# Comparative analysis of ARX transformations

Victor Ruzhentsev
Kharkiv National University of Radioelectronics,
Ukraine, information technologies security department,
e-mail: victorruzh@gmail.com

CECC 2020

# Philosophies of lightweight cryptography algorithms building

## Big S-box

- bigger S-boxes are more effective in terms of cryptographic strength
- use large S-boxes based on efficiently implemented computational operations, for example, ARX operations

## Small S-box

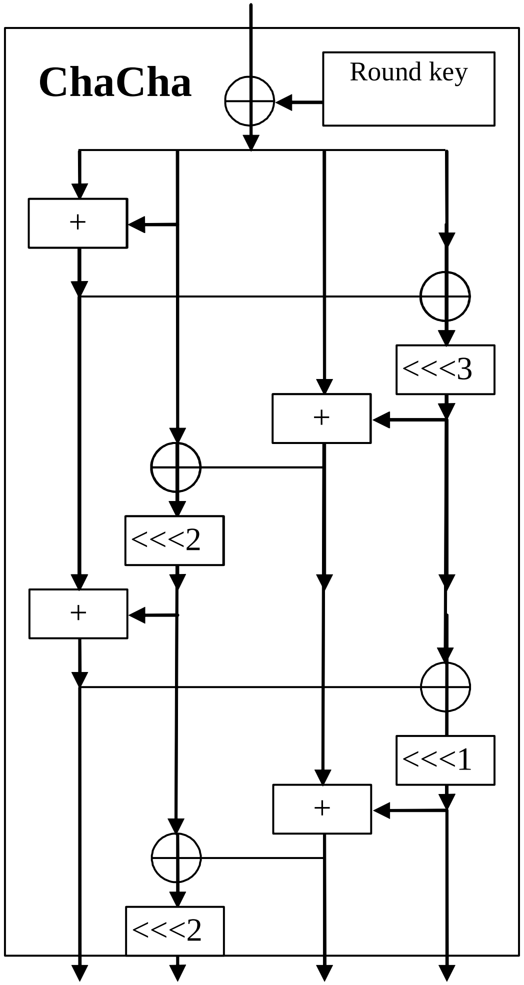
- smaller S-boxes tend to cost less on memory usage
- use small-size substitutions (4 to 4 bits)

# The aim and objectives

The aim of this work is to find the optimal approach to building ARX S-boxes in terms of maximum speed and cryptographic security.

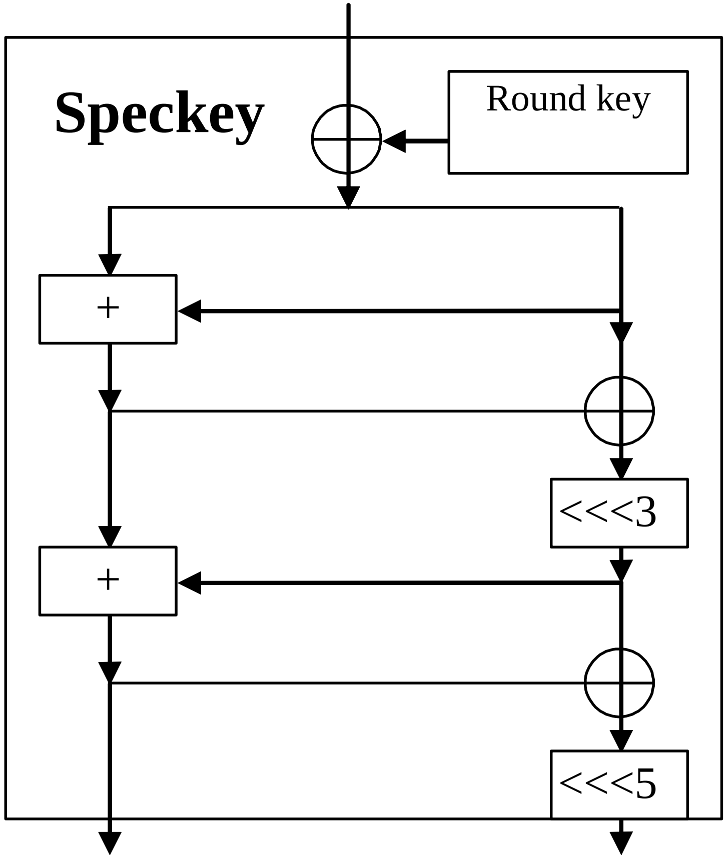
To achieve the goal, we will analyze the most famous solutions for building ARX S-boxes. Considering the fact that ARX algorithms are easily scalable, we will develop reduced models for their comparison and determine how many rounds are needed to achieve the cryptographic parameters of random permutation.

# ChaCha



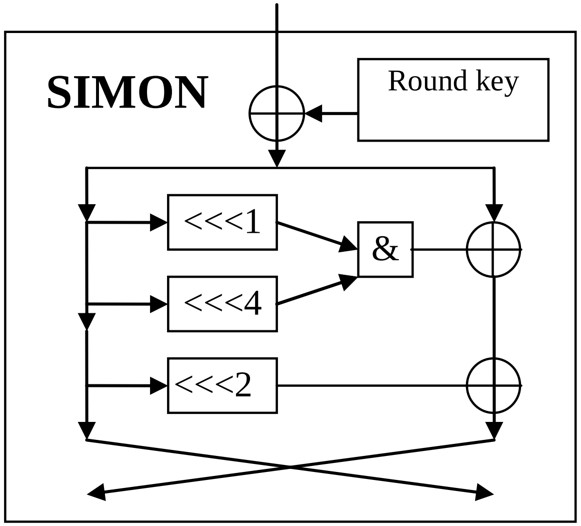
16-bit state of the our reduced model ChaCha consists of four 4-bit subblocks

# Speckey



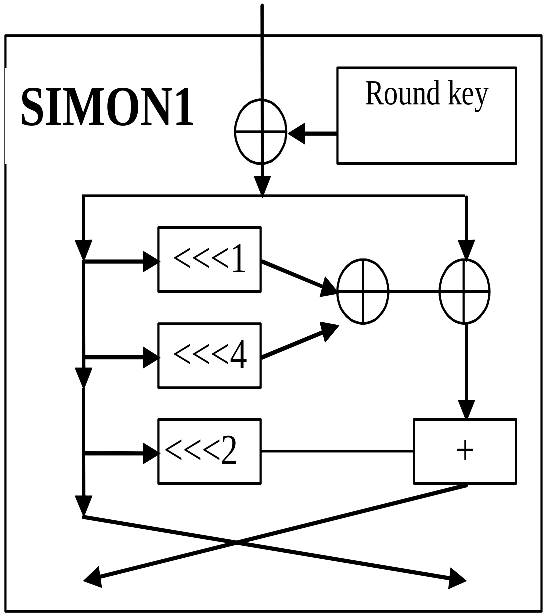
The Speckey 16-bit block consists of two 8-bit subblocks.

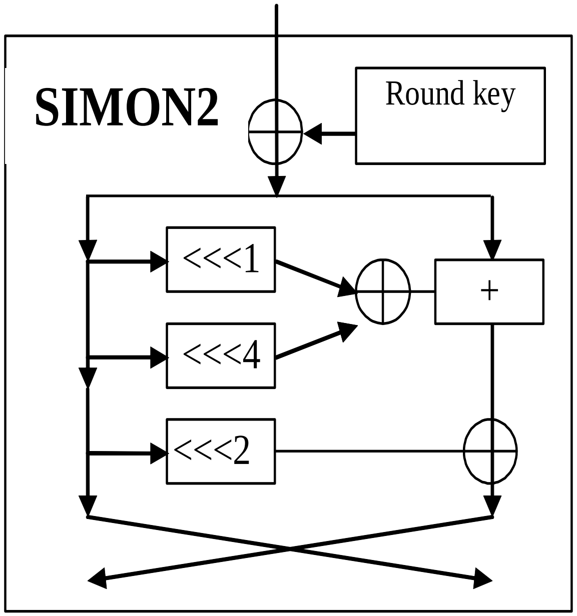
# Simon

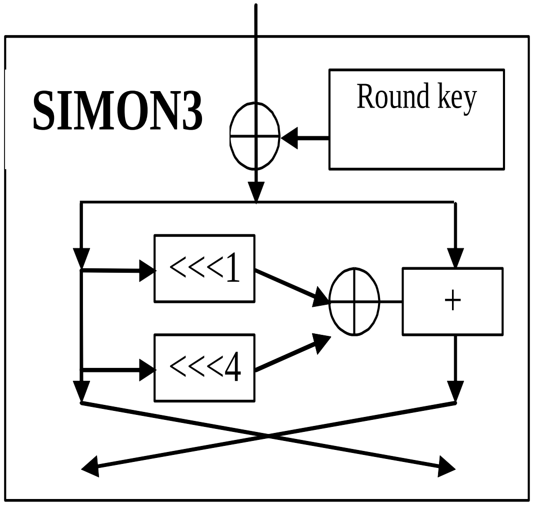


The 16-bit block of all Simon’s variants consists of two 8-bit subblocks

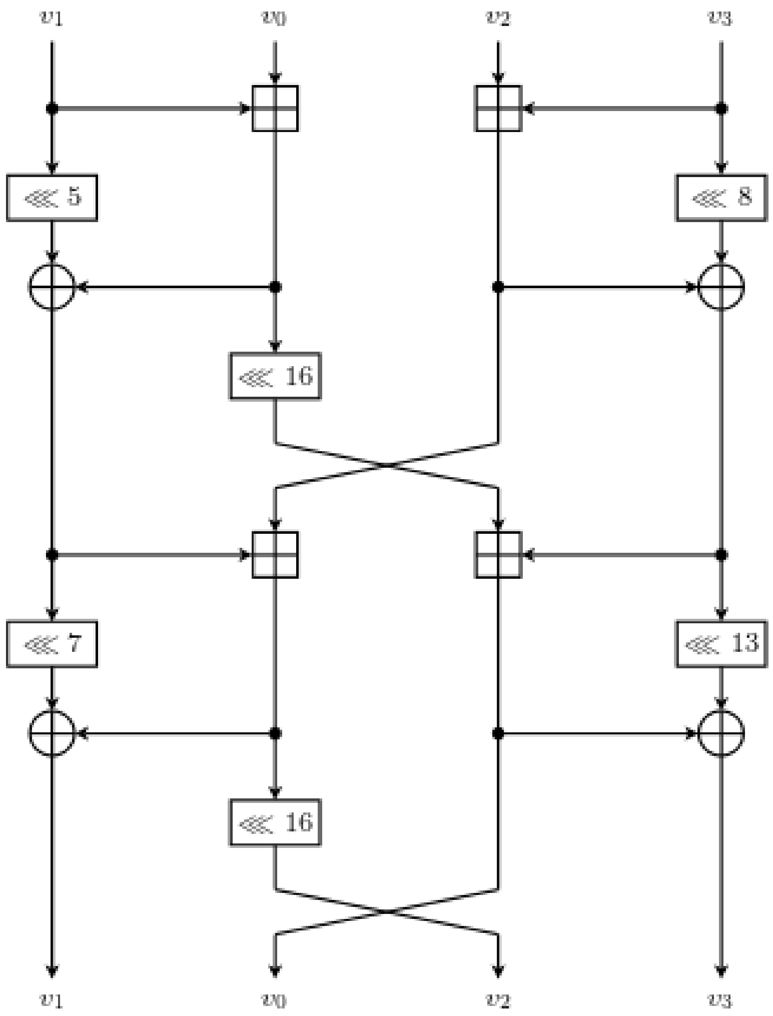
# Variants of Simon





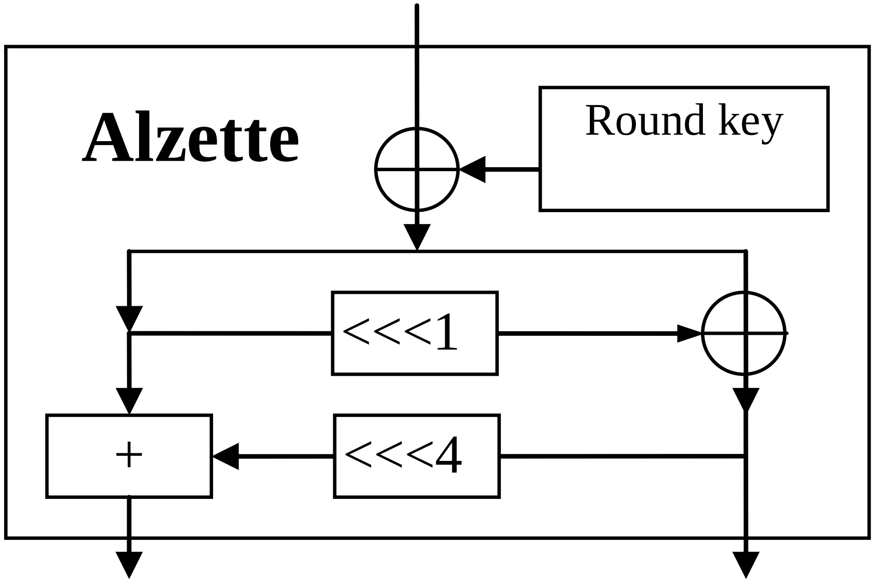


# Chaskey



The 16-bit Chaskey block consists of four 4-bit subblocks with values of rotations 1,2,3,1,3,2.

# ARX S-box of the Sparkle algorithm, called Alzette



Block consists of two 8-bit subblocks.

# Description of experiments

In our experiments, all models, at first, use the XOR addition of 16-bit block with a random key of the same size, and then use keyless rounds.

# Analysis of cryptographic security

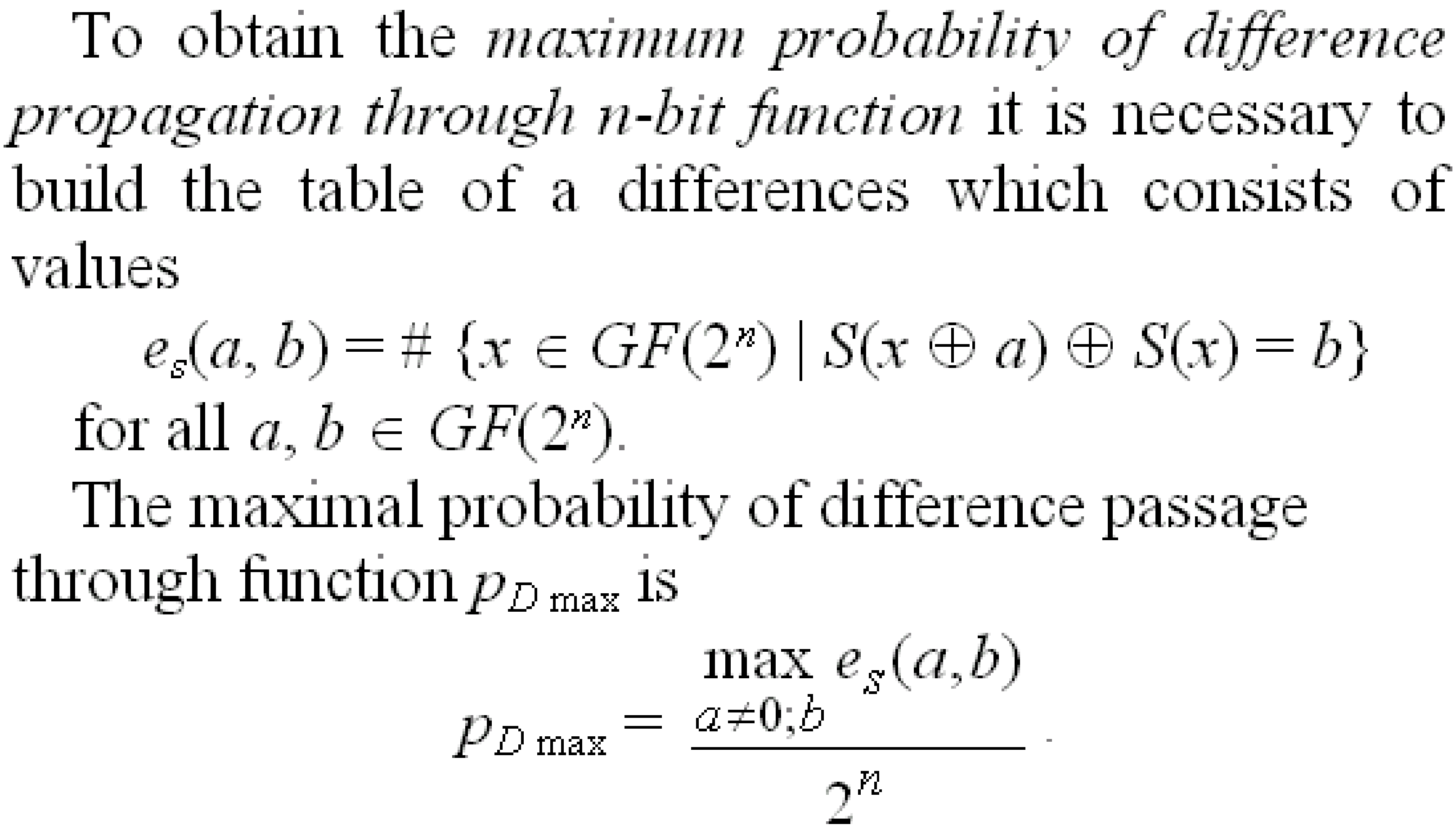
The most important cryptographic parameters of an encryption function or substitution are:

- maximum probability of the difference propagation (determines the resistance of the cipher to differential attacks);

- maximum probability of linear approximation (determines the resistance of the cipher to linear cryptanalysis);

- nonlinear order (determines the resistance of the cipher to interpolation attacks).

# *Maximum probability of difference propagation*



To obtain the *maximum probability of difference propagation through n-bit function* it is necessary to build the table of a differences which consists of values

$$e_s(a, b) = \# \{x \in GF(2^n) \mid S(x \oplus a) \oplus S(x) = b\}$$

for all $a, b \in GF(2^n)$.

The maximal probability of difference passage through function $p_{D\,\max}$ is

$$p_{D\,\max} = \frac{\max\limits_{a \neq 0; b} e_S(a,b)}{2^n} .$$

# Exhaustive search for differentials with maximum probability

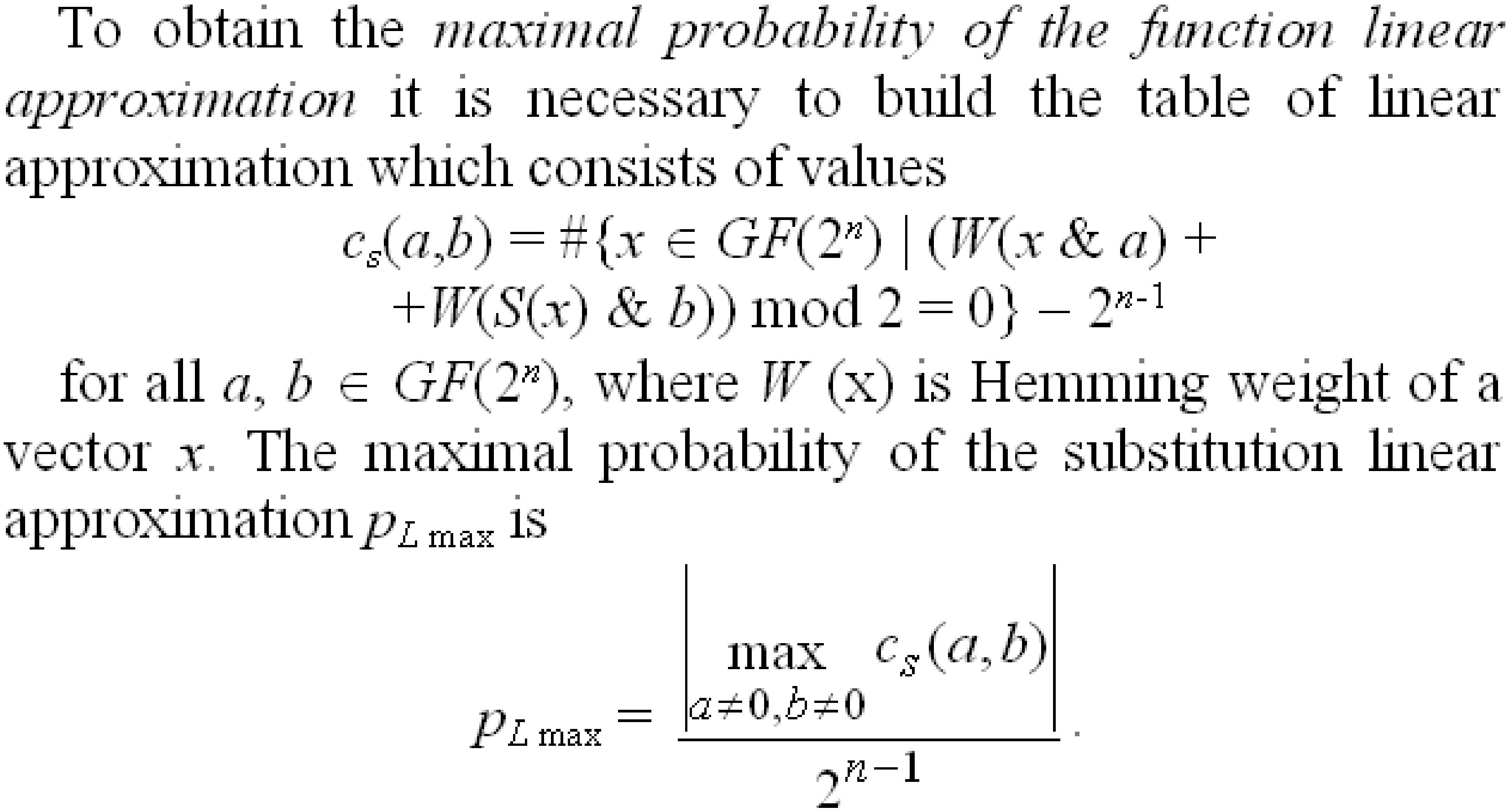
Randomly chosen 64 16-bit keys were used in this search

| Schemes | Number of rounds | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Speckey | 1 | $2^{-2}$ | $2^{-4,6}$ | $2^{-9,1}$ | $2^{-11,7}$ | $2^{-11,7}$ | $2^{-11,7}$ | $2^{-11,7}$ |
| ChaCha | 1 | $2^{-2}$ | $2^{-5}$ | $2^{-10,2}$ | $2^{-11,7}$ | $2^{-11,7}$ | $2^{-11,7}$ | $2^{-11,7}$ |
| Simon | - | - | - | $2^{-3}$ | - | $2^{-6,6}$ | - | $2^{-7,9}$ |
| Simon1 | 1 | $2^{-0,8}$ | $2^{-1,7}$ | $2^{-4}$ | $2^{-5,9}$ | $2^{-9,8}$ | $2^{-11,5}$ | $2^{-11,5}$ |
| Simon2 | 1 | $2^{-2}$ | $2^{-3,8}$ | $2^{-5,8}$ | $2^{-8,9}$ | $2^{-11,8}$ | $2^{-11,8}$ | $2^{-11,8}$ |
| Simon3 | 1 | $2^{-2}$ | $2^{-2,5}$ | $2^{-4,4}$ | $2^{-6}$ | $2^{-8,3}$ | $2^{-10}$ | $2^{-11,7}$ |
| Chaskey | 1 | $2^{-3}$ | $2^{-8,7}$ | $2^{-11,1}$ | $2^{-11,8}$ | $2^{-11,8}$ | $2^{-11,8}$ | $2^{-11,7}$ |
| Alzette | - | - | - | - | - | $2^{-5,8}$ | - | $2^{-10}$ |

# The results of differentials search

- As a rule, the models come to a stable value $2^{–11,7}$ after using sufficient number of rounds.
- Speckey, ChaCha and Chaskey require 5 rounds for this, Simon1 – 7 rounds, Simon2 – 6 rounds, Simon3 – 8 rounds, Alzette – 9 rounds.
- Scheme Simon, on the other hand, does not match the random permutation value $2^{–11,7}$ for any number of rounds.

# Maximum probability of linear approximation



To obtain the *maximal probability of the function linear approximation* it is necessary to build the table of linear approximation which consists of values

$$c_s(a,b) = \#\{x \in GF(2^n) \mid (W(x \,\&\, a) + \\ +W(S(x) \,\&\, b)) \bmod 2 = 0\} - 2^{n\text{-}1}$$

for all $a$, $b \in GF(2^n)$, where $W$ (x) is Hemming weight of a vector $x$. The maximal probability of the substitution linear approximation $p_{L\max}$ is

$$p_{L\max} = \frac{\left|\max\limits_{a \neq 0, b \neq 0} c_S(a,b)\right|}{2^{n-1}}.$$

# Maximum probability of linear approximation was searched for the few variants of the input mask and for the 5 randomly selected keys

| Schemes | Number of rounds | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Speckey | - | $2^{-3,6}$ | $2^{-6}$ | $2^{-6,3}$ | $2^{-5,9}$ | $2^{-8,1}$ | $2^{-6,4}$ | $2^{-6,4}$ |
| ChaCha | - | $2^{-4}$ | $2^{-4,3}$ | $2^{-5}$ | $2^{-5,8}$ | $2^{-6,5}$ | $2^{-6,6}$ | $2^{-8,1}$ |
| Simon2 | - | $2^{-2,7}$ | $2^{-3,7}$ | $2^{-5,6}$ | $2^{-6,6}$ | $2^{-6,5}$ | $2^{-6,6}$ | $2^{-6,6}$ |
| Simon3 | - | $2^{-2}$ | $2^{-3,7}$ | $2^{-5,2}$ | $2^{-5,4}$ | $2^{-5,4}$ | $2^{-7}$ | $2^{-6,6}$ |
| Chaskey | $2^{-0,7}$ | $2^{-5,3}$ | $2^{-5,2}$ | $2^{-5,7}$ | $2^{-6,6}$ | $2^{-6,6}$ | $2^{-8,1}$ | $2^{-6,6}$ |
| Alzette | - | $2^{-1,7}$ | $2^{-2,6}$ | $2^{-5,2}$ | $2^{-4,5}$ | $2^{-6,2}$ | $2^{-6,6}$ | $2^{-6,6}$ |

# The results of linear approximations search

- The models come to a stable value of $2^{-6,4}$ after using sufficient number of rounds.
- Simon2 and Chaskey require 5 rounds, Speckey and ChaCha – 6 rounds, Simon3 and Alzette – 7 rounds.
- Scheme Simon does not match the random permutation value $2^{-6,4}$ for any number of rounds

# Nonlinear order

The nonlinear order for a random permutation 16 to 16 bits must be 15.

It was determined that all models come to this value after using 3 rounds.

# Number of addition and shift operations required to provide cryptographic parameters of random permutation

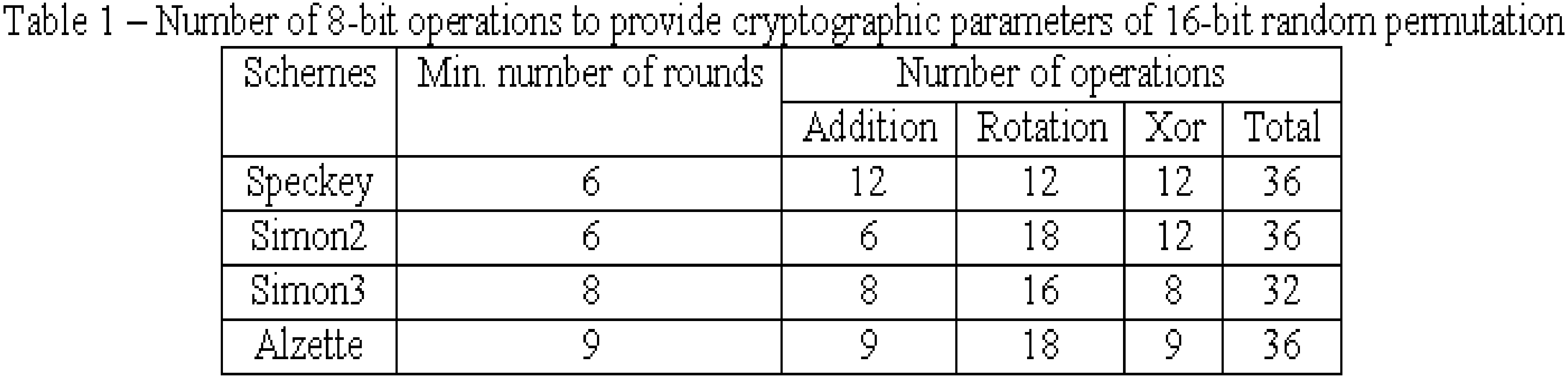


Table 1 – Number of 8-bit operations to provide cryptographic parameters of 16-bit random permutation

| Schemes | Min. number of rounds | Number of operations | | | |
|---|---|---|---|---|---|
| | | Addition | Rotation | Xor | Total |
| Speckey | 6 | 12 | 12 | 12 | 36 |
| Simon2 | 6 | 6 | 18 | 12 | 36 |
| Simon3 | 8 | 8 | 16 | 8 | 32 |
| Alzette | 9 | 9 | 18 | 9 | 36 |

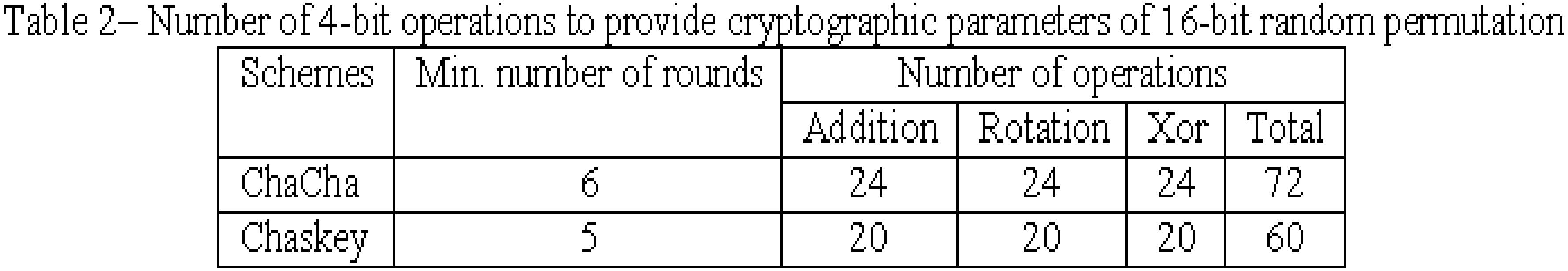


Table 2– Number of 4-bit operations to provide cryptographic parameters of 16-bit random permutation

| Schemes | Min. number of rounds | Number of operations | | | |
|---|---|---|---|---|---|
| | | Addition | Rotation | Xor | Total |
| ChaCha | 6 | 24 | 24 | 24 | 72 |
| Chaskey | 5 | 20 | 20 | 20 | 60 |

# Conclusions

1 The analysis of cryptographic parameters of reduced models (16 bit block) of the most known ARX encryption algorithms was performed. These algorithms are Salsa, ChaCha, Cypress, Speckey, Simon, Chaskey, Sparkle and their modifications. It has been demonstrated that most models come to stable value of most important cryptographic parameters after using sufficient number of rounds. But this situation is not true for maximum probability of the difference propagation for ARX scheme from Simon cipher. Therefore, a reduced model of the Simon algorithm requires additional more careful consideration.

2 ARX schemes which use 8-bit operations and schemes which use 4-bit operations are considered in the work. Using these schemes it is shown that, potentially, ARX schemes with larger size of operations are more flexible and efficient, since, according to our results, they require, approximately, half the number of operations to provide cryptographic parameters of random permutation.

3 According to the Table 1 and 2 Chaskey model is the most efficient ARX scheme with 4-bit operations, and Simon3 is the most efficient scheme with 8-bit operations. At the same time, for example, implementation on 8-bit processor of Simon3 requires almost twice less operations than Chaskey to achieve cryptographic parameters of random permutation.