On Post Decryption Error Probability in Counter Mode Operation with Explicit Counter Transmittal

Fouz Sattar and Muid Mufti
(Corresponding author: Fouz Sattar)

Department of Electrical Engineering, Univiersity of Engineering and Technology, Taxila, Pakistan
(Email: fouz@ieee.org, muid@uettaxila.edu.pk)
(Received May 3, 2007; revised and accepted Jan. 4, 2008)

Abstract

This paper analyzes the post decryption error probability in Counter mode operation in an error prone communications channel. A finite state stochastic model has been developed that quantifies the impact of bit errors in the ciphertext and cipher synchronization counter. Analytical results are used to compute post decryption error probabilities and are found to be in reasonable agreement with the simulation results.

Keywords: Counter mode, decryption, encryption, error probability, stochastic modelling

1 Introduction

Communications channels are prone to errors due to various physical impairments. Although application of error correcting codes overcomes or reduces the impact of these errors, residual errors can pass through undetected in some cases. These residual errors can in turn have significant impact on the transmitted data if it is block encrypted prior to transmission. Characterization of the effect of encrypting data before transmission over error prone channel and quantifying the impact of residual errors on decryption process is one of the key technical problems.

In [4], the authors have shown that the use of data encryption over an error prone channel significantly increases the post decryption bit error rate (BER) at the receiver. The impact of ciphering on the receiver BER has been analyzed for Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB) modes of operation. The influence of various binary error correction codes and bit interleaving on the receiver BER has also been investigated. However, the results, derived from computer simulations, are only empirical and no analytical relationships have been established between the channel error rate and the receiver BER.

In [10], the author has developed stochastic models to describe the error structures of secret key ciphers. By deriving the first order statistics of these models such as the mean lengths of the error events and mean lengths of time between error events, the author has shown that the end-to-end confidentiality can increase the average post decryption BER by more than an order of magnitude. The scope of the study however is limited to four primary modes of operation: ECB, CBC, CFB and OFB.

With the proliferation of high speed networking the demand for efficient, robust and secure encryption modes is ever increasing. In 2001, the National Institute of Technology and Standards (NIST) included Counter (CTR) mode as one of the standard modes of operation for block ciphers [3]. This mode has received much attention lately in context of secure communications because of its significant efficiency advantages, its ability to be fully parallelized, and its proven security. These features make CTR mode an attractive encryption Algorithm for use in high-speed networking [8]. CTR mode, in combination with CBC-MAC, has been standardized as data link confidentiality mechanism for wireless local area networks [7]. It has also been proposed as an IPsec Encapsulating Security Payload (ESP) confidentiality mechanism [6]. ATM Forum Security Specifications [12] have also standardized CTR mode for encrypting virtual circuits in ATM communications.

Despite the growing popularity of CTR mode and its wide spread standardization and adoption in high speed communications, the performance analysis of this mode of operation in error prone channels still remains an open research subject. While most research efforts on CTR mode focus on investigating its security properties and efficient implementations, the characterization of effect of residual errors on CTR mode operation has never been addressed. We believe that this characterization is most relevant to the design of higher layer encoding Algorithms for image, video and other mixed media transmission, when CTR

encryption is applied at the physical layer. The results presented in this paper are a contribution towards addressing this problem.

2 Approach

CTR mode is a sort of synchronous stream cipher and features the application of the forward cipher to a set of input blocks, called counters, to produce a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext. Decryption process is identical to encryption with plaintext and ciphertext interchanged. The counter values can be explicitly communicated between sender and receiver or they can be maintained at each end with some kind of synchronization mechanism between sender and receiver. In either case, if there is a bit error in the counter value, a bit error may occur independently in any bit position of the decrypted cipher text block, with an expected error rate of fifty percent, depending on the strength of the underlying block cipher. Furthermore, in CTR mode, the bit errors in the decrypted cipher text occur in the same bit position as in the cipher text block; the other bit positions are not affected. Taking these properties into consideration, this paper analyzes the post decryption probability of error in CTR mode operation. The analysis is based on the finite state stochastic characterization of the decryption process. It is assumed that the bit errors before decryption, after all the error control, are independent and any correlated burst error effects have been mitigated using interleaving or any other diversity techniques.

The paper has following organization: Section 3 describes the CTR mode encryption and decryption Algorithms. Sections 4 presents a stochastic model of CTR mode and provides an analysis of the post decryption error probability. Section 5 discusses the analytical results and presents a simulation model for verification of the analytical results. Finally in Section 6, conclusions are given.

3 Review of Counter Mode Operation

3.1 Notations

Let $E_K(M)$ denote a block cipher that takes a key K and n-bit plaintext P to return n-bit ciphertext C.

$f : B \leftarrow A$ denotes a function or mapping which assigns to each element a in A precisely one element b in B.

$|x|$ denotes the length of string x. If $|x|$ is multiple of n then we view it as divided into sequence of n-bit blocks such that $x[i]$ denotes i-th block, $\forall\ i = 0, 1 \ldots L-1$ i.e. $x = x[0] \ldots x[L-1]$ where $L = \frac{|x|}{n}$.

3.2 Operation

Encryption of L-bit message M using CTR mode with key K and n-bit counter ctr is processed as follows:

Algorithm 1 $E_K(ctr, M[0] \ldots M[L-1])$

1: **for** $i = 1 \ldots L-1$ **do**
2: $\quad C[i] \leftarrow E_K(ctr + i) \bigoplus M[i]$
3: **end for**
4: **return** $C[0] \ldots C[L-1]$

Decryption process is identical to encryption and is defined as follows:

Algorithm 2 $D_K(ctr, C[0] \ldots C[L-1])$

1: **for** $i = 1 \ldots L-1$ **do**
2: $\quad M[i] \leftarrow E_K(ctr + i) \bigoplus C[i]$
3: **end for**
4: **return** $M[0] \ldots M[L-1]$

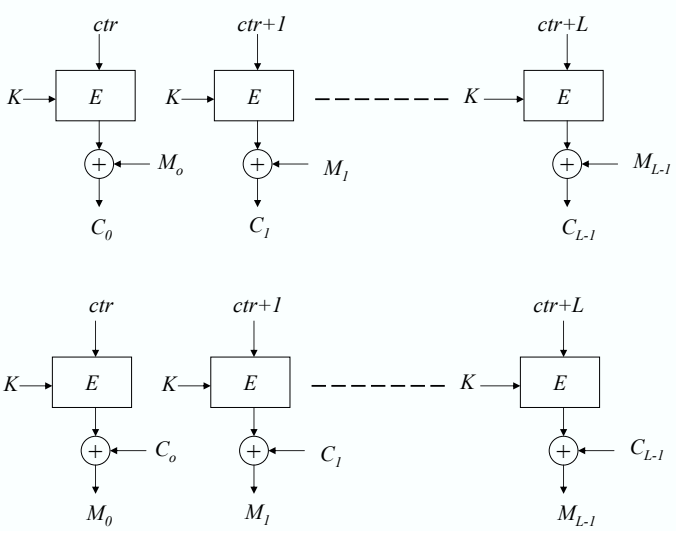

Figure 1: Encryption and decryption in counter mode

Figure 1 depicts the ciphering and deciphering processes. In practical usage scenarios, the same counter value is shared between the sender and receiver by any of the following methods:

1) The counter is randomly initialized and transmitted along with each cipher text message explicitly or in an encoded form. This ensures that the decryptor can generate the key stream needed for decryption, even when some messages are lost or reordered.

2) The counter starts at a random value and is incremented independently at sender and receiver sides after respective message transmittal or reception. This requires that both sender and receiver maintain state synchronization and communicate over a reliable channel.

This paper concerns with the first case whereby complete or partial counter value is explicitly exchanged between the two parties. This synchronization mechanism is also followed in most of the system implementations such as [6, 7].

4 Error Model of Decryption Process

The channel seen by decryptor is the physical channel as modified by the error correcting mechanisms used at the physical level. In most of the cases, the error correcting and interleaving mechanisms provide less than perfect protection and some amount of residual errors pass through undetected.Our goal is to determine the impact of residual bit errors seen on the physical channel on the CTR mode decryption process. To this end, we first develop a stochastic model of the decryption process. The impact of the residual errors on the decryption is then subsequently analyzed.

Let N_c denote the length of transmitted counter block and L denote the length (in multiples of n) of corresponding ciphertext block. At the receiver side, since the decryption is performed by the exclusive-OR of the ciphertext with the generated key stream, if bit errors occur in the ciphertext, then the recovered plaintext will have the same number of bit errors in the same bit positions as in the ciphertext. In this condition, the decryptor is said to be preserving bit errors.

Furthermore, if there is a bit error in the transmitted counter block, then a bit error may occur independently, in any bit position of the decryption of the corresponding ciphertext, with an expected error rate of fifty percent. In this state, decryptor is said to be expanding errors.

Bit error expansion is because of the fact that the underlying block cipher is assumed to adhere to strict avalanche criterion (SAC) [5] implying that each bit of its output function changes with probability one half, whenever an input bit is complemented. In brief, we can associate four possible events with the reception of ciphered message. As shown in Figure 2, these events are defined as follows:

D is the event when both counter block and ciphertext block are in error.

C is the event when ciphertext block is correct while counter block is in error.

B is the event when counter block is correct while ciphertext block is in error.

A is the event when both counter block and ciphertext block are correct.

When event D or C happens, the decryptor is in the state of error expansion. When event B takes place, preservation of bit errors occurs. When event A happens,

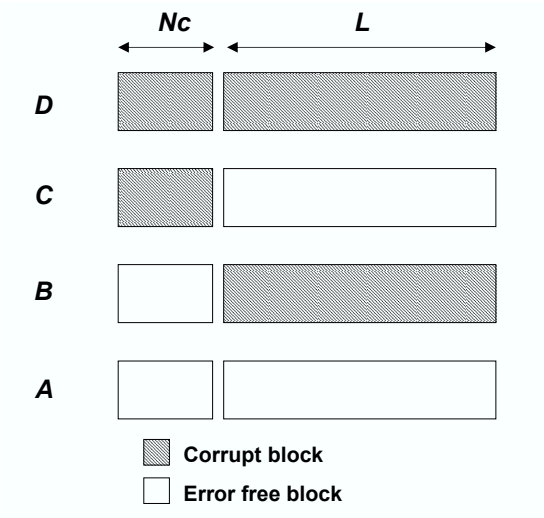

Figure 2: Error events associated with counter and ciphertext

the decryptor is free of errror expansion and error preservation. Hence depending on the state of the received ciphertext and counter blocks at each decryption cycle, the decryptor is in one of the three states namely "error free", "error preservation" and "error expansion". If the states corresponding to occurrence of events A,B,C and D are respectively referred to as **0**, **1**, **2** and **3** respectively, then the state diagram of the stochastic error model for the decryption process can be expressed as illustrated in Figure 3.

Assuming the decryption process initially starts in state **0**, the first transition to state **1** occurs when event B happens. This state is then retained until event A happens or either of events C or D happens. In the former case, transition to state **0** is made and in the latter case transition to state **2** or **3** takes place depending on whether event C happens or event D takes place.

The stochastic process updates its state every decryption cycle with the transition probabilities indicated in Figure 3 whereby $Pr(X)$ denotes the probability of occurrence of event X. If P_b represents the channel bit error probability after all the error control then we can express $Pr(A)$, $Pr(B)$, $Pr(C)$ and $Pr(D)$ in terms of P_b as follows:

Let C_i denote the i-th bit of the counter block $\forall\ i = 1..N_c$. Let $C_1C_2...C_{N_c}$ and $C_1^{'}C_2^{'}...C_{N_c}^{'}$ be the transmitted and received counter blocks respectively. Let $P(C_i^{'}|C_i)$ denote the probability of receiving $C_i^{'}$ when C_i is transmitted and $P(C_1^{'}C_2^{'}...C_{N_c}^{'}|C_1C_2...C_{N_c})$ denote the probability that the received counter block is $C_1^{'}C_2^{'}...C_{N_c}^{'}$ when the transmitted block is $C_1C_2...C_{N_c}$. Assuming reception of each bit is independent of all the remaining bits then:

$$\begin{aligned} & P(C_1^{'}C_2^{'}\cdots C_{N_c}^{'}|C_1C_2\cdots C_{N_c}) \\ = \ & P(C_1^{'}|C_1)\cdot P(C_2^{'}|C_2)\cdots P(C_{N_c}^{'}|C_{N_c}). \end{aligned}$$

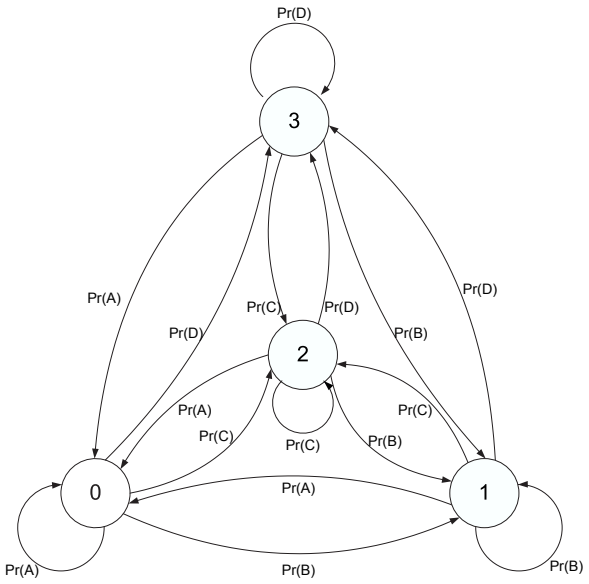

Figure 3: State diagram of the decryption process

If in a certain received block, j bits are in error, then $N_c - j$ bits are correct. The probability of a specific combination of j bits in error is $P_b^j \cdot (1-P_b)^{N_c-j}$. There are $\begin{pmatrix} N_c \\ j \end{pmatrix}$ different ways in which j errors can occur in N_c bits. Hence

$$\begin{aligned} & P(\textit{receiving } j \textit{ out of } N_c \textit{ bits in error}) \\ = & \begin{pmatrix} N_c \\ j \end{pmatrix} P_b^j \cdot (1-P_b)^{N_c-j} \end{aligned}$$

and the probability P_c of receiving correct counter block is

$$P_c = \begin{pmatrix} N_c \\ 0 \end{pmatrix} P_b^0 \cdot (1-P_b)^{N_c-0} = (1-P_b)^{N_c}$$

The probability P_{ct} of receiving correct ciphertext block can similarly be given as:

$$P_{ct} = (1-P_b)^L.$$

Since $Pr(A)$ denotes the probability of event when both counter block and ciphertext block are correct, therefore

$$Pr(A) = P_c \cdot P_{ct} = (1-P_b)^{N_c} \cdot (1-P_b)^L. \quad (1)$$

Similarly:

$$\begin{aligned} Pr(B) &= (1-(1-P_b)^L) \cdot (1-P_b)^{N_c}; & (2) \\ Pr(C) &= (1-P_b)^L \cdot (1-(1-P_b)^{N_c}); & (3) \\ Pr(D) &= (1-(1-P_b)^L) \cdot (1-(1-P_b)^{N_c}). & (4) \end{aligned}$$

The transition probability matrix of the stochastic decryption model can be written as follows:

$$\mathbf{P} = [p_{ij}],$$

where the elements p_{ij} of the transition probability matrix denote the probability of moving from state i to j and are given as follows:

$$\begin{aligned} p_{00} = p_{10} = p_{20} = p_{30} &= Pr(A); \\ p_{01} = p_{11} = p_{21} = p_{31} &= Pr(B); \\ p_{02} = p_{12} = p_{22} = p_{32} &= Pr(C); \\ p_{03} = p_{13} = p_{23} = p_{33} &= Pr(D), \end{aligned}$$

where $Pr(A), Pr(B), Pr(C)$ and $Pr(D)$ are given by Equations (1), (2), (3) and (4) respectively.

The mean probability of error P_e can be calculated as:

$$P_e = Pr(A) \cdot e_0 + Pr(B) \cdot e_1 + Pr(C) \cdot e_2 + Pr(D) \cdot e_3, \quad (5)$$

where e_k denotes the bit error rate associated with state k, $\forall k = 0, 1, 2, 3$.

As the underlying block cipher is assumed to adhere to SAC, $e_2 = \frac{1}{2}$.

Also, the bit error rates in states **0** and **1** are $e_0 = 0$ and $e_1 = P_b$ respectively.

If we assume that the residual channel bit errors and the errors introduced by the block cipher avalanche effect occur independently, the bit error rate in state **3** can be expressed as:

$$\begin{aligned} e_3 &= 1 - (1 - \frac{1}{2}) \cdot (1 - P_b) \\ &= \frac{1}{2}(1 + P_b). \end{aligned}$$

Substituting these values of bit error rates in Equation (5) along with the event probabilities from Equations (1) to (4), the post decryption error probability can be written as:

$$\begin{aligned} P_e = \; & \frac{P_b}{2}(1-(1-P_b)^L)(1+(1-P_b)^{N_c}) \\ & + \frac{1}{2}(1-(1-P_b)^{N_c}). \end{aligned}$$

5 Numerical and Simulation Results

Figure 4 shows the analytical post decryption error probability plotted against the channel bit error probability for L=128 and N_c=128,192 and 256. The dotted line represents the situation when plaintext stream is passed unencrypted through the channel i.e. $P_e = P_b$. The vertical distance between the curves representing encrypted and unencrypted cases gives the bit error expansion for a given P_b. For a fixed N_c, the error expansion is approximately constant for P_b less than 10^{-1}. Furthermore, P_e starts saturating when $P_b \geq 0.5$. At this saturation point,

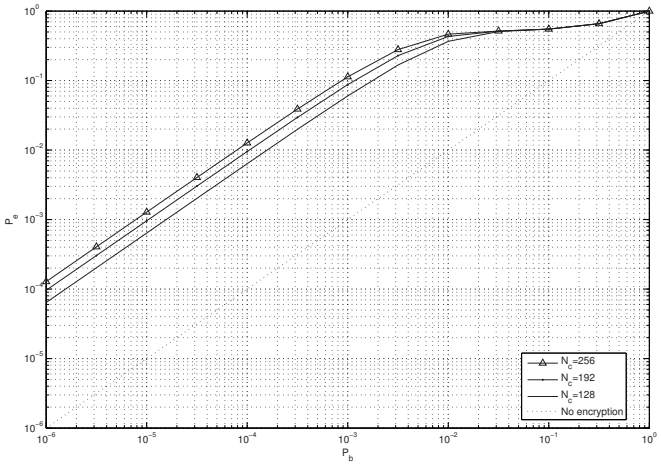

Figure 4: Analytical post decryption error probability for L=128, N_c=128,192 and 256

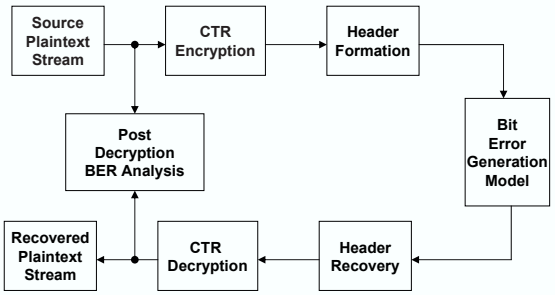

Figure 5: Simulation model for post decryption error probability analysis

events C and D occur predominantly i.e. received couter block and payload are always in error causing decryptor to garble the output.

To demonstrate the accuracy of our analytical results, computer simulation is performed following the model shown in Figure 5. Plaintext message stream is first read in 16 byte chunks, which constitutes the payload. The plaintext is then CTR encrypted using Advanced Encryption Standard (AES) [9] with arbitrary cipher key and 128 bit counter value. Before transmission through the channel, the payload is packetized by prepending a header to it which contains the counter value. The packet is then passed through the channel model, where it experiences corruption from bit errors. The channel model simulates the behavior of binary symmetric channel such that the number of bit errors X_e within the actual packet follows a binomial distribution:

$$X_e \sim B(N_p, P_b),$$

where N_p represents the packet size in bits. The location of the bit errors L_x within the packet is then calculated using a uniform distribution, as shown in the following equation:

$$L_x \sim \lfloor N_p \cdot U(0,1) \rfloor.$$

The corrupted packet is then depacketized, the payload is decrypted and compared with the original plaintext to determine the average post decryption error probability. Simulation was performed for bit error rates ranging from 10^{-5} to 10^{-1}.

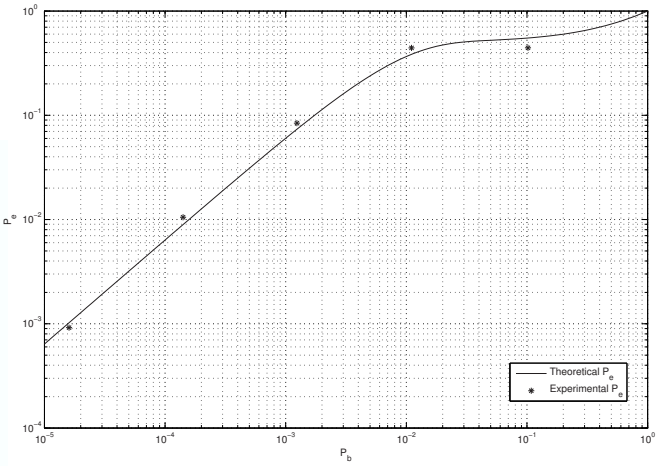

Figure 6: Analytical post decryption error probability for L=128, N_c=128,192 and 256

Figure 6 shows the corresponding simulation results, which are in a reasonable agreement with analytical results.

6 Conclusions

In this paper, CTR mode decryption process is modeled as a finite-state stochastic process and post decryption error rate is investigated. The error probability is found to be proportional to the size of the synchronization counter explicitly transmitted along with the ciphertext. The validity and accuracy of model is also shown through a computer simulation. Analytical results can be used for determining an optimum combination of transmission SNR, explicit encryption counter size and error control coding scheme subject to spectral limitations and transmission resources constraints. The cost of confidentiality [11] with CTR mode encryption in Voice over IP wireless networks can also be investigated. Although the analysis is focussed on CTR mode operation, the methodology can similarly be extended towards analysis of other wireless data link confidentiality schemes such as third generation

Universal Mobile Telecommunication Standard (UMTS) $f8$ Algorithm [1, 2], which is a combination of the Output Feedback (OFB) and Counter modes.

References

[1] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security, *Security Architecture*, 3GPP TS 33.102 V6.3.0, Dec. 2004.

[2] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security, *Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification*, 3GPP TS 35.201 V6.0.0, Dec. 2004.

[3] M. Dworkin, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, NIST Special Publication 800-38A, Dec. 2001.

[4] G. Ferland, and J. Y. Chouinard, "Error rate performance analysis of stream and block ciphers in a digital mobile communication channel," *1992 Vehicle Navigation and Information Systems Conference (VNIS '92)*, pp. 426-433, Oslo, Norway, Sep. 2-4, 1992.

[5] R. Forre, "The strict avalanche criterion: Spectral properties of boolean functions and an extended definition," *Crypto '88*, Aug. 21-25, 1988.

[6] R. Housley, *Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulating Security Payload (ESP)*, RFC 3686, Jan. 2004.

[7] IEEE Std 802.11i, *IEEE Standard for Information Technology - Telecommunication and information exchnage between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Media Access Control (MAC) Security Enhancements*, July 2004.

[8] H. Lipmaa, P. Rogaway, and D. Wagner, *Comments to NIST Concerning AES Modes of Operation: CTR-Mode Encryption*, NIST Workshop on AES Modes of Operation, Jan. 2001. (http://csrc.nist.gov/encryption/aes/modes/lipmaa-ctr.pdf)

[9] National Institute of Standards and Technology, *FIPS Pub 197: Advanced Encryption Standard (AES)*, Nov. 2001.

[10] J. Reason, *End-to-end Confidentiality for Continuous-media Applications in Wireless Systems*, Doctoral Dissertation, UC Berkeley, Dec. 2000.

[11] J. M. Reason, and D. G. Messerschmitt, *The Impact of Confidentiality on Quality of Service in Heterogeneous Voice over IP Networks*, Springer-Verlag, Berlin Heidelberg, 2001.

[12] The ATM Forum Technical Committee, *ATM Security Specification Version 1.1*, af-sec-0100.002, Mar. 2001.

Fouz Sattar obtained his MS Electrical Engineering degree from University of Engineering and Technology Taxila. His research interests include Cryptography, Communications, Network Design, Modeling and Simulation with regard to Network Security and Network Application Identification.

Muid Mufti is currently professor at University of Engineering and Technology, Taxila. He did his Ph.D. from Georgia Institute of Technology, USA in 1995 in the filed of signal processing and image analysis. Dr. Mufti has authored number of research publication in the filed of computer vision and wireless communication and has co authored many book chapters. He holds many patents on defect detection and identification. His current areas of interest include image processing and wireless communications.