Homomorphic Secret Sharing – Questions

December 2018

1. **(Private search via DPF)** Suppose that 2 servers hold the same set of M documents, each containing N keywords in $\{0,1\}^n$. We are interested in obtaining efficient private search protocols in which a client sends $O(\lambda n)$ bits to each server, where λ is a security parameter, and receives $O(\log M)$ bits in return. The client's search query should remain hidden from each individual server.

   (a) Use a DPF to obtain a private search protocol as above allowing the client to learn the number of documents containing a secret keyword $w \in \{0,1\}^n$.

   (b) Show a similar protocol allowing the client to learn the number of documents containing *both* w_1, w_2, where $w_1, w_2 \in \{0,1\}^n$ can be arbitrarily chosen by the client. The computational complexity of the servers can grow quadratically with N.

   (c) Show how to use 4 servers for making the computational complexity of the servers linear in N.

2. **(Error-free share conversion)** Show that an error-free implementation of the multiplicative-to-additive share conversion procedure implies an efficient algorithm for discrete logarithm.