Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 199 – 209

Procedia Computer Science

1st International Conference on Information Security and Privacy

"Cryptic Mining for Automatic Variable Key based Cryptosystem"

"Shaligram Prajapat a*, Ramjeevan Singh Thakur b"

"a Maulana Azad National Institute of Technology a(MANIT) and Devi Ahilya University, IIPS D.A.V.V., Indore 452001,INDIA"
"Maulana Azad National Institute of Technology a(MANIT) ,Bhopal462003 ,Madhya Pradesh,INDIA"

Abstract

This paper presents evolution of Automatic variable key cryptosystem with study and analysis of state of symmetric cryptosystem. It presents framework of AVK model and extension by parameterized approach.The evaluation of cryptosystem from perspective of cryptanalyst has been presented. The paper opens direction of "Cryptic Mining "discipline. The AVK approach finds application in low power secure device communication, which is most desirable feature of Internet of Things.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords:"Automatic Variable Key;Symmetric Key Cryptosystem; perameterized AVK; Internet of Things (IOT)"

1. Intoduction

The importance of low power devices and device to device communication is the central demand in framework of internet of things (IOT). The security of these devices together with a balance with power efficiency will decide the long term of sustainability of the system. Automatic variable key is also gaining pace and finding it's applicability in low power devices. Due to short life period of key and small size makes it promising candidate for energy efficient secure communication. Parameterized key based cryptosystem, will add one more level of security in the design of efficient cryptosystem. We provides idea of Automatic Variable key, A framework of Key exchange by parameters only, it's importance and benefits and investigation of AVK based framework from hackers/cryptanalyst perspective and evolution of cryptic mining discipline. This specialized study will be useful for auditing of AVK based cryptosystem.

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.034

Information security plays a pivotal role nowadays. So far as per literature survey the key is fixed during the entire transmission hence the probability of frequency attack increases in case of redundant message transmission. Here first we focus the current way of handling key with increasing key size of symmetric key based cryptosystems and its future consequences. Later, we will present some technique where the key is made to vary from session to session hence even though the hacker hacks the key of session i it will be not valid for original message extraction in session i+1 onwards. We can also enhance the security level based on variability concept applied on the message using an optimum function accordingly the receiver will receive the data correctly after the application of reverse operation of that particular operation.

Another aspect of this chapter is the method of shared key computation using parameterized approach. In this section we have pointed out the method of key generation without the transmission of entire key throughout the communication channel .Hence instead of just passing the entire key we will transmit the parameters only. The standard we compute a result based on a particular function involving those parameter and receiver will also do so. The beauty of this section is that even though the sender and receiver has applied two different function with identical parameters value but still the result is similar and hence that is the shared key used for the communication among themselves. Hence from our original contribution in this section we can reveal that in cryptology there is no need to send the entire key to the receiver. The further scope of what in this section is generation of a patent provided there is generation of key based on reversible function like XOR.

Cipher text = F_Encrypt (plaintext, key)
Plaintext =F_Decrypt (Cipher text, key)
Traditionally F_Encrypt and F_Decrypt= XOR operation ($\oplus$)

Symbolically: $Y = X \oplus K$, If we get the value of Y and knowing K then we will get X from $X = K \oplus Y$. This leads to scope for investigation of another similar reversible function.

1.1. Analysis of convention fixed length key with increasing key size

In this section we will focus on background for AVK based cryptosystem. For this we will first focus on some popular symmetric cryptic algorithms and will present the behavior of encryption and decryption of symmetric cryptic algorithm, using a web based tool(SGcrypter) dedicatedly developed for this purpose and will find out efficient algorithm among DES,3DES, BlowFish, TwoFish. These algorithm increases key size to enhance security.

Table 1. Some Symmetric key algorithms

S. No.	Algorithm	Block size	Key length
1	DES	64 bits	56 bits
2	3DES	64 bits	168, 112 or 56 bits
3	RC2	64 bits	8-128 bits (variable length key)
4	Blowfish	64 bits	32-448 bits (variable length key)