SE 4472 / ECE 9064
Information Security

Collisions in Hash Functions

Given a hash function $\mathcal{H}$ where

$$\mathcal{H} : \{0,1\}^* \to \{0,1\}^\ell,$$

how many messages would you have to hash until you would expect to find a collision, i.e., two messages $m_i \neq m_j$ for which $\mathcal{H}(m_i) = \mathcal{H}(m_j)$?

A related problem in the so-called *birthday problem*: how many people would you need to gather in a room before you would expect there to be two people that shared a birthday?

The Birthday Problem

Although there are $n = 365$ possible birthdays, it turns out you only need $k = 23$ people for the probability of two people sharing a birthday to be greater than 50%.

Now instead of $n = 365$ birthdays, suppose we have $n = 2^\ell$ possible hash values. How many messages k must we hash for the probability of two messages hashing to the same value to be greater than 50%? Let's try to compute this probability for arbitrary n, k.

Generalized Birthday Problem

Draw k things uniformly at random from the range $1 \ldots n$. What is the probability of at least one duplicate? Let's break it down. First we observe:

$$P(\text{duplicates} > 0) = 1 - P(\text{duplicates} = 0).$$

Ok, so what is $P(\text{duplicates} = 0)$? Well let's figure it out for the base case. If you draw one thing the probability it is not duplicate is

$$P(\text{one thing not duplicate}) = \frac{n}{n}.$$

If you draw two things, the probability the second thing is different from the first thing equals the number of ways to be different from the first thing, divided by the total number of things:

$$P(\text{two things not duplicate}) = \frac{n}{n} \cdot \frac{n-1}{n}.$$

So what is the probability three things would be different? Well, it would be the probability of two things being different, times the probability third thing would be different from those:

$$P(\text{three things not duplicate}) = \frac{n}{n} \cdot \frac{n-1}{n} \cdot \frac{n-2}{n}.$$

Continuing this we have:

$$\begin{aligned} P(k \text{ things not duplicate}) &= \frac{n}{n} \cdot \frac{n-1}{n} \cdot \frac{n-2}{n} \cdot \ \ldots \ \cdot \frac{n-k+1}{n} \\ &= n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1) \cdot \frac{1}{n^k} \\ &= \frac{n!}{(n-k)!} \cdot \frac{1}{n^k} \\ &= \frac{n!}{(n-k)!\ n^k}. \end{aligned}$$

This expression is a little extravagant, so let's try to create an easier-to-write approximation.

Taylor Series Approximation. To begin to simplify the probability above, we first recall the following Taylor series approximation:

$$e^x = 1 + x + \frac{x^2}{2!} + \cdots.$$

Next we notice if $x \ll 1$, the higher order of terms in the series trend toward 0 leaving us with

$$e^x \approx 1 + x \quad \text{for } x \ll 1.$$

So a term of the form

$$\frac{n-a}{n}$$

can be approximated as

$$\frac{n-a}{n} = 1 - \frac{a}{n} \approx e^{-\frac{a}{n}}.$$

Applying this to our series we have

$$\begin{aligned} \left(\frac{n}{n} \cdot \frac{n-1}{n} \cdot \frac{n-2}{n} \cdot \ldots \cdot \frac{n-k+1}{n} \cdot \right) &\approx e^{-\frac{0}{n}} \cdot e^{-\frac{1}{n}} \cdot e^{-\frac{2}{n}} \cdot \ldots e^{-\frac{n-k+1}{n}} \\ &= e^{-\left(0+1+2+\ldots+(k-1)\right)/n} \\ &= e^{-\left(\frac{k(k-1)}{2n}\right)} \\ &= e^{-\frac{k^2}{2n}}. \end{aligned}$$

So this allows us to express the probability of *no* duplicates in a slightly simpler form than before:

$$P(\text{duplicates } = 0) \approx e^{-\frac{k^2}{2n}}$$

and therefore

$$P(\text{duplicates } > 0) \approx 1 - e^{-\frac{k^2}{2n}}.$$

Now we want to know what value k we need for the probability of duplicates to be $\frac{1}{2}$. So we set $P = \frac{1}{2}$ and solve for k:

$$\begin{aligned}
\frac{1}{2} &= 1 - e^{-\frac{k^2}{2n}} \\
0 &= \frac{1}{2} - e^{-\frac{k^2}{2n}} \\
e^{-\frac{k^2}{2n}} &= \frac{1}{2} \\
-\frac{k^2}{2n} &= \ln\left(\frac{1}{2}\right) \\
k^2 &= -2n \cdot \ln\left(\frac{1}{2}\right) \\
k &= \sqrt{-2n \cdot \ln\left(\frac{1}{2}\right)} \\
k &\approx 1.17 \cdot \sqrt{n}
\end{aligned}$$

Putting it all Together

Returning to our hash function, suppose the hash length is ℓ-bits, i.e., $n = 2^\ell$. How many hashes k must be generated for you to expect to find a collision, i.e, for the probability of a collision to be at least 50%?

$$\begin{aligned}
k &\approx 1.17 \cdot \sqrt{2^\ell} \\
&\approx \sqrt{2^\ell} \\
&= 2^{\frac{\ell}{2}}
\end{aligned}$$

Therefore you would expect to find a collision, i.e., two values $m_i \neq m_j$ for which $\mathcal{H}(m_i) = \mathcal{H}(m_j)$ after approximately $2^{\frac{\ell}{2}}$ hashes. □