Security Analysis of Electronic Exams

Rosario Giustolisi[4], Ali Kassem[1], Gabriele Lenzini[4], Peter Y. A. Ryan[4], Jannik Dreier[3], Yliès Falcone[2] and **Pascal Lafourcade**[5]

[1]Univ. Grenoble Alpes, VERIMAG, Grenoble, France

[2]Univ. Grenoble Alpes, Inria, LIG, Grenoble

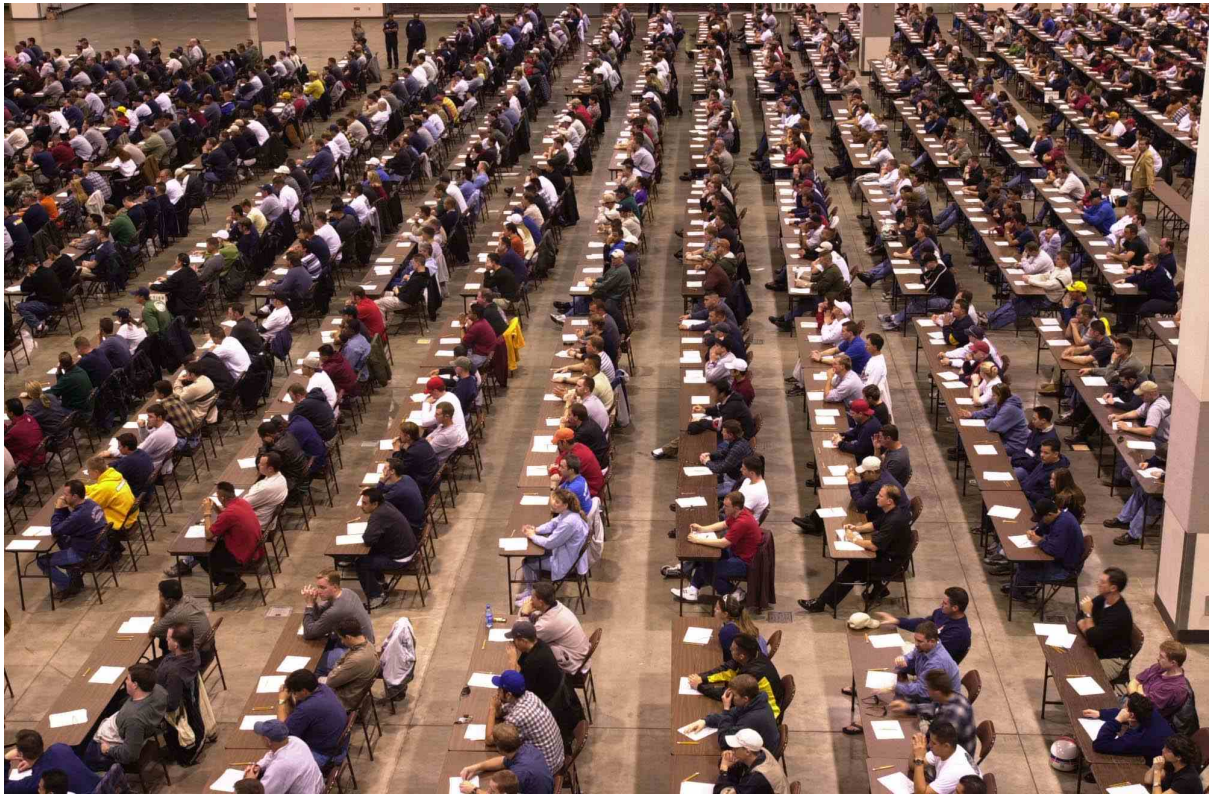
[3]Loria, Equipe Cassis, Inria, Nancy
[4]SnT/University of Luxembourg
[5]University Clermont Auvergne, LIMOS

Eurecom, 25th February 2016

Exam

Filippo Galanti (Sora in Caserta 1852 - Buenos Aires 1953)

Traditional Exam



e-exam

Information technology for the assessment of knowledge and skills.

Reality


coursera


UDACITY

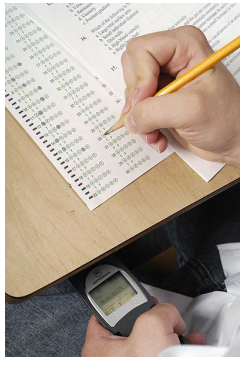

edX


IELTS
English for International Opportunity


CISCO
CCNA


TOEFL iBT

Threats. . .



- Candidate cheating
- Bribed, corrupted or unfair examiners
- 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

ProctorU
Real People.
Real Proctoring.

. . . and their Mitigation

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

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

ProctorU
Real People.
Real Proctoring.

Yet also the **other threats** are real:

- Atlanta Public Schools cheating scandal (2009)
- Turkish Public Personnel Selection Exam (2010)
- 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

ProctorU
Real People.
Real Proctoring.

Yet also the **other threats** are real:

- Atlanta Public Schools cheating scandal (2009)
- Turkish Public Personnel Selection Exam (2010)
- UK student visa tests fraud (2014)

So what about **security** of **e-exams**?

Our Results

Secrypt'14 Authentication Properties: Mark Authenticity, Answer Origin Authentication, Form Authorship, Form Authenticity.
Privacy Properties: Anonymous Marking, Question Indistinguishability, Anonymous Examiner, Mark Privacy, Mark Anonymity

ISPEC'15 Individual Verifiability: Question Validity, Marking Correctness, Exam-Test Integrity, Exam-Test Markedness, Marking Integrity, Marking Notification Integrity
Universal Verifiability: Eligibility (Registration), Marking Correctness Exam-Test Integrity, Exam-Test Markedness, Marking Integrity.

RV'15 How can we use previous results on real e-exam?
Monitoring of reals e-exams.

Plan

Plan

E-exam: Players and Organization

Three Roles:

Candidate

Examination Authority

Examiner

E-exam: Players and Organization

Three Roles:

Candidate

Examination Authority

Examiner

Four Phases:

1. Registration 2. Examination 3. Marking 4. Notification

Model

- **Processes** in the applied π-calculus [AF01]
- Annotated using **events**
- **Authentication** properties as **correspondence** between events
- **Privacy** properties as **observational equivalence** between instances
- **Automatic** verification using ProVerif [Bla01]

Model

Model

1. Registration

Model

1. Registration

Register

register()

Model

1. Registration

Register

register()

2. Examination

Model

1. Registration

Register

register()

2. Examination

Questions

Model

1. Registration

Register

register( )

2. Examination

Questions

submit(, ,)

Answer

accept(, ,)

Model

1. Registration

Register

register( )

2. Examination

Questions

submit(, ,)

Answer

accept(, ,)

3. Marking

Model

1. Registration

Register

register( )

2. Examination

Questions

submit(, ,)

Answer

accept(, ,)

3. Marking

distrib(, , , ,)

Form

Model

1. Registration

Register

register( )

2. Examination

Questions

submit(, ,)

Answer

accept(, ,)

3. Marking

distrib(, , , ,)

Form

Mark

mark(, , ,)

Model

1. Registration

Register

register( )

2. Examination

Questions

submit(, ,)

Answer

accept(, ,)

3. Marking

distrib(, , , ,)

Form

Mark

mark(, , ,)

4. Notification

Model

1. Registration

Register

register( )

2. Examination

Questions

submit(, ,)

Answer

accept(, ,)

3. Marking

distrib(, , , ,)

Form

Mark

mark(, , ,)

4. Notification

notified(,)

Mark

Plan

Answer Origin Authentication

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

Definition:

On every trace:

1. Registration — Register — *register*( )
2. Examination — Questions — Answer — *submit*(, ,) — *accept*(, ,)

preceeded by distinct occurence

Form Authorship

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

Definition:

On every trace:

1. Registration — Register — *register*( )
2. Examination — Questions — *submit*(, ,) — Answer — *accept*(, ,)

preceeded by distinct occurence

Form Authenticity

Answers are marked as collected.

Definition:

On every trace:

2. Examination

Questions

submit(, ,)

Answer

accept(, ,)

preceeded by dist. occ.

3. Marking

distrib(, , , ,)

Form

Mark

mark(, , ,)

Mark Authenticity

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

Definition:

On every trace:

3. Marking

distrib(, , , ,) — Form

Mark — *mark*(, , ,)

4. Notification

notified(,)

Mark

preceeded by distinct occurence

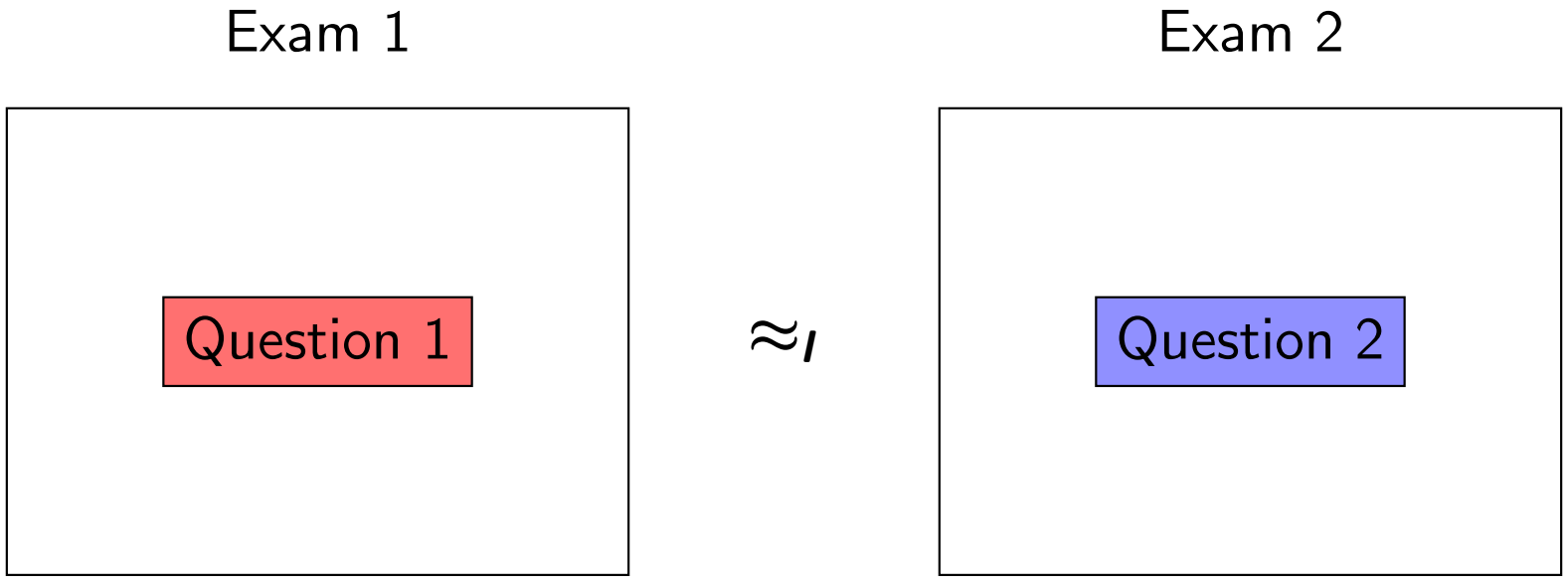
Plan

Question Indistinguishability

No premature information about the questions is leaked.

Definition:

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

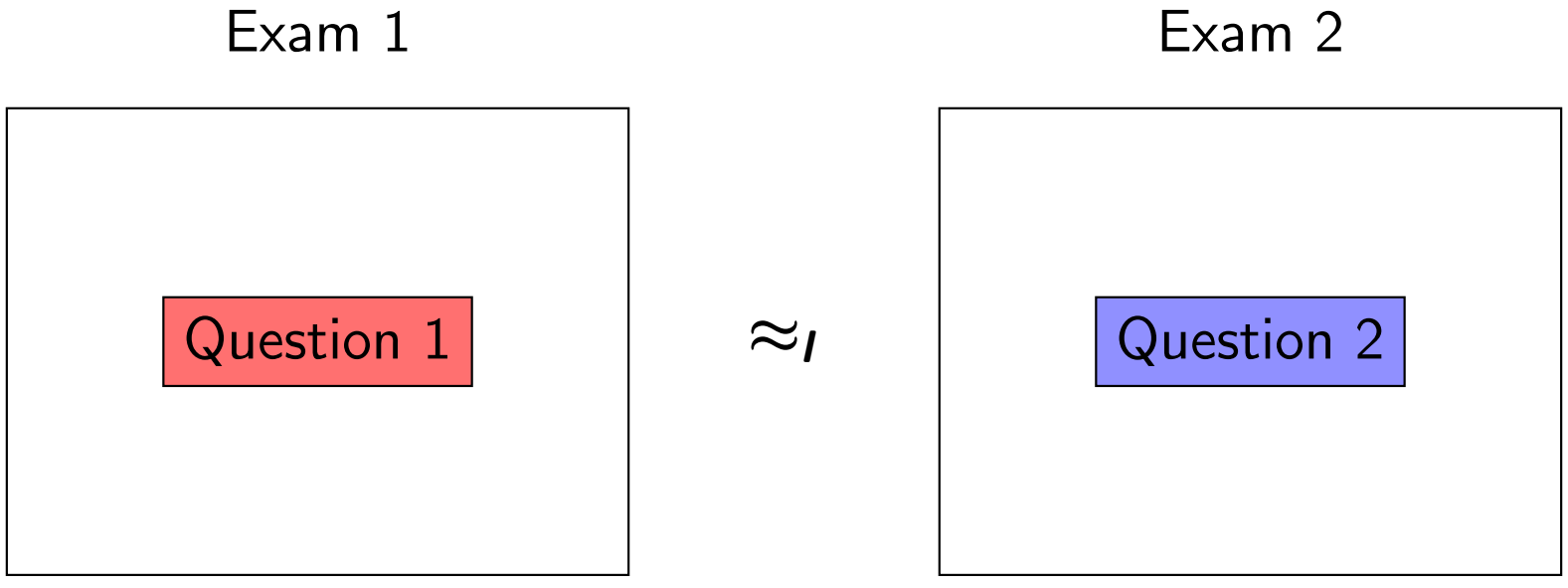


Question Indistinguishability

No premature information about the questions is leaked.

Definition:

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



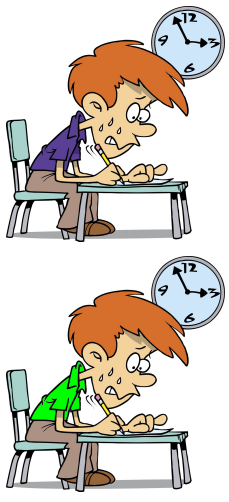
Can be considered with or without dishonest candidates.

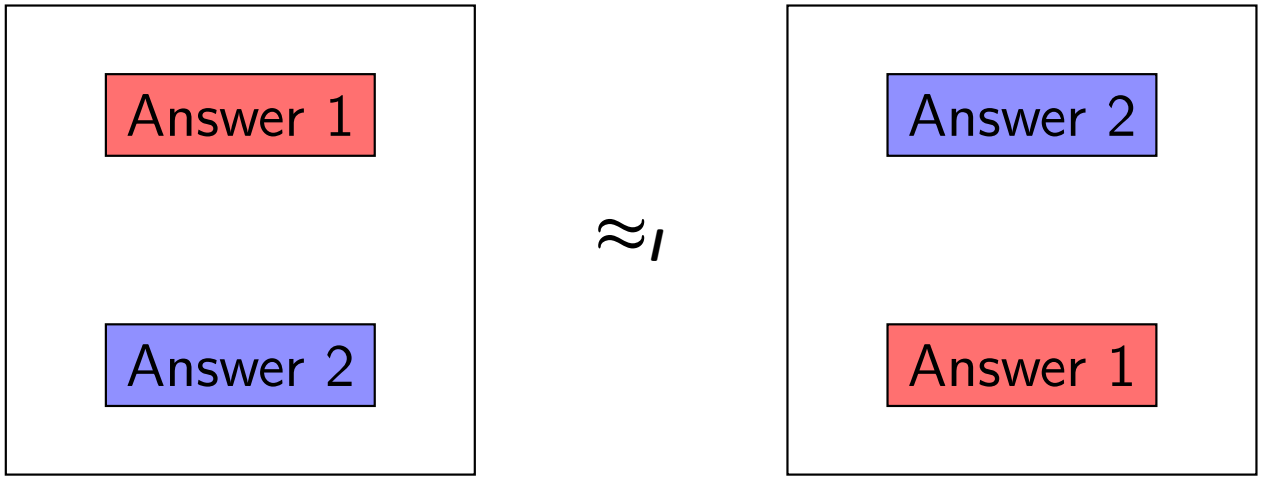
Anonymous Marking

An examiner cannot link an answer to a candidate.

Definition:

Up to the end of marking phase:



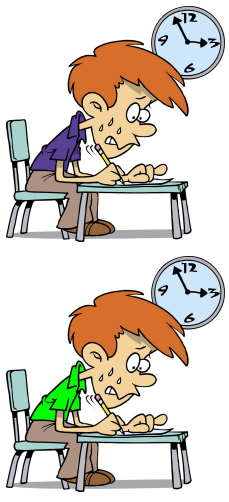


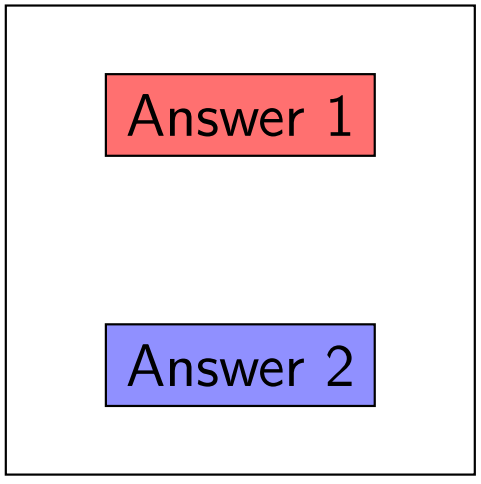
Anonymous Marking

An examiner cannot link an answer to a candidate.

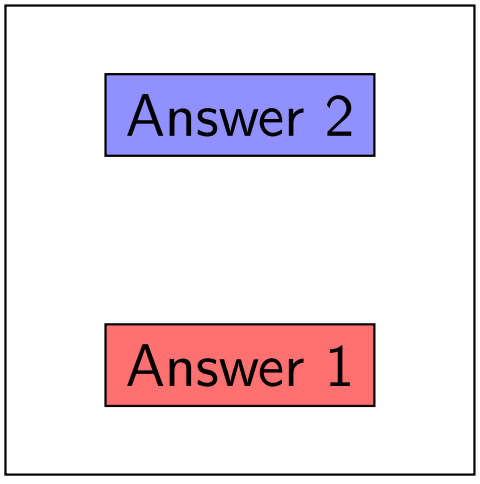
Definition:

Up to the end of marking phase:





$\approx_I$

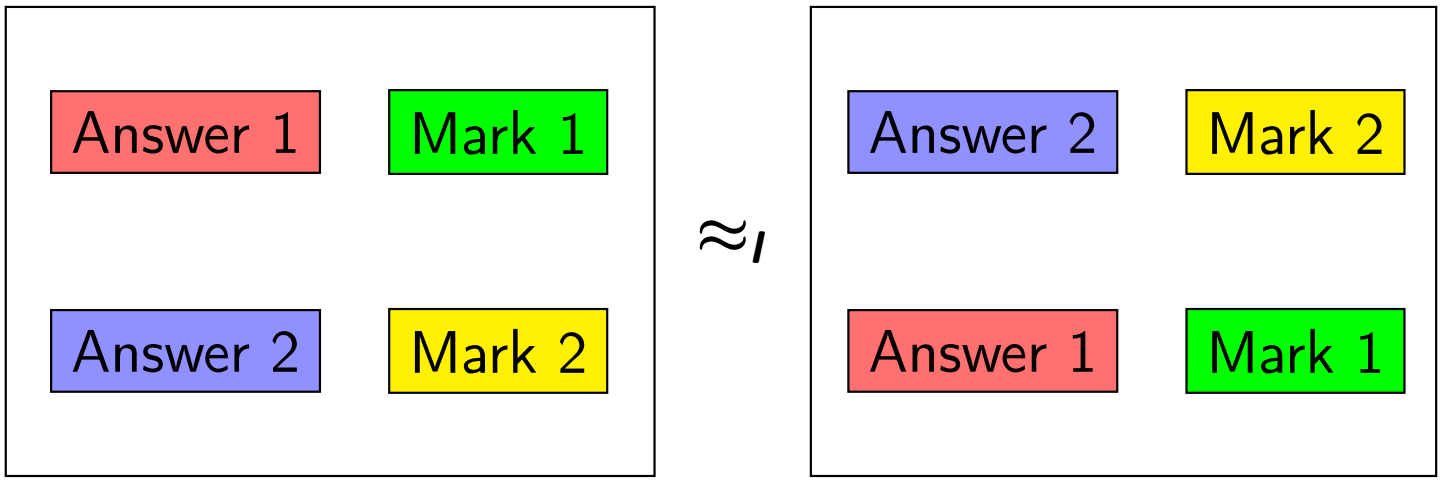


Can be considered with or without dishonest examiners and authorities.

Anonymous Examiner

A candidate cannot know which examiner graded his copy.

Definition:

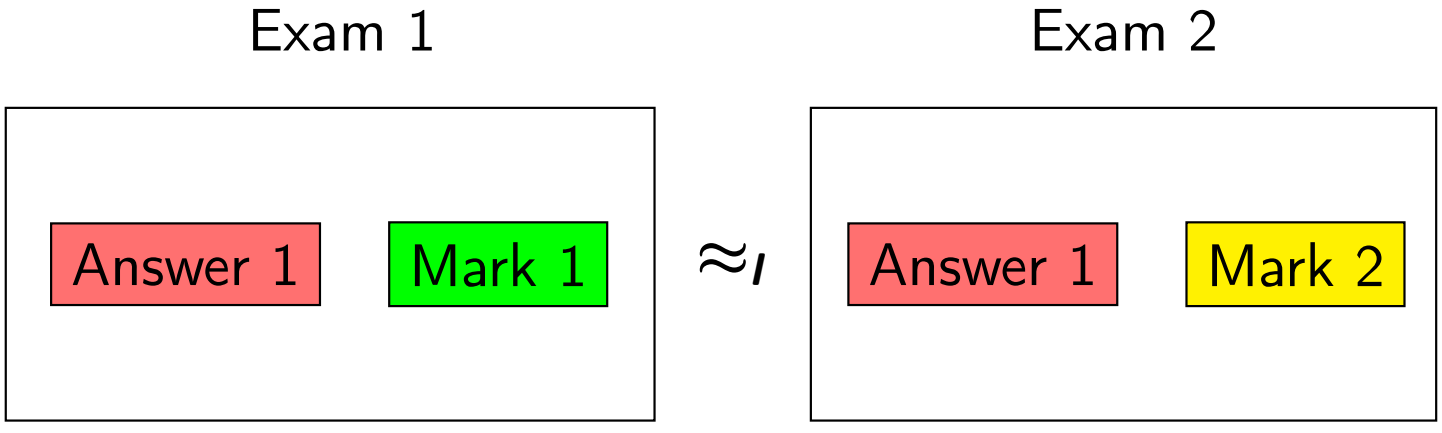


Can be considered with or without dishonest candidates.

Mark Privacy

Marks are private.

Definition:

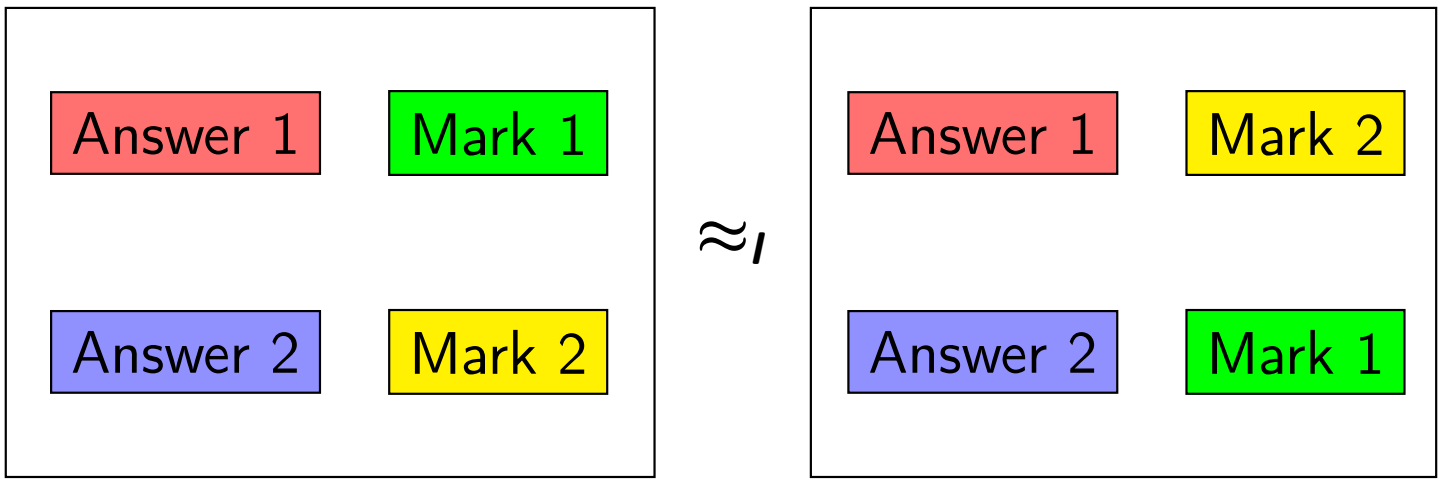


Can be considered with or without dishonest candidates, examiners and authorities.

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

Application: Huszti & Pethő's Protocol

"A Secure Electronic Exam System" [HP10] using

- ElGamal Encryption
- a Reusable Anonymous Return Channel (RARC) [GJ03] 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

Results

Formal Verification with ProVerif [Bla01]:

Property	**Result**	**Time**
Answer Origin Authentication	×	< 1 s
Form Authorship	×	< 1 s
Form Authenticity	×	< 1 s
Mark Authenticity	×	< 1 s
Question Indistinguishability	×	< 1 s
Anonymous Marking	×	8 m 46 s
Anonymous Examiner	×	9 m 8 s
Mark Privacy	×	39 m 8 s
Mark Anonymity	×	1h 15 m 58 s

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.

Plan

Application: Remark! Protocol

A recent protocol [GLR14] using

- ElGamal encryption
- an **exponentiation mixnet** [HS11] 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

Results

Formal Verification with ProVerif:

Property	Result	Time
Answer Origin Authentication	✓	< 1 s
Form Authorship	✓	< 1 s
Form Authenticity	✓[1]	< 1 s
Mark Authenticity	✓	< 1 s
Question Indistinguishability	✓	< 1 s
Anonymous Marking	✓	2 s
Anonymous Examiner	✓	1 s
Mark Privacy	✓	3 m 32 s
Mark Anonymity	✓	-[2]

[1] after fix

[2] implied by Mark Privacy

Plan

Plan

Exam model

Very abstract model:

- Four **sets:**
  - $\{$  $\}$: candidate identities, subset $\{$  $\}_r$ registered candidates
  - $\{$  $\}$: questions, subset $\{$  $\}_g$ correct questions
  - $\{$  $\}$: answers
  - $\{$  $\}$: marks
- Three **relations:**
  - `Accepted` $\subseteq \{$  $\} \times (\{$  $\} \times \{$  $\})$
  - `Marked` $\subseteq \{$  $\} \times (\{$  $\} \times \{$  $\}) \times \{$  $\}$
  - `Assigned` $\subseteq \{$  $\} \times \{$  $\}$
- A **function** `Correct` : $(\{$  $\} \times \{$  $\}) \to \{$  $\}$
- An exam protocol is ***X*-verifiable**, if we have a **sound** and **complete** test for ***X***.

Defining **Individual Verifiability**

Each **candidate** knows

- her identity  ,
- question  ,
- answer  ,
- mark  ,
- and a log  .

Properties:

The candidate can verify that...

- Question Validity: ...she received questions generated by the question committee

$$\mathtt{QV}_{\mathtt{IV}}(\,,\,,\,,\,,\,) \Leftrightarrow (\,\in \{\,\}_g)$$

Defining **Individual Verifiability**

Each **candidate** knows

- her identity  ,
- question  ,
- answer  ,
- mark  ,
- and a log  .

Properties:

The candidate can verify that...

- Question Validity: ...she received questions generated by the question committee

$$\mathtt{QV}_{\mathtt{IV}}(\text{  }, \text{  }, \text{  }, \text{  }, \text{  }) \Leftrightarrow (\text{} \in \{\text{}\}_g)$$

sound & complete

Defining Individual Verifiability Cont'd

The candidate can verify that...

- Marking Correctness: ...the mark attributed to her answer is correct.

$$\mathtt{MC}_{\mathtt{IV}}(\text{  }, ?, !, A^{+}, \text{LOG}) \Leftrightarrow (\mathtt{Correct}(?, !) = A^{+})$$

- Exam-Test Integrity: ...her answer was accepted and marked as submitted.

$$\mathtt{ETI}_{\mathtt{IV}}(\text{  }, ?, !, A^{+}, \text{LOG}) \Leftrightarrow ((\text{  }, (?, !)) \in \mathtt{Accepted} \wedge \exists m' : (\text{  }, (?, !), m') \in \mathtt{Marked})$$

- Exam-Test Markedness: ...her answer was marked.

$$\mathtt{ETM}_{\mathtt{IV}}(\text{  }, ?, !, A^{+}, \text{LOG}) \Leftrightarrow (\exists m' : (\text{  }, (?, !), m') \in \mathtt{Marked}))$$

Defining Individual Verifiability Cont'd

The candidate can verify that...

- Marking Integrity: ...her registered mark is the one assigned by the examiner

$$\mathtt{MI}_{\mathtt{IV}}(\text{  }, \text{  }, \text{  }, \text{  }, \text{  }) \Leftrightarrow \exists m' : \big((\text{  }, (\text{  }, \text{  }), m') \in \mathtt{Marked} \wedge (\text{  }, m') \in \mathtt{Assigned}\big)$$

- Marking Notification Integrity: ...she received the assigned mark

$$\mathtt{MNI}_{\mathtt{IV}}(\text{  }, \text{  }, \text{  }, \text{  }, \text{  }) \Leftrightarrow (\text{  }, \text{  }) \in \mathtt{Assigned}$$

Universal Verifiability

An **outside auditor** only has access to some evidence 

.

The auditor can verify that...

Properties:

- Registration: ...all the accepted answers were submitted by registered candidates.

$$\mathtt{R}_{\mathtt{UV}}(\text{LOG}) \Leftrightarrow \{\text{  }\}_r \supseteq \langle i : (i, x) \in \mathtt{Accepted} \rangle$$

- Marking Correctness: ...all the marks were calculated correctly.

$$\mathtt{MC}_{\mathtt{UV}}(\text{LOG}) \Leftrightarrow \forall (i, x, m) \in \mathtt{Marked}, \mathtt{Correct}(x) = m$$

Universal Verifiability Cont'd

The auditor can verify that...

- Exam-Test Integrity: ...all and **only** accepted test answers were marked.

$$\texttt{ETI}_{\texttt{UV}}(\texttt{LOG}) \Leftrightarrow \texttt{Accepted} = \langle (i, x) : (i, x, m) \in \texttt{Marked} \rangle$$

- Exam-Test Markedness: ...all accepted test answers were marked.

$$\texttt{ETM}_{\texttt{UV}}(\texttt{LOG}) \Leftrightarrow \texttt{Accepted} \subseteq \langle (i, x) : (i, x, m) \in \texttt{Marked} \rangle$$

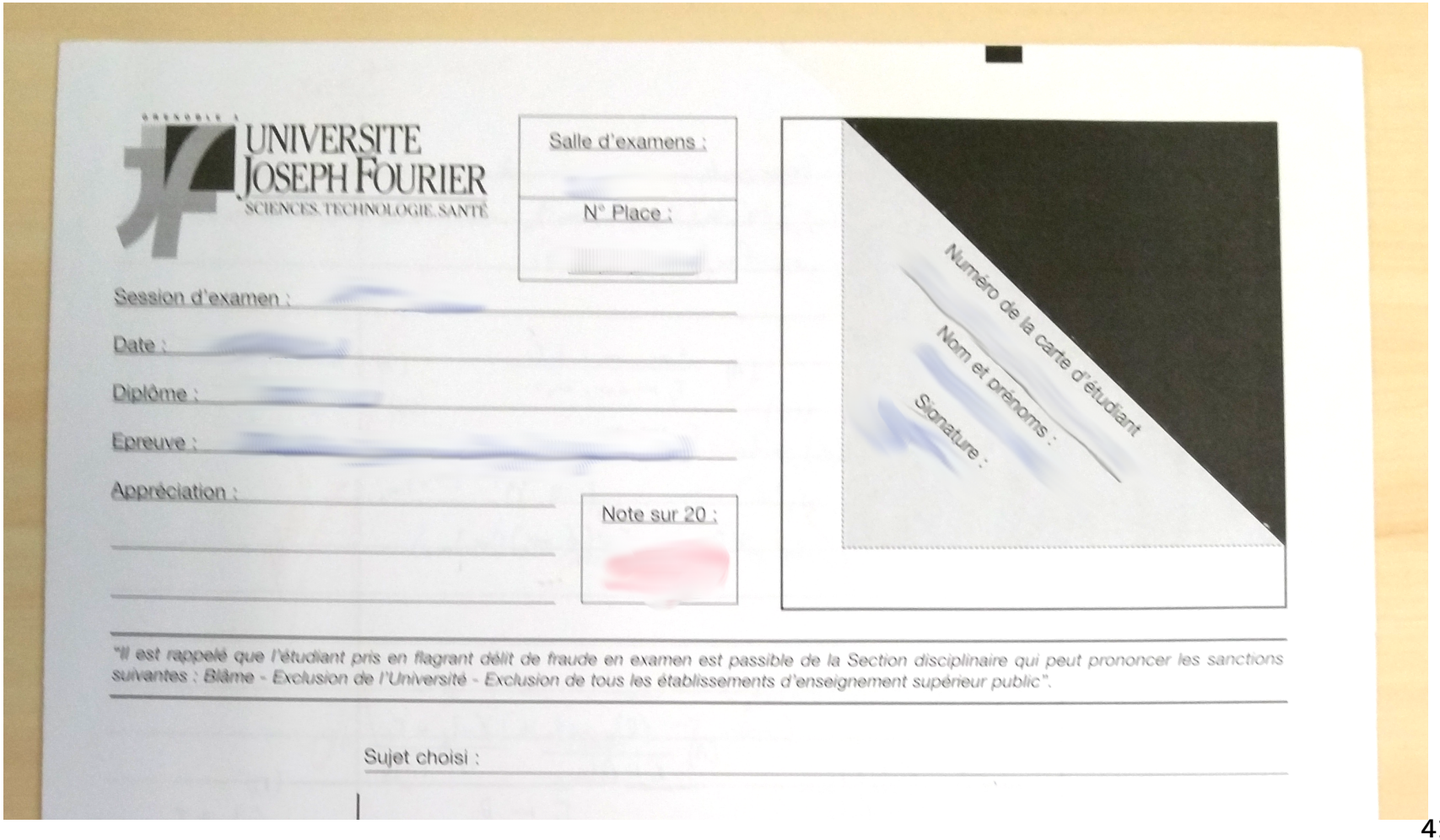
- Marking Integrity: ...all and **only** the marks assigned to test answers were registered.

$$\texttt{MI}_{\texttt{UV}}(\texttt{LOG}) \Leftrightarrow \texttt{Assigned} = \langle (i, m) : (i, x, m) \in \texttt{Marked} \rangle$$

Plan

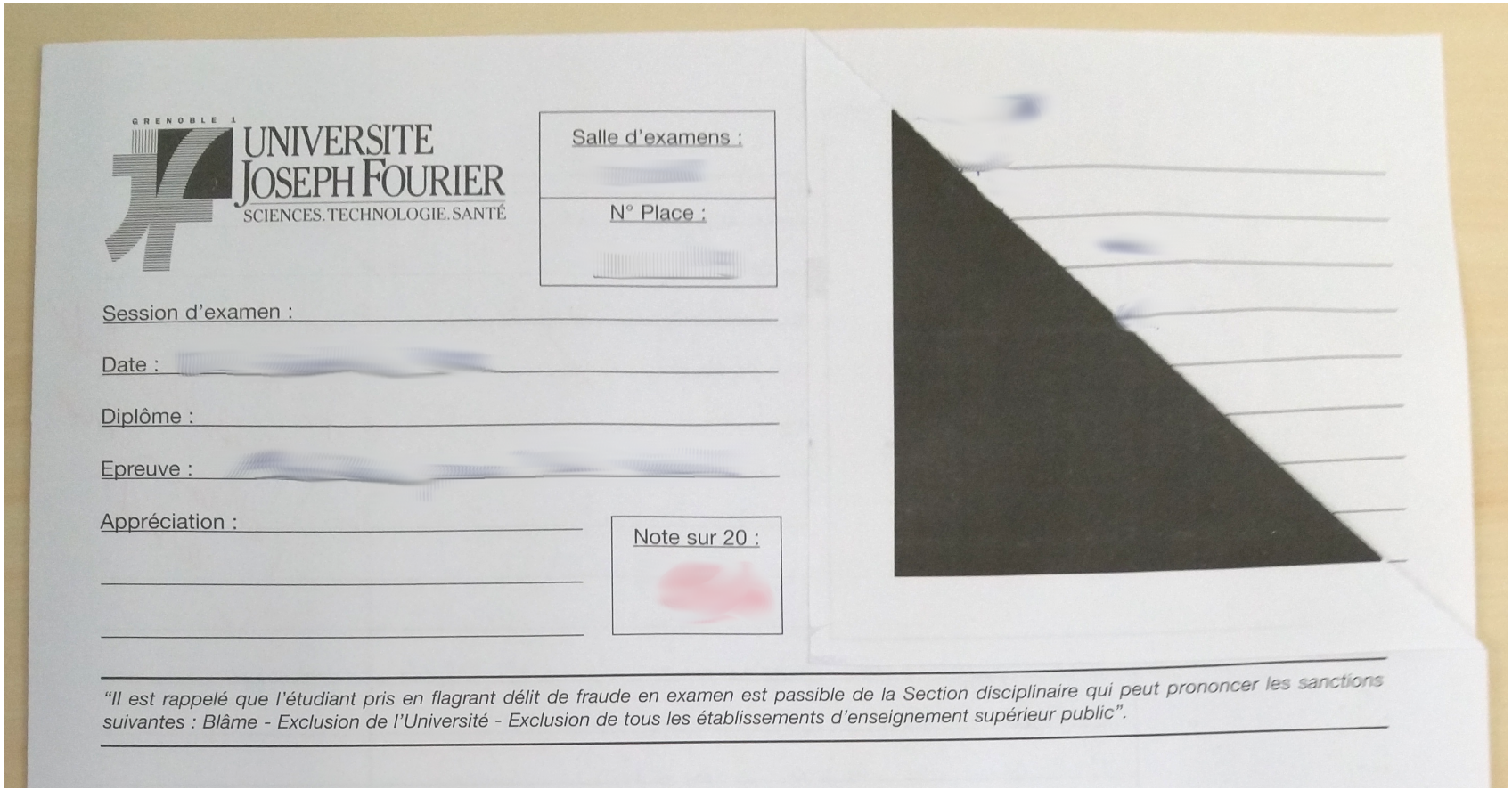
Case Study I: Grenoble Exam

- **Paper-based** exam system at the University Joseph Fourier
- **Goal:** Privacy (Anonymous Marking)
- **Special exam paper** with corner that is folded and glued:



Case Study I: Grenoble Exam

- **Paper-based** exam system at the University Joseph Fourier
- **Goal:** Privacy (Anonymous Marking)
- **Special exam paper** with corner that is folded and glued:


GRENOBLE 1
UNIVERSITE JOSEPH FOURIER
SCIENCES.TECHNOLOGIE.SANTÉ

Salle d'examens :

N° Place :

Session d'examen :

Date :

Diplôme :

Epreuve :

Appréciation :

Note sur 20 :

"Il est rappelé que l'étudiant pris en flagrant délit de fraude en examen est passible de la Section disciplinaire qui peut prononcer les sanctions suivantes : Blâme - Exclusion de l'Université - Exclusion de tous les établissements d'enseignement supérieur public".

Grenoble Exam: Results

Individual Verifiability:

- Input: the candidate's values
- Assumptions: `Correct` is published after the exam, and candidates can consult their copies
- Verification using ProVerif:

Property	Sound	Complete
Question Validity	× (EA)	✓
Test Answer Integrity	× (EA, E)	✓
Test Answer Markedness	× (E)	✓
Marking Correctness	✓	✓
Mark Integrity	× (EA, E)	✓
Mark Notification Integrity	× (EA)	✓

- No guarantee that the records are correct.

Grenoble Exam: Results Cont'd

Universal Verifiability:

- Assumption: the auditor gets access to the EA's and Es' records and the function `Correct`.
- Verification using ProVerif:

Property	Sound	Complete
Registration	× (EA)	✓
Exam-Test Integrity	× (EA, E)	✓
Exam-Test Markedness	× (EA, E)	✓
Marking Correctness	× (E)	✓
Mark Integrity	× (EA, E)	✓

- No guarantee that the records are correct, EA and E can make up fake records as long as they are coherent.

Plan

Remark!: Results

Individual Verifiability:

- Input: the candidate's values and the messages on the bulletin board
- Assumption: `Correct` is published after the exam
- Verification using ProVerif:

Property	Sound	Complete
Question Validity	× (EA)	✓
Test Answer Integrity	✓	✓
Test Answer Markedness	✓	✓
Marking Correctness	× (EA)	✓
Mark Integrity	✓	✓
Mark Notification Integrity	✓	✓

Remark!: Results Cont'd

Universal Verifiability:

- Input: the messages on the bulletin board, the function `Correct`, as well as **additional data from the EA**
- Verification using ProVerif:

Property	**Sound**	**Complete**
Registration	✓	✓
Exam-Test Integrity	✓	✓
Exam-Test Markedness	✓	✓
Marking Correctness	× (EA)	✓
Mark Integrity	✓	✓

Plan

Plan

Event Based Model

Event Based Model

1. Registration

Event Based Model

1. Registration

Register

register( )

Event Based Model

1. Registration

Register

register( )

2. Examination

Event Based Model

1. Registration

Register

register( )

2. Examination

begin( )

Event Based Model

1. Registration

Register

register( )

2. Examination

begin( )

get(, ?)

Question

Event Based Model

1. Registration

Register

register( )

2. Examination

begin( )

get(,)

Question

change(, ,)

Event Based Model

1. Registration

Register

register( )

2. Examination

begin( )

get(, ?)

Question

change(, ? , !)

submit(, ? , !)

Answer

accept(, ? , !)

Event Based Model

1. Registration

Register

register( )

2. Examination

begin( )

get(, ?)

Question

change(, ? , !)

submit(, ? , !)

Answer

accept(, ? , !)

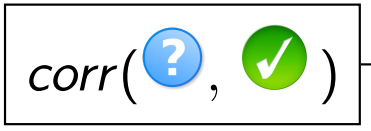
end( )

Event Based Model

3. Marking

Event Based Model

3. Marking



Correct Answer

Event Based Model

3. Marking

corr( ,)

Correct Answer

Evaluation

mark( ,  ,  , )

Event Based Model

3. Marking

corr( ,)

Correct Answer

Evaluation

mark( ,  ,  , )

4. Notification

Event Based Model

3. Marking

corr( ,)

Correct Answer

Evaluation

mark( ,  ,  , )

4. Notification

Mark

assign( , )

Plan

Quantified Event Automata (QEAs)

- Properties expressed as **QEAs**: **event automaton** with quantified variables.
- An event automaton is a **finite-state machine** with transitions labeled by parametric events.
- Transitions may include **guards** and **assignments**.
- We extend the initial definition of QEAs by:
  1. variable declaration and **initialization** before reading the trace
  2. **global variable** shared among all event automaton instances.
     - $event(parameters)\frac{[guard]}{assignment}$

Candidate Eligibility

No answer is accepted from an unregistered candidate

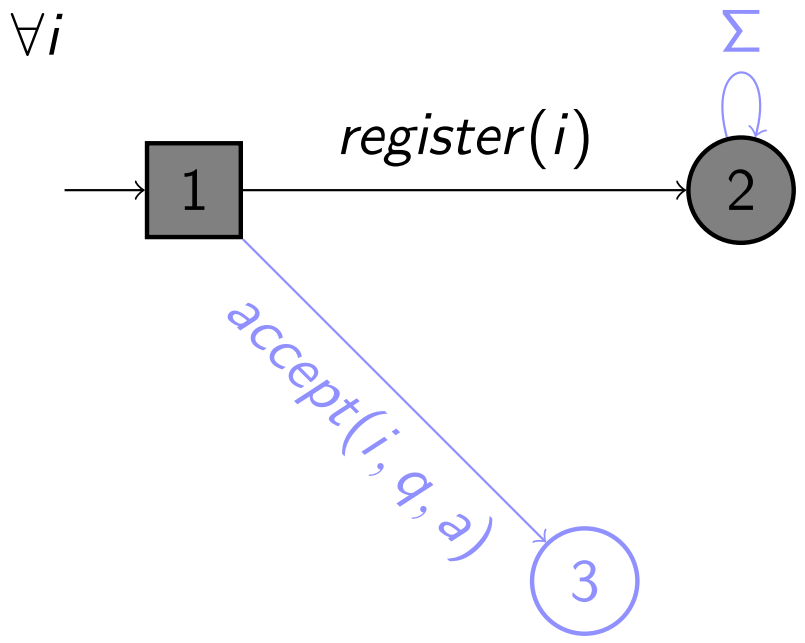
$$\Sigma = \{register(i), accept(i, q, a)\}$$

$\forall i$

Candidate Eligibility

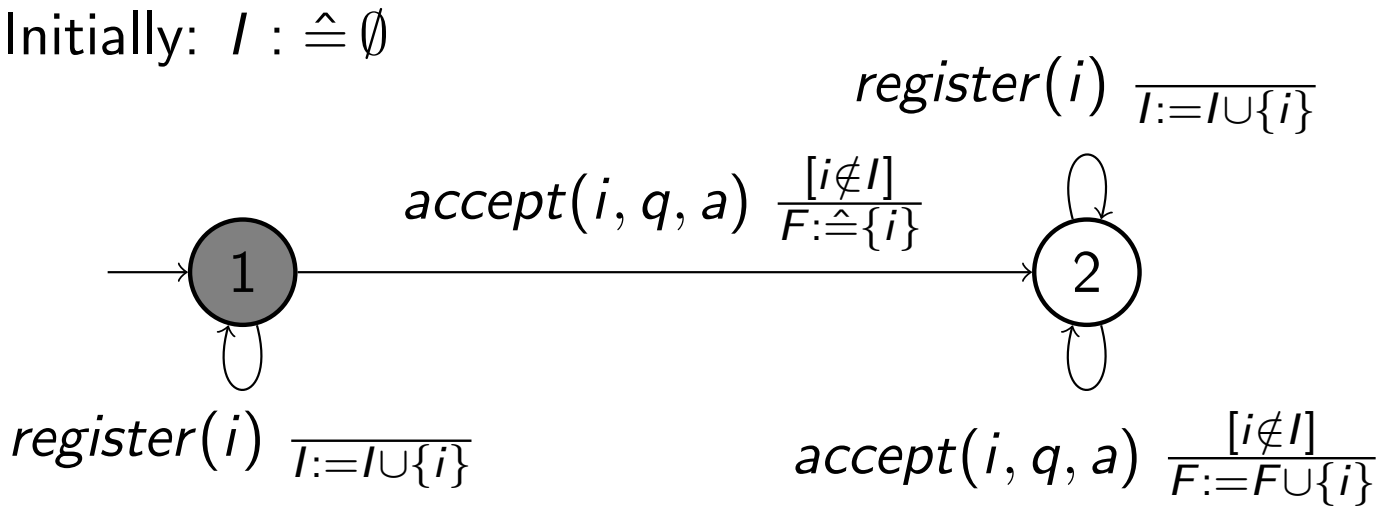
No answer is accepted from an unregistered candidate

$$\Sigma = \{register(i), accept(i, q, a)\}$$



Candidate Eligibility with Auditing

All candidates that violates the requirement are collected in a set F.



Properties

Candidate Registration: an unregistered candidate tried to take the exam.

Properties

Candidate Registration: an unregistered candidate tried to take the exam.

Answer Authentication:

- an unsubmitted answer was considered as accepted; or
- more than one answer were accepted from a candidate.

Properties

Candidate Registration: an unregistered candidate tried to take the exam.

Answer Authentication:

- an unsubmitted answer was considered as accepted; or
- more than one answer were accepted from a candidate.

Questions Ordering:

- a candidate got a question before validating the previous ones.

Properties (continued)

Exam Availability: an answer was accepted outside exam time.

Properties (continued)

Exam Availability: an answer was accepted outside exam time.

Exam Availability with Flexibility:

- supports different duration and starting time between candidates.

Properties (continued)

Exam Availability: an answer was accepted outside exam time.

Exam Availability with Flexibility:

- supports different duration and starting time between candidates.

Marking Correctness: an answer was marked in a wrong way.

Properties (continued)

Exam Availability: an answer was accepted outside exam time.

Exam Availability with Flexibility:

- supports different duration and starting time between candidates.

Marking Correctness: an answer was marked in a wrong way.

Mark Integrity:

- an accepted answer was not marked; or
- a candidate was not assigned the corresponding mark.

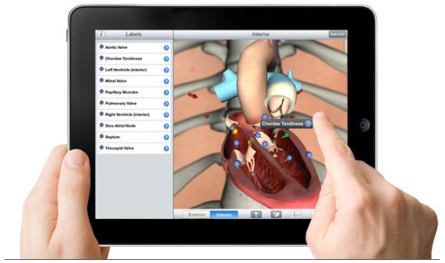
Plan

E-exam at Université Joseph Fourier (UJF)

Registration:

- 2 weeks before the exam.
- Using login/password.

E-exam at Université Joseph Fourier (UJF)



Examination in a supervised room

Authentication and answers questions as follows:

- In a fixed order.
- Once validates the current question, he gets the next one.
- He can change the answer unlimited times before validating.
- Once he validates, then he cannot go back and change any of the validated answers.

E-exam at Université Joseph Fourier (UJF)

Marking:

- For each question, the professor specifies the correct answer(s).
- For each question, all the answers provided by the candidates are collected.
- Each answer is evaluated by an examiner to 0 or 1.
- The mark for each candidate is calculated as the summation of all the scores attributed to his answers.

Notification:

- The marks are notified to the candidates.
- A candidate can consult his submission and check the marking.

Analysis

Verification of two real e-exam executions using MarQ tool [RCR15].

From the logs: $register(i)$, $change(i, q, a)$, $submit(i, q, a)$, $accept(i, q, a)$.

4 Properties

- Candidate Registration
- Candidate Eligibility
- Answer Authentication
- Exam Availability

5 new properties

- Answer Authentication *:
  - All accepted answers are submitted by candidates.
  - **Allow the acceptance of the same answer again**.
  - **But, still forbids the acceptance of a different answer**.

5 new properties

- Answer Authentication *:
  - All accepted answers are submitted by candidates.
  - **Allow the acceptance of the same answer again**.
  - **But, still forbids the acceptance of a different answer**.
- Answer Authentication Reporting: Collects in a set F every candidate from which more than one answer are accepted.

5 new properties

- Answer Authentication *:
  - All accepted answers are submitted by candidates.
  - **Allow the acceptance of the same answer again**.
  - **But, still forbids the acceptance of a different answer**.
- Answer Authentication Reporting: Collects in a set F every candidate from which more than one answer are accepted.
- Answer Editing: A candidate cannot change an answer after validation it.

5 new properties

- Answer Authentication *:
  - All accepted answers are submitted by candidates.
  - **Allow the acceptance of the same answer again**.
  - **But, still forbids the acceptance of a different answer**.
- Answer Authentication Reporting: Collects in a set F every candidate from which more than one answer are accepted.
- Answer Editing: A candidate cannot change an answer after validation it.
- Question Ordering *: A candidate cannot changes the answer to a future question before validating the current question.

5 new properties

- Answer Authentication *:
  - All accepted answers are submitted by candidates.
  - **Allow the acceptance of the same answer again**.
  - **But, still forbids the acceptance of a different answer**.
- Answer Authentication Reporting: Collects in a set F every candidate from which more than one answer are accepted.
- Answer Editing: A candidate cannot change an answer after validation it.
- Question Ordering *: A candidate cannot changes the answer to a future question before validating the current question.
- Acceptance Order: A candidate has to validate the questions in order, but he can skip some questions.

Results: Exam 1

233 students, 40875 events

Property	Result	Time (ms)
Candidate Registration	✓	538
Candidate Eligibility	✓	517
Answer Authentication	×	310
Exam Availability	✓	518
Answer Authentication *	✓	742
Answer Authentication Reporting	×[1]	654
Answer Editing	✓	641
Question Ordering *	×	757
Acceptance Order	✓	697

Results: Exam 2

90 students, 4641 events

Property	Result	Time (ms)
Candidate Registration	✓	230
Candidate Eligibility	✓	214
Answer Authentication	✓	275
Exam Availability	×[1]	237
Answer Authentication *	✓	223
Answer Authentication Reporting	✓	265
Answer Editing	×	218
Question Ordering *	×	389
Acceptance Order	✓	294

Plan

Conclusion

- Formal model for security and verifiability
- Security Analysis of 2 e-exams and one “real” exam
- Trust parties are required for verifiability
- Monitoring analysis of 2 real e-exams at UJF using MarQ tool
- Discovering some misbehaviours and flaws

Conclusion

- Formal model for security and verifiability
- Security Analysis of 2 e-exams and one “real” exam
- Trust parties are required for verifiability
- Monitoring analysis of 2 real e-exams at UJF using MarQ tool
- Discovering some misbehaviours and flaws

Designing secure protocols is difficult

Conclusion

- Formal model for security and verifiability
- Security Analysis of 2 e-exams and one “real” exam
- Trust parties are required for verifiability
- Monitoring analysis of 2 real e-exams at UJF using MarQ tool
- Discovering some misbehaviours and flaws

Designing secure protocols is difficult

Use formal methods !

Future Work

- Analyze more existing e-exams from other universities.
- Perform on-line verification with our monitors during live e-exams.
- Study more expressive and quantitative properties that can detect colluded students through similar answer patterns.
- Automatic transformation from verifiability to monitors.

Thank you for your attention!

Questions?

pascal.lafourcade@udamail.fr


M. Abadi and C. Fournet.
Mobile values, new names, and secure communication.
In *POPL*, pages 104–115. ACM, 2001.


Bruno Blanchet.
An efficient cryptographic protocol verifier based on prolog rules.
In *CSFW*, pages 82–96. IEEE Computer Society, 2001.


P. Golle and M. Jakobsson.
Reusable anonymous return channels.
In *Proc. of the 2003 ACM workshop on Privacy in the electronic society*, WPES '03, pages 94–100, New York, NY, USA, 2003. ACM.


R. Giustolisi, G. Lenzini, and P.Y.A. Ryan.
Remark!: A secure protocol for remote exams.
In *Security Protocols XXII*, LNCS. Springer, 2014.

to appear. Draft
http://apsia.uni.lu/stast/codes/exams/preSPW14.pdf.


A. Huszti and A. Pethő.
A secure electronic exam system.
Publicationes Mathematicae Debrecen, 77:299–312, 2010.


R. Haenni and O. Spycher.
Secure internet voting on limited devices with anonymized dsa public keys.
In *Proc. of the 2011 Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*, EVT/WOTE'11. USENIX, 2011.


Giles Reger, Helena Cuenca Cruz, and David E. Rydeheard.
MarQ: Monitoring at runtime with QEA.
In *Tools and Algorithms for the Construction and Analysis of Systems - 21st International Conference, TACAS, London, UK*, pages 596–610, 2015.