6.897: Advanced Topics in Cryptography April 30, 2004

Lecture 24: Neff Voting

Scribed by: abhi shelat

1 Introduction

This lecture is a synopsis of Neff's voting scheme.

Each ballot is identified with a unique id number, i, and a unique codebook, VC_i which maps voter options (such as Bush, Kerry, Nader) to *verification codes*. These voter verification codes are specially computed numbers (small, say 4-digit numbers which are easily parsable by humans) for each option on a ballot which are based on the secret keys of the trustees who eventually count the ballots.

In particular, the codebooks are formed as follows during the setup phase. The set of l trustees commit to each ballot i in the following way. First, the trustees independently choose secret keys $\sigma_{ij} \in \{0,1\}^k$ for $1 \leq j \leq l$. Let $\sigma_i = \bigoplus_{j=1}^{l} \sigma_{ij}$. For ballot i, the trustees jointly compute $VC_i = \{h(B_i^{\sigma_i})|B_i\}$ where B_i represents all of the possible voting configurations, and where $h()$ is the last few digits of a hash function. In addition, the trustees jointly commit to their σ_i by computing $(\alpha, \alpha^{\sigma_i})$ for a random α.

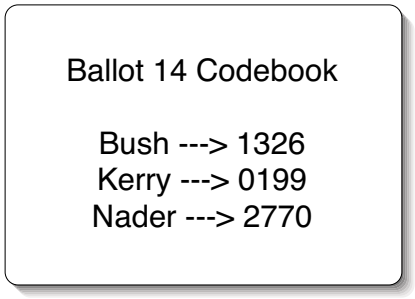

Figure 1: A sample codebook, VC_{14}, for ballot 14.

1.1 Instructions for voting

1. A voter anonymously receives a ballot i at registration along with a codebook. Note, it is important in this scheme that the codebook be destroyed at the end of the voting session (and that in particular, the voter is not allowed to leave with the codebook). Otherwise, the codebook along with the signatures that the voter receives can act as a voting receipt.

2. The voter fills out her ballot, B.

3. The voting machine prints $BR = \langle i, VC_i(B) \rangle$ for the user.

4. When the voter finalizes the vote, the machine signs BR and gives the user the signed BR. Additionally, the machine enters the encrypted vote, (g^r, By^r), into the mixnet for tabulation. The encryption is standard El Gamal encryption. In addition, the machine forwards the pair $\langle i(g^r, By^r)\rangle$ into a protocol involving the trustees.

5. The trustees take $\langle i(g^r, By^r)\rangle$ and execute a threshold function evaluation procedure in order to compute the pair $\langle i, VC_i(B)\rangle$. Along with the receipt, BR, this value allows the voter to confirm that the machine has properly prepared her ballot.

The last two steps require further explanation. How do we know that the encryption which is posted to the mixnet is the same as the ballot submitted by the user?

Given an encryption $\langle g_r, By^r\rangle$, the trustees jointly compute $\langle g^{r\sigma_i}, B^{\sigma_i} y^{r\sigma_i}\rangle$. They are then able to decrypt the value B^{σ_i}, and then publish the hash $h(B^{\sigma_i})$.

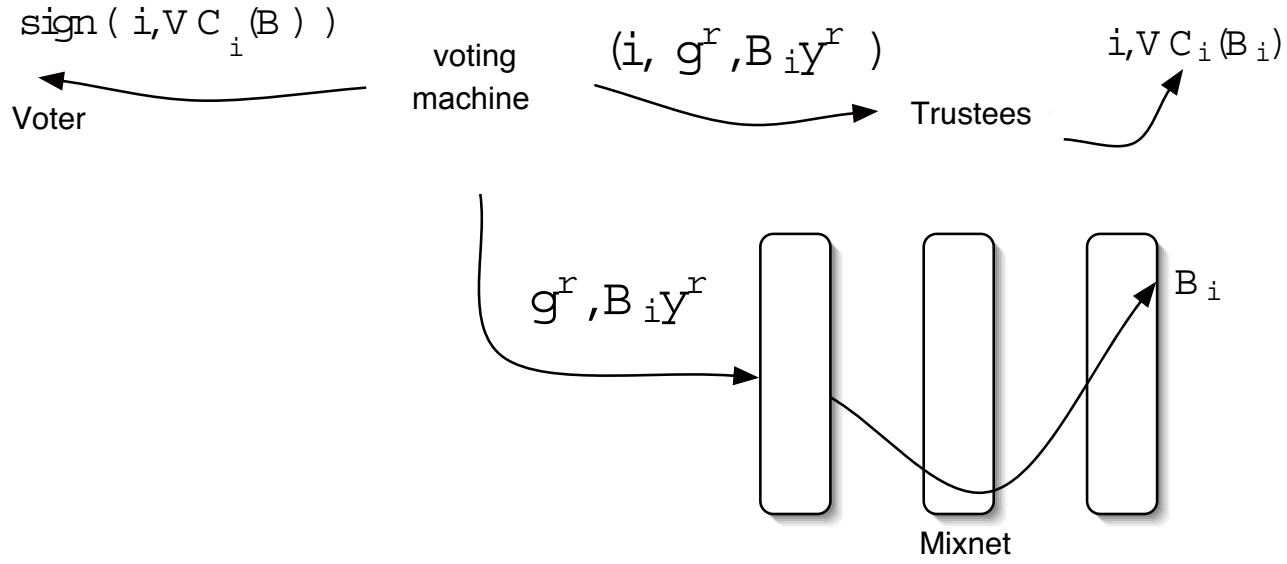

Figure 2: The trail of a ballot during the decryption process.