

Finite Field Expansion Methods for the More Secure Information Protecting Code

Hyeong-Keon An

Department of Information and Telecommunication Engineering,
 Tong Myung University, 608-711 Pusan, Republic of Korea

Abstract: We show the method of expanding the order of the finite field. As the order becomes bigger and bigger, the more powerful security code comes out, since, the encrypting code becomes the more and more difficult to decrypt. This is because the number of the occurring cases is exponentially increasing as the order of the primitive equation of the finite field is increasing. In this study, we show the method to expand the finite field length. Especially, the zero crossing detector is designed and designing method is precisely described.

Key words: Reed Solomon, zero crossing detector, VHDL, asymmetric encryption, cyphertext, $GF(2^{16})$, internet data

INTRODUCTION

In this study, we describes how to expand the order of the Reed Solomon code system to make the more secure and powerful security code. As the order of the finite field is increasing, everytime the number of the occurring cases is doubling, so, decrypting the code becomes more and more difficult, so that, means the code becomes the more secure and stable. In this study, we describes the way to expand the code length of the finite field code, especially, the Reed Solomon code. Here, operation method and apparatus over Galois Field $GF(2^m)$ using a subfield $GF(2^{m/2})$ are described (Keon, 2016). In this study, we show the designing method to make the zero crossing detector circuit. Here, the VHDL language is used to get the solution and later we can synthesize the hardware circuit to expand the order of the finite field. Using this method we can find the solution of the equations $\beta^2 + \beta = \gamma$ and $\gamma^4 + \gamma^3 + 1 = 0$ for transforming the $GF(2^4)$ field into the $GF(2^8)$ field. We can generalize the method for transforming the $GF(2^{m/2})$ field into the $GF(2^m)$ field (Billinton and Khan, 1992). In this study, we apply the algorithm to expand the order from $GF(2^4)$ to the order of $GF(2^8)$ more precisely. VHDL simulation is shown in the chapter. In this study, we show the expanding method from the order of $GF(2^8)$ to $GF(2^{16})$. Finally, in this study, concluding remarks is made and our future research is described (Ferguson and Schneier, 2003). The powerful higher order multiplier and divider will be designed and real application to the data protection will be performed. Once higher order is realized, a reversion circuit for reverting the operated elements represented by the basis of the $GF(2^{m/2})$ field to the elements represented by the

basis of $GF(2^m)$ can easily be designed. The transforming circuits multiplier, divider, inverse circuit are also designed and described (Cormen *et al.*, 2001).

MATERIALS AND METHODS

Algorithm to expand the order of the finite field: An operational method and apparatus over Galois Field $GF(2^m)$ using a subfield $GF(2^{m/2})$ is described in the study. This field extension gives us a more powerful and secure code system for us to implement the more stable and powerful endecryption system. The operation apparatus includes a conversion circuit for converting the elements represented by a basis of $GF(2^m)$ into the elements represented by a basis of $GF(2^{m/2})$ with respect to the elements represented by the basis of $GF(2^{m/2})$. In this way, we can expand the finite field from the $GF(2^{m/2})$ field to the $GF(2^m)$ field (Hyeong-Keon, 2013).

If we summarize the theory when we expand the field from $GF(2^4)$ to the $GF(2^8)$ field, we do the followings. Suppose that a root of a Primitive polynomial $P(x)$ of $GF(2^8)$ is α , then $\alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1 = 0$. Suppose also that a root of a primitive polynomial $P(x)$ of $GF(2^4)$ is γ , then $\gamma^4 + \gamma^3 + 1 = 0$. Here, we should find the element $\gamma \in GF(2^8)$ which satisfy $\beta^4 + \beta^3 + 1 = 0$. It is α^{119} . Also, we should find the element $\beta \in GF(2^8)$ to satisfy $\beta^2 + \beta + \gamma = 0$ and it is α^7 . As we see we need the zero crossing detector circuit. Figure 1 shows one example of the zero crossing detector. A more detailed description is as follows. Suppose that $\alpha^4 \in GF(2^8)$ is represented as $a + b\beta$ where $a, b \in GF(2^4)$ and $\beta \in GF(2^8)$. If so, suppose that an arbitrary element over $GF(2^8)$ is:

$$\alpha^K = \sum_{i=0}^3 z_i \gamma^i + \beta \sum_{i=4}^7 z_i \gamma^i$$

where $\gamma \in \text{GF}(2^8)$ and $\text{GF}(2^4)$, $z_i = \{0, 1\}$

Notice also:

$$\{\lambda_i\} = \{1, \gamma, \gamma^2, \gamma^3, \beta, \beta\gamma, \beta\gamma^2, \beta\gamma^3\}$$

and $\{\lambda_i\}$ is mutually independent (Schneier, 1996). From the zero crossing detector, we know $\gamma \in \text{GF}(2^8)$ is α^{119} and β is α^7 . According to the above, the basis over $\text{GF}(2^4)$ of $\text{GF}(2^8)$ is:

$$\{1, \gamma, \gamma^2, \gamma^3, \beta, \beta\gamma, \beta\gamma^2, \beta\gamma^3\} = \{1, \alpha^{119}, \alpha^{238}, \alpha^{102}, \alpha^7, \alpha^{126}, \alpha^{245}, \alpha^{109}\}$$

and an arbitrary element Z is represented by the above basis as follows:

$$Z = z_0 + z_1 \alpha^{119} + \alpha^{238} + z_3 \alpha^{102} + z_4 \alpha^7 + z_5 \alpha^{126} + z_6 \alpha^{245} + z_7 \alpha^{109} = (z_0 + z_1 + z_2 + z_6 + z_7) + (z_1 + z_2 + z_5) \alpha + (z_3 + z_5 + z_7) \alpha^2 + (z_2 + z_6 + z_7) \alpha^3 + (z_1 + z_7) \alpha^4 + (z_5 + z_6 + z_7) \alpha^5 + (z_3 + z_5 + z_6) \alpha^6 + (z_1 + z_4 + z_6 + z_7) \alpha^7$$

(1)

From the Eq. 1, a conversion formula from elements represented by the basis of $\text{GF}(2^4)$ into elements represented by the basis of $\text{GF}(2^8)$ can easily be derived (Schneier, 1996).

Zero crossing detector circuit design to expand the order of the finite field: Now:

$$\beta^2 + \beta + \alpha^{119} = \{a_0 + a_1 \alpha + a_2 \alpha^2 + a_3 \alpha^3 + \dots + a_7 \alpha^7\}^2 + \{a_0 + a_1 \alpha + a_2 \alpha^2 + a_3 \alpha^3 + a_7 \alpha^7\} + \alpha^{119} = 0 \quad (2)$$

Hence:

$$\begin{aligned} \{a_0 + a_1 \alpha + a_2 \alpha^2 + a_3 \alpha^3 + \dots + a_7 \alpha^7\}^2 = \\ a_0 + a_1 \alpha^2 + a_2 \alpha^4 + a_3 \alpha^6 + a_4 (1, 0, 1, 1, 0, 0, 0, 0) + \\ a_5 (0, 0, 1, 0, 1, 1, 1, 0) + a_6 (1, 0, 1, 1, 0, 0, 1, 1) + a_7 \\ (1, 1, 0, 0, 1, 0, 0, 0) = (a_0 + a_4 + a_6 + a_7, a_7, a_1 + a_4 + \\ a_5 + a_6, a_2 + a_4 + a_5 + a_7, a_5, a_3 + a_5 + a_6, a_6) \end{aligned} \quad (3)$$

From Eq. 2 and 3:

$$\begin{aligned} (a_4 + a_6 + a_7, a_1 + a_7, a_1 + a_4 + a_5 + a_6 + a_2, \\ a_6 + a_3, a_2 + a_5 + a_7, 0, a_3 + a_5, a_6 + a_7) + \\ (1, 1, 0, 0, 1, 0, 0, 1) = (0, 0, 0, 0, 0, 0, 0, 0) \end{aligned} \quad (4)$$

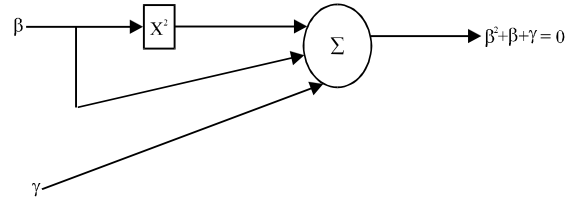


Fig. 1: Zero crossing detector application

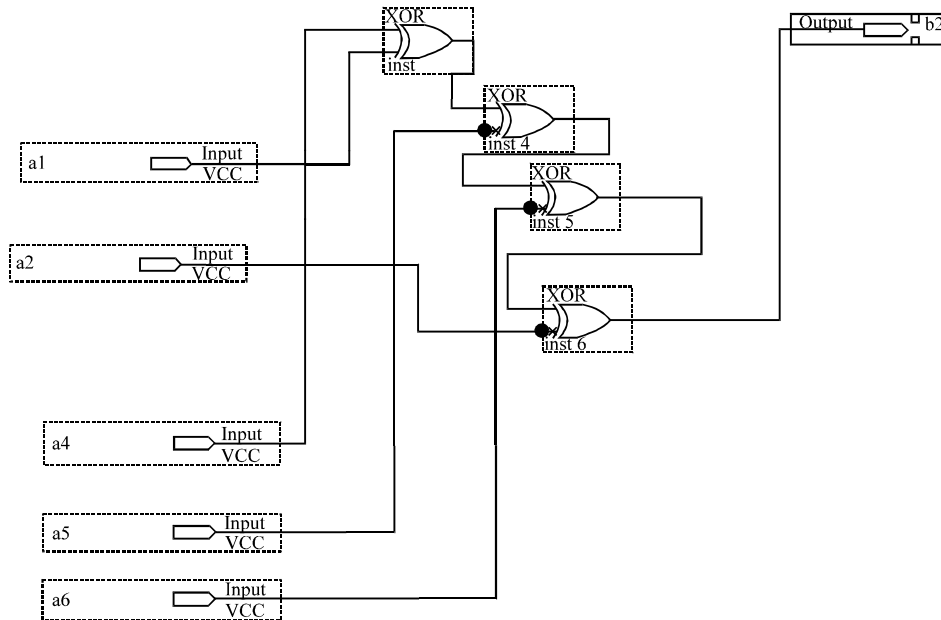


Fig. 2: $\alpha^2 + \alpha$ mapping from α field (b2 element)

Hence, using Eq. 4, we substitute $\beta = \alpha^i$ ($i = 0, 1, 2, \dots, 255$) to find the solution of the Eq. 4. It is α^7 . The solution is found by the VHDL simulation. In Fig. 2, we see $\alpha^2 + \alpha$ mapping from α (b2 element), $b2 = a1 + a2 + a4 + a5 + a6$.

RESULTS AND DISCUSSION

Inverse logic construction and the results: Assuming that the inverse of Z is Z^{-1} and:

$$Z^{-1} = y0 + \beta y1$$

where, $\beta^2 = \beta + \gamma$ then:

$$\begin{aligned} Z \times Z^{-1} &= (x0 + \beta x1) (y0 + \beta y1) = x0y0 + \\ &x1y1\gamma + \beta (x1y0 + (x0 + x1) y1) = 1 \end{aligned} \quad (5)$$

$(\because \beta^2 = \beta + \gamma)$

So, from Eq. 5:

$$\begin{aligned} x0y0 + x1y1\gamma &= 1 \text{ and} \\ x1y0 + (x0 + x1) y1 &= 0 \end{aligned} \quad (6)$$

From the Eq. 6:

$$\begin{aligned} y0 &= \frac{x0 + x1}{x0 (x0 + x1) + \gamma x1^2} \\ &= \frac{x0 + x1}{\Delta}, y1 = \frac{x1}{\Delta} \end{aligned}$$

Where:

$$\Delta = x0 (x0 + x1) + \gamma x1^2 \quad (7)$$

Using Eq. 7, we can derive the divider circuit. Here, to implement the γA^2 circuit, suppose that the element A is represented $a0 + a1\gamma + a2\gamma^2 + a3\gamma^3$. Where $\gamma^4 = \gamma^3 + 1$. Then, $\gamma A^2 = (a2 + a3) + (a0 + a2 + a3)\gamma + a3\gamma^2 + (a1 + a2)\gamma^3$. So, the circuit of the Eq. 7 can be implemented easily (Keon, 2016). Similarly, γA is represented as the Eq. 8:

$$\gamma A = (a3 + a0\gamma + a1\gamma^2 + (a2 + a3)\gamma^3) \quad (8)$$

CONCLUSION

In this study, we show the field expansion method to derive the more powerful and secure endecryption code.

RECOMMENDATIONS

In future, we want to derive the more economical hardware to implement the above algorithm. That means we will derive the powerful ALU which performs the very powerful secure endecryption process. Especially γA and γA^2 circuit is implemented for the inverse circuit for the field transformation (Billinton and Khan, 1992).

ACKNOWLEDGEMENT

"This research was supported by the Tongmyong University Research Grants 2016".

REFERENCES

- Billinton, R. and E. Khan, 1992. A security based approach to composite power system reliability evaluation. IEEE. Trans. Power Syst., 7: 65-72.
- Cormen, T.H., C.E. Leiserson, R.L. Rivest and C. Stein, 2001. Introduction to Algorithms. 2nd Edn., The MIT Press, Cambridge, UK., ISBN-13: 9780262032933, Pages: 1180.
- Ferguson, N. and B. Schneier, 2003. Practical Cryptography. Wiley, Hoboken, New Jersey, USA., ISBN: 9780471223573, Pages: 410.
- Hyeong-Keon, A., 2013. Fast and low cost GF(28) multiplier design based on double subfield transformation. Intl. J. Software Eng. Appl., 7: 285-294.
- Keon, A.H., 2016. Security of wireless sensor network using the subfield transformed reed Solomon code. Intl. Inf. Inst. Tokyo Inf., 19: 1587-1592.
- Schneier, B., 1996. Applied Cryptography. 2nd Edn., John Wiley and Sons, Australia, ISBN: 0-471-11709-9.