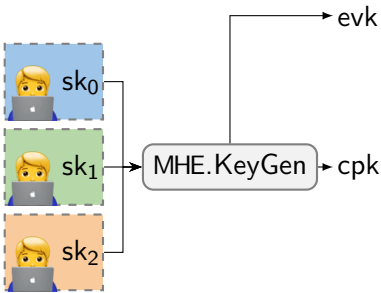
Helium: A Low-Requirement MPC Framework based on Multiparty Homomorphic Encryption

Call for Contributors

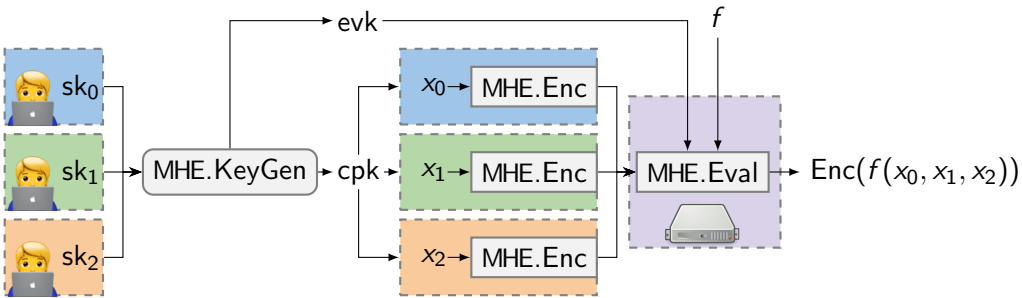
Christian Mouchet, Hasso-Plattner-Institute, University of Potsdam

23.09.2024 @ Berlin Crypto, Berlin, DE

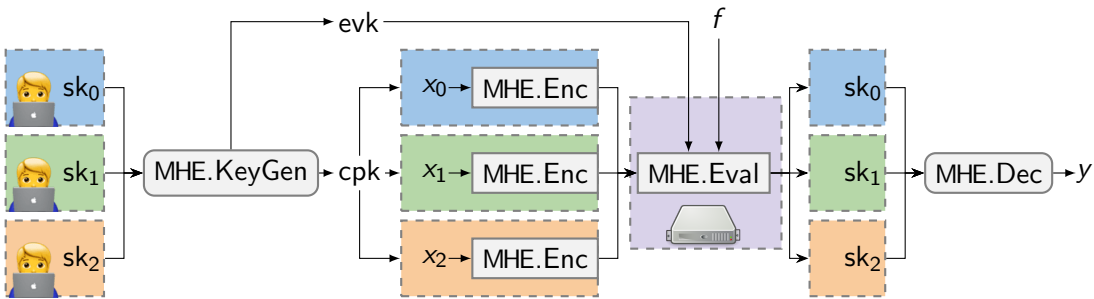
MHE-Based MPC with Helium



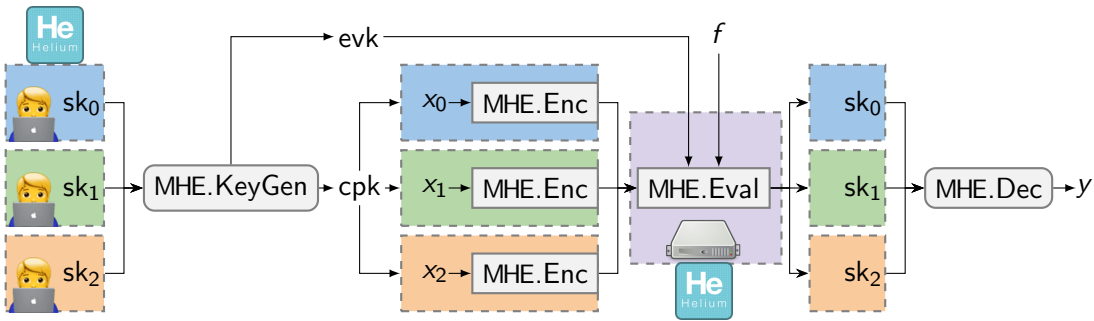
MHE-Based MPC with Helium



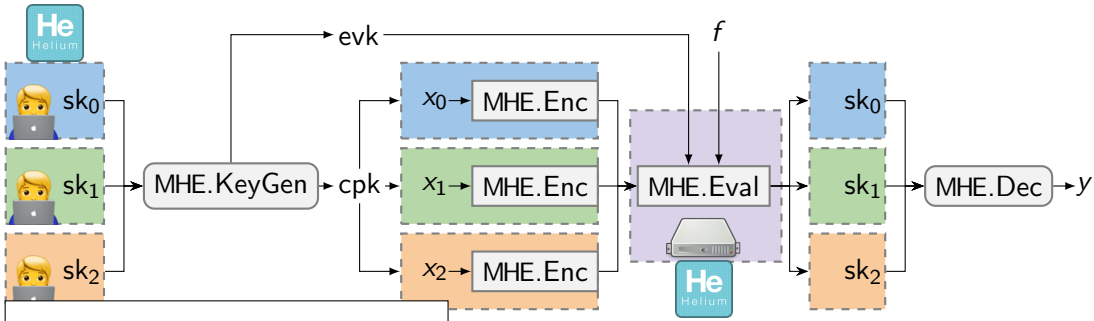
MHE-Based MPC with Helium



MHE-Based MPC with Helium



MHE-Based MPC with Helium



Helium: Scalable MPC among Lightweight Participants and under Churn

Christian Mouchet
Hasso-Plattner-Institute, University of Potsdam
Potsdam, Germany
christian.mouchet@hpi.de

Sylvain Chatel
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
sylvain.chatel@cispa.de

Apostolos Pyrgelis
RISE Research Institutes of Sweden
Stockholm, Sweden
apostolos.pyrgelis@ri.se

Carmela Troncoso
SPRING Lab, EPFL
Lausanne, Switzerland
carmela.troncoso@epfl.ch

ABSTRACT

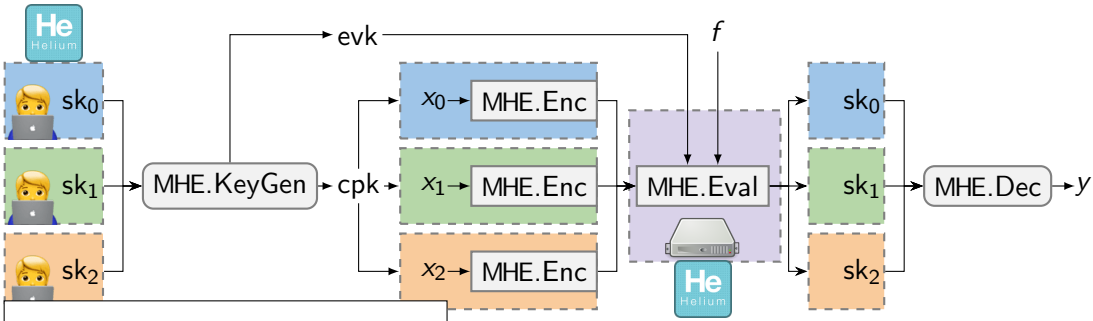
We introduce Helium, a novel framework that supports scalable secure multiparty computation (MPC) for lightweight participants and tolerates churn. Helium relies on multiparty homomorphic encryption (MHE) as its core building block. While MHE schemes have been well studied in theory, prior works fall short of addressing critical considerations paramount for adoption such as supporting resource-constrained and unstably connected participants. In this work, we systematize the requirements of MHE-based MPC protocols from a practical lens, and we propose a novel execution

1 INTRODUCTION

Cryptographic techniques for secure multiparty computation (MPC) can alleviate the need for trust between actors and enable collaborations that may otherwise be impossible due to privacy concerns. For example, MPC techniques have found applications in medical research [45], fraud detection [7], trading [40], and social sciences [46]. But the deployment of MPC is hindered by practical considerations related to the particularly resource-demanding nature of current MPC solutions, even in the semi-honest setting.

In this work, we focus on a long-standing problem in MPC sys-

MHE-Based MPC with Helium



Helium: Scalable MPC among Lightweight Participants and under Churn

Christian Mouchet
Hasso-Plattner-Institute, University of Potsdam
Potsdam, Germany
christian.mouchet@hpi.de

Sylvain Chatel
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
sylvain.chatel@cispa.de

Apostolos Pyrgelis
RISE Research Institutes of Sweden
Stockholm, Sweden
apostolos.pyrgelis@ri.se

Carmela Troncoso
SPRING Lab, EPFL
Lausanne, Switzerland
carmela.troncoso@epfl.ch

ABSTRACT

We introduce Helium, a novel framework that supports scalable secure multiparty computation (MPC) for lightweight participants and tolerates churn. Helium relies on multiparty homomorphic encryption (MHE) as its core building block. While MHE schemes have been well studied in theory, prior works fall short of addressing critical considerations paramount for adoption such as supporting resource-constrained and unstably connected participants. In this work, we systematize the requirements of MHE-based MPC protocols from a practical lens, and we propose a novel execution

1 INTRODUCTION

Cryptographic techniques for secure multiparty computation (MPC) can alleviate the need for trust between actors and enable collaborations that may otherwise be impossible due to privacy concerns. For example, MPC techniques have found applications in medical research [43], fraud detection [7], trading [40], and social sciences [46]. But the deployment of MPC is hindered by practical considerations related to the particularly resource-demanding nature of current MPC solutions, even in the semi-honest setting.

In this work, we focus on a long-standing problem in MPC sys-

- Implemented in Go, uses Lattigo for MHE
- Proof-of-concept implementation:
  1. Helper-assisted coordination
  2. No program-to-circuit compiler
  3. Passive-adversary setting

I'm looking for contributors!

Repo: `https://github.com/christianmct/helium`
Paper: `https://eprint.iacr.org/2024/194`

`christian.mouchet@hpi.de`

I'm looking for contributors!

Repo: `https://github.com/christianmct/helium`
Paper: `https://eprint.iacr.org/2024/194`

`christian.mouchet@hpi.de`

Course Announcement!

Computing on Encrypted Data: 3 ECTS course on FHE/MHE starting this fall semester