Privacy Enhancing Techniques (408)

Computing on Untrusted Servers

Exercises

The following questions 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.

2. Show that step 6 produces m.

3. 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) replace 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.

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

   (iii) raises both elements of the re-encryption keys for each of her remaining location-sharing friends (not Bob) to the power x_a' / x_a

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