16-124-836
Marcel Zauder

4.1 Deterministic Libraries

A deterministic library is one that uses no random choices. Therefore the output for any input will be always the same. Let L_1 and L_2 be such deterministic libraries.

Further the advantage or bias of A is defined as follows:

$$Bias(A) \ = \mid Pr(A \diamond L_1 \Rightarrow 1) - Pr(A \diamond L_2 \Rightarrow 1) \mid$$

Therefore it is clear that if the deterministic libraries are interchangeable the bias will be Zero. The bias will only be 1 if the algorithm $Pr(A \diamond L_1 \Rightarrow 1) = 1$ and $Pr(A \diamond L_2 \Rightarrow 1) = 0$ (or vice versa). This is only possible if L_1 and L_2 are different. Therefore L_1 and L_2 are either equivalent or can be distinguished with advantage 1.

4.2 Hash-function collisions

4.2.a $\lambda = 40$

For $\lambda = 40$ we have $2^{40} \ \approx \ 1.1 * 10^{12}$ different keys. Because we do 1'000'000 hashes on this which is clearly much less than $1,1 * 10^{12}$, we should use the Lemma of *PColl(q, N)* $\approx \ 1 - e^{\frac{q^2}{2N}}$:

$$\begin{aligned} PColl(10^6, 2^{40}) \ &\approx \ 1 \ - \ e^{\frac{(10^6)^2}{2 \times 2^{40}}} \\ &= \ 1 \ - \ 0.634608281 \\ &= \ 0.365391719 \ \approx \ 36.54\% \end{aligned}$$

4.2.b $\lambda = 256$

For $\lambda = 256$ we have $2^{256} \ \approx \ 1.16 * 10^{77}$ different keys. Again we will use the *PColl(q, N)* function to estimate the number of hashes needed to exceed the probability $\frac{1}{2}$ for a collision:

$$\begin{aligned} & PColl(q, N) \ \approx \ 1 - e^{\frac{q^2}{2N}} \\ \Rightarrow \quad & q \ \approx \ \sqrt{ln(PColl(q, N)) \times (-2N)} \\ \Rightarrow \quad & q \ \approx \ \sqrt{ln(\frac{1}{2}) \times (-2 \times 2^{256})} \\ & \approx \ 4 * 10^{38} \end{aligned}$$

So approximately $4 * 10^{38}$ hashes are needed to exceed the probability of $\frac{1}{2}$ for a collision.

4.3 Salt

4.3.a Without *Salt*

From the exercise we know that $\lambda = 20$. We will use the *BirthdayProb(q, N)* function:

$$BirthdayProb(q,\ N) \ \geq \ 1 \ - \ 0.632 \cdot \frac{q(q-1)}{2N} \qquad if\ q \ << \ \sqrt{2N}$$

$$\Rightarrow \qquad q \ = \ \frac{1}{2} \ \pm \ \sqrt{\frac{1}{4} + \frac{(1 - BirthdayProb(q,\ N)) \times 2N}{0,632}}$$

$$\Rightarrow \qquad q \ = \ \frac{1}{2} \ + \ \sqrt{\frac{1}{4} + \frac{2^{20}}{0,632}} \ \approx \ 1289$$

4.3.b With *Salt*

Through the salt the length of the $\lambda = 256 + 20 = 276$. So we get (similar as above):

$$q \ = \ \frac{1}{2} \ + \ \sqrt{\frac{1}{4} + \frac{2^{276}}{0,632}} \ = \ 4.4 * 10^{41}$$