Report Speaker 2

Rohon Kundu

1 Summary

Modern cryptography is based on a gap between efficient algorithms provided for the legitimate users and the computational infeasibility of abusing or breaking this algorithms by an illegitimate adversary. To illustrate this gap we need secure encryption schemes where the legitimate users should be able to decipher the messages using some private information (private key) available to them and yet an adversary which do not have access to the private key should not be able to decrypt the ciphertext efficiently(i.e. in probabilistic polynomial time). So the existence of a secure encryption scheme implies the existence of an efficient way to generate hard problems with certain set of inputs such that it is easy to solve the hard problem when the set of inputs are provided but it becomes difficult to solve it without knowing the set of inputs. This give rise to the concept of *one-way functions*(OWFs). Informally, a one-way function might be described as a function for which evaluation in one direction is straightforward, while computation of the inverse is difficult.

We can generalize a family of one-way functions by introducing trapdoor functions. Trapdoor functions (TDFs) are a foundational primitive in cryptography and are typically used as a fundamental building block in the construction of advanced primitives such as Chosen Ciphertext Attacks (CCA-2)-secure encryption schemes. In this paper the author have introduced the concept of *One-Way Functions with Encryption*(OWFE) and proposed the construction of efficient TDFs using OWFE. The fundamental difference between OWFE and any OWF is that the former is defined using encapsulation/decapsulation algorithms (E, D) together with a OWF. The introduction of additional encapsulation/decapsulation algorithms provide security against Chosen Plaintext Attack (CPA) and Chosen Ciphertext Attack(CCA). This is an important result because in order to create a secure encryption scheme it is expected to be indistinguishable under Chosen Plaintext Attack and Chosen Ciphertext Attack i.e IND-CPA and IND-CCA.

Chosen-Plaintext Attacks could capture the ability of an adversary to exercise control over what the honest parties encrypt. A cryptosystem is indistinguishable under chosen plaintext attack (IND-CPA) if every probabilistic polynomial time adversary has only a negligible advantage over random guessing. A chosen-ciphertext attack is even more powerful. In CCA, the adversary has the ability not only to obtain encryptions of messages of its choice (as in CPA), but also decryption of ciphertext of its choice. In case of non-adaptive CCA (CCA 1), the adversary is allowed to query the decryption oracle only up until it receives the challenge ciphertext. In the adaptive definition (CCA-2), the adversary may continue to query the decryption oracle even after it has received a challenge ciphertext.A given public key encryption scheme is said to have the strongest security notion if it is IND-CCA 2.

2 Importance of the obtained result in this fields

Previously Trapdoor Functions were built based on various assumptions like Quadratic Residues (QR), Decisional Diffie-Hellman (DDH) and Learning With Error (LWE). There were two major setback of the pre-existing TDFs: a) They were neither IND-CPA or IND-CCA 1/2. b) The size of the image of TDF increased quadratically with the length of input n. Both were considered to be a significant drawbacks as it both cause compromisation of security and storage capacity. With the new construction of efficient TDFs from OWFE, the author was able to address and solve both the pre-existing drawbacks. We already know that the OWFE are both IND-CPA and IND-CCA. Accordingly, the author have proved in this paper that the TDFs constructed from OWFE are indistinguishable under chosen-plaintext and chosen-ciphertext attack. In addition it was also proved that with the new construction of TDFs from OWFE the size of the image grows linearly instead of quadratically. This could solve the storage problem faced with the pre-existing TDFs.

3 What is good about the paper?

I think the introduction to a new concept of OWFE could open up several possibilities of research in the upcoming year. The concept has only been introduced to the crypto community in 2019 and I predict there are several paradigm shifting research possibilities to be uncovered in the future. The security proofs has been done in a very detailed and explicit way, which provides the reader with an entire mathematical knowledge on the significance of the proposed construction. On understanding the security proof one can reiterate the same concept for other encryption schemes.

4 What is bad about the paper?

I think the paper lack basic introduction to the field of Trapdoor Functions for new readers. The work on the paper has been presented under the presumption that the readers are well acquainted with the previous works done in constructing TDFs from various other schemes like QR,DDH and,LWE. This creates certain difficulty for a novice in this field to understand the content and it's relevance. Also each section lack intuition on the respective content and has been left to the readers to make their own impression. It would have been helpful for the reader to have a section on conclusion, where the outline of the work and it's relevance could have been explained. This would help in understanding the work as a whole and facilitate future research ideas based on the paper.