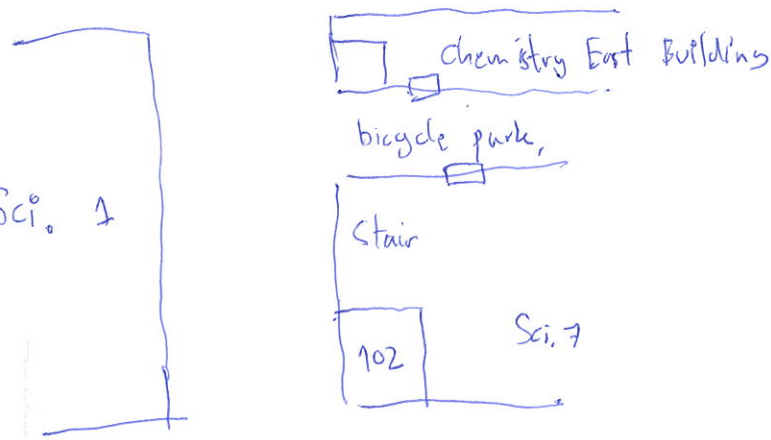
4810-1184 Algorithms for Information Security and Privacy.

Instructor: Vorapong Suppakitpaisarn. , vorapong@is.s.u-tokyo.ac.jp
(International Center for IST)

I sometimes discuss about our international activities at classes.

Office Hour: Thursday 15:00 – 16:30

How to get at my office? Room 137, Chemistry East Building.



First room after you get into the building.
The room has no room nuber at the gate!!!

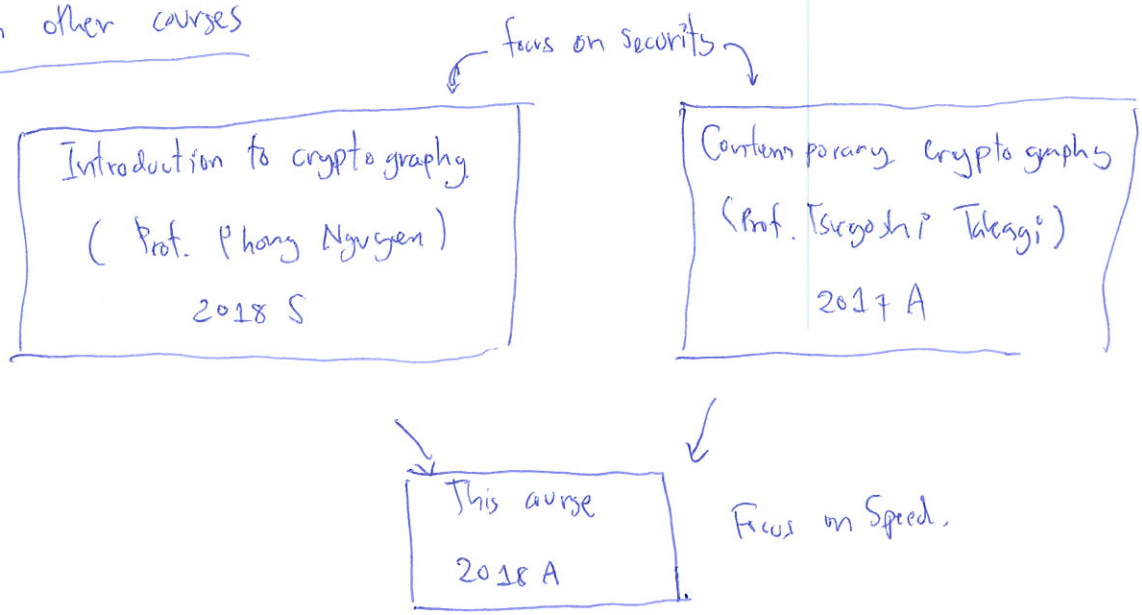
Class Schedule

9/25	Course Introduction, PAC Learning
10/~~2~~ 2	Differential Privacy: Laplacian Mechanism
10/~~9~~ 9	Diffential Privacy: Exponential Mechanism
10/~~15~~ 16	Diffential Privacy: Composition, Small PB algorithm
10/~~22~~ 23	Diffential Privacy: Private PAC Learning
10/~~29~~ 30	Countermeasures for Linking Attack.
11/26	Midterm Examination
	[30% to grade]

11/13	No class ~~[ISF will]~~
	[Day for cancelled classes]
11/20	Optional Class: Introduction to Abstract Algebra.
11/27	Calculation on Elliptic Curve Cryptosystem
12/3	Discrete Logarithm Problems
12/10	Elliptic Curve Cryptography Protocol
12/17	Identity-based Cryptosystem
12/25, 1/1	No class. [Holiday]
1/8	Final Examination [70% of credits]

Please inform me if you are not available on 11/6 or 1/8 before 10/9

Relationship with other courses



Differential Privacy

Name	Weight
Alice	40
Bob	60
Charles	80
Doe	60

Private Information

Average Weight = 60 } public information

- Charles does not want to publish his weight, but Alice, Bob, and Doe do publish.
- Average Weight $= \frac{w_{Alice} + w_{Bob} + w_{Charles} + w_{Doe}}{4}$

$$60 = \frac{40 + 60 + w_{Charles} + 60}{4}$$

$w_{Charles} = 80$

Information leakage!!!

Idea: Add noise to public information

Average Weight = 60

public information

$\Longrightarrow$ Average Weight + noise $= 55$

public information

By the noise, it is impossible to predict Charles' weight.

Linking Attack

Data published by goverment

Name	Age	Occupation
Alice	25	Student
Bob	30	Student
Charles	30	Banker

Data that hospitals give to machine learners.

[They want to find the diabete potential of each person.]

Name	Age	Occupation	Diabetes
Alice	25	Student	✓
Bob	30	Student	✗
Charley	35	Banker	✗

Direct publish ↗

- We do not want people to know that Alice has Diabete.
- We know from public information that the only 25-year-old is Alice.
- We know from hospital information that the only 25-year-old has diabete.

⇓

Alice has diabete. ☹

87% of U.S. citizen can be uniquely identified by sex, birthdate, and city [Sweeney 2002]

Elliptic Curve Cryptography (ECC)

- Alternative choice to RSA
- Used in industrail web services (Google, facebook, Microsoft)
- Have features that RSA does not have. [forward secrecy]
- Have better security level.