**RAD HRVATSKE AKADEMIJE ZNANOSTI I UMJETNOSTI
MATEMATIČKE ZNANOSTI**

V. Ruzhentsev

Comparative analysis of ARX transformations

Manuscript accepted for publication

COMPARATIVE ANALYSIS OF ARX TRANSFORMATIONS

Victor Ruzhentsev

Abstract. ARX encryption schemes are considered in this work. These schemes use only three operations: modular addition, XOR addition and cyclic shift. 16-bit reduced models of the most famous algorithms of this class are being developed. Among these algorithms are Salsa, Chacha, Speck, Simon, Chaskey, Sparkle. Some of them operate with 4-bit words, others with 8-bit words. By an exhaustive search for models of these algorithms specific cryptographic parameters are determined. These parameters are the maximum probability of difference propagation (determines the resistance of the cipher to attacks of differential cryptanalysis); maximum probability of linear approximation (determines the resistance of the cipher to attacks of linear cryptanalysis); non-linear order (determines the resistance of the cipher to interpolation attacks). It is demonstrated that most of the models with increasing the number of rounds come to the parameters of random permutations. It is determined that the Simon algorithm model does not possess this property. Several modifications of this algorithm are proposed. Comparing the number of operations required to achieve random permutation's parameters, the most successful ARX schemes are selected. The most efficient 4-bit scheme is the reduced Chaskey model, and the most effective 8-bit scheme is the modification of the Simon scheme which was proposed in this work. It is shown that, potentially, ARX schemes with a larger format of operations are more flexible and efficient, since they require less operations to provide cryptographic parameters of random permutation.

1. Introduction

Lightweight cryptography is a rapidly growing field of symmetric cryptography. Confirmation of this is a global Lightweight cryptography project of the American National Institute of Standards and Technology [9]. One of

2010 *Mathematics Subject Classification.* 62K05.

Key words and phrases. cryptanalysis, ARX algorithm, modular addition, cyclic shift, differential cryptanalysis, difference, linear cryptanalysis, random permutation.

the most important issues in constructing lightweight algorithms is the approach to building nonlinear elements. On the one hand, it is known that bigger S-boxes are more effective in terms of cryptographic strength. On the other hand, bigger S-boxes tend to cost more on memory usage, which is an important parameter for lightweight cryptography. We reflect on which philosophy in lightweight cryptography is more advantageous: use large S-boxes based on efficiently implemented computational operations, for example, ARX operations (Addition, Rotation, Xor), or use small-size substitutions (4 to 4 bits).

The perspective direction for lightweight symmetrical ciphers (SC) constructing are ARX transformations (Addition, Rotation, Xor). It is possible to get strong cipher using only these three operations. Examples of such algorithms are ciphers from RC family, from Salsa family [2, 3]. Younger ARX ciphers are Chaskey [8], Sparx [5], LAX [5], Speck [1].

ARX transformations are fast and can be effectively realized on many modern processors. The main problem is proof of cryptographic security for these algorithms. The most efficient attacks on ARX algorithms are differential and linear cryptanalysis [4], algebraic attacks, integral attack [14] and its variant, which has name division attack [13], impossible differential attack [15], rotational cryptanalysis [7] and others.

Scalability is one of the advantages of ARX structures. Thus, we believe that reduced model of such transformations will have almost similar cryptographic features as the full-scale prototype. The approach with the analysis of cryptographic properties based on consideration of the reduced models was used and earlier, including our works, for instance [6] and [12], as well as at analysis of algorithms participants of Ukrainian national public cryptographic competition [11].

The aim of this work is to find the optimal approach to building ARX transformations in terms of maximum speed and cryptographic security. To achieve the goal, we analyze the most famous solutions for building ARX transformations. Considering the fact that ARX algorithms are easily scalable, we develop reduced models for their comparison and determine how many rounds are needed to achieve the cryptographic parameters of random permutation.

2. Scaled reduced models of ARX transformations

Among the 16-bit schemes chosen for analysis there are those that work with 4-bit blocks (ChaCha and Chaskey), and those that work with 8-bit blocks (Speckey, Alzette and variants of the Simon). The 16-bit block consists of four 4-bit subblocks in the first case and of two 8-bit subblocks in the second case. In our experiments, all models, at first, use the XOR addition of 16-bit block with a random 16-bit key, and then use few keyless rounds.

Scaled reduced models of ChaCha [2] and Chaskey [8] are presented on Fig. 1 and 2, respectively.

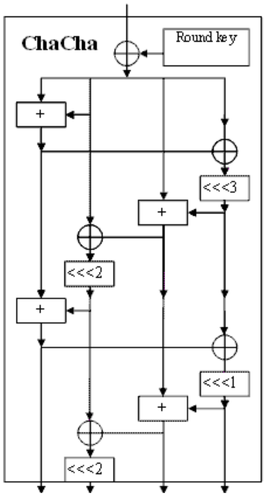


FIGURE 1. ChaCha reduced model

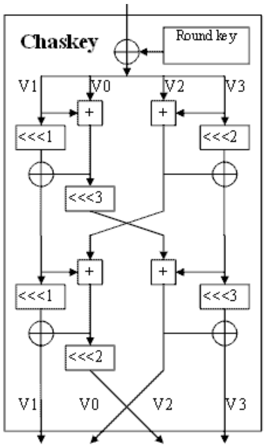


FIGURE 2. Chaskey reduced model

Simplified non-linear element of the Speck algorithm [1], named Speckey is presented on Fig. 3. The simplification is the absence of two cyclic shift

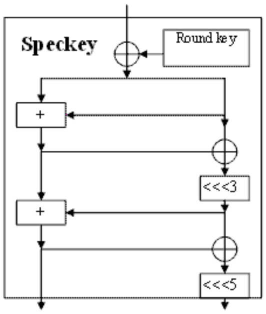


FIGURE 3. Speckey reduced model

operations, which in the original version preceded the modular addition operations.

The reduced model of the Simon [1] encryption algorithm is on Fig. 4.

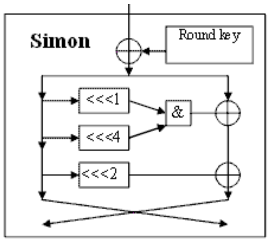


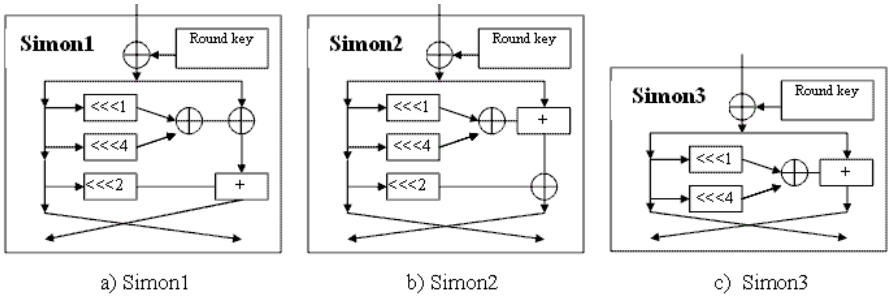
FIGURE 4. Simon reduced model

Three modifications of original scheme are also considered in this work (Fig. 5). Simon1 and Simon2 use modular addition instead of AND and some XOR operations. Simon3 uses two cyclic shifts of the left subblock, XOR addition of these two shift results and modular addition of the result to the right subblock.

The reduced ARX S-box of the Sparkle algorithm [9], called Alzette, is on Fig. 6.

The schemes differ by the amount and format of operations (tabl. 1).

Any addition operation (modular or XOR) that operates on 8-bit blocks is almost equivalent to two 4-bit identical operations. Performing an 8-bit cyclic shift is more resource intensive than two identical 4-bit operations. But for simplicity, we can assume that each 8-bit operation is equivalent to two such 4-bit operations. For example, the Speckey scheme contains half the number of operations in ChaCha in one round, but the format of these operations is two times larger. Therefore, in terms of speed on a 4-bit platforms, these



a) Simon1

b) Simon2

c) Simon3

Figure 5. Simon's variants

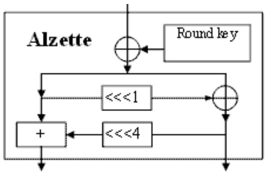


Figure 6. Alzette reduced model

Table 1. Format and number of operation in one round for reduced ARX models

ARX models	Additions	Rotations	XOR additions
ChaCha	4 * 4 bit	4 * 4 bit	4 * 4 bit
Chaskey	4 * 4 bit	4 * 4 bit	4 * 4 bit
Speckey	2 * 8 bit	2 * 8 bit	2 * 8 bit
Simon	1 * 8 bit	3 * 8 bit	1 * 8 bit + 1 AND
Simon1	1 * 8 bit	3 * 8 bit	2 * 8 bit
Simon2	1 * 8 bit	3 * 8 bit	2 * 8 bit
Simon3	1 * 8 bit	2 * 8 bit	1 * 8 bit
Alzette	1 * 8 bit	1 * 8 bit	1 * 8 bit

schemes can be considered equivalent, but Speckey is almost two times faster on an 8-bit platforms.

3. Analysis of cryptographic security

The most important cryptographic properties of encryption function are:

- the maximal probability of difference propagation (determines the resistance to differential cryptanalysis);

- the maximal probability of the function linear approximation (determines the resistance to linear cryptanalysis);

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

It is possible to estimate these parameters for 16-bit models of encryption functions.

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.

3.1. *Security against differential cryptanalysis.* Differential cryptanalysis is one of the most powerful and universal kinds of attacks on SC. To obtain the maximal probability of difference passage through n-bit function S it is necessary to build the table of a differences which consists of values

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

The maximal probability of difference propagation is

$$p_{Dmax} = \frac{\max e_s(a,b)}{2^n} \text{ for } a, b \neq 0.$$

It is known that for random substitution 16 to 16 bits [10]

$$p_{Dmax} \approx \frac{20}{2^{-16}} \approx 2^{-11,7}.$$

The maximum probability of the difference propagation was searched for the considered ARX schemes. 64 randomly selected keys were used in the search. The results are presented in tabl. 2.

Table 2. Probability of differentials

ARX models	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}

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. Using the same number of operation in round algorithm Simon2 shows much better results of security than Simon and Simon1. Thus Simon and Simon1 excluded from the further analysis.

3.2. *Security against linear cryptanalysis.* To obtain the maximal probability of the n-bit function S linear approximation it is necessary to build the table of linear approximation which consists of values

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

for all $a, b \in GF(2^n)$, where $W(x)$ is Hemming weight of vector x.

The maximal probability of linear approximation is

$$p_{Lmax} = \frac{\max c_s(a,b)}{2^{n-1}} \text{ for } a \neq 0, b \neq 0.$$

Exhaustive search for the linear approximation of function with maximum probability was used to analyze security against linear cryptanalysis. Randomly chosen 5 16-bit keys and first five (5 from 65536) input masks were used in this search. The Results are presented in tabl. 3.

Table 3. Probability of linear approximation

ARX models	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 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.

4. Comparative analysis of ARX transformations

Three cryptographic parameters (see Section 3) were used to determine how many addition and shift operations are required to achieve cryptographic parameters of a random permutation. Tables 4 and 5 show required number of operations, respectively, for the 8-bit and 4-bit ARX schemes.

Table 4 and 5 show that Chaskey is the most efficient 4-bit scheme, and Simon3 is the most efficient 8-bit scheme. In general, the considered schemes with the same format of operations demonstrate quite a similar results. For example, the difference in the number of operations for 8-bit schemes does not exceed 4.

Comparing the implementations of 4-bit and 8-bit schemes on a 4-bit platform, if each 8-bit operation is equated to two 4-bit ones, then the 4-bit Chaskey scheme is the most efficient (60 operations for Chaskey versus 64 for Simon3). But the implementation of the Chaskey scheme on an 8-bit platforms will require almost twice as many operations as for Simon3

Table 4. Number of 8-bit operations to provide cryptographic parameters of 16-bit random permutation

ARX models	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 5. Number of 4-bit operations to provide cryptographic parameters of 16-bit random permutation

ARX models	Min. number of rounds	Number of operations			
		Addition	Rotation	XOR	Total
ChaCha	6	24	24	24	72
Chaskey	5	20	20	20	60

(60 operations for Chaskey versus 32 for Simon3). Therefore, the general conclusion can be made about the greater efficiency of ARX schemes with a large format of operations.

5. Conclusions

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, 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 and linear approximation for ARX scheme from Simon cipher. Therefore, a reduced model and original Simon algorithm requires additional more careful consideration.

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.

According to the Table 4 and 5 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.

Acknowledgements.
The author is grateful to an anonymous referee for helpful comments.

References

[1] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, *The SIMON and SPECK families of lightweight block ciphers*, Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/2013/404.

[2] D. J. Bernstein, *Chacha, a variant of Salsa20,* SASC 2008 –the State of the Art in Stream Ciphers, 2008. https://cr.yp.to/chacha.html.

[3] D. J. Bernstein, *The salsa20 family of stream ciphers*, in: New Stream Cipher Designs: The eSTREAM Finalists (eds. M. Robshaw and O. Billet), volume 4986 of Lecture Notes in Computer Science, Berlin, Heidelberg, 2008, 84–97.

[4] A. Biryukov, V. Velichkov, and Y. Le Corre, *Automatic Search for the Best Trails in ARX: Application to Block Cipher Speck*, Lecture Notes in Computer Science 9783, Springer, Heidelberg, 2016, 289–310.

[5] D. Dinu, L. Perrin, A. Udovenko, V. Velichkov, J. Grosschadl, and A. Biryukov, *Design strategies for ARX with provable bounds: Sparx and LAX*, in: Advances in Cryptology – ASIACRYPT 2016 (eds. J. H. Cheon and T. Takagi), Part I, volume 10031 of Lecture Notes in Computer Science, Springer, Heidelberg, 2016, 484–513.

[6] V. I. Dolgov, I. V. Lisitskaya and V. I. Ruzhentsev, *Analysis of cyclic properties of block ciphers*, Applied radio electronics, Vol. 6, N2, Kharkiv, 2007, 257–263 (in Russian).

[7] D. Khovratovic, I. Nikolic *Rotational Cryptanalysis of ARX*, in: Fast Software Encryption 2010 (eds. S. Hong and T. Iwata), volume 6147 of Lecture Notes in Computer Science, Berlin, Heidelberg, 2010, 4–19.

[8] N. Mouha, B. Mennink, A. V. Herrewege, D. Watanabe, B. Preneel, and I. Verbauwhede, *Chaskey: An effcient MAC algorithm for 32-bit microcontrollers*, in: SAC 2014: 21st Annual International Workshop on Selected Areas in Cryptography (eds. A. Joux and A. M. Youssef), volume 8781 of Lecture Notes in Computer Science, Springer, Heidelberg, 2014, 306–323.

[9] Lightweight cryptography project of the American National Institute of Standards and Technology. https://csrc.nist.gov/projects/lightweight-cryptography.

[10] L. O'Connor, *On distribution of characteristics in bijective mappings*, in: Eurocrypt'93 (ed. T. Helleseth), volume 765 of Lecture Notes in Computer Science, Springer-Verlag, 1994, 360–370.

[11] R. Oliynykov, I. Gorbenko, V. Dolgov, V. Ruzhentsev, *Results of Ukrainian national public cryptographic competition*, Tatra Mountains Mathematical Publications, vol. 47, Bratislava, 2010, 99–114.

[12] V. Ruzhentsev, Y. Onishchenko, *Development of the approach to proving the security of block ciphers to impossible differential attack*, Eastern-European Journal of Enterprise Technologies, Mathematics and cybernetics - applied aspects, vol. 4, N 4 (88), Kharkiv, 2017, 28–33.

[13] Y. Todo, *Structural evaluation by generalized integral property*, in: Advances in Cryptology – EUROCRYPT 2015 (eds. E. Oswald and M. Fischlin), Part I, volume 9056 of Lecture Notes in Computer Science, Springer, Heidelberg, 2015, 287–314.

[14] L. Wen, and M. Wang, *Integral zero-correlation distinguisher for ARX block cipher, with application to shacal-2*, Information Security and Privacy, Springer, 2014, 454–461.

[15] X. Zheng, and K. Jia, *Impossible differential attack on reduced-round TWINE*, in: ICISC 13: 16th International Conference on Information Security and Cryptology (eds. H.-S. Lee and D.-G. Han), volume 8565 of Lecture Notes in Computer Science, Springer, Heidelberg, 2014, 123–143.

Naslov

Prvi autor, drugi autor i treći autor

Sažetak. Hrvatski prijevod sažetka.

Victor Ruzhentsev
Department of Secure Information Technologies
Kharkiv National University of Radioelectronics
61000 Kharkiv, Ukraine
E-mail: victorruzh@gmail.com