CS6290 Privacy-enhancing Technologies
Tutorial 2

We have prepared a few questions for you to examine your understanding of some concepts covered in Lecture 1 and Lecture 2.

Question 1: Birthday Attack

Let H be an ideal hash function that produces an n-bit output. By ideal, we mean that, as far as we can tell, each hash value is independent and uniformly distributed in $\{0,1\}^n$. Trivially, we can go through $2^n + 1$ different values, and we are guaranteed to find a collision. If we're constrained for space, we can just store 1 input-output pair and keep trying new inputs until we hit the same output again. This has time complexity $O(2^n)$, but has $O(1)$ space complexity.

Alternatively, we could compute the hashes of about $O(2^{n/2})$ different inputs and store all the input-output pairs. As we saw in the text, theres a good chance that some two of those outputs would collide (the birthday paradox). This shows that we can achieve a time-space trade-off: $O(2^{n/2})$ time and $O(2^{n/2})$ space.

Q1-a: Show that the time-space trade-off is parameterizable: we can achieve any space complexity between $O(1)$ and $O(2^{n/2})$ with a corresponding decrease in time complexity.

Q1-b: Is there an attack for which the product of time and space complexity is $o(2^n)$? [Recall the *little oh notation*.]

Question 2: Hash Function Properties

Q2: Let H be a hash function that is both hiding and puzzle-friendly. Consider $G(z) = H(z)\|z_{last}$ where z_{last} represents the last bit of z. Show that G is puzzle-friendly but not hiding.

(Question 1 and Question 2 come from Chapter 1 of book [NBF+16]. Read Chapter 1 to find the answers.)

Question 3: The Longest Chain Rule

Q3-a: In a proof-of-work system, an attacker must modify all subsequent blocks following the targeted block to avoid being rejected by the system. As the chain grows longer, the attackers workload increases. Therefore, does the probability of a successful attack decrease over time?

Q3-b: If, over time, old blocks are compacted by pruning branches of the tree, will the chain become shorter and the system less secure than before?

References

[NBF+16] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, USA, 2016.