and speed are optimal

Every windows are converted to odd-value windows

Types of Countermeasures

Randomized addition chains type	Randomized window method Overlapping window method	[LS01] [IYTT02]
New Type !		
Fixed probability type	Our proposed method	[OT03b]
Fixed procedure type	Dummy Addition Parallelizable Window Method Non-Zero window method wNAF method	[Cor99] [Möl02] [Möl01] [OT03a]
SPA countermeasure	SPA & DPA countermeasure	

Contents

Proposed Countermeasure

Motivation & Problem

Motivation

- Available memory on devices depends on individual situations
- Cryptosystems should be adjusted to such situations

Problem

To construct a countermeasure with the followings:

- The size of pre-computed table can be freely chosen
- The speed should be optimal
- Of course, prevent against side channel attacks

The proposed countermeasure is converted from wNAF method

Our Achievement

If we allow to use only 300 bytes, ...

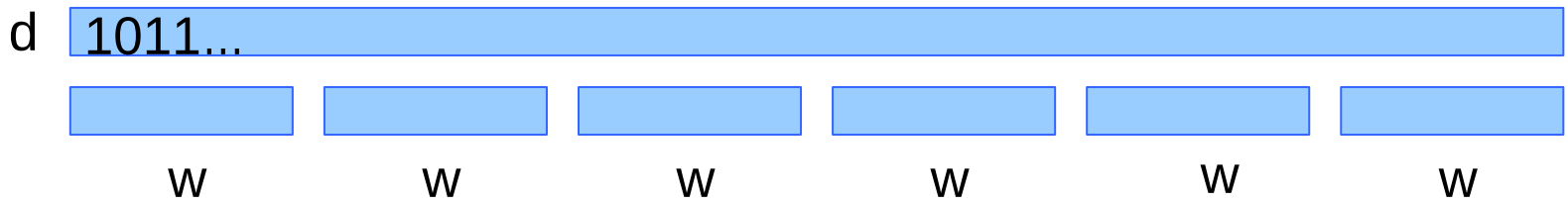
Width	2	2.5	3	3.25	3.5	3.75	4	4.125	...
Table Size	2	3	4	5	6	7	8	9	...
160-bit ECC (byte)	80	120	160	200	240	280	320	360	...
Non-Zero Density	0.5	0.42	0.33	0.313	0.291	0.271	0.25	0.244	...

With our proposed method,
we can choose these table sizes

Speed
- New Choice of Width -

wNAF method

[OT03a



The choice of width is fixed

Proposed method

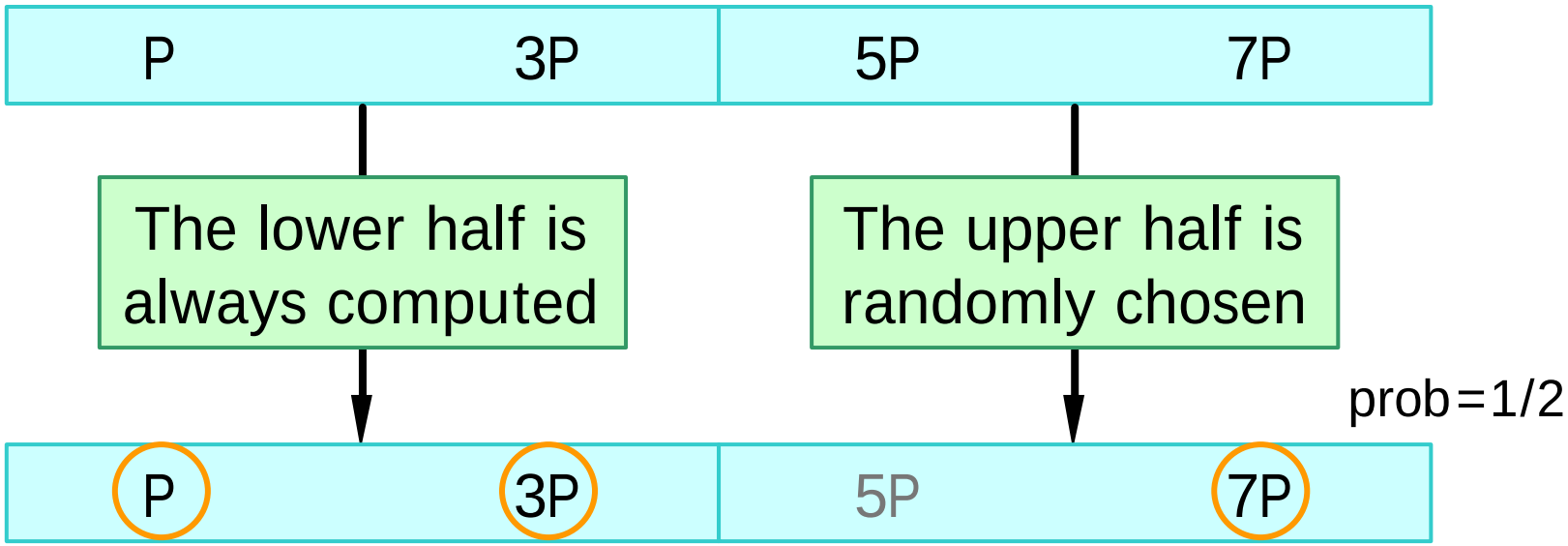
[OT03b

The choice of width is probabilistic

Memory
- Our Pre-Computation Table -

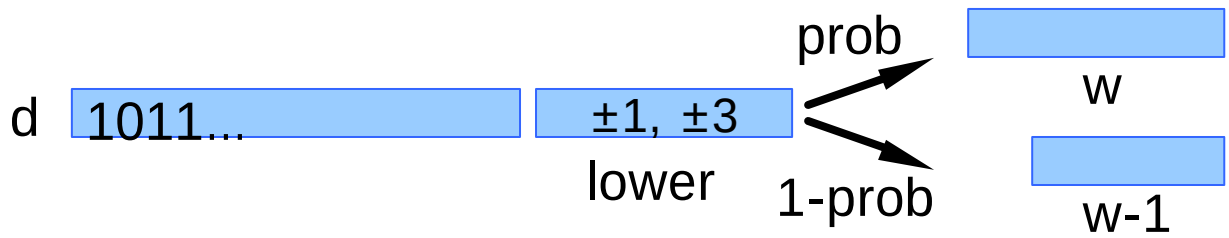
width = 2.5 (three points are pre-computed)

Pre-computation table

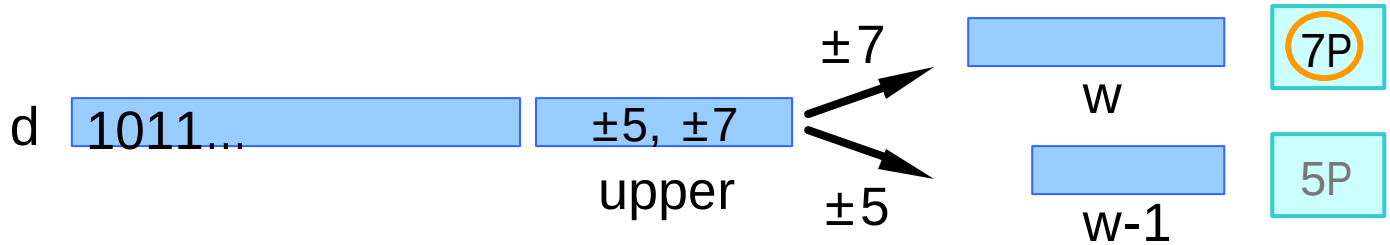


Security
- Main Trick -

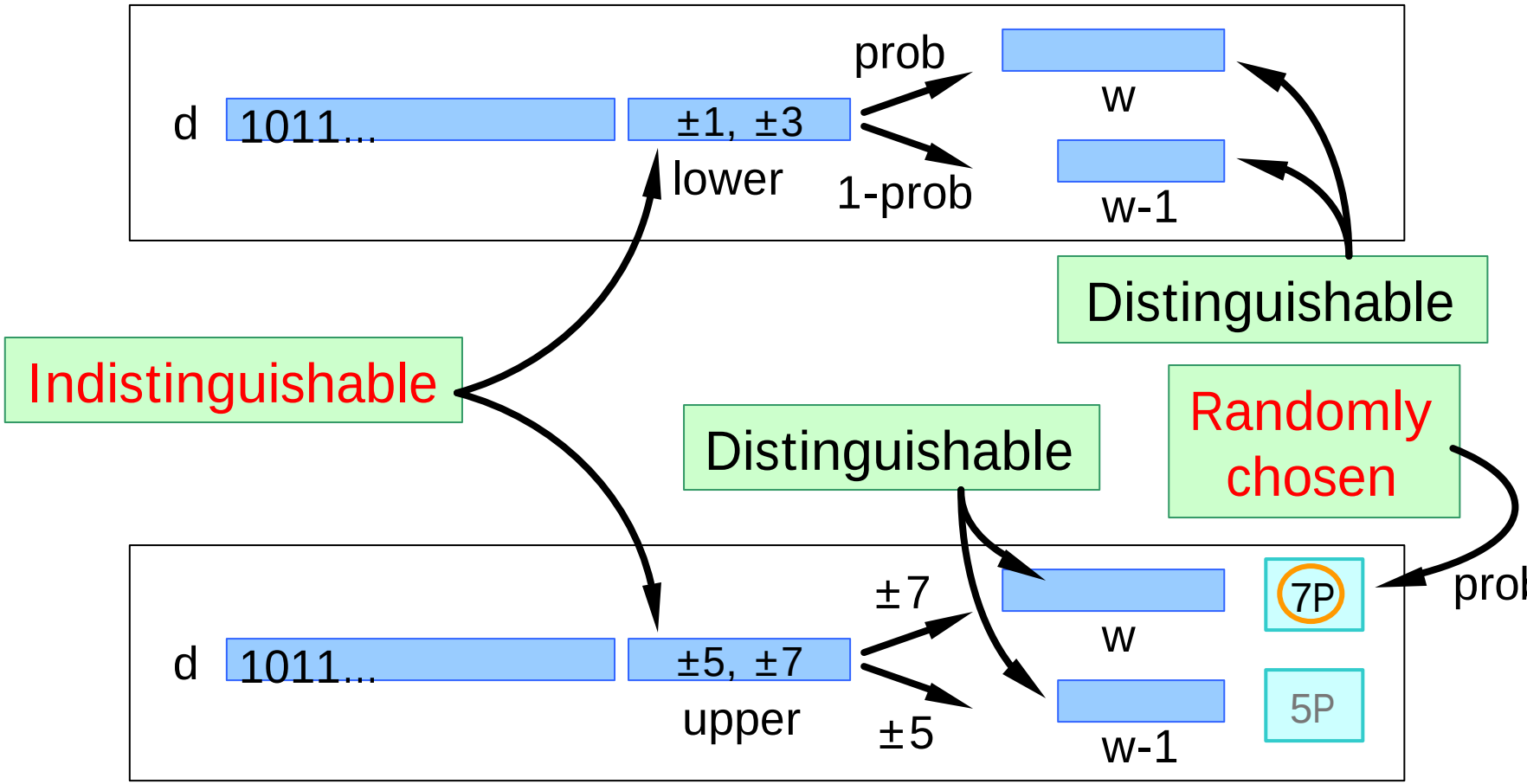
If the current digit is in the lower half,
the width w is chosen with probability prob



If the current digit is in the upper half,
the width w is chosen if the digit is pre-computed



Security of Proposed Scheme



Conclusion

Problem	Side channel attacks break the implementation of cryptography on memory-constraint devices.
Result	We proposed an ECC implementation in which we can freely choose the table size without losing its security.
Points	The proposed scheme uses two widths and chooses one of them with fixed probability.