Privacy Engineering (408)

Computing on Untrusted Servers

Solutions

Questions 1-3 are for the Longitude privacy-preserving location sharing service.

1. Show that c_2 simplifies to $m \cdot e(g,g)^{r_a n}$ in step 4.

$$c_2 = m \cdot Z_a^{r_a} \cdot e\left(g^{r_a}, g^n h_{a2}^{-x_a}\right)$$

$$c_2 = m \cdot e(g^{x_a}, g^{z_a})^{r_a} \cdot e(g^{r_a}, g^n) \cdot e(g^{r_a}, g^{-x_a z_a})$$

$$c_2 = m \cdot e(g,g)^{x_a z_a r_a} \cdot e(g^{r_a}, g^n) \cdot e(g,g)^{-x_a z_a r_a}$$

$$c_2 = m \cdot e(g^{r_a}, g^n)$$

$$c_2 = m \cdot e(g,g)^{r_a n}$$

2. Show that step 6 produces m

$$c_2 \cdot c_1^{-\frac{1}{y_b}}$$

$$m \cdot e(g,g)^{r_a n} \cdot e(g^{r_a}, h_{b1}^n)^{-\frac{1}{y_b}}$$

$$m \cdot e(g,g)^{r_a n} \cdot e(g^{r_a}, g^{y_b n})^{-\frac{1}{y_b}}$$

$$m \cdot e(g,g)^{r_a n} \cdot e(g,g)^{-r_a y_b n \frac{1}{y_b}}$$

$$m \cdot e(g,g)^{r_a n} \cdot e(g,g)^{-r_a n}$$

$$m$$

3. In Longitude in order for Alice to revoke Bob's access to her location, Alice needs to update parts of her secret and public key and both elements of the re-encryption key for each of her remaining location-sharing friends:

(i) updates x_a in her secret key (sk_a) to a new random value x_a', note x_a is not replaced in Z_a but Z_a' will cancel it.

$sk_a = (x'_a, y_a)$

(ii) updates Z_a in her public key(pk_a) to $Z_a' = Z_a^{\,x_a'/\,x_a}$

$$pk_a = (h_{a1}, h_{a2}, z'_a)$$
$$z'_a = z_a^{x'_a/x_a}$$
$$z'_a = e(g^{x_a}, g^{z_a})^{x'_a/x_a}$$
$$z'_a = e(g,g)^{x_a z_a x'_a/x_a}$$
$$z'_a = e(g,g)^{x'_a z_a}$$
$$z'_a = e\left(g^{x'_a}, g^{z_a}\right)$$
$$z'^{\,r_a}_a = e(g^{x'_a}, g^{z_a})^{r_a}$$

(iii) raises both elements of the re-encryption key for her remaining friends (but not Bob) to the power $x_a'/\,x_a$

$rk_{a\to b} = (h_{b1}^n, g^n h_{a2}^{-x_a})$ for Alice to Bob

$rk_{a\to f} = (h_{f1}^{n'}, (g^n h_{a2}^{-x_a})^{x'_a/x_a})$ where $n' = nx'_a/x_a$ for Alice's friend f

$rk_{a\to f} = (h_{f1}^{n'}, g^{n'} h_{a2}^{-x'_a})$

Show that Alice's location sharing friend Carol can still decrypt messages, but revoked Bob can't.

For Alice's friend *f* we have

$$c_1 = e\left(g^{r_a}, h_{f1}^{n'}\right)$$
$$c_2 = m \cdot Z'^{\,r_a}_a \cdot e\left(g^{r_a}, g^{n'} h_{a2}^{-x'_a}\right)$$
$$\ldots$$
$$c_2 = m \cdot e\left(g^{r_a}, g^{n'}\right)$$
$$c_2 = m \cdot e(g,g)^{r_a n'}$$

Decryption

$$m \cdot e(g,g)^{r_a n'} \cdot e(g^{r_a}, g^{y_f n'})^{-\frac{1}{y_f}}$$
$$m \cdot e(g,g)^{r_a n'} \cdot (g,g)^{-r_a n'}$$
$$m$$

For revoked Bob (*b*) we have

$$c_1 = e(g^{r_a}, h_{b1}^n)$$
$$c_2 = m \cdot Z'^{\,r_a}_a \cdot e\left(g^{r_a}, g^n h_{a2}^{-x_a}\right)$$
$$c_2 = m \cdot e(g^{x'_a}, g^{z_a})^{r_a} \cdot e(g^{r_a}, g^n) \cdot e(g^{r_a}, g^{-x_a z_a})$$
$$c_2 = m \cdot e(g,g)^{x'_a z_a r_a} \cdot e(g^{r_a}, g^n) \cdot e(g,g)^{-x_a z_a r_a}$$

2nd and last multiplicands don't cancel!