High Diffusion Cipher: Encryption and Error Correction in a Single Cryptographic Primitive

Chetan Nanjunda Mathur, Karthik Narayan and K.P. Subbalakshmi

Department of Electrical and Computer Engineering
Stevens Institute of Technology, Hoboken, NJ 07030, USA
cnanjund@stevens.edu

Abstract. In this paper we combine the error correction and encryption functionality into one block cipher, which we call High Diffusion (HD) cipher. The error correcting property of this cipher is due to the novel error correction code which we call High Diffusion code used in its diffusion layer. Theoretical bounds on the performance of the HD cipher in terms of security and error correction are derived. We show that the proposed HD cipher provides security equivalent to Rijndael cipher against linear and differential cryptanalysis. Experiments based on a four round HD cipher reveal that traditional concatenated systems using the Rijndael cipher followed by Reed Solomon codes require 89% more expansion to match the performance of HD cipher.

Key words: Error correcting cipher, Joint error correction and encryption, Coding and cryptography, Block cipher, Error correcting code

1 Introduction

In most cases, the very same properties that provide security to a cipher (e.g. avalanche effect) makes them sensitive to transmission errors. In block ciphers (which operates on a fixed block length of data at a time) a single bit flip in the encrypted data can cause a complete decryption failure. This sensitivity causes more retransmissions compared to unencrypted transmission, reducing the overall throughput [20]. Hence, transmitting encrypted data often requires the use of error correction codes to efficiently and reliably recover the information during decryption. Although, traditionally error correction and encryption are handled independently, some of the motivations to combine them into one primitive are a) both error correction and encryption are now performed in the same layer (e.g. link layer in wireless networks) b) error correction codes are already present in communication devices, therefore using codes as building blocks for a cipher is advisable from an implementation standpoint c) the increasing popularity of resource constrained devices in noisy media like the wireless networks could potentially benefit from a joint design of the error correction and encryption primitives in terms of achieving a better system level operating point than the traditional disjoint approach. Hence, designing ciphers to provide error correction functionality in addition to encryption is of significance in many applications.

Although mathematical relationships exist between error correction and encryption [24], there have been only a few attempts to build error correcting ciphers. Some of the notable results include the McEliece cipher [18], the Hwang and Rao cipher [13] and the Godoy-Pereira scheme [12]. Some of the issues with these ciphers are (a) these systems are not designed based on well known security principles (and hence are vulnerable to various attacks [2]) (b) they are not as efficient as traditional forward error correcting (FEC) codes in terms of error correction capability, as they trade error correction capacity to achieve security. In fact, in order to achieve meaningful error correction capacity, the parameters of the system have to be very large leading to high computational complexity. The difficulty in designing error correcting ciphers arise from the fact that error correction and encryption work at cross purposes to each other.

In this paper, we propose an error correcting block cipher called the High Diffusion (HD) cipher. The HD cipher, like standard block ciphers [23], is composed of several iterations of the round transformation and mixing with the secret key. The round transformation functions are composed of a non-linear substitution layer and a linear diffusion layer. The error correcting property of the HD cipher is due to the use of a novel class of codes that we call High Diffusion codes [16] [21] in the diffusion layer of a cipher. We show that HD ciphers are not vulnerable to known plaintext type of attacks described in [2] which were effective on previously known error correcting ciphers [13] [12] [18]. In fact, we show that the HD ciphers are as secure as the Rijndael cipher [10] against the well known differential, linear cryptanalysis [3][17] and Square attacks [14]. To assess the performance of our proposed cipher, we compare it with the traditional concatenated system that use Rijndael cipher followed by Reed Solomon codes [25]. We show that HD cipher outperforms the traditional mechanism both in terms of security and error correction.

2 Proposed High Diffusion Cipher (HD cipher)

A block diagram of the High Diffusion cipher encryption is given in Fig. 1. The HD cipher is a Key-Alternating [8] block cipher, composed of several iterations of the round transformation and key mixing operation. The round transformation consists of three layers. The first one is the non linear substitution layer, this is followed by the symbol transposition layer and finally the High Diffusion encoding layer. Note that, HD encoding is not performed in the final round.

The key mixing layer follows every round transformation and is also performed once before the first round. The HD cipher decryption proceeds in the exact reverse order to that of the encryption process, however the HD encoding layer is replaced by the HD decoding layer.

Now, we introduce some notations that are used in the rest of this paper. The inputs to the HD cipher encryption are the plaintext (denoted by P) and

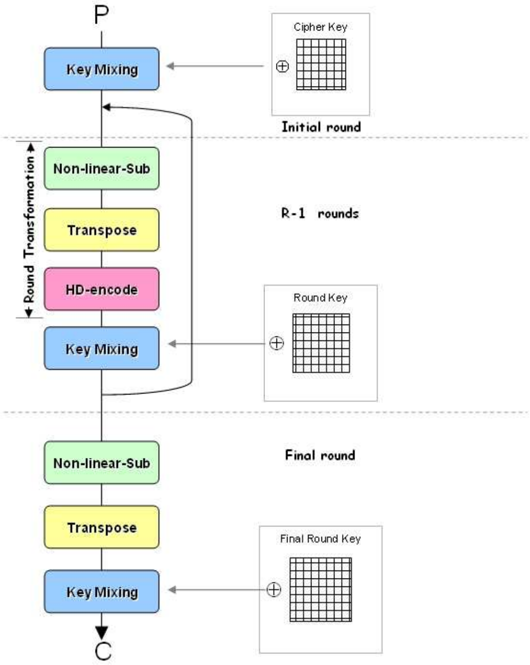

Fig. 1. Block Diagram of High Diffusion Cipher.

the key (denoted by K). The output is the ciphertext (denoted by C). The total number of rounds in the cipher is denoted by R. The plaintext as it goes through each round of the cipher is referred to as the *cipher state*. The number of bits in the cipher state after $r \in \{0...R\}$ rounds is denoted by n_b^r. Note that, n_b^0 is the number of bits in P and n_b^R is the number of bits in C. The total number of key bits, denoted by n_k, is equal to n_b^R. We propose to use the same key schedule algorithm as in Rijndael [10], which extends the n_k bit cipher key into $(R+1) \times n_k$ bits to produce $R+1$ round keys $\{\boldsymbol{k}^0, \boldsymbol{k}^1, ..., \boldsymbol{k}^R\}$. All the operations in HD cipher are performed in the finite field of order 2^m, denoted by GF(2^m). Hence, the n_b^r bits are logically grouped into n_s^r symbols represented by m bits each. A detailed description of all the layers of HD cipher will follow.

2.1 Key Mixing Layer

The key mixing layer, which we denote by σ, is a bitwise XOR operation of the cipher state with the round key. Note that, the round keys are larger than the intermediate cipher states for all but the last round of the cipher. The input and output of σ at round r are denoted by $\boldsymbol{x}_\sigma^r$ and $\boldsymbol{x}_\gamma^r$ respectively. The σ transformation for round r can be expressed by,

$$\sigma^r : \boldsymbol{x}_\gamma^{r+1} = \sigma(\boldsymbol{x}_\sigma^r, \boldsymbol{k}^r) \Longleftrightarrow \boldsymbol{x}_\gamma^{r+1} = (\boldsymbol{x}_\sigma^r \oplus \boldsymbol{k}^r). \quad (1)$$

Note that, the output of the key mixing layer forms the input to the next round. However, when $r = R$, the output of σ is the C.

2.2 Non-linear Substitution Layer

The substitution layer, denoted by γ, is the only non-linear step in the HD cipher. This layer uses an invertible local non-linear transformation called the S-box, S_γ. The construction of S_γ is similar to that in Rijndael [22], where the substitution box is generated by inverting elements in GF(2^m) and applying an invertible affine transform (to prevent zeroes mapping to zero). The design of the S_γ minimizes large correlation and difference propagation (see Section 3) between input bits and output bits. The S_γ so designed, causes intra symbol avalanche [9] (that is every bit in the output symbol of the S-box flips with a probability of half for a single bit flip in the input symbol), which is essential for the security of the cipher. S_γ transforms the input vector $\boldsymbol{x}^r_\gamma$ to the output vector $\boldsymbol{x}^r_\pi$ by acting on each of the n^r_s symbols in the input vector independently.

The γ transformation can be expressed by,

$$\gamma^r : \boldsymbol{x}^r_\pi = \gamma(\boldsymbol{x}^r_\gamma) \Longleftrightarrow x^r_\pi(j) = S_\gamma(x^r_\gamma(j)) \ , \tag{2}$$

where, $j \in \{1...n^r_s\}$. During HD cipher decryption, inverse substitution box, $s_{\gamma^{-1}}$, is used instead of s_γ.

2.3 Symbol Transposition Layer

The symbol transposition layer, denoted by π, is the first of the two diffusion operations used in the HD cipher. The aim of this layer is to permute the cipher state using a diffusion optimal transformation. It applies a matrix transposition type of permutation on the cipher state. With respect to π, the input state $\boldsymbol{x}^r_\pi$ is arranged into $n^r_u \times n^r_v$ matrix X^r_π (with n^r_u rows and n^r_v columns). This matrix is then transposed to obtain $n^r_v \times n^r_u$ matrix X^r_θ. This is then mapped to the vector representation $\boldsymbol{x}^r_\theta$. The π transformation can be expressed by,

$$\pi^r : \boldsymbol{x}^r_\theta = \pi(\boldsymbol{x}^r_\pi) \Leftrightarrow \mathrm{X}^r_\theta = (\mathrm{X}^r_\pi)^T \tag{3}$$

In matrix transposition transformation, any two symbols appearing in the same column before the transformation appear in different columns after the transformation. Hence, this transformation is a diffusion optimal transformation [6].

2.4 High Diffusion Coding Layer

The High Diffusion coding layer is the second of the two diffusion operations used in the HD cipher. The aim of this layer is to diffuse the intra symbol avalanche caused by the substitution layer to a large number of symbols in the resulting cipher state. In HD cipher, this layer has an additional aim, which is to correct transmission errors during decryption. Hence, we need to use an error correcting code, with encoding operation θ, to perform this transformation.

In this section, we first introduce the criteria that channel codes to be used in this transformation should satisfy. We call the channel codes that satisfy these criteria as HD codes. Some techniques to construct HD codes are given. Finally, we define the HD coding and decoding transformations as applied in the HD cipher.

Design criteria for HD coding transformation: The aim of HD coding transformation is to design θ such that we attain the highest possible security (in terms of diffusion) and error correction. Therefore, we derive two criteria that θ codes must satisfy:

- *Security Criterion:* Since, the θ will be used in the diffusion layer it needs to spread the intra symbol avalanche caused by the substitution operation to a large number of output symbols. The spreading power, diffusion, is measured using the concept of *branch number* [8]. Let vectors $\boldsymbol{a}$, $\boldsymbol{b}$ represent any two arbitrary k symbol input vectors and $\theta(\boldsymbol{a})$, $\theta(\boldsymbol{b})$ represent the corresponding n symbol output vectors. Then the branch number of the transformation θ is defined as,
$$\mathcal{B}(\theta) = \min_{\boldsymbol{a},\boldsymbol{b}\neq\boldsymbol{a}} \{H_d(\boldsymbol{a},\boldsymbol{b}) + H_d(\theta(\boldsymbol{a}),\theta(\boldsymbol{b}))\} \tag{4}$$
Here, H_d denotes the symbol hamming distance. Since, the maximum output difference corresponding to a single non-zero symbol input difference is n. The upper bound for $\mathcal{B}(\theta)$ is $n+1$. To provide good security, θ must have the maximum possible branch number. Hence, we set
$$\mathcal{B}(\theta) = n + 1 \tag{5}$$
as the security criterion of θ.
- *Error Resilience Criterion:* The number of errors that can be corrected by a code is governed by the pairwise minimum distance between the codewords [25]. A large minimum distance would ensure good error resilience property. The minimum distance between two codewords in the code space is usually denoted by $d_{\min}$. The best possible $d_{\min}$ for a code is attained when the code satisfies the Singleton bound. That is,
$$d_{\min} = n - k + 1 \tag{6}$$
where, n is the codeword length and k is the message length. Codes that satisfy Singleton bounds are referred to as Maximum Distance Separable (MDS) codes. Hence, we set θ to be an encoding function of an $[n, k, 2^m]$ MDS code as the error resilience criterion.

The following is an interesting property that connects the security criterion 5 to the error resilience criterion 6.

Theorem 1. *Any $[n, k, q]$ code $\mathcal{C}$ with encoding operation θ, that satisfies $\mathcal{B}(\theta) = n + 1$ also satisfies $d_{\min} = n - k + 1$.*

Proof. Consider any two codewords $\mathbf{c}_i$ and $\mathbf{c}_j$ and $\mathbf{m}_i$ and $\mathbf{m}_j$ be the corresponding messages. Then,

$$\begin{aligned}H_d(\boldsymbol{c}_i, \boldsymbol{c}_j) + H_d(\boldsymbol{m}_i, \boldsymbol{m}_j) &= n + 1\\ H_d(\boldsymbol{c}_i, \boldsymbol{c}_j) &= n - H_d(\boldsymbol{m}_i, \boldsymbol{m}_j) + 1\\ H_d(\boldsymbol{c}_i, \boldsymbol{c}_j) &\geq n - k + 1\end{aligned}$$

Since, $\boldsymbol{c}_i$ and $\boldsymbol{c}_j$ are any two codewords. We have $d_{\min} = n - k + 1$.

However, the converse is not true. That is any code that satisfies 6 need not satisfy 5. To the best of our knowledge, there are no known channel codes that inherently satisfy both security and error resilience criteria.

The new codes that satisfy both the security and error resilience criterion are called as High Diffusion (HD) codes. The following is the definition of HD codes.

Definition 1. *High Diffusion codes are $[n, k, q]$ MDS codes that satisfy the branch number of $n + 1$.*

Construction of HD codes: Unlike usual error correcting codes, the branch number criterion for HD codes involves *pairs of messages* and their associated codewords. This makes deriving a closed form expression (or encoding transformation θ) for the construction of the codes tricky. A brute force search produces the complete mapping with the highest expected runtime. Then, the θ has to derived from these mappings. We have, so far developed some shortcut techniques to generate HD codes. A brief outline of these techniques follow:

- *Coset Based Search*: Cosets are formed such that the codewords are assigned to the coset leaders only. The codewords for the rest of the coset elements are related to each other, often they are rotations of each other. The coset based search makes use of cosets to reduce the complexity of the code assignment. This searching technique only needs to find codewords for the coset leaders. We then use the message to codeword mapping to derive θ.
- *Transformation from Reed Solomon Codes*: In this technique, we start with a known MDS code and transform the encoding transformation of this MDS code into an encoding transformation of the HD code. As Reed Solomon (RS) codes are an important subclass of MDS codes, we start with $[q-1, k, q]$ RS codes and transform them into $[q-1, k, q]$ HD codes using permutations of the message-codeword assignments that satisfy the branch number criterion. An example of this method is given in [16]. *Note that the traditional method to generate an RS code cannot be directly used to generate an HD code, because the HD codes have a second property to be satisfied viz., the branch number criterion.*

- *Puncturing Existing Codes:* This gives us an easy way to generate new HD codes from existing HD codes. The following Theorem 2 proves that Puncturing HD codes result in HD codes.

  Theorem 2. *Punctured HD codes are HD codes.*

  Proof. Let $\mathcal{C}$ be an $[n, k, q]$ HD code and $\mathcal{C}'$ be the punctured $[n-1, k, q]$ code obtained from $\mathcal{C}$. Let $\boldsymbol{m}_i$, $\boldsymbol{m}_j$ be any two messages with their corresponding codewords $\boldsymbol{c}_i$, $\boldsymbol{c}_j$ in $\mathcal{C}$ and $\boldsymbol{c'}_i$,$\boldsymbol{c'}_j$ in $\mathcal{C}'$. We know that $\mathcal{C}$ is an HD code, therefore $H_d(\boldsymbol{m}_i, \boldsymbol{m}_j) + H_d(\boldsymbol{c}_i, \boldsymbol{c}_j) \geq n + 1$. We know that, $\boldsymbol{c'}_i$ and $\boldsymbol{c'}_j$ are obtained by puncturing $\boldsymbol{c}_i$ and $\boldsymbol{c}_j$ in one symbol position. This implies that $H_d(\boldsymbol{m}_i, \boldsymbol{m}_j) + H_d(\boldsymbol{c'}_i, \boldsymbol{c'}_j) \geq n$. Hence, $\mathcal{C}'$ is an HD code.

HD encoding operation ($\boldsymbol{\theta}$) : The HD encoding operation, denoted by θ, uses HD codes. The cipher state, $\boldsymbol{x}^r_\theta$, at the input to the HD encoding operation, is arranged in the form of an $n^r_u \times n^r_v$ matrix X^r_θ. An $[n^r_{u'}, n^r_u, 2^m]$ HD code with encoding operation θ^r is used to encode each column of X^r_θ independently. The resulting output cipher state is now represented by a $n^r_{u'} \times n^r_v$ matrix X^r_σ which is then mapped to $\boldsymbol{x}^r_\sigma$. The HD encoding operation θ can be represented as,

$$\theta^r : \boldsymbol{x}^r_\sigma = \theta(\boldsymbol{x^r_\theta}) \Leftrightarrow \mathrm{X}^r_\sigma(j) = \theta^r(\mathrm{X}^r_\theta(j)) \ , \tag{7}$$

where $\mathrm{X}^r(j)$ represents the j-th column of the matrix. As the same θ^r is used on all the input columns, branch number $\mathcal{B}(\cdot)$ is lower bounded by:

$$\begin{aligned} \mathcal{B}(\theta^r) &\geq n^r_{u'} + 1, & (8)\\ &\geq n^r_u + d^r_{min}. & (9) \end{aligned}$$

HD decoding operation $\boldsymbol{\psi}$: HD decoding operation, denoted by ψ, is used during decryption. So far, we have generated HD codes by transforming the RS codes. Hence, we use the Berlekamp-Massey [1] algorithm, which is used to decode RS codes, to decode HD codes. For all valid cipher states, the branch number property of θ^r is also inherent in ψ^r. The bound on error correction capability, t^r, of ψ^r is derived from the minimum distance between codewords of the HD code θ^r as follows:

$$\begin{aligned} t^r &= \lfloor \frac{d^r_{min}}{2} \rfloor \\ t^r &= \lfloor \frac{n^r_{u'} - n^r_u + 1}{2} \rfloor \\ \therefore t^r &= \lfloor \frac{\mathcal{B}(\theta^r) - n^r_u}{2} \rfloor \end{aligned} \tag{10}$$

From 9 and 10 we can observe that the parameter $d_{\min}$ jointly controls the diffusion strength and error correction capacity in the HD cipher.

3 Security Analysis of HD ciphers

Security of symmetric block ciphers is usually measured by their key lengths. This is because for an attacker, the complexity of the attack grows exponentially with the key length. Although the key length n_k used in HD cipher is n_b^R bits, we look at the existence of attacks with complexity lesser than $\mathcal{O}(2^{n_b^0})$, where n_b^0 is the length of plaintext. This is because, with $n_b^0 \leq n_b^R$, a dictionary attack will perform better than a brute force key search. However, a brute force attack is not the only possible attack. For example, shortcut attacks make use of the structure of the cipher to come up with a technique to break it (deduce the secret key) with complexity lesser than $\mathcal{O}(2^{n_b^0})$. In this section, we analyze the security of HD ciphers by looking at the resistance it offers against some well known cryptanalytic attacks.

3.1 Linear and Differential Cryptanalysis

In this section, we analyze the security of HD cipher in terms of linear and differential cryptanalysis. Differential cryptanalysis [3, 4] is a chosen plaintext-ciphertext attack that makes use of difference propagation property of a cipher to deduce the key bits. The difference propagation property of an S-box is the relative amount of all input pairs that for the given input difference results in a specific output difference and it is expressed as propagation ratio [5]. Let $\boldsymbol{x}_{*_1}^r$ be any intermediate cipher state at round r resulting from the plaintext P_1. Similarly, let $\boldsymbol{x}_{*_2}^r$ be the corresponding intermediate cipher state resulting from P_2. The non zero symbols in $\boldsymbol{x}_{*_1}^r \oplus \boldsymbol{x}_{*_2}^r$ are called active S-boxes or active symbols. The pattern that specifies the positions of the active symbols is called the (difference) activity pattern. The propagation ratio over all the rounds of a differential trail can be approximated by the product of the propagation ratios of the active symbols in its activity pattern. Differential cryptanalysis is possible if the maximum possible propagation ratio is significantly larger than $2^{1-n_b^0}$.

Linear cryptanalysis [17] is a known plaintext-ciphertext attack that makes use of linearity in the cipher to obtain the key bits. The substitution is the only non-linear step in most of the block ciphers including the proposed HD cipher. The linearity of an active symbol can be approximated to the maximum input-output correlation exhibited by it. The active symbols in a round are determined by the non zero symbols in the selection vectors at the input of the round. The pattern that specifies the positions of active symbols is called (correlation) activity pattern. The linearity of one round can be extended to multiple rounds to form a linear trail. The correlation (measure of linearity) of a linear trail (multiple rounds) can be approximated to the product of input-output correlations of its active symbols. Linear cryptanalysis is possible if the maximum possible correlation of any linear trail is significantly larger than $2^{-n_b^0/2}$, where n_b^0 is the size of the plaintext in bits.

The number of active symbols in an activity pattern, $\boldsymbol{a}_*^r$, is called the *symbol weight*, denoted by $\mathrm{W_S}(\boldsymbol{a}_*^r)$. Let A_*^r be the matrix representation of $\boldsymbol{a}_*^r$. Then any column $\mathrm{A}_*^r(j)$ is said to be active if it contains at least one active symbol. The number of active columns in an activity pattern is called the *column weight*, denoted by $\mathrm{W_C}(\boldsymbol{a}_*^r)$. The difference and correlation activity patterns propagate through the transformations of different rounds of the cipher forming linear and differential trails. The number of active symbols in a trail is given by $\sum_{r=1}^{R}(\mathrm{W_S}(\boldsymbol{a}_\gamma^r))$. To defend a cipher against linear and differential cryptanalysis, the cipher design should ensure a large number of active symbols in any linear and difference trail. Hence, a lower bound on the number of active symbols in any linear or differential trail will give a lower bound on the resistance of the cipher to linear and differential cryptanalysis. In Theorem 4 we show that this lower bound for HD cipher is $\mathcal{B}(\theta^1) \times \mathcal{B}(\theta^2)$.

Lemma 1. *The total number of active columns of the function $\pi \circ \theta \circ \pi$ is lower bounded by the branch number of θ, $\mathcal{B}(\theta)$.*

This is true for any diffusion optimal π. Proof given in [7].

Theorem 3. *The number of active S-boxes or symbols for a two round trail of HD cipher is lower bounded by the branch number of the first round of HD code, $\mathcal{B}(\theta^1)$.*

Proof. Consider the first two rounds of HD cipher. Since γ and σ operate on the symbols locally, they do not affect the propagation pattern. Hence the number of active S-boxes or symbols for a two round trail, $\mathrm{W_S}(\boldsymbol{a}_\gamma^1)+\mathrm{W_S}(\boldsymbol{a}_\gamma^2)$, is bounded by the propagation property of θ^1. From the definition of HD codes and Equation 9 it follows that the sum of active S-boxes before and after θ^1 encoding of the first round is lower bounded by $\mathcal{B}(\theta^1)$.

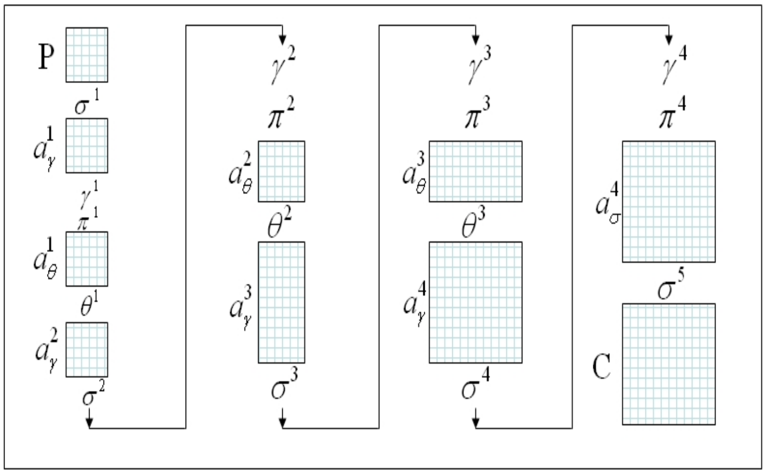

Fig. 2. Activity pattern propagation in four round HD cipher encryption.

Theorem 4. *The number of active S-boxes or symbols for a four round trail (starting with round* 1*) of HD cipher is lower bounded by $\mathcal{B}(\theta^1) \times \mathcal{B}(\theta^2)$.*

Proof. The sum of the number of active columns in $\boldsymbol{a}_\gamma^2$ and $\boldsymbol{a}_\theta^3$ is lower bounded by $\mathcal{B}(\theta^2)$ (from Lemma 1). Hence we have,

$$\mathrm{W_C}(\boldsymbol{a}_\gamma^2) + \mathrm{W_C}(\boldsymbol{a}_\theta^3) \geq \mathcal{B}(\theta^2) \tag{11}$$

but, $\mathrm{W_C}(\boldsymbol{a}_\gamma^4) = \mathrm{W_C}(\boldsymbol{a}_\theta^3)$ (θ does not change the number of active columns). Therefore,

$$\mathrm{W_C}(\boldsymbol{a}_\gamma^2) + \mathrm{W_C}(\boldsymbol{a}_\gamma^4) \geq \mathcal{B}(\theta^2) \tag{12}$$

The total number of active S-boxes in $\boldsymbol{a}_\theta^1$ and $\boldsymbol{a}_\gamma^2$ is given by,

$$\mathrm{W_S}(\boldsymbol{a}_\theta^1) + \mathrm{W_S}(\boldsymbol{a}_\gamma^2) \geq \mathrm{W_C}(\boldsymbol{a}_\gamma^2)\mathcal{B}(\theta^1) \tag{13}$$

Similarly, the total number of active S-boxes in $\boldsymbol{a}_\theta^3$ and $\boldsymbol{a}_\gamma^4$ is given by,

$$\mathrm{W_S}(\boldsymbol{a}_\theta^3) + \mathrm{W_S}(\boldsymbol{a}_\gamma^4) \geq \mathrm{W_C}(\boldsymbol{a}_\gamma^4)\mathcal{B}(\theta^3) \tag{14}$$

Combining 12 13 and 14 will give,

$$\begin{aligned}\mathrm{W_S}(\boldsymbol{a}_\theta^1) \ + \ \mathrm{W_S}(\boldsymbol{a}_\gamma^2) \ + \ \mathrm{W_S}(\boldsymbol{a}_\theta^3) \ + \ \mathrm{W_S}(\boldsymbol{a}_\gamma^4) \\ \geq \mathrm{W_C}(\boldsymbol{a}_\gamma^2)\mathcal{B}(\theta^1) \ + \ \mathrm{W_C}(\boldsymbol{a}_\gamma^4)\mathcal{B}(\theta^3) \\ \geq (\mathrm{W_C}(\boldsymbol{a}_\gamma^2) + \mathrm{W_C}(\boldsymbol{a}_\gamma^4))\mathcal{B}(\theta^1) \ + \\ \mathrm{W_C}(\boldsymbol{a}_\gamma^4)(d_{min}^2 + d_{min}^3 - 2)\end{aligned}$$

Since, $\mathrm{W_C}(\boldsymbol{a}_\gamma^4)(d_{min}^2 + d_{min}^3 - 2)$ is non negative ($d_{min}^2, d_{min}^3 \geq 1$) and $\mathrm{W_S}(\boldsymbol{a}_\theta^j) = \mathrm{W_S}(\boldsymbol{a}_\gamma^j)$ we get,

$$\mathrm{W_S}(\boldsymbol{a}_\gamma^1) + \mathrm{W_S}(\boldsymbol{a}_\gamma^2) + \mathrm{W_S}(\boldsymbol{a}_\gamma^3) + \mathrm{W_S}(\boldsymbol{a}_\gamma^4) \geq \mathcal{B}(\theta^1)\mathcal{B}(\theta^2) \tag{15}$$

The security of HD cipher against linear and differential cryptanalysis thus depends on the branch number of the HD coding operation at the diffusion layer.

Consider the Rijndael cipher and the HD cipher operating on the plaintext block length. Then, the design of HD cipher guarantees that the number of active S-boxes in any four round linear or differential trail of HD cipher is lower bounded by the number of active S-boxes in any four round linear or differential trail of Rijndael cipher. Also, the S-boxes used in the HD cipher are the same as the S-boxes used in the Rijndael cipher. Hence, we can conclude that HD cipher is as secure as the Rijndael with respect to linear and differential cryptanalysis. This also shows that, the error correction property of the HD code does not lead to information leakage or weakness in security with respect to linear and differential cryptanalysis. However, the HD ciphers use a larger key length ($n_k = n_b^R \geq n_b^0$) to achieve the same security level as that of Rijndael. The resistance to linear and differential cryptanalysis also shows that, the HD ciphers are not vulnerable to known plaintext type of attacks described in [2].

3.2 Square Attack

The square attack [6] (also known as Integral attack or the Saturation attack) makes use of the byte oriented nature of the Square block cipher which was the predecessor of Rijndael. As Rijndael is also a byte oriented cipher, this attack has been extended to reduced versions of Rijndael cipher [15, 11]. Although the attacks described applies directly to ciphers operating with symbol size in bytes, it can be easily extended to other symbol sizes. HD ciphers also comprise of symbol oriented operations which are loosely based on Rijndael, hence HD ciphers with fewer than seven rounds would be as weak as reduced versions of the Rijndael cipher.

4 Error Correction Capacity of HD ciphers

In this section, we prove bounds on the error correction capacity of HD ciphers. After encryption the ciphertext of length n_s^R symbols (equivalently n_b^R bits) is transmitted across a noisy channel. Specifically, we consider a bursty channel and use the term "full weight burst error" to denote an error burst where all the symbols in the burst are in error. In order to formalize our analysis we introduce the following assumptions, definitions and notations. Without loss of generality we consider HD ciphers in which HD codes have equal error correcting capacity in all rounds. That is, $t^r = t;\ \forall r \in \{1, .., R-1\}$. A symbol of the cipher state that is in error (due to channel or propagation due to decryption) is referred to as an *error symbol*. An *error pattern* is a vector whose non zero symbols represent the error symbols. The error patterns for each round are denoted by, $\boldsymbol{e}_*^r,\ \forall r \in \{1, ..., R\}$. In the matrix representation of the error pattern (denoted by E_*^r), a column (or row) in the error pattern is said to be in error if there are at least $t+1$ error symbols in the corresponding column (or row). We refer to such columns and rows as *error column* and *error row* respectively. We say that error correction is *complete* in round r if $\boldsymbol{e}_*^r$ is a zero vector, otherwise error correction is said to be *incomplete*. Error correction capacity of a four round HD cipher decryption is analysed in Theorem 5. An outline of a four round HD cipher decryption is represented in the Fig. 3.

Lemma 2. *For a four round HD cipher, if there are at most t error columns or rows in the ciphertext before decryption, the error correction will be complete after at most three rounds of decryption. Here, t denotes the error correction capacity of HD codes used in the HD cipher.*

Proof. Consider the first three rounds of HD cipher decryption in Fig. 3. Since the inverse non-linear transform γ and round key addition σ operations do not convert an error symbol to an error free symbol and vice versa, it can be excluded from the analysis.

First, we consider the case in which the error pattern $\boldsymbol{e}_\sigma^4$ contains at most t error columns. After π^4 transformation, we will have at most t error rows in $\boldsymbol{e}_\pi^4$. Since, ψ^3 has an error correcting power of t, errors across each of the columns

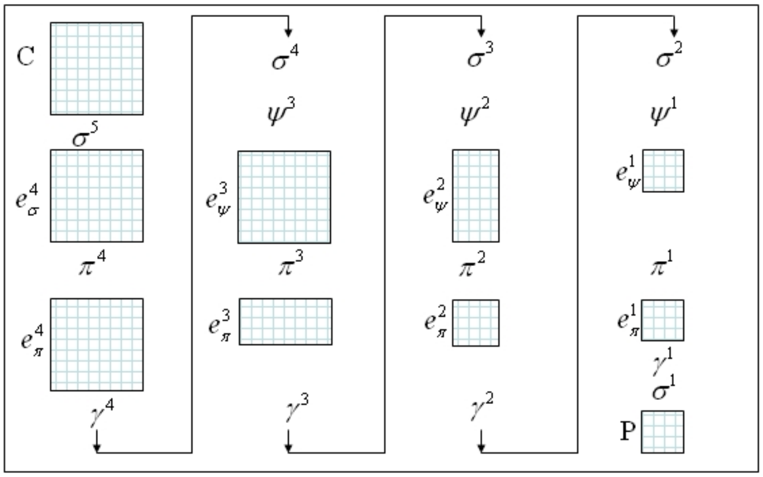

Fig. 3. Error pattern propagation in four round HD cipher decryption.

are corrected. Hence, the error pattern $\boldsymbol{e}_\psi^3$ will contain all zeros, completing the error correction.

Consider the second case, in which the error pattern $\boldsymbol{e}_\sigma^4$ contains at most t error rows. After π^4 transformation, we have at most t error columns in $\boldsymbol{e}_\pi^4$. This is beyond the error correction capacity of ψ^3, hence we take the worst case scenario of having at most t error columns in $\boldsymbol{e}_\psi^3$. Now, applying the same argument as the first case, the error pattern $\boldsymbol{e}_\psi^2$ should have all zeros.

Lemma 3. *For a four round HD cipher, if there are at least $t+1$ error columns or rows in the ciphertext before decryption, the error correction will remain incomplete after three rounds of decryption.*

Proof. Consider the case in which the error pattern $\boldsymbol{e}_\sigma^4$ contains $t+1$ error columns. After π^4 transformation, $\boldsymbol{e}_\pi^4$ will contain at least $t+1$ error rows. This is beyond the error correction capacity of ψ^3. Hence $\boldsymbol{e}_\psi^3$ will have all of its symbols in error and the decryption will remain incomplete even after ψ^2 in $\boldsymbol{e}_\psi^2$. Similarly, when there are $t+1$ error rows in $\boldsymbol{e}_\sigma^4$, there will be $t+1$ error columns in $\boldsymbol{e}_\psi^3$ and every symbol will be in error in $\boldsymbol{e}_\psi^2$. Hence the decryption will remain incomplete.

We now analyze the maximum full weight burst error length that is guaranteed to be corrected by a four round HD cipher. Our analysis is independent of the starting and ending locations of the burst with respect to the cipher state.

Theorem 5. *The full weight burst error correcting capacity of a four round HD cipher is $(t-1)(\mathcal{B}(\theta^3)-1)+2t+1$.*

Proof. Without loss of generality we consider the row-wise transmission (with respect to matrix representation) of the ciphertext and hence full weight bursts that occur across the rows of the ciphertext. The following analysis can be trivially extended to column-wise transmission as well.

We know that a burst of $t+1$ errors in one row makes that an error row. The minimum full weight burst error length required to create two error rows is $2(t+1)$. Similarly, a full weight burst error of length $n^3_{u'}+2(t+1)$ can cause three error rows. Generalizing this result, we get that, a burst length of $(l-2)(n^3_{u'})+2(t+1)$ can cause l error rows. This is in fact the minimum length for a full weight error burst to cause l error rows. It follows that a full weight burst length of at least $(t-1)(n^3_{u'})+2(t+1)$ is required to generate $l=t+1$ error rows. This implies that a full weight burst of length $(t-1)(n^3_{u'})+2(t+1)-1$ cannot generate $l \geq t+1$ error rows. From Lemma 2 a burst of length $(t-1)(n^3_{u'})+2(t+1)-1$ is correctable and from Lemma 3 a burst of length $(t-1)(n^3_{u'})+2(t+1)$ is not correctable. Hence the minimum burst length that is guaranteed to be corrected by a 4 round HD cipher decryption is $(t-1)(n^3_{u'})+2(t+1)-1$. Which is equal to $(t-1)(\mathcal{B}(\theta^3)-1)+2t+1$ (from 8).

Although this gives the error correction capacity of the system, in some cases the system can correct longer burst errors. In other words, some longer bursts can be corrected, depending on their start and end positions. Theorem 6 gives the smallest burst length for which the probability of complete error correction in a four round HD cipher decryption is zero. Any full weight error burst that is smaller than this has some non zero probability of being correctable.

Theorem 6. *The smallest burst length of a full weight burst error, for which the probability of complete decoding is zero (by a four round HD cipher) is* $t(\mathcal{B}(\theta^3)+1)+1$ *symbols.*

Proof. We again assume row-wise transmission of the ciphertext and hence full weight burst errors occurring across rows. The maximum number of error rows for which error correction will be complete in three rounds is t (Lemma 2). The minimum length of a full weight burst that makes a row in error is $t+1$, hence the maximum full weight burst length that can occur in an error free row is t. Therefore, the maximum full weight burst length that produces a error pattern with at most t error rows is $tn^3_{u'}+2t$. This is equal to $t(\mathcal{B}(\theta^3)+1)$. Hence a burst length of $t(\mathcal{B}(\theta^3)+1)+1$ is the smallest burst length of a full weight burst, for which the probability of complete decoding is zero.

5 Simulation Results

To assess the performance of our proposed cipher, we compare it with a conventional, concatenated system that uses Rijndael for encryption and Reed-Solomon codes for error correction. As a proof of concept, we construct a four round HD cipher in the Gallois Field of order 8 (GF(2^3)) and compare it against a system that uses the Rijndael in GF(2^3) concatenated with three RS codes, A, B and C with parameters $[7,3,8]$, $[15,3,16]$, $[31,3,32]$ respectively. We use three different RS codes, because there is no RS code with parameters that match

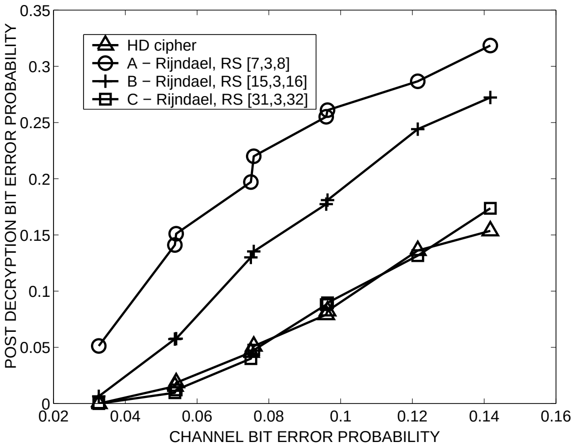

Fig. 4. Comparison of error resilience of HD cipher and Rijndael concatenated with Reed Solomon codes.

the HD cipher performance exactly in terms of error correction. The selection here compares two systems which cause smaller data expansion (A and B) and one that causes more data expansion (C) compared to the HD cipher. Let us refer to the concatenated system produced by using RS code A, as "System A", and that produced by using RS code B and C, as "System B" and "System C" respectively. The HD cipher produces 147 bits of cipher text for every 27 bits of plaintext; System A, System B and System C produce 63, 135 and 279 bits of ciphertext for every 27 bits of plaintext respectively.

The parameters of the High Diffusion cipher in GF(2^3) is as follows: $n_b^0 = 27$ bits, $m = 3$, $R = 4$, HD code used for $\theta^1 = [3, 3, 2^3]$, $\theta^2 = \theta^3 = [7, 3, 2^3]$ (generated using RS code A) and $n_b^4 = 147$ bits. The parameters for Rijndael cipher in GF(2^3) are as follows: $n_b^0 = n_b^4 = 27$ bits, MixColumn transformation uses an invertible 3×3 matrix in GF(2^3) with branch number 4.

The sum of active S-boxes for a four round trail of HD cipher is $\mathcal{B}(\theta^1) \times \mathcal{B}(\theta^2) = 32$. The sum of active S-boxes for a four round trail of the Rijndael cipher is 16. The resistance to linear and differential cryptanalysis is lower bounded by the product of correlation and propagation ratio of the active S-boxes (see Section 3.1). This implies that *HD cipher is exponentially twice as resistant to linear and differential cryptanalysis as the Rijndael cipher*. However, HD cipher uses 147 bit key length to attain a security comparable to the 27 bit Rijndael cipher.

To simulate the bursty nature of wireless channel environment, we used the Gilbert-Elliott channel model with the following parameters [19], the transition probability from bad state to good state, $g = 0.1092$, the transition probability from good state to bad state, $b = 0.0308$, bit error probability in the bad state, $p_b = 0.5$ and bit error probability in the good state $p_g = 0.0128$. Fig. 4 plots the post decryption bit error rate of the proposed HD cipher and the concatenated

Systems A, B and C against the channel bit error rate. It can be observed that the HD cipher performs significantly better than system A, B and matches the performance of System C. We can see that in order to match the HD cipher in terms of error correction performance, the conventional system will increase the data expansion by 89% when compared to the expansion in HD cipher.

We now compare HD cipher and Rijndael in terms of computational complexity. In Rijndael, the cipher state is multiplied with the MixColumn transformation matrix in every round. Whereas, in HD cipher encryption, the cipher state is multiplied with the generator matrix of HD code in every round. A large generator matrix will incur higher computational costs. The size of MixColumn used in our experiment is 3×3, whereas the size of generator matrix for HD code is 3×7. In HD cipher decryption, RS decoding algorithm is used, which requires higher computational complexity compared to the inverse MixColumn matrix multiplication. Since, the design of HD cipher is still in a theoretical stage, we have not done extensive analysis on its computational complexity.

6 Conclusions

Several motivating factors for the design of error correcting ciphers were discussed. The High Diffusion cipher, which combines a block cipher with a block error correcting code was proposed. A new class of Maximum Distance Separable (MDS) codes called High Diffusion codes were introduced. These codes were shown to achieve optimal diffusion and error resilience. Some techniques to construct HD codes were presented. The security of the four round HD cipher against linear and differential cryptanalysis was shown to be lower bounded by $\mathcal{B}(\theta^1)\mathcal{B}(\theta^2)$, where $\mathcal{B}(\cdot)$ is the branch number and θ^r is the r^{th} round HD coding operation. We proved that the full weight burst error correction capacity of a four round HD cipher is $(t-1)(\mathcal{B}(\theta^3)-1)+2t+1$ symbols. Simulation results of a four round HD cipher operating in GF(2^3) revealed that (a) HD cipher is as secure as Rijndael cipher with respect to linear and differential cryptanalysis (b) conventional, concatenated systems that independently perform encryption (using Rijndael) and error correction (using Reed Solomon codes) need to increase the data expansion by 89% to match the performance of HD cipher.

References

1. Berlekamp, E. R.: 1968, *Algorithmic Coding Theory*, Chapt. Ch. 7. New York: McGraw-Hill.
2. Berson, T. A.: 1997, ‘Failure of the McEliece public-key cryptosystem under message-resend and related-message attack’. In: *Advances in Cryptology-CRYPTO ’97, Lecture notes in computer science.*
3. Biham, E. and A. Shamir: 1991, ‘Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer (Extended Abstract)’. *Lecture Notes in Computer Science* **576**, 156.

4. Biham, E. and A. Shamir: 1993, 'Differential Cryptanalysis of the Full 16-Round DES'. In: *CRYPTO '92: Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology*. London, UK, pp. 487–496.
5. Daemen, J.: 1995, 'Cipher and hash function design strategies based on linear and differential cryptanalysis'. Ph.D. thesis, K.U.Leuven.
6. Daemen, J., L. R. Knudsen, and V. Rijmen: 1997, 'The Block Cipher Square'. In: *FSE '97: Proceedings of the 4th International Workshop on Fast Software Encryption*. London, UK, pp. 149–165.
7. Daemen, J. and V. Rijmen: 2001, 'The Wide Trail Design Strategy'. In: *Proceedings of the 8th IMA International Conference on Cryptography and Coding*. London, UK, pp. 222–238.
8. Daemen, J. and V. Rijmen: 2002, *The Design of Rijndael*. Secaucus, NJ, USA: Springer-Verlag New York, Inc.
9. Feistel, H.: 1973, 'Cryptography and Computer Privacy'. **228**(5), 15–23.
10. FIPS: 2001, 'Specification for the Advanced Encryption Standard (AES)'. Federal Information Processing Standards Publication 197.
11. Gilbert, H. and M. Minier: 2000, 'A Collision Attack on 7 Rounds of Rijndael.'. In: *AES Candidate Conference*. pp. 230–241.
12. Godoy, W. and D. Periera: 1997, 'A proposal of a cryptography algorithm with techniques of error correction'. *Computer Communications* **20**(15), 1374–1380.
13. Hwang, T. and T. Rao: 1988, 'Secret Error-Correcting Codes (SECC)'. In: *Advances in Cryptography - Crypto 1988*.
14. Kundsen, L. and D. Wagner: 2002, 'Integral Cryptanalysis'. *Lecture Notes in Computer Science* **2365**, 112.
15. Lucks, S.: 2000, 'Attacking Seven Rounds of Rijndael under 192-bit and 256-bit Keys.'. In: *AES Candidate Conference*. pp. 215–229.
16. Mathur, C. N., K. Narayan, and K. Subbalakshmi: 2005, 'High Diffusion Codes: A Class of Maximum Distance Separable Codes for Error Resilient Block Ciphers'. *2nd IEEE International Workshop on Adaptive Wireless Networks (AWiN), Globecom*.
17. Matsui, M.: 1993, 'Linear cryptanalysis method for DES cipher'. In: *Advances in cryptology -EUROCRYPT93, Lecture Notes in Computer Science*, Vol. 765. pp. 1–11.
18. McEliece, R.: 1978, 'A Publick Key Cryptosystem Based on Algebraic Codes'. *DNS Progress Reports 42-44, NASA Jet Propulsion Labaratory*.
19. Mushkin, M. and I. Bar-David, 'Capacity and coding for the Gilbert-Elliot channels'. *Information Theory, IEEE Transactions on* **35**, 1277–1290.
20. Nanjunda, C., M. Haleem, and R. Chandramouli: 2005, 'Robust Encryption for Secure Image Transmission over Wireless Channels'. In: *ICC' 2005, IEEE International Conference on Communications, May 16-20, 2005 - Seoul, Korea*.
21. Narayan, K.: 2005, 'On the Design of Secure Error Resilient Diffusion Layers for Block Ciphers'. Master's thesis, Steven Institute Of Technology, Hoboken, New Jersey.
22. Nyberg, K.: 1994, 'Differentially uniform mappings for cryptography'. In: *EUROCRYPT '93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology*. Secaucus, NJ, USA, pp. 55–64.
23. Stinson, D.: 2002, *Cryptography: Theory and Practice,Second Edition*. CRC/C&H.
24. van Tilborg, H.: 1998, 'Coding theory at work in cryptology and vice versa'.
25. Wicker, S. B.: 1995, *Error control systems for digital communication and storage*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc.