

รายการอ้างอิง

- [1] Certicom. An Elliptic Curve Cryptography (ECC) Primer. The Certicom "Catch the Curve" White Paper Series. (2004).
- [2] Certicom. Online Elliptic Curve Cryptography Tutorial. Available from: <http://www.certicom.com>.
- [3] Stalings, W. Key Management: Other Public-Key Cryptosystem. Cryptography and Network Security, (2003): 286-306.
- [4] Certicom. The Elliptic Curve Cryptosystem. Remarks on The Security of The Elliptic Curve Cryptosystem. (1997).
- [5] Booth, A. D. A Signed Binary Multiplication Technique. Q. J. Mech.Appl. Math. 4 (1951): 236-240.
- [6] Solinas, J. A. Low-weight Binary Representations for Pairs of Integers. Technical Report CORR. (2001).
- [7] Ercegovac, M. D.; and Trivedi, K. S. On-line Algorithm for Division and Multiplication. IEEE Transaction on Computer. (1977): 681-687.
- [8] Avizienis, A. Signed-digit Number Representation for Fast Parallel Arithmetic. IRE Transaction on Electronic Computer. (1961): 389-400.
- [9] Frougny, C.; and Surarerks, A. On-line Multiplication in Real and Complex Base. IEEE Symposium on Computer Arithmetic. (2003).
- [10] Joye, M.; and Yen, S. M. Optimal Left-to-right Binary Signed digit Recoding. IEEE Transactions on Computers. (2000): 740-748.
- [11] Ruan, X.; and Katti, R. S. Low-weight Left-to-right Binary Signed digit Representation for n Integers. IEEE International Symposium on Information Theory, (2004): 517.
- [12] Ruan, X.; and Katti, R. S. Left-to-right Signed-binary Representation of a Pair of Integers. IEEE Transactions on Computers, (2005): 124-131.
- [13] Ruan, X.; and Katti, R. S. Algorithm and Implementation of Signed-Binary Recoding with Asymmetric Digit Sets for Elliptic Curve Cryptosystems. IEEE Transactions on Computers. (2006).

ประวัติผู้เขียนวิทยานิพนธ์

นายตะวัน ฉายกลิ่น เกิดเมื่อวันที่ 16 มีนาคม พ.ศ. 2526 ที่จังหวัดภูเก็ต สำเร็จ การศึกษาระดับมัธยมศึกษาตอนปลายจากโรงเรียนภูเก็ตวิทยาลัย อำเภอเมือง จังหวัดภูเก็ต เข้าศึกษาต่อในระดับปริญญาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ จนสำเร็จการศึกษาในปี พ.ศ. 2547 และเข้า ศึกษาต่อในระดับปริญญาโทบัณฑิต ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย