New Constructions of Systematic Authentication Codes from Three Classes of Cyclic Codes

Longjiang Qu

joint work with Yunwen Liu and Chao Li

Department of Mathmatics,
National University of Defense Technology, P. R. China

July 3, 2018

Outline

Authentication

Authentication

Systematic Authentication Codes

Systematic authentication codes

A systematic authentication code is defined as a four-tuple

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_k : k \in \mathcal{K}\}),$$

where $\mathcal{S}$ is the source state, $\mathcal{T}$ is the tag space, $\mathcal{K}$ is the key space, and $E_k : \mathcal{S} \to \mathcal{T}$ is called the encoding rule.

Systematic Authentication Codes

Systematic authentication codes

A systematic authentication code is defined as a four-tuple

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_k : k \in \mathcal{K}\}),$$

where $\mathcal{S}$ is the source state, $\mathcal{T}$ is the tag space, $\mathcal{K}$ is the key space, and $E_k : \mathcal{S} \to \mathcal{T}$ is called the encoding rule.

- The sender generates a tag $t \in \mathcal{T}$ for an information $s \in \mathcal{S}$, and sends out $m = (s, t)$

Systematic Authentication Codes

Systematic authentication codes

A systematic authentication code is defined as a four-tuple

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_k : k \in \mathcal{K}\}),$$

where $\mathcal{S}$ is the source state, $\mathcal{T}$ is the tag space, $\mathcal{K}$ is the key space, and $E_k : \mathcal{S} \to \mathcal{T}$ is called the encoding rule.

- The sender generates a tag $t \in \mathcal{T}$ for an information $s \in \mathcal{S}$, and sends out $m = (s, t)$
- The receiver gets $m' = (s', t')$ and check if $t' = E_k(s')$

Systematic Authentication Codes

Systematic authentication codes

A systematic authentication code is defined as a four-tuple

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_k : k \in \mathcal{K}\}),$$

where $\mathcal{S}$ is the source state, $\mathcal{T}$ is the tag space, $\mathcal{K}$ is the key space, and $E_k : \mathcal{S} \to \mathcal{T}$ is called the encoding rule.

- The sender generates a tag $t \in \mathcal{T}$ for an information $s \in \mathcal{S}$, and sends out $m = (s, t)$
- The receiver gets $m' = (s', t')$ and check if $t' = E_k(s')$
  - if so, m' is authentic
  - otherwise, reject m'

Construct systematic authentication codes

SECURITY +

Construct systematic authentication codes

SECURITY + EFFICIENCY

Construct systematic authentication codes

SECURITY + EFFICIENCY

- Error-correcting codes
  - generic construction
  - q-twisted construction
  - rank distance codes

Construct systematic authentication codes

SECURITY + EFFICIENCY

- Error-correcting codes
  - generic construction
  - q-twisted construction
  - rank distance codes
- Projective geometry
- Functions over Galois Rings
- ...

General Attacks

- **Impersonation attack**
  A tag is guessed for a message s by an adversary, with maximum success probability P_I

General Attacks

- **Impersonation attack**
  A tag is guessed for a message s by an adversary, with maximum success probability P_I
- **Substitution attack**
  A tag is guessed for a message s by an adversary, based on some authentic message-tag pairs, with maximum success probability P_S

General Attacks

- **Impersonation attack**
  A tag is guessed for a message s by an adversary, with maximum success probability P_I
- **Substitution attack**
  A tag is guessed for a message s by an adversary, based on some authentic message-tag pairs, with maximum success probability P_S

For systematic authentication codes

$$P_S \geq P_I \geq \frac{1}{|\mathcal{T}|}$$

Outline

Generic construction

A generic construction [Ding-Helleseth-Kløve-Wang]

Let $\mathcal{C}$ be an (n, M) code over an alphabet B where $(B, +)$ is an Abelian group with q elements.

Generic construction

A generic construction [Ding-Helleseth-Kløve-Wang]

Let $\mathcal{C}$ be an (n, M) code over an alphabet B where $(B, +)$ is an Abelian group with q elements. We define a Cartesian authentication code by

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_k : k \in \mathcal{K}\}) = (\mathbb{Z}_M, B, \mathbb{Z}_n \times B, \{E_k : k \in \mathcal{K}\}),$$

Generic construction

A generic construction [Ding-Helleseth-Kløve-Wang]

Let $\mathcal{C}$ be an (n, M) code over an alphabet B where $(B, +)$ is an Abelian group with q elements. We define a Cartesian authentication code by

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_k : k \in \mathcal{K}\}) = (\mathbb{Z}_M, B, \mathbb{Z}_n \times B, \{E_k : k \in \mathcal{K}\}),$$

where for any $k = (k_1, k_2) \in \mathcal{K}$ and $s \in \mathcal{S}$, the encoding rule is defined by

$$E_k(s) = c_{s,k_1} + k_2,$$

and c_{s,k_1} is the $(k_1 + 1)$-th component of the codeword $\mathbf{c}_s$.

[Ding-Helleseth-Kløve-Wang] C. Ding, T. Helleseth, T. Kløve and X. Wang, A generic construction of Cartesian authentication codes, IEEE Transactions on Information Theory, 2007.

Generic construction

Proposition

Let $\mathcal{C}$ be an $[n, \kappa, d]$ linear code over $\mathrm{GF}(q)$. Let $(B, +) = (\mathrm{GF}(q), +)$, $M = q^{\kappa}$.

Generic construction

Proposition

Let $\mathcal{C}$ be an $[n, \kappa, d]$ linear code over $\mathrm{GF}(q)$. Let $(B, +)$ $= (\mathrm{GF}(q), +)$, $M = q^{\kappa}$. The authentication code becomes

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_k : k \in \mathcal{K}\}) = (\mathbb{Z}_{q^{\kappa}}, \mathrm{GF}(q), \mathbb{Z}_n \times \mathrm{GF}(q), \{E_k : k \in \mathcal{K}\}).$$

Generic construction

Proposition

Let $\mathcal{C}$ be an $[n, \kappa, d]$ linear code over $\mathrm{GF}(q)$. Let $(B, +)$ $= (\mathrm{GF}(q), +)$, $M = q^{\kappa}$. The authentication code becomes

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_k : k \in \mathcal{K}\}) = (\mathbb{Z}_{q^{\kappa}}, \mathrm{GF}(q), \mathbb{Z}_n \times \mathrm{GF}(q), \{E_k : k \in \mathcal{K}\}).$$

We have

$$P_I = \frac{1}{q}, P_S = \max_{0 \neq \mathbf{c} \in \mathcal{C}} \max_{u \in \mathrm{GF}(q)} \frac{N(\mathbf{c}, u)}{n}.$$

and

$$|\mathcal{S}| = q^{\kappa}, |\mathcal{T}| = q, |\mathcal{K}| = nq.$$

Generic construction

Proposition

Let $\mathcal{C}$ be an $[n, \kappa, d]$ linear code over $\mathrm{GF}(q)$. Let $(B, +)$ $= (\mathrm{GF}(q), +)$, $M = q^\kappa$. The authentication code becomes

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \{E_k : k \in \mathcal{K}\}) = (\mathbb{Z}_{q^\kappa}, \mathrm{GF}(q), \mathbb{Z}_n \times \mathrm{GF}(q), \{E_k : k \in \mathcal{K}\}).$$

We have

$$P_I = \frac{1}{q}, P_S = \max_{0 \neq \mathbf{c} \in \mathcal{C}} \max_{u \in \mathrm{GF}(q)} \frac{N(\mathbf{c}, u)}{n}.$$

and

$$|\mathcal{S}| = q^\kappa, |\mathcal{T}| = q, |\mathcal{K}| = nq.$$

$N(\boldsymbol{c}, u)$ is the number of times that an element u occurs as a coordinate in the codeword $\boldsymbol{c}$

Generic construction

Criteria for the linear codes we choose

Generic construction

Criteria for the linear codes we choose

- $N(\boldsymbol{c}, u)$ is crucial for the resistance against substitution attacks

Generic construction

Criteria for the linear codes we choose

- $N(\boldsymbol{c}, u)$ is crucial for the resistance against substitution attacks
- To obtain $N(\boldsymbol{c}, u)$ is difficult in general

Generic construction

Criteria for the linear codes we choose

- $N(\boldsymbol{c}, u)$ is crucial for the resistance against substitution attacks
- To obtain $N(\boldsymbol{c}, u)$ is difficult in general
- Cyclic codes with only a few zeroes

Generic construction

Criteria for the linear codes we choose

- $N(\boldsymbol{c}, u)$ is crucial for the resistance against substitution attacks
- To obtain $N(\boldsymbol{c}, u)$ is difficult in general
- Cyclic codes with only a few zeroes

We propose 3 classes of systematic authentication codes

Outline

Cyclic codes with two zeroes

$[q-1, tm]$ cyclic code $\mathcal{C}_{(i_1,\ldots,i_t)}$

$p \leftarrow$ prime, $m \leftarrow$ positive integer, $q = p^m$ and $\pi \in \mathrm{GF}(q) \leftarrow$ primitive. $\Gamma_j \leftarrow p$-cyclotomic coset modulo $q-1$ containing j.

Cyclic codes with two zeroes

$[q-1, tm]$ cyclic code $\mathcal{C}_{(i_1,\ldots,i_t)}$

$p \leftarrow$ prime, $m \leftarrow$ positive integer, $q = p^m$ and $\pi \in \mathrm{GF}(q) \leftarrow$ primitive. $\Gamma_j \leftarrow p$-cyclotomic coset modulo $q-1$ containing j. $\{i_1, \ldots, i_t | t \geq 1 \in \mathbb{Z}_{q-1}\}$ s.t. $\Gamma_{i_1}, \ldots, \Gamma_{i_t}$ are pairwise disjoint with size m.

Cyclic codes with two zeroes

$[q-1, tm]$ cyclic code $\mathcal{C}_{(i_1,...,i_t)}$

$p \leftarrow$ prime, $m \leftarrow$ positive integer, $q = p^m$ and $\pi \in \mathrm{GF}(q) \leftarrow$ primitive. $\Gamma_j \leftarrow p$-cyclotomic coset modulo $q-1$ containing j. $\{i_1, ..., i_t | t \geq 1 \in \mathbb{Z}_{q-1}\}$ s.t. $\Gamma_{i_1}, ..., \Gamma_{i_t}$ are pairwise disjoint with size m.
Define cyclic code $\mathcal{C}_{(i_1,...,i_t)}$ with parity-check polynomial $h(x) = m_{i_1}(x)...m_{i_t}(x)$, with $m_i(x)$ being the minimal polynomial of π^{-i} over $\mathrm{GF}(p)$.

Cyclic codes with two zeroes

$[q-1, tm]$ cyclic code $\mathcal{C}_{(i_1,...,i_t)}$

$p \leftarrow$ prime, $m \leftarrow$ positive integer, $q = p^m$ and $\pi \in \mathrm{GF}(q) \leftarrow$ primitive. $\Gamma_j \leftarrow p$-cyclotomic coset modulo $q-1$ containing j. $\{i_1, ..., i_t | t \geq 1 \in \mathbb{Z}_{q-1}\}$ s.t. $\Gamma_{i_1}, ..., \Gamma_{i_t}$ are pairwise disjoint with size m.
Define cyclic code $\mathcal{C}_{(i_1,...,i_t)}$ with parity-check polynomial $h(x) = m_{i_1}(x)...m_{i_t}(x)$, with $m_i(x)$ being the minimal polynomial of π^{-i} over $\mathrm{GF}(p)$.

Trace representation

$$\mathcal{C}_{(i_1,...,i_t)} = \left\{ \left(\sum_{s=1}^{t} \mathrm{Tr}(a_s x^{i_s}) \right)_{x \in \mathrm{GF}(q)^*} \mid a_1, ..., a_t \in \mathrm{GF}(q) \right\}.$$

Cyclic codes with two zeroes

$[q-1, tm]$ cyclic code $\mathcal{C}_{(i_1,...,i_t)}$

$p \leftarrow$ prime, $m \leftarrow$ positive integer, $q = p^m$ and $\pi \in \mathrm{GF}(q) \leftarrow$ primitive. $\Gamma_j \leftarrow p$-cyclotomic coset modulo $q-1$ containing j. $\{i_1, ..., i_t | t \geq 1 \in \mathbb{Z}_{q-1}\}$ s.t. $\Gamma_{i_1}, ..., \Gamma_{i_t}$ are pairwise disjoint with size m.
Define cyclic code $\mathcal{C}_{(i_1,...,i_t)}$ with parity-check polynomial $h(x) = m_{i_1}(x)...m_{i_t}(x)$, with $m_i(x)$ being the minimal polynomial of π^{-i} over $\mathrm{GF}(p)$.

Trace representation

$$\mathcal{C}_{(i_1,...,i_t)} = \left\{ \left(\sum_{s=1}^{t} \mathrm{Tr}(a_s x^{i_s}) \right)_{x \in \mathrm{GF}(q)^*} \mid a_1, ..., a_t \in \mathrm{GF}(q) \right\}.$$

We use $\mathcal{C}_{(1,e)}$ with two zeroes

First class of authentication codes

Lemma ([Zhou-Ding])

Let $m \geq 3$ *be odd,* $p = 3$ *and* $e = 3^{(m+1)/2} - 1$. *Then,* $\mathcal{C}_{(1,e)}$ *is a*

$$[p^m - 1, 2m]$$

cyclic code over $\mathrm{GF}(p)$ *with three nonzero weights*

$$(p-1)p^{m-1} \pm \frac{p-1}{2} p^{(m-1)/2}, (p-1)p^{m-1}$$

[Zhou-Ding] Z. Zhou and C. Ding, Seven classes of three-weight cyclic codes, IEEE Transactions on Communications, 2013.

First class of authentication codes

Theorem

The authentication code constructed from code $\mathcal{C}_{(1,3^{(m+1)/2}-1)}$ *is*

$$(\mathbb{Z}_{3^{2m}}, \mathrm{GF}(3), \mathbb{Z}_{3^m-1} \times \mathrm{GF}(3), \{E_k : k \in \mathcal{K}\}),$$

First class of authentication codes

Theorem

The authentication code constructed from code $\mathcal{C}_{(1,3^{(m+1)/2}-1)}$ *is*

$$(\mathbb{Z}_{3^{2m}}, \mathrm{GF}(3), \mathbb{Z}_{3^m-1} \times \mathrm{GF}(3), \{E_k : k \in \mathcal{K}\}),$$

with

$$P_I = \frac{1}{3}$$

and

$$P_S = \frac{3^{m-1} + \frac{1}{2}(3^{(m-1)/2} + 3^{(m+1)/2})}{3^m - 1}.$$

First class of authentication codes

Theorem

The authentication code constructed from code $\mathcal{C}_{(1,3^{(m+1)/2}-1)}$ *is*

$$(\mathbb{Z}_{3^{2m}}, \mathrm{GF}(3), \mathbb{Z}_{3^m-1} \times \mathrm{GF}(3), \{E_k : k \in \mathcal{K}\}),$$

with

$$P_I = \frac{1}{3}$$

and

$$P_S = \frac{3^{m-1} + \frac{1}{2}(3^{(m-1)/2} + 3^{(m+1)/2})}{3^m - 1}.$$

In addition,

$$|\mathcal{S}| = 3^{2m}, |\mathcal{T}| = 3, |\mathcal{K}| = 3^{m+1} - 3.$$

Sketch of proof (1)

Let $n = p^m - 1$ and $h = (m+1)/2$.

Sketch of proof (1)

Let $n = p^m - 1$ and $h = (m+1)/2$. We have

$$N(c(a,b),u) = \frac{1}{p}[\sum_{x\in \mathrm{GF}(q)^*} \sum_{y\in \mathrm{GF}(p)} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)}]$$

$$= \frac{1}{p}[\sum_{x\in \mathrm{GF}(q)} \sum_{y\in \mathrm{GF}(p)} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)} - \sum_{y\in \mathrm{GF}(p)} \omega^{-yu}].$$

Sketch of proof (1)

Let $n = p^m - 1$ and $h = (m+1)/2$. We have

$$N(c(a,b),u) = \frac{1}{p}[\sum_{x\in \mathrm{GF}(q)^*}\sum_{y\in \mathrm{GF}(p)} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)}]$$
$$= \frac{1}{p}[\sum_{x\in \mathrm{GF}(q)}\sum_{y\in \mathrm{GF}(p)} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)} - \sum_{y\in \mathrm{GF}(p)} \omega^{-yu}].$$

1. When $u = 0$

$$\max N(c(a,b),0) = \max(n - wt(c(a,b)))$$
$$= n - d = p^{m-1} + \frac{p-1}{2}p^{(m-1)/2} - 1.$$

Sketch of proof (2)

2. When $u \neq 0$

Sketch of proof (2)

2. When $u \neq 0$

$$N(c(a,b),u) = \frac{1}{p}[\sum_{x \in \mathrm{GF}(q)} \sum_{y \in \mathrm{GF}(p)} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)}]$$

Sketch of proof (2)

2. When $u \neq 0$

$$N(c(a,b),u) = \frac{1}{p}[\sum_{x\in \mathrm{GF}(q)} \sum_{y\in \mathrm{GF}(p)} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)}]$$

$$= \frac{1}{p}[q + \sum_{x\in \mathrm{GF}(q)} \sum_{y\in \mathrm{GF}(p)^*} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)}]$$

Sketch of proof (2)

2. When $u \neq 0$

$$
\begin{aligned}
N(c(a,b),u) &= \frac{1}{p}\Big[\sum_{x\in \mathrm{GF}(q)} \sum_{y\in \mathrm{GF}(p)} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)}\Big] \\
&= \frac{1}{p}\Big[q + \sum_{x\in \mathrm{GF}(q)} \sum_{y\in \mathrm{GF}(p)^*} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)}\Big] \\
&= p^{m-1} + \frac{1}{p} \sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \sum_{x\in \mathrm{GF}(q)} \omega^{y\mathrm{Tr}(ax+bx^{3^h-1})}.
\end{aligned}
$$

Sketch of proof (2)

2. When $u \neq 0$

$$
\begin{aligned}
N(c(a,b),u) &= \frac{1}{p}\Big[\sum_{x\in \mathrm{GF}(q)} \sum_{y\in \mathrm{GF}(p)} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)}\Big] \\
&= \frac{1}{p}\Big[q + \sum_{x\in \mathrm{GF}(q)} \sum_{y\in \mathrm{GF}(p)^*} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)}\Big] \\
&= p^{m-1} + \frac{1}{p} \sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \underbrace{\sum_{x\in \mathrm{GF}(q)} \omega^{y\mathrm{Tr}(ax+bx^{3^h-1})}}_{\sigma}.
\end{aligned}
$$

Sketch of proof (2)

2. When $u \neq 0$

$$
\begin{aligned}
N(c(a,b),u) &= \frac{1}{p}\Big[\sum_{x\in \mathrm{GF}(q)} \sum_{y\in \mathrm{GF}(p)} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)}\Big] \\
&= \frac{1}{p}\Big[q + \sum_{x\in \mathrm{GF}(q)} \sum_{y\in \mathrm{GF}(p)^*} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)}\Big] \\
&= p^{m-1} + \frac{1}{p} \sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \underbrace{\sum_{x\in \mathrm{GF}(q)} \omega^{y\mathrm{Tr}(ax+bx^{3^h-1})}}_{\sigma}.
\end{aligned}
$$

Let $R(a,b) = \sum_{x\in \mathrm{GF}(3^m)} \omega^{\mathrm{Tr}(ax^{3^h+1}+bx^2)}$.

Sketch of proof (2)

2. When $u \neq 0$

$$N(c(a,b),u) = \frac{1}{p}[\sum_{x\in \mathrm{GF}(q)} \sum_{y\in \mathrm{GF}(p)} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)}]$$

$$= \frac{1}{p}[q + \sum_{x\in \mathrm{GF}(q)} \sum_{y\in \mathrm{GF}(p)^*} \omega^{y(\mathrm{Tr}(ax+bx^{3^h-1})-u)}]$$

$$= p^{m-1} + \frac{1}{p} \sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \underbrace{\sum_{x\in \mathrm{GF}(q)} \omega^{y\mathrm{Tr}(ax+bx^{3^h-1})}}_{\sigma}.$$

Let $R(a,b) = \sum_{x\in \mathrm{GF}(3^m)} \omega^{\mathrm{Tr}(ax^{3^h+1}+bx^2)}$. We have

$$T(a,b) := \sum_{x\in \mathrm{GF}(3^m)} \omega^{\mathrm{Tr}(ax+bx^{3^h-1})} = \frac{1}{2}(R(a,b) + R(-a,b)).$$

Sketch of proof (3)

If $u = 1$

Sketch of proof (3)

If $u = 1$

$$\sigma = \sum_{y \in \mathrm{GF}(3)^*} \omega^{-y} \sum_{x \in \mathrm{GF}(3^m)} \omega^{y\mathrm{Tr}(ax + bx^{3^h-1})}$$

Sketch of proof (3)

If $u = 1$

$$\sigma = \sum_{y \in \mathrm{GF}(3)^*} \omega^{-y} \sum_{x \in \mathrm{GF}(3^m)} \omega^{y\mathrm{Tr}(ax+bx^{3^h-1})}$$
$$= \sum_{y \in \mathrm{GF}(3)^*} \omega^{-y} T(ya, yb)$$

Sketch of proof (3)

If $u = 1$

$$\begin{aligned}\sigma &= \sum_{y \in \mathrm{GF}(3)^*} \omega^{-y} \sum_{x \in \mathrm{GF}(3^m)} \omega^{y\mathrm{Tr}(ax+bx^{3^h-1})} \\ &= \sum_{y \in \mathrm{GF}(3)^*} \omega^{-y} T(ya, yb) \\ &= \omega^{-1} T(a,b) + \omega T(-a,-b)\end{aligned}$$

Sketch of proof (3)

If $u = 1$

$$\begin{aligned}
\sigma &= \sum_{y \in \mathrm{GF}(3)^*} \omega^{-y} \sum_{x \in \mathrm{GF}(3^m)} \omega^{y\mathrm{Tr}(ax+bx^{3^h-1})} \\
&= \sum_{y \in \mathrm{GF}(3)^*} \omega^{-y} T(ya, yb) \\
&= \omega^{-1} T(a,b) + \omega T(-a,-b) \\
&= (-\frac{1}{2} - \frac{\sqrt{3}}{2} i) T(a,b) + (-\frac{1}{2} + \frac{\sqrt{3}}{2} i) T(-a,-b)
\end{aligned}$$

Sketch of proof (3)

If $u = 1$

$$\begin{aligned}
\sigma &= \sum_{y \in \mathrm{GF}(3)^*} \omega^{-y} \sum_{x \in \mathrm{GF}(3^m)} \omega^{y\mathrm{Tr}(ax+bx^{3^h-1})} \\
&= \sum_{y \in \mathrm{GF}(3)^*} \omega^{-y} T(ya, yb) \\
&= \omega^{-1} T(a,b) + \omega T(-a,-b) \\
&= (-\frac{1}{2} - \frac{\sqrt{3}}{2} i) T(a,b) + (-\frac{1}{2} + \frac{\sqrt{3}}{2} i) T(-a,-b) \\
&= -\frac{1}{2}[\frac{1}{2}(R(a,b) + R(-a,b) + R(-a,-b) + R(a,-b))] \\
&\quad - \frac{\sqrt{3}}{2} i[\frac{1}{2}(R(a,b) + R(-a,b) - R(-a,-b) - R(a,-b))].
\end{aligned}$$

Sketch of proof (4)

Lemma

Let $d = \gcd(m, k)$ *and let* $Q(a, b) = \mathrm{Tr}_{m/d}(ax^{p^k+1} + bx^2)$. *For* $j = 0, 1, 2$, *assume that the rank of* $Q(a, b)$ *is* $s - j$. *Thus, the possible values of* $\sum_{x \in \mathrm{GF}(q)} \omega^{\mathrm{Tr}_{d/1} Q(a,b)}$ *are*

$$\sum_{x \in \mathrm{GF}(q)} \omega^{\mathrm{Tr}_{d/1} Q(a,b)} := v_j = \begin{cases} \varepsilon p^{(m+jd)/2}, & \text{if } m + jd \text{ is even;} \\ \varepsilon \sqrt{p i^{p-1}} p^{(m+jd-1)/2}, & \text{if } m + jd \text{ is odd.} \end{cases} \tag{1}$$

Sketch of proof (4)

Lemma

Let $R(a,b) = \sum_{x \in \mathrm{GF}(q)} \omega^{Q(a,b)}$. *Define*

$$N^+_{\varepsilon,j} = \{(a,b) \in \mathrm{GF}(q)^2 | R(a,b) = \varepsilon v_j\},$$
$$N^-_{\varepsilon,j} = \{(a,b) \in \mathrm{GF}(q)^2 | R(-a,b) = \varepsilon v_j\}.$$

Sketch of proof (4)

Lemma

Let $R(a,b) = \sum_{x \in \mathrm{GF}(q)} \omega^{Q(a,b)}$. *Define*

$$N^+_{\varepsilon,j} = \{(a,b) \in \mathrm{GF}(q)^2 | R(a,b) = \varepsilon v_j\},$$
$$N^-_{\varepsilon,j} = \{(a,b) \in \mathrm{GF}(q)^2 | R(-a,b) = \varepsilon v_j\}.$$

Assume that λ *is a non-square of* $\mathrm{GF}(p)^*$. *Then, the relation between* $N^+_{\varepsilon,j}$ *and* $N^-_{\varepsilon,j}$ *can be fully characterised.*

Sketch of proof (4)

Lemma

Let $R(a,b) = \sum_{x \in \mathrm{GF}(q)} \omega^{Q(a,b)}$. *Define*

$$N^+_{\varepsilon,j} = \{(a,b) \in \mathrm{GF}(q)^2 | R(a,b) = \varepsilon v_j\},$$
$$N^-_{\varepsilon,j} = \{(a,b) \in \mathrm{GF}(q)^2 | R(-a,b) = \varepsilon v_j\}.$$

Assume that λ *is a non-square of* $\mathrm{GF}(p)^*$. *Then, the relation between* $N^+_{\varepsilon,j}$ *and* $N^-_{\varepsilon,j}$ *can be fully characterised.*
For odd $m \geq 3$ *and* $\{k \geq 0 | \gcd(m,k) = 1\}$,

Sketch of proof (4)

Lemma

Let $R(a,b) = \sum_{x \in \mathrm{GF}(q)} \omega^{Q(a,b)}$. *Define*

$$N^+_{\varepsilon,j} = \{(a,b) \in \mathrm{GF}(q)^2 | R(a,b) = \varepsilon v_j\},$$
$$N^-_{\varepsilon,j} = \{(a,b) \in \mathrm{GF}(q)^2 | R(-a,b) = \varepsilon v_j\}.$$

Assume that λ *is a non-square of* $\mathrm{GF}(p)^*$. *Then, the relation between* $N^+_{\varepsilon,j}$ *and* $N^-_{\varepsilon,j}$ *can be fully characterised.*
For odd $m \geq 3$ *and* $\{k \geq 0 | \gcd(m,k) = 1\}$,

$$\{(R(a,b), R(-a,b)) | a,b \in \mathrm{GF}(q)\}$$

takes the following possible values
$(\pm v_0, \pm v_0), (\pm v_0, \pm v_1), (\pm v_1, \pm v_0), \pm(v_0, v_2), \pm(v_2, v_0), (p^m, p^m)$.

Sketch of proof (5)

With the Lemma, the possible values of σ can be predicted, and we have

$$N(c(a,b),\pm 1) = \begin{cases} 3^{m-1}, \\ 3^{m-1} \pm 3^{(m-1)/2}, \\ 3^{m-1} \pm \frac{1}{2}(3^{(m+1)/2} + 3^{(m-1)/2}). \end{cases}$$

Sketch of proof (5)

With the Lemma, the possible values of σ can be predicted, and we have

$$N(c(a,b),\pm 1) = \begin{cases} 3^{m-1}, \\ 3^{m-1} \pm 3^{(m-1)/2}, \\ 3^{m-1} \pm \frac{1}{2}(3^{(m+1)/2} + 3^{(m-1)/2}). \end{cases}$$

Therefore, the maximum can be obtained by

$$\max N(c(a,b),u) = 3^{m-1} + \frac{1}{2}(3^{(m-1)/2} + 3^{(m+1)/2}).$$

Sketch of proof (5)

With the Lemma, the possible values of σ can be predicted, and we have

$$N(c(a,b),\pm 1)=\begin{cases} 3^{m-1}, \\ 3^{m-1}\pm 3^{(m-1)/2}, \\ 3^{m-1}\pm \frac{1}{2}(3^{(m+1)/2}+3^{(m-1)/2}). \end{cases}$$

Therefore, the maximum can be obtained by

$$\max N(c(a,b),u)=3^{m-1}+\frac{1}{2}(3^{(m-1)/2}+3^{(m+1)/2}).$$

We have

$$P_S=\frac{3^{m-1}+\frac{1}{2}(3^{(m-1)/2}+3^{(m+1)/2})}{3^m-1}.$$

Second class of authentication codes

Lemma

Let m be odd, p be a prime such that $p \equiv 3 \pmod 4$, $q = p^m$,

$$e = (p^m + 1)/(p^k + 1) + (p^m - 1)/2$$

with $k|m$. Then, $\mathcal{C}_{(1,e)}$ is a

$$[p^m - 1, 2m]$$

cyclic code over $\mathrm{GF}(p)$ with three nonzero weights

$$p^m - p^{m-1}, (p-1)(p^{m-1} \pm \frac{1}{2} p^{(m+k)/2-1}).$$

Second class of authentication codes

Theorem

The authentication code constructed from the code $\mathcal{C}_{(1,e)}$ is

$$(\mathbb{Z}_{p^{2m}}, \mathrm{GF}(p), \mathbb{Z}_{p^m-1} \times \mathrm{GF}(p), \{E_k : k \in \mathcal{K}\}),$$

Second class of authentication codes

Theorem

The authentication code constructed from the code $\mathcal{C}_{(1,e)}$ *is*

$$(\mathbb{Z}_{p^{2m}}, \mathrm{GF}(p), \mathbb{Z}_{p^m-1} \times \mathrm{GF}(p), \{E_k : k \in \mathcal{K}\}),$$

with

$$P_I = \frac{1}{p}, P_S = \begin{cases} \frac{\frac{3}{2}p^{m-1}+\frac{1}{2}p^{(m-1)/2}}{p^m-1}, & \text{if } m = k; \\ \frac{p^{m-1}+\frac{1}{2}p^{(m-1)/2}+\frac{1}{2}p^{(m+2k-1)/2}}{p^m-1}, & \text{if } m > k. \end{cases}$$

Second class of authentication codes

Theorem

The authentication code constructed from the code $\mathcal{C}_{(1,e)}$ is

$$(\mathbb{Z}_{p^{2m}}, \mathrm{GF}(p), \mathbb{Z}_{p^m-1} \times \mathrm{GF}(p), \{E_k : k \in \mathcal{K}\}),$$

with

$$P_I = \frac{1}{p}, P_S = \begin{cases} \frac{\frac{3}{2}p^{m-1}+\frac{1}{2}p^{(m-1)/2}}{p^m-1}, & \text{if } m = k; \\ \frac{p^{m-1}+\frac{1}{2}p^{(m-1)/2}+\frac{1}{2}p^{(m+2k-1)/2}}{p^m-1}, & \text{if } m > k. \end{cases}$$

Furthermore, we have

$$|\mathcal{S}| = p^{2m}, |\mathcal{T}| = p, |\mathcal{K}| = (p^m - 1)p.$$

Sketch of proof (1)

$$N(c(a,b),u) = \frac{1}{p}[\sum_{x\in \mathrm{GF}(q)} \sum_{y\in \mathrm{GF}(p)} \omega^{y(\mathrm{Tr}_{m/1}(ax+bx^e)-u)}]$$

Sketch of proof (1)

$$N(c(a,b),u) = \frac{1}{p}[\sum_{x\in \mathrm{GF}(q)} \sum_{y\in \mathrm{GF}(p)} \omega^{y(\mathrm{Tr}_{m/1}(ax+bx^e)-u)}]$$

$$= \frac{1}{p}[q + \sum_{x\in \mathrm{GF}(q)} \sum_{y\in \mathrm{GF}(p)^*} \omega^{y(\mathrm{Tr}_{m/1}(ax+bx^e)-u)}]$$

Sketch of proof (1)

$$
\begin{aligned}
N(c(a,b),u) &= \frac{1}{p}\Big[\sum_{x\in \mathrm{GF}(q)}\sum_{y\in \mathrm{GF}(p)} \omega^{y(\mathrm{Tr}_{m/1}(ax+bx^e)-u)}\Big] \\
&= \frac{1}{p}\Big[q+\sum_{x\in \mathrm{GF}(q)}\sum_{y\in \mathrm{GF}(p)^*} \omega^{y(\mathrm{Tr}_{m/1}(ax+bx^e)-u)}\Big] \\
&= p^{m-1}+\frac{1}{p}\sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu}\sum_{x\in \mathrm{GF}(q)} \omega^{y\mathrm{Tr}_{m/1}(ax+bx^e)}.
\end{aligned}
$$

Sketch of proof (1)

$$
\begin{aligned}
N(c(a,b),u) &= \frac{1}{p}\Big[\sum_{x\in \mathrm{GF}(q)}\sum_{y\in \mathrm{GF}(p)} \omega^{y(\mathrm{Tr}_{m/1}(ax+bx^e)-u)}\Big] \\
&= \frac{1}{p}\Big[q+\sum_{x\in \mathrm{GF}(q)}\sum_{y\in \mathrm{GF}(p)^*} \omega^{y(\mathrm{Tr}_{m/1}(ax+bx^e)-u)}\Big] \\
&= p^{m-1}+\frac{1}{p}\sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \underbrace{\sum_{x\in \mathrm{GF}(q)} \omega^{y\mathrm{Tr}_{m/1}(ax+bx^e)}}_{S(ya,yb)}.
\end{aligned}
$$

Sketch of proof (2)

Lemma

$m \geq 2$, $k \in \mathbb{Z}$, $d = \gcd(m, k)$, $s = m/d$.

Sketch of proof (2)

Lemma

$m \geq 2$, $k \in \mathbb{Z}$, $d = \gcd(m, k)$, $s = m/d$.
$p \leftarrow$ *odd prime*, $q_0 = p^d$, $q = p^m = q_0^s$.

Sketch of proof (2)

Lemma

$m \geq 2$, $k \in \mathbb{Z}$, $d = \gcd(m, k)$, $s = m/d$.
$p \leftarrow$ *odd prime*, $q_0 = p^d$, $q = p^m = q_0^s$.
$Q(a, b) = \mathrm{Tr}_{m/d}(ax^{p^k+1} + bx^2)$, $rank(Q(a, b)) = s - j, j = 0, 1, 2$.

Sketch of proof (2)

Lemma

$m \geq 2$, $k \in \mathbb{Z}$, $d = \gcd(m, k)$, $s = m/d$.
$p \leftarrow$ *odd prime*, $q_0 = p^d$, $q = p^m = q_0^s$.
$Q(a, b) = \mathrm{Tr}_{m/d}(ax^{p^k+1} + bx^2)$, $rank(Q(a, b)) = s - j, j = 0, 1, 2$.
Then

$$\sum_{x \in \mathrm{GF}(q)} \omega^{\mathrm{Tr}_{d/1} Q(a,b)} = \begin{cases} \varepsilon p^{(m+jd)/2}, & \text{if } m + jd \text{ is even;} \\ \varepsilon \sqrt{p i^{p-1}} p^{(m+jd-1)/2}, & \text{if } m + jd \text{ is odd.} \end{cases}$$

Sketch of proof (2)

Lemma

$m \geq 2$, $k \in \mathbb{Z}$, $d = \gcd(m, k)$, $s = m/d$.
$p \leftarrow$ *odd prime*, $q_0 = p^d$, $q = p^m = q_0^s$.
$Q(a, b) = \mathrm{Tr}_{m/d}(ax^{p^k+1} + bx^2)$, $rank(Q(a, b)) = s - j, j = 0, 1, 2$.
Then

$$\sum_{x \in \mathrm{GF}(q)} \omega^{\mathrm{Tr}_{d/1} Q(a,b)} = \begin{cases} \varepsilon p^{(m+jd)/2}, & \text{if } m + jd \text{ is even;} \\ \varepsilon \sqrt{p i^{p-1}} p^{(m+jd-1)/2}, & \text{if } m + jd \text{ is odd.} \end{cases}$$

For any $y \in \mathrm{GF}(p)^*$,

$$\sum_{x \in \mathrm{GF}(q)} \omega^{y \mathrm{Tr}_{d/1} Q(a,b)} = \eta_0(y^r) \sum_{x \in \mathrm{GF}(q)} \omega^{\mathrm{Tr}_{d/1} Q(a,b)},$$

where r *is the rank of the quadratic form* $Q(a, b)$, η_0 *is the quadratic character.*

Sketch of proof (3)

Hence

$$S(ya, yb) = \frac{1}{2}\Big(\sum_{x \in \mathrm{GF}(p^m)} \omega^{y\mathrm{Tr}_{k/1}Q(a,b)} + \sum_{x \in \mathrm{GF}(p^m)} \omega^{y\mathrm{Tr}_{k/1}Q(-a,b)} \Big)$$

Sketch of proof (3)

Hence

$$S(ya, yb) = \frac{1}{2}\Big(\sum_{x \in \mathrm{GF}(p^m)} \omega^{y\mathrm{Tr}_{k/1}Q(a,b)} + \sum_{x \in \mathrm{GF}(p^m)} \omega^{y\mathrm{Tr}_{k/1}Q(-a,b)} \Big)$$

$$= \frac{1}{2}\Big(\eta_0(y^{r_1}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1}Q(a,b)}$$

$$+ \eta_0(y^{r_2}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1}Q(-a,b)} \Big).$$

Sketch of proof (3)

Hence

$$S(ya, yb) = \frac{1}{2}\Big(\sum_{x \in \mathrm{GF}(p^m)} \omega^{y\mathrm{Tr}_{k/1}Q(a,b)} + \sum_{x \in \mathrm{GF}(p^m)} \omega^{y\mathrm{Tr}_{k/1}Q(-a,b)} \Big)$$

$$= \frac{1}{2}\Big(\eta_0(y^{r_1}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1}Q(a,b)}$$

$$+ \eta_0(y^{r_2}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1}Q(-a,b)} \Big).$$

CASE A.1: $r_1 = r_2 = s$

Sketch of proof (3)

Hence

$$S(ya, yb) = \frac{1}{2}\Big(\sum_{x \in \mathrm{GF}(p^m)} \omega^{y\mathrm{Tr}_{k/1}Q(a,b)} + \sum_{x \in \mathrm{GF}(p^m)} \omega^{y\mathrm{Tr}_{k/1}Q(-a,b)} \Big)$$

$$= \frac{1}{2}\Big(\eta_0(y^{r_1}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1}Q(a,b)}$$

$$+ \eta_0(y^{r_2}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1}Q(-a,b)}\Big).$$

CASE A.1: $r_1 = r_2 = s$

$$S(ya, yb) = \eta_0(y^s)\varepsilon\sqrt{pi^{p-1}}p^{(m-1)/2}$$

$$= \pm\eta_0(y^s)ip^{m/2},$$

Sketch of proof (4)

As a result,

$$\sum_{y \in \mathrm{GF}(p)^*} \omega^{-yu} S(ya, yb) = \pm i p^{m/2} \sum_{y \in \mathrm{GF}(p)^*} \omega^{-yu} \eta_0(y^s)$$

Sketch of proof (4)

As a result,

$$\sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} S(ya, yb) = \pm i p^{m/2} \sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \eta_0(y^s)$$
$$= \pm i p^{m/2} \sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \eta_0(y)$$

Sketch of proof (4)

As a result,

$$\begin{aligned}\sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} S(ya, yb) &= \pm i p^{m/2} \sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \eta_0(y^s) \\ &= \pm i p^{m/2} \sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \eta_0(y) \\ &= \pm i p^{m/2} G(\eta_0, \hat{\chi}_{-u})\end{aligned}$$

Sketch of proof (4)

As a result,

$$\begin{aligned}
\sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} S(ya, yb) &= \pm i p^{m/2} \sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \eta_0(y^s) \\
&= \pm i p^{m/2} \sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \eta_0(y) \\
&= \pm i p^{m/2} G(\eta_0, \hat{\chi}_{-u}) \\
&= \pm i p^{m/2} \eta_0(-u)(-1)^{(p+1)/2} i^{(p^2+2p+5)/4} p^{1/2}
\end{aligned}$$

Sketch of proof (4)

As a result,

$$\begin{aligned}
\sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} S(ya, yb) &= \pm i p^{m/2} \sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \eta_0(y^s) \\
&= \pm i p^{m/2} \sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \eta_0(y) \\
&= \pm i p^{m/2} G(\eta_0, \hat{\chi}_{-u}) \\
&= \pm i p^{m/2} \eta_0(-u)(-1)^{(p+1)/2} i^{(p^2+2p+5)/4} p^{1/2} \\
&= \pm p^{(m+1)/2} \eta_0(-u)(-1)^{(p+1)/2} i^{(p^2+2p+5)/4}
\end{aligned}$$

Sketch of proof (4)

As a result,

$$\begin{aligned}
\sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} S(ya, yb) &= \pm i p^{m/2} \sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \eta_0(y^s) \\
&= \pm i p^{m/2} \sum_{y\in \mathrm{GF}(p)^*} \omega^{-yu} \eta_0(y) \\
&= \pm i p^{m/2} G(\eta_0, \hat{\chi}_{-u}) \\
&= \pm i p^{m/2} \eta_0(-u)(-1)^{(p+1)/2} i^{(p^2+2p+5)/4} p^{1/2} \\
&= \pm p^{(m+1)/2} \eta_0(-u)(-1)^{(p+1)/2} i^{(p^2+2p+5)/4}
\end{aligned}$$

Thus, we have

$$\max N(c(a,b),u) = p^{m-1} + p^{(m-1)/2}.$$

Sketch of proof (5)

CASE A.2: $r_1 = s, r_2 = s - 1$

Sketch of proof (5)

CASE A.2: $r_1 = s, r_2 = s - 1$

$$S(ya, yb) = \frac{1}{2}(\eta_0(y^{r_1}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1} Q(a,b)} + \eta_0(y^{r_2}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1} Q(-a,b)}).$$

Sketch of proof (5)

CASE A.2: $r_1 = s, r_2 = s-1$

$$S(ya, yb) = \frac{1}{2}(\eta_0(y^{r_1}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1} Q(a,b)} + \eta_0(y^{r_2}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1} Q(-a,b)}).$$

$$= \frac{1}{2}(\eta_0(y^s)\varepsilon\sqrt{pi^{p-1}}p^{(m-1)/2} + \eta_0(y^{s-1})\varepsilon p^{(m+k)/2})$$

Sketch of proof (5)

CASE A.2: $r_1 = s, r_2 = s-1$

$$S(ya, yb) = \frac{1}{2}(\eta_0(y^{r_1}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1} Q(a,b)} + \eta_0(y^{r_2}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1} Q(-a,b)}).$$

$$= \frac{1}{2}(\eta_0(y^s)\varepsilon\sqrt{pi^{p-1}}p^{(m-1)/2} + \eta_0(y^{s-1})\varepsilon p^{(m+k)/2})$$

$$= \pm\frac{1}{2}(\eta_0(y^s)i\sqrt{p}p^{(m-1)/2} \pm \eta_0(y^{s-1})p^{(m+k)/2})$$

Sketch of proof (5)

CASE A.2: $r_1 = s, r_2 = s-1$

$$S(ya, yb) = \frac{1}{2}(\eta_0(y^{r_1}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1} Q(a,b)} + \eta_0(y^{r_2}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1} Q(-a,b)}).$$

$$= \frac{1}{2}(\eta_0(y^s)\varepsilon\sqrt{p i^{p-1}} p^{(m-1)/2} + \eta_0(y^{s-1})\varepsilon p^{(m+k)/2})$$

$$= \pm\frac{1}{2}(\eta_0(y^s) i\sqrt{p} p^{(m-1)/2} \pm \eta_0(y^{s-1}) p^{(m+k)/2})$$

$$= \pm\frac{1}{2}(\eta_0(y) i p^{m/2} \pm p^{(m+k)/2}).$$

Sketch of proof (5)

CASE A.2: $r_1 = s, r_2 = s-1$

$$S(ya, yb) = \frac{1}{2}(\eta_0(y^{r_1}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1} Q(a,b)} + \eta_0(y^{r_2}) \sum_{x \in \mathrm{GF}(p^m)} \omega^{\mathrm{Tr}_{k/1} Q(-a,b)}).$$

$$= \frac{1}{2}(\eta_0(y^s)\varepsilon\sqrt{pi^{p-1}}p^{(m-1)/2} + \eta_0(y^{s-1})\varepsilon p^{(m+k)/2})$$

$$= \pm\frac{1}{2}(\eta_0(y^s) i\sqrt{p} p^{(m-1)/2} \pm \eta_0(y^{s-1}) p^{(m+k)/2})$$

$$= \pm\frac{1}{2}(\eta_0(y) i p^{m/2} \pm p^{(m+k)/2}).$$

Similarly, we derive $\sum_{y \in \mathrm{GF}(p)^*} \omega^{-yu} S(ya, yb)$ and

$$\max N(c(a,b), u) = p^{m-1} + \frac{1}{2}(p^{(m-1)/2} + p^{(m+k-2)/2}).$$

Sketch of proof (6)

We omit the details of

- **CASE A.3**: $r_1 = s, r_2 = s - 2$
- **CASE B**: $r_1 \leq r_2$
- **CASE C**: $s = 1$

Sketch of proof (6)

We omit the details of

- **CASE A.3**: $r_1 = s, r_2 = s - 2$
- **CASE B**: $r_1 \leq r_2$
- **CASE C**: $s = 1$

To wrap up, we have

$$P_S = \begin{cases} \frac{\frac{3}{2}p^{m-1} + \frac{1}{2}p^{(m-1)/2}}{p^m - 1}, & \text{if } m = k; \\ \frac{p^{m-1} + \frac{1}{2}p^{(m-1)/2} + \frac{1}{2}p^{(m+2k-1)/2}}{p^m - 1}, & \text{if } m > k. \end{cases}$$

Third class of authentication codes

Lemma

$m, k \in \mathbb{Z}^+$, $d = \gcd(m, k)$, $s = m/d$ *is odd*, $s \geq 3$.

Third class of authentication codes

Lemma

$m, k \in \mathbb{Z}^+$, $d = \gcd(m, k)$, $s = m/d$ *is odd*, $s \geq 3$.
$p \leftarrow$ *odd prime*, $q = p^m$, $q_0 = p^d$.

Third class of authentication codes

Lemma

$m, k \in \mathbb{Z}^+$, $d = \gcd(m, k)$, $s = m/d$ *is odd,* $s \geq 3$.
$p \leftarrow$ *odd prime,* $q = p^m$, $q_0 = p^d$.
The cyclic code $\mathcal{C}$ *with parity check polynomial* $h_1(x)h_2(x)$, *where* $h_1(x), h_2(x)$ *are the minimal polynomials of* $(-\pi)^{-1}$ *and* $\pi^{-(p^k+1)/2}$, *has the parameter*

$$[p^m - 1, 2m, p^m - p^{m-1} - \frac{p-1}{2}p^{(m+d-2)/2}].$$

Third class of authentication codes

Lemma

$m, k \in \mathbb{Z}^+$, $d = \gcd(m, k)$, $s = m/d$ *is odd,* $s \geq 3$.
$p \leftarrow$ *odd prime,* $q = p^m$, $q_0 = p^d$.
The cyclic code $\mathcal{C}$ *with parity check polynomial* $h_1(x)h_2(x)$, *where* $h_1(x), h_2(x)$ *are the minimal polynomials of* $(-\pi)^{-1}$ *and* $\pi^{-(p^k+1)/2}$, *has the parameter*

$$[p^m - 1, 2m, p^m - p^{m-1} - \frac{p-1}{2} p^{(m+d-2)/2}].$$

Trace representation:

$$\boldsymbol{c}(a, b) = \left(\mathrm{Tr}\left(a(-\pi)^t + b\pi^{(p^k+1)t/2} \right) \right)_{t=0}^{q-2}.$$

Third class of authentication codes

Theorem

The authentication code constructed is

$$(\mathbb{Z}_{p^{2m}}, \mathrm{GF}(p), \mathbb{Z}_{p^m-1} \times \mathrm{GF}(p), \{E_k : k \in \mathcal{K}\}),$$

Third class of authentication codes

Theorem

The authentication code constructed is

$$(\mathbb{Z}_{p^{2m}}, \mathrm{GF}(p), \mathbb{Z}_{p^m-1} \times \mathrm{GF}(p), \{E_k : k \in \mathcal{K}\}),$$

with

$$P_I = \frac{1}{p}, P_S = \begin{cases} \frac{p^{m-1}+\frac{1}{2}p^{(m-1)/2}+\frac{1}{2}p^{(m+2d-1)/2}}{p^m-1}, & \text{if } k/d \text{ is even;} \\ \frac{p^{m-1}+p^{(m+2d-1)/2}}{p^m-1}, & \text{if } k/d \text{ is odd.} \end{cases}$$

Third class of authentication codes

Theorem

The authentication code constructed is

$$(\mathbb{Z}_{p^{2m}}, \mathrm{GF}(p), \mathbb{Z}_{p^m-1} \times \mathrm{GF}(p), \{E_k : k \in \mathcal{K}\}),$$

with

$$P_I = \frac{1}{p}, P_S = \begin{cases} \frac{p^{m-1}+\frac{1}{2}p^{(m-1)/2}+\frac{1}{2}p^{(m+2d-1)/2}}{p^m-1}, & \text{if } k/d \text{ is even;} \\ \frac{p^{m-1}+p^{(m+2d-1)/2}}{p^m-1}, & \text{if } k/d \text{ is odd.} \end{cases}$$

Furthermore, we have

$$|\mathcal{S}| = p^{2m}, |\mathcal{T}| = p, |\mathcal{K}| = (p^m - 1)p.$$

Third class of authentication codes

Theorem

The authentication code constructed is

$$(\mathbb{Z}_{p^{2m}}, \mathrm{GF}(p), \mathbb{Z}_{p^m-1} \times \mathrm{GF}(p), \{E_k : k \in \mathcal{K}\}),$$

with

$$P_I = \frac{1}{p}, P_S = \begin{cases} \frac{p^{m-1}+\frac{1}{2}p^{(m-1)/2}+\frac{1}{2}p^{(m+2d-1)/2}}{p^m-1}, & \text{if } k/d \text{ is even;} \\ \frac{p^{m-1}+p^{(m+2d-1)/2}}{p^m-1}, & \text{if } k/d \text{ is odd.} \end{cases}$$

Furthermore, we have

$$|\mathcal{S}| = p^{2m}, |\mathcal{T}| = p, |\mathcal{K}| = (p^m - 1)p.$$

We omit the details of the proof

Outline

Comparison

- The proposed authentication codes $C1$, $C2$, $C3$

Comparison

- The proposed authentication codes $C1$, $C2$, $C3$
- Compare the parameters $|\mathcal{S}|, |\mathcal{T}|, |\mathcal{K}|, P_I$ and P_S

Comparison

- The proposed authentication codes $C1$, $C2$, $C3$
- Compare the parameters $|\mathcal{S}|, |\mathcal{T}|, |\mathcal{K}|, P_I$ and P_S
- P_I and P_S: as small as possible

Comparison

- The proposed authentication codes $C1$, $C2$, $C3$
- Compare the parameters $|\mathcal{S}|, |\mathcal{T}|, |\mathcal{K}|, P_I$ and P_S
- P_I and P_S: as small as possible
- $|\mathcal{S}|, |\mathcal{T}|, |\mathcal{K}|$: consider tradeoff

Example 1

Example 1

When $p = 3$:
$|\mathcal{S}(C1)| = |\mathcal{S}(C2)|$, $|\mathcal{T}(C1)| = |\mathcal{T}(C2)|$, $|\mathcal{K}(C1)| = |\mathcal{K}(C2)|$
$P_I(C1) = P_I(C2)$

Example 1

When $p = 3$:
$|\mathcal{S}(C1)| = |\mathcal{S}(C2)|$, $|\mathcal{T}(C1)| = |\mathcal{T}(C2)|$, $|\mathcal{K}(C1)| = |\mathcal{K}(C2)|$
$P_I(C1) = P_I(C2)$

$$P_S(C1) = \frac{3^{m-1} + \frac{1}{2}(3^{(m-1)/2} + 3^{(m+1)/2})}{3^m - 1},$$

$$P_S(C2) = \begin{cases} \frac{\frac{3}{2}p^{m-1} + \frac{1}{2}p^{(m-1)/2}}{p^m - 1}, & \text{if } m = k; \\ \frac{p^{m-1} + \frac{1}{2}p^{(m-1)/2} + \frac{1}{2}p^{(m+2k-1)/2}}{p^m - 1}, & \text{if } m > k. \end{cases}$$

Example 1

When $p = 3$:
$|\mathcal{S}(C1)| = |\mathcal{S}(C2)|$, $|\mathcal{T}(C1)| = |\mathcal{T}(C2)|$, $|\mathcal{K}(C1)| = |\mathcal{K}(C2)|$
$P_I(C1) = P_I(C2)$

$$P_S(C1) = \frac{3^{m-1} + \frac{1}{2}(3^{(m-1)/2} + 3^{(m+1)/2})}{3^m - 1},$$

$$P_S(C2) = \begin{cases} \frac{\frac{3}{2}p^{m-1} + \frac{1}{2}p^{(m-1)/2}}{p^m - 1}, & \text{if } m = k; \\ \frac{p^{m-1} + \frac{1}{2}p^{(m-1)/2} + \frac{1}{2}p^{(m+2k-1)/2}}{p^m - 1}, & \text{if } m > k. \end{cases}$$

- If $k = 1 < m$: $P_S(C1) = P_S(C2)$

Example 1

When $p = 3$:
$|\mathcal{S}(C1)| = |\mathcal{S}(C2)|$, $|\mathcal{T}(C1)| = |\mathcal{T}(C2)|$, $|\mathcal{K}(C1)| = |\mathcal{K}(C2)|$
$P_I(C1) = P_I(C2)$

$$P_S(C1) = \frac{3^{m-1} + \frac{1}{2}(3^{(m-1)/2} + 3^{(m+1)/2})}{3^m - 1},$$

$$P_S(C2) = \begin{cases} \frac{\frac{3}{2}p^{m-1} + \frac{1}{2}p^{(m-1)/2}}{p^m - 1}, & \text{if } m = k; \\ \frac{p^{m-1} + \frac{1}{2}p^{(m-1)/2} + \frac{1}{2}p^{(m+2k-1)/2}}{p^m - 1}, & \text{if } m > k. \end{cases}$$

- If $k = 1 < m$: $P_S(C1) = P_S(C2)$
- If $m > k \geq 2$ or $m = k > 3$: $P_S(C1) < P_S(C2)$

Example 1

When $p = 3$:
$|\mathcal{S}(C1)| = |\mathcal{S}(C2)|$, $|\mathcal{T}(C1)| = |\mathcal{T}(C2)|$, $|\mathcal{K}(C1)| = |\mathcal{K}(C2)|$
$P_I(C1) = P_I(C2)$

$$P_S(C1) = \frac{3^{m-1} + \frac{1}{2}(3^{(m-1)/2} + 3^{(m+1)/2})}{3^m - 1},$$

$$P_S(C2) = \begin{cases} \frac{\frac{3}{2}p^{m-1} + \frac{1}{2}p^{(m-1)/2}}{p^m - 1}, & \text{if } m = k; \\ \frac{p^{m-1} + \frac{1}{2}p^{(m-1)/2} + \frac{1}{2}p^{(m+2k-1)/2}}{p^m - 1}, & \text{if } m > k. \end{cases}$$

- If $k = 1 < m$: $P_S(C1) = P_S(C2)$
- If $m > k \geq 2$ or $m = k > 3$: $P_S(C1) < P_S(C2)$
- $C1$ is better than $C2$

Example 2

Example 2

$$|\mathcal{S}(C2)| = |\mathcal{S}(C3)|, |\mathcal{K}(C2)| = |\mathcal{K}(C3)|$$

Example 2

$$|\mathcal{S}(C2)| = |\mathcal{S}(C3)|, |\mathcal{K}(C2)| = |\mathcal{K}(C3)|$$

When $d = k$ in $C3$

$$P_S(C2) = \begin{cases} \frac{\frac{3}{2}p^{m-1}+\frac{1}{2}p^{(m-1)/2}}{p^m-1}, & \text{if } m = k; \\ \frac{p^{m-1}+\frac{1}{2}p^{(m-1)/2}+\frac{1}{2}p^{(m+2k-1)/2}}{p^m-1}, & \text{if } m > k. \end{cases}$$

Example 2

$$|\mathcal{S}(C2)| = |\mathcal{S}(C3)|, |\mathcal{K}(C2)| = |\mathcal{K}(C3)|$$

When $d = k$ in $C3$

$$P_S(C2) = \begin{cases} \frac{\frac{3}{2}p^{m-1}+\frac{1}{2}p^{(m-1)/2}}{p^m-1}, & \text{if } m = k; \\ \frac{p^{m-1}+\frac{1}{2}p^{(m-1)/2}+\frac{1}{2}p^{(m+2k-1)/2}}{p^m-1}, & \text{if } m > k. \end{cases}$$

$$P_S(C3) = \frac{p^{m-1} + p^{(m+2d-1)/2}}{p^m - 1}$$

Example 2

$$|\mathcal{S}(C2)| = |\mathcal{S}(C3)|, |\mathcal{K}(C2)| = |\mathcal{K}(C3)|$$

When $d = k$ in $C3$

$$P_S(C2) = \begin{cases} \frac{\frac{3}{2}p^{m-1}+\frac{1}{2}p^{(m-1)/2}}{p^m-1}, & \text{if } m = k; \\ \frac{p^{m-1}+\frac{1}{2}p^{(m-1)/2}+\frac{1}{2}p^{(m+2k-1)/2}}{p^m-1}, & \text{if } m > k. \end{cases}$$

$$P_S(C3) = \frac{p^{m-1} + p^{(m+2d-1)/2}}{p^m - 1}$$

We have

$$P_S(C2) \leq P_S(C3)$$

Thus, under a special condition, C2 is better than C3.

Example 3

Example 3

C4: authentication code from [Ding-Helleseth-Kløve-Wang]

$|\mathcal{S}| = p^{2m}, |\mathcal{T}| = p, |\mathcal{K}| = p^{m+1}$

$$P_I = \frac{1}{p}, P_S = \begin{cases} \frac{1}{p} + \frac{p-1}{p^{m/2+1}}, & \text{when } m \text{ is even;} \\ \frac{1}{p} + \frac{1}{p^{(m+1)/2}}, & \text{when } m \text{ is odd,} \end{cases}$$

Example 3

C4: authentication code from [Ding-Helleseth-Kløve-Wang]

$|\mathcal{S}| = p^{2m}, |\mathcal{T}| = p, |\mathcal{K}| = p^{m+1}$

$$P_I = \frac{1}{p}, P_S = \begin{cases} \frac{1}{p} + \frac{p-1}{p^{m/2+1}}, & \text{when } m \text{ is even;} \\ \frac{1}{p} + \frac{1}{p^{(m+1)/2}}, & \text{when } m \text{ is odd,} \end{cases}$$

Compared with C2,

- same $|\mathcal{S}|, |\mathcal{T}|$ and P_I

Example 3

C4: authentication code from [Ding-Helleseth-Kløve-Wang]

$|\mathcal{S}| = p^{2m}, |\mathcal{T}| = p, |\mathcal{K}| = p^{m+1}$

$$P_I = \frac{1}{p}, P_S = \begin{cases} \frac{1}{p} + \frac{p-1}{p^{m/2+1}}, & \text{when } m \text{ is even;} \\ \frac{1}{p} + \frac{1}{p^{(m+1)/2}}, & \text{when } m \text{ is odd,} \end{cases}$$

Compared with C2,

- same $|\mathcal{S}|, |\mathcal{T}|$ and P_I
- $|\mathcal{K}(C2)| < |\mathcal{K}(C4)|$

Example 3

C4: authentication code from [Ding-Helleseth-Kløve-Wang]

$|\mathcal{S}| = p^{2m}, |\mathcal{T}| = p, |\mathcal{K}| = p^{m+1}$

$$P_I = \frac{1}{p}, P_S = \begin{cases} \frac{1}{p} + \frac{p-1}{p^{m/2+1}}, & \text{when } m \text{ is even;} \\ \frac{1}{p} + \frac{1}{p^{(m+1)/2}}, & \text{when } m \text{ is odd,} \end{cases}$$

Compared with C2,

- same $|\mathcal{S}|, |\mathcal{T}|$ and P_I
- $|\mathcal{K}(C2)| < |\mathcal{K}(C4)|$
- $P_S(C2) \geq P_S(C4)$

Example 3

C4: authentication code from [Ding-Helleseth-Kløve-Wang]

$|\mathcal{S}| = p^{2m}, |\mathcal{T}| = p, |\mathcal{K}| = p^{m+1}$

$$P_I = \frac{1}{p}, P_S = \begin{cases} \frac{1}{p} + \frac{p-1}{p^{m/2+1}}, & \text{when } m \text{ is even;} \\ \frac{1}{p} + \frac{1}{p^{(m+1)/2}}, & \text{when } m \text{ is odd,} \end{cases}$$

Compared with C2,

- same $|\mathcal{S}|, |\mathcal{T}|$ and P_I
- $|\mathcal{K}(C2)| < |\mathcal{K}(C4)|$
- $P_S(C2) \geq P_S(C4)$
- Asymptotically, the difference between $P_S(C2)$ and $P_S(C4)$ is negligible.

Example 3

C4: authentication code from [Ding-Helleseth-Kløve-Wang]

$|\mathcal{S}| = p^{2m}, |\mathcal{T}| = p, |\mathcal{K}| = p^{m+1}$

$$P_I = \frac{1}{p}, P_S = \begin{cases} \frac{1}{p} + \frac{p-1}{p^{m/2+1}}, & \text{when } m \text{ is even;} \\ \frac{1}{p} + \frac{1}{p^{(m+1)/2}}, & \text{when } m \text{ is odd,} \end{cases}$$

Compared with C2,

- same $|\mathcal{S}|, |\mathcal{T}|$ and P_I
- $|\mathcal{K}(C2)| < |\mathcal{K}(C4)|$
- $P_S(C2) \geq P_S(C4)$
- Asymptotically, the difference between $P_S(C2)$ and $P_S(C4)$ is negligible.
- tradeoff between the key length and P_S

Example 4

Example 4

A similar example with Example 3 can be found as following

C5: authentication code from [Ding-Niederreiter]

When $q = p \geq 3$, $|\mathcal{S}| = p^{2m}$, $|\mathcal{T}| = p$, $|\mathcal{K}| = p^{m+1}$

$$P_I = \frac{1}{p}, \ P_S = \frac{1}{p} + \frac{p-1}{p^{(m+2)/2}}$$

Example 4

A similar example with Example 3 can be found as following

C5: authentication code from [Ding-Niederreiter]

When $q = p \geq 3$, $|\mathcal{S}| = p^{2m}$, $|\mathcal{T}| = p$, $|\mathcal{K}| = p^{m+1}$

$$P_I = \frac{1}{p}, \ P_S = \frac{1}{p} + \frac{p-1}{p^{(m+2)/2}}$$

- same $|\mathcal{S}|, |\mathcal{T}|$ and P_I

Example 4

A similar example with Example 3 can be found as following

C5: authentication code from [Ding-Niederreiter]

When $q = p \geq 3$, $|\mathcal{S}| = p^{2m}$, $|\mathcal{T}| = p$, $|\mathcal{K}| = p^{m+1}$

$$P_I = \frac{1}{p}, \ P_S = \frac{1}{p} + \frac{p-1}{p^{(m+2)/2}}$$

- same $|\mathcal{S}|, |\mathcal{T}|$ and P_I
- $|\mathcal{K}(C2)| < |\mathcal{K}(C5)|$

Example 4

A similar example with Example 3 can be found as following

C5: authentication code from [Ding-Niederreiter]

When $q = p \geq 3$, $|\mathcal{S}| = p^{2m}$, $|\mathcal{T}| = p$, $|\mathcal{K}| = p^{m+1}$

$$P_I = \frac{1}{p}, \ P_S = \frac{1}{p} + \frac{p-1}{p^{(m+2)/2}}$$

- same $|\mathcal{S}|, |\mathcal{T}|$ and P_I
- $|\mathcal{K}(C2)| < |\mathcal{K}(C5)|$
- tradeoff between the key length and P_S

[Ding-Niederreiter] C. Ding and H. Niederreiter, Systematic authentication codes from highly nonlinear functions, IEEE Transactions on Information Theory, 2004.

Conclusion

- Systematic authentication codes can be constructed from cyclic codes with only a few zeroes

Conclusion

- Systematic authentication codes can be constructed from cyclic codes with only a few zeroes
- New authentication codes proposed based on cyclic codes with two zeroes

Conclusion

- Systematic authentication codes can be constructed from cyclic codes with only a few zeroes
- New authentication codes proposed based on cyclic codes with two zeroes
- Detailed analysis of the maximum success probability P_S

Conclusion

- Systematic authentication codes can be constructed from cyclic codes with only a few zeroes
- New authentication codes proposed based on cyclic codes with two zeroes
- Detailed analysis of the maximum success probability P_S
- Comparison and tradeoffs of their parameters

Conclusion

- Systematic authentication codes can be constructed from cyclic codes with only a few zeroes
- New authentication codes proposed based on cyclic codes with two zeroes
- Detailed analysis of the maximum success probability P_S
- Comparison and tradeoffs of their parameters

Thank you for your attention!