The Theory Behind Blockchains (Spring 19)
Problem Set 5

Submission: By 15:00 on June 12th, 2019. To be graded by Nathan Geier.

Instructions: You can collaborate with each other and consult external resources. However, you should write the solution on your own, and for each question, list all collaborators and external resources. Otherwise, write explicitly "None". Do not discuss solutions in the course forums; you are welcome to ask for clarifications if needed.

1 Unique Signatures (35 points)

a. **(15 points)** RSA signature: Let $N, e \in \mathbb{N}$, let $\phi(N) = |\mathbb{Z}_N^*|$ where $\mathbb{Z}_N^* = \{x \in [N-1] : \gcd(x, N) = 1\}$, and let $\ell = \gcd(\phi(N), e)$. Prove that the mapping $x \mapsto x^e \bmod N$ over $x \in \mathbb{Z}_N^*$ is ℓ-to-1, i.e. for every image point $y \in \mathbb{Z}_N^*$ there exists ℓ distinct $x_1, \ldots, x_\ell \in \mathbb{Z}_N^*$ such that $x_i^e = y$ for all $i \in [\ell]$. Conclude that in the case $N = p \cdot q$ (for distinct primes p and q), the mapping $x \mapsto x^e \bmod N$ over $x \in [N-1]$ is a permutation iff $\gcd(\phi(N), e) = 1$.

b. **(10 points)** Consider the unique signature scheme from recitation 9 using general TDPs $(\text{Gen}_T, F, F^{-1})$. Assume that every key $pk \in \{0,1\}^n$ defines a function $F_{pk} : \{0,1\}^n \to \{0,1\}^n$. Describe a proof system that allows proving that a given public key $pk \in \{0,1\}^n$ represents a function that is $\frac{1}{n}$-close to a permutation:

- If F_{pk} is a permutation, the verifier should always except.
- If the size of F_{pk}'s image is at most $(1-\frac{1}{n})2^n$, the verifier rejects with constant probability.

c. **(10 points)** Assume that every pk defines a function $F_{pk} : \{0,1\}^n \to \{0,1\}^{2n}$. Describe a proof system for proving that the function is $\frac{1}{n}$-close to injective:

- If F_{pk} is a injective, the verifier should always except.
- If the size of F_{pk}'s image is at most $(1-\frac{1}{n})2^n$, the verifier rejects with constant probability.

2 Algorand's Consensus (35 points)

In this question, we consider several variations of Algorand. Assume that at the beginning of round r there are $N(r)$ nodes in the system, each with equal stake and that the function $N(r)$ is known through all rounds (on the blockchain). Throughout this question $H : \{0,1\}^* \to \{0,1\}^n$ is a hash function, modeled as a random oracle.

a. **(10 points)** Consider a variant of Algorand, where a given user, represented by a public key pk for a unique signature, that has joined the system by round r (by publishing her key on the blockchain) is on the committee for round $r+1$ if

$$H(Sign_{sk}(r)) \leq n2^n/N(r) \ ,$$

where $Sign_{sk}(r)$ is a signature on r with secret key sk corresponding to pk.

Describe an attacker that joins the system before round r and ensures that she is on the committee in round $r+1$ with probability 0.99. (The attacker's running time may scale with $N(r)$ and n).

b. **(10 points)** Consider yet another variant where we change the condition for choosing the committee/leader to

$$H(S_{r+1}, Sign_{sk}(r+1)) \leq n2^n/N(r) \ ,$$

where S_{r+1} is a string arbitrarily chosen by the leader of round r.

Describe an attacker that controls 10% of the nodes in the system and within a constant number of steps (in expectation) takes control of the entire system.

c. **(15 points)** Imagine instead that $S_{r+1} = H(S_r, Sign_{sk^*}(r+1))$ where sk^* is the secret key of the leader of round r. Assume that the leader always sends its signature (does not withhold it).

Assume the leader of any round r is chosen only among the users who have already published their public keys by round $r-n$ where in the first n rounds there is some default honest leader. Argue that the previous attack fails, except with negligible probability $2^{-\Omega(n)}$. No need for a formal proof.

3 Anonymous Coins (30 points)

The following question addresses various aspects of Zerocoin, which we touched in class. In what follows, assume that all zero knowledge proofs are non interactive.

a. **(15 points)** Say that a node with public key pk receives a zerocoin, namely a serial number S, plus a zero knowledge proof π that S corresponds to one of the zerocoin commitments on the blockchain. Consider a "take the money and run" attack where before the last transaction reaches the blockchain, the node pk tries to steal the coin and pay (S, π) to a different node pk'.

Describe how to use one-time signatures schemes and augment zerocoin to make sure that a zerocoin paid to pk cannot be redirected to some $pk' \neq pk$.

b. **(15 points)** In zerocoin the size of the zero knowledge statement to be proven scales with all zerocoins ever created (although the witness is small). Suggest how to use Merkle trees to guarantee that the statement only scales logarithmically in the amount of all coins. Say explicitly what are the zero knowledge statement and corresponding witness in your suggested solution.