**T-79.159 Cryptography and Data Security** **Spring 2003**
**Tutorial 10: Solutions**
**15.–16.4.2003**

1. In the withdrawal phase of the Chaum-Fiat-Naor E-cash protocol, the user generates $2k$ messages of the form $(H(r_i), H(r_i \oplus Id))$, where $r_i$ is a random string and $Id$ is the user's identity. He then sends them blinded to the bank. The bank picks at random $k$ of the messages and asks the user to unblind them. The bank verifies that the $k$ messages are correctly formed and signs blindly the remaining messages. The bill consists of the remaining messages and their signatures.

   In a completely faked bill that does not contain the user's identity at all, the user must construct $k$ correct messages and $k$ incorrect messages. If the bank asks the user to unblind any of the faked messages, she is caught. Thus, the probability that the user succeeds in creating a completely faked bill is
$$\binom{2k}{k}^{-1} = \frac{(k!)^2}{(2k)!} \ .$$
   For $k = 50$, this is about $2^{-96.35}$.

2. In the payment phase, the seller picks $k$ bits $c_1, \ldots, c_k$ and sends them to the buyer. If $c_i = 0$, the buyer replies with $(r_i, H(r_i \oplus Id))$. If $c_i = 1$, the buyer replies with $(H(r_i), r_i \oplus Id)$. In both cases, the seller can compute $(H(r_i), H(r_i \oplus Id))$ and verify the bank's signature on it.

   In the deposit phase, the seller sends the challenge $c_1, \ldots, c_k$ and the corresponding replies from the buyer to the bank. The bank verifies the messages. If the user reuses a valid bill and the challenges in the payment step differ in (say) the $i$th bit, $c'_i \neq c_i$, the bank learns both $(r_i, H(r_i \oplus Id))$ and $(H(r_i), r_i \oplus Id)$. Thus, the bank can compute $r_i \oplus (r_i \oplus Id) = Id$ and the user's identity is revealed.

   If the user succeeds in reusing a valid bill, both challenges must be the same. This happens with probability $2^{-k}$, which is much higher than the success probability in Exercise 1.

3. The seller have to come up with two different challenges and the corresponding buyer replies—otherwise, the bank gets two identical transcripts that does not reveal the buyer's identity. Thus, the bank can detect that the seller is trying to cheat. In order to come up with two different valid transcripts, the seller must find an $r$, an identity $Id$ and the bank's signature on $(H(r), H(r \oplus Id))$—this would require breaking either the hash function or the signature scheme.

4. The idea here is that if the user leaves her identity on some parts of the bill, she can hope that, when reusing the bill, the buyer will pick a new challenge that only differs in the bits corresponding to the parts with faked identity. We assume that the user creates $\ell$ messages with a faked identity, $1 \leq \ell \leq k$, and $2k - \ell$ valid messages in the withdrawal phase. Since there are $\binom{2k}{k}$ sets of size $k$ and $\binom{2k-\ell}{k}$ sets of size $k$ that contain only valid

messages, the probability that the bank does not detect that the user is cheating in the withdrawal phase is

$$\binom{2k-\ell}{k}\binom{2k}{k}^{-1} .$$

This probability is larger than the probability in Exercise 1 by a factor of $\binom{2k-\ell}{k} = \frac{(2k-\ell)!}{(k-\ell)!k!}$.

The probability that the user succeeds in reusing the bill once without getting caught is $2^{-(k-\ell)}$, since her identity is only revealed if the two challenges differs in some of the $k-\ell$ bits that corresponds to messages containing her identity. This is larger than the probability in Exercise 2 by a factor of $2^{\ell}$.

The probability of not getting caught in the withdrawal phase decreases with $\ell$ whereas the probability of not getting caught when reusing a bill grows with $\ell$. Thus, there is a trade-off between the two probabilities. One measure for the total cheating probability is the product $\binom{2k-\ell}{k}\binom{2k}{k}^{-1}2^{-(k-\ell)}$ (assuming that both events are independent, this is the probability that the user succeeds in cheating in both phases). Numerically, is is easy to see that the product decreases with $\ell$. For small values of $\ell$, it is close to $2^{-k}$. Thus, the user cannot cheat in this way with a probability larger than $2^{-k}$.

We conclude that the best cheating strategy is to be honest in the withdrawal phase and try to reuse a valid bill. This succeeds with probability $2^{-k}$.