

# Implimentation of Cryptographic Algorithm for GSM and UMTS Systems

<sup>1</sup>Alpesh R. Sankaliya, <sup>2</sup> V.Mishra and <sup>3</sup>Abhilash Mandloi

Department of Electronics

Sardar Vallabhbhai National Institute of Technology, Surat-395007

Gujarat, India

<sup>1</sup>alpeshrs@yahoo.com, <sup>2</sup>vive@eced.svnit.ac.in and <sup>3</sup>asm@eced.svnit.ac.in

*Abstract— Due to extremely high demand of mobile phones among people, over the years there has been a great demand for the support of various applications and security services. Cryptographic algorithms used by Mobile Subscribers to protect the privacy of their cellular voice and data communication. Cipherring provides the mean to regain control over privacy and authentication. A5/x are the encryption algorithms used in order to ensure privacy of conversations on mobile phones. A5/3 encryption algorithm used for 3G and GEA3 encryption algorithm used for GPRS. f8 is confidentiality algorithms developed by 3GPP used in UMTS System. The following paper is based on simulation of A5/3 and f8 algorithms.*

Keywords- Mobile security, Security, Cryptography , Stream Cipher, A5/3, f8.

## 1. INTRODUCTION

Encryption in mobile communication is very crucial to protect information of the subscribers and avoid fraud. In the GSM security layer, A5 stream cipher is used, which employs a 64-bit secret key [1]. Versions A5/1 and A5/2 were kept secret for a long period of time. Since the GSM A5 algorithm was developed, the climate for cryptography has changed substantially [2]. Recently, A5/1 and A5/2 were reverse-engineered from a GSM handset and published by Briceno et al. [2]. Afterwards A5/2 was cryptanalysis and proved to be completely insecure. The attack required very few pseudo random hits and only 216 steps [1][3]. A new security algorithm, known as A5/3 for GSM and F8 for UMTS provides users of mobile phones with an even higher level of protection against eavesdropping than they have already [4][5].

A5/3 and f8 have been developed by a joint working party between the GSM Association Security Group and the 3<sup>rd</sup> Generation Partnership Project (3GPP)[10]. It will also be applicable for the General Packet Radio Service (GPRS) where it will be known as GEA3, and other modes such as High Speed Circuit Switched Data (HSCSD) and Enhanced Data Rates for GSM Evolution (EDGE) [5][6]. The A5/3 and f8 encryption algorithm specifically supplies signaling protection, so that sensitive information is protected over the radio path, and user data protection, to protect voice calls and other user generated data passing over the radio path [18].

## 2. GSM AND UMTS CIPHERING ALGORITHM FOR 3G

Third generation mobile system offering mobile users content rich services, wireless broadband access to internet, and worldwide roaming. However, this includes serious security vulnerabilities. In this document are specified two ciphering algorithms: A5/3 for GSM and F8 for UMTS. The algorithms are stream ciphers that are used to encrypt/decrypt blocks of data under a confidentiality key **KC**. Each of these algorithms is based on the **KASUMI** algorithm

International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011  
 which is a block cipher that produces a 64-bit output from a 64-bit input under the control of a 128-bit key. The algorithms defined here use **KASUMI** in a form of output-feedback mode as a keystream generator.

The UMTS confidentiality mechanism operates on both signaling information and user data. The algorithm defined to perform the confidentiality tasks is called  $f_8$  and operates on the following way: First, using the ciphering key CK, and some other parameters, the  $f_8$  algorithm in the user equipment computes an output bit stream. Second, this output bit stream is xored bit by bit with the data stream, also called plaintext, in order to obtain a ciphered data block or ciphertext. Third, the ciphertext is send to the network through the radio interface. Fourth, the  $f_8$  algorithm in the RNC uses the same inputs as the user equipment, including the shared cipher key CK, to generate the same output bit stream that was computed in the user equipment. Finally, the output bit stream is xored with the ciphertext received to recover the initial information.

The Two algorithms are all very similar. **KGCORE** function is shown in Fig.1. Table 1 gives the detail of variables used in figure. KASUMI used in these algorithms is the Feistel cipher with eight rounds with associated subkeys (KL, KI and KO), which is generated from CK using rounding manner. It operates on a 64-bit data block and uses a 128-bit key. Its eight rounds are shown in Fig 2. Each KASUMI operator uses FL and FO functions. In each odd round of KASUMI operator uses  $R_i = FO(FL(L_{i-1}, KL_i), KO_i, KI_i)$  function and for each even round uses  $R_i = FL(FO(L_{i-1}, KO_i, KI_i), KL_i)$ . The FL and FO algorithms based on number of iteration round with substitutions (S-Boxes) and permutations (PBoxes) shown in Fig 3 and 5.

In FL algorithm  $R' = R \text{ exor } \text{ROL}(L \text{ bit-and } KL_{i,1})$ ,  $L' = L \text{ ex-or } \text{ROL}(R \text{ bit-or } KL_{i,2})$ . In FO algorithm  $R_j = FI(L_{j-1} \text{ ex-or } KO_{ij}, KI_{ij}) \text{ ex-or } R_{j-1}$ ,  $L_j = R_{j-1}$ . In FI algorithm shown in Fig 4 for odd round  $R_i = L_{i-1}$ ,  $L_i = S9[L_{i-1}] \text{ ex-or } ZE(R_{i-1})$ , for 2<sup>nd</sup> round  $L_i = R_{i-1} \text{ ex-or } KI_{i,j,2}$ ,  $R_i = S7[R_{i-1}] \text{ ex-or } TR(L_{i-1}) \text{ ex-or } KI_{i,j,1}$ , for 4th round out =  $S7[L_{i-1}] \text{ ex-or } TR(L_{i-1})$ .

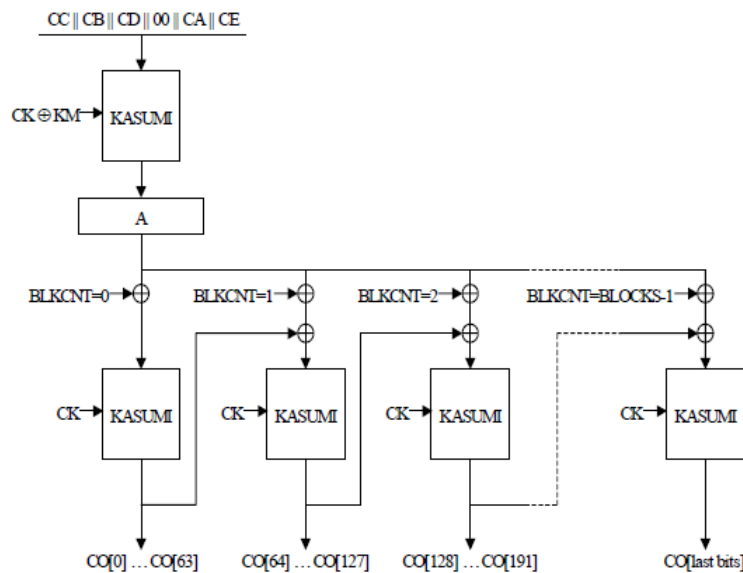


Figure 1. KGCORE Core Keystream Generator Function with  
 KM=0x55555555555555555555555555555555 (in hex)

	A5/3	F8
CA	00001111	00000000
CB	00000	BEARER
CC	INPUT	COUNT
CD	DIRECTION	DIRECTION
CE	0000000000000000	
CK	Cipher Key repeated to fill 128 bits	128 bit
CO	Block1  Block2(114 bit  114bit)	Ks(Key stream)

Table 1: GSM A5/3 & F8 in terms of KGCORE

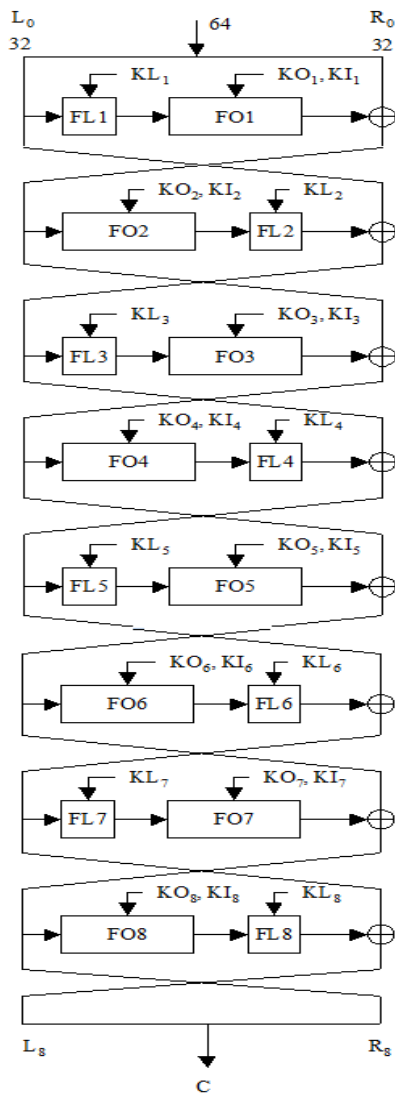


Figure 2. KASUMI algorithm

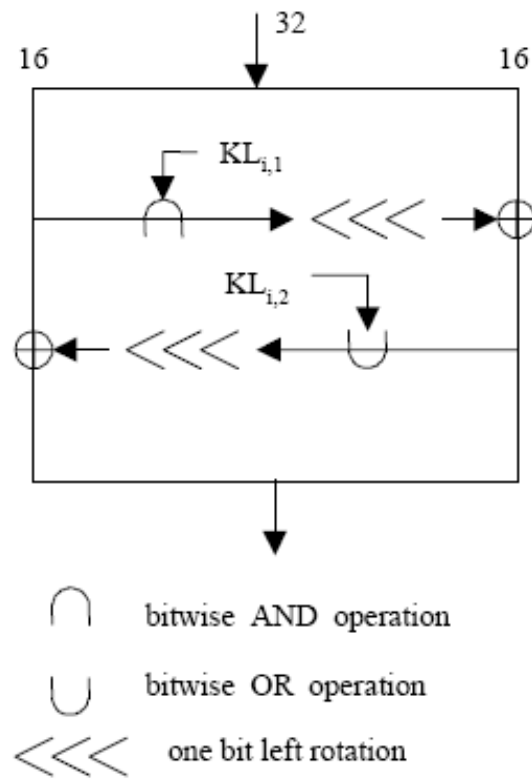


Figure 3. FL algorithm

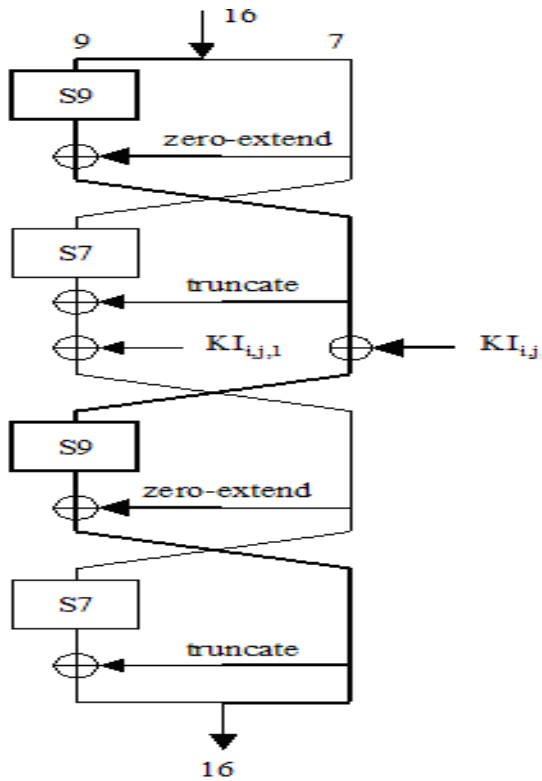


Figure 4. FI algorithm

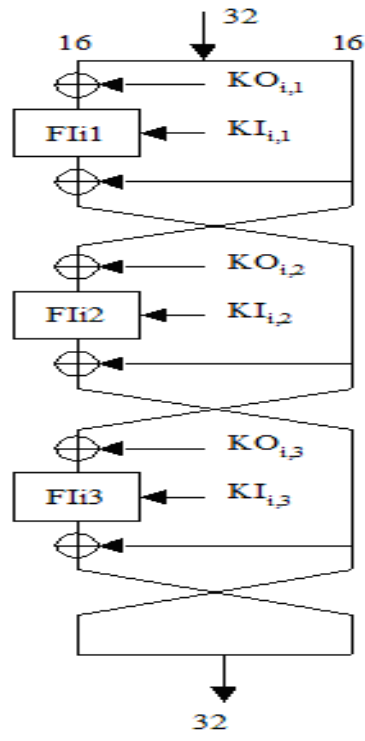


Figure 5. FO algorithm

### Simulation of A5/3 Ciphering Algorithm

The GSM A5/3 algorithm produces 228 bit keystream strings, 114 bit is used for uplink encryption/decryption and the 114 bit is for downlink encryption/decryption. Figure 6 shows simulation of A5/3 algorithm.

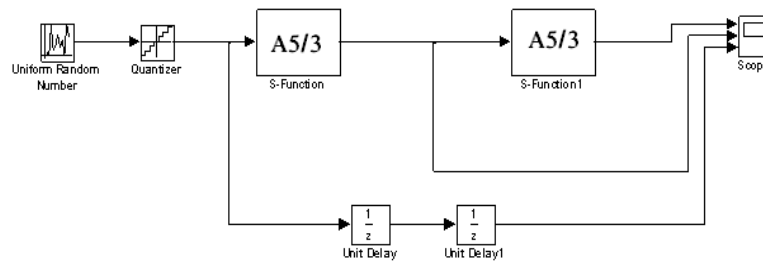


Figure 6. Simulation of A5/3 Algorithm using Matlab

Scope output is shown in Fig. 7 by taking sampling time=0.1ms, key=[16 14 18 23 22 43 12 35 37 11 28 26 25 31 30 29], count=32.

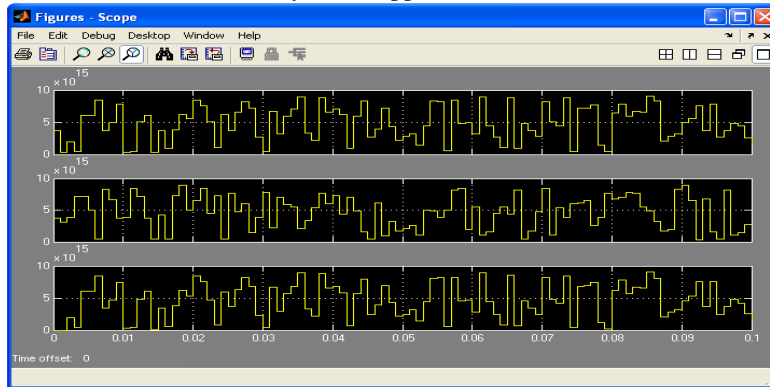


Figure 7. Simulation result of A5/3 Algorithm

### Simulation of F8 Ciphering Algorithm

Simulation of UMTS Encryption Algorithm f8 algorithm is shown in Figure 8 by taking sampling time = 0.1ms, key=[1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16], count=140, bearer=32 and direction of transmission upward.

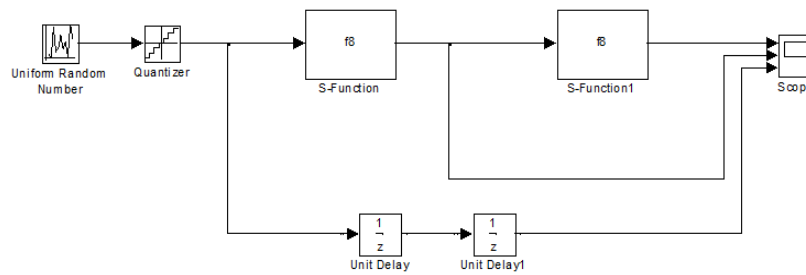


Figure 8. Simulation of f8 Algorithm

Scope output for UEA algorithm(F8) for UMTS is shown in Fig. 7.

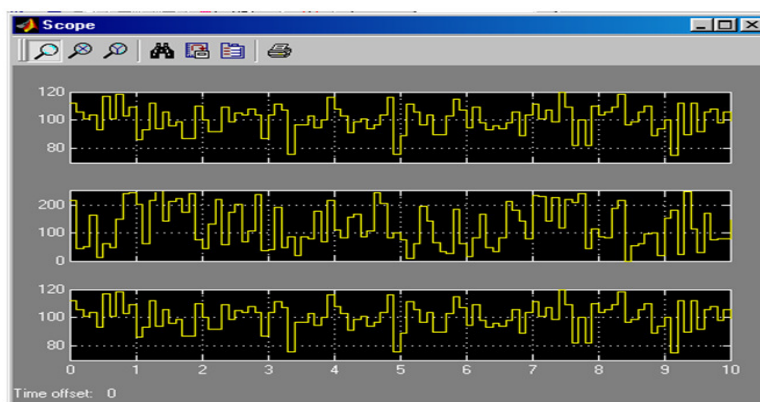


Figure 9. Simulation result of f8 Algorithm

### 3. PERFORMANCE ANALYSIS

The simulation works were carried out on a Pentium Core 2 Duo processor with 3 GB of RAM running on Window7. Codes for A5/3 and f8 were written and executed in MATLAB 7.8. Fig.10 shows the spectrogram of speech\_dft.wav sound in Matlab. The dark bands in Fig 10 are called formants and are frequency of resonance. The darkness of these bands is energy[9]. Modern speech secrecy systems are mainly based on digital enciphering techniques. In the area of speech ciphers, mainly symmetric key algorithms are used. Fig 11 and 12 shows the spectrograms of the plain speech ciphered by A5/3 and f8 algorithms respectively and easily compared the energy band of ciphered signals and easily compared the spectrogram of ciphered signals.

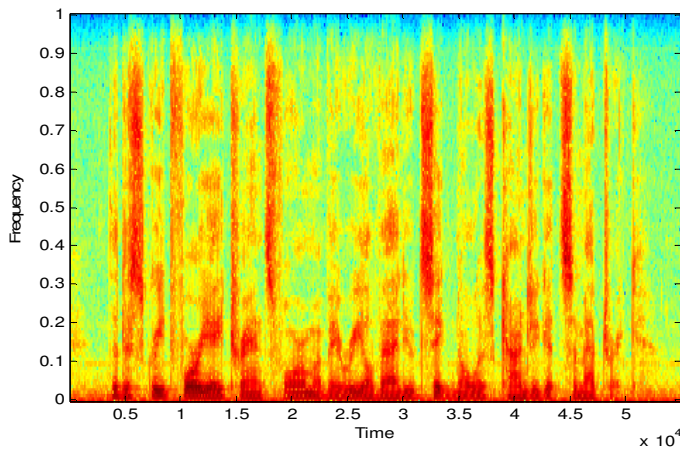


Figure 10 Spectrogram of plain speech

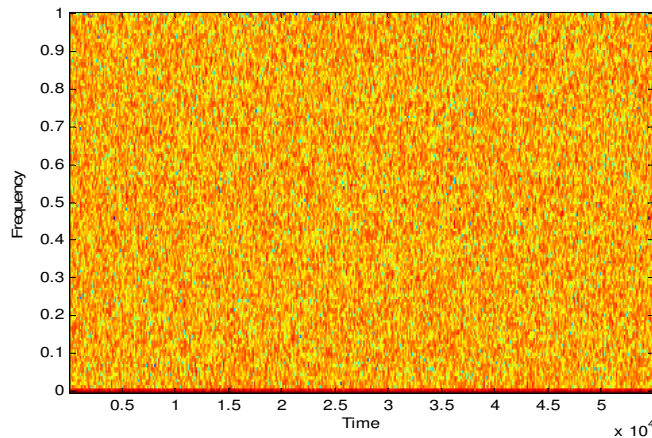


Figure 11. Speech encrypted by A5/3 algorithm

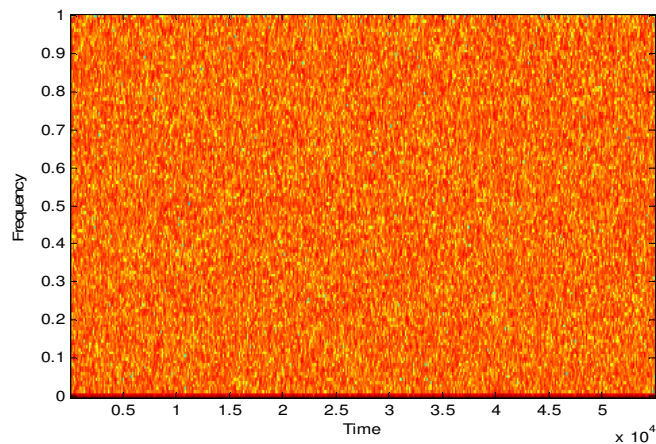


Figure 12. Speech encrypted by f8 algorithm

#### 4. Future Enhancement

A new security algorithm, known as UEA2 and UIA2 will provide users of UMTS mobile phone with an even higher level of against eavesdropping than they have already. It will ensure that, even if a prospective attacker manages to pull a UMTS phone call out of radio waves, he will be completely unable to make sense of it, even if throws massive computing resources at the task. UMTS system use several security element, designed to safeguard the interests of the user, network operator and service providers. The UEA2 and UIA2 algorithms specifically supplies signaling protection, so that sensitive information such as telephone numbers is protected over the radio path, and user data protection, to protect voice call and other user generated data passing over the radio path.

#### 5. CONCLUSION

Now a Days Mobile communication system is vulnerable to attack by unauthorised users. A number of vendors are operating around the world and they employ various operating standards and equipments. It has been estimated that computing power doubles every two-three years. An algorithm that is secure today may be secure after 5-6 years. Since any algorithms being designed today must work for many years after design.

#### REFERENCES

- [1] <http://www.cryptography.com/>
- [2] Bruce Schneier, " *Applied Cryptography*," John Wiley & Sons Inc., 1996,New York
- [3] C E Veni Madhavan & P K Saxena, " *Recent Trends in Applied Cryptology* ", IETE Technical Review, Vol 20, No 2, March-April 2003.
- [4] V. K. Garg, " *Wireless and Personal Communication System* ", 1997 Prentice Hall of India Private Ltd.,New Delhi.
- [5] William Stallings, " *Cryptography and Network Security* ", 2006 Prentice Hall, New Jersey

- International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011
- [6] Technical specification of 3GPP TS 55.216 V6.2.0 (2003- 09)
  - [7] Uylesblock , "*Wireless and personal communications system*", 2000 PHI, New Delhi
  - [8] Dr. Kamilo Feher, "*Wireless Digital Communication - Modulation and Spread Spectrum Applications*, 2000" Prentice Hall of India Private Ltd., New Delhi
  - [9] Marc Briceno, Ian Goldberg and David Wagner, "*A Pedagogical Implementation of the A5/I*, 1999.
  - [10] Simon Haykin, "*Communication System*", 2001 Library of Congress in publication Cataloging Data, Singapore.
  - [11] Eli Biham and Orr Dunkelmna, "*Cryptanalysis of the A5/IGSM stream Cipher*", 2000.
  - [12] Ross Anderson, Mike Roe, "*A5-The GSM Encryption Algorithm*", 1994
  - [13] Fayyaz Ahmed, Dr. Mudassar Imran, "*Cryptographic Analysis of GSM Network*", 2009 IEEE
  - [14] Li Wei Dai Zibin Nan Longmei, "*Research and Implementation of a High speed Reconfigurable A5 Algorithm*", 2008 IEEE
  - [15] Xu Huang, Pritam Gajkumar Shah and Dharmendra Sharma "*Protecting from Attacking the man-in-middle in wireless sensor Network with elliptic curve cryptography key exchange*" 2010 Fourth International Conference on Network and System Security
  - [16] Stefan Pitz, Roland Schmitz, Tobias Martin, "*Security mechanism in UMTS*", Datenschutz and Datensicherheit (DUD), vol 25, pp 1-10, 2001
  - [17] Musheer Ahmad and Izharuddin "*Enhanced A5/I Cipher with improved linear Complexity*" 2009 IEEE
  - [18] Stefan Pitz, Roland Schmitz, Tobias Martin, "*Security mechanism in UMTS*", Datenschutz and Datensicherheit(DUD), Vol 25, pp 1-10,2001
  - [19] Geir M. Koen, Telenor R&D and Agder University College, "*An Introduction to wireless security in UMTS*", 2004 IEEE
  - [20] Kaisa Nyberg, "*Cryptographic algorithms for UMTS*", 2004 European Congress on Computational Methods in Applied Sciences and Engineering (ECCOMAS)
  - [21] Wang Yingsong, Chen Wei, "*f8 Keystream Generator with SMS4 as Core Algorithm*" 2009 Fifth International Conference on Information Assurance and Security