



UCC

Coláiste na hOllscoile Corcaigh, Éire
University College Cork, Ireland

Damh na hinnealtoireachta
School of Engineering

Roinn na hinnealtoireachta Leictreolaíochta agus Leictreonaíochta
Department of Electrical & Electronic Engineering

University College Cork
Cork, Ireland

T +353 (0)21 4902210 / 2923
F +353 (0)21 4271698
E eee@ucc.ie
<http://eee.ucc.ie>

PhD thesis review

Dissertation Title:

Arithmetic operators on $GF(2^m)$ for cryptographic applications: performance – power consumption – security tradeoffs

Author:

Danuta Pamula

Supervisors:

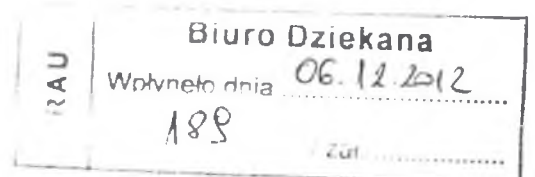
dr hab. Inż. Edward Hrynkiewicz, prof., nzw. W Politechnice Śląskiej (PL)
Arnaud Tisserand, CNRS researcher, HDR (FR)

Content of the Dissertation

The aim of this Dissertation is to investigate the arithmetic operator in the finite field $GF(2^m)$, that are required for elliptic curve based cryptography. In particular the novel efficient implementations of the $GF(2^m)$ operation of multiplication at field sizes appropriate for use in elliptic curve cryptography are presented. In addition the implementation of these operators such that they are secure against side channel attacks is presented. The research presented in this Dissertation has resulted in 4 international conference publications and a journal publication.

Chapter 1 introduces the concept of modern cryptography, namely symmetric or private key cryptography and asymmetric or public key cryptography. The requirements and application areas for modern cryptography are also introduced. Finally an overview of the Dissertation is presented.

Chapter 2 introduces the concept of an elliptic curve over a finite field and its use in elliptic curve cryptography. In particular the Elliptic Curve Discrete Logarithm Problem (ECDLP) is explained along with its use in encryption and signature schemes. At the heart of the ECDLP is point scalar multiplication and this requires point addition and point doubling. These point operations in turn are carried out through arithmetic operations on the underlying finite or Galois field. Finally this chapter introduces the concepts of efficiency and security as required in a cryptographic system and poses the research question to be addressed by the Dissertation in terms of the efficient and secure implementation of the underlying finite field operators.



Chapter 3 primarily is concerned with the efficient implementation of multiplication in Finite fields. A thorough investigation of the implementation of multiplication on FPGAs using the two step and interleaved methods is carried out. Results are given for multiplication in the large field sizes required for elliptic curve cryptography.

Chapter 4 investigates the effect of side channel attacks and power analysis attacks in particular against the hardware implementation of the arithmetic operators presented in Chapter 3. An analysis of the leakage of information through the use of activity counting is carried on three multiplier designs. This analysis is novel and introduces a new concept of arithmetic operator level countermeasures to information leakage. This analysis is then used to propose new counter measures that eliminate this information leakage at a minimum cost in area and timing overhead.

Chapter 5 presents a summary and conclusions to the research.

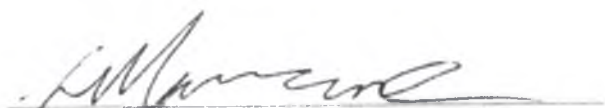
Standard of the Dissertation

The Dissertation is well written and presented, with a good structure. A logical and systematic analysis is carried out, with detailed implementations on Field Programmable Gate Arrays of the proposed architectures. The results of these implementations clearly support the arguments presented in the Dissertation. Another strength of this Dissertation is the thorough analysis of existing research in this area and a comparison to the proposed solutions. The candidate has developed a good understanding of the issues and developments in the area. The PhD Dissertation presents several original research contributions that clearly advance the state of the art.

One small criticism of the research presented relates to the field sizes considered. For much of Chapter 3, results for field sizes up to $m=512$ are analyzed. However subsequently the Dissertation focuses on field size $m=233$ in particular. The Dissertation would have benefited from results for the larger field sizes being presented for all designs or at least a statement on how the results scale up to the larger values of m .

Recommendation

The Dissertation of Danuta Pamula is of the standard required for a PhD and I recommend that the Dissertation be submitted for a public defense. In addition given the articles published as a result of the research I recommend that the award be "with distinction".



Dr Liam Marnane
Department of Electrical & Electronic Engineering
University College Cork
Ireland

22/11/2012