Astudy of Authentication Encryption Algorithms (POET, Deoxys, AEZ, MORUS, ACORN, AEGIS, AES-GCM) For Automotive Security

Sahar Sharaf
Communications and electrical electronics
Cairo University
Cairo, Egypt
tsaharsharaf@gmail.com

Hassan Mostafa
Communications and electrical electronics
Cairo University
Cairo, Egypt
hmostafa@uwaterloo.ca

***Abstract*— Connected and autonomous cars present a major challenge for securing vehicles against outside or inside attacks which may affect the safety of the driver. In this paper there is a comparison between seven light weight authenticated algorithms, and a classification of automotive embedded systems for helping in choosing the suitable algorithm for each application as per system safety and security requirements. The authenticated algorithms used in this paper are POET, Deoxys, AEZ, MORUS, ACORN, AEGIS, and AES-GCM.**

Keywords—Authentication Encryption, AEZ, POET, DEOXYS, AEGIS, ACORN, MORUS, AES-GCM, automotive security algorithms, FPGA, CAESAR.

I. INTRODUCTION

Nowadays, security and safety are a major area of concern in automotive systems. Currently, Embedded systems are used in every automotive system. In highly engineering automobiles, the number of the used electronic control units (ECUs) may exceed 100 ECUs. These ECUs communicate either together over an inside network or with the outer world. Embedded automotive systems have limited resources, so there is a high need for efficient and robust cryptographic algorithms. For these systems to be secure; the content of the messages received or sent shall be protected and the owner of these messages shall be verified. Those two functions are executed either using two separate algorithms for the encryption and authentication processes, or using a unique authenticated encryption algorithm [1].

Table I shows the cryptography algorithms classification. These algorithms are classified as per message length, encryption, and authentication. The algorithms used in this paper belong to authenticated ciphers. Authenticated ciphers are a class of symmetric key cryptography. They ensure confidentiality of messages, authentication of source, and integrity of data. This leads to a smaller area and low power consumption comparing with the results of using two separate algorithms for hardware implementation. The authenticated algorithms used in this paper are POET, Deoxys, AEZ, MORUS, ACORN, AEGIS, and AES-GCM [2] [3].

These algorithms were chosen as follow: (1) the algorithms POET, DEOXYS, and AEZ were categorized to be more efficient for lightweight automotive embedded systems [4], (2) the algorithms AEGIS, ACORN, and MORUS were announced to be the finalist of CAESAR competition (Competition for Authenticated Encryption) in March 2018 [5], and (3) the last one is AES-GCM, it is the authenticated algorithm of the standardized AES algorithm.

TABLE I. CRYPTOGRAPHY ALGORITHMS' COMPARISON

	Message length	**Encryption**	**Authentication**
Block cipher	Fixed	Yes	No
Stream cipher	Variable	Yes	No
Message authentication code	Variable	No	Yes
Authenticated cipher	Variable	Yes	Yes

II. AUTHENTICATED CIPHERS

A. AES-GCM

AES-GCM is a standardized authenticated Galois/counter mode (GCM). It provides both authenticity and confidentiality. The confidentiality is achieved by AES, and the authenticity is provided by the Galois/counter mode using a universal hash function[7] [8].

AES_GCM's inputs are a secret key (k), an Initialization vector (IV) that is used as a nonce (public message number), a plain text (P) that represents the message content, and an additional associated data (AAD) that represent the header. AES-GCM's outputs are a cipher text (C) that has the same length as the input plain text, and an authentication tag (T) that affects AES_GCM's strength [7] [8].

AES-GCM shall use a unique nonce for each key and this requires a careful implementation and a good practice from the users. AES-GCM's features are high speed at low cost, low latency, parallelism, pipelining, efficient software implementation, and ease of hardware implementation [7] [8].

B. AEGIS

AEGIS is a dedicated authenticated encryption algorithm. It's constructed from AES encryption round functions, but not the last round. Its computational cost is about half that of AES. Its speed is faster than AES in the counter mode and about 8 times that of AES in Cipher block chaining (CBC) mode. Its authentication is achieved almost for free. AEGIS supports Parallel AES round functions at each step, so it's suitable for fast software and Hardware implementations [9] [10].

AEGIS has three parameter sets which are AEGIS-128L, AEGIS-128, and AEGIS-256. They vary in the length of the key and the state. AEGIS-128L is the fastest. AEGIS-128's

978-1-5386-8167-1/18/$31.00 ©2018 IEEE

state is smaller than that of AEGIS-128L, and its structure is the simplest among those three algorithms [9] [10].

AEGIS is secure as long as its security requirements are met. Its nonce should not be reused, the key and IV pair should be used to protect only one message and shouldn't be used with two different tag sizes [9] [10].

AEGIS is suitable for network communications since AEGIS can protect a packet while leaving the packet header (associated data) unencrypted [9] [10].

C. ACORN

ACORN is an authenticated encryption algorithm. It is a stream cipher based on linear feedback shift registers (LFSR). It is used for lightweight applications that has limited resources and for high performance applications[11].

For ACORN being secure each key should be generated in a secure and random way, each key and IV pair should be used to protect only one message and should not be used with two different tag sizes. If IV is reused seven times, the security of ACORN would be lost. But, if initialization vector is used only once for each key, it would be difficult to apply any statistical attacks and it would be strong against traditional attacks [11].

ACORN doesn't check the length of the message of associated data and plain text or cipher text, and doesn't need to pad the message to a multiple of block size which reduces the cost of hardware implementation. Furthermore, it separates the processing of associated data and the plain text or cipher text [11].

D. MORUS

MORUS is a dedicated authentication cipher. The design of MORUS is based on the method of designing stream ciphers which has small number of operations in the state update function. It is efficient in hardware because only logic gates AND, XOR, and rotations are used in its update function. Also, it's efficient in SW, and offers more steady performance across platforms [12].

MORUS has three parameter sets which are MORUS-640-128, MORUS-1280-128, and MORUS-1280-256. All of them are suitable for light weight applications. Furthermore, MORUS-640-128 is suitable for high performance applications [12].

In MORUS, key and nonce should be used to protect only one message. MORUS's state size and key generation function is contributing to its strength against the cipher attacks [12].

E. Deoxys

Deoxys is an authenticated encryption cipher which is based on a tweakable block cipher (Deoxys-BC). It uses the well studied AES round function as a building block.

Deoxys uses several sets of parameters that use different key and tweak sizes. Deoxys has two authentication and encryption modes: (1) Deoxys-I for non repeating nonce, and (2) Deoxys-II for the nonce repeating scenario. In this paper, Deoxys-II is the one synthesized and considered here because it is more secure than Deoxys-I [8] [13].

Deoxys performs well for small messages which benefits lightweight applications. It shows excellent hardware and software performance, and has a good security margin for all its recommended parameters. Also, Deoxys doesn't have the pre computation overhead or long initialization [8] [13].

F. AEZ

AEZ acts as an enciphering or an authentication encryption Scheme. It has a strong security and usability properties. AEZ is parallelizable, has a computational cost close to that of AES-CTR and its architecture suffers from being difficult to be implemented in Hardware [4] [14].

AEZ has a plain text with a variable length, and the way AEZ enciphers depends on the length of the plaintext. If the plaintext length is fewer than 32 bytes, AEZ-tiny will be used, and if its length is 32 bytes or more, then AEZ-core will be used. Moreover, its nonce and key have a variable length and its AD can be an arbitrary list of arbitrary strings [14].

G. POET/POE

POET/POE is a family of On-Line Authenticated Encryption schemes. It is a self-contained family of fast and secure ciphers. POE and POET difference is that POE performs the encryption and decryption functions of POET without processing the associated data and authentication. POET/POE is fast, secure, robust, flexible, and efficient on a variety of platforms [15] [16].

POET/POE it's suitable for low end applications since it allows utilizing a single core processor more efficiently. Also, thanks to pipelining, it's efficient for high end devices and provides high throughput on multi core architecture. POET is robust against nonce misuse and robust against decryption misuse [15] [16].

III. CLASSIFICATIONS OF AUTOMOTIVE ECUS

Automotive embedded systems are based on Electronic control unit (ECU). The ECUs are categorized based on safety and security requirements. ECUs are connected through an inside network with different protocols such as CAN, LIN, Flex Ray, and Ethernet.

In automotive, the functional safety requirements are standardized in ISO26262 to develop and design dependable automotive systems with minimum development cost. This is called ASIL (Automotive safety integrity level) [17].

ASIL stands for the severity of the safety requirements. It takes 5 levels (QM=0, A=1, B=2, C=3, D=4). Level QM is used for systems that don't need safety requirements, level D is allocated to the highest critical safety system, and level A is allocated for the least functional safety requirements [17].

ECUs are classified based on how the failure of their functionality may affect the safety of the driver and based on that they are classified into 5 groups as follow:

- Power train ECUS provide critical resource control as in engine control functionality such as brake systems. These ECUs are highly critical safety systems. A failure of their functionality causes the driver to lose control which affects the driver safety so it takes ASIL 4 [20].
- Vehicle safety ECUs provide safety assistance to the driver such as airbag and collision avoidance system.

A failure of their functionalities could have an uncontrollable impact on safety, so it takes ASIL 4 [20].

- Comfort ECUs provide driver assistance such as thermal management and parking assistance. A failure of their functionalities is not directly related to safety, but a combination of their failures could lead to debilitating effects. It takes ASIL 1 [20].
- Infotainment ECUs supports audio and video in the vehicle such as audio streams, systems that receive data from external sources as in traffic and weather information systems. A failure of their functionalities doesn't immediately affect the safety of the driver but is considered a distracting. It takes ASIL 1 [20].
- Telematics ECUs are systems that integrate telecommunications and informatics to the vehicle. They provide networked software applications such as mobile communications and GPRS. A failure of their functionalities doesn't directly affect the safety of the driver, but it could be a distracting. It takes ASIL 1 [20].

IV. Results

A synthesis is done for these algorithms on FPGA board (Virtex-7VC707Evaluation Platform). "Fig. 1" shows the results of these algorithms in terms of throughput [6], area [19], and power at clock period equals 100ns.

As in "Fig. 1", AEGIS and MORUS have the highest throughput values, AEGIS throughput equals 60GB/S and MORUS throughput equals 59GB/S, so they are efficient for the applications that require high throughput like Infotainment ECUs that provide audio and video streaming functionalities.

AEGIS and ACORN are efficient for the telematics ECUS that provide communication functionalities because AEGIS can protect a packet while leaving the packet header, and ACORN, which is a bit based sequential algorithm, doesn't need to pad the message to a multiple of the block size, and it separates the processing of associated data and the plain text or cipher text [10] [11].

From the security point of view, all those mentioned algorithms have security requirements that shall be met for ensuring that they are secure.

These algorithms vary in the security provided by them since: (1) AEZ, POET and Deoxys-II are the algorithms that are more secure because they are robust a against nonce misuse which is not supported by the other algorithms, as in Table II, (2) moreover, AEZ and POET ensure security up to the birthday-bound, while Deoxys-II (the one synthesized here) ensures security beyond-birthday-bound. As a result, Deoxys-II is considered the most secure one of them, so it can be used for the ECUs or the applications whose functionalities have high security and safety requirements and don't require very high values of throughput.

"Fig. 2" shows the relation between the frequency used and the consumed power. As shown in "Fig. 2", the consumed power decreases with the increase of the clock cycle, so as per the system requirements, the designers can choose the frequency that achieves the system requirements with minimum cost.

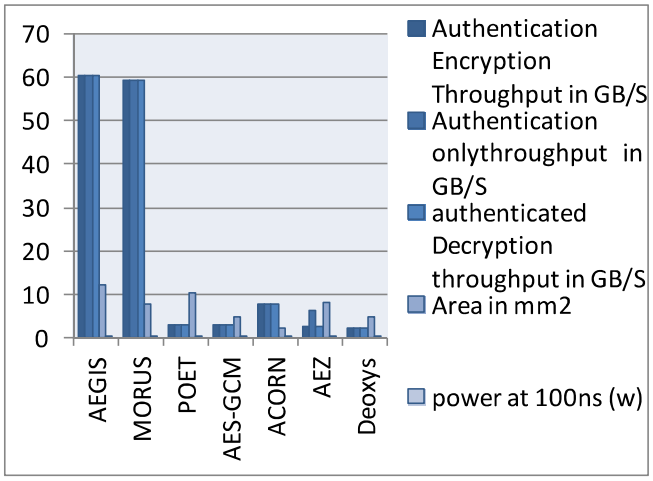

Fig. 1. Synthesis results in terms of throughput, power, area.

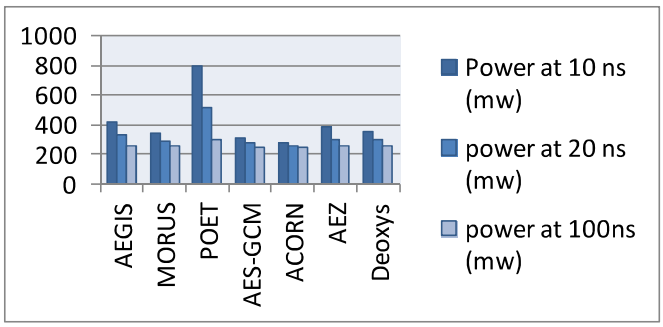

Fig. 2. Power consumption of algorithms at different clock periods.

V. Metrics

In automotive system throughput is very important for the ECUs that either require fast responses or for the ECUS that provide audio and video streams functionalities or require high throughput. "Fig. 3" is used to represent the metrics of those algorithms. The metric is shown in (1).

$$Metrics = Throughput / (Area * Power) \quad (1)$$

As shown in "Fig. 3", MORUs has the highest metrics and POET has the least metrics. Thus, MORUS is the most efficient algorithm when the throughput is the main concern. But, when the security is the main concern then Deoxys-II is the most efficient one because it has the highest security bound comparing to the other algorithms and it has the highest metrics comparing to POET and AEZ.

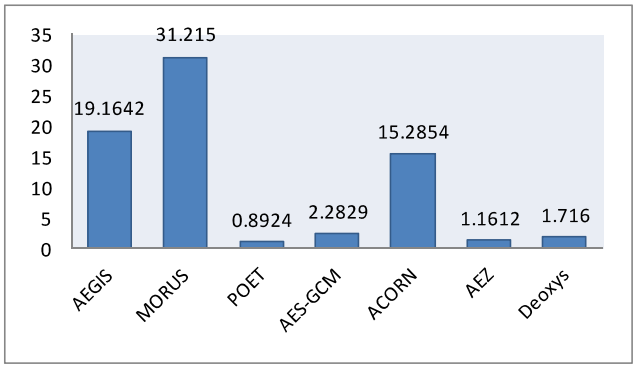

Fig. 3. Metrics of algorithms that is shown in (1).

TABLE II. COMPARISONS BETWEEN ALGORITHMS

Factors	AEGIS	AEZ	MORUS	ACORN	POET	Deoxys	AES-GCM
Key	128, 256	>=128, default:384	128, 256	128	128	128, 256	128, 192, 256
IS	1024,640, 768	128	1280,640	293	128	128	128
Nonce	128, 256	<=128	128	128	128	128	1-264
Tag	>=128	64	>=128	>=128	>=128	>=128	128
Rounds	5,8	4, 10	5	8	14, 20	14, 16	10, 12, 14
Message length	Variable	Variable	Variable	Variable	Variable	Variable	Variable
Parallelizability[2]	No	Yes	No	Partial	Yes	Yes	Yes
Nonce misuse resistance[2]	None	Complete	None	Partial	Complete	Complete	None[18]
Application	-High performance application - Network communications since AEGIS can protect a packet while leaving the packet header (associated data) unencrypted.	-High-performance applications - For low-energy or bandwidth constrained applications -Defense in depth	-High performance application -Light weight application	- High performance application -Light weight application (resource constrained environments)	- Well-suited for low-end, Mid-range and high-end devices applications.	- High performance application -Light weight application (Deoxys is efficient for small message) -Defense in depth	- Can be used with IP security and 802.1AE Media Access Control (MAC) Security[7]

VI. CONCLUSION

In this paper, A comparison between seven authenticated encryption algorithms in terms of throughput, power, and area, the consumed power at different frequencies, the metrics that is mentioned in (1), and the main differences, as in Table II, is interpreted. Additionally, a classification of the automotive ECUs, as per their functional safety and security requirements, is mentioned for helping the designers in choosing the algorithm that satisfies the requirements of their systems with minimum cost. Finally, from the above results, choosing the efficient and suitable algorithm depends on the system's requirements, resources, and restrictions.

ACKNOWLEDGMENT

This work was partially funded by ONE Lab at Zewail City of Science and Technology, Egypt and Cairo University, Egypt.

REFERENCES

[1] K. Khateb, M. Ahmed, A. K. ELdin, M. AbdelGhany, and H. Mostafa, "Dynamically Reconfigurable Power Efficient Security for Internet of Things Devices", IEEE International Conference on Modern Circuits and Systems Technologies (MOCAST'2018), Thessaloniki, Greece, pp. 1-4, 2018.

[2] M. A. Bahnasawi, K. Ibrahim, A. Mohamed, M. Khalifa, A. Moustafa, K. Abelmonim, Y. ismail, and H. Mostafa, "ASIC-Oriented Comparative Review of Hardware Security Algorithms for Internet of Things Applications", IEEE International Conference on Microelectronics (ICM 2016), Cairo, Egypt, IEEE, pp. 285-288, 2016.

[3] https://competitions.cr.yp.to/secret.html.

[4] S.Koteshwara, and A.Amitabh, "Comparative study of Authenticated encryption targeting lightweight IOT applications", IEEE Design & Test, vol.34, no. 4, PP.26-33, 2017.

[5] http://www3.ntu.edu.sg/home/wuhj/research/caesar/caesar.html.

[6] https://cryptography.gmu.edu/athena/CAESAR_HW_Summary_2.html.

[7] V. Arun, K. Vanisree, and D. L. Reddy, "Implementation of AES-GCM encryption algorithm for high performance and low power architecture Using FPGA", International Journal of Research and Applications,vol. 1, no. 3, PP. 120-131, 2014.

[8] S.Koteshwara, A.Das, and K.K.Parhi, "FPGA implementation and comparison of AES-GCM and Deoxys authenticated encryption schemes", 2017 IEEE International Symposium on Circuits and Systems (ISCAS).

[9] K.abdellatif, R.Chotin, H.Mehrez, "AES-GCM and AEGIS: Efficient and High Speed Hardware Implementations", vol. 88, no. 1, PP 1-12, 2017.

[10] H.Wu, and B.Preneel, "AEGIS: A Fast Authenticated Encryption Algorithm (v1.1)", CAESAR competition, 2016.

[11] H.Wu," ACORN: A Lightweight Authenticated Cipher (v3)", CAESAR competition, 2016.

[12] H.Wu, T.Huang, "The Authenticated Cipher MORUS (v2)", CAESAR competition, 2016.

[13] J.Tean, I.Nikolic, and T.Peyrin, Y.Seurin, "Deoxys v1.41", CAESAR competition, 2016.

[14] V.T.Hoang, T.Krovetz, and P.Rogaway, "AEZ v5: Authenticated Encryption by Enciphering", CAESAR competition, 2017.

[15] F.Abed, S. Fluhrer, J.Foley, C.Forler, E.List, S.Lucks, D.McGrew, and J.Wenzel, "The POET Family of On-Line Authenticated Encryption Schemes",CAESAR competition, 2015.

[16] F.Abed, S. Fluhrer, J.Foley, C.Forler, E.List, S.Lucks, D.McGrew, and J.Wenzel, "The POET Family of On-Line Authenticated Encryption Schemes",CAESAR competition, 2014.

[17] Y.Gheraibia, S. Kabir, K. Djafri, and K. Krimou, "An Overview of the Approaches for Automotive Safety Integrity Levels Allocation", Journal of Failure Analysis and Prevention, vol. 18, no. 3, pp 707–720, 2018.

[18] https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/presentations/d2-03_zeh_noncemisuseresistantaead_v2.pdf.

[19] N.Gamal, H.Mostafa, H.Fahmy, and Y.Ismail, "Design guidelines for embeded NoCs on FPGAs", Conference: 2016 17th International Symposium on Quality, 2016.

[20] D. Nilsson, P.Phung, and U.Larson, "Vehicle ECU classification based on safety security characteristics", IET Road Transport Information and Control - RTIC 2008 and ITS United Kingdom Members' Conference,2008.