Signed Binary Representations Revisited

Katsuyuki Okeya, Hitachi
Katja Schmidt-Samoa, Christian Spahn,
Tsuyoshi Takagi, TU Darmstadt

http://www.cdc.informatik.tu-darmstadt.de/reports/reports/crypto04-eprint.pdf

Conteúdo

Motivação

Non-Adjacent Form (NAF)

Mutual Opposite Form (MOF)

wNAF

wMOF

Conclusão

Motivação para Algoritmos de Exponenciação

***Smart-cards*:** verdadeiros computadores de bolso, pela enorme capacidade de armazenamento e pela versatilidade, já que as informações guardadas nele podem ser lidas e alteradas por terminais autorizados.

Baseia-se em curvas elípticas uma vez que criptossistemas de curvas elípticas (ECC) dão grande segurança com chaves de comprimento moderado.

Motivação para Algoritmos de Exponenciação (cont.)

Em multiplicação escalar usual, temos: $d \times P = P + P + \ldots + P$

d vezes

Já a multiplicação escalar usando curvas elípticas é mais rápida, uma vez que o NAF ajuda a diminuir o número de somas pois, 15 P = P + P + …+ P (15 vezes) vira 15P = P + 2(P + 2(P + 2P)), por exemplo.

O método mais comum para calcular exponenciação de elementos em Grupos Abelianos é o esquema das janelas deslizantes.

Non-Adjacent Form (NAF)

Non-Adjacent Form (NAF) - representação binária com sinal, que é obtida aplicando-se a conversão: 1|0|-1← 1|1, repetidamente, onde *a*|*b* denota a concatenação dos bits a e b.

Um exemplo de NAF:

345 =	1	0	1	0	**1**	**1**	0	0	1	(Binary representation)
	1	0	**1**	**1**	0	-1	0	0	1	
	1	**1**	0	-1	0	-1	0	0	1	
1	0	-1	0	-1	0	-1	0	0	1	(NAF representation)

Mutual Opposite Form (MOF)

Mutual Opposite Form (MOF) é um string binário com sinal que satisfaz as seguintes propriedades:

Os sinais dos bits adjacentes não nulos (sem considerar os bits nulos) são opostos.

O maior bit não nulo e o menor bit não nulo são 1 e -1, respectivamente.

Um exemplo de MOF é:

345 = 1 0 1 0 1 1 0 0 1 (Binary representation)

1 -1 1 -1 1 0 -1 0 1 -1 (MOF representation)

Mutual Opposite Form (MOF)

Para gerar um MOF, é feita a subtração bit-a-bit (*2d – d)*:

$$
\begin{array}{rcccccccccc}
2d & = & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
-\,d & = & & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
\hline
 & & 1 & -1 & 1 & -1 & 1 & 0 & -1 & 0 & 1 & -1
\end{array}
$$

Mutual Opposite Form (MOF)

Teorema 1: Seja n um inteiro positivo. O (n+1)-bit MOF tem 2^n pares de representações diferentes, ou seja, qualquer n-bit de string binário pode ser unicamente representado pelo (n+1)-bit MOF.

Mutual Opposite Form (MOF)

Demonstração:

Para n = 1, temos que o 2-bit MOF é 0|0 ou 1|-1, uma vez que o 1-bit dos strings binários 0 e 1 são convertidos para os MOFs 0|0 e 1|-1, respectivamente.

Mutual Opposite Form (MOF)

Demonstração:

Para n = 1, temos que o 2-bit MOF é 0|0 ou 1|-1, uma vez que o 1-bit dos strings binários 0 e 1 são convertidos para os MOFs 0|0 e 1|-1, respectivamente.

Para n = k+1, temos 2 casos:

(k+1)-bit do string binário é 0 → podemos assumir que o (k+2)-bit MOF é 0 e aplicar a conversão um-para-um dos k-bits restantes.

(k+1)-bit do string binário é 1 → o k-bit do string binário pode ser 0 ou 1. Logo, convertemos o (k+1)-bit dos string binários 1|0|* e 1|1|* para o (k+2)-bit MOF 1|-1|* e 1|0|*, respectivamente.

Mutual Opposite Form (MOF)

Proposição 1: A operação $\mu = 2d - d$ converte o string binário para μ MOF.

Mutual Opposite Form (MOF)

Proposição 1: A operação $\mu = 2d - d$ converte o string binário para μ MOF.

Demonstração:

Sabemos que $\mu_n = 1$ se $d_{n-1} = 1$. Por $\mu_i = d_{i-1} - d_i$, temos $\mu_i = 0$ ou 1 para $d_i = 0$. Então, o bit mais a esquerda de μ será 1.

De $\mu_i = d_{i-1} - d_i = 1$, sabemos que $d_{i-1} = 1$ e que $\mu_{i-1} = d_{i-2} - d_{i-1} = 0$ ou -1, baseado em $d_{i-2} = 1$ ou 0, respectivamente. Essa relação nos dá $\mu_i | \mu_{i-1} | \ldots | \mu_{i-k+1} | \mu_{i-k} = 1|0|\ldots|0|-1$ para algum k.

\ /

k-1

MOF & NAF

Se aplicarmos o método das janelas deslizantes da direita-para-esquerda (sem carry) 0|1 ← 1|-1 e 0|-1 ← -1|1 para MOF de d, então o NAF de d é obtido:

345=	1	0	1	0	1	1	0	0	1	(Binary representation)
	1	-1	1	-1	1	0	-1	0	**1**	**-1** (MOF representation)
	1	-1	1	**-1**	**1**	0	-1	0	0	1
	1	**-1**	**1**	0	-1	0	-1	0	0	1
	1	0	-1	0	-1	0	-1	0	0	1 (NAF representation)

wNAF

Uma seqüência de dígitos com sinal é chamada wNAF se e somente se:

- O bit mais significativo não nulo é positivo.
- Dentre quaisquer w dígitos consecutivos, ao menos um é não nulo.
- Cada dígito não nulo é ímpar e menor que 2^{w-1} em valor absoluto.

W	2^{w-1}	Dígitos
2	$2^{2-1} = 2$	-1, 1
3	$2^{3-1} = 4$	-3, -1, 1, 3
4	$2^{4-1} = 8$	-7, -5, -3, -1, 1, 3, 5, 7

wNAF

Um exemplo de wNAF:

345 =	1	0	1	0	1	1	**0**	**0**	**1**	(Binary representation)
	1	0	1	**0**	**1**	**1**	0	0	1	
	1	**0**	**1**	0	0	3	0	0	1	
1	0	0	-3	0	0	3	0	0	1	(3NAF representation)

MOF & wNAF

Aplicando o método das janelas deslizantes de largura w para o MOF de d, obtemos o wNAF de d.

Para w = 3:

0|0|1	←	0|1|-1
0|0|-1	←	0|-1|1
0|0|3	←	1|-1|1 ou 1|0|-1
0|0|-3	←	-1|1|-1 ou -1|0|1

MOF & wNAF

345 =	1	0	1	0	1	1	0	0	1	(Binary representation)
	1	-1	1	-1	1	0	-1	**0**	**1**	**-1** (MOF representation)
	1	-1	1	-1	**1**	**0**	**-1**	0	0	1
	1	**-1**	**1**	**-1**	0	0	3	0	0	1
	1	0	0	-3	0	0	3	0	0	1 (3NAF representation)

wNAF

Teorema 2: Todo inteiro d não-negativo tem uma representação wNAF, que é única exceto pelo número de zeros a esquerda.

wNAF

Teorema 2: Todo inteiro d não-negativo tem uma representação wNAF, que é única exceto pelo número de zeros a esquerda.

Demonstração:

Há 3 casos a tratar.

1) conversão MOF → wNAF (já visto)

2) conversão wNAF → MOF

3) estas 2 conversões são inversas uma da outra.

wMOF

Definimos *w*MOF como o resultado do método das janelas deslizantes de largura w da esquerda-para-direita sobre MOF.

De modo semelhante, construímos wMOF:

Para w = 3, temos:

1|-1|1 ou 1|0|-1	→	0|0|3
-1|1|-1 ou -1|0|1	→	0|0|-3
1|-1|0	→	0|1|0
-1|1|0	→	0|-1|0

wMOF

345 =	1	0	1	0	1	1	0	0	1	(Binary representation)
	1	**-1**	**1**	-1	1	0	-1	0	1	-1 (MOF representation)
	0	0	3	**-1**	**1**	**0**	-1	0	1	-1
	0	0	3	0	-1	0	**-1**	**0**	**1**	-1
	0	0	3	0	-1	0	0	0	-3	-1 (3MOF representation)

wMOF

Teorema 3: Todo inteiro d não-negativo tem uma representação wMOF, que é única exceto pelo número de zeros a esquerda.

wMOF

Teorema 3: Todo inteiro d não-negativo tem uma representação wMOF, que é única exceto pelo número de zeros a esquerda.

Demonstração:

Há 3 casos a tratar.

1) conversão MOF → wMOF (já visto)

2) conversão wMOF → MOF

3) estas 2 conversões são inversas uma da outra.

wMOF

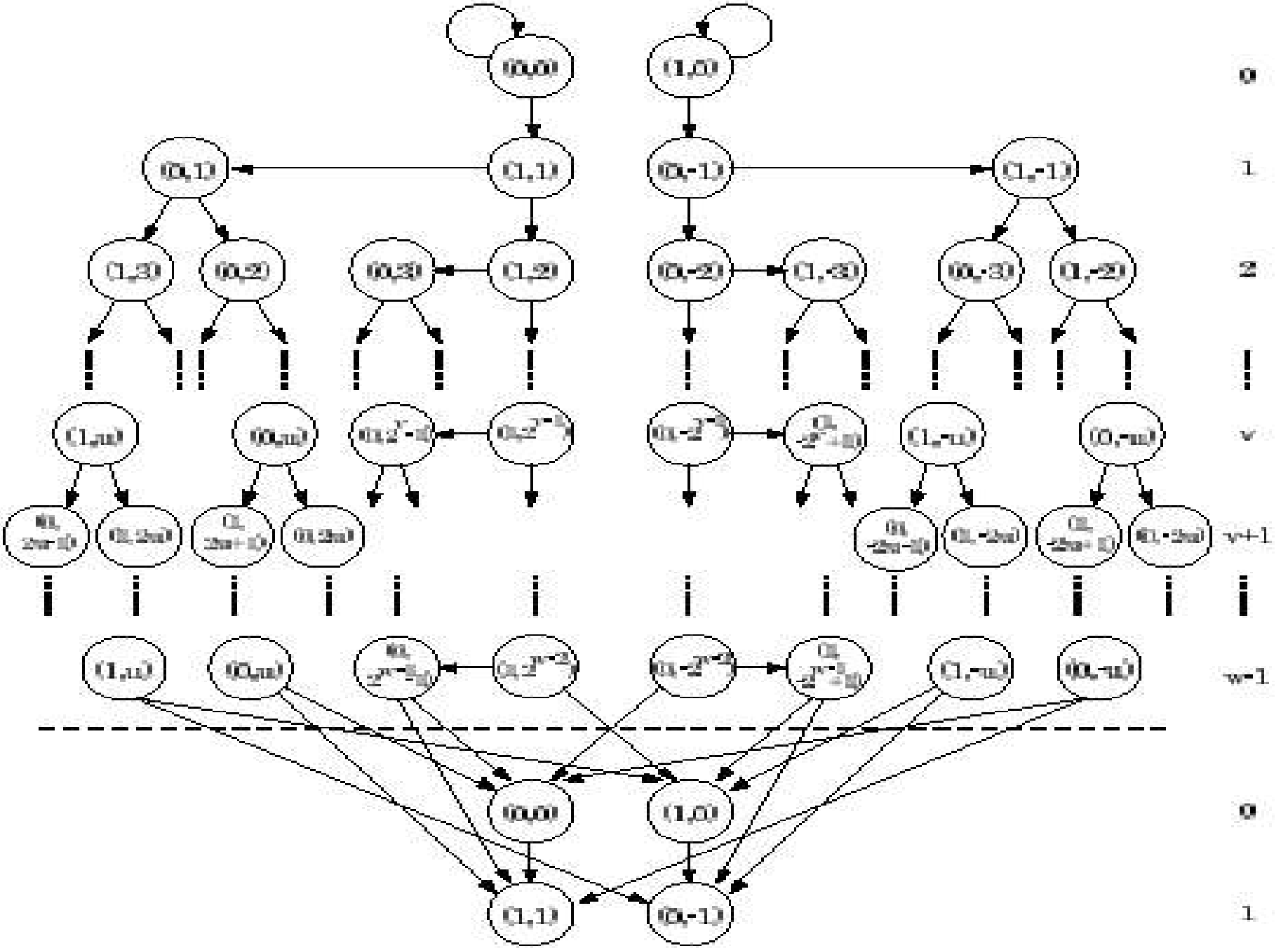
Teorema 4: A densidade média não-nula de wMOF é assintoticamente 1/(w+1) para n $\mapsto$ *oo*.

wMOF

Teorema 4: A densidade média não-nula de wMOF é assintoticamente 1/(w+1) para n $\mapsto$ *oo*.

Demonstração:

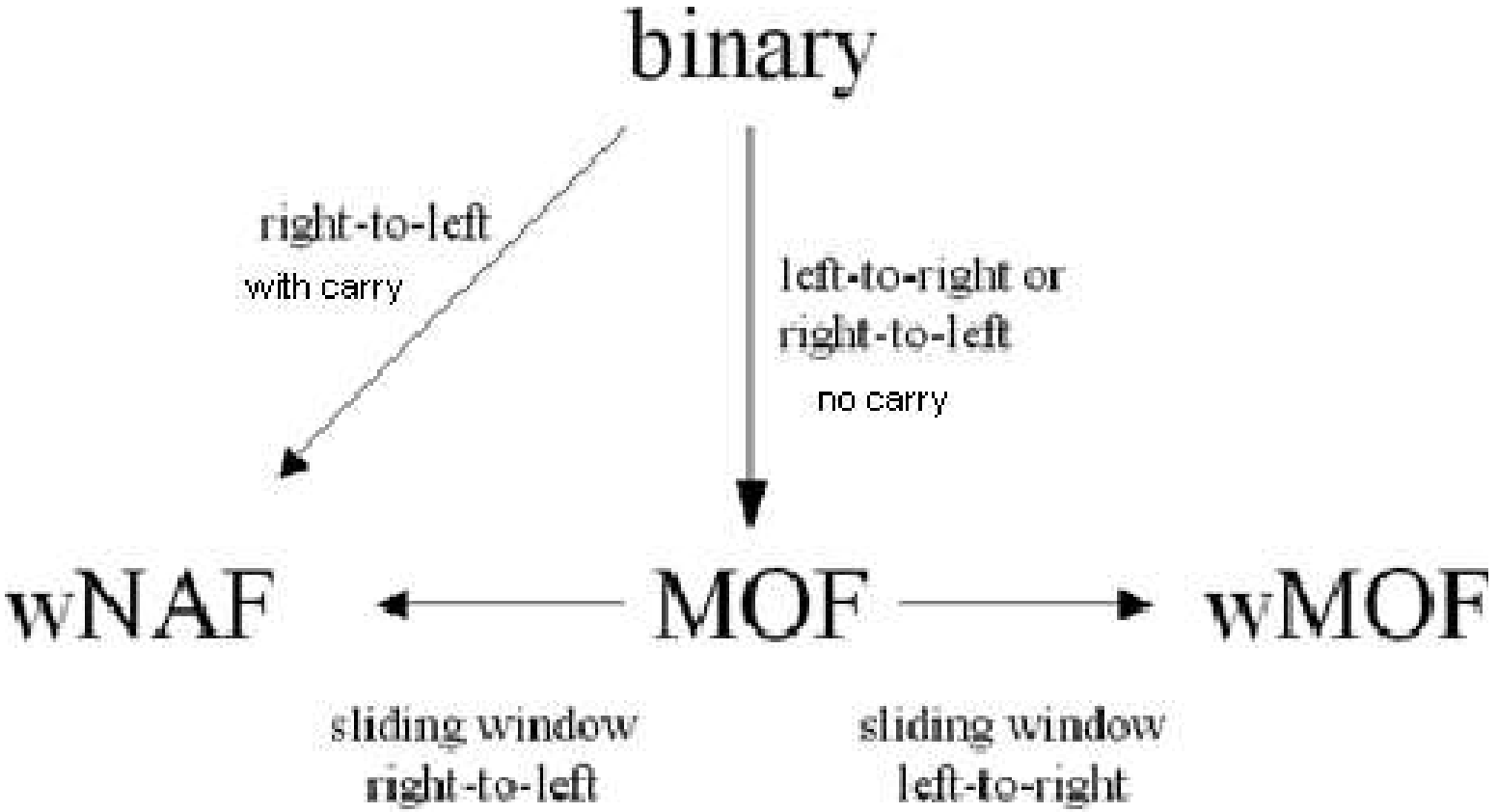
Usando Cadeia de Markov para provar isso, temos…..


(0,0)
(1,0)
0
(0,1)
(1,1)
(0,-1)
(1,-1)
1
(1,2)
(0,2)
(0,3)
(1,3)
(0,-2)
(1,-3)
(0,-3)
(1,-2)
2
v
v+1
w-1
(0,0)
(1,0)
0
(1,1)
(0,-1)
1

wMOF

Largura w	1 / densidade observada	1 / densidade esperada
2	2.988	3
3	3.970	4
4	4.946	5
5	5.914	6
6	6.878	7

Conclusão: Métodos janela sobre MOF



Referência

http://www.cdc.informatik.tu-darmstadt.de/reports/reports/crypto04-eprint.pdf

Maiores Informações

http://www.linux.ime.usp.br/~julee/mac499/monografia.html