Comparison of Two Self-Synchronizing Cipher Modes

Fang Yang and Howard M. Heys
Electrical and Computer Engineering
Faculty of Engineering and Applied Science
Memorial University of Newfoundland
St. John's, NL, Canada A1B 3X5
E-mail: {fyang, howard}@engr.mun.ca

Keywords: Security, Cryptography, Block Cipher

Abstract
In this paper, two recently proposed modes of operation for block ciphers, referred to as statistical cipher feedback (SCFB) mode and optimized cipher feedback (OCFB) mode, are investigated. Both cipher modes have the capability of self-synchronization with high efficiency. In particular, the paper studies the performance of SCFB mode and OCFB mode with respect to characteristics such as the theoretical efficiency, the synchronization recovery delay (SRD), and the error propagation factor (EPF). Furthermore, for digital hardware implementations of both modes, the relationship between efficiency, probability of buffer overflow, and buffer size is investigated. It is definite that both modes can obtain higher efficiency than the basic cipher feedback (CFB) mode, but, although both modes are suitable for high speed digital hardware implementation, our analysis has concluded that SCFB is preferred over OCFB for high-speed physical layer security implementations.

I. INTRODUCTION

Stream ciphers are an important class of encryption algorithms. They usually encrypt data symbol-by-symbol or bit-by-bit. Stream ciphers often use block ciphers to generate pseudo-random data bits, referred to as the keystream, to exclusive-or (XOR) with plaintext to produce ciphertext at the transmitter. The ciphertext is then sent to the receiver via the communication channel. At the receiver, the identical keystream is generated and XORed with the ciphertext to produce the recovered plaintext. Stream ciphers can be used for high-speed networks at the physical layer in a communication system.

In a stream cipher, it is important to keep the keystream of both the transmitter and receiver synchronized because the communication channel may suffer from periodic bit slips or insertions. There is a class of stream ciphers, referred to as self-synchronizing stream ciphers, which extract data from the ciphertext to synchronize the transmitter and the receiver. In this paper, we discuss two recently proposed self-synchronizing stream cipher modes, referred to as statistical cipher feedback (SCFB) mode [1] and optimized cipher feedback (OCFB) mode [2].

II. BACKGROUND

Cipher feedback (CFB) mode and output feedback (OFB) mode are two conventional operational modes of block ciphers which can be applied to create stream ciphers [4]. In this paper, we use E to represent the block cipher, B to represent the block length and m to represent the feedback size.

CFB mode, as shown in Figure 1, encrypts m bits of plaintext with m bits of keystream to produce m bits of ciphertext. When $m = 1$, it is possible to resynchronize for a slip or insertion of any number of bits. Unfortunately, it is costly to achieve the property of self-synchronization because each bit encryption requires a complete encryption of the block cipher. This makes CFB mode with $m = 1$ very inefficient.

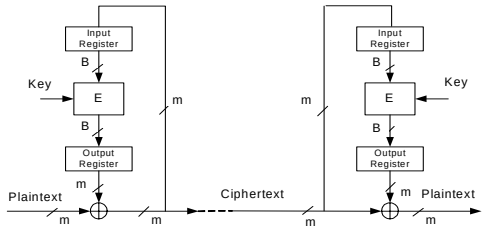

Fig. 1 - Cipher Feedback Mode

OFB mode, as shown in Figure 2, is similar to CFB mode except OFB mode takes the previous output of the block cipher as the next input to the block cipher to produce the next keystream block. Of all modes of operation, OFB mode provides minimal error propagation. That is, errors from the communication channel are not multiplied through the decryption process. However, OFB needs an extra signalling channel to periodically transfer an initialization vector (IV) from the transmitter to the receiver to obtain the ability of resynchronization to recover from any synchronization loss that may occur due to bit slips or insertions.

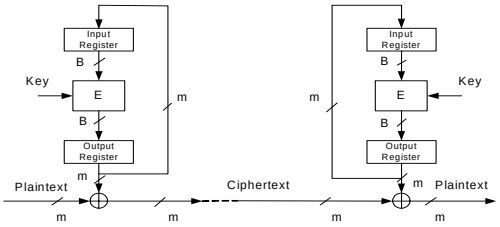

Fig. 2 - Output Feedback Mode

III. SCFB MODE AND OCFB MODE

SCFB mode, illustrated in Figure 3, is a hybrid of CFB mode and OFB mode that achieves the capability of self-synchronization

and higher efficiency than CFB mode. A switch is used to connect either point A or point B to the input of the block cipher. When the switch is connected to point A, SCFB mode works as OFB mode and when the switch is connected to point B, SCFB mode works as CFB mode and collects *B* bits of ciphertext as a new initialization vector to feedback into the input register to synchronize the system. The time at which the switch acts is dependent on whether an *n* bit sync pattern in ciphertext is found. If the sync pattern occurs in the ciphertext, the next *B* bits are used as the new IV to feedback into the input register. During the collection of the new IV, the sync pattern is not checked for.

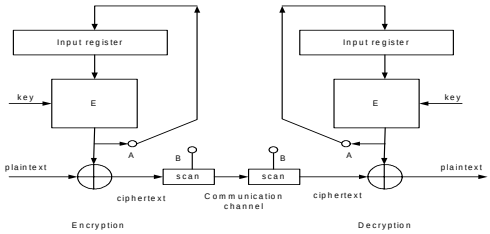

Fig. 3 - Statistical Cipher Feedback Mode

OCFB mode, shown in Figure 4, is another mode which optimizes CFB mode to obtain higher efficiency and achieve the property of self-synchronization. OCFB mode buffers all output bits of the block cipher into shift register SR2 as the keystream. During each clock period, SR1 and SR2 shift one position from right to left. One bit of keystream is XORed with one bit of plaintext to produce the corresponding bit of ciphertext. The ciphertext is then sent out to the communication channel. A counter is used to count the number of shifts. When it counts to the maximum, the counter triggers the block cipher to encrypt the contents of SR1 to produce one block of keystream that is saved into SR2. The pattern in the figure represents the sync pattern. On each clock cycle, the first *n* bits of SR1 are used to compare with the sync pattern. If the sync pattern is recognized in SR1, the counter is set to the maximum to trigger the encryption of the block cipher, effectively using the contents of SR1 as a new IV.

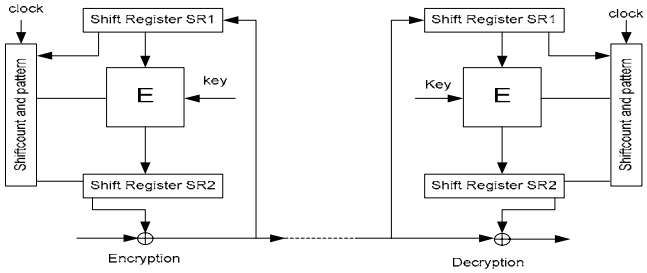

Fig. 4 - Optimized Cipher Feedback Mode

Unlike SCFB mode, OCFB mode checks for the sync pattern in all of the ciphertext bits even when IV is collecting. As a result, OCFB mode has more opportunity to resynchronize.

IV. PERFORMANCE COMPARISON

(a) Theoretical Efficiency

The theoretical efficiency represents the rate at which the stream cipher can encrypt compared with the rate of the block cipher [3]:

$$\eta = \lim_{D\to\infty} \frac{D/B}{E\{\#\text{block cipher operations for } D \text{ bits}\}}.$$

We define a synchronization cycle in the ciphertext as the number of bits from the beginning of the sync pattern until the beginning of the next sync pattern. Since there is no checking for the sync pattern in the next *B* bits after the sync pattern, a synchronization cycle of SCFB mode is *n*+*B*+*k* bits where *k* represents the number of bits following an IV until the next sync pattern. However, since in OCFB the sync pattern is checked for continuously, a synchronization cycle of OCFB mode is *n*+*k* bits. The theoretical efficiencies of SCFB mode and OCFB mode are shown in Figure 5 based on using the Advanced Encryption Standard (AES) [5] with a 128 bit block size as the block cipher. SCFB mode achieves at least 50% theoretical efficiency because it has at least one full *B*-bit block (IV) in one synchronization cycle. However, the efficiency of OCFB can vary from 0% to 100%.

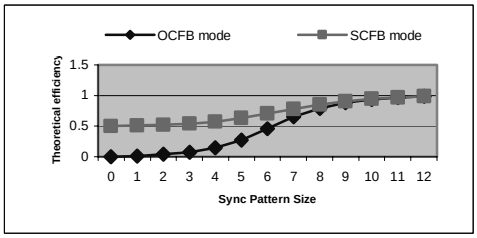

Fig. 5 - Theoretical Efficiency

(b) Synchronization Recovery Delay

The synchronization recovery delay (SRD) is the expected number of bits between the synchronization loss and resynchronization [3]. The SRD of SCFB mode and OCFB mode, determined through simulation using AES, is illustrated in Figure 6. Both modes have a similar trend when the sync pattern size *n* is increased. However, SCFB mode has higher SRD than OCFB mode when $n \leq 6$, indicating that OCFB mode recovers more quickly from the loss of synchronization as expected. Essentially, because SCFB mode does not check for the sync pattern in the IV block, SCFB mode needs a longer time to recover for small *n*, when the synchronization cycles are expected to be small in comparison to *B*, the size of the IV.

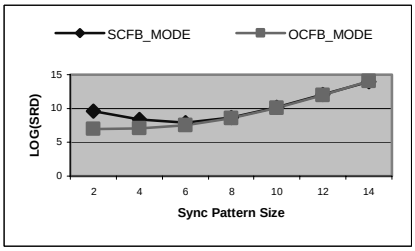

Fig. 6 - Sync Recover Delay

(c) Error Propagation Factor

The error propagation factor (EPF) is the bit error rate of the plaintext recovered by the decryption system divided by the bit error rate in the communication channel [3]. It essentially measures the bit errors at the output of the decryption when a bit error occurs in the communication channel. The EPF, as determined by simulation, of SCFB mode and OCFB mode is shown as Figure 7. This figure indicates that OCFB mode has better EPF for small sync patterns; for large sync patterns, there is little difference between the modes.

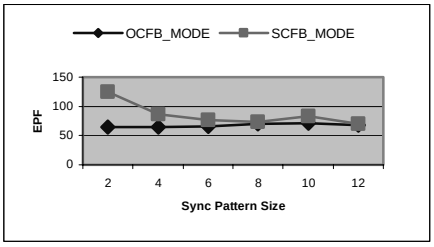

Fig. 7 - Error Propagation Factor

(d) Hardware Characteristics

In practice, in order to ensure the incoming and outgoing data speeds are constant even while the processing of data inside the system is not constant, a plaintext buffer and a ciphertext buffer are required to provide elasticity to the flow of data within the system [3]. As a result, the relationship between probability of overflow, buffer size and efficiency are of concern when considering implementations of SCFB and OCFB modes. The simulations of Figure 8 (using AES as the block cipher) show that 50% efficiency with a B = 128 bit buffer size guarantees that an SCFB system does not have any buffer overflow. (This can also be easily deduced.) However, it is clear that the OCFB system suffers from a significantly higher probability of overflow than SCFB mode, when buffer size is small. Using a small buffer is desirable as it keeps down hardware costs and reduces the latency of the encryption (and decryption) process.

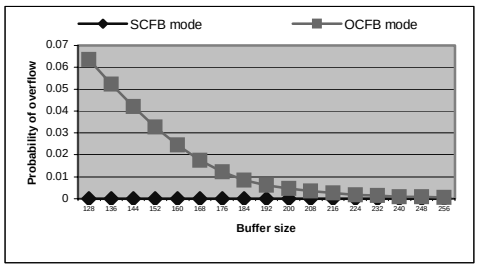

Fig. 8 - Probability of overflow vs. buffer size with full-queue efficiency =50%

Figure 9 indicates the relationship between probability of overflow and efficiency when buffer size is fixed. It shows that OCFB mode has higher probability of overflow buffer than SCFB mode because of the expected more frequent resynchronization.

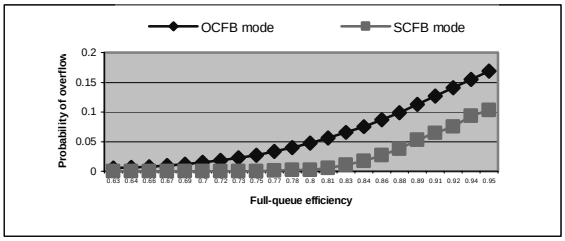

Fig. 9 - Probability of overflow vs. full-queue efficiency with buffer size = 256 bits

V. CONCLUSIONS

In this paper, we have analyzed the performances of OCFB mode and SCFB mode with respect to characteristics such as theoretical efficiency, the synchronization recovery delay, the error propagation factor, and hardware characteristics related to buffer size. Although OCFB has lower SRD and EPF for small sync patterns, it is revealed to be generally less efficient that SCFB mode. Notably, given a fixed buffer size and efficiency, SCFB has a much lower probability of buffer overflow than OCFB.

Significantly, when the buffer size is greater than or equal to the block size B, SCFB mode is guaranteed to obtain at least 50% theoretical efficiency without any buffer overflow and up to close to 100% efficiency with some buffer overflow. OCFB mode can achieve the efficiency from 0 to approximately 100% but always suffers from some buffer overflow that is higher than the equivalent SCFB system. In fact, it is not possible to guarantee no overflow in OCFB mode, even for efficiencies that are much less than 50%. This point in particular implies that SCFB mode is more suitable for high-speed physical layer security than OCFB mode.

References

[1] O.Jung and C. Ruland, "Encryption with Statistical Self-Synchronization in Synchronous Broadband Networks", *Cryptographic Hardware and Embedded Systems* – CHES'99, Lecture Notes in Computer Science 1717, Springer – Verlag, pp. 340-352, 1999.

[2] A.Alkassar, A. Geraldy, B. Pfitzmann, A-R, Sadeghi, "Optimized Self-Synchronization Mode of Opertation", *Fast Software Encryption Workshop – FSE 2001*, Lecture Notes in Computer Science 2355, Springer – Verlag, pp. 78-91, 2002.

[3] Howard M. Heys, "Analysis of the Statistical Cipher Feedback Mode of Block Ciphers", *IEEE Transactions on Computers*, vol. 52, no. 1, pp. 77-92, Jan. 2003.

[4] William Stallings, *Cryptography and Network Security*, 2nd ed., Prentice Hall, 1999.

[5] Nat'l Inst. Standards and Technology, "Advanced Encryption Standard (AES)", Federal Information Processing Standard 197, 2001.