VLR Group Signatures: How to Achieve Both Backward Unlinkability and Efficient Revocation Checks

Julien Bringer (Morpho), Alain Patey (Morpho, Télécom ParisTech)
Outline

1. VLR Group Signatures
2. Efficient Revocation Checks
3. Adding Backward Unlinkability
4. Experimental Results and Analysis
5. Conclusion
VLR Group Signatures
Setting/Definitions

- **Setting**:
  - a group of users
  - a Group Manager (GM)
  - GM fixes the group parameters and issues the signing keys

- **Group signatures enable members of a group to sign anonymously on behalf of the group**

- **Anonymity can only be raised by the GM**

- **Applications**: e-Cash, e-Vote, VANETs, TPMs, anonymous authentication, ...
Components of a Group Signature Scheme

**KeyGen**  GM creates a set of public parameters and a secret key. The public parameters are published

- **Join**  Creation of keys for a new member joining the group
- **Sign**  Signature of a message by a member of the group
- **Verify**  Verification of a signature by a person knowing the public parameters of the group
- **Revoke**  GM revokes a member from the group
- **Open**  GM raises the anonymity of a signature
Verifier-Local Revocation

Revocation

User i

Group Manager

Revocation List

rt_i

Group Public Parameters
VLR : Verifier-Local Revocation

→ Dynamic schemes
  ■ Members join and leave the group at different times

→ Leaving members lose their signing capacity

→ Several existing solutions (certificates, accumulators, . . .)

→ VLR (Verifier-Local Revocation) solution :
  ■ A Revocation List (RL) is published and used by the verifiers when they check a signature. The signers do not take it into account when they sign.
  ■ RL is set up and updated by the GM, who is the only one who can derive the revocation tokens
  ■ Advantages : less interactivity, no need to re-issue keys, no additional computation asked to the signer
Generic Construction of a VLR Group Signature

Sign: Zero-knowledge proof of knowledge, linked to the message, of a secret key of a group member

Verify: Signature Check  Check of the Proof of Knowledge
Revocation Check  Check that the signer is not one member whose revocation token is on the revocation list RL

Open: GM uses the Revocation Check algorithm using 1-token (one for each member) Revocation Lists. When the test fails, the signer’s identity is obtained.
Signature Verification

User signs using his secret key

Verifier (≠ GM)

1) Signature Check: Validity of the signature

2) Revocation Check: Is the signer revoked?
Security Properties

**Correctness** : Every signature correctly issued by an unrevoked member is checked as valid

**Backward Unlinkability** : Signatures do not reveal anything (to anyone but the signer and the GM) about their author and they remain anonymous even after the revocation of the user.

**Traceability** : No group of attackers can forge a signature that can not be traced to one of the members of the coalition.

**Exculpability** : Nobody (including GM) is able to issue another’s member signature
Pairings

Let
- $G_1$ and $G_T$ be two cyclic groups of prime order $p$
- $G_2$ be a group of order $p^k$
- $\psi$ a homomorphism from $G_2$ to $G_1$
- $g_2 \in G_2$, and $g_1$ be a generator of $G_1$ such that $\psi(g_2) = g_1$

$e : G_1 \times G_2 \rightarrow G_T$ is a pairing if:
- $e$ is bilinear: $e(u^a, v^b) = e(u, v)^{ab}$
- $e$ is non-degenerate: $e(\psi(g_2), g_2) \neq 1$

$q$-SDH Problem [BB04]:
- Given $(g_1, g_2, g_2^{\gamma}, ..., g_2^{\gamma^q})$ and $e$
- Return a couple $(x, g_1^{\gamma + x})$, with $x \in \mathbb{Z}_p^*$
Efficient Revocation Checks
Towards Efficient Revocation Checks

→ Revocation Check in usual VLR schemes ([BS04, NF06],...) :
  - One pairing per item in the Revocation List
  - Pairings are costly, and we need a linear number of them!
    \[ \implies \text{not applicable in large groups (e.g. a country)} \]

→ Idea : Replace pairings by exponentiations
  - [YO08] : first attempt, not coalition-resistant
  - [CL10] : our starting point
Chen-Li Scheme [CL10]

→ **Enjoys Exculpability**
  - the GM does not know the full secret key of a member

→ **Parameters :**
  - $G_1 = \langle g_1 \rangle$, $G_2 = \langle g_2 \rangle$, both of order $p$
  - $\tilde{g}_1, \tilde{g}_2 \in_R \mathbb{Z}_p$
  - a pairing $e : G_1 \times G_2 \rightarrow G_T$
  - $w = g_2^\gamma$ where $\gamma \in_R \mathbb{Z}_p^*$ is the group manager’s secret key.

→ **User’s key :** $sk_i = f_i$ and $cre_i = (A_i, x_i)$ such that $A_i = (g_1 \tilde{g}_1 f_i)^{\frac{1}{x+\gamma}}$.
  - GM only knows $cre_i$ and $id_i = \tilde{g}_1 f_i$, but not $sk_i$.
  - The revocation token is $rt_i = x_i$
Chen-Li Scheme [CL10] (2)

→ **Sign**($m$)
  - Choose $B \in_R G_1$. Compute $J = B^{f_i}$, $K = B^{x_i}$ and $T = A\tilde{g}_2^a$.
  - Compute $\Pi = \text{SPK}\{f_i, A_i, x_i | J = B^{f_i}, K = B^{x_i}, e(A, g_2^{x_i}w) = e(g_1\tilde{g}_1^{f_i}, g_2)\}(m)$
  - Return $\sigma = (B, J, K, T, \Pi)$

→ **Verify**($m, \sigma$)
  - Signature Check : Check $\Pi$
  - Revocation Check : Check that $\forall rt \in RL, K \neq B^{rt}$
Our first contribution

- The proofs in [CL10] were not much developed
- We found out there was something missing in the SPK and we patched it
- Patched Scheme:
  - Signature components: 4 elts of $G_1$ and 4 elts of $\mathbb{Z}_p$
  - Sign operations: 6 multi-exp. in $G_1$, 1 me in $G_T$
    - These operations can be pre-computed offline. Only a hash function computation is required when the user knows the message to sign.
  - Verify operations: $4 + |RL|$ me in $G_1$, 1 me in $G_T$ and 1 pairing
Adding Backward Unlinkability
Periods and Tokens

→ Time is divided into \( T \) periods

→ For each period \( j \), a public token \( h_j \) is introduced
  
  - Without BU, a revocation token is of the form \( rt_i = x_i \), part of the user’s key
  - With BU, there is one revocation token per user and per period: \( rt_{ij} = h_j^{x_i} \)

\[ \implies \text{We cannot link } rt_{ij} \text{ and } rt_{ik} \text{ for } j \neq k, \text{ thus we enjoy Backward Unlinkability} \]

→ All operations (Sign, Verify, Open) are dependent of the time period. Moreover, there is one revocation list \( RL_j \) per time period.
In schemes using pairing-based revocation checks

→ An element of the form $T = f^{x_i}$ is introduced in the signature, where $f$ is also sent to the verifier and where $x_i$ is the user’s key

→ For every $rt_{i\prime j} \in RL_j$, the verifier computes $e(f, rt_{i\prime j}) = e(f, h_j^{x_{i\prime}}) = e(f, h_j)^{x_{i\prime}}$.

→ He checks that these values are different from $e(T, h_j)$ ($= e(f^{x_i}, h_j) = e(f, h_j)^{x_i}$).

→ $\implies$ Number and nature of computations in the Revocation Check are unchanged (at almost no cost).
An element of the form $L = B^{h_j x_i} = B^{rt_{ij}}$ should be inserted in the signature.  
Nature and Number of operations in the Revocation Check do not change.  
BUT one needs to prove the knowledge of $x_i$, and the cost is here non negligible.
PK of the equality between a log and a double log

→ Given $B, h, K = B^x$ and $L = B^{h^x}$. We want to prove that $\log_B K = \log_h (\log_B L)$.

→ Proof:

- Given a security parameter $\lambda$, pick $r_1, \ldots, r_\lambda \in_R \mathbb{Z}_p$ and compute $V_i = B^{r_i}$ and $W_i = B^{h^{r_i}}$, for $i = 1, \ldots, \lambda$.
- Compute $d = H((\ldots), B, K, L, (V_i, W_i)_{i=1\ldots\lambda})$.
- Let $b_i$ be the $i^{th}$ bit of $d$, set $s_i = r_i - b_i d$, for $i = 1 \ldots \lambda$.
- Return $B, h, K, L, d, s_1, \ldots, s_\lambda$.

→ Verification:

- Let $b_i$ be the $i^{th}$ bit of $d$. For $i = 1, \ldots, \lambda$, compute $V'_i = g^{s_i} K^{b_i}$ and $W'_i = (g^{1-b_i} L^{b_i})^{h^{s_i}}$.
- Compute $d' = H((\ldots), B, K, L, (V'_i, W'_i)_{i=1\ldots\lambda})$.
- Check that $d = d'$

→ see [CS97]
Our Proposal

We integrate the POK to enable BU in the patched CL scheme.

→ **System Parameters**: \( G_1 = \langle g^1 \rangle, \ G_2 = \langle g^2 \rangle, \) both of order \( p, \) 

\( \tilde{g}_1, \tilde{g}_2, h_1, \ldots, h_\lambda \in_R \mathbb{Z}_p, e : G_1 \times G_2 \to G_T, \ w = g_2^\gamma \) where \( \gamma \in_R \mathbb{Z}_p^* \) is the GM’s private key.

→ **Member’s key**: \( sk_i = f_i \) and \( cre_i = (A_i, x_i) \) such that \( A_i = (g_1 \tilde{g}_1 f_i)^{1 \over x + \gamma} \). GM only knows \( cre_i \) and \( id_i = \tilde{g}_1 f_i \), but not \( sk_i \).

- The member’s revocation token at period \( j \) is \( rt_{ij} = h_j^{x_i} \)

→ **Sign(\( m \))**

- Pick \( B \in_R G_1 \). Compute \( J = B^{f_i}, \ K = B^{x_i}, \ L = B^{h_j f_i} \) and \( T = A\tilde{g}_2^a \).
- Compute \( \Pi = SPK\{f_i, A_i, x_i | J = B^{f_i}, K = B^{x_i}, e(A, g_2^{x_i} w) = e(g_1 \tilde{g}_1 f_i, g_2)\}\( m \)\)
- Choose \( r_1, \ldots, r_\lambda \in_R \mathbb{Z}_p \) and compute \( V_l = B^{r_l} \) and \( W_l = B^{h_i r_l} \), for \( l = 1, \ldots, \lambda \).
- Compute \( d = H(gpk, m, B, J, K, L, T, (V_l, W_l)_{l=1\ldots\lambda}) \)
- Let \( b_l \) be the \( l^{th} \) bit of \( d \), set \( s_l = r_l - b_l d, \) for \( l = 1 \ldots \lambda \).
- Return \( \sigma = (B, J, K, L, T, \Pi, d, s_1, \ldots, s_\lambda) \)
Our Proposal (2)

\[ \text{Verify}(m, \sigma) \]

- Signature Check : Check $\Pi$
- Let $b_l$ be the $l^{th}$ bit of $d$. For $l = 1, \ldots, \lambda$, compute $V'_l = g^{s_l} K^{b_l}$ and $W'_l = (g^{1-b_l} L^{b_l})^{h^{s_l}}$
- Compute $d' = H(gpk, m, B, J, K, L, T, (V'_l, W'_l)_{l=1}^{\lambda})$
- Check that $d = d'$
- Revocation Check : Check that \( \forall rt \in RL_j, L \neq B^t \)
Security Properties

In the random oracle model, the scheme satisfies:

→ **Correctness**
→ **Backward Unlinkability (adapted DDH)**
→ **Traceability** ($q$-SDH)
→ **Exculpability** (DL)
Experimental Results and Analysis
Using 256-bit Barreto-Naehrig Curves

→ patched CL (exp.-based revocation checks) : 2308 bits
→ Our proposal with $\lambda = 80$(exp.-based revocation checks + BU) : 23,301 bits

To compare with [NF06](pairing-based revocation checks + BU) : 1533 bits
Computation

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Cost of ( \text{Sign} ) (offline)</th>
<th>Cost of ( \text{Sign} ) (online)</th>
<th>Cost of ( \text{Verify} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>patched CL</td>
<td>( 6 \text{ me} ) + 1 ME</td>
<td>negligible (1 hash)</td>
<td>( (4 +</td>
</tr>
<tr>
<td>Our scheme (CL-BU( \lambda ))</td>
<td>( (7 + 2\lambda) \text{ me} ) + ( \lambda \text{ me} ) + 1 ME</td>
<td>negligible (2 hash)</td>
<td>( (4 +</td>
</tr>
</tbody>
</table>

**Table:** Computational costs for [CL10] and our scheme

- **me:** multi-exponentiations in \( G_1 \)
- **me:** multi-exponentiations in \( G_1 \)
- **ME:** multi-exponentiations in \( G_T \)
- **P:** pairings.
### Experimental Results

<table>
<thead>
<tr>
<th>Revoked members</th>
<th>NF</th>
<th>CL-BU_{80}</th>
<th>CL-BU_{128}</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>3 s</td>
<td>9 s</td>
<td>14 s</td>
</tr>
<tr>
<td>50</td>
<td>10 s</td>
<td>10.5 s</td>
<td>15.5 s</td>
</tr>
<tr>
<td>100</td>
<td>19 s</td>
<td>13 s</td>
<td>18 s</td>
</tr>
<tr>
<td>1000</td>
<td>3 min</td>
<td>53 s</td>
<td>58 s</td>
</tr>
</tbody>
</table>

**Table:** Overall computational time for the *Verify* algorithm, depending on the number of revoked members.

**NF**: Nakanishi-Funabiki VLR scheme with BU, using pairing-based checks [NF06]

**CL-BU_λ**: our proposal with a security parameter \( \lambda \)
Conclusion
Conclusion

→ In VLR schemes for large groups, the bottleneck is the revocation check
→ In all known schemes it has to be linear in the size of the revocation list
→ We introduced the most efficient VLR scheme with BU, using exponentiation-based revocation checks

Open Problems

- Other revocation check operations? Linear Algebra? not constant-time signing yet
- is it possible to have a sublinear revocation check? (it looks like we would loose anonymity somewhere)

- Full version of this paper available on the IACR ePrint Archive [BP11]
Thursday Afternoon (4.30pm-5.30pm), Posters Session 3
Group Sig. with BU used for identity management in a hierarchical setting

An Application of a Group Signature Scheme with Backward Unlinkability to Biometric Identity Management

VLR Group Signatures
- Group Signatures: Registered signers sign anonymously on behalf of a group.
- Each signer has a secret key but there is only one verification key for the group.
- A Group Manager issues keys and revokes users.
- Verifier Local Revocation (VLR) Group Signature:
  - A Revocation List is maintained and published by the GM.
  - Only with revocation tokens of the revoked members.
- Verifiers only need the group public parameters and the RL to check group signatures.
- VLR Group Signatures can be used for biometric anonymous authentication.

Backward Unlinkability
- VLR Group Signatures (without BU):
  - Authentication is revocable.
  - Anonymity of revoked users on their previous signatures is lost.
- With Backward Unlinkability:
  - Time is divided into periods.
  - Revocation tokens and Revocation Lists are linked to these periods.
  - Users only lose their anonymity in the periods when they are revoked.
- Using efficient schemes, it is very slightly increases the performance for an important gain in privacy.

A Hierarchical Setting
- Several identity domains in a tree structure.
- Authentication using an identity is constrained by the use of VLR group signature. Identity Providers are GMI.
- To obtain an identity is a domain, a user needs to:
  - Have a VLR Group Signature.
  - The revocation process takes the hierarchy into account.
- Can anonymously use a given identity, guaranteed against the management of the other identity domains.
- We call this property Cross-Unlinkability.

From Backward Unlinkability to Cross-Unlinkability
- Idea to achieve Cross-Unlinkability:
  - Use Group Signatures with Backward Unlinkability.
  - Time periods are translated to children of a given domain in the identity domain tree.
- Unlinkability across periods implies unlinkability across identity domains.

Authors
Julien Bringer (Morpho), Hame Chalyane (Morpho, Telecom ParisTech), Alain Patey (Morpho, Telecom ParisTech)
Questions ?
Dan Boneh and Xavier Boyen.
Short signatures without random oracles.

Julien Bringer and Alain Patey.
Backward unlinkability for a VLR group signature scheme with efficient revocation check.
http://eprint.iacr.org/.

Dan Boneh and Hovav Shacham.
Group signatures with verifier-local revocation.
Liqun Chen and Jiangtao Li. 
VLR group signatures with indisputable exculpability and efficient revocation. 
In PASSAT, 2010.

Jan Camenisch and Markus Stadler. 
Efficient group signature schemes for large groups (extended abstract). 

Toru Nakanishi and Nobuo Funabiki. 
A short verifier-local revocation group signature scheme with backward unlinkability. 
Takuya Yoshida and Koji Okada.
Simple and efficient group signature scheme assuming tamperproof devices.