# $GF(2^n)$ Bit-Parallel Squarer Using Generalized Polynomial Basis For a New Class of Irreducible Pentanomials

Xi Xiong and Haining Fan

We present explicit formulae and complexities of bit-parallel $GF(2^n)$ squarers for a new class of irreducible pentanomials $x^n + x^{n-1} + x^k + x + 1$, where $n$ is odd and $1 < k < (n-1)/2$. The squarer is based on the generalized polynomial basis of $GF(2^n)$. Its gate delay matches the best results, while its XOR gate complexity is $n+1$, which is only about 2/3 of the current best results.

*Introduction:* Squarer is an important circuit building block in square-and-multiply-based exponentiation and inversion circuits. When $GF(2^n)$ elements are represented in a normal basis, squaring is simply a circular shift operation. Therefore, most previous works on squarers focused on other representations of $GF(2^n)$ elements.

For practical applications where values of $n$ are often in the range of $[1, 10000]$, $GF(2^n)$ can be defined by either an irreducible trinomial or an irreducible pentanomial. Paar et al. and Wu presented explicit squaring formulae of polynomial basis squarers for an arbitrary irreducible trinomial respectively [1], [2] and [3]. Using Montgomery's presentation with the factor $x^k$, Wu also proposed an optimized Montgomery squarer [4].

On the other hand, Hariri and Reyhani-Masoleh presented a Montgomery squarer for a special class of irreducible pentanomials $x^n + x^{k+1} + x^k + x^{k-1} + 1$ $(3 < k < (n-3)/2)$ [5]. For an arbitrary irreducible pentanomial, Park derived explicit formulae and complexities of squarers based on weakly dual basis [6]. The numbers of XOR gates used in these pentanomial-based squarers are about $1.5n$, and the gate delays of these squarers are $2T_X$, where $T_X$ is the delay of one 2-input XOR gate.

In this work, we consider bit-parallel squarers based on a new $GF(2^n)$ representation – generalized polynomial basis (GPB), which is defined by Cilardo and is a generalisation of the shifted polynomial basis [7].

*Definition 1: Let the ordered set $M = \{x^i | 0 \le i \le n-1\}$ be a polynomial basis of $GF(2^n)$ over $GF(2)$ and $R(x) \in GF(2^n)^*$. The ordered set $\{R(x)x^i | 0 \le i \le n-1\}$ is called a Generalized Polynomial Basis with respect to $M$.*

In [7], Cilardo presented a general analysis methodology to concisely express gate count, subexpression sharing, and time delay of parallel GPB multipliers. Specially, he suggested to define $GF(2^n)$ using the following two new classes of irreducible pentanomials:

Type **C.1**: $x^n + x^{n-1} + x^k + x + 1$ $(n-1 > k > 1)$ and

Type **C.2**: $x^n + x^{n-r} + x^q + x^r + 1$ $(n-r > q > r > 1)$.

His experiments revealed that at least one such pentanomial exists for all values of $n$ such that $n < 10,000$ and no degree-$n$ irreducible trinomial exists. The highlight of Cilardo's multipliers is that he selected a new parameter $R(x)$, which is not equal to $x^{-v}$ used in a shifted polynomial basis. Because of this new parameter, Cilardo showed that the complexities of such GPB multipliers match or outperform previous best parallel multipliers.

In the following, we present explicit formulae and complexities of GPB squarers in $GF(2^n)$ defined by Type **C.1** irreducible pentanomials, where $n$ is odd and $1 < k < (n-1)/2$. While the gate delays of the proposed GPB squarers match the best results, their XOR gate complexities are only $n+1$, which is lower than the current best result – about $1.5n$ reported in [5] and [6].

*GPB Squarers for Type* **C.1** *irreducible pentanomials:* Let $f(x) = x^n + x^{n-1} + x^k + x + 1$ be the type **C.1** irreducible pentanomial defining $GF(2^n)$. As indicated in [7], parameter $R(x) = x^{n-k} + x^{n-k-1} + 1$ can result in an optimised multiplier. In the following, we derive explicit expressions of the GPB squarers using this value of $R(x)$.

Given a $GF(2^n)$ element $A(x) = R(x)\sum_{i=0}^{n-1} a_i x^i$ represented in the GPB, its GPB square $C(x)$ is defined as

$$C(x) = R(x)\sum_{i=0}^{n-1} c_i x^i = R(x)\sum_{i=0}^{2n-2} R(x) a'_i x^i,$$

where $a'_i$ is defined as follows [3]:

$$a'_i = \begin{cases} a_{\frac{i}{2}} & \text{if } i \text{ is even,} \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, we have

$$\begin{aligned}
\sum_{i=0}^{n-1} c_i x^i &= \sum_{i=0}^{2n-2} R(x) a'_i x^i \\
&= \sum_{i=0}^{2n-2} (x^{n-k} + x^{n-k-1} + 1) a'_i x^i \\
&= \sum_{i=0}^{2n-2} (x^{1-k} + x^{-k}) a'_i x^i = \sum_{i=-k}^{2n-k-2} (x+1) a'_{i+k} x^i \\
&= r_- + r + r_+,
\end{aligned}$$

where $r_- = \sum_{i=-k}^{-1} (x+1) a'_{i+k} x^i$, $r = \sum_{i=0}^{n-1} (x+1) a'_{i+k} x^i$ and $r_+ = \sum_{i=n}^{2n-k-2} (x+1) a'_{i+k} x^i$.

The two terms $r_-$ and $r_+$ above should be reduced respectively by the following two reduction equations:

$$\begin{cases} x + 1 = x^n + x^{n-1} + x^k, & -k \le i \le -1, \\ x + 1 = x^{-n+1} + x^{-n+2} + x^{-n+k+1}, & n \le i \le 2n-k-2. \end{cases}$$

The reduced results are as follows:

$$\widetilde{r}_- = \sum_{i=n-k}^{n-1} a'_{i-n+k} x^i + \sum_{i=n-k-1}^{n-2} a'_{i-n+k+1} x^i + \sum_{i=0}^{k-1} a'_i x^i,$$

and

$$\widetilde{r}_+ = \sum_{i=1}^{n-k-1} a'_{i+n+k-1} x^i + \sum_{i=2}^{n-k} a'_{i+n+k-2} x^i + \sum_{i=k+1}^{n-1} a'_{i+n-1} x^i.$$

Moreover, the term $\sum_{i=0}^{n-1} a'_{i+k} x^{i+1}$ of $r$ should also be reduced. So we have

$$r = a'_{n+k-1} x^n + \sum_{i=1}^{n-1} a'_{i+k-1} x^i + \sum_{i=0}^{n-1} a'_{i+k} x^i,$$

where $x^n = x^{n-1} + x^k + x + 1$.

Therefore, we obtain the following expression:

$$\begin{aligned}
\sum_{i=0}^{n-1} c_i x^i &= \left(\sum_{i=0}^{n-1} a'_{i+k} x^i + \sum_{i=1}^{n-1} a'_{i+k-1} x^i\right) \\
&+ \left(\sum_{i=1}^{n-k-1} a'_{i+n+k-1} x^i + \sum_{i=n-k-1}^{n-2} a'_{i-n+k+1} x^i\right) \\
&+ \left(\sum_{i=2}^{n-k} a'_{i+n+k-2} x^i + \sum_{i=n-k}^{n-1} a'_{i-n+k} x^i\right) \\
&+ \left(\sum_{i=0}^{k-1} a'_i x^i + \sum_{i=k+1}^{n-1} a'_{i+n-1} x^i\right) + a'_{n+k-1}(x^{n-1} + x^k + x + 1).
\end{aligned}$$

In [7], the following reciprocal property was proved: the circuit performing the GPB multiplication for a given irreducible polynomial $f(x) = x^n + x^{n-1} + x^k + x + 1$ with $k > n/2$ and a certain GPB parameter $R(x)$ is as same as the circuit for polynomial $g(x) = x^n + x^{n-1} + x^{\tilde{k}} + x + 1$ with $\tilde{k} = n - k < n/2$ and parameter $R'(x) = R(x^{-1}) \cdot x^{-(n-1)}$. Therefore, we only need to consider the case of $1 < k < (n-1)/2$. Similar to [5] and [6], we also consider only the case of "$n$ odd" in this work. The other reason that we do not consider even values of $n$ is that, for security reasons, there are always concerns about using composite extension Galois fields to construct elliptic curve cryptosystems.

---

Xi Xiong and Haining Fan are with the Key Laboratory for Information System Security, Ministry of Education; Tsinghua National Laboratory for Information Science and Technology; School of Software, Tsinghua University, Beijing, China, 100084. E-mails: xixiong91@gmail.com, fhn@tsinghua.edu.cn

For the case $3 < k < (n-1)/2$, we can obtain the explicit expressions of $c_i$ $(0 \le i \le n-1)$ by comparing the coefficients of $x^i$ in the above equation. These expressions can be grouped into nine cases depending on the values of $i$:

**Case 1:** $i = 0$

$$c_0 = a'_k + a'_0 + a'_{n+k-1};$$

**Case 2:** $i = 1$

$$c_1 = a'_{k+1} + a'_k + a'_{n+k} + a'_{n+k-1};$$

**Case 3:** $2 \le i \le k-1$

$$c_i = a'_{i+k} + a'_{i+k-1} + a'_{i+n+k-1} + a'_{i+n+k-2} + a'_i;$$

**Case 4:** $i = k$

$$c_k = a'_{2k} + a'_{n+2k-1} + a'_{n+2k} + a'_{n+k-1};$$

**Case 5:** $k+1 \le i \le n-k-2$

$$c_i = a'_{i+k} + a'_{i+k-1} + a'_{i+n+k-1} + a'_{i+n+k-2} + a'_{i+n-1};$$

**Case 6:** $i = n-k-1$

$$c_{n-k-1} = a'_{n-1} + a'_{n-2} + a'_{2n-2} + a'_0 + a'_{2n-k-2};$$

**Case 7:** $i = n-k$

$$c_{n-k} = a'_n + a'_{n-1} + a'_0 + a'_{2n-k-1} + a'_{2n-2};$$

**Case 8:** $n-k+1 \le i \le n-2$

$$c_i = a'_{i+k} + a'_{i+k-1} + a'_{i-n+k} + a'_{i-n+k+1} + a'_{i+n-1};$$

**Case 9:** $i = n-1$

$$c_{n-1} = a'_{n+k-2} + a'_{k-1} + a'_{2n-2}.$$

The above expressions can be further simplified since $a'_i = 0$ when $i$ is odd. Therefore, we have the following explicit formulae of $c_i$ for the case "$n$ odd, $k$ even":

$$c_i = \left\{ \begin{array}{ll} \underline{a'_k + a'_{n+k-1}} + a_0 & i = 0, \\ \underline{a'_k + a'_{n+k-1}} & i = 1, \\ \underline{a'_{i+k} + a'_{i+n+k-1}} + a'_i & i \doteq 2, \ldots, k-2, \\ \underline{a'_{i+k-1} + a'_{i+n+k-2}} & i \doteq 3, \ldots, k-1, \\ \underline{a'_{i+k} + a'_{i+n+k-1}} + a'_{i+n-1} & i \doteq k, \ldots, n-k-3, \\ \underline{a'_{i+k-1} + a'_{i+n+k-2}} & i \doteq k+1, \ldots, n-k-2, \\ \underline{a_0 + a'_{n-1}} + a_{n-1} + a'_{2n-k-2} & i = n-k-1, \\ \underline{a_0 + a'_{n-1}} + a_{n-1} & i = n-k, \\ \underline{a'_{i+k} + a'_{i-n+k+1}} + a'_{i+n-1} & i \doteq n-k+1, \ldots, n-3, \\ \underline{a'_{i+k-1} + a'_{i-n+k}} & i \doteq n-k+2, \ldots, n-2, \\ a_{n-1} & i = n-1, \end{array} \right. \quad (1)$$

where "$i \doteq j, \ldots, l$" denotes that "$i = j, j+2, j+4, \ldots, l-2, l$".

The total number of "+" in (1) is $\frac{3n+1}{2}$. However, there are some common expressions, which are underlined, and $1 + \frac{k-2}{2} + \frac{n-2k-1}{2} + 1 + \frac{k-2}{2} = \frac{n-1}{2}$ XOR gates can be saved. Therefore the total number of XOR gates used in the GPB squarer is $n+1$ for the case "$n$ odd, $k$ even".

Similarly, for the case "$n$ odd, $k$ odd", we have

$$c_i = \left\{ \begin{array}{ll} a_0 & i = 0, \\ \underline{a'_{k+1} + a'_{n+k}} & i = 1, \\ \underline{a'_{k+1} + a'_{n+k}} + a_1 & i = 2, \\ \underline{a'_{i+k} + a'_{i+n+k-1}} & i \doteq 3, \ldots, k-2, \\ \underline{a'_{i+k-1} + a'_{i+n+k-2}} + a'_i & i \doteq 4, \ldots, k-1, \\ \underline{a'_{i+k} + a'_{i+n+k-1}} & i \doteq k, \ldots, n-k-3, \\ \underline{a'_{i+k-1} + a'_{i+n+k-2}} + a'_{i+n-1} & i \doteq k+1, \ldots, n-k-2, \\ a'_{n-1} + \underline{a_{n-1} + a_0} & i = n-k-1, \\ a'_{n-1} + a'_{2n-k-1} + \underline{a_{n-1} + a_0} & i = n-k, \\ \underline{a'_{i+k} + a'_{i-n+k+1}} & i \doteq n-k+1, \ldots, n-2, \\ \underline{a'_{i+k-1} + a'_{i-n+k}} + a'_{i+n-1} & i \doteq n-k+2, \ldots, n-1. \end{array} \right. \quad (2)$$

The total number of "+" in (2) is also $\frac{3n+1}{2}$, and $1 + \frac{k-3}{2} + \frac{n-2k-1}{2} + 1 + \frac{k-1}{2} = \frac{n-1}{2}$ XOR gates can be saved. Therefore the total number of XOR gates used in the GPB squarer is $n+1$ for the case "$n$ odd, $k$ odd".

The formulae for the two cases "$k = 2$" and "$k = 3$" are slightly different from (1) and (2), but the total number of XOR gates is also $n+1$ for the case "$n$ odd".

Finally, we summarise the proposed GPB squarers as follows:

*Theorem 1: Let $GF(2^n)$ be generated by the irreducible pentanomial $f(x) = x^n + x^{n-1} + x^k + x + 1$ ($n$ is odd and $1 < k < \frac{n-1}{2}$) and the GPB parameter $R(x) = x^{n-k} + x^{n-k-1} + 1$. Then a bit-parallel GPB squarer can be constructed using $n+1$ XOR gates. The gate delay of this squarer is $2T_X$.*

*An Example:* Type **C.1** pentanomial $f(u) = x^{11} + x^{10} + x^4 + x + 1$ is irreducible over $GF(2)$. Given a $GF(2^{11})$ element $A(x) = R(x)\sum_{i=0}^{10} a_i x^i$ represented in the GPB, where $R(x) = x^7 + x^6 + 1$, coefficients $c_i$s of its GPB square $C(x) = R(x)\sum_{i=0}^{n-1} c_i x^i$ are as follows:

$$\begin{array}{ll} c_0 = a_0 + (a_2 + a_7), & c_5 = a_4 + a_9, \\ c_1 = a_2 + a_7, & c_6 = (a_0 + a_5) + (a_8 + a_{10}), \\ c_2 = a_1 + (a_3 + a_8), & c_7 = (a_0 + a_5) + a_{10}, \\ c_3 = a_3 + a_8, & c_8 = (a_1 + a_6) + a_9, \\ c_4 = a_7 + (a_4 + a_9), & c_9 = a_1 + a_6, \\ & c_{10} = a_{10}. \end{array}$$

The coefficient $c_6$ can also be computed using $c_6 = c_7 + a_8$, which can save 1 XOR gate, but the gate delay of the squarer increases to $3T_X$.

*Conclusions:* While keeping the same gate delays as those of $GF(2^n)$ squarers using other representations [5] [6], the number of XOR gates used in the proposed GPB squarer is only about 2/3 of previous best results.

Our experiments revealed that for $n \in [10, 999]$, there are 452 $n$ values that no degree-$n$ irreducible trinomial exists. Among them, there are 292 $n$ values that degree-$n$ Type **C.1** irreducible pentanomials exist. Especially, NIST has recommended five finite fields $GF(2^n)$ for the elliptic curve digital signature algorithm: $GF(2^{163})$, $GF(2^{233})$, $GF(2^{283})$, $GF(2^{409})$ and $GF(2^{571})$, but no irreducible trinomials exist for three of them, namely, 163, 283 and 571. For these three fields, Type **C.1** irreducible pentanomials exist, e.g., $x^{163} + x^{162} + x^{25} + x + 1$, $x^{283} + x^{282} + x^{66} + x + 1$ and $x^{571} + x^{570} + x^9 + x + 1$ are irreducible over $GF(2)$. Therefore, GPB squarers defined by Type **C.1** irreducible pentanomials are of importance for both theoretical and practical purposes.

We had examined some expressions of GPB squarers for Type **C.2** irreducible pentanomials. Because parameters $q$ and $r$ ($n - r > q > r > 1$) are arbitrary integers, it becomes difficult to summarise a simple and coherent expression for a GPB squarer. Nevertheless, for a given Type **C.2** irreducible pentanomial, it is possible to derive explicit formulae of a GPB squarer, and then obtain its exact time and space complexities.

*Acknowledgment:* The work was supported by NSFC under grant No. 61373141 and 91218302, and 973 project No. 2010CB328004.

## References

1 C. Paar, P. Fleischmann and P. Soria-Rodriguez, "Fast Arithmetic for Public-Key Algorithms in Galois Fields with Composite Exponents," *IEEE Trans. Comput.*, vol. 48, no. 10, pp. 1025-1034, 1999.

2 H. Wu, "Low Complexity Bit-Parallel Finite Field Arithmetic Using Polynomial Basis," *Proc. First Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES)*, LNCS-1717, pp. 280-291, 1999.

3 H. Wu, "Bit-parallel Finite Field Multiplier and Squarer Using Polynomial Basis," *IEEE Trans. Comput.*, vol. 51, no. 7, pp. 750-758, July 2002.

4 H. Wu, "Montgomery Multiplier and Squarer for a Class of Finite Fields," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 521-529, May 2002.

5 A. Hariri and A. Reyhani-Masoleh, "Bit-Serial and Bit-Parallel Montgomery Multiplication and Squaring over $GF(2^m)$," *IEEE Trans. Comput.*, vol. 58, no. 10, pp. 1332-1345, OCT, 2009.

6 S. M. Park, "Explicit Formulae of Polynomial Basis Squarer for Pentanomials Using Weakly Dual Basis," *Integration, the VLSI journal*, vol. 45, no. 2, pp. 205-210, 2012.

7 A. Cilardo, "Fast Parallel $GF(2^m)$ Polynomial Multiplication for All Degrees," *IEEE Transactions on Computers*, vol. 62, no. 5, pp. 929-943, May 2013.