Privacy Engineering (70018)

Computing on Untrusted Servers - Solutions

3.1 Here's one solution. Others are possible also. Using some cryptographic notation in the steps is ok also.

Alice is submitting document P. Bob is searching for documents on keyword Q.
Assuming: EncH(Word, Key) = Encrypt(Hash(Keyword))

Document insertion

Alice:

```
AEP    = Encrypt(P, K)                     // Encrypt P with random symmetric key K
AK     = Encrypt(K, Ae1)                   // Encrypt symmetric key with Alice's key
AW[i] = EncH(W[i], Ae1) for each keyword   // Encrypt hashes of keywords with Alice's key
Send AEP, AK, AW[] to DB                   // Send to DB
```

DB:

```
DK    = Encrypt(AK, Ae2)            // Document encryption key now encrypted by DB(e)
DW[i] = Encrypt(AW[i], Ae2) for each keyword  // Keyword hashes now encrypted by DB(e)
Store AEP and DK indexed by each DW[i]        // e.g. Store[DW[i]] = (AEP, AK) for each i
```

Document query

Bob:

```
Send BQ=EncH(Q, Be1) to DB   // Encrypt hash of search keyword and send to DB
```

DB:

```
DQ   = Encrypt(BQ, Be2)                    // Search keyword now encrypted by DB (e)
AEP[j], DK[j] = Lookup(DQ)                 // Lookup entries for matching encrypted keywords
BK[j] = Decrypt(DK[j], Bd2) for each document j  // Documents encryption keys half
                                           // decrypted for Bob
Send AEP[], BK[] to Bob
```

Bob:

```
K[j] = Decrypt (BK[j], Bd1)          // Retrieve symmetric keys for encrypted documents
Docs[j] = Decrypt(AEP[j], K[j])      // Decrypt encrypted documents
```

3.2 Alice publishes her public key online and generates a secret function key for her spam filtering rule predicate and sends it to Bob the spam filtering service. Users sending email to Alice will encrypt the email with her public key. Bob can now determine, for each email, whether to store it in Alice's mailbox or to discard it as spam, without learning anything about Alice's email (except for whether it was considered spam or not).

3.3 (a) Show that c_2 simplifies to $m \cdot e(g,g)^{r_a n}$ in step 5.

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

(b) Show that step 6 produces m

$$c_2 \cdot c_1^{-\frac{1}{y_b}}$$
$$m \cdot e(g,g)^{r_a n} \cdot e(g^{r_a}, h_{b1}^n)^{-\frac{1}{y_b}}$$
$$m \cdot e(g,g)^{r_a n} \cdot e(g^{r_a}, g^{y_b n})^{-\frac{1}{y_b}}$$
$$m \cdot e(g,g)^{r_a n} \cdot e(g,g)^{-r_a y_b n \frac{1}{y_b}}$$
$$m \cdot e(g,g)^{r_a n} \cdot e(g,g)^{-r_a n}$$
$$m$$

(c) (i)

$$sk_a = (x'_a, y_a)$$

(ii)

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

$z_a'^{\,r_a} = e(g^{x_a'}, g^{z_a})^{r_a}$

(iii)

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

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

(iv)

For Alice's friend *f* we have

$c_1 = e\left(g^{r_a}, h_{f1}^{n'}\right)$

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

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

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

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

$c_1 = e(g^{r_a}, h_{b1}^{n})$

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

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

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

2nd and last multiplicands don't cancel!