Creative ways of applying combinatorics to cryptography

Laura Johnson

Postdoctoral Research Fellow at the University of Bristol

PiWORKS Seminar Series

25th of November, 2024

In this talk I want to demonstrate that:

- Mathematical journeys are non-linear – you might start off interested in one area and then end up doing something else.
- You don’t have to fit into the perceived mould of what a mathematician “should look like” to succeed.

My mathematical journey

The basics of cryptography

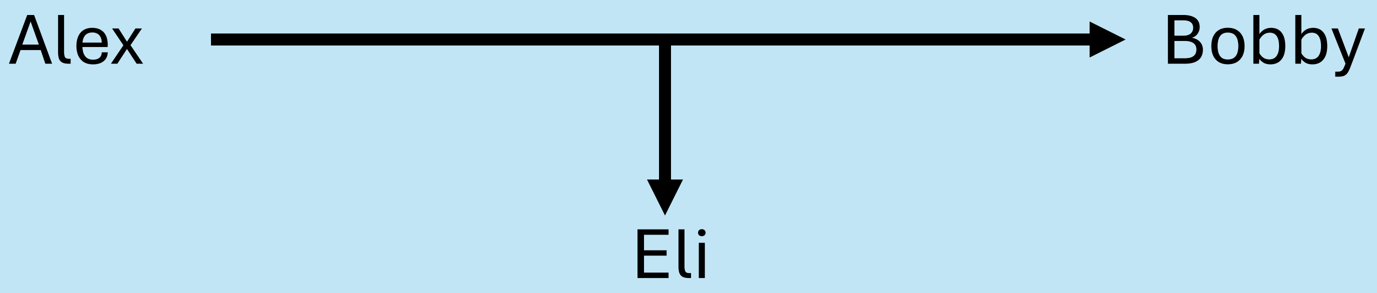
Cryptography is the science of ensuring that secret information stays secret in the presence of an adversary.

Here an **adversary** is someone who wishes to infer with the communications between two other parties; this could be through eavesdropping, corrupting information, pretending to be someone else or forcing a system to shutdown.

The **plaintext** message is the original message that one party wishes to send to another. The **ciphertext** message is the secure message that they send to the other party.

Passive adversary model:

Passive adversary = someone who wants to gain access to information that one party is trying to send to another party.



An early example of a ciphersystem

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Plaintext message: “The quick brown fox”
Ciphertext message: “Xli uymgo fvsar jsb”

How Eli could crack this cipher

Ciphertext Message: “Xli uymgo fvsar jsb”

Most common letters in English language: E, T, A, O, I

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N

Attempt one plaintext message: “LZW…”

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Alternative attack

Ciphertext Message: “Xli uymgo fvsar jsb”

Most common trinomial: “The”

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Alternative Ciphertext Message: “xliuymgofvsarjsb”

How I ended up looking at Latin square cryptography

- Many modern cryptographical schemes rely on technical elements from number theory.
- I had little coding experience.
- Latin square cryptography project sounded interesting because as part of the project, I was assessing the usefulness of various creative ways of using Latin squares in cryptography.

What is a Latin square?

A **Latin square** is an nxn array comprising of n distinct elements such that each element occurs exactly once in each row and column.

1	2	3
2	3	1
3	1	2

1	2	3
2	1	3
3	1	2

What is a partial Latin square?

A **partial Latin square** is an nxn array comprising of n distinct elements such that each element occurs at most once in each row and column.

1	2	
		1
	1	

1	2	
	1	3

Completable partial Latin squares

A partial Latin square is said to be **completable** if the blank entries of the Latin square can be filled to produce a Latin square.

1	2	
		1
	1	

1	2	
	1	3

Completable partial Latin squares

A partial Latin square is said to be **completable** if the blank entries of the Latin square can be filled to produce a Latin square.

1	2	3
		1
	1	

1	2	
	1	3

Completable partial Latin squares

A partial Latin square is said to be **completable** if the blank entries of the Latin square can be filled to produce a Latin square.

1	2	3
		1
	1	2

1	2	
	1	3

Completable partial Latin squares

A partial Latin square is said to be **completable** if the blank entries of the Latin square can be filled to produce a Latin square.

1	2	3
		1
3	1	2

1	2	
	1	3

Completable partial Latin squares

A partial Latin square is said to be **completable** if the blank entries of the Latin square can be filled to produce a Latin square.

1	2	3
2		1
3	1	2

1	2	
	1	3

Completable partial Latin squares

A partial Latin square is said to be **completable** if the blank entries of the Latin square can be filled to produce a Latin square.

1	2	3
2	3	1
3	1	2

1	2	
	1	3

Completable partial Latin squares

A partial Latin square is said to be **completable** if the blank entries of the Latin square can be filled to produce a Latin square.

1	2	3
2	3	1
3	1	2

1	2	
	1	3
	3	1

Completable partial Latin squares

A partial Latin square is said to be **completable** if the blank entries of the Latin square can be filled to produce a Latin square.

1	2	3
2	3	1
3	1	2

1	2	
	1	3
2	3	1

Uniquely completable partial Latin square

A partial Latin square is said to be **uniquely completable** if there is only Latin square it complete’s to.

1	2	
		1
	1	

1		
		1
	1	

Uniquely completable partial Latin square

A partial Latin square is said to be **uniquely completable** if there is only Latin square it complete's to.

1	2	3
2	3	1
3	1	2

1		
		1
	1	

Uniquely completable partial Latin square

A partial Latin square is said to be **uniquely completable** if there is only Latin square it complete's to.

1	2	3
2	3	1
3	1	2

1	2	3
2	3	1
3	1	2

Uniquely completable partial Latin square

A partial Latin square is said to be **uniquely completable** if there is only Latin square it complete’s to.

1	2	3
2	3	1
3	1	2

1	3	2
3	2	1
2	1	3

Critical sets of Latin squares

A **critical set** of a Latin square is a partial Latin square containing the minimum number of entries required in order for the Latin square to be uniquely completable.

Example: The following Latin square is a critical set.

1	2	
	1	

To see this, we need it's uniquely completable and it's subsquares are not uniquely completable.

Critical sets of Latin squares

A **critical set** of a Latin square is a partial Latin square containing the minimum number of entries required in order for the Latin square to be uniquely completable.

1	2	
	1	

1	2	

1		
	1	

Critical sets of Latin squares

A **critical set** of a Latin square is a partial Latin square containing the minimum number of entries required in order for the Latin square to be uniquely completable.

1	2	3
2	3	1
3	1	2

1	2	

1		
	1	

Critical sets of Latin squares

A **critical set** of a Latin square is a partial Latin square containing the minimum number of entries required in order for the Latin square to be uniquely completable.

1	2	3
2	3	1
3	1	2

1	2	3

1		
	1	

Critical sets of Latin squares

A **critical set** of a Latin square is a partial Latin square containing the minimum number of entries required in order for the Latin square to be uniquely completable.

1	2	3
2	3	1
3	1	2

1	2	3

1		
		1
	1	

Secret sharing schemes

- Secret sharing schemes are examples of authentication schemes.
- A group of t participant need to combine shares to produce the key K.
- Each participant has a share of K.
- There are k participants in the scheme in total.

Secret sharing scheme involving critical sets

Idea: Each participant in the scheme is given a part of a critical set. The participants have to combine their shares and complete the critical set to find the key k.

Participant 1:

1		

Participant 2:

	2	

Participant 3:

	1	

Problems with this secret sharing scheme

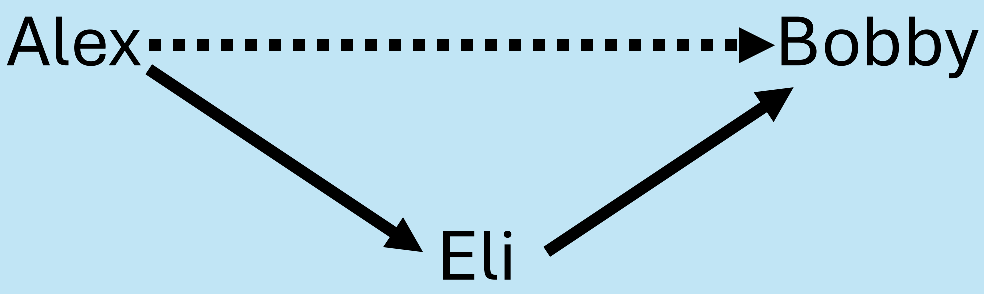
- Once t-1 participants have pooled their shares, it’s not infeesible for them to guess what the Latin square is.
- Identifying critical sets of Latin squares is hard.

How I ended up being a combinatorialist

- I liked the combinatorial/algebraic aspect of my masters project work.
- I wanted to do something with a more practical information security application.

Active adversaries

An **active adversary** is someone who wishes to disrupt communications between two parties by altering the message that one party sends to the other.



The basics of AMD codes:

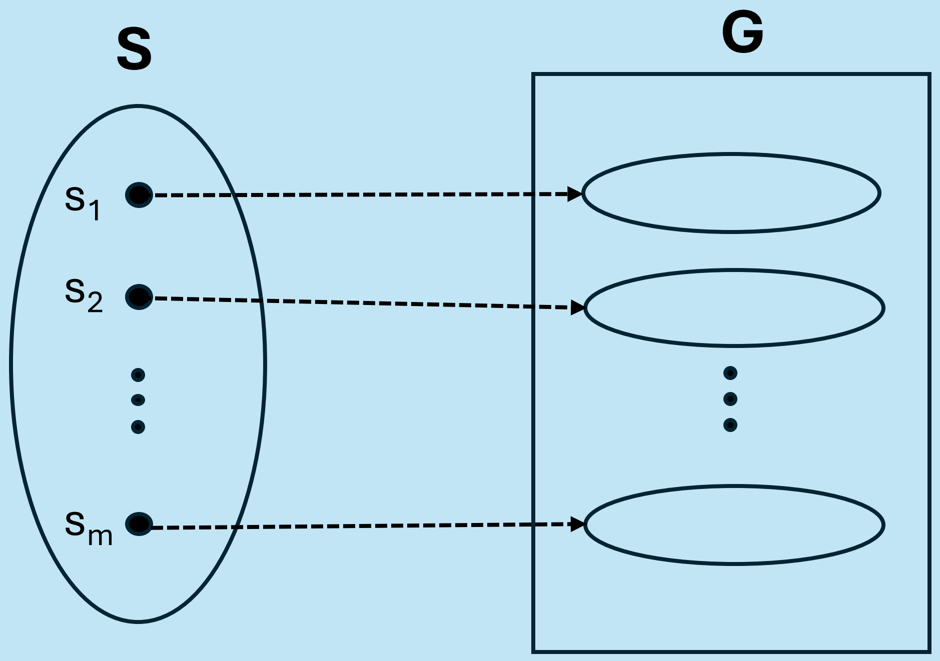
Algebraic manipulation detection (or AMD) codes are a type of cryptographical tool used to protect against attacks from active adversaries.

AMD codes consist of:

- A set of plaintext messages.
- A (usually) randomised encoding function.
- Several collections of tags, which live inside a group G.

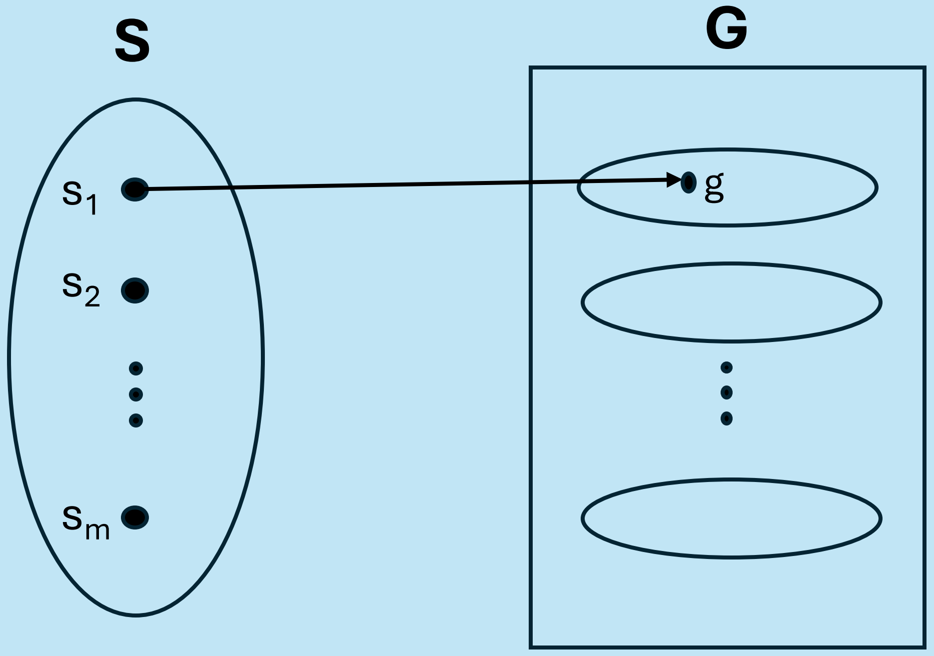
Idea: Each plaintext message has several valid encodings and any one time, the encoding function randomly maps to one valid encoding of a plaintext message.

AMD code model



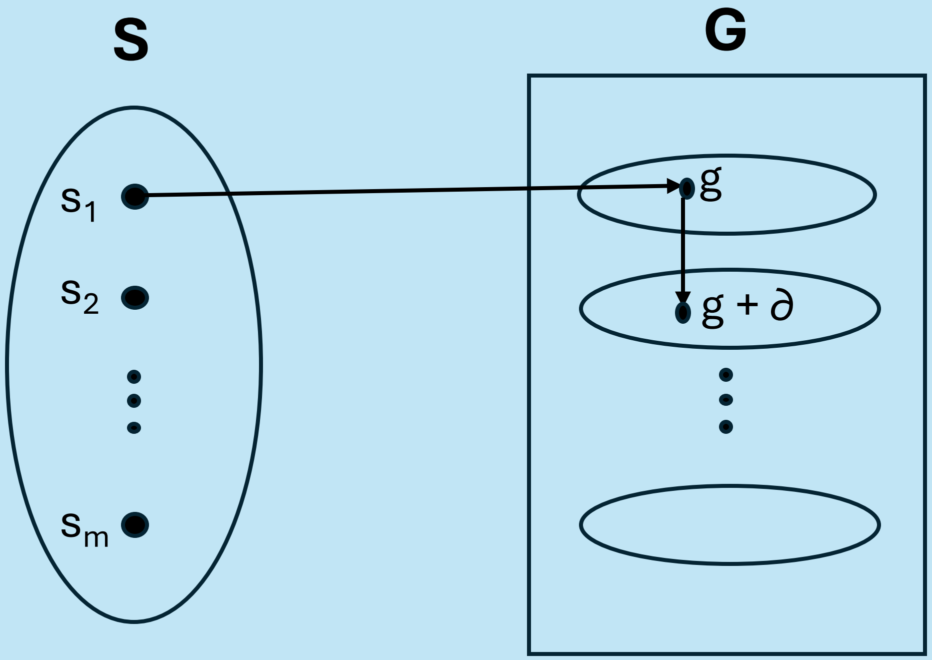
Eli's attack strategy

Suppose Alex tries to send the message s_1 to Bobby

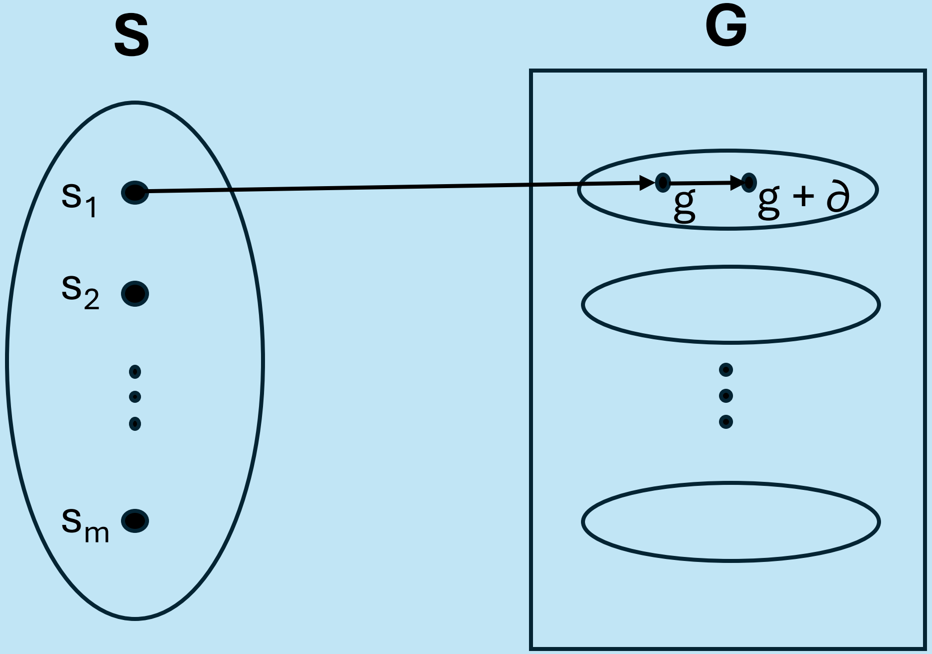


Eli's attack strategy

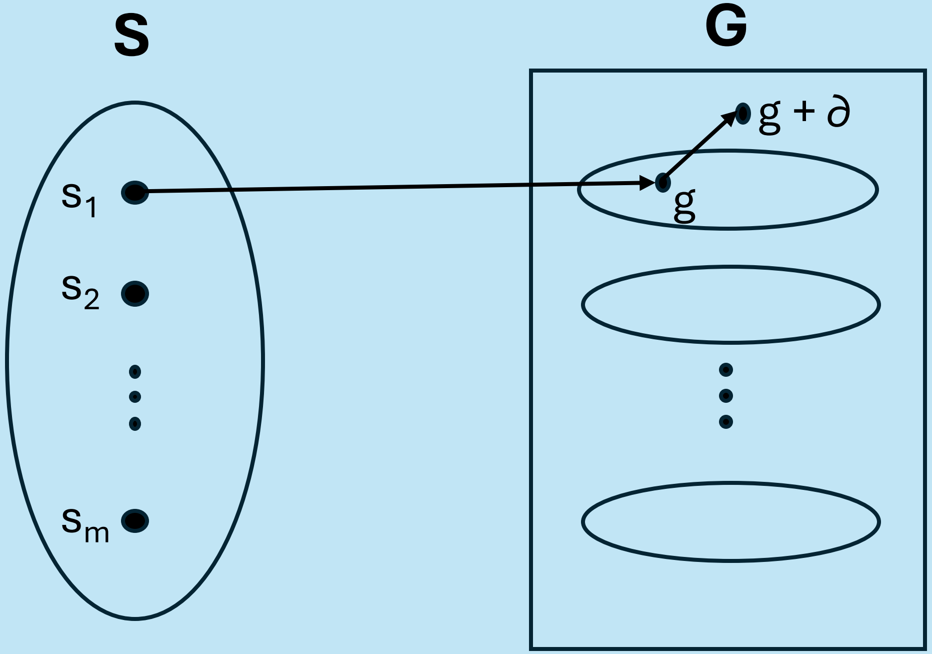
If Eli decided to force a miscommunication between the two, they would Need to pick a manipulation ∂ and add this to g.



The first way Eli's attack can fail



The second way Eli's attack can fail



R-optimal AMD codes

An AMD code is said to be **R-optimal** if every possible manipulation ∂ is equally likely to succeed.

Example: In the group Z_{13} the sets {1,12}, {3,10} and {4,9} can be used to build an R-optimal AMD code. Here each ∂ has a success probability of 1/3.

+	1	12	3	10	4	9
1	2	0	4	11	5	10
2	3	1	5	12	6	11
3	4	2	6	0	7	12
4	5	3	7	1	8	0
5	6	4	8	2	9	1
6	7	5	9	3	10	2

+	1	12	3	10	4	9
7	8	6	10	4	11	3
8	9	7	11	5	12	4
9	10	8	12	6	0	5
10	11	9	0	7	1	6
11	12	10	1	8	2	7
12	0	11	2	9	3	8

Why do we want R-optimality?

Suppose we are in Z_{13} again, but this time we pick the sets {1,3,9} and {4,10,12} as our sets of tags.

+	1	3	9	4	10	12
1	2	4	10	5	11	0
3	4	6	12	7	0	2
9	10	12	5	0	6	8
4	5	7	0	8	1	3
10	11	0	6	1	7	9
12	0	2	8	3	9	11

+	1	3	9	4	10	12
2	3	5	11	6	12	1
5	6	8	1	9	2	4
6	7	9	2	10	3	5
7	8	10	3	11	4	6
8	9	11	4	12	5	7
11	12	1	7	2	8	10

How do we ensure optimality?

An **external difference family (or EDF)** is a collection of subsets of group G such that each non-zero of G occurs precisely λ as a pairwise difference between elements of distinct subsets.

Example: We will look again at our original example in Z_{13}.

-	1	12	3	10	4	9
1			11	4	10	5
12			9	2	8	3
3	2	4			12	7
10	9	11			6	1
4	3	5	1	7		
9	8	10	6	12		

Notice that 1-3 = 11, this implies that 3+11 = 1.

My maths now:

- I’m still looking at EDF constructions in both groups and finite fields.
- I look now look at finite field cyclotomy (relating the additive and multiplicative structures of fields).
- I look at how derangements of arithmetic progressions can be used to tackle problems in number theory.
- I have been looking at topological embeddings of cyclic graphs onto surfaces.

My route into academia

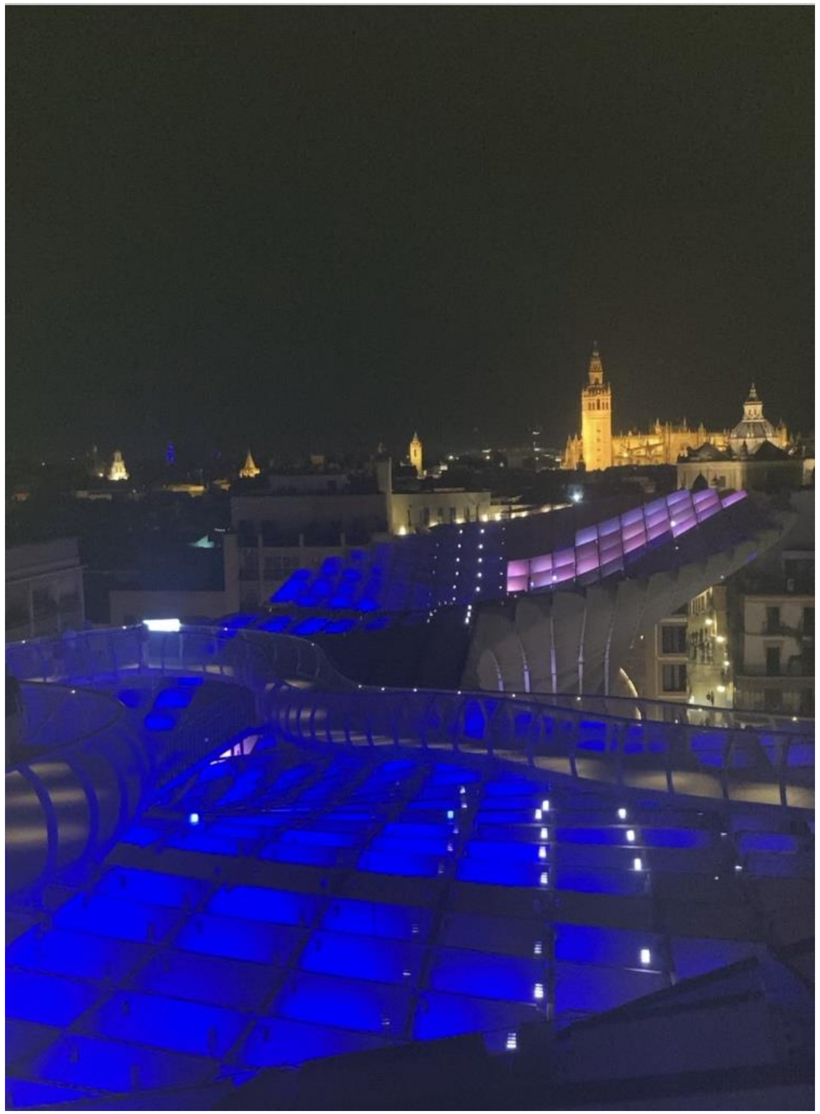
School:

- I did okay at school but never got astounding grades.
- Struggled to get homework done.
- Teachers thought I didn’t particularly like maths.
- Things improved in sixth form because I started studying more and got more attention from teachers.

University of South Wales

The University of South Wales

My year out:

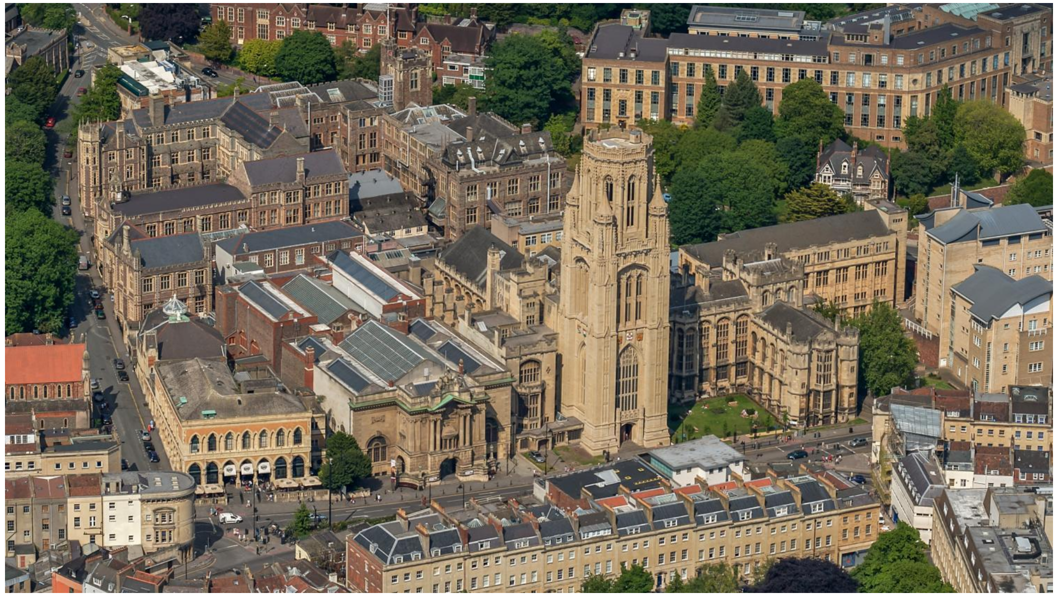


University of St Andrews

My PhD

Ways I made money during my PhD

- Took on as much teaching as possible.
- For petty cash/vouchers, I participated in university wide surveys.
- Did some consultancy work for my former employer.
- Worked on the University of St. Andrews STEP programme.
- Helped run a session at the Golf Museum in St. Andrews.
- Worked as a part-time administrator for the “History for Diversity in Mathematics” Network.



Now

Advice I would give to prospective PhDs (particularly those with ADHD/dyslexia/anxiety etc.)

- Make sure you pick an understanding supervisor.
- Don’t rule yourself out of academia because you don’t think you fit the mould
- Just do what you enjoy and see where it takes you!
- Self-funding is hard but not impossible. If you chose this route make sure you have a plan.
- Use organisations like PiScopia to build a support network.
- Take any opportunities to travel; experience of independent research and having international collaborators can be very helpful

Thank you for listening!