ASIC-Oriented Comparative Review of Hardware Security Algorithms for Internet of Things Applications

Mohamed A. Bahnasawi[1], Khalid Ibrahim[2], Ahmed Mohamed[3], Mohamed Khalifa Mohamed[4], Ahmed Moustafa[5],
Kareem Abdelmonem[6], Yehea Ismail[7], Hassan Mostafa[8]
[1,3,5,6,8]Electronics and Electrical Communications Engineering Department, Cairo University, Giza, Egypt
[2]Electronics Department, Faculty of Information Engineering and Technology, German University in Cairo, Cairo, Egypt
[4]Electrical, Electronics and Communications Engineering Department, Faculty of Engineering, Alexandria University, Egypt
[7,8]Center for Nanoelectronics and Devices, AUC and Zewail City of Science and Technology, New Cairo, Egypt
{[1]m_bahnasawi@outlook.com; [2]khalid.mohie@student.guc.edu.eg; [3]ahmedmohamed.eece@gmail.com;
[4]mohamed.mohamed@student.tut.fi; [5]ahmed_moustafa_94@yahoo.com; [6]kareem.men3em@gmail.com; [7]y.ismail@aucegypt.edu;
[8]hmostafa@uwaterloo.ca }

***Abstract*— Research into the security of the Internet of Things (IoT) needs to utilize particular algorithms that offer ultra-low power consumption and a long lifespan, along with other parameters such as strong immunity against attacks, lower chip area and acceptable throughput. This paper offers an ASIC-oriented comparative review of the most popular and powerful cryptographic algorithms worldwide, namely AES, 3DES, Twofish and RSA. The ASIC implementations of those algorithms are analyzed by studying statistical data extracted from the ASIC layouts of the algorithms and comparing them to determine the most suited algorithms for IoT hardware-security applications. The AES algorithm is found to be the most suitable algorithm for IoT applications.**

Keywords—Internet of Things (IoT); Hardware Security; Application Specific Integrated Circuit (ASIC); Cryptography; Cryptographic Algorithms; AES; 3DES; Twofish; RSA

I. Introduction

Cryptography has been used for centuries to secure communication. Due to the enormous expansion of the digital world, secure cryptographic algorithms have become intensively used in a wide number of applications such as Wireless Local Area Networks (WLAN), Wireless Sensor Networks (WSN), smart cards and medical devices. Accordingly, efficient, secure and low power cryptographic algorithms have become crucial.

Many cryptographic algorithms are widely available and used in information security. They can be categorized into symmetric (private) and asymmetric (public) key cryptographic algorithms. In symmetric-key cryptography, only one key is used to encrypt and decrypt data. In contrast, asymmetric-key cryptography uses two keys, a private and a public key [1]. The public key is used for encryption while the private key is used for decryption. The RSA algorithm is an example of an asymmetric-key algorithm. Public key encryption is based on mathematical functions and is computationally intensive. Symmetric-key algorithms are suited for certain applications while asymmetric-key algorithms are better for different ones.

Applications have different requirements for the cryptographic algorithms that secure them, varying in the throughput needed, the extent of immunity against attacks, power consumption, the area needed on-chip, etc. The Internet of Things (IoT) focuses mainly on low-power implementations of security algorithms. This is because most of them are related to autonomous applications or embedded systems applications (i.e. an ultra-thin sensor system [2] embedded inside clothes or biomedical applications). These applications have very limited power budgets to lengthen the lifetime of their batteries.

In this paper, different symmetric-key and asymmetric-key cryptographic algorithms are investigated. ASIC implementations of these algorithms are presented and statistical data such as power consumption are compared to conclude which algorithms are the most suited for IoT security constraints. The following popular and powerful algorithms are chosen to be studied: AES, 3DES, Twofish and RSA.

The rest of this paper is organized as follows. Section II gives a brief overview of each of the chosen algorithms and analyzes the immunity against attacks of each algorithm. The statistical data extracted out of the ASIC implementations are tabulated and compared in Section III. In addition, the corresponding layout implementations are presented. Finally, Section IV concludes and discusses the results of the paper.

II. Immunity Against attacks

A. AES

The Advanced Encryption Standard (AES) was established in 2001 by NIST as the current standard for encrypting electronic data. AES uses the Rijndael cipher, which is a symmetric-key block cipher. The Rijndael cipher supports numerous block and key sizes, but AES chooses to have a fixed block size of 128 bits and three key size variants to choose from: 128, 192 and 256. The AES therefore benefits from strong security and high flexibility.

978-1-5090-5721-4/16/$31.00 ©2016 IEEE

Brute force attacks against AES implementations are currently not feasible due to the large key size of AES, but future advances in Quantum Computing could be a threat in this regard. In addition, there are possible attacks published in the literature that are computationally faster than a full brute force attack. attack, but they are still not computationally feasible [3]. No practical attacks are currently known against correct implementations of AES. Furthermore, researchers have attempted to enhance the security of AES against certain attacks, such as algebraic attacks.

AES has proved its immunity against attacks. Hence, AES has become the perfect choice for numerous applications, including not only wireless standards such as Wi-Fi, ZigBee and WiMAX but also, the security of smart cards and bit-stream security in FPGAs [4].

B. 3DES

The fundamental standard for encrypting information was for a time a symmetric algorithm known as the Data Encryption Standard (DES). However, nowadays the 56-bit key of DES is not considered sufficient to encrypt critical data. Therefore, 3DES or the Triple Data Encryption Standard was developed to solve the clear issues in DES without needing to design a completely new cryptosystem.

3DES simply extends the key size of DES by applying the algorithm three times successively with three different keys. Thus, the combined key size is 168 bits. Moreover, repeating the iteration three times leads to benefits such as increases in encryption level and average time.

3DES is considerably more immune to brute force attacks than DES. Furthermore, the time required to check all possible keys at 50 billion keys per second is 800 days [5]. However, 3DES is vulnerable to meet-in-the-middle attacks. This is because 3DES uses three independent keys, giving an overall key length of 168 bits. The overall key length can be reduced to 112 bits if only two independent keys are used, but this might not be secure enough. A different attack, linear cryptanalysis (LC), was made in 1994 by Matsui and Yamagishi. LC is one of the most powerful attacks against block ciphers. In LC, a linear approximation is performed to discover the block cipher behavior. If enough pairs of a plaintext and its corresponding cipher text are available, LC can be used to obtain information about the key [6].

C. Twofish

The Twofish cipher was first published in 1998 by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall and Niels Ferguson. It is a 128-bit symmetric key block cipher with a variable key length of 128, 192 or 256 bits. Furthermore, it is derived from the Blowfish, SAFER and DES algorithms and was one of the five finalists of the AES contest.

Niels Ferguson published an impossible differential attack in 1999 [7], which could break 6 rounds out of 16 for the 256-bit key version. Moreover, one of the best published cryptanalysis on the Twofish is a truncated differential cryptanalysis of the full 16-round version. Theoretically, it would take 251 plaintexts, which are 32 petabytes of data, to find a good truncated differential pair [8]. Accordingly, Twofish can't be broken remotely.

D. RSA

The RSA cryptosystem, invented by Ron Rivest, Adi Shamir and Len Adleman, was first publicized in the August 1977 issue of Scientific American. Furthermore, RSA is the most used public-key algorithm which is used to send an encrypted message without a separate exchange of secret keys. Nowadays, many protocols like S/MIME, SSH, SSL/TLS and OpenPGP rely on RSA for encryption and digital signature functions.

Prime factorization of the modulus N is the first attack on an RSA public key. If N is factorized, the attacker can get Φ(N), then the decryption exponent D. This attack is referred to as a brute-force attack on RSA [9]. This attack is not feasible when RSA is used properly with a sufficiently long key. Hence, it is recommended to use a key size larger than 2048 bits [10]. There are other indirect attacks that can break RSA without using prime factorization. However, they are not devastating attacks. Given that the RSA has been properly implemented, it can be trusted to provide the required security.

III. Comparison of the ASIC Implementations' Extracted Data

Verified modules obtained for AES [11], 3DES [12], Twofish [13] and RSA [14] were implemented and synthesized using Synopsys DC Tools to get the netlist and the Cadence Encounter Tool to get the layout. These implementations are analyzed to establish a full comparison on post-layout level between the four algorithms, making it possible to estimate their performance in IoT applications.

This comparison is based on the UMC 130nm CMOS technology with an operating voltage of 1.08 V. Fig. 1 portrays the layouts of the cryptographic algorithms. Table I shows the extracted power in mWatt and area in mm^2 at a constant frequency and Table II shows the extracted frequency in MHz and area in mm^2 at a constant power.

The RSA implementation results in the highest power consumption and area compared to the other cryptographic algorithms at the same operating frequency. Comparing the results of RSA with other published designs [18] proves that the RSA algorithm is a high power encryption algorithm. Even though these designs depend on low power methods, the power consumption of each of them is still very high. Table III shows a comparison between our results and the results of some of the most suitable designs for each algorithm which are published in literature. This comparison is based on frequency, power and area.

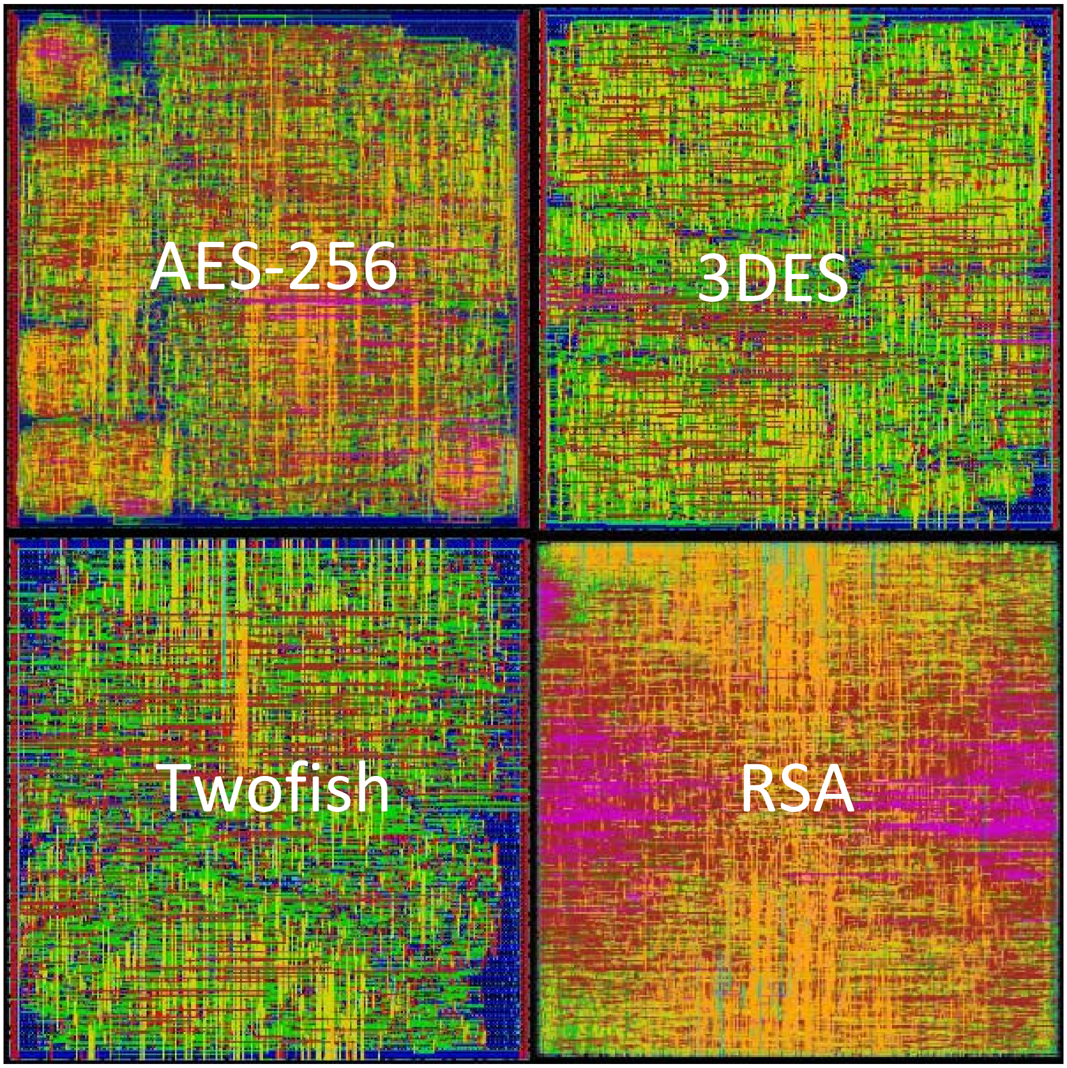

Fig. 1. ASIC layouts of the cryptographic algorithms

TABLE I. COMPARISON AT CONSTANT FREQUENCY

Frequency (MHz)		10		100		200	
		Power (mWatt)	Area (mm^2)	Power (mWatt)	Area (mm^2)	Power (mWatt)	Area (mm^2)
AES	128	0.724	0.148	6.197	0.148	12.24	0.148
	192	0.729	0.149	6.218	0.149	12.31	0.149
	256	0.727	0.149	6.216	0.149	12.28	0.149
3DES		0.968	0.217	8.728	0.217	17.75	0.217
Twofish		0.675	0.101	N/A		N/A	
RSA		9.38	1.236	N/A		N/A	

TABLE II. COMPARISON AT CONSTANT POWER

Power (mWatt)		1		10		20	
		Freq. (MHz)	Area (mm^2)	Freq. (MHz)	Area (mm^2)	Freq. (MHz)	Area (mm^2)
AES	128	15	0.148	160	0.148	320	0.150
	192		0.149		0.149		0.151
	256		0.149		0.149		0.151
3DES		10	0.217	110	0.217	227	0.217
Twofish		15	0.108	N/A		N/A	
RSA		0.5	1.030	11	1.257	N/A	

TABLE III. COMPARISON BETWEEN OUR DESIGNS AND PREVIOUS DESIGNS

Design		Freq. (MHz)	Area (mm^2)	Power (mWatt)	Voltage (Volt)	Technology
AES	**Ours [11]**	20	0.148	1.328	1.08	UMC 130nm
	Ref. [15]	20	0.2489	1.477	1.62	SMIC 180nm
3DES	**Ours [12]**	181.81	0.217	15.75	1.08	UMC 130nm
	Ref. [16]	181.81	0.55	17.47	-	TSMC 130nm
Twofish	**Ours [13]**	66	0.1007	4.273	1.08	UMC 130nm
	Ref. [17]	66	2.75*2.75	44	3.3	TSMC 130nm
RSA	**Ours [14]**	11.9	1.283	11.43	1.08	UMC 130nm
	Ref. [18]	13.56	0.27	15	-	SMIC 130nm

As can be seen in Table III, our implementation of the AES verified module, obtained from [11], results in less area and power than the implementation of [15]. Similarly, our implementations of the 3DES and Twofish modules, which were obtained from [12] and [13], also use less area and consume less power than the implementations they are compared to. In the case of the AES implementations, the improved performance of our implementation, compared to the published design, can be credited in part to the improvement in technologies used.

IV. CONCLUSION

This paper presents a thorough ASIC hardware implementation comparison of some of the most commonly used security algorithms in IoT applications. Our implementations are conducted using the ASIC approach and are evaluated using the UMC 130nm CMOS technology. This comparative review covers a variety of the most crucial specifications that are the main constraints of IoT applications, such as power consumption, frequency, throughput, area and immunity against attacks. The chosen algorithms in our study are AES, 3DES, Twofish and RSA.

The ASIC implementations of the AES, 3DES and Twofish have acceptable power consumption and chip area. Hence, we recommend them for ultra-low-power IoT applications that are mostly used in biomedical applications. The results for the RSA implementation are not acceptable for IoT applications due to its huge power consumption and chip area. In terms of throughput, RSA is also not recommended because of the huge number of required cycles to finish the encryption process. Choosing to use 3DES is not recommended in applications requiring impeccable security. The AES algorithm is the most secure against practical attacks, especially the 256-bit flavor. Furthermore, the AES implementation results show that it needs only 99, 119 and 139 cycles for the 128-bits, 192-bits and 256-bits keys, respectively. In addition, the power consumption and area of the AES implementation are more suitable for IoT applications, compared with the other algorithms that focus mainly on achieving the best security and ultra-high throughput. Thus, it is concluded that AES is the most suitable security algorithm for IoT applications.

ACKNOWLEDGEMENT

This research was partially funded by Cairo University, ITIDA, NTRA, NSERC, Zewail City of Science and Technology, AUC, the STDF, Intel, Mentor Graphics, SRC, ASRT and MCIT.

REFERENCES

[1] Idrizi, Florim, Dalipi, Fisnik & Rustemi, Ejup. "Analyzing the speed of combined cryptographic algorithms with secret and public key". International Journal of Engineering Research and Development, Volume 8, Issue 2 (August 2013) , pp. 45.

[2] Shaza D. Rihan, Ahmed Khalid, Saife Eldin F. Osman, "A performance comparison of encryption algorithms AES and DES", International Journal of Engineering Research & Technology (IJERT), Volume 4, Issue 12 (December 2015).

[3] http://research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf

[4] S. Trimberger, "Security in SRAM FPGAs", IEEE Design and Test of Computers, vol. 24, no. 6, p. 581, Nov./Dec. 2007.

[5] C. Paar, J. Pelzl and B. Preneel, "Understanding cryptography: a textbook for students and practitioners", Springer Heidelberg Dordrecht, Bochum, (2010).

[6] R. A. Mollin, "Codes: The Guide To Secrecy From Ancient To Modern Times", Chapman and Hall/CRC, Boca Raton, (2005).

[7] https://www.schneier.com/cryptography/archives/1999/10/impossible_different.html

[8] Shiho Moriai, Yiqun Lisa Yin (2000). "Cryptanalysis of Twofish (II)"

[9] Boneh, D., "Twenty years of attacks on the RSA cryptosystem." Notices of the American, Mathematical Society (AMS) 46, 1999.

[10] Wen Hu, Peter Corke, Wen Chan Shih, and Leslie Overs, "A public key technology platform for wireless sensor networks.", Proceedings of the European Conference on Wireless Sensor Networks, 2009, pp. 296–311.

[11] OpenCores. (2006). Open core AES Core module, [Online]. Available: http://opencores.org/project,aes_128_192_256

[12] OpenCores. (2006). Open core 3DES (Triple DES) / DES, [Online]. Available: http://opencores.org/project,3des_vhdl

[13] OpenCores. (2002). Open core Twofish Core, [Online]. Available: http://opencores.org/project,twofish_team

[14] OpenCores. (2003). Open core Basic RSA Encryption Engine, [Online]. Available: http://opencores.org/project,basicrsa

[15] Liling Dong, Ning Wu, and Xiaoqiang Zhang "Low Power State Machine Designfor AES Encryption Coprocessor" International MultiConference of Engineers and Computer Scientists 2015 Vol II, IMECS 2015, March 18 - 20, 2015, Hong Kong.

[16] P.V Rao, Mallikarjun H M, Nagendra and S.Manjusha "Design and ASIC Implementation of Triple Data Encryption and Decryption Standard Algorithm", *International Journal of Power Elecronics and Technology* January-June 2011, Volume 1, Number 1, pp. 1–15.

[17] Yeong-Kang Lai, Liang-Gee Chen, Jian-Yi Lai and Tai-Ming, " VLSI architecture design and implementation for TWOFISH block cipher," in Circuits and Systems, 2002. ISCAS 2002.

[18] X. Zheng, Z. Liu and B. Peng, "Design and Implementation of an Ultra Low Power RSA Coprocessor," *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, Dalian, 2008, pp. 1-5.