Representações Binárias com Sinal

Aluna: Juliana Lai Yeh Lee
Orientador: Routo Terada
Novembro / 2005

Motivação

***Smart-cards*:** verdadeiros computadores de bolso, pela enorme capacidade de armazenamento e pela versatilidade.

Algoritmos de criptografia baseiam-se em curvas elípticas.

Para calcular a exponenciação de elementos em Grupos Abelianos, são utilizadas as representações binárias com sinal, uma vez que estas aumentam a velocidade das multiplicações escalares (em outras palavras, diminuem o número de operações).

Motivação (cont.)

Em multiplicação escalar usual, temos: $15 \times P = P + P + \ldots + P$

15 vezes

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

Os métodos mais comuns para cálculos em curvas elípticas são os métodos NAF (*Non-Adjacent Form)*, MOF (*Mutual Opposite Form)* e suas variações, como o *wNAF* e o *wMOF*.

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)*:

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

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)

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:

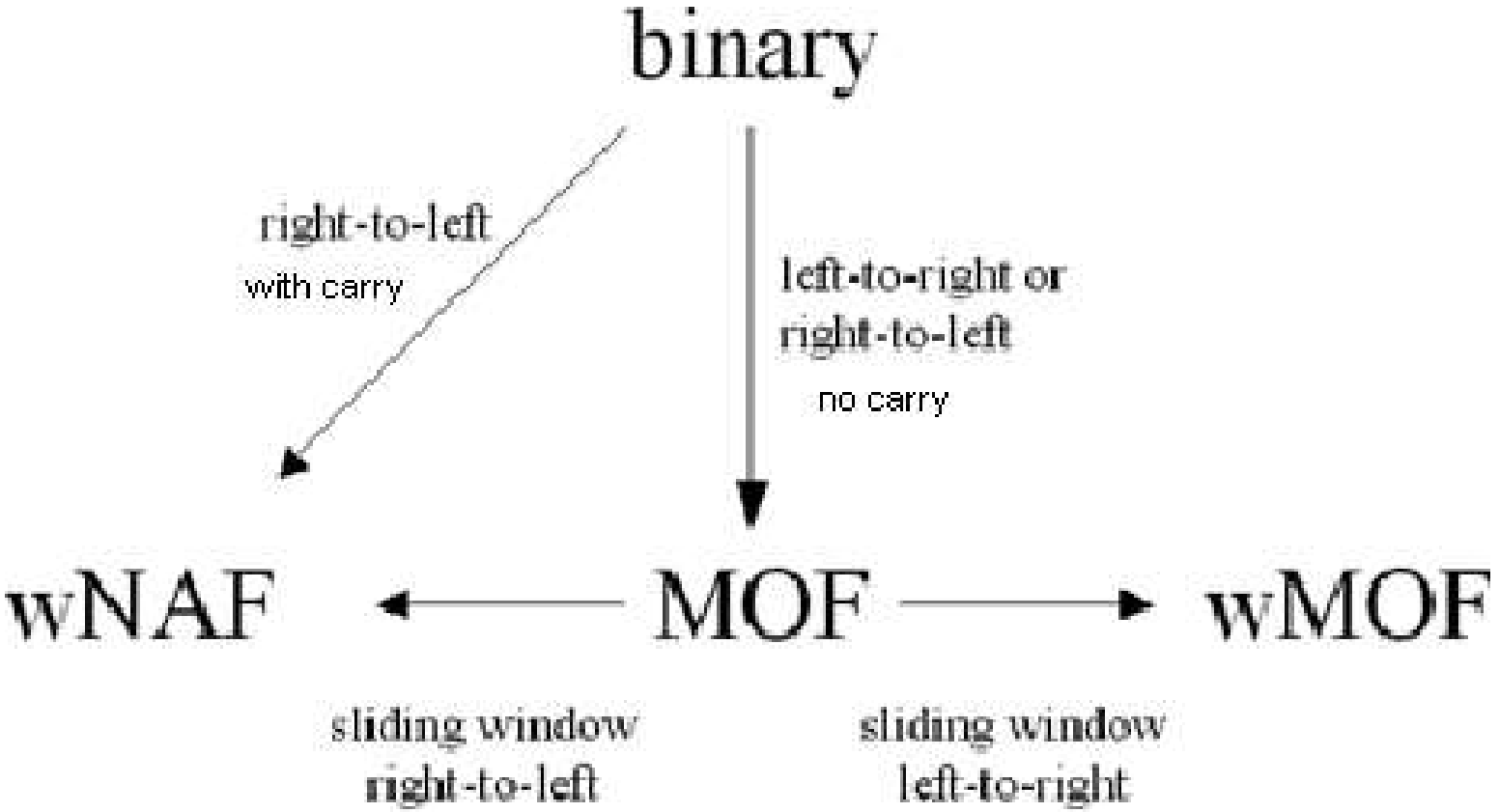
Para w = 3, temos:

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

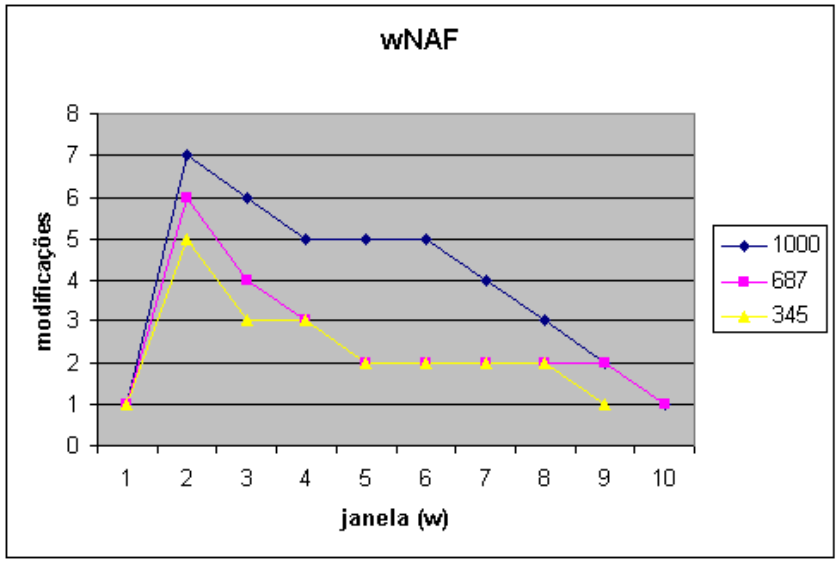
wMOF

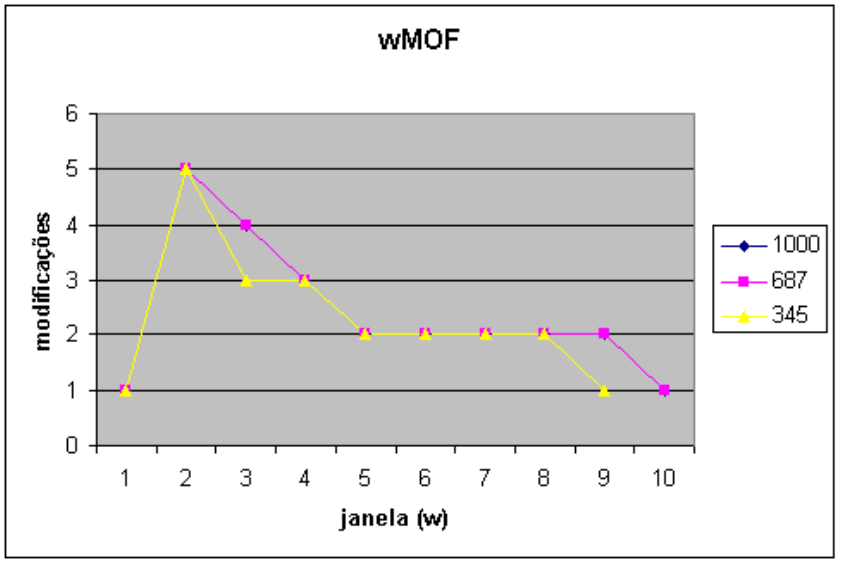
345 =	1	0	1	0	1	1	0	0	1	(Binary representation)
	1	**-1**	**1**	-1	1	0	-1	0	1	-1 (MOF representation)
	0	0	3	**-1**	**1**	**0**	-1	0	1	-1
	0	0	3	0	-1	0	**-1**	**0**	**1**	-1
	0	0	3	0	-1	0	0	0	-3	-1 (3MOF representation)

Conclusão: Métodos janela sobre MOF



Conclusão


wNAF
modificações
janela (w)
1000
687
345


wMOF
modificações
janela (w)
1000
687
345

Informações

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

Maiores Informações:

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