Project
INSE 6110: Foundations of Cryptography
Due: Last class, but no Late Penalty for Submission anytime before the Final Exam

1  Paper

Choose one of the topics below. You may suggest other topics (either as a survey or a novel contribution), but they must be approved by me. Projects are to be done individually. Once again, you may suggest a group project but it must be approved by me.

For this project, research the topic and write a short-paper (max 6 pages) explaining the subject, with references to the related literature. A template you may use (LaTeX and Word available) is available here:

http://www.springer.com/computer/lncs?SGWID=0-164-6-793341-0

You are not obliged to use it, however many papers are published in this template, and so it is useful to learn.

Your paper should summarize the subject with an introduction, explaining very clearly what the research problem is and how the subject addresses it. It should also explain the subject in technical detail.

To find resources on the subject, use Google and try scholar.google.com to find relevant research papers. Wikipedia is another useful resource, however you must not copy it or any source verbatim. A final useful resource is the Encyclopedia of Encryption and Security (PDF available on the campus network):


When using these resources, you should look at the sources they themselves cite to discover the relevant sources. Be sure to cite at sources you use. Review Concordia’s plagiarism policy and if you have any questions or doubts, you can ask me.

http://www.concordia.ca/students/academic-integrity/plagiarism.html

2  Topics

Cryptographic Primitives

• Bitcoin
• Oblivious Transfer
• Visual Cryptography
• Garbled Circuits
• Mix Networks
• Dining Cryptographers
• Group Signatures
• Ring Signatures
• Blind Signatures
• GCM Mode of Operation
• Identity-based Cryptography
• Attribute-based Encryption
• Fully Homomorphic Encryption
• Post-Quantum Cryptography
• Timed-Release Encryption
• Direct Anonymous Attestation (used by TPMs)
• Secure Time-stamping
• Cryptographic Accumulators
• Perfectly Secure Message Transmission
• Fair Exchange
• Universal Composability
• Off-the-Record Messaging

Cryptanalysis and Attacks
• Differential Cryptanalysis
• Boomerang Attack
• Biclique Cryptanalysis

News-worthy Events
• BEAST attack on SSL/TLS
• CRIME attack on SSL/TLS
• Lucky 13 attack on SSL/TLS
• Misuse of CBC-MAC by Mega
• RC4 biases in SSL/TLS
• AACS encryption for Blu-ray
• NSA backdoor in Dual EC DRGB
• Password breaches of major sites (LinkedIn, Adobe) and what kind of password hashing they were / were not using