Séminaire SAMOVAR/R3S

Quand : jeudi 18 mai 2017 à 10h00
Où : salle E408, Télécom SudParis, Evry.

Dr. Tarik Moataz (Brown University)

Title: Boolean Searchable Symmetric Encryption with Worst-Case Sub-Linear Complexity **(Joint work with Seny Kamara, Brown University)**

Abstract: Recent work on searchable symmetric encryption (SSE) has focused on increasing its expressiveness. A notable example is the OXT construction (Cash et al., CRYPTO '13) which is the first SSE scheme to support conjunctive keyword queries with sub-linear search complexity. While OXT efficiently supports disjunctive and boolean queries that can be expressed in searchable normal form, it can only handle arbitrary disjunctive and boolean queries in linear time. This motivates the problem of designing expressive SSE schemes with worst-case sub-linear search; that is, schemes that remain highly efficient for any keyword query.

In this work, we address this problem and propose non-interactive highly efficient SSE schemes that handle arbitrary disjunctive and boolean queries with worst-case sub-linear search and optimal communication complexity. Our main construction, called IEX, makes black-box use of an underlying single keyword SSE scheme which we can instantiate in various ways. Our first instantiation, IEX-2Lev, makes use of the recent 2Lev construction (Cash et al., NDSS '14) and is optimized for search at the expense of storage overhead. Our second instantiation, IEX-ZMF, relies on a new single keyword SSE scheme we introduce called ZMF and is optimized for storage overhead at the expense of efficiency (while still achieving asymptotically sub-linear search). Our ZMF construction is the first adaptively-secure highly compact SSE scheme and may be of independent interest. At a very high level, it can be viewed as an encrypted version of a new Bloom filter variant we refer to as a Matryoshka filter. In addition, we show how to extend IEX to be dynamic and forward-secure.

To evaluate the practicality of our schemes, we designed and implemented a new encrypted search framework called Clusion. Our experimental results demonstrate the practicality of IEX and of its instantiations with respect to either search (for IEX-2Lev) and storage overhead (for IEX-ZMF).

Short Bio: Tarik Moataz is a Postdoctoral Research Associate in Computer Science at Brown University working with Seny Kamara. He received a French-American joint Ph.D. degree from IMT Atlantique and Colorado State University. His main research area is applied cryptography and, especially, its intersection with algorithms and data structures. His research focuses on designing provably-secure protocols that are efficient and ready for real-world deployment.