The security of Symmetric Cipher Algorithms in IoT Applications

Dr. Khalid Fadhil Jasim

Department of Computer Science
Cihan University-Erbil, Erbil, Iraq
khalid.jassim@cihanuniversity.edu.iq

Outlines

- Introduction
- Cipher Algorithms
- PRESENT Cipher
- DESXL Cipher
- CLEFIA Cipher
- AES Cipher
- Conclusions and Future Work

Introduction

- **Lightweight cryptography** is a developing term which **secures** the **information** in an improved way utilizing **low assets** and giving **higher throughput**, and having **low power** utilization.
- **Security**, **Cost**, and **Performance** are three noteworthy parts to deal with for each lightweight cryptographic architect.
- **In 1998** by Kevin Ashton, the expression **"IoT"** was **introduced** for the first time is a future of internet and widespread computing.
- **IoT** is a shortening of "**Internet of Things**."

Introduction (Cont.)

- "**Things**" are **associated** physically and are **accessed through the web**.
- **Things** can be anything like **home appliances, vehicles, machines**, etc., which can speak with each-other without manual help.
- This **procedure of association** between **smart devices** is referred as "**machine to-machine**" (M2M) **communication** [4].
- In this embedded technology there are few building blocks of **architecture: Sensors/computers, Internet gateways, Cloud/server** framework and **Big Data**, lastly **End users**.

Introduction (Cont.)

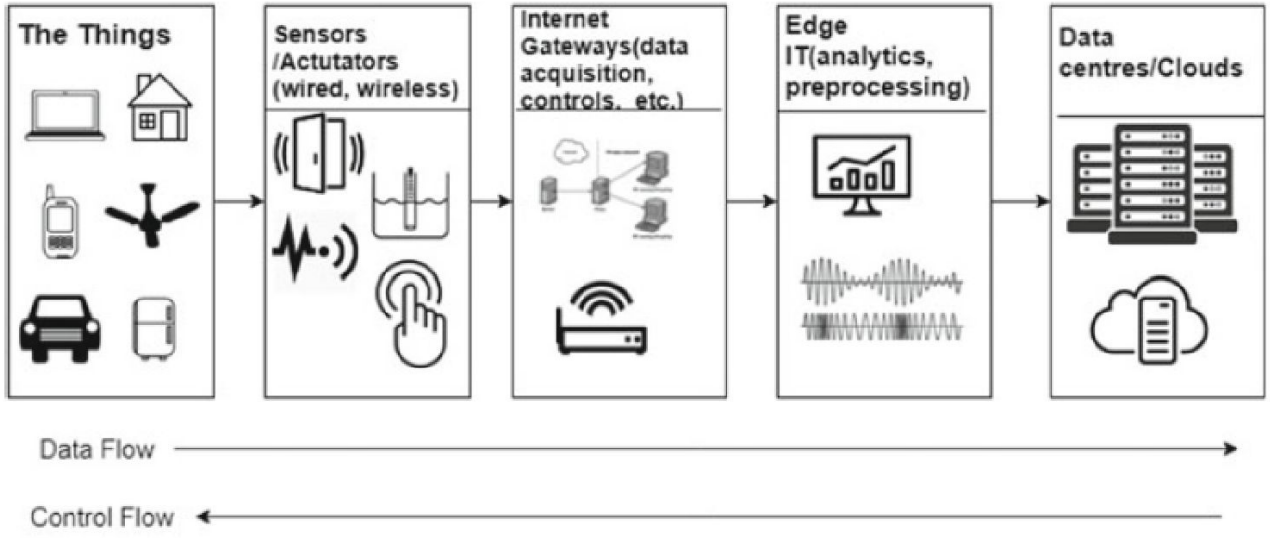


Fig. 1: Architecture of internet of things (IoT)

Cipher Algorithms

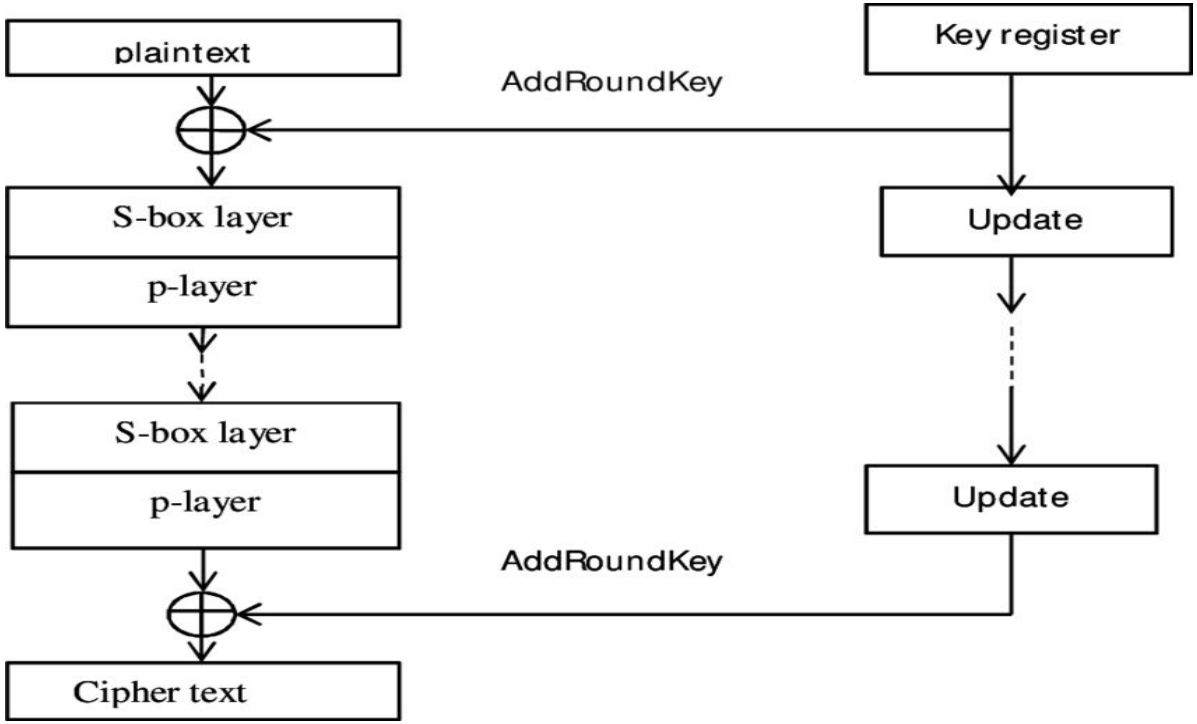
- Some Lightweight symmetric cryptographic algorithms which are PRESENT, DESXL, CLEFIA, etc. Next is AES [6] another block cipher was implemented on different platforms.
- These Cipher Algorithms designed based on Block Ciphers techniques.
- These cipher algorithms proposed for the security of IoT applications.

PRESENT Cipher

- **PRESENT** is a lightweight block cipher, developed by the Orange Labs (France), Ruhr University Bochum (Germany) and the Technical University of Denmark .
- ***PRESENT*** is intended to be used in situations where low-power consumption and high chip efficiency is desired.

Cipher detail	
Key sizes	80 or 128 bits
Block sizes	64 bits
Structure	SPN (Substit. , Permut. Net.)
Rounds	31

PRESENT Cipher (Cont.)



DESXL Cipher

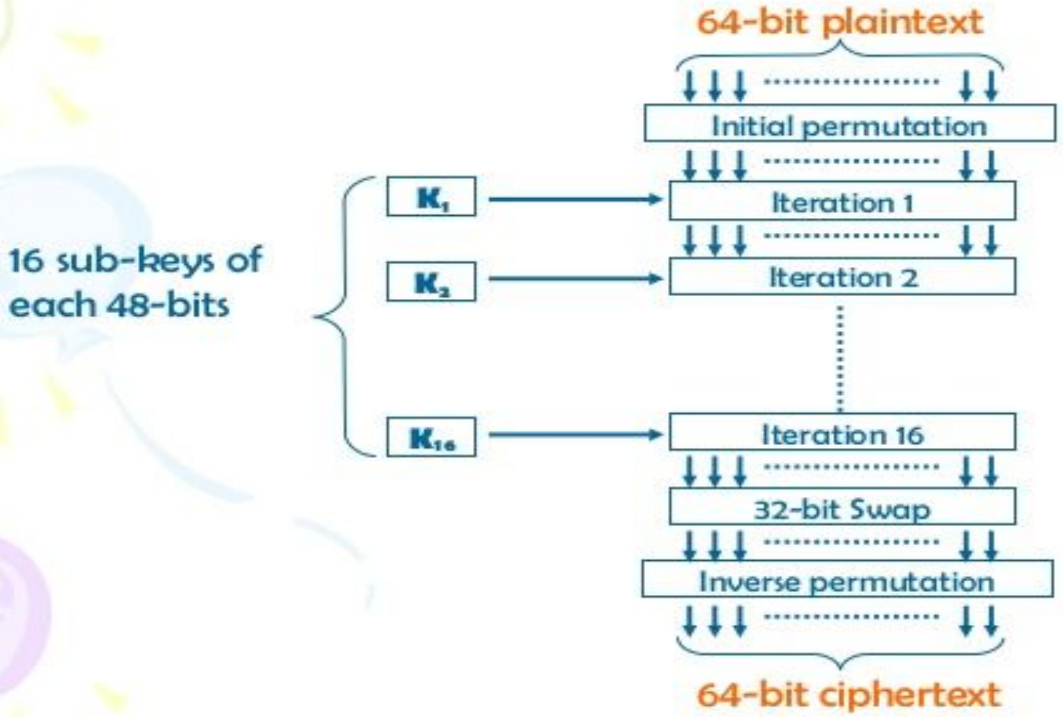
- DESXL lightweight variants of the DES cipher.
- All eight DES S-boxes are replaced by a single S-Box.
- Key of the form: $DESX_{k,k1,k2}(x) = k2 \oplus DES_k(k1 \oplus x)$.
- The main goal of the developer was a low gate count in hardware implementations as for the original DES.

DESXL Cipher (Cont.)

- The **Data Encryption Standard** (**DES**) is a symmetric-key algorithm for the encryption of electronic data. Although its short key length is of 56 bits.
- It was highly influential in the advancement of modern cryptography.

Cipher detail	
Key sizes	56 bits (+8 parity bits)
Block sizes	64 bits
Structure	Balanced Feistel network
Rounds	16

DES Encryption Diagram

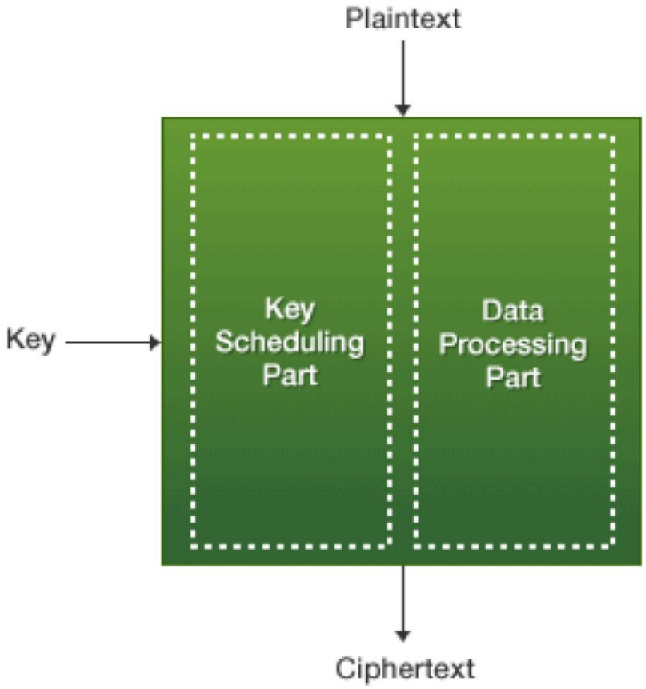


CLEFIA Cipher

- **CLEFIA** is a proprietary block cipher algorithm, developed by Sony. Its name is derived from the French word clef, meaning "key".
- The block size is 128 bits and the key size can be 128 bit, 192 bit or 256 bit. It is intended to be used in DRM systems (Digital Right Managements). It is recommended candidate for Japanese

Cipher detail	
Key sizes	128, 192, or 256 bits
Block sizes	128 bits
Structure	Feistel network
Rounds	18, 22, or 26

CLEFIA Cipher (Cont.)



AES Cipher

- **AES** is developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal[5] to NIST during the AES selection process.[6].
- Rijndael is a family of ciphers with different key and block sizes.

Cipher detail	
Key sizes	128, 192 or 256 bits
Block sizes	128 bits
Structure	Substitution–permutation network
Rounds	10, 12 or 14 (depending on key size)

AES Cipher (Cont.)

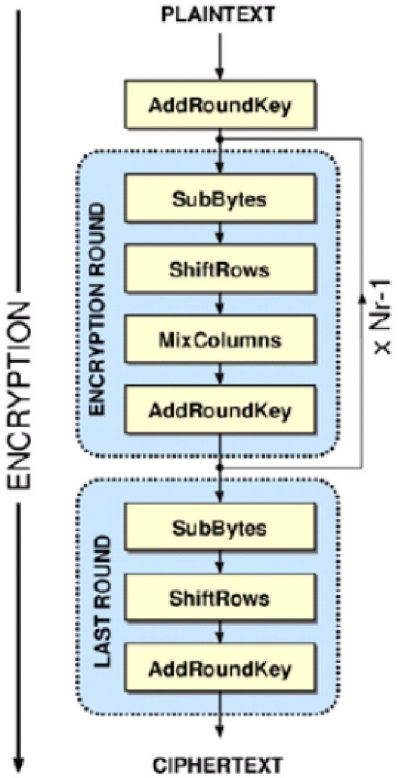


TABLE 1. Comparison of Symmetric Ciphers

	Symmetric Ciphers			
	PRESENT	DES	CLEFIA	AES
Type of Cipher	Block Cipher	Block Cipher	Block Cipher	Block Cipher
Secret Key Size	80 or 128 bits	56 bits	128, 192, or 256 bits	128, 192, 256 bit
Computational Complexity of Secret Key	2^{80} , 2^{128}	2^{56}	2^{128} , 2^{192}, 2^{256}	2^{128}, 2^{192}, 2^{256}
Block Size	64 bit block	64 bit block	128 bits block	128 bit block
Algorithm Structure	SPN, -Substitution, -Permutation Network	Feistel Network	Feistel Network	-Bytes Substitution, -Shift Rows, (Byte Permute), -Mix Columns, (Linear Transform), -Add Round Key
No. of Rounds	31	16	18, 22, or 26	10, 12, 14

Conclusions

- This **research provides a comparative study** of some **symmetric ciphers** such as **PRESENT, DESXL, CLEFIA, and AES** cipher, which have been proposed for the **security of IoT applications.**
- These **symmetric ciphers** are **very efficient at processing** large amounts of information and have been used to **maintain information confidentiality, authenticity, and integrity.**
- The **comparison** (Table 1) illustrates **secret key size,** computational **complexity of secret key**, **block size**, and **number of rounds.**

Conclusions (cont.)

- These **algorithms** can **withstand against** some **cryptanalysis techniques** (e.g. Man-in-the-center attack, Differential attacks, and key-IV attack, etc.).
- Finally, **Future analysts** can work on **different lightweight algorithms** and investigate other **cryptanalysis techniques for IoT applications.**

THANK YOU