Group-Signature Schemes on Constrained Devices

Raphael Spreitzer and Jörn-Marc Schmidt

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology
Inffeldgasse 16a, A-8010 Graz, Austria

raphael.spreitzer@iaik.tugraz.at
Group-Signature Schemes (GSS)

- Introduced by Chaum and van Heyst [CvH91]
- Members within a predefined group are able to sign messages on behalf of the group
- Verifier can only determine whether a signature stems from a specific group
- ... but verifier cannot determine the ID of the signer

Participants
- Signer
- Verifier
- Group manager (GM)
Motivation

Why GSS on constrained devices?

Scenarios
- Prove the age of majority without revealing date of birth
- Prove that you are in possession of a valid driving license
- Anonymous entrance control
- Travel anonymously within the EU?

So where’s the problem?

GSS are based on a complex mathematical concept
Pairing-Based Cryptography (PBC)

- $G_1 = \langle g_1 \rangle$, $G_2 = \langle g_2 \rangle$, and $G_T$ are cyclic groups
- $G_1$ points on $E(\mathbb{F}_q)$
- $G_2$ points on $E(\mathbb{F}_{q^k})$
- $G_T$ is a subgroup of $\mathbb{F}_{q^k}^*$
- Bilinear map: $e(u^a, v^b) = e(u, v)^{ab}$, $u \in G_1$, $v \in G_2$, and $a, b \in \mathbb{Z}_n^*$
- **Type 1**: $G_1 = G_2$
- **Type 3**: $G_1 \neq G_2$, no efficiently computable isomorphism
- PBC is a complex mathematical concept
- Implementations are available, e.g., RELIC [AG]
Comparison of Group-Signature Schemes

- Investigated four schemes [BBS04, BS04, DP06, HLC+11]
- Hide a user’s certificate within a group signature - GM can decrypt the certificate
- Different ...
  - Mathematical assumptions
  - Types of pairings
  - Revocation mechanisms (in case of misbehavior)
    - Perform setup phase again
    - Private-key update
    - Verifier-local revocation (complicated opening mechanism)
  - Number of group operations
- BBS [BBS04], Type 1 pairings
- HLCCN [HLC+11, Int13], Type 3 pairings
- Both types of pairings are implemented in RELIC
Implementation and Performance

- RELIC [AG]
  - $\eta_T$ (eta-t) pairing over $E(\mathbb{F}_{2^{353}})$
  - optimal-ate pairing over 158-bit BN-curve $E(\mathbb{F}_p)$

![Execution Time Graph](image-url)

Raphael Spreitzer  GSS on Constrained Devices
High-Level Performance Optimization?

- Computation of $e(u, v)^a$, $u \in G_1$, $v \in G_2$, $a \in \mathbb{Z}$
  - $E$ in $G_1$, and evaluate pairing: $e(u^a, v)$
  - $E$ in $G_2$, and evaluate pairing: $e(u, v^a)$
  - $E$ in $G_T$: $e(u, v)^a$

- So, which one is the best?
Implementation of Schemes

- BBS
  - Use cached pairings

- HLCCN

\[
R_2 = e(D_2, h_1)^{r_x} e(w, h_\theta)^{-r_\alpha} e(w, h_1)^{-r_\gamma} e(g_2, h_1)^{r_y}
\]

\[
R_2 = e(D_2^{r_x} w^{-r_\gamma} g_2^{r_y}, h_1) e(w^{-r_\alpha}, h_\theta)
\]
\[ R_2 = \frac{4 \text{ E in } \mathbb{G}_T}{\Sigma} \cdot 4 \times 83.2 \cdot 10^6 \]

\[ \sum 332.8 \cdot 10^6 \]

\[ R_2 = e(D_2^{rx} w^{-r\gamma} g_2^{ry}, h_1) e(w^{-r\alpha}, h_\theta) \]

\[ \frac{4 \text{ M in } \mathbb{G}_1}{\Sigma} \cdot 4 \times 6.5 \cdot 10^6 \]

\[ \frac{2 \text{ pairings}}{} \cdot 2 \times 62.7 \cdot 10^6 \]

\[ \sum 151.4 \cdot 10^6 \]

\[ \times 2 \]
Overall Performance

Raphael Spreitzer

GSS on Constrained Devices
Type 1 pairings are considered insecure [GGMZ13, Jou13, Sma]
Type 3 pairings seem to be the desirable choice
Top-down approach instead of bottom-up approach
Cached pairings vs. evaluation of pairings
  - Speedup of factor of 2
6 seconds on a 32 MHz microcontroller
Future work
  - Instruction-set extensions
  - Secure delegation
Group-Signature Schemes on Constrained Devices

Raphael Spreitzer and Jörn-Marc Schmidt

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology
Inffeldgasse 16a, A-8010 Graz, Austria

raphael.spreitzer@iaik.tugraz.at


<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
</table>