Daniel Garcia

ECE 548

Homework 4

3.10 Consider the Bloom filter discussed in Section 3.3 Token-Based Authentication.

Define *k* = number of hash functions;

*N* = number of bits in hash table; and

*D* = number of words in dictionary.

1. Show that the expected number of bits in the hash table that are equal to zero is expressed as

=

**Answer**

The probability that for any one position in the hash table, the value is 1 is equal to k/N. This is because there are k hash functions which have an equal probability of setting a value to 1 in the set of N bits. Therefore, the probability of any value being 0 is (1 - k/N). Finally, to find the expected value of the number of zeros in the table, each probability is multiplied to itself D times, thus: =

1. Show that the probability that an input word, not in the dictionary, will be falsely accepted as being in the dictionary is

*P* =

**Answer**

Given that is the probability of bits equal to zero in the table, (1 - ) is the probability that any value is equal to one. Given any input word, the probability that the word will falsely be accepted as in the dictionary is

1. Show that the preceding expression can be approximated as

*P* ≈

**Answer**

Given the following equation from part b

*P* =

And the following equation from part a

=

Therefore

3.11 For the biometric authentication protocols illustrated in Figure 3.12, note that the biometric capture device is authenticated in the case of a static biometric but not authenticated for a dynamic biometric. Explain why authentication is useful in the case of a stable biometric but not needed in the case of dynamic biometric.

**Answer**

In the case of the stable biometric, it is important to identify which biometric reading the resulting template represents. This allows the server to authenticate the biometric device in case the client attempts to authenticate using a different device. This also solves the issue of many devices generating the same biometric template for different users. In the case of dynamic biometric authentication, since a challenge is used as well as a biometric reading, the user must know the answer. If the user knows the answer, and generates the correct biometric signal, then the user must be who they say they are and is therefore authenticated. The device must therefore be correct since the challenge is answered.