Sponsored by the project:

Secure implementation of post-quantum cryptography

SPS Project Number: 984520

Andrej Boledovič and Juraj Varga
Slovak University of Technology in Bratislava, Slovakia

Practical Implementation of McEliece Cryptosystem on Android

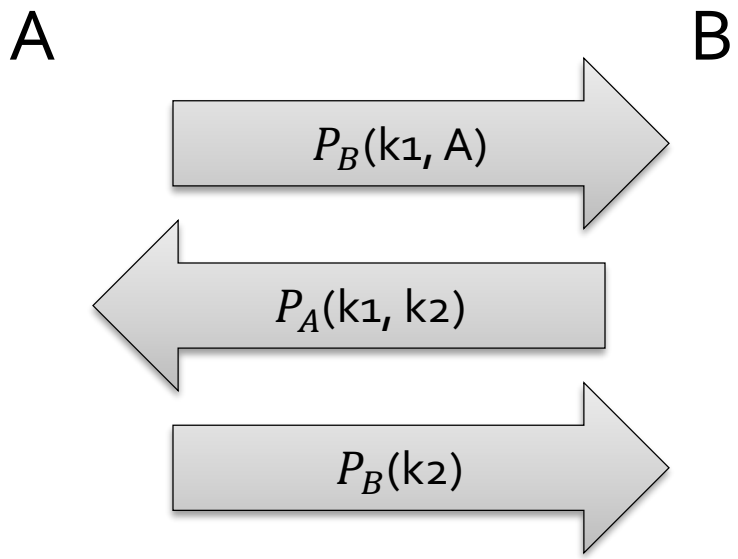
Central European Conference on Cryptography '16
Piestany, Slovakia
24.6. 2016

Introduction

- Post-quantum cryptography
- McEliece algorithm
  - Based on decoding problem (NP-complete)
- CCA2 extension
  - Pointcheval
  - Fujisaki
  - Kobara-Imai – the most suitable for mobile devices

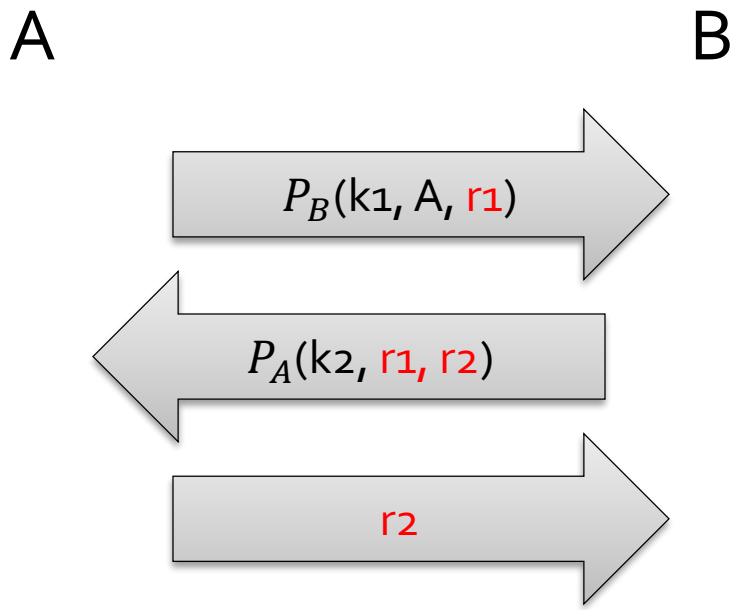
Securing communication (protocols)

- Needham-Schroeder



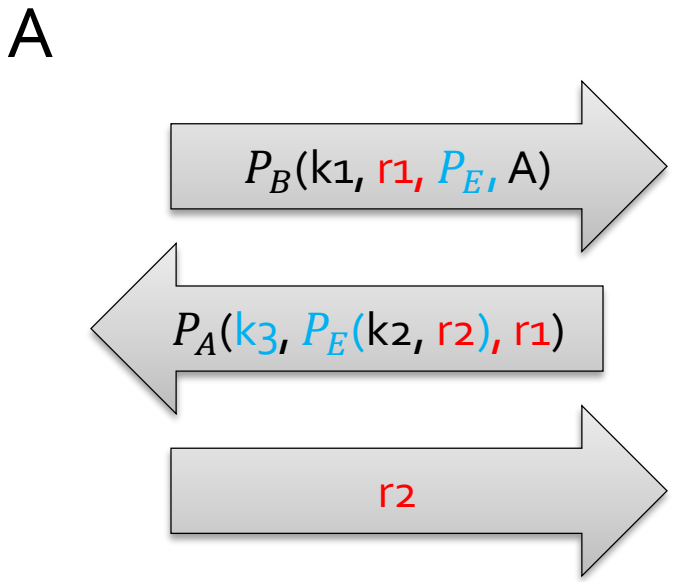
Securing communication (protocols)

- Needham-Schroeder
- Modified Needham-Schroeder



Securing communication (protocols)

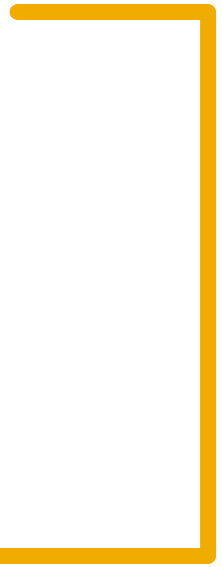
- Needham-Schroeder
- Modified Needham-Schroeder
- Perfect Forward Secrecy extension



Android and McEliece

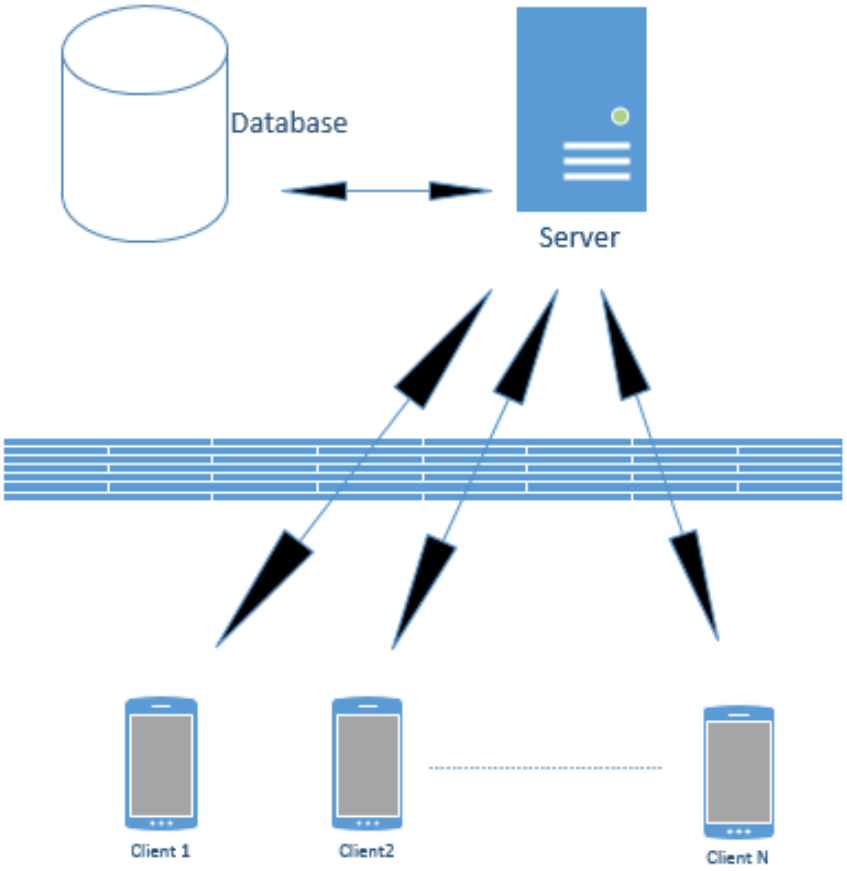
- BitPunch
- Bouncy Castle
  - Pointcheval
  - Kobara Imai
  - Fujisaki
- Bouncy Castle Beta
  - Kobara Imai (11, 50)

SpongyCastle



Architecture

- Unsecured web-service (RESTful)
- Secured channel (sockets) by protocol

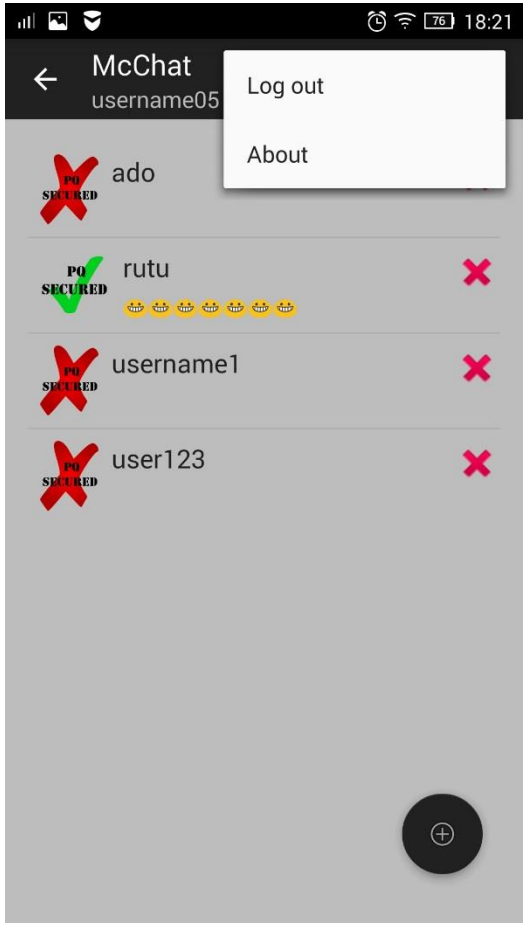


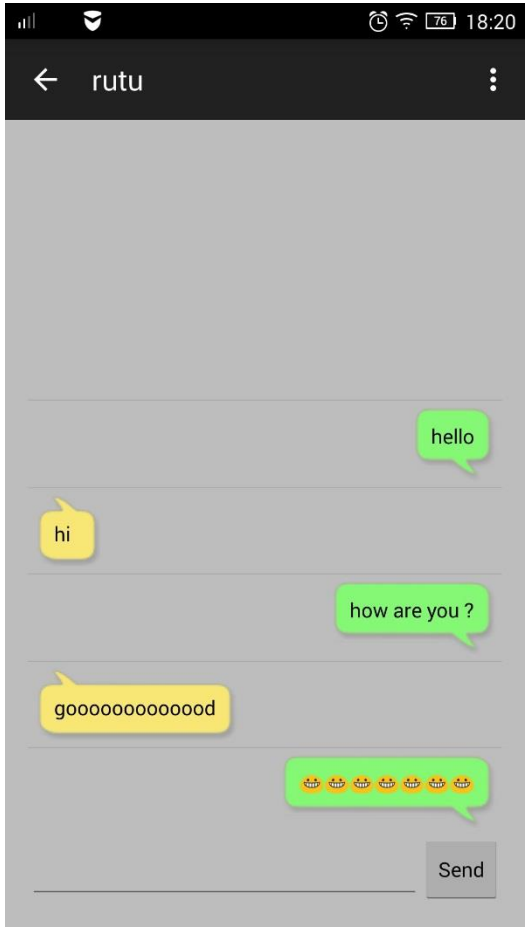
Users
Login : VARCHAR (10) NOT NULL PUBLICK : BLOB NOT NULL SECRETK : VARCHAR (16) NULL

Communication

- Log-in by protocol (client-server connection)
  - Mutual autentication, password not required
  - Hello server, key expiration…
- Client-client connection
  - JSON objects
    - {"WHAT":"GET_PUBLIC","TO":"SERVER","PROT":"P0A","OF":"user_name"}
    - {"TO":"user_name","PROT":"P1B","MESSAGE":"DDXSXCRgmrsTilpSoWSpi4…"}
    - {"TO":"user_name","PROT":"NO","MESSAGE":"KeSJfzP3f3rpgitMAWTOoA=="}

Application

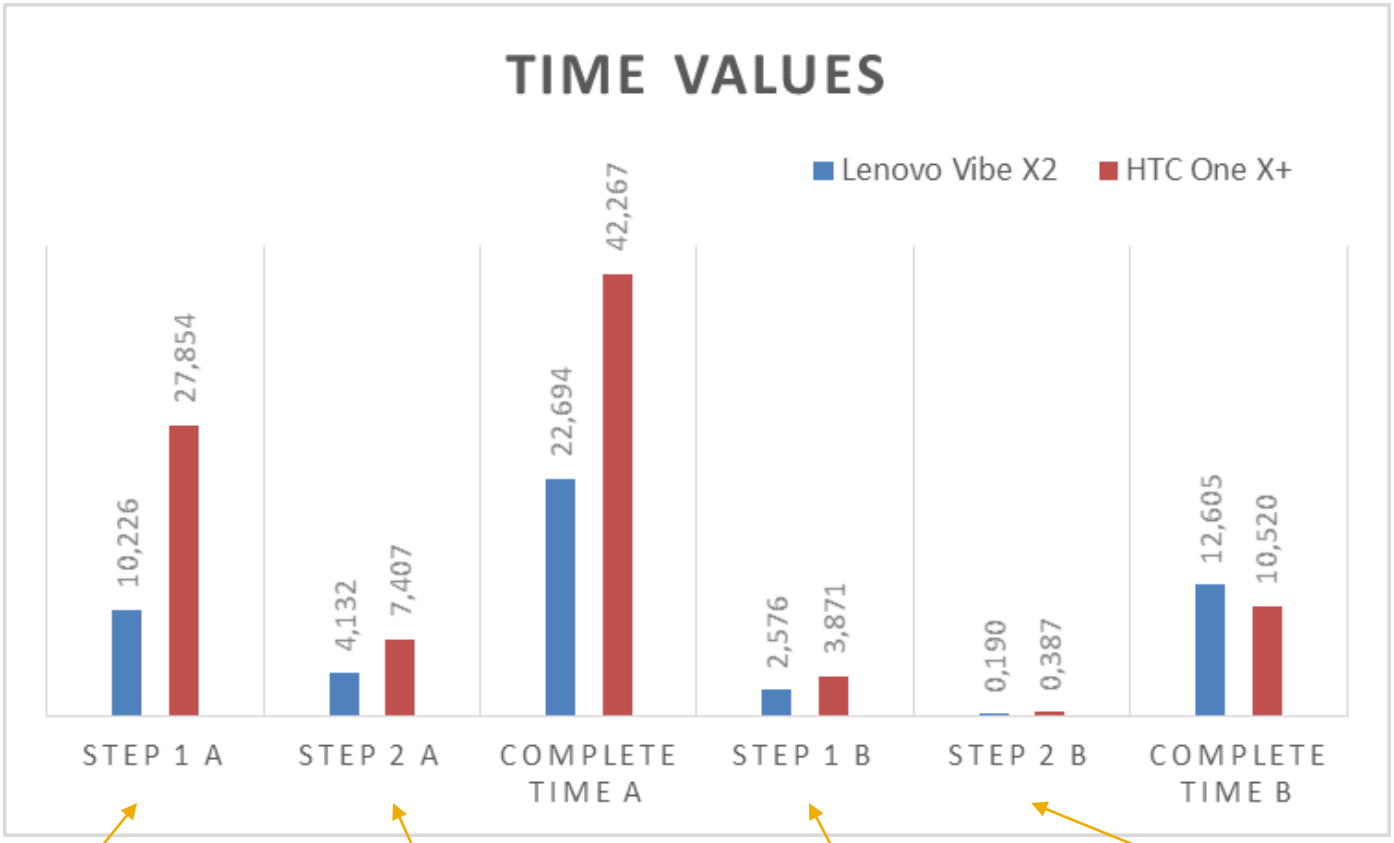




Tests

- HTC One X+
  - App memory: 64 MB
  - After enlargement: 256 MB
- Lenovo Vibe X2
  - App memory: 195 MB
  - After enlargement: 512 MB

Tests



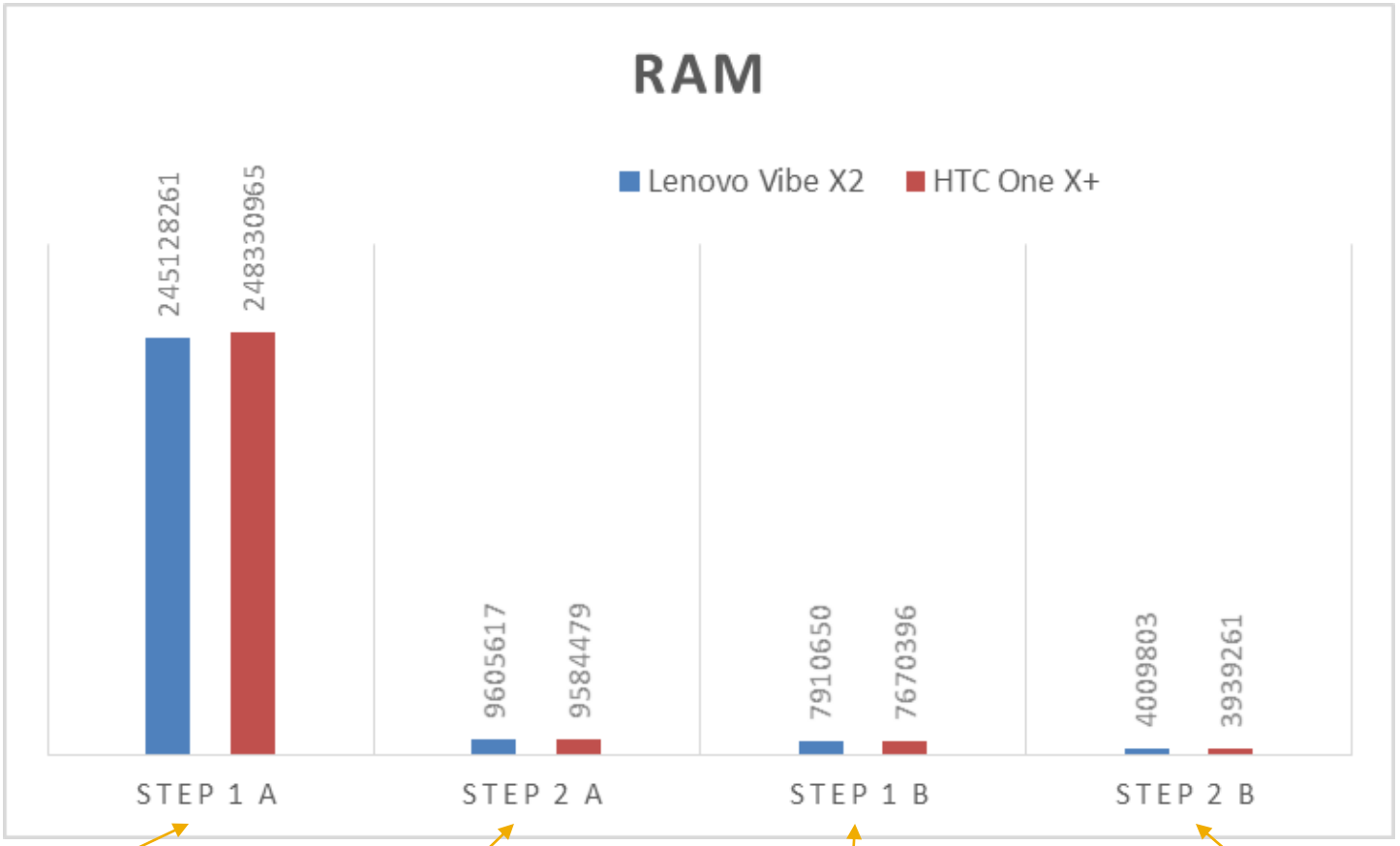
generating keys
1x encryption

2x decryption

1x decryption

2x encryption

Tests



generating keys
1x encryption

2x decryption

1x decryption

2x encryption

Conclusion

- First known McEliece implementation on OS Android (Real-time messenger app)
- Performance depends on device
- Some parts need further optimization
- Source codes will be published on git-hub

Questions?

Thank you for your attention