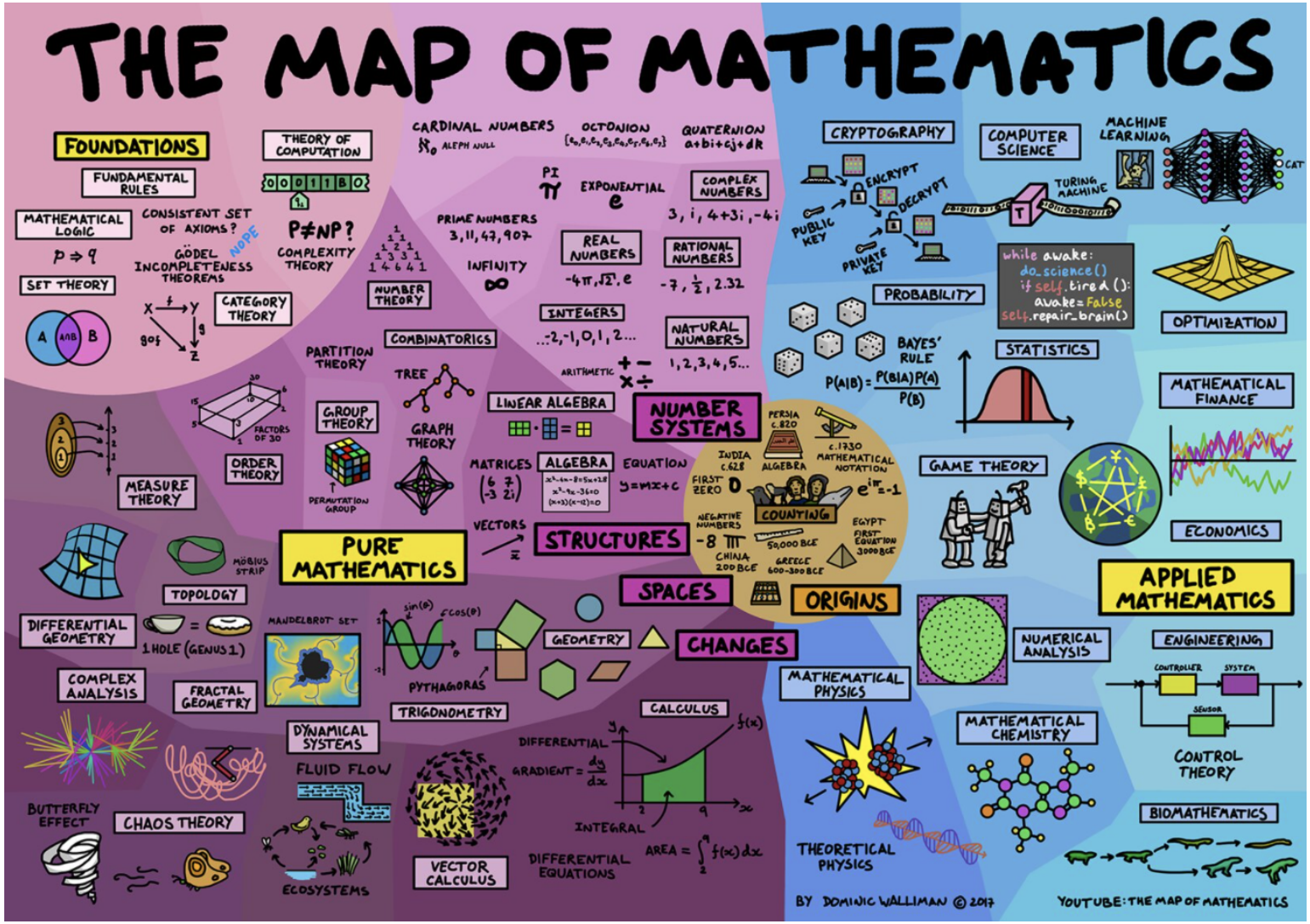
CS4236 Cryptography Theory and Practice Assignment 4

Hugh Anderson

National University of Singapore
School of Computing

November, 2022

Where are we then?



Outline

Outline

1. **Admin**
   - Special help sessions
   - Presentation and project submission
2. **Assignment 4**
   - Comments on question 1
   - Comments on question 2
   - Comments on question 3
   - Comments on questions 4 and 5

Outline

Special help sessions on Saturdays

Or extra tutorial, or open house, or town square, or ...

On Saturdays, from 2:00 to 3:00, I run a zoom session from my home. You can join at any time, and just yell out or something (I will leave the machine running in the living room, and try to keep an eye on it).

If you have any questions, come and talk to me via zoom on Saturday:

URL: `https://nus-sg.zoom.us/j/82466546798?pwd=Z1FXZnF6OWdCQnJNeFAyTDEzKzFkZz09`

Meeting ID: 824 6654 6798

Passcode: 182428

Outline

Project due on 9th November - extension to 11th!

One week from now... plus a few days

Your project is submitted as a paper, and a short conference style video presentation, and the due date is extended to Friday 11th evening.

For your presentation, there is no requirement for you to all present. If you wish to all present, then do so. If just one of you presents, then one of you presents. If you decide to let an automaton narrate your project, feel free.

If you use presentation slides, then you should send these to me as well.

Outline

Question 1

Comment...

The original question suggested you work out a particular $\Delta_{in}, \Delta_{out}$ pair:

1. (Differential) Assume the SPN given in the slides (Session9, and graphic given on the next page). Find a trail which significantly affects some of the least-significant 8-bits of the output: perhaps $\Delta_{in} = 0001000000010000$ and $\Delta_{out} = 0000000010110000$ (have I worked that out correctly?).
   (a) Show the complete trail on the SPN diagram. (2 marks)
   (b) Calculate $\Pr[\langle \Delta_{in}, \Delta_{out} \rangle]$. Show and explain your working. (2 marks)

If you have worked out a reasonable trail and probability from that, then that is OK - do not bother re-working. However, for various reasons it is not a good example for use in differential cryptanalysis. Instead - I have provided a better pair:

1. (Differential) Assume the SPN given in the slides (Session9, and graphic given on the next page). Find a trail which significantly affects some of the least-significant 8-bits of the output: perhaps $\Delta_{in} = 1100\ 0000\ 0000\ 0000$ and $\Delta_{out} = 0000\ 0000\ 0100\ 0100$ (have I worked that out correctly this time?).
   (a) Show the complete trail on the SPN diagram. (2 marks)
   (b) Calculate $\Pr[\langle \Delta_{in}, \Delta_{out} \rangle]$. Show and explain your working. (2 marks)

It might be useful for you to find out why the first example would not be effective for cryptanalysis.

Outline

Question 2

Comment...

I have not had any questions or feedback about this question.

Outline

Question 3

Comment...

The original question was taken directly from a previous exam, but this year I have changed the ordering of the elements of the keys from $k = \langle \ldots, \mathcal{G}, g \rangle$ to $k = \langle \mathcal{G}, g, \ldots \rangle$ in the lecture slides. The original statement of the question was:

> 3. (Exam) Alice is going to send a message to Bob using ECC *encryption*. Bob has a private/secret key $K_S = \langle 4, E_{31}(1,1), (0,1) \rangle$, and public key $K_P = \langle (22,21), E_{31}(1,1), (0,1) \rangle$. If Alice encoded her message as the point $(4,21)$, and chooses a random value $k = 2$, what message does she send to Bob? Show your working. (4 marks)

The new statement clarifies the keys, and follows the ordering given in this year's notes:

> 3. (Like exam) Alice is going to send a message to Bob using ECC *encryption*. Bob has a private/secret key $K_S = \langle \mathcal{G}, g, x \rangle = \langle E_{31}(1,1), (0,1), 4 \rangle$, and public key $K_P = \langle \mathcal{G}, g, h \rangle = \langle E_{31}(1,1), (0,1), (22,21) \rangle$. If Alice encoded her message as the point $(4,21)$, and chooses a random value $k = 2$, what message does she send to Bob? Show your working. (4 marks)

There is no change to the actual meaning of the question.

Outline

Question 4,5

4. (Exam) Show/prove that there exists a MAC that is secure (existentially unforgeable) but that is not strongly secure.
5. In Session8, and in the textbook in Section 5.6.5, a commitment scheme is described, whereby the sender (Alice) commits to a message m, by sending $c_A = \mathcal{H}(m \| r)$, where $\mathcal{H}$ is a collision resistant hash, $\|$ is string concatenation, and r is a randomly generated string. Prove that this scheme is secure in terms of the Hiding experiment (only).

Comments...

Make it clear you understand the question. Follow the form of proof. State any assumptions you make.