Chinese Journal of Electronics
Vol.32, No.2, Mar. 2023

On the Linear Complexity of a Class of Periodic Sequences Derived from Euler Quotients

LUO Bingyu[1], ZHANG Jingwei[2], and ZHAO Chang'an[1,3,4]

(1. *School of Mathematics, Sun Yat-sen University, Guangzhou 510275, China*)

(2. *School of Information Science, Guangdong University of Finance and Economics, Guangzhou 510320, China*)

(3. *Guangdong Key Laboratory of Information Security, Guangzhou 510006, China*)

(4. *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*)

Abstract — In this paper, a family of binary sequences derived from Euler quotients with RSA modulus pq is introduced. Here two primes p and q are distinct and satisfy gcd(pq, (p—1)(q—1))=1. The linear complexities and minimal polynomials of the proposed sequences are determined. Besides, this kind of sequences is shown not to have correlation of order four although there exist some special relations by the properties of Euler quotients.

Key words — Cryptography, Binary sequences, Linear complexity, Euler quotients, RSA modulus.

I. Introduction

Pseudo random binary threshold sequences derived from the Fermat quotient can achieve good cryptographic properties [1]. For example, they have high linear complexities [2] and stable k-error linear complexities [3]. The study of linear complexities of sequences defined from polynomial quotients, a variant of the Fermat quotient, was given in [4]. Chen described trace representations for binary sequences defined from the Fermat quotient and also determined linear complexities of the corresponding sequences [5]. A natural extension of binary threshold sequences from Fermat quotients was considered for its cryptographic properties in [6]. The linear complexity of a family of p^2-periodic binary sequences derived from polynomial quotients modulo an odd prime p was determined in [7].

By the Euler's Theorem, Fermat quotients can be generalized for composites [8]. Therefore, it is natural to construct binary sequences derived from Euler quotients for cryptographic purposes. Firstly, the distribution of vectors of consecutive Euler-Fermat quotients modulo a composite was described in [9]. Trace representations of sequences deduced from Euler quotients modulo a prime power were studied in [10]. Furthermore, the k-error linear complexity of binary sequences deduced from Euler quotients modulo a prime power was determined [11]. Zhang *et al.* determined linear complexities of binary sequences deduced from Euler quotients modulo a product pq, where p and q are two distinct odd primes and p is a divisor of $q-1$ [12]. A novel approach for sequence constructions based on Euler quotients was presented in [13]. In summary, the pseudo random sequence derived from Fermat/Euler quotients and their variants is one of important classes in sequence sets.

In this paper, a family of binary sequence $\boldsymbol{s}$ derived from the Euler quotient is investigated. In our case, RSA modulus number $m=pq$ is taken for the Euler quotient where p and q are two distinct odd primes. For an integer $t \geq 0$ with $\gcd(t,m)=1$, the Euler quotient $\Psi(t) \pmod m$ is defined by

$$\Psi(t)=\frac{t^{\varphi(m)}-1}{m} \pmod m \qquad (1)$$

where $\varphi(\cdot)$ is the Euler-phi function. One can define $\Psi(t)=0$ if $\gcd(t,m)\neq 1$.

Manuscript Received May 6, 2020; Accepted Aug. 21, 2021. This work was supported by Guangdong Major Project of Basic and Applied Basic Research (2019B030302008), the National Natural Science Foundation of China (61972428), the Open Fund of State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences) (2020-ZD-02), and Guangdong Basic and Applied Basic Research Foundation (2019A1515011797).

DOI:10.23919/cje.2020.00.125

It can be seen easily that

$$\Psi(t+km) \equiv \Psi(t) + kt^{-1}\varphi(m) \pmod{m} \tag{2}$$

where t, k are positive integers with $\gcd(t, m) = 1$.

Without loss of generality, one can assume that p is smaller than q. The following is devoted to the study of a binary threshold sequence $\boldsymbol{S} = (s_t)_{t=0}^{\infty}$ from the Euler quotient modulo $m = pq$. The sequence $\boldsymbol{S} = (s_t)_{t=0}^{\infty}$ can be defined as

$$s_t = \begin{cases} 0, & \text{if } \ 0 \le \dfrac{\Psi(t)}{m} < \dfrac{1}{2} \\ 1, & \text{if } \ \dfrac{1}{2} \le \dfrac{\Psi(t)}{m} < 1 \end{cases} \tag{3}$$

For our purpose, the concept of the linear complexity of binary sequences is needed in the sequel.

The linear complexity $L(\boldsymbol{G})$ of an N-periodic sequence $\boldsymbol{G} = (g_i)_{i=0}^{\infty}$ over the binary field $\mathbb{F}_2$ is the smallest nonnegative integer L for which there exist elements $a_1, a_2, \ldots, a_L \in \mathbb{F}_2$ such that

$$g_i + a_1 \cdot g_{i-1} + \cdots + a_L \cdot g_{i-L} = 0, \text{ for all } i \ge L$$

Let $G(x) = g_0 + g_1 x + \cdots + g_{N-1}x^{N-1} \in \mathbb{F}_2[x]$ be the generating polynomial of sequences $\boldsymbol{G}$. Then the linear complexity of sequences $\boldsymbol{G}$ can be computed as follows [14]:

$$L(\boldsymbol{G}) = \deg\left(\frac{x^N - 1}{\gcd(x^N - 1, G(x))}\right)$$

In sequences designs [14]–[16], the linear complexity plays a vital role as a complexity measure for binary sequences. Depending on the requirements in applications of communication and cryptography, other measures including low autocorrelation or cross-correlation [17], [18], good nonlinear properties [19]–[21], k-error complexity [3], [22] are also required. According to the Berlekamp-Massey algorithm [14], [23], the linear complexity of a cryptographically strong sequence should be greater than a half of the least period of the sequence.

The presented paper contributes to the calculation of linear complexities of the sequence defined from the Euler quotients (3) with RSA modulus. The modulus in the Euler quotients is equal to pq with $\gcd((p-1)(q-1), pq) = 1$. Note that this result is different from [12] since the latter is considered under the condition that $\gcd((p-1)(q-1), pq) = p$. The proposed sequence will be balanced when both primes p and q tend to the infinity. The main result shows that the proposed sequences have high linear complexities. It should be emphasized that the proposed sequences have no high correlations of order four at the end.

The remainder of this paper is organized in the following way. In Section II, we give a proof of the main result. Section III concludes this paper.

II. Main Result

This section is devoted to the proof of the main theorem given in the following:

Theorem 1 Let two odd primes p and q be distinct with $\gcd((p-1)(q-1), pq) = 1$. Suppose that $2^{q-1} \not\equiv 1 \pmod{q^2}$ and $2^{p-1} \not\equiv 1 \pmod{p^2}$. A binary threshold sequence $\boldsymbol{S} = (s_t)_{t=0}^{\infty}$ can be defined by

$$s_t = \begin{cases} 0, & \text{if } \ 0 \le \dfrac{\Psi(t)}{pq} < \dfrac{1}{2} \\ 1, & \text{if } \ \dfrac{1}{2} \le \dfrac{\Psi(t)}{pq} < 1 \end{cases}$$

Then

1) The least period of $\boldsymbol{S}$ is p^2q^2;

2) The minimal polynomial of $\boldsymbol{S}$ is

$$M(x) = \begin{cases} \Phi_{p^2q^2}(x)\Phi_{p^2q}(x)\Phi_{pq^2}(x), \text{if } pq \equiv 1 \pmod{4} \\ \Phi_{p^2q^2}(x)\Phi_{p^2q}(x)\Phi_{pq^2}(x)\Phi_{pq}(x), \text{otherwise} \end{cases}$$

where we denote by$\Phi_n(x)$ for a positive integer n;

3) the linear complexity of $\boldsymbol{S}$ is given as follows:

$$L(\boldsymbol{S}) = \begin{cases} (p^2-1)(q^2-1)-(p-1)(q-1), \text{if } pq \equiv 1 \pmod{4} \\ (p^2-1)(q^2-1), \text{ otherwise} \end{cases}$$

For the proof of the main theorem, a series of the useful lemmas are required in the following.

It is first shown that p^2q^2 is a period of the sequence $\boldsymbol{S}$ under the condition that both p and q are not the divisors of $(p-1)(q-1)$.

Setting $m = k = pq$ in (2), we get

$$\Psi(t + p^2q^2) = \Psi(t) \pmod{pq}$$

which yields $s_{t+p^2q^2} = s_t$ for all $t \ge 0$ and thus the sequence $\boldsymbol{S}$ is p^2q^2-periodic. In the following, it will be demonstrated that p^2q^2 is the least period of the sequence $\boldsymbol{S}$.

Lemma 1 Using the same notation as previous, the sequence $\boldsymbol{S}$ has the least period $N = p^2q^2$.

Proof It will be first proved that pq^2 is not a period of the sequence $\boldsymbol{S}$. This is argued by contradiction. Assume that pq^2 is a period of the sequence $\boldsymbol{S}$. On one hand, it follows that

$$s_{-1+apq^2} = s_{-1+(p-a)pq^2}$$

where $0 < a < p$ by assumption.

On the other hand, letting $t = -1$ and taking $k = aq$ and $k = (p-a)q$ respectively in (2), one can obtain the following two equalities

$$\begin{aligned}\Psi(apq^2-1)\equiv&\Psi(-1)-aq(p-1)(q-1)\\ \equiv&aq(q-1)\pmod{pq}\end{aligned}$$

and

$$\Psi((p-a)pq^2-1)\equiv(p-a)q(q-1)\pmod{pq}$$

respectively. It can be inferred from

$$(p-a)q(q-1)+aq(q-1)=pq(q-1)\equiv 0\pmod{pq}$$

that one element in the set $\{(p-a)q(q-1), aq(q-1)\}$ is greater than $pq/2$ and the other is smaller than $pq/2$. This implies that

$$s_{-1+apq^2}+s_{-1+(p-a)pq^2}=1$$

This is a contradiction to the equality $s_{-1+apq^2}=s_{-1+(p-a)pq^2}$. Hence, the assumption is not valid. Similarly, it can be shown that qp^2 is not a period of the sequence $\boldsymbol{S}$. This completes the proof.

Denote by $\mathbb{Z}_n=\{0,1,\dots,n-1\}$ all representatives for the residue classes of integers modulo n and by $\mathbb{Z}_n^*$ all representatives that are relatively prime to n in $\mathbb{Z}_n$, respectively. Since the least period of $\boldsymbol{S}$ is $N=p^2q^2$, one only need to analyze properties of $\boldsymbol{S}=(s_t)_{i=0}^{N-1}$. Therefore, the action of Ψ is sometimes restricted to $\mathbb{Z}_{p^2q^2}$.

Let d and e be the greatest common divisor (gcd) and least common multiple (lcm) of $p-1$ and $q-1$ respectively. Write $d=\gcd(p-1,q-1)$ and $e=\mathrm{lcm}(p-1,q-1)=(p-1)(q-1)/d$. Let $\alpha\in\mathbb{Z}_{p^2q^2}^*$ be a fixed common primitive root of both p^2 and q^2. By the Chinese Reminder Theorem (CRT), there exists an element β of $\mathbb{Z}_{p^2q^2}^*$ such that

$$\begin{cases}\beta\equiv\alpha\pmod{p^2}\\ \beta\equiv 1\pmod{q^2}\end{cases}$$

As a consequence, we have

$$\mathbb{Z}_{p^2q^2}^*=\{\alpha^i\beta^j:0\le i<pqe, 0\le j<d\}\tag{4}$$

The following lemma shows that the map Ψ is a group homomorphism when the action of Ψ is restricted to the unit group $\mathbb{Z}_{p^2q^2}^*$.

Lemma 2 Let $\Psi:t\to\Psi(t)$ be the map from $\langle\mathbb{Z}_{p^2q^2}^*,\cdot\rangle$ to $\langle\mathbb{Z}_{pq},+\rangle$. Then Ψ is a surjective group homomorphism.

And then $\gcd(\Psi(\alpha),pq)=1$ and $\Psi(\alpha^{pq})=\Psi(\beta^p)=0\pmod{pq}$. Furthermore, the image and the kernel of Ψ is

$$Img(\Psi)=\mathbb{Z}_{pq}$$

and

$$Ker(\Psi)=\langle\alpha^{pq},\beta^p\rangle=\{\alpha^{ipq}\beta^{jp}:0\le i<e, 0\le j<d\}$$

respectively.

Proof For $u,v\in\mathbb{Z}_{p^2q^2}^*$, by the Euler's Theorem, we have

$$\begin{aligned}\Psi(uv)=&\frac{(uv)^{\varphi(pq)}-1}{pq}\\ =&\frac{(uv)^{\varphi(pq)}-u^{\varphi(pq)}+u^{\varphi(pq)}-1}{pq}\\ =&u^{\varphi(pq)}\Psi(v)+\Psi(u)\\ \equiv&\Psi(u)+\Psi(v)\pmod{pq}\end{aligned}$$

and thus Ψ is a group homomorphism.

There is a positive integer a_1 such that $\alpha^{q-1}=1+a_1q$ with $\gcd(a_1,q)=1$ as α is a generator in the group $\mathbb{Z}_{q^2}^*$. This gives

$$\begin{aligned}\Psi(\alpha)=&\frac{\alpha^{\varphi(pq)}-1}{pq}\\ \equiv&\frac{(1+a_1q)^{p-1}-1}{pq}\\ \equiv&a_1(p-1)p^{-1}\not\equiv 0\pmod{q}\end{aligned}$$

and so $\gcd(\Psi(\alpha),q)=1$. In a similar manner, it can be shown that $\gcd(\Psi(\alpha),p)=1$. It follows that $\gcd(\Psi(\alpha),pq)=1$. It can be seen that $\Psi(\alpha)$ is a generator of the cyclic group $\langle\mathbb{Z}_{pq},+\rangle$. This implies that the map Ψ is surjective from $\langle\mathbb{Z}_{p^2q^2}^*,\cdot\rangle$ to $\langle\mathbb{Z}_{pq},+\rangle$. Hence, Ψ is a surjective group homomorphism.

On the basis of homomorphic properties of the map Ψ, it yields that

$$\Psi(\alpha^{pq})=pq\Psi(\alpha)\equiv 0\pmod{pq}$$

Therefore $\alpha^{pq}\in\mathrm{Ker}(\Psi)$. Now it is claimed that $\beta^p\in\mathrm{Ker}(\Psi)$. By noting that $\beta^p\equiv 1\pmod{q^2}$ and writing $\beta^p=1+q^2b_1$ for some integer b_1. We immediately derive that

$$\Psi(\beta^p)\equiv p^{-1}\frac{(1+q^2b_1)^{\varphi(pq)}-1}{q}\equiv 0\pmod{q}$$

It follows from the homomorphic properties of the map Ψ that $\Psi(\beta^p)=p\Psi(\beta)\equiv 0\pmod{p}$. Thus, by the CRT, it can be seen that $\Psi(\beta^p)\equiv 0\pmod{pq}$. Therefore, it follows that

$$\langle\alpha^{pq},\beta^p\rangle\subseteq\mathrm{Ker}(\Psi)$$

Now it is claimed that $|\langle\alpha^{pq},\beta^p\rangle|=(p-1)(q-1)$ and $\langle\alpha^{pq},\beta^p\rangle=\{(\alpha^{pq})^i\beta^{pj}\pmod{p^2q^2}:0\le i<e, 0\le j<d\}$. In fact, it follows from the Second Isomorphism Theorem (see [24] page 227) that

$$\langle \alpha^{pq}, \beta^{p}\rangle/\langle \alpha^{pq}\rangle \simeq \langle \beta^{p}\rangle/\langle \alpha^{pq}\rangle \cap \langle \beta^{p}\rangle$$

Choose $x \in \langle \alpha^{pq}\rangle \cap \langle \beta^{p}\rangle$. Then write $x = \alpha^{ipq} \equiv \beta^{jp} \pmod{p^2q^2}$ for some $0 \le i \le e-1$ and $0 \le j \le p-2$. By the CRT, it follows that

$$\begin{cases} \alpha^{ipq} \equiv \beta^{jp} \equiv 1 \pmod{q^2} \\ \alpha^{ipq} \equiv \beta^{jp} \equiv \alpha^{jp} \pmod{p^2} \end{cases}$$

This implies that

$$\begin{cases} ipq \equiv 0 \pmod{q(q-1)} \\ ipq \equiv jp \pmod{p(p-1)} \end{cases}$$

There exist $\frac{e}{q-1}$ many solutions of the first equation in the above. Furthermore, Let i_0 be a solution of the first equation in the above. One can see that $q-1$ divides i_0. Thus, for each i_0, there exists one solution j_0 and $d = \gcd(p-1, q-1)$ divides j_0. Hence, we obtain $|\langle \beta^{p}\rangle/\langle \alpha^{pq}\rangle \cap \langle \beta^{p}\rangle| = \frac{p-1}{e/(q-1)} = d$. This gives that

$$\langle \beta^{p}\rangle/\langle \alpha^{pq}\rangle \cap \langle \beta^{p}\rangle = \{\beta^{pj}(\langle \alpha^{pq}\rangle \cap \langle \beta^{p}\rangle) : 0 \le j \le d-1\}$$

By the group isomorphism, it yields

$$\langle \alpha^{pq}, \beta^{p}\rangle/\langle \alpha^{pq}\rangle \simeq \langle \beta^{p}\rangle/\langle \alpha^{pq}\rangle \cap \langle \beta^{p}\rangle$$

This means that $\langle \alpha^{pq}, \beta^{p}\rangle = \{(\alpha^{pq})^i \beta^{pj} \pmod{p^2q^2} : 0 \le i < e, 0 \le j < d\}$ and $|\langle \alpha^{pq}, \beta^{p}\rangle| = (p-1)(q-1)$. This implies that $|\mathrm{Ker}(\Psi)| \ge (p-1)(q-1)$. Moreover, by the Fundamental Homomorphism Theorem [24], we get

$$|\mathrm{Ker}(\Psi)| = \frac{|\mathbb{Z}^*_{p^2q^2}|}{|\mathrm{Img}(\Psi)|} = \frac{(p-1)(q-1)pq}{pq} = (p-1)(q-1)$$

and thus $\mathrm{Ker}(\Psi) = \langle \alpha^{pq}, \beta^{p}\rangle$. This completes the proof.

It will be given that a partition of $\mathbb{Z}^*_{p^2q^2}$ is useful for giving an equivalent definition of the sequence $\boldsymbol{S}$ in the following.

Lemma 3 Using the same notation as above, define

$$D_\ell = \{t : \Psi(t) \equiv \ell \pmod{pq}, t \in \mathbb{Z}^*_{p^2q^2}\}$$

for $\ell = 0, 1, \ldots, pq-1$. In particular, we have $D_0 = \mathrm{Ker}(\Psi)$. There exists an integer $b \in \mathbb{Z}^*_{pq}$ such that $\hat{\alpha} = \alpha^b$ in $\mathbb{Z}^*_{p^2q^2}$ satisfies $\Psi(\hat{\alpha}) \equiv 1 \pmod{pq}$.

Define

$$\hat{D}_\ell = \hat{\alpha}^\ell D_0 = \{\hat{\alpha}^\ell \cdot t \pmod{p^2q^2} : t \in D_0\}$$

for $\ell = 0, 1, \ldots, pq-1$. Then $D_\ell = \hat{D}_\ell = \hat{\alpha}^\ell D_0$ for all $\ell \in \mathbb{Z}_{pq}$. Hence, $\mathbb{Z}^*_{p^2q^2} = \bigcup_{\ell=0}^{pq-1} D_\ell$ and each set D_ℓ has the same cardinality $|D_\ell| = (p-1)(q-1)$.

Proof According to the definition of D_0 and $\mathrm{Ker}(\Psi)$, it is seen that $D_0 = \mathrm{Ker}(\Psi)$. From the proof of Lemma 2 it follows that $\Psi(\alpha) \equiv a \pmod{pq}$ for some a with $\gcd(a, pq) = 1$. Let b be an integer in $\mathbb{Z}_{pq}$ such that $ab \equiv 1 \pmod{pq}$ and $\hat{\alpha} = \alpha^b$ in $\mathbb{Z}^*_{p^2q^2}$. Then

$$\psi(\hat{\alpha}) \equiv b \cdot \Psi(\alpha) \equiv 1 \pmod{pq}$$

since the map Ψ is a homomorphism.

For $\hat{\alpha}^\ell t \in \hat{D}_\ell$ with $t \in D_0 = \mathrm{Ker}(\Psi)$ it follows that

$$\Psi(\hat{\alpha}^\ell t) = \ell \cdot \Psi(\hat{\alpha}) + \Psi(t) \equiv \ell \pmod{pq}$$

and hence we have $\hat{D}_\ell \subseteq D_\ell$. Conversely, for $t \in D_\ell$ one can obtain

$$\Psi(t) = \ell = \ell\Psi(\hat{\alpha}) = \Psi(\hat{\alpha}^\ell) \pmod{pq}$$

and thus

$$\Psi\left(\frac{t}{\hat{g}^\ell}\right) \equiv 0 \pmod{pq}$$

since the map Ψ is a homomorphism. Hence, we have

$$\frac{t}{\hat{\alpha}^\ell} \in \mathrm{Ker}(\Psi) = D_0$$

and there exists an element $t_0 \in D_0$ such that

$$\frac{t}{\hat{\alpha}^\ell} \equiv t_0 \pmod{pq}$$

This means that $t = \hat{\alpha}^\ell \cdot t_0 \in \hat{\alpha}^\ell D_0 = \hat{D}_\ell$ and thus $D_\ell = \hat{D}_\ell$. By the definition of D_ℓ, we obtain $|D_\ell| = |D_0| = (p-1)(q-1)$ for $\ell = 0, 1, \ldots, q-1$. This completes the proof.

Let $T = \{t : t \in \mathbb{Z}_{p^2q^2}, \gcd(t, pq) \ne 1\}$. The first period value of the sequence $\boldsymbol{S} = (s_t)_{t=0}^{N-1}$ can be stated as

$$s_t = \begin{cases} 0, & \text{if } t \in D_0 \cup \cdots \cup D_{(pq-1)/2} \cup T \\ 1, & \text{if } t \in D_{(pq+1)/2} \cup \cdots \cup D_{pq-1} \end{cases} \tag{5}$$

It will be useful to compute the linear complexity from the pointview of different interpretation of the sequence S. To prove Theorem 1, we need the following lemmas.

Lemma 4 For any $0 \le i < pq$, if $u \pmod{p^2q^2} \in D_j$ for some $0 \le j < pq$, the following equality holds

$$uD_i = \{uv \pmod{p^2q^2} : v \in D_i\} = D_{i+j}$$

Proof If $u \in D_j$ and $v \in D_i$, we can get $u = \hat{\alpha}^j u_0$ and $v = \hat{\alpha}^i v_0$ for $u_0, v_0 \in D_0$. This means that $uv = \hat{\alpha}^{i+j} u_0 v_0 \in \hat{\alpha}^{i+j} D_0 = D_{i+j}$ and thus $uD_i \subseteq D_{i+j}$. It is easy to see that $D_{i+j} \subseteq uD_i$ and so the result follows.

For an arbitrary set A and a positive integer n, denote by $n * A$ the multiset in which each element of A appears with multiplicity n from now on.

Lemma 5 Let $\ell \in \mathbb{Z}_{pq}$be an nonnegative integer. Then we have

$$\{u \pmod p : u \in D_\ell\} = (q-1) * \mathbb{Z}_p^*$$

and

$$\{u \pmod q : u \in D_\ell\} = (p-1) * \mathbb{Z}_q^*$$

Proof We take an arbitrary element u in D_ℓ. It follows from Lemma 3 that $u = \hat{\alpha}^\ell \alpha^{pqi} \beta^{pj}$ where $i \in \mathbb{Z}_e$ and $j \in \mathbb{Z}_d$. Let $\hat{\alpha} = \alpha^b$ for some fixed $b \in \mathbb{Z}_{pq}^*$. Then

$$u = \hat{\alpha}^\ell \alpha^{qi} \beta^{pj} \equiv \alpha^{pqi+b\ell+pj} \equiv \alpha^{b\ell+pj} \cdot (\alpha^{pq})^i \pmod p$$

Note that pq is coprime to $p-1$. Therefore α^{pq} must be a primitive root modulo p. For any chosen $j_0 \in \mathbb{Z}_d$, the element $u \equiv \alpha^{pqi+b\ell+pj_0}$ modulo p runs over $\mathbb{Z}_p^*$ when i runs over the set $\mathbb{Z}_e$. Now we count the multiplicity of u in $\mathbb{Z}_p^*$ when i and j run over $\mathbb{Z}_e$ and $\mathbb{Z}_d$ respectively. Let

$$u \equiv \alpha^{pqi+b\ell+pj_0} \equiv \alpha^{a_0} \pmod p$$

for $a_0 \in \mathbb{Z}_p$. Then

$$i \equiv (a_0 - pj_0 - b\ell)(pq)^{-1} \pmod{p-1}$$

for $i \in \mathbb{Z}_e$ since$p-1$ has no divisors p and q.

$$i \equiv (pq)^{-1}(a_0 - j_0 - b\ell) \pmod{p-1}$$

Note that there are $\frac{q-1}{d}$ many solutions of the integer i in the form of $i_0, i_0 + (p-1), \ldots, i_0 + (\frac{q-1}{d} - 1)(p-1)$ with $i_0 \equiv (pq)^{-1}(a_0 - j_0 - b\ell) \pmod{p-1}$. In addition, the integer j_0 can be chosen in d ways. Hence there exist $(q-1)$ many elements in D_ℓ mapping into one element in $\mathbb{Z}_p^*$. The second equality is proved similarly.

Lemma 6 The map $f : D_\ell \to \mathbb{Z}_{pq^2}^*$ defined by $f(u) = u \pmod{pq^2}$ is injective, i.e.,

$$\{u \pmod{pq^2} : u \in D_\ell\} \subset \mathbb{Z}_{pq^2}^*$$

Proof Note that the map f is naturally defined well. The remained task is to prove that the map is injective indeed. Assume that u and v be two elements in D_l such that $f(u) = f(v)$. Write u and v by using the powers of α and β. The whole idea of the proof of this lemma can be finished on the basis of the Chinese Reminder Theorem.

It follows from the basic of definition of $f(u) = f(v)$ that we can see that $u = v \pmod{pq}$. We can convert this equality into the two equalities $u =v \pmod p$ and $u = v \pmod q$.

Note that pq^2 is a divisor of p^2q^2. On the basis of the Chinese Reminder Theorem, we can consider the relations of $u = v \pmod p$ and $u = v \pmod q$. We can express u and v by using the product of the powers of α and β. By comparing the exponents of u and v, we can establish the relations for the exponents of u and v when u and v are equal modulo p or q.

Since pq is relatively prime to $(p-1)(q-1)$, we consider the equality relations of the exponents $(\bmod\ (p-1))$ and $(\bmod\ (q-1))$. Recall that $d = \gcd(p-1, q-1)$ and $e = \operatorname{lcm}(p-1, q-1)$. We can prove the exponents for u and v are identical up to $p-1$ (or $q-1$). This means that the map is injective which finishes the proof of this lemma.

Lemma 7 With above notations, we denote $\hat{\alpha} \pmod n$ and $\alpha \pmod n$ by $\hat{\alpha}_{(n)}$ and $\alpha_{(n)}$ for an integer n, respectively. For $0 \le \ell < pq$, we have

$$\{u \pmod{q^2} : u \in D_\ell\} = (p-1) * \hat{\alpha}^\ell_{(q^2)} \langle \alpha^q_{(q^2)} \rangle \subset (p-1) * \mathbb{Z}^*_{q^2}$$

and

$$\{u \pmod{p^2} : u \in D_\ell\} = (q-1) * \hat{\alpha}^\ell_{(p^2)} \langle \alpha^p_{(p^2)} \rangle \subset (q-1) * \mathbb{Z}^*_{p^2}$$

Proof Since $u = \hat{\alpha}^\ell \alpha^{pqi} \beta^{pj}$ in $\mathbb{Z}_{p^2q^2}$ and q^2 is a divisor of p^2q^2, it gives that

$$u = \hat{\alpha}^\ell \alpha^{pqi} \beta^{pj} \equiv \hat{\alpha}^\ell_{(q^2)} \cdot (\alpha^q_{(q^2)})^{pi} \pmod{q^2}$$

It follows that $(u \pmod{q^2})$ belongs to $\hat{\alpha}^\ell_{(q^2)} \langle \alpha^q_{(q^2)} \rangle$ in $\mathbb{Z}^*_{q^2}$. Hence the map from D_ℓ to $\hat{\alpha}^\ell_{(q^2)} \langle \alpha^q_{(q^2)} \rangle$ with $u \to u \pmod{q^2}$ is well-defined. Supppose that

$$\alpha^{b\ell} \cdot (\alpha^q)^{pi} \equiv \alpha^{b\ell} \cdot (\alpha^q)^{pa_0} \pmod{q^2}$$

for some fixed $a_0 \in \mathbb{Z}_{q-1}$.This implies that

$$pqi \equiv pqa_0 \pmod{q(q-1)}$$

and thus

$$i \equiv a_0 \pmod{q-1}$$

There exist $\frac{p-1}{d}$ many solutions for $i \in \mathbb{Z}_e$ in the form of $a_0, a_0 + (q-1), \ldots, q_0 + (\frac{p-1}{d} - 1)(q-1)$. Together with $j \in \mathbb{Z}_d$ and this shows that the multiplicity is $p-1$ when u runs through the set D_ℓ. The second equality can be proved in a similar manner.

Lemma 8 With above notations, for $0 \le \ell < pq$, we have

$$\{u \pmod{pq^2} : u \in D_\ell\} = \hat{\alpha}^\ell_{(pq^2)} \langle \alpha^{pq}_{(pq^2)}, \beta^p_{(pq^2)} \rangle \subset \mathbb{Z}^*_{pq^2}$$

$$\{u \pmod{pq^2} : u \in D_\ell\} = \{u \pmod{pq^2} : u \in D_{\ell+q}\}$$

and

$$\mathbb{Z}^*_{pq^2} = \bigcup_{\ell=0}^{q-1} \hat{\alpha}^\ell_{pq^2} \langle \alpha^{pq}_{(pq^2)}, \beta^p_{(pq^2)} \rangle$$

Similarly, we get

$$\{u \pmod{p^2q} : u \in D_\ell\} = \hat{\alpha}^{\ell}_{(p^2q)}\langle \alpha^{pq}_{(p^2q)}, \beta^{p}_{(p^2q)}\rangle \subset \mathbb{Z}^*_{p^2q}$$

$$\{u \pmod{p^2q} : u \in D_\ell\} = \{u \pmod{p^2q} : u \in D_{\ell+p}\}$$

and

$$\mathbb{Z}^*_{p^2q} = \bigcup_{\ell=0}^{p-1} \hat{\alpha}^{\ell}_{p^2q}\langle \alpha^{pq}_{(p^2q)}, \beta^{p}_{(p^2q)}\rangle$$

Proof Since $u = \hat{\alpha}^\ell \alpha^{pqi}\beta^{pj}$ in $\mathbb{Z}_{p^2q^2}$ and pq^2 is a divisor of p^2q^2, it is seen that

$$u = \hat{\alpha}^\ell \alpha^{pqi}\beta^{pj} \equiv \hat{\alpha}^{\ell}_{(pq^2)}(\alpha^{pq}_{(pq^2)})^i(\beta^{p}_{(pq^2)})^j \pmod{pq^2}$$

Therefore $u \pmod{pq^2} \in \hat{\alpha}^{\ell}_{(pq^2)}\langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \subset \mathbb{Z}^*_{pq^2}$. By Lemma 6, we conclude that the map from D_ℓ to $\mathbb{Z}^*_{pq^2}$ with $u \to u \pmod{pq^2}$ is injective. In addition, it follows from $D_\ell = \hat{\alpha}^\ell\langle \alpha^{pq}, \beta^p\rangle$ that

$$\{u \pmod{pq^2} : u \in D_\ell\} = \hat{\alpha}^{\ell}_{(pq^2)}\langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \subset \mathbb{Z}^*_{pq^2}$$

Now it is claimed that if $\gcd(\ell, q) = 1$, then $\hat{\alpha}^{\ell}_{(pq^2)} \notin \langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \subset \mathbb{Z}^*_{pq^2}$; otherwise, it follows that $\hat{\alpha}^{\ell}_{(pq^2)} \in \langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \subset \mathbb{Z}^*_{pq^2}$. Now the proof of the above claim is given. In fact, for any $x \in \langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \subset \mathbb{Z}^*_{pq^2}$, it follows from

$$x \equiv \alpha^{ipq} \pmod{q^2}$$

that

$$x^{q-1} \equiv 1 \pmod{q^2}$$

If $\gcd(\ell, q) = 1$, assume that $\hat{\alpha}^{\ell}_{(pq^2)} \in \langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \subset \mathbb{Z}^*_{pq^2}$. Then

$$\hat{\alpha}^{\ell(q-1)}_{(pq^2)} = \alpha^{b\ell(q-1)}_{(pq^2)} \equiv 1 \pmod{q^2}$$

This yields that $b\ell(q-1)$ is divisible by q, which contradicts $\gcd(\ell, q) = 1$. So $\hat{\alpha}^{\ell}_{(pq^2)} \notin \langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \subset \mathbb{Z}^*_{pq^2}$ under the condition that $\gcd(\ell, q) = 1$.

If $\gcd(\ell, q) = q$, it is seen that $\hat{\alpha}^{\ell}_{(pq^2)} = \alpha^{qt}_{(pq^2)} \in \langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \subset \mathbb{Z}^*_{pq^2}$ for some t. Thus, $\hat{\alpha}^{\ell}_{(pq^2)} \in \langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \subset \mathbb{Z}^*_{pq^2}$ if and only if the following equation with respect to unknown integers i and j have solutions

$$\begin{cases} \alpha^{pqi+pj} \equiv \alpha^{qt} \pmod{p} \\ \alpha^{pqi} \equiv \alpha^{qt} \pmod{q^2} \end{cases}$$

Equivalently,

$$\begin{cases} qi + j \equiv qt \pmod{p-1} \\ pi \equiv t \pmod{q-1} \end{cases}$$

By the generalized Chinese Reminder Theorem (see [25] Lemma 1), we see that the equations have one solution if and only if $j \equiv q(1-a)t \pmod{d}$ where $a = (p^{-1} \bmod q-1)$. So two suitable integers j and i can be selected such that $\alpha^q t = \alpha^{ipq}\beta^{pj} \in \langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \subset \mathbb{Z}^*_{pq^2}$. This finishes the proof of the claim.

Since $D_\ell = \hat{\alpha}^\ell\langle \alpha^{pq}, \beta^p\rangle$, it follows that

$$\{u \pmod{p^2q} : u \in D_\ell\} = \{u \pmod{p^2q} : u \in D_{\ell+q}\}$$

by $\hat{\alpha}^{q}_{(pq^2)} \in \langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \subset \mathbb{Z}^*_{pq^2}$. Let $0 \le \ell_1 < \ell_2 \le q-1$. It gives that

$$\varnothing = \hat{\alpha}^{\ell_1}_{(pq^2)}\langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \cap \hat{\alpha}^{\ell_2}_{(pq^2)}\langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \subset \mathbb{Z}^*_{pq^2}$$

by $\hat{\alpha}^{\ell_1-\ell_2}_{(pq^2)} \notin \langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \subset \mathbb{Z}^*_{pq^2}$. Therefore the set $\bigcup_{\ell=0}^{q-1} \hat{\alpha}^{\ell}_{(pq^2)}\langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle$ is a disjoint union and

$$\left|\bigcup_{\ell=0}^{q-1} \hat{\alpha}^{\ell}_{(pq^2)}\langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle\right| = q(p-1)(q-1)$$

The fact that $\bigcup_{\ell=0}^{q-1} \hat{\alpha}^{\ell}_{(pq^2)}\langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle \subset \mathbb{Z}^*_{pq^2}$ yields that $\bigcup_{\ell=0}^{q-1} \hat{\alpha}^{\ell}_{(pq^2)}\langle \alpha^{pq}_{(pq^2)}, \beta^{p}_{(pq^2)}\rangle = \mathbb{Z}^*_{pq^2}$. In a similar manner, the second part of the lemma can be proved.

Define a polynomial $D_\ell(x) = \sum_{u \in D_\ell} x^u \in \mathbb{F}_2[x]$ for $0 \le \ell < pq$. Based on the new interpretation of the seqeunce $\boldsymbol{S}$ in (5), we see that its the generating polynomial of $\boldsymbol{S}$ is

$$\Lambda_0(x) = \sum_{\ell=\frac{pq+1}{2}}^{pq-1} D_\ell(x)$$

Now some useful lemmas about $D_\ell(x)$ and $\Lambda_0(x)$ are given as follows.

Lemma 9 Let γ be a fixed p^2q^2-th primitive root of unity in $\overline{\mathbb{F}}_2$. For $v \in \mathbb{Z}_{p^2q^2}$,

$$D_\ell(\gamma^v) = \begin{cases} 1, & \text{if } \gcd(v, p^2q^2) = pq \\ 0, & \text{if } \gcd(v, p^2q^2) \in \{p^2, q^2, p^2q, pq^2, p^2q^2\} \end{cases}$$

Proof Let $m = \gcd(v, p^2q^2)$ and $n = p^2q^2/m$. This means that γ^v is a n-th primitive root of unity in $\overline{\mathbb{F}}_2$.

If $m = p^2q^2$ and $n = 1$, then

$$D_\ell(\gamma^v) = |D_\ell| \cdot 1 = (p-1)(q-1) \equiv 0 \pmod{2}$$

If $m \in \{p^2, q^2, p^2q, pq^2\}$, then $n \in \{q^2, p^2, p, q\}$. By Lemmas 5 and 7, it can be found that $\{u \bmod n : u \in D_\ell\}$ is always a multiset and the multiplicity is even. It follows that

$$D_\ell(\gamma^v) \equiv 0 \pmod{2}$$

If $m = pq$ and $n = pq$, then $\{u \mod n : u \in D_\ell\} = \mathbb{Z}_{pq}^*$ in this case. It follows that

$$D_\ell(\gamma^v) = \sum_{u \in D_\ell} \gamma^{uv} = \sum_{u \in \mathbb{Z}_{pq}^*} (\gamma^v)^u$$

By noting that $\sum_{u \in \mathbb{Z}_{pq}^*} \gamma^{uv}$ is the coefficient of the second highest term of the cyclotomic polynomial$\Phi_{pq}(x)$ that is also equal to the sum of all pq-th primitive roots of unity in $\overline{\mathbb{F}}_2$. It follows from Exercise 2.57 in [26] that for

$$\Phi_{pq}(x) = \frac{\Phi_q(x^p)}{\Phi_q(x)} = \frac{x^{p(q-1)} + x^{p(q-2)} + \cdots + 1}{x^{q-1} + x^{q-2} + \cdots + 1}$$
$$= x^{(p-1)(q-1)} + 1 \cdot x^{(p-1)(q-1)-1} + \cdots$$

We have

$$D_\ell(\gamma^v) = \sum_{u \in D_\ell} \gamma^{uv} = \sum_{u \in \mathbb{Z}_{pq}^*} \gamma^{uv} = 1$$

Lemma 10 Let $I = \{i \in \mathbb{Z} : \frac{pq+1}{2} \le i \le pq-1\}$, $I_p = \{i \in \mathbb{Z} : \frac{p+1}{2} \le i \le p-1\}$ and $I_q = \{i \in \mathbb{Z} : \frac{q+1}{2} \le i \le q-1\}$, respectively. Then the following two multiset equalities hold

$$\{\ell \pmod p) : \ell \in I\} = \left(\frac{q-1}{2} * \mathbb{Z}_p\right) \cup I_p$$

and

$$\{\ell \pmod q) : \ell \in I\} = \left(\frac{p-1}{2} * \mathbb{Z}_q\right) \cup I_q$$

Proof Note that

$$\frac{pq+1}{2} + i = \frac{pq-p+p+1}{2} + i = \left(\frac{q-1}{2}\right)p + \frac{p+1}{2} + i$$

for $0 \le i \le \frac{pq-3}{2}$. Then the set I can be written as

$$I = \bigcup_{j=1}^{\frac{q-1}{2}} \left\{\left(j + \frac{q-1}{2}\right)p + i : 0 \le i \le p-1, i \in \mathbb{Z}\right\}$$
$$\bigcup \left\{\left(\frac{q-1}{2}\right)p + i : \frac{p+1}{2} \le i \le p-1, i \in \mathbb{Z}\right\}$$

We have

$$\{\ell \pmod p) : \ell \in I\} = \left(\frac{q-1}{2} * \mathbb{Z}_p\right) \cup I_p$$

Similarly, the second assertion can be proved. This finishes the proof of the lemma.

Lemma 11 Let $\mathcal{D}_\ell = \hat{\alpha}^\ell_{(pq^2)} \langle \alpha^{pq}_{(pq^2)}, \beta^p_{(pq^2)} \rangle \subset \mathbb{Z}^*_{pq^2}$ for $\ell \in Z_q$. For $j \in \mathbb{Z}_q$, denote $\Gamma_j(x) = \sum_{\ell = \frac{q+1}{2}}^{q-1} \mathcal{D}_{j+\ell}(x)$. If $2^{q-1} \not\equiv 1 \pmod{q^2}$, we have $\Gamma_0(\gamma^p) \ne 0$. Furthermore, if $2^{p-1} \not\equiv 1 \pmod{p^2}$, we have $\Lambda_0(\gamma^p) \ne 0$ and $\Lambda_0(\gamma^q) \ne 0$.

Proof It is first proved that $2 \notin \mathcal{D}_0$ provided that $2^{q-1} \not\equiv 1 \pmod{q^2}$. Assume that $2 \in \mathcal{D}_0$, i.e., $2 \in \langle \alpha^{pq}_{(pq^2)}, \beta^p_{(pq^2)} \rangle$ according to the definition of $\mathcal{D}_0$. Put $2 \equiv \alpha^{i_0 pq}_{(pq^2)} \beta^{j_0 p}_{(pq^2)} \pmod{pq^2}$. This implies that

$$2^{q-1} = \alpha^{i_0 pq(q-1)}_{(pq^2)} \beta^{j_0 p(q-1)}_{(pq^2)} = \left(\alpha^{q(q-1)}_{(pq^2)}\right)^{i_0 p} \cdot 1 \equiv 1 \pmod{q^2}$$

which is a contraction. Hence, by Lemma 8, we get $2 \in \mathcal{D}_\sigma$ for some fixed $\sigma \in \mathbb{Z}_q^*$.

Let $\theta = \gamma^p$ for simplicity. For $j \in \mathbb{Z}_q$, now it is claimed that $\Gamma_j(\theta) \ne 0$.Suppose that there exists an element $j_0 \in \mathbb{Z}_q$ such that $\Gamma_{j_0}(\theta) = 0$. It can be inferred from Lemmas 4 and 8 it that

$$0 = \Gamma_{j_0}(\theta)^{2^i} = \Gamma_{j_0}(\theta^{2^i}) = \Gamma_{j_0 + i\sigma}(\theta)$$

for any $i \in \mathbb{Z}_q$. It is worth noting that $\sigma \ne 0$ in $\mathbb{Z}_q$. When the number i runs through $\mathbb{Z}_q$, so does $j_0 + i\sigma$. Hence we have $\Gamma_j(\theta) = 0$ for all $j \in \mathbb{Z}_q$. Particularly, we have $\Gamma_0(\theta) = 0$.

By Lemma 4, for any $v \in D_j$ with $j \in \mathbb{Z}_q$, we obtain

$$\Gamma_0(\theta^v) = \sum_{\ell = \frac{q+1}{2}}^{q-1} D_\ell(\theta^v) = \sum_{\ell = \frac{q+1}{2}}^{q-1} D_{\ell+j}(\theta) = \Gamma_j(\theta) = 0$$

Note that $\mathbb{Z}^*_{pq^2} = \bigcup_{j=0}^{q-1} \mathcal{D}_j$ by Lemma 8. It is immediate that $\Gamma_0(\theta^v) = 0$ for any $v \in \mathbb{Z}^*_{pq^2}$. Thus the cyclotomic polynomial $\Phi_{pq^2}(x)$ divides $\Gamma_0(x)$. Following the proof process of Lemma 9, we get $\Phi_{q^2}(x)$ divides $\Gamma_0(x)$. Therefore $\Phi_{pq^2}(x)\Phi_{q^2}(x)$ divides $\Gamma_0(x)$ according to $\gcd(\Phi_{pq^2}(x), \Phi_{q^2}(x)) = 1$. It follows from Exercise 2.57 in [26] that

$$\Phi_{pq^2}(x)\Phi_{q^2}(x) = \Phi_{q^2}(x^p) = \sum_{j=0}^{q-1} x^{jpq}$$

Let

$$\Gamma_0(x) \equiv \Phi_{q^2}(x^p)\Omega(x) \pmod{x^{pq^2} - 1}$$

Note that

$$x^{pq}\Phi_{q^2}(x^p) = x^{pq} \sum_{j=0}^{q-1} x^{jpq}$$
$$\equiv \sum_{j=0}^{q-1} x^{jpq}$$
$$\equiv \Phi_{q^2}(x^p) \pmod{x^{pq^2} - 1}$$

Thus we can limit $\deg \Omega(x) < pq$. Then it can be stated as $\Omega(x) = \sum_{i=0}^{t-1} x^{\nu_i}$ with $0 \le \nu_0 < \nu_1 < \cdots < \nu_{t-1} < pq$. This implies that

$$\begin{aligned}\Gamma_0(x) \equiv & \Omega(x)\Phi_{q^2}(x^p) \\ \equiv & \sum_{i=0}^{t-1} x^{\nu_i} \sum_{j=0}^{q-1} x^{jpq} \\ \equiv & \sum_{i=0}^{t-1}\sum_{j=0}^{q-1} x^{\nu_i+jpq} \pmod{x^{pq^2}-1}\end{aligned}$$

Note that $\Gamma_0(x)$ has $\frac{1}{2}(p-1)(q-1)^2$ terms, but $\sum_{i=0}^{t-1}\sum_{j=0}^{q-1} x^{\nu_i+jpq}$ has qt terms, which give us a contradiction since the prime q does not divide $\frac{1}{2}(p-1)(q-1)^2$. Hence, we have $\Gamma_j(\theta) \ne 0$ for any $j \in \mathbb{Z}_q$, particularly, $\Gamma_0(\theta) \ne 0$.

By Lemma 8, we have $\sum_{\ell=0}^{q-1} D_\ell(\theta) = \sum_{u\in\mathbb{Z}^*_{pq^2}} \theta^u$. It is known that $\sum_{u\in\mathbb{Z}^*_{pq^2}} \theta^u$ is equal to the coefficient of the second highest term $x^{q(p-1)(q-1)-1}$ of the polynomial $\Phi_{pq^2}(x)$. Using $\Phi_{pq^2}(x) = \Phi_{pq}(x^q)$ implies that the coefficient of $x^{q(p-1)(q-1)-1}$ in $\Phi_{pq^2}(x)$ is equal to zero. Therefore, by Lemma 10, it gives that

$$\Lambda_0(\theta) = \Gamma_0(\theta) + \frac{p-1}{2}\sum_{u\in\mathbb{Z}^*_{pq^2}} \theta^u = \Gamma_0(\theta) \ne 0$$

Similarly, it can be shown that $\Lambda_0(\gamma^q) \ne 0$ under the assumption that $2^{p-1} \not\equiv 1 \pmod{p^2}$.

Lemma 12 With above notations, for $j \in \mathbb{Z}_{pq}$, denote $\Lambda_j(x) = \sum_{\ell=\frac{pq+1}{2}}^{pq-1} D_{j+\ell}(x)$. If $2^{q-1} \not\equiv 1 \pmod{q^2}$ and $2^{p-1} \not\equiv 1 \pmod{p^2}$, we have $\Lambda_j(\gamma) \ne 0$.

Proof Similarly as in the proof of Lemma 11, under the condition that $2^{q-1} \not\equiv 1 \pmod{q^2}$ and $2^{p-1} \not\equiv 1 \pmod{p^2}$, it is claimed that $2 \in D_\sigma$ where $\gcd(\sigma, pq) = 1$. According to Lemma 3, it can be seen that $2 = \hat{\alpha}^\sigma \alpha^{i_0pq}\beta^{j_0p} \in \mathbb{Z}_{p^2q^2}$. This implies that

$$2^{q-1} = \hat{\alpha}^{\sigma(q-1)}\alpha^{i_0pq(q-1)}\beta^{j_0p(q-1)} \equiv \hat{\alpha}^{\sigma(q-1)} \pmod{q^2} \tag{6}$$

and

$$2^{p-1} = \hat{g}^{\sigma(p-1)}g^{i_0pq(p-1)}h^{j_0p(p-1)} \equiv \hat{g}^{\sigma(p-1)} \pmod{p^2} \tag{7}$$

If q divides σ, (6) shows that $2^{q-1} \equiv 1 \pmod{q^2}$; and if p divides σ, (7) implies that $2^{p-1} \equiv 1 \pmod{p^2}$. This contradicts the assumption. Hence $2 \in D_\sigma$ with $\gcd(\sigma, pq) = 1$.

Since σ is a generator of the additive group $\langle \mathbb{Z}_{pq}, + \rangle$, there exists a number i_0 such that

$$i_0\sigma \equiv 1 \pmod{pq}$$

It follows from Lemma 4 that $2^{i_0}D_0 = D_{i_0\sigma} = D_1$. Therefore,

$$2^{i_0} \in D_1$$

For $j \in \mathbb{Z}_{pq}$, it is claimed that $\Lambda_j(\gamma) \ne 0$. Assume that there exists some $j_0 \in \mathbb{Z}_{pq}$ such that $\Lambda_{j_0}(\gamma) = 0$. By Lemma 4, for any k, we get

$$0 = \Lambda_{j_0}(\gamma)^{2^{i_0k}} = \Lambda_{j_0}(\gamma^{2^{i_0k}}) = \Lambda_{j_0+k}(\gamma)$$

For $j \in \mathbb{Z}_{pq}$, let $k = j - j_0 \in \mathbb{Z}_{pq}$. It follows that $\Lambda_j(\gamma) = \Lambda_{j_0+k}(\gamma) = 0$, and

$$\begin{aligned} 0 = & \Lambda_j(\gamma)^{2^{i_0}} \\ = & \sum_{\ell=j+\frac{pq+1}{2}}^{j+pq-1} D_\ell(\gamma^{2^{i_0}}) \\ = & D_{pq+j}(\gamma) + \sum_{\ell=j+\frac{pq+1}{2}+1}^{j+pq-1} D_\ell(\gamma) \end{aligned} \tag{8}$$

by using $2^{i_0} \in D_1$. On the other hand, we have

$$0 = \Lambda_j(\gamma) = D_{j+\frac{pq+1}{2}}(\gamma) + \sum_{\ell=j+\frac{pq+1}{2}+1}^{j+pq-1} D_\ell(\gamma) \tag{9}$$

Combining (8) with (9) one can obtain that

$$D_j(\gamma) = D_{j+\frac{pq+1}{2}}(\gamma) \tag{10}$$

by using $j = pq + j \in \mathbb{Z}_{pq}$. It is known that $\sum_{u\in\mathbb{Z}^*_{p^2q^2}} \gamma^u$ is equal to the coefficient of the second highest term $x^{pq(p-1)(q-1)-1}$ of the polynomial $\Phi_{p^2q^2}(x)$. Note that $\Phi_{p^2q^2}(x) = \Phi_{pq}(x^{pq})$. It is seen that the coefficient of the second highest term $x^{pq(p-1)(q-1)-1}$ of the polynomial $\Phi_{p^2q^2}(x)$ is equal to 0. Therefore, by Lemma 3, one can see that

$$\sum_{\ell=0}^{pq-1} D_\ell(\gamma) = \sum_{u\in\mathbb{Z}^*_{p^2q^2}} \gamma^u = 0$$

Using (10), it follows that

$$\begin{aligned} & \sum_{l=0}^{\frac{pq-1}{2}-1} D_l(\gamma) + \sum_{l=\frac{pq-1}{2}+1}^{pq-1} D_l(\gamma) \\ = & \sum_{l=0}^{\frac{pq-1}{2}-1} \left(D_l(\gamma) + D_{l+\frac{pq+1}{2}}(\gamma)\right) = 0 \end{aligned}$$

Since

$$\sum_{\ell=0}^{pq-1} D_\ell(\gamma) = \sum_{\ell=0}^{\frac{pq-1}{2}-1} D_\ell(\gamma) + \sum_{\ell=\frac{pq-1}{2}+1}^{pq-1} D_\ell(\gamma) + D_{\frac{pq-1}{2}}(\gamma)$$

it has been shown that $D_{\frac{pq-1}{2}}(\gamma) = 0$.

Replacing $j = (pq-1)/2$ in (10), we find $D_0(\gamma) = 0$. Hence $D_k(\gamma) = D_0(\gamma)^{2^{i_0 k}} = 0$ for $k \in \mathbb{Z}_{pq}$.

Then it follows from Lemma 4 for any $v \in D_j$ with $j \in \mathbb{Z}_{pq}$ that

$$D_\ell(\gamma^v) = D_{\ell+j}(\gamma) = 0$$

By noting that $\mathbb{Z}^*_{p^2q^2} = \bigcup_{j=0}^{pq-1} D_j$, we immediately derive that $D_\ell(\gamma^v) = 0$ for any $v \in \mathbb{Z}^*_{p^2q^2}$. Hence, we get the cyclotomic polynomial $\Phi_{p^2q^2}(x)$ divides $D_\ell(x)$.

Setting $\theta = \gamma^p$, we see that it is a pq^2-th primitive root of unity in $\overline{\mathbb{F}}_2$. By Lemma 8, it follows that $\hat{\alpha}^{\ell+q}\langle\alpha^{pq}, \beta^p\rangle = \hat{\alpha}^{\ell}\langle\alpha^{pq}, \beta^p\rangle \subset \mathbb{Z}^*_{pq^2}$. Therefore, it can be seen that $D_\ell(\theta){=}D_{\ell+q}(\theta)$. It follows that $D_\ell(\theta){+}D_{\ell+q}(\theta) = 0$. And for $v \in \mathbb{Z}$ and $\gcd(v, pq) = 1$, it follows that v must belong to D_{j_0} for some j_0. This gives that

$$D_\ell(\theta^v) + D_{\ell+q}(\theta^v) = D_{\ell+j_0}(\theta) + D_{\ell+j_0+q}(\theta) = 0$$

This shows that all roots of the cyclotomic polynomial $\Phi_{pq^2}(x)$ are also the roots of $D_\ell(x) + D_{\ell+q}(x)$, i.e., the polynomial $D_\ell(x) + D_{\ell+q}(x)$ is divisible by the polynomial $\Phi_{pq^2}(x)$.

By Lemma 9, it gives that $\Phi_{q^2}(x)$ divides $D_k(x)$ for all $k \in \mathbb{Z}_{pq}$.

Since $\Phi_{p^2q^2}(x) = \Phi_{pq}(x^{pq}) = \Phi_q(x^{p^2q})/\Phi_q(x^{pq})$ and $\Phi_q(x^{pq})/\Phi_q(x^q) = \Phi_{pq}(x^q) = \Phi_{pq^2}(x)$ (see Exercise 2.57 in [26]), it follows that

$$\Phi_q(x^{p^2q}) = \Phi_{p^2q^2}(x)\Phi_{pq^2}(x)\Phi_{q^2}(x)$$

Because these three cyclotomic polynomials are pairwise coprime, this means that $\Phi_q(x^{p^2q})$ divides $D_\ell(x) + D_{\ell+q}(x)$ for all ℓ.

Let

$$D_\ell(x) + D_{\ell+q}(x) \equiv \Phi_q(x^{p^2q})\Delta(x) \mod (x^{p^2q^2} - 1)$$

Note that

$$\begin{aligned} x^{p^2q}\Phi_q(x^{p^2q}) &= x^{p^2q}\sum_{j=0}^{q-1} x^{jp^2q} \equiv \sum_{j=0}^{q-1} x^{jp^2q} \\ &= \Phi_q(x^{p^2q}) \mod (x^{p^2q^2} - 1) \end{aligned}$$

and the degree of the polynomial $\Delta(x)$ is less than p^2q. Thus it can be stated as $\Delta(x) = \sum_{i=0}^{t-1} x^{\nu_i}$, in which $0 \le \nu_0 < \nu_1 < \cdots < \nu_{t-1} < p^2q$. We can observe that $D_\ell(x) + D_{\ell+q}(x)$ has $2\,(p-1)(q{-}1)$ terms, while $\sum_{i=0}^{t-1}\sum_{j=0}^{q-1} x^{\nu_i + jp^2q}$ has qt terms, which give us a contradiction since the prime q does not divide $2(p{-}1)(q{-}1)$. Hence, we obtain $\Lambda_j(\gamma) \ne 0$ for any $j \in \mathbb{Z}_{pq}$.

We are now in a position to give a short proof of Theorem 1.

Proof of Theorem 1 1) It is obvious by Lemma 1.

2) Since the minimal polynomial of $\boldsymbol{S}$ is

$$\frac{x^N - 1}{\gcd(x^N - 1, G(x))}$$

where the generation polynomial of the proposed sequence is $G(x) = \Lambda_0(x)$.

It is required to compute $\gcd(x^N - 1, G(x))$. By Lemmas 11 and 12, it is seen that there exists no common root of the polynomial $\Phi_{p^2q^2}(x)\Phi_{p^2q}(x)\Phi_{pq^2}(x)$ and $G(x)$. It follows that

$$\gcd(\Phi_{p^2q^2}(x)\Phi_{p^2q}(x)\Phi_{pq^2}(x), G(x)) = 1$$

By Lemma 9, it can be found that

$$\Phi_1(x)\Phi_p(x)\Phi_q(x)\Phi_{p^2}(x)\Phi_{q^2}(x)$$

divides $G(x)$.

For the divisor $\gcd(\Phi_{pq}(x), g(x))$, there are two cases. By Lemma 9, it follows that $D_\ell(\gamma^{pq}) = 1$, where γ is a p^2q^2-th primitive root of unity in $\overline{\mathbb{F}}_2$. It is seen that

$$\Lambda_0(\gamma^{pq}) = \sum_{\ell=\frac{pq+1}{2}}^{pq-1} D_\ell(\gamma^{pq}) = pq - 1 - \frac{pq+1}{2} + 1 = \frac{pq-1}{2}$$

Therefore, $\Lambda_0(\gamma) = 0$ if $pq \equiv 1 \pmod 4$ and $\Lambda_0(\gamma) = 1$ if $pq \equiv 3 \pmod 4$. Thus, it is seen that $\Lambda_0(x)$ divides $G(x)$ if and only if $pq \equiv 1 \pmod 4$. Therefore, the common factor of $G(x)$ and $x^N - 1$ is described in Theorem 1.

3) It is obvious by 2).

In the following, some facts are given about the proposed sequence.

Remark 1 Recall that $m = pq$. Although there exists an equality in the following

$$\Psi(t){-}\Psi(t{+}pm){-}\Psi(t{+}qm){+}\Psi(t{+}(p{+}q)m) = 0 \pmod{pq}$$

for any integer t with $\gcd(t, m) = 1$ by using the properties of Euler quotients, it can not be obtained that the following relation

$$s_t + s_{t+pm} + s_{t+qm} + s_{t+(p+q)m} = 0$$

holds for all $t \in \mathbb{Z}$. In fact, the sum $s_t{+}s_{t+pm}{+}s_{t+qm}{+}s_{t+(p+q)m}$ will vary in the finite field $\mathbb{F}_2$ along with the value t changing.

Finally, a "toy" example is taken for illustrating this fact. Assume that $p = 3$ and $q = 5$. Let $t = 2$. A direct computation gives $\Psi(t) = 2$, $\Psi(t + pm) = 14$, $\Psi(t + qm) = 7$ and $\Psi(t + (p + q)m) = 4$. This indeed yields that

$$\Psi(t)-\Psi(t+pm)-\Psi(t+qm)+\Psi(t+(p+q)m) = 0 \pmod{pq}$$

However, by the definition of proposed sequence, we have $s_t = 0$, $s_{t+pm} = 1$, $s_{t+qm} = 0$, and $s_{t+(p+q)m} = 0$. This implies that

$$s_t + s_{t+pm} + s_{t+qm} + s_{t+(p+q)m} = 1$$

For some other value t, one can get that $s_t + s_{t+pm} + s_{t+qm} + s_{t+(p+q)m} = 0$. For instance, letting $t = 1$ gives $\Psi(t) = 0$, $\Psi(t+pm) = 9$, $\Psi(t+qm) = 10$ and $\Psi(t+(p+q)m) = 4$. Thus we have $s_t = 0$, $s_{t+pm} = 1$, $s_{t+qm} = 1$, and $s_{t+(p+q)m} = 0$. This means that

$$s_t + s_{t+pm} + s_{t+qm} + s_{t+(p+q)m} = 0$$

for $t = 1$. Therefore, the proposed sequence can not have a high correlation of order 4.

III. Conclusions

The linear complexities of p^2q^2-periodic sequences derived from Euler quotients can be determined provided that $\gcd(pq, (p–1)(q–1))=1$, $2^{p-1} \not\equiv 1 \pmod{p^2}$ and $2^{q-1} \not\equiv 1 \pmod{q^2}$. Our results showed that binary pseudo random sequences with long periods can also be deduced from Euler quotients with RSA modulus. Furthermore, it was pointed out that this kind of sequences can not have high correlation of order four.

References

[1] Z. Chen, A. Ostafe, and A. Winterhof, "Structure of pseudorandom numbers derived from Fermat quotients," in *Arithmetic of Finite Fields – WAIFI 2010, Lecture Notes in Computer Science (vol.6087)*, Springer, Berlin, Heidelberg, pp.73–85, 2010.

[2] Z. Chen and X. Du, "On the linear complexity of binary threshold sequences derived from Fermat quotients," *Designs, Codes and Cryptography*, vol.67, no.3, pp.317–323, 2013.

[3] Z. Chen, Z. Niu, and C. Wu, "On the k-error linear complexity of binary sequences derived from polynomial quotients," *Sci. China Inform. Sci.*, vol.58, no.9, pp.1–15, 2015.

[4] Z. Chen and A. Winterhof, "Additive character sums of polynomial quotients," *Contemp Math.*, vol.579, pp.67–73, 2012.

[5] Z. Chen, "Trace representation and linear complexity of binary sequences derived from Fermat quotients," *Sci. China Inform. Sci.*, vol.57, no.11, pp.1–10, 2014.

[6] X. Du, C. Wu, and W. Wei, "An extension of binary threshold sequences from fermat quotients," *Adv. in Math. of Comm.*, vol.10, no.4, pp.743–752, 2016.

[7] C. e. Zhao, W. Ma, T. Yan, and Y. Sun, "Linear complexity of least significant bit of polynomial quotients," *Chinese Journal of Electronics*, vol.26, no.3, pp.573–578, 2017.

[8] T. Agoh, K. Dilcher, and L. Skula, "Fermat quotients for composite moduli," *Journal of Number Theory*, vol.66, no.1, pp.29–50, 1997.

[9] Z. X. Chen and A. Winterhof, "On the distribution of pseudorandom numbers and vectors derived from Euler-Fermat quotients," *International Journal of Number Theory*, vol.8, pp.631–641, 2012.

[10] Z. Chen, X. Du, and R. Marzouk, "Trace representation of pseudorandom binary sequences derived from Euler quotients," *Appli. Alg. Eng. Commun. Comp.* , vol.26, no.6, pp.555–570, 2015.

[11] Z. Niu, Z. Chen, and X. Du, "Linear complexity problems of level sequences of Euler quotients and their related binary sequences," *Sci. China Inform. Sci.*, vol.59, pp.1–12, 2016.

[12] J. Zhang, S. Gao, and C.-A. Zhao, "Linear complexity of a family of binary pq^2-periodic sequences from Euler quotients," *IEEE Trans. Inform. Theory*, vol.66, no.9, pp.5774–5780, 2020.

[13] Z. Ye, P. Ke, and Z. Chen, "Linear complexity of d-ary sequence derived from Euler quotients over $GF(q)$," *Chinese Journal of Electronics*, vol.28, no.3, pp.529–534, 2019.

[14] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers*, Springer, Berlin-Verlag, 1991.

[15] P. Fan and M. Darnell, *Sequence Design for Communications Applications*, Australia and New Zealand: Jacaranda Wiley Ltd, 1996.

[16] S. W. Golomb and G. Gong, *Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar*, Cambridge University Press, 2005.

[17] W. Su, Y. Yang, Z. Zhou, and X. Tang, "New quaternary sequences of even length with optimal auto-correlation," *Sci. China Inform. Sci.*, vol.61, no.2, pp.1–13, 2018.

[18] Y. Yang and X. Tang, "Generic construction of binary sequences of period $2n$ with optimal odd correlation magnitude based on quaternary sequences of odd period N," *IEEE Trans. Inform. Theory*, vol.64, no.1, pp.384–392, 2018.

[19] X.-X. Zhao, T. Tian, and W.-F. Qi, "A ring-like cascade connection and a class of NFSRs with the same cycle structures," *Designs, Codes and Cryptography* , vol.86, no.12, pp.2775–2790, 2018.

[20] Y. Jiang and D. Lin, "Lower and upper bounds on the density of irreducible NFSRs," *IEEE Trans. Inform. Theory*, vol.64, no.5, pp.3944–3952, 2018.

[21] J. Zhang, T. Tian, W. Qi, and Q. Zheng, "A new method for finding affine sub-families of NFSR sequences," *IEEE Trans. Inform. Theory*, vol.65, no.2, pp.1249–1257, 2019.

[22] Z. Chen, V. Edemskiy, P. Ke, and C. Wu, "On k-error linear complexity of pseudorandom binary sequences derived from Euler quotients," *Advances in Mathematics of Communications*, vol.12, no.4, pp.805–816, 2018.

[23] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol.15, no.1, pp.122–127,

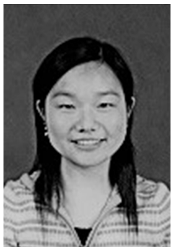
1969.

[24] A. Michael, *Algebra*. Pearson Prentice Hall, 2011.

[25] C. Ding and T. Helleseth, "New generalized cyclotomy and its applications," *Finite Fields and Their Applications*, vol.4, no.2, pp.140–166, 1998.

[26] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, New York, NY, USA: Cambridge University Press, 1986.

LUO Bingyu received the B.E. degree in mathematics from Sun Yat-sen University. He is a Ph.D. candidate of Sun Yat-sen University. His research interests include sequences design and number theory.
(Email: luoby@mail2.sysu.edu.cn)



ZHANG Jingwei received the Ph.D. degree in electronics engeneering from Sun Yat-sen University. She currently works in School of Information Science, Guangdong University of Finance and Economics in Guangdong. Her research interests include sequences design and coding theory.
(Email: jingweizhang@gdufe.edu.cn)

ZHAO Chang'an (corresponding author) received the B.E. degree in electronical engineering in 2001, the M.E. degree in applied mathematics in 2005, the Ph.D. degree in information science and technology in 2008 respectively from Sun Yat-sen University, Guangzhou, China. He presently works in School of Mathmatics in Sun Yat-sen University. His research interest lies in elliptic curve cryptography, sequences designs, and coding theory. (Email: zhaochan3@mail.sysu.edu.cn)