A privacy preserving electronic submission process

Jon Callas
PGP
USA

Yvo Desmedt
BT Chair of Information Security
University College London, UK

August 19, 2008

1. INTRODUCTION

IACR is modernizing, e.g.:

- switched from paper submissions (1980's, 1990's) to electronic (today),
- considering to use techniques developed by researchers, e.g., for: e-voting.

Can we use some of our tools for improving our conferences, submission process, etc.?

2. TODAY'S SYSTEM

Today's system leaks your paper. Worse, it leaks it to experts (i.e., competitors) in your area!

Even if we trust them, we have no guarantee that it will not influence the unconscious mind of the referee.

So, privacy is a concern. However, how to check the paper is worth accepting.

3. A FIRST PROPOSAL

Idea: the authors make a zero-knowledge proof that their paper is worth accepting.

How? Anything is provable in zero-knowledge!(?)

3. A FIRST PROPOSAL

Idea: the authors make a zero-knowledge proof that their paper is worth accepting.

How? Anything is provable in zero-knowledge!(?)

Problem: What if too many papers worth accepting???

4. A SECOND PROPOSAL

Trivially: We need secure multiparty computation.

4. A SECOND PROPOSAL

Trivially: We need secure multiparty computation.

No: not so trivial! Questions:

- How to compare acceptable papers? Do we need AI???

4. A SECOND PROPOSAL

Trivially: We need secure multiparty computation.

No: not so trivial! Questions:

- How to compare acceptable papers? Do we need AI???
- Who are the participants:
  - The people who submit, and
  - the people of the program committee (what is their task in such an automated system?)

4. A SECOND PROPOSAL

Trivially: We need secure multiparty computation.

No: not so trivial! Questions:

- How to compare acceptable papers? Do we need AI???
- Who are the participants:
  - The people who submit, and
  - the people of the program committee (what is their task in such an automated system?)
  - However, we also have the audience, which we do not know in advance who they will be!! So secure multiparty computation with unknown participants???

- Who are the adversaries?

5. Voting aspect

We are in the Voting mini-session. A link?

Today the program committee votes. In a automated system, the question will be what are the criteria? Possible answers:

5. VOTING ASPECT

We are in the Voting mini-session. A link?

Today the program committee votes. In a automated system, the question will be what are the criteria? Possible answers:

- Most scientifically challenging papers are accepted,
- Papers most interesting for the expected audience will be accepted,
- or a mix.
- Easy criteria: minimum & maximum number of papers

6. Research Issues

Due to the state of the art of AI, above will likely not be possible for a long time.

However, we hope you will come up with an intermediate submission process which has a better scientific justification than the current one, e.g., from a privacy viewpoint.