Design of Strongly Secure Communication and Computation Channels by Nonlinear Error Detecting Codes

Mark Karpovsky, *Life Fellow, IEEE,* Zhen Wang

Abstract—
The security of communication or computational systems protected by traditional error detecting codes rely on the assumption that the information bits of the message (output of the device-under-attack) are not known to attackers or the error patterns are not controllable by external forces. For applications where the assumption is not valid, e.g. secure cryptographic devices, secret sharing, etc, the security of systems protected by traditional error detecting codes can be easily compromised by an attacker. In this paper, we present constructions for strongly secure codes based on the nonlinear encoding functions. For (k, m, r) strongly secure codes, a message contains three parts: k-bit information data y, m-bit random data x and r-bit redundancy $f(y, x)$. For any error e and information y, the fraction of x that masks the error e is less than 1. In this paper we describe lower and upper bounds on the proposed codes and show that the presented constructions can generate optimal or close to optimal codes. An efficient encoding and decoding method for the codes minimizing the number of multipliers using the multivariate Horner scheme is presented.

Index Terms—Nonlinear Codes, Reed-Muller Codes, Secure Hardware, Fault Injection Attacks

1 Introduction

Error detecting codes are widely used for communication channels and for computation channels to protect reliable and secure devices against soft errors, hard errors and malicious attacks in applications like Internet, data storage, cryptosystems and wireless communications.

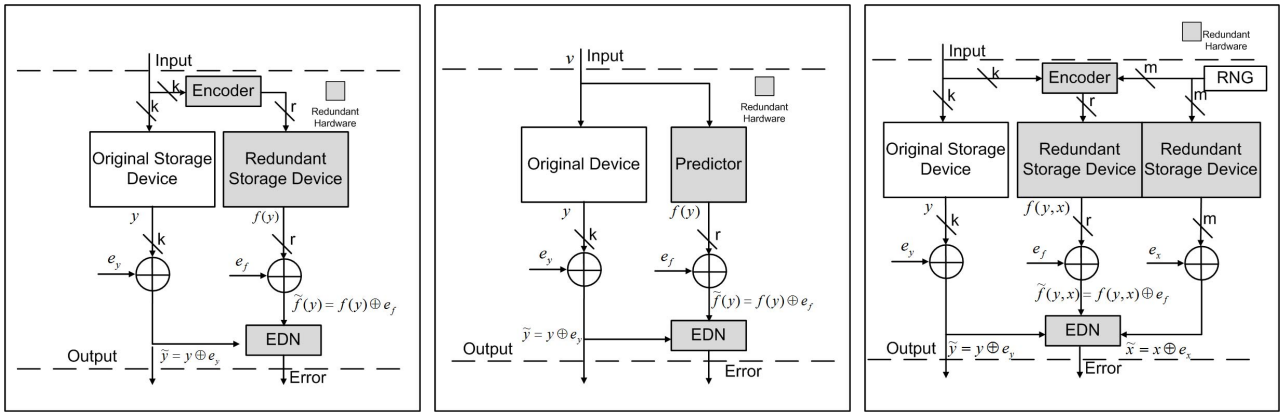
Most of the existing secure architectures [1], [2], [3], [4], [5], [6] are based on linear codes such as 1-d parity codes, duplication codes, Hamming codes, BCH codes, Reed-Solomon codes, etc. The error detecting capabilities these architectures largely depend on the accuracy of the error model and may not be sufficient if an attacker can control errors distorting the received messages for communication channels or errors distorting outputs of a device protected by an error detecting code for computation channels. For example, devices protected by linear 1-d parity codes can detect all errors with odd multiplicities but cannot provide any protection against errors with even multiplicities. An advanced attacker can easily bypass the protection mechanism based on 1-d parity codes by only injecting faults manifesting as errors with even multiplicities at the output of the protected devices [7].

Robust codes based on nonlinear encoding functions were proposed by the authors in [8], [7], [9], [10], [11], [12]. A code $C \in GF(2^n)$ is robust if $\{e | c \oplus e \in C, \forall c \in C\} = \{\mathbf{0} \in GF(2^n)\}$. These codes can provide nearly equal protection against all error patterns. The error masking probabilities $Q_C(e) = |C|^{-1}|\{c \in C, c \oplus e \in C\}|$ ($|C|$ is the size of the code) for robust codes are upper-bounded by a number less than 1 for all non-zero errors. Compared to the systems based on linear codes, systems based on robust codes can provide a guaranteed protection regardless of the accuracy of the error model under the assumption that all messages(codewords) are equiprobable. Variants of robust codes – partially robust and minimum distance robust codes – were proposed in [13], [10], which allow tradeoffs in terms of the robustness and the hardware overhead.

One limitation of robust codes is that these codes assume the information bits of messages or outputs of the device-to-be-protected are uniformly distributed and are not known to attacker, e.g. to an attacker during error injection attacks on devices. The security of the communication or computation channels protected by robust codes will be largely compromised if information bits of the messages are known to the attacker and the non-zero error patterns can be controlled by the attacker.

Example 1.1: Block ciphers such as AES are vulnerable to fault injection attacks. It has been shown that by injecting undetected errors into intermediate computation results of the encryption or decryption process, the attacker can compromise the security level of the cipher by revealing the secret key that is used for encryption and decryption [14]. Suppose the intermediate computation results of one AES block is buffered in a 32-bit storage device, e.g. registers, caches, etc, and is protected by a robust duplication code $C = \{y, f(y)\}$, where $y, f(y) \in GF(2^{32})$, $f(y) = y^3$ and all operations are in $GF(2^{32})$ (see Figure 1a). Let $e = (e_y, e_f)$ be the error

- *Mark Karpovsky is with the Department of Electrical and Computer Engineering, Boston University, Boston MA, 02135. His work is sponsored by the NSF grant CNR 1012910. E-mail: markkar@bu.edu*
- *Zhen Wang is with Mediatek Wireless, Inc.*



(a) (b) (c)

Fig. 1: (a) Secure storage device protected by a systematic $(k+r,k)$ error detecting code. (b) Secure computational device protected by a systematic $(k+r,k)$ error detecting code. (c) Secure storage device protected by a systematic error detecting code with k information bits, m random bits and r redundant bits. (RNG is the random number generator. EDN is the error detecting network.)

vector. An error e is masked by a codeword $c=(y,f(y))$ if and only if

$$f(y\oplus e_y)=f(y)\oplus e_f, \tag{1}$$

or equivalently

$$e_y y^2 \oplus e_y^2 y \oplus e_y^3 \oplus e_f = 0 \tag{2}$$

Since the error masking equation (2) is in quadratic form, for any non-zero e there are at most two solutions for y. Thereby, any non-zero error e will be masked by at most two codewords. Assume that an attacker have no knowledge of intermediate computation result y during attacks and y is uniformly distributed in $GF(2^{32})$, then the probability that the attacker conducts a successful attack ($e=(e_y,e_f)$ is not detected) is upper bounded by $2\times|C|^{-1}=2\times 2^{-32}=2^{-31}$, where $|C|$ is the number of the codewords in C. If an attacker has the ability to eardrop the data bus of the storage device (see Figure 1) and has full knowledge of y and and can inject any arbitrary bit vector pattern to the storage cells, then the attacker can easily select $e^*=(e_y^*,e_f^*)$ for the given y^* so that (2) is satisfied. In this case, the error will always be missed and the following computations in the block cipher will be incorrect. As a result, the security of the block cipher can be compromised. Similar problems occur when robust codes are used to protect computational devices, where the goal of the attacker is to distort the outputs y to jeopardize the following computations by injecting faults into the computational device (see Figure 1b). If the attacker has knowledge of the detailed hardware implementation and the correct output y of the original device, he can succeed by injecting faults manifesting as an error pattern $e=(e_y,e_f)$ at the output of the device, which can never be detected by robust codes.

For the situation shown in the above example, the attacker is able to observe the original information bits of the message (output of the device-under-attack) and then apply fault injection attacks correspondingly. All previous protection technologies based on traditional error detecting codes will not be sufficient.

Intuitively, the limitation of robust code described above can be efficiently eliminated by introducing randomness into the encoding procedure of the code. Due to the fact that the random data are independent of the user information y, they can always be made uniformly distributed. As a result, the assumption for robust codes that y is uniformly distributed is no longer required. Moreover, since the user has zero knowledge and no control of the random bits generated for each encoding operation, no matter how the attacker selects e for a given y, the probability that e is masked will be upper bounded by a number determined by the size of the set of possible random numbers. A coding technique based on adding to k information bits m random bits and r redundant bits (see Figure 1c)), which can still provide guaranteed security under the above circumstance, is called strongly secure algebraic manipulation detection (AMD) code . (The formal definition of these codes will be given in the next Section, see Definition 2.2).

A simple AMD code was first presented in [15]. A much more versatile strong AMD code was introduced in [16], where the construction of optimal AMD codes was presented for $k=br$ information digits and $m=r$ random digits (r is the number of redundant digits). In [17], the authors introduced the concept of AMD codes and put all previous constructions in a unified framework. Compared to the widely used Message Authentication Codes, AMD codes do not require a secret key and have simpler encoding and decoding. Codes combining AMD codes and list-decoding are described in [18]. Applications of AMD codes for the design of non-malleable codes are presented in [19]. Algebraic manipulation correction codes are presented in [20]. The main contributions of this paper are as follows. We present

$$Q_V(y,e) = 2^{-m}|\{x \,|\, (y,x,f(y,x)) \in V, (y \oplus e_y, x \oplus e_x, f(y,x) \oplus e_f) \in V\}|. \quad (4)$$

lower bounds for the probability of error masking for systematic AMD codes (Section 2) and propose several new constructions of systematic AMD codes (Section 3) for a wide range of parameters k, m and r, which are generalizations of the construction shown in [17]. Some of the proposed codes are optimal or close to be optimal. We show the relationship between the proposed codes and classical codes such as the Generalized Reed-Muller codes and the Reed-Solomon codes (Section 2 and 3). We also describe in Section 4 an efficient encoding and decoding algorithm for the presented codes based on the multivariate Horner scheme.

The proposed codes can be used for many different applications such as robust secret sharing schemes, robust fuzzy extractors [17] and secure cryptographic devices resistant to fault injection attacks [21].

All the codes described in this paper are binary. Generalization to a nonbinary case is straightforward.

2 Definitions and Bounds for Algebraic Manipulation Detection Codes

Throughout the paper we denote by $\oplus$ the componentwise modulo two addition in $GF(q), q = 2^r$. All the results presented in the paper can be easily generalized to the case where $q = p^r$ (p is a prime).

A code V with codewords $(y, x, f(y,x))$, where $y \in GF(2^k), x \in GF(2^m)$ and $f(y,x) \in GF(2^r)$, will be referred to as a (k,m,r) code. We will assume that y is a k-bit information, x is an m-bit uniformly distributed random vector (generated by a random number generator) and $f(y,x)$ is an r-bit redundant portion of the message $(y,x,f(y,x))$.

Definition 2.1: (**Security Kernel**) For any (k,m,r) error detecting code V with the encoding function $f(y,x)$, where $y \in GF(2^k), x \in GF(2^m)$ and $f(y,x) \in GF(2^r)$, the **security kernel** K_S is the set of errors $e = (e_y, e_x, e_f), e_y \in GF(2^k), e_x \in GF(2^m), e_f \in GF(2^r)$, for which there exists y such that $f(y \oplus e_y, x \oplus e_x) \oplus f(y,x) = e_f$ is satisfied for all x.

$$K_S = \{e | \exists y, f(y \oplus e_y, x \oplus e_x) \oplus f(y,x) \oplus e_f = \mathbf{0}, \forall x\}. \quad (3)$$

For any error $e^* = (e_y^*, e_x^*, e_f^*) \in K_S, e^* \neq \mathbf{0}$, there exists y^* (the output of the device to-be-protected) such that for this y^* the error e^* is not detected for any choice of the random variable x (the probability of not detecting e^* for the information y^* is equal to 1). Thus to conduct a successful attack, it is sufficient for the attacker to inject $e^* \in K_S$ when the expected output is in the format of $(y^*, x, f(y^*, x))$.

We note that in many applications $e_y \neq 0$ is a necessary condition for an attacker to conduct a successful fault injection attack. However, for secure architectures such as the one shown in [9], [22], the integrity of not only the information bits but also the redundant bits of the codes can be critical. Thereby, to conduct a more general analysis, we do not impose $e_y \neq 0$ in the above definition of the security kernel.

For the case of communication channels we assume that an attacker can select any k-bit vector y as the information bits of a message $(y,x,f(y,x))$ and any error $e = (e_y, e_x, e_f)$ that distorts the message. For the case of computation channels, we assume the attacker can inject faults that manifest as $e \in K_S$ at the output of the device and select y for which e is always masked. Under the above attacker model for communication or computation channels, the attacker can always mount a successful attack (see Example 1.1). Thereby an AMD code that can provide a guaranteed error detecting probability under the above strong attacker model should have no errors in the security kernel except for the all zero vector in $GF(2^n)$, where $n = k + m + r$ is the length of the code.

Definition 2.2: A (k,m,r) error detecting code is called Algebraic Manipulation Detection (AMD) code iff $K_S = \{\mathbf{0}\}$, where $\mathbf{0}$ is the all zero vector in $GF(2^n)$, $n = k + m + r$.

Remark 2.1: The original definition of AMD codes in [17] is for both systematic and nonsystematic codes defined in any group. In this paper we consider binary systematic AMD codes, which is the most practical for hardware implementation. The above definition and all other results in this paper can be easily generalized for non-binary cases.

AMD codes $V = \{(y,x,f(y,x))\}$ have no undetectable errors no matter how the attacker select $e = (e_y, e_x, e_f)$ and y. AMD codes for the case $m = r$ and $k = br$ were introduced in [16] and were used in [17] for robust secret sharing schemes and for robust fuzzy extractors.

For a (k,m,r) code V, denote by $Q_V(y,e)$ the probability of missing an error e once y is fixed. Then $Q_V(y,e)$ can be computed as the fraction of random vectors x such that e is masked (see (4)) and $K_S = \{e | \exists y : Q_V(y,e) = 1\}$. The code V is an AMD code if and only if $Q_V(y,e) < 1$ for any y and any $e \neq 0$.

For a (k,m,r) AMD code $V = \{(y,x,f(y,x)),\ y \in GF(2^k),\ x \in GF(2^m),\ f(y,x) \in GF(2^r)\}$, for any given $y^* \in GF(2^k)$ and $e^* = (e_y^*, e_x^*, e_f^*)$, $e_y^* \in GF(2^k), e_x^* \in GF(2^m)$, $e_f^* \in GF(2^r)$, $f(y^* \oplus e_y^*, x \oplus e_x^*) \oplus e_f^*$ considered as functions of $x \in GF(2^m)$ should all be different.

Example 2.1: Let $k = m = tr$, $y = (y_0, y_1, \cdots, y_{t-1}), y_i \in GF(2^r)$ be the information digits and $x = (x_0, x_1, \cdots, x_{t-1}), x_i \in GF(2^r)$ be the random digits. Let $f(y,x) = x_0 \cdot y_0 \oplus x_1 \cdot y_1 \oplus \cdots \oplus x_{t-1} \cdot y_{t-1}$ be the encoding function, where all the operations are in $GF(2^r)$.

Suppose $e_y = \mathbf{0}$ and e_x, e_f are not both $\mathbf{0}$. The error

masking equation is

$$e_f = e_{x_0} y_0 \oplus e_{x_1} y_1 \oplus \cdots \oplus e_{x_{t-1}} y_{t-1}, \quad (5)$$

where $e_x = (e_{x_0}, e_{x_1}, \cdots, e_{x_{t-1}})$ and $e_{x_i} \in GF(2^r)$. For any e_x and e_f, there always exist y such that $e = (\mathbf{0}, e_x, e_f), e \neq \mathbf{0}$ will be masked for all x. Thereby, this code is not a AMD code. In this case, K_S contains all vectors $e = (\mathbf{0}, e_x, e_f)$.

Suppose $e_y = (e_{y_0}, e_{y_1}, \cdots, e_{y_{t-1}})$, $e_{y_i} \in GF(2^r)$ is not zero. Without loss of generality, let us assume $e_{y_0} \neq \mathbf{0}$. Then the monomial $e_{y_0} \cdot x_0$ will appear in the error masking equation $f(x \oplus e_x, y \oplus e_y) \oplus f(y, x) \oplus e_f = \mathbf{0}$. Since $e_{y_0} \neq \mathbf{0}$, for every e, y and $x_1, x_2, \cdots, x_{t-1}$, there is a unique solution for x_0. Thereby the error is masked with probability 2^{-r}.

We will now establish a relationship between binary AMD codes and classical non-binary codes with given Hamming distances. We will show that for any (k, m, r) AMD code V there exists a q-ary code C_V with $C_V = 2^{k+m+r}$ and $q = 2^r$ such that the Hamming distance of C_V will determine the maximal error masking probability $\max_{y,e\neq 0} Q_V(y, e)$ for the AMD code V. This relationship combined with the well known bounds for Hamming distances results in a necessary condition for the existence of AMD codes given k, m, r and lower bounds for the maximal probability of missing errors $Q(k, m, r) = \min_{V \in V_{k,m,r}} \max_{y,e\neq 0} Q(y, e)$ for the best AMD codes, where $V_{k,m,r}$ is the set of (k, m, r) error detecting codes (see Theorem 2.1 and Corollary 2.1 $\sim$ 2.4).

Let C be a q-ary code ($q = 2^r$) of length 2^m with an encoding function $f : GF(2^m) \to GF(2^r)$. Let us define the **orbit of** f by (6). We note that for any $f \in C$, $1 \leq |Orb(f)| \leq q2^m = 2^{m+r}$. If $|Orb(f)| = 2^{m+r}$, then for any e_x and e_f there exists x such that $f(x) \neq f(x \oplus e_x) \oplus e_f$ ($f(x)$ and $f(x \oplus e_x) \oplus e_f$ are different functions). Moreover, if $\varphi \notin Orb(f)$, then $Orb(\varphi) \bigcap Orb(f) = \emptyset$.

$$Orb(f) = \{\varphi | \varphi(x) = f(x \oplus e_x) \oplus e_f\}, \quad (6)$$

where $e_x \in GF(2^m), e_f \in GF(2^r)$.

Definition 2.3: We will say that a q-ary ($q = 2^r$) code C of length 2^m is a **code with full orbit** if for any $f \in C$, $|Orb(f)| = 2^{m+r}$ and $Orb(f) \subseteq C$.

The notion of codes with full orbit will be used in the lower bound for the probability of error masking (see Theorem 2.1). For a (k, m, r) error detecting code $V = \{(y, x, f(y, x))\}$, when y is fixed to be y^*, $f(y^*, x)$ is a function of x. Let us denote $f(y^*, x)$ by $f_{(y^*)}$. If an error $e = (0, e_x, e_f)$ is masked with probability 1, then $f_{(y^*)}(x \oplus e_x) \oplus e_f = f_{(y^*)}(x)$ for all x. As a result $|Orb(f_{(y^*)})| < 2^{m+r}$. The code C_V that $f_{(y^*)}$ belongs to is not a code with full orbit. The existence of a q-ary ($q = 2^r$) code C of length 2^m with full orbit is a necessary condition for the existence of a (k, m, r) AMD code (see the proof of Theorem 2.1).

Any q-ary code C of length 2^m with full orbit is a union of disjoint orbits of size $q2^m$. The size of C is a multiple of $q2^m$. We note that codes with full orbit are nonlinear and for any code C with full orbit, $\mathbf{0} \in GF(2^m)$ is not a codeword of C.

Example 2.2: Let C be a binary code of length 8 and Hamming distance 2 containing all vectors with an odd number of $1's$. Let $y = (y_0, y_1, y_2), y_i \in GF(2)$ and $f_{(y)}(x) = y_0 \cdot x_0 \oplus y_1 \cdot x_1 \oplus y_2 \cdot x_2 \oplus x_0 \cdot x_1 \cdot x_2$ is a nonlinear function of x with y as the coefficient. Since $f_{(y)}(x)$ is nonlinear, for any given e_x and e_f, there always exists x such that $f_{(y)}(x \oplus e_x) \oplus e_f \neq f_{(y)}(x)$, i.e. $f_{(y)}(x \oplus e_x) \oplus e_f$ and $f_{(y)}(x)$ are different functions. Thus $|Orb(f_{(y)})| = 16$ for any $y \in GF(2^3)$. C is a code with full orbit and $|C| = |\cup_{y \in GF(2^3)} Orb(f_{(y)})| = 128$.

The optimal AMD code minimizes $\max_{y,e\neq 0} Q_V(y, e)$ among all codes with the same parameters. Thus, the criterion we use to construct good AMD codes is

$$\min_{V \in V_{k,m,r}} \max_{y,e\neq 0} Q_V(y, e), \quad (7)$$

where $V_{k,m,r}$ is the set of all (k, m, r) error detecting codes.

Definition 2.4: An AMD code is optimal if it achieves the minimum possible worst error masking probability among all codes with the same k, m and r, i.e. $Q_V = max_{y\neq 0} Q_V(y, e) = min_{V \in V_{k,m,r}} Q_V$.

We note that the optimization criterion selected in this paper is different from the one shown in [17]. The computational complexity of the encoding function for AMD codes is determined by both m and r. In cryptographic applications, the m random digits can be generated by a random number generator (RNG), which is already integrated in most of the modern cryptographic devices. Since the RNG is also used for other purposes such as generating the random mask for countermeasures against power analysis attacks, the number of random digits available for AMD codes in every clock cycle may be limited. The above criterion was selected to maximize the security level of the cryptographic device given the number of available random digits in every clock cycle and the amount of hardware redundancy we can bear.

Let us discuss now the relationship between the maximum Hamming distance of q-ary ($q = 2^r$) full-orbit codes of length 2^m with 2^{k+m+r} codewords and the worst case error masking probability for the optimal (k, m, r) AMD codes.

Let $Q_V = \max_{y,e\neq 0} Q_V(y, e)$ and $Q(k, m, r) = \min_{V \in V_{k,m,r}} Q_V$. Denote by $\hat{d}_q(2^m, M)$ the maximum Hamming distance of a q-ary ($q = 2^r$) code of length 2^m with full orbit containing M codewords. We have

$$\hat{d}_q(2^m, M) \leq d_q(2^m, M), \quad (8)$$

where $d_q(2^m, M)$ is the maximum possible Hamming distance of a q-ary code with length 2^m and M codewords.

We next present a lower bound for $Q(k, m, r)$. The constructions of codes providing tight upper bounds for $Q(k, m, r)$ can be found in Section 3.

Theorem 2.1: For any (k, m, r) AMD code, where k is

the number of information bits, m is the number of random bits and r is the number of redundant bits,

$$\begin{aligned} Q(k,m,r) &= \min_{V\in V_{k,m,r}} \max_{y,e\neq 0} Q_V(y,e) \\ &\geq 1-2^{-m}d_q(2^m,M), \end{aligned} \tag{9}$$

where $d_q(2^m,M)$ is the maximum possible Hamming distance of a (not necessarily systematic) q-ary code C ($q=2^r$) with length 2^m and $M=|C|=2^{k+m+r}$ codewords.

Proof: Let V be a (k,m,r) AMD code composed of vectors $(y,x,f(y,x))$, where $y\in GF(2^k), x\in GF(2^m)$ and $f(y,x)\in GF(2^r)$. When y is fixed, f is a function of x. Let us denote this function by $f_{(y)}$. Since V is an AMD code, $f_{(y)}(x\oplus e_x)\oplus e_f$ is not the same as $f_{(y')}(x\oplus e'_x)\oplus e'_f$ for any y,y',e_x,e'_x,e_f,e'_f, assuming that elements of at least one of the pairs (y,y'), (e_x,e'_x) and (e_f,e'_f) are not equal. Thereby, for different y, e_x and e_f, $f_{(y)}(x\oplus e_x)\oplus e_f$ corresponds to 2^{k+m+r} different functions.

Let $C_V=\cup_{y\in GF(2^k)}Orb(f_{(y)})$ be a q-ary ($q=2^r$) code of length 2^m with full orbit. Then $|Orb(f_{(y)})|=2^{m+r}$, $|C_V|=2^{k+m+r}$ and $Q_V=max_{y,e\neq 0}Q(y,e)=1-2^{-m}d(C_V)$, where $d(C_V)$ is the Hamming distance of C_V. By (8) and (9) we have

$$\begin{aligned} Q(k,m,r) &= 1-2^{-m}\max_{V\in V_{k,m,r}} d(C_V) \\ &\geq 1-2^{-m}\hat{d}_q(2^m,M) \\ &\geq 1-2^{-m}d_q(2^m,M). \end{aligned} \tag{10}$$

□

The following Corollary follows directly from Theorem 2.1 and provides a necessary condition of the existence of (k,m,r) AMD codes.

Corollary 2.1: There is no AMD codes V with $k > r2^m-m-r$. ($Q(k,m,r)=1$ if $k>r2^m-m-r$.)

Proof: According to the proof of Theorem 2.1, for any given y, $|Orb(f_{(y)})|=2^{m+r}$. The 2^k orbits $Orb(f_{(0)}), Orb(f_{(1)}),\cdots Orb(f_{(2^k-1)})$ are non-overlapping. Thereby if there exists an (k,m,r) AMD code ($Q_V<1$), then $q^{2^m}\geq 2^{k+m+r}$, or equivalently $k\leq r2^m-m-r$. □

Remark 2.2: We note that the bound in Theorem 2.1 is much stronger than the trivial bound $Q(k,m,r)\geq 2^{-r}$. In fact, $Q(k,m,r)\geq 2^{-r}$ is equivalent to $d_q(2^m,2^k+m+r)\geq 2^m-2^{m-r}$, which is a sub-case of Theorem 2.1.

Theorem 2.1 shows the relationship between the worst case error masking probability Q_V for an AMD code V and the Hamming distance of the corresponding code C_V with full orbit. The exact value of $\hat{d}_q(2^m,M)$ is hard to derive. However, the Hamming distance of C_V should not exceed the maximum possible distance for a q-ary code with length 2^m and 2^{k+m+r} codewords, $q=2^r$. We note that $d_q(2^m,M)$ can be estimated by classical bounds from coding theory such as the Hamming bound, the Johnson bound, the Singleton bound, the Plotkin bound, etc [23].

When $d_q(2^m,M)$ is estimated by the Singleton bound, the lower bound for $Q(k,m,r)$ can be written in a compact form as it is shown in the following Corollary.

Corollary 2.2: For any (k,m,r) AMD code,

$$Q(k,m,r)\geq \lceil\frac{k+m}{r}\rceil 2^{-m}. \tag{11}$$

Proof: According to the Singleton bound, for any q-ary code with length n and distance d, $|C_V|\leq q^{n-d+1}$. For the code C_V in the proof of Theorem 2.1, $n=2^m$, $q=2^r$ and $|C_V|=2^{k+m+r}$. Therefore $2^{k+m+r}\leq 2^{r(2^m-d+1)}$, or equivalently $d\leq 2^m-\lceil\frac{k+m}{r}\rceil$. Then from (9), we have (11). □

The constructions of codes achieving the bound described above are shown in Corollary 3.1, 3.2 and 3.4.

The error masking equation of a (k,m,r) AMD code can be written as

$$f_{(y)}(x)\oplus f_{(y\oplus e_y)}(x\oplus e_x)\oplus e_f=\mathbf{0}. \tag{12}$$

When m is a multiple of r ($m=tr$), the left hand side of (12) is a function from $GF(q^t)$ to $GF(q)$, $q=2^r$. Let $x=(x_0,x_2,\cdots,x_{t-1})\in GF(q^t), x_i\in GF(q), 0\leq i\leq t-1$. It is shown in [24] that $\{x_0^{i_0}x_1^{i_1}\cdots x_{t-1}^{i_{t-1}}\}$, where $0\leq i_v\leq q-1, v=0,1,2,\ldots,q-1$, is a basis of the function space for functions from $GF(q^t)$ to $GF(q)$, i.e., (12) can always be written in a polynomial form composed of monomials $x_0^{i_0}x_1^{i_1}\cdots x_{t-1}^{i_{t-1}}$. Theorem 2.1 can be further improved as shown in the next two Corollaries.

Corollary 2.3: When $r=1$,

$$Q(k,m,1)\geq 1-2^{\lfloor log_2 d_2(2^m,M)\rfloor-m}, M=2^{k+r+1}. \tag{13}$$

Proof: When $r=1$, let s be the maximal degree of the left hand side (LHS) of (12) over all y and $e=(e_y,e_x,e_f)$ for the a AMD code V with given k and m. Then the LHS with degree s is a codeword of a binary Reed Muller code $RM_2(s,m)$ with length 2^m and Hamming distance 2^{m-s}. (For the definition and the properties of binary Reed Muller codes, please refer to [23].) The maximum possible error masking probability for the AMD code is equal to the maximum number of nonzero components in a codeword of $RM_2(s,m)$ divided by the length of the Reed Muller code 2^m. Thereby the error masking probability for the AMD code is at most $(2^m-2^{m-s})2^{-m}=1-2^{-s}$. We have

$$1-2^{-s}\geq Q(k,m,1)\geq 2^{-m}d_2(2^m,M), M=2^{k+m+1}. \tag{14}$$

or equivalently (s is an integer)

$$s\geq m-\lfloor log_2 d_2(2^m,M)\rfloor. \tag{15}$$

When the maximal degree of the error masking equations for the AMD code achieves the equality in the above equation, the code has the smallest possible $Q(k,m,1)$. Thus

$$Q(k,m,1)\geq 1-2^{\lfloor log_2 d_2(2^m,2^M)\rfloor-m}.$$

□

Corollary 2.4: For any k and m, $Q(k,m,1)\geq 0.75$.

Proof: Since for any $k > 0$ and m, $d_2(n = 2^m, M = 2^{k+m+1}) < 2^{m-1}$, we have

$$\lfloor log_2 d_2(2^m, M) \rfloor \leq m - 2.$$

According to (13), $Q(k, m, 1) \geq 0.75$. □

The constructions of codes achieving the bound described above are shown in Corollary 3.2.

Example 2.3: Let $k = m = 3$ and $r = 1$. According to (11), $Q(3, 3, 1) \geq \frac{6}{8}$. Let V be the code composed of all vectors $(y, x, f(y, x))$, where $y, x \in GF(2^3)$ and

$$f(y, x) = x_0 \cdot x_1 \cdot x_2 \oplus x_0 \cdot y_0 \oplus x_1 \cdot y_1 \oplus x_2 \cdot y_2, f(y, x) \in GF(2). \quad (16)$$

The error masking equation is $f(x \oplus e_x, y \oplus e_y) \oplus f(y, x) = e_f$, which is a polynomial of x with degree 2. The function on the left hand side of the error masking equation corresponds to a codeword of the second order binary Reed-Muller code $RM_2(2, 3)$ with 3 variables [23]. Any codeword of $RM_2(2, 3)$ has a Hamming weight of at least 2. Thus the number of solutions for the error masking equation is upper bounded by 6. V is a AMD code with $Q_V = \frac{6}{8}$. It follows from (11) that this code is optimal and $Q(3, 3, 1) = 0.75$. (The optimality of the code can also be directly derived from Corollary 2.4.)

Optimal (k, m, r) AMD codes attain the equality in (9) or (13) and minimize the worst case error masking probability among all codes with the same parameters.

Remark 2.3: We note that AMD codes V with Q_V close to 1 may still be very useful for channels with memories where errors tend to repeat themselves, e.g. for the protection of cryptographic hardware against fault injection attacks when errors have a high probability to repeat for several clock cycles (slow fault injection attacks and lazy channels). This assumption can be true for most of the modern fault injection mechanisms due to their limited timing resolutions [25], [26], [27], [28], [29], [30]. In this case a repeating error will be ultimately detected by AMD codes after it distorts several consecutive messages.

In the next section, we will present several general constructions of AMD codes. Some of the generated codes are optimal with respect to the lower bounds (9) or (11).

3 Constructions of Codes

In the previous Section we have seen that there is an one-to-one mapping between the (k, m, r) AMD codes and the q-ary ($q = 2^r$) codes C_V of length 2^m with full orbit and $|C_V| = 2^{m+k+r}$. In this Section we will use Generalized Reed-Muller codes of length 2^m to construct C_V and the corresponding AMD codes. These AMD codes are optimal or close to optimal for many k, m and r.

The codewords of a (k, m, r) AMD code V are in the format $(y, x, f(y, x))$, where $y \in GF(2^k), x \in GF(2^m)$ and $f(y, x) \in GF(2^r)$. When y is fixed, $f_{(y)}$ is a function of x. In the proof of Theorem 2.1, we have shown that the necessary condition for V to be an AMD code is that $f_{(y)}(x \oplus e_x) \oplus e_f$ cannot be the same function as $f_{(y')}(x \oplus e'_x) \oplus e'_f$ for any $y, y', e_x, e'_x, e_f, e'_f$, assuming elements in at least one of the pairs (y, y'), (e_x, e'_x) and (e_f, e'_f) are not equal.

To compute $Q_V(y, e)$ for the code V, the error masking equation $f(x \oplus e_x, y \oplus e_y) \oplus f(y, x) \oplus e_f = \mathbf{0}$ should be evaluated for all 2^m possible $x \in GF(2^m)$.

We will say that an AMD code $V = \{(y, x, f(y, x))\}$ is based on code C if the error masking polynomial $f(y \oplus e_y, x \oplus e_x) \oplus f(y, x) \oplus e_f$ is a codeword of C for all y, e_x, e_y and e_f. Let us re-write $f(y, x)$ as $f(y, x) = A(x) \oplus B(y, x)$, where $A(x)$ is independent of y. We next show that by selecting $A(x)$ and $B(y, x)$ based on different error detecting codes such as the Generalized Reed-Muller codes and the Reed-Solomon codes, we can construct good (and in many cases optimal) AMD codes for different k and different $Q_V = \max_{y, e \neq 0} Q_V(y, e)$ for given m and r.

3.1 Constructions of codes Based on the Generalized Reed-Muller Codes

Let $x = (x_0, x_1, \cdots, x_{t-1}), x_i \in GF(q)$, $q = 2^r$. A b^{th} order q-ary Generalized Reed-Muller code $GRM_q(b, t)$ [24] with t variables ($1 \leq b \leq t(q-1)$) consists of all codewords $(f(\mathbf{0}), f(\gamma^0), \cdots, f(\gamma^{q^t-2}))$, where $f(x)$ is a polynomial of t variables $x_0, x_1, \cdots x_{t-1}$ and γ is a primitive element of $GF(q^t)$. The degree of $f(x)$ is less or equal to b.

It is shown in [24] that the dimension of $GRM_q(b, t)$ is

$$k_{GRM_q(b,t)} = \sum_{j=0}^{t} (-1)^j \binom{t}{j} \binom{t + b - jq}{b - jq}, \quad (17)$$

where $q = 2^r$ and $\binom{i}{j} = 0$ when $j < 0$.

If $b = u(q-1) + v, 0 \leq v \leq q-2$. Then the distance of $GRM_q(b, t)$ is $d_{GRM_q(b,t)} = (q - v)q^{t-u-1}$ [24].

Suppose $b + 2 = \alpha(q-1) + \beta \leq t(q-1), 0 \leq \alpha \leq t, 0 \leq \beta \leq q-2$. Assume that b is odd when $t = 1$. Let

$$A(x) = \begin{cases} \bigoplus_{i=0}^{t-1} x_i^{b+2} & \text{if } \alpha = 0, b \text{ is odd;} \\ \bigoplus_{i=1}^{t-1} x_0 x_i^{b+1}, t > 1 & \text{if } \alpha = 0, b \text{ is even;} \\ \bigoplus_{i=0}^{t-1} x_i^{\beta} \prod_{j=1}^{\alpha} x_{|i+j|_t}^{q-1} & \text{if } \alpha \neq 0, \alpha \neq t; \\ \prod_{i=0}^{\alpha-1} x_i^{q-1} & \text{if } \alpha = t; \end{cases} \quad (18)$$

where $x_i \in GF(2^r)$, $|i + j|_t$ is the modulo t addition, $\bigoplus$ is the sum in $GF(2^r)$.

Let

$$B(y, x) = \bigoplus_{1 \leq j_0 + j_1 + \cdots + j_{t-1} \leq b+1} y_{j_0, j_1, \cdots, j_{t-1}} \prod_{i=0}^{t-1} x_i^{j_i}, \quad (19)$$

where $0 \leq j_i \leq q-1$, $y_{j_0, j_1, \cdots, j_{t-1}} \in GF(2^r), x_i \in GF(2^r)$, $\prod_{i=0}^{t-1} x_i^{j_i}$ is a monomial of $x_0, x_1, \cdots, x_{t-1}$ of a degree between 1 and $b+1$ and $\prod_{i=0}^{t-1} x_i^{j_i} \notin \Delta B(x)$, where $\Delta B(x)$ is defined by (20).

$$\Delta B(x) = \begin{cases} \{x_0^{b+1}, x_1^{b+1}, \cdots, x_{t-1}^{b+1}\} & \text{if } \alpha = 0, b \text{ is odd;} \\ \{x_1^{b+1}, x_0x_1^b, x_0x_2^b, \cdots, x_0x_{t-1}^b, t > 1\} & \text{if } \alpha = 0, b \text{ is even;} \\ \{x_i^\beta x_{|i+1|_t}^{q-2} \prod_{j=2}^{\alpha} x_{|i+j|_t}^{q-1}, 0 \le i \le t-1\} & \text{if } \alpha \neq 0. \end{cases} \quad (20)$$

We note it follows from (20) that when $\alpha = t$, $\Delta B(x) = \{x_i^{q-2} \prod_{j \neq i} x_j^{q-1}, 0 \le i \le t-1\}$.

Example 3.1: Let $r = 3, q = 8, t = 2$ and $b = 10$. Since $b + 2 = 12 = \alpha(q-1) + \beta$, we have $\alpha = 1$ and $\beta = 5$. By (18) and (20), we have $A(x) = x_0^5 x_1^7 \oplus x_0^7 x_1^5$ and $\Delta B(x) = \{x_0^5 x_1^6, x_0^6 x_1^5\}$. $A(x \oplus e_x) \oplus A(x) \oplus B(y \oplus e_y, x \oplus e_x) \oplus B(y, x)$ is always a non-zero polynomial of x that has a degree of at most 11 and corresponds to a codeword in $GRM_8(11, 2)$.

AMD codes can be constructed based on $A(x), B(y, x)$ and the Generalized Reed-Muller codes as shown in the next Theorem.

Theorem 3.1: Let $f(y, x) = A(x) \oplus B(y, x)$ be a q-ary polynomial with $y_{j_0, j_1, \cdots, j_{t-1}} \in GF(q)$ as coefficients and $x \in GF(q^t)$ as variables, where $1 \le b \le t(q-1) - 2, q = 2^r$ and $A(x), B(y, x)$ are as shown above. Suppose $b + 2 = \alpha(q-1) + \beta$ and $b + 1 = u(q-1) + v$, $0 \le \alpha, u \le t, 0 \le \beta, v \le q - 2$. Assume $b + 2 \neq t(q-1) - 1$ and b is odd when $t = 1$. Then the code V composed of all vectors $(y, x, f(y, x))$ is an AMD code with $m = tr$,

$$\begin{aligned} k &= (k_{GRM_q(b+1,t)} - t - 1)r \\ &= (\sum_{i=0}^{t} (-1)^i \binom{t}{i} \binom{t + b + 1 - iq}{b + 1 - iq} - 1 - t)r, \quad (21) \end{aligned}$$

and

$$\begin{aligned} Q_V &= 1 - d_{GRM_q(b+1,t)} 2^{-m} \\ &= 1 - (2^r - v)2^{-(u+1)r}. \quad (22) \end{aligned}$$

Thus

$$\begin{aligned} &Q((\sum_{i=0}^{t} (-1)^i \binom{t}{i} \binom{t + b + 1 - iq}{b + 1 - iq} - 1 - t)r, tr, r) \\ &\le 1 - (2^r - v)2^{-(u+1)r}. \quad (23) \end{aligned}$$

Proof: An error e is masked by V if and only if for all x

$$A(x \oplus e_x) \oplus A(x) \oplus B(y \oplus e_y, x \oplus e_x) \oplus B(y, x) \oplus e_f = \mathbf{0}. \quad (24)$$

1) If $e_x = \mathbf{0}$ and $e_y = \mathbf{0}$, the error is always detected unless e_f is also $\mathbf{0}$. If $e_x = \mathbf{0}$ and $e_y \neq \mathbf{0}$, the left hand side of the error masking equation (24) is a polynomial of degree from 1 to $b + 1$, which corresponds to a codeword of a $(b+1)^{th}$ order q-ary Generalized Reed-Muller code. Since $d_{GRM_q(b+1,t)} = (q - v)q^{t-u-1}$, there are at most $q^t - (q - v)q^{t-u-1}$ solutions for the error masking equation.
2) If $e_x \neq \mathbf{0}$, the left hand side of (24) does not contain any monomials of degree $b + 2$ due to the fact that $A(x)$ and $A(x \oplus e_x)$ have exactly the same monomials of degree $b + 2$. Moreover,
   a) If $\alpha = 0$ and b is odd, x_i^{b+1} appears in (24) iff x_i is distorted, $0 \le i \le t - 1$;
   b) If $\alpha = 0$ and b is even, x_1^{b+1} appears in (24) iff x_0 is distorted, $x_0 x_i^b$ appears in (24) iff x_i is distorted $1 \le i \le t - 1$;
   c) If $\alpha \neq 0$, since $b + 2 \neq t(q-1) - 1$, $x_i^\beta x_{|i+1|_t}^{q-2} \prod_{j=2}^{\alpha} x_{|i+j|_t}^{q-1}$ appears in (24) iff $x_{|i+1|_t}$ is distorted, $0 \le i \le t - 1$. (When $\alpha = t$, $x_i{}^{q-2} \prod_{j \neq i} x_j^{q-1}$ appears in (24) if x_i is distorted.)

   Thereby, (24) always contains monomials of degree $b + 1$, the left hand side of the error masking equation again is a codeword in $GRM_q(b + 1, t)$. Thus the number of solutions for the error masking equation is still upper bounded by $q^t - (q - v)q^{t-u-1}$.

Thus for any fixed y and e, the probability Q_V of error masking is upper bounded by

$$(q^t - (q - v)q^{t-u-1})q^{-t} = 1 - (2^r - v)2^{-(u+1)r}.$$

The left hand side of (24) contains monomials of a degree from 1 to $b+1$ except for the t monomials from $\Delta B(x)$. Hence the number of different monomials in $B(y, x)$ is

$$k_{GRM_q(b+1,t)} - 1 - t = \sum_{i=0}^{t} (-1)^i \binom{t}{i} \binom{t + b + 1 - iq}{b + 1 - iq} - 1 - t. \quad (25)$$

The number, k, of bits in y is equal to the number of monomials in $B(y, x)$ multiplied by r, which is

$$(\sum_{i=0}^{t} (-1)^i \binom{t}{i} \binom{t + b + 1 - iq}{b + 1 - iq} - 1 - t)r. \quad (26)$$

□

Example 3.1 (Continued) For the code shown in Example 3.1, $k = 55 \times 3 = 165$. Since $b = 10 = u(q-1) + v, q = 8$, we have $u = 1$ and $v = 3$. The worst case error masking probability is $Q_V = 1 - 5 \times 2^{-6}$. Thus by (11), $1 - 7 \times 2^{-6} \le Q_V(165, 6, 3) \le 1 - 5 \times 2^{-6}$.

We will show next that the proposed AMD codes are optimal or close to be optimal (providing for minimum Q_V) for many combinations of k, m and r.

Corollary 3.1: When $b = t(q-1) - 2, q = 2^r$, codes generated by Theorem 3.1 are optimal. We have

$$Q(2^{tr} r - tr - 2r, tr, r) = 1 - 2^{-tr+1}. \quad (27)$$

Proof: According to (11), $Q(2^m r - m - 2r, m, r) \ge 1 - 2^{-m+1}$, where $m = tr$. The number, k, of information bits for the AMD code V generated by Theorem 3.1 is

$(q^t - t - 2)r$. Thus, we have

$$b + 1 = t(q-1) - 1 = (t-1)(q-1) + q - 2.$$

Thereby $u = t - 1$ and $v = q - 2$. The worst case error masking probability for V is

$$Q_V = 1 - (2^r - (q-2))2^{-tr} = 1 - 2^{-tr+1}.$$

The code is optimal with respect to the lower bound (11). □

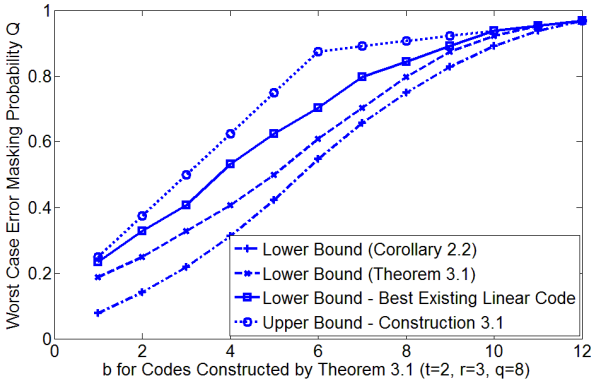


Fig. 2: Lower bounds and upper bounds for AMD codes with $t = 2, r = 3, q = 8$ and $1 \leq b \leq 12$. Lower bound (Corollary 2.2) derives $d_q(2^m, M)$ using Singleton bound. Lower bound (Theorem 2.1) derives $d_q(2^m, M)$ using upper bounds given in [31]. Lower bound - Best Existing Linear Code derives $d_q(2^m, M)$ based on the best available q-ary linear codes with length 2^m and size M.

The tightness of the lower bound given by Theorem 2.1 is strongly correlated to the tightness of existing classical upper bounds for the Hamming distance of error correcting codes. Figure 2 shows the lower bounds on the worst case error masking probability Q given by Theorem 2.1 and Q_V for codes constructed by Theorem 3.1 for $t = 2, r = 3, q = 8$ and $1 \leq b \leq 12$. When $d_q(2^m, M)$ in Theorem 2.1 is derived from the Singleton bound (Corollary 2.2), codes constructed by Theorem 3.1 are not very close to the lower bound except for $t = 11$ and $t = 12$ where the codes are optimal. As stronger upper bounds for Hamming distance are used to derive $d_q(2^m, M)$, codes constructed by Theorem 3.1 become closer and closer to the lower bound. (For a summary of upper bounds for Hamming distance of linear codes, please refer to [31].)

We note that in the literature the best available error correcting codes usually cannot achieve the upper bound for the Hamming distance [31]. If $d_q(2^m, M)$ is derived from the maximum Hamming distance of existing q-ary codes with length 2^m and size M, the codes constructed by Theorem 3.1 become even closer to the lower bound (see Figure 2). Generally speaking, the optimality of constructions of AMD codes based on generalized Reed-Muller codes is related to the optimality of Reed-Muller codes. For parameters where AMD codes based on GRM_q codes are non-optimal, better AMD codes can be constructed in a similar way if codes with larger Hamming distance than GRM_q codes exist.

More cases where codes constructed by Theorem 3.1 will be shown in the left part of the Section.

3.1.1 *Special Case:* $r = 1$

For this case the dimension of a $(b+1)^{th}$ order binary Reed-Muller code of t variables is $k_{RM_2(b+1,t)} = \sum_{i=0}^{b+1} \binom{t}{i}$ $(t = m)$ [23]. The distance of $RM_2(b+1, t)$ is $d_{RM_2(b+1,t)} = 2^{t-b-1}$. As a result, the dimension of the resulting AMD code V constructed by Theorem 3.1 is $k = \sum_{i=0}^{b+1} \binom{t}{i} - t - 1$. The worst case error masking probability of the code is $Q_V = 1 - 2^{-(b+1)}$.

Example 3.2: Suppose $m = 7$ and $r = 1$. Let $b = 1$ and

$$f(y, x) = x_0 \cdot x_1 \cdot x_2 \oplus x_3 \cdot x_4 \cdot x_5 \oplus x_0 \cdot x_3 \cdot x_6 \oplus \sum_{i=0}^{6} x_i \cdot y_i. \quad (28)$$

Because of the term $x_0 \cdot x_1 \cdot x_2 \oplus x_3 \cdot x_4 \cdot x_5 \oplus x_0 \cdot x_3 \cdot x_6$, $f(y \oplus e_y, x \oplus e_x) \oplus f(y, x) \oplus e_f$ is always a polynomial of degree 2, which is a codeword of $RM_2(2, 7)$. The distance of $RM_2(2, 7)$ is 32. The worst case error masking probability of the resulting AMD code is $Q_V = 0.75$. since $d_2(n = 128, |C| = 512) = 56$, the code is optimal according t o Corollary 2.4. (The optimality of the code can also be derived from (13).)

Corollary 3.2: When $q = 2$, the code V generated by Theorem 3.1 is a $(\sum_{i=0}^{b+1} \binom{t}{i} - t - 1, t, 1)$ AMD code with $Q_V = 1 - 2^{-(b+1)}$. The code is optimal when $b = 1$ or $b = t - 2$.

Proof: Corollary 3.2 follows from Corollary 2.4 (for the case $b = 1$) and Corollary 3.1 (for the case $b = t - 2$). □

Remark 3.1: When $r = 1 (q = 2)$ and $b = 1$, the code V generated by Theorem 3.1 is an optimal AMD code with $k = \binom{t}{2}$ and $Q = 0.75$. Removing codewords from an AMD code will not increase the worst case error masking probability Q of the code. Thereby, for all $k < \binom{t}{2}$, an AMD code with the same m, r and $Q = 0.75$ can be constructed by deleting some codewords from V. According to Corollary 2.4, the new code is also an optimal AMD code.

3.1.2 *Special Case:* $b \leq q - 3$

Another special case of Theorem 3.1 is the case $b \leq q-3$. In this case $k_{GRM_q(b+1,t)} = \binom{t+b+1}{t}$ and $d_{GRM_q(b+1,t)} = (q-b-1)q^{t-1}$ [24]. The dimension of the resulting AMD code is $(\binom{t+b+1}{t} - 1 - t)r$. The worst case error masking probability is $(b+1)2^{-r}$.

Corollary 3.3: Assume b is odd when $t = 1$. When $b \leq q - 3$, the code V generated by Theorem 3.1 is a $((\binom{t+b+1}{t} - 1 - t)r, tr, r)$ AMD code with $Q_V = (b+1)2^{-r}$.

Proof: By Theorem 3.1, k and Q_V of the AMD code V can be easily derived from the parameters of $GRM_q(b+1, t)$ for $b \leq q - 3$, $q = 2^r$. □

When $b = 1$ $B(y, x)$ is the quadratic form $x_0 \cdot y_0 \oplus x_1 \cdot y_1 \oplus \cdots \oplus x_{t-1} \cdot y_{t-1}$, where all the operations are in $GF(2^r)$. If e_y is always nonzero, let $A(x) = 0$ and $f(y, x) = B(y, x)$. Without lost of generality, assume $e_{y_0} \neq 0$. Then the error masking equation can be written as

$$x_0 \cdot e_{y_0} = F(y, x_1, x_2, \cdots x_{t-1}, e_y, e_x, e_f), \tag{29}$$

where F is a function independent of x_0. For any given y, e_y, e_x and e_f, there is at most one x_0 satisfying the above equation. Thereby the worst case error masking probability is q^{-1}. The construction of AMD codes does not require the term $A(x)$ when e_y is always nonzero.

3.1.3 Special Case: $t = 1$ [16], [17]

When $t = 1$ and b is odd, $A(x) = x^{b+2}$ and $B(y, x) = x \cdot y_0 \oplus x^2 \cdot y_1 \oplus \cdots \oplus x^b \cdot y_{b-1}$. The code generated by Theorem 3.1 coincides with the construction shown in [16], [17]. For this code, $k \leq r(q-3) = r(2^r - 3)$.

Corollary 3.4: [16], [17] When $b \leq q-3$ is an odd number, the code V composed of all vectors $(y, x, f(y, x))$, where $y \in GF(q^{bt}), x \in GF(q), q = 2^r$ and $f(y, x) = x^{b+2} \oplus x \cdot y_0 \oplus x^2 \cdot y_1 \oplus \cdots x^b \cdot y_{b-1}, f(y, x) \in GF(q)$, is an optimal (br, r, r) AMD code with $Q_V = \max_{y, e \neq 0} Q_V(y, e) = (b+1)2^{-r}$. Thereby, $Q(br, r, r) = (b+1)2^{-r}$.

Proof: For codes generated by Corollary 3.4, $m = r$, $k = br$ and $Q_V = (b+1)2^{-r}$. According to Corollary 2.2, $Q(k, m, r) \geq \lceil (k+m) r^{-1} \rceil 2^{-m}$. Thereby we have $Q(br, r, r) = (br + r) r^{-1} 2^{-m} = (b+1)2^{-r}$. □

Remark 3.2: One limitation of Corollary 3.4 is that b can only be an odd number when the characteristic of the field $GF(q)$ is 2. Otherwise, $A(x \oplus e_x)$ for $A(x) = x^{b+2}$ and $e_x \neq \mathbf{0}$ does not contain any monomial of degree $b+1$. The resulting code is not a secure AMD code as pointed out in [17]. When b is even, $A(x)$ can be chosen as x^{b+3}. In this case, $Q_V = (b+2)2^{-r}$.

Remark 3.3: When $t = 1$, the left hand side of the error masking equation $f(y \oplus e_y, x \oplus e_x) \oplus f(y, x) \oplus e_f = \mathbf{0}$ is a codeword of an extended q-ary $(q, b+2, q-b-1)$ Reed-Solomon code, $q = 2^r$ [23].

When $t > 1$, codes V generated by Theorem 3.1 may have a larger number of codewords than codes generated by Corollary 3.4 ($t = 1$), assuming the two codes have the same Q_V and the same r.

Example 3.3: Suppose $r = 16$, $Q_V = 2^{-14}$. Then for $t = 1$ and $b = 3$, for codes generated by Corollary 3.4, the maximum number of codewords is $2^{br} = 2^{48}$. When $t > 1$, the maximum number of codewords for codes generated by Theorem 3.1 depends not only on b but also on t. When $t = 2$, for example, the number of codewords of codes generated by Theorem 3.1 can be $2^{(\binom{t+b+1}{t} - 1 - t)r} = 2^{192}$.

We note that the lower bounds for $Q(k, m, r)$ presented in Section 2 can be further improved for cases where constructions based on Generalized Reed-Muller codes are available.

Theorem 3.2: Let $k \leq (\sum_{i=0}^{t} (-1)^i \binom{t}{i} \binom{t+s-iq}{s-iq} - 1 - t)r$, and $m = tr$, where $q = 2^r$. Let $s = u(q-1) + v, 0 \leq u \leq t-1, 0 \leq v \leq q-2$. Then

$$Q(k, tr, r) \geq \min_{1 \leq j \leq u+1} (1 - 2^{-jr} \lfloor d_q(2^m, 2^{m+k+r}) 2^{-m+jr} \rfloor), \tag{30}$$

where $d_q(2^m, 2^{m+k+r})$ is the maximal distance of q-ary codes with length 2^m and 2^{m+k+r} codewords.

Proof: When $k \leq (\sum_{i=0}^{t} (-1)^i \binom{t}{i} \binom{t+s-iq}{s-iq} - 1 - t)r$ and $m = tr$, the AMD code can be constructed based on Generalized Reed-Muller codes as described in Theorem 3.1. The LHS of the error masking equation $f(y, x) \oplus f(y \oplus e_y, x \oplus e_x) \oplus e_f = 0$ can always be written as a monomial of degree at most s. For any specific $e^* = (e_y^*, e_x^*, e_f^*)$ and y^*, let $s^* = u^*(q-1) + v^*$ be the degree of the LHS of the error masking equation. Following the proof of Theorem 3.1, we know that this error is masked with a probability Q^* of at most $1 - (2^r - v^*)2^{-(u^*+1)r}$, i.e. $Q^* \leq 1 - (2^r - v^*)2^{-(u^*+1)r}$. By the definition of $Q(k, m, r)$, we have

$$Q(k, m, r) \geq \max_{u^*, v^*} Q^* = 1 - (2^r - v^*)2^{-(u^*+1)r}. \tag{31}$$

On the other hand, $\max Q^*$ should be still larger or equal to the lower bound of $Q(k, m, r)$ given by (9). Thus

$$1 - (2^r - v^*)2^{-(u^*+1)r} \geq 1 - 2^{-m} d_q(2^m, 2^{m+k+r}), \tag{32}$$

or equivalently

$$v^* \geq 2^r - 2^{(u^*+1)r-m} d_q(2^m, 2^{m+k+r}). \tag{33}$$

Since v^* is an integer, we have

$$v^* \geq 2^r - \lfloor 2^{(u^*+1)r-m} d_q(2^m, 2^{m+k+r}) \rfloor. \tag{34}$$

From (31) and (34), we have

$$Q(k, m, r) \geq 1 - 2^{-(u^*+1)r} \lfloor 2^{(u^*+1)r-m} d_q(2^m, 2^{m+k+r}) \rfloor. \tag{35}$$

Since $0 \leq u^* \leq u$, we have the lower bound (30). □

The lower bound given by Theorem 3.2 is stronger than the lower bound described in Theorem 2.1. However, Theorem 3.2 is only valid when $m = tr$ and

$$k \leq (\sum_{i=0}^{t} (-1)^i \binom{t}{i} \binom{t+s-iq}{s-iq} - 1 - t)r.$$

In some cases, AMD codes based on Generalized Reed-Muller codes are optimal AMD codes achieving the equality of (30) as shown in the following example.

Example 3.4: Let $r = 3$, $t = 2$ and $s = 12$. Then the AMD code V constructed by Theorem 3.1 has $q = 8$, $b = 11$ and

$$k = 3(\sum_{i=0}^{2} (-1)^i \binom{14 - 8i}{12 - 8i} - 1 - 2) = 174. \tag{36}$$

For this code $u = 1$ and $v = 5$. According to Theorem 3.1, we hvae $Q_V = 61 \cdot 2^{-6}$. Thereby $Q(174, 6, 3) \leq 61 \cdot 2^{-6}$. On the other hand, since $d_8(8^2, 8^{61}) = 3$, from (30) we

have

$$\begin{aligned} Q(174,6,3) &\geq \min(1-2^{-3}\lfloor d_8(8^2,8^{61})2^{-3}\rfloor, \\ &\quad 1-2^{-6}\lfloor d_8(8^2,8^{61})\rfloor) \\ &= 61\cdot 2^{-6}. \end{aligned} \tag{37}$$

Thus $Q(174,6,3)=61\cdot 2^{-6}$ an the AMD code constructed by Theorem 3.1 is optimal.

Corollary 3.5: Let $k \leq (\binom{t+s}{t}-1-t)r$, where $q=2^r$ and $s \leq q-2$. Then

$$Q(k,tr,r) \geq 1-2^{-r}\lfloor d_q(2^m,2^{m+k+r})2^{-m+r}\rfloor. \tag{38}$$

Proof: The above corollary follows directly from Theorem 3.2 ($j=1$ in (30)). □

Corollary 3.6: If $k \leq (\binom{t+2}{t}-1-t)r$, then $Q(k,tr,r)=2^{-r+1}$.

Proof: The upper bound $Q(k,tr,r) \leq 2^{-r+1}$ follows from Corollary 3.3. Since $A(n,(q-1)nq^{-1})=qd$, where $d=(q-1)nq^{-1}$ and $A(n,d)$ is the maximal number of codewords given the length n and the distance d [32], we have

$$\begin{aligned} A(q^t,(q-1)q^{t-1}) &= (q-1)q^t < q^{t+1} \\ &= 2^{m+r} < 2^{k+m+r},\ (k \geq 1). \end{aligned} \tag{39}$$

Thereby, $\lfloor d_q(2^m,2^{m+k+r})2^{-m+r}\rfloor \leq q-2$. From Corollary 3.5, we have $Q(k,tr,r) \geq 2^{-r+1}$. □

It follows from Corollary 3.6 that when $b=1$, the AMD codes constructed by Theorem 3.1 are optimal. In this case the error masking probability for AMD codes decreases exponentially as the number of redundant bits r increases.

Example 3.5: Let $r=3, t=2$ and $b=1$. The code constructed by Theorem 3.1 has $k=9$, $m=6$, $q=8$ and $Q(9,6,3) \leq 2^{-2}$. Since $d_8(64,8^6) \leq 52$. By Corollary 3.5 we have $Q(9,6,3) \geq 1-6\cdot 2^{-3}=2^{-2}$. Thereby $Q(9,6,3)=2^{-2}$ and the code generated by Theorem 3.1 is optimal.

When y is fixed, the error masking probability for an error e is equal to the fraction of $x's$ that satisfy the error masking equation. The distribution of the error masking probability when both y and e are fixed for the AMD code described above is shown in Figure 3. Most of the errors are masked by less than 10 $x's$ resulting in a error masking probability of smaller than 0.15. (The total number of x is $2^m=64$.) More than 40% of errors are masked by a probability close to 0.1. The portion of errors masked by a probability of $Q_V=0.25$ is very small.

For AMD codes generated by Theorem 3.1, k and m are both multiples of r. We will now present three modification methods, which can largely increase the flexibility of parameters of the resulting AMD codes.

Theorem 3.3: Suppose there exists an (k,m,r) AMD code generated by Theorem 3.1 with $r \geq 1$, $m=tr$, $k=sr$ and $Q_V=\max_{y,e\neq 0} Q_V(y,e)$.

1) For the same r,m and $r \leq k < sr$, a shortened AMD code with the same Q_V can be constructed by appending $0's$ to y so that $(\mathbf{0},y) \in GF(2^{sr})$ and then apply the same encoding procedure as for the (sr,tr,r) code.
2) For the same m,k and $1 \leq r' < r$, an AMD code can be constructed by deleting $r-r'$ redundant bits from each codeword of the original (k,m,r) code. The maximum error masking probability of the resulting code will be $\min\{Q_V 2^{r-r'},1\}$.
3) Suppose there exists a (k_1,m,r_1) AMD code V_1 with $\max_{y,e\neq 0} Q_{V_1}(y,e) = Q_{V_1}$ and another (k_2,m,r_2) AMD code V_2 with $\max_{y,e\neq 0} Q_{V_2}(y,e) = Q_{V_2}$. By computing the redundant bits of the two codes separately and then concatenating them, we can construct a (k_1+k_2,m,r_1+r_2) AMD code with $Q_V \leq \max\{Q_{V_1},Q_{V_2}\}$.

Proof:

1) For codes constructed by Theorem 3.1, the error masking polynomial $f(y\oplus e_y,x\oplus e_x)\oplus f(y,x)\oplus e_f$ has a degree at most $b+1$, where $x=(x_0,x_1,\cdots,x_{t-1})$ is a variable and y, e_y,e_x and e_f are coefficients. Modifications of coefficients do not change the maximum possible degree of the polynomial thus do not change the maximum number of solutions for the error masking equation.
2) For the (sr,tr,r) AMD code with $Q_V=\max_{y,e} Q_V(y,e)$, every fixed e_y,e_x,e_f and y is masked by no more than $Q_V 2^m$ different x. After deleting $r-r'$ bits from the values of the function $f(y,x)$, the vectors (y,x) which previously mapped to $f(y,x)$ that are different in the deleted $r-r'$ bits will now map to the same value of the redundant bits. Thereby, when $r-r'$ bits are deleted, for any fixed e_y,e_x,e_f and y, the error is masked by at most $\min\{Q_V 2^{m+r-r'},2^m\}$ different $x's$.
3) For the concatenated (k_1+k_2,m,r_1+r_2) AMD code V, codewords are

$$(y_1,y_2,x,f_1(y_1,x),f_2(y_2,x)),$$

where $y_1 \in GF(2^{k_1}), y_2 \in GF(2^{k_2}), x \in GF(2^m)$,

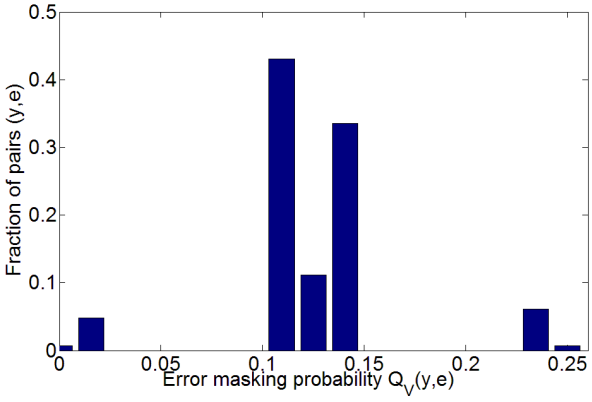


Fig. 3: The distribution of the error masking probability $Q_V(y,e)$ for the AMD code in Example 3.5 with $r=3, t=2$ and $b=1$.

$f_1(y_1, x) \in GF(2^{r_1})$ and $f_2(y_2, x) \in GF(2^{r_2})$. For any $y = (y_1, y_2)$ and any error $e = (e_{y_1}.e_{y_2}, e_x, e_{f_1}, e_{f_2})$, $e_{y_1} \in GF(2^{k_1})$, $e_{y_2} \in GF(2^{k_2})$, $e_x \in GF(2^m)$, $e_{f_1} \in GF(2^{r_1})$, $e_{f_2} \in GF(2^{r_2})$, denote $N(y, e)$ a number of $x's$ satisfying simultaneously the following two error masking equations

$$\begin{cases} f_1(y_1 \oplus e_{y_1}, x \oplus e_x) \oplus f_1(y_1, x) \oplus e_{f_1} = \mathbf{0} \\ f_2(y_2 \oplus e_{y_2}, x \oplus e_x) \oplus f_2(y_2, x) \oplus e_{f_2} = \mathbf{0} \end{cases} \tag{40}$$

Suppose $Q_{V_1} \geq Q_{V_2}$, then by the definition of the error masking probability Q_V, when $e_{y_2} = e_x = e_{f_2} = 0$, we have $\max_{y,e\neq 0} N(y, e) \leq 2^m Q_{V_1} = 2^m \max\{Q_{V_1}, Q_{V_2}\}$. Thereby, $Q_V \leq 2^{-m} \max_{y,e\neq \mathbf{0}} N(y, e) \leq \max\{Q_{V_1}, Q_{V_2}\}$.

□

Concatenation of L copies of a (k, m, r) AMD code constructed by Theorem 3.1 generates a (k', m', r') code with $k' = Lk, m' = m$ and $r' = Lr$. According to the Singleton bound,

$$Q(Lk, m, Lr) \geq \lceil \frac{Lk + m}{Lr} \rceil 2^{-m}. \tag{41}$$

When $b \leq q - 3$, from Corollary 3.3 we have

$$Q(Lk, m, Lr) \leq (b + 1)2^{-r}.$$

Thus

$$\lceil \frac{Lk + m}{Lr} \rceil 2^{-m} \leq Q(Lk, m, Lr) \leq (b + 1)2^{-r}, b \leq q - 3. \tag{42}$$

Corollary 3.7: Let V be an optimal (k, m, r) AMD code with $k = sr, m \leq r$ and $Q_V = \lceil \frac{k+m}{r} \rceil 2^{-m}$. Then for any L, the (Lk, m, Lr) code V' obtained by concatenation of L copies of V is also optimal.

Proof: By part 3 of Theorem 3.3, we have $Q_{V'} \leq Q_V = \lceil \frac{k+m}{r} \rceil = (s+1)2^{-m}$. On another hand by (11), we have $Q_{V'} \geq \lceil \frac{Lk+m}{Lr} \rceil 2^{-m} = \lceil s + \frac{m}{Lr} \rceil = (s + 1)2^{-m}$. □

The concatenation of AMD codes based on $GRM_q(b+1, 1)$ is optimal for $b \leq q-3$ and $Q(Lbr, r, Lr) = (b+1)2^{-r}$.

To end the section, we summarize cases the when codes constructed by Theorem 3.1 are optimal in the Table 1.

3.2 Constructions of Codes Based on Products of Generalized Reed-Muller Codes

Theorem 3.4: Let $C_{V_i}, 1 \leq i \leq L$ be a $(b_i + 1)^{th}$ order q-ary Generalized Reed-Muller code defined over t_i variables with dimension k_i and distance d_i, $q = 2^r$. Let V_i be an AMD code constructed based on C_{V_i} with the encoding function $f_i(y, x) = A_i(x) \oplus B_i(y, x)$ as shown in (18) - (20) in Theorem 3.1. Let $A(x) = \bigoplus_{i=1}^{L} A_i(x)$ and

$$B(y, x) = \bigoplus_{P_1, P_2, \cdots, P_L} y_{P_1, P_2, \cdots, P_L} \prod_{i=1}^{L} P_i, \tag{43}$$

where P_i is a polynomial of the t_i variables in C_{V_i}, $deg(P_i) \leq b + 1, P_i \notin \Delta B_i(x)$ and $\prod_{i=1}^{L} P_i$ is not a constant. Then code V defined by $f(y, x) = A(x) \oplus B(y, x)$ is a (k, m, r) AMD code V with $m = r \sum_{i=1}^{L} t_i$,

$$k = (\prod_{i=1}^{L} (k_i - t_i) - 1)r, \tag{44}$$

and

$$Q_V = 1 - 2^{-r \sum_{i=1}^{L} t_i} \prod_{i=1}^{L} d_i. \tag{45}$$

Proof: The error masking polynomial $f(y \oplus e_y, x \oplus e_x) \oplus f(y, x) \oplus e_y$ is a non-zero codeword of the product of $C_{V_i}, 1 \leq i \leq L$. The distance d of the product code is $\prod_{i=1}^{L} d_i$. Hence Q_V for the AMD code is $Q_V = 1 - d2^{-m} = 1 - 2^{-r \sum_{i=1}^{L} t_i} \prod_{i=1}^{L} d_i$. By (19) and (20), the number of P_i such that $deg(P_i) \leq b + 1$ and $P_i \notin \Delta B_i(x)$ is $k_i - t_i$. Thus the number of monomials in $B(y, x)$ is $\prod_{i=1}^{L} (k_i - t_i) - 1$. ($\prod_{i=1}^{L} P_i$ is not a constant.) The dimension of the AMD code V is equal to the number of monomials in $B(y, x)$ multiplied by r, which is $(\prod_{i=1}^{L} (k_i - t_i) - 1)r$. □

In the previous Section we've seen that the left hand side of the error masking equation for codes generated by Corollary 3.4 (special case of Theorem 3.1 when $t = 1$) is a codeword from a q-ary extended Reed-Solomon code with length 2^m and dimension $b+2$. When $t_i = 1, 1 \leq i \leq L$, the AMD codes generated by Theorem 3.4 are based on the product of L q-ary extended Reed-Solomon codes (PRS) [33]. The construction and the parameters of AMD codes based on the extended PRS code are shown in the next Corollary.

Corollary 3.8: When $t = 1$, the AMD code V generated by Theorem 3.4 are based on the extended PRS codes. Suppose each extended Reed-Solomon code has dimension $b + 2$ and length $q = 2^r, q \geq b + 3$. Let

$$A(x) = x_1^{b+2} \oplus x_2^{b+2} \oplus \cdots \oplus x_L^{b+2}. \tag{46}$$

Let

$$B(y, x) = \bigoplus_{s_1=0}^{b} \cdots \bigoplus_{s_L=0}^{b} y_{s_1, \cdots, s_L} \prod_{i=1}^{L} x_i^{s_i}, \quad (s_1, \cdots, s_t) \neq \mathbf{0}. \tag{47}$$

The resulting AMD code V is a $(((b + 1)^L - 1)r, Lr, r)$ code with

$$Q_V = \max_{y,e\neq 0} Q_V(y, e) = 1 - 2^{-Lr}(2^r - b - 1)^L. \tag{48}$$

Proof: The Corollary can be easily proved by substituting the parameters of the extended Reed-Solomon codes into (44) and (45). □

Example 3.6: Let $r = 3, L = 2$ and $b = 3$. For the AMD code V generated by Corollary 3.8, $m = 6$ and $k = ((b + 1)^L - 1)r = 45$. Each extended Reed-Solomon (RS) code has Hamming distance 5. For the extended PRS code, $d_{PRS} = 25$. Thereby the worst case error masking probability of the $(45, 6, 3)$ AMD code is $Q_V = 1 - 25 \cdot 2^{-6} = 39 \cdot 2^{-6}$.

For codes generated by Corollary 3.3, the worst case error masking probability is $Q_1 = (b_1 + 1)2^{-r}$. For codes

TABLE 1: Optimality of (k, m, r) AMD codes constructed by Theorem 3.1

k	m	r	Q_V	Optimality
$2^{tr}r - tr - 2r$	tr	r	$1 - 2^{-tr+1}$	Optimal (Corollary 3.1)
$\sum_{i=0}^{b+1} \binom{t}{i} - t - 1$	t	1	$1 - 2^{-(b+1)}$	Optimal when $b = 1$ or $b = t - 2$ (Corollary 3.2)
$(\binom{t+b+1}{t} - t - 1)r$	tr	r	$(b+1)2^{-r}$	Optimal when $t = 1$ (Corollary 3.4) or $b = 1$ (Corollary 3.6))

generated by Corollary 3.8, $Q_2 = 1 - 2^{-Lr}(2^r - b_2 - 1)^L$. Suppose the two codes have the same r and $Q_1 = Q_2$.

Let $b_1 + 1 = 2^r - u$, where $u \geq 2$. Then it can be easily proved that

$$b_2 + 1 = 2^r - 2^r(\frac{u}{2^r})^{\frac{1}{L}} = 2^r - 2^{(1-\frac{1}{L})r}u^{\frac{1}{L}}.$$

As it is illustrated by the following example, when r is large and b_1 (and b_2) is close to 2^r, the number of information bits for codes generated by Corollary 3.8 can be much larger than for codes generated by Corollary 3.3.

Example 3.7: Let $r = 8, q = 2^r = 256$, $u = 4$ and $m = 16$. For codes generated by Corollary 3.3, $t = 2$, $b_1 + 1 = 2^r - u = 252$, $k = (\binom{t+b_1+1}{t} - 1 - t)r = 32,131 \times 8$ bits. For codes generated by Corollary 3.8, $L = 2$, $b_2 + 1 = 2^r - 2^{(1-\frac{1}{L})r}u^{\frac{1}{L}} = 224$, $k = ((b+1)^L - 1)r = 50,175 \times 8$ bits. These two codes have the same worst case error masking probability Q_V. However, the number of information bits for the AMD code based on the extended PRS code is much larger than that based on the Generalized Reed-Muller code.

4 Encoding and Decoding Complexity for AMD Codes

In this section, we estimate the hardware complexity for the encoders and decoders for AMD codes based on q-ary Generalized Reed-Muller codes (Theorem 3.1). The hardware complexity for the encoders and decoders for AMD codes based on the product of GRM codes can be estimated in a similar way.

It is well known that a multivariate polynomial of t variables $x_i, 0 \leq i \leq t-1, x_i \in GF(2^r)$ can be efficiently computed using the multivariate Horner scheme [34]. When $t = 1$, any polynomial of degree $b + 1$ defined over $GF(2^r)$ can be represented as

$$f(x) = a_0 \oplus x(a_1 \oplus x(\cdots(a_b \oplus a_{b+1}x))), \qquad (49)$$

where $a_i \in GF(2^r), x \in GF(2^r)$. The computation of the polynomial requires $b+1$ multipliers and $b+1$ adders in $GF(2^r)$.

When $t > 1$, we can first apply Horner scheme as if x_0 is the variable and $x_1, x_2, \cdots, x_{t-1}$ are coefficients. In this case coefficients will be polynomials of $t-1$ variables $x_1, x_2, \cdots, x_{t-1}$. To compute these polynomials, we can select one of the remaining $x_i, 1 \leq i \leq t-1$ as variable and apply the Horner scheme again. We repeat the procedure until all $x_i, 0 \leq i \leq t-1$ are factored out.

The encoder for the (k, m, r) AMD codes constructed by Theorem 3.1 needs to compute $f(y, x) = A(x) \oplus B(y, x)$, where $B(y, x)$ contains $\lceil \frac{k}{r} \rceil$ monomials of degrees less or equal to $b + 1$ and $A(x)$ contains at most $t = \frac{m}{r}$ monomials of degree $b + 2$. Assume we always select a set of monomials with the smallest possible degrees for $B(y, x)$. For Horner scheme, the number of multiplication required for the computation is no more than the total number of monomials in $f(x)$ and is upper bounded by $\lceil \frac{k}{r} \rceil + \frac{m}{r}$.

Example 4.1: In Theorem 3.1, let $t = b = 2$ and assume r is large enough. Then the resulting code is a $(7r, 2r, r)$ AMD code. We have

$$f(y, x) = x_0x_1^3 \oplus x_0y_0 \oplus x_1y_1 \oplus x_0^2y_2 \oplus x_0x_1y_3 \oplus x_1^2y_4 \oplus x_0^3y_5 \oplus x_0^2x_1y_6. \qquad (50)$$

At most 8 multipliers in $GF(2^r)$ are required for the encoding or the decoding. The corresponding encoding network is shown in Figure 4. The critical path of the encoder contains 4 multipliers and 4 adders in $GF(2^r)$.

The encoder and decoder for AMD codes constructed by Theorem 3.1 are inherently suitable for parallel implementations. For instance, the three branches shown in Figure 4 can be implemented in parallel. Moreover, the encoder and decoder can be further parallelized by using two multipliers for computing x_1y_6 and x_0y_5 on the second branch. The same idea works on the encoder and decoder for any AMD codes constructed by Theorem 3.1.

We note that the actual number of multipliers in the encoder and decoder may be smaller than the number of monomials in $f(y, x)$ due to the fact that the power operation (exponentiation in $GF(2^r)$) can be simplified. For example, in the normal base Galois field, the square operation can be implemented by cyclic shifting [35]. In this case, the multiplier marked in Figure 4, which is used to compute x_1^2, is not needed and the total number of multipliers in the encoder becomes 7.

A case study of using AMD codes with $b = 1$ or $t = 1$ for the protection of digit-serial Massey-Omura multipliers in normal base Galois fields was shown in [21]. The overheads for several different secure Massey-Omura multiplier architectures based on AMD codes with $b = 1$ or $t = 1$ in $GF(2^{239})$ and $GF(2^{409})$ for the elliptic curve cryptographic devices were studied. It was showed that the area overheads for the presented architectures based on AMD codes were between 110% and 160%.

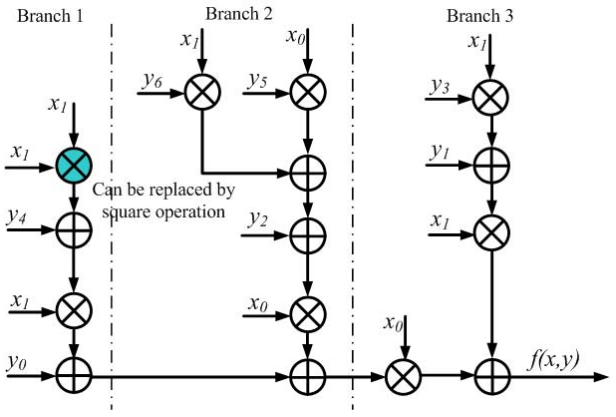


Fig. 4: Encoder Architecture for the $(7r, 2r, r)$ AMD Code Based on $GRM_q(3, 2)$ code

.

5 Conclusions

In this paper, we presented bounds, general constructions and encoding/decoding procedures for algebraic manipulation detection (AMD) codes based on q-ary Generalized Reed-Muller codes and their products. Some of the presented codes are optimal. These codes can provide a guaranteed level of security even if the information bits are known to the attackers and the non-zero error patterns are controllable by external forces. The same characteristic cannot be achieved by any previously known secure architectures based on error detecting codes. These codes can be applied for many different applications such as robust secret sharing scheme, robust fuzzy extractors and secure cryptographic devices resistant to fault injection attacks. An efficient encoding and decoding method minimizing the number of required multipliers are given for the presented AMD codes.

Acknowledgments

We would like to thank Prof. Reyzin from the Computer Science Department of Boston University in the United States and Prof. Keren from the Bar Ilan University in Israel for their important comments and suggestions for the paper.

References

[1] T. Malkin, F.-X. Standaert, and M. Yung, "A comparative cost/security analysis of fault attack countermeasures," in *Fault Diagnosis and Tolerance in Cryptography*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2006, vol. 4236, pp. 159–172.

[2] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "Error analysis and detection procedures for a hardware implementation of the advanced encryption standard," *IEEE Transactions on Computers*, vol. 52, no. 4, pp. 492–505, 2003.

[3] G. Bertoni, L. Breveglieri, I. Koren, and V. Piuri, "Fault detection in the advanced encryption standard," in *Proc. of the International Conference on Massively Parallel Computing Systems (MPCS 2002)*, Ischia, Italy, Apr. 2002, pp. 92–97.

[4] N. Joshi, K. Wu, and R. Karri, "Concurrent error detection schemes for involution ciphers," in *Cryptographic Hardware and Embedded Systems - CHES 2004*, ser. Lecture Notes in Computer Science, vol. 3156. Springer Berlin / Heidelberg, 2004, pp. 153–160.

[5] R. Karri, K. Wu, P. Mishra, and Y. Kim, "Concurrent error detection of fault-based side-channel cryptanalysis of 128-bit symmetric block ciphers," in *38th Design Automation Conference (DAC 2001)*. ACM Press, 2001, pp. 579–585.

[6] ——, "Concurrent error detection schemes for fault-based side-channel cryptanalysis of symmetric block ciphers," *IEEE Transactions on CAD of Integrated Circuits and Systems*, vol. 21, no. 12, pp. 1509–1517, 2002.

[7] M. Karpovsky., K. Kulikowski, and A.Taubin, "Robust protection against fault-injection attacks on smart cards implementing the advanced encryption standard," ser. Proc. Int. Conference on Dependable Systems and Networks (DNS 2004), July 2004.

[8] M. G. Karpovsky and A. Taubin, "New class of nonlinear systematic error detecting codes," *IEEE Transactions on Information Theory*, vol. 50, no. 8, pp. 1818–1820, 2004.

[9] G. Gaubatz, B. Sunar, and M. G. Karpovsky, "Nonlinear residue codes for robust public-key arithmetic," in *Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC '06)*, 2006.

[10] Z. Wang, M. Karpovsky, and K. Kulikowski, "Design of memories with concurrent error detection and correction by nonlinear SEC-DED codes," *Journal of Electronic Testing*, pp. 1–22, 2010, 10.1007/s10836-010-5168-5. [Online]. Available: http://dx.doi.org/10.1007/s10836-010-5168-5

[11] S. Engelberg and O. Keren, "A comment on the karpovsky-taubin code," *Information Theory, IEEE Transactions on*, vol. 57, no. 12, pp. 8007–8010, 2011.

[12] N. Admaty, S. Litsyn, and O. Keren, "Punctuating, expurgating and expanding the q-ary bch based robust codes," in *The 27-th IEEE Convention of Electrical and Electronics Engineers in Israel*.

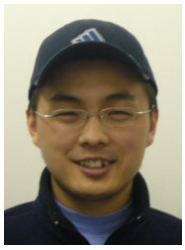
[13] K.Kulikowski, Z.Wang, and M.G.Karpovsky, "Comparative analysis of fault attack resistant architectures for private and public key cryptosystems," in *Proc of Int. Workshop on Fault-tolerant Cryptographic Devices*, 2008.

[14] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proceedings of the IEEE*, vol. 100, no. 11, pp. 3056–3076, 2012.

[15] S. Cabello, C. Padr, and G. Sez, "Secret sharing schemes with detection of cheaters for a general access structure," *Designs, Codes and Cryptography*, vol. 25, pp. 175–188, 2002, 10.1023/A:1013856431727. [Online]. Available:

http://dx.doi.org/10.1023/A:1013856431727
[16] Y. Dodis, B. Kanukurthi, J. Katz, L. Reyzin, and A. Smith, "Robust fuzzy extractors and authenticated key agreement from close secrets," in *In Advances in Cryptology CRYPTO 6*. Springer, 2006, pp. 232–250.
[17] R. Cramer, Y. Dodis, S. Fehr, C. Padró, and D. Wichs, "Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors," in *Proceedings of the theory and applications of cryptographic techniques, 27th annual international conference on Advances in cryptology*, ser. EUROCRYPT'08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 471–488.
[18] V. Guruswami and A. Smith, "Codes for computationally simple channels: Explicit constructions with optimal rate," in *51st Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 10 2010.
[19] S. Dziembowski, K. Pietrzak, and D. Wichs, "Non-malleable codes," in *Innovation in Computer Science, Cryptology ePrint Archive: Report 2009/608*.
[20] Z. Wang and M. Karpovsky, "Reliable and secure memories based on algebraic manipulation correction codes," in *IEEE 18th International On-Line Testing Symposium (IOLTS)*, 2012.
[21] ——, "Algebraic manipulation detection codes and their applications for design of secure cryptographic devices," in *IEEE 17th International On-Line Testing Symposium (IOLTS)*, 2011, pp. 234–239.
[22] Z. Wang, M. Karpovsky, B. Sunar, and A. Joshi, "Design of reliable and secure multipliers by multilinear arithmetic codes," in *Information and Communications Security*, ser. Lecture Notes in Computer Science, 2009, vol. 5927, pp. 47–62.
[23] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1998.
[24] E. F. Assmus, Jr, and J. D. Key, "Polynomial codes and finite geometries, Manuscript," 1995.
[25] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*. London, UK: Springer-Verlag, 2003, pp. 2–12. [Online]. Available: http://portal.acm.org/citation.cfm?id=648255.752727
[26] Y. Monnet, M. Renaudin, R. Leveugle, C. Clavier, and P. Moitrel, "Case study of a fault attack on asynchronous DES crypto-processors," in *Fault Diagnosis and Tolerance in Cryptography*, ser. Lecture Notes in Computer Science, L. Breveglieri, I. Koren, D. Naccache, and J.-P. Seifert, Eds. Springer Berlin / Heidelberg, 2006, vol. 4236, pp. 88–97.
[27] J. M. Schmidt and M. Hutter, "Optical and EM fault-attackson CRT-based RSA: Concrete results," in *15th Austrian Workshop on Microelectronics*, 2007.
[28] G. Canivet, P. Maistri, R. Leveugle, J. Cldire, F. Valette, and M. Renaudin, "Glitch and laser fault attacks onto a secure AES implementation on a SRAM-based FPGA," *Journal of Cryptology*, pp. 1–22, 2010, 10.1007/s00145-010-9083-9. [Online]. Available: http://dx.doi.org/10.1007/s00145-010-9083-9
[29] E. Trichina and R. Korkikyan, "Multi fault laser attacks on protected CRT-RSA," *Workshop on Fault Diagnosis and Tolerance in Cryptography*, vol. 0, pp. 75–86, 2010.
[30] S. Skorobogatov, "Optical fault masking attacks," *Workshop on Fault Diagnosis and Tolerance in Cryptography*, pp. 23–29, 2010.
[31] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Online available at http://www.codetables.de, 2007, accessed on 2012-12-09.
[32] C. Mackenzie and J. Seberry, "Maximal q-ary codes and Plotkin's bound," *ARS Combinatoria*, vol. 26B, pp. 37–50, 1988.
[33] N. Santhi, "On algebraic decoding of q-ary reed-muller and product reed-solomon codes," in *IEEE International Symposium on Information Theory, 2007. ISIT 2007.*, 2007, pp. 1351 –1355.
[34] M. Ceberio and V. Kreinovich, "Greedy algorithms for optimizing multivariate horner schemes," *SIGSAM Bull.*, vol. 38, pp. 8–15, March 2004. [Online]. Available: http://doi.acm.org/10.1145/980175.980179
[35] S. Gao, "Normal bases over finite fields," Ph.D. dissertation, University of Waterloo, 1993.

Mark Karpovsky Mark Karpovsky (M'80-SM'84-F'91) has been a professor of computer engineering and the director of the Reliable Computing Laboratory, Department of Electrical and Computer Engineering, Boston University, Massachusetts, since 1983. Before joining Boston University, he taught at the State University of New York, Binghamton, and Tel-Aviv university, Israel. He was a visiting prof essor at the University of Dortmund, Germany, the Ecole National Superieure des Telecommunication, Paris, France, and the New Jersey Institute of Technology, Newark. He has been a consultant for IBM, Digital Corporation, Honeywell Corporation, AT&T, Raytheon, and several companies in Europe. He has published more than 200 papers and several books in the areas of logical design, testing and diagnosis of computer systems, fault-tolerant computing, error-correcting codes, and computer communication networks. He conducts research in the areas of design, testing and diagnosis of computer networks, message routing for multiprocessors and computer communication networks, and design of cryptographic devices resistant to side-channel attacks.He recently published together with R.S. Stankovic and J.T. Astola the book "Spectral Logic and its Applications for the Design of Digital Devices" by Wiley & Sons. He is a life Fellow of the IEEE.



Zhen Wang Zhen Wang received his B.S and M.S degree in Information and Communication Engineering from Zhejiang University, China in 2006. Since the summer of 2006, he started working towards his PhD degree at Boston University under the supervision of Prof. Mark G. Karpovsky and Prof. Ajay Joshi. His research is focused on the design of robust codes and their variations for building reliable and secure devices, e.g. secure cryptographic devices and reliable memories. He also conducts research to investigate the influence of nano-scale technologies on the reliability of modern digital systems, etc. He is now working for Mediatek Wireless, Inc.