Reducing Signature Size of Matrix-code-based Signature Schemes

https://ia.cr/2024/495

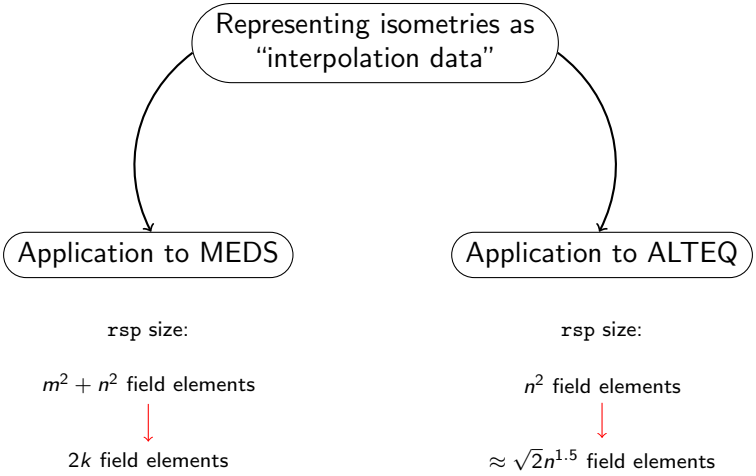
Tung Chou[1], Ruben Niederhagen[1], Lars Ran[2], Simona Samardjiska[2]

[1]Academia Sinica

[2]Radboud University

June 14, 2024

What this paper is about



Matrix code equivalence (MCE)

Definition

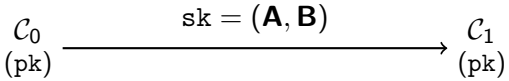
Given dimension-k linear codes $\mathcal{C}_0, \mathcal{C}_1$, where code words are considered as matrices in $\mathbb{F}_q^{m\times n}$. MCE asks to find $\mathbf{A} \in \mathbb{F}_q^{m\times m}, \mathbf{B} \in \mathbb{F}_q^{n\times n}$, such that $\mathcal{C}_1 = \mathbf{A} \cdot \mathcal{C}_0 \cdot \mathbf{B}$.

- The map induced by $(\mathbf{A}, \mathbf{B})$ is called an **isometry** between the codes.
- The first version of specification shows parameter sets with $m = n = k$.

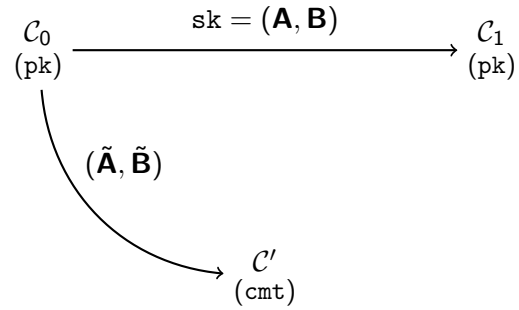
The MEDS Σ-protocol and signature scheme

$\mathcal{C}_0$
$(\mathtt{pk})$

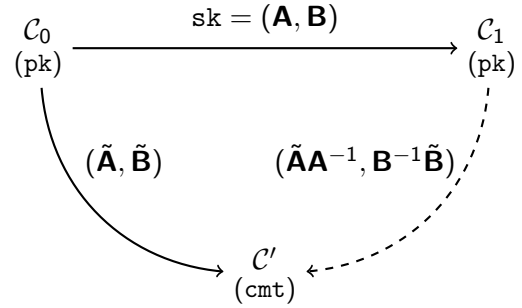
The MEDS Σ-protocol and signature scheme



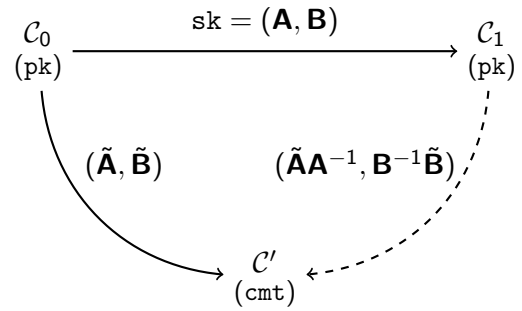
The MEDS Σ-protocol and signature scheme



The MEDS Σ-protocol and signature scheme

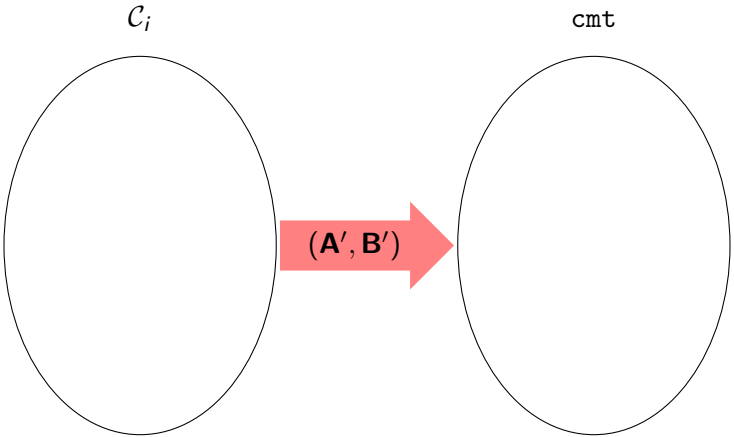


The MEDS Σ-protocol and signature scheme

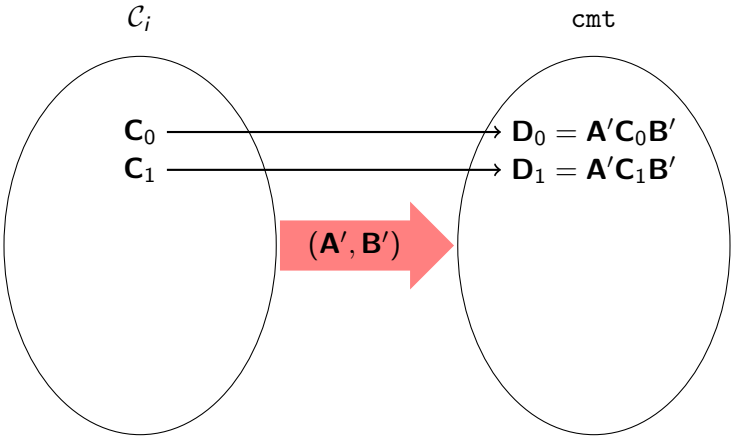


- Verification: apply $\mathtt{rsp}$ to $\mathcal{C}_{\mathtt{ch}}$, compare with $\mathtt{cmt}$.
- FS transform is applied to obtain the MEDS signature scheme.
- $\mathtt{rsp}$ takes $m^2 + n^2$ field elements to represent.

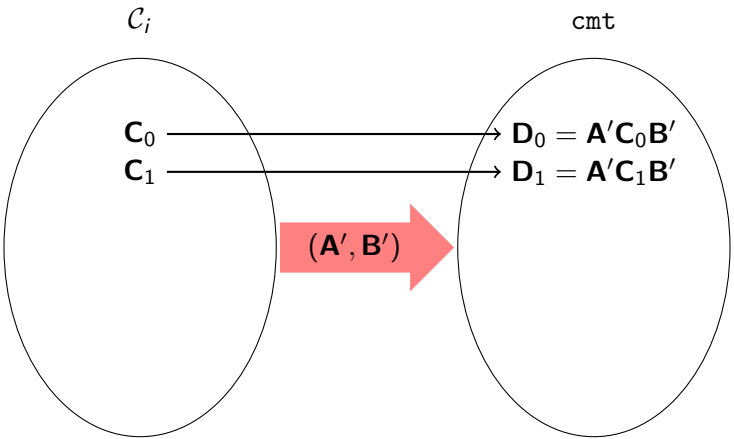
Main idea for MEDS



Main idea for MEDS

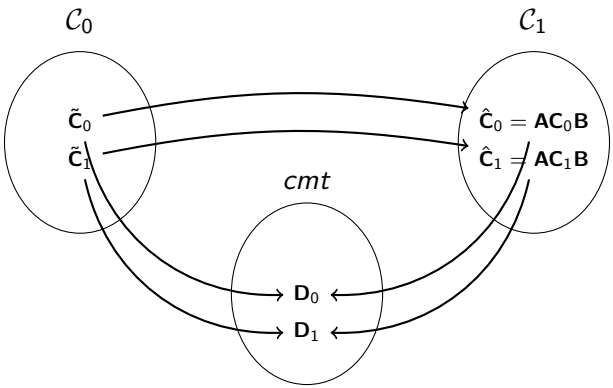


Main idea for MEDS

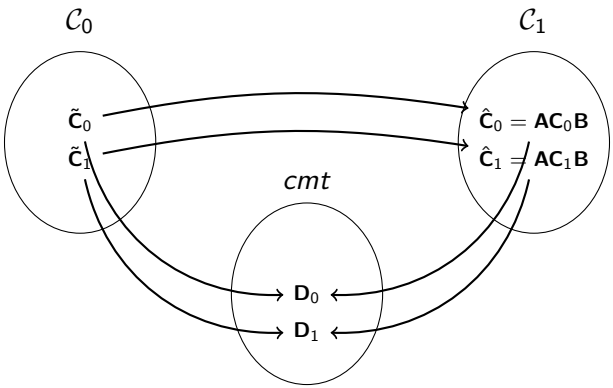


- What if we represent $(\mathbf{A}', \mathbf{B}')$ as $(\mathbf{C}_0, \mathbf{C}_1, \mathbf{D}_0, \mathbf{D}_1)$?

New Σ-protocol for MEDS ($|m - n| \leq 1$)



New Σ-protocol for MEDS ($|m - n| \leq 1$)



- $(\mathbf{C}_0, \mathbf{C}_1)$ takes $2k$ coordinates to represent.
- $(\mathbf{D}_0, \mathbf{D}_1)$ can be considered as public data.

Solving for $\tilde{\mathbf{A}}, \tilde{\mathbf{B}}$

- Want to find $\mathbf{A}, \mathbf{B}$ such that

$$\begin{aligned}\mathbf{D}_0 &= \mathbf{A} \cdot \mathbf{C}_0 \cdot \mathbf{B} \\ \mathbf{D}_1 &= \mathbf{A} \cdot \mathbf{C}_1 \cdot \mathbf{B}.\end{aligned}$$

- We solve the linear system ($m^2 + n^2$ variables, $2mn$ equations.) resulted from

$$\begin{aligned}\mathbf{D}_0 \cdot \mathbf{B}^{-1} &= \mathbf{A} \cdot \mathbf{C}_0 \\ \mathbf{D}_1 \cdot \mathbf{B}^{-1} &= \mathbf{A} \cdot \mathbf{C}_1.\end{aligned}$$

Solving for $\tilde{\mathbf{A}}, \tilde{\mathbf{B}}$

- Want to find $\mathbf{A}, \mathbf{B}$ such that

$$\mathbf{D}_0 = \mathbf{A} \cdot \mathbf{C}_0 \cdot \mathbf{B}$$
$$\mathbf{D}_1 = \mathbf{A} \cdot \mathbf{C}_1 \cdot \mathbf{B}.$$

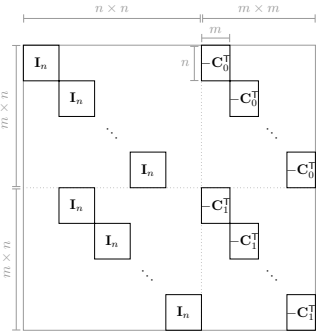
- We solve the linear system ($m^2 + n^2$ variables, $2mn$ equations.) resulted from

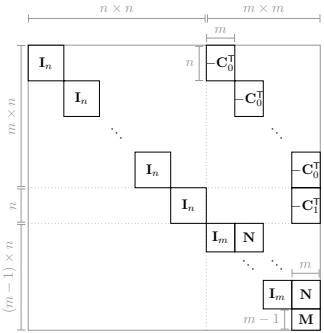
$$\mathbf{D}_0 \cdot \mathbf{B}^{-1} = \mathbf{A} \cdot \mathbf{C}_0$$
$$\mathbf{D}_1 \cdot \mathbf{B}^{-1} = \mathbf{A} \cdot \mathbf{C}_1.$$

- When $m = n$, $\#\text{eq} = \#\text{var}$, leading to $\mathbf{A} = \mathbf{B}^{-1} = 0$.
- When $|m - n| = 1$, $\#\text{var} - \#\text{eq} = 1$, leading to solutions $(\alpha\mathbf{A}, \alpha^{-1}\mathbf{B})$.
- Otherwise, $\#\text{var} - \#\text{eq} > 1$, leading to too many degrees of freedom.

A specific choice for $\mathbf{D}_0, \mathbf{D}_1$

- Let's try $n = m + 1$ and $\mathbf{D}_0 = (\mathbf{I}_m\ 0) \in \mathbb{F}_q^{m \times n}$, $\mathbf{D}_1 = (0\ \mathbf{I}_m) \in \mathbb{F}_q^{m \times n}$.





- Reducing the system boils down to reducing $\mathbf{M}$, which takes $O(n^3)$ field operations.
- Reducing the generator matrix of `cmt` takes $O(n^4)$ field operations.

Old and new parameter sets for MEDS

category	q	n	m	k	s	t	w	pk (bytes)	sig (bytes)
$<$ I	4093	14	14	14	4	1152	14	9923	9896
$\geq$ I		26	25	25	2	144	48	21595	5200
$<$ III	4093	22	22	22	4	608	26	41711	41080
$\geq$ III		35	34	34	2	208	75	55520	10906
$<$ V	2039	30	30	30	5	192	52	134180	132528
$\geq$ V	4093	45	44	44	2	272	103	122000	19068

- The attack from Eurocrypt 2024 is considered.

Application to ALTEQ

category	n	α	C	r	K	pk (bytes)	sig (bytes)
I	13		458	16	14	523968	9528
	13	6	657	29	11	512476	3752
III	20		229	39	20	1044264	32504
	20	7	297	69	17	1045464	10816
V	25		227	67	25	2088432	63908
	25	8	276	88	23	2070032	20544

- For MEDS, isometries are represented as code words.
- For ALTEQ, isometries are represented as **partial** code words.

https://ia.cr/2024/495