A secure electronic exam system using Identity-based Cryptography

Ádám Vécsi
Attila Pethő

CITDS 2020, Debrecen
November 6-8, 2020.
Introduction

E-learning,
E-exam
E-learning – What is it?

- Instruction delivered on a digital device that is intended to support learning.
- Examples
  - online courses
  - learning applications
  - tutorial videos
  - educational games
E-learning – Growth

source: classcentral.com
E-learning – During pandemic

2020 Web Traffic

visitors in millions

Source: SimilarWeb
E-learning – Is it good?

- Customizable training
  - Tailoring content
  - Asynchronous learning
- Multimedia
- Simulations
  - Practice infrequent scenarios
- Gamification
E-learning – e-exam

- What is an e-exam?

- Is it common?
  - KRESZ exam – traffic rule exam
  - IT certification
  - Online University Degree
Preliminaries

Secure e-exam properties,
Identity-based Encryption,
Mixnet
Secure e-exam

- Authenticity
- Anonymity
- Accountability
- Secrecy
- Robustness
- Correctness
- Receipt
Identity-based Encryption

- Unique branch of the public key cryptography.

- The public keys are clear identifiers of individuals.
  - Local or global domain.
  - E-mail, phone number, etc.

- Public key extended with data.
How IBE works in practice

0. SETUP
1. ENCRYPT
2-3. EXTRACT
4. DECRYPT
Anonym communication via mixnet
Identity-based mixnet

Public key certificates are NOT required.
E-exam scheme
E-exam participants

- Exam authority
- Students
- Teachers
Exam flow

1. **Registration**
2. **Request and receive questions**
2.5. **Anonymous communication**
3. **Hand in**
4. **Receive and correct exams**
5. **Send grade**
6. **After a timed event the EA sends the grades to students**
Conclusion

- Introduced the property of accountability.
- Decreased computational cost by using IBC.
- Convenient eligibility check via data-infused public keys.
This work is supported partially by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project is supported by the European Union, co-financed by the European Social Fund.

This work is supported partially by the SETIT (2018-1.2.1-NKP-2018-00004) project.
References

Thank you for your attention!