6.857 Computer and Network Security October 31, 2002

Lecture Notes 16 : Mixnets/Voting with Frogs

Lecturer: Ron Rivest *Scribe: Many*

[These scribe notes come from two groups of students from Fall 2001, Gilliland/Li/Lustbader/Wagner and Brunsman/Leon/Lin/Cheung. Check your own notes for new discussion brought up this year.]

Outline

- Mix-Nets
- Voting with Frogs

1 Mix Nets (David Chaum)

The Mix Net scheme uses a series of permuting-devices called *mix-servers* that output a random permutation of their inputs. By using several such mix-servers in series, no single person can unscramble the order of the outputs to reveal the order of the inputs. This brings us one step closer to voter privacy.

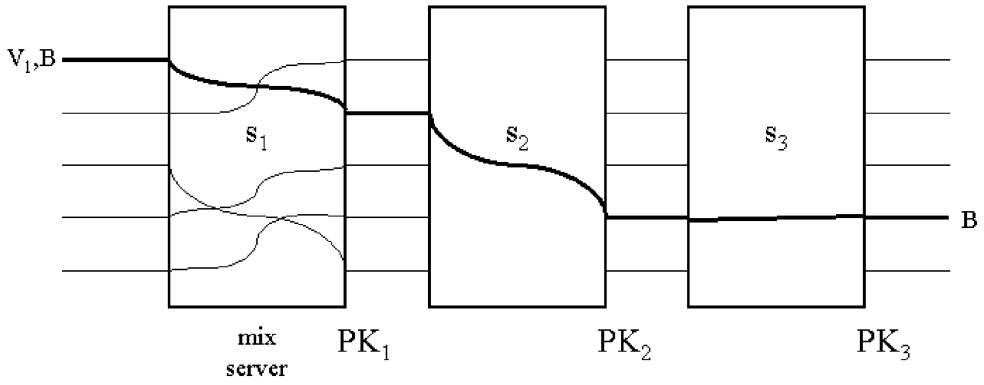

Figure 1: A Mix Net composed of three mix-servers

If the outputs are the same as the inputs, however, no amount of permutation will maintain voter anonymity. As such, we must either encrypt or decrypt the votes within the mix-servers so that the output appears different from the input.

David Chaum's approach decrypts the input within each mix-server:

$$\hat{\mathrm{B}} = PK_1(PK_2(PK_3(B)))$$

where $PK_a(X)$ is defined as the encryption of message X with public key PK_a. The voter submits $\hat{\text{B}}$ in this scheme.

A variation of this approach uses each mix-server to encrypt its input, and subsequently decrypts the final result at the end of the mix-server series. The encryption process manipulates the ciphertext input such that the contents remain the same but the appearance is different.

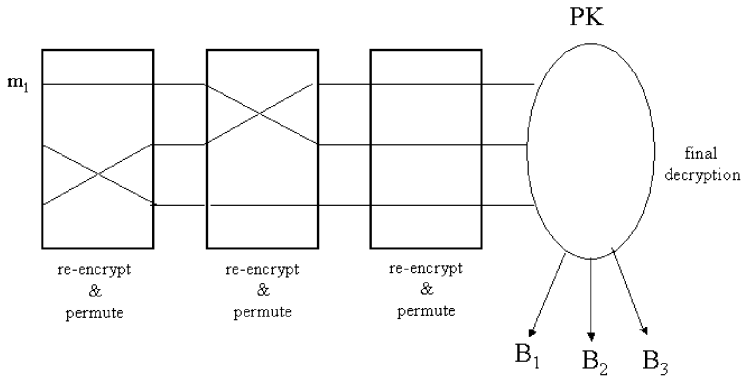

Figure 2: A variation of Chaum's Mix Next

In either approach, El Gamal can be used for encryption and decryption:

$$(PK, SK) = (y, x)$$
$$y = g^x \bmod p$$

Where g is a generator and p is a prime. The output of encryption is:

$$(g^r, m * y^r)$$

where r is a random integer and m is the message (in this case, the vote). Suppose, then, that a mix-server receives as input an encrypted ballot. The mix-server does not know the value of the secret key x, so to re-encrypt the input we simply choose a new random integer r' and multiply:

$$(g^r * g^{r'}, y^r * y^{r'} * m) = (g^{r+r'}, m * y^{r+r'})$$

Question: How do we decrypt the final output?
Answer: The same as we normally decrpyt: we simply treat $r + r'$ as the new r.

What are the risks to the Mix Net Voting Scheme? Substition attacks: we need proofs from each mix-server that the input votes are the same as the output votes. We also want these proofs to be ZK proofs to protect the election integrity.

What are the advantages of the Mix Net voting scheme? Voter anonymity: by permuting and encrypting the inputs, the output of a mix-server maintains voter privacy.

For additional reading about Mix Nets, see
http://www.inf.tu-dresden.de/∼hf2/publ/2000/BeFK2000cfp2000.

For additional reading about David Chaum, see
http://www.chaum.com/welcome.html.

2 Voting with Frogs

See the 6.857 Web page for a copy of the presentation on Voting/Frogs. Each ballot is recorded on an object called a "frog." This is not an acronym; it was chosen to be a neutral term with convenient clip-art for slides...

- A frog cannot simply be copied over and over because a randomized procedure is used for each frog. Two exact copies can be detected.
- Frogs for different voters should look different even if the voters vote the same.
- The signature schemes would have to be certified – they are part of the critical voting process.
- Vote generation hardware is important for security, but not critical. The casting hardware *is* critical.
- The voter may only approach the vote casting hardware once.