UDC 004.056.55:512.6+519.24

On the Security of Qalqan Cipher Against Differential Cryptanalysis

Serhii Yakovliev[1, a], Mykhailo Stolovych[1, b]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Institute of Physics and Technology*

Abstract

In 2021, the first version of block cipher Qalqan was presented. It is positioned as a candidate to the future national encryption standard of the Republic of Kazakhstan. This cipher features the usage of addition by different modules for mixing the round keys and for linear layer. In this work, we consider some cryptographic properties of Qalqan, related with the security against differential and linear cryptanalysis. We present variations of cipher's S-box with better cryptographic properties. We prove that branch number of Qalqan's linear layer is equal to 3, and the layer itself has a significant amount of fixed points. Also, we build a set of multi-round differential characteristics with high probabilities for the modified version of the Qalqan cipher, which uses only addition modulo 256. With these results, we can argue that the declared security of Qalqan against differential and linear cryptanalysis should be reconsidered.

Keywords: Qalqan cipher, branch number, differential cryptanalisys

Introduction

A block cipher Qalqan was presented in 2021 [1]; it is positioned as a candidate to become the future national encryption standard of the Republic of Kazakhstan. There are few published results of its cryptographic analysis; some security estimations were presented in reports [1, 2]. However, the methodology of security analysis was not presented alongside, making it impossible to perform independent external verification. Also, cryptographic properties of Qalqan cipher S-box were studied in [3]. They are quite sufficient for use in modern block ciphers.

This paper considers the cryptographic properties of structural elements of the Qalqan cipher. We present simple variations of Qalqan's S-box, which are potentially increase the security against differential cryptanalysis and algebraic attacks. We calculate branch number of linear layer and show that linear layer does not fulfill the *wide trail strategy* [4]. This may correspond to cipher vulnerabilities to differential and linear cryptanalysis. Consequently, we find large classes of fixed points for Qalqan's linear layer, which eases the construction of appropriate differential and linear attacks. To illustrate our claims, we find the multi-round differential characteristics with high probabilities for modified Qalqan cipher.

We strongly believe that Qalqan cipher will be improved further. Therefore, in our work, we will refer to the version of Qalqan cipher, presented in [1], as the first version of this cipher and denote it as Qalqan^{v1}.

1. Preliminaries

Let $V_n = \{0,1\}^n$ be the space of all binary vectors with bit-wise addition $\oplus$. The elements from the V_n are naturally correspond to non-negative integers from the set $\mathbb{Z}_{2^n} = \{0, 1, \ldots, 2^n - 1\}$: each vector is treated as a binary form of an integer number. With introduced notation for the set V_n, we will consider operation $+$ as addition modulo 2^n of two binary vectors in the form of integer numbers.

We name elements from the space V_8 (or, correspondingly, $\mathbb{Z}_{256}$) as *bytes* and elements from the space V_{128} as *blocks*. Each block $x \in V_{128}$ can be naturally represented as an array of bytes $x = (x_0, x_1, \ldots, x_{15})$, $x_i \in V_8$. For the modulo addition operation Little Endian format is used:

$$x + y = (x_0 + y_0, x_1 + y_1 + \nu_1, \ldots, x_{15} + y_{15} + \nu_{15}),$$

where $\nu_i = \nu_i(x_0, y_0, \ldots, x_{i-1}, y_{i-1})$ are carry bits from lower digits. Furthermore, for such representation, we consider byte-wise addition $\boxplus$ of vectors:

$$x \boxplus y = (x_0 + y_0, x_1 + y_1, \ldots, x_{15} + y_{15}).$$

[a] yasv@rl.kiev.ua

[b] stolovich@yahoo.com

Each block $x \in V_{128}$ can be represented as byte 4×4-matrix:

$$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix} \to \begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix}.$$

Let $\mathcal{M}$ be a set of all 4×4-matrix over V_8. A *weight* $wt(M)$ of matrix $M \in \mathcal{M}$ is a number of non-zero matrix cells (similarly to the weight of a vector). Then *branch number* of nonsingular linear transformation $L \colon \mathcal{M} \to \mathcal{M}$ is a value

$$B(L) = \min_{M \in \mathcal{M}, M \neq O} \{wt(M) + wt(L(M))\},$$

where O is a zero matrix.

Branch number has a significant value for resistance evaluation of SP-networks to the differential and linear cryptanalysis. In correspondence to "*wide trail strategy*", presented by J. Daemen and V. Rijmen [4], branch number must be maximized for the sake of security against the mentioned methods of cryptanalysis.

Let us remind the basic definitions of differential cryptanalysis [5, 6, 7]. For function $f \colon V_n \to V_n$ a *differential* is a pair of two arbitrary vectors $(\alpha, \beta) \in V_n^2$, which are considered as differences between an input and corresponding output of function f. In general case, differences can be calculated with respect to distinct operations. *A probability of differential* (α, β) of function f w.r.t. operations $\circ$ and $\bullet$ is a value

$$DP^f_{\circ,\bullet}(\alpha, \beta) = \frac{1}{2^n} \sum_{x \in V_n} [f(x \circ \alpha) = f(x) \bullet \beta],$$

where $[A]$ is an indicator of event A (Iverson's brackets). In our work, we mostly consider probabilities $DP^f_{\oplus,\boxplus}$ and $DP^f_{\boxplus,\boxplus}$.

Let $F_k \colon V_n \times \mathcal{K} \to V_n$ be an encryption mapping with key parameter $k \in \mathcal{K}$. Differential probability is defined for each input $x \in V_n$ independently:

$$DP^{F_k}_{\circ,\bullet}(x; \alpha, \beta) = \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} [F_k(x \circ \alpha) = F_k(x) \bullet \beta].$$

The encryption mapping is called *Markov mapping* with respect to a pair of operations $(\circ, \bullet)$, if the probability for all its differentials is independent of the input point [6, 7]:

$$\forall x \forall \alpha \forall \beta \colon DP^{F_k}_{\circ,\bullet}(x; \alpha, \beta) = DP^{F_k}_{\circ,\bullet}(0; \alpha, \beta).$$

Further, for the sake of simplicity, we omit the notation of the input point for differential probabilities of Markov mappings.

Let $E(x) = F^{(r)}_{k_r}(F^{(r-1)}_{k_{r-1}}(\ldots F^{(1)}_{k_1}(x)\ldots))$ — r-round iterative cipher with round functions $F^{(i)}$ and independent random round keys k_i. *Differential characteristic* of cipher E is an arbitrary sequence of non-zero binary vectors $\Omega = (\omega_0, \ldots, \omega_r)$, which represent the differences between input values and intermediate ciphertexts after each round of encryption. If cipher E is Markov with respect to some sequence of operations, then probability DCP of differential characteristics Ω is equal to [8]

$$DCP^E(\Omega) = \prod_{i=1}^{r} DP^{F^{(i)}}(\omega_{i-1}, \omega_i).$$

The sequence of operations for difference evaluation is considered to be known in advance.

2. Qalqan^{v1} Cipher and Its Modifications

The block cipher Qalqan [1] has an SP-network-based structure with a block size of 128 bits. The cipher key length is 256-1024 bits, with 17-23 encryption rounds. The number of rounds depends on the key length. Cipher has a byte-oriented structure: all operations, but adding round keys, are done over bytes (8-bit sequences) or sets of bytes.

Input texts and encryption states are represented as 128-bit vectors, arrays of 16 bytes, and byte matrix 4×4 at the same time, depending on applied transformation.

One encryption round $F_k(x) = L(S(K^\circ_k(x)))$ consists of three sequential layers:

1) round key addition K°_k with operation $\circ$;

2) non-linear substitution S;

3) linear transformation L, which consists of a series of state byte additions (details further).

At the end of encryption, extra whitening is applied with a separate round key.

Addition with the round key on the first round and at the end of the encryption is performed with the bit-wise operation ($K^\oplus_k(x) = x \oplus k$). All other rounds use addition modulo 2^{128} ($K^+_k(x) = (x + k) \bmod 2^{128}$) and encryption state is represented as 128-bit non-negative integer in Little-Endian format. In our work, we denote these functions as $F^\oplus_k$ and F^+_k for round functions. They use $K^\oplus_k$ and K^+_k keys respectively.

Non-linear substitution S is applied to all bytes in state matrix with fixed S-Box s: $a_{i,j} = s[a_{i,j}]$. Qalqan^{v1} S-Box is claimed to be constructed using Nyberg scheme [9], similarly to AES S-Box; however, its algebraic form had not be published.

Linear layer L of Qalqan^{v1} cipher is based on byte addition (modulo 2^8) and consists of two phases:

a) on the first phase («absorption») diagonal elements from the matrix are added with all elements

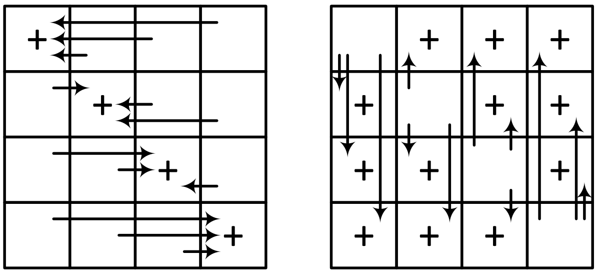

Fig. 1. General scheme of the linear layer L: on the left — absorption phase, on the right — distribution phase.

from the corresponding row:

$\forall i \in \{0,1,2,3\}\colon a_{i,i} = a_{i,0} + a_{i,1} + a_{i,2} + a_{i,3}$;

b) on the second phase («distribution») updated diagonal matrix elements are added to all elements of corresponding columns:

$$\forall j, i \in \{0,1,2,3\}, i \neq j\colon a_{i,j} = a_{i,j} + a_{j,j}.$$

The scheme of the linear layer L is presented in fig. 1.

It's worth mentioning that the linear layer of Qalqan^{v1} cipher has no analogs among other linear mappings used in known block ciphers.

A detailed description of the Qalqan^{v1} cipher, its components and key schedule are presented in [1, 2].

Further in our work, alongside with original cipher, we consider its modification, where byte-wise vector addition $\boxplus$ modulo 2^8 is used. The first modification has all its round key additions K_k^+ modulo 2^{128} substituted with additions $K_k^{\boxplus}(x) = x \boxplus k$. The modified round function we denote as $F_k^{\boxplus}$. The essence of this modification is a removal of carry bits between state bytes. This modification transforms cipher into Markov cipher w.r.t. the sequence of operations $(\oplus, \boxplus, \boxplus, \ldots, \boxplus, \oplus)$. The second modification uses byte-wise addition for first and last addition with key as well. This modification transforms the cipher into Markov cipher w.r.t. $\boxplus$ operation and can be considered as a cipher model without first round and final whitening. We denote these modifications as Qalqan$^{v1}_{\oplus\boxplus}$ and Qalqan$^{v1}_{\boxplus\boxplus}$ respectively.

3. Improvements for the Qalqan^{v1} cipher S-Box

It is claimed that the S-box of Qalqan^{v1} cipher is constructed based on the Nyberg scheme [9], but its algerbaic structure remains hidden. Detailed analysis of cryptographic properties if this S-Box can be found in [3]. Qalqan^{v1} S-Box has good values of parameters that indicate the security against known cryptanalytic attacks. Here are the main cryptographic properties (both mentioned in [3] and some extra):

1) balanced, compliance with strict avalanche criteria;

2) algebraic degree: 7;

3) $MDP_{\oplus,\oplus}(s) = 4/256 = 2^{-6}$;

4) $MDP_{+,+}(s) = 8/256 = 2^{-6}$;

5) $MDP_{\oplus,+}(s) = 6/256 = 2^{-5.415}$;

6) non-linearity: 112, maximum linear potential value: 2^{-6};

7) fixed point number: 0;

8) the number of cycles of length two: 1.

It is worth mentioning that the Nyberg scheme provides solid cryptographic properties for cipher if its algebraic structure (key addition and linear layer) constructed with respect to bit-wise addition. However, in Qalqan^{v1} cipher, the linear layer uses byte-wise addition, and the key adder uses both bit-wise addition and addition modulo 2^{128}. In our opinion, it would be more appropriate to focus on cryptographic parameters related to modular addition during choosing process of the S-box.

We considered all S-boxes of the form

$$s_{u,v}(x) = s(x \oplus u) \oplus v$$

for $u, v \in V_8$ and evaluated their cryptographic properties. Such affine transformation changes the cycle structure of permutation, but does not change imbalance, algebraic degree, non-linearity, maximum linear potential value, and $MDP_{\oplus,\oplus}$. Therefore, most of the cryptographic properties of S-boxes $s_{u,v}$ for all u, v have the same quality as the original Qalqan^{v1} S-box. However, we found 24 S-boxes with better cryptographic parameters:

1) $MDP_{+,+}(s) = 6/256 = 2^{-5.415}$;

2) $MDP_{\oplus,+}(s) = 5/256 = 2^{-5.678}$;

3) fixed point number: 0;

4) the number of cycles of length two: 0.

For instance, such S-boxes are $s_{02,0F}$ or $s_{52,70}$; full list is given in tab. 1. Weakening requirements for value $MDP_{\oplus,+}(s)$ to the original value 6/256 leads to an increasing number of appropriate S-boxes up to 1076.

In our opinion, considered improvements of Qalqan^{v1} S-box will make it possible to strengthen the security of the Qalqan cipher against differential cryptanalysis and algebraic attacks.

4. Properties of the Linear Layer of Qalqan^{v1} cipher

In this section, the cryptographic properties of the linear transformation of the Qalqan^{v1}cipher are

Table 1. List of u, v parameter values (in hexadecimal) for which S-boxes $s_{u,v}$ have the best cryptographic properties.

№	u	v	№	u	v
1	02	$0F$	13	82	$8F$
2	$0D$	70	14	$8D$	$F0$
3	13	70	15	93	$F0$
4	$2D$	$0F$	16	AD	70
5	$2D$	$F0$	17	AD	$8F$
6	$3F$	$F0$	18	BF	70
7	40	$8F$	19	$C0$	$0F$
8	52	70	20	$D2$	$0F$
9	52	$8F$	21	$D2$	$F0$
10	$6C$	$0F$	22	EC	$8F$
11	72	$0F$	23	$F2$	$8F$
12	$7D$	70	24	FD	$F0$

considered. In particular, we found its branch number, and describe large classes of its fixed points.

Claim 1. Branch number of the linear layer L of Qalqan^{v1} cipher is equal to 3.

Proof. It is known that the branch number of a linear transformation over the space of dimension m can take values only in the interval from 2 to $m+1$. Let us first show that $B(L) \neq 2$.

Since only $M \neq O$ are considered and L is non-singular and bijective, we have $wt(M) \geqslant 1$, $wt(L(M)) \geqslant 1$; therefore $B(L) = 2$ if and only if there exists a matrix M of weight 1 such that $L(M)$ also has weight 1. However, if the matrix $M \in \mathcal{M}$ contains only one non-zero byte on the diagonal, then the $L(M)$ matrix after the distribution phase will contain four — all bytes of the corresponding column will become non-zero; if the only non-zero byte of M is not on the diagonal, then there will be five of them in $L(M)$: after the absorption phase, the diagonal byte of the corresponding row becomes non-zero, and after the distribution phase — all the bytes of its column also become non-zero. Thus, if $wt(M) = 1$, we have $wt(L(M)) \geqslant 4$, and therefore $B(L) > 2$.

Let us now consider such bytes $a \neq 0$, $b \neq 0$ that $a + b \equiv 0 \pmod{256}$. Then

$$M = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & a & b \end{bmatrix} \to L(M) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 \end{bmatrix},$$

and thus $wt(M) + wt(L(M)) = 3$. It follows that $B(L) = 3$ by definition. □

The given claim shows that the linear layer of the Qalqan^{v1} cipher has a relatively low, almost minimal value of branch number, which in general, may indicate vulnerability to differential and linear cryptanalysis. However, an even more disturbing fact is that L has large classes of fixed points, in particular, of low weight.

Claim 2. Let a, b, x, y, z be such nonzero bytes that $a+b \equiv 0 \pmod{256}$, $x+y+z \equiv 0 \pmod{256}$. Let the rows of the matrix M be formed according to the following rule: the diagonal byte is zero, and the other bytes are either the bytes a, b, and 0 in any order, or the bytes x, y, z in an arbitrary order (all possible forms of rows of such matrices are shown in Fig. 2). Then $L(M) = M$.

$$\begin{aligned} &1\colon (0,a,b,0),\ \ (0,a,0,b),\ \ (0,0,a,b),\ \ (0,x,y,z);\\ &2\colon (a,0,b,0),\ \ (a,0,0,b),\ \ (0,0,a,b),\ \ (x,0,y,z);\\ &3\colon (a,b,0,0),\ \ (a,0,0,b),\ \ (0,a,0,b),\ \ (x,y,0,z);\\ &4\colon (a,b,0,0),\ \ (a,0,b,0),\ \ (0,a,b,0),\ \ (x,y,z,0). \end{aligned}$$

Fig. 2. Kinds of rows of matrices that form fixed points for the linear layer L. Each row of the matrix can take any of the following four forms.

Proof. It is easy to see that the values of the diagonal elements of the matrix becomes $0+a+b+0 = 0$ or $0 + x + y + z = 0$ after the absorption phase; so the rows of the matrix M preserve their values. Accordingly, in the distribution phase, diagonal bytes (which all remains zero) are added to all bytes of the matrix M; thus, the entire matrix M will remain unchanged. □

Corollary. The mapping L has at least $(2^{16}-1)^4$ fixed points.

Proof. Indeed, there are 255 pairs of bytes (a, b), where $a, b \neq 0$, and $a + b \equiv 0 \pmod{256}$; each such pair forms three possible types of a fixed-point matrix row. Similarly, with direct calculation we find that there are 64770 triples (x, y, z) such that $x, y, z \neq 0$, and $x + y + z \equiv 0 \pmod{256}$. Accordingly, each row of the fixed-point matrix described in the Claim 2 can be chosen in

$$3 \cdot 255 + 64770 = 65535 = 2^{16} - 1$$

ways; and since each of the four rows of the matrix is chosen independently, we have $(2^{16}-1)^4$ of such matrices in general. Of course, L can also have fixed points of a different kind, so given the number is only a lower estimate. □

We see that the linear layer of the cipher Qalqan^{v1} has a significant number of fixed points (at least $2^{63.99}$ out of 2^{128} values of the input argument in total); among them, in particular, there will be $4 \cdot 3 \cdot 255 = 3060$ fixed points of weight 2, which can be used to construct high-probability differential and linear characteristics. Thus, the propagation properties and avalanche effects of the L transformation can be considered insufficient to prevent algebraic and statistical attacks. In the next section, we illustrate this statement by constructing a differential attack on modified versions of this cipher.

5. High Probability Differential Characteristics for Modified Qalqan^{v1} Ciphers

Consider the family of three-round differential characteristics $\Omega_1 = \Omega_1(u, v, a, b, c, d)$, where parameters u, v, a, b, c, d are nonzero bytes, and $a + b \equiv 0 \pmod{256}$; the structure of the differential characteristics of this family is shown in Fig. 3. For the cipher Qalqan$^{v1}_{\oplus\boxplus}$ the first difference, which is determined by the bytes u and v, is calculated by the operation $\oplus$, for the cipher Qalqan$^{v1}_{\boxplus\boxplus}$ — by operation $\boxplus$; all other differences in both ciphers are calculated by the $\boxplus$ operation. We will use the notation $\Omega_1^{\oplus}$ and $\Omega_1^{\boxplus}$ to emphasize this distinction.

For the round functions $F_k^{\oplus}$ and $F_k^{\boxplus}$ of modified ciphers Qalqan$^{v1}_{\oplus\boxplus}$ and Qalqan$^{v1}_{\boxplus\boxplus}$ consider the differences $\alpha = (\alpha_0, \ldots, \alpha_{15})$, $\beta = (\beta_0, \ldots, \beta_{15})$, where $\alpha_i, \beta_j \in V_8$ — individual bytes; then

$$\begin{aligned} DP^{F_k^{\oplus}}_{\oplus,\boxplus}(\alpha, \beta) &= \prod_{i=0}^{15} DP^{s}_{\oplus,+}(\alpha_i, \tilde{\beta}_i), \\ DP^{F_k^{\boxplus}}_{\boxplus,\boxplus}(\alpha, \beta) &= \prod_{i=0}^{15} DP^{s}_{+,+}(\alpha_i, \tilde{\beta}_i), \end{aligned}$$

where $\tilde{\beta} = L^{-1}(\beta)$, and the symbol $+$ denotes addition modulo 256. So probabilities of the differential characteristics of the family $\Omega_1(u, v, a, b, c, d)$ are determined as

$$\begin{aligned} DCP(\Omega_1^{\oplus}) &= DP^{s}_{\oplus,+}(u, a) DP^{s}_{\oplus,+}(v, b) \times \\ &\times DP^{s}_{+,+}(a, c) (DP^{s}_{+,+}(c, d))^5, \\ DCP(\Omega_1^{\boxplus}) &= DP^{s}_{+,+}(u, a) DP^{s}_{+,+}(v, b) \times \\ &\times DP^{s}_{+,+}(a, c) (DP^{s}_{+,+}(c, d))^5. \end{aligned}$$

We found at least 10^6 various differential characteristics of $\Omega_1^{\oplus}$ with probabilities in the range of $2^{-42} \div 2^{-46}$, and at least 10^6 various differential characteristics $\Omega_1^{\boxplus}$ with probabilities in the range $2^{-41.8} \div 2^{-45.9}$. The characteristics with the highest probabilities are listed in tables 2 and 3. Note that we did not evaluate the probabilities of the bordering differentials for considered characteristics, although, by definition, they will be even greater than the given values.

The second family of differential characteristics $\Omega_2 = \Omega_2(u_1, u_2, a_1, a_2, b_1, b_2, c_1, c_2, \ldots)$, where parameters $u_1, u_2, a_1, a_2, b_1, b_2, c_1, c_2, \ldots$ are nonzero bytes, u_1 and u_2 can take arbitrary non-zero values, and all subsequent pairs of bytes must sum to zero: $a_1 + a_2 \equiv 0 \pmod{256}$, $b_1 + b_2 \equiv 0 \pmod{256}$, etc.; the structure of the differential characteristics of this family is shown in Fig. 4. This family of differential characteristics exploits the low-weight fixed points of the linear transformation L.

The probabilities of the differential characteristics of the family $\Omega_2(u_1, u_2, a_1, a_2, b_1, b_2, c_1, c_2, \ldots)$ are determined as

$$\begin{aligned} DCP(\Omega_2^{\oplus}) &= DP^{s}_{\oplus,+}(u_1, a_1) DP^{s}_{\oplus,+}(u_2, a_2) \times \\ &\times DP^{s}_{+,+}(a_1, b_1) DP^{s}_{+,+}(a_2, b_2) \times \\ &\times DP^{s}_{+,+}(b_1, c_1) DP^{s}_{+,+}(b_2, c_2) \times \ldots \\ DCP(\Omega_2^{\boxplus}) &= DP^{s}_{+,+}(u_1, a_1) DP^{s}_{+,+}(u_2, a_2) \times \\ &\times DP^{s}_{+,+}(a_1, b_1) DP^{s}_{+,+}(a_2, b_2) \times \\ &\times DP^{s}_{+,+}(b_1, c_1) DP^{s}_{+,+}(b_2, c_2) \times \ldots \end{aligned}$$

We found several hundred differential characteristics of the $\Omega_2^{\oplus}$ family for different numbers of encryption rounds. Probabilities of the best characteristics for $r = 2, 3, \ldots, 11$ are given in the table 4; at $r \geq 12$, the probabilities of the studied differential characteristics become smaller than 2^{-128}.

Interestingly, we had found one regular differential characteristic of the form $\Omega_2^{\boxplus}$ with high probability:

$$(9B, 65) \to (16, EA) \to (9B, 65) \to (16, EA) \to \ldots,$$

and the analog of the form $\Omega_2^{\oplus}$:

$$\begin{aligned} &(3C, 3C) \to (9B, 65) \to (16, EA) \to \\ &\qquad \to (9B, 65) \to (16, EA) \to \ldots \end{aligned}$$

The probability of a three-round characteristic of this type is $2^{-33.5424}$, and an eleven-round one is $2^{-122.287}$.

In [1] it is noted that the probabilities of the three-round differential characteristics of the cipher Qalqan^{v1} “by of all assumptions” do not exceed 2^{-132}, and the differential cryptanalysis for a four-round cipher has the complexity not lower than 2^{312}; unfortunately, the authors did not provide any information on how the assessment data were obtained. Our results contradict the declared security estimates. Of course, we considered differential characteristics for a modified Qalqan^{v1} cipher, but all the distinction from the original is the removal of carry bits between state bytes after adding a round key modulo 2^{128}. If we consider the original cipher version and differential characteristics of the described Ω_1 family, then the presence of carry bits in the key adder (under the most favorable condi-

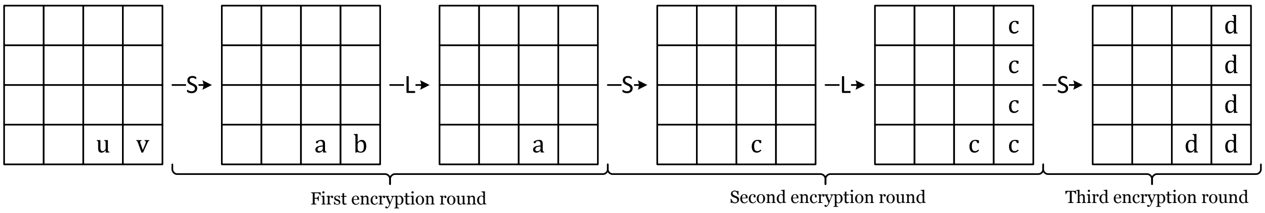

Fig. 3. The structure of the differential characteristic of the family $\Omega_1(u, v, a, b, c, d)$; empty cells correspond to zero differences, addition with keys is included in the S layer, in the third round of encryption the linear layer is removed. The application of L layer does not affect the probability of such characteristics, so the probabilities are determined only by the application of S layer.

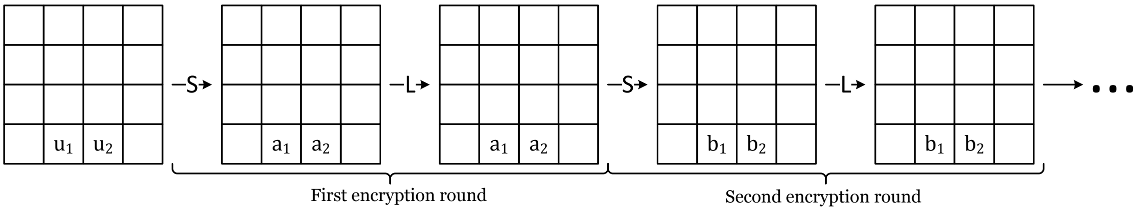

Fig. 4. The structure of the differential characteristic of the family $\Omega_2(u_1, u_2, a_1, a_2, b_1, b_2, c_1, c_2, \dots)$; empty cells correspond to zero differences, addition with keys is included in the S layer. Byte pairs (a_1, a_2), (b_1, b_2), etc., form fixed points of L, so the linear layer is actually excluded from the encryption process; the probabilities of such a characteristic are determined only by the application of S layer.

Table 2. Differential characteristics of $\Omega_1^{\oplus}$ with high probabilities; parameter values are given in hexadecimal

u	v	a	b	c	d	$DCP(\Omega_1^{\oplus})$
DA	36	12	EE	63	$C8$	$2^{-42.29}$
DA	CA	EE	12	$9D$	38	$2^{-42.29}$
$2C$	$8C$	27	$D9$	63	$C8$	$2^{-42.51}$
$2C$	74	$D9$	27	$9D$	38	$2^{-42.51}$

Table 3. Differential characteristics of $\Omega_1^{\boxplus}$ with high probabilities; parameter values are given in hexadecimal

u	v	a	b	c	d	$DCP(\Omega_1^{\boxplus})$
36	CA	EE	12	$9D$	38	$2^{-41.8}$
CA	36	12	EE	63	$C8$	$2^{-41.8}$
74	$8C$	27	$D9$	63	$C8$	$2^{-42.25}$
$8C$	74	$D9$	27	$9D$	38	$2^{-42.25}$

tions for the analyst) can only add one non-zero byte to the 15th position of the input difference for the second round of encryption and another eight non-zero bytes of the input difference for the third round of encryption. Since the maximum probability value of the Qalqan^{v1} S-box differential is 2^{-5}, the appearance of nine more non-zero bytes in the differential characteristic can reduce its probability to 2^{-87} (again, with the most favorable conditions for the analyst), but by no means up to 2^{-132}.

We can summarize that the simple structure of the linear layer of the Qalqan^{v1} cipher, the absence of proper avalanche effects, and a very small value of the branch number lead to the existence of classes of differential characteristics (and, accordingly, differentials) with very high probabilities. This indicates potential serious vulnerabilities of the cipher against differential cryptanalysis.

Table 4. Probabilities of the best found 255 differential characteristics $\Omega_2^{\oplus}$ depending on the number of encryption rounds r

r	$DCP(\Omega_2^{\oplus})$
2	$2^{-21.6601} \div 2^{-24.1862}$
3	$2^{-32.4902} \div 2^{-35.3561}$
4	$2^{-43.9277} \div 2^{-46.3724}$
5	$2^{-55.3203} \div 2^{-57.5424}$
6	$2^{-66.5587} \div 2^{-68.6764}$
7	$2^{-77.5065} \div 2^{-80.1139}$
8	$2^{-88.7449} \div 2^{-91.3203}$
9	$2^{-99.6927} \div 2^{-102.676}$
10	$2^{-110.931} \div 2^{-113.693}$
11	$2^{-121.879} \div 2^{-124.931}$

Conclusion

In this work we considered the Qalqan^{v1} cipher, which is positioned as a possible national encryption standard of the Republic of Kazakhstan. We show that the S-box of this cipher, which has sufficient quality from the modern cryptology perspective, can be easily improved to increase security against differential cryptanalysis and algebraic attacks. We proved that the branch number of the linear layer of this cipher is equal to 3, which is too small value for ciphers of this type; moreover, the linear layer has at least $2^{63.99}$ fixed points, which significantly reduces its avalanche effects.

For a modified Qalqan^{v1} cipher with byte-wise round key additions (or, equally, with removed carry bits between bytes in the key adder) we found at least one million three-round differential characteristics with probabilities in the range $2^{-42} \div 2^{-46}$; such characteristics allow to implement differential attack on a four-round cipher with very low complexity. Several hundreds of multi-round differential characteristics based on the low-weight fixed points of the linear layer of the cipher were also found.

The obtained results indicate that the structure of the linear transformation of the cipher Qalqan^{v1} has significant shortcomings against methods for assessing resistance to known cryptanalytic attacks. We hope that the found weaknesses will be taken into account in the development of the next versions of the Qalqan cipher.

References

[1] L. Gorlov, R. Ibrayev, G. Ospanov, R. Itemirov, and I. Kiyashko, "Algorithm shifrovaniya Qalqan / Qalqan Encryption Algorithm (in russian)," in *Proceedings of VI International Scientific Conference "Computer Science and Applied Mathematics" (September 29 – October 2, 2021, Almaty, the Republic of Kazakhstan)*, pp. 458–463, 2021. https://conf.iict.kz/6th-ispc-csam-en/.

[2] N. Seilova, A. Kungozhin, R. Ibrayev, L. Gorlov, Z. Ospanov, R. Itemirov, and I. Kiyashko, "About Cryptographic Properties of the Qalqan Encryption Algorithm," in *CEUR Workshop Proceedings "Cybersecurity Providing in Information and Telecommunication Systems II" — CPITS-II'2021 (October 26, 2021, Kyiv, Ukraine)*, pp. 206–215, 2021. https://ceur-ws.org/Vol-3187/paper19.pdf.

[3] N. Seilova, R. Ibrayev, L. Gorlov, and M. Turdalyuly, "Cryptographic Properties of a Nonlinear Node of a Block Symmetric Encryption Algorithm Qalqan," *News of the National Academy of Sciences of the Republic of Kazakhstan. Physico-mathematical Series*, vol. 6, no. 340, pp. 73–80, 2021. https://doi.org/10.32014/2021.2518-1726.104.

[4] J. Daemen and V. Rijmen, "The Wide Trail Design Strategy," in *Cryptography and Coding* (B. Honary, ed.), (Berlin, Heidelberg), pp. 222–238, Springer Berlin Heidelberg, 2001.

[5] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," *Journal of Cryptology*, vol. 4, pp. 3–72, Jan 1991.

[6] X. Lai, J. L. Massey, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis," in *Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'91, (Berlin, Heidelberg), pp. 17–38, Springer-Verlag, 1991.

[7] A. N. Alekseychuk and L. V. Kovalchuk, "Towards a Theory of Security Evaluation for GOST-like Ciphers against Differential and Linear Cryptanalysis." Cryptology ePrint Archive, Report 2011/489, 2011. https://eprint.iacr.org/2011/489.

[8] S. Vaudenay, "On the Security of CS-Cipher," in *Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings*, vol. 1636 of *Lecture Notes in Computer Science*, pp. 260–274, Springer, 1999.

[9] K. Nyberg, "Perfect Nonlinear S-boxes," in *Advances in Cryptology — EUROCRYPT '91* (D. W. Davies, ed.), (Berlin, Heidelberg), pp. 378–386, Springer Berlin Heidelberg, 1991.