| | | |
|---|---|---|
| 6.875 Spring 2017 | **Problem Set 4** | Problem 1 |
| Skanda Koppula | | |
| *Collaborators: Jonathan Frankle, Sam DeLaughter* | | April 22, 2017 |

**Problem 1.1** The function $H' : \{0,1\}^m \to \{0,1\}^n$ that applies the one-bit compression UOWHF $H$ repeatedly is also a UOWHF. Specifically, for a size-$m$ input $x$ and key $K = k_m | k_{m-1} | \dots | k_n$:

$$H'_K(x) = H_{k_m}(H_{k_{m-1}}(\dots H_{k_n}(x)))$$

We show that this construction is a UOWHF by contradiction. Suppose there existed a PPT $A$ that could produce such a colliding $x'$ for $H'$ (as per the UOWHF definition). We construct a PPT $B$ that breaks the UOWHF-ness of $H_{k_t}$ with probability $\frac{1}{\text{poly}}$:

1. $B$ begins by querying $A$ for its commitment pre-image $x$.
2. $B$ then guesses a specific location $t$ in the chain/UOWHF to break. The choice of $t$ is $m \leq t < n$, a poly-sized number of choices to guess among.
3. $B$ picks $k_t, k_{t-1}, \dots k_n$, and evaluates $\gamma = H_{k_t}(H_{k_{t-1}}(\dots H_{k_n}(x)))$.
4. Declare $\gamma$ as the commitment pre-image for the UOWHF $t$ that we chose to break.
5. Following UOWHF protocol, key $k_t$ is selected, and we select keys $k_m, k_{m-1}, \dots, k_{t+1}$ as well.
6. $B$ queries $A$ for its collision, $x'$.
7. $B$ outputs its collision guess $\gamma' = H_{k_t}(H_{k_{t-1}}(\dots H_{k_n}(x')))$.

$B$ outputs the correct guess $\gamma'$ with atleast $\frac{1}{m-n} = \mathsf{non\text{-}negl}(x)$ probability. By definition, $H'_K(x) = H'_K(x')$. This means that at some point in the chain, evaluation of the hash chain must switch from differing to being the same (evaluating on input $x$ vs. $x'$). The probability we select the correct such switching point $t$ is $\frac{1}{\mathsf{poly}}$, implying that $B$ breaks the UOWHF-ness of $H$ a non-negligible amount, contradiction. No $B$ can exist, $H'$ is a UOWHF.

**Problem 1.2.a.**

That $\bar{H}$ is a function that compresses its input by one bit is clear from the dimensionality of $M : n \times n + 1$. What remains is showing that $\bar{H}$ is universal: that given two randomly chosen $(x_1, y_1)$ and $(x_2, y_2)$, the probability of choosing $M$ such that $Mx_1 = y_1$ and $Mx_2 = y_2$ is $\frac{1}{2^{2n}}$

The total size of the space of all binary $n \times n + 1$ matrices is $2^{n(n+1)}$. Denote $M[i]$ as the $i$-th row of $M$, and $y[i]$ as the $i$-th entry in $y$. Mechanics of matrix multiplication tell us that $M[i] \cdot x_1 = y_1[i]$ and $M[i] \cdot x_2 = y_2[i]$. This means that every row corresponds to an underconstrained 2-equation, $n+1$ variable linear equation with binary coefficients and variables. From counting principles, we see that there are $2^{n-1}$ satisfying assignments to each row $M[i]$, and thus $2^{n(n-1)}$ $M$'s that satisfy the universal hash function condition. The probability of picking such an $M$ is thus $\frac{2^{n(n-1)}}{2^{n(n+1)}} = \frac{1}{2^{n(n+1)-n(n-1)}} = \frac{1}{2^{2n}}$ as desired for universality.

**Problem 1.2.b.**

This reduces to sampling a row-rank-$n$ $M$ such that $My = M(x_2 - x_1) = 0$. If we are able to sample a full-rank $n \times n$ matrix $M'$, we can always compute the necessary values for the last column in $M$ to satisfy the linear equality. This reduces the problem to sampling a full rank $n \times n$ matrix in poly-time w.h.p.

If we randomly sample the binary column vectors of the matrix in order: the first column vector is trivially linearly independent. The second column is linearly dependent with the first column vector with probability $\frac{1}{2^n}$, so the probability that it is linearly independent is $1 - \frac{1}{2^n}$. Similarly, the probability that the third column is linearly dependent with the first two is $\frac{2}{2^n}$, so the probability that it's linearly independent is $1 - \frac{1}{2^{n-1}}$. Because each draw is independent, the probability that all $n$ vectors are linearly independent is:

$$p(n) = \prod_{i=0}^{n-2} 1 - 2^{-(n-i)}$$

We want to show that $p(n)$ is greater than some constant non-negl $c$. Using the lower bound $e^{-2x} \leq 1 - x$ for every term in the product above, we obtain:

$$p(n) \geq \prod_{i=0}^{n-2} e^{-\frac{2}{2^{n-i}}} = e^{-2\sum_{j=2}^{n} \frac{1}{2^j}} = e^{-2(\frac{1}{2} - 2^{-n})} = e^{2^{-n+1}-1} \geq \lim_{n\to\infty} e^{2^{-n+1}-1} = \frac{1}{e}$$

This shows that we obtain a full rank matrix with non-negligible probability.

**Problem 1.2.c.**

$H_{M,i}(x)$ compresses its input by a single bit by virtue of the size-preserving permutation, and the single-bit compression function $\bar{H}$. We show $H$ is a UOWHF by contradiction. Assume there were a PPT $A$ that could break the UOWHF-ness. Using $A$, we construct PPT $B$ to break the one-wayness of permutation $f_i(x)$. On challenge input $f_i(\alpha)$:

1. Begin by querying $A$ for its commitment pre-image $x$
2. Use the Part 1.2.b. to sample $M$ such that $Mf_i(\alpha) = Mf_i(x)$.
3. Extract from $A$ the colliding pre-image $x'$ such that $Mf_i(x) = Mf_i(x') = \gamma$.
4. Output $x'$.

By Lemma 1.2.c, with high probability (non-negligible), there are only two non-zero values of $f_i(\zeta)$ that map to $\gamma$. This fact, combined with the fact that $Mf_i(x) = Mf_i(x') = Mf_i(\alpha)$, and the fact that $f_i$ is a permutation, means $\alpha$ must be either $x$ or $x'$ with non-negligible probability. This increases the probability of a one-wayness break of $f_i$ to non-negligible, contradiction. No such $A$ can exist, and $H$ is a UOWHF.

Proof of Lemma 1.2.c (with non-negligible probability, there is no other unique $x''$ such that $Mx' = Mx'' = Mx'' = \gamma$. The probability that $M\beta = \gamma$ is $\frac{1}{2^n}$. The probability that this is not the case is $1 - \frac{1}{2^n}$. Now, we want this to be true for all $x'' \neq x, x', 0$ in the input space of $f_i(x) = \beta$. There are $2^{n+1} - 3$ such possible inputs. Thus, the total probability that there is no other input that maps to $\gamma$ is thus:

$$p = (1 - \frac{1}{2^n})^{2^{n+1}-3} \geq e^{-2(\frac{1}{2^n})(2^{n+1}-3)} = e^{\frac{3}{2^{n-1}}-4} \geq \lim_{n\to\infty} e^{\frac{3}{2^{n-1}}-4} = \frac{1}{e^4}$$

Here, we've applied the bound $1 - x \geq e^{-2x}$. This shows the probability of no third valid $x''$ existing is bounded above a non-negligible amount.