Highway to Hull: A new algorithm solving the matrix code equivalence problem

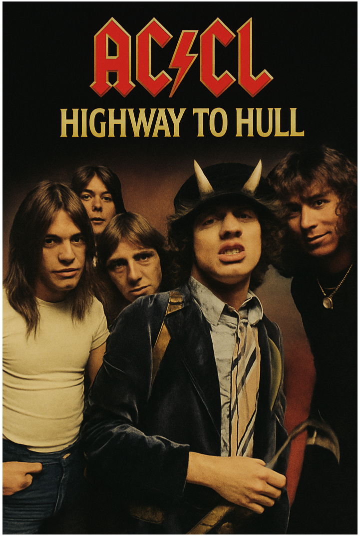
Alain Couvreur Christophe Levrat

Inria

CRYPTO 2025

16 June 2025

You may have heard of us



Picture created using ChatGPT, inspired by the original cover of the album *Highway to Hell* by AC/DC.

tl;wl

- A particular case of the matrix code equivalence problem is used in recent signature schemes MEDS, ALTEQ.

- Two recent attacks (2024) on some specific instances made them change their parameters.

- We provide an algorithm HtH for a much broader range of parameters, with competitive complexity.

- HtH is based on the following idea: compute one-dimensional *hulls* of various codes, and search for collisions among them.

1. The matrix code equivalence problem

2. Overview of HtH

1. The matrix code equivalence problem

2. Overview of HtH

MCE: decisional and search problems

Fix a finite field $\mathbb{F}_q$ and positive integers k, m, n such that $m \leqslant n$ and $k < mn$.

The matrix code equivalence problem (MCE)

Given k-dimensional linear subspaces $\mathcal{C}, \mathcal{D}$ of $\mathbb{F}_q^{m \times n}$:

- MCE Decisional problem: Do there exist matrices $P \in \mathrm{GL}_m(\mathbb{F}_q), Q \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $\mathcal{D} = P\mathcal{C}Q$?
- MCE Search problem: Find, if such matrices exist, $P \in \mathrm{GL}_m(\mathbb{F}_q), Q \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $\mathcal{D} = P\mathcal{C}Q$.
- Particular case $k = m = n$: cubic matrix code equivalence problem (CMCE).

We present a probabilistic algorithm for the MCE search problem.

- ☐ $m \leqslant n$
- ☐ $k < mn$
- ☐ $\mathcal{C}, \mathcal{D} \subset \mathbb{F}_q^{m \times n}$
- ☐ $k = \dim(\mathcal{C})$

Related problems

The following problems are equivalent to MCE.

- ◇ 3-Tensor Isomorphism
- ◇ Trilinear Forms Equivalence (TFE)
- ◇ Matrix Space Conjugacy (MCE with $Q = P^{-1}$)

- ☐ $m \leqslant n$
- ☐ $k < mn$
- ☐ $\mathcal{C}, \mathcal{D} \subset \mathbb{F}_q^{m \times n}$
- ☐ $k = \dim(\mathcal{C})$

Use of these problems in NIST submissions

Two signature schemes based on these problems were recently put forward.

- ALTEQ: based on TFE
  Parameters (NIST Level I): $q = 2^{32} - 5$, $k = m = n = 13$
  Parameters (NIST Level III): $q = 2^{32} - 5$, $k = m = n = 20$

- MEDS: based on MCE (but actually, the initial parameters were all instances of CMCE)
  Parameters (NIST Level I): $q = 2^{12} - 1$, $k = m = n = 14$
  Parameters (NIST Level III): $q = 2^{12} - 1$, $k = m = n = 22$

Both were thrown out of the NIST competition in October 2024.

- $m \leqslant n$
- $k < mn$
- $\mathcal{C}, \mathcal{D} \subset \mathbb{F}_q^{m \times n}$
- $k = \dim(\mathcal{C})$

Recent algorithms for MCE

[Narayanan, Qiao, Tang (2024)]

Method: Find matching points of corank 1 in both codes and construct equivalence from them

Strength: Best theoretical complexity to date $\widetilde{\mathcal{O}}(q^{n/2})$

Weakness: Only applies to CMCE problem ($k = m = n$)

[Ran, Samardjiska (2024)]

Method: Construct graphs associated with tensors, find triangles in them and construct equivalence from these triangles (low-degree polynomial system solving)

Strength: Best practical complexity to date

Weakness: Only works in $1/q$ of all cases (when graphs contain triangles)

- ☐ $m \leqslant n$
- ☐ $k < mn$
- ☐ $\mathcal{C}, \mathcal{D} \subset \mathbb{F}_q^{m \times n}$
- ☐ $k = \dim(\mathcal{C})$

How HtH compares to the state of the art

- ◇ Parameter range: $\{k, k^{\perp} < \min(m,n)^2 - 1\}$ where $k^{\perp} = mn - k$

$\rightarrow$ much broader than both previous algorithms.

- ◇ Time complexity when $k = m = n$: $\widetilde{\mathcal{O}}(q^{n/2})$

$\rightarrow$ similar to Narayanan et al.

$\rightarrow$ in practice, not better than Ran and Samardjiska.

- ◇ Space complexity when $k = m = n$: $\mathcal{O}\left(nq^{\frac{n}{2}-1}\right)$

$\rightarrow$ $\mathcal{O}(n^2)$ times smaller than Narayanan et al.

- ☐ $m \leqslant n$
- ☐ $k < mn$
- ☐ $\mathcal{C}, \mathcal{D} \subset \mathbb{F}_q^{m \times n}$
- ☐ $k = \dim(\mathcal{C})$

General structure

Data k-dimensional matrix codes $\mathcal{C}, \mathcal{D} \subset \mathbb{F}_q^{m \times n}$.

Goal Find P, Q such that $\mathcal{D} = P\mathcal{C}Q$.

1. Reduce to conjugacy problem (i.e. $Q = P^{-1}$) for codes $\mathcal{C}_A, \mathcal{D}_B$ computed from $\mathcal{C}, \mathcal{D}$
   ... for which we know a pair of conjugate 1-dimensional subspaces in $\mathcal{C}$ and $\mathcal{D}$ (collision search).

2. Solve this conjugacy problem.

3. Deduce solution to the original problem.

- ☐ $m \leqslant n$
- ☐ $k < mn$
- ☐ $\mathcal{C}, \mathcal{D} \subset \mathbb{F}_q^{m \times n}$
- ☐ $k = \dim(\mathcal{C})$

Reducing to conjugacy problem (1/2)

If $\mathcal{D} = P\mathcal{C}Q$, then for each $A \in \mathcal{C}^\perp$, $B = (P^{-1})^\top A(Q^{-1})^\top \in \mathcal{D}^\perp$.

We produce codes $\mathcal{C}_A = \mathcal{C}A^\top, \mathcal{D}_B = \mathcal{D}B^\top$ where $A \in \mathcal{C}^\perp, B \in \mathcal{D}^\perp$, hoping to find a matching pair (A, B). For such a pair, $\mathcal{D}_B = P\mathcal{C}_A P^{-1}$.

- ◇ Checking whether two k-dimensional codes are conjugate is hard.
- ◇ Checking whether two 1-dimensional codes are conjugate is easy.

→ We try to find A, B such that $\mathcal{C}_A$ and $\mathcal{D}_B$ contain specific conjugate 1-dimensional subspaces: their respective *hulls*.

- ☐ $m \leqslant n$
- ☐ $k < mn$
- ☐ $\mathcal{C}, \mathcal{D} \subset \mathbb{F}_q^{m \times n}$
- ☐ $k = \dim(\mathcal{C})$
- ☐ $A \in \mathcal{C}^\perp$
$B \in \mathcal{D}^\perp$
- ☐ $\mathcal{C}_A = \mathcal{C}A^\top$
$\mathcal{D}_B = \mathcal{D}B^\top$

Reducing to conjugacy problem (2/2)

Definition

In this talk, the hull of a matrix code $\mathcal{C} \subset \mathbb{F}_q^{m \times m}$ is

$$h(\mathcal{C}) = \{A \in \mathcal{C} \mid \forall B \in \mathcal{C}, \mathrm{Tr}(AB) = 0\}.$$

- ◇ Two conjugate codes have conjugate hulls.
- ◇ Roughly $1/q$ of all codes have 1-dimensional hull.
- ◇ Given a uniformly random code $\mathcal{C}$ and a uniformly random matrix A such that $h(\mathcal{C}_A)$ has dimension 1, the characteristic polynomial of a generator of $h(\mathcal{C}_A)$ is uniformly random.

- ☐ $m \leqslant n$
- ☐ $k < mn$
- ☐ $\mathcal{C}, \mathcal{D} \subset \mathbb{F}_q^{m \times n}$
- ☐ $k = \dim(\mathcal{C})$
- ☐ $A \in \mathcal{C}^\perp$
  $B \in \mathcal{D}^\perp$
- ☐ $\mathcal{C}_A = \mathcal{C}A^\top$
  $\mathcal{D}_B = \mathcal{D}B^\top$

Overview of the collision search

- Construct a dictionary (polynomial:matrix):

  1. Pick matrix $A \in \mathcal{C}^\perp$
  2. If $\dim h(\mathcal{C}_A) = 1$, compute the characteristic polynomial χ of a normalized generator of $h(\mathcal{C}_A)$, add $(\chi : A)$ to the dictionary
  3. Continue until the dictionary contains $\mathcal{O}(q^{(m-3)/2})$ entries

- Find matching pairs:

  1. Pick matrix $B \in \mathcal{D}^\perp$
  2. If $\dim h(\mathcal{D}_B) = 1$, compute the characteristic polynomial of a normalized generator of $h(\mathcal{D}_B)$ and look for collision in the dictionary

- ☐ $m \leqslant n$
- ☐ $k < mn$
- ☐ $\mathcal{C}, \mathcal{D} \subset \mathbb{F}_q^{m \times n}$
- ☐ $k = \dim(\mathcal{C})$
- ☐ $A \in \mathcal{C}^\perp$
$B \in \mathcal{D}^\perp$
- ☐ $\mathcal{C}_A = \mathcal{C}A^\top$
$\mathcal{D}_B = \mathcal{D}B^\top$

Solving conjugacy problem

Data Codes $\mathcal{C}_A, \mathcal{D}_B \subset \mathbb{F}_q^{m\times m}$ containing two conjugate vectors $U_A \in h(\mathcal{C}_A)$, $V_B \in h(\mathcal{D}_B)$:

$$V_B = P_0 U_A P_0^{-1}.$$

Goal Find P such that $\mathcal{D}_B = P\mathcal{C}_A P^{-1}$.

Solution If such a P exists, then there exist $f, g \in \mathbb{F}_q[t]_{\leqslant m}$ such that

$$P = P_0 f(U_A) \text{ and } P^{-1} = g(U_A)P_0^{-1}.$$

We compute the coefficients of f and g by linearizing the bilinear system:

$$P_0 f(U_A)\mathcal{C}_A g(U_A)P_0^{-1} \subseteq \mathcal{D}_B.$$

- ☐ $m \leqslant n$
- ☐ $k < mn$
- ☐ $\mathcal{C}, \mathcal{D} \subset \mathbb{F}_q^{m\times n}$
- ☐ $k = \dim(\mathcal{C})$
- ☐ $A \in \mathcal{C}^\perp$
  $B \in \mathcal{D}^\perp$
- ☐ $\mathcal{C}_A = \mathcal{C}A^\top$
  $\mathcal{D}_B = \mathcal{D}B^\top$

Solving the initial problem

Data Codes $\mathcal{C}, \mathcal{D}$ and matrices $A \in \mathcal{C}^\perp, B \in \mathcal{D}^\perp$, $P \in \mathrm{GL}_m(\mathbb{F}_q)$ such that $\mathcal{D}_B = P\mathcal{C}_A P^{-1}$.

Goal Find a matrix Q such that $\mathcal{D} = P\mathcal{C}Q$.

Solution Let $(C_1, \ldots, C_k)$ be a basis of $\mathcal{C}$. Define the linear map:

$$\begin{aligned} \psi_{\mathcal{C}} \colon \mathbb{F}_q^{n \times n} &\longrightarrow (\mathbb{F}_q^{m \times n})^k \\ Q &\longmapsto (PC_1Q, \ldots, PC_kQ). \end{aligned}$$

The suitable matrices Q are exactly the elements of $\psi_{\mathcal{C}}^{-1}(\mathcal{D}^k) \cap \mathrm{GL}_n(\mathbb{F}_q)$.

- ☐ $m \leqslant n$
- ☐ $k < mn$
- ☐ $\mathcal{C}, \mathcal{D} \subset \mathbb{F}_q^{m \times n}$
- ☐ $k = \dim(\mathcal{C})$
- ☐ $A \in \mathcal{C}^\perp$, $B \in \mathcal{D}^\perp$
- ☐ $\mathcal{C}_A = \mathcal{C}A^\top$, $\mathcal{D}_B = \mathcal{D}B^\top$

Total complexity

Theorem

For parameters k, m, n such that $m(n-m)+2 < k \leqslant mn/2$, the average number of operations in $\mathbb{F}_q$ required by algorithm HtH *to solve* $\mathsf{MCE}_{k,m,n}$ *is*

$$\widetilde{\mathcal{O}}\left(q^{\max\left(\frac{k^\perp}{2}, k^\perp - m + 2\right)}\right)$$

where $k^\perp = nm - k$.

Remark

For $k = m = n$, the above complexity is

$$\widetilde{\mathcal{O}}\left(q^{n/2}\right).$$

- ☐ $m \leqslant n$
- ☐ $k < mn$
- ☐ $\mathcal{C}, \mathcal{D} \subset \mathbb{F}_q^{m \times n}$
- ☐ $k = \dim(\mathcal{C})$
- ☐ $k^\perp = mn - k$
- ☐ $A \in \mathcal{C}^\perp$
$B \in \mathcal{D}^\perp$
- ☐ $\mathcal{C}_A = \mathcal{C}A^\top$
$\mathcal{D}_B = \mathcal{D}B^\top$

tl;dl

- We provide an algorithm HtH which solves the MCE problem with time complexity $\widetilde{\mathcal{O}}\left(q^{\max\left(\frac{k^\perp}{2}, k^\perp - m + 2\right)}\right)$ for a broad range of parameters.
- HtH is based on the following idea: compute one-dimensional hulls of various codes, and search for collisions among them.
- In the cubic case $k = m = n$: matches the state of the art in terms of time complexity and beats it in terms of space complexity.
- In the general case: first algorithm with this complexity.

- ☐ $m \leqslant n$
- ☐ $k < mn$
- ☐ $\mathcal{C}, \mathcal{D} \subset \mathbb{F}_q^{m \times n}$
- ☐ $k = \dim(\mathcal{C})$
- ☐ $k^\perp = mn - k$
- ☐ $A \in \mathcal{C}^\perp$
$B \in \mathcal{D}^\perp$
- ☐ $\mathcal{C}_A = \mathcal{C}A^\top$
$\mathcal{D}_B = \mathcal{D}B^\top$