Selected Topic in Cryptography

Sven Laur

September 11, 2007
I propose three topics

- A practical proof system for cryptographic protocol design
- Classical results about zero-knowledge in modern terms
- Hash proofs and security of Cramer-Shoup cryptosystem

These topics are difficult but they...

- teach you a lot about cryptography and scientific writing
- can be naturally extended to bachelor or master thesis

Since I’m abroad...

- You must be motivated and independent
- You must know how to use e-mail and Skype
- You must send me a progress report each week
A Practical proof system...

Ideal outcome
- A formal proof system with a graphical user interface that can be used to construct and verify various cryptographic proofs.

Practical outcome ($BSc \rightarrow MSc \rightarrow PhD$)
- A system that can handle simple cryptographic proofs.
- A system that student can use in cryptography courses.

Is it possible at all? Yes, since...
- cryptographic proofs are just syntactic transformations of programs and these transformations are well documented.
- the system **only** verifies proofs and **does not** derive them.
A Practical proofsystem...

What do you need to complete the task?

- Basic knowledge about proof systems (Introduction to logic)
- Basic knowledge about (syntax) trees and tree manipulations
- Basic knowledge about probabilities and cryptography
  (Essentially, you must comprehend Chapters 2 and 3 in http://www.tcs.hut.fi/ slaur/thesis/)
- Good programming skills in C++/Java
  (For various reasons solutions in Haskell, LISP or ML are not acceptable)

Why should you bother at all?

- It is an assignment with a guaranteed practical outcome.
- It provides you a natural ladder up to PhD.
- It is state of the art subject in cryptography.
- It allows you to do practical and theoretical research.
Classical results about zero-knowledge...

Ideal outcome
▶ An good educational treatment of zero knowledge.
▶ All results must be given in the exact security model.

Practical outcome
▶ A course report and possibly a MSc thesis.

What do you need to complete the task?
▶ You must read, understand and rewrite many classical results.
▶ It is difficult but doable and you learn a lot during the process.

(Ask Liina Kamm, she can tell how difficult such process is and what does it give to you.)
Classical results about zero-knowledge...

Articles to read

▶ Goldreich, O.; Micali, S. & Wigderson, A. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems J. ACM, ACM Press, 1991, 38, 690-728.
Hash proofs and Cramer-Shoup...

Ideal outcome

- Simple explanation what is a hash proof.
- An proof that Cramer-Shoup cryptosystem is CCA2 secure.
- All results must be given in the exact security model.

Practical outcome

- A course report and possibly a MSc thesis.

What do you need to complete the task?

- You must read, understand and rewrite many classical results.
- It is difficult but doable and you learn a lot during the process.

(Ask Liina Kamm, she can tell how difficult such process is and what does it give to you.)
Hash proofs and Cramer-Shoup...

Some articles to start the further research