Trade-Off Between Security and Performance in Block Ciphered Systems With Erroneous Ciphertexts

Shuangqing Wei, *Member, IEEE*, Jian Wang, *Member, IEEE*, Ruming Yin, and Jian Yuan

***Abstract*—It has long been held that errors in received noisy ciphertexts should be eliminated using as many as possible powerful error correcting codes in order to reduce the avalanche effect on legitimate users' performance in block ciphered systems. However, the negative effect of erroneous ciphertexts on cryptanalysis by an eavesdropper has not been well understood, nor the possible measurable trade-off between security enhancement and performance degradation under noisy ciphertexts. To address these questions, we have launched a case study in this paper using Data Encryption Standard (DES)-based block ciphers operating in cipher feedback (CFB) mode to show quantitatively the pros and cons of exploiting voluntarily or nonvoluntarily introduced binary errors in ciphertexts of block ciphered systems using our proposed comparison metrics. A serially concatenated scheme with both outer and inner encoder-encipher pairs is proposed which allows us to quantitatively reveal the sacrifice made by legitimate users in its postdecryption capacity, as well as the security improvement factor (SIF) which reflects the additionally required plaintext-ciphertext pairs for eavesdropper's known plaintext attack, in the presence of noise in ciphertexts. Simulation results demonstrate the accuracy of derived approximations of the postdecryption performance for the legitimate receiver.**

***Index Terms*—Block ciphered systems, concatenated encoding-encryption, linear cryptanalysis, noisy ciphertexts, postdecryption performance.**

I. Introduction

As WIRELESS devices and networks have become more and more ubiquitous, security issues of underlying systems shall be addressed as one of the foremost concerns of the integral solution to system and network design. There are many aspects on security issues in general [1]. In this paper our attention is focused on the confidentiality issues of communications.

One of the common practices behind those widely used cryptal primitives in wireless networks is to either separate crypto blocks from physical layer with the aim of getting error free ciphertexts at a legitimate receiver [2] or put stream-ciphered encryption right after coded modulation block [3]. The rationale is because of the diffusion property which any strong block cipher should satisfy [4], stipulating that a single bit change to a block ciphertext must result in significant and random-looking changes to the decrypted messages. In average, one half of the decrypted bits should change whenever a single input bit to the decryption device is flipped. Consequently, there will be severe error propagation in encryption systems if erroneous ciphertexts are received, which explains why encryption and encoding are put in such a way as described above.

Recently, the effects of channel error on the throughput of encryption system have received more and more attention [5]–[10]. Nonetheless, most works on studying how the physical channel quality worsens the reliability at Bob rely on extensive simulations. Very few analytical study on this issue exists in literature. More importantly, there is one critical missing component in existing works, namely, the study of consequences of having erroneous ciphertexts on Eve's efforts in her cryptanalysis. Intuitively, erroneous ciphertexts received by Eve could also make her attack more difficult. However, to the best of our knowledge, very few works in literature have investigated how noise in ciphertexts could further substantiate Eve's efforts engaged in cryptanalysis.

Therefore, one immediate question that needs to be addressed is: If we are willing to sacrifice the postdecryption system performance for legitimate users to some degree, how much additional gain could we attain from security perspective by having some erroneous ciphertexts due to either physical channel noise or some intentionally added interference,[1] and what is the proper way of reaping such security benefits? The primary objective of this work is to answer these questions by demonstrating both pros and cons in exploiting erroneous ciphertexts in block-ciphered systems.

To accomplish the precedent goals, we adopt a DES based block ciphered system working in cipher feedback (CFB) mode, and then investigate and quantify the effect of noise in received ciphertexts on both cryptanalysis at an eavesdropper and the postdecryption quality of recovered plaintext bits at Bob. The noise in binary ciphertexts is characterized by bit flipping probability, namely, the cross-over probability, of binary symmetric channels (BSC) between transmitted ciphertexts and received (eavesdropped) ciphertexts. The motivation of adopting BSC channel is due to its simplicity and also its wide application in modeling postdecoding errors from received ciphertexts, as well as its characterization of intentionally added independent binary noise in ciphertexts.

For security metric, we adopt the number of plaintext and ciphertext pairs required in linear cryptanalysis by an eavesdropper (Eve). The average information bit error rate (BER)

Manuscript received May 22, 2012; revised December 22, 2012; accepted February 06, 2013. Date of publication February 25, 2013; date of current version March 11, 2013. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Kah Chan Teh.

S. Wei is with the School of Electrical Engineering and Computer Science, Louisiana State University, Baton Rouge, LA 70803 USA (e-mail: swei@ece.lsu.edu).

J. Wang, R. Yin, and J. Yuan are with the Department of Electronic Engineering, Tsinghua University, Beijing, 100084, China (e-mail: jian-wang@tsinghua.edu.cn; jyuan@tsinghua.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2013.2248724

[1]In fact, in some recent designs of encryption algorithms, deliberate errors are used to enhance the security [11], [12].

after decryption at the legitimate receiver is taken as a performance metric. To further quantify the security enhancement, we propose security improving factor (SIF) which is defined as the ratio of known plain-ciphertext pairs for the case with errors in ciphertexts over that without errors. The degradation of performance is characterized by either the information BER normalized by BSC cross-over probability, or the factor of degradation of achieved postdecryption capacity.

DES is a symmetric key encryption cipher which has plaintexts and ciphertexts of size 64-bit with the key length of 56 bits. The rationale behind selecting DES as the block cipher in our case study is because of its widely known and mature cryptanalysis techniques [13], [14], namely, linear cryptanalysis and differential cryptanalysis. CFB mode is one of the operational modes that can be used to derive a key stream from block ciphers like DES and has also been considered in wireless communications [9], [15]. The reasoning for adoption of CFB mode, rather than counter-mode, is exactly because of its introduced error propagation which will certainly deteriorate postdecryption performance, but also pose a problem for cryptanalysis, whose trade-off is what we are going to characterize. Recently the idea of intentionally introducing noise in ciphertexts together with error propagation prone block chaining mode has also been explored in Error Correction Based Cipher (ECBC) [16], [17].

Three encryption systems are proposed with progressively increasing complexity and capability. They are DES only (DC), DES concatenated with Reed Solomon encoding (DCRS), and DES concatenated with RS coding and encrypted S-box diffusion (DCRSS). Selection of Reed Solomon coding is because of its power in correcting burst errors caused by inverse of S-box in the presence of noise in ciphertexts, and the off-the-shelf analytical results on evaluating its decoding performance. We have found the required known plain-cipher text pairs in each system for linear attack by Eve. In addition, performance analysis in terms of decoded information bit error probability for Bob, the legitimate receiver, has been conducted for each system, whose accuracy is later verified by simulation results.

Towards the end of our study, a serially concatenated scheme with both outer and inner encoder-encipher pairs is proposed which allows us to quantitatively reveal the sacrifice made by legitimate users in its postdecryption capacity, as well as the additional SIF gains, both of which are contributed by remaining noise in ciphertexts. In particular, some cryptanalysis method has been developed to exploit the linear relationship inherent in channel codewords before the block ciphering operation. Our proposed concatenated scheme carries the same spirit as the concatenation coding which serves the sole purpose of error correction [18]. As a contrast, the concatenated encoding-encryption approach proposed here could be deemed as the one making balance between security and error correction.

To the best of our knowledge, the most relevant to ours is [19] where an encoding-then-encryption framework was also proposed aiming at further enhancing security of the underlying stream-ciphers by exploiting Wyner-type wiretap channel coding [20], [21] and erroneous ciphertexts. The consideration of stream ciphers apparently is due to the concerns of negative consequence of avalanche effect on legitimate users' performance. In addition, they also focus on the known-plain text attack, but analyze the security from an information theoretical point of view, namely, the condition entropy metric as initially proposed in [20].

As a comparison, our work is a case study with a proposed outer-inner encoding-encipher framework including the chosen cipher, its cryptanalysis, error correction coding and encrypted S-box. Such framework is not as general as the one considered in [19] which is formulated in an information theoretic context in a stream-ciphered system. However, despite the specifications carried in our case study, our approach does provide a comparison framework under which performance degradation in terms of the normalized postdecryption capacity or error rate is measured against normalized security enhancement (e.g. SIF). More importantly, our case study demonstrates in a quantitative way that even in a block ciphered system noise in ciphertexts could be exploited to further enhance security at the cost of degraded legitimate user's performance.

Further commented is the generality of the principle developed here on reliability and security analysis for block ciphers, which function under a chaining mode in the presence of noise in ciphertexts. For security analysis under linear attacks, the equivalent channel error probability is reflected in the probability of a correct input to the block cipher. More precisely, the bias of the probability of satisfying the linear Boolean function is affected by the bit-wise error probability for those involved active bits, which is further determined by the equivalent channel error probability. For the analysis of information bit error probability at Bob after decryption, the properties related with avalanche effect of block ciphering [22], as well as the information bit error probability after channel decoding should be exploited. These principles could be applied to similar trade-off analysis in other block ciphered communication systems where different channel coder or encryption primitive is adopted.

II. Description of Three Encryption Systems

In this section, we describe the three encryption systems that will be analyzed. All the systems employ DES based block ciphers in cipher feedback (CFB) mode.

A. DES Encryption in CFB Mode (DC)

The first system uses DES in CFB mode. It encrypts 64-bit plain text each time. As is shown in Fig. 1(a), at time n, the 64-bit ciphertext c_n is produced by Xoring the plaintext p_n with the key-stream s_n:

$$c_n = p_n \oplus s_n. \tag{1}$$

The keystream s_n is obtained by encrypting the previous ciphertext block c_{n-1} with DES, and have the following iterative relationship:

$$s_n = DES_k(c_{n-1}). \tag{2}$$

For the first keystream s_0, the previous ciphertext does not exist. Therefore an initialization vector IV is used, i.e., $c_{-1} = IV$.

The ciphertext c_n is transmitted to the receiving point and may be intercepted by the eavesdropper. Here we define two different channels: $channel_b$ and $channel_e$. $channel_b$ is the

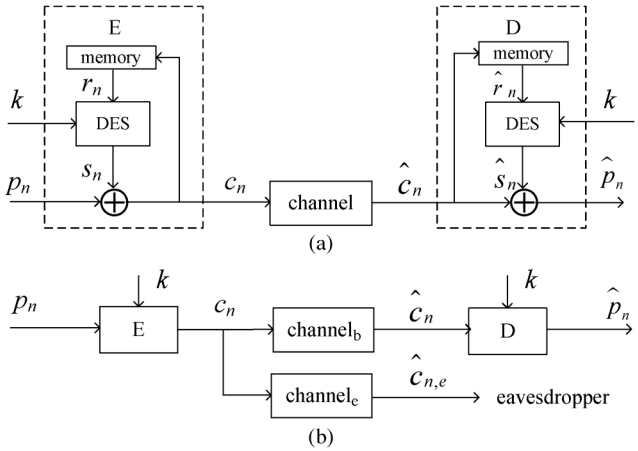


Fig. 1. Cipher feedback (CFB) mode of the DES.

Fig. 2. (a) CFB mode of the DES with RS channel code. (b) CFB mode of the DES with RS channel code and secret substitution box.

equivalent binary symmetric channel (BSC) between the legitimate parties and $channel_e$ represents the BSC channel via which a wire-tapper has access to the ciphertext, whose crossover probabilities are α_B and α_E, respectively. Assume that the ciphertext obtained by the legitimate receiver is $\hat{c}_n$. $\hat{c}_n$ may not be equal to c_n due to the error introduced by $channel_b$. Then at the receiving end the following transformation is applied to $\hat{c}_n$ to recover the original message $\hat{p}_n$.

$$\hat{s}_n = DES_k(\hat{c}_{n-1}), \quad \hat{p}_n = \hat{c}_n \oplus \hat{s}_n \tag{3}$$

Similarly, we assume the wire-tapper can intercept the transmitted ciphertext $\hat{c}_{n,e}$ via $channel_e$.

For compactness, the DES CFB encryption and decryption are represented with the block E and D respectively. In this way, the system in Fig. 1(a) is shown again in Fig. 1(b). In the following descriptions of other systems, we adopt this representation.

B. DES Encryption With RS Code (DCRS)

Since DES decryption in CFB mode is sensitive to bit errors induced in ciphertexts, the system in Fig. 1 has severe error propagation, thereby degrading its end-to-end performance. To overcome this problem, channel codes can be used to correct errors in the ciphertexts. In this paper, we adopt the Reed-Solomon (RS) codes [23] and thus obtain the system shown in Fig. 2(a). Reed-Solomon codes are maximum distance separable (MDS) codes with good burst error correcting capability, which is exploited to cope with burst errors introduced in the inverse nonlinear operation for the next scheme with encrypted S-box.

1) RS Codes: We consider (M, L) systematic RS codes over $GF(2^8)$, where L denotes the number of data symbols being encoded and M denotes number of symbols in the encoded block. The symbol-error correcting capability of (M, L) codes is $t = \lfloor (M-L)/2 \rfloor$ [23]. The $L \times M$ generator matrix has the following form $G = [I\ P]$, where I is a $L \times L$ identity matrix and P is a matrix of dimension $L \times (M-L)$. The codewords can be divided into two parts. The first L symbols denoted by $v_n^I = (v_{0,n}, v_{1,n}, \cdots, v_{L-1,n})$ are the same as the corresponding message symbols c_n, i.e., $v_n^I = c_n$. The following $M-L$ symbols are the parity symbols which are denoted by $v_n^P = (v_{L+1,n}, v_{1,n}, \cdots, v_{M-1,n})$. The following linear equation features the relationship between these two parts of a codeword:

$$v_n^P = v_n^I P. \tag{4}$$

2) Descriptions of the System: As is shown in Fig. 2(a), the 64-bit ciphertext of DES is divided into $L = 8$ bytes $c_n = (c_{0,n}, c_{1,n}, \cdots, c_{L-1,n})$. Then c_n is used as the input of the RS code. In this paper, a $(M, L) = (16, 8)$ RS code over $GF(2^8)$ is adopted. After RS encoding, 16-byte encoded block is obtained as $v_n = (v_{0,n}, v_{1,n}, \cdots, v_{M-1,n})$, which is sent to the receiver via channel $channel_b$. At the receiving end the received ciphertext $\hat{v}_n$ is first decoded by using Berlekamp–Massey algorithm [23] and then decrypted to obtain the plaintext $\hat{p}_n$.

C. DES Encryption With RS Codes and Secret Sbox (DCRSS)

When an error correcting code is put after enciphering, not only does that help alleviate the effect of channel distortion at Bob, but also result in an undesired effect in terms of security against Eve whose cryptanalysis is made easier thanks to the error correction to the noisy ciphertexts. Therefore, a second encrypted nonlinear operation (e.g. encrypted S-box) has to be concatenated after the channel encoder and designed in such a way that the decryption efforts at the eavesdropper is significantly increased without compromising the decoding performance at the legitimate receiver noticeably. This goal can only be attained by exploiting the characteristic of a properly selected channel error correcting code and the second encryption device. In this paper, we take advantage of MDS property of Reed Solomon code, as well as the strong nonlinearity in the S-box designed for Advanced Encryption Standard (AES) cipher, which allows us to achieve a better trade-off between reliability and security, as shown later in Section IV.

More specifically, for the system shown in Fig. 2(a), we add a secret substitution box (Sbox) after the RS coding and thus obtain the system in Fig. 2(b). This modification is to makes eavesdroppers not able to access c_n or $\hat{c}_n$, which is the 64-bit ciphertext of DES and can be used to attack the system. Therefore, the system in Fig. 2(b) is more secure in comparison with the other two systems. The secret Sbox is a one-to-one mapping under the control of a 128-bit secret key k_1. In this paper, we

adopt the well known Sbox used in Advanced Encryption Standard (AES) as our Sbox [24], which transforms one byte into another byte. It first computes the multiplicative inverse of the input byte in finite field $GF(2^8)$ and then use a affine transformation to obtain the output byte. The 128-bit secret key k_1 can be divided into $M = 16$ bytes $k_1 = (k_{1,0}, k_{1,1}, \cdots, k_{1,M-1})$, then the secret Sbox can be formulated as follows

$$b_{i,n} = S(v_{i,n}) \oplus k_{1,i}. \tag{5}$$

At the receiving end, the inverse S-box S^{-1} should be applied before RS decoding after the key stream is added back to the ciphertext. As S-box operates on byte basis, the bit error event out of the channel will be thus restricted over each byte after the inverse operation of the S-box at Bob. Thus adding an encrypted S-box after RS encoding does not affect the symbol-wise error probability.

III. Analysis of Channel Error Effects on Security and Reliability

In this section, we theoretically analyze the effects of errors in ciphertexts on security and reliability of the three systems. For security analysis, we consider the known plaintext attack for DC and DCRS, and both known plaintext attack and ciphertext only attack for DCRSS for its outer cipher (DES) and inner cipher (keyed S-box), respectively. In these attacking approaches, Eve has an oracle to query whose answers go through a noisy binary symmetric channel where noise sequences are introduced either voluntarily as an integral part of the underlying block ciphered system or nonvoluntarily by a physical channel. The security enhancement is measured quantitatively by using linear cryptanalysis. For the reliability analysis, the theoretically estimated information bit error rate (BER) between the legitimate parties are obtained.

A. DES Encryption in CFB Mode

1) Security Enhancement Against Wire-Tap Attack: We analyze the security enhancement for the system in Fig. 1(b). First, we provide a brief description on the classical linear cryptanalysis [14] against this system where there are no errors in received ciphertexts, i.e., $\hat{c}_{n,e} = c_n$ with zero cross-over probability in the corresponding BSC channel. The eavesdropper can apply linear cryptanalysis to the system as follows. Since the consecutive ciphertext of DES c_n is transmitted by wireless channel, it can be intercepted by the eavesdropper. Assume that the eavesdropper can also get the corresponding plaintext p_n, i.e., the eavesdropper can get many (p_n, c_n) pairs. Then the input and output of DES can be computed as $(r_n, s_n) = (c_{n-1}, p_n \oplus c_n)$, that is

$$s_n = p_n \oplus c_n = DES_k(c_{n-1}). \tag{6}$$

Linear cryptanalysis exploits high probability occurrences of linear equations involving bits in r_n and s_n to attack DES and obtain some key bits [25]. The linear equations to be used have the following form:

$$s_n^{[i_1]} \oplus s_n^{[i_2]} \oplus \cdots \oplus s_n^{[i_u]} \oplus r_n^{[j_1]} \oplus r_n^{[j_2]} \oplus \cdots \oplus r_n^{[j_v]} = 0. \tag{7}$$

where $s_n^{[i_u]}$ represents the i_u-th bit of s_n.

Generally, the complexity of linear cryptanalysis could be characterized by the data required to mount the attack. Assume the probability that the above equation holds is P_L, The bias from 1/2 of P_L, denoted by $\varepsilon = |P_L - 0.5|$ is called the linear probability bias. Then it requires about $(1/\varepsilon^2)(r_n, s_n)$ pairs to mount a successful attack [25]. For the attack against DES, $2^{47}(r_n, s_n)$ pairs are needed to achieve a desired success probability [25]. Note that two consecutive transmitted data blocks c_{n-1} and c_n are needed in order to obtain one (r_n, s_n) pair. For simplicity, assume that a transmitted data block is just used once in computing the (r_n, s_n) pair, thus it needs about $N = 2^{48}$ transmitted data blocks to mount a successful attack.

Next we analyze the security enhancement in the presence of errors in received ciphertexts. Due to noise, the intercepted transmitted data blocks $\hat{c}_{n,e}$ and $\hat{c}_{n-1,e}$ may have errors, which leads to a wrong (r_n, s_n) pair, i.e., $s_n \neq DES_k(r_n)$. The eavesdropper doesn't know whether a (r_n, s_n) pair is wrong or not, and thus she has to mount linear cryptanalysis all the same. This affects the probability that the linear equation holds. In this case, the complexity of the attack should be determined by the changed probability, which is computed below.

Assume that the bit error rate of BSC channel is α_E, the input and output of DES computed by eavesdropper is denoted by $(r_{n,e}, s_{n,e})$. Since $(r_{n,e}, s_{n,e}) = (\hat{c}_{n-1,e}, p_n \oplus \hat{c}_{n,e})$ and the known plaintext p_n does not have bit error, the error bits in $r_{n,e}$ and $s_{n,e}$ are just induced by the corresponding error bits in $\hat{c}_{n-1,e}$ and $\hat{c}_{n,e}$. The bit correct probability for bits in $\hat{c}_{n-1,e}$ or $\hat{c}_{n,e}$ is $1 - \alpha_E$, therefore we have

$$P\left(s_n^{[i_x]} = s_{n,e}^{[i_x]}\right) = 1 - \alpha_E, \quad x = 1, 2, \cdots, u \tag{8}$$

$$P\left(r_n^{[j_y]} = r_{n,e}^{[j_y]}\right) = 1 - \alpha_E, \quad y = 1, 2, \cdots, v \tag{9}$$

Then we substitute $s_n^{[i_x]}$ in (7) by $s_{n,e}^{[i_x]}$ and $r_n^{[j_y]}$ by $r_{n,e}^{[j_y]}$. The following expression is obtained:

$$s_{n,e}^{[i_1]} \oplus s_{n,e}^{[i_2]} \oplus \cdots \oplus s_{n,e}^{[i_u]} \oplus r_{n,e}^{[j_1]} \oplus r_{n,e}^{[j_2]} \oplus \cdots \oplus r_{n,e}^{[j_v]} = 0. \tag{10}$$

The eavesdropper just uses (10) to mount the linear attack. To estimate the complexity of attack, we need to compute the linear probability bias of (10). According to Piling-Up Lemma [13], [14], this linear probability bias ε_e can be calculated as

$$\begin{aligned} \varepsilon_e &= 2^{u+v}(1 - \alpha_E - 0.5)^{u+v}\varepsilon \\ &= (1 - 2\alpha_E)^{u+v}\epsilon \end{aligned} \tag{11}$$

where $\varepsilon = |P_L - 0.5|$ is the linear probability bias of (7), i.e., it is the linear probability bias when there is no wire-tap channel error.

We can apply similar analysis as that without noise in ciphertext to estimate the data needed, and the number of transmitted data blocks required to mount a successful attack is

$$\begin{aligned} N_{DC} &= \frac{1}{\varepsilon_e^2} = \frac{1}{2^{2(u+v)}(1 - \alpha_E - 0.5)^{2(u+v)}}N \\ &= \frac{N}{(1 - 2\alpha_E)^{2(u+v)}} \end{aligned} \tag{12}$$

where N is the number of transmitted blocks required when there is no wire-tap channel error, $u + v$ is the number of bits

involved in the linear (7). We find that the number of blocks required is $(1/2^{2(u+v)}(1-\alpha_E-0.5)^{2(u+v)})$ times larger than N in the presence of channel errors as featured by α_E. Therefore we can use the quantity $(1/2^{2(u+v)}(1-\alpha_E-0.5)^{2(u+v)})$ to measure the security enhancement induced by the wire-tap channel. Since the effective linear equations for DES block cipher involve about 15 bits, we choose $u+v=15$ in this paper.

2) Bit Error Rate Analysis: Let E_b denote the bit error event in restoring the plaintext $\hat{p}_n$ when compared with the transmitted plaintext p_n. From deciphering of DES block cipher, the deciphered text $\hat{p}_n$ satisfies: $\hat{p}_n = \mathrm{DES}_k(\hat{c}_{n-1}) \oplus \hat{c}_n$. Due to the highly nonlinear property as captured by its diffusion characteristic [26] of DES cipher, if there are bit errors in received cipher text $\hat{c}_{n-1}$ as an DES cipher input, the average bit error probability in the output ciphertext can be approximated as 0.5, i.e. $P(E_b|\hat{c}_{n-1} \neq c_{n-1}) \approx 0.5$. When no error occurs in receiving the ciphertext $\hat{c}_{n-1}$, i.e. $\hat{c}_{n-1} = c_{n-1}$, the bit error rate of $\hat{p}_n$ is the same as the bit error rate of $\hat{c}_n$, which is determined by the channel cross over probability α_B, i.e. $P(E_b|\hat{c}_{n-1} = c_{n-1}) = \alpha_B$. Therefore, we have

$$\begin{aligned} P_{DC}(E_b) &= P\left(E_b|\hat{c}_{n-1} \neq c_{n-1}\right) P(\hat{c}_{n-1} \neq c_{n-1}) \\ &\quad + P\left(E_b|\hat{c}_{n-1} = c_{n-1}\right) P(\hat{c}_{n-1} = c_{n-1}) \\ &= 0.5\left(1-(1-\alpha_B)^{8L}\right) + \alpha_B(1-\alpha_B)^{8L} \\ &= 0.5 - (0.5-\alpha_B)(1-\alpha_B)^{8L}, \end{aligned} \tag{13}$$

where $L = 8$.

B. DES Encryption With RS Code

1) Security Enhancement Against Wire-Tap Attack: We analyze the security enhancement for the system in Fig. 2(a). With RS codes in this system, the eavesdropper can correct some channel errors. In addition, as the eavesdropper can detect RS decoder failure, she can filter out some erroneous transmitted data blocks. In this way, the required transmitted data blocks to mount a successful attack is decreased.

With the intercepted data block $\hat{v}_{n,e}$, the eavesdropper can obtain the decoded block $\hat{c}_{n,e}$. A (16,8) Reed-Solomon code can correct up to $t = 4$ symbol errors in each codeword $\hat{v}_{n,e}$ [23]. Therefore if the transmitted codeword $\hat{v}_{n,e}$ suffers 4 or fewer symbol errors, the decoded block $\hat{c}_{n,e}$ is equal to c_n. That is

$$\begin{aligned} P(\hat{c}_{n,e} = c_n) &= V \\ &= \sum_{s=0}^{4} \binom{16}{s} \left[1-(1-\alpha_E)^8\right]^s \\ &\quad \times \left[(1-\alpha_E)^8\right]^{16-s}, \end{aligned} \tag{14}$$

On the other hand, if $\hat{v}_{n,e}$ suffers more than 4 symbol errors, RS decoder failure may happen. According to the results in [27], the probability of decoder failure is $P_f > 1 - \frac{1}{t!} = 1 - \frac{1}{4!} \approx 0.96$. In addition, the undetected error under our selected RS code is 4.18×10^{-7} [28], indicating Eve can nearly ignore undetected errors, thereby focusing on corrected errors and decoding failures. Therefore the eavesdropper can find out the erroneous decoded block $\hat{c}_{n,e}$ and then choose to either avoid it in the linear cryptanalysis or rather keep the information bits only for these blocks.

In the former case where failed blocks are discarded, which happens once $\hat{v}_{n,e}$ suffers more than 4 symbol errors, and under the additional assumption that two consecutive decoded blocks $\hat{c}_{n-1,e}$ and $\hat{c}_{n,e}$ are independent which holds due to independent channel errors, the probability that $\hat{c}_{n,e}$ and $\hat{c}_{n,e}$ are both correctly decoded is $P_r = P(\hat{c}_{n-1,e} = c_{n-1}, \hat{c}_{n,e} = c_n) \approx V^2$. Consequently, the number of $\hat{v}_{n,e}$ required to mount a successful attack is

$$N_{RS,1} = \frac{1}{Pr} N \approx \frac{1}{V^2} N. \tag{15}$$

where N is defined in the same way as in (12).

In the later case where Eve keeps the information bits of the systematic code even in the presence of decoding failure, the average decoded information bit error probability is reduced from α_E to $P_{c,e}^{(RS)} = (1-V)\alpha_E$. With the similar technique as that for the uncoded system by applying Piling-Up Lemma [13], [14], we obtain the number of transmitted data blocks required to mount a successful attack for coded system without dropping the failed codewords as

$$N_{RS,2} = \frac{N}{(1-2P_{c,e}^{(RS)})^{2(u+v)}}. \tag{16}$$

To drop or to keep the failed packets is subject to the comparison between $N_{RS,1}$ and $N_{RS,2}$, from which Eve always gets the smaller one. As a result, the ultimately required number of pairs of plain-cipher text pairs is

$$\begin{aligned} N_{DCRS} &= \min\{N_{RS,1}, N_{RS,2}\} \\ &= \frac{N}{\max\left\{V^2, (1-2P_{c,e}^{(RS)})^{2(u+v)}\right\}}. \end{aligned} \tag{17}$$

2) Bit Error Rate Analysis: The bit error rate analysis for coded systems is similar as that for uncoded systems. If there are errors in the input $\hat{c}_{n-1}$ to a DES cipher under CFB mode, the output cipher text has 0.5 error probability. Due to RS decoding, the probability $P(\hat{c}_{n-1} \neq c_{n-1})$ can be approximated by $1 - V_B$, where V_B is the probability of successful decoding of RS code for the channel between Alice and Bob, which can be obtained as of (14) by replacing α_E with α_B, the cross over probability of the BSC channel to Bob.

When no error occurs in the received cipher text $\hat{c}_{n-1}$, leading us to $P(E_b|\hat{c}_{n-1} = c_{n-1})$ which is essentially the information bit error probability under RS decoding at Bob. Under the given systematic RS code, the decoder could directly pick the received information bit when a decoding failure occurs. Hence we have an approximation for the information bit error probability under RS decoding, which is $P(E_b|\hat{c}_{n-1} = c_{n-1}) \approx (1-V_B)\alpha_B$. As a result, the overall information bit error probability under the coded DES cipher with CFB mode is

$$\begin{aligned} P_{DCRS}(E_b) &= P\left(E_b|\hat{c}_{n-1} \neq c_{n-1}\right) P(\hat{c}_{n-1} \neq c_{n-1}) \\ &\quad + P\left(E_b|\hat{c}_{n-1} = c_{n-1}\right) P(\hat{c}_{n-1} = c_{n-1}) \\ &\approx 0.5(1-V_B) + P\left(E_b|\hat{c}_{n-1} = c_{n-1}\right) V_B \\ &\approx 0.5(1-V_B) + \alpha_B(1-V_B)V_B \end{aligned} \tag{18}$$

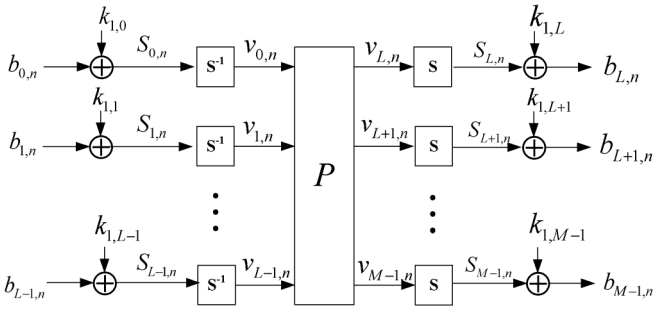


Fig. 3. Relations between bits in b_n.

C. DES Encryption With RS Code and Secret Sbox

1) Attack Against the Secret Sbox: For the system shown in Fig. 2(b), the secret Sboxes are employed after RS codes. Thus, there exist linear relationships between the input bits to the Sbox. The eavesdropper can use these linear relationships to mount an attack on the secret Sbox and get some k_1 bits [3]. In this section, we consider this kind of attack.

First, the wire-tap channel noise is not considered, i.e., we assume $\hat{b}_{n,e} = b_n$. In this case, we describe the linear cryptanalysis against this system and give the complexity of the attack. The linear correlation between bits in RS encoded codeword v_n have been shown in (4). The relationship between the transmitted codeword b_n and the RS encoded codeword v_n is given as below:

$$b_{i,n} = S(v_{i,n}) \oplus k_{1,i}. \tag{19}$$

For simplicity, we denote $S(v_{i,n})$ by $S_{i,n}$. Thus (19) can be rewritten as

$$b_{i,n} = S_{i,n} \oplus k_{1,i}. \tag{20}$$

With the analysis in (4) and (20), we get the relationships between the bits in the transmitted codeword b_n, which are shown in Fig. 3. The attacker can exploit some linear approximations between $b_n^I = (b_{0,n}, b_{1,n}, \cdots, b_{L-1,n})$ and $b_n^P = (b_{L,n}, b_{1,n}, \cdots, b_{M-1,n})$ to mount linear cryptanalysis. With such a cryptanalysis, the attacker can get some parts of the k_1 bits. The required linear approximations have the following form:

$$b_n^{[a_1]} \oplus b_n^{[a_2]} \oplus \cdots \oplus b_n^{[a_\lambda]} = k_1^{[d_1]} \oplus k_1^{[d_2]} \oplus \cdots \oplus k_1^{[d_\eta]}. \tag{21}$$

where $\{a_1, \cdots, a_\lambda\}$ and $\{d_1, \cdots, d_\eta\}$ are the active bits involved in linear cryptanalysis from the ciphertext and key sequence, respectively.

To find equation of the form (21), we first analyze the linear approximations between the inputs to the matrix P, v_n^I and the outputs, v_n^P. Since matrix P represents a linear transformation, there exist linear relations

$$v_{q_1,n}^{[A_1]} \oplus v_{q_2,n}^{[A_2]} \oplus \cdots \oplus v_{q_h,n}^{[A_h]} = 0, \quad q_1, q_2, \cdots, q_h \in [0, M-1], \tag{22}$$

which holds with the probability 1. In (22), $A_i = (a_{i,1}, a_{i,2}, \cdots, a_{i,\theta_i})$ denotes the active bits positions for the q_i-th symbol and $v_{q_i,n}^{[A_i]} = v_{q_i,n}^{[a_{i,1}]} \oplus v_{q_i,n}^{[a_{i,2}]} \oplus \cdots \oplus v_{q_i,n}^{[a_{i,\theta_i}]}$ denotes the Boolean summation of the active bits of the q_i-th symbol $v_{q_i,n}$. Corresponding to (22), the following linear approximations of Sbox are sought and constructed:

$$v_{q_w,n}^{[A_w]} = S_{q_w,n}^{[J_w]}, \quad w = 1, 2, \cdots, h. \tag{23}$$

where $[J_w]$ denotes the active bits to be approximated in the attacked Sbox. Since the Sbox is nonlinear, the probability that these equations hold is less than 1. The probability bias of these equations are denoted by $\varepsilon_{S,w}$. Then we substitute $v_{q_w,n}^{[A_w]}$ in (22) by $S_{q_w,n}^{[J_w]}$ and obtain the following expression:

$$S_{q_1,n}^{[J_1]} \oplus S_{q_2,n}^{[J_2]} \oplus \cdots \oplus S_{q_h,n}^{[J_h]} = 0. \tag{24}$$

Further, by using (20), we get

$$(b_{q_1,n} \oplus k_{1,q_1})^{[J_1]} \quad \oplus (b_{q_2,n} \oplus k_{1,q_2})^{[J_2]} \oplus \cdots \oplus (b_{q_h,n} \oplus k_{1,q_h})^{[J_h]} = 0. \tag{25}$$

This is just the required equation in the form of (21). We next compute the linear probability bias of this equation. According to Piling-Up Lemma, the linear probability bias of (25) can be calculated as

$$\varepsilon_s = 2^h \times \prod_{w=1}^{h} \varepsilon_{S,w} \times (1 - 0.5). \tag{26}$$

where $\varepsilon_{S,w}$ represents the probability bias of the Sbox. For AES Sbox, the probability bias is $\varepsilon_{S,w} < \varepsilon_S^{max} = 2^{-4}$ [24]. And h in (26) is the number of Sbox that needs to be approximated. From (22), we find that h is the number of input and output bytes that are linearly correlated. The value of h represents the diffusion property of matrix P.

We qualitatively describe the diffusion property of matrix P as follows. Assume two input values of matrix P, α_1 and α_2 satisfy $\alpha_1 \oplus \alpha_2 = (\Delta_0, \Delta_1, \cdots, \Delta_{L-1})$. The two corresponding output values are β_1 and β_2, $\beta_1 \oplus \beta_2 = (\Delta_L, \Delta_{L+1}, \cdots, \Delta_{M-1})$. In terms of RS encoder, (α_1, β_1) and (α_2, β_2) are both RS codewords. Since RS codes are linear block codes, $(\alpha_1 \oplus \alpha_2, \beta_1 \oplus \beta_2) = (\Delta_0, \Delta_1, \cdots, \Delta_{M-1})$ are also RS codewords. RS codes are MDS codes. Therefore there are at least $(M - L + 1 = L + 1)\Delta_i$ that is nonzero. Now we analyze the diffusion property of matrix P. When the input value of P changes from α_1 to α_2, the input difference $(\Delta_0, \Delta_1, \cdots, \Delta_{L-1})$ diffuse to output difference $(\Delta_L, \Delta_{L+1}, \cdots, \Delta_{M-1})$. The total number of changed symbols is at least $L + 1$. Intuitively, there are at least $L + 1$ input and output symbols of P that are correlated. In fact, the total number of changed symbols is defined as the branch number of matrix P in cryptography:

$$B = \min_{\alpha_1 \neq \alpha_2} \{|\{\Delta_i | \Delta_i \in \{\Delta_0, \Delta_1, \cdots, \Delta_{M-1}\}|\} \tag{27}$$

According to the results in [14], [29], for $(2L, L)$ RS codes, the branch number of matrix P is $B = L + 1$. Thus, the number of Sbox that needs to be approximated is $h \geq L + 1$, and the (26) can be further written as

$$\varepsilon_s < 2^L \left(\varepsilon_S^{max}\right)^{L+1} = 2^{-3L-4}. \tag{28}$$

Then it requires at least $N_S \approx (1/\varepsilon_s^2) = 2^{6L+8} = 2^{56}$ transmitted blocks b_n to mount a successful linear attack. N_S can be

further written as $N_S = 2^8 N$, where N is the number of data blocks needed for the attack on DES in CFB mode.

Now we analyze the security enhancement in the presence of wire-tap channel errors. Assume that there are totally H bits involved in (22). Then with the similar analysis as to the system in Fig. 2(a), the number of $\hat{b}_{n,e}$ required is

$$N_{S,e}^1 = \frac{1}{2^{2H}(1-\alpha_E-0.5)^{2H}} N_S = \frac{2^8}{(1-2\alpha_E)^{2H}} N \quad (29)$$

For each Sbox, there is at least one bit involved in (22). The number of Sbox need to be approximated is $h \geq L+1$. Therefore $H \geq L+1$. Thus we finally get a lower bound on the number of $\hat{b}_{n,e}$ required as

$$N_{S,e}^1 \geq \frac{2^8}{(1-2\alpha_E)^{2(L+1)}} N. \quad (30)$$

2) Attack Against the Entire System: The attack against the entire system shown in Fig. 2(b) consists of two steps. In the first step, the eavesdropper has to mount a known-ciphertext-only attack on the secret Sbox and get the key k_1. In the second step, with the key k_1, the eavesdropper launches a known plaintext attack by applying linear cryptanalysis to DES in CFB mode and get the key k. The attack in this step is very similar to the attack on the system in Fig. 2(a).

What we need to reevaluate is the resulting average bit error probability after the inverse operation of Sbox. For a powerful Sbox adopted in this work, the average bit error probability due to the channel distortion and inverse operation of Sbox is

$$\hat{\epsilon}_{se} = \left[1-(1-\alpha_E)^8\right] e_{sbox}, \quad (31)$$

where the first term is the probability of a symbol (8-bit) error over the BSC channel, as whenever there is an error in the input 8-bit symbol of the Sbox, the output surely has an error. The second term e_{sbox} denotes the average probability per output bit of S-box in Rijndeal, satisfying the bounds $0.5(1-e) \leq e_{sbox} \leq 0.5(1+e)$, where $e \leq e_{max} = 0.0352$ [30]. As a result, we have a bound on the equivalent bit error probability after the inverse of S-box at Bob or Eve. Actually, $\hat{\epsilon}_{se}$ can be computed precisely by exploring the differential uniformity of Rijndael S-box [24], which can be shown nearly the same as the approximation in (31).

As each Sbox has an 8-bit input and 8-bit output, the symbol error probability after S^{-1} remains the same as the one without Sbox, which is $1-V$ with V determined in (14). Therefore the resulting decoded average information bit error probability after RS decoding with Sbox is

$$P_{c,e}^{(RS,S)} = (1-V)\hat{\epsilon}_{se} \quad (32)$$

Using the similar approach as the case with only RS encoding but without Sbox in Fig. 2(a) and (17), the number of $\hat{b}_{n,e}$ required to mount the second step of the attack for DCRSS is

$$N_{S,e}^2 = \frac{N}{\max\left\{V^2, \left(1-2P_{c,e}^{(RS,S)}\right)^{2(u+v)}\right\}}, \quad (33)$$

which is subject to Eve's decision on whether to drop the entire information-bit block in the presence of decoding failure.

Note that the eavesdropper launches ciphertext only attack to analyze encrypted Sbox and then the known plaintext attack to analyze DES. Consider the most favorable case for the eavesdropper, we assume that the eavesdropper can get all the corresponding plaintexts for the ciphertexts used in the first step. Thus the total number of $\hat{b}_{n,e}$ needed to mount a successful attack on the entire system is

$$N_{DCRSS} = \max\left\{N_{S,e}^1, N_{S,e}^2\right\} = \max\left\{\frac{2^8 N}{(1-2\alpha_E)^{2(L+1)}}, \frac{N}{\max\left\{V^2, \left(1-2P_{c,e}^{(RS,S)}\right)^{2(u+v)}\right\}}\right\}. \quad (34)$$

3) Bit Error Rate Analysis: As S-box operates on byte basis, the bit error event out of the BSC channel will be thus confined over each byte after the inverse operation of the S-box at Bob. Thus adding an encrypted S-box after RS encoding does not affect the symbol-wise error probability, meaning that the probability V of correcting four or less symbol errors at Bob after the inverse mapping of S-box remains the same as in (14). When a decoding failure occurs, the information bit error probability after RS decoding is $(1-V_B)\hat{\epsilon}_{sb}$, where $\hat{\epsilon}_{sb} = [1-(1-P_c)^8]0.5$, as that obtained in (31). Therefore the overall average information bit error probability is

$$P_{DCRSS}(E_b) \approx 0.5(1-V_B) + V_B(1-V_B)\hat{\epsilon}_{sb}. \quad (35)$$

IV. Comparison Metrics and Simulation Results

A. Bit Error Rate at Bob

Simulations have been undertaken to find out the average information bit error probability at Bob for the three systems considered in this paper, namely, uncoded DES under CFB (DC), coded (RS coding) DES under CFB (DCRS), and S-box aided coded DES under CFB (DCRSS). In Fig. 4, theoretically derived approximation of the average BER for each scheme is compared against simulation results. It can be seen that simulation results agree well with the derived approximations. Furthermore, channel coding reduces error rate significantly as compared with the uncoded approach. In addition, adding nonlinear and encrypted S-box only increases the BER slightly as compared with the case DCRS, which is desired.

From Fig. 4, we can see that as the channel cross-over probability $\alpha_B = \epsilon$ is greater than 0.1, all approaches perform poorly, yielding nearly 0.5 information bit error probability. This is because as the channel becomes worse, the sequence error probability at the input of each DES cipher is close to one, thereby making the diffusion effect become dominant, and consequently creating nearly 0.5 bit error probability at the output of DES cipher. Thus, we can say given the system framework considered in this paper, the upper-bound $\alpha_{B,max}$ for α_B is 0.1, beyond which the end-to-end channel between Alice and Bob will be saturated with 0.5 postdecryption bit error probability, resulting in a zero capacity, not usable to legitimate users any more.

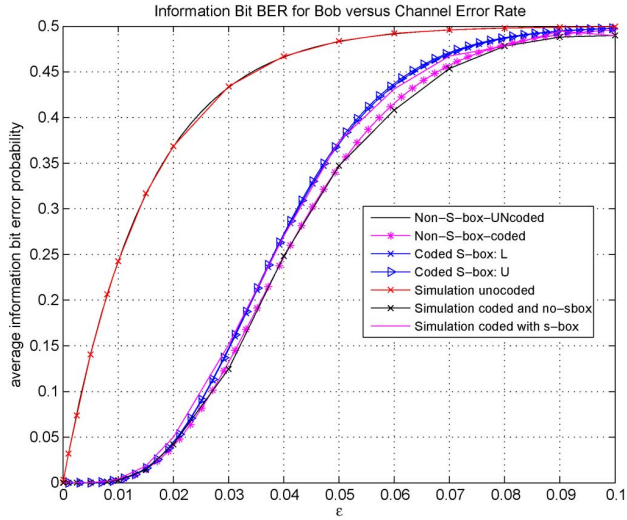


Fig. 4. Theoretical and simulated BER.

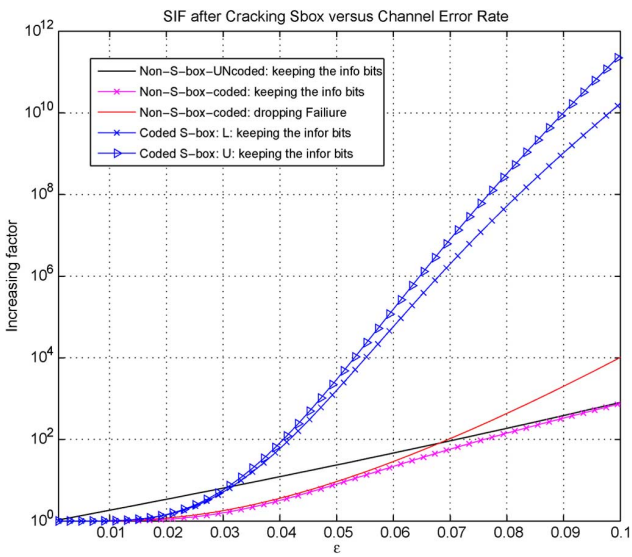


Fig. 5. Security increased factor (SIF) for DC, DCRS, and DCRSS.

B. Secrecy Improving Factor

From our analysis on the effect of channel error rate on the security of proposed three schemes, namely, DC, DCRS and DCRSS, we can see that the amount of efforts in terms of required plaintext and ciphertext (PC) pairs increases as the channel between Alice and the eavesdropper degrades. To quantify this effect, we herein introduce a metric coined as secrecy improving factor (SIF) defined as the ratio between the required PC pairs in the presence of channel error and that without channel errors, which can be obtained from (12), (17) and (34). In Fig. 5, different schemes are compared in terms of SIF.

In this figure, we intentionally separate the SIF of coded cases with or without Sbox under the option of dropping codewords and keeping the information bits, respectively, when decoding failure occurs. That means for (17) and (33), we consider the arguments of the maximum operation separately. In addition, for the coded case with Sbox (DCRSS), its SIF only includes the effort in the second step in its cryptanalysis by assuming the key for encrypted Sboxes has been cracked successfully so that DCRS and DCRSS can be compared on the same basis. It can be seen from Fig. 5 that the eavesdropper should keep the decoded information bits for DCRS whereas the failed packets should be dropped for the DCRSS in order to minimize the resulting SIF. Also can be seen is that the scheme DCRS yields smaller SIF than the uncoded DC scheme because channel coding improves channel quality.

Without concerning the efforts made in attacking the encrypted Sboxes, when channel error probability is below certain value (e.g. 0.06 in this case), DCRSS and DCRS attains the same SIF in cracking DES in CFB mode. On the other hand, when channel is degraded beyond certain extent (e.g. 0.09), the SIF for the uncoded case DC is nearly the same as DCRS, but much smaller than that under DCRSS.

C. Trade-Off Between BER and SIF

From Fig. 4 and Fig. 5, we can see that if the channel between Alice and Eve has $\alpha_E = \epsilon$ greater than $\epsilon = 0.1$, not only will that lead to a significant amount of additional efforts for Eve to engage in cryptanalysis, it also results in a nearly 0.5 information bit flipping probability even after Eve successfully gets the secrete key from its cryptanalysis, which demonstrates the powerfullness of channel errors in enhancing security of the studied block-cipher system.

However, the degradation in information bits restoration after decryption in the presence of channel errors also applies to the legitimate receiver. Therefore to take advantage of channel error effect, Alice could consider to put intentional errors to the output of either RS coder for DCRS or encrypted Sbox for DCRSS at its transmitter even if the actual physical channel errors could be completely eliminated. That additional error serves the purpose of making trade-off between BER degradation and SIF enhancement. To be noted is that Eve receives her erroneous ciphertexts during the course of making inquiries to an Oracle to conduct her known plaintext attack, whereas Bob gets his distorted ciphertexts in a phase of regular communication with Alice. The binary errors in their respective ciphertexts are therefore independently and identically distributed.

In order to further reveal the trade-off between reliability (to Bob) and security (to Eve), we consider a case where the crossover probabilities of the two BSC channels to Bob and Eve are the same, i. e. $\alpha_B = \alpha_E = \epsilon$. The trade-off for a scheme is characterized by a curve featuring the relationship between the normalized SIF in terms of SIF per key bit $\log(\mathrm{SIF}/K_j)$ and normalized information error probability $\log(P_e/\epsilon)$, as shown in Fig. 6 and Fig. 7, where K_1 and K_2 denote the total number secrete key bits for DCRS and DCRSS, respectively. The SIF for DCRSS in Fig. 6 has $K_2 = 56$ when we don't count the effort in attacking encrypted nonlinear Sboxes. As a contrast, that effort is incorporated in computing the total cryptanalysis SIF with $K_2 = 128 + 56 = 184$ for DCRSS in Fig. 7. Due to the space limitation and the focus of this paper, we are not able to provide a more comprehensive analysis about the cost in establishing an agreement on K_1 between legitimate users, and put that in the context of security enhancement as measured by a normalized secrecy enhancement factor (SIF), which will be further investigated in our future works.

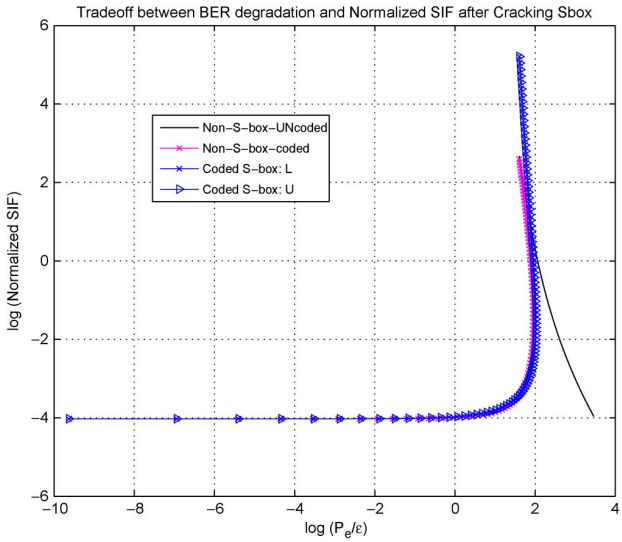


Fig. 6. Trade-off between security and reliability: Normalized SIF $\log(SIF/K)$ versus normalized information BER $\log(P(E_b)/\epsilon)$ without counting the efforts in cracking the Sbox.

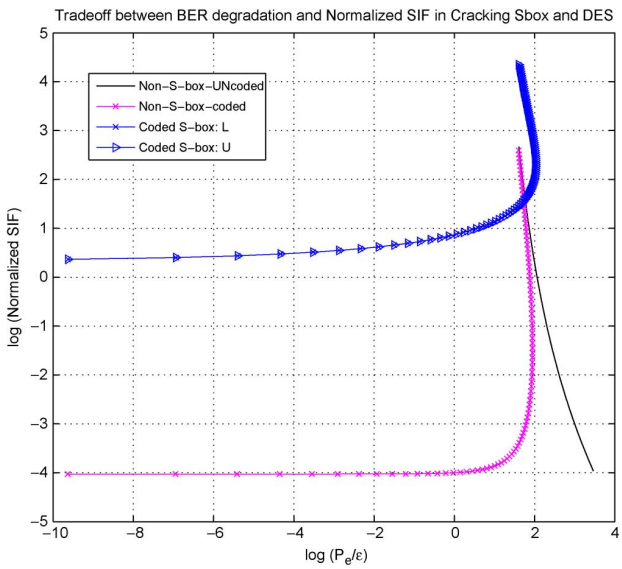


Fig. 7. Trade-off between security and reliability: Normalized SIF $\log(SIF/K)$ versus normalized information BER $\log(P(E_b)/\epsilon)$ after counting the efforts in cracking the Sbox.

As seen from these curves, DC achieves the same SIF as DCRS and DCRSS at the expense of more degradation of its performance in terms of larger P_e than ϵ at the legitimate receiver. Without counting the effort in cracking encrypted Sboxes, DCRS and DCRSS achieves nearly the same trade-off between security enhancement and performance degradation. Moreover, to have a notable SIF improvement, DCRS and DCRSS have to suffer a degradation of P_e around a factor of $e^2 = 7.4$ of ϵ for its restored information bits, corresponding to ϵ in the range of [0.05, 0.07]. However, when the effort in crypt-analyzing encrypted Sboxes is taken into account, there is a significant improvement in the resulting normalized SIF (by $K_2 = 184$) for DCRSS, which suggests the additional complexity expended in the second encryption block pays

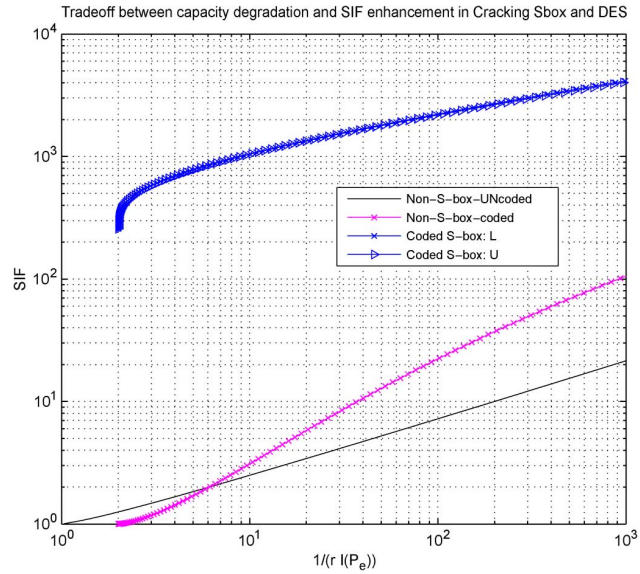


Fig. 8. Trade-off between capacity degradation and SIF in cracking both DES and encrypted Sboxes.

back well in terms the further gains in SIF under the same degradation of P_e.

The final remark is that in order to have the proposed system really work, we should add the last processing layer before DES encryption, which is intended to correct all residual errors at Bob caused by performance degradation due to the added intentional errors. We therefore have essentially proposed the following two-layer concatenated scheme: outer channel coding with outer encryption concatenated with inner channel coding and inner encryption, after which some intentionally induced channel noise could be added to further aggravate the crypt-analysis effort and postcryptanalysis performance at Eve. Some powerful error correction techniques, such as LDPC codes [31] or polar codes [32] could be adopted as candidates for the outer channel encoder to achieve the mutual information rate $I(P_e) = 1 + P_e \log(P_e) + (1 - P_e) \log(1 - P_e)$ of the resulting binary symmetric channel, where P_e denotes the postdecryption information bit error probability of the outer-decryption block of the concatenated system.

In Fig. 8, we compare the trade-off between SIF and its associated capacity degradation defined as $1/[rI(P_e)]$ where r is the coding rate of the inner-channel coder. For example, in our case study, $r = 1$ for DC (the uncoded case), and $r = 0.5$ for DCRS and DCRSS where 0.5 is the coding rate of the adopted RS code. From Fig. 8, we can see that, for instance, if the legitimate users are willing to sacrifice the rate reduction by a factor of 100 in decreasing from 1 for the case without induced noise to 0.01 for the case with induced noise, the gains attained in SIF for DC, DCRS, and DCRSS are roughly around 7, 20 and 2000, respectively. It is up to the system designer to decide if it is worthwhile to gain additional security enhancement at the expense of sacrificing the throughput of the system to such an extent. *Therefore putting SIF and* $1/[rI(P_e)]$ *together provides us an ultimate way in demonstrating the pros and cons of exploiting channel errors in terms of performance loss and security enhancement.*

REFERENCES

[1] B. Schneier, *Applied Cryptography*, 2nd ed. Hoboken, NJ, USA: Wiley, 1996.

[2] Establishing Wireless Robust Security Networks: A guide to IEEE 802.11i, NIST Special Publication 800-97, 2007.

[3] N. K. E. Barkan and E. Biham, "Instant cipher-text only cryptanalysis of GSM encrypted communications," *Lecture Notes Computer Sci.*, vol. 2729, pp. 600–616, 2006.

[4] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[5] G. Ferland and J. Chouinard, "Performance of BCH codes with DES encryption in a digital mobile channel," *Lecture Notes Computer Sci.*, vol. 793, pp. 153–172, 1994.

[6] M. Reason and D. Messerschmitt, "The impact of confidentiality on quality of service in heterogeneous voice over IP networks," *Lecture Notes Computer Sci.*, vol. 2216, pp. 175–192, 2001.

[7] M. A. Haleem, C. Mathur, R. Chandramouli, and K. Subbalakshmi, "Opportunistic encryption: A trade-off between security and throughput in wireless networks," *IEEE Trans. Depend. Secure Comput.*, vol. 4, no. 4, pp. 313–324, Oct./Dec. 2007.

[8] M. M. F. Sattar, "On modeling post decryption error processes in UMTS Air interface," *Lecture Notes Computer Sci.*, vol. 4990, pp. 507–516, 2008.

[9] Y. Xiao, H. Chen, X. Du, and M. Guizani, "Stream-based cipher feedback mode in wireless error channel," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 622–626, Feb. 2009.

[10] J. H. K. Kim, "Performance analysis of digital secure voice transmission over HF radio channel," *Lecture Notes Computer Sci.*, vol. 5576, pp. 337–346, 2009.

[11] I. E. O. Kara, "New approach to keystream based cryptosystems," in *Proc. Workshop Record SASC 2008*, 2008, pp. 205–221.

[12] M. J. Mihaljevic and H. Imai, "An approach for stream ciphers design based on joint computing over random and secret data," *Computing*, vol. 85, no. 1–2, pp. 153–168, 2009.

[13] H. M. Keys, "A tutorial on linear and differential cryptanalysis," *Cryptologia*, vol. 26, no. 3, pp. 189–221, 2002.

[14] M. Matsui, "Linear cryptanalysis method for DES cipher," *Lecture Notes Computer Sci.*, vol. 765, pp. 386–397, 1994.

[15] Y. W. Law, J. Doumen, and P. Hartel, "Survey and benchmark of block ciphers for wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 2, pp. 65–93, Feb 2006.

[16] O. Adamo, S. Fu, and M. Varanasi, "Physical layer error correction based cipher," in *Proc. 2010 IEEE Global Telecommunications Conf. (GLOBECOM 2010)*, Dec. 2010, pp. 1–5.

[17] Q. Chai and G. Gong, "Differential cryptanalysis of two joint encryption and error correction schemes," in *Proc. 2011 IEEE Global Telecommunications Conf. (GLOBECOM 2011)*, Dec. 2011, pp. 1–6.

[18] G. D. Forney, *Concatenated Codes (Research Monograph)*. Cambridge, MA, USA: MIT Press, Dec. 1966.

[19] M. Mihaljevic and F. Oggier, "A wire-tap approach to enhance security in communication systems using the encoding-encryption paradigm," in *Proc. IEEE 17th Int. Conf. Telecommunications (ICT)*, Apr. 2010, pp. 83–88.

[20] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[21] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[22] S. Lloyd, "Balance, uncorrelatedness and the strict avalanche criterion," *Discrete Appl. Math.*, vol. 41, no. 3, pp. 223–233, Feb. 1993.

[23] S. Lin, J. Daniel, and J. Constello, *Error Control Coding*, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2004.

[24] J. Daemen and V. Rijmen, *The Design of Rijndael: AES-The Advanced Encryption Standard*. Berlin, Germany: Springer Verlag, 2002.

[25] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proc. Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, 1994, pp. 386–397.

[26] S. E. Tavares and H. M. Heys, "Avalanche characteristics of substitution-permutation encryption networks," *IEEE Trans. Computers*, vol. 44, no. 9, pp. 1131–1139, Sep. 1995.

[27] L. S. R. J. Mceliece, "On the decoder error probability for Reed-Solomon codes," *IEEE Trans. Inf. Theory*, vol. 32, no. 5, pp. 701–703, Sep. 1986.

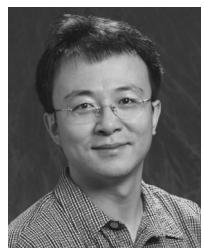
[28] D. Torrieri, "Information-bit, information-symbol, and decoded-symbol error rates for linear block codes," *IEEE Trans. Commun.*, vol. 36, no. 5, pp. 613–617, May 1988.

[29] V. Rijmen, J. Daemen, B. Preneel, A. Bossalaers, and E. Win, "The cipher shark," *Lecture Notes Computer Sci.*, vol. 1039, pp. 99–111, 1996.

[30] K. Nyberg, "S-boxes and round functions with controllable linearity and differential uniformity," *Fast Software Encryption*, pp. 111–130, 1994.

[31] D. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 399–431, Mar. 1999.

[32] E. Arikan, "Channel polarization: A method for constructing capacityachieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

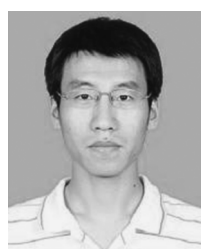


Shuangqing Wei (S'99–M'03) received the B.E. and M.E. degrees in electrical engineering from Tsinghua University in 1995 and 1998, respectively. He started his academic career at Louisiana State University (LSU) after receiving the Ph.D. degree from the University of Massachusetts, Amherst in 2003.

He is currently a Tenured Associate Professor at the School of Electrical Engineering and Computer Science at LSU. His research interests are in the areas of wireless security and cognitive radio networks. He is an Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He has served as a Technical Program Committee (TPC) Member for numerous IEEE Flagship communication conferences, such as ICC, Globecom, and MILCOM. His research has been funded by the NSF, AFRL, and DOE, and the Board of Regents of Louisiana.

Jian Wang (M'12) received the Ph.D. degree in electronic engineering from Tsinghua University in 2006.

In 2006, he joined the faculty of Tsinghua University, where he is currently an Associate Professor in the Department of Electronic Engineering. His research interests are in the areas of wireless security, signal processing in the encrypted domain, and cognitive radio networks.



Ruming Yin received the B.S. and Ph.D. degrees in electronic engineering from Tsinghua University in 2005 and 2010, respectively. His research is focused on chaos-based cryptography and cryptanalysis.

Jian Yuan received the M.S. degree in signals and systems from Southeast University, Nanjing, China, in 1989, and the Ph.D. degree in electrical engineering from the University of Electronic Science and Technology of China, in 1998.

He holds the position of Professor of electronic engineering at Tsinghua University, Beijing, China. His main interests are in network security and cognitive networks.