Poster: Practical PIR for Electronic Commerce

Ryan Henry
PhD Student
rhenry@cs.uwaterloo.ca

Femi Olumofin
PhD Student
fgolumofin@cs.uwaterloo.ca

Ian Goldberg
Assistant Professor
iang@cs.uwaterloo.ca

Cheriton School of Computer Science
University of Waterloo
Waterloo, ON, Canada N2L 3G1

(Poster Abstract)

We extend Percy++, an open source implementation of Goldberg's multi-server information-theoretic private information retrieval (PIR) [1], with a suite of protocols for privacy-preserving electronic commerce. Our enhancements provide a stronger and more realistic model of PIR that enables e-commerce to coexist happily with strong privacy protection.

Our first protocol adds support for single-payee priced symmetric private information retrieval (PSPIR) that supports a tiered pricing model and price lists with record-level granularity. In this model, users purchase database records using e-cash, without revealing the indices or prices of those records, while the seller may set the price of each individual record with respect to one or more different tiers of users; e.g., non-members may pay full price while members may receive a discounted rate. We then extend our tiered pricing construction to support group-based access control lists, which maintain the record-level granularity of the price lists; this lets the database servers set the access rights of each record with respect to each price tier, thus enabling a user to retrieve a record only if he belongs to a tier that has been explicitly granted authorization to access that record. Next, we show how to augment our protocols with some basic bookkeeping functionality to implement a novel top-K replication strategy that enables the servers to construct bestsellers lists, which facilitate faster retrieval for these most popular records. Finally, we build on our bookkeeping functionality to construct PSPIR with support for multiple payees, thus enabling several sellers to offer their digital goods through a common database while enabling the database servers to determine to what portion of revenues each seller is entitled. Our protocols maintain user anonymity in addition to query privacy; that is, queries do not leak information about the index or price of the record a user purchases, the price tier according to which the user pays, the user's remaining balance, or even whether the user has ever queried the database before. No other priced PIR or oblivious transfer protocol supports tiered pricing, access control lists, multiple payees, or top-K replication, whereas ours supports all of these features while preserving PIR's sublinear communication complexity.

As a first step in building our protocols, we transform Goldberg's PIR scheme into symmetric PIR (SPIR). The resulting SPIR scheme maintains the attractive t-privacy and v-Byzantine-robustness properties of the original scheme. To maintain efficiency, we also propose some new batch zero-knowledge proofs (ZKPs) that enable our protocols to scale to extremely large database sizes without becoming a bottleneck to performance. We believe that our SPIR construction and efficient ZKPs are of independent theoretical interest. Measurements from our implementation of these protocols indicate that they are practical for deployment in real-world e-commerce applications.

References

[1] I. Goldberg, "Improving the Robustness of Private Information Retrieval," in *Proceedings of IEEE S&P 2007*, Oakland, CA, May 2007.