Bi-braces and connections to private-key cryptography

Roberto Civino
University of L'Aquila

joint work with V. Fedele & N. Gavioli

Advances in Group Theory and Applications 2023 - Lecce

5th June 2023

The setting

- $\mathbb{F}_2$ be the field with two elements,
- $V = \mathbb{F}_2^n$ be the vector space of dimension n over $\mathbb{F}_2$,
- $T_+ < \mathrm{Sym}\, V$ be the group of translations of $(V, +)$.

Bi-braces

There is a one-to-one correspondence between

conjugacy classes under $GL(V)$ of elementary abelian regular subgroups of $AGL(V)$ which are normalised by T_+

isomorphism classes of commutative radical algebras $(V, +, \cdot)$ with $V^3 = 0$

isomorphism classes of commutative $\mathbb{F}_2$-braces $(V, +, \circ)$ such that $(V, \circ, +)$ is an $\mathbb{F}_2$-brace, that we call a **binary bi-braces**

[CDVS06, Chi19, Car20]

The socle

Recalling $u \cdot v = u + v + u \circ v$:

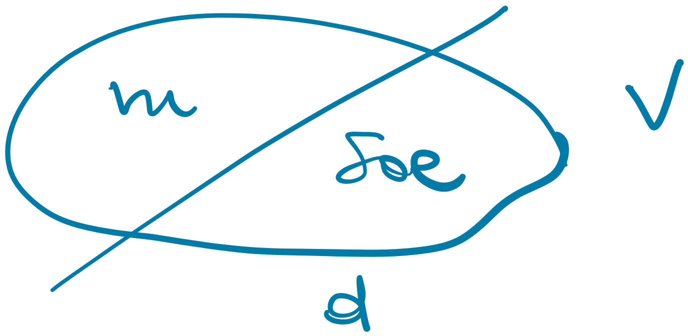
- $\operatorname{Soc}(V) = \{u \in V \mid \forall\ v \in V \quad u + v = u \circ v\}$,

  $\parallel$
- $\operatorname{Ann}(V) = \{u \in V \mid \forall\ v \in V \quad u \cdot v = 0\}$.

It is known that $\dim \operatorname{Soc}(V) \geqslant 1$ as $\mathbb{F}_2$-vector space [CDVS06]. Clearly bi-braces with socles of distinct dimension are not isomorphic.

Another representation

Assume that $d = \dim \operatorname{Soc}(V)$ and $m = n - d$.



Another representation

Assume that $d = \dim \operatorname{Soc}(V)$ and $m = n - d$.

We show that there exist

- a suitable subset $\Lambda(m, 2^d)$ of $m \times m$ alternating matrices over $\mathbb{F}_{2^d}$,
- an equivalence relation $\sim$ over $\Lambda(m, 2^d)$

such that

$\sim$ **equivalence classes** are in one-to-one correspondence with
isomorphism classes of binary bi-braces

[CFG23]

A ‘canonical’ socle

Let $(V, +, \circ)$ be a binary bi-brace with $d = \dim \mathrm{Soc}(V)$. Then

- $(V, \circ)$ is an $\mathbb{F}_2$-vector space;
- $\mathcal{B} = \{b_1, \ldots, b_n\}$ is a basis of $(V, +)$ if and only if $\mathcal{B}$ is a basis of $(V, \circ)$.

Let $\{e_1, \ldots, e_n\}$ be the canonical basis of $(V, +)$ and from now on let us assume that $Soc(V) = \langle e_{m+1}, \ldots, e_n \rangle$.

Introducing a brace-related alternating matrix

Since $u \cdot v = 0$ for each $v \in \mathrm{Soc}(V)$, under the assumption

$$V \cdot V \leq Soc(V) = \langle e_{m+1}, \ldots, e_n \rangle$$

Introducing a brace-related alternating matrix

Since $u \cdot v = 0$ for each $v \in \mathrm{Soc}(V)$, under the assumption

$$V \cdot V \leq Soc(V) = \langle e_{m+1}, \ldots, e_n \rangle$$

a binary bi-brace is determined by the values, for $1 \leq i < j \leq m$, of

$$e_i \cdot e_j = (\underbrace{0, \ldots, 0}_{m \text{ zero's}}, \Theta_{i,j})$$

where $\Theta_{i,j} \in \mathbb{F}_2^d$.

Introducing a brace-related alternating matrix

Since $u \cdot v = 0$ for each $v \in \mathrm{Soc}(V)$, under the assumption

$$V \cdot V \leq Soc(V) = \langle e_{m+1}, \dots, e_n \rangle$$

a binary bi-brace is determined by the values, for $1 \leq i < j \leq m$, of

$$e_i \cdot e_j = (\underbrace{0, \dots, 0}_{m \text{ zero's}}, \Theta_{i,j})$$

where $\Theta_{i,j} \in \mathbb{F}_2^d$.

We call **defining matrix** of $(V, +, \circ)$ the $m \times m$ matrix defined by

$$\Theta = \left[\Theta_{i,j}\right].$$

Representing vectors

Let a be a primitive element of $\mathbb{F}_{2^d}$. Then $\{1, a, \ldots, a^{d-1}\}$ is the canonical basis of $(\mathbb{F}_{2^d}, +)$ as a vector space over $\mathbb{F}_2$. By the following isomorphism of vector spaces

$$\varphi : \mathbb{F}_2^d \longrightarrow \mathbb{F}_{2^d}, \quad e_k \longmapsto a^{k-1} \quad (1 \leq k \leq d)$$

we can think to the defining matrix as

$$\Theta = \left[\Theta_{i,j}\varphi\right] \in {\mathbb{F}_{2^d}}^{m \times m}.$$

Brace from the defining matrix

A matrix $\Theta \in {\mathbb{F}_{2^d}}^{m \times m}$ defines a binary bi-brace if and only if:

[CCS21]

(1) Θ is alternating, i.e., symmetric and zero-diagonal,

Brace from the defining matrix

A matrix $\Theta \in {\mathbb{F}_{2^d}}^{m \times m}$ defines a binary bi-brace if and only if:

[CCS21]

(1) Θ is alternating, i.e., symmetric and zero-diagonal,

(2) for every $u_1, \ldots, u_m \in \mathbb{F}_2$

$$u_1\Theta_1 + \cdots + u_m\Theta_m = 0 \quad \Longrightarrow \quad u_i = 0 \quad \forall\, 1 \leq i \leq m.$$

Brace from the defining matrix

A matrix $\Theta \in {\mathbb{F}_{2^d}}^{m\times m}$ defines a binary bi-brace if and only if:

[CCS21]

(1) Θ is alternating, i.e., symmetric and zero-diagonal,

(2) for every $u_1, \dots, u_m \in \mathbb{F}_2$

$$u_1\Theta_1 + \cdots + u_m\Theta_m = 0 \quad \Longrightarrow \quad u_i = 0 \quad \forall\, 1 \le i \le m.$$

We denote the set of $m \times m$ alternating matrices satisfying (2) by

$$\Lambda(m, 2^d).$$

An equivalence relation on Λ

Theorem (C.F.G.)

Let $(V,+,\circ)$, $(V,+,\hat{\circ})$ *be two binary bi-braces with defining matrices* Θ, $\widehat{\Theta} \in \Lambda(m, 2^d)$. *They are isomorphic if and only if there exist* $A \in GL(m,2)$, $D \in GL(d,2)$ *such that*

$$A\left[\Theta_{i,j}\varphi\right]A^T = \left[\widehat{\Theta}_{i,j}D\varphi\right]$$

An equivalence relation on Λ

Theorem (C.F.G.)

Let $(V, +, \circ)$, $(V, +, \hat{\circ})$ *be two binary bi-braces with defining matrices* $\Theta, \widehat{\Theta} \in \Lambda(m, 2^d)$. *They are isomorphic if and only if there exist* $A \in GL(m, 2)$, $D \in GL(d, 2)$ *such that*

$$A \left[\Theta_{i,j}\right] A^T = \left[\widehat{\Theta}_{i,j} D\right]$$

An equivalence relation on Λ

Theorem (C.F.G.)

Let $(V,+,\circ)$, $(V,+,\hat{\circ})$ be two binary bi-braces with defining matrices Θ, $\widehat{\Theta} \in \Lambda(m, 2^d)$. They are isomorphic if and only if there exist $A \in GL(m,2)$, $D \in GL(d,2)$ such that

$$A\left[\Theta_{i,j}\varphi\right]A^T = \left[\widehat{\Theta}_{i,j}D\varphi\right]$$

In particular, $M \in \mathrm{Aut}(V,+,\circ)$ if and only if $M = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$ where

$$A \in GL(m,2),\ D \in GL(d,2),\ B \in \mathbb{F}_2^{m\times d}$$

and

$$A\left[\Theta_{i,j}\varphi\right]A^T = \left[\Theta_{i,j}D\varphi\right].$$

An example

$$\Theta = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & a & 0 \\ 0 & a & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \sim \quad \widehat{\Theta} = \begin{bmatrix} 0 & 0 & 1+a & 0 \\ 0 & 0 & 0 & 1 \\ 1+a & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$(1,0) \equiv 1$

$(0,1) \equiv a$

An example

$(1,0) \equiv 1$

$(0,1) \equiv a$

$$\Theta = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & a & 0 \\ 0 & a & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \sim \quad \widehat{\Theta} = \begin{bmatrix} 0 & 0 & 1+a & 0 \\ 0 & 0 & 0 & 1 \\ 1+a & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad D = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

$$\left[\widehat{\Theta}_{i,j} D\varphi\right] = \begin{bmatrix} 0 & 0 & (1,1)D\varphi & 0 \\ 0 & 0 & 0 & (1,0)D\varphi \\ (1,1)D\varphi & 0 & 0 & 0 \\ 0 & (1,0)D\varphi & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & a \\ 1 & 0 & 0 & 0 \\ 0 & a & 0 & 0 \end{bmatrix} = A\Theta A^T.$$

When condition (2) looks better

A cryptographically relevant case occurs when the subspace

$$V^2 = V \cdot V = \langle\, u \cdot v : \ u, v \in V \,\rangle_+ \subseteq \mathrm{Soc}(V)$$

is **uni-dimensional**,

$$x \circ y = x + y + \underbrace{x \cdot y}_{\in V^2}$$

When condition (2) looks better

A cryptographically relevant case occurs when the subspace

$$V^2 = V \cdot V = \langle\ u \cdot v :\ \ u, v \in V\ \rangle_+ \subseteq \mathrm{Soc}(V)$$

is **uni-dimensional**, i.e., there exists a vector $b \in V$ such that

$$V \cdot V = \{0, b\}\ \simeq\ \mathbb{F}_2.$$

When condition (2) looks better

A cryptographically relevant case occurs when the subspace

$$V^2 = V \cdot V = \langle\ u \cdot v :\ \ u, v \in V\ \rangle_+ \subseteq \mathrm{Soc}(V)$$

is **uni-dimensional**, i.e., there exists a vector $b \in V$ such that

$$V \cdot V = \{0, b\}\ \simeq\ \mathbb{F}_2.$$

In particular for each $1 \leq i < j \leq m$

$$(0, \ldots, 0, \Theta_{i,j}) \in \{0, b\}$$

and so the defining matrix Θ is an **invertible alternating matrix** over $\mathbb{F}_2$.

Uni-dimensional V^2

- $(V, +, \cdot)$ such that $V \cdot V = \langle b \rangle$ with defining matrix Θ
- $(V, +, \widehat{\cdot})$ such that $V \widehat{\cdot} V = \langle \widehat{b} \rangle$ with defining matrix $\widehat{\Theta}$

$$A \left[\Theta_{i,j} \varphi \right] A^T = \left[\widehat{\Theta}_{i,j} D \varphi \right] \quad \Longleftrightarrow \quad \begin{cases} A \Theta A^T = \widehat{\Theta} \\ \\ b = \widehat{b} D \end{cases}$$

Uni-dimensional V^2

It is well known that alternating matrices of the same rank are congruent, i.e. $\Theta = A\widehat{\Theta}A^T$ for some $A \in GL(m, 2)$. For this reason:

Theorem (C.F.G.)

There is a unique isomorphism class of n-dimensional binary bi-braces with d-dimensional socle and uni-dimensional V^2

$m = 2$ is easily classified

Notice that when socle co-dimension is $m = 2$, then $V^2 = \{0, e_1 \cdot e_2\}$, i.e. $\dim V^2 = 1$.

So there exists a unique isomorphism class of binary bi-braces with socle co-dimension $m = 2$.

$m = 3$ is still easy

Theorem (C.F.G.)

Let $(V, +, \circ)$, $(V, +, \hat{\circ})$ *be two binary bi-braces, both with socle co-dimension* $m = 3$. *Then they are isomorphic if and only if*

$$\dim V \cdot V = \dim V \hat{\cdot} V$$

In particular there are two isomorphism classes of binary bi-braces with socle co-dimension $m = 3$ and socle dimension $d \geq 3$. The representative matrices are

$$\begin{bmatrix} 0 & 1 & a \\ 1 & 0 & a^2 \\ a & a^2 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & a \\ 1 & 0 & 0 \\ a & 0 & 0 \end{bmatrix}.$$

For $d = 2$ and $m = 3$ the isomorphism class is unique because $\dim V^2 = 2$.

Troubles start with $m = 4$

The previous result is not true for $m \geqslant 4$. Indeed the representative matrices for the isomorphism classes when $d = 2$ and $m = 4$ are:

$$\dim V^2 = 1 \quad \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

$$\dim V^2 = 2 \quad \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & a \\ 1 & 0 & 0 & 0 \\ 0 & a & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & a \\ 0 & 0 & 1+a & 1 \\ 1 & 1+a & 0 & 0 \\ a & 1 & 0 & 0 \end{bmatrix}.$$

Classification results up(-ish) to $n = 8$

n	m	d	# classes	# operations $\circ$
*	2	$\geqslant 1$	1	
*	3	$\geqslant 3$	2	
5	3	2	1	42
5	4	1	1	28
6	4	2	4	3360
7	4	3	9	254968
7	5	2	2	937440
7	6	1	1	13888
8	4	4	13	16716840

Classification results up(-ish) to $n = 8$

n	m	d	# classes	# operations $\circ$
*	2	$\geqslant 1$	1	
*	3	$\geqslant 3$	2	
5	3	2	1	42
5	4	1	1	28
6	4	2	4	3360
7	4	3	9	254968
7	5	2	2	937440
7	6	1	1	13888
8	4	4	13	16716840
8	5	3	🤯	🤯
8	6	2		

¿Questions?

Bibliography

A. Caranti.
Bi-skew braces and regular subgroups of the holomorph.
Journal of Algebra, 562:647–665, 2020.

M. Calderini, R. Civino, and M. Sala.
On properties of translation groups in the affine general linear group with applications to cryptography.
J. Algebra, 569:658–680, 2021.

A. Caranti, F. Dalla Volta, and M. Sala.
Abelian regular subgroups of the affine group and radical rings.
Publ. Math. Debrecen, 69(3):297–308, 2006.

R. Civino, V. Fedele, and N. Gavioli.
Classification of binary bi-braces.
Work in progress, 2023.

L. N Childs.
Bi-skew braces and Hopf Galois structures.
New York J. Math, 25:574–588, 2019.