Group Signatures on Mobile Devices: Practical Experiences

Klaus Potzmader, Johannes Winter, Daniel Hein, Christian Hanser, Peter Teufl[1], Liqun Chen[2]

[1]Institute for Applied Information Processing and Communications, Graz Universityof Technology, Austria

[2]Hewlett-Packard Laboratories, Bristol, UK

June 17, 2013

Agenda

- Group Signature Schemes
  - General Introduction
  - Scheme Capabilities
- Sample Use Case
- ISO 20008-2
- Implementation
- Results
- Conclusion

Group Signature Schemes (1)

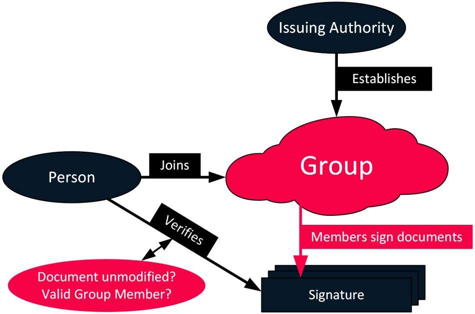
- A crowd of people form a group
  - A company
  - A family
  - People having something in common
- Initiator as issuing authority
  - Adds new members
- Group members can sign documents
  - On behalf of the group
  - Without revealing the individual's identity
- Membership is verifiable

Group Signature Schemes (2)

- One public key for the whole group
- Private counterpart: Group Membership Issuing Key
  - Issuing authority
- Each participant possesses
  - A private key
  - A Membership Credential
    - Created by the issuing authority
    - During joining

Scheme Construction

- Five general processing steps
  - Group Setup/Establishment
  - Join
  - Sign
  - Verify
  - Revoke (details omitted)



Scheme Capabilities

Linking Capability

- Two signatures signed by the same person are connectable
  - Observer knows they belong to the same person
  - No (computationally feasible) ability to identify the particular person
- Might be an undesired "capability"
  - Everyone can link signatures

Opening Capability

- Separate authority
- Capable of opening signatures
- Reveals identity of signer

Sample Use Case

Electronic Payment

- Group: Clients of a mobile payment company
- Issuing authority: A server within that company
- Shops as verifiers
  - Clients sign purchase order
  - Shops verify and deliver if successful
- Mobile payment company:
  - Opens the signature and reveals the client's ID
  - Charges the client
- *Need to know*
  - Customer name and other attributes hidden
  - It's a valid signature, period.

ISO 20008-2

- Upcoming ISO standard for anonymous digital signatures using a group public key
- DIS (Draft International Standard) stage
- Targeted release date: May 2014

Contents

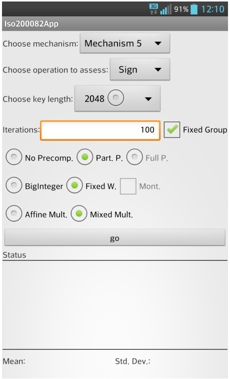
- 7 specified schemes (mechanisms)
- 4 with linking capability
- 2 with opening capability
- 1 supporting both

Implementation (1)

- Our goals
  - Are group signature schemes ready for mobile scenarios?
  - Are there any schemes suited better/worse for mobiles?
- 3/7 mechanisms implemented
- Mechanism 1 (Canard et al. [1])
  - RSA-based (List Signature Scheme)
  - Linking capability
- Mechanism 4 (Chen et al. [2])
  - ECC/Pairing based scheme (Direct Anonymous Attestation)
  - Linking capability
- Mechanism 5 (Isshiki et al. [3])
  - Uses RSA and ECC
  - Opening Capability

Implementation (2)

- Pure Java implementation
- Runs on JavaSE and Android
- Schemes embedded in common framework
- For ECC-DAA, the pairing implementation by Beuchat et al. [4] was ported from their C implementation
- Precomputation saves online signing times
  - Compute parts of the signature not depending on the message beforehand
  - Linkability: Two stages of precomputation



Iso200082App

Choose mechanism: Mechanism 5

Choose operation to assess: Sign

Choose key length: 2048

Iterations: 100 ☑ Fixed Group

○ No Precomp. ● Part. P. ○ Full P.

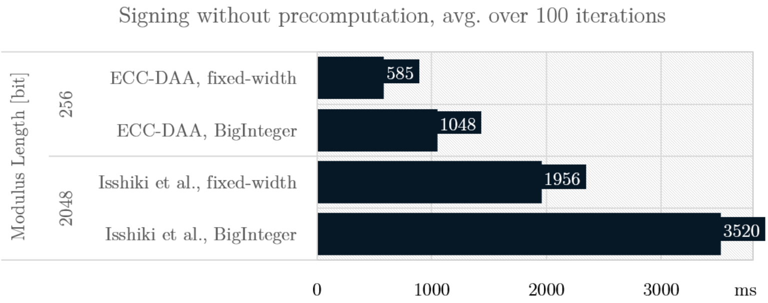
○ BigInteger ● Fixed W. □ Mont.

○ Affine Mult. ● Mixed Mult.

Status

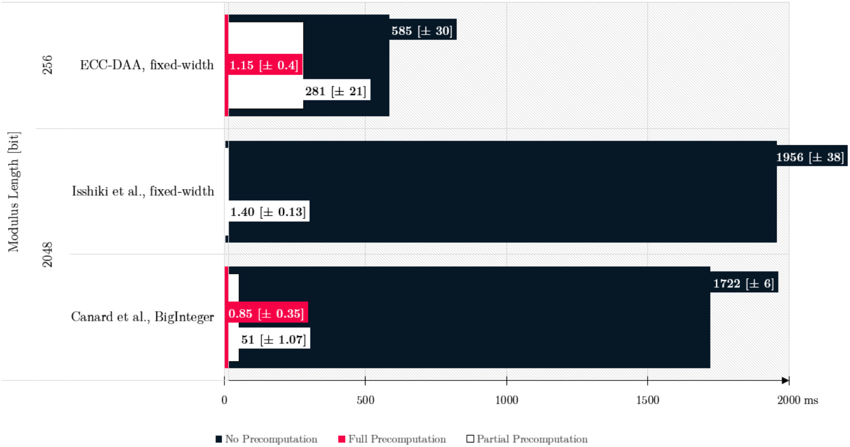
Mean: Std. Dev.:

Implementation (3)



- Android-optimized fixed-width integer implementation
  - Significantly reduces garbage collector activity
  - All-the-same-length int arrays are easily reuseable
  - Eliminates a lot of instantiation/collection cycles
- No issue in standard Java (faster, less aggressive GC)

Runtimes: Mobile Signing

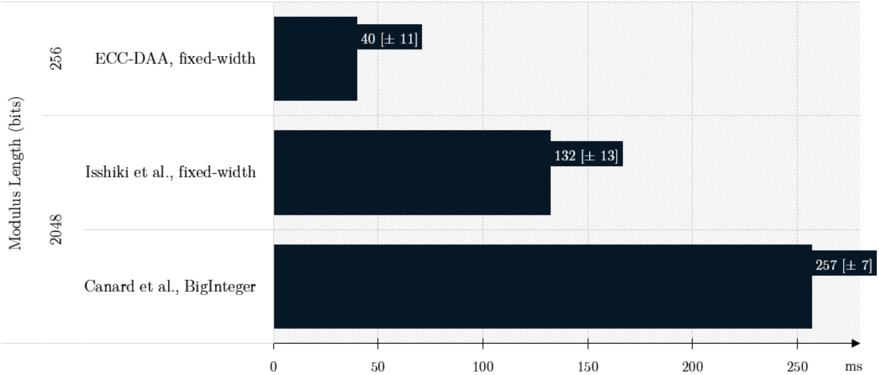


Values averaged over 100 iterations

Device: Samsung Galaxy S3

Security strength: $M1_{2048}$, $M5_{2048}$: 112, $M4_{256}$: 128 bit

Runtimes: Notebook Verification



Values averaged over 100 iterations

Device: Lenovo Thinkpad T420s

Security strength: $M1_{2048}$, $M5_{2048}$: 112, $M4_{256}$: 128 bit

Conclusion

- Evaluation of three group signature schemes on mobile devices
  - All of which use different cryptosystems
- Group Signatures considered ready for mobile environments
  - Application scenarios typically require fast signing
  - Acceptable timings using precomputation, even without native code
  - Significant drops in runtimes, depending on the age of the device
- Framework allows comparison regarding runtime, memory
  - Extendable with further schemes
- Source:
  - github.com/klapm/group-signature-scheme-eval

Group Signatures on Mobile Devices: Practical Experiences

Klaus Potzmader, Johannes Winter, Daniel Hein, Christian Hanser, Peter Teufl[1], Liqun Chen[2]

Thank you. Questions?

References

[1] Canard, S., Schoenmakers, B., Stam, M., Traoré, J.: List Signature Schemes. J. Discrete Applied Mathematics 154 (2), 189–201 (2006)

[2] Chen, L., Page, D., Smart, N.P.: On the Design and Implementation of an Efficient DAA Scheme. In: Gollmann, D., Lanet, J-L., Iguchi-Cartigny, J. (eds.) CARDIS 2010. LNCS, vol. 6035, pp. 223–237. Springer, Heidelberg (2010)

[3] Isshiki, T., Mori, K., Sako, K., Teranishi, I., Yonezawa, S.: Using Group Signatures for Identity Management and its Implementation. In: 2nd ACM workshop on Digital Identity Management, pp. 73–78. ACM Press, New York (2006)

[4] Beuchat J.-L., González-Díaz J.E., Mitsunari, S., Okamoto, E., Rodríguez-Henríquez, F., Teruya, T.: High-Speed Software Implementation of the Optimal Ate Pairing over BarretoNaehrig Curves. In: Joye, M., Miyaji, A., Otsuka, A. (eds.) Pairing 2010. LNCS, vol. 6487, pp, 21–39. Springer, Heidelberg (2010)