Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 16(3): 166-172, Sep. 2018 Regular paper

Relation between the Irreducible Polynomials that Generates the Same Binary Sequence Over Odd Characteristic Field

Md. Arshad Ali[1*], Yuta Kodera[1], Taehwan Park[2], Takuya Kusaka[1], Yasuyuki Nogmi[1], and Howon Kim[2], *Member*, *KIICE*

[1]Department of Information and Communication Systems, Okayama University, Okayama 700-8530, Japan
[2]Department of Electrical and Computer Engineering, Pusan National University, Busan 46241, Korea

Abstract

A pseudo-random sequence generated by using a primitive polynomial, trace function, and Legendre symbol has been researched in our previous work. Our previous sequence has some interesting features such as period, autocorrelation, and linear complexity. A pseudo-random sequence widely used in cryptography. However, from the aspect of the practical use in cryptographic systems sequence needs to generate swiftly. Our previous sequence generated by utilizing a primitive polynomial, however, finding a primitive polynomial requires high calculating cost when the degree or the characteristic is large. It's a shortcoming of our previous work. The main contribution of this work is to find some relation between the generated sequence and irreducible polynomials. The purpose of this relationship is to generate the same sequence without utilizing a primitive polynomial. From the experimental observation, it is found that there are $(p-1)/2$ kinds of polynomial, which generates the same sequence. In addition, some of these polynomials are non-primitive polynomial. In this paper, these relationships between the sequence and the polynomials are shown by some examples. Furthermore, these relationships are proven theoretically also.

Index Terms: Irreducible polynomial, Legendre symbol, Odd characteristic field, Pseudo-random sequence, Trace function

I. INTRODUCTION

Pseudo-random sequences have been widely employed in the field of information security and cryptography as a key stream of one-time pads, secret keys of symmetric cipher system, public key parameters, and so on [1-4]. To ensure the security of these cryptosystems, the pseudo-random sequence should have unpredictable random quantities, as well as sequence needs to generate very rapidly. The unpredictability of a sequence can be achieved by using some nonlinear mathematical calculation during the sequence generation procedure. On the other hand, to generate a sequence very swiftly, the expensive calculation needs to be avoided. Other pseudo-random sequences, such as M-sequence [5, 6] and Legendre sequence [7, 8] have been researched well due to most of their important properties already theoretically proven.

The authors previous work [9] proposed a new binary sequence by combining the features of an M-sequence and Legendre sequence. The generation procedure of our previous sequence includes three steps. Firstly, it utilized a primitive polynomial to generate maximum length vector sequence. This idea comes from M-sequence. Then, the trace function is applied to transform all the vectors to scalars. Finally, Legendre symbol applied to the scalars to generate the binary sequence. It should be noted that Legendre symbol is a non-linear function, that's why our previous sequence holds unpredictability quality. This sequence has some prominent

Received 19 June 2018, **Revised** 28 July 2018, **Accepted** 30 July 2018
***Corresponding Author** Md. Arshad Ali (E-mail: arshad@s.okayama-u.ac.jp, Tel: +81-80-4266-1986)
Department of Information and Communication Systems, Okayama University, Okayama 700-8530, Japan.

Open Access https://doi.org/10.6109/jicce.2018.16.3.166 print ISSN: 2234-8255 online ISSN: 2234-8883

features also such as period, autocorrelation, and linear complexity. All these properties have been theoretically proven in our previous work [9].

As previously mentioned, during the sequence generation procedure, in the beginning, a primitive polynomial used. However, finding a primitive polynomial takes much calculation cost when the degree or the characteristic is large. In other words, it takes much longer time to find a higher degree primitive polynomial. To overcome this complication (finding a primitive polynomial during the sequence generation procedure), this paper focused on the properties of the irreducible polynomials (which generates the proposed sequence) to find some prominent features, by which we can find an efficient way of generating the sequence. The authors of this paper accomplish some experiment on generating a sequence by using our previous method. After careful observation, we found a relation between the irreducible polynomial and a sequence. The purpose of finding this relation is to generate the same sequence without the primitive polynomial. After the experimental observation, the authors found that there are $(p-1)/2$ kinds of polynomial exist, which generates the same sequence and some of these irreducible polynomials are non-primitive polynomials. In other words, according to the observation of this paper, the same binary sequence can be generated without using a primitive polynomial. This idea can overcome the drawback (finding primitive polynomial, which is an expensive calculation) of our previous work [8]. The relation between the polynomial and sequence are mentioned as theorems in this paper. Furthermore, these theorems are theoretically proven as well justified with the aid of some example.

Throughout this paper, p denotes an odd prime number and mm be a natural number that denotes the extension degree. Then, q denotes p^m and $\mathbb{F}_q$ be the extension field of $\mathbb{F}_p$. $\mathbb{F}_q^*$ denotes the multiplicative group of $\mathbb{F}_q$, that is $= \mathbb{F}_q^* - \{0\}$. The discussion of this paper is basically given over an odd characteristic prime field $\mathbb{F}_p$ as the base field; an arbitrary odd characteristic extension field is adaptable as the base field.

II. BACKGROUND

This section introduces some fundamental concepts of finite field theory as preliminaries of this research work such as binary sequence, primitive polynomial, trace function, and Legendre symbol. In addition, this section also introduces our previous work along with its properties.

A. Binary Sequence

The binary sequence in this paper is defined as follows.

$$S = \{s_i\}, i = 0, 1, 2, \cdots n-1, \cdots \tag{1}$$

where $s_i \in \{0, 1\}$ and n be the period of the sequence such as $s_{i+n} = s_i$ for arbitrary non-negative integer i.

B. Primitive Element and Primitive Polynomial

Every finite $\mathbb{F}_q$ has a primitive element. This primitive element becomes a generator of $\mathbb{F}_q^*$. Let ω be a generator, then every non-zero element can be represented by its power such as ω^i, for $i = 0, 1, 2, \cdots, q-2$. According to the Fermat's little theorem, the following property between $\mathbb{F}_q$ and its base field $\mathbb{F}_p$ holds [10].

PROPERTY 1. *Let ω be a generator in $\mathbb{F}_q^*$, $\omega^{(q-1)/(p-1)}$ becomes a certain non-zero element in the prime field $\mathbb{F}_p$ and it also becomes a generator in $\mathbb{F}_p$.*

Thus, the generator in $\mathbb{F}_p^*$ is described as follows.

$$g = \omega^{(q-1)/(p-1)}. \tag{2}$$

C. Trace Function

This work utilizes the trace function to map an element of the extension field $X \in \mathbb{F}_{p^m}$ to an element of the prime field $x \in \mathbb{F}_p$ as,

$$x = \mathrm{Tr}(X) = \sum_{i=0}^{m-1} X^{p^i}. \tag{3}$$

A crucial point, the above trace becomes a scalar value and the trace function has a linearity property as follows [10].

PROPERTY 2. *Let $a, b \in \mathbb{F}_p$ and $X, Y \in \mathbb{F}_{p^m}$, then the trace function has a linearity property over the prime field $\mathbb{F}_p$ as follows.*

$$\mathrm{Tr}(aX + bY) = a\mathrm{Tr}(X) + b\mathrm{Tr}(Y). \tag{4}$$

D. Legendre Symbol

The Legendre symbol (a/p) for an arbitrary element $a \in \mathbb{F}_q$ is defined as,

$$\left(a/p\right) = \begin{cases} 0, & \text{if } a = 0 \\ 1, & \text{else if } a \text{ is a non} - \text{zero QR} \\ -1, & \text{otherwise } a \text{ is a non} - \text{zero QNR.} \end{cases} \tag{5}$$

It is calculated as,

$$\left(a/p\right) = a^{(p-1)/2} \bmod p. \tag{6}$$

The Legendre symbol is basically used for checking

whether a is QR or not in $\mathbb{F}_p$. Here, QR and QNR stands for Quadratic Residue and Quadratic Non-Residue, respectively. This paper uses Legendre symbol for translating a scalar over $\mathbb{F}_p$ to a binary sequence. Then the Legendre symbol holds the following property [10].

PROPERTY 3. *Let a and b be non-zero elements in the prime field $\mathbb{F}_p$, then the Legendre symbol holds the following relation*

$$\left(ab/p\right) = \left(a/p\right)\left(b/p\right). \tag{7}$$

E. Previous Work

In our previous work [9], a binary sequence T has been proposed, which is generated by the following equation.

$$T = \{t_i\}, t_i = M_2\left(\left(\mathrm{Tr}(\omega^i)/p\right)\right), \tag{8}$$

where ω is a primitive element in the extension field $\mathbb{F}_{p^m}$ and the mapping function $M_2(\cdot)$ is defined as follows.

$$M_2(x) = \begin{cases} 0, & \text{if } x = 0, 1 \bmod p \\ 1, & \text{else if } x = -1 \bmod p. \end{cases} \tag{9}$$

Our previous sequence generated by using three parameters such as p, m, and $f(x)$, where p be an odd prime and $f(x)$ be a primitive polynomial of degree m.

This sequence has some interesting features such as period, autocorrelation, and linear complexity. These features have been theoretically proven in our previous work [8]. For example, the period n is given by

$$n = \frac{2(p^m - 1)}{p - 1}. \tag{10}$$

As a small example, when the parameters are set as $p = 7$, $m = 2$, and $f(x) = x^2 + 6x + 3$, then the generated sequence becomes as follows:

$$T = \{0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1\}. \tag{11}$$

III. CONSIDERATION OF THE POLYNOMIALS

The authors in this work found that there are $(p - 1)/2$ kinds of different irreducible polynomials that can generates the same sequence (which generated by our previous method with a certain primitive polynomial [9]). In this section, the authors firstly introduce the relation between the polynomials with the aid of some examples. In addition, these relations also explained mathematically as theorems in the later part of this section.

A. Examples

This paper considers the relation between the irreducible polynomials over the odd characteristic field. Therefore, to make the better understanding (the concept of this paper) for the readers, the authors utilize a small prime number 7 as p and its extension degree 2 as m to construct an odd characteristic field. Let $p = 7$, $m = 2$, and $f(x) = x^2 + 6x + 3$, then the generated sequence is shown in (11). If we utilize other irreducible polynomials such as $x^2 + 5x + 5$ or $x^2 + 3x + 6$, instead of $x^2 + 6x + 3$, then the generated sequence also becomes the same. In other words, the following polynomials generate the same binary sequence.

$$\begin{aligned} f_0(x) &= x^2 + 6x + 3, \\ f_1(x) &= x^2 + 5x + 5, \\ f_2(x) &= x^2 + 3x + 6. \end{aligned} \tag{12}$$

Again, let $p = 11$, $m = 2$, and $f(x) = x^2 + 5x + 2$, then the generated sequence becomes as follows.

$$\begin{aligned} T = \{&1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, \\ &0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0\}. \end{aligned} \tag{13}$$

Alike the former case, there are more polynomials which can generate the same sequence which is shown in (13). These polynomials are as follows.

$$\begin{aligned} f_0(x) &= x^2 + 5x + 2, \\ f_1(x) &= x^2 + 9x + 10, \\ f_2(x) &= x^2 + 3x + 6, \\ f_3(x) &= x^2 + x + 8, \\ f_4(x) &= x^2 + 4x + 7. \end{aligned} \tag{14}$$

From these examples, it should be noted that there are $(p - 1)/2$ kinds of irreducible polynomials for the case of $p = 7$ and 11 which generates the same sequence. Moreover, it is also found that there exists a non-primitive polynomial for each case. Actually, $x^2 + 3x + 6$ in (12) and $x^2 + 9x + 10$ in (14) are non-primitive polynomials.

B. The Relation between the Polynomials

As an example, the polynomials in (14) are considered in this section. Let ω_0, ω_1, ω_2, ω_3, ω_4 be the zeros of $f_0(x)$, $f_1(x)$, $f_2(x)$, $f_3(x)$, $f_4(x)$, respectively. Then, they hold the following relations.

$$\begin{aligned} \omega_0 &= \omega_0^{0\times 24+1} = 4^0\omega_0 \bmod f_0(\omega_0), \\ \omega_1 &= \omega_0^{1\times 24+1} = 4^1\omega_0 \bmod f_0(\omega_0), \\ \omega_2 &= \omega_0^{2\times 24+1} = 4^2\omega_0 \bmod f_0(\omega_0), \\ \omega_3 &= \omega_0^{3\times 24+1} = 4^3\omega_0 \bmod f_0(\omega_0), \\ \omega_4 &= \omega_0^{4\times 24+1} = 4^4\omega_0 \bmod f_0(\omega_0). \end{aligned} \tag{15}$$

In this case, we could find that $f_2(x)$ becomes the minimum polynomial of $\omega_0^{2\times24+1} = \omega_0^{49}$ as,

$$\begin{aligned} f_2(\omega_0^{2\times24+1}) &= (4^2\omega_0)^2 + 3(4^2\omega_0) + 6 \\ &= 3\omega_0^2 + 4\omega_0 + 6 \\ &= 3(\omega_0^2 + 5\omega_0 + 2) \\ &\equiv 0 \bmod f_0(\omega_0). \end{aligned} \tag{16}$$

Furthermore, it is also shown that the other polynomials become the minimal polynomial of given ω_0 as,

$$\begin{aligned} f_1(4^1\omega_0) &= 5\omega_0^2 + 3\omega_0 + 10 \\ &= 5(\omega_0^2 + 5\omega_0 + 2) \\ f_3(4^3\omega_0) &= 4\omega_0^2 + 9\omega_0 + 8 \\ &= 4(\omega_0^2 + 5\omega_0 + 2) \\ f_4(4^4\omega_0) &= 9\omega_0^2 + \omega_0 + 7 \\ &= 9(\omega_0^2 + 5\omega_0 + 2)\cdot \end{aligned} \tag{17}$$

Thus, $\omega_0^{5\times24+1}$ becomes ω_0^1 because of the period of the primitive element in this case is 120, which means there are no more polynomials that satisfies these relations. Therefore, it can be found that there are 5 (= (11 − 1)/2) kinds of polynomials that generate the same binary sequence.

Additionally, it is found that the non-primitive polynomial $f_1(x)$ holds the following relation with its zero $\omega_1 = \omega_0^{1\times24+1}$ as,

$$\gcd(1 \cdot 24 + 1, 120) \neq 1. \tag{18}$$

In the following section, such relations are considered from the theoretical aspect.

C. Theorems and Its Proofs

After a lot of experimental observation, following theorems are obtained. In this section, the authors mathematically prove these theorems.

THEOREM 1. *Let $f_0(x)$ and w_0 be a primitive polynomial and its zero, respectively. The polynomial fk(x), (were k = 0, 1, ⋯, ((p − 1)/2) - 1) generates the same sequence, if it's zero ω_k satisfies the following condition.*

$$\omega_k \equiv \omega_0^{2k\left(\frac{q-1}{p-1}\right)+1} \bmod f_0(\omega_0). \tag{19}$$

Proof. Let $T_0 = (t_{0,i}\}$ be the sequence which is generated by the polynomial $f_0(x)$. Again let $T_k = \{t_{k,i}\}$ be the sequence generated by the polynomial $f_k(x)$. Then, these sequences can be described as follows.

$$\begin{aligned} t_{0,i} &= M_2\left(\left(\mathrm{Tr}\left(\omega_0^i\right)\Big/p\right)\right), \\ t_{k,i} &= M_2\left(\left(\mathrm{Tr}\left(\omega_k^i\right)\Big/p\right)\right). \end{aligned} \tag{20}$$

According to the condition of the theorem and the property of a primitive element (Property 1),$t_{k,i}$ can be further modified as follows.

$$\begin{aligned} t_{k,i} &= M_2\left(\left(\mathrm{Tr}\left(\omega_0^{\left(2k\left(\frac{q-1}{p-1}\right)+1\right)i}\right)\Big/p\right)\right) \\ &= M_2\left(\left(\mathrm{Tr}\left(\omega_0^{\left(\frac{q-1}{p-1}\right)2ki}\cdot\omega_0^i\right)\Big/p\right)\right) \\ &= M_2\left(\left(\mathrm{Tr}\left(g^{2ki}\cdot\omega_0^i\right)\Big/p\right)\right). \end{aligned} \tag{21}$$

where g is a generator in $\mathbb{F}_p^*$. Then, from the linearity of the trace function (Property 2) and the calculation of the Legendre symbol (Property 3), the above formula can be described by the multiplication of the Legendre symbol as,

$$\begin{aligned} t_{c,i} &= M_2\left(\left((g^{ki})^2\mathrm{Tr}\left(\omega_0^i\right)\Big/p\right)\right) \\ &= M_2\left(\underline{\left(\left(g^{ki}\right)^2\Big/p\right)}\left(\mathrm{Tr}\left(\omega_0^i\right)\Big/p\right)\right) \end{aligned} \tag{22}$$

Because of $(g^{ki})^2$ is a QR, thus the value of the underline part in the above equation becomes 1. Then, finally the sequence $t_{k,i}$ can be obtained as follows.

$$t_{k,i} = M_2\left(\left(\mathrm{Tr}\left(\omega_0^i\right)\Big/p\right)\right), \tag{23}$$

which means that the formula is same as $t_{1,i}$ for arbitrary i, therefore, the theorem has been proven.

Let ω_0 be a primitive element of $g_0(x)$ (where $g_0(x)$ be a primitive polynomial) which belongs to the extension field $\mathbb{F}_{p^m}$ and it can generate a maximum of $p^m - 1$ elements as like the red circle as shown in Fig. 1. Therefore, ω_0 holds the following relation as,

$$\omega_0^{q-1} = \omega_0^{\frac{2(q-1)}{p-1}\times\underline{\frac{p-1}{2}}} = 1.$$

Let the underlined part in the above equation be denoted as k. Then the above equation becomes as follows.

$$\omega_0^{\frac{2(q-1)}{p-1}\cdot k} = 1. \text{ (where } k = 0, 1, 2, \cdots, \frac{p-1}{2} - 1).$$

It should be noted that each value of k will generate different elements (ω_1, ω_2, ⋯) in $\mathbb{F}_{p^m}$, which can represent as a power of ω and these will become the zeros of different polynomials ($g_1(x)$, $g_2(x)$, ⋯) as shown in Fig. 1. Further-

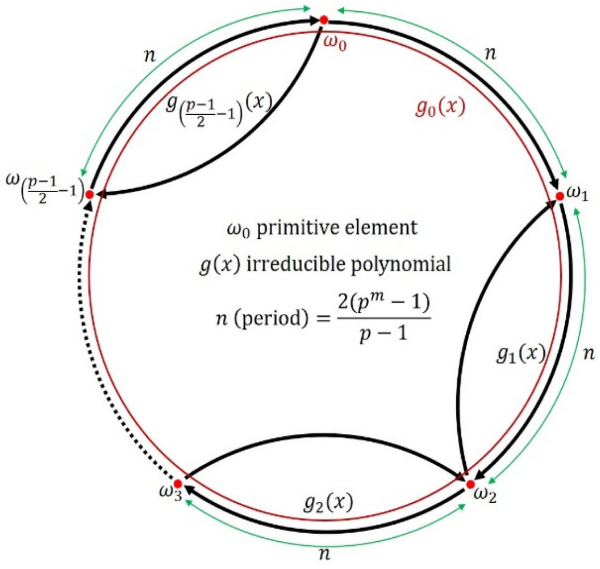


Fig. 1. Relation between the irreducible polynomials.

more, all these polynomials are irreducible polynomials. It should be noted that a primitive polynomial is a special kind of irreducible polynomial.

LEMMA 1. *In the theorem 1, $f_k(x)$ for all k becomes an irreducible polynomial of degree m.*

Proof. According to the condition of Theorem 1, the following relation should be satisfied.

$$f_k(\omega_k) = f_k(g^{2k}\omega_0) \equiv 0 \bmod f_0(\omega_0). \tag{24}$$

If $f_0(\omega_0)$ be an irreducible polynomial of degree m, then $f_k(g^{2k}\omega_0)$ should be also degree m irreducible polynomial to satisfy the above equation. When $f_k(x)$ is given as,

$$f_k(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0, \tag{25}$$

where c_i are the coefficients of $f_k(x)$. Then, $f_k(g^{2k}\omega_0)$ also becomes an irreducible polynomial of degree m as,

$$f_k(g^{2k}\omega_0) = (g^{2k})^m \omega_0^m + c_{m-1}(g^{2k})^{m-1}\omega_0^{m-1} + \cdots + c_1 g^{2k}\omega_0 + c_0. \tag{26}$$

LEMMA 2. *In the Theorem 1, $f_k(x)$ becomes a non-primitive polynomial if its zero $\omega_0^{2k((q-1)/(p-1))+1}$ holds the following relation as,*

$$\gcd\left(2k\left(\frac{q-1}{p-1}\right)+1, q-1\right) \neq 1. \tag{27}$$

Proof. This lemma is for the case that ω_k is not a primitive element of $f_k(x)$ and it can be proven by the following contradiction.

Let ω_k be an element in the proper subfield $\mathbb{F}_{q'}$ (where $\mathbb{F}_{q'} \subset \mathbb{F}_q$). According to the Property 1, ω_k needs to be represented by the generator g and zero of a polynomial ω_0 as,

$$\omega_k = g^{2k}\omega_0. \tag{28}$$

The above equation can be rewritten as follows.

$$\omega_0 = g^{-2k}\omega_k. \tag{29}$$

The RHS of the above equation be an element of the subfield $\mathbb{F}_q$ and ω_0 also belongs to $\mathbb{F}_q$ ($\omega_0 \notin \mathbb{F}_{q'}$). This is a contradiction. Thus, the above lemma is proven.

D. Application

Recently, there is a lot of consideration to use pseudo-random binary sequence in cryptographic applications. Consequently, to ensure the security of these applications, sequence needs to have unpredictable random quantities along with its rapid generation capabilities. If a sequence occupies these characteristics then it can be a prominent candidate in a stream cipher, where a lot of sequences are assigned to several users, respectively. The authors proposed a sequence in this paper already possesses good random quantities. Additionally, after utilizing the approach explained in this paper, the proposed binary sequence can be generated more swiftly. Consequently, it can be a substantial candidate for stream cipher like applications.

IV. DISCUSSION AND CONCLUSION

The authors previous work uses a primitive polynomial during the sequence generation procedure. Although the calculation cost for finding a primitive polynomial is high. However, from the viewpoint of security, if we use a sequence in some application, then the sequence needs to be generate very rapidly. The authors in this paper found that the same sequence (which generated by our previous work [9]) can be generated by some non-primitive polynomial. In addition, the following facts have been considered by the experimental observations and these are mathematically proven also.

- There are $(p - 1)/2$ irreducible polynomials which generates the same sequence (here, this number $(p - 1)/2$ related to the number of QR in $\mathbb{F}_p$).
- Some of the polynomials can be a non-primitive polynomial.

As mentioned previously, if the degree or the characteristic is large, then in that case finding a primitive polynomial

takes much calculation cost. A primitive polynomial is one kind of special polynomial which can generate maximum length vector sequence (for example, if $p = 11$ and $m = 2$, then a primitive polynomial can generate $p^m - 1 = 120$ distinct vectors without any duplication). There are only a few primitive polynomials are existing in the extension field. Therefore, when the characteristic field or the degree becomes large, then, to find a primitive polynomial becomes a time-consuming operation. Thus, the calculation cost becomes low if we can generate a sequence using our previous method without applying a primitive polynomial. Hence, as a future work, finding method of the non-primitive (irreducible) polynomials which generate the same sequence will be introduced.

ACKNOWLEDGMENTS

This work has been supported by JSPS KAKENHI Grant-in-Aid for Scientific Research (A) Number 16H01723 and the Ministry of Science and ICT (MSIT), Korea, under the Information Technology Research Center support program (No. IITP-2017-2014-1-00743) supervised by the Institute for Information & Communications Technology Promotion (IITP).

REFERENCES

[1] T. W. Cusick, C. Ding, and A. R. Renvall, *Stream Ciphers and Number Theory*. Amsterdam: Elsevier, 1998.
[2] S. W. Golomb, *Shift Register Sequences*. San Francisco, CA: Holden-Day, 1967.
[3] S. W. Golomb and G. Gong, *Sequence Design for Good Correlation*. Cambridge, MA: Cambridge University Press, 2005. DOI: 10.1017/CBO9780511546907.
[4] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1996.
[5] N. Zierler, "Linear recurring sequences," *Journal of the Society for Industrial and Applied Mathematics*, vol. 7, no. 1, pp. 31-48, 1959. DOI: 10.1137/0107003.
[6] C. Ding, T. Hesseseth, and W. Shan, "On the linear complexity of Legendre sequences," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1276-1278, 1998. DOI: 10.1109/18.669398.
[7] N. Zierler, *Legendre Sequences*. Lexington, MA: MIT Lincoln Laboratory, 1958.
[8] J. S. No, H. K. Lee, H. Chung, H. Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 2254-2255, 1996. DOI: 10.1109/18.556617.
[9] Y. Nogami, K. Tada, and S. Uehara, "A geometric sequence binarized with Legendre symbol over odd characteristic field and its properties," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 97, no. 12, pp. 2336-2342, 2014. DOI: 10.1587/transfun.E97.A.2336.
[10] R. Lidl and H. Niederreiter, *Finite Fields*. Boston, MA: Addison-Wesley, 1983.

Md. Arshad Ali

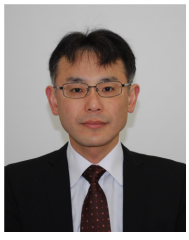
was born in 1986. He received the Master of Engineering degree from Okayama University, Japan in 2018. He worked as an assistant professor in Hajee Mohammad Danesh Science and Technology University (HSTU), Bangladesh. Currently, he is pursuing his Ph.D. degree in the field of information security and cryptography at Okayama University, Japan. His research interest includes information security, AES, pseudo-random sequence, and homomorphic encryption. He is a member of IEEE.

Yuta Kodera

received B.E. and M.E. degrees from Okayama University in 2017 and 2018, respectively. He is now pursuing his Ph.D. under the supervision of Professor Dr. Yasuyuki Nogami in the Graduate School of Natural Science and Technology, Okayama University, Japan. His research interests are finite field theory and its applications such as the pseudorandom number generator and recent cryptosystems. Currently, he is studying about the cryptographically secure pseudorandom number generator, searchable symmetric encryption and lattice-based cryptography.

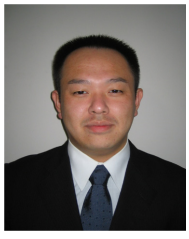
Taehwan Park

received his B.S.E.E. from Pusan National University, Pusan, Korea, in 2013. He is currently pursuing the combined M.S. and Ph.D. course in Computer Engineering at Pusan National University. His research interests include IoT device security, information security, elliptic curve cryptography, and post quantum cryptography.



Takuya Kusaka

was born in 1970. He received the B.E. degree in Electric Engineering from Kobe University in 1994, and he received M.E. and Ph.D. degrees in Information Science from the Graduate School of Information Science, Nara Institute of Science and Technology in 1996 and 1999, respectively. In 2004, he joined Okayama University. His current research interests include coding theory and information security.



Yasuyuki Nogami

graduated from Shinshu University in 1994 and received the Ph.D. degree in 1999 from Shinshu University. He is now a Professor of Okayama University. His main fields of research are finite field theory and its applications such as recent public key cryptographies. He is now studying about ECC, pairing-based cryptography, lattice-based cryptography, AES, and homomorphic encryptions. He is a member of IEICE and IEEE.

Howon Kim

received his B.S.E.E. from Kyungpook National University, Daegu, Korea, in 1993 and his M.S. and Ph.D. in Electronic and Electrical Engineering from Pohang University of Science and Technology (POSTECH), Pohang, Korea, in 1995 and 1999, respectively. From July 2003 to June 2004, he studied with the COSY group at the Ruhr-University of Bochum, Germany. He is currently working as a professor with the Department of Computer Engineering, School of Computer Science and Engineering, Pusan National University, Busan, Korea. Currently, his main research focus is on the Internet of Things (IoT) technology and the related security issues, mobile RFID technology, and sensor networks, public key cryptosystems, post quantum cryptography, and their security issues. He is a member of the IEEE and the International Association for Cryptographic Research (IACR).