

EVE: An Efficient Implementation of Homomorphic Encryption on Integer Vectors

Angel Yu
Wai Lok Lai
James Payor

May 6, 2015

Introduction to Homomorphic Encryption

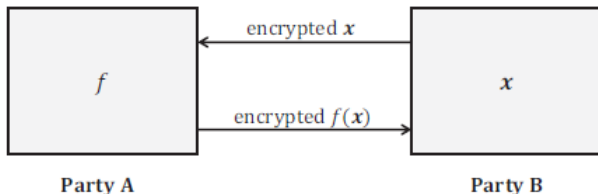


Figure: Most common usage of homomorphic encryption schemes

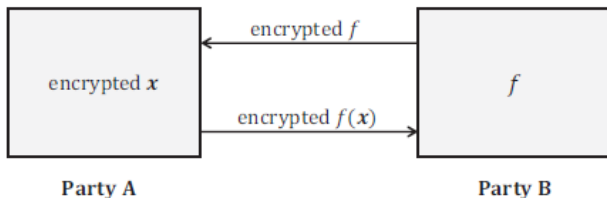


Figure: EVE, the homomorphic encryption scheme considered in our project

Overview of EVE: Supported Operations

Fundamental Operations:

- Encrypt: $\mathbf{c} = E_S(\mathbf{x})$
- Decrypt: $\mathbf{x} = D_S(\mathbf{c})$
- Switching secret keys from S to S'

Supported Operations on Integer Vectors:

- Addition of two vectors: $\mathbf{x}_1 + \mathbf{x}_2$
- Linear transformation: $G\mathbf{x}$
- Weighted inner product of two vectors: $\mathbf{x}_1^T H \mathbf{x}_2$

Can compose these operations to support arbitrary integer polynomials

Details of Fundamental Operations

Encrypt \mathbf{x} with secret key S :

- Choose \mathbf{c} such that $S\mathbf{c} = w\mathbf{x} + \mathbf{e}$

Decrypt \mathbf{c} with S :

- $\mathbf{x} = \left\lceil \frac{S\mathbf{c}}{w} \right\rceil$

Key switching from S to $S' = [I, T]$:

- Want $S'\mathbf{c}' = S\mathbf{c}$
- Want key-switch matrix M such that $S'M = S + E$
- $M = \begin{pmatrix} -TA + S + E \\ A \end{pmatrix}$ for random matrix A , random noise matrix E
- Then $\mathbf{c}' = M\mathbf{c}$

Details of the Three Supported Operations

Addition: $\mathbf{x}' = \mathbf{x}_1 + \mathbf{x}_2$:

- Let $\mathbf{c}' = \mathbf{c}_1 + \mathbf{c}_2$
- So $S\mathbf{c}' = w(\mathbf{x}_1 + \mathbf{x}_2) + (\mathbf{e}_1 + \mathbf{e}_2)$

Linear Transformation: $\mathbf{x}' = G\mathbf{x}$

- Note $GS\mathbf{c} = wG\mathbf{x} + G\mathbf{e}$
- Hence $E_S(\mathbf{x}) = E_{GS}(G\mathbf{x})$
- So $\mathbf{c}' = \mathbf{c}$ and decrypt with $S' = GS$

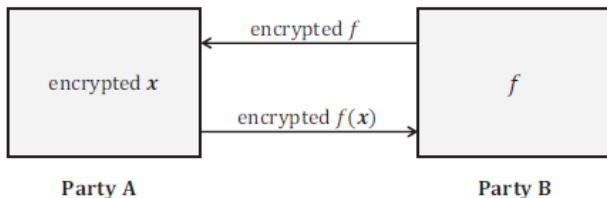
Details of the Three Supported Operations (con'd)

Weighted Inner Product: $\mathbf{x}' = \mathbf{x}_1^T H \mathbf{x}_2$

- Let $S' = \text{vec}(S^T H S)^T$
- Let $\mathbf{c}' = \left\lceil \frac{\text{vec}(\mathbf{c}_1 \mathbf{c}_2^T)}{w} \right\rceil$
- Note $(S \mathbf{c}_1)^T H (S \mathbf{c}_2) = w^2 (\mathbf{x}_1^T H \mathbf{x}_2) + (w \mathbf{x}_1^T H \mathbf{e}_2 + w \mathbf{e}_1^T H \mathbf{x}_2 + \mathbf{e}_1^T H \mathbf{e}_2)$
- So $S' \mathbf{c}' = w (\mathbf{x}_1^T H \mathbf{x}_2) + \mathbf{e}'$

Secrecy in the Scheme

- Clients (Party B) calculate key-switch matrices based on operations
- Server (Party A) calculates without knowing the operations



Applications

- In each application, we have:
 - ▶ Server with data (can be encrypted with S , known to the client)
 - ▶ Client that wants to learn a function of the data
- Effective when server has a lot of data, and results are small

Applications

- Search

- ▶ Server has (encrypted) feature vectors for our data
- ▶ Client wants to score each item to rank them

- Classification

- ▶ Want

Bibliography



Walter Rudin, *Principles of mathematical analysis*. McGraw-Hill Book Co., 3rd Edition, 1976.