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)
- CCA$_2$ extension
  - Pointcheval
  - Fujisaki
  - Kobara-Imai – the most suitable for mobile devices
Securing communication (protocols)

- Needham-Schroeder
Securing communication (protocols)

- Needham-Schroeder
- Modified Needham-Schroeder

\[ P_B(k_1, A, r_1) \]
\[ P_A(k_2, r_1, r_2) \]
Securing communication (protocols)

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

\[ P_B(k_1, r_1, P_E, A) \]

\[ P_A(k_3, P_E(k_2, r_2), r_1) \]
Android and McEliece

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

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

- Log-in by protocol (client-server connection)
  - Mutual authentication, password not required
  - Hello server, key expiration...

- Client-client connection
  - JSON objects
    - {"WHAT":"GET_PUBLIC","TO":"SERVER","PROT":"PoA","OF":"user_name"}
    - {"TO":"user_name","PROT":"P1B","MESSAGE":"DDXSXCRgmrsTilpSoWSpi4..."}
    - {"TO":"user_name","PROT":"NO","MESSAGE":"KeSJfzP3f3rpgitMAWTOoA=="}
Application

Search friends

us
user
username1
user123

McChat
username05

Log out
About

ado
PO SECURED

rutu
PO SECURED

username1
user123

rutu

how are you?
gooooooood

Send
Tests

- HTC One X+
  - App memory: 64 MB
  - After enlargement: 256 MB

- Lenovo Vibe X2
  - App memory: 195 MB
  - After enlargement: 512 MB
Tests

**TIME VALUES**

![Bar chart showing time values for different steps and processes with labels for generating keys, 1x encryption, 2x decryption, 1x decryption, and 2x encryption.](chart)

- **STEP 1 A**: 10,226, 27,854
- **STEP 2 A**: 4,132, 7,407
- **COMPLETE TIME A**: 22,694, 42,267
- **STEP 1 B**: 2,576, 3,871
- **STEP 2 B**: 0.190, 0.387
- **COMPLETE TIME B**: 12,605, 10,520
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