Encryption for Fine-Grained Access Control

Supervisor. Hoeteck Wee, wee@di.ens.fr http://www.di.ens.fr/~wee
Location. Ecole Normale Supérieure, Paris

Project

We live in an era of "Big Data", wherein a deluge of data is being generated, collected, and stored all around us. These data include not only government, financial and medical records, but also personal information exchanged over email, social networks and other data-sharing sites. Without taking measures to protect these data, we risk living under digital surveillance in an Orwellian future. Unfortunately, traditional encryption systems lack the expressiveness needed in applications involving big, complex data.

Functional encryption. Functional encryption [1] is an emerging paradigm for public-key encryption that enables more fine-grained access control to encrypted data. For instance, it provides the ability to specify a decryption policy in the ciphertext so that only individuals who satisfy the policy can decrypt, and the ability to associate keywords to a secret key so that it can only decrypt documents containing the keyword. This stands in contrast to traditional encryption, where access to the encrypted data is all or nothing one can either decrypt and read the entire plaintext or one learns nothing at all about the plaintext (other than its length). Furthermore, functional encryption enforces resilience to collusion attacks, namely any group of users holding different secret keys learns nothing about the plaintext beyond what each of them could individually learn.

Conditional disclosure of secrets. Let us begin with a much simpler primitive, namely that of conditional disclosure of secrets (CDS) [2]. CDS allows a set of n players $P_1, \ldots, P_n$ to disclose a secret $z \in \mathbb{F}_q$ to an external party Carol, subject to a given condition on their joint inputs. Carol knows all the inputs held by the players except for the secret to be conditionally disclosed, so she knows whether the condition holds and whether she will obtain the secret. Each player on the other hand only sees its portion of the input and does not necessarily know whether Carol will obtain the secret. We consider the shared randomness model where all players have access to the same random string which is hidden from Carol. For simplicity, we also assume that all players know z, and we focus on protocols involves only a unidirectional communication from the players to Carol. Note that CDS generalizes secret-sharing by considering the special case where each party holds a boolean input and the message sent by P_i corresponds to its share (c.f. [2, Section 3.2.1]).

For example, consider the scenario where player P_i holds $x_i \in \mathbb{F}_q$ and the players want to disclose the secret z to Carol subject to the condition $x_1 + \ldots + x_n = 0$; for $n = 2$, this captures "disclose z if x_1, x_2 are equal". Suppose all n players have access to the same random string $(r_1, \ldots, r_n, r') \in \mathbb{F}_q^{n+1}$, hidden from Carol. The CDS protocol proceeds as follows: player P_i sends $(r' x_i - r_i)$ to Carol; in addition, P_1 also sends $r_1 + \cdots + r_n + z$ to Carol. It is straight-forward to verify that

- if $x_1 + \ldots + x_n = 0$, then Carol can recover z by summing all the messages she receives;
- if $x_1 + \ldots + x_n \neq 0$, then Carol learns nothing about z (that is, the *joint* distribution of all the messages Carol sees is *independent* of z).

Project goals. We will study protocols for conditional disclosure of secrets, and explore the connection to functional encryption established in [3]. The research will take place within the cryptography group at ENS, Paris: http://www.di.ens.fr/CryptoTeam.html. The student is strongly encouraged to attend seminars and to interact with Ph.D. students, post-docs, and permanent researchers in the group.

Requirements. Being comfortable with mathematical proofs and the notion of efficient reductions between computational problems. Knowledge of probability and basic computational complexity is strongly recommended. It is also very strongly recommended to have taken at least one course in cryptography and having been exposed to the notion of "provable security" (as covered in 2.12.1 and 2.30 of the MPRI). Fluency in English is a necessity.

References.

[1] D. Boneh, A. Sahai, and B. Waters. Functional encryption: a new vision for public-key cryptography. *Commun. ACM*, 55(11):56–64, 2012.

[2] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin. Protecting data privacy in private information retrieval schemes. *J. Comput. Syst. Sci.*, 60(3):592–629, 2000.

[3] H. Wee. Dual system encryption via predicate encodings. In *TCC*, 2014. To appear.