Algebra-based Encryption for Adaptive Indexing

Artyom Nikitin and Panagiotis Karras

Skolkovo Institute of Science and Technology

Abstract. Today, outsourcing query processing tasks to remote cloud servers becomes a viable option for several financial applications; for example, a firm may deploy trading, analytics, and risk management modules to the cloud, while collecting financial data daily, or on a finer time scale [1]. At the same time, this model raises security and confidentiality concerns; sensitive data and query results may be leaked to malicious adversaries and/or an honest-but-curious service provider itself. Such concerns have motivated research on query answering over encrypted data [6]. Yet, to be efficiently managed, outsourced encrypted data should be indexed, and even adaptively so, as a side-effect of query processing [4]; extant encryption schemes suffer from one or more of the following drawbacks: (i) they are too computationally expensive; or (ii) leak too much information on the encrypted data, and/or (iii) require more data than the actual query results to be retrieved and then filtered in a post-processing step. We propose and analyze a scheme for lightweight and indexable encryption, based on linear-algebra operations, that allows for adaptively indexing encrypted data, so that only those values that are queried get indexed. To bring about such a result, we study the bare-bones requirements for indexing, and the ways in which such requirements may be reconciled with encryption. Our scheme relies on simple linear-algebra operations for encryption and decryption, while it can efficiently evaluate range and point queries over ciphertexts without disclosing the order among attribute values, as Order-Preserving Encryption Scheme [2] does, and without the computational and storage burdens of schemes like fully homomorphic encryption [3], with decryption performed at the client side. We implemented a prototype that performs incremental, query-triggered adaptive indexing over encrypted numeric data based on this scheme, without leaking order information in advance, and without prohibitive overhead, as our extensive experimental study demonstrates. The details of our scheme are presented in [5].

References

1. A. Agopyan, E. Şener, and A. Beklen. Financial business cloud for high-frequency trading: A research on financial trading operations with cloud computing. *IJAIS*, 4(3):203–217, 2011.
2. A. Boldyreva, N. Chenette, and A. O'Neill. Order-preserving encryption revisited: Improved security analysis and alternative solutions. In *CRYPTO*, 2011.
3. C. Gentry. Fully homomorphic encryption using ideal lattices. In *STOC*, 2009.
4. F. Halim, S. Idreos, P. Karras, and R. H. C. Yap. Stochastic database cracking: Towards robust adaptive indexing in main-memory column-stores. *PVLDB*, 5(6):502–513, 2012.
5. P. Karras, A. Nikitin, M. S. Malhotra, R. Bhatt, D. Antyukhov, and S. Idreos. Adaptive Indexing over Encrypted Numeric Data. In *SIGMOD*, 2016 (to appear).
6. R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan. CryptDB: protecting confidentiality with encrypted query processing. In *SOSP*, 2011.