Fully Homomorphic Encryption summary

dinsdag 17 januari 2023 18:35

- A homomorphism is a structure-preserving map.
- ElGamal is a homomorphic encryption scheme.

Homomorphic encryption schemes

- IND-CCA2 (indistinguishability under adaptive chosen ciphertext attack) security is unachievable for any homomorphic encryption scheme.
- IND-CCA1 security is achieved by ElGamal, as well as IND-CPA.
- Sensible homomorphic encryption schemes are rerandomizable.

Exponential ElGamal

- Exponential ElGamal does ***not*** require the use of special groups in which the discrete-logarithm problem is easy.
- Exponential ElGamal massively limits the size of the plaintext space compared to regular ElGamal.
- Exponential ElGamal does ***not*** support homomorphic multiplication of ciphertexts.
- Exponential ElGamal supports homomorphic addition of ciphertexts.
- Exponential ElGamal support ciphertexts that contain 0 as plaintext.

CGS voting scheme

Basic version involves a trusted authority to which all votes are encrypted and which can learn all individual votes. Encrypted ciphertext contains sum of all votes, which (due to homomorphic properties) can be decrypted to the actual sum of votes. The basic version also assumes that the votes are Boolean (e.g. for/against).
Trusted authority can be disturbed by encrypting to the product of keys of several parties; only the group of parties having those keys can decrypt. This does allow for obstruction by a party unwilling to collaborate, though. This issue can be resolved by having a threshold scheme.

Fully Homomorphic Encryption (FHE)

FHE allows for running cloud computing without the compute provider being able to see the data that is being computed on.

- Bootstrapping: encrypt the secret key with its corresponding public key. Allows 'decrypting' without knowing the key. Effectively, 'encrypting' and 'decrypting' in this way allows for reducing the noise associated with lattice based schemes.

Zero Knowledge proofs

Properties

- Correctness: honestly generated proofs of true statements are accepted;
- Soundness: it is impossible to create a valid proof for a false statement;
- Zero-knowledge; it can be simulated for false statements such that the result is indistinguishable from a real proof.

Shadow mixes are a technique based on random permutations and shuffling that allow for verifying whether a

The Fiat-Shamir heuristic allows for turning interactive zero-knowledge proofs into non-interactive zero-knowledge proofs *(which can be interpreted as signatures)*, under the assumption that random oracles exist.

Commitment schemes

Two properties are required:

- Hiding (of the content of the commitment)
- Binding (so that the content of the commitment cannot be changed).

A hash in general is deterministic and hence does not suffice (since it leaks information, it does not hide). A random oracle (when the message is prefixed with a sufficiently long random string) does suffice.

Pederson commitments

A scheme with a common reference string $h = g^x$. To commit on an exponent m, one samples a random exponent r and creates the commitment $x = g^m h^r = g^{m+rx}$. Under the assumption that x is unknown, this binds. It also achieves information-theoretical hiding.

Note: adaptive = attacker knows ciphertext
https://crypto.stackexchange.com/a/99671/7404

ElGamal and Exponential ElGamal

In regular ElGamal, multiplying two ciphertexts results in a ciphertext which corresponds to a plaintext in which the two original plaintexts have been multiplied.
In exponential ElGamal, we first change the plaintext messages by raising them to a power; that is, the plaintexts m_0' and m_1' are changed to $g^{m_0'}$ and $g^{m_1'}$. By doing this, upon multiplying the ciphertexts that result from this, we effectively multiply $g^{m_0'}$ and $g^{m_1'}$, which results in $g^{m_0'+m_1'}$ as the plaintext of the new message. Upon undoing this transformation, we end up with a plaintext where the messages have been added. (This can be done by taking a discrete log; this is reasonably efficient as long as the numbers remain small.) This can be useful for e.g. vote-counting.