DPF Using Learning With Errors

Albert Gao / sixiangg

04/05/2022

1 Context

Again, we explore the problem of PIR and the problem of DPF. We attempt to show that existing techniques in homomorphic encryption based on learning with errors (LWE) assumptions suffice to give a solution to PIR and to DPF. Specifically, if there is one server with a database of n items, then PIR can be done using $O(\text{polylog}(n))$ communication complexity and $\widetilde{O}(n)$ computation complexity on server side. Further, for our purposes, due to relative simplicity of circuits we evaluate, we can refrain from using fully homomorphic encryption and, for example, opt for somewhat/leveled homomorphic encryption without the so-called "bootstrapping" technique. In other words, this approach can be made practically feasible without relying on fully homomorphic encryption.

Extension from one-server PIR to the multi-server DPF setting is simple and uninteresting: perform exactly the same method for each server. This should tolerate collusion among all servers and/or failures from all but one servers. Indeed, this method sounds degenerate enough for the DPF setting that it makes replication of data on different servers unappealing for our purposes. However, the asymptotic or concrete complexity from this note can still serve as a benchmark for other DPF approaches.

2 Prelim

To keep it consistent, all relevant techniques in this section can be found in [1]. We provide a summary of the ones we need for our purposes.

2.1 Warmup

Homomorphic encryption involves computation on encrypted data. In our informal mental model, to evaluate a circuit on some plaintext inputs, we may also equivalently evaluate some procedure (that is based on this circuit) on inputs consisting of encrypted bits, and the resulting new ciphertext can be decrypted to the plaintext result we desire. An uninteresting approach to this problem can simply attach the original circuit to the ciphertext inputs and call it the new ciphertext. The decryption procedure would simply decrypt each of the ciphertext inputs and evaluate the attached circuit. In order to capture the notion of having a similar decryption procedure between "freshly generated" ciphertexts and "evaluated" ciphertexts, we need the nontrivial notion of *compactness* for our homomorphic encryption schemes, where complexity of decryption does not depend on the complexity of the circuit we evaluate.

Without specifying precise definitions of homomorphic encryption and compactness, we can still see that this can be used for PIR assuming constructions are feasible. A server can evaluate a circuit for the function $f_{db}(i) = db[i]$ using homomorphic encryption, where the database consisting of n items is hardwired in the circuit and the interested index i is encrypted before reaching the server. An example circuit with a database $(1, 0, 1, 1) \in \{0, 1\}^4$ and index bits a, b is illustrated in Figure 1. It is clear that homomorphic encryption should give us desired output if the server is given encrypted versions of $a, \neg a, b, \neg b$. One more important observation here is that the depth of this circuit before the last degree-n fan-in gate is exactly $\lceil \log n \rceil$. From a different perspective, we are computing the sum of n bits, each of which is the result of $\lceil \log n \rceil$ multiplications.

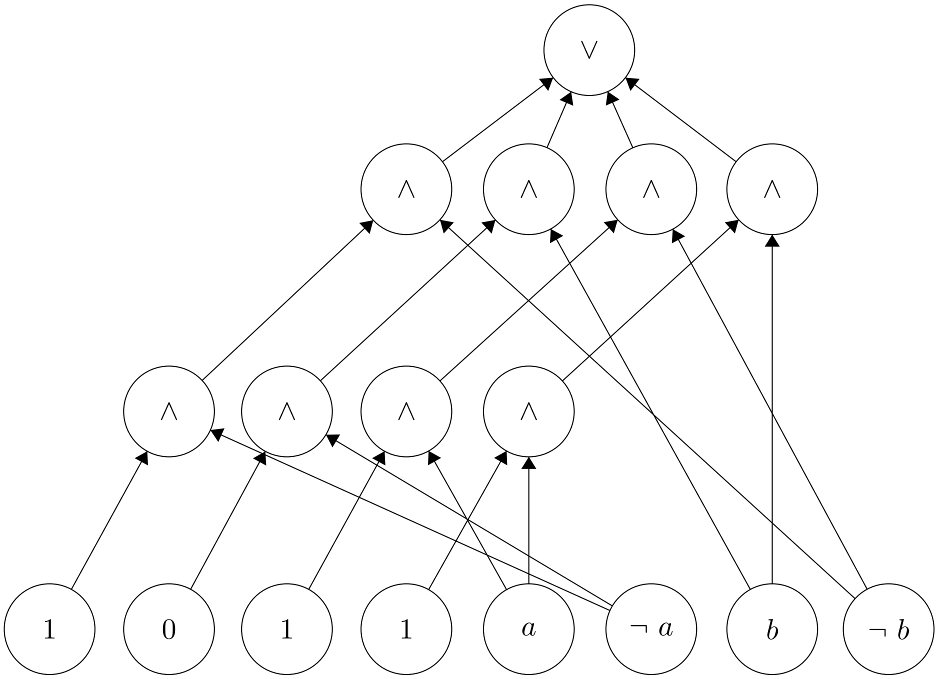

Figure 1: Circuit for retrieving an item from a database with four elements.

Now, we describe an approach for such evaluations on ciphertexts. The approach below originally comes from the GSW scheme from [2], but of course this is not the only scheme that would work. Our goal is to explain that such approaches can be natural and interesting not just in a theoretical setting.

Further, we observe that fully homomorphic encryption is not necessary for our purposes, which in turn should allow much more practical concrete applications.

2.2 Definitions

References

[1] Shai Halevi. Homomorphic encryption. In *Tutorials on the Foundations of Cryptography*, pages 219–276. Springer, 2017.

[2] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *Annual Cryptology Conference*, pages 75–92. Springer, 2013.