IMI Workshop: Next-generation Cryptography for Privacy Protection and Decentralized Control and Mathematical Structures to Support Techniques

September 1–3, 2015, Kyushu University

Homomorphic Encryption – are we there yet?

Anirban BASU

KDDI R&D Laboratories

basu@kddilabs.jp

With the proliferation of services offered on the Internet, large volumes of personal data have been collected and stored in cloud computing environments by different organisations to better understand and tailor goods and services for potential individuals. The recent advances in the Internet of Things usher yet another era of rapid growth of data, a lot of which is of a very personal nature, e.g., detailed physiological characteristics collected by wearable sensors or the trajectory data of the movement of individuals. While developing sophisticated intelligence to make sense of this data is a high priority, the privacy of individuals and even organisations is at stake. Even more so, when such rich datasets need to be shared across organisational boundaries.

Privacy-preserving analysis of data has become an increasingly important field of research in recent times. Various types of anonymisation and random perturbation of the data can help with guaranteeing certain privacy levels but these come at a cost of data utility. The other alternative is homomorphic encryption, which enables computing over encrypted data. In this talk, we explore how far is homomorphic encryption from being a reality.

To do so, we present two of our recent works that utilise homomorphic encryption and have been tested on real world cloud computing platforms. In [1], we discuss how an additively homomorphic encryption can be used to query a public cloud based classifier for collaborative filtering. We show evaluations of this scheme using datasets with prototypes built atop real world cloud computing platforms. In [2], we demostrate how a lightweight and practical (sender-)anonymous message routing network can be built and deployed on the cloud utilising additive homomorphic encryption.

We conclude with the outlook that a mixture of partially homomorphic schemes along with other techniques are practical in some real world application scenarios.

References

[1] A. Basu, J. Vaidya, H. Kikuchi, and T. Dimitrakos. Privacy-preserving collaborative filtering on the cloud – practical implementation experiences, In proc: IEEE Cloud, Santa Clara, CA, USA. 2013.

[2] A. Basu, J. C. Corena, J. Vaidya, J. Crowcroft, S. Kiyomoto, S. Marsh, Y. S. Van Der Sype, T. Nakamura, Lightweight practical private one-way anonymous messaging, In proc: IFIP WG 11.11 International Conference on Trust Management (IFIPTM), Hamburg, Germany, 2015.