LYU1901
Anonymous online course evaluation

CENG4999 FINAL YEAR PROJECT PRESENTATION
STEVEN YAU & LUTHER LUI PRESENT
SUPERVISED BY PROF. MICHAEL LYU
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
Design
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
**Clarity of Explanation**

1. The teacher presented in a clear manner. 完全了解清楚
2. The teacher used relevant examples to explain the concepts. 相关事例解释清楚
3. The teacher gave clear instructions. 清晰地给出指示
4. The teacher encouraged active participation in class. 积极鼓励课堂参与
5. There was effective communication between teacher and students. 教师与学生之间有效的沟通

**Motivation**

1. The content was interesting. 内容有趣
2. The course was stimulating. 课程刺激
3. The course enhanced my knowledge in this subject. 课程增强了我对该主题的理解

**Learning Outcomes and Organization**

1. The course was well-organized. 课程组织良好
2. The course outcomes were clear. 学习成果明确

**Assessment**

1. Assessment methods were appropriate. 评估方法适当
2. The amount of workload required was appropriate. 工作量合适
3. I found the amount of work required for assessment too much/too little. 评估工作量过少/过多

**Course Difficulty**

1. Recommended readings were useful. 推荐阅读材料有用
2. Course content was appropriate difficulty. 内容难度恰当
3. I found the course content too easy/too difficult. 课程内容太容易/太难

**Learning Support**

1. The course was well-supported by library resources. 图书馆资源支持充分
2. The course was well-supplied by IT resources. IT资源支持充分

**Overall Opinion**

1. Overall, I am satisfied with the course. 对课程总体满意
2. Overall, I am satisfied with the teacher’s performance. 对教师表现总体满意

Please enter the questions at the back of the page. 請問後面的問題。
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), \( \text{gcd}(G, \text{Private key}) = 1 \)
- Public key: \( G^{\text{Private Key}} \mod P \)
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
Q&A