Advanced Science and Technology Letters
Vol.134 (ACN 2016), pp.8-15
http://dx.doi.org/10.14257/astl.2016.134.02

Fast FPGA Implementations of Inversions for Special Irreducible Polynomials in Finite Fields

Haibo Yi[1], Weijian Li[2], Zhe Nie[1],

[1] School of Computer Engineering, Shenzhen Polytechnic. 518055 Shenzhen, China
[2] School of Computer Science, Guangdong Polytechnic Normal University. 510000 Guangzhou, China, weijianlee@126.com

haiboyi@126.com, weijianlee@126.com, niezhe@szpt.edu.cn

Abstract. Inversions in finite field have been playing a key role in areas of cryptography and engineering. The main algorithms for finite field inversions are based on Fermat's little theorem, extended Euclidean algorithm and other methods. We present techniques to exploit special irreducible polynomials for fast inversions in finite fields $GF(2^n)$, where n is a positive integer. We propose fast inversions based on Fermat's theorem for two special irreducible polynomials, i.e. trinomials and All-One-Polynomials (AOPs). Trinomials can be represented by polynomials $x^n + x^m + 1$ and AOPs can be represented by polynomials $x^n + x^{n-1} + ... + 1$, where m is a positive integer and 0<m<n. Our designs are programmed in Very-High-Speed Integrated Circuit Hardware Description Language (VHDL) by using Quartus II and implemented on a low-cost Field-Programmable Gate Array (FPGA). The experimental results show that our designs provide significant reductions in executing time.

Keywords: Inverter, finite field, Fermat's theorem, irreducible polynomial, trinomial, All-One-Polynomial (AOP), Field-Programmable Gate Array (FPGA)

1 Introduction

Finite field arithmetic has gained increasing importance due to the fact that it is one of the most fundamental operations in many areas, e.g. cryptography, signal processing and clustered file system. Among finite field arithmetic, multiplications and inversions have been received continuous attentions. Therefore, more and more designs and implementations of multiplications and inversions in finite fields have been proposed.

Irreducible polynomials are one for the focuses of finite fields due to the fact that they are playing an important role in finite field arithmetic: [1] proposes a multiplier for a special irreducible polynomial $x^n + x + 1$ in finite fields $GF(2^n)$, where n is a

ISSN: 2287-1233 ASTL

positive integer; [2] proposes a multiplier for trinomials in $GF(2^n)$, where m=1,2,...,n-1 and $m \neq n/2$; [3] proposes a multiplier for pentanomials in $GF(2^n)$; [4] proposes a multiplier for All-One-Polynomials (AOPs) and Equally-Spaced-Polynomials (ESPs) in $GF(2^n)$. Multiplications and inversions for special irreducible polynomials are efficient. However, there are few inversions for special irreducible polynomials.

We present techniques to exploit special irreducible polynomials for fast inversions in $GF(2^n)$. The main algorithms for finite field inversions are based on Fermat's little theorem [5-14], extended Euclidean algorithm [15-17] and other methods [18-24]. We propose fast inversions based on Fermat's theorem for two special irreducible polynomials, trinomials and AOPs, where trinomials can be represented by polynomials $x^n + x + 1$ and AOPs can be represented by polynomials $x^n + x^{n-1} + ... + 1$.

Our design is well suited for Field Programmable Logic Arrays (FPGAs). We back up the claims with implementations of our design on a low-cost Altera FPGA, which are programmed in Very-High-Speed Integrated Circuit Hardware Description Language (VHDL) by using Quartus II. The experimental results show that our designs provide significant reductions in executing time.

The rest of this paper is organized as follows: Section 2 introduces finite fields and inversions. Section 3 proposes fast inversions for special irreducible polynomials in finite fields. Section 4 presents implementations of our design on a low-cost Altera FPGA. Section 5 presents conclusions of this paper.

2 Preliminaries

In mathematics, a finite field is a field that contains a finite number of elements. As with any field, it is a set on which the basic operations of addition, multiplication and inversion have been defined.

The prime field $GF(p)$ of order and characteristic p is constructed as the integers modulo p, where p is a prime number. Thus, the elements are represented by integers in the range 0, ..., p-1. Given a prime power $q = 2^n$ with n > 1, the field $GF(q)$ can be explicitly constructed. One chooses first an irreducible polynomial f in $GF(2)[X]$ of degree n. Then the quotient ring $GF(q) = GF(2)[X]/f$ of the polynomial ring $GF(2)[X]$ by the ideal generated by f is a field of order q.

Suppose that a is an element in a finite field, the multiplicative inverse for a can be calculated a number of different ways. Brute-force search: by multiplying a by every number in the finite field until the product is one; Fermat's little theorem: since the nonzero elements of $GF(2^n)$ form a finite group with respect to multiplication, $a^{2^n-1} = 1$, thus the inverse of a is a^{2^n-2}; Extended Euclidean Algorithm; LUT [25].

3 Fast Inversions for Special Irreducible Polynomials in Finite Fields

3.1 Fast Inversions Based on Fermat's Theorem

First, let β be an element in $GF(2^n)$. According to Fermat's theorem [26], we have $\beta^{-1} = \beta^{2^n-2}$.

Since

$$2^n - 2 = \sum_{i=1}^{n-1} 2^i,$$

we have

$$\beta^{-1} = \prod_{i=1}^{n-1} \beta^{2^i}.$$

It can be observed that the first step is to compute β^{2^i}, where p(x) is the irreducible polynomial in $GF(2^n)$.

For $i = 1, 2, ..., n-1$, we compute

$$\beta^{2^i} = \sum_{j=0}^{n-1} u_{ij} x^{2^i \times j} \ mod \ p(x).$$

If p(x) is chosen, for $i = 1, 2, ..., n-1$, we can compute

$$x^{2^i \times j} \ mod \ p(x) = \sum_{j=0}^{n-1} v_j x^j.$$

Accordingly, for $i = 1, 2, ..., n-1$, we can compute

$$\beta^{2^i} = \sum_{j=0}^{n-1} k_{ij} x^j.$$

The second step of multiplicative inversion is to multiply $n-1$ elements, i.e. $\beta^2, \beta^4, ..., \beta^{2^{n-1}}$.

Finite field multiplication is performed in two steps. The first step is to perform the polynomial multiplication. The second step is to reduce modulo the irreducible polynomial.

Let $a(x) = \sum_{i=0}^{n-1} a_i x^i$ and $b(x) = \sum_{i=0}^{n-1} b_i x^i$ be elements in $GF(2^n)$, and

$$c(x) = a(x) \times b(x)(\mathrm{mod}\,(p(x))) = \sum_{i=0}^{n-1} c_i x^i$$

be the expected multiplication result.

First, we compute v_{ij} for $i = 0, 1, ..., 2(n-1)$ and $j = 0, 1, ..., n-1$ according to

$$x^i \bmod p(x) = \sum_{j=0}^{n-1} v_{ij} x^j.$$

Next, we compute S_i by AND logic gates for $i = 0,1,...,2(n-1)$ by
$S_i = \sum_{j+k=i} a_j b_k$.

After that, we compute c_i by XOR logic gates for $i = 0,1,...,n-1$ by
$c_i = \sum_{j=0}^{2(n-1)} v_{ji} S_j$.

Finally, the multiplication result is $c(x) = \sum_{i=0}^{n-1} c_i x^i$.

In sum, it can be observed from the above computations that efficient irreducible polynomials can provide significant reductions in executing time of inversions.

3.2 Fast Inversions for Trinomials $x^n + x + 1$

We present techniques to exploit special irreducible polynomials - trinomials $x^n + x + 1$ for fast inversions in $GF(2^n)$. Irreducible polynomials with the form of $x^n + x + 1$ in finite fields are summarized in Table 1, where some trinomials $x^n + x + 1$ cannot be chosen as irreducible polynomials, e.g. $x^5 + x + 1$, $x^8 + x + 1$.

Table 1. Irreducible Polynomials with the Form of $x^n + x + 1$ in Finite Fields.

Finite fields	Irreducible polynomials $x^n + x + 1$
$GF(2^2)$	$x^2 + x + 1$
$GF(2^3)$	$x^3 + x + 1$
$GF(2^4)$	$x^4 + x + 1$
$GF(2^6)$	$x^6 + x + 1$
$GF(2^7)$	$x^7 + x + 1$
$GF(2^9)$	$x^9 + x + 1$

Since $x^n + x + 1$ is chosen as the irreducible polynomial in $GF(2^n)$, for $i = 1,2,...,n-1$, $x^{2^i \times j}$ can be computed as follows.

$x^{2^i \times j}$ *mod* $(x^n + x + 1) = \sum_{j=0}^{n-1} v_j x^j$.

For $i = 0,1,...,n-1$, we compute x^i as follows.

x^i mod $p(x) = x^i$.

For $i = n$, we compute x^i as follows.

x^n mod $p(x) = x + 1$.

For $n < i < 2n-1$, we compute x^i as follows.

$x^i \bmod p(x) = x^{i-n+1} + x^{i-n}$.

It can be observed from that the inversions are efficient when the irreducible polynomials are $x^n + x + 1$ in $GF(2^n)$.

3.3 Fast Inversions for AOPs

We present techniques to exploit special irreducible polynomials - AOPs $x^n + x^{n-1} + ...x^2 + x + 1$ for fast inversions in $GF(2^n)$. Irreducible polynomials with the form of $x^n + x^{n-1} + ...x^2 + x + 1$ in finite fields are summarized in Table 2，where some AOPs $x^n + x + 1$ cannot be chosen as irreducible polynomials, e.g. $x^3 + x^2 + x + 1$, $x^5 + x^4 + ... + 1$, $x^7 + x^6 + ... + 1$, $x^8 + x^7 + ... + 1$, $x^9 + x^8 + ... + 1$, $x^{11} + x^{10} + ... + 1$.

Table 2. Irreducible Polynomials with the Form of $x^n + x^{n-1} + ... + 1$ in Finite Fields.

Finite fields	Irreducible polynomials $x^n + x^{n-1} + ... + 1$
$GF(2^2)$	$x^2 + x + 1$
$GF(2^4)$	$x^4 + x^3 + ... + 1$
$GF(2^6)$	$x^6 + x^5 + ... + 1$
$GF(2^{10})$	$x^{10} + x^9 + ... + 1$
$GF(2^{12})$	$x^{12} + x^{11} + ... + 1$

Since $x^n + x^{n-1} + ... + 1$ is chosen as the irreducible polynomial in $GF(2^n)$, for $i = 1, 2, ..., n-1$, $x^{2^i \times j}$ can be computed as follows.

$x^{2^i \times j} \; mod \; (x^n + x^{n-1} + ... + 1) = \sum_{j=0}^{n-1} v_j x^j$.

For $i = 0, 1, ..., n-1$, we compute x^i as follows.

$x^i \bmod p(x) = x^i$.

For $i = n$, we compute x^i as follows.

$x^n \bmod p(x) = x^{n-1} + x^{n-2} + ... + 1$.

For $n < i < 2n-1$, we compute x^i as follows.

$x^i \bmod p(x) = x^{i-n-1}$.

It can be observed from that the inversions are efficient when the irreducible polynomials are $x^n + x^{n-1} + ... + 1$ in $GF(2^n)$.

4 Implementation

In order to prove that our designs have low latency for inversions in $GF(2^n)$, the designs are modeled in VHDL by using Quartus II and implemented on EP2S130F1020I4 FPGA device, which is a member of ALTERA Stratix family. Table 3 gives insight in the performance of the implementations of our designs. The experimental results show that our designs provide significant reductions in executing time.

Table 3. Implementations of Inversions in Finite Fields for Special Irreducible Polynomials

Finite Fields	x^n+x+1 Time (ns)	AOPs Time (ns)	Normal Time (ns)
$GF(2^2)$	x^2+x+1 8.39	x^2+x+1 8.39	x^2+x+1 8.39
$GF(2^3)$	x^3+x+1 8.64	- -	x^3+x^2+1 8.65
$GF(2^4)$	x^4+x+1 8.61	$x^4+x^3...+1$ 8.61	x^4+x+1 8.61
$GF(2^6)$	x^6+x+1 8.87	$x^6+x^5+...+1$ 8.87	$x^6+x^4+x^2+x+1$ 8.88
$GF(2^7)$	x^7+x+1 18.80	- -	$x^7+x^6+...+x^2+1$ 22.60
$GF(2^9)$	x^9+x+1 22.81	- -	$x^9+x^8+x^6+...+1$ 25.06
$GF(2^{10})$	- -	$x^{10}+x^9+...+1$ 25.40	$x^{10}+x^3+x^2+...+1$ 27.61
$GF(2^{12})$	- -	$x^{12}+x^{11}+...+1$ 29.57	$x^{12}+x^3+x^2+...+1$ 31.19

5 Conclusion

Inversions in finite field have been playing a key role in many areas, e.g. cryptography, signal processing and clustered file system. We present techniques to exploit special irreducible polynomials for fast inversions in finite fields $GF(2^n)$, where n is a positive integer. We propose fast inversions based on Fermat's theorem for two special irreducible polynomials, i.e. trinomials and AOPs. Trinomials can be represented by polynomials x^n+x^m+1 and AOPs can be represented by polynomials $x^n+x^{n-1}+...+1$, where m is a positive integer and 0<m<n. Our designs are programmed in VHDL by using Quartus II and implemented on a low-cost ALTERA Stratix FPGA. The experimental results show that our designs provide significant reductions in executing time.

Acknowledgements. This work is supported by Major Project of Educational Scientific Planning of Shenzhen (No. ybfz15141), Ideological and Political Education Project of Shenzhen Polytechnic (No. 801522z20018), Shenzhen Science and Technology Program under Grant (No. JCYJ20150617155357681). Foundation for Distinguished Young Talents in Higher Education of Guangdong, China (No. 2014KQNCX177), and 2016 Guangdong Province Public Welfare Research and Ability Construction Project (Research on lightweight cryptographic chips for IoT that resist side-channel attacks), Quality Engineering Project of Department of Education of Guangdong Province (2014).

References

1. Paar, C.: A new architecture for a parallel finite field multiplier with low complexity based on composite fields. IEEE Transactions on Computers, 45(7):856-861, 1996.
2. Sunar, B. and Koc, C.K.: Mastrovito multiplier for all trinomials. Computers, IEEE Transactions on, 48(5):522-527, 1999.
3. Rodriguez-Henrquez, F., Koc, C. K.: Parallel multipliers based on special irreducible pentanomials. IEEE Transactions on Computers, pages 1535-1542, 2003.
4. Halbutogullari, A., Koc, C.K.: Mastrovito multiplier for general irreducible polynomials. Computers, IEEE Transactions on, 49(5):503-518, 2000.
5. Fenn, S.T.J., Benaissa, M., Taylor, D.: Fast normal basis inversion in $GF(2^n)$. Electronics Letters, 32:1566-1567, August 1996.
6. Rebeiro, C., Roy, S.S., Reddy, D.S., Mukhopadhyay, D.: Revisiting the Itoh-Tsujii inversion algorithm for FPGA platforms. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 19(8):1508-1512, 2011.
7. Azarderakhsh, R., Jarvinen, K., Dimitrov, V.: Fast inversion in $GF(2^m)$ with normal basis using hybrid-double multipliers. IEEE Transactions on Computers, 63(99):1041-1047, 2012.
8. Parrilla, L., Lloris, A., Castillo, E., Garcia, A.: Minimum-clock-cycle Itoh-Tsujii algorithm hardware implementation for cryptography applications over $GF(2^m)$ fields. Electronics Letters, 48(18):1126{1128, 2012.
9. Fenn, S.T.J., Benaissa, M., Taylor, D.: Finite field inversion over the dual basis. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 4(1):134-137, Mar. 1996.
10. Jing, M.-H., Chen, J.-H., Chen, Z.-H., Chen, Y.-H.: Low complexity architecture for multiplicative inversion in $GF(2^m)$. In IEEE Asia Pacific Conference on Circuits and Systems, APCCAS 2006, Singapore, pages 1492-1495. IEEE, Washington, DC, USA , 4-7 December 2006.
11. Dinh, A.V., Bolton, R.J., Mason, R.: A low latency architecture for computing multiplicative inverses and divisions in $GF(2^m)$. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 48(8):789-793, 2001.
12. Wang, C.C., Troung, T.K., Shao, H.M., Deutsch, L.J., Omura, J.K., Reed, I.S.: VLSI architectures for computing multiplications and inverses in $GF(2^m)$. IEEE Transactions on Computers, C-34(8):709{717, 1985.
13. Dinh, A.V., Palmer, R.J., Bolton, R. J., Mason, R.: A low latency architecture for computing multiplicative inverses and divisions in $GF(2^m)$. In 2000 Canadian

Conference on Electrical and Computer Engineering, Halifax, NS, Canada, volume 1, pages 43-47 vol.1. IEEE, Washington, DC, USA, 07-10 March 2000.
14. Itoh, T., Tsujii, S.: A fast algorithm for computing multiplicative inverses in $GF(2^m)$ using normal bases. Information and computation, 78(3):171-177, 1988.
15. Daneshbeh, A.K., Hasan, M.A.: A class of unidirectional bit serial systolic architectures for multiplicative inversion and division over $GF(2^m)$. IEEE Transactions on Computers, 54(3):370- 380, Mar. 2005.
16. Yan, Z., Sarwate, D.V.: New systolic architectures for inversion and division in $GF(2^m)$. IEEE Transactions on Computers, 52(11):1514-1519, Nov 2003.
17. Huang, C.-T., Wu, C.-W.: High-speed easily testable Galois field inverter. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 47(9):909{918, Sep 2000.
18. Jr. Kaliski, B.S: The Montgomery inverse and its applications. IEEE Transactions on Computers, 44(8):1064-1065, Aug. 1995.
19. Savas, E.: A carry-free architecture for Montgomery inversion. IEEE Transactions on Computers, 54(12):1508- 1519, Dec. 2005.
20. Bajard, J., Imbert, L., Negre, C.: Arithmetic operations in finite fields of medium prime characteristic using the lagrange representation. IEEE Transactions on Computers, 55(9):1167-1177, Sept 2006.
21. McIvor, C., McLoone, M., McCanny, J.V.: Improved Montgomery modular inverse algorithm. Electronics Letters, 40(18):1110-1112, Sept 2004.
22. Wei, S.-W.: VLSI architectures for computing exponentiations, multiplicative inverses, and divisions in $GF(2^m)$. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 44(10):847-855, Oct 1997.
23. Wang, C.-L., Lin, J.-L.,: A systolic architecture for computing inverses and divisions in finite fields $GF(2^m)$. IEEE Transactions on Computers, 42(9):1141-1146, Sep 1993.
24. Hasan, M.A., Bhargava, V.K.: Bit-serial systolic divider and multiplier for finite fields $GF(2^m)$. IEEE Transactions on Computers, 41(8):972-980, Aug 1992.
25. Hasan, M.A.: Look-up table-based large finite field multiplication in memory constrained cryptosystems. IEEE Transactions on Computers, 49(7):749-758, Jul 2000.
26. Schroeder, M.R., Schroeder, M.R.: Number theory in science and communication. Springer, 1984.