CS 346 Class Notes

Mark Lindberg

Mar 2, 2016

Last Time:
A strongly universal function:
Let p be prime.
$\mathcal{K} = \mathbb{Z}_p \times \mathbb{Z}_p$
$\mathcal{M} = \mathcal{T} = \mathbb{Z}_p$.
Then $h_{a,b}(m) = (a \times m + b) \mod p$, where $(a, b) = k \in \mathcal{K}$.
To show the strong universality we need:
$\forall m, m', t, t' \in \mathbb{Z}_p$ such that $m \neq m'$,
$\Pr[h_{a,b}(m) = t \wedge h_{a,b}(m') = t'] = \frac{1}{p^2}$,
where the probability is taken over the uniform choice of key a, b.
This Time:
We'll prove it!
$(am + b) \mod p = t$, $(am' + b) \mod p = t'$.
We'll argue there is a unique key a, b satisfying these equations.
Then, assume without loss of generality that $m' > m$. (Swap if necessary.) $t - t' \mod p = (a(m' - m)) \mod p$.
Let $x \in \{1, \ldots, p - 1\}$.
Then $ix \mod p$, $jx \mod p$ differ for $i, j \in \mathbb{Z}_p$, $i \neq j$.
PBC: Assume $j > i$, without loss of generality, such that $jx \mod p = ix \mod p$. Then $x(j - i) \mod p = 0$, then $p \mid x(j - i)$, since p is prime, $p \mid x$ or $p \mid j - i$. But $x, j - i \in \{1, \ldots, p - 1\}$, so contradiction.
The above shows that since $m' - m \leq p$, then there $\exists! a$ satisfying the equation. Then we can solve for b, and show that there is a unique key. Since there is a unique key, we see that probability is indeed $\frac{1}{p^2}$.

Chapter 5. Hash functions and applications.

Definition of a hash function: (Gen, H)
$\mathsf{Gen}(1^n)$ runs in polynomial time, and returns a key s. (We assume n is implicit in s.)
For any binary string x, $H^s(kx)$ is an $\ell(n)$-bit binary string.
Fixed-length version: If H^s is only defined for strings of length $\ell'(n)$, where $\ell'(n) > \ell(n)$, it is called a fixed-length hash function for inputs of length $\ell'(n)$. "compression function"
Collision resistance: It is hard to find input string hashing to the same output strings.

$\mathsf{Hash\text{-}coll}_{\mathcal{A},\Pi}(n)$. Run $\mathsf{Gen}(1^n) \to s$. $\mathcal{A}$ is given s, and also n, and outputs x, x'. The experiment outputs 1 iff $x \neq x'$ and $H^s(x) = H^s(x')$.

In the fixed-length case, we also require that $|x| = |x'| = \ell'(n)$.

(Gen, H) is collision resistant if $\forall$ PPT adversary $\mathcal{A}$, $\Pr[\mathsf{Hash\text{-}coll}_{\mathcal{A},\Pi}(n) = 1] \leq \mathtt{negl}(n)$.

Merkle-Damgård Transform:

Shows how to use a collision resistant fixed-length hash function (Gen, h) to obtain a collision resistant hash function (Gen, H) for arbitrary-length strings.

We'll assume that $\ell(n) = n$, and $\ell'(n) = 2n$ for h.

Construction: Let $IV = 0^n$. $x = x_1, x_2, \ldots, x_d$, where $|x_1| = |x_2| = \cdots = |x_d| = \ell(n)$, where last block is padded if necessary. Note that $d = \left\lceil \frac{|x|}{m} \right\rceil$. THIS IS WRONG: FIX WHEN UNDERSTAND s: Then $z_1 = h^{0^n}(x_1)$, $z_2 = h^{h_1}(x_2)$, $\ldots$. We introduce another block m_{d+1} which is the n-bit binary encoding of $|x|$. (Requires $|x| < 2^n$, ridiculously easy if $n = 128$ or something.)

Claim: $\Pi = (\mathsf{Gen}, h)$ is collision resistant $\Rightarrow \Pi' = (\mathsf{Gen}, H)$ is collision resistant.

Let $\mathcal{A}'$ be an arbitrary adversary in the experiment $\mathsf{Hash\text{-}coll}_{\mathcal{A}',\Pi'}(n)$. We'll construct an $\mathcal{A}$ for Π from $\mathcal{A}'$. How do we do this?

Run $\mathsf{Gen}(1^n)$, as in $\mathcal{A}'$, to get s. Simulate $\mathcal{A}'$ to get x, x'. Problem: $\mathcal{A}$ needs to output $2n$-bit strings. We have 2 cases:

1. $|x| \neq |x'|$. Then we can feed in the last blocks and have a collision in the original.

2. $|x| = |x'|$. Walk from the back until we find the first non-equal block, and that one gives a collision in the original.

   (Yeah, I don't understand this fully. I'll revise these notes after I've read the textbook on this...)

Example: Given $\Pi_1 = (\mathsf{Gen}_1, H_1)$, and $\Pi_2 = (\mathsf{Gen}_2, H_2)$, and we know that (at least) one of these is collision resistant. We'll define a $\Pi(\mathsf{Gen}, H)$ where Gen runs $\mathsf{Gen}_1 \to s_1$, $\mathsf{Gen}_2 \to s_2$, and output s_1, s_2. Then $Hs_1, s_2(x) = H_1^{s_1}(x) || H_2^{s_2}(x)$. Π is collision resistant:

Proof-ish: If we had an $\mathcal{A}$ for Π, we could define $\mathcal{A}_1$ and $\mathcal{A}_2$ for Π_1 and Π_2 respectively, and where we have a collision for x, x' with Π, we have collisions for x, x' with Π_1 AND Π_2 with s_1 and s_2 respectively. Then neither are secure. :)