Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2006, Article ID 42871, Pages 1–12
DOI 10.1155/WCN/2006/42871

On the Design of Error-Correcting Ciphers

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

Media Security, Networking and Communications Laboratory , Department of Electrical and Computer Engineering (ECE), Stevens Institute of Technology, Burchard 208, Hoboken, NJ 07030, USA

Received 2 October 2005; Revised 20 November 2006; Accepted 20 November 2006

Securing transmission over a wireless network is especially challenging, not only because of the inherently insecure nature of the medium, but also because of the highly error-prone nature of the wireless environment. In this paper, we take a joint encryption-error correction approach to ensure secure and robust communication over the wireless link. In particular, we design an *error-correcting cipher* (called the high diffusion cipher) and prove bounds on its error-correcting capacity as well as its security. Towards this end, we propose a *new class of error-correcting codes (HD-codes) with built-in security features* that we use in the diffusion layer of the proposed cipher. We construct an example, 128-bit cipher using the HD-codes, and compare it experimentally with two traditional concatenated systems: (a) AES (Rijndael) followed by Reed-Solomon codes, (b) Rijndael followed by convolutional codes. We show that the HD-cipher is as resistant to linear and differential cryptanalysis as the Rijndael. We also show that any chosen plaintext attack that can be performed on the HD cipher can be transformed into a chosen plaintext attack on the Rijndael cipher. In terms of error correction capacity, the traditional systems using Reed-Solomon codes are comparable to the proposed joint error-correcting cipher and those that use convolutional codes require 10% more data expansion in order to achieve similar error correction as the HD-cipher. The original contributions of this work are (1) design of a new *joint error-correction-encryption* system, (2) design of a *new class of algebraic codes with built-in security criteria*, called the high diffusion codes (HD-codes) for use in the HD-cipher, (3) mathematical properties of these codes, (4) methods for construction of the codes, (5) bounds on the error-correcting capacity of the HD-cipher, (6) mathematical derivation of the bound on resistance of HD cipher to linear and differential cryptanalysis, (7) experimental comparison of the HD-cipher with the traditional systems.

Copyright © 2006 Chetan Nanjunda Mathur et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. INTRODUCTION

The wireless communication medium, as opposed to the wired counterparts, is noisy and open to intruders. Hence, additional level of error protection and security is required to make the wireless network as reliable and secure as the wired network. The issue of using cryptographically secure ciphers [1] in noisy channel environments (like the wireless networks) is that the very same properties (avalanche effect) that gives ciphers their cryptographic strength makes them sensitive to channel errors [2]. 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 retransmissions thus reducing the overall throughput.

To improve the throughput in noisy environments, channel coding is performed after encryption. Unfortunately, performing both encryption and coding separately can potentially prove to be too computationally intensive for many wireless end devices (e.g., personal data assistants (PDA), mobile phones). In fact, as both encryption and coding can be performed at the link layer, a single operation which does both encryption and error correction would be preferable.

Although many mathematical relationships exist between error correction and cryptography [3–5], there have been only a few attempts to build error-correcting ciphers. Some of the notable results include the McEliece cipher [6], the Hwang and Rao cipher [7], and the Godoy-Pereira scheme [8]. Some of the issues with these ciphers are (a) these systems were not designed based on well-known security principles (and hence are vulnerable to various attacks [9]), (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 higher computational complexity. The difficulty in designing error-correcting ciphers arise from the fact that error correction and encryption work at cross purposes with each other. For example, the avalanche

effect, which is desirable for security, causes too much error expansion thereby undermining the goal of an error-correcting code.

In this paper, we propose an error-correcting block cipher called the high diffusion (HD) cipher. The HD cipher, like standard block ciphers [10], is composed of several iterations of the round function and mixing with the secret key. A round function is composed of a nonlinear 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 called high diffusion codes that we propose in this paper. We show that these codes possess maximum diffusion strength and at the same time achieve optimal error correction. It can be shown that a subclass of popular error-correcting codes can be transformed into HD codes by appropriate message transformations. Specifically, we have shown that it is possible to convert RS codes to HD codes using some easy-to-implement message transformations (see Section 2.3).

We prove that the HD ciphers are as secure as the Rijndael cipher (used in advanced encryption standard [11]) against the well-known differential and linear cryptanalysis. To assess the performance of our proposed cipher, we compare it with two traditional concatenated systems. One that uses the Rijndael cipher [12] followed by Reed Solomon codes [13], and the other that uses the Rijndael followed by convolutional codes. Simulation results show that error correction capacity of traditional concatenated systems that use Reed Solomon codes are comparable to that of the proposed HD cipher and those that use convolutional codes require 10% more expansion to match the performance of HD cipher. The main contributions of this work are (1) design of a new *joint error-correction-encryption* system, (2) design of a *new class of algebraic codes with built-in security criteria*, (3) a study of mathematical properties of these codes, (4) methods for construction of the codes, (5) bounds on the error-correcting capacity of the HD-cipher, (6) mathematical derivation of the bound on resistance of HD cipher to linear and differential cryptanalysis, (7) experimental comparison of the HD-cipher with the traditional system.

The rest of the paper is organized as follows. In Section 2, we propose a new class of algebraic codes, the high diffusion codes. This is followed by our proposed error-correction cipher, the high diffusion cipher in Section 3. Security analysis of HD cipher against well-known cryptanalytic attacks is performed in Section 4. In Section 5, we prove theoretical bounds on the burst error-correction capacity of HD cipher. Simulation results are presented in Section 6 followed by conclusion in Section 7.

2. PROPOSED HIGH DIFFUSION CODES

Since the goal is to design a joint error-correction-encryption code that does not sacrifice error resilience or security, we derive two criteria that these codes must satisfy as follows.

(i) *Security criterion*: since the new code will be used as a diffusion layer, it needs to spread the statistical properties of the input block to a large section of the output block. The spreading power, diffusion, is measured using the concept of *branch number*. The differential branch number of a function ϕ, with an input vector $\vec{x}$ and the output vector $\phi(\vec{x})$ is defined as

$$\mathcal{B}(\phi) = \min\left(H_d(\vec{x_i}, \vec{x_j}) + H_d(\phi(\vec{x_i}), \phi(\vec{x_j}))\right), \quad (1)$$

where, $i \neq j$, $i, j \in \{1, \ldots, 2^{|\vec{x}|}\}$, and H_d is the symbol Hamming distance. To provide good security the HD codes must have maximum branch number.

(ii) *Error resilience criterion*: the number of errors that can be corrected by a code is governed by the pairwise minimum distance between the codewords [13]. A large minimum distance would ensure good error-resilience property.

2.1. Definition of HD codes

Let us consider an $[n, k, q]$ block code, defined on the Galois field (GF) of order q; where n refers to the number of output symbols and k refers to the number of input symbols. The HD codes are defined as follows.

Definition 1. An $[n, k, q, b]$ code $\mathcal{C}$ is said to be a high diffusion (HD) code with the encoding operation, θ, and branch number b, if it satisfies the following inequality for all $i, j \in \{1, 2, \ldots, (q^k - 1)\}$ and $i \neq j$:

$$b = \mathcal{B}(\theta) \triangleq \min\left(H_d(\mathbf{m}_i, \mathbf{m}_j) + H_d(\mathbf{c}_i, \mathbf{c}_j)\right) \geq n + 1, \quad (2)$$

where $c_i = \theta(m_i)$.

That is, the branch number of θ is lower bounded by $n+1$, since the maximum output difference corresponding to a single nonzero symbol input difference is n. The upper bound for branch number is $n+1$. Hence, the branch number of HD codes should be exactly equal to $n + 1$.

2.2. Properties of HD codes

In this section, we show that the HD codes possess the maximum possible diffusion and error correction capacity as desired in the design criteria.

2.2.1. Optimality in diffusion

By definition, HD code has a branch number of $n+1$. For any Boolean transformation with n-tuples as its output the maximum branch number possible is $n+1$ [14]. As the HD coding operation θ is a Boolean transformation from k-tuples to n-tuples with the lower bound on the branch being $n + 1$, they achieve optimal diffusion.

2.2.2. Optimality in error correction

We prove that HD codes are maximum distance separable codes (MDS) [15], and hence show that they are optimal in terms of the minimum distance of the code.

Theorem 1. *An $[n, k, q]$ HD code $\mathbf{C}$ with encoding operation θ is an MDS code with $d_{\min} = n - k + 1$.*

Proof. Consider two codewords $\mathbf{c}_i$ and $\mathbf{c}_j$ and $\mathbf{m}_i$ and $\mathbf{m}_j$ be the corresponding messages. By the definition of HD codes (Definition 1), we have

$$\begin{aligned} H_d(\vec{\mathbf{c}}_i, \vec{\mathbf{c}}_j) + H_d(\vec{\mathbf{m}}_i, \vec{\mathbf{m}}_j) &= \mathcal{B}(\theta), \\ H_d(\vec{\mathbf{c}}_i, \vec{\mathbf{c}}_j) + H_d(\vec{\mathbf{m}}_i, \vec{\mathbf{m}}_j) &= n+1, \\ H_d(\vec{\mathbf{c}}_i, \vec{\mathbf{c}}_j) &= n - H_d(\vec{\mathbf{m}}_i, \vec{\mathbf{m}}_j) + 1. \end{aligned} \tag{3}$$

Since the messages are from a k-dimensional space and minimum $H_d(\vec{\mathbf{c}}_i, \vec{\mathbf{c}}_j)$ is achieved when $H_d(\vec{\mathbf{m}}_i, \vec{\mathbf{m}}_j)$ is maximum, we have

$$\begin{aligned} \max_{i,i\neq j} \left(H_d(\vec{\mathbf{m}}_i, \vec{\mathbf{m}}_j)\right) &= k, \\ \therefore\ d_{\min} &= n - k + 1. \end{aligned} \tag{4}$$

From (4) we see that HD codes satisfy the Singleton bound [15] with equality, which implies that HD codes are in fact MDS codes. □

The bound on error-correction capacity, t, of HD codes is derived from the minimum distance between codewords as follows:

$$\begin{aligned} t &= \left\lfloor \frac{d_{\min}}{2} \right\rfloor, \\ \therefore\ t &= \left\lfloor \frac{n-k+1}{2} \right\rfloor. \end{aligned} \tag{5}$$

2.2.3. Bound on n given q

One of the necessary conditions for the existence of an $[n, k, q]$ HD code is $n < q$ (Theorem 2).

Lemma 1. *For any $q > 1$, $q^x \geq q+1$ when $x > 1$. Therefore, for $n > k > 1$ the number of messages and the number of codewords is greater than the number of symbols.*

Lemma 2. *The first q messages can always be assigned codewords that satisfy HD code property in an $[n, k, q, b]$ HD code.*

Proof. A trivial HD code assignment for the first q messages is the $[n, 1, q]$ repetition code assignment. □

Theorem 2. *For a given $[n, k, q, b]$ HD code, $n \leq q - 1$.*

Proof. To prove $n \leq q-1$ for an $[n, k, q, b]$ HD code we show that, for $n > q - 1$, branch number of $b \geq n + 1$ cannot be satisfied with respect to all messages.

To prove this we assume the following, without loss of generality.

(i) For all high diffusion codes the all-zero message $\overrightarrow{\mathbf{m}_0}$ is mapped to the all-zero codeword $\vec{\mathbf{c}}_0$.

(ii) The first q messages can be assigned codewords that satisfy branch number property (see Lemmas 1 and 2),

$$\begin{array}{ccccccccccc} \overrightarrow{\mathbf{m}_0} & \longleftrightarrow & \vec{\mathbf{c}}_o & = & \{ & 0 & 0 & \cdots & 0 & \} \\ \overrightarrow{\mathbf{m}_1} & \longleftrightarrow & \vec{\mathbf{c}}_1 & = & \{ & \mathbf{c}_{1,1} & \mathbf{c}_{1,2} & \cdots & \mathbf{c}_{0,n} & \} \\ \overrightarrow{\mathbf{m}_2} & \longleftrightarrow & \vec{\mathbf{c}}_2 & = & \{ & \mathbf{c}_{2,1} & \mathbf{c}_{2,2} & \cdots & \mathbf{c}_{0,n} & \} \\ \overrightarrow{\mathbf{m}_3} & \longleftrightarrow & \vec{\mathbf{c}}_3 & = & \{ & \mathbf{c}_{3,1} & \mathbf{c}_{3,2} & \cdots & \mathbf{c}_{3,n} & \} \\ \vdots & \longleftrightarrow & \vdots & = & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \overrightarrow{\mathbf{m}_{(q-1)}} & \longleftrightarrow & \overrightarrow{\mathbf{c}_{(q-1)}} & = & \{ & \mathbf{c}_{(q-1),1} & \mathbf{c}_{(q-1),2} & \cdots & \mathbf{c}_{(q-1),n} & \} \\ \overrightarrow{\mathbf{m}_q} & \longleftrightarrow & \vec{\mathbf{c}}_q & = & \{ & \mathbf{c}_{q,1} & \mathbf{c}_{q,2} & \cdots & \mathbf{c}_{q,n} & \} \\ \vdots & \longleftrightarrow & \vdots & = & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array} \tag{6}$$

Consider the codeword assignment above, where the $(q-1)$ messages form $\vec{\mathbf{m}}_1$ to $\vec{\mathbf{m}}_{(q-1)}$ are of weight one, that is, $\vec{\mathbf{m}}_i = 0 \star (k-1)\|q_i\|$, where $i \in \{1, 2, \ldots, q-1\}$. The message $\vec{\mathbf{m}}_q = 0 \star (k-2)\|1\|0$ is also a weight one message, but has a distance of two form messages $\vec{\mathbf{m}}_1$ to $\vec{\mathbf{m}}_{q-1}$, that is, $H_d(\vec{\mathbf{m}}_i, \vec{\mathbf{m}}_q) = 2$ for all $i \in \{1, 2, \ldots, q-1\}$.

Messages $\overrightarrow{\mathbf{m}_1}$ through $\vec{\mathbf{m}}_{(q-1)}$ are at a distance of one form $\overrightarrow{\mathbf{m}_0}$, therefore to achieve a branch number of $b = n + 1$ the codewords corresponding to these messages should be of weight n. That is,

$$H_d(\vec{\mathbf{c}}_i, \vec{\mathbf{c}}_0) = n \quad \forall i \in \{1, 2, \ldots, q\}. \tag{7}$$

Now for all $i, j \in \{1, 2, \ldots, q-1\}$ and $i \neq j$, the difference between messages is

$$H_d(\vec{\mathbf{m}}_i, \vec{\mathbf{m}}_j) = 1. \tag{8}$$

Therefore, the differences between the codewords corresponding to these messages must be n, that is,

$$H_d(\vec{\mathbf{c}}_i, \vec{\mathbf{c}}_j) = n. \tag{9}$$

Now let us consider the code assignment for the first $q-1$ messages as a separate matrix shown as follows:

$$\mathbf{V} = \begin{pmatrix} \mathbf{c}_{1,1} & \mathbf{c}_{1,2} & \mathbf{c}_{1,3} & \cdots & \mathbf{c}_{1,n} \\ \mathbf{c}_{2,1} & \mathbf{c}_{2,2} & \mathbf{c}_{2,2} & \cdots & \mathbf{c}_{2,n} \\ \mathbf{c}_{3,1} & \mathbf{c}_{3,2} & \mathbf{c}_{3,2} & \cdots & \mathbf{c}_{3,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \mathbf{c}_{(q-1),1} & \mathbf{c}_{(q-1),2} & \mathbf{c}_{(q-1),3} & \ldots & \mathbf{c}_{(q-1),n} \end{pmatrix}. \tag{10}$$

Let $\mathbf{V}(\alpha)$ be the αth column vector of the matrix $\mathbf{V}$, that is,

$$\mathbf{V}(\alpha) = \{\mathbf{c}_{1,\alpha}, \mathbf{c}_{2,\alpha}, \mathbf{c}_{3,\alpha}, \ldots, \mathbf{c}_{(q-1),\alpha}\} \quad \forall \alpha \in \{1, 2, 3, \ldots, n\}. \tag{11}$$

We see that $\mathbf{V}_{i,\alpha} \neq \mathbf{V}_{j,\alpha}$ for all $\alpha \in \{1, 2, 3, \ldots, n\}$ and for all $i \neq j$, $i, j \in \{1, 2, 3, \ldots, q-1\}$. That is, all the entries in each of the columns of $\mathbf{V}$ are unique. If this is not the case, (8) cannot be satisfied.

Now try to assign a codeword to the qth message. As the difference between $\vec{\mathbf{m}}_q$ and $\vec{\mathbf{m}}_0$ is one, the weight of the assigned codeword $\vec{\mathbf{c}}_q$ should be n, that is,

$$\begin{aligned} H_d(\vec{\mathbf{m}}_q, \vec{\mathbf{m}}_0) &= 1, \\ \therefore\ H_d(\vec{\mathbf{c}}_q, \vec{\mathbf{c}}_0) &= n. \end{aligned} \tag{12}$$

This implies $\vec{\mathbf{c}}_q$ cannot have "0" as one its components.

Comparing $\vec{\mathbf{m}}_q$ with the messages $\vec{\mathbf{m}}_i$ for all $i \in \{1, 2 \ldots, q-1\}$, we have

$$\begin{aligned} H_d(\vec{\mathbf{m}}_q, \vec{\mathbf{m}}_i) &= 2, \\ H_d(\vec{\mathbf{c}}_q, \vec{\mathbf{c}}_i) &= n-1. \end{aligned} \tag{13}$$

In other words, to achieve a branch number $b = n+1$, $\vec{\mathbf{c}}_q$ needs to have a distance of at least $n-1$ with respect to $\vec{\mathbf{c}}_i$ for all $i \in \{1, 2 \ldots, q-1\}$.

We now try to assign a codeword $\vec{\mathbf{c}}_q$ to $\vec{\mathbf{m}}_q$ that satisfies these conditions. From (8) and (9), we note that

$$\mathbf{c}_{q,\alpha} = \mathbf{V}_{\alpha,i} \quad \forall \alpha \in \{1, 2, 3, \ldots, n\}, \tag{14}$$

that is, the αth component of $\vec{\mathbf{c}}_q$ is a repetition of the αth component of $\vec{\mathbf{c}}_i$ for some $i \in \{1, 2, 3, \ldots, n\}$. Now consider columns $\alpha \in \{1, 2, \ldots, n\}$, as all elements in $\vec{\mathbf{c}}_q$ are repetitions of elements in some codeword from $\vec{\mathbf{c}}_1$ to $\vec{\mathbf{c}}_{(q-1)}$, we have

$$\begin{aligned} \exists i \in \{1, 2, \ldots, (q-1)\} \quad \forall \alpha \in \{1, 2, \ldots, (q-1)\}, \\ \mathbf{c}_{q,\alpha} = \mathbf{V}_{\alpha,i}. \end{aligned} \tag{15}$$

Without loss of generality, we can assume that the ith component of $\vec{\mathbf{c}}_q$ is the ith component of $\vec{\mathbf{c}}_i$, that is, $\mathbf{c}_{q,i} = \mathbf{c}_{i,i}$. Following this technique, we note that when we reach the qth component of $\vec{\mathbf{c}}_q$, we will have one symbol repetition corresponding to each codeword $\vec{\mathbf{c}}_i$ for $i \in \{1, 2, \ldots, (q-1)\}$. This means the distance between $\vec{\mathbf{c}}_q$ and $\vec{\mathbf{c}}_i$ for $i \in \{1, 2, \ldots, (q-1)\}$ can at most be $n-1$. Now when we try to assign any component to $\vec{\mathbf{c}}_{q,q}$ we see that this assignment will be a repetition of the qth component of some codeword $\vec{\mathbf{c}}_i$ in $\{\vec{\mathbf{c}}_1, \vec{\mathbf{c}}_2, \ldots, \vec{\mathbf{c}}_{q-1}\}$, let us say $\vec{\mathbf{c}}_j$. But this would mean $\vec{\mathbf{c}}_q$ now and can be only $n-2$ away from $\vec{\mathbf{c}}_j$. This would be a violation of the branch number condition. This situation cannot be avoided when $n > q-1$, therefore $n \leq q-1$ for an $[n, k, q, b]$ HD code. □

2.3. Construction of HD codes

Unlike usual error-correcting codes, the definition of HD codes involves pairs of messages and their associated codewords. This makes deriving a closed form expression for the construction of the codes tricky. A brute force search with backtracking produces the complete mapping but has the highest expected runtime. We have, therefore, developed three different shortcut techniques to generate HD codes.

2.3.1. Coset-based search

The coset-based search makes use of cosets in the code to reduce the complexity of the code assignment. The cosets are formed such that the codewords assigned to the coset leaders and the rest of the coset are related to each other. Often, they are rotations of each other. This searching technique only needs to find codewords for the coset leaders.

Table 1: A [3, 2, 4, 4] HD code.

Message	⟷	Codeword
00	⟷	000
01	⟷	111
02	⟷	222
03	⟷	333
10	⟷	123
20	⟷	231
30	⟷	312
11	⟷	032
21	⟷	320
31	⟷	203
12	⟷	301
22	⟷	013
32	⟷	130
13	⟷	210
23	⟷	102
33	⟷	021

Table 2: Cosets and coset leaders for the [3, 2, 4, 4] HD code.

Cosets	⟷	Coset leaders
{00,01,02,03}	⟷	No leader
{10,20,30}	⟷	10
{11,21,31}	⟷	11
{12,22,32}	⟷	12
{13,23,33}	⟷	13

Example code assignments

Message-codeword assignments of an $[n = 3,\ k = 2,\ q = 2^2,\ b = 4]$ HD code are given in Table 1. This mapping is not unique but has several properties that are useful in analyzing general HD codes. For example, the most useful property of this mapping is that the set of codewords can be partitioned into cosets such that the codewords for each of the messages in a particular coset are rotations of each other. Table 2 identifies these cosets and their leaders for the code in Table 1. The coset $\{00, 01, 02, 03\}$ is unique in that it has no leaders. It contains the first q messages, the codewords for which can be defined as $\vec{\mathbf{c}}_i = i \star n$ for all $i = \{0, 1, 2 \ldots, (q-1)\}$. The rest of the cosets, unlike the first coset, have codewords that are rotations of the codeword assigned to its leader. The identification of cosets speeds up the search algorithm as codewords for only the leaders need to be found. For the [2–4] HD code with the brute force search algorithm, we would have to search codewords for fifteen messages, whereas using the coset method implies finding seven mappings.

Table 3: List of parameters of some HD codes.

Codeword length (n)	Message length (k)	Galois Field GF(q)	Branch number (b)	Error-correction capacity (t)
3	2	4	4	0
7	3	8	8	2
7	5	8	8	1
15	9	16	16	3
15	7	16	16	4
15	5	16	16	5
15	3	16	16	6
6	4	256	7	1

2.3.2. Transformation from Reed Solomon codes

We have shown that all HD codes are MDS codes (see Theorem 1.) Reed Solomon (RS) codes are a subclass of MDS codes. So another way of constructing a subclass of HD codes is to start with $[q-1, k, q]$ RS codes and transform them into $[q-1, k, q, q]$ HD codes, using permutations of the message-codeword assignments of the original RS code. *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, namely, the branch number criterion*. The relationship between the messages of HD codes and the messages of RS codes that generate the corresponding HD codewords upon RS encoding is still an open problem. However, we have found transformations for several HD codes. For example, to generate HD codes from [7,3,8] RS codes [16], we multiply the message with the transformation matrix $\begin{pmatrix} 1 & 5 & 4 \\ 1 & 3 & 2 \\ 6 & 2 & 1 \end{pmatrix}$ before RS encoding using the generator polynomial $(x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)$. Here, α is the primitive element in GF(2^3). Similarly, we multiply with the inverse transformation matrix $\begin{pmatrix} 4 & 2 & 2 \\ 2 & 5 & 2 \\ 1 & 6 & 2 \end{pmatrix}$ after RS decoding. A list of the parameters of HD codes obtained using this method is given in Table 3. As RS codes are present in most of the communication systems and the transformations are simple add-on operations, HD codes can be easily deployed on those systems. The brute force generation of HD codes from RS codes that operate in fields greater than GF(16) requires significantly higher computational power and memory.

2.3.3. Puncturing existing codes

This gives us an easy way to generate new HD codes from existing HD codes.

Theorem 3. *Punctured HD codes are HD codes.*

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

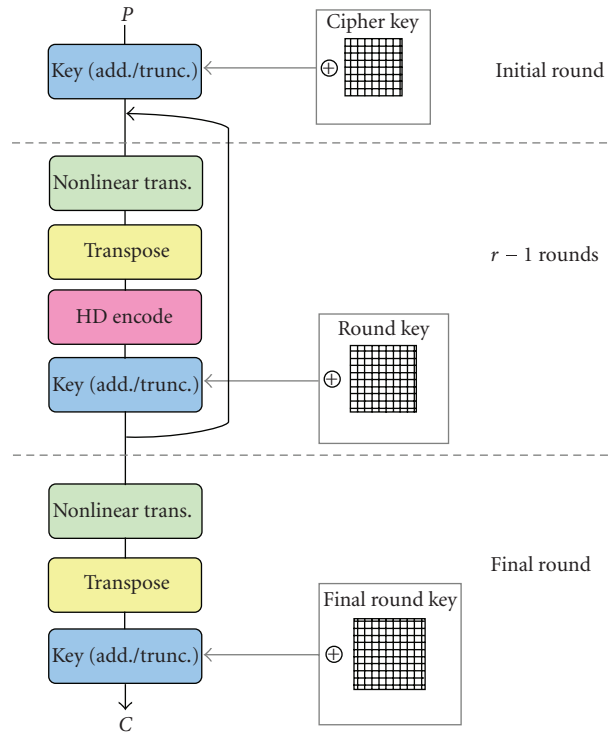

Figure 1: Block diagram of high diffusion cipher.

This implies that $H_d(\vec{m}_i, \vec{m}_j) + H_d(\vec{c'}_i, \vec{c'}_j) \geq n$. Hence, $\mathcal{C}'$ is an HD code. □

3. PROPOSED HIGH DIFFUSION CIPHER (HD CIPHER)

The HD-code-based cipher (or HD cipher) encrypts n_b^0 bits of plaintext to n_b^r bits of ciphertext, where r is the number of encryption/decryption rounds. As HD codes cause bit expansion, $n_b^r \geq n_b^0$. The set of initial, intermediate, and final block lengths of the HD cipher is $\{n_b^i;\ \forall i \in [0 \cdots r]\}$. The n_b^i bits are divided into n_t^i symbols represented by m bits each. All the operations in the HD cipher are performed in the Galois field of order 2^m. The round transformation, ρ, is defined as

$$\rho = \theta \circ \pi \circ \gamma, \tag{16}$$

where γ is the substitution layer, θ and π form the diffusion layer. These layers are explained in the following sections. The number of key bits n_k is equal to n_b^r. We propose to use the same key schedule algorithm as in Rijndael, which extends the n_b^r-bit cipher key into $(r+1) \times n_b^r$ bits to produce round keys $\{k^1, k^2, \ldots, k^r\}$. The r round iterated HD cipher $\mathcal{H}$ is described as follows:

$$\begin{aligned} \mathcal{H}[k] =& \sigma\left[k^{(r)}\right] \circ \rho^{(r)}_{n_b^{r-1}, n_b^r} \circ \sigma\left[\chi(k^{(r-1)})\right] \circ \cdots \circ \\ & \sigma\left[\chi(k^{(1)})\right] \circ \rho^{(1)}_{n_b^0, n_b^1} \circ \sigma\left[\chi(k^{(0)})\right]. \end{aligned} \tag{17}$$

A block diagram of the HD cipher encryption is given in Figure 1. It follows that HD cipher is a *key-alternating* block cipher [12].

3.1. Key mixing layer (σ, χ)

The key addition operation σ is a bitwise XOR operation of the cipher state with the round key. As the cipher key uses $n_k = n_b^r < n_b^i$ (for all $i < r$) bits, the round keys are larger than the intermediate cipher states for all but the last round of the cipher. Additional bits of round keys are removed using the key truncation operation χ, which simply reduces the size of the round key to the size of the cipher state.

3.2. Nonlinear substitution layer (γ)

This layer uses a local nonlinear transformation γ. The construction of γ is similar to Rijndael [12], where the substitution box is generated by inverting elements in the finite field of 2^m and applying an invertible affine transform (to prevent zeros mapping to zero). The n_b input bits to each round operation, ρ, are represented by a vector (say $\vec{a}$) with n_t symbols each represented by m-bits. An invertible S-box, S_γ, transforms the input vector $\vec{a}$ to the output vector $\vec{b}$ by acting on each of the n_t symbols independently. The γ transformation can be expressed by

$$\gamma : \vec{b} = \gamma(\vec{a}) \Longleftrightarrow b_j = S_\gamma(a_j), \tag{18}$$

where a_j is one of the n_t, m-bit symbols. The inverse of γ operation is denoted by $\overline{\gamma}$. A Symbol or S-box is said to be active, if the input difference pattern a' is nonzero for a particular symbol or S-box position. The number of active S-boxes in a given pattern, a', is equal to $w_s(a')$, the symbol weight [12].

3.3. Diffusion layer (π, θ)

In this layer, we use high diffusion codes to jointly attain maximum diffusion and error-correction capability.

3.3.1. HD coding operation θ

With respect to θ, the symbols of the state are grouped into number of columns by a partition Ξ of the index space $\mathcal{I}$. The number of columns is denoted by n_Ξ. For the state $\vec{a}$, a_ξ denotes a column with column number $\xi \in [1, \ldots, n_\Xi]$. For HD ciphers, we impose the condition that every column a_ξ to have the same length denoted by n_ξ. To perform *HD encoding* θ, every column a_ξ is encoded using $[n_\xi + d_{\min} - 1, n_\xi, 2^m]$ HD code. The resulting state will contain n_Ξ columns with $n_\xi + d_{\min} - 1$ symbols in each column. We denote the HD encoding operation, θ_{n_ξ, n'_ξ}, where $n'_\xi = n_\xi + d_{\min} - 1$, by

$$\theta : \vec{b} = \theta(\vec{a}) \Longleftrightarrow b_\xi = \theta_{n_\xi, n'_\xi}(a_\xi). \tag{19}$$

Figure 2 represents this operation. Note that in HD cipher, HD coding is not performed in the last encryption round (see Figure 1.) The inverse of θ is the decoding operation, denoted by $\overline{\theta}$.

A column ξ is said to be active if it consists at least one active symbol or S-box. Similar to the symbol weight $w_s(a)$ (see Section 3.2), we denote the column weight by the number of active columns $w_c(a)$. Since all the columns ξ have equal

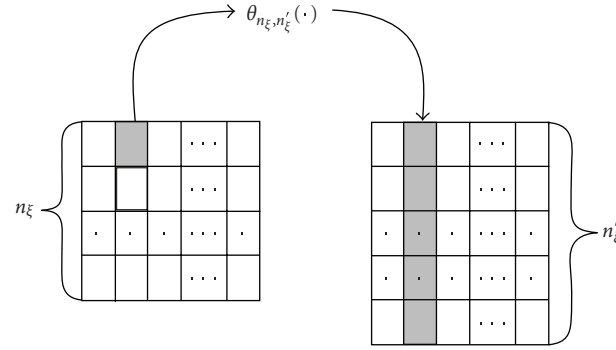

Figure 2: High-diffusion encoding process (HD encode).

number of symbols, n_ξ, the branch number of θ is lower bounded by

$$\mathcal{B}(\theta) \geq n_\xi + d_{\min}. \tag{20}$$

3.3.2. Symbol transposition transformation π

The HD coding operation diffuses the columns of the input state. To spread this effect to all rows a diffusion optimal symbol transposition transformation is used. The symbol transposition, π, is defined as

$$\pi : b = \pi(a) \Longleftrightarrow b_{j,i} = a_{i,j}. \tag{21}$$

It can be observed that this is a matrix *transpose* operation and every column of the input matrix to π is turned into the corresponding row in the output matrix. Matrix transposition is a diffusion-optimal transformation [17].

4. SECURITY ANALYSIS OF HD CIPHERS

Security of symmetric block ciphers are usually measured by their key lengths. This is because for a brute force 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 $\mathcal{O}(2^{n_b^0})$. This is because the plaintext for HD cipher is n_b^0 bits in length. 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 the brute force technique. In this section, we analyze the security of HD ciphers by looking at the resistance it offers against some well-known cryptanalytic attacks.

4.1. Linear and differential cryptanalysis

Linear cryptanalysis [18] is a known plaintext-ciphertext attack that makes use of linearity in the cipher to obtain the key bits. The success of linear cryptanalysis is related to the weight of a linear trail [12], which is the product of the sum of the weights of its active S-box positions and the minimum

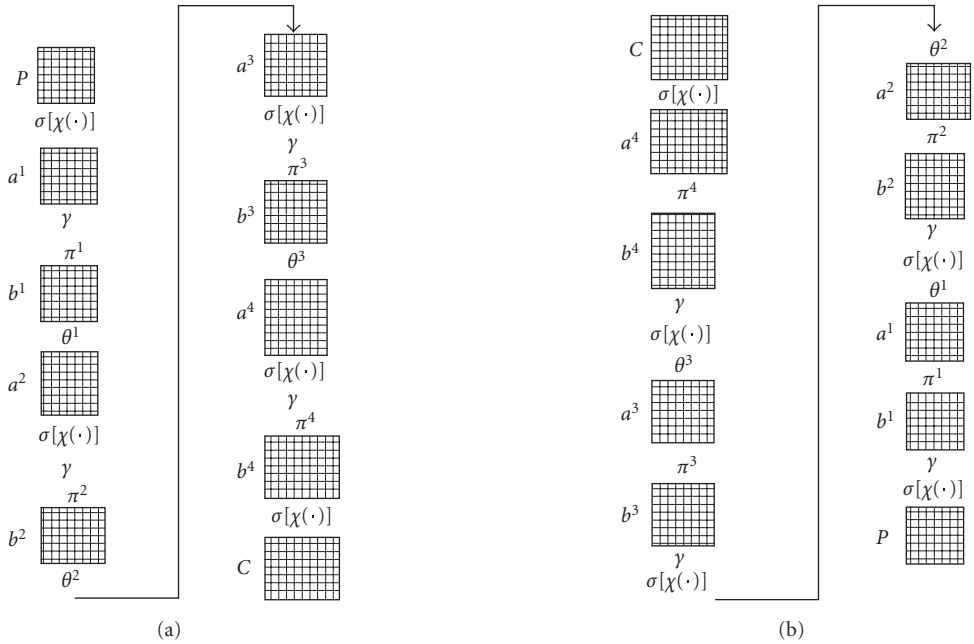

Figure 3: (a) Four-round HD cipher encryption. (b) Four-round HD cipher decryption.

correlation weight per S-box. If the input and output parity for all but a few rounds of a cipher has a correlation with an amplitude significantly larger than $2^{-n_b/2}$, it can be attacked using linear cryptanalysis. Hence, the cipher design should restrict the amplitude of the correlation between input and output parities to be lesser than $2^{-n_b/2}$.

Differential cryptanalysis [19, 20] is a chosen plaintext-ciphertext attack that makes use of difference propagation property of a cipher to deduce the key bits. The success probability of a differential cryptanalysis is the sum of the probabilities of all r round differential trails with a given plaintext and ciphertext difference. To secure a cipher against differential cryptanalysis, the design should restrict the probability of difference propagation to 2^{1-n_b}. The weight of a differential trail is the sum of the weights of the difference patterns of the trails [12].

As the structure of HD cipher is similar to Rijndael (especially the key alternating property), the maximum input-output correlation and difference propagation for linear and differential trails on HD cipher is given by the product of the sum of active S-boxes in all its selection patterns (for a few rounds) and the minimum correlation weight or minimum differential weight per S-box. Since our design is also based on the wide trail strategy, we lower bound the number of active S-boxes for a four-round trail (see Theorem 5) to achieve lower bounds on resistance against linear and differential cryptanalysis. Hence, the security of both HD cipher and Rijndael against linear and differential cryptanalysis can be quantified by using this lower bound.

Lemma 3. *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 [14].

Theorem 4. *The number of active S-boxes or symbols for a two-round trail of HD cipher is lower bounded by the branch numbers of HD code $\mathcal{B}(\theta^1)$.*

Proof. Four-round HD cipher encryption operation is depicted in Figure 3(a), consider the first two rounds of HD cipher. Let a^1 represent any input vector with n_t^1, m-bit symbols. a^2 is the output vector with n_t^2, m-bit symbols. Since γ and $\sigma[\chi(\cdot)]$ 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, $w_s(a^1) + w_s(a^2)$, is bounded by the propagation property of θ^1. From the definition of HD codes and (20), it follows that the sum of active S-boxes before and after θ^1 encoding of the first round is lower bounded by $\mathcal{B}(\theta^1)$. □

Theorem 5. *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 a^2 and b^3 is lower bounded by $\mathcal{B}(\theta^2)$ (from Lemma 3). Hence, we have

$$w_c(a^2) + w_c(b^3) \geq \mathcal{B}(\theta^2), \tag{22}$$

but $w_c(b^3) = w_c(a^4)$ (θ does not change the number of active columns). Therefore,

$$w_c(a^2) + w_c(a^4) \geq \mathcal{B}(\theta^2). \tag{23}$$

The total number of active S-boxes in b^1 and a^2 is given by

$$w_s(b^1) + w_s(a^2) \geq w_c(a^2)\,\mathcal{B}(\theta^1). \tag{24}$$

Similarly, the total number of active S-boxes in b^3 and a^4 is given by

$$w_s(b^3) + w_s(a^4) \geq w_c(a^4)\,\mathcal{B}(\theta^3). \tag{25}$$

Combining (23), (24), and (25) will give

$$\begin{aligned} &w_s(b^1) + w_s(a^2) + w_s(b^3) + w_s(a^4) \\ &\quad \geq w_c(a^2)\,\mathcal{B}(\theta^1) + w_c(a^4)\,\mathcal{B}(\theta^3) \\ &\quad \geq (w_c(a^2) + w_c(a^4))\,\mathcal{B}(\theta^1) + w_c(a^4)(d^2_{\min} + d^3_{\min} - 2). \end{aligned} \tag{26}$$

Since $w_c(a^4)(d^2_{\min} + d^3_{\min} - 2)$ is nonnegative ($d^2_{\min}, d^3_{\min} \geq 1$) and $w_s(b^j) = w_s(a^j)$, we get

$$w_s(a^1) + w_s(a^2) + w_s(a^3) + w_s(a^4) \geq \mathcal{B}(\theta^1)\,\mathcal{B}(\theta^2). \tag{27}$$

□

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. Using a more redundant code would imply higher branch number and hence higher resistance to linear and differential cryptanalysis.

Note that we do not assume that branch number implies security in all forms. However, in our cipher the branch number of the HD codes is the only additional entity for which we need to show optimality in security. This is because we use the "wide trail strategy," where small highly nonlinear substitution boxes (S-box) are coupled with optimal-diffusion operations to achieve a large number of active S-boxes in a few rounds. This is the same strategy employed in ciphers like Rijndael, Crypton, and so forth. To show that ciphers built on wide trail strategy are secure, it is necessary to show that (a) the S-boxes have high nonlinear property, (b) the diffusion functions are optimal (have highest possible branch number).

The S-boxes that we use in our cipher are based on the work by Nyberg [21] and are used in Rijndael. These S-boxes have been shown to be differentially 4 uniform [21] (i.e., very high nonlinear property). Therefore, the security of our cipher rests on the optimality of the diffusion operations. We have shown that HD codes achieve maximum possible branch number (measure of diffusion). Hence, the high branch number property of HD codes helps the HD cipher achieve security.

4.2. Square attack

The square attack (also known as integral attack [22] or the saturation attack [23]) 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 [24, 25]. Although the attacks described applies directly to cipher operations with symbol size in bytes, it can be easily extended to other symbol sizes. HD ciphers also comprise of symbol-oriented operations, hence HD ciphers with fewer than seven rounds would be as weak as reduced versions of the Rijndael cipher against these attacks.

5. ERROR DETECTION AND CORRECTION CAPACITIES OF HD CIPHERS

In this section, we prove bounds on the error-correction capacity of HD ciphers. Specifically, we consider a bursty channel and use the term "full weight burst error" to denote a burst with all 1's. After encryption, the ciphertext (represented in matrix form) is transmitted either rowwise or columnwise. In our analysis, we consider both these types of transmissions by considering bursts across rows and columns in the received ciphertext matrix before decryption. 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, $t^j = t$; for all $j \in [1, \ldots, r-1]$. A symbol of the cipher state that is in error (due to channel and/or error propagation due to decryption rounds) is referred to as an *error symbol*. We denote an ordered set of error symbols in the cipher state by an *error pattern*. The error patterns for each round are denoted by, $\vec{a}^j$ for all $j \in [1, \ldots, r]$. A column (row) in the error pattern is said to be in error if there are at least $t+1$ error symbols in the corresponding column (row). We refer to such columns (rows) as *error column* (*error row*), respectively. A *decoding trail* is a set of error patterns of the cipher state before each round of decryption. We say that the error correction is *complete* in round j if the error pattern, a^j, at the output of θ^j is all zero. Similarly, we say that error correction is *incomplete* in round j if the error pattern a^j at the output of round j is not all zero. We will now analyze the error-correction capacity of a four-round HD cipher decryption in Lemmas 4, 5 and Theorem 6. An outline of four-round HD cipher decryption is represented in the Figure 3(b).

Lemma 4. *For a three-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 Figure 3. Since the inverse nonlinear transform $\overline{\gamma}$ and round key addition σ operations do not convert an error symbol to an error-free symbol, it can be excluded from the analysis.

First, we consider the case in which the error pattern a^4 contains at most t error columns. After π^4 transformation, we will have at most t error rows in b^4. Since $\overline{\theta}^3$ has an error-correcting power of t, errors across each of the columns are corrected. Hence, the error pattern a^3 will contain all zeros. This implies that the error correction is complete.

Consider the second case, in which the error pattern a^4 contains at most t error rows. After π^4 transformation, we

have at most t error columns in b^4. This is beyond the error correction capacity of $\overline{\theta}^3$, hence we take the worst case scenario of having at most t error columns in a^3. Now, applying the same argument as the first case, the error pattern a^2 should have all zeros, thus proving the theorem. □

Lemma 5. *For a three-round HD cipher, if there are at least $t+1$ error columns or rows in the ciphertext before decryption, the error correction will be incomplete even after at three rounds of decryption.*

Proof. First, consider the case in which the error pattern a^4 contains $t+1$ error columns. After π^4 transformation, b^4 will contain at least $t+1$ error rows. This is beyond the error correction capacity of θ^3. Hence a^3 will have all of symbols in error and the decryption will remain incomplete even after θ^2 in a^2. Similarly, when there are $t+1$ error rows in a^4, there will be $t+1$ error columns in a^3 and every symbol will be in error in a^2. Hence, the decryption will remain incomplete. □

We now analyze the maximum full weight burst 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 6. *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 rowwise transmission and hence full weight bursts that occur across the rows of the cipher text. The following analysis can be trivially extended to columnwise transmission as well.

We know that a burst of $t+1$ errors in one row makes that an error row. Similarly, bursts of $2(t+1)$ and $n_\xi^4+2(t+1)$ can cause two and three error rows, respectively. Generalizing this result, we get that a burst length of $(l-2)(n_\xi^4)+2(t+1)$ can cause l error rows. This is in fact the minimum full weight burst length required to have l error rows. It follows that a full weight burst length of at least $(t-1)(n_\xi^4)+2(t+1)$ is required to generate $l=t+1$ error rows. This implies that a full weight burst of length $(t-1)(n_\xi^i)+2(t+1)-1$ cannot generate $l \geq t+1$ error rows. From Lemma 4, a burst of length $(t-1)(n_\xi^4)+2(t+1)-1$ is correctable and from Lemma 5 a burst of length $(t-1)(n_\xi^4)+2(t+1)$ is not correctable. Hence the minimum burst length that is guaranteed to be corrected by a 4-round HD cipher decryption is $(t-1)(n_\xi^4)+2(t+1)-1$ which is equal to $(t-1)(\mathcal{B}(\theta^3)-1)+2t+1$, where $\mathcal{B}(\theta^3)=n_\xi^4+1$. □

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 7 gives the smallest burst length for which the probability of complete decoding is zero.

Theorem 7. *The smallest burst length of a full weight burst, 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 rowwise 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 5). 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 an error pattern with at most t error rows is tn_ξ^4+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. □

6. SIMULATION RESULTS

In our experiments, we construct a 10-round HD-cipher with input data size of 128 bits and output ciphertext and keysize of 288 bits. This is achieved by using a [4,4,256] HD code for rounds 1 through 7 and a [6,4,256] HD code for rounds 8 and 9. The generator matrixes for these HD codes are

$$G(r)_{r=[1\cdots7]} = \begin{pmatrix} 1 & 1 & 3 & 2 \\ 2 & 1 & 1 & 3 \\ 3 & 2 & 1 & 1 \\ 1 & 3 & 2 & 1 \end{pmatrix},$$
$$G(r)_{r=[8,9]} = \begin{pmatrix} 1 & 1 & 3 & 2 & 189 & 71 \\ 2 & 1 & 1 & 3 & 169 & 27 \\ 3 & 2 & 1 & 1 & 192 & 209 \\ 1 & 3 & 2 & 1 & 91 & 179 \end{pmatrix}. \tag{28}$$

To perform HD encoding, each column of the input cipher state is multiplied with $G(r)$ to obtain the output cipher state. The branch number $\mathcal{B}(G(r))$ of $G(r)_{r=[1\cdots7]}$ is 5 and $G(r)_{r=[8,9]}$ is 7. The sum of active S-boxes for a four-round trail of HD cipher is $\mathcal{B}(\theta^1)\times\mathcal{B}(\theta^2)=35$. The sum of active S-boxes for a four-round trail of the AES cipher is 25. The additional 6 rounds have been added as a security margin (for both the AES and the HD cipher). In AES, the number of rounds is increased if (a) the input plaintext block length increases, (b) the key length increases. Since we use the same input block length in HD cipher and target the same security as a 128-bit key length that is used in AES, the number of rounds in the HD cipher is equal to the number of rounds in AES which is 10.

To evaluate the performance (error correction) of the HD cipher, we compare it with the following concatenated systems A and B (described below) with respect to error-correction capacity:

(i) *concatenated system A*: uses AES (128-bit) cipher with [36,16,256] Reed Solomon code;
(ii) *concatenated system B*: uses AES (128-bit) cipher and convolutional codes with rates varying from 1/2 to 1/6.

Wireless communication medium is characterized by bursty errors and fading phenomenon, which implies that bit errors occurring in wireless channels have memory. Alajaji

and Fuja [26] proposed an additive Markov channel (AMC) model for slow fading wireless channels. According to this model, the channel can be described by bit-error rate and correlation parameters. The burstyness of the channel can be controlled by the correlation parameter. In our experiments, we set the correlation to 0.9 and varied the bit-error rate from 0.001 to 0.2.

Figure 4 plots the post decryption bit-error rate of the proposed 128-bit HD cipher and the concatenated system A against channel-bit-error rate. It can be observed that HD cipher and the concatenated system are comparable in terms of error-correction capacity over all the channel-bit-error rates. This is because both HD cipher and the Reed Solomon code used in the concatenated system are burst error-correcting codes with similar coding rates. However, as the error correction is performed during decryption within the HD cipher, there is roughly a savings of two rounds per encryption/decryption compared to the concatenated system.

For the second set of experiments, we compare the proposed 128-bit HD cipher with the concatenated system B. Different convolutional codes with rates 1/2, 1/3, 1/4, 1/5, and 1/6 are considered. Since the channel is assumed to be bursty, a block interleaver is added after convolutional encoder to optimize the performance of the concatenated system. Hard decision Viterbi decoder is used at the receiver. Figure 5 plots the post decryption bit-error rate of the proposed HD cipher and the concatenated system B. The HD cipher clearly outperforms the concatenated system for all rates 1/2 through 1/6. Note that the coding rate of the HD cipher is between that of the concatenated systems with rate 1/5 and 1/6 yet it outperforms the rate 1/6 concatenated system. Although convolutional codes are more light weight compared to Reed Solomon codes, the total number of operations when it is combined with 10-round AES cipher is approximately equal to the number of operations in a 10-round HD cipher.

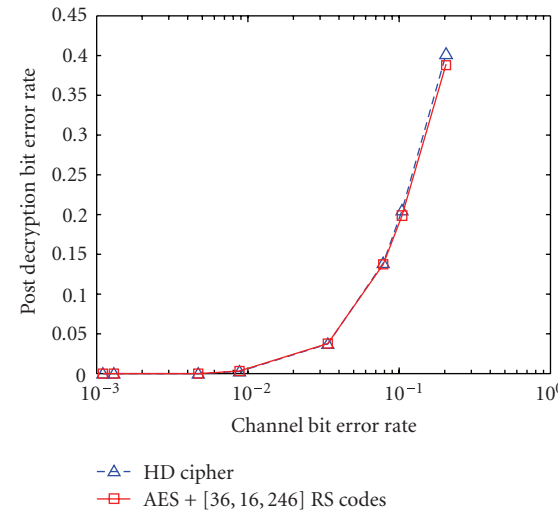

Figure 4: Comparison of error resilience of HD cipher and AES concatenated with [36, 16, 256] Reed Solomon codes.

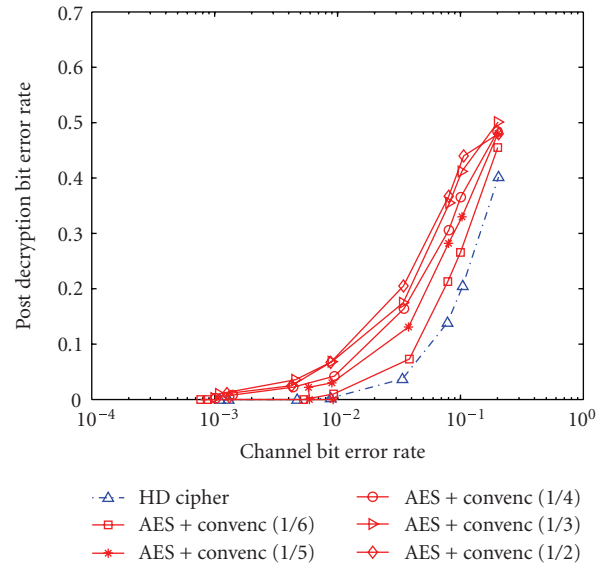

Figure 5: Comparison of error resilience of HD cipher and AES concatenated with convolutional codes. Notice that the coding rate of HD cipher is between 1/5 and 1/6, yet it outperforms the 1/6 rate concatenated system.

7. CONCLUSION

A new error-correcting cipher was proposed for use in wireless networks. Diffusion (measured by the branch number) and error resilience (measured by minimum distance between codewords) were identified as the two main criteria to be satisfied by channel codes that could aid as building blocks in this novel error-correcting ciphers. A new class of codes called the high diffusion codes (HD codes) were developed based on these two criteria. HD codes were shown to achieve optimal diffusion and error resilience and that they are MDS codes that satisfy an additional criterion for security. Several techniques to construct HD codes were presented. The error-correcting HD cipher, that uses HD codes in its diffusion layer was constructed. 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^i is the ith round HD encryption operation. We proved that the full weight burst error-correction capacity of 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(256) revealed that (a) HD cipher is as secure as AES cipher when security is quantified in terms of the number of active S-boxes, (b) joint encryption and error correction in HD cipher are comparable to disjoint error correction and encryption performed by a traditional concatenated system using AES encryption and Reed Solomon coding, (c) concatenated systems using AES encryption and convolutional codes need to increase the data expansion by 10% to match the performance of HD cipher.

ACKNOWLEDGMENTS

This work was partially supported by NSF Grant no. 062-7688. This work was supported in part by the US Army Picatinny Arsenal/Stevens Wireless Network Security Center (WiNSeC).

REFERENCES

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice-Hall, Upper Saddle River, NJ, USA, 2nd edition, 1999.

[2] C. Nanjunda, M. A. Haleem, and R. Chandramouli, "Robust encryption for secure image transmission over wireless channels," in *Proceedings of IEEE International Conference on Communications (ICC '05)*, vol. 2, pp. 1287–1291, Seoul, Korea, May 2005.

[3] H. C. A. van Tilborg, "Coding theory at work in cryptology and vice versa," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., pp. 1195–1227, North-Holland, Amsterdam, The Netherlands, 1998.

[4] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 384–386, 1978.

[5] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Fla, USA, 1996.

[6] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," DNS Progress Reports 42-44, NASA Jet Propulsion Laboratory, Pasadena, Calif, USA, 1978.

[7] T. Hwang and T. R. N. Rao, "Secret error-correcting codes (SECC)," in *Proceedings of the 8th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '88)*, pp. 540–563, Santa Barbara, Calif, USA, August 1988.

[8] W. Godoy Jr. and D. Pereira Jr., "A proposal of a cryptography algorithm with techniques of error correction," *Computer Communications*, vol. 20, no. 15, pp. 1374–1380, 1997.

[9] T. A. Berson, "Failure of the McEliece public-key cryptosystem under message-resend and related-message attack," in *Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '97)*, Lecture Notes in Computer Science, pp. 213–220, Santa Barbara, Calif, USA, August 1997.

[10] D. Stinson, *Cryptography: Theory and Practice*, CRC/C&H, London, UK, 2nd edition, 2002.

[11] FIPS, "Specification for the advanced encryption standard (AES)," Federal Information Processing Standards Publication 197, 2001.

[12] J. Daemen and V. Rijmen, *The Design of Rijndael*, Springer, New York, NY, USA, 2002.

[13] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice-Hall, Upper Saddle River, NJ, USA, 1995.

[14] J. Daemen and V. Rijmen, "The wide trail design strategy," in *Proceedings of the 8th IMA International Conference on Cryptography and Coding (IMA '01)*, pp. 222–238, Cirencester, UK, December 2001.

[15] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes. I and II*, vol. 16 of *North-Holland Mathematical Library*, North-Holland, Amsterdam, The Netherlands, 1977.

[16] X. Chen, *Error-Control Coding for Data Networks*, Kluwer Academic, Norwell, Mass, USA, 1999.

[17] J. Daemen, L. R. Knudsen, and V. Rijmen, "The block cipher square," in *Proceedings of 4th International Workshop on Fast Software Encryption (FSE '97)*, pp. 149–165, Haifa, Israel, January 1997.

[18] M. Matsui, "Linear cryptoanalysis method for DES cipher," in *Proceedings of Advances in Cryptology Workshop on the Theory and Application of of Cryptographic Techniques (EUROCRYPT '93)*, vol. 765 of *Lecture Notes in Computer Science*, pp. 386–397, Lofthus, Norway, May 1993.

[19] E. Biham and A. Shamir, "Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer," in *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '91)*, vol. 576 of *Lecture Notes In Computer Science*, pp. 156–171, Santa Barbara, Calif, USA, August 1991.

[20] E. Biham and A. Shamir, "Differential cryptanalysis of the full 16-round DES," in *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '92)*, pp. 487–496, Santa Barbara, Calif, USA, August 1992.

[21] K. Nyberg, "Differentially uniform mappings for cryptography," in *Proceedings of Advances in Cryptology Workshop on the Theory and Application of of Cryptographic Techniques (EUROCRYPT '93)*, pp. 55–64, Lofthus, Norway, May 1993.

[22] L. R. Knudsen and D. Wagner, "Integral cryptanalysis," in *Proceedings of the 9th International Workshop on Fast Software Encryption (FSE '02)*, vol. 2365 of *Lecture Notes in Computer Science*, pp. 112–127, Leuven, Belgium, February 2002.

[23] S. Lucks, "The saturation attack - a bait for twofish," in *Proceedings of the 8th International Workshop on Fast Software Encryption (FSE '01)*, vol. 2355 of *Lecture Notes in Computer Science*, pp. 1–15, Yokohama, Japan, April 2001.

[24] H. Gilbert and M. Minier, "A collision attack on 7 rounds of rijndael," in *Proceedings of the 3rd Advanced Encryption Standard Candidate Conference*, pp. 230–241, New York, NY, USA, April 2000.

[25] S. Lucks, "Attacking seven rounds of rijndael under 192-bit and 256-bit keys," in *Proceedings of the 3rd Advanced Encryption Standard Candidate Conference*, pp. 215–229, New York, NY, USA, April 2000.

[26] F. Alajaji and T. Fuja, "A communication channel modeled on contagion," *IEEE Transactions on Information Theory*, vol. 40, no. 6, pp. 2035–2041, 1994.

Chetan Nanjunda Mathur is currently pursuing his Ph.D. degree in computer engineering at Stevens Institute of Technology, Nj, USA. He received his B.E. degree in computer science from Visveshwaraiah Institute of Technology, Bangalore, India, in 2002. He has an M.S. in computer engineering from Stevens Institute of Technology, Nj, USA. Part of Chetan's M.S. thesis was patented by Stevens Institute of Technology. In the past few years, Chetan has published several research papers in the fields of Cryptography, Coding theory, and Dynamic spectrum access. He has also received numerous awards including the IEEE Best Student Paper Award Presented at IEEE Consumer Communications and Networking Conference (CCNC 2006) and the IEEE Student Travel Grant Award presented at International Conference on Communications (ICC 2005). He is an Active Student Member of IEEE and is in the advisory board of Tau Beta Pi, the National Organization of Engineering Excellence.

Karthik Narayan has a Bachelor's degree in computer engineering from VTU, Belgaum, India and an M.S. degree in computer engineering from Stevens Institute of Technology, Hoboken, Nj. His research interests include cryptography, channel coding, wireless and multimedia applications and finance. He is currently working at Merrill Lynch's Mortgage's Department.

K. P. Subbalakshmi is an Assistant Professor in the Department of Electrical and Computer Engineering, Stevens Institute of Technology where she leads research projects in information security, encryption for wireless security, joint source-channel and distributed source-channel coding, with funding from the NSF, AFRL, ONR, US Army, and other agencies. She is the Chair of the Security Special Interest Group of the IEEE Technical Committee on Multimedia Communications. She was a Program Cochair of the IEEE GLOBECOM 2006, Symposium on Network and Information Security Systems. She serves as an Associate Editor of Advances in Multimedia journal.