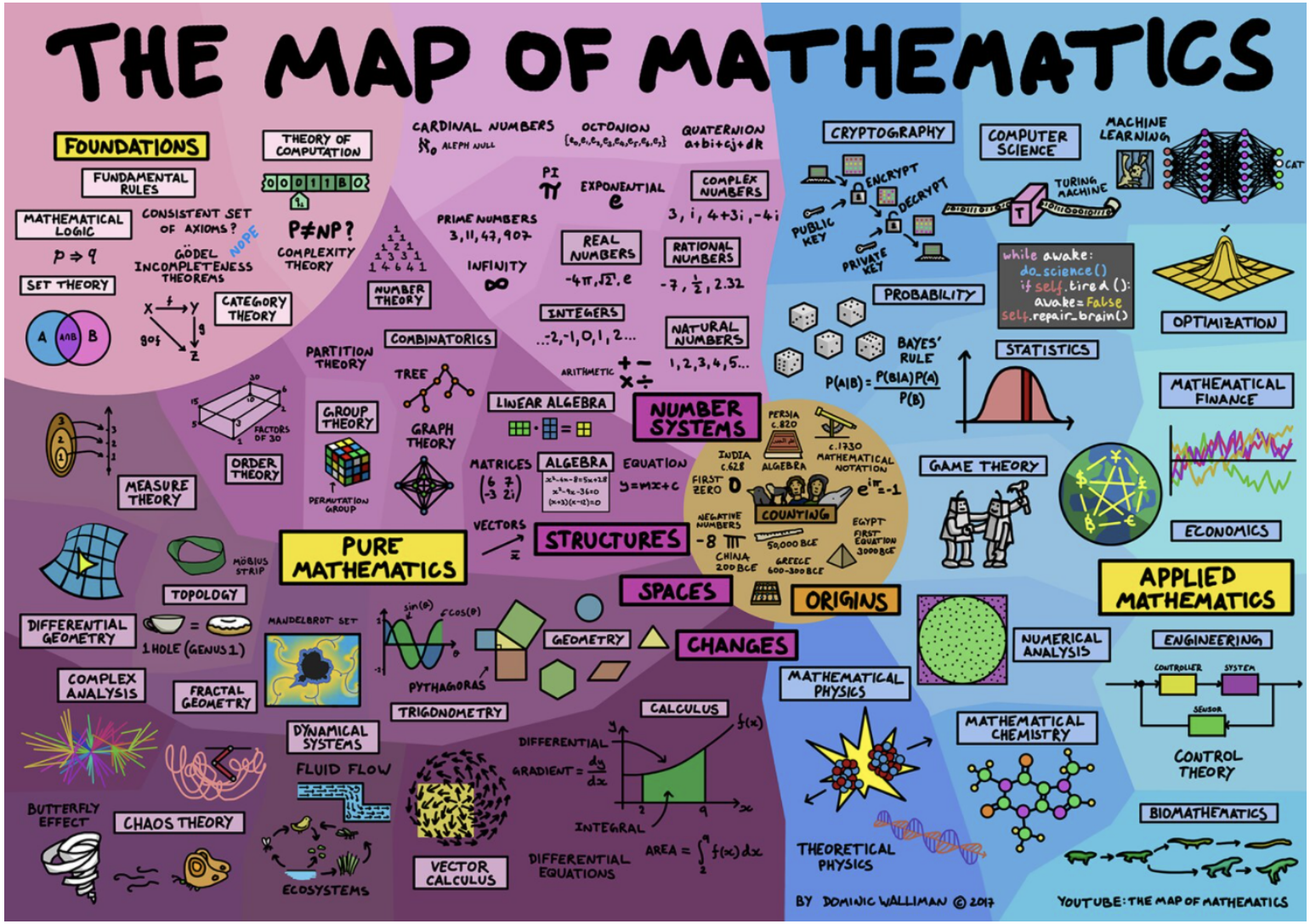
CS4236 Cryptography Theory and Practice Assignment 3

Hugh Anderson

National University of Singapore
School of Computing

October, 2022

Where are we then?



Outline

1. **Admin**
   - Special help sessions
2. **Assignment 3**
   - Comments on question 1
   - Comments on question 2
   - Comments on question 3
   - Comments on question 4
   - Comments on question 5

Outline

1. **Admin**
   - Special help sessions
2. **Assignment 3**
   - Comments on question 1
   - Comments on question 2
   - Comments on question 3
   - Comments on question 4
   - Comments on question 5

Outline

1. **Admin**
   - Special help sessions
2. **Assignment 3**
   - Comments on question 1
   - Comments on question 2
   - Comments on question 3
   - Comments on question 4
   - Comments on question 5

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

1. Admin
   - Special help sessions
2. **Assignment 3**
   - Comments on question 1
   - Comments on question 2
   - Comments on question 3
   - Comments on question 4
   - Comments on question 5

Question 1

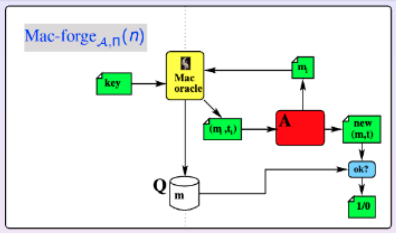
1. On page 188 is a description of $\text{Hiding}_{\mathcal{A},\Pi}(n)$... Draw the experiment/game ... Provide a formal definition of the hiding property.

Comment...

The question just asks about $\text{Hiding}_{\mathcal{A},\Pi}(n)$...

In class, diagram, game, definition. Here just diagram, AND definition.

Security requirement: Existential forgery



The first game: Mac-forge$_{\mathcal{A},\Pi}$ (Secure MAC)

1. Generate key $k = \text{Gen}(1^n)$.
2. Adversary has oracle access. Adversary outputs (m, t). Let Q be all the messages the adversary had sent to the oracle in this experiment.
3. Adversary wins (output of experiment is 1) iff (m, t) is valid and $m \notin Q$.

Definition 4.2 (pg 113) Existential unforgeability

We say that Π is existentially unforgeable under an adaptive chosen-message attack, or simply secure, iff for any $\mathcal{A}$, there is a negl, s.t.

$$\Pr[\text{Mac-forge}_{\mathcal{A},\Pi}(n) = 1] \leq \text{negl}(n)$$

Outline

1 Admin
- Special help sessions

2 Assignment 3
- Comments on question 1
- Comments on question 2
- Comments on question 3
- Comments on question 4
- Comments on question 5

Question 2

2. Assume that $h_1 : \{0,1\}^{2\times n} \to \{0,1\}^n$ is a collision resistant compression function. This is used to define a new compression function with an extra bit b concatenated to x:

$$h_2(x \# b) \stackrel{\text{def}}{=} \begin{cases} b = 1 & \to \quad b \# h_1(x) \\ b = 0 & \to \quad b^{n+1} \end{cases}$$

Is $h_2 : \{0,1\}^{2\times n+1} \to \{0,1\}^{n+1}$ also collision resistant? Show your reasoning.

Comment...

In this question you should consider both possible b cases. There is no particular trick here, but you should clearly state yes/no, and explain your reasoning clearly. To say NO - you can do a proof, or perhaps an attack/counterexample. To say YES - you show a proof.

Outline

1. Admin
   - Special help sessions
2. Assignment 3
   - Comments on question 1
   - Comments on question 2
   - Comments on question 3
   - Comments on question 4
   - Comments on question 5

Question 3

3. Given a collision resistant hash function $\mathcal{H}(x) \stackrel{\text{def}}{=} \mathcal{H}_1(\mathcal{H}_1(x))$. Prove that $\mathcal{H}_1$ is collision resistant.

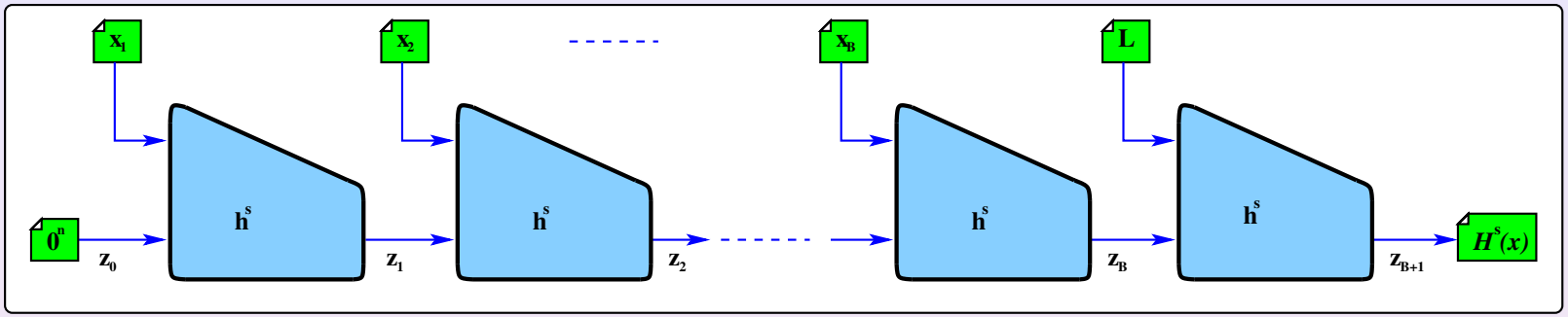
Comment...

I am expecting a formal clear proof, along the lines of proofs in CS4236.

Outline

1. Admin
   - Special help sessions
2. **Assignment 3**
   - Comments on question 1
   - Comments on question 2
   - Comments on question 3
   - Comments on question 4
   - Comments on question 5

Question 4



4. The above diagram shows the Merkle Damgård construction to construct collision resistant hashes over longer messages out of compression functions. We write the final hash as $\mathcal{H}^s(x) = Z_{B+1} = h^s(Z_B \# L)$. Consider the alternative final hash $\mathcal{H}_1^s(x) = Z_B \# L$. Is this still collision resistant?

Comment...

Make it clear you understand the question. Make it clear what stance you are taking. For YES - you will show a proof. For NO you would show a proof or an attack/counterexample.

Outline

1 Admin
- Special help sessions

2 Assignment 3
- Comments on question 1
- Comments on question 2
- Comments on question 3
- Comments on question 4
- Comments on question 5

Question 5

5. ... clients upload files to a server. Later, when a client retrieves a file, it wants a "fingerprint" δ-guarantee that it is the original, unmodified file. The signature is $\Pi(n) = (\mathrm{Put}(x_i), \mathrm{Get}(i), \mathrm{Vrfy}(i, x_i, \delta))$, where $\langle x_i, \delta \rangle \leftarrow \mathrm{Get}(i)$ returns the file and a fingerprint, and $\mathrm{ok} \leftarrow \mathrm{Vrfy}(i, x_i, \delta)$ returns $1/0$ if the fingerprint matches/does-not-match the file.

Comment...

As discussed last week in class, The $\langle i, \delta \rangle \leftarrow \mathrm{Put}(x)$ algorithm uploads a file, returning an index and a fingerprint δ. The $\mathrm{Vrfy}()$ function asserts that the file, the index, and the fingerprint all match to the previously uploaded x.

In Question 5, I expect each part to be answered: a description and diagram of a game, a definition of a property, and an outline of a possible construction for this server. Your construction can make use of existing schemes you have used (hashes, MACs, encryption and so on).