FPGA-based SoC Design

LAB Assignment #1

Team Members:

Girish Bheemaraddi Tabaraddi - 1119236

Chaitreya Shridhar Hegde - 1119179

a) What is a mathematical one-way function and what are specific applications?
Answer:

- ✓ A mathematical one way function(f(x)) is a function for which it is easy to compute the value of f(x) if x is the input, but it is hard to compute x back if one has f(x) value and wants to determine the value of x.
- ✓ Specific applications- In Pseudo random number generators, digital signatures, authentication of messages.

b) Define preimage resistance and the second preimage resistance characteristic of a one-way function.
Answer:

- ✓ Pre image resistance is the property of a one-way function that it is difficult to find the pre-image or the input for a specified output of the function.
- ✓ Second pre image resistance is the property of a one- way function that it is difficult to find any second input which has the same output as a specified input.

c) What is a collision and how does it affect the security of a hash function? Why do collisions necessarily exist?
Answer:

- ✓ If there are same hash outputs for different inputs after being processed by a particular hash input, then it is called a collision. If multiple inputs have the same hash values, then an attacker can create malicious or fake inputs that masquerade as the original input and will cause file or data integrity issues.
- ✓ Collisions exist because the hashing functions translate functions of any length to a fixed length code.

d) Does the Boolean XOR function represent a valid way to verify the integrity of a message? Justify your answer!
Answer:

- ✓ XOR function is suitable in case of random transmission errors. But if an attacker tries to modify the content deliberately, XOR function is not useful. The attacker can change the main message and add a bit block before the hashcode so that the final hashcode is unchanged.
- ✓ When one is using XOR for hashing text based on ASCII, this is even more problematic because the highest bit in every byte is zero. With this value always zero, some of the bits in the hashcode will be predictably zero. This will reduce the number of unique hashcodes available to us. Hence this increases the chances of collisions.

e) Explain the birthday problem and state the relation to hash collisions.
Answer:

- ✓ Birthday problem is as follows- In a random group of n people, what is the probability that two of them share the same birthday? Or that- In a random group of people, what is the minimum number of people needed in a group that the probability of any two of them sharing the same birthday is more than 50%? The birthday paradox is the solution to this problem.
- ✓ The minimum number of people required is 23 for having the probability more than 50% for two of them sharing the birthday. This applies to cryptographic hash functions too. Since they have a fixed length of the hash and infinite inputs, the chance that two inputs have the same hash or collision is definitely possible.
- ✓ By using the solution of the birthday problem, we can find that we will be having more than 50% chance of finding a collision after $2^{m/2}$ operations where m is the size of the message digest or sample space.

f) What role plays the SHA-256 algorithm in the context of the cryptocurrency Bitcoin?
Answer:

- ✓ SHA-256 is used in the Bitcoin in two ways
- ✓ In Bitcoin mining: While constructing the candidate blocks once a mining node has been set up. Here SHA 256 is used to calculate the previous hash, and to produce the Merkle root and during the mining process.
- ✓ During the creation of bitcoin addresses: The public key produced out of the private key is passed through SHA function.
- ✓ If K is public key and A is the Bitcoin address: A = RIPEMD160(SHA-256(K))

REFERENCES

- ✓ http://www.crypto-it.net/eng/theory/one-way-function.html (a)
- ✓ https://en.wikipedia.org/wiki/One-way_function (a)
- ✓ https://www.cs.purdue.edu/homes/ssw/cs355/hash.pdf (b)
- ✓ https://www.baeldung.com/cs/hash-collision-weak-vs-strong-resistance (c)
- ✓ https://wizardforcel.gitbooks.io/practical-cryptography-for-developers-book/content/cryptographic-hash-functions/crypto-hashes-and-collisions.html (c)
- ✓ https://justcryptography.com/the-birthday-paradox/ (e)
- ✓ https://auth0.com/blog/birthday-attacks-collisions-and-password-strength (e)