Efficient Finite Field Digit-Serial Multiplier Architecture for Cryptography Applications

Guido Bertoni[1], Luca Breveglieri[1], Pasqualina Fragneto[2]
[1]Politecnico di Milano , Italy - [2]ST Microelectronics Agrate Brianza (MI), Italy
[1]P.zza L. Da Vinci n. 32, I-20133 Milano, ITALY - [2]Via Olivetti 2, I-20041 Agrate B., ITALY
e-mail: Guido.Bertoni@PoliMI.IT, Luca.Breveglieri@PoliMI.IT, Pasqualina.Fragneto@ST.com

Abstract

Cryptographic applications in embedded systems for smart-cards require low-latency, low-complexity and low power dedicated hardvare. In this work the GBB *algorithm for finite field multiplication is optimised by recoding and the related digit-serial* VLSI *multiplier architecture is designed and evaluated* [6].

1. Introduction

A novel dedicated VLSI architecture for the efficient computation of multiplication in the finite fields of type $GF(2^n)$ is proposed, for some special values $n \in [150, 200]$. This architecture is intended as a basic functional block for the design of an efficient elliptic code (ECC) coprocessor [4] [5], suited for integration in a smart-card embedded system. The architecture is based on a novel multiplication algorithm proposed by Silverman [1]. In this work such algorithm is optimised by recoding and the related VLSI architecture (of digit-serial / parallel to parallel type) is designed at the functional blocks level, and is evaluated by means of SW simulation. Full details on algorithm, architecture and evaluations are in [6].

2. Algorithm and architecture

Until 1999 the multiplication algorithms for finite fields of type $GF(2^n)$ were related to two main representations for the elements of the field: *standard* (or polynomial) *basis* and *optimal normal basis*. In 1999 Silverman introduced a new algorithm [1], called *Ghost Bit Basis* (GBB). Given two n-bits factor polynomials $A(x)$ and $B(x)$, the GBB algorithm computes the product $C(x) = A(x)\ B(x) \bmod \phi(x)$, where $\phi(x)$ is the all-ones or cyclotomic polynomial $\phi(x) = x^n + x^{n-1} + \ldots + x + 1$. The algorithm can be mapped onto a VLSI LSB multiplier architecture of serial/parallel to parallel type, a well-known example of which is Paar's multiplier [2] [3], working for the standard basis representation.

In this work the GBB algorithm has been optimised for reducing time latency and power consumption, while bounding circuit complexity. The GBB LSB multiplication algorithm processes serially $A(x)$ and accumulates $B(x)$ to $C(x)$. The algorithm takes $n + 1$ clock cycles in total. The GBB algorithm can be recoded for speeding it up. The recoded GBB multiplication algorithm processes $k > 1$ bits of $A(x)$ per clock cycle. In this way the algorithm takes only $\lceil (n + 1) / k \rceil$ clock cycles. It can be mapped onto a digit-serial/parallel to parallel VLSI architecture. By SW simulation (in C language) the recoded GBB algorithm with $k = 4$ exhibits a speedup 2 with respect to normal GBB, while with $k = 2$ the speedup is 1.7. Power consumption follows a similar behaviour. The architecture contains a look-up table, of size related to the value of k. This table can be computed by HW or SW. For small values of k the size of the look-up table is limited. In case one factor is fixed, the contents of the look-up table are fixed as well.

3. Conclusions and further developments

The above analysis shows that the recoded GBB multiplication algorithm and the associated digit-serial VLSI architecture are suited for designing efficient finite field multipliers, since they allow short time latency, low power consumption and limited circuit complexity.

4. References

[1] J. H. Silverman, "Fast Multiplication in Finite Fields $GF(2^n)$", Proc. of CHESS '99, 1999, pp. 122-134

[2] C. Paar, "Implementation Options for Finite Fields Arithmetic for Elliptic Curve Cryptosystems", Proc. of 3rd Workshop on Elliptic Curve Cryptosystems, ECC '99, Waterloo, Ontario, Canada, November, 1999

[3] L. Song, K. Parhi, "Efficient Finite Field Serial / Parallel Multiplication", Proc. of ASAP '96, 1996, pp. 72-82

[4] M. Rosing, *"Implementing Elliptic Curve Cryptography*", Manning Publications, 1999

[5] A. Menezes, "*Elliptic Curve Public Key Cryptosystems*", Kluwer Academic Publishers Boston, 6th Printing, 1998

[6] G. Bertoni, L. Breveglieri, L. Cantini, P. Fragneto, "Efficient Digit-Serial Recoded Multiplier Architecture for Galois Fields" Int. Rep. n° 2000.46, Politecnico di Milano, Milano, Italy, December, 2000