ABE Scheme (modified)

Setup(λ) : Inputs security parameter λ to choose prime p

U = universal set of attributes.

G_1, G_2, G_T are cyclic groups of order p and a bilinear map $e : G_1 \times G_2 \longrightarrow G_T$.

generator of G_1 is g_1, generator of G_2 is g_2

randomly choose $\alpha \in \mathbb{Z}_p$

and randomly choose $t_i \in \mathbb{Z}_p$ for every $i \in U$.

public parameters : $PP = \{ Y = e(g_1, g_2)^{\alpha}, \{ T_i = g_2^{t_i} \mid i \in U \} \}$

master secret key : $MSK = \{ \alpha, \{ t_i \mid i \in U \} \}$

Keygen(MSK, access tree) : inputs master secret key and access tree.

It sets $S(r) = \alpha$ for the root node and shares α in top-down manner

OR (w, w_1, w_2) : If $S(w) = \delta$, then

$$S(w_1) = S(w_2) = \delta$$

AND (w, w_1, w_2) : If $S(w) = \delta$, randomly choose $v \in \mathbb{Z}_p$, then

$$S(w_1) = v$$

$$S(w_2) = \delta - v$$

For each leaf node x and its attached attribute t_x.

randomly choose $d \in \mathbb{Z}_p$

$$SK_x = g_1^{S(x)/t_x} + g_1^{d/t_x}$$

outputs the private key $SK = (\{ SK_x \}, g_2^d)$

Encrypt (M, A, PP): inputs public parameters PP, attribute set $A \subseteq U$ and message $m \in G_T$.

select random $a \in \mathbb{Z}_p$.

compute $w = e(g_1^{xv}, g_2^{a})$

select random $b \in \mathbb{Z}_p$.

ciphertext: $CT = \left(A, g_1^{b}, M \cdot e(g_1^{xv}, g_2^{a}) \cdot e(g_1, g_2)^{\alpha b}, \{T_i^{s} = g_2^{t_i b} \mid i \in A\}, g_2^{a}, g_1^{b}\right)$

Decryption (CT, PK): Inputs ciphertext with structure Γ and user's private key PK with attribute set A.

Following calculations are made:

CT contains g_1^{b} while PK contains g_2^{d}

calculate $e(g_1^{b}, g_2^{d})$

$$L = e(g_1, g_2)^{bd}$$

Leaf node (w): if $\Gamma_w(A) = 1$, it calculates

$$\begin{aligned}
R(w) &= e(SK_x, E_x) \\
&= e\left(g_1^{S(x)/t_x} + g_1^{d/t_x}, g_2^{t_x b}\right) \\
&= e\left(g_1^{S(x)/t_x}, g_2^{t_x b}\right) \cdot e\left(g_1^{d/t_x}, g_2^{t_x b}\right) \\
&= e(g_1, g_2)^{bS(x)} \cdot e(g_1, g_2)^{db}
\end{aligned}$$

dividing $R(w)$ by L:

$$\frac{e(g_1, g_2)^{bS(x)} \cdot \cancel{e(g_1, g_2)^{db}}}{\cancel{e(g_1, g_2)^{bd}}}$$

$= e(g_1, g_2)^{bS(x)}$ $\Rightarrow$ Store this back in $R(w)$

AND (w, w_1, w_2): if $\Gamma_w(A) = 1$, it calculates

$$R(w) = R(w_1) \cdot R(w_2)$$

$$= e(g_1, g_2)^{\nu b} \cdot e(g_1, g_2)^{(\delta - \nu) b}$$

$$= e(g_1, g_2)^{\delta b}$$

OR (w, w_1, w_2): if $\Gamma_w(A) = 1 = \Gamma_{w_1}(A)$, it sets

$$R(w) = R(w_1)$$

or if $\Gamma_w(A) = 1 = \Gamma_{w_2}(A)$, it sets

$$R(w) = R(w_2)$$

Finally, at the root node, it would have calculated $e(g_1, g_2)^{\alpha b}$ if $\Gamma(A) = 1$. To retrieve the message:

$$\frac{M \cdot e(g_1^{xv}, g_2^{a}) \cdot e(g_1, g_2)^{\alpha b}}{e(g_1, g_2)^{\alpha b}} = M \cdot e(g_1^{xv}, g_2^{a}).$$

and then we compute $w = e(g_1^{xv}, g_2^{a})$ to get

$$\frac{M \cdot e(g_1^{xv}, g_2^{a})}{e(g_1^{xv}, g_2^{a})} = M.$$

Proof of Security (for modified scheme)

reduces to hardness of DBDH assumption

Definition: Decisional Bilinear Diffie-Hellman (DBDH assumption)

Suppose $a, b, c, z \in \mathbb{Z}_p$ are chosen at random.

The DBDH assumption is that no polynomial-time adversary is able to distinguish the tuple $(A = g_1^a, B = g_2^b, C = g_2^c, Z = e(g_1, g_2)^{abc})$ from the tuple $(A = g_1^a, B = g_2^b, C = g_2^c, Z = e(g_1, g_2)^z)$ with more than a negligible advantage.

Theorem: If there exists a poly-time attacker who can break the KP-ABE scheme with advantage ϵ, the challenger can solve the DBDH problem with advantage $\epsilon/2$.

Proof: Challenger receives an instance of a BDHE assumption that includes (g_1^a, g_2^b, g_2^c, Z) and challenger flips a fair binary coin μ.

If $\mu = 0$, $Z = e(g_1, g_2)^{abc}$

else $\mu = 1$ and $Z = e(g_1, g_2)^z$.

note: a, b, c, z are chosen at random from $\mathbb{Z}_p$.

Universe of attributes U is defined.

Init: Attacker announces challenge attribute set $A^* \subseteq U$.

Setup: Challenger sets $Y = e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ and then it randomly chooses r_i $\forall i \in U$. It sets H_i as follows:

$$T_i = \begin{cases} g_2^{br_i} & \text{if } i \in A^* \\ g_2^{r_i} & \text{if } i \notin A^* \end{cases}$$

The public parameters published are: $\{e(g_1, g_2)^y, T_i\}$

$Y = e(g_1, g_2)^y$, $T_i = g_2^{t_i}$ $\forall i \in U$

Phase 1: Attacker submits an access tree Γ to start secret sharing procedure.

$y = S(r) = ab$ for root node and sharing y by access tree in a top down manner.

OR gate (w, w_1, w_2): if $S(w) = L$, it sets $S(w_1) = L$ and $S(w_2) = L$

AND gate (w, w_1, w_2): if $S(w) = L$, randomly select $K \in \mathbb{Z}_p$.

case 1: if $\Gamma_w(A^*) = \Gamma_{w_1}(A^*) = \Gamma_{w_2}(A^*) = 1$, it sets $S(w_1) = K$ and $S(w_2) = L - K$

case 2: if $\Gamma_w(A^*) = 0, \Gamma_{w_1}(A^*) = 1, \Gamma_{w_2}(A^*) = 0$, it sets $S(w_1) = K$ and $S(w_2) = \frac{L}{g_1^K}$

case 3: if $\Gamma_w(A^*) = 0, \Gamma_{w_1}(A^*) = 0, \Gamma_{w_2}(A^*) = 1$, it sets $S(w_1) = \frac{L}{g_1^K}$ and $S(w_2) = K$

case 4: if $\Gamma_w(A^*) = \Gamma_{w_1}(A^*) = \Gamma_{w_2}(A^*) = 0$, it sets $S(w_1) = g_1^K$ and $S(w_2) = \frac{L}{g_1^K}$

For each leaf node, it sets $SK_x = \begin{cases} (g_1^b)^{\frac{S(x)}{t_i}} + g_1^{d/r_i}, & x \in A^* \\ S(x)^{1/t_i} + g_1^{d/r_i}, & x \notin A^* \end{cases}$

At last, the challenger sends the private key $SK = \{SK_x\}, g_2^d$

Challenge: Attacker submits 2 equal length messages m_0, m_1 to the challenger. Then challenger flips a random fair coin $b \in \{0,1\}$ and outputs the ciphertext $CT = (m_b Z, \{g_2^{cr_i}\}_{i \in A^*})$

Phase 2: Same as phase 1

Guess: Attacker guesses b' about b. If $b' = b$, challenger decides $Z = e(g,g)^{abc}_{\mu' = 0}$; otherwise $Z = e(g,g)^z_{\mu' = 1}$.

μ' : challenger's output.

σ : overall advantage of challenger in DBDH game.

$Pr[b'=b \mid \mu=1] = \frac{1}{2}$ because attacker gains no information about b

$Pr[\mu'=\mu \mid \mu=1] = \frac{1}{2}$ because challenger guesses $\mu'=1$ when $b=b'$

If $\mu=0$, attacker sees encryption of m_b

$Pr[b'=b \mid \mu=0] = \frac{1}{2}+\epsilon$ because attacker's advantage is ϵ.

$Pr[\mu'=\mu \mid \mu=0] = \frac{1}{2}+\epsilon$ because simulator guesses $\mu'=0$ when $b=b'$

$$\sigma = \frac{1}{2}Pr[\mu'=\mu \mid \mu=0] + \frac{1}{2}Pr[\mu'=\mu \mid \mu=1] - \frac{1}{2}$$

$$= \frac{1}{2}\left(\frac{1}{2}+\epsilon\right) + \frac{1}{2}\left(\frac{1}{2}\right) - \frac{1}{2}$$

$$= \frac{\epsilon}{2}$$

$$(g_1^a)^{\frac{(ab-z)}{r_i}}$$

<u>Some calculations:</u>

if $i \in A^*$, $T_i = g_2^{br_i} = g_2^{t_i}$; $E_i = g_2^{cr_i}$

and $SK_i = (g_1^b)^{s(i)/t_i} + g_1^{d/r_i}$

then during decryption,

$$e(SK_i, E_i) = e\left(g_1^{b\,s(i)/t_i} + g_1^{d/r_i},\ g_2^{cr_i}\right)$$

$$= e(g_1,g_2)^{\frac{\cancel{b}S(i)}{\cancel{b}\cancel{r_i}} \times c\cancel{r_i}} \cdot e(g_1,g_2)^{d/\cancel{r_i} \times c\cancel{r_i}}$$

$$= e(g_1,g_2)^{cS(i)} \cdot e(g_1,g_2)^{cd}$$

↳ can be calculated and removed

we are left with $e(g_1,g_2)^{cS(i)}$

Finally, they all add up to $e(g_1, g_2)^{c\alpha}$

$= e(g_1, g_2)^{abc}$

message in ciphertext is bound by $e(g_1, g_2)^{c\alpha}$

$= e(g_1, g_2)^{abc}$

if $i \notin A^*$, $T_i = g_2^{r_i} = g_2^{t_i}$; $E_i = g_2^{cr_i}$

and $SK_i = S(i)^{1/t_i} + g_1^{d/r_i}$

then during decryption,

$e(SK_i, E_i) = e\left(S(i)^{1/t_i} + g_1^{d/r_i}, g_2^{cr_i}\right)$

$S(i)$ is of the form $L.g_1^{-K}$

$e(L.g_1^{-K/t_i}, g_2)^{cr_i} \cdot \underbrace{e(g_1, g_2)^{\frac{d}{\cancel{r_i}} \times c\cancel{r_i}}}_{\text{can be calculated and cancelled}}$

$= e(g_1^{-K/t_i}, g_2)^{Lcr_i}$

$= e(g_1, g_2)^{-LKc\cancel{r_i}/\cancel{t_i}} = e(g_1, g_2)^{-LKc}$

or if $S(i)$ is of the form g_1^K

$e(g_1, g_2)^{K/\cancel{t_i} \times c\cancel{r_i}} \underbrace{e(g_1, g_2)^{\frac{d}{\cancel{r_i}} \times c\cancel{r_i}}}_{\text{can be calculated and cancelled}}$

$= e(g_1, g_2)^{Kc}$