Fully Homomorphic Encryption

M.L. de Groot

University of Amsterdam

October 20, 2014

Homomorphic Encryption

Homomorphism

- Property
- Encryption that allows computation on ciphertext that corresponds to the same computations on the plaintext
- To perform arithmetic operations over encrypted bits

Operations

- $Enc(b_1) + Enc(b_2) = Enc(b_1 + b_2 \mod 2)$
- $Enc(b_1) \cdot Enc(b_2) = Enc(b_1 \cdot b_2 \mod 2)$

Example: RSA

$$Enc(m_1) = m_1^e \mod N$$

$$Enc(m_2) = m_2^e \mod N$$

Only supports multiplication: Somewhat Homomorphic Encryption (SHE)

Fully Homomorphic Encryption

With addition and multiplication any operation can be supported!

Fully Homomorphic Encryption (FHE)
Homomorphism under both addition *and* multiplication

Drawbacks

- Security
  - Can we control what is computed?
  - Structural information
- Computationally demanding
- Difficult to design

History

- 1978: Introduced by Rivest
- 2009: First to design Craig Gentry
  - Ideal lattices
  - Inefficient
- Since 2009: Refinements and improvements

Applications

Barak: "FHE is the swiss-army knife of cryptography"

- Arithmetic operations over encrypted bits
- No secret key needed

Applications

- Cloud computing
- Private queries in a search engine
- Secure multi-party computation
- Electronic voting

Questions?