Attribute-Based Encryption with Non-Monotonic Access Structures

Julian Kratzmann

Department of Computer Science
University of Paderborn

Project Group: Cryptographic Access Control for Large Scale Systems (CrACo), July 2013
Outline

1 Non Monotonic Access Structures
   Example
   Access Structure

2 Scheme
   Requirements
   Idea
   Construction

3 Security
   Game
   BDH Assumption
   Proof Sketch
Outline

1 Non Monotonic Access Structures
   Example
   Access Structure

2 Scheme
   Requirements
   Idea
   Construction

3 Security
   Game
   BDH Assumption
   Proof Sketch
Non Monotonic Access Structures

Example

Large Company

- employee from department marketing
- information marketing
- information about people
- no information about employees

Attributes:

marketing := \( p_1 \)
people-information := \( p_2 \)
employee := \( p_3 \)
Problems with Non Monotonic

- How to prove non existence
- LSSS works only with monotone access structures
- Simplest solution: add all negated attributes as new attributes to access structure
- ⇒ Problem: for every ciphertext all negative attributes have to be added
- Challenge: Use the idea without doubling the universe of attributes
**Access Structure**

**Definition**

Let $\{P_1, P_2, \ldots, P_n\}$ be a set of parties. A collection $A \subseteq 2^{\{P_1, P_2, \ldots, P_n\}}$ is monotone if $\forall B, C: \text{if } B \in A \text{ and } B \subseteq C \text{ then } C \in A$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) $A$ of non-empty subsets of $\{P_1, P_2, \ldots, P_n\}$, i.e. $A \subseteq 2^{\{P_1, P_2, \ldots, P_n\}} \setminus \{\emptyset\}$. The sets in $A$ are called the authorized sets, and the sets not in $A$ are called the unauthorized sets.
Non monotonic access structure:

\[ \tilde{P} = \{p_1, p_2, p_3\} \]

\[ \tilde{A} = \{\{p_1\}, \{p_2\}, \{p_1, p_2\}, \{p_1, p_3\}, \{p_1, p_2, p_3\}\} \]

Corresponding monotonic access structure:

\[ P = \{p_1, p_2, p_3, \overline{p_1}, \overline{p_2}, \overline{p_3}\} \]

\[ A = \{\{p_1\}, \ldots \text{ all with } p_1 \ldots, \{p_2, \overline{p_3}\}, (p_2, \overline{p_3}, \overline{p_1}), \{p_2, \overline{p_3}, \overline{p_2}\}, \{p_2, \overline{p_3}, p_3\}, \{p_2, \overline{p_3}, \overline{p_2}, \overline{p_1}\}, \{p_2, \overline{p_3}, \overline{p_1}, p_3\}, \{p_2, \overline{p_3}, \overline{p_2}, p_3\}, \{p_2, \overline{p_3}, \overline{p_2}, p_3, \overline{p_1}\}\} \]
Outline

1 Non Monotonic Access Structures
   Example
   Access Structure

2 Scheme
   Requirements
   Idea
   Construction

3 Security
   Game
   BDH Assumption
   Proof Sketch
Requirements
LSSS

Definition (Linear Secret Sharing Schemes)

A secret-sharing scheme $\Pi$ over a set of parties $P$ is called linear (over $\mathbb{Z}_p$) if

1. The shares for each party form a vector over $\mathbb{Z}_p$.
2. There exists a matrix $M$ called the share-generation matrix for $\Pi$. The Matrix $M$ has $l$ rows and $n$ columns. For all $i = 1, \ldots, l$, the $i$'th row of $M$ is labeled with a party named $\hat{x} \in P$. When we consider the column vector $v = (s, r_1, \ldots, r_n)$, where $s \in \mathbb{Z}_p$ is the secret to be shared, and $r_1, \ldots, r_n \in \mathbb{Z}_p$ are randomly chosen, then $Mv$ is the vector of $l$ shares of the secret $s$ according to $\Pi$. The share $(Mv)_i$ belongs to party $\hat{x}$.
Definition (Linear Reconstruction Property)

Suppose that $\Pi$ is a Linear Secret Sharing Scheme for the access structure $\mathbb{A}$. Let $S \in \mathbb{A}$ be any authorized set, and let $I \subset \{1, 2, \ldots, l\}$ be defined as $I = \{i : \hat{x}_i \in S\}$. Then, there exist constants $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$ such that, if $\{\lambda_i\}$ are valid share of any secret $s$ according to $\Pi$, then

$$\sum_{i \in I} \omega_i \lambda_i = s.$$ 

These constants $\{\omega_i\}$ can be found in time polynomial in the size of the share-generating matrix $M$. 

Requirements

LSSS
Definition (Bilinear Maps)

Let $G$ and $G_T$ be two cyclic groups of prime order $p$. Let $g$ be a generator of $G$ and $e$ be a bilinear map:

$$e : G \times G \rightarrow G_T$$

The bilinear map $e$ has the following properties:

1. **Bilinearity:** for all $u, v \in G$ and $a, b \in \mathbb{Z}_p$, we have
   $$e(u^a, v^b) = e(u, v)^{ab}.$$  

2. **Non-degeneracy:** $e(g, g) \neq 1$.  

Requirements
Bilinear Maps
Attribute Based Encryption Scheme

**Setup:**
- input: security parameter (implicit)
- output: public parameters $PK$ and master key $MK$

**Encryption:**
- input: message $m$, set of attributes $\gamma$, $PK$
- output: ciphertext $E_\gamma$

**Key Generation:**
- input: access structure $A$, $PK$, $MK$
- output: decryption key $D_A$

**Decryption**
- input: $E_\gamma$, $D_A$, $PK$
- output $m$ if $\gamma \in A$
Idea

- Secret Key:
  - for each leaf in the tree (positive and negative attributes) generate a key $D_i$

- Encryption:
  - Encryption parameter for each positive attribute
  - One item $E_{not}$ for all negative attributes

![Diagram of a decision tree with nodes labeled with conditions and keys]

Scheme Idea Julian Kratzmann 12/25
Setup\((d)\)

\((p, \mathbb{G}, \mathbb{G}_T, g \in \mathbb{G}, e) \leftarrow \mathcal{G}(1^n)\)

\(\alpha, \beta \leftarrow \mathbb{Z}_p^*, \quad g_1 = g^\alpha, \quad g_2 = g^\beta, \quad MK = \alpha\)

\(h(x), q(x) \leftarrow \mathbb{Z}_p[x] \text{ of } \text{deg}(d) \quad q(0) = \beta\)

\(PK = (g, g_1; g_2 = g^{q(0)}, \ldots, g^{q(d)}; g^{h(0)}, \ldots, g^{h(d)})\)

\(T(x) = g_2^x g^{h(x)}\)

\(V(x) = g^{q(x)}\)
Construction

Encryption

Enc(\(m, \gamma, PK\))

\[
\begin{align*}
\text{Attributes } & \gamma \subset \mathbb{Z}_p^*, \quad |\gamma| = d, \quad s \leftarrow \mathbb{Z}_p^* \\
E & = (\gamma, E^1 = m \cdot e(g_1, g_2)^s, E^2 = g^s, \\
& \{ E^3_x = T(x)^s \}_{x \in \gamma}, E_{\text{not}} = \{ E^4_x = V(x)^s \}_{x \in \gamma})
\end{align*}
\]
Construction

Key Generation

KeyGen($\tilde{A}$, $MK$, $PK$)

Let $A$ correspond to $\tilde{A}$ and $\Pi$ a LSSS for $A$ and $\alpha$.
Let $\{\lambda_i\}$ be shares from $\Pi$ for secret $\alpha$ corresponds to a positive or negative attribute.

$r_i \leftarrow \mathbb{Z}_p$

For each $\lambda_i$ which correspond to an positive attribute:

$$D_i = \left( D_i^1 = g^{\lambda_i} \cdot T(x_i)^{r_i}, D_i^2 = g^{r_i} \right)$$

For each $\lambda_i$ which corresponds to an negative attribute:

$$D_i = \left( D_i^3 = g^{\lambda_i + r_i}, D_i^4 = V(x_i)^{r_i}, D_i^5 = g^{r_i} \right)$$
Dec$(E, D)$

Finally we want to compute

$$\frac{E^{(1)}}{\prod_{i \in I} Z_i^{\omega_i}} = \frac{E^{(1)}}{\prod_{i \in I} e(g_2, g)^{s\lambda_i \omega_i}} = \frac{me(g_2, g)^{s\alpha}}{e(g_2, g)^{s\alpha}} = m$$

For every positive attribute:

$$Z_i = \frac{e(D_i^{(1)}, E_i^{(2)})}{e(D_i^{(2)}, E_i^{(3)})} = e(g_2, g)^{s\lambda_i}$$
For every negative attribute:

• \( \gamma_i = \gamma \cup x_i \)
• \( \Delta_{i,S}(y) = \prod_{j \in S, j \neq i} \frac{y-j}{i-j} \)
• \( \sigma_x = \Delta_{x,\gamma_i}(0) \)
• \( \sum_{x \in \gamma_i} \sigma_x q(x) = q(0) = \beta \)

\[
Z_i = \frac{e \left( D_i^{(3)}, E^{(2)} \right)}{e \left( D_i^{(5)}, \prod_{x \in \gamma} (V(x)^s)^{\sigma_x} \right) \cdot e \left( D_i^{(4)}, E^{(2)} \right)^{\sigma_{xi}}} = e \left( g_2, g \right)^{s \lambda_i}
\]
Outline

1. Non Monotonic Access Structures
   - Example
   - Access Structure

2. Scheme
   - Requirements
   - Idea
   - Construction

3. Security
   - Game
   - BDH Assumption
   - Proof Sketch
Selective Set Model for ABE ABE-SelSet_{A,Γ}^{CPA}(n)

**Init:** adversary $A$ declares set of attributes $γ$ to be challenged on

**Setup:** challenger runs setup$(1^n)$ and gives $PK$ to $A$

**Phase 1:** $A$ queries private keys for Access Structures $A_j$ where $γ ∉ A_j$ for all $j$

**Challenge:** $A$ submits $m_0, m_1$ with $|m_0| = |m_1|$, $b ← \{0, 1\}$, encrypt $m_b$ with $γ$ and return ciphertext to $A$

**Phase 2:** same as Phase 1

**Guess:** $A$ outputs $b' ∈ \{0, 1\}$ Output 1 if $b = b'$ else output 0

Write ABE-SelSet_{A,Γ}^{CPA}(n) = 1, if output is 1. Say $A$ has succeeded or $A$ has won.
An attribute-based encryption scheme is secure in the selectivest-set model of security if for every ppt adversary $A$ there is a negligible function $\mu : \mathbb{N} \rightarrow \mathbb{R}^+$ such that

$$\Pr \left[ \text{ABE-SelSet}^{CPA}_{A,\Gamma}(n) = 1 \right] \leq \frac{1}{2} + \mu(n)$$
Let $a, b, c, z \rightarrow \mathbb{Z}_p$, $g$ generator for $\mathbb{G}$. The decisional bilinear Diffie-Hellman assumption according to $\mathcal{G}(1^n)$ is that every ppt $B$ can not distinguish the tuple $(g^a, g^b, g^c, e(g, g)^z)$ from the tuple $(g^a, g^b, g^c, e(g, g)^{abc})$ with probability greater $\mu(n)$ where $\mu(n)$ is negligible.

$$\left| \Pr \left[ B \left( g^a, g^b, g^c, e(g, g)^z \right) = 1 \right] - \Pr \left[ B \left( g^a, g^b, g^c, e(g, g)^{abc} \right) = 1 \right] \right| = \mu(n)$$
Proof Sketch

B gets $A = g^a$, $B = g^b$, $C = g^c$, $Z = g^z$ or $g^{abc}$

- **Init**: A chooses $\gamma \in \mathbb{Z}_p^*$, $|\gamma| = d$, $\gamma = (x_1, \ldots, x_d)$

- **Setup**:
  - $g_1 = A$, $g_2 = B$
  - $\theta_{x_1}, \ldots, \theta_{x_d} \leftarrow \mathbb{Z}_p$

  - $f(x) \leftarrow \mathbb{Z}_p[x]$ of $\deg(d)$
    
    
    $u(x) = -x^d \forall x \in \gamma$ and $u(x) \neq -x^d \forall x \notin \gamma$

  - $PK = (g, A; B, g^{\theta_1}, \ldots, g^{\theta_d}; B^{u(0)} \cdot g^{f(0)}, \ldots, B^{u(d)} \cdot g^{f(d)})$

- **Phase 1**: ...
Proof Sketch

• Challenge:
  • get \( m_0, m_1 \) from A
  • \( \nu \leftarrow \{0, 1\} \)
  • output \( E = (\gamma, E^{(1)} = m_{\nu} Z, E^{(2)} = C, \)
  \[ \{E^{(3)}_x = Cf(x)\}_{x \in \gamma}, \{E^{(4)}_x = C^{\theta x}\}_{x \in \gamma} \]

• Phase 2: ...

• Guess:
  • get \( \nu' \in \{0, 1\} \) from A
  • if \( \nu = \nu' \) output 1, else 0
Proof Sketch

Probability

- \( \Pr[\text{ABE-SelSet}_{A,\Gamma}^{\text{CPA}}(n) = 1] = \frac{1}{2} + \epsilon(n) \)
- \( |\Pr\left[B\left(g^a, g^b, g^c, e(g, g)^z\right) = 1\right] - \Pr\left[B\left(g^a, g^b, g^c, e(g, g)^{abc}\right) = 1\right]| = \mu(n) \)
- \( \Pr\left[B\left(g^a, g^b, g^c, e(g, g)^z\right) = 1\right] = \Pr[v = v'|z \leftarrow \mathbb{Z}_p] = \frac{1}{2} \)
- \( \Pr\left[B\left(g^a, g^b, g^c, e(g, g)^{abc}\right) = 1\right] = \Pr[v = v'|z \leftarrow \mathbb{Z}_p] = \frac{1}{2} + \epsilon(n) \)

\[
\left| \Pr[v = v'|z \leftarrow \mathbb{Z}_p] - \Pr[v = v'|z \leftarrow \mathbb{Z}_p] \right|
= \left| \frac{1}{2} - \frac{1}{2} - \epsilon(n) \right|
= \epsilon(n) \Rightarrow \epsilon(n) \text{ negl.}
\]
Ostrovsky, Rafail and Sahai, Amit and Waters, Brent
Attribute-based encryption with non-monotonic access structures
Proceedings of the 14th ACM conference on Computer and communications security CCS ’07