Cryptology ePrint Archive: Report 2011/617

Charm: A framework for Rapidly Prototyping Cryptosystems

Joseph A. Akinyele and Matthew D. Green and Avi D. Rubin

Abstract: We describe Charm, an extensible framework designed for rapid prototyping of cryptographic systems that utilize the latest advances in cryptography, such as identity and attribute-based encryption, as well as the traditional cryptographic functions. Charm is designed to minimize code complexity, promote code re-use, and to automate interoperability, while not compromising one efficiency.

Charm was designed from the ground up to support the implementation of advanced cryptographic schemes. It includes support for multiple cryptographic settings, an extensive library of re-usable code, and a protocol engine to aid in the development of interactive protocols. Our framework also provides a series of specialized tools that enable di fferent cryptosystems to interoperate. We implemented over twenty cryptographic schemes using Charm, including some new ones that to our knowledge have never been built in practice.

This paper describes our modular architecture, which includes a built-in benchmarking module that we use to compare the performance of primitives written in Python to comparable C implementations. We show that in many cases our techniques result in a potential order of magnitude decrease in code size, while inducing an acceptable performance impact.

Category / Keywords: cryptographic protocols / applied cryptography, protocol design, implementation, zero-knowledge protocols

Date: received 16 Nov 2011

Contact author: jakinye3 at jhu edu