UNIVERSITI PUTRA MALAYSIA

NEW SIGNED-DIGIT {0,1,3}-NAF SCALAR MULTIPLICATION ALGORITHM FOR ELLIPTIC CURVE OVER BINARY FIELD

SHARIFAH MD YASIN

FSKTM 2011 31

NEW SIGNED-DIGIT {0,1,3}-NAF SCALAR MULTIPLICATION ALGORITHM FOR ELLIPTIC CURVE OVER BINARY FIELD

SHARIFAH MD YASIN

DOCTOR OF PHILOSOPHY

UNIVERSITI PUTRA MALAYSIA

2011

NEW SIGNED-DIGIT {0,1,3}-NAF SCALAR MULTIPLICATION ALGORITHM FOR ELLIPTIC CURVE OVER BINARY FIELD

By

SHARIFAH MD YASIN

Thesis Submitted to the School of Graduate Studies, University Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

February 2011

Abstract of thesis presented to the Senate of University Putra Malaysia in fulfillment of the requirement for the degree of Doctor of Philosophy

NEW SIGNED-DIGIT {0,1,3}-NAF SCALAR MULTIPLICATION ALGORITHM FOR ELLIPTIC CURVE OVER BINARY FIELD

By

SHARIFAH MD YASIN

February 2011

Chair: Associate Professor Ramlan Mahmod, PhD

Faculty: Computer Science and Information Technology

Elliptic curve cryptography introduced by Neil Koblitz and Victor Miller in the 80's. Elliptic curve cryptosystem is very popular recently in comparison with the other public-key cryptosystem such as RSA. This is because elliptic curve cryptosystem uses smaller key size than RSA but it provides equivalent security level with the RSA. Smaller key size means less storage requirement, low power consumption and computing cost. These features are suitable for portable devices such as PDAs, mobile phone, and smartcards.

Scalar multiplication is a major operation in elliptic curve cryptosystem. It is the most time consuming and costly operation. It involves with three levels of computations: Scalar arithmetic (Level 1), Point arithmetic (Level 2) and Field arithmetic (Level 3). In the literature, improving scalar representation and efficient point operation can reduce the scalar multiplication cost.

In this research, a new left-to-right recoding algorithm is proposed to convert a binary expansion into a new {0,1,3}-NAF representation. The new scalar representation is in base 2 using digit 0, 1 and 3. The special NAF property is adopted in the new {0,1,3}-NAF scalar. Also, a new point tripling formula and algorithm are introduced for elliptic curve over binary field using Lopez-Dahab projective coordinates. The tripling operation is done by computing (2P+P) using one doubling followed by one mixed addition. The tripling cost is (12M+7S) which is cheaper than the cost of computing (2P+P) using traditional method. The new tripling formula saved (2M+2S) when compared with the traditional method. Finally, a new signed-digit {0,1,3}-NAF scalar multiplication algorithm is proposed to utilize the new scalar representation and the new tripling operation.

Mathematical analysis is carried out to identify important features, advantages and disadvantages of the new signed-digit {0,1,3}-NAF scalar multiplication algorithm. Cost measurement is based on number of point operations per scalar throughout the execution of the scalar multiplication algorithm. The cost of three

scalar multiplication algorithms are compared: double-and-add, addition-subtraction and new signed-digit {0,1,3}-NAF scalar multiplication. By comparison with the double-and-add algorithm, the new signed-digit {0,1,3}-NAF scalar multiplication algorithm has better performance when the value of p is greater than or equal to 2, where p is the number of digit 3 in the new {0,1,3}-NAF representation. By comparison with the addition-subtraction algorithm, the new signed-digit {0,1,3}-NAF scalar multiplication algorithm has better performance when $(h_2 - h_1) \geq 0$ where h_1 and h_2 are the Hamming weight of the new {0,1,3}-NAF and {-1,0,1}-NAF scalars respectively. Also, from observation, it is effective to use the new signed-digit {0,1,3}-NAF scalar multiplication algorithm when the percentage of the nonzero digit in the binary expansion is less than 75%.

In conclusion, performance of a scalar multiplication algorithm depends on the digits used in the scalar representation, and the efficiency of the point operations involved in the scalar multiplication algorithm. Efficiently managed point operations can give optimal number of point operations involved throughout the execution of the scalar multiplication algorithm and can reduced cost of the scalar multiplication.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

ALGORITMA BARU DIGIT BERTANDA {0,1,3}-NAF PENDARABAN SKALAR UNTUK KELUK ELIPTIK DALAM MEDAN BINARI

Oleh

SHARIFAH MD YASIN

Februari 2011

Pengerusi: Profesor Madya Ramlan Mahmod, PhD

Fakulti: Sains Komputer dan Teknologi Maklumat

Kriptografi keluk eliptik diperkenalkan oleh Neil Koblitz dan Victor Miller dalam 80an. Sistem kripto keluk eliptik adalah terkenal di masa kini berbanding dengan sistem kripto kunci awam seperti RSA. Ini adalah kerana sistem kripto keluk elliptik menggunakan saiz kunci yang lebih kecil dari RSA tetapi menyediakan tahap sekuriti yang serupa dengan RSA. Saiz kunci yang kecil bermakna keperluan storannya kecil, penggunaan kuasa dan kos komputeran yang rendah. Fitur tersebut adalah sesuai untuk alat mudah alih seperti PDA, telefon mudah alih dan kad pintar.

Pendaraban skalar adalah operasi utama dalam sistem kripto keluk eliptik. Ia adalah operasi yang menggunakan masa yang lama dan mahal. Ia melibatkan tiga tahap komputeran: Aritmetik skalar (Tahap 1), Aritmetik titik (Tahap 2) dan Aritmetik medan (Tahap 3). Dalam literatur, pembaikan pewakilan skalar dan operasi titik yang efisien boleh mengurangkan kos pendaraban skalar.

Dalam penyelidikan ini, satu algoritma pengkodan kiri-ke-kanan yang baru di cadangkan untuk menukar pewakilan binari kepada pewakilan {0,1,3}-NAF yang baru. Pewakilan skalar yang baru ini adalah dalam asas dua menggunakan digit 0, 1 dan 3. Ciri istimewa NAF di adaptasikan di dalam skalar {0,1,3}-NAF yang baru. Formula titik gandaan tiga yang baru dan algoritmanya diperkenalkan kepada keluk eliptik medan binari menggunakan kordinat projektif Lopez-Dahab. Operasi gandaan tiga ini dilakukan dengan pengkomputan 2P+P menggunakan satu gandaan dua diikuti dengan satu tambahan campuran. Kos gandaan tiga adalah 12M+7S, di mana ianya lebih murah daripada kos pengkomputan 2P+P menggunakan kaedah tradisional. Formula gandaan tiga yang baru menjimatkan (2M+2S) bila di bandingkan dengan kos kaedah tradisional. Akhir sekali, algoritma digit bertanda {0,1,3}-NAF pendaraban skalar yang baru di cadangkan untuk menggunakan sepenuhnya pewakilan skalar dan operasi gandaan tiga yang baru.

Analisa matematik dijalankan untuk mengenalpasti fitur penting, kebaikan dan kelemahan algoritma digit bertanda {0,1,3}-NAF pekalian scalar yang baru. Ukuran kos

adalah berasaskan bilangan operasi titik per skalar di sepanjang larian algoritma pendaraban skalar. Kos untuk tiga algoritma pendaraban skalar dibandingkan: *double-and-add*, *addition-subtraction* dan digit bertanda {0,1,3}-NAF pendaraban skalar yang baru. Melalui perbandingan dengan algoritma *double-and-add*, algoritma digit bertanda {0,1,3}-NAF pekalian scalar yang baru mempunyai prestasi yang lebih baik apabila nilai p adalah lebih besar atau sama dengan 2, di mana p adalah bilangan digit 3 dalam pewakilan scalar {0,1,3}-NAF yang baru. Melalui perbandingan dengan algoritma *addition-subtraction,* algoritma digit bertanda {0,1,3}-NAF pendaraban skalar yang baru mempunyai prestasi yang lebih baik apabila $(h_2 - h_1) \geq 0$, di mana h_1 dan h_2 adalah berat *Hamming* untuk scalar-skalar {0,1,3}-NAF dan {-1,0,1}-NAF mengikut urutan. Melalui pemerhatian juga, algoritma digit bertanda {0,1,3}-NAF pendaraban skalar yang baru adalah efektif di gunakan apabila peratus digit bukan kosong dalam pewakilan binari adalah kurang dari 75%.

Kesimpulannya, prestasi algoritma pendaraban skalar bergantung kepada digit yang digunakan dalam pewakilan skalar, dan keberkesanan operasi titik yang terlibat dalam algoritma pendaraban skalar. Operasi titik yang disusun secara efisien boleh memberikan bilangan operasi titik yang optima di sepanjang larian algoritma pendaraban skalar dan boleh mengurangkan kos pendaraban skalar.

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Associate Professor Dr Ramlan Mahmod, for giving me helpful comments, guidance and continuous support to complete this thesis. Also, I would like to thank the committee members, Associate Professor Dr Azmi Jaafar and Associate Professor Dr Muhammad Rushdan, for their valuable comments. Lastly, I would like to express my gratitude to my family for their support and inspiration.

Sharifah Md Yasin

February 2011

I certify that a Thesis Examination Committee has met on 24th February 2011 to conduct the final examination of Sharifah Md Yasin on her thesis entitled "New Signed-Digit {0,1,3}-NAF Scalar Multiplication Algorithm for Elliptic Curve over Binary Field" in accordance with the Universities and Universities Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the degree of Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Ali Mamat, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Zuriati Ahmad Zukarnain, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Kamel ariffin Mohd Atan, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Internal Examiner)

Tsuyoshi Takagi, PhD
Professor
Faculty of Mathematics
Kyushu University, Japan
(External Examiner)

BUJANG KIM HUAT, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as the fulfillment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Ramlan Mahmod, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Azmi Jaafar, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Muhammad Rushdan Md Said, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Member)

HASANAH MOHD GHAZALI, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

SHARIFAH MD YASIN

Date: 24 February 2011

TABLE OF CONTENTS