Leakage-resilient Algebraic Manipulation Detection Codes with Optimal Parameters [☆]

Divesh Aggarwal[a], Tomasz Kazana[b], Maciej Obremski[c]

[a] *National University of Singapore*
[b] *University of Warsaw*
[c] *Aarhus University*

Abstract

Algebraic Manipulation Detection (AMD) codes [CDF+08] are keyless message authentication codes that protect messages against additive tampering by the adversary assuming that the adversary cannot "see" the codeword. For certain applications, it is unreasonable to assume that the adversary computes the added offset without any knowledge of the codeword c. Recently, Ahmadi and Safavi-Naini [AS13], and then Lin, Safavi-Naini, and Wang [LSW16] gave a construction of leakage-resilient AMD codes where the adversary has some partial information about the codeword before choosing added offset, and the scheme is secure even conditioned on this partial information.

In this paper we show the bounds on the leakage rate ρ and the code rate κ for leakage-resilient AMD codes. In particular we prove that $2\rho + \kappa < 1$ and for the weak case (security is averaged over a uniformly random message) $\rho + \kappa < 1$. These bounds hold even if adversary is polynomial-time bounded, as long as we allow leakage function to be arbitrary.

We present the constructions of AMD codes that (asymptotically) fulfill above bounds for almost full range of parameters ρ and κ. This shows that above bounds and constructions are in-fact optimal.

In the last section we show that if a leakage function is computationally bounded (we use Ideal Cipher Model) then it is possible to break these bounds.

[☆] This work was supported by:

- Polish National Science Centre (NCN) SONATA GRANT UMO-2014/13/D/ST6/03252;
- Singapore Ministry of Education and the National Research Foundation, also through the Tier 3 Grant "Random numbers from quantum processes" MOE2012-T3-1-009;
- European research Council (ERC) under the European Unions's Horizon 2020 research and innovation programme (grant agreement No 669255.

1. Introduction

Algebraic Manipulation Detection (AMD) codes [CDF+08] are keyless message authentication codes that protect messages against additive tampering by the adversary assuming that the adversary cannot "see" the codeword. In AMD codes, a message $m \in \{0,1\}^k$ is encoded to a codeword C in $\{0,1\}^n$, and the codeword is stored such that the adversary cannot get any information about the codeword. The adversary is assumed to be able to add an arbitrary element A to C such that $C + \mathsf{A}$ could potentially decode to a message $m' \neq m$. In a δ-secure AMD code, such a manipulation succeeds with probability δ, and with probability $1 - \delta$, the decoder on input $c + \mathsf{A}$, either outputs m or a special symbol $\perp$ indicating that the tampering (by the adversary) has been detected. Another notion that has been considered in [CDF+08] is that of weakly secure AMD codes (also called weak AMD codes), where the security guarantee is only for a uniformly random message over the message space $\{0,1\}^k$, and the coding scheme is deterministic.

As mentioned in [CDF+08], AMD codes find useful applications in linear secret sharing schemes (e.g. Shamir's secret sharing [Sha79]) and Fuzzy Extractors [DORS06]. In particular, AMD codes can be used to turn any linear secret sharing scheme into a so called *robust secret sharing scheme* [TW89], which ensures that no unqualified subset of players can modify their shares and cause the reconstruction of a string s' which is different from the secret s. Similarly, AMD codes can help turn fuzzy extractors into robust fuzzy extractors that were first considered by Boyen et al. [Boy04, BDK+05]. We direct the reader to [CDF+08] for a more detailed discussion of these applications.

For certain applications, it is unreasonable to assume that the adversary computes the offset A without any knowledge of the codeword c. Recently, Ahmadi and Safavi-Naini [AS13], and then Lin, Safavi-Naini, and Wang [LSW16] gave a construction of so called ρ-Linear Leakage-Resilient AMD (ρ-LLR-AMD) codes where the adversary has some partial information about the codeword c before choosing A, and the scheme is secure even conditioned on this partial information. In [AS13], the authors consider the notion of a coding scheme from $m \in \{0,1\}^k$ to $c \in \{0,1\}^n$ where the encoding algorithm uses randomness $R \in \{0,1\}^\sigma$, and the adversary computes A given partial information Z such that the entropy of R conditioned on Z is at least $(1-\rho)\sigma$. A similar notion of weak ρ-LLR-AMD codes was defined and constructed where the security is for a uniformly random message M, and the entropy of M conditioned on Z is assumed to be at least $(1-\rho)k$.

In the subsequent work, Lin, Safavi-Naini, and Wang [LSW16] considered a stronger notion of ρ-AMD codes, where Z carries information about the codeword, and the entropy of the codeword C conditioned on Z is at least $(1-\rho)n$. Similar to the original AMD codes defined in [CDF+08], the authors defined weak and strong ρ-AMD codes as deterministic and randomized codes that guarantee security for a uniformly distributed message and any message, respectively. Since ρ-AMD codes are the main topic of our paper, we briefly restate the main application of ρ-AMD codes as discussed in [LSW16].

Robust ramp secret sharing scheme.. A (t, r)-ramp secret sharing scheme [BM84, IY06] is a secret sharing scheme such that any t or fewer shares reveal nothing about the secret s, and any r or more shares are enough to reconstruct the secret. If the number of shares a is between r and t, then an $\frac{a-t}{r-t}$ fraction of the secret is leaked. By encoding a secret with a ρ-AMD code with error δ, and then using a (t, r)-ramp secret sharing scheme, we can ensure that as long as the number of shares are at most $t + \lfloor \rho(r-t) \rfloor$, the probability of being able to reconstruct the secret is upper bounded by δ. Notice that if we assume that the secret is chosen uniformly at random, then even a weak ρ-AMD code will be sufficient for this application.

For this application, or for that matter any other application of ρ-AMD codes, we want the leakage fraction ρ to be as large as possible and for the efficiency of the scheme, we additionally want the rate of the codeword $\kappa := \frac{k}{n}$ also to be as large as possible. In [LSW16], the authors give a construction of strong ρ-AMD codes with error δ, where $\kappa = \frac{d}{d+2}$, and $\rho = \frac{1}{d+2} - \varepsilon$, where ε is a small constant that depends on δ, and d is a positive integer. In order to maximise the leakage, we can set $d = 1$, which will imply that $\rho \approx \frac{1}{3}$, and the rate of the code is $\frac{1}{3}$. Also, it was shown in [LSW16] that for any strong ρ-AMD code with any error δ, we must have that $\kappa + \rho < 1$. This leads us to the following question.

Question 1. *Does there exist a strong ρ-AMD code with leakage rate $\rho \geq \frac{1}{3}$? Can we obtain a better tradeoff between κ and ρ?*

In this paper, we answer both these questions in the affirmative. In Section 4, we generalise the construction from [LSW16] to obtain a construction of a whole family of ρ-AMD codes for a wider range of parameters. More precisely (see Corollary 14 for details), we have constructions that are secure as long as $2\rho+\kappa < 1$. Moreover, we show in Section 5 that there exists no construction of strong ρ-AMD codes that is secure if $2\rho + \kappa \geq 1$. This means that we covered the whole space of possible values of ρ and κ. (Surprisingly, in Section 6 we prove that if we work in Ideal Cipher Model we can go even further: we can break proven barrier and achieve ρ arbitrary close to 1.)

Similarly, as above, for weak ρ-AMD codes with error δ, Lin et al. gave a construction with $\kappa = \frac{d}{d+1}$, and $\rho = \frac{1}{d+1} - \varepsilon$, where ε is a small constant that depends on δ, and d is a positive integer. Setting $d = 1$, we get $\rho \approx \frac{1}{2}$, and $\kappa = \frac{1}{2}$. They, however, failed to obtain any nontrivial condition under which there exist weak ρ-AMD codes. We can again ask a question similar to Question 1 for weak ρ-AMD codes.

Question 2. *Does there exist a weak ρ-AMD code with leakage rate $\rho \geq \frac{1}{2}$? Can we obtain some nontrivial tradeoff between κ and ρ?*

We answer the first question in the negative and the second in the affirmative by showing in Section 5 that for any there exists no weak ρ-AMD code with $\rho + \kappa \geq 1$, or $\rho \geq \kappa$. In other words, for any secure weak ρ-AMD code, we must have $\rho + \kappa < 1$, and $\rho < \kappa$. We also include a construction achieving parameters similar to [LSW16] in Section 4.

We would again like to remark that all our constructions and proofs in Section 4 closely resemble those in [CDF+08, LSW16]. Our main contribution is to show that these constructions are optimal and that we can cover the whole space of feasible parameters.

2. Preliminaries

For an integer $m \in \mathbb{N}$, we denote the set of integers $\{1, \ldots, m\}$ by $[m]$. Unless otherwise stated, $\mathbb{F} = \mathbb{F}_q$ denotes a finite field of size q.

The *min-entropy* of a random variable X is defined as $\mathbf{H}_\infty(X) \stackrel{\text{def}}{=} -\log(\max_x \Pr[X = x])$. We also define *average (aka conditional) min-entropy* of a random variable X conditioned on another random variable Z as

$$\begin{aligned}\widetilde{\mathbf{H}}_\infty(X|Z) &\stackrel{\text{def}}{=} -\log\left(\mathbb{E}_{z\leftarrow Z}\left[\max_x \Pr[X = x|Z = z]\right]\right)\\ &= -\log\left(\mathbb{E}_{z\leftarrow Z}\left[2^{-\mathbf{H}_\infty(X|Z=z)}\right]\right) .\end{aligned}$$

where $\mathbb{E}_{z\leftarrow Z}$ denotes the expected value over $z \leftarrow Z$.

We will need the following result.

Lemma 3. *Let $0 < p < 1$, and let $E_1, \ldots, E_t$ be pairwise independent events such that $\Pr(E_i) = p$ for all $i \in [t]$. Then*

$$\Pr(\cup_{i=1}^t E_i) \geq t \cdot p - \frac{t^2 \cdot p^2}{2} .$$

Proof. Using Bonferroni inequality [Bon36], we have that

$$\begin{aligned}\Pr(\cup_{i=1}^t E_i) &\geq \sum_{i=1}^t \Pr(E_i) - \sum_{i,j\in[t],i\neq j} \Pr(E_i \cap E_j)\\ &= t \cdot p - \frac{t(t-1)}{2}p^2\\ &> t \cdot p - \frac{t^2 \cdot p^2}{2} .\end{aligned}$$

□

3. Definitions

We first define a general coding scheme.

Definition 4. *A coding scheme is given by an encoding function $\mathsf{Enc} : \mathbb{F}^k \times \mathbb{F}^\sigma \mapsto \mathbb{F}^n$ from k-length messages to n-length codewords[1], and a decoding function*

[1] The encoding function takes randomness of length σ that we make explicit in the definition for convenience.

$\mathsf{Dec} : \mathbb{F}^n \mapsto \mathbb{F}^k \cup \{\perp\}$ *such that, for each* $m \in \mathbb{F}^k$, $r \in \mathbb{F}^\sigma$, *we have that* $\Pr(\mathsf{Dec}(\mathsf{Enc}(m, r)) = m) = 1$.

Additionally, the coding scheme is called regular if Enc *is a one-to-one function.*

We now define AMD codes.

Definition 5. *Let* $\mathsf{Enc} : \mathbb{F}^k \times \mathbb{F}^\sigma \mapsto \mathbb{F}^n$, $\mathsf{Dec} : \mathbb{F}^n \mapsto \mathbb{F}^k \cup \{\perp\}$ *be a coding scheme. We say that (*Enc, Dec*) is a strong* (ρ, δ)*-AMD code if for any* $m \in \mathbb{F}^k$, R *uniform in* $\mathbb{F}^\sigma$,

$$\Pr[\mathsf{Dec}(\mathsf{Enc}(m, R) + \mathsf{A}(Z)) \notin \{m, \perp\}] \leq \delta \ ,$$

where $Z \in \mathcal{Z}$ *is a leakage variable such that* $\mathbf{H}_\infty(\mathsf{Enc}(m, R)|Z) \geq \mathbf{H}_\infty(\mathsf{Enc}(m, R)) - \rho \cdot (n \log q)$, *and* $A : \mathcal{Z} \mapsto \mathbb{F}^n$ *is an arbitrary function chosen by the adversary.*

If the adversary is only allowed time polynomial in n *to compute* $\mathsf{A}(Z)$, *then the underlying scheme is said to be a* computationally secure strong *(*ρ, δ*)*-AMD code.

If the security guarantee is only for a uniform message distribution, then we call such an AMD code a weak AMD code. More formally,

Definition 6. *Let* $\mathsf{Enc} : \mathbb{F}^k \mapsto \mathbb{F}^n$, $\mathsf{Dec} : \mathbb{F}^n \mapsto \mathbb{F}^k \cup \{\perp\}$ *be a coding scheme.*[2] *We say that (*Enc, Dec*) is a weak* (ρ, δ)*-AMD code if for* M *uniform in* $\mathbb{F}^k$, *we have that*

$$\Pr[\mathsf{Dec}(\mathsf{Enc}(M) + \mathsf{A}(Z)) \notin \{M, \perp\}] \leq \delta \ ,$$

where $Z \in \mathcal{Z}$ *is a leakage variable such that* $\mathbf{H}_\infty(\mathsf{Enc}(M)|Z) \geq \mathbf{H}_\infty(\mathsf{Enc}(M)) - \rho n \log q$, *and* $A : \mathcal{Z} \mapsto \mathbb{F}^n$ *is an arbitrary function chosen by the adversary.*

If the adversary is only allowed time polynomial in n *to compute* $\mathsf{A}(Z)$, *then the underlying scheme is said to be a computationally secure weak* (ρ, δ)*-AMD code.*

4. Constructing Leakage-resilient AMD codes

In the following, we show that given AMD codes with no leakage, we can construct leakage-resilient AMD codes.

Lemma 7. *For any* $\delta > 0$, $0 < \rho < 1$, *any regular coding scheme* $\mathsf{Enc} : \mathbb{F}^k \times \mathbb{F}^\sigma \mapsto \mathbb{F}^n$, $\mathsf{Dec} : \mathbb{F}^n \mapsto \mathbb{F}^k \cup \{\perp\}$ *that is a strong* $(0, \delta)$*-AMD code is also a strong* $(\rho, q^{\rho n}\delta)$*-AMD code.*

Proof. Since $(\mathsf{Enc}, \mathsf{Dec})$ is a $(0, \delta)$-AMD code, we have that for a uniform R in $\mathbb{F}^\sigma$, and any $m \in \mathbb{F}^k, \alpha \in \mathbb{F}^n$,

$$\Pr(\mathsf{Dec}(\mathsf{Enc}(m, R) + \alpha) \notin \{m, \perp\}) \leq \delta \ .$$

[2] Weak AMD codes assume that the encoding scheme is deterministic.

Define $\mathsf{BAD}(m, \alpha)$ to be the set of all c in the support of $\mathsf{Enc}(m, R)$ such that $\mathsf{Dec}(c + \alpha) \notin \{m, \perp\}$. From the equation above, we have that

$$|\mathsf{BAD}(m, \alpha)| \leq \delta \cdot q^{\sigma} \ . \tag{8}$$

Now, consider a leakage variable Z such that $\mathbf{H}_{\infty}(\mathsf{Enc}(m, R)|Z) \geq \mathbf{H}_{\infty}(\mathsf{Enc}(m, R)) - \rho n \log q$. Since $(\mathsf{Enc}, \mathsf{Dec})$ is a regular coding scheme, we have that $\mathbf{H}_{\infty}(\mathsf{Enc}(m, R)) = \mathbf{H}_{\infty}(R) = \sigma \log q$, and hence $\mathbf{H}_{\infty}(\mathsf{Enc}(m, R)|Z) \geq (\sigma - \rho n) \log q$. Thus, using the definition of conditional min-entropy, we have that

$$\sum_{z \in \mathcal{Z}} \Pr(Z = z) \cdot \max_{c \in \mathbb{F}^n} \Pr(\mathsf{Enc}(m, R) = c \mid Z = z) \leq \frac{1}{q^{\sigma - \rho n}} \ . \tag{9}$$

We now bound the probability of incorrect decoding when the adversary computes the offset given Z.

$$\begin{aligned}
&\Pr[\mathsf{Dec}(\mathsf{Enc}(m, R) + \mathsf{A}(Z)) \notin \{m, \perp\}] \\
&= \sum_{z \in \mathcal{Z}} \Pr[\mathsf{Dec}(\mathsf{Enc}(m, R) + \mathsf{A}(Z)) \notin \{m, \perp\} \mid Z = z] \cdot \Pr[Z = z] \\
&= \sum_{z \in \mathcal{Z}} \Pr[\mathsf{Dec}(\mathsf{Enc}(m, R) + \mathsf{A}(Z)) \notin \{m, \perp\} \mid Z = z] \cdot \Pr[Z = z] \\
&= \sum_{z \in \mathcal{Z}} \Pr[\mathsf{Enc}(m, R) \in \mathsf{BAD}(m, \mathsf{A}(Z)) \mid Z = z] \cdot \Pr[Z = z] \\
&\leq \sum_{z \in \mathcal{Z}} |\mathsf{BAD}(m, \mathsf{A}(Z)| \max_{c \in \mathbb{F}^n} \Pr(\mathsf{Enc}(m, R) = c \mid Z = z) \cdot \Pr(Z = z) \\
&\leq \delta \cdot q^{\sigma} \cdot \frac{1}{q^{\sigma - \rho n}} \\
&= \delta \cdot q^{\rho n} \ ,
\end{aligned}$$

where the last inequality uses the inequalities (8) and (9). □

Similar to the above, we can construct weak AMD codes with leakage from a weak AMD code without leakage. The proof of the following lemma is similar to that of Lemma 7, but we include it here for completeness.

Lemma 10. *For any $\delta > 0$, $0 < \rho < 1$, any regular coding scheme $\mathsf{Enc} : \mathbb{F}^k \mapsto \mathbb{F}^n$, $\mathsf{Dec} : \mathbb{F}^n \mapsto \mathbb{F}^k \cup \{\perp\}$ that is a weak $(0, \delta)$-AMD code is also a weak $(\rho, q^{\rho n}\delta)$-AMD code.*

Proof. Since $(\mathsf{Enc}, \mathsf{Dec})$ is a $(0, \delta)$-AMD code, we have that for a uniform M in $\mathbb{F}^k$, and any $\alpha \in \mathbb{F}^n$,

$$\Pr(\mathsf{Dec}(\mathsf{Enc}(M) + \alpha) \notin \{M, \perp\}) \leq \delta \ .$$

Define $\mathsf{BAD}(\alpha)$ to be the set of all c in the support of $\mathsf{Enc}(M)$ such that $\mathsf{Dec}(c + \alpha) \notin \{M, \perp\}$. From the equation above, we have that

$$|\mathsf{BAD}(\alpha)| \leq \delta \cdot q^{k} \ . \tag{11}$$

Now, consider a leakage variable Z such that $\mathbf{H}_\infty(\mathsf{Enc}(M)|Z) \geq \mathbf{H}_\infty(\mathsf{Enc}(M)) - \rho n \log q$. Since $(\mathsf{Enc}, \mathsf{Dec})$ is a regular coding scheme, we have that $\mathbf{H}_\infty(\mathsf{Enc}(M)) = \mathbf{H}_\infty(M) = k \log q$, and hence $\mathbf{H}_\infty(\mathsf{Enc}(M)|Z) \geq (k - \rho n) \log q$. Thus, using the definition of conditional min-entropy, we have that

$$\sum_{z \in \mathcal{Z}} \Pr(Z = z) \cdot \max_{c \in \mathbb{F}^n} \Pr(\mathsf{Enc}(M) = c \mid Z = z) \leq \frac{1}{q^{k-\rho n}} \ . \tag{12}$$

We now bound the probability of incorrect decoding when the adversary computes the offset given Z.

$$\begin{aligned}
&\Pr[\mathsf{Dec}(\mathsf{Enc}(M) + \mathsf{A}(Z)) \notin \{M, \perp\}] \\
&= \sum_{z \in \mathcal{Z}} \Pr[\mathsf{Dec}(\mathsf{Enc}(M) + \mathsf{A}(Z)) \notin \{M, \perp\} \mid Z = z] \cdot \Pr[Z = z] \\
&= \sum_{z \in \mathcal{Z}} \Pr[\mathsf{Dec}(\mathsf{Enc}(M) + \mathsf{A}(Z)) \notin \{M, \perp\} \mid Z = z] \cdot \Pr[Z = z] \\
&= \sum_{z \in \mathcal{Z}} \Pr[\mathsf{Enc}(M) \in \mathsf{BAD}(\mathsf{A}(Z)) \mid Z = z] \cdot \Pr[Z = z] \\
&\leq \sum_{z \in \mathcal{Z}} |\mathsf{BAD}(\mathsf{A}(Z)| \max_{c \in \mathbb{F}^n} \Pr(\mathsf{Enc}(M) = c \mid Z = z) \cdot \Pr(Z = z) \\
&\leq \delta \cdot q^k \cdot \frac{1}{q^{k-\rho n}} \\
&= \delta \cdot q^{\rho n} \ ,
\end{aligned}$$

where the last inequality uses the inequalities (11) and (12). □

We now give a construction of an efficient coding scheme without any leakage.

Theorem 13. *For any positive integers $k < q - 2, \sigma$, there exists an efficient regular coding scheme $\mathsf{Enc} : \mathbb{F}^k \times \mathbb{F}^\sigma \mapsto \mathbb{F}^{k+2\sigma}$, $\mathsf{Dec} : \mathbb{F}^{k+2\sigma} \mapsto \mathbb{F}^k \cup \{\perp\}$ that is a strong $(0, \left(\frac{k+1}{q}\right)^\sigma)$-AMD code.*

Proof. Let $f : \mathbb{F}^k \times \mathbb{F} \mapsto \mathbb{F}$ be defined as

$$\forall m \in \mathbb{F}^k,\ a \in \mathbb{F},\ f(m, a) := a^{k+2} + \sum_{i=1}^{k} m_i a^i \ ,$$

where $m = (m_1, \ldots, m_k)$ such that $m_i \in \mathbb{F}$ for $i \in [k]$. Then consider the coding scheme is defined as

$$\forall m \in \mathbb{F}^k, x \in \mathbb{F}^\sigma,\ \mathsf{Enc}(m, x) := (m, x, f(m, x_1), \ldots, f(m, x_\sigma)) \ ,$$

The decoding function Dec on input $m' \in \mathbb{F}^k, x' \in \mathbb{F}^\sigma, y_1, \ldots, y_\sigma \in \mathbb{F}$ checks whether $y_i = f(m', x'_i)$ for $i \in [\sigma]$. If there exists an i such that $y_i \neq f(m', x'_i)$, then $\mathsf{Dec}(m', x', y_1, \ldots, y_\sigma) = \perp$, else $\mathsf{Dec}(m', x', y_1, \ldots, y_\sigma) = m'$.

Clearly the coding scheme is regular. We now proceed to show that the scheme is secure.

For any $m \in \mathbb{F}^k$, $\alpha \in \mathbb{F}^k$, $\beta \in \mathbb{F}^\sigma$, $\gamma \in \mathbb{F}^\sigma$, and a uniform $X \in \mathbb{F}^\sigma$ we need to bound

$$\Pr(\mathsf{Dec}(\mathsf{Enc}(m, X) + (\alpha, \beta, \gamma)) \notin \{m, \perp\}) .$$

Notice that if $\alpha = 0$, then the above probability is 0, since by definition, for any m, β, γ, $\mathsf{Dec}(\mathsf{Enc}(m, X) + (\alpha, \beta, \gamma))$ is either m or $\perp$. Also, if $\alpha \neq 0$, then $\mathsf{Dec}(\mathsf{Enc}(m, X) + (\alpha, \beta, \gamma))$ is either $m + \alpha \neq m$, or $\perp$. Thus, it is sufficient to bound

$$\Pr(\mathsf{Dec}(\mathsf{Enc}(m, X) + (\alpha, \beta, \gamma)) \neq \perp)$$

for any $m \in \mathbb{F}^k$, $\alpha \in \mathbb{F}^k \setminus \{0\}$, $\beta \in \mathbb{F}^\sigma$, $\gamma \in \mathbb{F}^\sigma$, and a uniform $X \in \mathbb{F}^\sigma$. Using the independence of $X_1, \ldots, X_\sigma$, we have that

$$\begin{aligned}
&\Pr(\mathsf{Dec}(\mathsf{Enc}(m, X) + (\alpha, \beta, \gamma)) \neq \perp) \\
&= \prod_{j=1}^{\sigma} \Pr\left(X_j^{k+2} + \sum_{i=1}^{k} m_i X_j^i + \gamma_j = (X_j + \beta_j)^{k+2} + \sum_{i=1}^{k} (m_i + \alpha_i)(X_j + \beta_j)^i \right) \\
&= \prod_{j=1}^{\sigma} \Pr\left(X_j^{k+2} + \sum_{i=1}^{k} m_i X_j^i + \gamma_j - (X_j + \beta_j)^{k+2} - \sum_{i=1}^{k} (m_i + \alpha_i)(X_j + \beta_j)^i = 0 \right) \\
&\leq \left(\frac{k+1}{q} \right)^{\sigma} ,
\end{aligned}$$

since

$$P(X_j) = X_j^{k+2} + \sum_{i=1}^{k} m_i X_j^i + \gamma_j - (X_j + \beta_j)^{k+2} - \sum_{i=1}^{k} (m_i + \alpha_i)(X_j + \beta_j)^i$$

is a non-zero polynomial in X_j of degree at most $k+1$. To see that the polynomial is non-zero, note that if $\beta_j \neq 0$, then the co-efficient of X_j^{k+2} in $P(X_j)$ is zero, and that of X_j^{k+1} is $(k+2)\beta_j \neq 0$. On the other hand, if $\beta_j = 0$, then let t be the largest index such that $\alpha_t \neq 0$. Note that one such index exists since $\alpha \neq 0$. Then, the coefficients of $X_j^{k+2}, \ldots, X_j^{t+1}$ in $P(X_j)$ are 0, and that of X^t is $-\alpha_t \neq 0$.

The desired result follows. □

The following corollary immediately follows from Lemma 7 and Theorem 13.

Corollary 14. *For any positive integers $k < q - 2, \sigma$, and $0 < \rho < \frac{1}{2}$, there exists an efficient regular coding scheme $\mathsf{Enc} : \mathbb{F}^k \times \mathbb{F}^\sigma \mapsto \mathbb{F}^{k+2\sigma}$, $\mathsf{Dec} : \mathbb{F}^{k+2\sigma} \mapsto \mathbb{F}^k \cup \{\perp\}$ that is a strong $(\rho, q^{\rho(k+2\sigma)-\sigma}(k+1)^\sigma)$-AMD code.*

We remark that assuming $q \gg k$, as long as $\rho < \frac{\sigma}{k+2\sigma}$, or in other words, $2\rho + \kappa < 1$, the above construction is secure.

Now we will construct weak AMD codes without any leakage. Notice that a construction with similar parameters was already shown in [LSW16]. We include the construction here for completeness. In Section 5, we show that the parameters obtained in this construction are optimal.

Theorem 15. *Let k be a positive integer, and let the characteristic of $\mathbb{F}$ be greater than 2. Then there exists an efficient regular coding scheme $\mathsf{Enc} : \mathbb{F}^k \mapsto \mathbb{F}^{k+1}$, $\mathsf{Dec} : \mathbb{F}^{k+1} \mapsto \mathbb{F}^k \cup \{\perp\}$ that is a weak $(0, \frac{1}{q})$-AMD code.*

Proof. Let $g : \mathbb{F}^k \mapsto \mathbb{F}$ be defined as

$$\forall m \in \mathbb{F}^k,\ g(m) := \sum_{j=1}^{k} m_j^2 \ .$$

where $m = (m_1, \ldots, m_k)$ such that $m_j \in \mathbb{F}$ for $j \in [k]$. Then consider the coding scheme is defined as

$$\forall m \in \mathbb{F}^k,\ \mathsf{Enc}(m) := (m, g(m)) \ ,$$

The decoding function Dec on input $m' \in \mathbb{F}^k, y \in \mathbb{F}$ checks whether $y = g(m')$. If $y \neq g_i(m')$, then $\mathsf{Dec}(m', y) = \perp$, else $\mathsf{Dec}(m', y) = m'$.

For any $\alpha \in \mathbb{F}^k$, $\beta \in \mathbb{F}$, and a uniform $M \in \mathbb{F}^k$ we need to bound

$$\Pr(\mathsf{Dec}(\mathsf{Enc}(M) + (\alpha, \beta)) \notin \{M, \perp\}) \ .$$

Notice that if $\alpha = 0$, then the above probability is 0, since by definition, for any β, $\mathsf{Dec}(\mathsf{Enc}(M) + (\alpha, \beta))$ is either M or $\perp$. Also, if $\alpha \neq 0$, then $\mathsf{Dec}(\mathsf{Enc}(M) + (\alpha, \beta))$ is either $M + \alpha \neq M$, or $\perp$. Thus, it is sufficient to bound

$$p = \Pr(\mathsf{Dec}(\mathsf{Enc}(M) + (\alpha, \beta)) \neq \perp)$$

for any $\alpha \in \mathbb{F}^k \setminus \{0\}$, $\beta \in \mathbb{F}$, and a uniform $M \in \mathbb{F}^k$. Without loss of generality, let $\alpha_i \neq 0$. Then,

$$\begin{aligned} p &= \Pr\left(\sum_{j=1}^{k} \left((M_j + \alpha_j)^2 - M_j^2\right) = \beta\right) \\ &= \Pr\left(\sum_{j=1}^{k} \left(2\alpha_j M_j + \alpha_j^2\right) = \beta\right) \\ &= \Pr(2\alpha_i M_i = A) \ , \end{aligned}$$

where A depends on $M_1, \ldots, M_{i-1}, M_{i+1}, \ldots, M_k, \alpha_1, \ldots, \alpha_k, \beta$, and is independent of M_i. Thus, using the independence of M_i from $M_1, \ldots, M_{i-1}, M_{i+1}, \ldots, M_k$, we see that $p = \frac{1}{q}$. □

The following corollary immediately follows from Lemma 10 and Theorem 15.

Corollary 16. *For any positive integers k, and $0 < \rho < \frac{1}{k+1}$, there exists an efficient regular coding scheme $\mathsf{Enc} : \mathbb{F}^k \mapsto \mathbb{F}^{k+1}$, $\mathsf{Dec} : \mathbb{F}^{k+1} \mapsto \mathbb{F}^k \cup \{\perp\}$ that is a weak $(\rho, q^{\rho(k+1)-1})$-AMD code.*

Thus, as long as $\rho < \frac{1}{k+1}$, or in other words, $\rho + \kappa < 1$, and $\rho < \kappa$, the above construction is secure.

5. Optimal Bounds on Leakage and Code Rate

In this section we show that the constructions in Section 4 are asymptotically optimal. In fact, even if we allow that adversary is polynomial-time bounded (as long as the leakage is arbitrary), there still does not exist a construction of leakage resilient AMD codes that allow a better tradeoff between the rate of the code and the allowed leakage.

The following corollary is immediate from Lemma 3.

Corollary 17. *Let $\mathbb{F}_N$ be a finite field, and let A, B be uniform and independent in $\mathbb{F}_N$. Let $y_1, \ldots, y_t$ be some fixed distinct elements of $\mathbb{F}_N$. Also, let S be a subset of $\mathbb{F}_N$. Then the probability that there exists $i \in [t]$ such that $Ay_i + B \in S$ is at least*

$$\frac{t \cdot |S|}{N} - \frac{t^2 \cdot |S|^2}{2N^2} \ .$$

Proof. For all $i \in [t]$, let E_i be the event that $Ay_i + B \in S$. It is easy to see that $E_1, \ldots, E_t$ are pairwise independent. To see this, note that for any $a, b \in \mathbb{F}_N$, and any $i, j \in [t]$ such that $i \neq j$, we have that

$$\begin{aligned} \Pr(Ay_i + B = a, Ay_j + B = b) &= \Pr\left(A = \frac{b-a}{y_j - y_i}\right) \Pr\left(B = \frac{by_i - ay_j}{y_i - y_j}\right) \\ &= \frac{1}{N^2} \\ &= \Pr(Ay_i + B = a) \cdot \Pr(Ay_j + B = b) \ . \end{aligned}$$

The result then follows from Lemma 3. □

We are now ready to prove the optimality of our leakage-resilient AMD codes.

Theorem 18. *For any $\rho \in (0,1)$, there does not exist a computationally secure strong $(\rho, \frac{3}{16})$-AMD code $\mathsf{Enc} : \{0,1\}^k \times \{0,1\}^\sigma \mapsto \{0,1\}^n$, $\mathsf{Dec} : \{0,1\}^n \mapsto \{0,1\}^k \cup \{\perp\}$ with $2\rho + \frac{k}{n} \geq 1$.*

Proof. Let R be uniform in $\{0,1\}^\sigma$. Also, let $t = 2^{(n-k)/2}$. We divide the proof in two cases.

CASE 1: There exists a message m such that the support of $\mathsf{Enc}(m, R)$ has cardinality at most t. Let $\mathcal{C}(m)$ be the support of $\mathsf{Enc}(m, R)$. We define the set of good codewords $\mathcal{G} \subseteq \mathcal{C}(m)$ such that

$$\mathcal{G} := \{c \in \mathcal{C}(m) \ : \ \Pr(\mathsf{Enc}(m, R) = c) \geq \frac{1}{2t} \ .$$

The probability that $\mathsf{Enc}(m, R) \notin \mathcal{G}$ is less than $\frac{1}{2t} \cdot t = \frac{1}{2}$. Thus, the probability that $C = \mathsf{Enc}(m, R) \in \mathcal{G}$ is greater than $\frac{1}{2}$.

Now, we interpret the domain of the randomness of the Enc function, i.e., $\{0,1\}^\sigma$ as a finite field of size 2^σ, and let A, B be uniformly random

variables in $\{0,1\}^\sigma$ chosen by the adversary. Also, let $y_1, \ldots, y_t$ be fixed and distinct elements of $\{0,1\}^\sigma$.

We define the random variable Z to be the index $i \in [t]$ such that $\mathsf{Enc}(m, Ay_i + B) = \mathsf{Enc}(m, R)$. If no such i exists, then Z is chosen to be an arbitrary index in $[t]$. Furthermore, we fix a codeword c^* such that $\mathsf{Dec}(c^*) \notin \{m, \perp\}$.

Then the function $\mathsf{A}(Z)$ chosen by the adversary is defined as

$$\mathsf{A}(Z) = -\mathsf{Enc}(m, Ay_Z + B) + c^* \ .$$

Notice that $\mathsf{Dec}(\mathsf{Enc}(m, R) + \mathsf{A}(Z)) = \mathsf{Dec}(c^*)$ if $\mathsf{Enc}(m, R) \in \mathcal{G}$ and there exists an $i \in [t]$ such that $\mathsf{Enc}(m, Ay_i + B) = \mathsf{Enc}(m, R)$. Conditioned on the event that $\mathsf{Enc}(m, R) \in \mathcal{G}$ (which happens with probability greater than $1/2$), the number of $r \in \{0,1\}^\sigma$ such that $\mathsf{Enc}(m, r) = \mathsf{Enc}(m, R)$ is at least $\frac{2^\sigma}{2t}$. Thus, using Corollary 17, the probability that there exists an $\in [t]$ such that $\mathsf{Enc}(m, Ay_i + B) = \mathsf{Enc}(m, R)$ is at least

$$\frac{t}{2t} - \frac{t^2}{2 \cdot 4t^2} = 3/8 \ .$$

Thus, $\mathsf{Dec}(\mathsf{Enc}(m, R) + \mathsf{A}(Z)) = \mathsf{Dec}(c^*) \notin \{m, \perp\}$ with probability $3/16$.

CASE 2: For every message m', the support of $\mathsf{Enc}(m', R)$ has cardinality greater than t. We fix a message $m \in \{0,1\}^k$, and the codeword $C = \mathsf{Enc}(m, R)$.

Now, we interpret the code space, i.e., $\{0,1\}^n$ as a finite field of size 2^n, and let A, B be uniformly random variables in $\{0,1\}^n$ chosen by the adversary. Also, let $y_1, \ldots, y_t$ be fixed and distinct elements of $\{0,1\}^n$. We define the random variable Z to be the index $i \in [t]$ such that $\mathsf{Dec}(C + Ay_i + B) \notin \{m, \perp\}$. If no such i exists, then Z is chosen to be an arbitrary index in $[t]$. The function $\mathsf{A}(Z)$ chosen by the adversary is defined as $Ay_Z + B$.

We now compute the probability that $\mathsf{Dec}(C + \mathsf{A}(Z)) \notin \{m, \perp\}$. The number of strings $x \in \{0,1\}^n$ such that $\mathsf{Dec}(C + x) \notin \{m, \perp\}$ is greater than $(2^k - 1)t$ since by assumption, for every message m', the support of $\mathsf{Enc}(m', R)$ has cardinality greater than t. Thus, using Corollary 17, the probability that there exists an index $i \in [t]$ such that $\mathsf{Dec}(C + Ay_i + B) \notin \{m, \perp\}$ is at least

$$\frac{t^2(2^k - 1)}{2^n} - \frac{t^4(2^k - 1)^2}{2 \cdot 2^{2n}} = \frac{1}{2} - \frac{1}{2^{2k+1}} \geq \frac{3}{8} \ ,$$

for $k \geq 1$.

□

Next, we show that there is no leakage-resilient (even computationally secure) weak AMD code from k-bit messages to n-bit codewords with leakage rate ρ such that $\rho + \frac{k}{n} \geq 1$.

Theorem 19. *For any $\rho \in (0,1)$, there does not exist a computationally secure weak $(\rho, \frac{3}{8})$-AMD code $\mathsf{Enc} : \{0,1\}^k \mapsto \{0,1\}^n$, $\mathsf{Dec} : \{0,1\}^n \mapsto \{0,1\}^k \cup \{\perp\}$ with $\rho + \frac{k}{n} \geq 1$ or $\rho \geq \frac{k}{n}$.*

Proof. Let M be chosen uniformly at random in $\{0,1\}^k$, and let $C = \mathsf{Enc}(M)$ be fixed. If $\rho \geq \frac{k}{n}$, then let Z be $\mathsf{Dec}(C)$, and let $\mathsf{A}(Z)$ be $-\mathsf{Enc}(Z) + \mathsf{Enc}(m')$ for some $m' \in \{0,1\}^k \setminus \{M\}$. Then, it is easy to see that $\mathsf{Dec}(C + \mathsf{A}(Z)) = m' \notin \{M, \perp\}$ with probability 1. This shows that $\rho < \frac{k}{n}$.

Let $t = 2^{n-k}$. We interpret the code space, i.e., $\{0,1\}^n$ as a finite field of size 2^n, and let A, B be uniformly random variables in $\{0,1\}^n$ chosen by the adversary. Also, let $y_1, \ldots, y_t$ be fixed and distinct elements of $\{0,1\}^n$. We define the random variable Z to be the index $i \in [t]$ such that $\mathsf{Dec}(C + Ay_i + B) \notin \{M, \perp\}$. If no such i exists, then Z is chosen to be an arbitrary index in $[t]$. The function $\mathsf{A}(Z)$ chosen by the adversary is defined as $Ay_Z + B$.

We now compute the probability that $\mathsf{Dec}(C + \mathsf{A}(Z)) \notin \{M, \perp\}$. The number of strings $x \in \{0,1\}^n$ such that $\mathsf{Dec}(C + x) \notin \{m, \perp\}$ is $2^k - 1$, one corresponding to each message in $\{0,1\}^k \setminus \{M\}$. Thus, using Corollary 17, the probability that there exists an index $i \in [t]$ such that $\mathsf{Dec}(C + Ay_i + B) \notin \{M, \perp\}$ is at least

$$\frac{t(2^k - 1)}{2^n} - \frac{t^2(2^k - 1)^2}{2 \cdot 2^{2n}} = \frac{1}{2} - \frac{1}{2^{2k+1}} \geq \frac{3}{8}\,,$$

for $k \geq 1$. □

6. Breaking the $\rho < \frac{1}{2}$ barrier for AMD codes in the Ideal Cipher Model

In Section 5 we state an inequality $2\rho + \frac{k}{n} \geq 1$ that must hold for all strong $(\rho, 3/16)$-AMD codes as introduced in Definition 5. The definition assumes that the leakage variable Z is arbitrary with the only constraint being that the entropy of the codeword conditioned on the knowledge of Z is $1 - \rho$ fraction of the original entropy. However, as we will see in this section, our result does not necessarily hold if we impose further conditions on the leakage variable Z.

We will work in the Ideal Cipher Model (abbr. ICM), which is equivalent to the Random Oracle Model, see [CHK+16]). As a reminder: ICM is a model with a public oracle (accessible fully to all parties) that gives access to a family $\{f_i\}_{i \in I}$ of random (and independent) permutations. Any party may ask for $f_i(u)$ and for $f_i^{-1}(u)$ for any chosen i and u. For our application we can even simplify the model and assume that we have only one random permutation f with access to both forward and inverse queries to the oracle for f.

We will consider the following simple encoding: $\mathsf{Enc}_{br}(m, r) = (m, f(m, r))$, where $m \in \mathbb{F}^k$, $f : \mathbb{F}^k \times \mathbb{F}^\sigma \mapsto \mathbb{F}^{2k+\sigma}$ is the oracle permutation from ICM described above and $r \in \mathbb{F}^\sigma$ is some (potentially huge in comparison to m) randomness. Obviously the function Enc_{br} is efficient and also there exists efficient decoding function that may efficiently (using f^{-1} oracle) check if the codeword is correct.

Now we are ready for introducing the theorem about an interesting property of Enc_{br}. Please note that this time we assume something about Z from Definiton 5. More specifically: We assume that Z is computed by some Turing Machine (called leakage oracle) that is bounded by the number of queries to the ICM oracle.

Theorem 20. *The above* Enc_{br} *is a strong* $(\rho, q^{-k} + t/q^{\sigma-\rho n})$*-AMD code in the Ideal Cipher Model if the number of queries to ICM oracle (made together by both the adversary and the leakage oracle) is bounded by* t*.*

Proof. Let us assume that the adversary knows original m and let us denote by m' the new value of the message in the modified codeword. Also let us denote $x = f(m, r)$. Now the goal of the adversary is to construct e such that $f^{-1}(x + e) = (m', r')$ for some r'.

During the execution, the adversary and the leakage oracle learned at most t values $y_1, \ldots, y_t$ such that $f^{-1}(y_j) = (m', r')$ for some r'. This means that if $(x + e)$ is not equal to any of such y_j for $j \in [t]$, then the result is simply uniform at random so the probability of success is exactly q^{-k}.

So, the only hope to make the probability of winning greater is to pick e such that $x + e = y_j$ for some $1 \leq j \leq t$. However since $\mathbf{H}_\infty(x|Z) \geq \sigma \log q - \rho n \log q$ then this happens with probability less or equal to $\frac{t}{2^{\sigma \log q - \rho n \log q}} = \frac{t}{q^{\sigma - \rho n}}$.

These two facts about two cases above together imply the statement. □

Thus, this construction gives an AMD code in the Ideal Cipher Model with $\rho \approx \frac{\sigma}{2k+\sigma}$, and $\kappa = \frac{k}{2k+\sigma}$. In this case, we can achieve leakage arbitrarily close to 1 by having $k \ll \sigma$.

[AS13] Hadi Ahmadi and Reihaneh Safavi-Naini. Detection of algebraic manipulation in the presence of leakage. *Information Theoretic Security - 7th International Conference, ICITS 2013, Singapore, November 28-30, 2013, Proceedings*, pages 238–258, 2013.

[BDK+05] Xavier Boyen, Yevgeniy Dodis, Jonathan Katz, Rafail Ostrovsky, and Adam Smith. Secure remote authentication using biometric data. In Ronald Cramer, editor, *Advances in Cryptology—EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 147–163. Springer-Verlag, 2005.

[BM84] G. R. Blakley and C. Meadows. Security of ramp schemes. LNCS 196:242–268, 1984.

[Bon36] Bonferroni. Teoria statistica delle classi e calcolo delle probabilita. *Libreria internazionale Seeber*, 1936.

[Boy04] Xavier Boyen. Reusable cryptographic fuzzy extractors. In *11th ACM Conference on Computer and Communication Security*. ACM, October 25–29 2004.

[CDF+08] Ronald Cramer, Yevgeniy Dodis, Serge Fehr, Carles Padro, and Daniel Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. In *EUROCRYPT 2008*, April 2008. To Appear.

[CHK+16] J. Coron, T. Holenstein, R. Kunzler, J. Patarin, Y. Seurin, and S. Tessaro. How to build an ideal cipher: The indifferentiability of the feistel construction. *Journal of Cryptology*, 29(1):61–114, 2016.

[DORS06] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. Technical Report 2003/235, Cryptology ePrint archive, `http://eprint.iacr.org`, 2006. Previous version appeared at *EUROCRYPT 2004*.

[IY06] M. Iwamoto and H. Yamamoto. Strongly secure ramp secret sharing schemes for general access structures. *Information Processing Letters*, 97(2):52–57, January 2006.

[LSW16] Fuchun Lin, Reihaneh Safavi-Naini, and Pengwei Wang. Detecting algebraic manipulation in leaky storage systems. *Information Theoretic Security - 9th International Conference, ICITS 2016, Tacoma, WA, USA, August 9-12, 2016, Revised Selected Papers*, pages 129–150, 2016.

[Sha79] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[TW89] Martin Tompa and Heather Woll. How to share a secret with cheaters. *Journal of Cryptology*, 1.3:133–138, 1989.