Journal of Network and Computer Applications 49 (2015) 15–50

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments

Jia Hao Kong [a,*], Li-Minn Ang [b], Kah Phooi Seng [b]

[a] Department of Electrical and Electronic Engineering, University of Nottingham, Malaysia Campus, 43500 Semenyih, Malaysia
[b] School of Engineering, Edith Cowan University, Joondalup, WA 6027, Australia

ARTICLE INFO

Article history:
Received 16 February 2014
Received in revised form
10 August 2014
Accepted 16 September 2014
Available online 14 October 2014

Keywords:
Symmetric cipher
Lightweight block cipher
WSN
RFID
WISP
IOT

ABSTRACT

Modern cryptographic algorithms play an irreplaceable role in data communication systems for various areas of applications. These algorithms are the backbone of data protection and secrecy for highly sensitive and classified data. The selection of a suitable crypto-algorithm will dynamically affect the lifespan and performance of a device in terms of battery-life, hardware memory, computation latency and communication bandwidth. In the current developments of the resource constrained environments, the trend is shifting towards lightweight algorithmic hardware designs. To select a suitable cryptographic algorithm for an application or an environment, the understandings of both the algorithmic requirements in terms of hardware and the specifications of the development platform intended has to be established. However, there are numerous ciphers in the literature that has various functionality, specifications and strength. Moreover, there are numerous literatures that cover the trend and specifications of security solutions in hardware constrained environment, employing known cryptographic algorithms. In this paper, we present a comprehensive survey of modern symmetric cryptographic solutions used in resource constrained environment (RCE), including literatures from the area of wireless sensor network (WSN), radio frequency identification (RFID), wireless identification and sensing platform (WISP) and other resource constrained platforms. This paper aims to provide a survey of the ciphers that were used in the past, and what are the ciphers that are currently active, and their respective specifications and applications in the area of modern world RCEs. On top of that, descriptive summaries of (a total of 100 symmetric ciphers) modern block ciphers (38), involution ciphers (6), lightweight block ciphers (28) and stream ciphers (28) are included and discussed, and an overview of the current contributions of various literatures, comparison and analysis of modern ciphers from the hardware and software perspective are also discussed.

Contents

1. Introduction 17
2. Resource constrained environments and cryptographic approaches 19
   2.1. Wireless Sensor Network (WSN) RCE 19
   2.2. Radio Frequency Identification (RFID) RCE 23
   2.3. Wireless Identification and Sensing Platform (WISP) RCE 26
   2.4. Internet of Things (IOT) RCE 27
   2.5. Other reviews or surveys on cipher candidates 29
3. Taxonomy of symmetric cryptographic solutions in resource constrained environments 29
   3.1. Modern symmetric key block ciphers 29
   3.2. Involution ciphers 29
   3.3. Lightweight symmetric block ciphers 29
   3.4. Stream ciphers 29
   3.5. Substitution-Permutation Network (SPN) 30

* Corresponding author.
E-mail addresses: keyx9kjh@nottingham.edu.my (J.H. Kong), li-minn.ang@ecu.edu.au (L.-M. Ang), kp.seng@ecu.edu.my (K.P. Seng).

http://dx.doi.org/10.1016/j.jnca.2014.09.006
1084-8045/© 2014 Elsevier Ltd. All rights reserved.

3.6. Feistel network (FN) . . . 30
4. Modern symmetric key block ciphers . . . 30
4.1. 3DES (triple DES, TDEA) . . . 30
4.2. 3-Way . . . 30
4.3. A5/3 (also known as the KASUMI) . . . 30
4.4. Advanced Encryption Standard (AES, Rijndael) . . . 32
4.5. Blowfish . . . 32
4.6. Camelia . . . 32
4.7. CAST-128 . . . 32
4.8. CAST-256 . . . 32
4.9. Crypton . . . 32
4.10. CURUPIRA-1 . . . 32
4.11. CURUPIRA-2 . . . 32
4.12. DEAL . . . 32
4.13. Data Encryption Standard (DES) . . . 32
4.14. FEAL-4 . . . 33
4.15. Feal-N/Nx . . . 33
4.16. GOST . . . 33
4.17. ICE . . . 33
4.18. International Data Encryption Algorithm (IDEA) . . . 33
4.19. Khafre . . . 33
4.20. Khufu . . . 33
4.21. LOKI97 . . . 33
4.22. Lucifer . . . 33
4.23. Magenta . . . 33
4.24. Mars . . . 33
4.25. MISTY-1 . . . 33
4.26. MISTY-2 . . . 34
4.27. Rainbow . . . 34
4.28. RC2 . . . 34
4.29. RC5 . . . 34
4.30. RC6 . . . 34
4.31. SEED (SEED 128) . . . 34
4.32. SEED 192/256 . . . 34
4.33. Serpent . . . 34
4.34. Shark . . . 34
4.35. Skipjack . . . 34
4.36. Square . . . 34
4.37. Threefish . . . 35
4.38. Twofish . . . 35
4.39. Summary of ciphers . . . 35
5. Involution cipher . . . 35
5.1. Anubis . . . 35
5.2. ARIA . . . 35
5.3. ICEBERG . . . 35
5.4. KHAZAD . . . 35
5.5. PP-1 . . . 35
5.6. PUFFIN . . . 35
5.7. Summary of ciphers . . . 35
6. Lightweight block ciphers . . . 35
6.1. CLEFIA . . . 35
6.2. DESL . . . 35
6.3. DESX . . . 37
6.4. DESXL . . . 37
6.5. DST40 . . . 37
6.6. EPCBC . . . 37
6.7. HIGHT . . . 37
6.8. KATAN . . . 38
6.9. KEELOQ . . . 38
6.10. KLEIN . . . 38
6.11. KTANTAN . . . 38
6.12. LBlock . . . 38
6.13. Light Encryption Device (LED) . . . 38
6.14. Miniature CRYPTON (mCRYPTON) . . . 38
6.15. MIBS . . . 38
6.16. NOEKEON . . . 38
6.17. Piccolo . . . 38
6.18. PRESENT . . . 38
6.19. PRINCE . . . 39
6.20. PRINTcipher . . . 39
6.21. Scalable Encryption Algorithm (SEA) . . . 39
6.22. SIMON . . . 39