Attribute-Based Signatures for Circuit from Bilinear Map

Yusuke Sakai (AIST, Japan)
Nuttapong Attrapadung (AIST, Japan)
Goichiro Hanaoka (AIST, Japan)
Our Contribution

• Propose attribute-based signature scheme for arbitrary circuits
  – Secure under SXDH assumption in bilinear groups
  – Fairly practical
  – No a priori bound on size and depth of circuits

The first scheme that simultaneously achieves simplicity of assumption, efficiency, and expressiveness of predicates!
Attribute-based Signatures

\[ x \xrightarrow{sk_x} \]

\[ sk_x \]

\[ sk_y \]
Attribute-based Signatures

\[ \sigma \leftarrow \text{AttrSign}(pp, sk_x, M, C) \]
Attribute-based

\[
\sigma \text{ is made by someone whose attributes } x \text{ satisfy } C(x) = 1
\]
Anonymity

Cannot tell who made $\sigma$ among signers who satisfy $C(x) = 1$
Unforgeability

Cannot make valid $\sigma$ if $C(x) = 0$

$sk_x$, $sk_y$, $M$, $C$, $\sigma$
Previous Work

[MPR11] The notion, schemes monotone span programs (bilinear groups)

[OT11] non-monotone span programs (bilinear groups)

[BF14] (1) AND/OR of pairing product equation
    (2) Arbitrary circuit via Karp reduction (implicit)
        (generic construction from policy-based signature)

[TLL14] bounded-depth circuits (multilinear maps)
Previous Work

[MPR11] The notion, schemes \textit{monotone span programs} (bilinear groups)

[OT11] \textit{non-monotone span programs} (bilinear groups)

[BF14] (1) \textit{AND/OR of pairing product equation}  
(2) Arbitrary circuit via \textit{Karp reduction} (implicit)  
(generic construction from policy-based signature)

[TLL14] bounded-depth circuits (\textit{multilinear maps})
Previous Work

[MPR11] The notion, schemes \textit{monotone span programs} (bilinear groups)

[OT11] non-monotone span programs

No known scheme simultaneously achieves \textit{simplicity of assumption, efficiency,} and \textit{expressiveness of predicates}!

(2) Arbitrary circuit via \textit{Karp reduction} (implicit) (generic construction from policy-based signature)

[TLL14] bounded-depth circuits (\textit{multilinear maps})
Our Contribution

• Propose attribute-based signature scheme for arbitrary circuits
  – Secure under SXDH assumption in bilinear groups
  – Fairly practical
  – No a priori bound on size and depth of circuits

• Use NIZK and signature as building blocks
  – Make a “fusion” of Groth-Sahai proofs and Groth-Ostrovsky-Sahai proofs
Groth-Sahai (GS) Proofs

• Non-interactive proofs suitable for proving algebraic equation

\[ \prod_{i=1}^{n} e(A_i, Y_i) \prod_{j=1}^{m} e(X_j, B_j) \prod_{i=1}^{n} \prod_{j=1}^{m} e(X_i, Y_j)^{\gamma_{i,j}} = T \]

• Proof consists of two phases:
  – To commit to the witness group elements
  – To prove the elements committed to satisfies the equation to be proven
Groth-Ostrovsky-Sahai (GOS) Proofs

• Non-interactive proofs system which can prove satisfiability of circuits

• Proof consists of two phases:
  – To commit to each assignments to wires
  – To prove the assignments committed to follows input/output relation of each gate
Groth-Ostrovsky-Sahai (GOS) Proofs

• Non-interactive proofs system which can prove satisfaction.

\[ \neg(x_1 \land x_2) = x_4 \quad \neg(x_4 \land x_3) = x_5 \quad \neg(x_3 \land x_3) = 1 \]

• Proof consists of two phases:
  – To commit to each assignments to wires
  – To prove the assignments committed to follows input/output relation of each gate
Overview of the Proposed Scheme

Each signer receives a signature on his attribute

\[ sk_x = \theta_x = Sign(msk, x) \]

\[ sk_y = \theta_y = Sign(msk, y) \]
Overview of the Proposed Scheme

\[ sk_x = \theta_x = \text{Sign}(\text{msk}, x) \]

\[ sk_y = \theta_y = \text{Sign}(\text{msk}, y) \]

Prove knowledge of \((x, \theta_x)\):
(1) \(\text{Verify}(x, \theta_x) = 1\)
(2) \(C(x) = 1\)
Overview of the Proposed Scheme

Prove knowledge of \((x, \theta_x)\):

1. \(\text{Verify}(x, \theta_x) = 1\)
2. \(C(x) = 1\)

• GS proofs are suitable for (1), while GOS proofs are suitable for (2)
• If we have a “fusion” of GS proofs and GOS proofs...?
“Fusion” of GS and GOS

• Both follow the "commit-and-prove" structure

• Translate "¬(x ∧ y) = z" into algebraic equation

• ¬(x ∧ y) = z

    ⇔ 1 − xy = z

    ⇔ $e(g, h) e(g^x, h^y)^{-1} = e(g^z, h)$
Overview of the Proposed Scheme

The entire proof can be constructed with GS proofs!

Prove knowledge of \((x, \theta_x)\):

1. \(\text{Verify}(x, \theta_x) = 1\)
2. \(C(x) = 1\)

\[ sk_x = \theta_x = \text{Sign}(\text{msk}, x) \]

\[ sk_y = \theta_y = \text{Sign}(\text{msk}, y) \]
But...

• It doesn’t provide **CMA security**
• $\sigma$ is not bound to $M$

Receives $\sigma$ from signing oracle

$M, C, \sigma$

Uses $\sigma$ as a forgery for different $M^*$

$M^*, C, \sigma$
Dummy Attribute [MPR11]

M, C, σ

Prove knowledge of \((x, \theta_x)\):

\[\theta_x \text{ is } x \text{ s.t. } C(x) = 1\]

(a) Signature on dummy \(t\) defined by \(M\)

(b) Signature on dummy \(t\) defined by \(M\)

Point

Use different \(t\) for different \(M\)

Intuition for Security

- If adversary sees $(M, C, \sigma)$ and outputs $(M^*, C^*, \sigma^*)$, the reduction
  - uses **signature on** $t$ for simulating $\sigma$,
  - extracts **signature on** $t^*$ from $\sigma^*$
    - Reduction works successfully because $t \neq t^*$
Main Theorem

Theorem  Non-interactive proof system is witness-indistinguishable and extractable, signature scheme is unforgeable, the proposed scheme is anonymous and unforgeable

 Instantiate this with GS proofs in SXDH setting and Kiltz-Pan-Wee structure-preserving signature

Theorem  If SXDH assumption holds, the proposed scheme satisfies anonymity and unforgeability
### Performance

<table>
<thead>
<tr>
<th>Signature size [Group Elements]</th>
<th>Assumption</th>
<th>Predicate</th>
</tr>
</thead>
<tbody>
<tr>
<td>[MPR11] (1) 36s+2t+24ks</td>
<td>q-SDH, SXDH</td>
<td>Monotone Span Program</td>
</tr>
<tr>
<td>[MPR11] (2) 28s+2t+12k+8</td>
<td>SXDH</td>
<td>Monotone Span Program</td>
</tr>
<tr>
<td>[MPR11] (3) s+t+2</td>
<td>Generic Group</td>
<td>Monotone Span Program</td>
</tr>
<tr>
<td>[OT11] 9s+11</td>
<td>DLIN</td>
<td>Non-Monotone Span Program</td>
</tr>
<tr>
<td>Ours 12ɿ+20N+26</td>
<td>SXDH</td>
<td>Non-monotone Circuit</td>
</tr>
</tbody>
</table>

k: Security parameter  
$s\times t$: Size of span program  
ɿ: Input size of circuit  
N: Number of gates in circuit

Almost same performance as previous schemes while more expressive!!!
Our Contribution

• Propose attribute-based signature scheme for arbitrary circuits
  – Secure under SXDH assumption in bilinear groups
  – Fairly practical
  – No a priori bound on size and depth of circuits
  – Use Groth-Sahai proofs and Kiltz-Pan-Wee structure-preserving signature as building blocks