International Journal of Engineering & Technology, 7 (3) (2018) 1888-1892

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i3.14138
Research paper

Review on lightweight hardware architectures for the crypt-analytics in FPGA

Sunitha Tappari [1] *, K. Sridevi [2]

[1] G. Narayanamma institute of Technology and science
[2] GITAM University
**Corresponding author E-mail: sunitha.tappari@gmail.com*

Abstract

Internet of Things (IoT) plays a vital role in the Wireless sensor networks (WSNs), which is used for many applications, such as military, health, and environmental. Security is the major concern and it is very difficult to achieve because of a different kind of attack in the network. In recent years, many authors have introduced different Hardware Architectures to solve these security problems. This paper has discussed about a review of various Hardware Architectures for the lightweight Crypt-analytics methods and the comparative learning of various Crypt-analytics and authentication systems carried out. The comparative study result showed that the lightweight algorithms have good per-formance compared to the conventional Crypt-analytics algorithm in terms of memory requirement, operations, and power consumption.

Keywords: *Use About Five Key Words or Phrases in Alphabetical Order; Separated by Semicolon.*

1. Introduction

With an ever-growing world of technology and communication, the amount of information shared with the rest of the digital universe is constantly increasing. The IoT is a method of interrelated computing devices like digital machines, mechanical machine and objects. All these things contain some unique identifiers, which converted into digital data and transfer the data through the inter network (Net) without any human interaction [1]. IoT provides different kind of facilities such as automation, controlling the sensors, cameras, actuators, etc. [2]. Nowadays, most of the application development and research depend on IoT. WSNs are one of the major parts of the IoT technology and it used for IoT requests [3]. WSN extensively used to monitor the real-time ecological factors like humidity, pressure, sound, temperature, etc. The ecological factors collected and transmitted (wirelessly) to a sink node [4]. The Information-security and the IoT cloud distribute those risks to the conventional Internet, which is the major limitation of the IoT and WSN [5].

The major reasons for the limitation is the large amount of sensitive data on the Net such as financial, military, health care, etc., The computing devices in the Net has limited computational capabilities which are more vulnerable to the physical attacks. These limitations considered while designing the privacy and security solutions of an IoT [5]. Subsequently typical devices in IoT (i.e., sensor nodes in a WSN) are prepared with lower end micro-controllers with small dimensions and slow oscillators, software-friendly lightweight primitives require. However, the representative devices in IoT has the RFID tags that do not have a software-programmable processor, requires realizing a Crypt-analytics-based resolution only through hardware implementations. The security improvements over software solutions provided by hardware-based Crypt-analytics solutions [7]. Crypt-analytics classified into two different types such as Asymmetric and Symmetric [8]. Symmetric Crypt-analytics also named as shared key Crypt-analytics. In this mechanism, the sender and Receiver shares a common Key for both Encryption (Ecy) and Decryption (Dcy) [9]. The asymmetric Crypt-analytics are also named as as Public Key (PK) Crypt-analytics. In this technique, the source uses a PK of the destination for Ecy and the destination of PK used for decrypting the Message (MSG). The concept of self-certification is absent here instead Digital Signatures (DS) used to certify the Key. This method is more convenient and provides better authentication. Most of the constrained devices requires Shared Key Crypt-analytics, because of its nature of operations [11].

The paper organized as follows. Section II provides a brief description of the Crypt-analytics Mechanism. Section III focus on shared key and public key crypt-analytics. Section IV discussed about Comparative analysis of recent technique and its performances. In section, V gives a summary of this paper.

2. Crypt-analytics mechanism

Crypt-analytics is a strategy for putting away and transmitting information in a specific frame, at the time of receiving receiver can read and process it. Usually the scrambling Plain text (PT) MSG converted into cipher-text by using some Key values; this process named as Ecy. Inverse process of Eny is Dcy. There are three sorts of Crypt-analytics plans: mystery Key (or shared Key) Crypt-analytics, open Key (or hilter kilter) Crypt-analytics and hash works those commonly used to achieve these objectives.

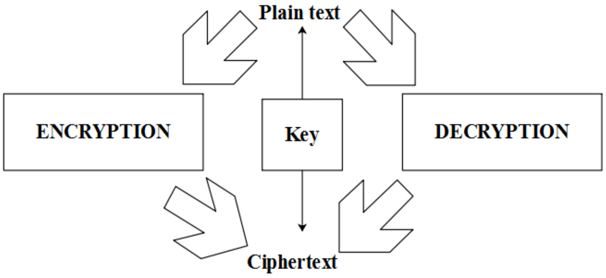

Fig.1: Crypt-Analytics Mechanism.

2.1. Key

A Key is a numeric or alphanumeric manuscript or may be a unique figure.

2.2. Plain text

The information that the person need to convey called as PT. For instance, a man named Alice wishes to send "Hello dear" MSG to the individual Bob. Here "Hello dear "is a plain instant MSG.

2.3. Cipher text

The PT MSG converted into any one or an aimless MSG, the aimless message named as Cipher content or Cipher Text. For example, consider, "Azx143@qz12+124" is a Cipher Text (CT) created for "Hi Friend how are you". CT otherwise named as scrambled or encoded data. The encoded data is unpredictable by a human or machine without the correct Key to unscramble it. So that Decoding process is required, Decoding is the inverse process of encoding where the encoded data have converted into the PT MSG.

2.4. Encryption

Ecy is a procedure of changing PT into CT. This procedure requires two major things such as Ecy calculation and a Key.

2.5. Decryption

A turn around procedure of Ecy named as Dcy. In this procedure, Cipher content changed into PT. Decoding process requires two things such as unscrambling calculation and a Key.

3. Shared key and public key crypt-analytics

There are commonly two types of techniques are used for Crypt-analytics such as PK Crypt-analytics and shared key Crypt-analytics which has been discussed in the [12-13]. Some of the PK Crypt-analytics and shared key Crypt-analytics defined below.

3.1. Data encryption standard (DES)

R.Davis introduced the DES Encryption Standard. DES is a block cipher algorithm which consist of 64-bit blocks and 56-bit Key [15]. DES is a fixed-length string of PT bits and transforms it through a series of complicated operations into CT bit string of the same length. 3-DES [16] is an up-gradation of DES, which consist of 64-bit block size for 192 bits Key size. The basic block diagram of the DES shown in Figure 2.

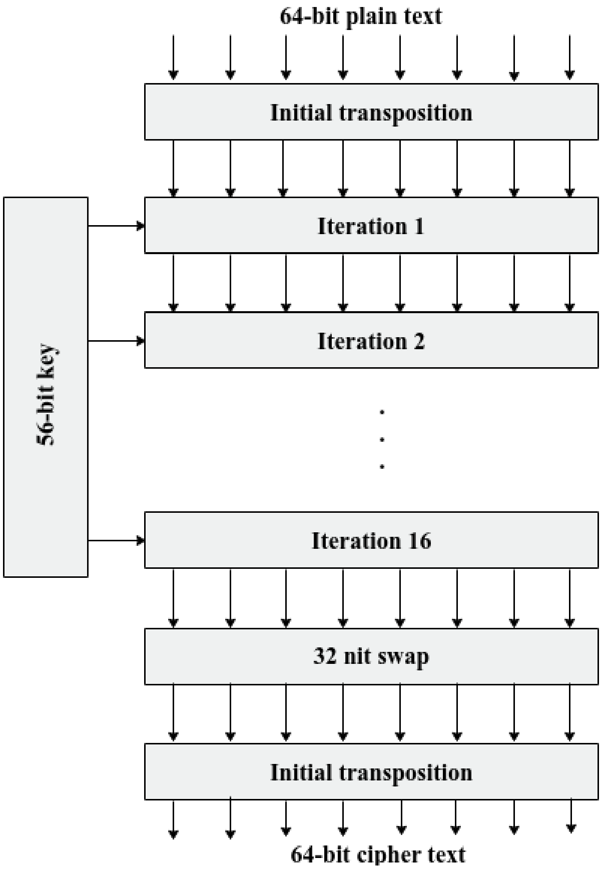

Fig. 2: Block Diagram of Data Encryption Standard.

3.2. Advanced encryption standard (AES)

AES [17] is a block cipher intended to replace the DES for commercial applications. It uses a Key size of 128, 192 or 256 bits and a 128-bit block size. The number of internal rounds of the cipher is a function of the Key length. The number of cycles for 128-bit Key is 10. Unlike its predecessor DES, AES does not use a Feistel Net. Feistel Nets do not encrypt an entire block per cycle, e.g., in DES, $\frac{64}{2} = 32$bits encrypted in one round. AES, on the other hand, encrypts all 128 bits in one iteration. The basic block diagram of the AES showed in Figure 3.

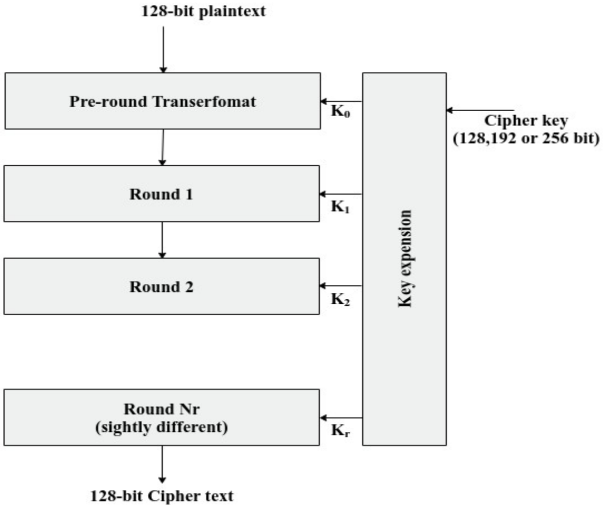

Fig. 3: Block Diagram of Advanced Encryption Standard.

3.3. Blowfish

Bruce Schneier introduced the Blowfish algorithm, which consist of 64-bit block cipher larger data catches. Compared to DES, Blowfish is significantly faster in Pentium machine. The key length of the Blowfish varies from 32 to 448 bits. One entry of the P-array is used at each round, after completing the final round; each half of the information block is XOR ed with one of the two remaining unused P-entries. The basic structure of Blowfish shown in figure 4.

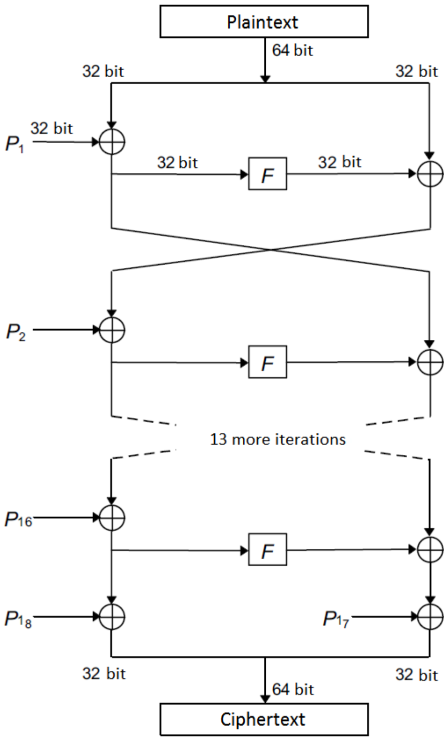

Fig. 4: Block Diagram of Blowfish.

3.4. Rivest–shamir–adleman (RSA)

Ronald Rivest et al. [18] have done the first, and still most common, PK Crypt-analytics implementation. Presently RSA used in hundreds of software products and used for Key exchange, DS, or Ecy of data. Variable size (VS) Ecy block and a VS Key used in the RSA. The large n, number derived as a Key-pair, which is a product of two prime numbers, according to the special rules; these primes may be 100 or more digits in length each, yielding n with roughly twice as many digits as the prime factors. The RSA consist of three phases such as Key Generation, Ecy, and Dcy.

3.4.1. Algorithm

Two prime numbers x and y are generated using the RSA Crypt-analytics. A modulus n calculated by multiplying p and q. The number used by both private and public keys provides the link among the users. The user sends PT to the encrypted public key.

Key Generation	
Select p, q p, q both are prime $p \neq q$	
Calculate n = pxq	
Calculate $(n) = (p-1)x(q-1)$	
Select integer e $gcd(\ (n), e) = 1; 1 < e < \ (n)$	
Calculate d	
Public keyKU ={e, n}	
Private keyKR={d, n}	
Encryption	Decryption
Plain text M< n	Cipher text C
Cipher text $C = M^e (modn)$	Plain text $M = C^d (modn)$

3.5. Elliptic curve crypt-analytics (ECC)

ECC is an analogy of Hellman Key Exchange. It is a elliptic curves (EC)) based Crypt-analytics PK algorithm [19]. EC arithmetic used for different Crypt-analytics. The coefficients and variables in the eqn are elements of a finite field. Security of ECC is based on the intractability of ECDLP i.e. EC Unconnected Logarithm Difficulty. The basic Block diagram of ECC showed in figure 5.

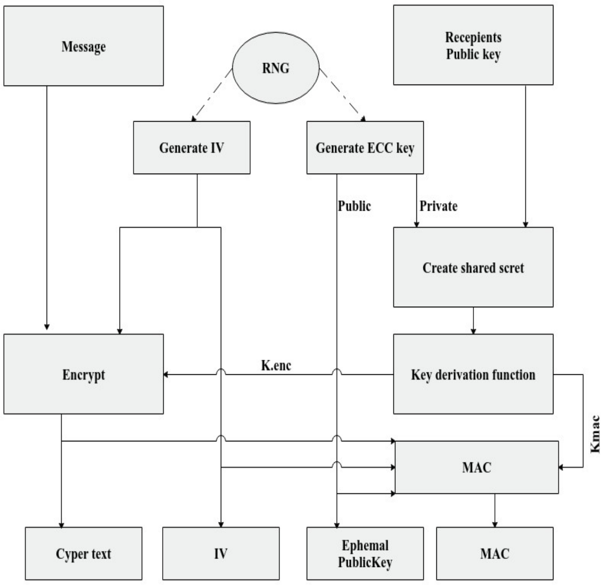

Fig. 5: Block Diagram of Elliptic Curve Crypt-Analytics.

3.6. Present cipher

PRESENT lightweight cipher is a shared key block cipher introduced in 2012 by ISO/IEC as "[block cipher] [20]. The cipher based on a Substitution-Permutation Net (SPN), with a round-based processing system. PRESENT supports 64-bit input data blocks and Key sizes of 128 and 80-bits. The key materials are generated using hardware primitives such as Physical Un-clonable Functions for improving the security of hardware implementations [21-23]. In PRESENT, the state is a 1-D array of 64 bits that supports shift operations and parallel access over the data. The input Key processed internally to generate a round Key for each of the 31 total rounds. The cipher uses three basic operations over the state, which is a structure that contains the PT and modified in each round to produce confusion and diffusion over the data.

3.6.1. Add round key

Add Round Key adds the state to 64-bit word from the round Key using finite field arithmetic.

3.6.2. S-box layer

S-box consists of 4 to 4-bit subtraction, here with 16 values.

3.6.3. P-layer

P-layer also known as bit level shifts (because of the level shifting) for a clear specification of the PRESENT, the reader could refer to [21].

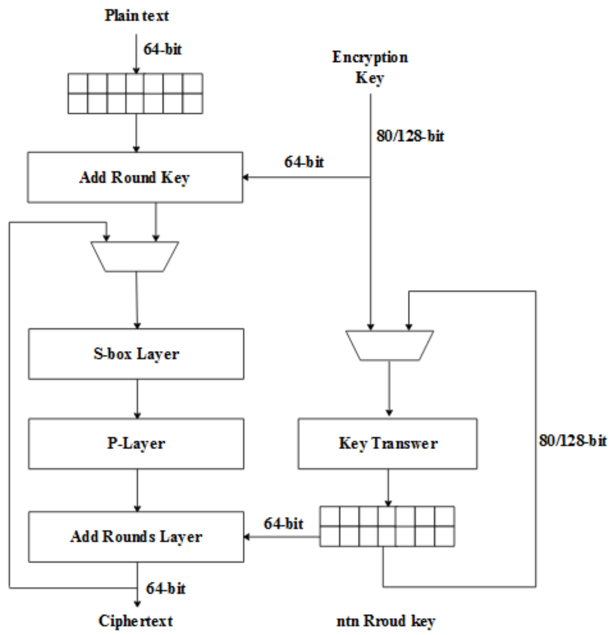

Fig. 6: The Present Block Diagram of Cipher.

The PRESENT block diagram showed in Fig. 6 that closely follow its algorithm specification. This design directly derived from the algorithm specification and the latency is equivalent to the number of cycles.

4. Comparative analysis of recent technique and its performances

Table 1: Comparison of Existing Methods

Author and Publication	Methodology	Key Size (bit)	Power (µW)	Area	Throughput At 100Khz (Kbps)	Advantage	Attacks
Zhang, et al. [22]	RECTANGLE	128	1.78	1787	246	Low cost efficient.	Related key attack
Kushwaha, et al. [23].	TWINE	128	1.30	1866	178	Efficient for small hardware architecture	Saturation attacks
J.H. Park [24]	Speck	128	--	2500	__	Low-cost Ubiquitous Computing Devices and Applications	rectangle attack
De Canniere, et al. [25].	KATAN	80	--	1054	--	More flexible	middle attacks
De Canniere, et al. [25]	KTANTAN	80	--	688	--	More compact in hardware	middle attacks
T. Eisenbarth, and S. Kumar	Present	80	--	11,970	--	Low cost efficient.	--
Hocquet et al. [10].	AES	128	0.25	--	--	Minute power budget	--
Andreeva et al. [6].	DM-PRESENT	64	1.83	2213	--	A compact hash function	--
Andreeva et al. [6].	DM-PRESENT	128	2.94	1886	--	Compact hash function	--

5. Conclusion

In present days, the growth of Net and data security has become the major concern in an organization. In this paper, a survey of various Hardware Architectures for the lightweight Crypt-analytics methods and the comparative survey of various Crypt-analytics and authentication systems carried out. The comparative study result showed that the lightweight algorithms have good fulfillment compared to conventional Crypt-analytics algorithm in terms of memory requirement, operations, and power consumption. Lightweight algorithms also have some issues such as architectures, security, and privacy that taken to solve them. Scopes for further research include the extension of this work towards more algorithms and the addition of countermeasures against physical attacks.

References

[1] A. Passi, and D. Batra, "Future of internet of things (IoT) in 5G wireless networks", *International Journal of Engineering & Technology*, Vol.7, No.1.5, pp.245-248, 2017.

[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities", IEEE Internet of Things journal, Vol.1, No.1, pp.22-32, 2014.

[3] Fan, F.R., Lin, L., Zhu, G., Wu, W., Zhang, R. and Wang, Z.L., 2012. Transparent triboelectric nanogenerators and self-powered pressure sensors based on micropatterned plastic films", *Nano letters*, Vol.12, No.6, pp.3109-3114. https://doi.org/10.1021/nl300988z.

[4] C. Baskar, C. Balasubramaniyan, and D. Manivannan, "Establishment of light weight cryptography for resource constraint environment using FPGA", *Procedia Computer Science*, Vol.78, pp.165-171, 2016. https://doi.org/10.1016/j.procs.2016.02.027.

[5] C.A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Lightweight hardware architectures for the PRESENT cipher in FPGA", *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol.64, No.9, pp. 2544-2555, 2017. https://doi.org/10.1109/TCSI.2017.2686783.

[6] E. Andreeva, B. Mennink, and B. Preneel, "Security Properties of Domain Extenders for Cryptographic Hash Functions", *JIPS,* Vol. 6, No. 4, pp. 453-480, 2010. https://doi.org/10.3745/JIPS.2010.6.4.453.

[7] C.J. McIvor, M. McLoone, and J.V. McCanny, "Hardware Elliptic Curve Cryptographic Processor Over $ rm GF (p) $", IEEE Transactions on Circuits and Systems I: Regular Papers, Vol. 53, No.9, pp.1946-1957, 2006. https://doi.org/10.1109/TCSI.2006.880184.

[8] M. Agrawal, and P. Mishra, “A comparative survey on symmetric key encryption techniques”, *International Journal on Computer Science and Engineering*, Vol.4, No.5, pp. 877, 2012.

[9] R. Terec, M.F. Vaida, L. Alboaie, and L. Chiorean, “DNA security using symmetric and asymmetric cryptography”, *International Journal of New Computer Architectures and Their Applications (IJNCAA),* Vol.1, No.1, pp.34-51, 2011.

[10] C. Hocquet, D. Kamel, F. Regazzoni, J.D. Legat, D. Flandre, D. Bol, and F.X. Standaert, “Harvesting the potential of nano-CMOS for lightweight cryptography: an ultra-low-voltage 65 nm AES coprocessor for passive RFID tags”, *Journal of Cryptographic Engineering*, Vol.1, No. 1, pp.79-86, 2011. https://doi.org/10.1007/s13389-011-0005-z.

[11] T. Eisenbarth, and S. Kumar, “A survey of lightweight-cryptography implementations”, *IEEE Design & Test of Computers,* Vol. 24, No. 6, pp. 522 - 533, 2007. https://doi.org/10.1109/MDT.2007.178.

[12] J. Thakur, and N. Kumar, “DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis”, *International journal of emerging technology and advanced engineering*, Vol.1, No.2, pp.6-12, 2011.

[13] R. Davis, “The data encryption standard in perspective”, *IEEE Communications Society Magazine*, Vol.16, No.6, pp.5-9, 1978. https://doi.org/10.1109/MCOM.1978.1089771.

[14] E. Barker, “SP 800-67 Rev. 2, Recommendation for Triple Data Encryption Algorithm (TDEA) Block Cipher”, *NIST special publication*, Vol.800, pp.67, 2017.

[15] S. Heron, “Advanced encryption standard (AES)”, *Network Security,* Vol.2009, No.12, pp.8-12, 2009. https://doi.org/10.1016/S1353-4858(10)70006-4.

[16] R.L. Rivest, A. Shamir, and L. Adleman, “A method for obtainin digital signatures and public-key cryptosystems”, *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1978. https://doi.org/10.1145/359340.359342.

[17] N. Koblitz, “Elliptic curve cryptosystems”, *Mathematics of computation*, Vol. 48, No. 177, pp. 203-209, 1987. https://doi.org/10.1090/S0025-5718-1987-0866109-5.

[18] M.O.J.T.A.B.A. Alizadeh, M. Salleh, M. Zamani, J. Shayan, and S. Karamizadeh, “Security and performance evaluation o lightweight cryptographic algorithms in RFID”, In *16th WSEAS International Conference on Communications (part of the 16th CSCC / CSCC 2012),* Kos Island, Greece. July 14-17, 2012.

[19] T. Addabbo, A. Fort, M.D. Marco, L. Pancioni, and V. Vignoli, “Physically unclonable functions derived from cellular neural networks”, *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 60, No. 12, pp. 3205-3214, 2013. https://doi.org/10.1109/TCSI.2013.2255691.

[20] Y. Cao, L. Zhang, S.S. Zalivaka, C.H. Chang, and S. Chen, “CMOS image sensor based physical unclonable function for coherent sensor-level authentication”, *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 62, No. 11, pp. 2629-2640, 2015. https://doi.org/10.1109/TCSI.2015.2476318

[21] M. Wan, Z. He, S. Han, K. Dai, and X. Zou, “An invasive-attackresistant PUF based on switched-capacitor circuit”, *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 62, No. 8, pp. 2024-2034, 2015. https://doi.org/10.1109/TCSI.2015.2440739.

[22] W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, and I. Verbauwhede, “RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms”, *Science China Information Sciences*, Vol. 58, No. 12, pp. 1-15, 2015. https://doi.org/10.1007/s11432-015-5459-7.

[23] P.K. Kushwaha, M.P. Singh, and P. Kumar, “A Survey on Lightweight Block Ciphers”, *International Journal of Computer Applications*, Vol.96, No.17, 2014.

[24] J.H. Park, “Security analysis of mCrypton proper to low-cost ubiquitous computing devices and applications”, *International Journal of Communication Systems,* Vol. 22, No. 8, pp. 959-969, 2009. https://doi.org/10.1002/dac.1008.

[25] C. De Canniere, O. Dunkelman, and M. Knežević, “KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers”, In *Cryptographic Hardware and Embedded Systems-CHES 2009*, pp. 272-288. Springer, Berlin, Heidelberg, 2009. https://doi.org/10.1007/978-3-642-04138-9_20.