CSE 5852: Problem Set 9

Due: December 5, 2016

In this assignment you'll be working with hash functions. Recall the different security properties of a hash function:

Collision resistance For all PPT $\mathcal{A}$, there exists a negligible function $\epsilon(n)$ such that for $k \leftarrow \mathsf{Gen}(1^n)$,

$$\Pr[(m_1, m_2) \leftarrow \mathcal{A}(1^n, k) \wedge m_1 \neq m_2 \wedge H_k(m_1) = H_k(m_2)] \leq \epsilon(n).$$

this probability is over the choice of k and any randomness used by $\mathcal{A}$.

Second-preimage resistance A hash function is second preimage resistant if given k and a uniform m it is infeasible for a PPT adversary to find some $m' \neq m$ such that $H_k(m') = H_k(m)$. Note: Look at the distinction between this and collision resistance. Here $\mathcal{A}$ doesn't get to choose the point m they are forced to find a preimage on a random point.

Preimage resistance A hash function is preimage resistant if given k and uniform y it is infeasible for a PPT $\mathcal{A}'$ to find a value m such that $H(x) = y$.

1 Collision-resistant hashing

20 pts

Theorem 1. *Let $H : \{0,1\}^\ell \times \{0,1\}^{n+k} \to \{0,1\}^n$ be a family of collision resistant hashes. Show that $H' : \{0,1\}^\ell \times \{0,1\}^{n+2k} \to \{0,1\}^n$ defined as follows is a family of collision resistant hashes:*

1. *$H'_k(m)$. Interpret $m = m_{1...k}, m_{k+1...n+2k}$. Set $y = H_k(m_{k+1....n+2k})$.*
2. *Compute $z' = H_k(m||y)$.*

Show that this H'_k is collision resistant. Let m, m' be a collision output by $\mathcal{A}$. Separately consider the following cases (what is the collision output by $\mathcal{A}'$?):

1. **5 pts** $m_{k+1...n+2k} \neq m_{k+1...n+2k}$ and $y = y'$.
2. **5 pts** $m_{1...k} = m'_{1...k}$ and $m_{k+1...n+2k} \neq m_{k+1...n+2k}$ and $y \neq y'$.
3. **5 pts** $m_{1...k} \neq m'_{1...k}$ and $m_{k+1...n+2k} \neq m_{k+1...n+2k}$ and $y \neq y'$.
4. **5 pts** $m_{1...k} \neq m'_{1...k}$ and $m_{k+1...n+2k} = m_{k+1...n+2k}$.

20 pts Consider a hash function $H : \{0,1\}^\ell \times \{0,1\}^{2n} \to \{0,1\}^n$. Consider the following adversary $\mathcal{A}$:

1. While all y_i are distinct:

   Choose random (but distinct) x_i.

   Compute $y_i = H_k(x_i)$.

2. Output x_i, x_j such that $H_k(x_i) = H_k(x_j)$.

10 pts Assume an output space of 2^n. What needs to happen for each value x_i to be unique? What is that probability? Your answer can be an algebraic expression, you don't need to try and simplify? Does this quantity get bigger or smaller with the number of guesses?

10 pts Assume we want to build an adversary that succeeds with probability .5 how many x_i need be generated by $\mathcal{A}$? You can consult https://en.wikipedia.org/wiki/Birthday_problem for some approximations on this value.

2 Repeated Hashing

20 pts Let Gen, H be a family of collision resistant hash functions. Define Gen', H' as the following:

- Gen': Set $k = k_1, k_2$ where $k_1 \leftarrow \mathsf{Gen}(1^n)$ and $k_2 \leftarrow \mathsf{Gen}(1^n)$.
- $H'_{k_1,k_2}(m) = H_{k_1}(m)||H_{k_2}(m)$.

Show that (Gen', H') is collision resistant. Provide a reduction to the collision resistance of (Gen, H).

20 pts Let Gen_1, H_1 and Gen_2, H_2 be two families of second-preimage resistant hash functions. Define Gen, H as the following:

- $k = k_1, k_2$ where $k_1 \leftarrow \mathsf{Gen}_1(1^n)$ and $k_2 \leftarrow \mathsf{Gen}_2(1^n)$.
- $H_{k_1,k_2}(m) = H_{1,k_1}(m)||H_{2,k_2}(m)$.

Show that (Gen, H) is second-preimage resistant if both (Gen_1, H_1) and (Gen_2, H_2) are second preimage resistant.

20 pts Let Gen_1, H_1 and Gen_2, H_2 be two families of preimage resistant hash functions. Define Gen, H as the following:

- $k = k_1, k_2$ where $k_1 \leftarrow \mathsf{Gen}_1(1^n)$ and $k_2 \leftarrow \mathsf{Gen}_2(1^n)$.
- $H_{k_1,k_2}(m) = H_{1,k_1}(m)||H_{2,k_2}(m)$.

Provide an example of Gen_1, H_1 and Gen_2, H_2 such that Gen, H is not preimage resistant.

20 pts Let Gen_1, H_1 and Gen_2, H_2 be two families of preimage resistant hash functions. Define Gen, H as the following:

- $k = k_1, k_2$ where $k_1 \leftarrow \mathsf{Gen}_1(1^n)$ and $k_2 \leftarrow \mathsf{Gen}_2(1^n)$.
- $H_{k_1,k_2}(m) = H_{1,k_1}(m) || H_{2,k_2}(m)$.

Provide an example of Gen_1, H_1 and Gen_2, H_2 such that Gen, H is not preimage resistant.