Homomorphic Secret Sharing – Exercise Session

March 2017

1. **(Simple closure properties for Function Secret Sharing)** This question is concerned with enhancing the power of FSS via simple closure operations.

   (a) **Closure under sum:** $(\mathcal{F}, \mathcal{G}) \to \mathcal{F} + \mathcal{G}$.
   Given FSS schemes for function families $\mathcal{F}, \mathcal{G}$, there exists an FSS scheme for the family $\mathcal{F} + \mathcal{G} := \{f + g | f \in \mathcal{F}, g \in \mathcal{G}\}$, with key size $\mathsf{size}(\mathcal{F} + \mathcal{G}) = \mathsf{size}(\mathcal{F}) + \mathsf{size}(\mathcal{G})$.

   (b) **Including the zero function:** $\mathcal{F} \to \mathcal{F} \cup \{0\}$.
   For any FSS scheme for family $\mathcal{F}$, there exists an FSS scheme for the family $\mathcal{F}$ together with the all-0 function (defined by $0(x) = 0$ for all x) with key size $\mathsf{size}(\mathcal{F} \cup \{0\}) = \mathsf{size}(\mathcal{F})$.

   (c) **Closure under union:** $(\mathcal{F}, \mathcal{G}) \to \mathcal{F} \cup \mathcal{G}$.
   Given FSS schemes for families $\mathcal{F}, \mathcal{G}$, there exists an FSS scheme for the class $\mathcal{F} \cup \mathcal{G}$, with key size $\mathsf{size}(\mathcal{F} \cup \mathcal{G}) = \mathsf{size}(\mathcal{F}) + \mathsf{size}(\mathcal{G})$.

2. **(Information-theoretic Distributed Point Functions)** This question is concerned with an information-theoretic variant of DPFs, where both the correctness and the secrecy requirements are perfect.

   (a) Show that there is a perfect 2-party DPF such that on input domain $\{0,1\}^n$ and output group $\mathbb{Z}_2$ the key size is 2^n.

   (b) Prove that the above key size is optimal.

   (c) What is the optimal key size of perfect FSS for the class of *non-zero* point functions with input domain $\{0,1\}^n$ and output group $\mathbb{Z}_2$? Prove your answer.

3. **(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.

4. **(Homomorphic Secret Sharing from Fully Homomorphic Encryption)** Show that there is an HSS scheme for *circuits*, with inverse polynomial error, assuming *both*: (1) DDH; (2) the existence of an FHE scheme for circuits with decryption in NC^1 (in particular, an encrypted bit can be decrypted by a polynomial-size branching program whose inputs are the ciphertext and the secret key).

5. **(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.