Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest

Handout 23
October 23, 2001

Problem Set 4-1 Solutions

Problem 4-1. Vote all you want

John Bevilacqua, Robert Kochman, Gabriel Reinstein, and Dan Itsara submitted this solution.

In order to allow voters to vote several times and have only the last one count, we can modify FOO in the following way.

When a voter wants to start voting, rather than sending a blinded version of his commitment to the Authority to get it signed, he instead creates a public key/private key pair (PK, SK), blinds the public key, and sends the blinded version of the key to the Authority. The authority checks to see that the voter is registered and eligible to vote, and if so, signs the blinded key and sends it back to the voter, and also marks down that the voter has obtained a key. Once the Authority has signed the key for a voter, the voter will not be allowed to get any more keys. After this operation, the voter has $\sigma_A(PK)$.

The voter generates a commitment x for his ballot as before, and then signs the commitment with his secret key to obtain $\sigma_{SK}(x)$. To cast a vote, the voter sends to the counter, through the anonymous channel, $(PK, \sigma_A(PK), x, \sigma_{SK}(x))$: the public key, the signature from the authority of the public key, the commitment, and the voter's signature on the commitment. First, the counter verifies that the signature on the public key from the Authority is valid—in other words, this is a valid voter. Then, he checks that the signature on the commitment is valid, using the public key—this assures him that the vote was cast by the correct voter. Finally, he checks to see if there is already a commitment registered for this public key, and if so, replaces it with the newest vote. In this way, only the last vote gets counted.

Finally, in the same way as in the FOO scheme, the reveal is sent at the end of the day and votes are counted.

Completeness is maintained, because each valid vote will be counted. It has soundness because voting cannot be interrupted and votes can't be forged or replaced without knowing a voter's secret key. Although each voter is uniquely identified through his or her public key, this system has Privacy because public keys have nothing to do with the voter ID—and, because the Authority only sees a blinded version of the public key, even if the Authority colluded with the Counter, there would be no way to link a voter ID to a particular vote. Eligibility is clear, because the Authority still checks each voter, and a vote can't be cast without an authorization from the Authority. It's still fair and verifiable, as it uses the same reveal procedure as before.

Finally, in terms of unreusability, each voter can vote as many times as he likes, but only the last one will be counted. In order to cast a valid vote which will be counted, he must use his public key which was verified by the Authority. But, since the Counter keeps a table which links each vote to a public key, each new vote will replace any previous votes made by the voter.