Defeating an Active Adversary Using Difference Families in Groups

Lily Rhodes

Supervisor: Dr Sophie Huczynska
School of Mathematics and Statistics

University of St Andrews

LAIDLAW SCHOLARS

Aims

The main aims of this project were to:

- Compare examples of **GSEDFs** found by computer search with known constructions
- Investigate new constructions for **GSEDFs**

Background

Algebraic manipulation detection (AMD) codes are often described as a game between an encoder and an adversary. We begin with sets of **sources** (messages we want to encode), possible codewords known as **tags**, **keys** and **encoding functions** each related to a **key**. The encoder chooses a secret **key** at random and can then create pairs of **sources** and **tags** using the corresponding **encoding function**. The adversary's job is then to create fake pairs that could pass as a real pair.

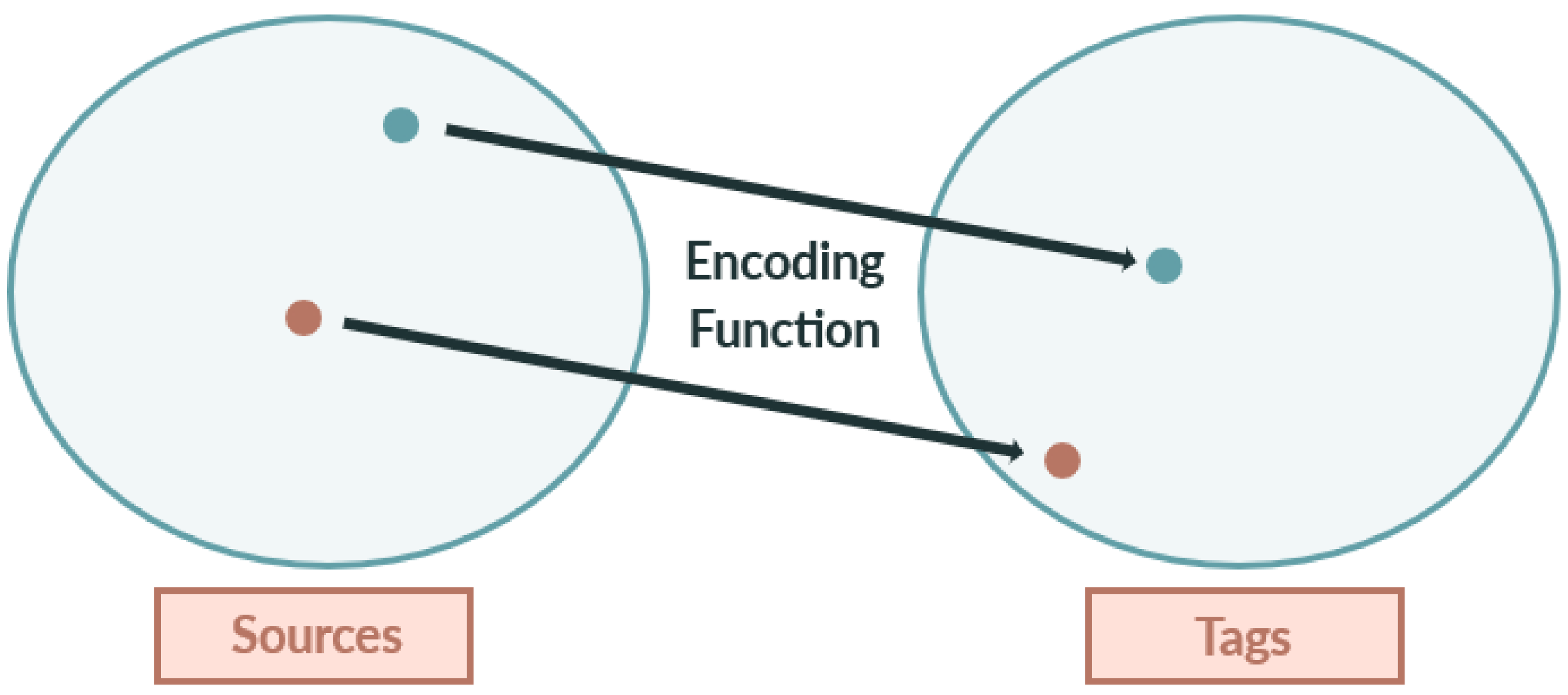

Figure 1. A Visual Representation of an AMD Code

AMD codes create unconditionally secure secret sharing schemes meaning they are unaffected by the adversary's computing power. Therefore, unlike many other cryptographical ideas, they are not at risk from quantum computers.

Difference Sets

A difference set is a subset of a group G such that, if we take the *'difference'* of all the elements ($x - y$ for all **non-equal** x and y in G) each element in G appears λ times apart from 0.

$\{1, 2, 4\}$ is a **difference set** in $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. In Table 1, we subtract the numbers down the left from those on the top. Working in $\mathbb{Z}_7$ means addition and subtraction work as expected, however we must add or subtract 7 in order to stay between 0 and 6.

−	1	2	4
1	0	1	3
2	6	0	2
4	4	5	0

Table 1. A Difference Set

If, repeating the process in Table 1 using multiple sets of the same size, produces λ copies of each **non-zero** element of G, then this is called a **difference family**.

For the family

$$\{\{0, 1\}, \{0, 2\}, \{0, 3\}\}$$

in $\mathbb{Z}_7$. The differences are:

Subset	Differences
$\{0, 1\}$	$\{1, 6\}$
$\{0, 2\}$	$\{2, 5\}$
$\{0, 3\}$	$\{3, 4\}$

$$\Downarrow$$

Every non-zero element of $\mathbb{Z}_7$ appears exactly once.

GSEDFs

This project focused on constructing a syecific type of **difference family** known as a **generalised strong external difference family (GSEDF)**. These can then be used to construct **AMD codes** [3].

GSEDFs consist of multiple subsets that must be **pairwise disjoint**, meaning if we choose any two they must have no elements in common. However, it is not necessary for the subsets to be the same size. If, taking the *difference* between any two of the subsets always gives every **non-zero** element of G a constant number of times, then the subsets form a **GSEDF**.

$\{\{0, 1\}, \{2, 4, 6, 8\}\}$ is a **GSEDF** in $\mathbb{Z}_9$. Each section of Table 2 contains the **non-zero** elements of $\mathbb{Z}_9$ exactly once.

−	0	1	2	4	6	8
0			2	4	6	8
1			1	3	5	7
2	7	8				
4	5	6				
6	3	4				
8	1	2				

Table 2. A Generalised Strong External Difference Family

A Review of Constructions

The main ways to construct **GSEDFs** are:

- **Near Factorisations**: A λ-fold **near factorisation** is two subsets of a group that, when added together, form λ copies of the group excluding zero.
- **Recursive formulas**: Taking two smaller **GSEDFs** to construct another. [2]
- **Difference Sets**: Splitting a group into **difference sets** will produce a **GSEDF**. [3]
- **Cyclotomic Classes**: **Cyclotomic classes** arise from splitting a group into e classes consisting of a subgroup and its **cosets** (certain shifts of the subgroup). For certain values of e, these classes form **difference sets** from which create **GSEDFs**.

A New Construction

Pêcher presents a way to convert a **near factorisation** from the **direct product** $\mathbb{Z}_n \times \mathbb{Z}_2$ to the **semi-direct product** $\mathbb{Z}_n \rtimes \mathbb{Z}_2$ [4]. We have adapted this for direct/semi-direct products with $\mathbb{Z}_3$.

For certain near factorisations in the direct product $\mathbb{Z}_n \times \mathbb{Z}_3$, we can construct a near factorisation in the semidirect product $\mathbb{Z}_n \rtimes \mathbb{Z}_3$.

Further Research

- Extending this new construction semidirect products $\mathbb{Z}_n \rtimes \mathbb{Z}_i$ for $i > 2$.
- Investigating when partitioning a group into difference sets is possible.
- GSEDFs with more than two subsets
- Considering two non-equivalent GSEDFs with the same parameters.

References

[1] Donald L. Kreher, Shuxing Li, and Douglas R. Stinson. λ-fold near-factorizations of groups. *Des. Codes Cryptogr.*, 94(5):Paper No. 106, 34, 2026.

[2] Xiaojuan Lu, Xiaolei Niu, and Haitao Cao. Some results on generalized strong external difference families. *Des. Codes Cryptogr.*, 86(12):2857–2868, 2018.

[3] Maura B. Paterson and Douglas R. Stinson. Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families. *Discrete Math.*, 339(12):2891–2906, 2016.

[4] Arnaud Pêcher. Cayley partitionable graphs and near-factorizations of finite groups. volume 276, pages 295–311. 2004. 6th International Conference on Graph Theory.

I thank Lord Laidlaw and the Laidlaw Foundation for their funding and support. It has been a fantastic experience.

 lmr33@st-andrews.ac.uk