Mahesh Tubaki. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 12, Issue 11, November 2022, pp. 118-123

RESEARCH ARTICLE OPEN ACCESS

The Effectiveness of Different Lightweight Block Cipher FPGA (KASUMI) Architectures: A Review

Mahesh Tubaki *
*Electronics and Communication Engineering **
*Government Polytechnic Belagavi **
*Maheshtubaki1@gmail.com **

ABSTRACT
There are networks everywhere on the globe and in every living thing's brain. Transport networks may be seen on city streets, and water pipe networks can be seen inside of homes and businesses. And in the era of digital information, we can observe the development of mobile and computer networks as well as their yearly upgrades. We need networks to efficiently share resources, and since data may represent knowledge and information in the form of text, speech, picture, or video, it is the most important resource that humans can exchange through time and between generations. We give a brief introduction of network creation and IoT applications in this article. We also highlight the security risks facing these generations.

Keywords:FPGA, Lightweight, Block Cipher, XXTEA,RoadRunnerR, AES, KASUMI

I. INTRODUCTION

In the past, communication equipment like actuators and sensors did not need to be encrypted. End-to-end communication must be confidential. Since the information gathered might be utilized by a burglar to decide, for example, the optimal time to break into to the home, data received from smart metres can detect the occupancy of a residence [1][2]. Most sensors and actuators still only have basic hardware. As a result, in recent years, several academic papers proposing lightweight cryptography have concentrated on developing the algorithms for this type of encryption. Lightweight encryption is therefore encryption that has been specifically designed for implementation in constrained environments [3].

In the present digital era, all it takes is a single click to make data available everywhere and available for future generations to access for an unlimited amount of time without any physical work. [5] For instance, GitHub is keeping a backup of open-source project source code in the **Frozen Arctic in 2020** so that it will be available 1,000 years from now, even if a nuclear holocaust occurs [6].

The actual power of networking and resource sharing in the modern day is made possible by mobile networks and various routing protocols, but this has also greatly increased the security issues. This study examines the development of mobile networks from the first to the sixth generation and focuses on the security issues posed by 6G Internet of Things applications [7].Algorithms from lightweight cryptography are available for use in IoT-based healthcare systems. These cryptographic primitive people have straightforward computing requirements, which enables them to be space and power effective. Their hardware solutions are ideal for a variety of health applications that either focus on low-area or high throughput and are frequently used for IoT systems. The trade-off between these implementational characteristics and the equilibrium state of hardware technology is more significant in other healthcare situations.

Because of the reduction in computational complexity relative to the more well-known heavy cryptographic approaches, hardware of lightweight algorithms has a disadvantage in terms of security. This may be characterized as a hardware constraint in the IoT context, where the efficiency and hardware characteristics of the used resource-constrained devices are strongly correlated with the lack of high-level security. However, this does not change the fact that, despite the hardware constraints, these lightweight solutions can nonetheless offer effective security and partially satisfy the requirements for a reliable e-healthcare system. These hardware restrictions can be overcome by the effective and adaptable architecture of a lightweight algorithm with perhaps extra security components that improve the primary security principles, namely secrecy, integrity, and availability.

RELATED WORK

The Internet-of-Things (IoT) era has significantly increased both the number of linked devices and the amount of data that is exchanged between them. In addition to increasing in quantity, these devices' computational power also rises yearly, while their size and cost decline. Concern over users' security and privacy is raised by the increase in the volume of communications sent that contain the widest range of information [7]. Therefore, suitable information security methods are being researched and created for this novel situation. It has been demonstrated that developing a safe and efficient ciphering technique is required to guarantee consistency [8].Various FPGA boards were used to implement and use the idea of lightweight cryptography. It is easy to show that the present algorithms for cypher blocks have enhanced throughput, make more effective use of hardware logic resources, and are more resistant to the bulk of cryptanalysis attacks by comparing the algorithms to prior work [9].

To get over these problems, the Extended Tiny Encryption Algorithm (XTEA), which at the time was thought to be the fastest encryption algorithm with the least amount of operation code and the simplest block cypher, was developed. The XTEA is a Lightweight Block Cipher (LWBC) having 64 rounds of encryption and decryption, a 64-bit block size (Plain Text), and a 128-bit key size. It operates as a Feistel structure. To meet the needs of contemporary security, the key size is enough. The four 32-bit wide components of the 128-bit Key, K0, K1, K2, and K3, carry out both the encryption and decryption processes [10].

The PRESENT algorithm, a symmetric encryption technique, was introduced by the authors at [11]. The PRESENT technique is also known as the substitution permutation network (SPN), which has two possible key sizes: 80 or 128 bits and a block size of 64 bits. From this point, it was referring to two renditions: one with a 128-bit key called PRESENT-128 and the other with an 80-bit key called PRESENT-80. There are 31 ordinary rounds in the PRESENT algorithm, and the last round solely consists of the crucial error phase. A key blundering step, a substitution layer, and a permutation layer make up a normal round.

Furthermore, **(Biswas et al. 2020)** proposed a set of new standards for comparing block cyphers equally. The LRBC has improved security by combining the structural benefits of the substitution-permutation network (SPN) and **feistel** structure (FN). As a result, the lengthy plaintext bit was divided into many blocks, each of which had 16 bits of data. These blocks were then processed using a data route, and the same steps would be repeated for subsequent data blocks. The results of processing all the data blocks were combined to create the final encrypted text.The lightweight resource-constrained block cypher approach with a single, easy-to-understand phase was built using the four keys, each of which has a 4-bit length. The feistel structure often requires a lot of rounds and only uses half the block. The SPN structure employs a confusion and diffusion approach that boosts plaintext redundancy and verifies a heavily encrypted ciphertext. In contrast to applying those tactics separately, the combination of these two structures has produced a system that is better protected. Storage, power, memory, and performance limitations are the primary design considerations for lightweight encryption algorithms [12].

The underlying design of the symmetric block cypher LED, which has a block size of 64 bits, is based on the reformat network (SPN). Based on key size, it is created in two versions: 64-bit key (LED-64) and 128-bit key (LED-128). The amount of the encryption key determines how many rounds it has; LED-64 has 32 rounds, while LED-128 has 48 rounds [13].

The 64-bit blocks are encrypted with a 256-bit key using the GOST lightweight block cypher algorithm, which has a structure like the DES method. It features a **Fiestal** network topology and 32 rounds of iterative encryption for the data. Due to the lengthy calculation required by encryption methods, real-time and quick algorithms were developed. Decryption is completed in 32 rounds, after which plain text is created. As an alternative to the DES algorithm, GOST methods have been created [14].

A 64-bit, lightweight block cypher algorithm, the **mCrypton algorithm** uses cryptography. It has a Substitution Permutation (SP) structure that is utilized in the architecture design of the mCrypton algorithm. The algorithm is divided into three categories, mCrypton-64, mCrypton-96, and mCrypton-128, based on the size of the key. The method primarily consists of five distinct processes: nonlinear substitution, bit permutation, row-to-column transposition, key scheduling, and key addition. Wireless sensor networks (WSNs), the Internet of Things (IoT), and RFID tags are just a few unimportant or invisible gadgets that might gain from lightweight cryptography [15].

The Corrected block TEA algorithm, also known as the XXTEA algorithm, was created to enhance the security features of the TEA family of cyphers. This algorithm uses an imbalanced feistel network and is a feistel block cypher. It supports variable-length plain text and requires a minimum block size of 64 bits. XXTEA uses keys that are 128

bits in size. Simple addition, shift, and XOR operations are used by XXTEA. Modulo 32-bit addition is used for the addition. It makes use of a nonlinear function to enhance the cipher's security and confusion properties. It is more efficient and convenient to work on larger lot size plain texts because of the ability to deal with variable length plain text [16].

TYPES OF BLOCK CIPHER

In this section, we give a concise overview of each block cypher that has been used from the design standpoint (without going into detail into the key schedule) and the cryptanalytic perspective, restricting our state-of-the-art to the case of known key settings and corresponding key settings [17].

AES:Because of their great speed and compactness, KASUMI designs, which are run on the FPGA Xilinx Vertex 7, are advised for wireless applications. Using CSB for S9/S7 and less combinational logic, the FI function was optimized, resulting in a reasonably short KASUMI implementation. A highly optimized pipeline structure for high-speed deployments effectively boosted throughput and efficiency with important route savings. These designs are perfect for wireless communication networks. The block cypher KASUMI is utilized in mobile communications systems including UMTS, GSM, and GPRS. The KASUMI algorithm is used by the UEA1 and UIA1 secrecy (f8) and integrity (f9) algorithms in UMTS [19]. The KASUMI block cypher, which has not yet been broken, is an advantage of this architecture.Many efforts have been made and are still being made to produce an efficient hardware implementation for cryptographic cyphers like KASUMI since the bulk of identifying systems today require small-size hardware cyphers. The disadvantage of KASUMI is that, despite the specification's acceptance of a 128-bit key, there are some situations in which the key length must be reduced. To prevent fault injection, the final two rounds of the KASUMI application should be carefully designed [20].

XXTEA:A straightforward, adaptable hardware design that involves fewer computations and makes key scheduling simpler is the foundation of the Tiny Encryption Algorithm (TEA). To counter security threats in key scheduling on TEA, an Extended TEA (XTEA) is developed with pipelined design and parallel computing to boost throughput and provide stronger security. This XTEA algorithm can be changed to perform encryption or decryption in a different way. The TEA and XTEA simulation results are implemented using the Xilinx ISE tools on the ModelSim (6.5f) simulator on the FPGA Platform-Artix-7.

The XXTEA technique works with a 128-bit key and an array of 32-bit integers (at least two integers), but it doesn't explain how to convert between array and bits. As a result, several XXTEA implementations can work together. In this approach, the conversions among bites and array are handled by the longs2bytes and bytes2longs functions. These measures make it possible to encrypt every binary byte, regardless of length, as well as messages. The input bytes are padded to multiples of 4 bytes (the size of a 32-bit integer) and are at least 8 bytes long. One advantage of this design is that it is compatible with wireless systems. For FPGA or reconfigurable devices, hardware approaches for XXTEA implementation have limitations that may be established.An FPGA system offers the highest encryption rate, but flexibility is sacrificed. Even small circuit modifications require a completely new circuit layout [16].

ROADRUNNERR: With a key length of 128 bits, 64-bit text, and a total of 12 or 10 rounds, depending on the key size, Roadrunner is a balanced Feistel-based network that supports 128/80-bit keys. The encryption is especially made to have a very short code size, the least amount of delay, a high throughput, and shown security, as indicated by the least number of active S-boxes in differential and linear trails. Implementations of the RoadRunneR architecture have been made using data-path sizes of 8 bits, 16 bits, and 32 bits. All these data-path designs are evaluated using a variety of criteria, such as energy usage, throughput, the quantity of GEs and LUTs required, efficiency, clock cycles, and latency.It is small, rapid, and secure against several cryptographic attacks. It is also well optimized for software implementation [11]. The comparison showed the effectiveness of different cyphers for an application and occasionally for research purposes. Since each platform and application has its own limitations, comparing just area or throughput numbers is neither sufficient nor fair.

LED:The substitution permutation network serves as the foundation for the symmetric block cypher LED, which has a block size of 64 bits (SPN). It is built in two forms based on key size: (64-bit) key (LED-64) and (128-bit) key (LED-128). The number of rounds in an encryption key depends on how much of it there is; for example, (LED-64) has 32 rounds whereas (LED-128) has 48 rounds.Both the serialized nibble-wise mode and iterative round-based method may be utilized to create the architecture of the thin LED. The round-based design of the compact block cypher LED-64. The

design is based on the LED-64 and employs a (64-bit) input block and (64-bit) key size. The internal operations of this architecture are entirely designed in Verilog HDL, considering both low-cost and high-end Altera and Xilinx FPGAs.shows the block diagram of the round-based (LED-64) design. This architecture has the advantage that it makes great candidates for lightweight applications; for example, these implementations offer the best area of all lightweight hashfunction solutions that have been revealed up to this point. Smart cards, WSN nodes, and RFID tags are just a few examples of the little devices that are becoming common in our daily life. These sophisticated, portable devices might possibly alter important data, needing security precautions [13].

PRESENT:

"PRESENT" is the name of the most well-known lightweight block cypher displayed at CHES 2007. Using keys with an average length of 80 or 128 bits, it encrypts blocks of 64 bits. There are a total of 31 rounds. The fundamental SPN network of the round function consists of a sub-key addition layer, an S-box layer that always calls the same nibble S-box, and a layer for bit permutation. Security PRESENT has attracted a lot of cryptanalytic interest due its very specific linear biases. The investigations investigate the linear behavior of PRESENT in relation to several linear paths. This type of cryptanalysis permits the development of multi-linear attacks on up to 27 rounds of PRESENT by using the whole codebook.Also indicated in [11] are two different versions of PRESENT with complexity complexities that are roughly equal to those discovered after a full key search against the two versions of PRESENT. The implementation maintains the block cipher's key and block in tables of 16-bit data. The Present [12] method, which is advantageous for maintaining confidentiality in constrained settings, is used in this design.

PICCOLO

A compact hardware-based block cypher is the Piccolo block cypher. Hardware has finite amounts of memory and processing power. the process for implementing various trade-offs between area and speed. use the iterative and 4-bit serial FPGA designs as alternates. Using a 128-bit key, the Piccolo block cypher algorithm was built. This method has been implemented on the Xilinx Spartan-3. 76% of the available resources are being used in the iterative implementation. With this method, the encryption or decryption is finished in 31 clock cycles. It produces a throughput of 151.1 Mbps as a result. To cut expenses, the area of the serial implementation was optimized. It requires 496, and only 54% of the resources are being used.

Table 1 compares the results on the performance of light-weight block cyphers with keys bigger than 64 bits. Piccolo provides excellent security and a remarkably small implementation, in contrast to earlier Feistel-type structure-based lightweight block cyphers. About known analyses, current relevant key differential attacks, and MITM efforts, Piccolo offers a sufficient level of protection. This design has the advantage of being suitable for passive RFID tags and being made with a minimal amount of hardware implementation. The examination of the architecture and the serial and iterative implementation of the Piccolo block-cipher. PICCOLO's performance is insufficient and unreliable in this area since new applications need a lot of hardware resources [13].

myCrypton:A 64-bit lightweight block cipher called mCrypton is developed for low-cost and resource-constrained applications like RFID tags and WSN sensors. According to the creators, mCrypton is resistant to both differential and linear cryptanalysis [4]. On eight rounds of mCrypton-128, however, a related-key rectangle attack has just been introduced in [5]. The attack has a success rate of 0.94 and requires roughly 246 plaintexts, 246 encryptions, and 5248 bytes of memory, respectively. To utilize the parameters of a 64-bit block length and variable key lengths of 64 bits, 96 bits, and 128 bits since the major benefit of building mCrypton is to provide a block cipher optimized for resource-constrained applications.Encrypting large amounts of data in bulk is either unnecessary or perhaps impossible. The disadvantage of constructing utilizing Crypton's overall architecture while revamping and streamlining each component function to enable noticeably smaller implementation in both hardware and software [15].

KLEIN:RFID tags frequently lack the hardware power and capabilities that sensors do. Due to the adaptability and affordability of software implementations in manufacturing and maintenance, software-efficient block cyphers are seen to be more practicable for sensors. A new family of block cyphers called KLEIN was created for devices with constrained resources. Compared to earlier ideas, KLEIN has the benefit of software performance on older sensor systems, but its hardware implementation may not be as robust. The security analysis finds that KLEIN has a respectable security margin against several cryptanalyses.

The capability of this architecture to do three circular operations—Sub Nibbles, Rotate Nibbles, and Mix Nibbles—is a benefit. This network employs 64-bit plaintext and 64/80/96-bit

variable keys to encrypt the plaintext in 12/16/20 rounds, respectively. It is based on substitution-permutation. Sub Nibbles is the only non-linear KLEIN cypher phase that provides enough security for devices with constrained resources. Lightweight block cyphers' flaw, which was that they were mostly developed on outdated sensor systems. KLEIN leverages the Feistel-based structure in key scheduling to defend against weak key assaults [15].

II. DISCUSSION

When compared to the stream cypher, the block cypher is slower, but the symmetric technique is faster. Hardware algorithms are more effective and have higher throughput when compared to software algorithms, especially with FPGA platforms. In existing studies, the performance of the LWC algorithm implemented with FPGA is compared using various performance metrics, including maximum frequency, throughput, area, and efficiency. This paper examines several lightweight block cypher algorithms, such as AES, KASUMI, XXTEA192, RoadRunnerR, LED, XTEA, Piccolo, PRESEN, mCrypton, and KLEIN.
The results of the study demonstrate that the hardware implementation of KASUMI uses significantly more frequency and efficiency than other algorithms, and its throughput is superior to that of the other algorithms we looked at. The analysis revealed that the hardware implementation of XXTEA192 used significantly less space than other algorithms and had a higher throughput [13]. Iterative architecture's design increases the number of CLKs when it is employed, which lowers frequency, efficiency, and throughput. As a result, the cost goes up and the area grows larger.The space is lowered because of the pipeline architecture's design, which lowers costs while raising frequency, efficiency, and throughput. When compared to the other architectures, Table -1 demonstrates that the pipeline architecture has the maximum throughput, frequency, efficiency, and fewest slices. Therefore, it is evident that algorithm performance depends on the kind of architecture [14].

Algorithm	Key (bit)	Block (bit)	Area Slice	Max Frequency (MHz)	Throughput (Mbps)	Efficiency /Slice	FPGA	Architecture
AES [19]	128	128	4092	480	6341	1.55	Virtex - 7	Iterative
KASUMI [21]	128	64	470	644	5155	1.10	Virtex - 5	Internal
XXTEA [191]	128	192	50	364	834	17	Spartan – 6	Pipeline
RoadRunnerR	128	64	405	105	18	0.043	Spartan -5	Iterative
LED	64	64	122	486	972	7.96	Kintex -7	Iterative
PICCOLO	128	64	238	264	18	0.35	Artix -7	Pipeline
XTEA	64	64	552	74	152	0.294	Vertx – 6	Iterative
PRESENT	64	64	152	364	172	1.12	Spartan -5	Pipeline
MyCrypton	80	64	375	302	646	1.70	Spartan	Iterative
KLEIN	128	16	150	388	2070	-	Spartan - 8	Iterative

Table 1:Comparison of LWC algorithm Implemented FPGA

III. CONCLUSION

FPGA are excellent for prototyping, which eventually lowers the cost of algorithm creation. The goal of this study is to compare the frequency, throughput, area, and efficiency of ten LWC algorithms implemented with FPGA studies against different architectures: AES, KASUMI, XXTEA192, RoadRunnerR, LED, XTEA, Piccolo, PRESENT, mCrypton, and KLEIN. This article's study shows that iterative architecture needs additional hardware resources. With crucial route reductions, a highly efficient pipeline layout quickly increased throughput and efficiency. One of the key duties is to ensure the security of the resources and services while storing and transferring sensitive or otherwise essential data. This directly leads to an increase in the need for cryptographic components.

The adoption of safe algorithms that are often used in other fields but with less weight is necessary even though these devices have limited resources due to the constant need for smaller sizes and lower production costs. These choices are often made by other areas. For embedded system security, lightweight cryptography is required. The most current developments and the most lightweight block cypher implementations on FPGA have been the focus of the professionals working in this field. Research was conducted on

both software and hardware block cypher implementations to accomplish this goal. The findings of a comparison analysis were presented in terms of architecture's design to demonstrate the effectiveness, affordability, and security of each idea.

References

[1]. K. Sahu, S. Sharma, and D. Puthal, "Lightweight Multi-party Authentication and Key Agreement Protocol in IoT-based EHealthcare Service," ACM Trans. Multimed. Comput. Commun. Appl., vol. 17, no. 2s, pp. 1–20, 2021, doi: 10.1145/3398039.

[2]. B. J. Mohd, T. Hayajneh, and A. V. Vasilakos, "A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues," J. Netw. Comput. Appl., vol. 58, pp. 73–93, 2015, doi: 10.1016/j.jnca.2015.09.001.

[3]. Nayancy, S. Dutta, and S. Chakraborty, "A survey on implementation of lightweight block ciphers for resource constraints devices," J. Discret. Math. Sci. Cryptogr., pp. 1–22, 2020.

[4]. Khan, M.N.; Rao, A.; Camtepe, S. Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey. IEEE InternetThings J. 2021, 8, 4132–4156.

[5]. Dutta, I.K.; Ghosh, B.; Bayoumi, M. Lightweight Cryptography for Internet of Insecure Things: A Survey. In Proceedings of the2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January2019; pp. 0475–0481.

[6]. Shah, A.; Engineer, M. A Survey of Lightweight Cryptographic Algorithms for IoT-Based Applications. In Smart Innovations inCommunication and Computational Sciences. Advances in Intelligent Systems and Computing; Tiwari, S., Trivedi, M., Mishra, K., Misra,A., Kumar, K., Eds.; Springer: Singapore, 2019; Volume 851.

[7]. Thakor, V.A.; Razzaque, M.A.; Khandaker, M.R.A. Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices:A Review, Comparison and Research Opportunities. IEEE Access 2021, 9, 28177–28193.

[8]. ienan, D.; Xiangning, C.; Shuai, C. Overview of Application Layer Protocol of Internet of Things. In Proceedings of the 2021IEEE 6th International Conference on Computer and Communication Systems (ICCCS), Chengdu, China, 23–26 April 2021;pp. 922–926.

[9]. Derryberry, R.T., Gray, S.D., Ionescu, D.M., Mandyam, G. and Raghothaman,

[10]. B., 2002. Transmit diversity in 3G CDMA systems. IEEE communications magazine, 40(4), pp.68-75.

[11]. Khan, A.H., Qadeer, M.A., Ansari, J.A. and Waheed, S., 2009, April. 4G as a next generation wireless network. In 2009 International Conference on Future Computer and Communication (pp. 334-338). IEEE.

[12]. Andrews, J.G., Buzzi, S., Choi, W., Hanly, S.V., Lozano, A., Soong, A.C. and Zhang, J.C., 2014. What will 5G be? IEEE Journal on selected areas in communications, 32(6), pp.1065-1082.

[13]. I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G Security Challenges and Solutions," IEEE Commun. Stand. Mag., vol. 2, no. 1, pp. 36–43, 2018, doi: 10.1109/MCOMSTD.2018.1700063.

[14]. O. Salman, A. Kayssi, A. Chehab, and I. Elhajj, "Multi-level security for the 5G/IoT ubiquitous network," 2017 2nd Int. Conf. Fog Mob. Edge Comput. FMEC 2017, pp. 188–193, 2017, doi: 10.1109/FMEC.2017.7946429.

[15]. A Close Examination of Performance and Power Characteristics of 4GLTE Networks, Junxian Huang, Feng Qian, Alexandre Gerber, Z. MorleyMao, Subhabrata Sen, Oliver Spatscheck, University of Michigan, AT&TLabs - Research.

[16]. Application of FSM Machine and S-Box in KASUMI Block Cipherto Improve Its Resistance Against Attack, Raja Muthalagu and SubeenJain(Corresponding author: Raja Muthalagu), Department of Electricaland Electronic Engineering, Birla Institute of Technology and Science,Pilani, 345055 Dubai International Academic City, Dubai, United ArabEmirates, (Email: raja.m@dubai.bits-pilani.ac.in), (Received July 2,2017; revised and accepted Oct. 22 & Nov. 5, 2017).