# LYU1901 Anonymous online course evaluation CENG4999 FINAL YEAR PROJECT PRESENTATION STEVEN YAU & LUTHER LUI PRESENT SUPERVISED BY PROF. MICHAEL LYU

0

### Motivation

- Cost of paper-based course evaluation
- User-authenticated course evaluation



# Objective

- Teachers and officers cannot track the identity of evaluation participants
- Participants validation
- Data encryption
- Web user interface



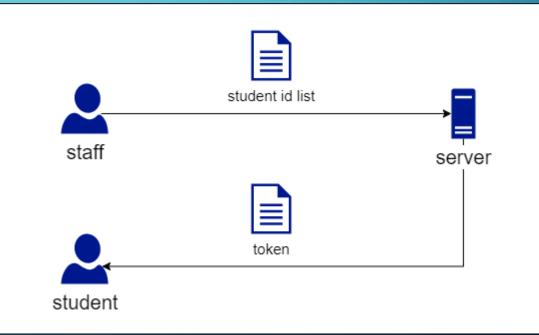
 $\bigcirc$ 

 $\bigcirc$ 

0

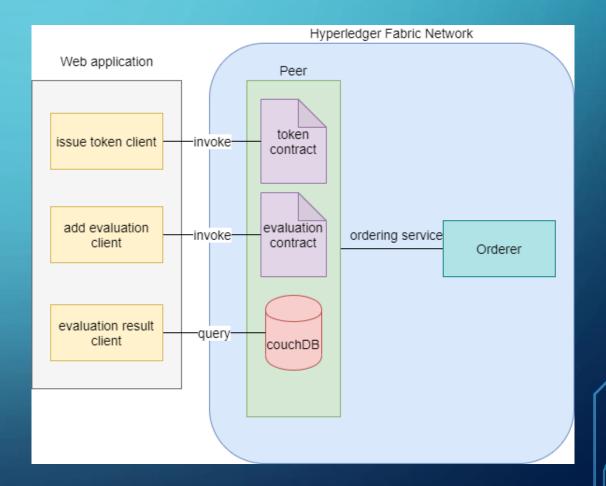
#### Token validation

- Random generated token
- No token owner record
- Distribute through email
- Mark the used tokens



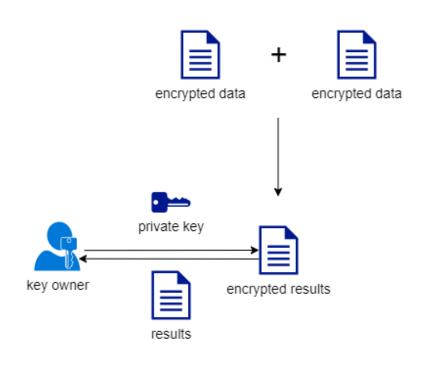
#### Hyperledger fabric

- Invoke smart contract through web app
- Query or update data with the contract response



#### Data encryption

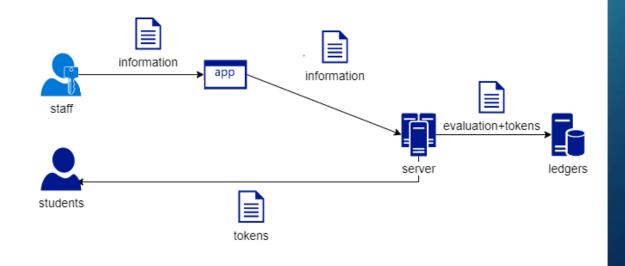
- Additive ElGamal encryption
- Tally with encrypted data
- Teachers/officers keep private key



# Implementation

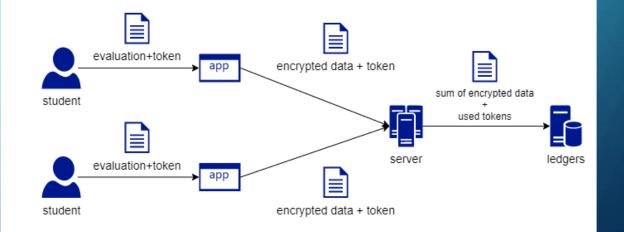
### System workflow

- Staff provide information for creating evaluation
- System distribute tokens to students



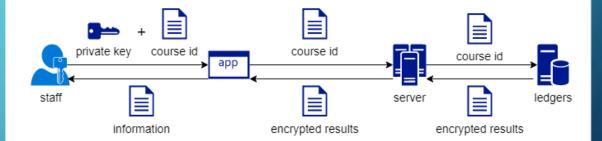
#### System workflow

- Students spend tokens to submit evaluation
- Sum encrypted evaluation data
- Store the data and used tokens in ledgers



### System workflow

- Staff decrypt the results with private key
- Local decryption



#### **Evaluation form**

п.	My faculty	O ART O	BAS	O EDU	O ERG	OLAW	O MED O	SCI O SSC	OOTHER
b.,	Level	O Undergradua	ate	O Postgrad	fuate	O Other			
¢.,	Year of study:	O Year I O	Year 2	O Year 3	O Year 4	O Year 5	O Year ≥6		
d.	This course is (select one):	O Major Requi	ired	O Major Elective O Minor O Elective O U Core (GE,				Core (GE, Lang, PE	IT) ONA
e.	Sex:	O Female		O Male					
f.	Primary spoken language used in class:			<b>O</b> English	O Ca	O Cantonese O Putonghua		O Others	
	Fraction of class time the pr	imary language wa	s used:	O 51-60%	O 61-	70%	O 71-80%	O 81-90%	O 91-100%
	Supplementary language(s) (can select more than one):		<b>O</b> English	O Ca	ntonese O Putonghua		O Others	O N/A	
g.	Hours per week spent on this	course outside cla	155	O 0-2.0	0214.0	041-80	O 8.1-12.	O 12.0+	O N/A
h.	<ul> <li>Expected grade in the course:</li> </ul>		O A	OA.	OB+	OB/B-	O C+ or below	O N/A	

		Di	rom; sagr	ee	<	2		Agree	N/A THE
	Clarity of Explanation 解释清楚		1	2	3	4	5	6	N/A
	The teacher presented in a clear manner. 老師表達清晰	1.	0	0	0	0	0	0	0
2	The teacher used relevant examples to assist my learning. 老師運用濾當例子,有助學習	2.	0	0	0	0	0	0	0
	Enthusiasm and Communication 熱忱與講通								
	The teacher was enthusiastic about teaching, 老師熟心教學	3.			0				0
	The teacher encouraged active participation in class. 老丽鼓動學生積極參與課意活動			1.00	0	-	0	0	0
5.	There was effective communication between teacher and students. 郁生溝通真好	5.	0	0	0	0	0	0	0
	Motivation # 28								
	The course was interesting, 本科富有趣味性	6,	0	0	0	0	0	0	0
	The course was stimulating. 本科富有啓發性	7.			0			0	0
8.	The course enhanced my knowledge in this subject. 學習本科能增進我對本科目的認識	8.	0	0	0	0	0	0	0
	Learning Outcomes and Organisation 目標及目錄								
	The course was well-organised. 本科編排台當		-	1.00	0	100		1.00	0
10	. Learning outcomes of the course were clear. 本科的學習目標清晰	10	0	0	0	0	0	0	0
	Assessment Frit								
	Assessment methods were appropriate. 評核方法遺當		0			0	0	0	0
12	. The amount of workload required was appropriate. 要求的作業份量合適	12	0	0	0	0	0	0	0
	If your answer is 1, 2 or 3 to Q12; 如第12期答案母1 - 2 成 3						~		
	I found the amount of work required for assessment 我認爲要求的作業份量:	0	) To	io Mi	ich /	3	0	Tao Litt	e.1.9
	Course Difficulty 料目離皮				- 23		125	022	- 2
	Recommended readings were useful. 推測書目很有用		1.00		0	-			0
14	Course content was of appropriate difficulty. 本科內容深度適中	14	0	0	0	0	0	0	0
	If your answer is 1, 2 or 3 to Q14; 如第14團答案用1、2 成3 1 found the course content 我認保定的內容:	1	1.			-	0		ple 1:38
		`	2.10	io tri	Jacun	1.10	.0	100 300	pre 2756
	Learning Support 學習實證支持	12	0	~	-	~	~	0	0
	The course was well supported by library resources. 圖書館有足夠賣重支持本料的學習		0	0	0	0	0	0	0
10	. The course was well supported by IT resources. 大學有足夠的資訊科技資源支持本科的學習	10	0	0	0	0	0	0	0
	Overall Opinion		-		100	1	-	1023	0.2
	Overall, I am satisfied with the course. 整體而言,我對本科感到滿意		0		0	0	0	0	0
18	Overall, I am satisfied with the teacher's performance. 整體而習,我對本科老師的數學表現感到纖維	18	0	0	0	0	0	0	0

Please answer the questions at the back of the page. 請填答背面的問題 ·

#### Evaluation Form Basic Information

My forully	$\odot APT = SA2 + EDO = ERE + LAW + MED +$	30 = 50C = 014E8						
Level:	U Undergraduate II Portunate II Other							
Near of shady	$\pm$ then $1$ $\pm$ then $2$ $\pm$ then $2$ $\pm$ then $4$ $\pm$ then $5$ $\pm$ then $4$ are above							
This course is palacel on a	Uniger Requirem in Higher Dection in Minor in	$r' \in Bactive = \cup Core p(E,Long,PE,P) = NN.$						
See.	U Fermile II Male							
Primary spoken integrape contributions		$\pm$ Digital: $\pm$ Contonese $\pm$ Patanghas: $\pm$ Others						
Fraction of data line the primary language eas	$\simeq 5140N_{\rm c} \approx 45.70R_{\rm c} \approx 7740R_{\rm c} \approx 8740R_{\rm c} \approx 97402N_{\rm c}$							
Supplementary tempological (), on solid more that	= English = Containeau = Nationghais = Others = Nat							
Place per seek sport or this course advide do	an	-5.22 + 27.42 - 47.42 + 87.52 + 529 + 8,0.						
Expected profe in the course		U.A. U.A. U.B. U.B.R. U.C. or Solow						

#### Clarity of Explanation 1. The teacher presented in a clear moreal. In Stranger Disarger Disarger

2. The teacher used relevant examples to assist my learning. In Strongly Stronger II Stronger II Stightly Stronger II Stightly Agree II Agree II Strongly Agree II Hulk

Enthusiasm and Communication The teacher was anth-associated teaching,
 Strongy Disarger. I: Disarger. D A. The basilier encodingent active participation in class. In Strongly Disarges: In Disarges: In Stylety Disagnes: In Sightly Agres: In Agres: In Disarge, Agres: In 1644.

There was effective communication between two feer and doublers.
 Strongly Descripe: IS Discript: IS 2014/J Discript: IS 2014/J Agree II Agree II Strongly Agree II 10/A

Motivation
4. The course and interesting
© Drongly Dronger © Dronger © Dronger © Stighty Agree © Agree © Strongly Agree © 10.4  $\label{eq:constraint} \begin{array}{l} 1 \mbox{ the constraint} q, \\ \otimes \mbox{ Energy} \mbox{ Straingly Encoupler } \otimes \mbox{ Energy} \mbox{ Agree } \otimes \mbox{ Encouple Agree } \otimes \mbox{ Note } \end{array}$ 

8. The course entropy of the constant we investigate the subgroup of the strange of the set of the strange of the set of the set of the strange of the set of the se Learning Outcomes and Organisation

3.The course and engenised. In Decempt Decempter: In Decempter: In Decempter of Staphily Agrees: In Agrees: In Decempter Agrees: In Note. RE Learning robotines of the course were clear In Decorpty Charges: In Discorpt In Signify Discorption III Signify Agree III Agree III Decorpty Agree III 100.

Assessment
E. Samonet Institution were opposition
© Drange Dranger © Dranger © Dranger © Dranger © Standy, Agree © Standy, Agree © Standy, Agree © Sta St. The prevant of excitation required eco suppropriate. In Strangey Descripte: In Descripte In Stightly Descripter. In Sightly Agree: In Agree In Description Agree (1918). If your stream is Diracely Obsergen, Discogen is Stightly Disagree to GO I found the sensure of work required for spacement.

Course Difficulty 13 Receiveranted receivings were confut. Il Strongs Disargee - Disargee - Stightly Disagnee - Slightly Rignee - Strongs Rignee - NAR. N. Course content was of appropriate difficulty. In Strange Disargee: In Diargee: In Statisty Disagnee: In Digitally Agree: In Agree: In Diarge, Agree: In 1616.

Fyour senser is Strangy Disages, Disages or Skythy Disages to Orl House the course context I to Difficult in Tax Singles

Learning Support (b) The Locale and adjusted by Diracy resources.
(c) Strangly Discreps: (c) Discreps: (c) Digits's Discreps: (c) Strangly Agree: (c) Agree: (c) Discreps: (c) Di 3. The source edd with supported by IT resources. In Strange Stranger II Stranger II Stranger II Stranger II Stightly Agree II Agree II Strange Agree II 10.

Overall Opinion 0 Diversit, Lan extrataci with the course. In Discrept Obsergee II: Discrept II: Discrept II: Discrept II: Discrept Agree II: NA

H. Owend, I. on applicate with the insultance performance. I: Strongs Stranger: I: Disarger: I: Sightly Disagree: I: Sightly: Agree: I: Agree: I: Disarger, Agree: I: NA.

# Keys generation

- P: 512 bits big prime number
- G: random no. with range of 1 to (P-1)
- Private key: random no. with range of 1 to (P-1), gcd(G, Private key) is 1
- Public key: G ^ (Private Key) mod P



 $\bigcirc$ 

 $\bigcirc$ 

# Future improvement

#### **Functional improvement**

- Customized questionnaire
- Open-ended question
- Keys management
- Export results with various file formats

# Security improvement

- Evaluation data validation
- More secure communication protocol
- Distribute tokens in safer way

# Performance improvement

- Better encryption algorithm
- Data handling method

