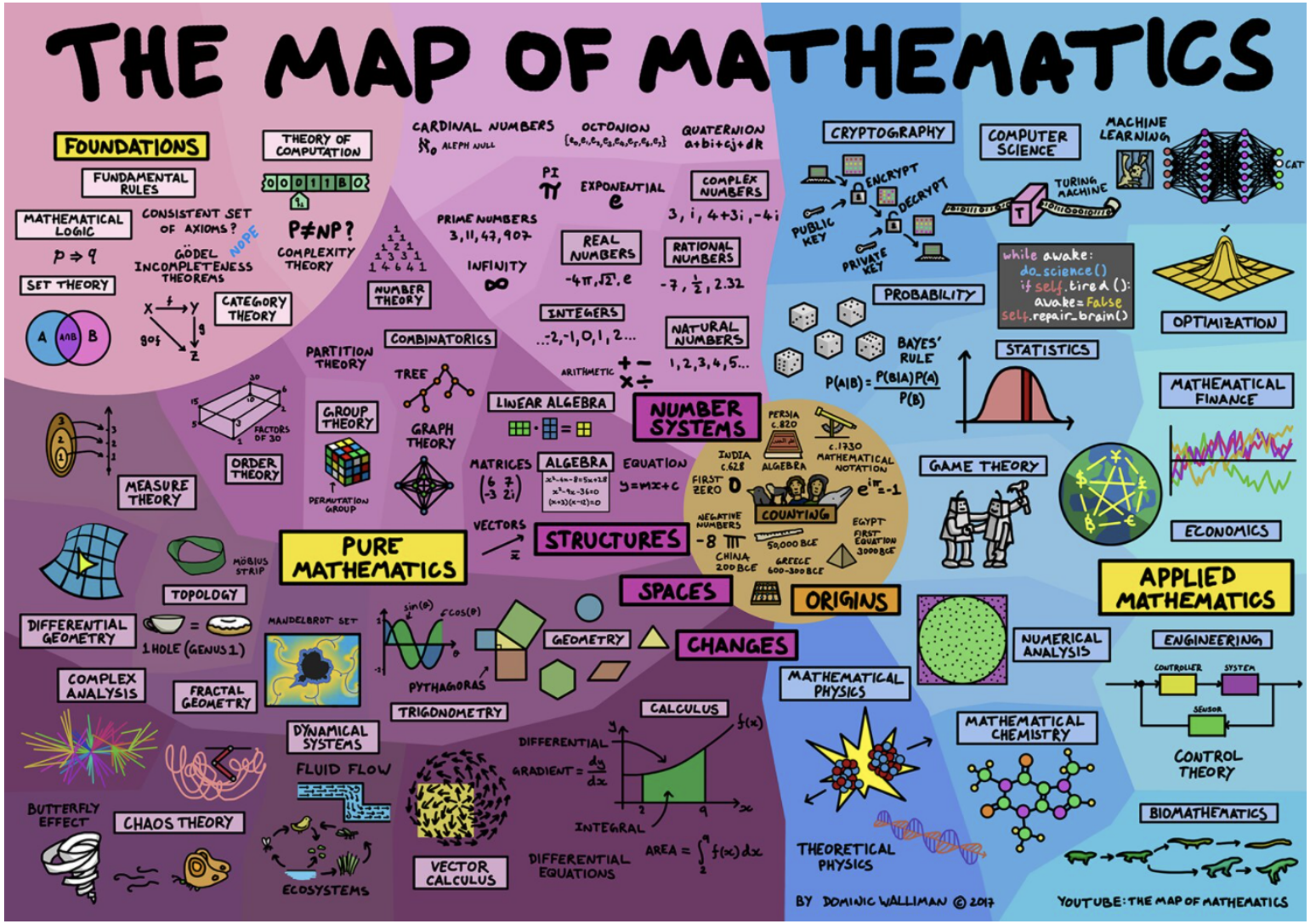
CS4236 Cryptography Theory and Practice Assignment 2

Hugh Anderson

National University of Singapore
School of Computing

September, 2022

Where are we then?



Outline

Outline

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

Question 1

1. Let $G(s) \stackrel{\text{def}}{=} s \oplus \text{rand}()$, where $\text{rand}()$ is a function which returns a truly random bitstring the same size as s, and as usual, $\oplus$ is XOR. Prove or disprove that $G(s)$ is a PRG (a pseudorandom generator).

Comment...

You should remind yourself of the (two-part) definition of a PRG given in Session 3 (Definition 3.14). From the definition, you should be able to establish if $G(s)$ is, or is not, a PRG.

No more clues...

Outline

Question 2

2. Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG. Prove or disprove that the function $G'(s) \stackrel{\text{def}}{=} G(s')$ is also a PRG, where s' is the least significant $n-1$ bits of s.

Comment...

This is a little trickier. Two things have come up - not sure of the relevance of them, but I have had some questions about

- ...what to do with lower-end boundary conditions (for example if $n = 1$, what is $\{0,1\}^1$ when you use the "least significant $n - 1 = 0$ bits of s?). In my view you can just assume, or state that $n \geq 2$.
- ...what is the signature of the PRG - in my view it is still $G' : \{0,1\}^n \to \{0,1\}^{2n}$, although I have sympathy for the argument that it might be considered to be $G' : \{0,1\}^{n-1} \to \{0,1\}^{2n}$. I do not hold with the view that it is $G' : \{0,1\}^{n-1} \to \{0,1\}^{2n-2}$, but my view may change given a good argument. I have doubts about the relevance of the signature.

Outline

Question 3

3. A length preserving function is where the key, the index and the result are all the same size. For example the function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. If $n = 4$, how many different such functions are there?

Comment...

Again I have had "interpretation" style questions about this. In my view, the question clearly asks for how many different functions are there of the type given. It does not discuss $F_k(x)$ as used in PRFs.

Outline

Questions 4&5

4. In the third lecture session, we saw Construction 3.17 which was EAV-Secure (Theorem 3.18, described in class, is the proof). Prove the opposite - i.e. if G is not a PRG, then 3.17 cannot be EAV-secure.

5. Construct a PRG G from a (length preserving) PRF F, and show it is a PRG.

Comment...

Question 4 should just be a proof, along the lines of others we have discussed in class - no further clues sorry.

In Question 5, I expect a construction that meets the two required restraints on a PRG, and a clear outline or proof that the construction is a PRG.