A Framework for Analyzing Verifiability in Traditional and Electronic Exams

Jannik Dreier[1], Rosario Giustolisi[2], Ali Kassem[3], Pascal Lafourcade[4] and Gabriele Lenzini[2]

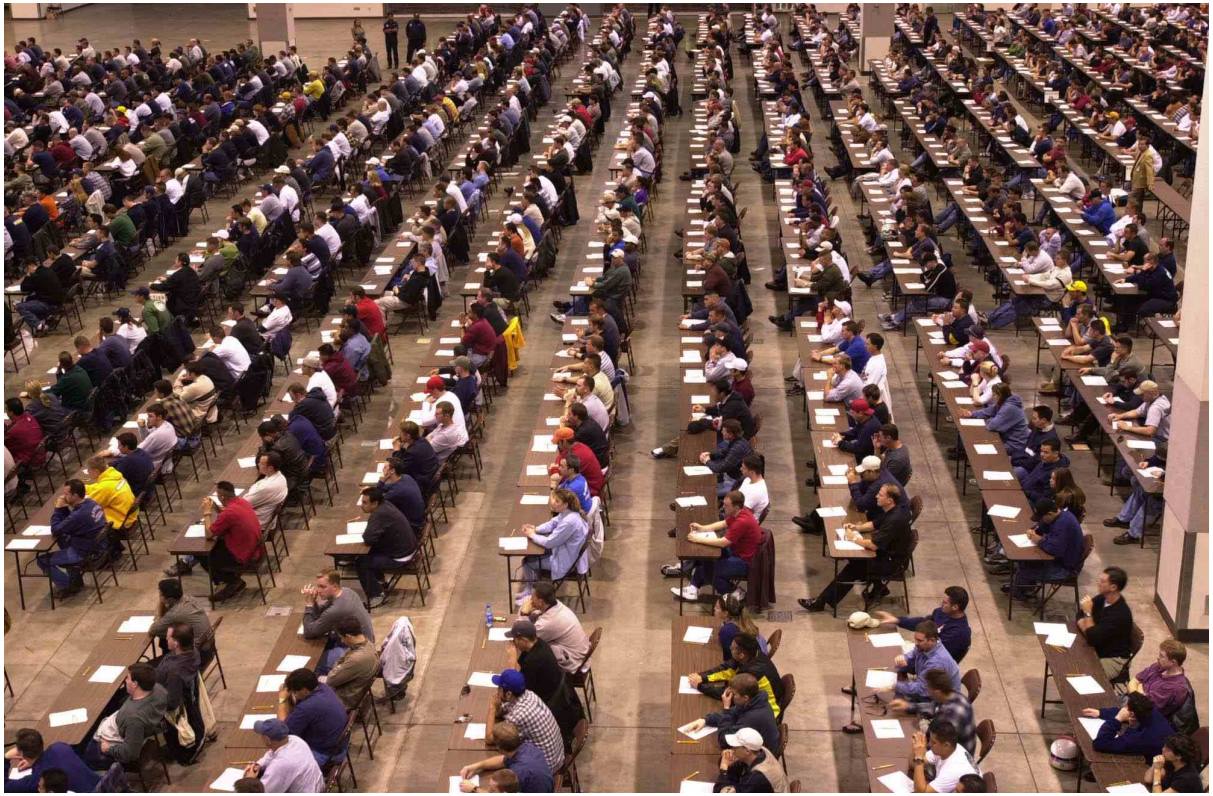
[1]Institute of Information Security, ETH Zurich
[2]SnT/University of Luxembourg
[3]Université Grenoble Alpes, CNRS, VERIMAG
[4]University d'Auvergne, LIMOS

11th Information Security Practice & Experience Conference
Beijing, 8th May 2015

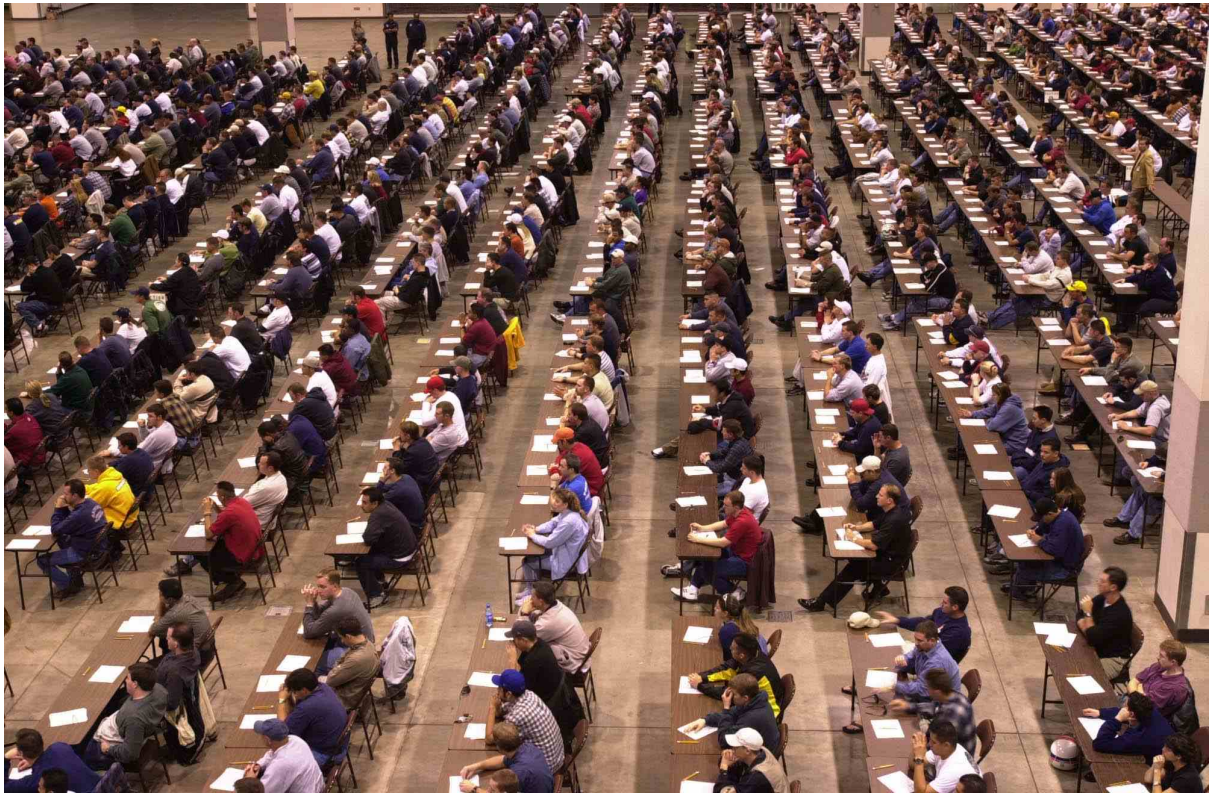
Exam

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

Exam



Exam



Electronic Exam: Information technology for the assessment of knowledge and skills.

Exam

- Evaluation of individuals
  - Educational assement
  - Skills test
  - Personnel selection
  - Project proposal
  - Public tender
  - Competition (e.g., games)
- Evaluation of groups
  - Organization performances
  - Country benchmarks
  - Societal census

Exam: Players and Organization

Roles:

Candidate

Exam Authority

Exam: Players and Organization

Roles:

Candidate

Exam Authority

Question Committee

Invigilator

Examiner

...

Exam: Players and Organization

Roles:

Candidate

Exam Authority

Question Committee

Invigilator

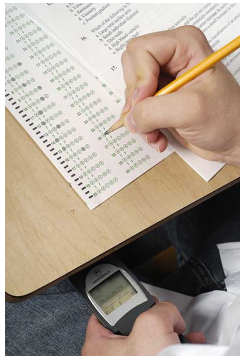
Examiner

...

Four Phases:

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

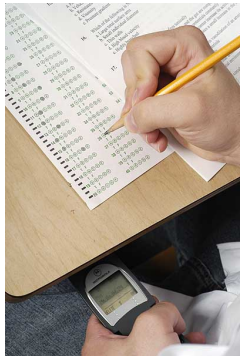
Threats. . .



- Candidate cheating
- Corrupted exam authority
- Unfair examiners
- Outside attackers

  - Data integrity
  - Fair marking
  - Privacy leaks

Threats. . .



- Candidate cheating
- Corrupted exam authority
- Unfair examiners
- Outside attackers

- Data integrity
- Fair marking
- Privacy leaks

Real Threats!

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

. . . and their Mitigation

Exam protocols employ some countermeasures mostly focusing on **student cheating**:

- Exam centres

- Software solutions, e.g. ProctorU

ProctorU
Real People.
Real Proctoring.

. . . and their Mitigation

Exam protocols employ some countermeasures mostly focusing on **student cheating**:

- Exam centres

- Software solutions, e.g. ProctorU

ProctorU
Real People.
Real Proctoring.

Can we prevent exam frauds?

Towards Verifiability

Probably not. But we can check for the presence of irregularities.

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

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

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.

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

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

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

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

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

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.

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

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

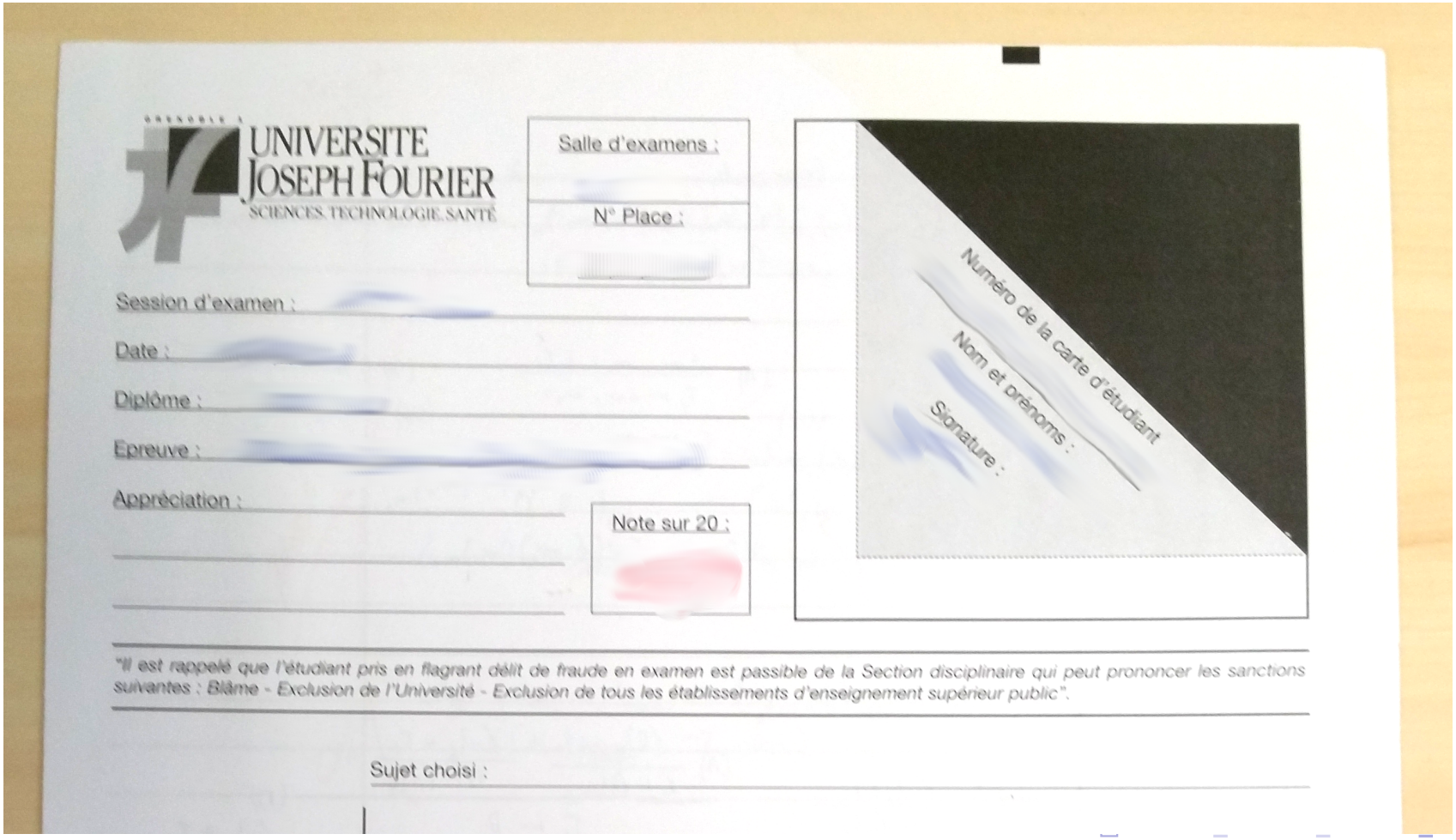
$$\mathtt{ETM}_{\mathtt{UV}}(\text{LOG}) \Leftrightarrow \mathtt{Accepted} \subseteq \langle (i, x) : (i, x, m) \in \mathtt{Marked} \rangle$$

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

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

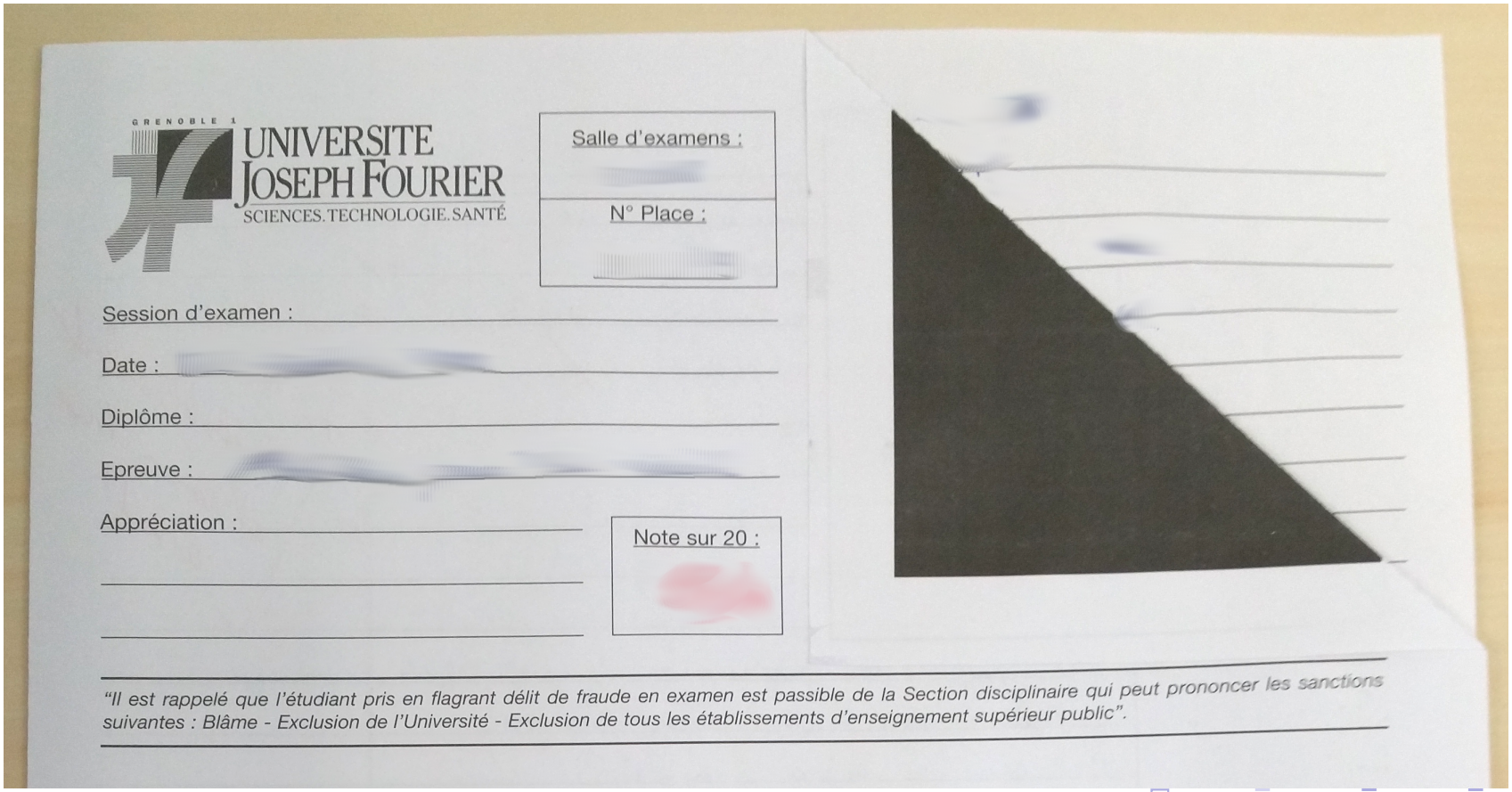
Case Study I: Grenoble Exam

- **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 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.

Case Study II: Remark!

Goal

- Authentication
  - signatures
- Privacy
  - ElGamal encryption
  - an exponentiation mixnet to create pseudonyms based on the parties' public keys
    $\Rightarrow$ allows to encrypt and sign anonymously
- **Verifiability**
  - a public append-only bulletin board

Assumptions

- The model answers are kept secret from the candidate until after the examination.
- At least one mix server is honest.

Remark!: Exponentiation Mixnet

Input				$\cdots$	**Output**
PK_1^0	$(PK^0_{\pi_1(1)})^{r_1} =: PK_1^1$		$(PK^1_{\pi_2(1)})^{r_2} =: PK_1^2$	$\cdots$	$(PK^0_{\pi(1)})^{\overline{r}}$
PK_2^0	$(PK^0_{\pi_1(2)})^{r_1} =: PK_2^1$		$(PK^1_{\pi_2(2)})^{r_2} =: PK_2^2$	$\cdots$	$(PK^0_{\pi(2)})^{\overline{r}}$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
PK_n^0	$(PK^0_{\pi_1(n)})^{r_1} =: PK_n^1$		$(PK^1_{\pi_2(n)})^{r_2} =: PK_n^2$	$\cdots$	$(PK^0_{\pi(n)})^{\overline{r}}$
g	g^{r_1}		g^{r_2}		$g^{\overline{r}} =: h_C$

where $\overline{r} = \prod_{i=1}^{k} r_i$ and $\pi = \pi_1 \circ \pi_2 \circ \cdots \circ \pi_k$

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	✓	✓

Conclusion

- General framework to analyse both electronic and traditional exam protocols
- Formal verification in ProVerif of most properties
  - Traditional exam: Grenoble
  - Electronic exam: Remark!
- Manual proofs needed for few properties

Future and Ongoing Work

- Design fully verifiable protocols
- CryptoVerif
- Accountability

Thanks!

Questions?