Calculating the Efficiency of Elliptic Curve Cryptography by Reducing the Suffix Tree of Hamming Weight Array

Vorapong Suppakitpaisarn (U. Tokyo), Masato Edahiro (Nagoya U.) Hiroshi Imai (U. Tokyo)

Introduction & Contribution

Speed Up **Elliptic Curve Cryptography**

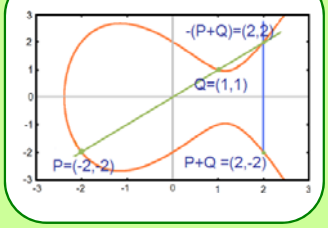
(Scalar Point Multiplication $r_1P_1 + r_2P_2 + \dots + r_dP_d$)

=

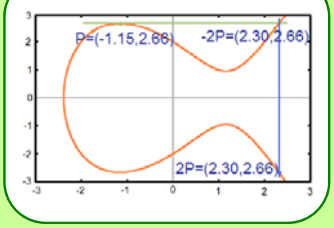
Optimize the number of elementary operations

Point Additions ($P + Q$) and Point Doubles ($2P$)

Point Addition



Point Double



Example Let Compute $12P + 21Q$

Represent 12,21 using Digit Set {0, ±1}

Point Addition
Point Double
Do Nothing

Redundant Representation
(We can represent some numbers using more than one ways)

$r_1 = 12 = (1\ 0\ -1\ 0\ 0)_2$

$r_2 = 21 = (1\ 0\ 1\ 0\ 1)_2$

$P+Q$ $2P+2Q$ $3P+5Q$ $6P+10Q$ $12P+21Q$

O $2P+2Q$ $4P+4Q$ $6P+10Q$ $12P+20Q$

Fast Operation???
We need least point additions= Minimal Weight
(number of green block = Weight)

Min. Average Weight (MAW) = Minimal Weight / Length of Bit String

Average for all integer $r_1, r_2, \dots, r_d$

Contribution 1:
Algorithm to find Expansion with Minimal Weight
(for any digit sets)

Contribution 2:
Find MAW for
$\{0, \pm1, \pm3, \dots, \pm(2n+1)\}$

Methods(1)

Previous Works

Mathematical Construction

Very hard to find (In some digit sets)

Conversion (might not min. weight)

Markov chain by hand

Average Weight

Our Work

Min. Weight Conversion

Algorithm for constructing Markov chain

Min. Average Weight

Contribution 1

1. Based on **Dynamic Programming** Scheme
2. **Replacing the bit vectors** causes **Carry**.

Digit Set {0,1,3}

bit 1 2 3

$3 = (0\ 1\ 1)_2$

$7 = (1\ 1\ 1)_2$

Carry

$\begin{pmatrix}0\\-1\end{pmatrix} \times 2 + \begin{pmatrix}1\\3\end{pmatrix}$

bit 1 2 3

$3 = (0\ 1\ 1)_2$

$7 = (0\ 3\ 1)_2$

Input Bit 1 <0,0> / <0,1> / <1,0> /<1,1>

Input Bit 2 <0,0> / <0,1> / <1,0> /<1,1>

Linked List of Hamming Weight Array

Initial Weight Array → Weight Array Bit 1 → Weight Array Bit 2 → … → Weight Array Bit n

Minimal Weight of Bit 1 When **Carry** to Bit 1 is <-2,-2>

$= [w_{1,<-2,-2>}, w_{1,<-2,-1>}, \dots, w_{1,<3,3>}]$

$= [w_{n,<-2,-2>}, w_{n,<-2,-1>}, \dots, w_{n,<3,3>}]$

Methods(2)

Contribution 2

AverageWeight(n) = Average of **joint Hamming Weight** for **all bit string length** n / n

n tends to infinite

Input Bit 1 = <0,1>
Input Bit 1 = <0,0>
Initial Weight Array
Input Bit 1 = <1,0>
Input Bit 1 = <1,1>

Input Bit 2 = <0,1>
Input Bit 2 = <0,0>
Input Bit 2 = <1,0>
Input Bit 2 = <1,1>

Weight Array Bit 1 for <0,1>
Weight Array Bit 1 for <1,0>
Weight Array Bit 1 for <1,1>

Weight Array Bit 2 for <00,10>
Weight Array Bit 2 for <00,11>
Weight Array Bit 2 for <01,10>
Weight Array Bit 2 for <01,11>

Weight Array … Weight Array

Average of 4^n nodes

Remove Unnecessary Nodes

Equivalent Weight Array

Finite State Markov Chain (3189 States for {0, ±1, ±3})

Infinite Tree

Same Weight Array = Same Node

n tends to infinite

Results

Integer Pair, $h = 1$

Solinas, Comb. and Opt. Report, 2001	Open Problem	
Avanzi, Crypto. e-Print Achieve, 2002	0.3750	
Kuang, Zhu, Zhang, ACNS 2004, 2004	0.3712	
Moller, ICISC 2004, 2004	0.3636	
Dahmen, Okeya, Takagi, IEICE Trans., 2007	0.3615	
Our Result	0.3575	

We prove that
0.3575 **is the least number**
and **solve open the problem**

Other Cases

h	Single Integer	Integer Pair	Triple	Quadruple
0	$\frac{1}{3} \approx 0.3333$ [Egecioglu 94]	$\frac{1}{2} = 0.5$ [Solinas 01]	$\frac{23}{39} \approx 0.5897$ [Heuberger 07]	$\frac{115}{179} \approx 0.6424$ [Heuberger 07]
1	$\frac{1}{4} = 0.25$ [Muir 04]	$\frac{281}{786} \approx 0.3575$ [Improved Result]	0.4090 [New Result]	
2	$\frac{2}{9} \approx 0.2222$ [Moller 05]	$\frac{1496396}{4826995} \approx 0.3100$ [New Result]	0.3529 [New Result]	
3	$\frac{1}{5} = 0.2$ [Moller 05]	0.2660 [New Result]		
4	$\frac{4}{21} \approx 0.1904$ [Moller 05]	0.2574 [New Result]		
5	$\frac{2}{11} \approx 0.1818$ [Moller 05]	0.2342 [New Result]		
6	$\frac{4}{23} \approx 0.1739$ [Moller 05]			
7	$\frac{1}{6} \approx 0.1667$ [Muir 04]			

Match existing results

Improve existing results

Discover new results

1. V. Suppakitpaisarn, M. Edahiro, H. Imai, "Optimal Average Joint Hamming Weight and Minimal Weight Conversion of d Integers", Cryptology ePrint Archive **2010/300**, 2010.
2. V. Suppakitpaisarn, "Optimal Average Joint Hamming Weight and Digit Set Expansion", Master Thesis, The University of Tokyo, 2009.