International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 3 Issue: 3 18-Sep-2014,ISSN_NO: 2321-3337

# COMPARISON BETWEEN HUMMINGBIRD AND ALE ALGORITHMS

[1,] Dr.K.Ravikumar,[2,] S.Anbueniyal[3,] A.Arokiya Benita

Asst. Professor Dept. of computer Science [1], Research scholar[2]

Department of Computer Science, Tamil University, Thanjavur

***ABSTRACT***−*This paper includes a fair comparison between the widely used algorithms in the data encryption field. The two main characteristics, which indentify and differentiate one from another by its ability to secure data against attacks. This paper provides comparison between to widely used encryption algorithms: Hummingbird and ALE encryption algorithms. The comparison has been conducted by running the process of different sizes of data blocks to evaluate the algorithm speed and quality. The presented comparison takes into consideration the behavior and performance of the algorithm with different data size.*

**Keyword: ALE, Hummingbird**

## 1. INTRODUCTION

Encryption is a process of converting “unhidden” text to a “hidden” text to secure it against attacks. This process has another part where hidden text to be decrypted at the other end to be visible to all.

## 2. DATA ENCRYPTION ALGORITHMS

ALE: Authenticated light weight encryption algorithm, is the new encryption standard. The basic operation of ALE is the AES round transformation and the AES 128 key format. ALE is an online single pass authenticated encryption algorithm that supports operational associated data. ALE which is efficient both in hardware and software. It has a 256-bit secret internal state depended on both key and nonce. ALE is about half the size of AES-OCB. In the terms of speed for medium size messages in the light weight implementation, ALE is about 2.5 times faster than AES-OCB and about 4.5 times faster than ASE in its smallest implementation ALE in software using AES-NI instructions on a sandy bridge.

### 2.1 ALE Algorithm

ALE is an online single pass nonce based authenticated data encryption algorithm. Its encrypts and accepts 128 bit master key m, a message μ, associated data α and a 128 bit nonce $\nu \neq 0$.

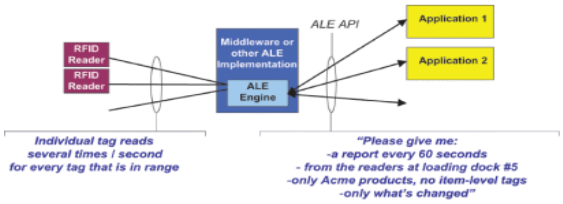
**ENCRYPTION OPERATIONS IN ALE:**

i. Padding

ii. Initialization

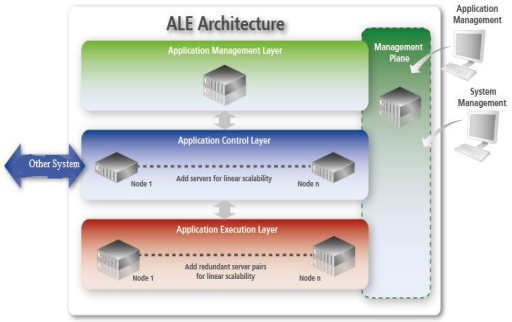
iii. Processing associated data

iv. Processing message




*Encryption and authentication technique of ALE*

### 2.2 Hardware architecture




**ALE includes the three layers:**

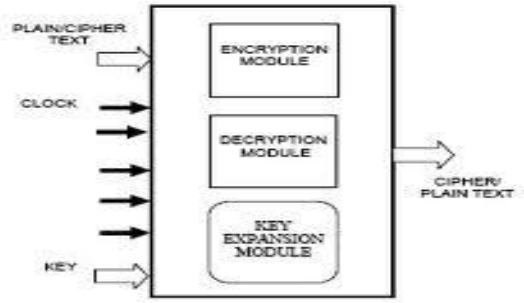
1. Application management layer Management layer for configuration and monitoring.

2. Application control layer Control layer for protocol level interaction with other system
3. Application execution layer For processing logic application

## 3. Hummingbird Algorithm

Hummingbird is an ultra-light weight encryption scheme used for privacy preserving identification and authentication protocol for RFID application. Hummingbird provides security with a small block size and also stringent response time and power consumption. Hummingbird listen elegant combination of above to cipher structure with a 16 bit block size, 256 bit key size and 80 bit internal state. The size of key and bit block size of Humming bird provides security level which is applicable for any RFID applications.

### 3.1 Encryption and decryption:




### 3.2 Attacks avoided by Hummingbird:

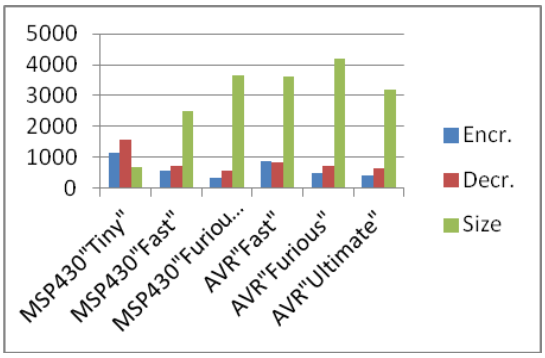
- Birthday Attack on the initialization
- Differential cryptanalysis
- Linear cryptanalysis
- Structural Attack
- Algebraic Attacks
- Cube Attack

**Encryption and Decryption process of ALE:**

| Design | Area (GE) | Net per 128-bit block (cc) | Overhead per message(CC) | Power (uW) |
|---|---|---|---|---|
| AES-ECB | 2,437 | 226 | - | 87.84 |
| AES-OCB2 | 4,611 | 226 | 451 | 171.23 |
| AES-OCB2 e/d | 5,915 | 226 | 451 | 211.01 |
| ASC-1 A | 4,792 | 370 | 902 | 169.11 |
| ASE-1A e/d | 4,963 | 374 | 902 | 193.71 |
| ASE-1B | 5,516 | 234 | 902 | 207.13 |
| ALE | 2,570 | 105 | 678 | 94.87 |
| ALE e/d | 2,709 | 105 | 678 | 102.32 |

**Encryption and Decryption of Hummingbird:**

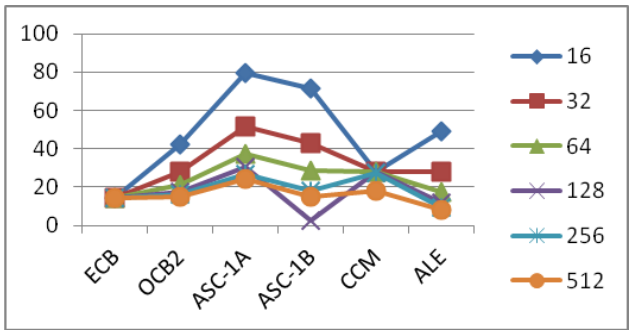
| Target | Encr. | Decr. | Size |
|---|---|---|---|
| MSP430"Tiny" | 1150 | 1555 | 670 |
| MSP430"Fast" | 566 | 729 | 2510 |
| MSP430"Furious" | 333 | 570 | 3648 |
| AVR"Fast" | 890 | 830 | 3600 |
| AVR"Furious" | 475 | 720 | 4178 |
| AVR"Ultimate" | 395 | 642 | 3200 |




**Hardware implementation of ALE compare with other:**

Massage in bytes

| Algorithm | 16 | 32 | 64 | 128 | 256 | 512 |
|---|---|---|---|---|---|---|
| ECB | 14.11 | 14.11 | 14.11 | 14.11 | 14.11 | 14.11 |
| OCB2 | 42.38 | 28.25 | 21.19 | 17.66 | 15.89 | 15.03 |
| ASC-1A | 79.62 | 51.38 | 37.25 | 30.19 | 26.66 | 24.15 |
| ASC-1B | 71.19 | 42.94 | 28.81 | 2.66 | 18.22 | 15.15 |
| CCM | 28.25 | 28.25 | 28.25 | 28.25 | 27.22 | 18.25 |
| ALE | 48.93 | 27.75 | 17.15 | 11.85 | 9.21 | 7.88 |




**Hardware implementation of Hummingbird2:**

| Profile | Frequency | Clocks per | Peak | Leakage | Area | Gate equiv. |
|---|---|---|---|---|---|---|

| | | word | | | | |
|---|---|---|---|---|---|---|
| HB2-ee4c<br>HB2-ee4c | 100kHz<br>10MHz | 8<br>8 | 1.93<br>163.1 | 4.17<br>4.17 | 27381<br>27381 | 3220<br>3220 |
| HB2-ee16c<br>HB2-ee16c | 100kHz<br>10MHz | 32<br>32 | 1.845<br>156.8 | 2.85<br>2.85 | 20871<br>20871 | 2332<br>2332 |

| **ALE: AES based light weight authenticated encryption** | **Hummingbird light weight authenticated encryption** |
|---|---|
| ALE is an online single pass authenticated encryption algorithm | Hummingbird encryption scheme is used in RFID tags |
| ALE supports operational associated data | Hummingbird I combination of block cipher and steam cipher |
| It has 256-bit secret internal state dependent on both key and nonce | It is an combination of 16 bit block size, 256 bit key size, 80 bit internal state |
| It includes operational steps: Padding, Initialization, Processing message, finalization | This protocol separates the phases of private identification and mutual identification |
| For long message ALE needs only about 4AES rounds to both encrypt and authenticate a block of message | It encrypts 16 bits at a time within 20 clock cycles |
| AES encryption engine is needed for both encrypt and decrypt by ALE | It used ISO18000-6c protocol |
| ALE resistant in distinguishing attacks, slide attacks | It resistant many attacks: Linear attacks, Structure attack, etc,. |

## CONCLUSION

The simulation process is taken between Hummingbird and ALE encryption algorithm in data encryption field to find the better performance. Since ALE is not known any weak points as longer. ALE is showing the good process and memory allocation than Hummingbird. Same as Hummingbird used in low cost RFID also. We going on the process with other category comparison between these two further we conclude the best one.

## REFERENCES

**[1]** Daniel Engels, Markku-Juhani O. Saarinen, Peter Schweitzer, and Eric M. Smith **"**The Hummingbird-2 Lightweight Authenticated Encryption Algorithm"

[2] E. BIHAM AND A. SHAMIR. "Differential Cryptanalysis of the Data Encryption Standard." Springer (1993)

[3] Andrey Bogdanov1, Florian Mendel2, Francesco Regazzoni3,4, Vincent Rijmen5, and Elmar Tischhauser "ALE: AES-Based Lightweight Authenticated Encryption"

[4] Daniel Engels2, Xinxin Fan1, Guang Gong1,
Honggang Hu1, and Eric M. Smith2 Ultra-Lightweight Cryptography for Low-Cost RFID Tags: Hummingbird Algorithm and Protocol

[5] K. Akdemir, M. Dixon, W. Feghali, P. Fay, V. Gopal, J. Guilford, G.W. Erdinc Ozturk, and R. Zohar. Breakthrough AES Performance with Intel AES New Instructions. Intel white paper, January 2010.