Formal Analysis of Electronic Exams

Jannik Dreier\textsuperscript{1}, Rosario Giustolisi\textsuperscript{2}, Ali Kassem\textsuperscript{3}, Pascal Lafourcade\textsuperscript{4}, Gabriele Lenzini\textsuperscript{2} and Peter Y. A. Ryan\textsuperscript{2}

\textsuperscript{1}Institute of Information Security, ETH Zurich
\textsuperscript{2}SnT/University of Luxembourg
\textsuperscript{3}Université Grenoble Alpes, CNRS, VERIMAG
\textsuperscript{4}University d’Auvergne, LIMOS

11th International Conference on Security and Cryptography (SECRYPT 2014), Vienna

August 28, 2014
E-exam
Information technology for the assessment of knowledge and skills.
Educational assessment
E-exam: Players and Organization

Three Roles:

Candidate | Examination Authority | Examiner
E-exam: Players and Organization

Three Roles:

Candidate  Examination Authority  Examiner

Four Phases:

Threats...

- Candidate cheating
- Bribed, corrupted or unfair examiners
- Dishonest/untrusted exam authority
- Outside attackers
- ...
...and their Mitigation

Most existing e-exam systems assume trusted authorities and focus on student cheating:

- Exam centers

- Software solutions, e.g. ProctorU
Most existing e-exam systems assume trusted authorities and focus on student cheating:

▶ Exam centers

▶ Software solutions, e.g. ProctorU

Yet also the other threats are real:

▶ Atlanta Public Schools cheating scandal (2009)
▶ UK student visa tests fraud (2014)
...and their Mitigation

Most existing e-exam systems assume trusted authorities and focus on student cheating:

- Exam centers
- Software solutions, e.g. ProctorU

Yet also the other threats are real:

- Atlanta Public Schools cheating scandal (2009)
- UK student visa tests fraud (2014)

So what about dishonest authorities or hackers attacking the system?
Most existing e-exam systems assume trusted authorities and focus on student cheating:

- Exam centers
- Software solutions, e.g. ProctorU

Yet also the other threats are real:
- Atlanta Public Schools cheating scandal (2009)
- UK student visa tests fraud (2014)

So what about dishonest authorities or hackers attacking the system?
⇒ need for better protocols and systems (cf. case studies)
...and their Mitigation

Most existing e-exam systems assume trusted authorities and focus on student cheating:

▶ Exam centers

▶ Software solutions, e.g. ProctorU

Yet also the other threats are real:

▶ Atlanta Public Schools cheating scandal (2009)
▶ UK student visa tests fraud (2014)

So what about dishonest authorities or hackers attacking the system?

⇒ need for better protocols and systems (cf. case studies)
⇒ precise formal definitions of required properties
Plan

Introduction

Model and Properties
  Authentication Properties
  Privacy Properties

Case Studies
  Huszti & Pethő’s Protocol
  Remark! Protocol

Conclusion
Plan

Introduction

Model and Properties
  Authentication Properties
  Privacy Properties

Case Studies
  Huszti & Pethő’s Protocol
  Remark! Protocol

Conclusion
Model

- **Processes** in the applied $\pi$-calculus
- Annotated using **events**
- **Authentication** properties as **correspondence** between events
- **Privacy** properties as **observational equivalence** between instances
- **Automatic** verification using ProVerif
Model

1. Registration

2. Examination

Questions submitted, collected

3. Marking

distributed, collected

Form marked

4. Notification

notified

Mark
1. Registration

Register

reg( )

2. Examination

Questions submitted

Answer

3. Marking

Form marked

Mark

4. Notification

notified

Mark
1. Registration

2. Examination

Register

\( \text{reg(\text{\textbullet})} \)

Marking

Notification
1. Registration

Register

\( reg(\cdot) \)

2. Examination

Questions

\[ \text{Submitted} \quad \text{Collected} \quad \text{Answer} \quad \text{Mark} \quad \text{Distributed} \quad \text{Form} \quad \text{Marked} \quad \text{Notified} \]
Model

1. Registration
   Register
   \( \text{reg}() \)

2. Examination
   Questions
   \( \text{submitted}(\text{？}, \text{？}, \text{？}) \)
   Answer
   \( \text{collected}(\text{？}, \text{？}, \text{？}) \)

4. Notification
   \( \text{notified}(\text{？}, \text{？}) \)
1. Registration
   Register
   \( \text{reg}(\cdot) \)

2. Examination
   Questions
   \( \text{submitted}(\cdot, ?, !) \) \( \xrightarrow{\text{Answer}} \) \( \text{collected}(\cdot, ?, !) \)

3. Marking
Model

1. Registration
   Register
   $\text{reg}(\text{ })$

2. Examination
   Questions
   $\text{submitted}(\text{ }, \text{?}, \text{!})$  \rightarrow  $\text{collected}(\text{ }, \text{?}, \text{!})$

3. Marking
   $\text{distrib}(\text{ }, \text{?}, \text{!}, \text{QR code}, \text{ })$
   \rightarrow  Form
Model

1. Registration
   Register
   \( \text{reg}(\ ) \)

2. Examination
   Questions
   \( \text{submitted}(\ , \ , \ ) \rightarrow \text{collected}(\ , \ , \ ) \)

3. Marking
   \( \text{distrib}(\ , \ , 
   \ , \ , \ , \ ) \rightarrow \text{marked}(\ , \ , 
   \ , \ , \ , \ ) \)

4. Notification
   \( \text{notified}(\ , \ ) \)
1. Registration
   Register
   \( \text{reg}(\cdot) \)

2. Examination
   Questions
   \( \text{submitted}(\cdot, ?, !) \) → \( \text{collected}(\cdot, ?, !) \)

3. Marking
   \( \text{distrib}(\cdot, ?, !, 
   \text{Form} \)
   \( \text{marked}(?, !, \text{mark} \)

4. Notification

---

Model
Model

1. Registration
   Register
   \( \text{reg}(\; ) \)

2. Examination
   Questions
   \( \text{submitted}(\; , ?, !) \)
   \( \text{collected}(\; , ?, !) \)

3. Marking
   \( \text{distrib}(\; , ?, !, \),, \)
   \( \text{marked}(?, !, \),, \)

4. Notification
   \( \text{notified}(?, \)\)
Plan

Introduction

Model and Properties
  Authentication Properties
  Privacy Properties

Case Studies
  Huszti & Pethő’s Protocol
  Remark! Protocol

Conclusion
Answer Origin Authentication

All collected answers originate from registered candidates, and only one answer per candidate is accepted.

Definition:

On every trace:

1. Registration
   
2. Examination

\[\text{submitted}(\text{student}, \text{question}, \text{answer})\]  \[\text{collected}(\text{student}, \text{question}, \text{answer})\]

\[\text{reg}(\text{student})\]

\textit{Preceeded by distinct occurrence}
Form Authorship

Answers are collected as submitted, i.e. without modification.

Definition:

On every trace:

1. Registration

\[ \text{Register} \quad \text{reg}(\cdot) \]

2. Examination

\[ \text{Questions} \quad \text{submitted}(\cdot, ?, !) \rightarrow \text{Answer} \rightarrow \text{collected}(\cdot, ?, !) \]

preceded by distinct occurrence
Form Authenticity

Answers are marked as collected.

Definition:

On every trace:

2. Examination

Questions

submitted(?, ?, !)

Answer

collected(?, ?, !)

3. Marking

distrib(?, ?, !, ?, ?)

Form

marked(? ! ? ?)

preceeded by distr. occ.
Mark Authenticity

The candidate is notified with the mark associated to his answer.

Definition:

On every trace:

3. Marking

4. Notification

preceded by distinct occurrence
Plan

Introduction

**Model and Properties**
  - Authentication Properties
  - Privacy Properties

**Case Studies**
  - Huszti & Pethő’s Protocol
  - Remark! Protocol

Conclusion
Question Indistinguishability

No premature information about the questions is leaked.

Definition:

Observational equivalence of two instances up to the end of registration phase:

Exam 1

Question 1

\approx

Exam 2

Question 2
Question Indistinguishability

No premature information about the questions is leaked.

**Definition:**

Observational equivalence of two instances up to the end of registration phase:

Exam 1

\[ \text{Question 1} \approx \text{Question 1} \]

Exam 2

\[ \text{Question 2} \]

Can be considered with or without dishonest candidates.
Anonymous Marking

An examiner cannot link an answer to a candidate.

Definition:

Up to the end of marking phase:

Exam 1

Answer 1

Answer 2

Exam 2

Answer 2

Answer 1
Anonymous Marking

An examiner cannot link an answer to a candidate.

**Definition:**

Up to the end of marking phase:

- **Exam 1**
  - Answer 1
  - Answer 2

- **Exam 2**
  - Answer 2
  - Answer 1

Can be considered with or without dishonest examiners and authorities.
Anonymous Examiner

A candidate cannot know which examiner graded his copy.

**Definition:**

![Diagram showing two exams with answers and marks]

Can be considered with or without dishonest candidates.
Marks are private.

Definition:

Can be considered with or without dishonest candidates, examiners and authorities.
Mark Anonymity

Marks can be published, but may not be linked to candidates.

Definition:

Can be considered with or without dishonest candidates, examiners and authorities.

Implied by Mark Privacy.
Plan

Introduction

Model and Properties
  Authentication Properties
  Privacy Properties

Case Studies
  Huszti & Pethő’s Protocol
  Remark! Protocol

Conclusion
Plan

Introduction

Model and Properties
  Authentication Properties
  Privacy Properties

Case Studies
  Huszti & Pethő’s Protocol
  Remark! Protocol

Conclusion
“A Secure Electronic Exam System” [?] using

- ElGamal Encryption
- a Reusable Anonymous Return Channel (RARC) [?] for anonymous communication
- a network of servers providing a timed-release service using Shamir’s Secret Sharing:
  A subset of servers can combine their shares to de-anonymize a candidate after the exam

**Goal:** ensure

- authentication and privacy

in presence of **dishonest**

- candidates
- examiners
- exam authorities
Formal Verification with ProVerif [?]:

<table>
<thead>
<tr>
<th>Property</th>
<th>Result</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Answer Origin Authentication</td>
<td>×</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Form Authorship</td>
<td>×</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Form Authenticity</td>
<td>×</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Mark Authenticity</td>
<td>×</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Question Indistinguishability</td>
<td>×</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Anonymous Marking</td>
<td>×</td>
<td>8 m 46 s</td>
</tr>
<tr>
<td>Anonymous Examiner</td>
<td>×</td>
<td>9 m 8 s</td>
</tr>
<tr>
<td>Mark Privacy</td>
<td>×</td>
<td>39 m 8 s</td>
</tr>
<tr>
<td>Mark Anonymity</td>
<td>×</td>
<td>1h 15 m 58 s</td>
</tr>
</tbody>
</table>
Main reason

Given its security definition, the RARC

- provides anonymity, but not necessarily secrecy
- does not necessarily provide integrity or authentication
- is only secure against passive attackers

Corrupted parties or active attackers can break secrecy and anonymity, as the following attack shows.
RARC: Mode of Operation and Attack

**Input** (A to RARC, destination B):

\[
\{ ID_A, PK_A \}^{PK_{RARC}} + PoK; \{ MSG \}^{PK_{RARC}}; \{ ID_B, PK_B \}^{PK_{RARC}} + PoK
\]
RARC: Mode of Operation and Attack

Input (A to RARC, destination B):
\[ \{ID_A, PK_A\}_{PK_{RARC}} + PoK; \{MSG\}_{PK_{RARC}}; \{ID_B, PK_B\}_{PK_{RARC}} + PoK \]

Output (RARC to B):
\[ \{ID_A, PK_A\}_{PK_{RARC}} + Signature; \{MSG\}_{PK_{B}} \]
RARC: Mode of Operation and Attack

Input (A to RARC, destination B):
\[ \{ ID_A, PK_A \}^{PK_{RARC}} + PoK; \{ MSG \}^{PK_{RARC}} ; \{ ID_B, PK_B \}^{PK_{RARC}} + PoK \]

Output (RARC to B):
\[ \{ ID_A, PK_A \}^{PK_{RARC}} + Signature; \{ MSG \}^{PK_B} \]

Return (B to RARC, destination A):
\[ \{ ID_B, PK_B \}^{PK_{RARC}} + PoK; \{ MSG \}^{PK_{RARC}} ; \{ ID_A, PK_A \}^{PK_{RARC}} + Signature \]
RARC: Mode of Operation and Attack

**Input (A to RARC, destination B):**

\[
\{ ID_A, PK_A \}^{PK_{RARC}} + PoK; \{ MSG \}^{PK_{RARC}}; \{ ID_B, PK_B \}^{PK_{RARC}} + PoK
\]

**Output (RARC to B):**

\[
\{ ID_A, PK_A \}^{PK_{RARC}} + Signature; \{ MSG \}^{PK_B}
\]

**Return (B to RARC, destination A):**

\[
\{ ID_B, PK_B \}^{PK_{RARC}} + PoK; \{ MSG \}^{PK_{RARC}}; \{ ID_A, PK_A \}^{PK_{RARC}} + Signature
\]

**Attack**

**Input (AD to RARC, destination AD):**

\[
\{ ID_{AD}, PK_{AD} \}^{PK_{RARC}} + PoK; \{ MSG \}^{PK_{RARC}}; \{ ID_{AD}, PK_{AD} \}^{PK_{RARC}} + PoK
\]
RARC: Mode of Operation and Attack

Input (A to RARC, destination B):
\{ID_A, PK_A\}^{PK_{RARC}} + PoK; \{MSG\}^{PK_{RARC}}; \{ID_B, PK_B\}^{PK_{RARC}} + PoK

Output (RARC to B):
\{ID_A, PK_A\}^{PK_{RARC}} + Signature; \{MSG\}^{PK_B}

Return (B to RARC, destination A):
\{ID_B, PK_B\}^{PK_{RARC}} + PoK; \{MSG\}^{PK_{RARC}}; \{ID_A, PK_A\}^{PK_{RARC}} + Signature

Attack

Input (AD to RARC, destination AD):
\{ID_{AD}, PK_{AD}\}^{PK_{RARC}} + PoK; \{MSG\}^{PK_{RARC}}; \{ID_{AD}, PK_{AD}\}^{PK_{RARC}} + PoK

Output (RARC to AD):
\{ID_{AD}, PK_{AD}\}^{PK_{RARC}} + Signature; \{MSG\}^{PK_{AD}}
Plan

Introduction

Model and Properties
  Authentication Properties
  Privacy Properties

Case Studies
  Huszti & Pethő’s Protocol
  Remark! Protocol

Conclusion
Application: Remark! Protocol

A recent protocol \([^1]\) using

- ElGamal encryption
- an exponentiation mixnet \([^2]\) to create pseudonyms based on the parties’ public keys
  \(\Rightarrow\) allows to encrypt and sign anonymously
- a public append-only bulletin board

**Goal:** ensure

- authentication and integrity
- privacy
- verifiability

in presence of dishonest

- candidates
- examiners
- exam authorities
Formal Verification with ProVerif:

<table>
<thead>
<tr>
<th>Property</th>
<th>Result</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Answer Origin Authentication</td>
<td>✓</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Form Authorship</td>
<td>✓</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Form Authenticity</td>
<td>✓¹</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Mark Authenticity</td>
<td>✓</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Question Indistinguishability</td>
<td>✓</td>
<td>&lt; 1 s</td>
</tr>
<tr>
<td>Anonymous Marking</td>
<td>✓</td>
<td>2 s</td>
</tr>
<tr>
<td>Anonymous Examiner</td>
<td>✓</td>
<td>1 s</td>
</tr>
<tr>
<td>Mark Privacy</td>
<td>✓</td>
<td>3 m 32 s</td>
</tr>
<tr>
<td>Mark Anonymity</td>
<td>✓</td>
<td>-²</td>
</tr>
</tbody>
</table>

¹ after fix
² implied by Mark Privacy
Plan

Introduction

Model and Properties
  Authentication Properties
  Privacy Properties

Case Studies
  Huszti & Pethő’s Protocol
  Remark! Protocol

Conclusion
Conclusion

- **E-exams** are used and vulnerable to attacks
- Cryptographic protocols exist, but **lack formal verification**
- **First formal framework** for analysis of e-exams:
  - Formal model in the **applied \( \pi \)-calculus**
  - **Definitions** for central authentication, integrity and privacy properties
- **Automated verification in ProVerif** of two case studies:
  - Huszti & Pethő’s protocol: Fails on all properties due to severe flaws in protocol design
  - Remark! protocol: Ensures all properties after one fix
- **Future work**: verifiability and accountability, analyzing implementations
Thank you for your attention!

Questions?

jannik.dreier@inf.ethz.ch
Definition (E-exam protocol). An e-exam protocol is a tuple

\[(C, E, Q, A_1, \ldots, A_l, \tilde{n}_p),\]

where

- \(C\) is the process executed by the candidates,
- \(E\) is the process executed by the examiners,
- \(Q\) is the process executed by the question committee,
- \(A_i\)'s are the processes executed by the authorities, and
- \(\tilde{n}_p\) is the set of private channel names.
Definition (E-exam instance). An e-exam instance is a closed process

\[ EP = \nu \tilde{n}. (C_{\sigma_{id_1} \sigma_{a_1}} | \ldots | C_{\sigma_{id_j} \sigma_{a_j}} | E_{\sigma_{id_1}' \sigma_{m_1}} | \ldots | E_{\sigma_{id_k}' \sigma_{m_k}} | Q_{\sigma_q} | A_{1\sigma_{dist}} | \ldots | A_l), \]

where

- \( \tilde{n} \) is the set of all restricted names, which includes the set of the protocol’s private channels;
- \( C_{\sigma_{id_i} \sigma_{a_i}} \)'s are the processes run by the candidates, the substitutions \( \sigma_{id_i} \) and \( \sigma_{a_i} \) specify the identity and the answers of the \( i^{th} \) candidate respectively;
- \( E_{\sigma_{id_i}' \sigma_{m_i}} \)'s are the processes run by the examiners, the substitution \( \sigma_{id_i}' \) specifies the \( i^{th} \) examiner’s identity, and \( \sigma_{m_i} \) specifies for each possible question/answer pair the corresponding mark;
Definition (E-exam instance). An e-exam instance is a closed process

\[ EP = \nu \tilde{n}. (C \sigma_{id_1} \sigma_{a_1} | \ldots | C \sigma_{id_j} \sigma_{a_j} | E \sigma_{id'_1} \sigma_{m_1} | \ldots | E \sigma_{id'_k} \sigma_{m_k} | Q \sigma_q | A_1 \sigma_{dist} | \ldots | A_l), \]

where

- \( Q \) is the process run by the question committee, the substitution \( \sigma_q \) specifies the exam questions;
- the \( A_i \)'s are the processes run by the exam authorities, the substitution \( \sigma_{dist} \) determines which answers will be submitted to which examiners for grading.

Without loss of generality, we assume that \( A_1 \) is in charge of distributing the copies to the examiners.
Definition (Answer Origin Authentication)

An e-exam protocol ensures Answer Origin Authentication if, for every e-exam process EP, each occurrence of the event \( \text{collected}(id\_c, \text{ques}, \text{ans}) \) is \textit{preceded} by a distinct occurrence of the event \( \text{reg}(id\_c) \) on every execution trace.

Definition (Form Authorship)

An e-exam protocol ensures Form Authorship if, for every e-exam process EP, each occurrence of the event \( \text{collected}(id\_c, \text{ques}, \text{ans}) \) is \textit{preceded} by a distinct occurrence of the event \( \text{submitted}(id\_c, \text{ques}, \text{ans}) \) on every execution trace.
Definition (Form Authenticity)

An e-exam protocol ensures Form Authenticity if, for every e-exam process EP, each occurrence of the event \(\text{marked}(\text{ques, ans, mark, id\_form, id\_e})\) is preceded by a distinct occurrence of the events \(\text{distrib}(\text{id\_c, ques, ans, id\_form, id\_e})\) and \(\text{collected}(\text{id\_c, ques, ans})\) on every execution trace.

Definition (Mark Authenticity)

An e-exam protocol ensures Mark Authenticity if, for every e-exam process EP, each occurrence of the event \(\text{notified}(\text{id\_c, mark})\) is preceded by a distinct occurrence of the events \(\text{marked}(\text{ques, ans, mark, id\_form, id\_e})\) and \(\text{distrib}(\text{id\_c, ques, ans, id\_form, id\_e})\) on every execution trace.
Definition (Question Indistinguishability)
An e-exam protocol ensures Question Indistinguishability if for any e-exam process $EP$ that ends with the registration phase, any questions $q_1$ and $q_2$, we have that:
$EP_{\{id_Q\}}[Q_{\sigma_q_1}]_{\text{reg}} \approx l EP_{\{id_Q\}}[Q_{\sigma_q_2}]_{\text{reg}}$.

Definition (Anonymous Marking)
An e-exam protocol ensures Anonymous Marking if for any e-exam process $EP$ that ends with the marking phase, any two candidates $id_1$ and $id_2$, and any two answers $a_1$ and $a_2$, we have that:
$EP_{\{id_1, id_2\}}[C_{\sigma_{id_1}a_1} | C_{\sigma_{id_2}a_2}]_{\text{mark}} \approx l EP_{\{id_1, id_2\}}[C_{\sigma_{id_1}a_2} | C_{\sigma_{id_2}a_1}]_{\text{mark}}$. 
Privacy Properties cont’d

Definition (Anonymous Examiner)

An e-exam protocol ensures Anonymous Examiner if for any e-exam process $EP$, any two candidates $id_1$, $id_2$, any two examiners $id'_1$, $id'_2$, and any two marks $m_1$, $m_2$, we have that:

$$EP\{id_1, id_2, id'_1, id'_2, id_{A_1}\} [C \sigma_{id_1} \sigma_{a_1} | C \sigma_{id_2} \sigma_{a_2} | E \sigma_{id_1} \sigma_{m_1} | E \sigma_{id'_2} \sigma_{m_2} | A_1 \sigma_{dist_1}] \approx l EP\{id_1, id_2, id'_1, id'_2, id_{A_1}\} [C \sigma_{id_1} \sigma_{a_1} | C \sigma_{id_2} \sigma_{a_2} | E \sigma_{id'_2} \sigma_{m_2} | E \sigma_{id'_1} \sigma_{m_1} | A_1 \sigma_{dist_2}]$$

where $\sigma_{dist_1}$ attributes the exam form of candidate $id_1$ to examiner $id'_1$ and the exam form of candidate $id_2$ to examiner $id'_2$, and $\sigma_{dist_2}$ attributes the exam form of candidate $id_1$ to examiner $id'_2$ and the exam form of candidate $id_2$ to examiner $id'_1$.

Definition (Mark Privacy)

An e-exam protocol ensures Mark Privacy if for any e-exam process $EP$, any marks $m_1$, $m_2$, we have that:

$$EP\{id'\} [E \sigma_{id'} \sigma_{m_1}] \approx l EP\{id'\} [E \sigma_{id'} \sigma_{m_2}]$$
Definition (Mark Anonymity)

An e-exam protocol ensures Mark Anonymity if for any e-exam process $EP$, any candidates $id_1$, $id_2$, any examiner $id_1'$, any answers $a_1$, $a_2$ and a distribution $\sigma_{dist}$ that assigns the answers of both candidates to the examiner, and two substitutions $\sigma_{ma}$ and $\sigma_{mb}$ which are identical, except that $\sigma_{ma}$ attributes the mark $m_1$ to the answer $a_1$ and $m_2$ to $a_2$, whereas $\sigma_{mb}$ attributes $m_2$ to the answer $a_1$ and $m_1$ to $a_2$, we have that:

$$EP_{\{id_1, id_2, id_1', id_A_1\}} \left[ C_{\sigma id_1 \sigma a_1} | C_{\sigma id_2 \sigma a_2} | E_{\sigma id_1' \sigma m_a} | A_1 \sigma_{dist} \right] \approx 1$$

$$EP_{\{id_1, id_2, id_1', id_A_1\}} \left[ C_{\sigma id_1 \sigma a_1} | C_{\sigma id_2 \sigma a_2} | E_{\sigma id_1' \sigma m_b} | A_1 \sigma_{dist} \right]$$
checkpseudo(pseudo\_pub(pk(k), rce),
pseudo\_priv(k, exp(rce))) = true

decrypt(encrypt(m, pk(k), r), k) = m

decrypt(encrypt(m, pseudo\_pub(pk(k), rce), r), pseudo\_priv(k, exp(rce))) = m

getmess(sign(m, k)) = m

checksign(sign(m, k), pk(k)) = m

checksign(sign(m, pseudo\_priv(k, exp(rce))), pseudo\_pub(pk(k), rce)) = m
**Remark! Protocol**

Assumption: The protocol assumes a list of eligible examiners and their public keys $PK_E$, and a list of eligible candidates and their public keys $PK_C$.

**Examiner Registration**
1. $NET$ calculates $r_e = \prod_{i=1}^{k} r_{e_i}$, $PK_E = PK_E^{r_e}$ and $h_e = g^{r_e}$
2. $NET$ publishes $\text{sign}((PK_E, h_e), SK_{NET})$
3. $E$ checks if $PK_E = h_e^{SK_E}$

**Candidate Registration**
4. $NET$ calculates $r_c = \prod_{i=1}^{k} r_{c_i}$, $PK_C = PK_C^{r_c}$ and $h_c = g^{r_c}$
5. $NET$ publishes $\text{sign}((PK_C, h_c), SK_{NET})$
6. $C$ checks if $PK_C = h_c^{SK_C}$

**Examination**
7. $EA \rightarrow C : \{\text{sign(} \text{question, } SK_{EA} \text{)}\}_{PK_C}$
8. $C \rightarrow EA : // C_a = \{\text{question, answer, } PK_C\}$
   $\{C_a, \text{sign(} C_a, SK_C, h_c \text{)}\}_{PK_{EA}}$
9. $EA \rightarrow C : \{C_a, \text{sign(} C_a, SK_{EA} \text{)}\}_{PK_C}$
Marking
10- $EA \rightarrow E : \{C_a, \text{sign}(C_a, SK_{EA})\}_{PK_E}$
11- $E \rightarrow EA : \text{// } M_a = (\text{sign}(C_a, SK_{EA}), \text{mark})$
\{\text{sign}(M_a, SK_E, h_e)\}_{PK_{EA}}$

Notification
12- $EA \rightarrow C : \{M_a, \text{sign}(M_a, SK_E, h_e)\}_{PK_C}$
13- $NET \rightarrow EA : \{\overline{r}_c, \text{sign}(\overline{r}_c, SK_N)\}_{PK_{EA}}$
Huszti Equational Theory

\[
\text{decrypt}(\text{encrypt}(m, pk(k), r), k) = m
\]
\[
\text{getmess}(\text{sign}(m, k)) = m
\]
\[
\text{checksign}(\text{sign}(m, k), pk(k)) = m
\]
\[
\text{exp}(\text{exp}(g, x), y) = \text{exp}(\text{exp}(g, y), x)
\]
\[
\text{checkproof}(\text{xproof}(p, p1, g, \text{exp}(g, e), e),
\quad
p, p1, g, \text{exp}(g, e)) = true
\]
\[
\text{zkpsec}(\text{zkp\_proof}(\text{exp}(b, e), e), \text{exp}(b, e)) = true
\]
Huszti’s Protocol

Setup
1 - *EA* publishes \( g \) and \( h = g^s \)
2 - *Committee* \( \rightarrow_{\text{priv}} \) \( EA \):
\[ \{ \text{question}, \{ \text{question} \} \}_{\text{SSK}_{\text{committee}}}, \text{time}_{x1} \}_{\text{PK}_{\text{MIX}}} \]

Candidate Registration
3 - \( EA \) checks \( C \)'s eligibility, and calculates \( \tilde{p} = (PK_C)^s \)
4 - \( EA \to NET : \{ \tilde{p}, g_C \} \)
5 - \( NET \) calculates \( p' = \tilde{p}^\Gamma \), and \( r = g_C^\Gamma \), and stores \( time_{nt} \)
6 - \( NET \to C : \{ p', r \} \)
7 - \( C \) calculates \( p = r^{SK_C} \)
8 - \( EA \leftrightarrow C : \text{ZKP}_{eq}((p, p'), (g, h)) \) // \( C \)'s pseudonym: \( (r, p, p') \)
Huszti’s Protocol

Examiner Registration
9 - $EA$ checks $E$’s eligibility, and calculates $\tilde{q} = (PK_E)^s$
10 - $EA \rightarrow E : \{\tilde{q}, g_E\}$
11 - $E$ calculates $q' = \tilde{q}^\alpha$, $t = g_E^\alpha$, and $q = t^{SK_E}$
12 - $EA \leftrightarrow E : \text{ZKP}_{eq}((q, q'), (g, h))$
13 - $E \rightarrow EA : \{t, q, q', h\}$
14 - $EA$ checks $q^s = q'$
15 - $E \leftrightarrow EA : \text{ZKP}_{sec}(SK_E)$
16 - $EA$ stores $\{ID_E, PK_E\}_{PK_{Mix}}, h$

Examination
17 - $C \rightarrow EA : \{r, p, p', h\}$
18 - $EA$ checks $p^s = p'$
19 - $C \leftrightarrow EA : \text{ZKP}_{sec}(SK_C)$
20 - $EA \rightarrow C : \{\text{question}, \{\text{question}\}_{SSK_{\text{committee}}}, time_{x1}\}_{PK_{Mix}}$
21 - $C \rightarrow EA : \{r, p, \{\text{answer}\}_{PK_{Mix}}, time_{x2}\}$
22 - $EA \rightarrow C : \text{Hash}(r, p, p', h, trans_C, \text{question}, time_{x1}, time_{x2} \{\text{answer}\}_{PK_{Mix}})$
Huszti’s Protocol

Marking
23 - $EA \rightarrow E: \{answer\}_{PK_{Mix}}$ // Note that $EA$ stored
{$ID_E, PK_E}_{PK_{Mix}, h}$
24 - $E \rightarrow EA: \{mark, Hash(mark, answer), [Hash(mark, answer)]^{SK_E}, verzkp, t, q\}$
25 - $E \leftrightarrow EA: ZKP_{eq}(Hash(mark, answer), [Hash(mark, answer)]^{SK_E}, (t, q))$

Notification
26 - $EA \rightarrow NET: \{p'\}$ //Note that $r = g^\Gamma_C, p = PK^\Gamma_C, p' = g^{\Gamma_s}_C$
27 - $NET$ calculates $p' = \bar{p}^\Gamma$
28 - $NET \rightarrow EA: \{p', \bar{p}\}$
29 - $EA$ publishes $mark, Hash(mark, answer), [Hash(mark, answer)]^{SK_E}, verzkp$