CS 5594: Blockchain Technologies (Spring 2021)

Homework 1
Due March 05, 2021 (Friday) 11:59 PM

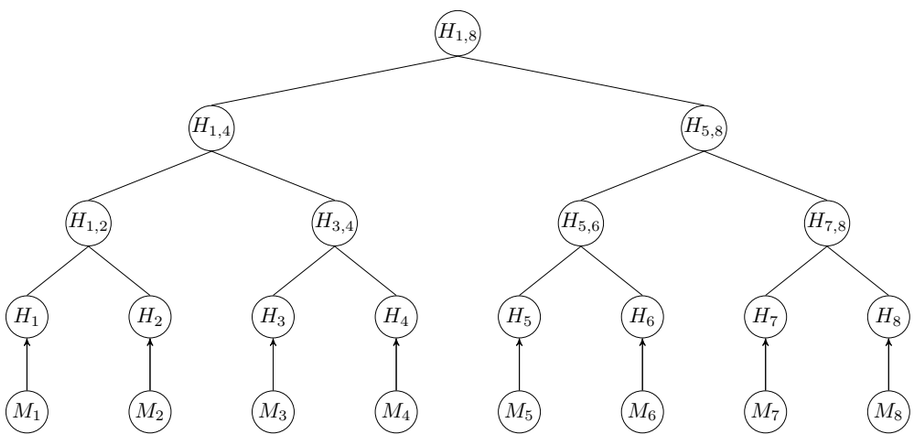
1. Prove that a distributed system cannot achieve three attributes: Consistency, Availability, and Partition Tolerance simultaneously (CAP Theorem). (5pt)

2. Show how public blockchain manages to achieve Consistency, Availability, and Partition Tolerance. Specifically, which attribute is scarified in favor of the other two attributes? Describe the core technique that the public blockchain used to fully achieve those two attributes, while managing to (eventually) offer the remaining one. (10pt)

3. What is the random oracle and its relevance to hash functions? Describe the birthday attack against hash functions. Given an n-bit hash output, mathematically formulate the upper bound of collision probability. Specifically, write how birthday paradox is formulated (use approximations if needed). (5pt)

4. Provide formal definitions for second preimage resistance and preimage resistance. Prove that any hash function that is collision resistance is second preimage resistance. (5pt)

5. Suppose a sender S uses the following Merkle-hash tree T to authenticate these messages to a receiver R.



   (a) How would one authenticate message M_4? Write which elements of T must be transmitted from S to R, and write the correct verification equation. (5pt)

   (b) Explain why the Merkle-hash tree T has an additional level of hash in the leaves? (5pt)

   (c) What are two necessary conditions for a set of data to be authenticated by the Merkle-hash tree? (3pt)

   (d) Show how to find a collision in the Merkle-hash tree with a *flexible* structure (i.e., the number of the inputs is not fixed). Specifically show how to find two sets of inputs $\mathcal{S} = \{x_1, \ldots, x_t\}$ and $\mathcal{S}' = \{x'_1, \ldots, x'_{2t}\}$ such that $\mathsf{MerkleRoot}(\mathcal{S}) = \mathsf{MerkleRoot}(\mathcal{S}')$. (5pt)

   (e) Describe how Merkle-hash trees are used to achieve integrity in public blockchain (e.g., bitcoin). (2pt)

6. Consider the plain RSA signature scheme as follows.

   - Gen: Given a security parameter λ, generate a public key $pk = (e, N)$ and a private key $sk = (d, N)$ as in the original RSA signature scheme.
   - Sign: Given a private key $sk = (d, N)$ and a message $m \in \mathbb{Z}_N^*$, compute the signature as $\sigma := m^d \mod N$.
   - Verify: Given a public key $pk = (e, N)$, a message $m \in \mathbb{Z}_N^*$, and a signature $\sigma \in \mathbb{Z}_N^*$, output 1 if and only if $m = \sigma^e \mod N$.

   (a) Show that the attacker can forge the signature of any message of its choice by querying *two* signatures from the signer that uses the plain RSA signature scheme above. (5pt)

   (b) Show that the attacker can forge the signature of any message of its choice by querying only a *single* signature from the signer. (5pt)

7. Consider a variant of DSA algorithm, in which the second component of the signature generation is computed as $s := k^{-1} \cdot (m + xr) \mod q$ (instead of $s := k^{-1} \cdot (H(m) + xr) \mod q$). Show that this variant is not secure, in which the attacker can forge valid signature for any arbitrary message of it choice without querying any signatures from the signer. (10pt)

8. In 2010, Sony PS3 was hacked by a group of hacker named fail0Overflow, who demonstrated a key recovery attack on the ECDSA digital signatures computed by Sony PS3. Explain what caused the attack and show the steps of the attack in details. (10pt)

9. Compute nP in $E(\mathbb{F}_p)$ using the *double-and-add* algorithm for the following ECC curves.

   (a) $E : Y^2 = X^3 + 23X + 13$, $p = 83$, $P = (24, 14)$, $n = 19$ (2pt)

   (b) $E : Y^2 = X^3 + 143X + 367$, $p = 613$, $P = (195, 9)$, $n = 23$ (2pt)

   (c) $E : Y^2 = X^3 + 1828X + 1675$, $p = 1999$, $P = (1756, 348)$, $n = 11$ (2pt)

   (d) $E : Y^2 = X^3 + 1541X + 1335$, $p = 3221$, $P = (2898, 439)$, $n = 3211$ (4pt)

10. Consider the following ECC curve:

$$E : Y^2 = X^3 + 231X + 473, p = 17389, q = 1321, G = (11259, 11278) \in E(\mathbb{F}_p).$$

    (a) Assume the signing key of Alice is $sk = 542$. What is her corresponding public key? What is her signature on the message $m = 644$ with ephemeral key $e = 847$? (5pt)

    (b) Assume the public key of Bob is $pk = (11017, 14637)$. Is $(s_1, s_2) = (907, 296)$ his valid signature on message $m = 993$? (5pt)

    (c) Assume the public key of Dave is $pk = (14594, 307)$. What is his private key sk? (you can use any method you want to find it). Use his private key sk that you found to forge his signature on a message $m = 516$ using ephemeral key $e = 365$. (5pt)