New Bounds and Constructions of Weak Systematic Algebraic Modification Detection Codes

Yao Chen, Yin Tan, Guang Gong

Department of Electrical and Computer Engineering
University of Waterloo, Canada

{y449chen, yin.tan, ggong}@uwaterloo.ca

December 4, 2017

Abstract

Algebraic Manipulation Detection (AMD) codes are introduced by Cramer et al. to fill in the gap between error-detecting/correcting codes and message authentication codes (MACs). Unlike MACs, AMD codes do not require a secret key to provide resilience against malicious modifications of data, thus avoid key distributions. An ε-secure AMD code is able to detect abitrary alteration of the encoded data with probability at least $1 - \varepsilon$. One primary goal about AMD codes is to obtain the smallest possible ε, the cheating probility. In this paper, we summarize existing results on general AMD codes and present our work on a particular category of AMD codes, the *weak systematic* ones, which is not fully studied before. We establish a new lower bound on ε for weak systematic AMD codes in terms of the nonlinearity of functions. We then give a few constructions attaining our new bound and demonstrating that this bound is better than the general one.

1 Introduction

Algebraic manipulation detection (AMD) codes (defined in Section 2.1) are first introduced in [2] as a cryptographic primitive providing some authenticity in linear security schemes. They can be viewed as a special class of nonlinear error detecting codes, and they fill in the gap between linear error detecting codes and message authentication codes (MACs). (See [8] and [11] for details about linear error correcting codes and MACs.) For example, considering the encryption by one-time pad: it is unconditionally secure, but an adversary can easily flip any bit in the ciphertext without being discovered due to its linearity. Linear error detecting codes cannot fix this problem since they cannot prevent an adversary from flipping more bits than their error-detecting capability; MACs may provide authenticity, but they require additional shared keys. In this case, AMD codes, aiming to the detection of malicious manipulations, can be a relatively lightweight alternative in the sense that they do not require a key.

The attack model of AMD codes consists of a storage device that is capable of storing a single element α of some finite abelian group $\mathcal{G}$ and an adversary who cannot read the content of the storage device, but can alter it by a manipulation of the form $\alpha + \delta$, for some $0 \neq \delta \in \mathcal{G}$ (this assumption is met, for example, in the one-time pad scenario above). AMD codes guarantee that for any δ, such manipulation will be detected with high probability. We shall also distinguish the strong model, where the adversary has control over the input used to generated the codeword α, from the weak model, where the adversary does not have such control. Accordingly, there are a strong version and a weak version of AMD codes defined for each model (see Section 2.1).

Since the introduction of AMD codes, it has found many interesting applications such as robust secret sharing, robust fuzzy extractors [2], non-malleable codes [5], secure communication [7], secure memories [12], and error correcting codes for computationally bounded channels [6]. Following Cramer et al.'s work, a few new constructions have been proposed, and extensions of the concept of AMD codes have been studied. For example, Cramer et al. give an optimal AMD code that can encode messages of arbitrary lengths [4]; a recent work by Alekseev extends a design of Wang et al. [12] and gives a thorough analysis [1].

In this paper, we focus on the study of a particular category of AMD codes, the *weak systematic* (defined in 2.1) ones, which was not fully studied before. We first present a new characterization of weak systematic AMD codes (Theorem 8) by using the differential uniformity of the core function f (see Definition 3) for such AMD codes. Using this new characterization, we may provide two new lower bounds (Theorems 9 and 11) on ε, the cheating probability, of these AMD codes. We prove that these newly discovered lower bounds are much tighter than the lower bound for general weak AMD code obtained by Cramer et al. in [3]. Furthermore, we discovered new constructions of weak systematic AMD codes which attain these new bounds (Examples 12 and 13), which shows the tightedness of the new bounds.

The rest of the paper is organized as following. We first describe different types of AMD codes and necessary mathematical tools in Section 2. The new characterization of weak systematic AMD codes is presented in Section 3. Following this, the two new lower bounds and related constructions are given in Section 4. Some concluding remarks are given in Section 6.

2 Preliminary

In this section, we will provide necessary definitions and results, which will be used throughout the paper.

2.1 AMD Codes

First we give the definitions of various *algebraic modification dection* (AMD) codes.

Definition 1 (**(m, n, ε)**-AMD codes, [2])**.** Let $\mathcal{S}$ be a set of size $m > 1$ and $\mathcal{G}$ be an abelian group of order n. Consider a pair $(\mathtt{Enc}, \mathtt{Dec})$ formed by a probabilistic encoding

map $\mathtt{Enc} : \mathcal{S} \to \mathcal{G}$ and a deterministic decoding map $\mathtt{Dec} : \mathcal{G} \to \mathcal{S} \cap \{ \perp \}$ such that $\mathtt{Dec}(\mathtt{Enc}(s)) = s$ with probability 1 for every $s \in \mathcal{S}$. The pair $(\mathtt{Enc}, \mathtt{Dec})$ is an (m, n, ε)-*AMD code* if for every $s \in \mathcal{S}$ and for every $\delta \in \mathcal{G}$, the probability

$$\Pr\left[\, \mathtt{Dec}(\mathtt{Enc}(s) + \delta) \notin \{ s, \perp \} \mid s, \delta \,\right] \tag{1}$$

is at most ε.

There's also a weak version of AMD codes defined below, where the probability (1) for certain values of s may exceed ε. In order to avoid confusion between the two versions, we sometimes call those defined in Definition 1 *strong* (m, n, ε)*-AMD codes*.

Definition 2 (Weak (m, n, ε)-AMD codes, [2])**.** Let $\mathcal{S}$, $\mathcal{G}$, $\mathtt{Enc}$ and $\mathtt{Dec}$ be defined as in Definition 1. The pair $(\mathtt{Enc}, \mathtt{Dec})$ is a *weak* (m, n, ε)*-AMD code* if for s uniformly sampled over $\mathcal{S}$ and for every $\delta \in G$, the probability

$$\Pr\left[\, \mathtt{Dec}(\mathtt{Enc}(s) + \delta) \notin \{ s, \perp \} \mid \delta \,\right] \tag{2}$$

is at most ε.

Let p_s denote the probability that s is chosen when sampling. Since s is uniformly sampled, the probability (2) can be computed as

$$\begin{aligned} (2) &= \sum_{s \in \mathcal{S}} \Pr\left[\, \mathtt{Dec}(\mathtt{Enc}(s) + \delta) \notin \{ s, \perp \} \mid s, \delta \,\right] \cdot p_s \\ &= \frac{1}{|\mathcal{S}|} \sum_{s \in \mathcal{S}} \Pr\left[\, \mathtt{Dec}(\mathtt{Enc}(s) + \delta) \notin \{ s, \perp \} \mid s, \delta \,\right]. \end{aligned}$$

Definition 3 (Systematic AMD codes, [2])**.** Furthermore, an AMD code (or a weak AMD code) is systematic if $\mathcal{S}$ is a group, $\mathcal{G} = \mathcal{S} \times \mathcal{G}_1 \times \mathcal{G}_2$ where $\mathcal{G}_1$ and $\mathcal{G}_2$ are groups, and the encoding mapping is given by

$$\mathtt{Enc}(s) = (s, x, f(x, s)),$$

where x is chosen uniformly at random from $\mathcal{G}_1$, and f is a function $f : \mathcal{G}_1 \times \mathcal{S} \to \mathcal{G}_2$. It follows that the decoding function of a systematic AMD code is

$$\mathtt{Dec}(s, x, e) = \begin{cases} s, & \text{if } e = f(x, s), \\ \perp, & \text{otherwise.} \end{cases}$$

2.2 Group rings and character theory

Character theory is one of the most important tools for applying group rings to combinatorial objects and cryptography. In this section we only review the characters of the group ring $\mathbb{C}[G]$, where G is an abelian group. For the theory of the representation of a general group ring, please refer to [9].

In the language of group rings, we identify a subset S of G with the group ring element $\sum_{s \in S} s$ in $\mathbb{C}[G]$, which will also be denoted by S (by abuse of notation). For $A = \sum_{g \in G} a_g g$

in $\mathbb{C}[G]$ and for an integer t, we define $A^{(t)} = \sum_{g\in G} a_g g^t$. A character χ of a finite abelian group G is a homomorphism from G to $\mathbb{C}^*(\triangleq \mathbb{C}\setminus\{0\})$. A character χ is called *principal* if $\chi(c) = 1$ for all $c \in G$, otherwise it is called *non-principal*. A principal character is usually denoted by χ_0. All characters form a group denoted by $\widehat{G}$, and the *character group* is isomorphic to G. The following result states the well-known *orthogonal relations* of characters.

Proposition 4 (Orthogonal relations of characters, [10])**.** *Let G be an abelian group, then the following equations hold:*

$$\sum_{g\in G}\chi(g) = \begin{cases} 0 & \text{if } \chi \neq \chi_0, \\ |G| & \text{if } \chi = \chi_0; \end{cases}$$

and

$$\sum_{\chi\in\widehat{G}}\chi(g) = \begin{cases} 0 & \text{if } g \neq 1_G, \\ |G| & \text{if } g = 1_G. \end{cases}$$

By linearity, we may extend each character $\chi \in \widehat{G}$ to a ring homomorphism from $\mathbb{C}[G]$ to $\mathbb{C}$, and we denote this homomorphism by χ, again. In particular, if G is the additive group of the finite field $\mathbb{F}_{p^n}$, all characters of G can be represented as follows. Define $\chi_1 : \mathbb{F}_{p^n} \to \mathbb{C}$ as $\chi_1(x) := \zeta_p^{\mathrm{Tr}(x)}$ for all $x \in \mathbb{F}_{p^n}$, where ζ_p is a primitive p-th root of unity and $\mathrm{Tr}(x)$ is the absolute trace function defined as $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{p^i}$. Then χ_1 is an additive character of $\mathbb{F}_{p^n}$ (i.e. χ_1 is a character of the additive group of $\mathbb{F}_{p^n}$). Moreover, every additive character χ is of the form χ_b ($b \in \mathbb{F}_{p^n}$), where χ_b is defined by $\chi_b(x) = \chi_1(bx)$ for all $x \in \mathbb{F}_{p^n}$. Furthermore, if $G = \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, all characters of G can be represented by $\chi_{u,v}$, where $\chi_{u,v}(a, b) = \zeta_p^{\mathrm{Tr}(au+bv)}$ for any $(a, b) \in G$.

For a group ring element $M \in \mathbb{C}[G]$, the *Fourier transform* of M is defined as the element $\widetilde{M} = \sum_{\chi\in\widehat{G}} \chi(M)\chi$ in $\mathbb{C}[\widehat{G}]$. It is easy to verify that $\widetilde{\widetilde{M}} = |G|M^{(-1)}$ by noting that $\widehat{\widehat{G}} \cong G$ (since $g(\chi) := \chi(g)$ for any $g \in G$ defines a character of $\widehat{G}$). The following results are important properties of group rings:

Proposition 5 ([10])**.** *Let $D = \sum_{g\in G} a_g g \in \mathbb{C}[G]$. Then the following hold:*

$$a_g = \frac{1}{|G|}\sum_{\chi\in\widehat{G}} \chi(D)\chi(g^{-1}), \tag{3}$$

$$\sum_{g\in G} |a_g|^2 = \frac{1}{|G|}\sum_{\chi\in\widehat{G}} |\chi(D)|^2. \tag{4}$$

Equation (3) is the so-called *Inversion Formula*, and Equation (4) is called *Parseval's relation*. It is worth to mention that Inversion Formula provides a useful method to show that two group ring elements are equal.

Corollary 6. *Let $A = \sum_{g\in G} a_g g$ and $B = \sum_{g\in G} b_g g$ be two group ring elements of $\mathbb{C}[G]$. Then $A = B$ if and only if $\chi(A) = \chi(B)$ for all $\chi \in \widehat{G}$.*

3 A new characterization of weak systematic AMD codes

In this section, we will present a new characterization of weak systematic AMD codes by the *differential uniformity* of the function f (see Definition 3). In the light of this characterization, we will give new bounds of ε for weak systematic AMD codes and provide new constructions attaining these bounds.

Definition 7. A mapping $f : G_1 \to G_2$ between two finite abelian groups is *differentially δ-uniform* if for all $0 \neq \alpha \in G_1$ and $\beta \in G_2$,

$$|\{\, x \mid f(x+\alpha) - f(x) = \beta\}| \leq \delta.$$

And the smallest such δ is called *differential uniformity* of f.

For the convenience of the following discussions, we first fix some notations. Let $\mathcal{S}, \mathcal{G}_1, \mathcal{G}_2$ be finite abelian groups and f be a mapping from $\mathcal{S} \times \mathcal{G}_1$ to $\mathcal{G}_2$. W.l.o.g. we may write the operations in $\mathcal{S}, \mathcal{G}_1, \mathcal{G}_2$ additively. For each $\alpha = (\Delta_s, \Delta_k, \Delta_y) \in \mathcal{S} \times \mathcal{G}_1 \times \mathcal{G}_2 \triangleq \mathcal{G}$, define

$$\delta_\alpha = |\{\, (s,k) \in \mathcal{S} \times \mathcal{G}_1 \mid f(s+\Delta_s, k+\Delta_k) - f(s,k) = \Delta_y \,\}|\,, \tag{5}$$

where $|X|$ denotes the size of a finite set X. If we let $\delta = \max_{\alpha \in \mathcal{G} \setminus \{0\} \times \{0\} \times \mathcal{G}_2} \delta_\alpha$, then f is a differentially δ-uniform function, or the differential uniformity of f is δ. In the following we assume that $|\mathcal{S}| = m, |\mathcal{G}_1| = n_1, |\mathcal{G}_2| = n_2$ and $n = mn_1n_2$. For the aforementioned function f, we define two functions, `Enc` and `Dec`, as follows:

$$\texttt{Enc} : \mathcal{S} \to \mathcal{G} = \mathcal{S} \times \mathcal{G}_1 \times \mathcal{G}_2,\ s \mapsto (s, x, f(x,s)), \tag{6}$$

where x is taken uniformly at random from $\mathcal{G}_1$. The function $\texttt{Dec} : \mathcal{S} \times \mathcal{G}_1 \times \mathcal{G}_2 \to \mathcal{S} \cap \{\perp\}$ is defined by

$$\texttt{Dec}(s,x,e) = \begin{cases} s, & \text{if } e = f(x,s), \\ \perp, & \text{otherwise.} \end{cases} \tag{7}$$

Now we are ready to present the main result of this section.

Theorem 8. *Let* `Enc` *and* `Dec` *be the functions in (6) and (7). Then* $(\texttt{Enc}, \texttt{Dec})$ *is a weak systematic (m, n, ε)-AMD code defined in Definition 3 if and only if*

$$\begin{aligned} \textstyle\sum_{\substack{\Delta_k \in \mathcal{G}_1 \setminus \{0\} \\ \Delta_y \in \mathcal{G}_2}} \delta_{(0,\Delta_k,\Delta_y)} &\geq (mn_1)^2 - mn_1 - \varepsilon(m-1)mn_1^2n_2, \text{ and} \\ \delta_{(\Delta_s,\Delta_k,\Delta_y)} &\leq \varepsilon mn_1, \text{ if } \Delta_s \neq 0, \end{aligned} \tag{8}$$

where $\delta_{(\Delta_s,\Delta_k,\Delta_y)}$ is defined in (5).

Proof. Denoting the subgroup $\mathcal{S} \times \mathcal{G}_1 \times \{0\}$ of $\mathcal{G}$ by $\mathcal{G}'$. Define the group ring element $D = \sum_{(s,k) \in \mathcal{G}'} (s, k, f(s,k))$, we have

$$\begin{aligned} DD^{(-1)} &= \sum_{(s_1,k_1) \in \mathcal{G}'} \sum_{(s_2,k_2) \in \mathcal{G}'} ((s_2,k_2,f(s_2,k_2)) - (s_1,k_1,f(s_1,k_1))) \\ &= \sum_{(s_1,k_1) \in \mathcal{G}'} \sum_{(\Delta_s,\Delta_k) \in \mathcal{G}'} (\Delta_s, \Delta_k, f(s_1+\Delta_s, k_1+\Delta_k) - f(s_1,k_1)) \\ &= \sum_{(\Delta_s,\Delta_k,\Delta_y) \in \mathcal{G}} \delta_{(\Delta_s,\Delta_k,\Delta_y)} (\Delta_s, \Delta_k, \Delta_y), \end{aligned} \tag{9}$$

where $\delta_{(\Delta_s,\Delta_k,\Delta_y)}$ is defined in (5). Now, assume $(\mathtt{Enc},\mathtt{Dec})$ is an (m,n,ε)-AMD code. In the following, for some $(\Delta_s,\Delta_k,\Delta_y)$, we determine the value or bound of $\delta_{(\Delta_s,\Delta_k,\Delta_y)}$:

Case 1: $\Delta_s=\Delta_k=\Delta_y=0$. In this case it is clear to see that $\delta_{(\Delta_s,\Delta_k,\Delta_y)}=|\mathcal{S}||\mathcal{G}_1|=mn_1$;

Case 2: $\Delta_s=\Delta_k=0$ and $\Delta_y\neq 0$. Since f is a function of (s,k), $\delta_{(\Delta_s,\Delta_k,\Delta_y)}=0$;

Case 3: $\Delta_s\neq 0$. By the definition of weak (m,n,ε)-AMD code, we have that for every $\alpha=(\Delta_s,\Delta_k,\Delta_y)\in\mathcal{G}$ with $\Delta_s\neq 0$ and s sampled uniformly from $\mathcal{S}$,

$$\begin{aligned}
\Pr\left[\,\mathtt{Dec}(\mathtt{Enc}(s)+\alpha)\notin\{\,s,\perp\,\}\mid\alpha\,\right] &= \sum_{s\in\mathcal{S}}\Pr\left[\,\mathtt{Dec}(\mathtt{Enc}(s)+\alpha)\notin\{\,s,\perp\,\}\mid s,\alpha\,\right]\cdot p_s\\
&= \frac{1}{|S|}\sum_{s\in\mathcal{S}}\Pr\left[\,\mathtt{Dec}(\mathtt{Enc}(s)+\alpha)\notin\{\,s,\perp\,\}\mid s,\alpha\,\right]\\
&= \frac{1}{|\mathcal{S}|}\sum_{s\in\mathcal{S}}\frac{|\{\,k\in\mathcal{G}_1\mid f(k+\Delta_k,s+\Delta_s)-f(k,s)=\Delta_y\,\}|}{|\mathcal{G}_1|}\\
&= \frac{|\{\,(s,k)\in\mathcal{S}\times\mathcal{G}_1\mid f(k+\Delta_k,s+\Delta_s)-f(k,s)=\Delta_y\,\}|}{|\mathcal{S}||\mathcal{G}_1|}\\
&= \frac{\delta_\alpha}{|\mathcal{S}||\mathcal{G}_1|}\leq\varepsilon,
\end{aligned}$$

which gives $\delta_\alpha\leq\varepsilon mn_1$.

Now, applying the principal character χ_0 on $DD^{(-1)}$, we get

$$(mn_1)^2=\sum_{(\Delta_s,\Delta_k,\Delta_y)\in\mathcal{G}}\delta_{(\Delta_s,\Delta_k,\Delta_y)}.$$

Substituting the values of $\delta_{(\Delta_s,\Delta_k,\Delta_y)}$ into the above equation, we obtain the following inequality:

$$(mn_1)^2\leq n_1(m-1)n_2\cdot\varepsilon n_1m+mn_1+\sum_{\substack{\Delta_k\in\mathcal{G}_1\setminus\{\,0\,\}\\ \Delta_y\in\mathcal{G}_2}}\delta_{(0,\Delta_k,\Delta_y)}$$

Rearranging its terms gives us the inequality (8).

Conversely, let f be a function satisfying the property in (8), we need to show that $(\mathtt{Enc},\mathtt{Dec})$ is an (m,n,ε)-AMD code. In particular, we need to show that for every $\alpha=(\Delta_s,\Delta_k,\Delta_y)\in\mathcal{G}$ and s sampled uniformly from $\mathcal{S}$,

$$\Pr\left[\,\mathtt{Dec}(\mathtt{Enc}(s)+\alpha)\notin\{\,s,\perp\,\}\mid\alpha\,\right]\leq\varepsilon.$$

We discuss two cases of α:

1. $\Delta_s \neq 0$: Similar to Case 3 above, we have

$$\begin{aligned}
&\Pr\left[\,\mathtt{Dec}(\mathtt{Enc}(s)+\alpha) \notin \{\, s, \perp \,\} \mid \alpha \,\right] \\
=&\frac{1}{|\mathcal{S}|}\sum_{s\in\mathcal{S}} \Pr\left[\,\mathtt{Dec}(\mathtt{Enc}(s)+\alpha) \mid s, \alpha \,\right] \\
=&\frac{1}{|\mathcal{S}|}\sum_{s\in\mathcal{S}} \frac{|\{\,(s,k)\in\mathcal{S}\times\mathcal{G}_1 | f(k+\Delta_k, s+\Delta_s) - f(k,s) = \Delta_y \,\}|}{|\mathcal{S}||\mathcal{G}_1|} \\
=&\frac{\delta_\alpha}{|\mathcal{S}||\mathcal{G}_1|} \leq \frac{\varepsilon m n_1}{m n_1};
\end{aligned}$$

2. $\Delta_s = 0$: According to the definition of $\mathtt{Dec}$, $\mathtt{Dec}(\mathtt{Enc}(s)+\alpha)$ always yields s or $\perp$ in this case. Therefore the probability $\Pr\left[\,\mathtt{Dec}(\mathtt{Enc}(s)+\alpha) \notin \{\, s, \perp \,\} \mid \alpha \,\right] = 0$.

The proof is completed. □

4 Two new lower bounds on ε for weak systematic AMD codes

In this section, we present two new lower bounds on the value of ε, based on our discussion above.

4.1 The first lower bound

The following result gives the first lower bound of ε.

Theorem 9. *Let f be a function from $\mathcal{S}\times\mathcal{G}_1$ to $\mathcal{G}_2$, and $(\mathtt{Enc}, \mathtt{Dec})$ be the systematic AMD code derived from f. Then*

$$\varepsilon \geq \max\left\{ \frac{(mn_1)^2 - mn_1 - \sum\limits_{\Delta_k\in\mathcal{G}_1^*, \Delta_y\in\mathcal{G}_2} \delta_{(0,\Delta_k,\Delta_y)}}{(m-1)mn_1^2n_2}, \max_{\substack{(\Delta_s,\Delta_k,\Delta_y)\\ \Delta_s\neq 0}} \frac{\delta_{(\Delta_s,\Delta_k,\Delta_y)}}{mn_1} \right\}.$$

Particularly, assuming the differential uniformity of f is d, then

$$\varepsilon \geq \frac{(mn_1)^2 - mn_1 - d(n_1-1)n_2}{(m-1)mn_1^2n_2},$$

Proof. By Theorem 8, we have both

$$\sum_{\substack{\Delta_k\in\mathcal{G}_1\setminus\{\,0\,\}\\ \Delta_y\in\mathcal{G}_2}} \delta_{(0,\Delta_k,\Delta_y)} \geq (mn_1)^2 - mn_1 - \varepsilon(m-1)mn_1^2n_2 \tag{10}$$

and

$$\delta_{(\Delta_s,\Delta_k,\Delta_y)} \leq \varepsilon m n_1, \text{ for } \Delta_s \neq 0. \tag{11}$$

From (10), we have $\varepsilon \geq \frac{\sum_{\Delta_k \in \mathcal{G}_1^*, \Delta_y \in \mathcal{G}_2} \delta_{(0,\Delta_k,\Delta_y)} - (mn_1)^2 + mn_1}{(m-1)mn_1^2 n_2}$ and from (11) we have $\varepsilon \geq \max_{\substack{(\Delta_s,\Delta_k,\Delta_y) \\ \Delta_s \neq 0}} \frac{\delta_{(\Delta_s,\Delta_k,\Delta_y)}}{mn_1}$.

If the differential uniformity of f is d, then $\delta_\alpha \leq d$ for every $\alpha = (\Delta_s, \Delta_k, \Delta_y)$ where either $\Delta_s \neq 0$ or $\Delta_k \neq 0$, therefore

$$\varepsilon \geq \frac{(mn_1)^2 - mn_1 - \sum_{\Delta_k \in \mathcal{G}_1^*, \Delta_y \in \mathcal{G}_2} d}{(m-1)mn_1^2 n_2} = \frac{(mn_1)^2 - mn_1 - d(n_1-1)n_2}{(m-1)mn_1^2 n_2}.$$

□

Similarly, given parameters m, n_1, n_2, and ε, we can establish a lower bound on the differential uniformity of the function f.

Proposition 10. *Let $\mathcal{S}, \mathcal{G}_1$ and $\mathcal{G}_2$ be abelian groups with $|\mathcal{S}| = m$, $|\mathcal{G}_1| = n_1$ and $|\mathcal{G}_2| = n_2$. Let f be a function $f : \mathcal{G}_1 \times \mathcal{S} \to \mathcal{G}_2$. If f generates a weak systematic (m, n, ε)-AMD code as in Definitions 3 and 2, then a lower bound for the maximum differential uniformity of $f_s(k) \triangleq f(k, s)$ is*

$$\frac{mn_1^2 - n_1 - \varepsilon(m-1)n_1^2 n_2}{(n_1-1)n_2}.$$

Proof. Let d_s be the differential uniformity of $f_s(k)$, then

$$\begin{aligned} \sum_{\substack{s \in \mathcal{S} \\ \Delta_k \in \mathcal{G}_1 \setminus \{0\} \\ \Delta_y \in \mathcal{G}_2}} d_s &\geq \sum_{\substack{\Delta_k \in \mathcal{G}_1 \setminus \{0\} \\ \Delta_y \in \mathcal{G}_2}} \delta_{(0,\Delta_k,\Delta_y)} \\ &\geq (mn_1)^2 - mn_1 - \varepsilon m(m-1)n_1^2 n_2, \end{aligned}$$

according to Theorem 8. Therefore

$$\max_{s \in \mathcal{S}} \{ d_s \} \geq \frac{(mn_1)^2 - mn_1 - \varepsilon m(m-1)n_1^2 n_2}{m(n_1-1)n_2} = \frac{mn_1^2 - n_1 - \varepsilon(m-1)n_1^2 n_2}{(n_1-1)n_2}.$$

□

4.2 The second lower bound

Below we adapt a lower bound given by Cramer et al. for weak AMD codes [3] into one for weak systematic AMD codes.

Proposition 11. *Let $\mathcal{S}, \mathcal{G}_1$ and $\mathcal{G}_2$ be abelian groups with $|\mathcal{S}| = m$, $|\mathcal{G}_1| = n_1$ and $|\mathcal{G}_2| = n_2$. Let $(\mathtt{Enc}, \mathtt{Dec})$ be a weak systematic (m, n, ε)-AMD code where $n = mn_1n_2$, and encoding map $\mathtt{Enc}$ is from $\mathcal{S}$ to $\mathcal{S} \times \mathcal{G}_1 \times \mathcal{G}_2 \triangleq \mathcal{G}$ and decoding map $\mathtt{Dec}$ is from $\mathcal{G}$ to $\mathcal{S} \cap \{\perp\}$, respectively. Then $(\mathtt{Enc}, \mathtt{Dec})$ satisfies*

$$\varepsilon \geq \frac{(m-1)n_1}{n-1}.$$

Proof. Let p_δ denote the probability that δ is chosen by the adversary. Since probability (2) is at most ε for every δ, the probability

$$\begin{aligned} &\Pr\left[\,\mathtt{Dec}(\mathtt{Enc}(s)+\delta) \notin \{\, s, \perp \,\}\,\right] && (12)\\ =&\sum_{\delta\in\mathcal{G}} \Pr\left[\,\mathtt{Dec}(\mathtt{Enc}(s)+\delta) \notin \{\, s, \perp \,\} \mid \delta\,\right] \cdot p_\delta \\ \le&\sum_{\delta\in\mathcal{G}} \varepsilon \cdot p_\delta = \varepsilon. && (13)\end{aligned}$$

Now suppose δ is uniformly sampled from $\mathcal{G}$. Let $\mathtt{Dec}^{-1}(s)$ denote the set $\{\, g \in \mathcal{G} \mid \mathtt{Dec}(g) = s \,\}$. Since s and δ are independently chosen, for any s fixed,

$$\begin{aligned}\Pr\left[\,\mathtt{Dec}(\mathtt{Enc}(s)+\delta) \notin \{\, s, \perp \,\} \mid s\,\right] &= \frac{\left|\bigcup_{s'\in\mathcal{S}\setminus\{s\}} \mathtt{Dec}^{-1}(s')\right|}{|\mathcal{G}|-1} \\ &= \frac{\sum_{s'\in\mathcal{S}\setminus\{s\}} |\mathtt{Dec}^{-1}(s')|}{|\mathcal{G}|-1},\end{aligned}$$

therefore probability (12) can be computed in a second way as

$$\begin{aligned}(12) &= \frac{1}{|\mathcal{S}|}\sum_{s\in\mathcal{S}} \Pr\left[\,\mathtt{Dec}(\mathtt{Enc}(s)+\delta) \notin \{\, s, \perp \,\} \mid s\,\right] \\ &= \frac{1}{|\mathcal{S}|} \cdot \frac{(|\mathcal{S}|-1)\sum_{s\in\mathcal{S}} |\mathtt{Dec}^{-1}(s)|}{|\mathcal{G}|-1} \\ &= \frac{|\mathcal{S}|-1}{|\mathcal{G}|-1} \cdot \frac{\sum_{s\in\mathcal{S}} |\mathcal{G}_1|}{|\mathcal{S}|} \\ &= \frac{|\mathcal{S}|-1}{|\mathcal{G}|-1} \cdot |\mathcal{G}_1| = \frac{m-1}{n-1}\cdot n_1. \qquad (14)\end{aligned}$$

Combining (13) and (14) gives us

$$\varepsilon \ge \frac{(m-1)n_1}{n-1}.$$

□

We will give a construction in the next section, which asymptotically attains the bound in Proposition 11. Between the two bounds (Theorem 9 and Proposition 11), the tightness depends on the exact parameters; but we can expect the first bound (Theorem 9) to be tighter than the other for functions with perfect or almost perfect nonlinearity.

5 New Constructions

In this section, we present two constructions of weak systematic AMD codes. The following example gives one construction of weak systematic AMD codes attaining the lower bounds in Theorem 9.

Example 12. Let $\mathcal{S} = \mathcal{G}_2 = \mathbb{F}_{q^b}, \mathcal{G}_1 = \mathbb{F}_{q^a}$, where $a \mid b$ (so that $\mathcal{G}_1$ is a subfield of $\mathcal{S}$). Let f be a function

$$\begin{aligned} f : \mathbb{F}_{q^b} \times \mathbb{F}_{q^a} &\to \mathbb{F}_{q^b} \\ (s, k) &\mapsto k\text{Ł}(s), \end{aligned}$$

where $L(x)$ is a linearized permutation in $\mathbb{F}_{q^b}$. Then f generates a weak systematic $(q^b, q^{2b+a}, 1/q^a)$-AMD code. (To see it is indeed a weak AMD code, consider the case $s = 0$.) Also note that overall, f has a differential uniformity of q^b.

Here we demonstrate the differential uniformity of f and the computation of cheating probability ε.

To compute the differential uniformity of f, we need to determine the number of solutions (s, k) such that $f(s+\Delta_s, k+\Delta_k) - f(s, k) = \Delta_y$, for any $(\Delta_s, \Delta_k, \Delta_y)$ such that Δ_s and Δ_k are not both zero. We first simplify the equation:

$$\begin{aligned} f(s + \Delta_s, k + \Delta_k) - f(s, k) &= (k + \Delta_k)L(s + \Delta_s) - kL(s) \\ &= kL(\Delta_s) + \Delta_k L(s) + \Delta_k L(\Delta_s) = \Delta_y. \end{aligned}$$

Moving the constant $\Delta_k L(\Delta_s)$ to the right hand side, the equation becomes

$$kL(\Delta_s) + \Delta_k L(s) = a \triangleq \Delta_y - \Delta_k L(\Delta_s).$$

We consider the differential uniformity in three cases:

1. $\Delta_s = 0, \Delta_k \neq 0$: in this case, $L(\Delta_s) = 0$ and $L(s) = a/\Delta_k$. Since L is a permutation, there is only one solution for s, and k can be arbitrary. Hence there are q^a solutions of (s, k).

2. $\Delta_s \neq 0, \Delta_k = 0$: in this case, $\Delta_k L(s) = 0$ and $L(\Delta_s) \neq 0$, so $k = a/L(\Delta_s)$ has only one solution for k, and s can be arbitrary. Hence there are q^b solutions of (s, k).

3. $\Delta_s \neq 0, \Delta_k \neq 0$: in this case, for every k we have one solution of s. Hence there are q^a solutions of (s, k).

The computation of cheating probability is similar to that above, but we notice that cases where $\Delta_s = 0$ are not included, since they do not alter the message.

Another construction is from difference sets. It is given in Example 13 and may be of interest.

Example 13. A (v, k, λ)-*difference set* is a subset D of a group G (written additively) such that

- $|G| = v$,
- $|D| = k$, and
- every $0 \neq \alpha \in G$ can be expressed as $\alpha = d_1 - d_2$ for some $d_1, d_2 \in D$ in exactly λ different ways.

Let $D \subset G$ be a (v, k, λ)-difference set. Let $\mathcal{S}$ be an abelian group with order $|S| = |D|$ and $\mathcal{G}_1 = \mathcal{G}_2 = G$. Let g be a (nonlinear) bijection between $\mathcal{S}$ and D and f be a function

$$\begin{aligned} f : D \times G &\to G \\ (g(s), t) &\mapsto g(s) + t. \end{aligned}$$

Then f generates a $(k, kv^2, \lambda/k)$-weak systematic AMD code.

To calculate the cheating probability, we discuss the following two cases where $\Delta_s \neq 0$:

1. $\Delta_t = \Delta_y$: this implies that $g(s + \Delta_s) = g(s)$, which is impossible for a bijection;
2. $\Delta_t \neq \Delta_y$: among the k different choices of s, there are at most λ representations of $\Delta_y - \Delta_t$.

Therefore $\varepsilon \leq \lambda/k$.

For this example, we should notice that the choice of mapping g has an impact on ε, and the value λ/k given above is a loose overall upper bound. However, the effect has not been fully understood yet.

6 Conclusions and Future Work

In this paper we characterized weak systematic AMD codes with the nonlinearity of functions, and based on this characterization, we developed a tight lower bound of the parameter ε; we also extended the bound established by Cramer et al. for weak AMD codes. We provided two new constructions – the first shows that our bound is indeed tight, and the second involves difference set and may serve as another step to further reveal the connections between combinatorial designs and AMD code constructions.

There are potentially many new constructions still to be discovered, such as with perfect nonlinear (PN) functions and almost perfect nonlinear (APN) functions. This will be left as a future work.

7 Acknowledgement

The authors want to thank Steven Wang for his suggestions to use linearized polynomial.

References

[1] Maksim Alekseev. Two Algebraic Manipulation Detection Codes Based on a Scalar Product Operation. In *International Workshop on Coding and Cryptography (WCC 2015)*, 2015.

[2] Ronald Cramer, Yevgeniy Dodis, Serge Fehr, Carles Padró, and Daniel Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. In *Advances in Cryptology–EUROCRYPT 2008*, pages 471–488. Springer, 2008.

[3] Ronald Cramer, Serge Fehr, and Carles Padró. Algebraic manipulation detection codes. *Science China Mathematics*, 56(7):1349–1358, 2013.

[4] Ronald Cramer, Carles Padró, and Chaoping Xing. Optimal algebraic manipulation detection codes in the constant-error model. In *Theory of Cryptography Conference*, pages 481–501. Springer, 2015.

[5] Stefan Dziembowski, Krzysztof Pietrzak, and Daniel Wichs. Non-Malleable Codes. In *ICS*, pages 434–452, 2010.

[6] Venkatesan Guruswami and Adam Smith. Codes for computationally simple channels: Explicit constructions with optimal rate. In *Foundations of Computer Science (FOCS), 2010 51st Annual IEEE Symposium on*, pages 723–732. IEEE, 2010.

[7] Xiang He and Aylin Yener. Secure communication with a byzantine relay. In *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, pages 2096–2100. IEEE, 2009.

[8] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. Northholland Publishing Company, 2nd edition, 1978.

[9] César Polcino Milies and Sudarshan K Sehgal. *An introduction to group rings*, volume 1. Spring, 2002.

[10] Alexander Pott. *Finite geometry and character theory*. Springer-Verlag Berlin Heidelberg, 1995.

[11] Douglas R Stinson. *Cryptography: theory and practice*. CRC press, 2005.

[12] Zhen Wang and Mark Karpovsky. Algebraic manipulation detection codes and their applications for design of secure cryptographic devices. In *On-Line Testing Symposium (IOLTS), 2011 IEEE 17th International*, pages 234–239. IEEE, 2011.