# Techniques in Applied Cryptography

CSCE 689 Section 602

#### **Instructor:**

Yupeng Zhang, HRBB 414A

office hour by appointment, <a href="mailto:zhangyp@tamu.edu">zhangyp@tamu.edu</a>

#### **Instructor:**

Yupeng Zhang, HRBB 414A

office hour by appointment, <a href="mailto:zhangyp@tamu.edu">zhangyp@tamu.edu</a>

#### **Time and Location:**

Tuesday and Thursday 12:45-2:00pm, HRBB 126

## Course Description

Applied Cryptography

- Basic concepts
- State-of-the-art constructions
- Applications
- Research directions

CSCE 689 section 600: Introduction to Modern Cryptography

## Topics

- Secure Multi-Party Computation (MPC)
  - Privacy-preserving Machine Learning
- Searchable Encryption
  - Search on Encrypted Files
- Zero Knowledge Proof
  - Privacy-preserving crypto-currencies and smart contract

## Webpage and piazza

https://tamucsce.github.io/csce689/

• piazza.com/tamu/fall2019/csce689section602

Secure Multiparty   Secure Multiparty   Secure Multiparty   Computation and Privacy-Preserving g Machine Learning   Privacy-preserving machine learning   10/31   11/5   11/12   11/26   10/8   11/28   11/28	Date	Section	Topic	Date	Section	Topic
Secure Multiparty   Secure Multiparty   Computation and   Privacy-Preserving   Generic solutions: SNARK	8/27	Introduction	Introduction and logistics			Introduction to verifiable
Secure Multiparty   Yao's garbled circuit   10/15   Computation and   Privacy-Preservin   g Machine   Learning   9/12   Privacy-preserving   10/24   Privacy-preserving   10/31   11/5   Proof and   Proof and   Privacy-preserving   10/31   11/14   Privacy-preserving   10/31   11/14   Privacy-preserving   Privacy-preserving   11/14   Privacy-preserving   Privacy-preserving   11/14   Privacy-preserving   Privacy-preserving	8/29	Secure Multiparty Computation and Privacy-Preservin g Machine Learning	Introduction to secure	10/10		computation and zero
Computation and Privacy-Preserving g Machine Learning   Dylam			multiparty computation		Computation, Zero Knowledge Proof and	0 1
Privacy-Preserving g Machine Learning 9/12  9/12  9/12  9/12  9/17  9/19  9/24  9/26  10/1  10/2  Searchable Encryption  10/1  10/3  10/3  10/3  10/3  Privacy-Preserving algorithms 10/24  10/29  10/29  10/29  11/5  11/7  11/12  Proof and Blockchain  11/12  Privacy-preserving contract  Privacy-preserving machine learning  11/12  Proof and Blockchain  11/12  Privacy-preserving crypto-currency and smart contract  Privacy-preserving crypto-currencies  Privacy-preserving mart contract  No class due to travel  11/19  Attacks to searchable encryption  11/21  10/8  10/8  Project  No class. Thanksgiving	9/3		Yao's garbled circuit	10/15		Customized solutions:
9/10 g Machine Learning learning algorithms  9/12 Privacy-preserving machine learning  9/17 Privacy-preserving machine learning  9/17 Introduction to searchable encryption  9/19 Privacy-preserving machine learning  9/19 Proof and Blockchain  11/12 Proof and Blockchain  11/12 Privacy-preserving crypto-currency and smart contract  Privacy-preserving crypto-currencies  Privacy-preserving smart contract  No class to searchable encryption  11/21 11/26 Project  Docality of searchable 11/28 Project  Proserving Searchable presentations  No class. Thanksgiving	9/5			10/17		Authenticated data structures
Privacy-preserving machine learning   10/24   Privacy-preserving machine learning   10/29   10/31     11/5   Proof and Blockchain   Introduction to searchable encryption   11/12   Proof and Blockchain   Introduction to blockchain, crypto-currency and smart contract   Privacy-preserving crypto-currencies   Privacy-preserving crypto-currencies   Privacy-preserving crypto-currencies   Privacy-preserving smart contract   11/19   Project   11/26   Project   11/28   Project   Project	0/10		C			
9/12 Privacy-preserving machine learning 10/29 10/31 Zero Knowledge Project presentation  9/17 Introduction to searchable encryption  9/19	9/10		learning algorithms			
machine learning  9/17  9/17  9/19  9/24  9/26  Searchable Encryption  10/3  10/3  11/5  11/7  No class due to travel 10/3  10/3  11/14  Forward and backward security  Attacks to searchable encryption  10/3  10/3  10/8  Machine learning 11/3  11/5  11/7  Proof and Blockchain  Introduction to blockchain, crypto-currency and smart contract  Privacy-preserving crypto-currencies  Privacy-preserving smart contract  Privacy-preserving smart contract  11/19  Attacks to searchable encryption  10/8  Project  Project  Project  No class Thanksgiving	9/12		Privacy-preserving	-		Midterm project presentation
Introduction to searchable encryption   Dynamic searchable encryption			machine learning			Generic solutions: Interactive
9/19 9/24 9/26 10/1  10/3  encryption  Dynamic searchable encryption  Dynamic searchable encryption  11/7  Blockchain  Introduction to blockchain, crypto-currency and smart contract  Privacy-preserving crypto-currencies  Privacy-preserving smart contract  Privacy-preserving smart contract  11/19  Attacks to searchable encryption  11/20  Project  Locality of searchable  11/28  Project  No class. Thanksgiving			Introduction to searchable			
Dynamic searchable encryption    11/12	9/17	Searchable	_			•
9/24 9/26 10/1 Searchable Encryption Forward and backward security Attacks to searchable encryption  10/3  10/8  Searchable Encryption  Locality of searchable  11/12  11/12  11/12  11/14  Crypto-currency and smart contract  Privacy-preserving crypto-currencies  Privacy-preserving smart contract  11/19  Project Dresentations  No class. Thanksgiving			V 1	11/12		· I
9/24 9/26 Encryption Forward and backward security  10/3  10/8  Searchable Encryption Forward and backward security  Attacks to searchable encryption Locality of searchable  11/14  11/14  Privacy-preserving crypto-currencies Privacy-preserving smart contract	9/19		-			· -
Searchable   No class due to travel   11/14     Crypto-currencies	9/24					
Forward and backward security  10/3  10/8  Forward and backward security  Attacks to searchable encryption  Locality of searchable  11/26  Locality of searchable  11/28  Privacy-preserving smart contract  11/21  Project  Dresentations  No class, Thanksgiving				11/14		
security  10/3  Security  Attacks to searchable encryption  Locality of searchable  11/26  Locality of searchable  11/28  Privacy-preserving smart contract  11/21  Project  Project  No class, Thanksgiving			Forward and backward	11/19		• 1
Attacks to searchable encryption  Locality of searchable  10/8  Attacks to searchable  11/21  Project  Dresentations  No class, Thanksgiving	10/1					· -
encryption  Locality of searchable  encryption  11/21  11/26  Project  presentations  No class, Thanksgiving			•			contract
Locality of searchable 11/28 presentations No class, Thanksgiving	10/3		_	_	Dwoisst	
10/8    NO CIASS, HIAHKSEIVINE	10		<u> </u>	· · · · · · · · · · · · · · · · · · ·	· ·	No aloga Thankarinina
encryption 12/3	10/8		encryption		presentations	No class, I nanksgiving

## **Grading Policy**

Class participation (10%):

• Reading assignment (25%):

#### • **Project (65%):**

- Proposal (10%)
- Mid-term report and presentation (10%)
- Final presentation (20%)
- Final report (25%)

## **Projects**

• 2-3 people each team. Team formation due 9/10.

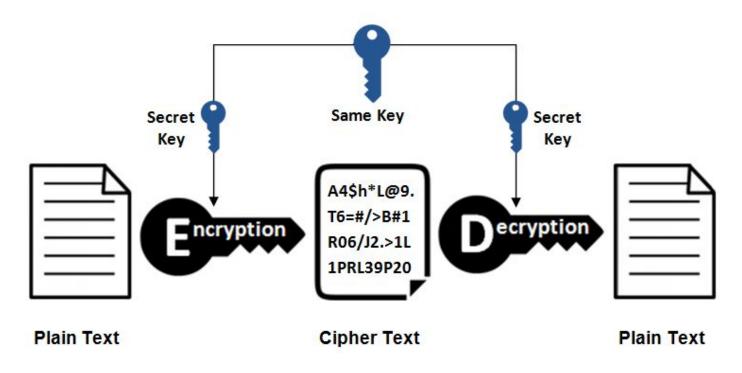
• Post list of suggested projects later. You can come up with your own ideas.

• Discuss the projects with me before proposal. Proposal due 9/26.

## Background

## Encryption

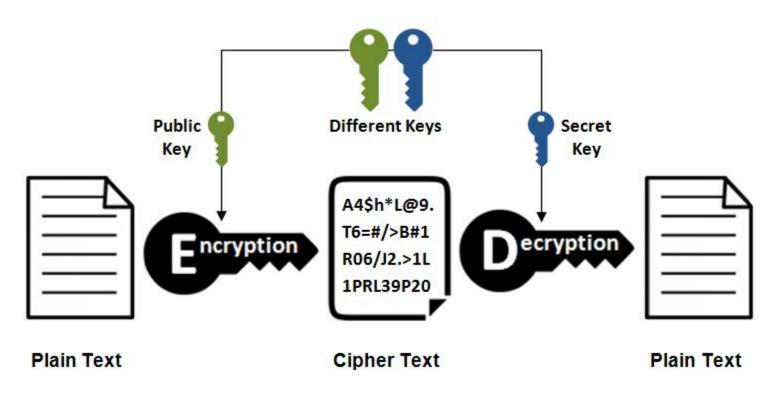
#### **Symmetric Encryption**



Deterministic vs. randomized

## Public key encryption (Asymmetric)

#### **Asymmetric Encryption**



## Message authentication code and signatures

Integrity

• Symmetric: message authentication code (MAC)

• Asymmetric: signature

## Cryptographic hash function

•  $H: \{0,1\}^* \to \{0,1\}^k$  any string to 256-bit string, deterministic

• Collision resistant: hard to find x,y such that H(x) = H(y)

• One-way: easy to compute, hard to invert (find x such that H(x) = y)

## Algorithms, data structures and asymptotic complexity

• Binary tree, hash table, skip list etc.

• Big O notation O(n), O(2^n)

## Binary representation

## Boolean circuits

• AND, OR, NOT, XOR, NAND

Truth table

### Arithmetic circuits

• + and × modulo a prime p

• Universal, can simulate Boolean circuits

### Field and finite field

• + and × modulo a prime p

• Generator of the group g (e.g. 2) s.t.  $g^1, g^2, \dots, g^{p-1}$  generates all elements in the group

• Discrete-log assumption: hard to compute x such that  $g^x = y$