Sharemind: (possibly) the world's fastest solution for privacy-preserving computations

Dan Bogdanov and Sven Laur

September 12, 2007
The ”problem” of privacy

- Information about someone's medical, financial or political status is considered private.
The "problem" of privacy

- Information about someone's medical, financial or political status is considered private.
- There are people who want to process it for legitimate purposes.
The "problem" of privacy

▶ Information about someone's medical, financial or political status is considered private.
▶ There are people who want to process it for legitimate purposes.
▶ The privacy protection law restricts them from such processing.
The "problem" of privacy

- Information about someone's medical, financial or political status is considered private.
- There are people who want to process it for legitimate purposes.
- The privacy protection law restricts them from such processing.
- How could they process the data without breaking privacy?
What Doesn’t Work?

- Just taking out the name of the person doesn’t help.
What Doesn’t Work?

- Just taking out the name of the person doesn’t help.
- What if the following attributes are still available?
  - home_town
  - number_of_children
  - monthly_income
What Doesn’t Work?

- Just taking out the name of the person doesn’t help.
- What if the following attributes are still available?
  - home_town
  - number_of_children
  - monthly_income
- Some attributes might determine the person for people with additional information!
What works?

- The data analyst won’t see the data at all - only results.
What works?

- The data analyst won’t see the data at all - only results.
- Modern cryptography allows us to do just that.
What works?

► The data analyst won’t see the data at all - only results.
► Modern cryptography allows us to do just that.
► Combining secret sharing and secure multi-party computation we can work on data without seeing it.
What works?

- The data analyst won’t see the data at all - only results.
- Modern cryptography allows us to do just that.
- Combining secret sharing and secure multi-party computation we can work on data without seeing it.
- We are developing a ”private computer” to make such data processing practical.
What You could do

- There are practical tasks...
  - developing the framework for privacy-preserving applications
  - developing the actual applications
  - requires (and improves!) C++ programming skills

- ...which go hand-in-hand with the theoretical ones
  - analysing the security of such applications
  - optimising the performance of our implementation
  - proving the security of our implementation
  - requires (and improves!) some computer science skills

- I’m interested in working with you also after the seminar, as some topics are suitable for bachelors/masters work.
More information:

- The webpage is under construction(TM)
  - you can help with that too, but outside the scope of the seminar
- Currently I’m the source of all relevant information
  - and my e-mail is db@math.ut.ee