Robust and Non-malleable Threshold Schemes, AMD codes and External Difference Families

Douglas R. Stinson

University of Waterloo and Carleton University

SAC 2023
August 16–18, 2023

Road Map

We study robust and non-malleable threshold schemes in two settings:

1. equiprobable sources (secrets)
2. known sources (secrets)

threshold scheme	equiprobable sources	known sources
robust	difference set external difference family weak AMD code	strong EDF strong AMD code
non-malleable	circular EDF weak circular AMD code	strong circular EDF strong circular AMD code

(k, n)-Threshold Schemes

- Let $1 < k \leq n$ and let $\mathcal{S}$ be the set of possible secrets.
- There are n participants in the scheme, denoted $P_1, \ldots, P_n$, as well as an additional participant called the dealer.
- A secret $s \in \mathcal{S}$ is chosen by the dealer.
- The dealer then constructs n shares, which we denote by $s_1, \ldots, s_n$.
- The share s_i is given to participant P_i, for $1 \leq i \leq n$.
- The following two properties should be satisfied.

Correctness: Any set of k participants can recover the secret from the shares that they hold collectively.

Perfect privacy: No set of $k - 1$ or fewer participants can obtain any information about the secret from the shares that they hold collectively.

Shamir's Threshold Scheme

- Suppose $\mathbb{F}_q$ is a finite field, where q is a prime power.
- The (k, n)-threshold scheme will share a secret $s \in \mathbb{F}_q$, where $q \geq n + 1$.

Share: The dealer selects a random polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $k - 1$ such that $f(0) = s$. Each share s_i is an ordered pair, i.e., $s_i = (x_i, y_i)$, where the x_i's are distinct and non-zero and $y_i = f(i)$. The x_i's are public and the y_i's are secret.

Recover: Given k shares, the participants use Lagrange interpolation to reconstruct $f(x)$ and then they evaluate the polynomial $f(x)$ at $x = 0$ to recover the secret s.

Lagrange Interpolation Formula

- Let $y_1, \ldots, y_k \in \mathbb{F}_q$ and let $x_1, \ldots, x_k \in \mathbb{F}_q$ be distinct.
- Then there is a unique polynomial $f(x) \in \mathbb{F}_q[x]$ with degree at most $k-1$ such that $f(x_i) = y_i$ for $1 \leq i \leq k$.
- The Lagrange interpolation formula (LIF) states that

$$f(x) = \sum_{j=1}^{k} y_j \prod_{1 \leq h \leq k, h \neq j} \frac{x - x_h}{x_j - x_h}.$$

- Since $s = f(0)$, it is sufficient to compute

$$s = \sum_{j=1}^{k} y_j \prod_{1 \leq h \leq k, h \neq j} \frac{x_h}{x_h - x_j}.$$

- If we define

$$b_j = \prod_{1 \leq h \leq k, h \neq j} \frac{x_h}{x_h - x_j},$$

for $1 \leq j \leq k$, then we can write $s = \sum_{j=1}^{k} b_j y_j$.

Robust Threshold Schemes

We review the model introduced by Tompa and Woll (1988). Assume a (k, n)-threshold scheme, where the secret s is chosen equiprobably from the set $\mathcal{S}$. Fix t such that $1 \leq t < k$. We consider the following Robustness Game.

1. t of the n shares are given to the adversary. The adversary modifies the t shares to create new "bad shares".
2. A secret s' is reconstructed using the t "bad shares" and $k - t$ of the original "good shares". The adversary may choose which of the "good shares" are used in reconstruction. The adversary wins the robustness game if the reconstructed secret s' is a valid secret and $s' \neq s$.

Typically, we let $t = k - 1$. For $0 < \epsilon < 1$, if the adversary can only win this game with probability at most ϵ, then we say that the threshold scheme is ϵ-robust (here ϵ is the cheating probability).

The Basic Shamir Scheme is Not Robust

- It is possible for a single adversary to win the Robustness Game with probability $\epsilon = 1$.
- Suppose that the first share is modified: $y_1' = y_1 + \delta$, where $\delta \neq 0$.
- Suppose that the first k shares are used to reconstruct the secret.
- Recalling the LIF, the reconstructed secret will be

$$s' = b_1 y_1' + \sum_{j=2}^{k} b_j y_j = b_1(y_1 + \delta) + \sum_{j=2}^{k} b_j y_j = s + b_1\delta \neq s.$$

- Observe also that the adversary knows the relation between s and s', even though they do not know s.

How to Make the Shamir Scheme Robust

- Tompa and Woll's solution requires that both co-ordinates of shares (x_i, y_i) are secret.
- More recent solutions follow the standard convention where only the y-co-ordinate of a share is secret.
- We discuss the approach due to Ogata and Kurosawa (1996).
- The basic idea is that only some secrets are considered to be "valid."
- A secret is first encoded, using a public encoding function, and the resulting encoded secret is shared using Shamir's scheme.
- The encoding function suggested by Ogata and Kurosawa uses a classic combinatorial structure known as a difference set.

Difference Sets

- Suppose that $(G, +)$ is an abelian group of order v.
- $D \subseteq G$ is a (v, m, λ)-difference set if
  1. $|D| = m$ and
  2. for every $g \in G \setminus \{0\}$, there are exactly λ pairs $d_i, d_j \in D$ such that $d_i - d_j = g$.
- If a (v, m, λ)-difference set exists, then $\lambda(v-1) = m(m-1)$.
- If $\lambda = 1$, then $v = m^2 - m + 1$; this is called a planar difference set.
- The development of a planar difference set D, which consists of D and all of its translates, is a finite projective plane of order $m - 1$.

Singer Difference Sets

- $\{0, 1, 3\}$ is a $(7, 3, 1)$-difference set in $\mathbb{Z}_7$.
- Its development consists of the seven 3-sets

$$\begin{array}{llll} \{0,1,3\} & \{1,2,4\} & \{2,3,5\} & \{3,4,6\} \\ \{4,5,0\} & \{5,6,1\} & \{6,0,2\}, & \end{array}$$

  which is the famous Fano plane.
- $\{0, 1, 3, 9\}$ is a $(13, 4, 1)$-difference set.
- $\{3, 6, 12, 7, 14\}$ is a $(21, 5, 1)$-difference set.
- In general, if q is a prime or prime power, then there is a Singer difference set, which is a $(q^2 + q + 1, q + 1, 1)$-difference set in $\mathbb{Z}_{q^2+q+1}$.

The Ogata-Kurosawa Scheme

- Suppose we have a (v, m, λ) difference set D in the abelian group $\mathbb{F}_v$, where v is prime.
- We can use D to robustly share one of m equiprobable secrets, denoted as $s_1, \ldots, s_m$.
- Let $D = \{g_1, \ldots, g_m\}$.
- We require that $v \geq n + 1$ in order to implement a Shamir scheme in $\mathbb{F}_v$.

The Ogata-Kurosawa Scheme works as follows:

1. Given a secret s_i (where $1 \leq i \leq m$), encode s_i as $g = g_i$.
2. Compute shares for the encoded secret g using a (k, n)-Shamir scheme in $\mathbb{F}_v$.
3. To reconstruct a secret from k shares, first use the LIP to reconstruct $g' \in \mathbb{F}_v$.
4. If $g' \notin D$, then g' is invalid; if $g' = g_j$, then the reconstructed (i.e., decoded) secret is s_j.

Analysis of the Ogata-Kurosawa Scheme

- The effect of modifying one or more shares (up to $k-1$ shares) is to replace g by $g+\Delta$, where Δ is a quantity that is known to the $k-1$ adversaries.
- The adversaries win the Robustness Game if $g+\Delta \in D$.
- For any nonzero Δ, there are exactly λ choices of $g \in D$ such that $g+\Delta \in D$.
- Since $|D| = m$ and the secrets are equiprobable, it follows that the adversaries win the Robustness Game with probability λ/m.

Example

- Suppose we start with $D = \{0, 1, 3, 9\}$ which is a $(13, 4, 1)$-difference set.
- We have four secrets and the possible encoded secrets are $0, 1, 3$ and 9.
- We share an encoded secret g using a (k, n)-Shamir scheme implemented over $\mathbb{F}_{13}$ (this requires $n \leq 12$).
- Each possible modification $g \mapsto g + \Delta$, where $\Delta \in \mathbb{F}_{13} \setminus \{0\}$, succeeds with probability $1/4$.
- $\Delta = 1$ succeeds iff $g = 0$;
  $\Delta = 2$ succeeds iff $g = 1$;
  $\Delta = 3$ succeeds iff $g = 0$;
  $\Delta = 4$ succeeds iff $g = 9$;
  etc.

External Difference Families

- Ogata, Kurosawa, Stinson and Saido (2004) observed that external difference families (EDFs) could also be used to construct robust threshold schemes.
- A $(19, 3, 3, 3)$-EDF is given by the three sets $\{1, 7, 11\}$, $\{4, 9, 6\}$ and $\{16, 17, 5\}$ in $\mathbb{Z}_{19}$.
- Every nonzero element of $\mathbb{Z}_{19}$ occurs three times as a difference between two elements in two different sets.
- For the purposes of a robust threshold scheme, there would be three secrets, say s_1, s_2, s_3.
- The secret s_i would be encoded by choosing a random element in the ith set.
- Then the encoded secret is shared, as before.

AMD Codes

- Cramer, Dodis, Fehr, Padró and Wichs (2008) defined algebraic manipulation detection codes (AMD codes).
- They also described applications of these structures to robust secret sharing schemes, robust fuzzy extractors, secure multiparty computation, and non-malleable codes.
- $\mathcal{S}$ is the source space, where $|\mathcal{S}| = m$.
- An additive abelian group $\mathcal{G}$ is the message space.
- For every source $s \in \mathcal{S}$, let $A(s) \subseteq \mathcal{G}$ denote the set of valid encodings of s. We require that $A(s) \cap A(s') = \emptyset$ if $s \neq s'$. Denote $\mathcal{A} = \{A(s) : s \in \mathcal{S}\}$.
- $E : \mathcal{S} \to G$ is a (randomized) encoding function that maps a source $s \in \mathcal{S}$ to $g \in A(s)$ that is chosen uniformly at random.

Security of an AMD Code

- We define a weak AMD code $(\mathcal{S}, \mathcal{G}, \mathcal{A}, E)$ by considering a certain game incorporating an adversary.
- The adversary has complete information about the AMD code.
- Based on this information, the adversary will choose a value $\Delta \neq 0$ from $\mathcal{G}$.
- Suppose $(\mathcal{S}, \mathcal{G}, \mathcal{A}, E)$ is an AMD code.
    1. The value $\Delta \in \mathcal{G} \setminus \{0\}$ is chosen by the adversary.
    2. The source $s \in \mathcal{S}$ is chosen uniformly at random.
    3. s is encoded into $g \in A(s)$ using the encoding function E.
    4. The adversary wins if and only if $g + \Delta \in A(s')$ for some $s' \neq s$.
- The success probability, denoted ϵ_Δ, is the probability that the adversary wins this game.
- The code $(\mathcal{S}, \mathcal{G}, \mathcal{A}, E)$ is an $(v, m, \hat{\epsilon})$-AMD code, where $\hat{\epsilon}$ denotes the success probability of the adversary's optimal strategy (i.e., $\hat{\epsilon} = \max_\Delta\{\epsilon_\Delta\}$.)

R-optimal Weak AMD Codes

- Paterson and Stinson (2016) introduced R-optimal weak AMD codes.
- Recall that m is the number of sources, and the encoded sources are in an abelian group of cardinality v.
- We denote the total number of valid encodings by a.

Theorem 1 (PS16)

In any $(v, m, \hat{\epsilon})$-weak AMD code, it holds that

$$\hat{\epsilon} \geq \frac{a(m-1)}{m(v-1)}.$$

- If we have equality in Theorem 1, then the code is defined to be R-optimal.
- In an R-optimal weak AMD code, any choice of Δ is optimal!

Examples of R-optimal Weak AMD Codes

- We summarize a few results from [PS16].
- An AMD code is ℓ-regular if every every source has exactly ℓ possible encodings.
- In an ℓ-regular AMD code, we have $a = \ell m$ and hence

$$\hat{\epsilon} \geq \frac{a(m-1)}{m(v-1)} = \frac{\ell(m-1)}{v-1}. \qquad (1)$$

- An R-optimal ℓ-regular weak AMD code is equivalent to an (v, m, ℓ, λ)-EDF, where $\lambda = \ell^2 m(m-1)/(v-1)$.
- Note that the lower bound for $\hat{\epsilon}$ is minimized when $\ell = 1$.
- In this case, the optimal R-optimal weak AMD codes are (v, m, λ)-difference sets.

Near-optimal Weak AMD Codes

- Since optimal AMD codes exist only for certain parameters, it is useful for applications to consider "near-optimal" codes.
- Instead of using a difference set, we can employ a cyclic difference packing.
- A (v, m)-cyclic difference packing is an m-subset of $\mathbb{Z}_v$ such that, for every $g \in \mathbb{Z}_v \setminus \{0\}$, there is at most one pair $d_i, d_j \in D$ such that $d_i - d_j = g$.
- Difference packings are equivalent to other well-studied combinatorial objects, including modular Golomb rulers and optical orthogonal codes.
- The corresponding 1-regular (weak) AMD code has $\hat{\epsilon} = 1/m$ (an optimal strategy is to choose any Δ that occurs as a difference of two elements of D).

Near-optimal Weak AMD Codes (cont.)

Buratti and Stinson (2021) proved the following result.

Theorem 2 (BS21)

For any $m \geq 3$ and any $v \geq 3m^2 - 1$, there is a (v, m)-cyclic difference packing.

- Theorem 2 is proven using Singer difference sets, some computational results for small m, and known results on the distribution of primes.
- In Theorem 2, we have $v \approx 3m^2$.
- $\hat{\epsilon} = 1/m$ is a factor of three greater than the lower bound from (1), namely,

$$\hat{\epsilon} \geq \frac{m-1}{v-1} \approx \frac{1}{3m}.$$

Nonuniform Source Distributions

- So far, the AMD codes and robust threshold schemes we have discussed assume uniformly distributed secrets (or sources).
- It would be nice be able to construct robust threshold schemes that are secure even if the secrets are not equally likely.
- In an extreme case, the secret would be known to the adversary.
- The associated AMD codes are termed strong AMD codes:
  1. The source $s \in \mathcal{S}$ is given to the adversary.
  2. Then the value $\Delta \in \mathcal{G} \setminus \{0\}$ is chosen by the adversary.
  3. s is encoded into $g \in A(s)$ using the encoding function E.
  4. The adversary wins if and only if $g + \Delta \in A(s')$ for some $s' \neq s$.
- The adversary chooses a value $\Delta = \sigma(s)$ for every source s.
- The code $(\mathcal{S}, \mathcal{G}, \mathcal{A}, E)$ is an $(v, m, \hat{\epsilon})$-strong AMD code, where $\hat{\epsilon}$ denotes the success probability of the adversary's optimal strategy (i.e., $\hat{\epsilon} = \max_\sigma\{\epsilon_\sigma\}$.)

R-optimal Strong AMD Codes

- Suppose we have an ℓ-regular $(v, m, \hat{\epsilon})$-strong AMD code.
- Then

$$\hat{\epsilon} \geq \frac{\ell(m-1)}{v-1}. \qquad (2)$$

- This is the same bound as in the case of weak AMD codes.
- R-optimal strong AMD codes can be constructed from strong external difference families, which were defined in [PS16].
- A (v, m, ℓ, λ)-strong external difference family (SEDF) is a set of m disjoint ℓ-subsets of an abelian group G of order v, say $A_1, \ldots, A_m$, such that the following multiset equation holds for all i:

$$\bigcup_{\{j\,:\,i \neq j\}} \mathcal{D}(A_i, A_j) = \lambda(G \setminus \{0\}).$$

  where $\mathcal{D}(A_1, A_2) = \{x - y : x \in A_1, y \in A_2\}$.
- If an (v, m, ℓ, λ)-SEDF exists, then $v \geq m\ell$ and $\lambda(v-1) = \ell^2(m-1)$.

SEDF with $\lambda = 1$

Example 3

Let $\mathcal{G} = (\mathbb{Z}_{\ell^2+1}, +)$, $A_1 = \{0, 1, \ldots, \ell - 1\}$ and $A_2 = \{\ell, 2\ell, \ldots, \ell^2\}$. This is an $(\ell^2 + 1, 2, \ell, 1)$-SEDF.

When $\ell = 4$, we have $\mathcal{G} = (\mathbb{Z}_{17}, +)$, $A_1 = \{0, 1, 2, 3\}$ and $A_2 = \{4, 8, 12, 16\}$.

Example 4

Let $\mathcal{G} = (\mathbb{Z}_v, +)$ and $A_i = \{i\}$ for $0 \leq i \leq v - 1$. This is an $(v, v, 1, 1)$-SEDF.

The above two examples are quite special:

Theorem 5 (PS16)

There exists an $(v, m, \ell, 1)$-SEDF if and only if $m = 2$ and $v = \ell^2 + 1$, or $\ell = 1$ and $v = m$.

SEDF with $\lambda > 1$

- There are numerous examples of SEDF with $m = 2$ and $\lambda > 1$.
- On the other hand, Martin and Stinson (2017) used the group algebra and character theory to prove nonexistence of nontrivial SEDF with $m = 3, 4$ or with v prime.
- Many other nonexistence results were subsequently proven by a variety of authors using the character theory approach.
- At the present time, there is only one known example of an SEDF with $m > 2$ and $\ell > 1$. It was found independently by two sets of authors: Wen, Yang and Feng (2018) and Jedwab and Li (2019).
- In the finite field $\mathbb{F}_{3^5}$, let C_0 be the subgroup of $\mathbb{F}_{3^5}^*$ of order 22 and let $C_1, \ldots, C_{10}$ be its cosets.
- It turns out that $\{C_0, \ldots, C_{10}\}$ is a $(243, 11, 22, 20)$-SEDF.

Near-optimal Strong AMD Codes

- Fortunately, it is possible to find good constructions for near-optimal strong AMD codes.
- Cramer, Fehr and Padro (2013) proved the following result.

Theorem 6 (CFP13)

For all prime powers q, there exists a q-regular $(q^3, q, 1/q)$-strong AMD code.

Proof.

For every $s \in \mathbb{F}_q$, let $A_s = \{(s,0,0) + \alpha(0,1,s) : \alpha \in \mathbb{F}_q\}$. □

- The lower bound from (2) is

$$\hat{\epsilon} \geq \frac{\ell(m-1)}{v-1} = \frac{q(q-1)}{q^3-1} = \frac{q}{q^2+q+1},$$

which is quite close to $1/q$.

Non-malleable Threshold Schemes

- Non-malleable threshold schemes have been considered by various authors, and several different definitions can be found in the literature. Here I discuss the approach of Veitch and Stinson (2023).
- We use the term "non-malleable" to denote a scheme that protects against certain pre-specified adversarial attacks.
- Suppose $\sim$ is an irreflexive binary relation on the set $\mathcal{S}$ of possible secrets.
- The adversary's goal in the Malleability Game is to modify one or more shares in such a way that $s' \sim s$, where s is the true secret and $s' \neq s$ is the reconstructed secret.
- If we define $s' \sim s$ if and only if $s \neq s'$, then the requirement for the adversary to win the Malleability Game is that $s' \neq s$. This is the same a a robust scheme.
- We consider an additive relation, e.g., $s' \sim_1 s$ iff $s' = s + 1$.

Optimal Non-malleable Threshold Schemes

- Optimal non-malleable threshold schemes for the additive relation $\sim_1$ can be obtained from circular external difference families and strong circular external difference families.

Definition 7

Let G be an additive abelian group of order v and suppose $m \geq 2$. An $(v, m, \ell; \lambda)$-circular external difference family (or $(v, m, \ell; \lambda)$-CEDF) is a set of m disjoint ℓ-subsets of G, say $\mathcal{A} = (A_0, \ldots, A_{m-1})$, such that the following multiset equation holds:

$$\bigcup_{j=0}^{m-1} \mathcal{D}(A_{j+1 \bmod m}, A_j,) = \lambda(G \setminus \{0\}).$$

We observe that $m\ell^2 = \lambda(v-1)$ if a $(v, m, \ell; \lambda)$-CEDF exists.

An Example of a CEDF

There are a number of different constructions for CEDF. Here is a small example.

Example 8

The following four sets of size 2 form a $(17,4,2,1)$-CEDF in $\mathbb{Z}_{17}$:

$$\mathcal{A} = (\{1,16\},\{9,8\},\{13,4\},\{15,2)\}).$$

To verify, we compute:

$$\begin{array}{llll}
9-1=8 & 8-1=7 & 9-16=10 & 8-16=9 \\
13-9=4 & 4-9=12 & 13-8=5 & 4-8=13 \\
15-13=2 & 2-13=6 & 15-4=11 & 2-4=15 \\
1-15=3 & 16-15=1 & 1-2=16 & 16-2=14
\end{array}$$

Strong CEDF

Definition 9

Let G be an additive abelian group of order v and suppose $m \geq 2$. An $(v, m, \ell; \lambda)$-strong circular external difference family (or $(v, m, \ell; \lambda)$-SCEDF) is a set of m disjoint ℓ-subsets of G, say $\mathcal{A} = (A_0, \ldots, A_{m-1})$, such that the following multiset equation holds for every j, $0 \leq j \leq m-1$:

$$\mathcal{D}(A_{j+1 \bmod m}, A_j) = \lambda(G \setminus \{0\}).$$

We observe that $\ell^2 = \lambda(v-1)$ if an $(v, m, \ell; \lambda)$-SCEDF exists.

- Each pair of adjacent sets in an SCEDF form an SEDF.
- In general, SCEDF seem to be difficult to construct.
- There are examples with $m = 2$: any $(v, 2, \ell; \lambda)$-SEDF is automatically strong.
- At present, we are unable to construct any $(v, m, \ell; \lambda)$-SCEDF with $m \geq 3$.

Near-optimal Strong Circular AMD Codes

- Since strong CEDF (i.e., optimal strong circular AMD codes) are apparently very difficult to find, we instead explore constructions for near-optimal strong circular AMD codes.
- One possibility is to use cyclotomic classes in a finite field.
- The security of a resulting AMD code depends on the relevant cyclotomic numbers.
- Let $q = ef + 1$ be a prime power and let $\alpha \in \mathbb{F}_q$ be a primitive element.
- Define $C_0 = \{\alpha^{je} : 0 \leq j \leq f - 1\}$ and define $C_i = \alpha^i C_0$ for $1 \leq i \leq e - 1$.
- $C_0, \ldots, C_{e-1}$ are the cyclotomic classes of index e.
- The cyclotomic numbers of order e are the integers denoted $(i, j)_e$ $(0 \leq i, j \leq e - 1)$ that are defined as follows:

$$(i, j)_e = |(C_i + 1) \cap C_j|.$$

Near-optimal Strong Circular AMD Codes (cont.)

Theorem 10

Let $q = ef + 1$ be a prime power. Denote

$$\lambda = \max\{(i, i+1 \bmod e)_e : 0 \le i \le e-1\}.$$

Then $\mathcal{A} = \{C_0, \ldots, C_{e-1}\}$ is an f-regular strong circular $(q, e, \hat{\epsilon})$-AMD code, where $\hat{\epsilon} = \lambda/f$.

Strong Circular $(q, 4, \hat{\epsilon})$-AMD Codes

- Suppose $q \equiv 1 \bmod 8$ and we take $e = 4$ in Theorem 10.
- The security of the resulting AMD code depends on the cyclotomic numbers $(0,1)_4$, $(1,2)_4$, $(2,3)_4$ and $(3,0)_4$.
- To compute them, express q in the form $q = \mu^2 + 4\nu^2$, where $\mu \equiv 1 \bmod 4$; the sign of ν is undetermined.
- Then we have

$$\begin{aligned}(0,1)_4 &= \frac{q-3+2\mu+8\nu}{16}\\(1,2)_4 &= \frac{q+1-2\mu}{16}\\(2,3)_4 &= \frac{q+1-2\mu}{16}\\(3,0)_4 &= \frac{q-3+2\mu-8\nu}{16}.\end{aligned}$$

- Switching the sign of ν interchanges the values of $(0,1)_4$ and $(3,0)_4$, but the resulting value of λ is not affected.

Example

- Suppose $q = 97 = 4 \times 24 + 1$.
- We have $97 = 9^2 + 4 \times 2^2$, so $\mu = 9$ and $\nu = \pm 2$.
- The largest of the four cyclotomic numbers is

$$\frac{97 - 3 + 18 + 16}{16} = 8.$$

- We obtain a 24-regular strong circular $(97, 4, 1/3)$-AMD code.

An Asymptotic Result

- To analyse the asymptotic behaviour of this approach, we maximize the function

$$\frac{q-3+2\mu+8\nu}{16q/4} = \frac{q-3+2\mu+8\nu}{4q}$$

subject to the constraint $q = \mu^2 + 4\nu^2$.

- Using elementary calculus, we see that

$$2\mu + 8\nu \leq 2\sqrt{5}\sqrt{q}.$$

- The following result is obtained.

Theorem 11

Suppose $q \equiv 1 \bmod 8$ *is a prime power. Then there is a* $(q-1)/4$*-regular strong circular* $(q, 4, \hat{\epsilon})$*-AMD code with* $\hat{\epsilon} < \frac{1}{4} + \frac{\sqrt{5}}{2} q^{-1/2}$.

Some References

[1] M. Tompa and H. Woll. How to share a secret with cheaters. *J. Cryptology* **1** (1989), 133–138.

[2] W. Ogata and K. Kurosawa. Optimum secret sharing scheme secure against cheating. *Lecture Notes in Computer Science* **1070** (1996), 200–211 (EUROCRYPT '96).

[3] R. Cramer, Y. Dodis, S. Fehr, C. Padró and D. Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. *Lecture Notes in Computer Science* **4965** (2008), 471–488 (EUROCRYPT 2008).

[4] M.B. Paterson and D.R. Stinson. Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families. *Discrete Math.* **339** (2016), 2891–2906.

[5] S. Veitch and D.R. Stinson. Unconditionally secure non-malleable secret sharing and circular external difference families. To appear in *Designs, Codes and Cryptography*.

[6] M.B. Paterson and D.R. Stinson. New results on circular external difference families. In preparation.

Thank You For Your Attention!