CMPT 733 Project Milestone

Frederic Guo & Zhenrong Qu

Topic

Zero-Knowledge proof algo investigation & implementation

Current Progress

1) Investigation on different types of cipher
   including One-time Pad, Stream Cipher, Block Cipher
2) Investigation on encryption algos
   Including DES, AES, RSA, PKE, SKE, cryptographic hashes, Diffie-Hellman Ratchet, Double ratchet
3) Investigation on key exchange approaches
   including Diffie-Hellman, PKI and SSL/TLS
4) Investigation on basic Zero-Knowledge proof algo with scenarios:
   ZKP of discrete log, ZKP of 3-coloring, Non-Interactive ZKP, Blind Signature
5) Investigation on three improved ZKP algos:
   three new strongly deniable key exchange protocols—DAKEZ, ZDH, and XZDH

   - DAKEZ: DAKE with Zero-knowledge
   - ZDH: Zero-knowledge Diffie-Hellman
   - XZDH: eXtended Zero-knowledge Diffie-Hellman

6) Initial implementation of DAKEZ (not fully finished)

Initial Results

1) Review summary on encryption cipher
2) Review summary on key exchange approaches
3) Initial implementation of DAKEZ (not fully finished)

Next Steps

1) Implementation of DAKEZ
2) Implementation of at least one of ZDH and XZDH
3) Code repository
4) Test plan and test cases
5) Preparation of demo and final presentation
6) Final report