Security definitions for electronic exam systems

Andrea Huszti

huszti.andrea@inf.unideb.hu

University of Debrecen, Faculty of Informatics

NetLock Kft

My talk

- Scenario - Participants, algorithms
- Experiment-based security definitions - authenticity, correctness, secrecy, anonymity
- Proposed scheme - Registry and anonymizer server are trusted

Scenario

Participants:

- Examinees (EX)
- Exam Correctors (EC)
- Registry (R)
- Examination Authority (EA)
- Adversary ($\mathcal{A}$)

Scheme

Stages:

- Registration - EX, EC prove their identity to R and receive pseudonyms
  $register(i, SK_R) \longrightarrow \{pseudonym, 0\}$
- Examination - EX receive questions, generate answers with time stamp and send them to EA, EX receive receipt
  $takeexam(questions, pseudonym, SK_{TS}) \longrightarrow \{receipt, 0\}$

Scheme

- Evaluation - EA sends exam answers to EC, who gives marks that are transmitted back to EA
  $correct(exam, index) \longrightarrow$
  $\{(mark, checksum), 0\}$
  Examinees' real identity are revealed from their pseudonyms.
  $getidentity(pseudonym) \longrightarrow \{i, 0\}$

We define an exam scheme as
ExS=$\{register, takeexam, correct, getidentity\}$.

Adversary model

- non-eligible examinees and examiners - authenticity
- simulation attack - authenticity
- modification - correctness
- confidentiality of answers and marks - secrecy
- bribing, threatening attack - anonymity

Notation

n/m: number of examinees/exam correctors identified by R

$I_{\mathcal{BB}}$: all data being sent to $\mathcal{BB}$ by honest participants

$\bar{n}/\bar{m}$: number of ineligible examinees/exam correctors

$\bar{I}_{\mathcal{BB}}$: all data being sent to $\mathcal{BB}$ by $\mathcal{A}$

$\tilde{n}/\tilde{m}$: number of examinees received a mark/exam correctors gave a mark

$\tilde{I}_{\mathcal{BB}}$: all data available on $\mathcal{BB}$

Correctness

Exp$^{corr}_{ExS,\mathcal{A}}(.)$

for all honest $i \in EX \bigcup EC$ **do**

$I_{\mathcal{BB}} \leftarrow$ register(i, SK)

$I_{\mathcal{BB}} \leftarrow$ takeexam$(questions, pseudonym_i, SK_{TS})$

$I_{\mathcal{BB}} \leftarrow$ correct$(exam_i, index)$

$I_{\mathcal{BB}} \leftarrow$ getidentity$(pseudonym_i)$

end for

$\bar{I}_{\mathcal{BB}} \leftarrow \mathcal{A}$(control participants,"$modify\ and\ generate\ data$")

if $\exists i \in [1, .., \tilde{n}]$: verify$(\tilde{I}_{\mathcal{BB}}\ for\ id_i) = 0$ **then**

return 0

else if $I_{\mathcal{BB}} \not\subseteq \tilde{I}_{\mathcal{BB}}$ **then**

return 1

else

return 0

Correctness

The advantage of an adversary $\mathcal{A}$ is

$$\mathbf{Adv}^{corr}_{ExS,\mathcal{A}}(.) = \Pr[\mathbf{Exp}^{corr}_{ExS,\mathcal{A}}(.) = 1].$$

A scheme for electronic exam ExS possesses property of **correctness** if for any $\mathcal{A} \in PT^*$ the advantage $\mathbf{Adv}^{corr}_{ExS,\mathcal{A}}(.)$ is negligible.

Secrecy

$\mathbf{Exp}^{secr-b}_{ExS,\mathcal{A}}(.)$

$I_{\mathcal{BB}} \leftarrow \text{register}(i, SK, SK_{AC})$
$(exam_0, exam_1) \leftarrow \mathcal{A}(\text{"}generate\ exams\text{"})$
$\bar{I}_{\mathcal{BB}} \leftarrow$
$\mathcal{A}^{takeexam(.),corrrect(.)\ with\ exam_b}(control\ channels)$
$d \leftarrow \mathcal{A}(\text{"}guess\ b\text{"})$
return d

The advantage of an adversary $\mathcal{A}$ is

$$\mathbf{Adv}^{secr}_{ExS,\mathcal{A}}(.) = |\Pr[\mathbf{Exp}^{secr-0}_{ExS,\mathcal{A}}(.) = 1] - \Pr[\mathbf{Exp}^{secr-1}_{ExS,\mathcal{A}}(.) = 1]|$$

A scheme for electronic exam ExS possesses property of **secrecy** if for any $\mathcal{A} \in PT^*$ the advantage $\mathbf{Adv}^{secr}_{ExS,\mathcal{A}}(.)$ is negligible.

Anonymity

$\mathbf{Exp}^{anon-b}_{ExS,\mathcal{A}}(.)$

$(i_0, i_1) \leftarrow \mathcal{A}(\text{"}choose\ examinees/exam\ correctors\text{"})$

$(\bar{I}_{\mathcal{BB}}, pseudonym_{i_b}) \leftarrow$

$\mathcal{A}^{register(i_b,.),takeexam(.),correct(.),getidentity(.)}(control\ participants)$

if $Ver_{PK}(pseudonym_{i_b}) = 1$ **then**

  $d \leftarrow \mathcal{A}(\text{"}guess\ b\text{"})$

  if $b = d$ **then**

    return 1

  else

    return 0

  end if

else

  return 0

Anonymity

The advantage of an adversary $\mathcal{A}$ is

$$\mathbf{Adv}^{anon}_{ExS,\mathcal{A}}(.) = |\Pr[\mathbf{Exp}^{anon-0}_{ExS,\mathcal{A}}(.) = 1] - \Pr[\mathbf{Exp}^{anon-1}_{ExS,\mathcal{A}}(.) = 1]|$$

A scheme for electronic exam ExS possesses property of **anonymity** if for any $\mathcal{A} \in PT^*$ the advantage $\mathbf{Adv}^{anon}_{ExS,\mathcal{A}}(.)$ is negligible.

The proposed scheme

- honest anonymizer server (AC)
- honest R during registration
- flexible design (e.g. symmetric encryption - IND-CPA secure, asymmetric encryption - IND - CCA)
- Secure key-generation using common reference string

Theorem 0.1 *If there exists a family of trapdoor permutations and we assume that the Registry during registration and the anonymizer server are honest, then there exists a scheme for electronic exam which is secure in the common reference string model.*

Idea of the proof of anonymity:

Let $\mathcal{A}$ be an adversary that is successful in Experiment $\mathbf{Exp}_{ExS,\mathcal{A}}^{anon-b}(.)$ with non-negligible probability.

Then $\mathcal{A}$ can construct a machine $\mathcal{A}_{ind-cca}$ that breaks indistinguishability of asymmetric encryption scheme under CCA.

Thank you for your attention!