Middle-East Journal of Scientific Research 11 (8): 1078-1086, 2012
ISSN 1990-9233
© IDOSI Publications, 2012

A Novel Design of the KASUMI Block Cipher Using One-Hot Residue Number System

Hamidreza Mahyar

Department of Computer Engineering, Sharif University of Technology, Tehran, Iran

Abstract: The KASUMI block cipher is used for the cellular communications networks and safety of many wireless standards. Third generation cellular network technology (3G) permits to transmit information, voice and video at very high data rates never seen before that will revolutionize personal communications and information exchange. On the other hand, Residue Number System (RNS) is a modular representation and is evidenced to be serviceable equipment in many applications which need high-speed computations and high-performance components. RNS is a non-weighted and integer number system that can support secure, high-speed, low-power, parallel and carry-free arithmetic. For attaining the most performance a technique is declared that named "One-Hot Residue Number System". The propagation delay of this implementation is just one transistor. In this paper, synthesizing the KASUMI encryption algorithm and One-Hot RNS for improving the KASUMI features are presented. In this document, we represent a novel design of the KASUMI block cipher using OHRNS. The goals of this design include strategies to reduce delay, power consumption, hardware and lastly power-delay product.

Key words: Cryptography · KASUMI Block Cipher · Residue Number System (RNS) · High-Speed Computation · One-Hot · VLSI

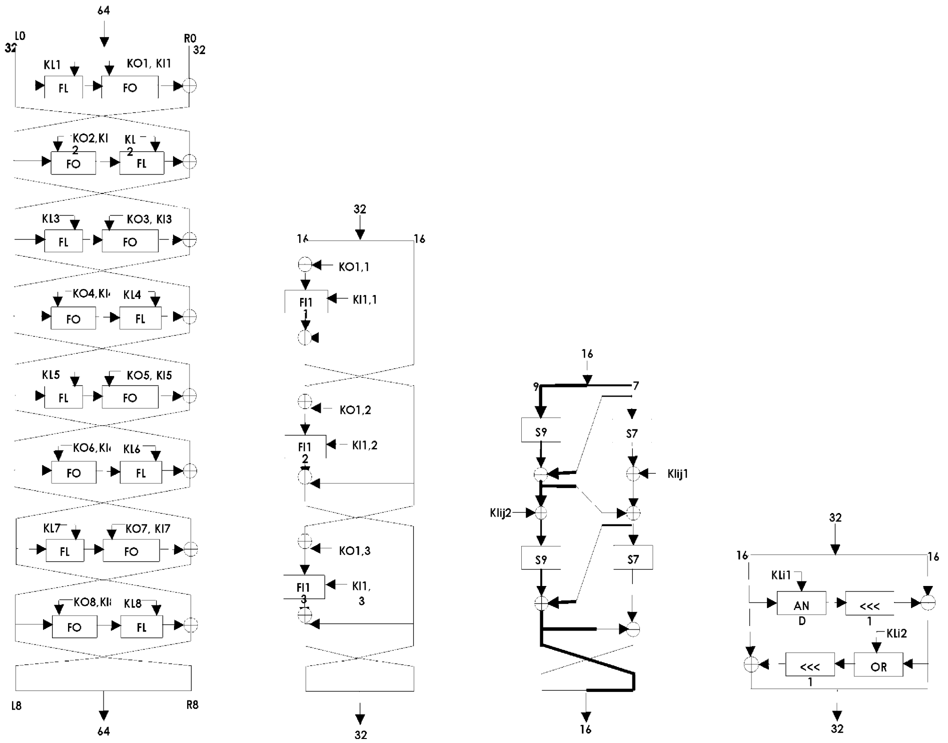
INTRODUCTION

The KASUMI block cipher was adopted by the 3rd Generation Partnership Program [1] based on prior work performed for MISTY [2], an encryption algorithm that has asserted its security against the most advanced cryptanalysis techniques and is proper for high-speed implementation in hardware and software platforms. With the recent developments in the field of cellular communications and the quick progress of the wireless standards, the topic of security has gained more significance.

The UMTS (Universal Mobile Telecommunications system) f8 confidentiality and f9 integrity algorithms, the GSM (Global System for Mobile Communications) A5/3 and the GPRS (General Packet Radio Service) GEA3 encryption/decryption algorithms rely on the KASUMI block cipher [3-5]. KASUMI has a Feistel structure containing eight rounds, operates on 64-bit data blocks and its processing is controlled by a 128-bit encryption key K [6]. By using a 128-bit ciphering key K, it modifies a 64-bit Plaintext to a 64-bit Ciphertext. Moreover, it has the following further traits derived from its Feistel nature: input plaintext blocks are the input to the first round, Ciphertext blocks are the last round's output, the encryption key K is used to generate a set of round keys {KLi, KOi, KIi} for each round i, each round computes a different function as long as the round keys are different. The same algorithm is used both for encryption and decryption.

Fig. 1 shows the structure and components of the KASUMI block cipher. For odd rounds the round-function is computed by applying the FL function followed by the FO function. For even rounds the FO function is applied before FL. FL, shown in Fig. 1(d), is a 32-bit function made up of simple AND, OR, XOR and left rotation operations. FO, depicted in Fig. 1(b), is also a 32-bit function having a three-round Feistel organization which contains one FI block per round. FI, see Fig. 1(c), is a non-linear 16-bit function having itself a four-round Feistel structure; it is made up of two nine-bit substitution boxes (S-boxes) and two seven bit S-boxes. Fig. 1(c) shows that data in the FI function flow along two different paths: a nine-bit long path (thick lines) and a seven-bit

Corresponding Author: Hamidreza Mahyar, Department of Computer Engineering, Sharif University of Technology, Tehran, Iran. Tel: +98 912 2499095, Fax: +98 21 88055794, E-mail: Hamidreza_mahyar@yahoo.com.



a. Feistel structure *b.* FO function *c.* FI function *d.* FL function

Fig. 1: The KASUMI Block Cipher.

path (thin lines). Notice that in Feistel structures, such as the one used in this algorithm, each round's output is twisted before being applied as input to the following round.

After completing eight rounds, KASUMI produces a 64-bit long Ciphertext block corresponding to the plaintext input block.

Digital systems are used in many applications in telecommunications and cryptography. The main objective of VLSI digital design is to proximately decrease the cost and increase the performance of the digital systems in terms of complexity, speed, delay and power. Meanwhile, Residue Number System is an interesting method for designing high-speed and low-power VLSI digital systems. The RNS is carry-free and offers high-speed operations. As we can easily see in the KASUMI block cipher, the most used parts are XOR logical gates and the improvement of these parts can increase the performance of the KASUMI algorithm. In this paper, we firstly present an instrumental circuit for computing XOR operation with only one transistor delay using One-Hot RNS and secondly, describe a novel design of the KASUMI block cipher using this method. Then, the simulation results and discussion with previous works are shown. Finally, the paper conclusions are given.

Security of the KASUMI Algorithm: The first example of a block cipher with provable security against the basic forms of differential and linear cryptanalysis under and independent round key assumption was presented by Nyberg and Knudsen, 1995 [7]. Later, Matsui, 1996 [8] introduced a methodology for designing block ciphers with provable security against differential and linear cryptanalysis. This methodology has since been used in the design of the block ciphers MISTY and KASUMI.

Kang *et al.*, 2001 [9] examined the pseudo randomness of the KASUMI and its provable security.

Tanaka *et al.*, 2001 [10] attacked the KASUMI without FL functions by using Higher Order Differential Attack and found that KASUMI has a provable security against Linear cryptanalysis and Differential attack.

Meier and Roy, 2004 [11] showed that their results clarify the assumptions necessary in order for f8 and f9 to be secure and, since no related-key attacks are known against the full eight rounds of KASUMI, lead us to believe that the confidentiality and integrity mechanisms used in real 3GPP applications are secure.

Iwata *et al.* [12] presented that the KASUMI is a block cipher which forms the heart of the 3GPP confidentiality and integrity algorithms. They studied the security of the five-round KASUMI type permutations and derived a highly non-trivial security bound against adversaries with adaptive chosen plaintext and chosen Ciphertext attacks. To derive their security bound, they heavily used the tools from graph theory. However the results didn`t not show its super-pseudo randomness, this gives a strong evidence that the design of the KASUMI is sound.

The existence of better related-key attacks on the full KASUMI was already shown in Biham *et al.* [13] and Kim *et al.* [14]. Their attack had more data complexity and time complexity, which are absolutely impractical but better than exhaustive search.

Dunkelman *et al.* [15] described a new type of attack called a sandwich attack and used it to construct a simple distinguisher for 7 of the 8 rounds of KASUMI. However, they liked to emphasize that even though their attack on the underlying cryptosystem has a practical time complexity, they did not claim that they can practically apply such a related key attack to the way KASUMI is used in the f8 and f9 modes of operation in cellular telephony. They certainly did not stand on their proposed method and results.

Nadjah *et al.* [16] demonstrated that S-boxes constitute a cornerstone component in symmetric-key cryptographic algorithms. In block ciphers, they are typically used to obscure the relationship between plaintext and Ciphertext. Non-linear and non-correlated S-boxes are the most secure against linear and differential cryptanalysis and it is profitable for KASUMI.

Therefore, we can strongly believe the KASUMI block cipher and its provable security.

Residue Number System and its Operations: RNS is specified by moduli set like $\{m_1, m_2, \ldots, m_n\}$ in which all the moduli are positive integers. If all the moduli are relatively pair wise prime, this system will have the largest conceivable dynamic range that equals $[\alpha, \alpha+M)$ in which α is an integer and M is:

$$M = \prod_{i=1}^{n} m_i \tag{1}$$

Any integer X in interval of $[\alpha, \alpha+\mathrm{M})$ has a unique RNS representation given by:

$$X \xrightarrow{RNS} (x_1, x_2, x_3, \ldots, x_n) \tag{2}$$

Where

$$x_i = \langle X \rangle_{m_i}, \; i = 1,2,3,\ldots,n \tag{3}$$

Provided $\langle X \rangle_{m_i}$ denotes the operation $X\ mod\ m_i$. If the two integers X and Y have RNS representations $(x_1, x_2, x_3, \ldots, x_n)$ and $(y_1, y_2, y_3, \ldots, y_n)$ respectively, then the RNS representation of $Z = X \text{ o } Y$ (where o specifies XOR, addition, subtraction, or multiplication) is as follows:

$$z_i = \langle x_i \text{ o } y_i \rangle_{m_i}, \quad i = 1,2,3,\ldots,n \tag{4}$$

Equation (4) proves the parallel, carry-free nature of the RNS [17-20]. The reconstruction of X from its residues $(x_1, x_2, x_3, \ldots, x_n)$ is based on the Chinese Remainder Theorem (CRT) shown by:

$$X = \left\langle \sum_{i=1}^{n} \langle x_i, N_i \rangle_{m_i} \times Mi \right\rangle_M$$

$$M = \prod_{i=1}^{n} m_i$$

$$M_i = \frac{M}{m_i}, N_i = \left\langle M_i^{-1} \right\rangle_{m_i}, i = 1,2,3,\ldots,n \tag{5}$$

The notation $\left\langle M_i^{-1} \right\rangle_{m_i}$ in (5) denotes the multiplicative inverse of M_i modulo m_i [21, 22].

Because of its specific features, the Residue Number System has numerous applications in arithmetic functions such as Cryptosystem, Digital Signal Processing, Digital Filtering, Coding, RSA ciphering system, KASUMI block cipher, digital communications, Ad-hoc network, storing and retrieving information, Error detection and Correction and fault tolerant systems. This system is commonly gained in those areas where XOR, addition, subtraction and multiplication operations of numbers are being repeated. Additionally, since in these systems the computations on the remainders are done independently if one error occurs on one remainder it won't be transferred to other moduli. In other words, the nature of RNS architecture is tolerant against faults and also error detection and correction are wholly possible [23-27].

Considering the impact of Residue Number System in increasing calculation speed, reducing power consumption and increasing the security and fault tolerance, it would be possible to perform arithmetic calculations on each modulus with a new Residue Number System. It is possible to repeat this procedure until we reach very small moduli, in other words this procedure could be repeated in several levels. The system which is achieved form the above mentioned procedure is called Multi-Level Residue Number System (MLRNS). The only restriction that should be considered in Multi-Level Residue is that the Residue Number System dynamic range that is considered for *i* level of each (*i*-1) moduli-level should be greater or equal to those moduli. In two-level Residue Number System, two symmetrical coding key algorithms are used inside each other; therefore the system has a much higher security level than the Residue Number System.

The other advantage of two-level Residue Systems is the simple selection of moduli set for a large dynamic range that is by selecting a few large moduli and applying a new Residue Number System with a lower power for second level this capability is achieved. By having few moduli with higher power in the first level; first the need for moduli to be relatively pair wise prime is eliminated and there is no obligation for the moduli to be symmetric and regular, second as the number of moduli is reduced the concerning conversion circuits, become simple and the operation is done rapidly. Also, in the second level since the moduli are small because of the limited propagation of carries, the internal calculations of the Residue Number System are done faster.

One-Hot Residue Number System: The advantages of using the One-Hot to present the digits of RNS are very obliging and it is putative the resulting "number system" with the new name "One-Hot Residue Number System". Frankly speaking, the OHRNS and the RNS have the same arithmetic. The main and basic elements in One-Hot are Barrel shifters. In addition to mi moduli, one of the operands is shifted as the other shifter. Barrel shifters are used for the primary operations (which contain excellent Power-Delay Product), simple and regular layout of arithmetic circuits and zero-cost implementation of inverse and index calculation and moduli conversion. Lower Power-Delay Product (PDP) happens as an affect of signal activity factors are near-minimal and less critical path transistors in referred papers [28-29]. m_i moduli remainders are from zero to m^i-1 that in One-Hot representation a signal line is reserved for each of these numbers. The activity of each signal indicates the equivalent remainder with it. One–Hot representation for mi moduli remainders are depicted in Fig. 2 only one of the lines is active (driven high) and the rest of lines are inactive at any time. During a change in digit value, at most two lines change their value at maximum level. Therefore the power dissipation is at minimum level. Hence, OHRNS is simple, rapid, low-power and has orderly and explicit structure.

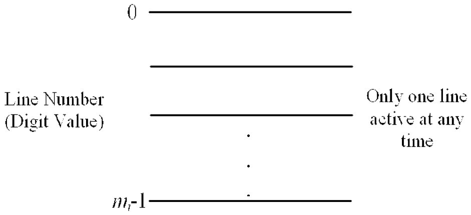


Fig. 2: OHRNS representation for digit xi

With this One-Hot representation of residue digits, XOR logical operation can be performed by cyclic shifts ("rotations"). The rotation can be presented by one of several types of circuits; in our work we have selected to utilize barrel shifters. These circuits compute all possible rotations in parallel when required the appropriate one to the output.

One of the significant features of One-Hot is its independence to the type of moduli but one of the shortcomings of One-Hot System is that it couldn't be implemented for large moduli for the reason that the number of transistors are increased. Consequently, this system is appropriate for small moduli. Notice that we can solve this problem with combining Multi-Level RNS and One-Hot RNS. As it was mentioned in this section, One-Hot Residue Number System is suitable for small moduli, but for large moduli it is not applicable because the transistors are added in arithmetic calculations. On the other hand, in Multi-Level Residue Number System the arithmetic operations are done on small moduli. With combining these two techniques the new system is resulted that named "One-Hot Multi-Level Residue Number System" (OHMLRNS). In this technique, first a moduli collection with large modulus is selected and then for each of these moduli one new Residue System is chosen and the procedure is repeated. Hence in the final level, one Residue Number System with small moduli is gained and it is the best condition to make a profit of OHRNS on small moduli.

Proposed OHRNS XOR Gate: In this section, we present a new symbol and circuit for computing XOR logical operation and 2-bit inputs XOR gate with using OHRNS. As it was mentioned in the prior section, we can also use OHMLRNS if we have a problem with large moduli.

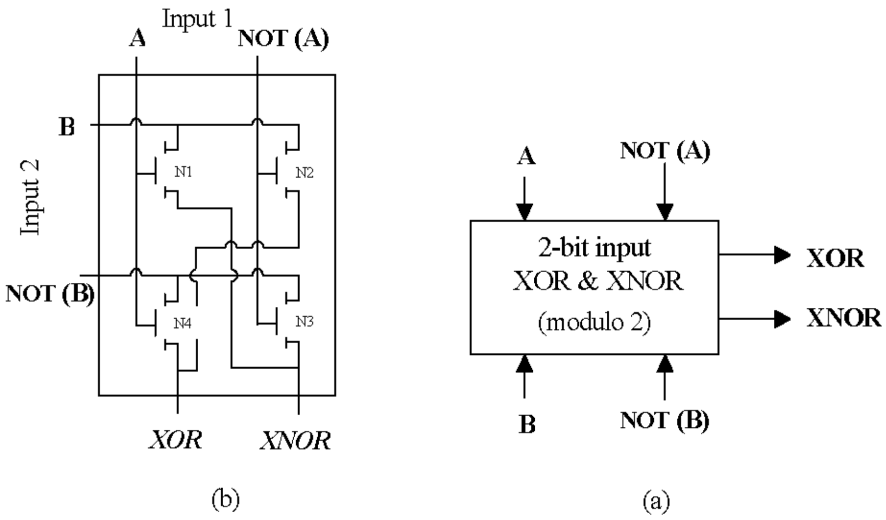


Fig. 3: OHRNS XOR Gate: (a) symbol and (b) circuit

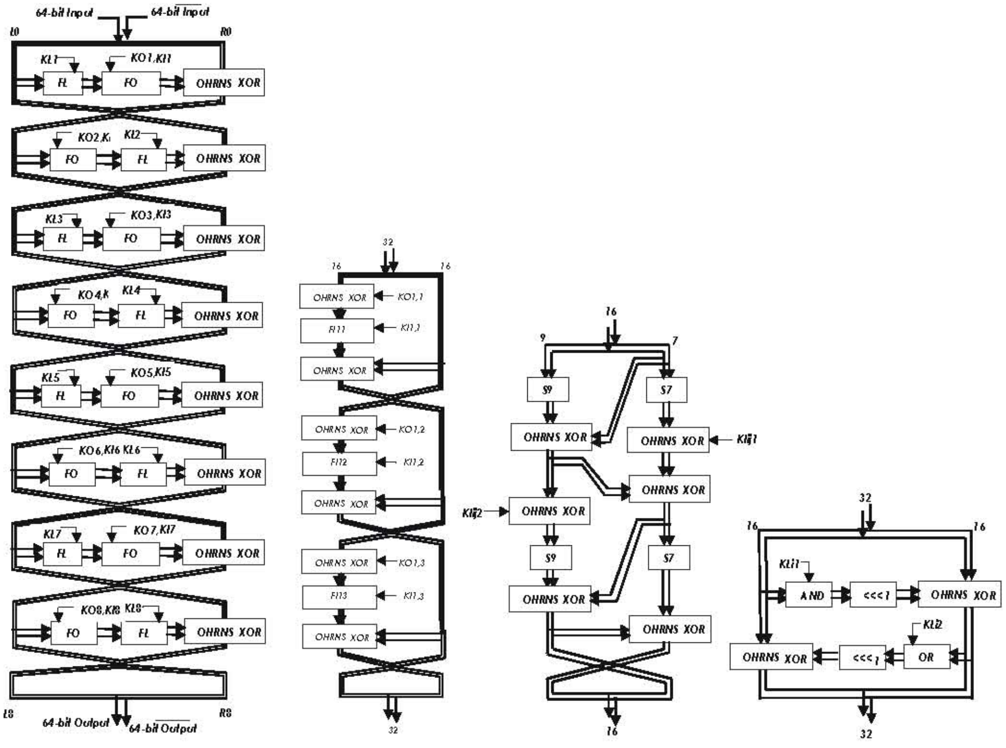
Table 1: Operation of the proposed XOR-XNOR circuit

Input 1 (A)	Input 2 (B)	XOR	XNOR	Function
0	0	0	1	N3 turns ON and XNOR is ACTIVE
0	1	1	0	N2 turns ON and XOR is ACTIVE
1	0	1	0	N4 turns ON and XOR is ACTIVE
1	1	0	1	N1 turns ON and XNOR is ACTIVE

Whereas, the functionality of XOR operation do not change but we propose a new symbol instead of using common XOR gate in many applications that need high-speed and low-power components. The proposed modulo 2 OHRNS XOR is illustrated by Fig. 3. In Fig. 3(a) the each of two inputs is denoted as “data” and “ $\overline{data}$ ” to make the internal operation [Fig. 3(b)] more easily understood. The barrel shifter generates, in parallel, all possible rotations of the data inputs and selects one of them for output. We assume that there are input and $\overline{input}$ (Negative of input) in entrance at the same time for each line of two inputs. In Fig. 3(b) the inner structure of OHRNS XOR is depicted and it shows a rapid XOR–XNOR circuit using four transistors. It generates XOR and XNOR outputs simultaneously but the XOR output is more important in this document. This circuit provides a high speed and low power operations. The proposed XOR–XNOR circuit is based on pass-transistor logic. From the simulation, it can be seen that the XOR and XNOR outputs have a good logic level for input signals (A,B) = (0,0), (0,1), (1,0), (1,1). One of the transistors will be ON when each line of two inputs are active at the same time and the results will be in the actual output.

For example, when (A and $\overline{B}$) or ($\overline{A}$ and B) are driven high simultaneously then the XOR output is active. Thus, in this implementation the propagation is only equal to one transistor delay. While we try to represent a new circuit for computing XOR and XNOR logical gates, Table 1 indicates the functioning of the proposed circuit more clearly. In Fig. 3(b), consider the case when the input vector AB is in state “00”, logic “1” is passed through the nMOS transistor N3 to XNOR output. Then the next input state “01” arrives, the nMOS transistor N2 is ON and XOR output is ACTIVE. In the third input state “10”, logic “1” is went by way of the nMOS transistor N4 to XOR output. Finally, in the fourth input state “11”, XNOR output has logic “1” and the nMOS transistor N1 is ON. These input states repeat perpetually. XOR output is at high impedance state since N2 and N4 are OFF; also it is the same for XNOR output when N1 and N3 are OFF.

Proposed Design of the KASUMI Using Proposed OHRNS XOR: The aim of the proposed circuit is twosome: to direct the needs of high performance and to provide system users and producers with a compact design and small components that has low penalties regarding to delay and power consumption. This section explains the new design of the KASUMI block cipher on the basis of OHRNS that used to achieve the goals. Since it is clarified in the KASUMI algorithm, the main and essential component is XOR logical gate. Therefore if we can improve these XOR gates and increase the performance of XOR computation



a. Feistel structure *b.* FO function *c.* FI function *d.* FL function

Fig. 4: A proposed novel design of the KASUMI block cipher using proposed OHRNS XOR.

in terms of complexity, speed, delay and power; then the KASUMI block cipher will be progressed and finally we will revolutionize cellular communications networks and safety of many wireless standards.

As it was illustrated in the earlier chapter, OHRNS XOR is suitable for applications need high-speed and low-power portions and it is the fundamental reason that we want to use it instead of common XOR gates for above promotion. The beneficial approach imagined for this project is illustrated in Fig. 4. Fig. 4(a) shows the Feistel structure of the KASUMI algorithm using OHRNS XOR instead of XOR gates. In the basic structure of the KASUMI block cipher (Fig. 1(a)) each of symbols contains 32 XOR_2 (2-bit input XOR gate) and the propagation is equal to 1 XOR_2 delay and totally in the eight rounds, there are 8×32=256 XOR_2 hardware with the delay of 8 XOR_2; meanwhile if we use OHRNS XOR in lieu of XOR_2 then the propagation delay decreases to 8 transistors and also hardware reduces. Notice that as we want, the functionality does not change and OHRNS XOR and XOR_2 do the same operation. Consider that the datapath has two lines which mean there are 64-bit inputs and 64-bit $\overline{\text{inputs}}$ (negative of inputs) in entrance of first round simultaneously and it causes increasing of speed. FO, depicted in Fig. 1(b), has 6×16=96 XOR_2 hardware with the propagation delay of 6 XOR_2. Improved FO, see Fig. 4(b), reduces the propagation delay to 6 transistors by using OHRNS XOR. Reformed FI, shown in Fig. 4(c), also has the same delay and hardware like FO. Fig. 4(d) shows that redesigned FL decreases delay from 2 XOR_2 to 2 transistors and we have reduction in hardware too. Thereupon, fundamental changes will occur in many communication networks with using OHRNS XOR instead of usual XOR gate in the KASUMI block cipher.

Simulation Results: All the circuits are extracted using TSMC 0.90-μm technology and simulations are carried out using HSPICE. The circuits performance is evaluated in terms of worst-case delay, power consumption and power-delay product for a supply voltage 1.2V VDD at 50-MHz frequency. The delay is calculated from 50% of voltage level of input to 50% of voltage level of resulting output all the rise and fall output transitions. For the calculation of the power-delay product, worst-case delay is chosen to be the larger delay amongst the two outputs. Toward an accurate result, all the possible input combinations are considered for all the circuits. The PDP is a quantitative measure of the efficiency of the tradeoff between power dissipation and speed. Fig. 5 shows the input stimulus used for the OHRNS XOR. The first four

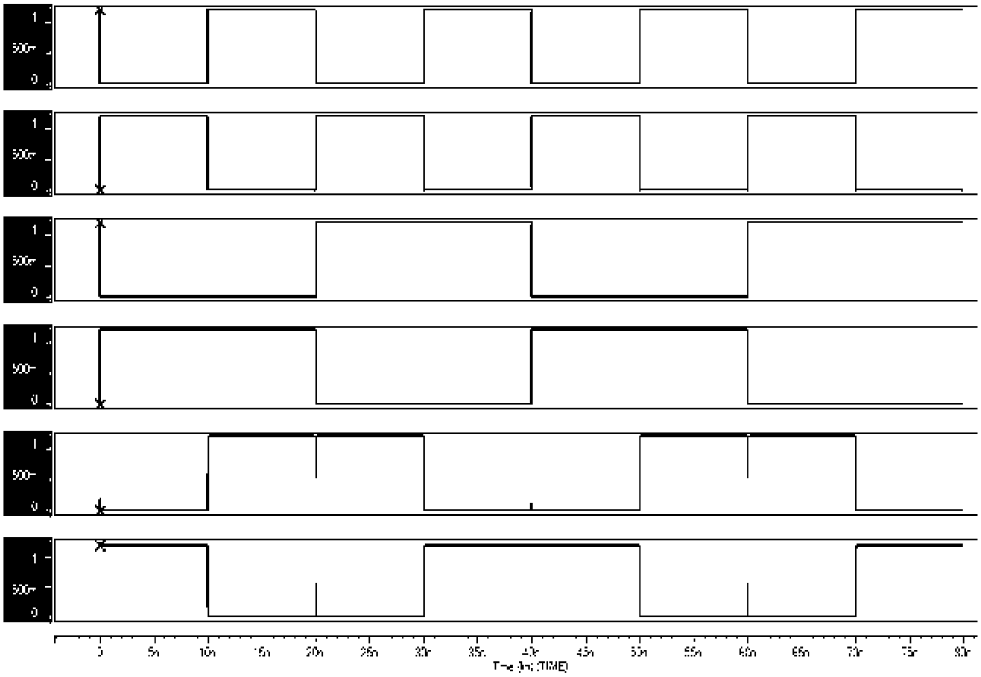


Fig. 5: Input stimulus for OHRNS XOR gate. The first four are inputs A, $\overline{A}$, B, $\overline{B}$ and the remaining two are outputs XOR and XNOR. Frequency of the inputs is 50-MHz with a supply voltage of 1.2-V VDD.

Table 2: Simulation results for proposed OHRNS XOR-XNOR circuit in 0.90-μm technology at 50-MHz frequency and 1.2-V V_{DD}

	Goel *et al.* 2006 [30]	Hassoune *et al.* 2010 [31]	Tien Bui *et al.* 2000 [32]		Rashmi *et al.* 2011 [33]	Proposed circuit
Circuit in:	Figure 6 (c)	Figure 8 (a)	Figure 3 (g)	Figure 3 (e)	Figure 5	
No. of Transistor	8	6	5	4	3	4
Power (nW)	82.91	118.26	56.66	179.41	7544.6	65.70
Delay (ps)	24.85	16.8	24.93	12.43	30006	9.31
PDP (e^{-18})	2.06	1.987	1.413	2.23	226383.268	0.612
Improvement (PDP)	70%	69%	57%	73%	99%	

are inputs A, $\overline{A}$, B, $\overline{B}$ and the remaining two are outputs XOR and XNOR that frequency of the inputs is 50-MHz with a supply voltage of 1.2-V VDD. In Table 2, the simulation environment and experimental results will be shown. By optimizing the transistor sizes of the OHRNS XOR considered, it is possible to reduce the delay without significantly increasing the power consumption and transistor sizes can be set to achieve minimum PDP.

DISCUSSION

The proposed OHRNS XOR circuit was compared to circuits in Goel *et al.* [30], Hassoune *et al.* [31], Tien Bui *et al.* [32], Rashmi *et al.* [33] and for more circuits we can also see Mishra *et al.* [34]. The simulation results at 1.2-V VDD and TSMC 0.90-μm technology are shown in Table II. We consider all the possible input transitions with an output transition at every input transition. The results indicate that the performance of the proposed circuit is better than the performance of the compared circuits. The proposed circuit is 2.7× faster than the circuit in [30] and also consumes low power. This is due to the its structure that is inherently high power consuming but is expected to be lesser than the compared XOR circuits due to the reduced number of transistors. The proposed circuit is 1.8× faster than circuit in [31] and consumes very low power. Owing to the higher speed of our circuit, there is almost 69%–70% saving in PDP in this circuit. The proposed circuit uses only four transistors whereas the circuit in Goel and., 2006 uses 8 and the circuit in Hassoune and., 2010 uses 6 transistors. It is really clear in comparing proposed circuit with other circuits in Table 2.

Since it was demonstrated in the previous section, the proposed OHRNS XOR was utilized for the KASUMI block cipher and the proposed KASUMI circuits were reached the high performance of computation with regard to speed, delay and power consumption. When we only contemplate on the XOR gate in the Feistel structure of the KASUMI block cipher and according to the 8 rounds structures that each round contains 32 2-bit input XOR gate hardware and 1 XOR gate delay, for example in comparison with circuits in [30-31] then the following results are obtained: if it uses XOR circuit in Goel and., 2006 with 8 transistors then the propagation delay is 8×1×8=64 transistors and hardware includes 8×32×8=2048 transistors; if it uses XOR circuit in Hassoune and., 2010 with 10 transistors then delay is 8×1×6=48 transistors and hardware is 8×32×6=1536 transistors; whereas if it utilizes the OHRNS XOR with 4 transistors then the propagation is only equal to 8×1×4=32 transistors delay and also hardware decreases to 8×32×4= 1024 transistors. So the proposed circuit is 2× and 1.5× faster than using the circuit in Goel and., 2006 and Hassoune and., 2010; also there is considerable reduction in the PDP achieved by the proposed circuit. As we can easily observe the increasing of performance in the Feistel structure, so this improvement occurs for the FO, FI and FL functions too.

CONCLUSIONS

System component manufacturers and network users have high hopes about the expansion and utilization of 3rd generation networks in the upcoming years. The KASUMI block cipher is used in many systems and networks of this generation. The main parts of this algorithm are XOR gates. The pass transistor logic is used to efficiently generate the XOR and XNOR functions simultaneously. A novel XOR gate that named “One-Hot Residue Number System XOR” was presented in this paper, along with the results of its simulation in TSMC 0.90-μm technology using HSPICE. Lastly, an efficient and high-speed hardware design of the KASUMI block cipher using OHRNS XOR instead of using usual XOR gate was explained in this document which targets low PDP. It can outperform all the previous published designs. The proposed circuits face the needs of any manufacturer looking for a high performance ciphering circuits which is high-speed and has low power consumption. We recommend the use of OHRNS for the design of high-performance circuits.

ACKNOWLEDGEMENT

The author would like to thank the reviewers for their constructive comments to improve the readability and quality for this paper.

REFERENCES

1. 3rd Generation Partnership Program. 3GPP Home Page. http://www.3gpp.org.
2. Matsui, M., 1997. New Block Encryption Algorithm MISTY. 4th International Fast Software Encryption Workshop, Haifa, Israel: pp: 54-68.
3. Kitsos, P., Y.N. Sklavos and O. Koufopavlou, 2007. UMTS security: system architecture and hardware implementation. Wireless Communications and Mobile Computing, 7: 483–494.
4. 3rd Generation Partnership Program. Document 1: f8 and f9 Specification 35.201, Release 5, Version 5.0.0.
5. 3rd Generation Partnership Program. Document 1: A5/3 and GEA3 Specifications. Technical Specification 55.216, Release 6, Version 6.2.0.
6. 3rd Generation Partnership Program. Document 2: KASUMI Specification. Technical Specification 35.202, Release 5, Version 5.0.0.
7. Nyberg, K. and L. Knudsen, 1995. Provable security against a differential attack. Journal of Cryptology, 8(1): 27-37.
8. Matsui, M., 1996. New structure of block ciphers with provable security against differential and linear cryptanalysis. Fast Software Encryption ’96 Springer-Verlag, 1039: 205-218.
9. Kang, J.S., S.U. Shin, D. Hong and O. Yi, 2001. Provable Security of KASUMI and 3GPP Encryption Mode f8. 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, Springer-Verlag: 3-540-42987-5.
10. Tanaka, H., C. Ishii and T. Kaneko, 2001. On the Strength of KASUMI without FL Functions against Higher Order Differential Attack. Third International Conference on Information Security and Cryptology, Springer-Verlag: 3-540-41782-6.
11. Meier, W. and B. Roy, 2004. New Security Proofs for the 3GPP Confidentiality and Integrity Algorithms. Fast Software Encryption, Lecture Notes in Computer Science, Springer-Verlag.
12. Iwata, T., T. Yagi and K. Kurosawa, 2008. Security of the Five-Round KASUMI Type Permutation. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences archive, 91-A(1).
13. Biham, E., O. Dunkelman and N. Keller, 2005. A Related-Key Rectangle Attack on the Full KASUMI, Advances in Cryptology, Lecture Notes in Computer Science, 3788: 443-461.

14. Kim, J., S. Hong, B. Preneel, E. Biham, O. Dunkelman and N. Keller, 2010. Related-Key Boomerang and Rectangle Attacks, IACR ePrint report 2010.
15. Dunkelman, O., N. Keller and A. Shamir, 2010. A Practical-Time Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony. 30th annual conference on Advances in cryptology Springer-Verlag Berlin: 3-642-14622-8 978-3-642-14622-0.
16. Nedjah, N., L.M. Mourelle and M.P.M Araujo, 2011. Quantum-inspired design of resilient substitution boxes: From coding to hardware implementation. Applied Soft Computing, 11(7).
17. Hosseinzadeh, M., K. Navi and S. Timarchi, 2006. Design Residue Number System Circuits in Current mode. 14th Iranian Conference of Electrical Engineering.
18. Chren, W.A., 1998. One-Hot Residue Coding for Low Delay-Power Product CMOS Design. IEEE Transactions On Circuits And Systems II: Analog And Digital Signal Processing, 45(3).
19. Hurst, S.L., 1984. Multiple-Valued Logic - Its status and its future. IEEE Transaction on Computers, pp: 1160-1179.
20. Gonzalez, A.F. and P. Mazumdar, 2000. Redundant Arithmetic, "Algorithms and Implementations". Integration: The VLSI Journal, 30(1): 13-53.
21. Noorimehr, M.R., M. Hosseinzadeh and R. Farshidi, 2010. A new four-moduli set with high speed RNS arithmetic unit and efficient reverse converter. IEICE Electronics Express, 7(20): 1584-1591.
22. Hosseinzadeh, M., M.A. Sabbagh and K. Navi, 2008. An improved reverse converter for the moduli set {2^n-1, 2^n, 2^n+1, 2^{n+1}-1}. IEICE Electronics Express, 5(17): 672-677.
23. Bajard, J.C. and L. Imbert, 2004. A Full Implementation RSA in RNS. IEEE Transactions on Computer, pp: 53(6).
24. Ramirez, J., 2002. Fast RNS FPL-Based Communications Receiver Design and Implementation. 12th Int'l Conf. Field Programmable Logic, pp: 472-481.
25. Krishna, H., K.Y. Lin and J.D. Sun, 1992. A coding theory approach to error control in redundant Residue Number Systems - Part I: theory and single error correction. IEEE Transactions Circuits Systems, 39: 8-17.
26. Sun, J.D. and H. Krishna, 1992. A coding theory approach to error control in redundant Residue Number Systems -Part II: multiple error detection and correction. IEEE Transaction Circuits Systems, 39: 18-34.
27. Parhami, B., 2001. RNS Representation with Redundant Residues. 35th Asilomar Conference on Signals Systems and Computers, Pacific Grove CA, pp: 1651-1655.
28. Hanzawa, S., T. Sakata, K. Kajigaya, R. Takemura and T. Kawahara, 2005. A Large-Scale and Low-Power CAM Architecture Featuring a One-Hot- Spot Block Code for IP-Address Lookup in a Network Router. IEEE Journal of Solid-State Circuits, 40(4).
29. Chren, W.A., 1999. Delta-Sigma Modulator with Large OSR Using the One-Hot Residue Number System. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 46(8).
30. Goel, S., A. Kumar and M.A. Bayoumi, 2006. Design of Robust, Energy-Efficient Full Adders for Deep-Submicrometer Design Using Hybrid-CMOS Logic Style. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 14(12).
31. Hassoune, I., D. Flandre, I. O'Connor and J.D. Legat, 2010. ULPFA: A New Efficient Design of a Power-Aware Full Adder. IEEE Transactions on Circuits and Systems I: Regular Papers, 57(8).
32. Tien Bui, H., A.K. Al-Sheraidah and Y. Wang, 2000. New 4-Transistor XOR and XNOR Designs. The Second IEEE Asia Pacific Conference on ASICs, pp: 7803-6470.
33. Rashmi, S.B., B.G. Tilak and B. Praveen, 2011. Transistor Implementation of Reversible PRT Gates. International Journal of Engineering Science and Technology, 3(3): 0975-5462.
34. Mishra, S.S., A.K. Agrawal and R.K. Nagaria, 2010. A comparative performance analysis of various CMOS design techniques for XOR and XNOR circuits. International Journal on Emerging Technologies, 1(1): 0975-8364.