Performance Evaluation of Primitives for Privacy-Enhancing Cryptography on Current Smart-cards and Smart-phones

Jan Hajny, Lukas Malina, Zdenek Martinasek and Ondrej Tethal

Cryptology Research Group
Department of Telecommunications
Brno University of Technology
hajny@feec.vutbr.cz
crypto.utko.feec.vutbr.cz

Technology Agency of the Czech Republic

BRNO UNIVERSITY OF TECHNOLOGY

Crypto Research Group, Brno University of Technology, CZ

- Small group of cca 10 people,
- part of Department of Telecommunications, FEEC BUT in Brno, Czech Republic,
- equipped by SIX Research Centre,
- both basic and applied research,
- http://crypto.utko.feec.vutbr.cz/.

R&D in Cryptology and Computer Security

Basic research:

- provable cryptographic protocol design,
- privacy-enhancing technologies (PETs),
- light-weight cryptography.

Implementation:

- smart-cards (Java, .NET, MultOS),
- mobile OS (iOS, Android),
- sensors, micro-controllers.

Current Research Projects

Cryptographic system for the protection of electronic identity

TA02011260

- Funded by the National Budget through the Technology Agency of the Czech Republic.
- Focused on anonymous attribute-based authentication.
- 3-year project in applied research.
- Industrial partner OKsystem for smart-card implementation.
- Based on cooperation with NIST and UofM.
- 01/2012 - 12/2014.

Goal 1: Limit Existing Threats to Privacy

Many services don't need users' identities for access control

- **Identification**
  - Our identity is released even if it is not necessary.
- **Tracing and Profiling**
  - All verification sessions are linkable to one user profile.
- **Unnecessary gathering of personal information**
  - We release more information than needed.

Goal 2: Limit New Threats from Emerging Technologies

- **Electronic IDs**
  - Tracing of people, leak of personal information, behavioural profiling...
- **Clouds**
  - Linkage between our identity and our data, behavioural profiling, unnecessary gathering of personal information...
- **Portable devices (Tablets, Phones with NFC)**
  - Tracing by linking of verification sessions, gathering of personal data...
- ...

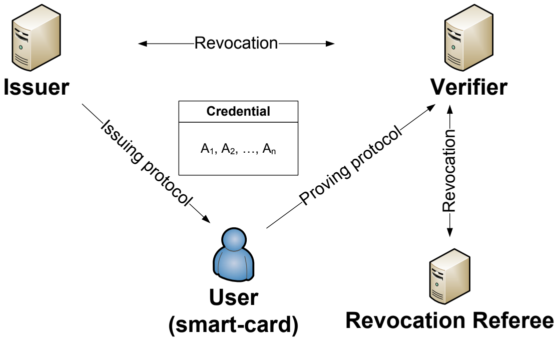
Solution (?): Attribute-Based Credentials (ABCs)

ABCs provide means for proving personal attributes (such as age, citizenship or valid registration) anonymously, untraceably, efficiently.

- **IBM's Idemix**
  - http://www.zurich.ibm.com/security/idemix/
- **Microsoft's U-Prove**
  - http://research.microsoft.com/en-us/projects/u-prove/
- **Our HM12**
  - CARDIS'12: http://link.springer.com/chapter/10.1007%2F978-3-642-37288-9_5

Communication Pattern

A system for efficient proving of attributes[1]



[1] HAJNÝ, J.; MALINA, L. Practical Revocable Anonymous Credentials. In *Proceedings of the 13th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security - CMS 2012*. Springer, 2012. pp. 211-213.

Crucial Privacy Enhancing Features

Required features (EU (ENISA), NSTIC):

- (Provable) Security
- Anonymity
- Untraceability
- Unlinkability
- Selective disclosure of attributes
- Non-transferability
- *Working* revocation

Problems of ABCs

ABCs are quite complex cryptosystems, technical problems arise.

- **Implementation on resource-limited devices (smart-cards) is often slow**.
- Programmable smart-cards do not provide necessary API.
- Revocation of invalid users is still an unresolved problem.

The concept of attribute verification is new, non-technical problems arise.

- Missing legislative.
- Unresolved incorporation into existing authentication technologies.
- Difficult business model (who pays for better privacy?).

Benchmarks

Benchmarks

Selection of Cryptographic Operations

Operations were selected according to their usage in ABCs.

- Basic cryptography
  - Hash functions, RNGs
- Modular biginteger arithmetic
  - Modular multiplication
  - Modular exponentiation
- Non-modular biginteger arithmetic
  - Plain subtraction
  - Plain multiplication

Selection of Cryptographic Operations

- RNG - Random Number Generation
  - RNG_160, RNG_560
- Hash Functions
  - SHA1_4256, SHA1_7328, SHA1_20000, SHA2_8448, SHA2_14592, SHA2_20000
- Big-Integer Modular Arithmetic Operations
  - MExp1024_160, MExp1024_368, MExp2048_160, MExp2048_560, MMult1024, MMult2048
- Big-Integer Arithmetic Operations
  - Mult320, Sub400

Selection of Benchmarked Devices

- **Programmable smart-cards**
  - JavaCard
    - Oberthur ID-One V7.0-A
    - Gemalto TOP IM GX4
  - .NET
    - Gemalto .NET V2+
  - MultOS
    - ML2-80K-65
    - ML3-36K-R1
- **Android mobile devices**
  - Mobile phones
    - Samsung Galaxy S i9000
    - Samsung Galaxy Nexus I9250M
  - Tablet
    - ASUS TF 300T

Selection of Benchmarked Devices

Table: The specification of the .NET cards and the MultOS cards used in benchmarks.

Software Specifications			
OS Type	.NET	MultOS	MultOS
Card Type	.NET V2+	ML2-80K-65	ML3-36K-R1
Asymmetric Crypto	RSA 2048 bits	RSA 2048, EC 384 bits	RSA 2048, EC 512 bits
Symmetric Crypto	3DES, AES	DES, 3DES, AES	DES, 3DES, AES
Hash	SHA1, SHA2, MD5	SHA1, SHA2	SHA1, SHA2

Hardware Specifications			
Chip	SLE 88CFX4000P	SLE66CLX800PEM	SLE78CLXxxxPM
CPU	32 bit	16 bit	16 bit
Int./Ext. clock	66 MHz/10 MHz	30 MHz/7.5 MHz	33 MHz/7.5 MHz
RAM Memory	16 kB	702+960 B	1088+960 B
ROM/EEPROM	80 kB/400 kB	236 kB/78 kB	280 kB/60 kB
Temperature Range	-25 °C to +85 °C	-25 °C to +85 °C	-25 °C to +85 °C
Modular API	No	Yes	Yes

Smart-Card Results - Modular Exponentiation

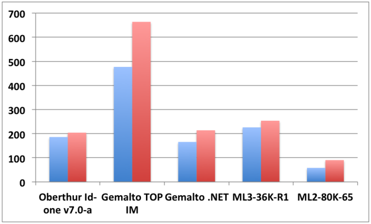


Figure: **MExp1024_160** (blue) and **MExp1024_368** (red)

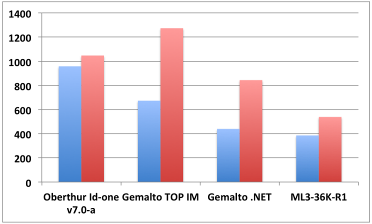


Figure: **MExp2048_160** (blue) and **MExp2048_560** (red)

Smart-Card Results - Modular Multiplication with 1024 b

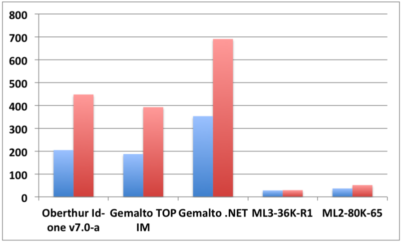


Figure: **MMult1024_160** (blue) and **MMult1024_368** (red)

Android Results - Modular Exponentiation

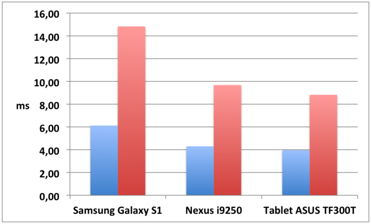


Figure: **MExp1024_160** (blue) and **MExp1024_368** (red)

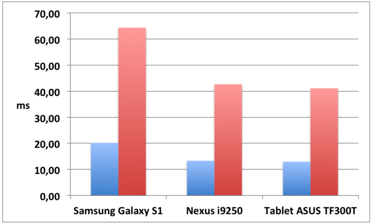


Figure: **MExp2048_160** (blue) and **MExp2048_560** (red)

Android Results - (Modular) Multiplication

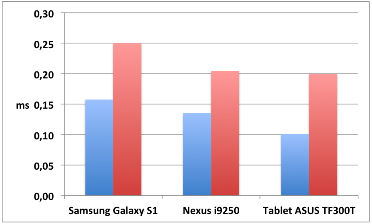


Figure: **MMult1024** (blue), **MMult2048** (red)

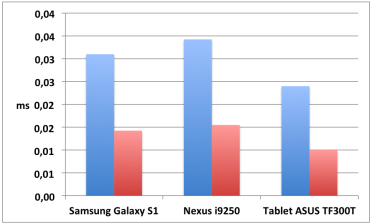


Figure: **Mult320** (blue) and **Sub400** (red)

Results Analysis

Smart-cards

- Modular arithmetic is practical with 1024 b numbers only.
- Necessary API (particularly modular multiplication) is missing on JavaCard, .NET.
- Small RAM is the bottleneck of MultOS.
- 2048 b operations are too slow, impractical.

Android Devices

- Big integer operations natively supported.
- Devices are fast enough for 2048 b operations.
- No hardware-protected storage.
- PETs can be efficiently implemented.

Results Analysis

Table: Performance Estimation Based on Benchmarks.

	Time in milliseconds							
	S1	**S2**	**S3**	**S4**	**S5**	**A1**	**A2**	**A3**
$c = g^w$ (DL commitment)	186	476	165	226	58	6	4	4
$c = g^w h^r$ (Pedersen commit.)	580	1161	717	513	195	12	9	8
$PK\{w : c = g^w\}$	325	830	433	352	222	15	10	9
$PK\{w : c_1 = g_1^w \wedge c_2 = g_2^w\}$	529	1494	646	605	313	30	20	18
$SPK\{w : c = g^w\}(m)$	354	842	498	393	332	15	10	9
Idemix	4519	9433	7270	4219	4208	153	100	91
U-Prove	837	1618	1295	827	633	13	9	8
HM12	2540	6016	3312	2509	1467	102	68	62

Glossary:

- S1: Oberthur Technologies ID-One Cosmo V7.0-A
- S2: Gemalto TOP IM GX4
- S3: Gemalto .NET V2+
- S4: MultOS ML2-80K-65
- S5: MultOS ML3-36K-R1
- A1: Samsung Galaxy S i9000 (smart-phone)
- A2: Samsung Galaxy Nexus I9250M (smart-phone)
- A3: ASUS TF 300T (tablet)

Summary

Smart-cards

On smart-cards, current privacy-enhancing schemes can be practically implemented only in smaller groups (1024 b) and with limited functionality (no revocation for U-Prove and Idemix). U-Prove is the fastest scheme, Idemix is the slowest. HM12 is somewhere between but includes revocation features.

Android Devices

Android smart-phones and tablets are computationally fast enough for all schemes even in 2048 b groups. Nevertheless, they are not protected against tampering as smart-cards. Smart-phones with secure elements (a smart-card) might help.

Thank you for attention!

hajny@feec.vutbr.cz
crypto.utko.feec.vutbr.cz

This research work is funded by project SIX CZ.1.05/2.1.00/03.007, the Technology Agency of the Czech Republic projects TA02011260 and TA03010818; the Ministry of Industry and Trade of the Czech Republic project FR-TI4/647.