Containerized Secure Multiparty Computing (MPC) Module for RSA Keypair Generation, Encryption and Decryption

(RSA 키생성 및 암/복호화를 위한 컨테이너화된 안전한 다자간 계산 모듈)

지도교수 : Bernard Egger

이 보고서를 공학학사 학위 논문
대체 보고서로 제출함.

2022년 5월 28일

서울대학교 자연과학대학
생명과학부
Minghang Li

2022년 8월

Containerized Secure Multiparty Computing (MPC) Module for RSA Keypair Generation, Encryption and Decryption

(RSA 키생성 및 암/복호화를 위한 컨테이너화된 안전한 다자간 계산 모듈)

지도교수 : Bernard Egger

이 보고서를 공학학사 학위 논문
대체 보고서로 제출함.

2022년 5월 28일

서울대학교 자연과학대학
생명과학부
Minghang Li

2022년 8월

Abstract

Secure Multiparty Computing (MPC) is a heated research field in cryptography with the goal of creating methods for multiple parties to jointly contribute to the computation while keeping the input private to each party. Rives-Shamir-Adleman (RSA) encryption algorithm, which requires lots of computations involving multiplication and modulus on large prime numbers, is suitable to be modified to work in an MPC scenario. However, there is no existing implementation for distributed RSA keypair generation.

Here we present a modern containerized MPC module for RSA keypair generation, encryption and decryption. It implements the classic Boneh & Franklin Scheme in a highly parallel manner using `gRPC`, a high performance Remote Procedure Call (RPC) framework. The implementation achieved the goal of eliminating the need for trusted dealer in secret sharing and successfully demonstated the effectiveness of shared RSA key generation. With the sieving method and several pruning techniques applied, it also showed sufficiently high performance, which is about 50 times faster than the traditional single-threaded scheme.

The MPC RSA module is freely open source at *https://github.com/matchy233/mpc-rsa*. The Docker images can be found at `matchy233/mpc-project_manager` and `machy233/mpc-project_worker`.

keywords: Cryptography, Secure Multiparty Computing (MPC), Distributed RSA algorithm, Distributed computing, Containerization

Contents

1 Introduction **1**

1.1 Secure Multiparty Computing (MPC) 1

1.2 Rivest-Shamir-Adleman (RSA) Algorithm 1

1.3 1

1 Introduction

1.1 Secure Multiparty Computing (MPC)

Secure Multiparty Computing (MPC) is a way of enabling a group of data owners to jointly compute a function using all their data as inputs, without disclosing any participant's private input to each other or any third party [1]. This idea was first introduced in Yao's discussion on the famous Yao's millionaire problem in the early 1980s [2]. He also raised the first MPC protocol: the Garbled Circuits Protocol [2], which remains the basis for many current MPC implementations. From then on, various MPC protocols have been proposed.

1.2 Rivest-Shamir-Adleman (RSA) Algorithm

1.3

Reference

[1] D. Evans, V. Kolesnikov, M. Rosulek, *et al.*, "A pragmatic introduction to secure multi-party computation," *Foundations and Trends® in Privacy and Security*, vol. 2, no. 2-3, pp. 70–246, 2018.

[2] A. C. Yao, "Protocols for secure computations," in *23rd annual symposium on foundations of computer science* (*sfcs 1982*), IEEE, 1982, pp. 160–164.

국문초록

RSA 키생성 및 암/복호화를 위한 컨테이너화된 안전한 다자간 계산 모듈

Minghang Li

College of Natural Sciences

Department of Biological Sciences

Seoul National University

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

주요어: