Optimal Parameters for the WG Stream Cipher Family

Kalikinkar Mandal, Guang Gong, Xinxin Fan and Mark Aagaard

Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ontario, Canada
{kmandal,ggong,x5fan,maagaard}@uwaterloo.ca

Abstract. In this paper, we first present some new results about the Welch-Gong (WG) transformations, followed by a description of the WG stream cipher family which is built upon an LFSR and a WG transformation over an extension field. The randomness properties of keystreams produced by a decimated WG cipher are derived based on the new results. We also discuss the selection criteria for choosing the optimal parameters for a WG cipher in order to achieve the maximum level of security. Finally, we present the optimal parameters for the WG transformations over $\mathbb{F}_{2^m}, 7 \leq m \leq 16$ based on the proposed criteria.

Keywords: Welch-Gong (WG) transformations, Stream ciphers, Boolean functions, Sequences.

1 Introduction

The WG stream cipher family is a set of hardware-oriented synchronous stream ciphers based on the Welch-Gong (WG) transformations, which consists of the WG stream ciphers and their decimated variants. A (decimated) WG cipher is composed of a linear feedback shift register (LFSR) over an extension field, followed by a (decimated) WG transformation defined over the same extension field, where the LFSR with a primitive polynomial is able to generate a sequence of maximum period. The WG stream cipher family can be regarded as nonlinear filtering generators and output one keystream bit per clock cycle. In particular, the generated keystreams of the WG cipher family have the desired randomness properties such as long period, balanced, 2-level autocorrelation, and t-tuple distributions. Moreover, the linear complexity of a keystream produced by a WG cipher is high and can be determined exactly.

The WG stream cipher is first proposed by Nawaz and Gong in 2005, which is a profile 2 candidate of the eSTREAM project [6]. Later on, two lightweight variants of the WG stream cipher named WG-7 [13] and WG-8 [7] have been proposed for securing resource-constraint smart devices. While the WG-7 stream cipher is composed of an LFSR of length 23 and a WG-7 transformation over $\mathbb{F}_{2^7}$, the WG-8 stream cipher consists an LFSR of length 20 and a WG-8 transformation over $\mathbb{F}_{2^8}$. Recently, Fan and Gong proposed to use the stream cipher WG-16 for providing confidentiality and integrity over 4G-LTE networks [8].

The security of a WG cipher is dependent on the length of the LFSR and the cryptographic strength of the WG transformation used in the cipher. As a result, the known cryptanalytic attacks such as correlation attacks [19, 15], algebraic attacks [3], cube attacks [5], discrete fourier transformation (DFT) attacks [11], distinguishing attacks [18], differential attacks [20], and time-memory-data tradeoff attacks [2] can be applied to the WG stream cipher family. Therefore, the selection of the parameters for a WG cipher is crucial in order to thwart existing attacks. In this paper, we first present some new results on WG transformations. We then give a mathematical description of the WG stream cipher family, including its operation as well as the randomness properties of the keystreams produced by a decimated WG cipher. In order to achieve the highest security against exiting attacks, we describe some criteria

on selecting the optimal parameters for a WG cipher. Finally, we summarize the optimal parameters for the WG transformations over $\mathbb{F}_{2^m}, 7 \leq m \leq 16$.

The remainder of the paper is organized as follows. In Section 2, we define some terms and notations that will be used in this paper. In Section 3, we present some new results on WG transformations. Section 4 describes the WG stream cipher family and characterizes the randomness properties of the generated keystreams. In Section 5, we list a set of criteria for selecting a decimated WG transformation for a WG cipher and in Section 6 we present the optimal parameters for WG transformations over $\mathbb{F}_{2^m}, 7 \leq m \leq 16$. Finally, in Section 7, we conclude the paper.

2 Background

In this section, we define and describe some terms and notations that will be used throughout this work.

Notation:

- $\mathbb{F}_2$: the Galois field with two elements.
- $\mathbb{F}_{2^m} = GF(2^m)$: an extension field with 2^m elements, which is defined by a primitive element α that is a root of a primitive polynomial over $\mathbb{F}_2$.
- $\mathbb{F}_2^m$: a vector space with 2^m elements and each element is of m-tuple.
- $\mathrm{Tr}(x) = x + x^2 + \cdots + x^{2^{m-1}}$: the trace function mapping from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$.

2.1 Nonlinearity of Boolean Functions and Vector Boolean Functions

Let $f(x_0, \cdots, x_{n-1})$ be a Boolean function in n variables. The *Hadamard* (or Walsh or Fourier) transform of f is defined by

$$\hat{f}(\mathbf{w}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) + \mathbf{w} \cdot \mathbf{x}} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}(\mathbf{w}x)}$$

where $\mathbf{w} = (w_0, \cdots, w_{n-1}) \in \mathbb{F}_2^n$ and $\mathbf{w} \cdot \mathbf{x} = \sum_{i=0}^{n-1} w_i x_i$, the inner product of $\mathbf{w}$ and $\mathbf{x}$.

The *distance* between two binary vectors $\mathbf{a} = (a_0, \cdots, a_{n-1})$ and $\mathbf{b} = (b_0, \cdots, b_{n-1})$, denoted by $d(\mathbf{a}, \mathbf{b})$, is defined as the number of disagreements of terms of $\mathbf{a}$ and $\mathbf{b}$, i.e.,

$$d(\mathbf{a}, \mathbf{b}) = |\{i : \ a_i \neq b_i, 1 \leq i < n \ \}| \text{ or equivalently } d(\mathbf{a}, \mathbf{b}) = H(\mathbf{a} + \mathbf{b})$$

where $H(\mathbf{x})$ is the Hamming weight of $\mathbf{x}$.

The *nonlinearity* of f, denoted as N_f, is defined by the *minimum distance* between f and all affine functions. In other words,

$$N_f = \min_{\mathbf{w} \in \mathbb{F}_2^n, c \in \mathbb{F}_2} d(f, \mathbf{w} \cdot \mathbf{x} + c)$$

or equivalently

$$N_f = 2^{n-1} - \frac{1}{2} \hat{f}_{\max}$$

where

$$\hat{f}_{\max} = \max_{\mathbf{w} \in \mathbb{F}_2^n} |\widehat{f}(\mathbf{w})|.$$

We say that F is an (n,m)-vectorial Boolean function or simply an (n,m)-function if it a function mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. An (n,m)-function F can be written as

$$F(x_0,\cdots,x_{n-1}) = (f_0(x_0,\cdots,x_{n-1}), f_1(x_0,\cdots,x_{n-1}),\cdots,f_{m-1}(x_0,\cdots,x_{n-1}))$$

where f_i's are Boolean functions in n variables.

The *nonlinearity* of F, denoted as N_F, is defined by

$$N_F = \min_{\mathbf{b}\in\mathbb{F}_{2^m}} N_{\mathbf{b}\cdot F}$$

where $\mathbf{b}\cdot F$ is the inner product. Or equivalently,

$$N_F = 2^{n-1} - \frac{1}{2}\hat{F}_{\max}$$

where

$$\hat{F}_{\max} = \max_{\mathbf{w}\in\mathbb{F}_2^n,\mathbf{b}\in\mathbb{F}_2^m} |\widehat{\mathbf{b}\cdot F}(\mathbf{w})|.$$

Let F be an (n,m)-vectorial boolean function. For any $\mathbf{a}\ (\neq \mathbf{0}) \in \mathbb{F}_2^n, \mathbf{b}\in\mathbb{F}_2^m$, we call that F is *differently k-uniform distributed* if the following equation has at most k solutions in $\mathbb{F}_2^n$

$$F(\mathbf{x}) + F(\mathbf{x}+\mathbf{a}) = \mathbf{b}.$$

2.2 Resiliency and Propagation of Boolean Functions

Let f be a Boolean function in n variables. The *additive autocorrelation* of f is defined as

$$A_f(a) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+f(x+a)},\ a\in\mathbb{F}_{2^n}.$$

We say that f has *k-order propagation* if $A_f(a) = 0$ for $1 \le H(a) \le k$. Again, we say that a balanced Boolean function f is *k-resilient* if $\hat{f}(\lambda) = 0$ for $1 \le H(\lambda) \le k$.

2.3 Algebraic Immunity of Boolean Functions

Let B_n be the set consisting of all Boolean functions in n variables. The *algebraic immunity* of f in n variables, denoted by $AI(f)$, is defined as

$$AI(f) = \min_{g\in B_m} \{\deg(g) \mid fg = 0 \text{ or } (f+1)g = 0\}$$

where $\deg(g)$ is the algebraic degree of g. For a Boolean function f in n variables, the maximum value of the algebraic immunity is equal to $\lceil \frac{n}{2} \rceil$.

The *linear span or linear complexity* of a sequence is defined as the length of the shortest LFSR that generates the sequence. Moreover, the linear span of a function $f(x)$ is defined by the number of nonzero coefficients in $f(x) = \sum_i c_i x^i$.

2.4 WG transformations

Let $m \bmod 3 \neq 0$ and k be a positive integer such that $m = 3k-1$ or $m = 3k-2$. We define a function $t(x) = x + x^{q_1} + x^{q_2} + x^{q_3} + x^{q_4}$ over $\mathbb{F}_{2^m}$ where q_i's are given by $q_1 = 2^k + 1$, $q_2 = 2^{2k-1} + 2^{k-1} + 1$, $q_3 = 2^{2k-1} - 2^{k-1} + 1$, and $q_4 = 2^{2k-1} + 2^k - 1$ for $m = 3k-1$ and $q_1 = 2^{k-1} + 1$, $q_2 = 2^{2k-2} + 2^{k-1} + 1$, $q_3 = 2^{2k-2} - 2^{k-1} + 1$, and $q_4 = 2^{2k-1} - 2^k + 1$ for $m = 3k-2$. Then, the *Welch-Gong (WG) transformation* is defined by

$$f(x) = \mathrm{Tr}(t(x+1)+1), x \in \mathbb{F}_{2^m}. \tag{1}$$

Fact 1 ([17]) *Let $f(x)$ be the WG transformation defined by Eq. (1), then*

$$f(x) = \sum_{i \in I} \mathrm{Tr}(x^i)$$

where $I = I_1 \cup I_2$, $I_1 = \{2^{2k-1} + 2^{k-1} + 2 + i : 0 \leq i \leq 2^{k-1} - 3\}$ and $I_2 = \{2^{2k} + 3 + 2i : 0 \leq i \leq 2^{k-1} - 2\}$ for $m = 3k-1$ and $I = \{1\} \cup I_3 \cup I_4$, $I_3 = \{2^{k-1} + 2 + i : 0 \leq i \leq 2^{k-1} - 3$ and $I_4 = \{2^{2k-1} + 2^{k-1} + 2 + i : 0 \leq i \leq 2^{k-1} - 3\}$ for $m = 3k-2$.

3 The New Results on the WG Transformations

Let $m \not\equiv 0 \bmod 3$ and k be a positive integer such that $3k \equiv 1 \bmod m$. The function $t(x)$ from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ is defined as $t(x) = x + x^{r_1} + x^{r_2} + x^{r_3} + x^{r_4}$, where $r_1 = 2^k + 1$, $r_2 = 2^{2k} + 2^k + 1$, $r_3 = 2^{2k} - 2^k + 1$, $r_4 = 2^{2k} + 2^k - 1$. A WG permutation, denoted by $WGperm(x)$, is a permutation over $\mathbb{F}_{2^m}$, whereas a WG transformation, denoted by $WG(x)$, is a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. The functions $WGperm(x)$ and $WG(x)$ are defined as

$$WGperm(x) = t(x+1) + 1 \tag{2}$$

$$WG(x) = \mathrm{Tr}(WGperm(x)) = \sum_{i \in I} \mathrm{Tr}(x^i), x \in \mathbb{F}_{2^m} \tag{3}$$

where I is the set consisting of coset leaders modulo $2^m - 1$.

Note that r_i's are computed by the rules given in [4] for making $t(x)$ a permutation, and the exponents r_i's are different from the exponents q_i's in Eq. (1) which are taken from [17]. However, $WG(x)$ is identical for both representations.

In this section, we investigate how to determine the set I in Eq. (3) in the case of $3k \equiv 1 \bmod m$. Based on the set I, we compute the algebraic degree of the Boolean form as well as the linear span of a WG transformation. Moreover, we show that the algebraic degree and linear span are the same as those presented in [10].

3.1 New Exponent Sets *I*'s

When k in $WG(x)$ is computed from the equation $m = 3k-1$ or $m = 3k-2$, the exponent sets I's have been discovered in Fact 1. We now determine the new exponent sets I's in Theorems 1 and 2 when k is chosen as $3k \equiv 1 \bmod m$ for $m \equiv 2 \bmod 3$ and $m \equiv 1 \bmod 3$, respectively. Note that for $m \bmod 3 = 1$ and $m \bmod 3 = 2$, we have $2m = 3k-1$ and $m = 3k-1$ for some positive integer k, respectively. These facts are extensively used in the proofs of Theorems 1 and 2 below.

Theorem 1. *Let k be a positive integer such that $3k \equiv 1 \bmod m$ and $m \equiv 2 \bmod 3$. Then*

$$WG(x) = \mathrm{Tr}(t(x+1)+1) = \sum_{i \in I} \mathrm{Tr}(x^i) \tag{4}$$

where $I = I_1 \cup I_2$, $I_1 = \{2^{2k-1} + 2^{k-1} + 2 + j : 0 \le j \le 2^{k-1} - 3\}$ and $I_2 = \{2^{2k} + 2 \cdot j + 1 : 1 \le j \le 2^{k-1} - 1\}$.

Proof. After expansion, the first three terms of $t(x+1)+1$ can be written as

$$x + (x+1)^{2^k+1} + (x+1)^{2^{2k}+2^k+1} = x + x^{2^k} + x^{2^{2k}+1} + x^{2^{2k}+2^k} + x^{2^{2k}+2^k+1}. \tag{5}$$

$$(x+1)^{2^{2k}-2^k+1} = (x+1)(x+1)^{2^k(2^k-1)} = (x+1)(x^{2^k}+1)^{2^k-1} = \sum_{i=0}^{2^k-1} x^{i \cdot 2^k+1} + \sum_{i=0}^{2^k-1} x^{i \cdot 2^k}. \tag{6}$$

$$(x+1)^{2^{2k}+2^k-1} = (x+1)^{2^{2k}}(x+1)^{2^k-1} = \sum_{i=0}^{2^k-1} x^{2^{2k}+i} + \sum_{i=0}^{2^k-1} x^i. \tag{7}$$

Combining Eqs. (5) - (7), we obtain

$$\begin{aligned}
\mathrm{Tr}(t(x+1)+1) &= \mathrm{Tr}\left(x^{2^{2k}+2^k+1} + \sum_{i=0}^{2^k-1} x^{i \cdot 2^k+1} + \sum_{i=0}^{2^k-1} x^{2^{2k}+i} \right) \\
&= \mathrm{Tr}\left(x^{2^{2k}+2^k+1} + \sum_{i=0}^{2^k-1} x^{M(i)} + \sum_{i=0}^{2^k-1} x^{N(i)} \right)
\end{aligned}$$

where $M(i) = i \cdot 2^k + 1$ and $N(i) = 2^{2k} + i$. Using the facts that $M(i) = N(2i)$ and $\mathrm{Tr}(x^{M(2^{k-1})}) = \mathrm{Tr}(x^{N(2)})$, we obtain

$$\begin{aligned}
WG(x) &= \mathrm{Tr}(t(x+1)+1) \\
&= \mathrm{Tr}\left(x^{2^{2k}+2^k+1} + \sum_{i=1}^{2^{k-1}-1} x^{M(i+2^{k-1})} + \sum_{i=1}^{2^{k-1}-1} x^{N(2i+1)} \right) \\
&= \mathrm{Tr}\left(x^{2^{2k}+2^k+1} + \sum_{i=1}^{2^{k-1}-1} x^{2^{2k-1}+1+2^k \cdot i} + \sum_{i=1}^{2^{k-1}-1} x^{2^{2k}+2i+1} \right) \\
&= \mathrm{Tr}\left(\sum_{i=2}^{2^{k-1}-1} x^{2^{2k-1}+2^{k-1}+i} + \sum_{i=1}^{2^{k-1}-1} x^{2^{2k}+2i+1} \right) \\
&= \mathrm{Tr}\left(\sum_{i=0}^{2^{k-1}-3} x^{2^{2k-1}+2^{k-1}+2+i} + \sum_{i=1}^{2^{k-1}-1} x^{2^{2k}+2i+1} \right) \\
&= \sum_{i=0}^{2^{k-1}-3} \mathrm{Tr}\left(x^{2^{2k-1}+2^{k-1}+2+i} \right) + \sum_{i=1}^{2^{k-1}-1} \mathrm{Tr}\left(x^{2^{2k}+2i+1} \right)
\end{aligned} \tag{8}$$

as $2^{2k-1}(2^{2k-1} + 1 + 2^k \cdot i) = 2^{2k-1} + 2^{k-1} + i$ when $2^{3k-1} \equiv 1 \bmod 2^m - 1$. □

Theorem 2. *Let k be a positive integer such that $3k \equiv 1 \bmod m$ and $m \equiv 1 \bmod 3$. Then*

$$WG(x) = \mathrm{Tr}(t(x+1)+1) = \sum_{i \in I} \mathrm{Tr}(x^i) \tag{9}$$

where $I = I_1 \cup I_2 \cup I_3 \cup I_4$, $I_1 = \{2^{\frac{k-1}{2}} + 2 + i : \ 0 \le i \le 2^{\frac{k-1}{2}} - 2\}$, $I_2 = \{2^{\frac{k+1}{2}} + 1 + 2(i + 2^{\frac{k-1}{2}}(2^{j+1} - 1) + 2^j - 1) : 0 \le j \le \frac{k-7}{2}, 1 \le i \le 2^j\}$, $I_3 = \{2^{\frac{k+1}{2}} + 1 + 2(i + 2^{\frac{k-1}{2}}(2^{\frac{k-3}{2}} - 1) + 2^{\frac{k-5}{2}} - 1) : 1 \le i \le 2^{\frac{k-5}{2}}\}$ and $I_4 = \{2^{\frac{k+1}{2}} + 1 + 2(i + 2^{\frac{k-1}{2}}(2^{\frac{k-1}{2}} - 1) + 2^{\frac{k-3}{2}} - 1) : 2 \le i \le 2^{\frac{k-3}{2}}\}$.

Proof. For $m \equiv 1 \bmod 3$, we have $2m = 3k - 1$ for some odd positive integer k. Therefore, we obtain $2^{3k-1} \bmod (2^m - 1) = 1$ and $2^{\frac{3k-1}{2}} \bmod (2^m - 1) = 1$. Using the equation $2^{3k-1} \bmod (2^m - 1) = 1$, we can write $WG(x)$ as Eq (8). Furthermore, using the equation $2^{\frac{3k-1}{2}} \bmod (2^m - 1) = 1$, Eq (8) can be written as

$$\begin{aligned} WG(x) &= \mathrm{Tr}(t(x+1)+1) \\ &= \sum_{i=0}^{2^{k-1}-3} \mathrm{Tr}\left(x^{2^{\frac{k-1}{2}} + 2^{k-1} + 2 + i}\right) + \sum_{i=1}^{2^{k-1}-1} \mathrm{Tr}\left(x^{2^{\frac{k+1}{2}} + 2i + 1}\right) \\ &= \sum_{i=0}^{2^{k-1}-3} \mathrm{Tr}\left(x^{P(i)}\right) + \sum_{i=1}^{2^{k-1}-1} \mathrm{Tr}\left(x^{Q(i)}\right) \end{aligned} \tag{10}$$

where $P(i) = 2^{\frac{k-1}{2}} + 2^{k-1} + 2 + i$ and $Q(i) = 2^{\frac{k+1}{2}} + 2i + 1$ and we denote by P and Q the set of $P(i)$'s and $Q(i)$'s, respectively. Note that all $Q(i)$'s are odd and $P(i)$'s might be odd or even and some exponents belong to both P and Q. We then apply the following transformation $\frac{k-1}{2}$ times: at j-th ($2 \le j \le \frac{k-1}{2}$) iteration, 2^{k-1-j} odd exponents will be canceled out from P and Q as they occur in both P and Q and after cancellation $P(i)$ is set to be $\frac{P(i)}{2}$. In the first iteration (i.e., $j = 1$), only $2^{k-2} - 1$ elements will be canceled out from $P(i)$ and $Q(i)$. Then, after simplification, Eq. (10) can be written as

$$WG(x) = \mathrm{Tr}(t(x+1)+1) = \sum_{i=0}^{2^{\frac{k-1}{2}-2}} \mathrm{Tr}\left(x^{2^{\frac{k-1}{2}} + 2 + j}\right) + \sum_{j=0}^{\frac{k-7}{2}} \sum_{i=1}^{2^j} \mathrm{Tr}\left(x^{2^{\frac{k+1}{2}} + 1 + 2\left(i + 2^{\frac{k-1}{2}}(2^{j+1} - 1) + 2^j - 1\right)}\right)$$

$$+ \sum_{i=1}^{2^{\frac{k-5}{2}}} \mathrm{Tr}\left(x^{2^{\frac{k+1}{2}} + 1 + 2\left(i + 2^{\frac{k-1}{2}}\left(2^{\frac{k-3}{2}} - 1\right) + 2^{\frac{k-5}{2}} - 1\right)}\right) + \sum_{i=2}^{2^{\frac{k-3}{2}}} \mathrm{Tr}\left(x^{2^{\frac{k+1}{2}} + 1 + 2\left(i + 2^{\frac{k-1}{2}}\left(2^{\frac{k-1}{2}} - 1\right) + 2^{\frac{k-3}{2}} - 1\right)}\right).$$

Hence the result is established. □

We note that in both cases the total number of exponents in I is equal to $(2^{\lceil \frac{m}{3} \rceil} - 3)$ for $m \bmod 3 = 1$ and $\frac{k+1}{2} = \lceil \frac{m}{3} \rceil$ as well as for $m \bmod 3 = 2$ and $k = \lceil \frac{m}{3} \rceil$. Moreover, the set I contains the exponents that belong to different cyclotomic cosets.

3.2 Algebraic Degree and Linear Span

We now calculate the algebraic degree of a WG transformation for the case of $m \bmod 3 = 1$. When m satisfies $m \bmod 3 = 2$, the algebraic degree of a WG transformation is $(\lceil \frac{m}{3} \rceil + 1)$ and the proof is similar to that of Theorem 5 in [10].

Property 1. Let $WG(x)$ be the WG transformation defined by (9), then the algebraic degree of $WG(x)$, denoted as $\deg(WG(x))$, is given by

$$\deg(WG(x)) = \frac{k+1}{2} + 1 = \left\lceil \frac{m}{3} \right\rceil + 1.$$

Proof. It is known that the algebraic degree of $WG(x)$ is determined by the largest Hamming weight of the exponents in (9). For $j = 2^k + 2^{\frac{k+1}{2}} - 1 \in I_4$, $H(j) = \frac{k+1}{2} + 1$ is the maximum Hamming weight among all exponents in I and for $m \equiv 1 \bmod 3$. Thus, the algebraic degree of $WG(x)$ is equal to $\frac{k+1}{2} + 1 = \lceil \frac{m}{3} \rceil + 1$. □

Theorem 3. *Let $WG(x)$ be the WG transformation defined by (9), then the linear span of $WG(x)$, denoted as $LS(WG(x))$, is given by*

$$LS(WG(x)) = m\left(2^{\frac{k+1}{2}} - 3\right) = m\left(2^{\lceil \frac{m}{3} \rceil} - 3\right).$$

Proof. The proof is similar to that of Theorem 3 in [10]. □

Theorem 4. *Let $WG(x) = \sum_{i \in I} \mathrm{Tr}(x^i)$ be the WG transformation defined by Eq. (3). Then there exists at least one exponent $j \in I$ such that j is coprime with $2^m - 1$.*

Proof. We observe that for $m \bmod 3 = 2$, $j = r = 2^{2k} + 3$ and for $m \bmod 3 = 1$, $j = s = 2^{k-1}$ always exist in the exponent set I. To prove the result, we only need to show that $\gcd(r, 2^m - 1) = 1$ as the exponent $s = 2^{k-1}$ is coprime to $2^m - 1$. We have

$$\begin{aligned}
\gcd(2^{2k} + 3, 2^m - 1) &= \gcd(2^{2k} + 3, 2^{3k-1} - 1) \\
&= \gcd(2^{2k} + 3, (2^{3k-1} - 1) - (2^{2k} + 3) \cdot 2^{k-1}) \\
&= \gcd(2^{2k} + 3, 3 \cdot 2^{k-1} + 1) \\
&= \gcd(3 \cdot (2^{2k} + 3), 3 \cdot 2^{k-1} + 1) \text{ since } \gcd(3, 3 \cdot 2^{k-1} + 1) = 1 \\
&= \gcd(3 \cdot (2^{2k} + 3) - 2^{k+1} \cdot (3 \cdot 2^{k-1} + 1), 3 \cdot 2^{k-1} + 1) \\
&= \gcd(2^{k+1} - 9, 3 \cdot 2^{k-1} + 1) \\
&= \gcd(2^{k+1} - 9, 31) \text{ since } \gcd(4, 2^{k+1} - 9) = 1.
\end{aligned}$$

We now need to show that $\gcd(2^{k+1} - 9, 31) = 1$. It can be easily checked that $31 \nmid (2^{k+1} - 9)$ for $k = 0, 1, 2, 3, 4$. For $k \geq 5$, we write k as $k = 5l + i$, $0 \leq i \leq 4$ and $l \geq 1$. Again it can be verified that $(2^{k+1} - 9) \equiv (2^{i+1} - 9) \bmod 31$ for $k \geq 5$. Therefore, $\gcd(2^{k+1} - 9, 31) = 1$. This completes the proof. □

4 The Decimated WG Stream Cipher Family

In this section, we describe the WG stream cipher family that consists of the WG ciphers as well as their decimated variants. Moreover, we also present the randomness properties of the keystreams generated by various instances of the WG stream cipher family.

4.1 Description of a WG Stream Cipher and Its Decimation

A WG stream cipher is based on a WG transformation and can be regarded as a nonlinear filter generator over an extension field $\mathbb{F}_{2^m}$. A WG cipher, as shown in Figure 1, consists of an

LFSR of length l, followed by a WG transformation over $\mathbb{F}_{2^m}$. The characteristic polynomial of the LFSR is a primitive polynomial $p(x)$ of degree l over $\mathbb{F}_{2^m}$, i.e., $p(x) = x^l + \sum_{i=0}^{l-1} c_i x^i$, $c_i \in \mathbb{F}_{2^m}$ and the LFSR generates an m-sequence over $\mathbb{F}_{2^m}$ with period $2^n - 1$ where $n = ml$. Note that the WG cipher family is defined over $\mathbb{F}_{2^m}$ for $m \not\equiv 0 \bmod 3$ as a WG transformation exists only if $m \not\equiv 0 \bmod 3$. During the initialization phase, the cipher is executed for $2l$ clock cycles with the feedback signal Init. When the cipher goes into the running phase, the only feedback is within the LFSR and one keystream bit is generated per clock cycle. We denote a WG cipher/generator with an LFSR of l stages over $\mathbb{F}_{2^m}$ as a $\mathsf{WG}(m, l)$ generator.

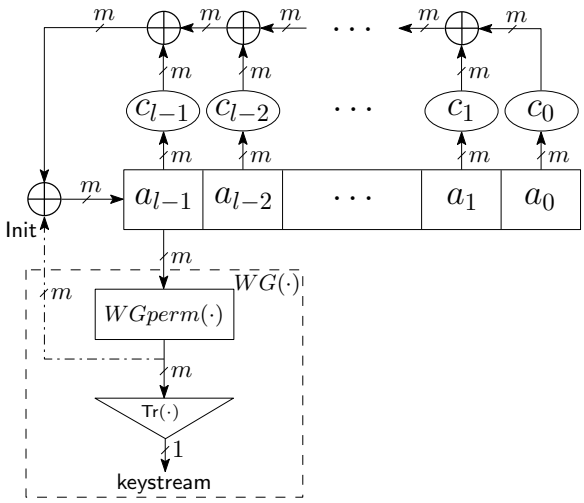

Fig. 1. The WG Stream Cipher Family

We denote by $\{a_k\}_{k\geq 0}$ the LFSR sequence over $\mathbb{F}_{2^m}$ and $\{s_k\}_{k\geq 0}$ the output sequence or keystream over $\mathbb{F}_2$. The mathematical expressions of updating the LFSR internal state and the output sequence of the $\mathsf{WG}(m, l)$ generator are given by

$$a_{k+l} = \begin{cases} \sum_{i=0}^{l-1} c_i a_{i+k} + WGperm(a_{k+l-1}) & 0 \leq k < 2l \text{ (initialization phase)} \\ \sum_{i=0}^{l-1} c_i a_{i+k} & k \geq 2l \text{ (running phase)} \end{cases}$$
$$s_k = WG(a_{k+3l-1}), \quad k = 0, 1, \cdots$$

where $WGperm(x)$ and $WG(x)$ denote the WG permutation and WG transformation, respectively, as defined in Section 3.

Definition 1. *A decimated WG permutation and decimated WG transformation are defined as $WGperm(x^d)$ and $WG(x^d)$, respectively, where $\gcd(d, 2^m - 1) = 1$. In other words, $WGperm(x^d)$ is the composition of $WGperm(x)$ and the monomial x^d, whereas $WG(x^d)$ is the composition of $WG(x)$ and x^d. In symbol, $WGperm(x^d) = WGper(x) \circ x^d$ and $WG(x^d) = WG(x) \circ x^d$.*

Definition 2. *When two functions $WGperm(x)$ and $WG(x)$ in a $\mathsf{WG}(m, l)$ generator are replaced by their respective decimations, i.e., $WGperm(x^d)$ and $WG(x^d)$, the resulting generator, denoted as $\mathsf{WG}_d(m, l)$, is referred to as a* decimated WG cipher/generator.

4.2 Randomness Properties of Decimated WG Keystreams

It is known that an output sequence or keystream of a $\mathsf{WG}(m,l)$ generator has the following randomness properties.

Proposition 1 ([9]). *For a $\mathsf{WG}(m,l)$ generator, an output sequence/keystream has the following randomness properties.*

(a) Period is 2^n-1.
(b) It is balanced.
(c) It has an ideal 2-level autocorrelation property.
(d) Any t-tuple is equally likely distributed (ideal t-tuple distribution) $(1 \le t \le l)$.
(e) Linear span or linear complexity, denoted by $LS_{\mathsf{WG}(m,l)}$, increases exponentially in m, which can be determined exactly as

$$LS_{WG(m,l)} = m\sum_{i\in I} l^{H(i)},$$

where $H(i)$ is the Hamming weight of integer i.

Note that both the linear span and the resistance to algebraic attacks are determined by the algebraic degree of the WG transformation when the LFSR is fixed. The algebraic degree of $WG(x)$ is given by

$$\deg(WG(x)) = \max_{i\in I} H(i) = \left\lceil \frac{m}{3} \right\rceil + 1$$

where $WG(x) = \sum_{i\in I} \mathrm{Tr}(x^i)$.

According to Theorem 8.4 and Proposition 8.7 in [9], a decimated $WG_d(m,l)$ has the same randomness properties as those listed in Proposition 1 except for the linear span. Furthermore, we have the following randomness properties for a keystream produced by a decimated WG cipher.

Proposition 2. *The decimated $WG_d(m,l)$ has the same randomness properties (a)-(d) as described in Proposition 1, and the linear span of a $WG_d(m,l)$ keystream is given by*

$$LS_{WG_d(m,l)} = m\sum_{i\in I} l^{H(d\cdot i)}$$

where $(d\cdot i)$ is reduced by modulo 2^m-1. Furthermore, the algebraic degree of $WG(x^d)$ is determined by

$$\deg\left(WG_d(x^d)\right) = \max_{i\in I} H(d\cdot i).$$

Theorem 5. *For $WG(x) = \sum_{i\in I}\mathrm{Tr}(x^i)$, there exist some coset leader d modulo 2^m-1 with $\gcd(d, 2^m-1) = 1$ and some $i \in I$ satisfying*

$$H(d\cdot i) = m-1$$

and for this d, $WG(x^d)$ achieves the maximum algebraic degree.

Proof. In Theorem 4, we have showed that there exists at least one $i \in I$ such that $\gcd(i, 2^m-1) = 1$. Since the set I contains $(2^{\lceil \frac{m}{3} \rceil} - 3)$ decimation numbers and for some $i \in I$ with $\gcd(i, 2^m-1) = 1$, the decimation numbers $d_i = \frac{(2^{m-1}-1)}{i}\cdot 2^{j-1}$, $1 \le j \le m$, reduced by modulo (2^m-1), can be used in $WG(x)$ to achieve the maximum Hamming weight $m-1$ in the decimated exponent set I. Therefore, for $d = d_i$, the algebraic degree of $WG(x^d)$ achieves the maximum value $m-1$. □

Definition 3. *The decimation d such that $WG(x^d)$ has maximum algebraic degree and maximum algebraic immunity is referred to an* optimal decimation.

Proposition 3. *If $\mathsf{WG}_d(m,l)$ has an optimal decimation d, the linear span is lower bounded by*

$$LS_{\mathsf{WG}_d(m,l)} > ml^{m-1}.$$

For a WG cipher $\mathsf{WG}(m,l)$, the lower bound of the linear span of a keystream is bounded by $ml^{\lceil \frac{m}{3} \rceil + 1}$. On the other hand, the linear span of a ketsream produced by a decimated WG cipher $\mathsf{WG}_d(m,l)$ for an optimal decimation d is lower bounded by ml^{m-1}.

4.3 Optimal Decimations for decimated WG ciphers

In a decimated WG cipher $\mathsf{WG}_d(m,l)$, the most complicated module is $WGperm(x^d)$ from an implementation point of view, where one needs to first compute x^d. Thus the Hamming weight of d should be as small as possible subject to other requirements such as nonlinearity, and differential k-uniform distribution. In Tables 1 to 4, we list all values of d for which $\deg(WG(x^d)) = m-1$ for $7 \le m \le 16$.

5 Cryptographic Properties of Decimated WG Permutations and Transformations

In this section, we present the criteria of selecting an optimal decimation number for a (decimated) WG cipher. With an optimal decimation number, a decimated WG transformation has good cryptographic properties, thereby offering a maximum level of security.

5.1 Resilience to Linear and Differential Cryptanalysis

For odd m's, it is known that $WG(x)$ has the following cryptographic properties (see [10]).

(a) Nonlinearity is given by $2^{m-1} - 2^{(m-1)/2}$.
(b) It is 1-order resilient.
(c) Additive autocorrelation between $f(x+a)$ and $f(x)$ has three values: $0, \pm 2^{(m+1)/2}$.
(d) It has 1-order propagation property.

However, there are no theoretical results about: 1) The above cryptographic properties of $WG(x)$ when m is even; 2) The above cryptographic properties of $WG(x^d)$ for both odd and even m's; and 3) The nonlinearity and differential k-uniform distribution of $WGperm(x)$ and $WGperm(x^d)$ for both odd and even m's. Fortunately, we can check those properties by computation for $7 \le m < 30$ in practice.

5.2 Criteria for Selecting Decimated WG Transformations and Permutations

Together with the results in Section 4, we obtain the following criteria for selecting an optimal decimation d.

1. Optimal decimation number for $WG(x^d)$: select d such that both the algebraic degree and the algebraic immunity of $WG(x^d)$ are maximum, i.e., $\deg(WG(x^d)) = m-1$ and $AI(WG(x^d)) = \lceil m/2 \rceil$. Define

$$O = \{d : \gcd(d, 2^m - 1) = 1, \deg(WG(x^d)) = m-1, AI(WG(x^d)) = \lceil m/2 \rceil\}.$$

2. Cryptographic properties of $WG(x^d)$: select $d \in O$ such that $WG(x^d)$ has the following properties.
   (a) Hamming weight of d should be as small as possible.
   (b) Nonlinearity of $WG(x^d)$, denoted by N_d, should be as large as possible.
   (c) Let $Resi_d$ be the number of λ such that $\hat{WG}_d(\lambda) = 0$ for $H(\lambda) = 1$. Since the degree of $WG(x^d)$ is maximum, the resiliency is equal to zero. Hence, the decimation number d should be chosen such that $Resi_d$ is as large as possible. Essentially, $Resi_d$ characterizes the number of components functions that cannot be approximated by the linear functions.
   (d) Let A_{WG_d} be the additive correlation of $WG(x^d)$ and $A_d = \max_{a \in \mathbb{F}_{2^m}} A_{WG_d}(a)$. The decimation number d should be chosen such that A_d is as small as possible. Moreover, in order to thwart the differential attacks, the selection of d also needs to satisfy that for $H(a) = 1$ we have as many $A_d(a) = 0$ as possible.
3. Cryptographic properties of $WGperm(x^d)$: select $d \in O$ such that $WGperm(x^d)$ has the following properties.
   (a) The nonlinearity should be as large as possible.
   (b) The value of k in a differential k-uniform distribution should be as small as possible.

6 Optimal Decimations for WG Permutations and Transformations

Based on the criteria presented in Section 5.2, we calculate the algebraic degree, nonlinearity, algebraic immunity, $Resi_d$, and A_d for WG transformations as well as the nonlinearity and differential k-uniform for WG permutations over the finite field $\mathbb{F}_{2^m}$, $7 \leq m \leq 16$, where the primitive polynomials given in Table 3.5 of [9] are used to construct $\mathbb{F}_{2^m}$. Our results are summarized in Tables 1 to 4. Due to the high computational complexity, we cannot compute the nonlinearity and differential k-uniform of WG permutation for $m = 14$ and 16. Instead we compute the upper and lower bounds, denoted by N_u and N_l, respectively, of the nonlinearities of the component functions of WG permutations in these cases, where we consider a WG permutation as an (m, m)-vector Boolean function.

Table 1. Optimal parameters for WG-7/8

Decimation d	Hamming weight of d	Degree of $WG(x^d)$	AI of $WG(x^d)$	Nonlinearity of $WG(x^d)$	$(Resi_d, A_d)$ of $WG(x^d)$	Nonlinearity of $WGperm(x^d)$	k-uniform of $WGperm(x^d)$
WG-7							
63	6	6	4	50	$(1, 3)$	42	10
5	2	6	3	30	$(1, 0)$	30	10
9	2	6	3	50	$(1, 3)$	44	8
13	3	6	3	42	$(3, 0)$	42	6
21	3	6	3	42	$(0, 2)$	42	12
WG-8							
19	3	7	4	108	$(3, 4)$	92	10
61	5	7	4	110	$(0, 0)$	92	12
13	3	7	3	80	$(0, 0)$	80	16

Table 2. Optimal parameters for WG-10/11

Decimation d	Hamming weight of d	Degree of $WG(x^d)$	AI of $WG(x^d)$	Nonlinearity of $WG(x^d)$	$(Resi_d, A_d)$ of $WG(x^d)$	Nonlinearity of $WGperm(x^d)$	k-uniform of $WGperm(x^d)$
WG-10							
73	3	9	5	470	$(1,0)$	436	14
29	4	9	5	456	$(0,0)$	424	18
43	4	9	5	460	$(0,0)$	416	14
179	5	9	5	460	$(3,1)$	436	14
125	6	9	5	456	$(0,2)$	412	12
511	9	9	5	460	$(1,0)$	436	12
59	5	9	4	420	$(0,0)$	412	12
WG-11							
203	5	10	6	932	$(0,0)$	908	14
373	6	10	6	882	$(0,0)$	882	12
149	4	10	5	946	$(0,0)$	922	14
179	5	10	5	962	$(0,0)$	920	12
333	5	10	5	952	$(0,0)$	920	12
245	6	10	5	962	$(2,2)$	918	12
175	6	10	5	902	$(0,0)$	902	14
687	7	10	5	946	$(0,0)$	920	12
251	7	10	5	954	$(0,1)$	924	14
501	7	10	5	958	$(0,0)$	918	12
751	8	10	5	926	$(0,1)$	914	12

7 Conclusion

In this paper, we presented some new results on WG transformations including determining the new exponent set I when k is chosen as $3k \equiv 1 \bmod m$. Then, we listed the randomness properties of keystreams produced by a decimated WG cipher and discussed the selection criteria for choosing the parameters of a (decimated) WG stream cipher in order to offer the maximum level of security against existing attacks. Furthermore, we summarized all the optimal parameters for WG transformations over $\mathbb{F}_{2^m}$, $7 \leq m \leq 16$.

Acknowledgements: The authors would like to thank Dr. Zilong Wang for his help in proving Theorem 4.

References

1. E.R. Berlekamp. *Algebraic Coding Theory*, McGraw-Hill, New York, ch. 7, 1968.
2. A. Biryukov and A. Shamir. Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers, *Advances in Cryptology-Asiacrypt'00,* Vol. 1976, LNCS, pp. 1-13, Springer-Verlag, 2000.
3. N. Courtois and W. Meier. Algebraic Attacks on Stream Ciphers with Linear Feedback Shift Registers, *Advances in Cryptology-Eurocrypt'03,* Vol. 2656, LNCS, pp. 345-359, Springer-Verlag, 2003.
4. J. Dillon and H. Dobbertin. New Cyclic Difference sets with Singer parameters, *Finite Fields and Their Application,* 10(2004), pp. 342-389, August 1999.
5. I. Dinur, and A. Shamir. Cube Attacks on Tweakable Black Box Polynomials, *Advances in Cryptology-EUROCRYPT '09*, LNCS, pp. 278-299, Springer-Verlag, 2009.
6. eSTREAM - The ECRYPT Stream Cipher Project, `http://www.ecrypt.eu.org/stream/.`
7. X. Fan, K. Mandal, G. Gong. WG-8: A Lightweight Stream Cipher for Resource-Constrained Smart Devices, *Proceedings of the 9th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, January 2013.

8. X. Fan and G. Gong. Specification of the Stream Cipher WG-16 Based Confidentiality and Integrity Algorithms. Technical Report CACR 2013-06, University of Waterloo, February 2013.
9. S.W. Golomb, and G. Gong. *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*, Cambridge University Press, New York, NY, USA, 2004.
10. G. Gong, and A. Youssef. Cryptographic Properties of the Welch-Gong Transformation Sequence Generators, *IEEE Transactions on Information Theory*, Vol. 48, No. 11, pp. 2837-2846, November 2002.
11. G. Gong, S. Rønjom, T. Helleseth, and H. Hu. Fast Discrete Fourier Spectra Attacks on Stream Ciphers, *IEEE Transactions on Information Theory*, Vol 57, No. 8, pp. 5555-5565, August 2011.
12. C. Lam, M. Aagaard and G. Gong. Hardware Implementations of Multi-output Welch-Gong Ciphers. Technical Report CACR 2011-01, University of Waterloo, 2011.
13. Y. Luo, Q. Chai, G. Gong, and X. Lai. WG-7: A Lightweight Stream Cipher with Good Cryptographic Properties, *IEEE Global Communications Conference* – GLOBECOM 2010, pp. 1-6, 2010.
14. J.L. Massey. Shift-Register Synthesis and BCH Decoding, *IEEE Transactions on Information Theory* Vol. 15, No. 1, pp. 122-127, 1969.
15. W. Meier, and O. Staffelbach. Fast Correlation Attacks on Certain Stream Ciphers, *Journal of Cryptology*, pp.159-176, 1989.
16. Y. Nawaz and G. Gong. WG: A Family of Stream Ciphers with Designed Randomness Properties, *Information Science*, vol. 178, no. 7, pp. 1903-1916, 2008.
17. J.S. No, S.W. Golomb, G. Gong, H.K. Lee, and P. Gaal. New Binary Pseudorandom Sequences of Period $2^n - 1$ with Ideal Autocorrelation, *IEEE Transactions on Information Theory*, Vol. 44, No. 2, pp. 814-817, March 1998.
18. M. Orumiehchiha, J. Pieprzyk and R. Steinfeld. Cryptanalysis of WG-7: A Lightweight Stream Cipher, Cryptography and Communications, Vol. 4, No. 3-4, pp. 277-285, 2012.
19. T. Siegenthaler. Correlation-immunity of Nonlinear Combining Functions for Cryptographic Applications, *IEEE Transactions on Information Theory*, Vol. 30, No. 5, pp. 776-780, September 1984.
20. H. Wu, and B. Preneel. Chosen IV Attack on Stream Cipher WG, *ECRYPT Stream Cipher Project Report 2005/045*. Available at http://cr.yp.to/streamciphers/wg/045.pdf

Table 3. Optimal parameters for WG-13/14

Decimation d	Hamming weight of d	Degree of $WG(x^d)$	AI of $WG(x^d)$	Nonlinearity of $WG(x^d)$	$(Resi_d, A_d)$ of $WG(x^d)$	Nonlinearity of $WGperm(x^d)$	k-uniform of $WGperm(x^d)$
WG-13							
195	4	12	7	3950	$(0,0)$	3856	14
345	5	12	7	3912	$(0,0)$	3858	54
377	6	12	7	3968	$(1,0)$	3872	14
1365	6	12	7	3962	$(1,0)$	3856	14
733	7	12	7	3948	$(0,1)$	3850	14
951	8	12	7	3968	$(0,0)$	3836	16
1271	8	12	7	3936	$(0,4)$	3832	14
273	3	12	6	3902	$(0,0)$	3844	16
85	4	12	6	3926	$(0,0)$	3860	14
585	4	12	6	3910	$(0,0)$	3868	14
227	5	12	6	3914	$(0,1)$	3870	16
327	5	12	6	3950	$(1,0)$	3850	14
301	5	12	6	3944	$(0,0)$	3860	14
1189	5	12	6	3718	$(0,0)$	3718	16
315	6	12	6	3936	$(0,3)$	3854	14
455	6	12	6	3874	$(0,0)$	3856	14
489	6	12	6	3954	$(0,0)$	3850	14
725	6	12	6	3954	$(0,1)$	3846	16
819	6	12	6	3926	$(0,0)$	3860	14
1175	6	12	6	3934	$(0,0)$	3840	18
1205	6	12	6	3798	$(0,0)$	3798	16
431	7	12	6	3926	$(0,0)$	3866	16
505	7	12	6	3946	$(1,0)$	3858	16
875	7	12	6	3970	$(0,0)$	3862	14
863	8	12	6	3822	$(0,0)$	3822	14
893	8	12	6	3964	$(0,2)$	3850	16
1879	8	12	6	3926	$(0,0)$	3848	28
1979	9	12	6	3642	$(0,0)$	3642	16
4095	12	12	6	3932	$(2,4)$	3860	14
WG-14						(N_l, N_u)	
47	5	13	7	7960	$(0,0)$	$(7900, 7966)$	–
59	5	13	7	7868	$(0,0)$	$(7900, 7958)$	–
203	5	13	7	7936	$(0,0)$	$(7898, 7940)$	–
461	6	13	7	7868	$(0,0)$	$(7898, 7956)$	–
1133	6	13	7	7936	$(0,0)$	$(7888, 7962)$	–
1181	6	13	7	7824	$(1,1)$	$(7874, 7952)$	–
1351	6	13	7	7924	$(1,3)$	$(7896, 7946)$	–
2771	7	13	7	7980	$(1,0)$	$(7906, 7960)$	–
703	8	13	7	7954	$(0,0)$	$(7908, 7962)$	–
1003	8	13	7	7968	$(0,0)$	$(7908, 7946)$	–
2519	8	13	7	7900	$(0,1)$	$(7884, 7954)$	–
3757	8	13	7	7700	$(0,0)$	$(7908, 7944)$	–
1019	9	13	7	7946	$(0,0)$	$(7908, 7952)$	–
2527	9	13	7	7926	$(1,0)$	$(7884, 7946)$	–
3059	9	13	7	7974	$(0,0)$	$(7902, 7962)$	–
3563	9	13	7	7940	$(2,0)$	$(7896, 7946)$	–
1919	10	13	7	7948	$(2,0)$	$(7898, 7950)$	–
7103	11	13	7	7898	$(0,3)$	$(7856, 7944)$	–
7151	11	13	7	7644	$(0,0)$	$(7892, 7968)$	–

Table 4. Optimal parameters for WG-16

Decimation d	Hamming weight of d	Degree of $WG(x^d)$	AI of $WG(x^d)$	Nonlinearity of $WG(x^d)$	$(Resi_d,\ A_d)$ of $WG(x^d)$	(N_l, N_u) of $WGperm(x^d)$	k-uniform of $WGperm(x^d)$
WG-16							
1057	3	15	8	32160	$(0,1)$	$(32146, 32240)$	–
157	5	15	8	32192	$(1,0)$	$(32048, 32230)$	–
409	5	15	8	32224	$(0,0)$	$(32080, 32256)$	–
451	5	15	8	32176	$(0,0)$	$(32168, 32252)$	–
1187	5	15	8	32272	$(0,0)$	$(32150, 32236)$	–
2137	5	15	8	31960	$(0,0)$	$(32134, 32242)$	–
4681	5	15	8	32240	$(0,1)$	$(32084, 32254)$	–
469	6	15	8	32288	$(0,0)$	$(32098, 32244)$	–
1393	6	15	8	32048	$(0,0)$	$(32172, 32248)$	–
2251	6	15	8	31968	$(0,0)$	$(32112, 32248)$	–
2473	6	15	8	32252	$(0,0)$	$(32138, 32252)$	–
1327	7	15	8	32256	$(0,0)$	$(32142, 32252)$	–
1397	7	15	8	32128	$(0,0)$	$(32152, 32236)$	–
1933	7	15	8	32204	$(1,0)$	$(32128, 32242)$	–
2741	7	15	8	32096	$(0,4)$	$(32108, 32236)$	–
3223	7	15	8	32136	$(0,0)$	$(32144, 32256)$	–
4411	7	15	8	32248	$(0,0)$	$(32182, 32236)$	–
4789	7	15	8	32292	$(0,0)$	$(32130, 32246)$	–
5213	7	15	8	32290	$(0,0)$	$(32140, 32252)$	–
1771	8	15	8	32242	$(0,0)$	$(32040, 32250)$	–
3419	8	15	8	32328	$(1,0)$	$(32124, 32260)$	–
3449	8	15	8	32032	$(0,0)$	$(32124, 32264)$	–
10651	8	15	8	32208	$(0,0)$	$(32154, 32254)$	–
10667	8	15	8	32016	$(1,0)$	$(32152, 32252)$	–
6043	9	15	8	32276	$(2,0)$	$(32134, 32240)$	–
7771	9	15	8	32248	$(0,0)$	$(32126, 32242)$	–
3581	10	15	8	32188	$(0,0)$	$(32172, 32256)$	–
7673	10	15	8	31840	$(1,0)$	$(32114, 32260)$	–
13631	10	15	8	32232	$(0,0)$	$(32102, 32266)$	–
14327	12	15	8	32262	$(0,0)$	$(32170, 32244)$	–
32767	15	15	8	32310	$(0,0)$	$(32146, 32244)$	–