the out-of-phase autocorrelation is equal to -1, then the sequence is said to have *ideal two-level autocorrelation*.

- Linear span (LS): The linear span or linear complexity of a binary sequence is defined as the length of the smallest linear feedback shift register (LFSR) which generates the entire binary sequence.
- Nonlinearity: The nonlinearity of a function f is defined as the minimum distance from f to any affine function with the same number of variables.
- Algebraic immunity (AI): The algebraic immunity of a function f is defined as the minimum degree of an annihilator Boolean function g such that g is equivalent to either f or the complement of f (i.e., $fg = 0$ or $(f + 1)g = 0$). In the ideal case, the algebraic immunity of a function f is equal to the degree of f, thus making it immune to algebraic attacks.
- $\oplus$, the bitwise addition operator (i.e., XOR).
- $\otimes$, the multiplication operator over $\mathbb{F}_{2^8}$.

2.2. The Description of the Stream Cipher WG-8

WG-8 is a lightweight variant of the well-known Welch-Gong (WG) stream cipher family with 80-bit secret key and 80-bit initial vector (IV), which can be regarded as a nonlinear filter generator over finite field $\mathbb{F}_{2^8}$. The stream cipher WG-8 consists of a 20-stage LFSR with the feedback polynomial $l(x)$ followed by a WG-8 transformation module with decimation $d = 19$, and operates in two phases, namely an initialization phase and a running phase.

Initialization Phase. The key/IV initialization phase of the stream cipher WG-8 is shown in Figure 1.

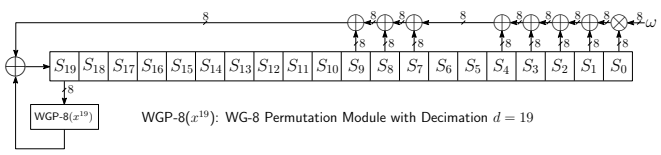

Figure 1. The Initialization Phase of the Stream Cipher WG-8

Let the 80-bit secret key be $K = (K_{79}, \ldots, K_0)_2$, the 80-bit IV be $IV = (IV_{79}, \ldots, IV_0)_2$, and the internal state of the LFSR be $S_0, \ldots, S_{19} \in \mathbb{F}_{2^8}$, where $S_i = (S_{i,7}, \ldots, S_{i,0})_2$ for $i = 0, \ldots, 19$. The key and IV initialization process is conducted as follows: $S_{2i} = (K_{8i+3}, \ldots, K_{8i}, IV_{8i+3}, \ldots, IV_{8i})_2$ and $S_{2i+1} = (K_{8i+7}, \ldots, K_{8i+4}, IV_{8i+7}, \ldots, IV_{8i+4})_2$ for $i = 0, \ldots, 9$.

Once the LFSR is loaded with the key and IV, the apparatus runs for 40 clock cycles. During each clock cycle, the 8-bit internal state S_{19} passes through the nonlinear WG-8 permutation with decimation $d = 19$ (i.e., the WGP-8(x^{19}) module) and the output is used as the feedback to update the internal state of the LFSR. The LFSR update follows the recursive relation:

$$S_{k+20} = (\omega \otimes S_k) \oplus S_{k+1} \oplus S_{k+2} \oplus S_{k+3} \oplus S_{k+4} \oplus S_{k+7} \oplus S_{k+8} \oplus S_{k+9} \oplus \text{WGP-8}(S^{19}_{k+19}), \quad 0 \le k < 40.$$

After the key/IV initialization phase, the stream cipher WG-8 goes into the running phase and 1-bit keystream is generated after each clock cycle.

Running Phase. The running phase of the stream cipher WG-8 is illustrated in Figure 2. During the running phase, the 8-bit internal state S_{19} passes through the nonlinear WG-8 transformation with decimation $d = 19$ (i.e., the WGT-8(x^{19}) module) and the output is the keystream. Note that the only feedback in the running phase is within the LFSR and the recursive relation for updating the LFSR is given below:

$$S_{k+20} = (\omega \otimes S_k) \oplus S_{k+1} \oplus S_{k+2} \oplus S_{k+3} \oplus S_{k+4} \oplus S_{k+7} \oplus S_{k+8} \oplus S_{k+9}, \quad k \ge 40.$$

The WG-8 transformation module WGT-8(x^{19}) comprises of two sub-modules: a WG-8 permutation module WGP-8(x^{19}) followed by a trace computation module $\text{Tr}(\cdot)$. While the WGP-8(x^{19}) module permutes elements over $\mathbb{F}_{2^8}$, the $\text{Tr}(\cdot)$ module compresses an 8-bit input to 1-bit keystream.

2.3. Randomness Properties of the WG-8 Keystream

The keystream generated by the stream cipher WG-8 has the following desired randomness properties [8]:

N) required for the attack to be successful is given by $N \approx (k \cdot 12 \cdot \ln 2)^{\frac{1}{3}} \cdot \epsilon^{-2} \cdot 2^{\frac{160-k}{3}}$ and the decoding complexity is given by $C_{dec} = 2^k \cdot k \cdot \frac{2 \ln 2}{(2\epsilon)^6}$, where $\epsilon = (\Pr(\text{WGT-8}(x^{19}) = f(x)) - 0.5) = 0.078125$ and k is the number of LFSR internal state bits recovered. If we choose a small value of k (e.g., $k = 7$), the number of bits required to launch the attack is about $2^{60.31}$, which is not possible in practice. Similarly, if we choose a large value of k (e.g., $k = 80$), the number of bits required to mount the attack is about $2^{37.15}$. However, the decoding complexity of the attack is approximately $2^{102.68}$, which is worse than the exhaustive search. Hence, the stream cipher WG-8 is secure against the fast correlation attack.

3.3. Differential Attack

The initialization phase in the first design of the WG stream cipher was vulnerable to the chosen IV attack [43], where an attacker can distinguish several output bits by building a distinguisher based on the differential cryptanalysis. This weakness has been fixed in the later design by placing the WG permutation module at the last position of the LFSR [31]. For the proposed stream cipher WG-8, the differential distribution of the WGP-8(x^{19}) is 8-uniform, which provides a maximum 2^{-5} possibility for differential characteristic. During the initialization phase the WGP-8(x^{19}) is applied for 40 times. Thus, after the initialization phase, it would be quite hard for an attacker to distinguish the output keystream since the differentials become complex and contain most key/IV bits.

3.4. Cube Attack

Cube attack [13] is a generic key-recovery attack that can be applied to any cryptosystem, provided that the attacker can obtain a bit of information that can be represented by a low-degree decomposition multivariate polynomial in Algebraic Normal Form (ANF) of the secret and public variables of the target cryptosystem. Note that the nonlinearity of WGP-8(x^{19}) is 92 and the algebraic degrees of the component functions of WGP-8(x^{19}) are 7. Moreover, the ANF representations of 8 component functions contain 133, 113, 146, 124, 137, 109, 122, and 120 terms, respectively, and only the ANF of the second component contains 7 linear terms and other terms are of degree greater than or equal to 2. In the WG-8 stream cipher, after 40 rounds of the initialization phase, the degree of the output polynomial can be very high. As a result, it would be hard for an attacker to collect low-degree relations among the secret key bits.

3.5. Distinguishing Attack

Recently, a distinguishing attack has been proposed against the stream cipher WG-7 [32]. Due to the small number of tap positions in the LFSR of the WG-7, the characteristic polynomial of the LFSR allows an attacker to build a distinguisher for distinguishing a keystream generated by WG-7 from a truly random keystream. For the WG-8 cipher, the characteristic polynomial of the LFSR consists of 8 tap positions and a similar distinguisher as in [32] can be built as

$$F(S_i, ..., S_{i+4}, S_{i+7}, ..., S_{i+9}) = \text{WGT-8}(\omega \otimes S_i \oplus S_{i+1} \oplus S_{i+2} \oplus S_{i+3} \oplus S_{i+4} \oplus S_{i+7} \oplus S_{i+8} \oplus S_{i+9}) \oplus \text{WGT-8}(S_i) \oplus \text{WGT-8}(S_{i+1}) \oplus \text{WGT-8}(S_{i+2}) \oplus \text{WGT-8}(S_{i+3}) \oplus \text{WGT-8}(S_{i+4}) \oplus \text{WGT-8}(S_{i+7}) \oplus \text{WGT-8}(S_{i+8}) \oplus \text{WGT-8}(S_{i+9}),$$

which is a Boolean function in 64 variables. For the distinguisher F, the probability $\Pr(F(x) = 0) = \frac{1}{2} \pm \epsilon$, where $x = (a_0, ..., a_7), a_i \in \mathbb{F}_{2^8}$. Note that the value of ϵ will be quite small due to a huge number of variables in the distinguisher, which requires an attacker to obtain more keystream bits for distinguishing the keystream. However, the computation of the exact value of ϵ is infeasible in this case because the number of possible values of x is 2^{64}. Hence the WG-8 stream cipher is resistant to the distinguishing attack. Note that this type of distinguishing attacks can also be extended to the case in which a distinguisher can be built using a linear relation of a remote term of the LFSR, say S_τ for not large τ, and the sequences addressed in a subset of tap positions of the LFSR, denoted by $I = \{i_1, \cdots, i_t\} \subset \{0, 1, \cdots, 19\}$. In other words, a distinguisher could be built using the linear relation $S_\tau = S_{i_1} + \cdots + S_{i_t}$. Since this property is controlled by the characteristic polynomial of the LFSR, it can be easily teared done by a proper selection of the characteristic polynomial of the LFSR. For our selection of the characteristic

permutation with decimation $d = 19$ by

$$\mathsf{WGP\text{-}8}(x^{19}) = q(x^{19} + 1) + 1$$

for all elements $x \in \mathbb{F}_{2^8}$. Hence, a 256-byte look-up table $T_{\mathsf{WGP\text{-}8}}$ can be generated to compute $\mathsf{WGP\text{-}8}(x^{19})$.

Coset Leader Based Look-up Table (CLT) Approach. This approach assumes that a normal basis is used to represent elements in $\mathbb{F}_{2^8}$ and uses the essential property of the WG-8 permutation with decimation d below:

$$\begin{aligned}\mathsf{WGP\text{-}8}\left((x^{2^i})^d\right) &= q\left((x^{2^i})^d + 1\right) + 1 \\ &= q\left((x^d)^{2^i} + 1\right) + 1 = \left(q(x^d + 1)\right)^{2^i} + 1 \\ &= \left(q(x^d + 1) + 1\right)^{2^i} = \left(\mathsf{WGP\text{-}8}(x^d)\right)^{2^i} \qquad (1)\end{aligned}$$

for $x \in \mathbb{F}_{2^8}$ and $i = 0, 1, \ldots, 7$. According to the Equation (1), if we know the WG-8 permutation $\mathsf{WGP\text{-}8}(x^d)$ for an element $x \in \mathbb{F}_{2^8}$, we can easily obtain the WG-8 permutation $\mathsf{WGP\text{-}8}((x^{2^i})^d)$ for the entire conset $\{x^2, x^{2^2}, \ldots, x^{2^7}\}$ of x by cyclically shifting $\mathsf{WGP\text{-}8}(x^d)$ to the right by i positions, provided that a normal basis is employed to represent finite field elements. The complete cosets and coset leaders of $\mathbb{F}_{2^8}$ (in hexadecimal notation) are shown in Table 1. We note that under the normal basis representation the elements in $\mathbb{F}_{2^8}$ have been grouped into 34 different cosets except for 0 and 1. Since $\mathsf{WGP\text{-}8}(0) = \mathsf{0x00}$ and $\mathsf{WGP\text{-}8}(1) = \mathsf{0xFF}$, we only need to generate a 34-byte look-up table $T_{\mathsf{Co\text{-}WGP\text{-}8}}$ for storing the WG-8 permutation results for each coset leader. Here we present the following Algorithm 1 that uses the table $T_{\mathsf{Co\text{-}WGP\text{-}8}}$ to compute $\mathsf{WGP\text{-}8}(x^d)$ for any $x \in \mathbb{F}_{2^8}$.

Tower Field Arithmetic (TFA) Based Approach. The software implementation of the $\mathsf{WGP\text{-}8}(x^{19})$ module involves the arithmetic (i.e., addition, multiplication, and exponentiation) over finite field $\mathbb{F}_{2^8}$. Although we can directly implement all the operations over $\mathbb{F}_{2^8}$, it is well known that using the isomorphic tower constructions of $\mathbb{F}_{2^8}$ might save the memory consumption. Therefore, we investigate the tower construction $\mathbb{F}_{(2^4)^2}$ in this work.

Tower Construction $\mathbb{F}_{(2^4)^2}$ and Its Arithmetic. To obtain the tower construction $\mathbb{F}_{(2^4)^2}$, we first construct $\mathbb{F}_{2^4}$ by using an irreducible polynomial $e(X)$ of degree 4 over $\mathbb{F}_2$, and then construct $\mathbb{F}_{(2^4)^2}$ by using a certain irreducible polynomial $f(X)$ of degree 2 over $\mathbb{F}_{2^4}$. In our tower construction, we use $e(X) = X^4 + X^3 + 1$ with its polynomial basis $\{1, \alpha, \alpha^2, \alpha^3\}$ for $\mathbb{F}_{2^4}$ and $f(X) = X^2 + X + \alpha$ with its normal basis $\{\beta, \beta^{16}\}$ for $\mathbb{F}_{(2^4)^2}$, where $\alpha = \omega^{119} \in \mathbb{F}_{2^4}$ and $\beta = \omega^7 \in \mathbb{F}_{(2^4)^2}$ are zeros of the polynomials $e(X)$ and $f(X)$, respectively.

Algorithm 1 Coset Leader Based Look-up Table Approach

Input: $x \in F_{2^8}$, a decimation d, a look-up table $T_{\mathsf{Co\text{-}WGP\text{-}8}}$
Output: $\mathsf{WGP\text{-}8}(x^d)$

1: **if** $x = \mathsf{0x00}$ or $x = \mathsf{0xFF}$ **then**
2: **return** x
3: **end if**
4: Find the coset leader x_c of x by cyclically shifting x to the right by i positions, where $0 \le i \le 7$ (i.e., x_c is the smallest odd integer in the coset containing x.)
5: Find the position j of x_c in the table $T_{\mathsf{Co\text{-}WGP\text{-}8}}$
6: $a \leftarrow T_{\mathsf{Co\text{-}WGP\text{-}8}}[j]$
7: **return** $a \lll i$

Arithmetic operations in $\mathbb{F}_{2^4}$. The arithmetic in $\mathbb{F}_{2^4}$ is conducted with the aid of a 4×4 exponentiation table T_{exp} and a 4×4 logarithm table T_{log}. While the table T_{exp} stores exponentiation $\alpha^i, i = 0, 1, \ldots, 14$, the table T_{log} keeps the exponent i for each $\alpha^i, i = 0, 1, \ldots, 14$. Let $A = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ and $B = b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3$ be two non-zero elements in $\mathbb{F}_{2^4}$, where $a_i, b_i \in \mathbb{F}_2, i = 0, 1, 2, 3$. We can perform the arithmetic in $\mathbb{F}_{2^4}$ as follows:

$$\begin{aligned}AB &= T_{exp}[(T_{log}[(a_0, a_1, a_2, a_3)] + \\ &\qquad T_{log}[(b_0, b_1, b_2, b_3)]) \bmod 15], \\ A^2 &= T_{exp}[(T_{log}[(a_0, a_1, a_2, a_3)] \ll 1) \bmod 15], \\ \alpha A &= T_{exp}[(T_{log}[(a_0, a_1, a_2, a_3)] + 1) \bmod 15].\end{aligned}$$

Arithmetic operations in $\mathbb{F}_{(2^4)^2}$. Let $A = a_0\beta + a_1\beta^{16}$ and $B = b_0\beta + b_1\beta^{16}$, where $a_0, a_1, b_0, b_1 \in \mathbb{F}_{2^4}$. A multiplication AB in $\mathbb{F}_{(2^4)^2}$ is computed as follows:

$$\begin{aligned}AB &= (a_0\beta + a_1\beta^{16})(b_0\beta + b_1\beta^{16}) \\ &= (c\alpha \oplus a_0b_0)\beta + (c\alpha \oplus a_1b_1)\beta^{16},\end{aligned}$$

Table 1. The Cosets and Coset Leaders of $\mathbb{F}_{2^8}$

Coset Leader	Coset							Coset Leader	Coset						
0x00	–	–	–	–	–	–	–	0x27	0x4E	0x9C	0x39	0x72	0xE4	0xC9	0x93
0x01	0x02	0x04	0x08	0x10	0x20	0x40	0x40	0x2B	0x56	0xAC	0x59	0xB2	0x65	0xCA	0x95
0x03	0x06	0x0C	0x18	0x30	0x60	0xC0	0x81	0x2D	0x5A	0xB4	0x69	0xD2	0xA5	0x4B	0x96
0x05	0x0A	0x14	0x28	0x50	0xA0	0x41	0x82	0x2F	0x5E	0xBC	0x79	0xF2	0xE5	0xCB	0x97
0x07	0x0E	0x1C	0x38	0x70	0xE0	0xC1	0x83	0x33	0x66	0xCC	0x99	–	–	–	–
0x09	0x12	0x24	0x48	0x90	0x21	0x42	0x84	0x35	0x6A	0xD4	0xA9	0x53	0xA6	0x4D	0x9A
0x0B	0x16	0x2C	0x58	0xB0	0x61	0xC2	0x85	0x37	0x6E	0xDC	0xB9	0x73	0xE6	0xCD	0x9B
0x0D	0x1A	0x34	0x68	0xD0	0xA1	0x43	0x86	0x3B	0x76	0xEC	0xD9	0xB3	0x67	0xCE	0x9D
0x0F	0x1E	0x3C	0x78	0xF0	0xE1	0xC3	0x87	0x3D	0x74	0xF4	0xE9	0xD3	0xA7	0x4F	0x9E
0x11	0x22	0x44	0x88	–	–	–	–	0x3F	0x7E	0xFC	0xF9	0xF3	0xE7	0xCF	0x9F
0x13	0x26	0x4C	0x98	0x31	0x62	0xC4	0x89	0x55	0xAA	–	–	–	–	–	–
0x15	0x2A	0x54	0xA8	0x51	0xA2	0x45	0x8A	0x57	0xAE	0x5D	0xBA	0x75	0xEA	0xD5	0xAB
0x17	0x2E	0x5C	0xB8	0x71	0xE2	0xC5	0x8B	0x5B	0xB6	0x6D	0xDA	0xB5	0x6B	0xD6	0xAD
0x19	0x23	0x64	0xC8	0x91	0x23	0x46	0x8C	0x5F	0xBE	0x7D	0xFA	0xF5	0xEB	0xD7	0xAF
0x1B	0x36	0x6C	0xD8	0xB1	0x63	0xC6	0x8D	0x6F	0xDE	0xBD	0x7B	0xF6	0xED	0xDB	0xB7
0x1D	0x3A	0x74	0xE8	0xD1	0xA3	0x47	0x8E	0x77	0xEE	0xDD	0xBB	–	–	–	–
0x1F	0x3E	0x7C	0xF8	0xF1	0xE3	0xC7	0x8F	0x7F	0xFE	0xFD	0xFB	0xF7	0xEF	0xDF	0xBF
0x25	0x4A	0x94	0x29	0x52	0xA4	0x49	0x92	0xFF	–	–	–	–	–	–	–

where $c = (a_0 \oplus a_1)(b_0 \oplus b_1)$. For a non-zero element $A \in \mathbb{F}_{(2^4)^2}$, the squaring of A is calculated as follows:

$$\begin{aligned} A^2 &= (a_0\beta + a_1\beta^{16})^2 \\ &= [(a_0 \oplus a_1)^2\alpha \oplus a_0^2]\beta + [(a_0 \oplus a_1)^2\alpha \oplus a_1^2]\beta^{16}. \end{aligned}$$

The Frobenius mapping of A with respect to $\mathbb{F}_{2^4}$, which is the 16^{th} power operation, is computed as follows:

$$A^{2^4} = (a_0\beta + a_1\beta^{16})^{16} = a_0\beta^{16} + a_1\beta^{256} = a_1\beta + a_0\beta^{16}.$$

Implementation of WGP-8(x^{19}) Module. For an element $x \in \mathbb{F}_{2^8}$, the WGP-8(x^{19}) can be computed as follows:

$$\begin{aligned} &\text{WGP-8}(x^{19}) = q(x^{19} + 1) + 1 \\ &= y + y^{2^3+1} + y^{2^6}(y^{2^3+1} + y^{2^3-1}) + y^{2^3(2^3-1)+1} + 1, \end{aligned}$$

where $y = x^{19} + 1 = x^{2^4} \cdot x^2 \cdot x + 1$. Note that for the tower construction $\mathbb{F}_{(2^4)^2}$, 1 can be denoted by the vector $(1, 0, 0, 0, 1, 0, 0, 0)$. Therefore, the addition with 1 under the TF representation is equivalent to XORing with a constant 0x88.

4.2. Implementation of the Trace Computation Module $\mathrm{Tr}(\cdot)$

Depending on the bases chosen, the trace of an element $x \in \mathbb{F}_{2^8}$ can be computed as shown in Table 2.

4.3. Implementation of the Multiplication by ω Module

The multiplication by ω module can be implemented using either finite field arithmetic or an 8×8 look-up table.

Multiplication by ω Using Finite Field Arithmetic. We consider the following three cases when the PB, NB, and TF are used to represent finite field elements, respectively. With the PB representation, the multiplication of an element $x \in \mathbb{F}_{2^8}$ by ω can be computed as follows:

$$\begin{aligned} x \cdot \omega &= x_0\omega + x_1\omega^2 + \cdots + x_6\omega^7 + x_7\omega^8 \\ &= x_7 + x_0\omega + (x_1 \oplus x_7)\omega^2 + (x_2 \oplus x_7)\omega^3 + \\ &\quad (x_3 \oplus x_7)\omega^4 + x_4\omega^5 + x_5\omega^6 + x_6\omega^7. \end{aligned} \tag{2}$$

Therefore, the result of $x \cdot \omega$ is represented as an 8-bit vector $(x_7, x_0, x_1 \oplus x_7, x_2 \oplus x_7, x_3 \oplus x_7, x_4, x_5, x_6)$ with respect the PB.

Table 2. Trace Computation of an Element $x \in \mathbb{F}_{2^8}$ Using Different Bases

Basis	Element Representation	Tr(x)
Polynomial Basis (PB)	$x_0 + x_1\omega + \cdots + x_7\omega^7$	x_5
Normal Basis (NB)	$x_0\theta + x_1\theta^2 + \cdots + x_7\theta^{2^7}$	$\bigoplus_{i=0}^{7} x_i$
Tower Field (TF)	$(x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3)\beta +$ $(x_4 + x_5\alpha + x_6\alpha^2 + x_7\alpha^3)\beta^{16}$	$x_1 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_7$

With the NB representation, the multiplication of an element $x \in \mathbb{F}_{2^8}$ by ω can be calculated as follows:

$$\begin{aligned} x \cdot \omega &= (x_0\theta + x_1\theta^2 + \cdots + x_6\theta^{2^6} + x_7\theta^{2^7}) \cdot \omega \\ &= \mathbf{M} \cdot (x_0, x_1, \cdots, x_6, x_7)^T, \end{aligned} \tag{3}$$

where the matrix $\mathbf{M}$ is given below:

$$\mathbf{M} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

With the TF representation, the multiplication of an element $x \in \mathbb{F}_{2^8}$ by ω can be calculated as follows:

$$\begin{aligned} x \cdot \omega &= [(x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3)\beta + \\ &\quad (x_4 + x_5\alpha + x_6\alpha^2 + x_7\alpha^3)\beta^{16}] \cdot \omega \\ &= \mathbf{M}' \cdot (x_0, x_1, \cdots, x_6, x_7)^T, \end{aligned} \tag{4}$$

where the matrix $\mathbf{M}'$ is given below:

$$\mathbf{M}' = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Multiplication by ω Using Look-Up Tables. Based on the Equations (2)–(4), one can generate 256-byte look-up tables with respect to the chosen bases.

4.4. Implementation Platforms and Development Tools

In this section, we briefly describe two low-power microcontrollers for implementing the WG-8 stream cipher as well as the corresponding development tools.

8-Bit Microcontroller ATmega128L and Development Tool. The low-power 8-bit microcontroller ATmega128L [1] from Atmel is based on the AVR enhanced RISC architecture with 128 Kbytes of In-System Self-Programmable Flash, 4 Kbytes EEPROM and 8 Kbytes Internal SRAM. It is equipped with 133 highly-optimized instructions and most of them can be executed within one clock cycle. Moreover, the clock frequency of the ATmega128L can run from 0 to 8 MHz and the power supplies can go from 2.7 to 5.5 V. We use the latest integrated development environment Atmel Studio 6.0 [2] from Atmel for implementing and testing the performance of the WG-8 on the target platform.

16-Bit Microcontroller MSP430F1611 and Development Tool. The 16-bit microcontroller MSP430F1611 [40] from Texas Instruments has a traditional von-Neumann architecture with 48 Kbytes Flash memory and 10 Kbytes RAM. All special function registers, peripherals, RAM and Flash/ROM share the same address space. The clock frequency of the MSP430F1611 ranges from 0 to 8 MHz and the power supplies can go from 1.8 to 3.6 V. The MSP430F1611 features 27 instructions and 7 different addressing modes that provide great flexibility in data manipulation. To implement and simulate the WG-8 on the target platform, we use the CrossWorks for MSP430 Version 2.1 from Rowley Associates [37].

4.5. Experimental Results and Comparisons

In this section, we report our experimental results for implementing the stream cipher WG-8 on the low-power microcontrollers ATmega128L and MSP430F1611 and compare our results with other lightweight-cryptography implementations on the same or similar platforms. We focus on three major performance criteria for implementing cryptographic primitives on resource-constrained environments, namely throughput, code size, and energy consumption (i.e., energy/bit). Table 3 compares our implementation results with previous work in terms of the aforementioned three performance criteria. Note that we estimate the per bit energy consumptions by the formula: $\text{energy/bit} = \frac{\text{Supply Voltage} \times \text{Current} \times \text{Cycles}}{\text{Clock Frequency} \times \text{Number of Bits}}$, which is based on the typical current consumption of a low-power microcontroller for the given clock frequency and supply voltage.

From Table 3, we note that on 8-bit ATmega microcontrollers the throughput of WG-8 is about $2 \sim 15$ times higher than that of stream ciphers Grain, Trivium, Salsa20, and WG-7, block ciphers PRESENT-80 and XTEA as well as the hybrid cipher Hummingbird, whereas the energy consumption of WG-8 is around $2 \sim 220$ times smaller than that of those ciphers. Moreover, WG-8 has the comparable throughput and energy efficiency with the hybrid cipher Hummingbird-2 (optimized with assembly language). On the 8-bit platform, WG-8 is less efficient than AES in terms of throughput and energy consumption. The main reason is that WG-8 is a bit-oriented stream cipher whereas AES is a block cipher with block size 128-bit. Furthermore, the code size of WG-8 is medium and the SRAM usage of WG-8 is small among all the lightweight implementations.

On 16-bit MSP430 microcontrollers, the throughput of WG-8 is about $1 \sim 20$ times higher than that of the stream cipher WG-7 as well as block ciphers PRINTcipher-48, AES, PRESENT-80, and KLEIN-64, whereas the energy efficiency is comparable with that of those ciphers. While WG-8 has similar throughput and energy efficiency as the hybrid cipher Hummingbird, it is less efficient when compared to the Hummingbird-2 cipher. The main reason comes from the optimization with the assembly language in the speed-optimized Hummingbird-2 implementation. Furthermore, the code size of WG-8 is about $2 \sim 7$ times smaller than block ciphers PRINTcipher-48, AES, PRESENT-80, and KLEIN-64 as well as the hybrid cipher Hummingbird-2, and is comparable with the Hummingbird cipher. Regarding to the SRAM usage, the stream cipher WG-8 is superior to other block cipher and stream ciphers.

In addition, for the three implementation variants, we note that on both 8-bit and 16-bit platforms the DLT method is consistently better than both CLT and TFA methods with respect to throughput and energy consumption. The reason lies in the efficient memory access for look-up tables on both microcontrollers.

5. Efficient Hardware Implementation of the Stream Cipher WG-8

Efficient hardware implementation of the WG-8 stream cipher on both FPGA and ASIC platforms has been extensively investigated in [42]. One look-up table based and three tower field based hardware architectures were proposed and compared to each other in terms of throughput, area, and power consumption. The experimental results show that a direct look-up table based hardware architecture can achieve a maximum throughput of 190 Mbps (resp. 500 Mbps) and require 137 slices (resp. 1786 Gate Equivalents (GEs)) on a Xilinx Spartan-3 FPGA (resp. 65nm CMOS ASIC) platform, at the cost of the dynamic power consumption of 0.005 W (resp. 0.983 mW). Moreover, the look-up table based method is optimal with respect to the defined performance metrics when compared to the tower field based approaches. For certain performance metrics, the WG-8 hardware core compares well with the lightweight stream ciphers Grain [22], Trivium [7], and MICKEY [3].

6. Conclusion

In this paper, we present a lightweight stream cipher WG-8 targeted for resource-constrained devices like RFID tags, smart cards, and wireless sensor nodes, which inherits all the good randomness and cryptographic properties of the well-known WG stream cipher family. A detailed cryptanalysis shows that WG-8 is resistant to the most common attacks against stream ciphers. Moreover, the software implementations on low-power microcontrollers demonstrate the high performance and

Table 3. Performance Comparison of Lightweight-Cryptography Implementations on Low-Power Microcontrollers

Low-Power Microcontroller	Cryptographic Primitive	Clock Freq. [MHz]	Opt. Goal/ Method	Memory Usage [byte]		Setup [cycle]	Throughput [Kbits/sec]	Energy/Bit [nJ]
				Flash	SRAM			
ATmega	AES [33]	8 MHz	RAM	1,912	176	789	475.6	179
			Speed	1,912	256	747	513.8	165
	PRESENT-80 [35]		Size	1,474	32	–	0.99	85,819
			Speed	2,398	528	–	66.7	1,274
	Hummingbird [16]		Size	1,308	–	14,735	34.9	2,433
			Speed	10,918	–	8,182	91.5	929
	Hummingbird-2 [17]		RAM	3,600	114	2,970	171.8	495
			Speed	3,200	1,500	1,800	258.6	329
	XTEA [34]		Speed	820	–	–	51.7	1,645
	Grain[34]		Speed	778	20	107,336	12.9	6,556
	Trivium[34]		Speed	424	36	775,726	12.0	7,066
	Salsa20[29]		Speed	3,842	258	318	83.7	101,564
	WG-7[27]		Size	938	–	20,917	34.0	2,497
	WG-8		TFA	2,450	20	99,702	3.58	23,739
			CLT	2,238	148	10,683	31.7	2,683
			DLT	**1,984**	**20**	**1,379**	**185.5**	**458**
MSP430	PRINTcipher-48 [19]	8 MHz	Speed	6,424	48	–	4.5	153
	AES [19]		Speed	10,898	218	–	78.0	154
	PRESENT-80 [19]		Speed	6,424	288	–	19.4	619
	KLEIN-64 [19]		Speed	6,424	288	–	65.0	185
	Hummingbird [16]		Size	1,064	–	9,667	53.0	226
			Speed	1,360	–	4,824	104.9	114
	Hummingbird-2 [17]		Size	770	50	5,984	84.2	143
			Speed	3,648	114	1,361	356.5	34
	WG-7[27]		Size	1,050	–	18,379	21.0	572
	WG-8		TFA	2,110	20	127,944	2.44	4,926
			CLT	2,628	148	15,265	10.8	1,107
			DLT	**1,558**	**20**	**3,604**	**95.9**	**125**

low energy consumption of the WG-8 stream cipher, when compared to most of previous block ciphers and stream ciphers. Therefore, the stream cipher WG-8 is a competitive candidate for securing a wide range of smart devices and embedded applications.

Ackowledgement

The authors would like to thank the reviewers for their helpful and constructive comments that greatly improve the final version of this paper. This work is supported by NSERC Discovery and ORF-RE grants.

References

[1] Atmel Corporation (2011) ATmega128(L): 8-bit Atmel Microcontroller with 128 KBytes In-System Programmable Flash, Available at http://www.atmel.com/Images/doc2467.pdf.

[2] Atmel Corporation (2012) Atmel Studio 6 – The Integrated Development Environment, Available at http://www.atmel.com/microsite/atmel_studio6/.

[3] Babbage S. and Dodd M. (2006) The Stream Cipher MICKEY 2.0, ECRYPT Stream Cipher, Available at http://www.ecrypt.eu.org/stream/p3ciphers/mickey/mickey_p3.pdf.

[4] Biryukov A. and Shamir A. (2000) Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers,

Advances in Cryptology - ASIACRYPT 2000, LNCS 1976, T. Okamoto (Ed.), Berlin, Germany: Springer-Verlag, pp. 1-13.

[5] Bogdanov A. and Knudsen L. R. and Leander G. and Paar C. and Poschmann A. and Robshaw M. J. B. and Seurin Y. and Vikkelsoe C. (2007) PRESENT: An Ultra-Lightweight Block Cipher, *The 9th International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2007*, LNCS 4727, P. Paillier and I. Verbauwhede (eds.), Berlin, Germany: Springer-Verlag, pp. 450-466.

[6] De Cannière C. and Dunkelman O. and Knežević M. (2009) KATAN and KTANTAN – A Family of Small and Efficient Hardware-Oriented Block Ciphers, *The 11th International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2009*, LNCS 5747, C. Clavier and K. Gaj (eds.), Berlin, Germany: Springer-Verlag, pp. 272-288.

[7] De Cannière C. and Preneel B. (2005) Trivium – A Stream Cipher Construction Inspired by Block Cipher Design Principles, ECRYPT Stream Cipher, Available at http://www.ecrypt.eu.org/stream/papersdir/2006/021.pdf.

[8] Chen L. and Gong G. (2012) *Communication System Security*, Boca Raton, Florida, USA: Chapman & Hall/CRC.

[9] Chepyzhov V.V. and Johansson T. and Smeets B.J.M. (2000) A Simple Algorithm for Fast Correlation Attacks on Stream Ciphers, *The 7th International Workshop on Fast Software Encryption - FSE 2000*, LNCS 1978, B. Schneier (Ed.), Berlin, Germany: Springer-Verlag, pp. 181-195.

[10] Courtois N. (2003) Fast Algebraic Attacks on Stream Ciphers with Linear Feedback, *Advances in Cryptology - CRYPTO 2003*, LNCS 2729, D. Boneh (Ed.), Berlin, Germany: Springer-Verlag, pp. 176-194.

[11] Courtois N. and Meier W. (2003) Algebraic Attacks on Stream Ciphers with Linear Feedback, *Advances in Cryptology - EUROCRYPT 2003*, LNCS 2656, E. Biham (Ed.), Berlin, Germany: Springer-Verlag, pp. 345-359.

[12] Ding L. and Jin C. and Guan, J. and Wang Q. (2014) Cryptanalysis of Lightweight WG-8 Stream Cipher, *IEEE Transactions on Information Forensics and Security*, vol.9, no.4, pp. 645 – 652.

[13] Dinur I. and Shamir A. (2009) Cube Attacks on Tweakable Black Box Polynomials, *Advances in Cryptology - EUROCRYPT'09*, LNCS 5479, A. Joux (Ed.), Berlin, Germany: Springer-Verlag, pp. 278-299.

[14] Driessen B. and Hund R. and Willems C. and Paar C. and Holz T. (2012) Don't Trust Satellite Phones: A Security Analysis of Two Satphone Standards, *The 33th IEEE Symposium on Security and Privacy - S&P 2012*, pp. 128-142.

[15] Eisenbarth T. and Kumar S. and Paar C. and Poschmann A. and Uhsadel L. (2007) A Survey of Lightweight-Cryptography Implementations, *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 522-533.

[16] Engels D. and Fan X. and Gong G. and Hu H. and Smith E.M. (2010) Hummingbird: Ultra-Lightweight Cryptography for Resource- Constrained Devices, *FC 2010 Workshops, RLCPS, WECSR, and WLC 2010*, LNCS 6054, R. Sion et al. (Eds.), Berlin, Germany: Springer-Verlag, pp. 3-18.

[17] Engels D. and Saarinen M.-J. O. and Schweitzer P. and Smith E.M. (2011) The Hummingbird-2 Lightweight Authenticated Encryption Algorithm, *The 7th International Workshop on RFID Security and Privacy - RFIDSec 2011*, LNCS 7055, A. Juels and C. Paar (Eds.), Berlin, Germany: Springer-Verlag, pp. 19-31.

[18] Feldhofer M. and Wolkerstorfer J. and Rijmen V. (2005) AES Implementation on a Grain of Sand, *IEE Proceedings Information Security*, vol. 15, no. 1, pp. 13-20.

[19] Gong Z. and Nikova S. and Law Y. (2012) KLEIN: A New Family of Lightweight Block Ciphers, *The 7th International Workshop on RFID Security and Privacy - RFIDSec 2011*, LNCS 7055, A. Juels and C. Paar (Eds.), Berlin, Germany: Springer-Verlag, pp. 1-18.

[20] Gong G. and Rønjom S. and Helleseth T. and Hu H. (2011) Fast Discrete Fourier Spectra Attacks on Stream Ciphers, *IEEE Transactions on Information Theory*, vol. 57, No. 8, pp. 5555-5565.

[21] Guo J. and Peyrin T. and Poschmann A. and Robshaw M.J.B. (2011) The LED Block Cipher, *The 13th International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2011*, LNCS 6917, B. Preneel and T. Takagi (eds.), Berlin, Germany: Springer-Verlag, pp. 326-341.

[22] Hell M. and Johansson T. and Meier W. (2007) Grain: A Stream Cipher for Constrained Environments, *International Journal of Wireless and Mobile Computing*, vol. 2, no. 1, pp. 86-93.

[23] Kaps J.-P. (2008) Chai-Tea, Cryptographic Hardware Implemenations of xTEA, *The 9th International Conference on Cryptology in India - INDOCRYPT 2008*, LNCS 5356, D. R. Chowdhury, V. Rijmen, and A. Das

(eds.), Berlin, Germany: Springer-Verlag, pp. 363-375.

[24] Knudsen L. and Leander G. and Poschmann A. and Robshaw M. J. B. (2010) PRINTcipher: A Block Cipher for IC-Printing, *The 12th International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2010*, LNCS 6225, S. Mangard and F.-X. Standaert (eds.), Berlin, Germany: Springer-Verlag, pp. 16-32.

[25] Leander G. and Paar C. and Poschmann A. and Schramm K. (2007) New Lightweight DES Variants, *The 14th Annual Fast Software Encryption Workshop - FSE 2007*, LNCS 4593, A. Biryukov (ed.), Berlin, Germany: Springer-Verlag, pp. 196-210.

[26] Liu D. and Yang Y. and Wang J. and Min H. (2009) A Mutual Authentication Protocol for RFID Using IDEA, *Auto-ID Labs White Paper*, WP-HARDWARE-048, available at http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-HARDWARE-048.pdf.

[27] Luo Y. and Chai Q. and Gong G. and Lai X. (2010) WG-7: A Lightweight Stream Cipher with Good Cryptographic Properties, *IEEE Global Communications Conference – GLOBECOM 2010*, pp. 1-6.

[28] Meier W. and Staffelbach O. (1989) Fast Correlation Attacks on Certain Stream Ciphers, *Journal of Cryptology*, vol. 1, No. 3, pp. 159-176.

[29] Meiser G. and Eisenbarth T. and Lemke-Rust K. and Paar C. (2008) Efficient Implementation of eSTREAM Ciphers on 8-bit AVR Microcontrollers, *International Symposium on Industrial Embedded Systems – SIES 2008*, pp. 58-66.

[30] Mihaljević M.J. and Gangopadhyay S. and Paul G. and Imai H. (2012) Internal State Recovery of Grain-v1 Employing Normality Order of the Filter Function, *IET Information Security*, vol.6, No.2, pp.55 – 64.

[31] Nawaz Y. and Gong G. (2008) WG: A Family of Stream Ciphers with Designed Randomness Properties, *Information Science*, vol. 178, no. 7, pp. 1903-1916.

[32] Orumiehchiha M.A. and Pieprzyk J. and Steinfeld R. (2012) Cryptanalysis of WG-7: A Lightweight Stream Cipher, *Cryptography and Communications*, vol. 4, Iss. 3-4, pp. 277-285.

[33] Osvik D. A. and Bos J. W. and Stefan D. and Canright D. (2010) Fast Software AES Encryption, *The 17th International Workshop on Fast Software Encryption - FSE 2010*, LNCS 6147, S. Hong and T. Iwata (eds.), Berlin, Germany: Springer-Verlag, pp. 75-93.

[34] Otte D. (2012) AVR-Crypto-Lib, Available at http://www.das-labor.org/wiki/AVR-Crypto-Lib/en.

[35] Poschmann A. (2009) *Lightweight Cryptography – Cryptographic Engineering for a Pervasive World*, Ph.D. Thesis, Department of Electrical Engineering and Information Science, Ruhr-Universitäet Bochum, Bochum, Germany.

[36] Rønjom S. and Helleseth T. (2007) A New Attack on the Filtering Generator, *IEEE Transactions on Information Theory*, vol 53, No. 5, pp. 1752-1758.

[37] Rowley Associates, (2012) CrossWorks for MSP430, Available at http://www.rowley.co.uk/msp430/.

[38] Shibutani K. and Isobe T. and Hiwatari H. and Mitsuda A. and Akishita T. and Shirai T. (2011) Piccolo: An Ultra-Lightweight Blockcipher, *The 13th International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2011*, LNCS 6917, B. Preneel and T. Takagi (eds.), Berlin, Germany: Springer-Verlag, pp. 342-357.

[39] Siegenthaler T. (1985) Decrypting a Class of Stream Ciphers Using Ciphertext Only, *IEEE Transactions on Computers*, vol. 34, No. 1, pp. 81-85.

[40] Texas Instuments Inc., MSP430F15x, MSP430F16x, MSP430F161x Mixed Signal Microcontroller, Available at http://www.ti.com/lit/ds/symlink/msp430f1611.pdf, 2011.

[41] Verdult R. and Garcia F. D. and Balasch J. (2012) Gone in 360 Seconds: Hijacking with Hitag2, *The 21st USENIX Security Symposium - USENIX Security 2012*, USENIX Association, pp. 237-252.

[42] Yang G. and Fan X. and Aagaard M. and Gong G. (2013) Design Space Exploration of the Lightweight Stream Cipher WG-8 for FPGAs and ASICs, *The 8th Workshop on Embedded Systems Security (WESS'13)*, ACM Press, Article No. 8, 2013.

[43] Wu H. and Preneel B. (2005) Chosen IV Attack on Stream Cipher WG, *ECRYPT Stream Cipher Project Report 2005/045*. Available at http://cr.yp.to/streamciphers/wg/045.pdf.