November 16, 2012.

prof. Tadeusz Łuba
Warsaw University of Technology
Institute of Telecommunications
Nowowiejska 15/19
00-665 Warsaw

Review of the doctoral dissertation for the Faculty Council
of Automatic Control, Electronics and Computer Science
Silesian University of Technology

Title of the Dissertation:
Operators on GF(2^m) for cryptographic applications: performance - power consumption - security tradeoff

Author: mgr inż. Danuta Pamula

Advisors: Arnaud Tisserand PhD, DSc. IRISA France and Edward Hrynkiewicz, PhD, DSc, Prof. in Silesian University of Technology

1. Scientific content of the dissertation

The topic of the dissertation is on security of ECC (Elliptic Curve Cryptography) systems from side-channel type attacks, which is one the most widely researched topics in cryptography. Systems based on elliptic curves are considered to be the most possible next generation replacement for the public-key based RSA systems. However, satisfactory level of security, effectiveness without compromising security and hardware power consumption deserve further research. In order to solve these problems, the candidate (Ms Pamula) has set the following goals in her research:

1) To develop effective systems to implement arithmetic operations on GF (2^m). Criteria for effectiveness are assumed to be system complexity, speed and power.

2) To develop security for hardware against side-channel attacks and an analysis of power consumption for the cryptographic equipment.

The theory and application of the dissertation aim on developing new algorithms for implementing arithmetic operations on GF (2^m), targeting FPGA based implementation.

2. Merit of the dissertation

The excellent scientific merit of the work is reflected in its holistic approach of the problem, encompassing both effectiveness and security of the hardware implementing the ECC problems. Important elements of originality of the work are:

a) efficient in terms of speed and area GF(2^m) hardware arithmetic operators dedicated to ECC applications; unusually elaborate and at the same time, detailed analysis of several existing solutions deserve special appreciation; inferences from such analysis have led to the development of better solutions;

b) successful protections against some power analysis side channel attacks for GF(2^m) hardware arithmetic operators; in order to reduce information leakage, the author has introduced necessary algorithmic and structural modifications. To avoid degradation effectiveness in hardware, the modifications have been proposed at the lower level of implementation;

c) the tradeoff between efficiency and security of GF(2^m) hardware arithmetic operators.

The author has rightly avoided analyzing the effectiveness of multiplication that use optimal normal bases, which give acceleration only for GF(2^m), when m is a small natural number. With increase in the value of m, the presented algorithms (with the exception of naïve ones) become more effective. This is the result of complicated conversion from normal base to polynomial. Moreover, optimal normal base does not exist for all values of m.

3. Organization and editing of the dissertation

The knowledgebase of the topic is very wide. Therefore, the author was compelled to do a thorough literature study of the methods and algorithms developed in other academic and research centers implementing GF(2^m) arithmetic operations. The bibliography with 116 entries, sufficiently covers the area of the dissertation. A good comparative study of exceptionally wide

array of algorithms and their implementation in FPGA was made possible by the elaborate list of references.

The dissertation is written with conscientiousness from the editorial point of view. The quality of the work is reflected in a lot of good examples with clarity of presentation, tables, diagrams, symbolic pictures and a solid documentation of experimental results.

4. Critical Observations

According to me, the author could have examined the use of algorithms for arithmetic operation on GF($2m$) for irreducible polynomials that are lexicographically small. In such cases, for example, the *divide-and-conquer* matrix is very simple for all values of m. This could be a general conclusion that could have particular implication in hardware implementation.

The above observation is more for discussion and does not imply in any way on my highly possitive opinion of the dissertation. The merit of the dissertation rests with the in-depth analysis of multiplication algorithms in GF(2^m), taking into account effective hardware implementation of ECC systems.

5. Final Grade

The value of the theoratical aspect of the dissertation of Ms. Danuty Pamuli is the new and nontrivial solution to the problem of tradeoff between effectiveness and security in ECC systems. The candidate has modified existing arithmatic algorithms, so that they are applicable and easy to map on to cells and macrocells of modern generation FPGA.

In summary, I state that the dissertation clearly meets and exceeds the expectations for doctoral dissertation set by existing rules and regulations. Therefore, I recommend and request the Faculty Council of Automatic Control, Electronics and Computer Science of Silesian University of Technology that the dissertation be allowed for public defense and that „distinction" be conferred on the dissertation.

T. Jurba