Cryptanalytic Challenges for FHE

Craig Gentry, Shai Halevi

IBM T.J. Watson

Rump session, Crypto 2010

Calling All Cryptanalysts!

- Visit https://researcher.ibm.com/researcher/view_project.php?id=1548

Calling All Cryptanalysts!

- Visit https://researcher.ibm.com/researcher/view_project.php?id=1548
- You will find:
  - A paper: “Implementing Gentry's Fully-Homomorphic Encryption Scheme”. Plus code!
  - A promise: We’ll post cryptanalytic challenges soon, when we find a site to put 3GB of files to download

Calling All Cryptanalysts!

- Visit https://researcher.ibm.com/researcher/view_project.php?id=1548
- You will find:
  - A paper: “Implementing Gentry's Fully-Homomorphic Encryption Scheme”. Plus code!
  - A promise: We’ll post cryptanalytic challenges soon, when we find a site to put 3GB of files to download
- Meantime: challenges are on DVDs (mail, in person)

About the Challenges…

- Challenge 1: Public key of FHE scheme
  - Range of lattice dimensions: toy (512), small (2048), medium (8192), large (32768)

https://researcher.ibm.com/researcher/view_project.php?id=1548

About the Challenges…

- Challenge 1: Public key of FHE scheme
  - Range of lattice dimensions: toy (512), small (2048), medium (8192), large (32768)
- Challenge 2: instances of the sparse subset sum problem

https://researcher.ibm.com/researcher/view_project.php?id=1548

About the Challenges…

- Challenge 1: Public key of FHE scheme
  - Range of lattice dimensions: toy (512), small (2048), medium (8192), large (32768)
- Challenge 2: instances of the sparse subset sum problem
- Cash reward for breaking large challenge:

https://researcher.ibm.com/researcher/view_project.php?id=1548

About the Challenges…

- Challenge 1: Public key of FHE scheme
  - Range of lattice dimensions: toy (512), small (2048), medium (8192), large (32768)
- Challenge 2: instances of the sparse subset sum problem
- Cash reward for breaking large challenge:

  $200,000, as soon as I get it from Scott Aaronson

https://researcher.ibm.com/researcher/view_project.php?id=1548