Cryptology ePrint Archive: Report 2011/561

A Domain-Specific Language for Computing on Encrypted Data

Alex Bain and John Mitchell and Rahul Sharma and Deian Stefan and Joe Zimmerman

Abstract: In cloud computing, a client may request computation on confidential data that is sent to untrusted servers. While homomorphic encryption and secure multiparty computation provide building blocks for secure computation, software must be properly structured to preserve confidentiality. Using a general definition of \emph{secure execution platform}, we propose a single Haskell-based domain-specific language for cryptographic cloud computing and prove correctness and confidentiality for two representative and distinctly different implementations of the same programming language. The secret sharing execution platform provides information-theoretic security against colluding servers. The homomorphic encryption execution platform requires only one server, but has limited efficiency, and provides secrecy against a computationally-bounded adversary. Experiments with our implementation suggest promising computational feasibility, as cryptography improves, and show how code can be developed uniformly for a variety of secure cloud platforms, without explicitly programming separate clients and servers.

Category / Keywords: applications / Domain-Specific Language, Secret Sharing, Homomorphic Encryption

Publication Info: Full version of FSTTCS 2011 publication.

Date: received 14 Oct 2011, last revised 14 Feb 2012

Contact author: deian at cs stanford edu

Available formats: Postscript (PS) | Compressed Postscript (PS.GZ) | PDF | BibTeX Citation

Note: Listings 3-6 incorrectly included some elements of an environment-based reference semantics for the core calculus, making some of the rules incorrect. In ongoing development of this work, the authors have moved to a standard substitution-based semantics. In addition, one of the indistinguishability conditions was erroneously omitted. This document corrects the above errors.

Version: 20120215:005138 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]