Homomorphic Encryption and our current research

Chris Carr
ccarr@item.ntnu.no

Department of Telematics
Norwegian University of Science and Technology

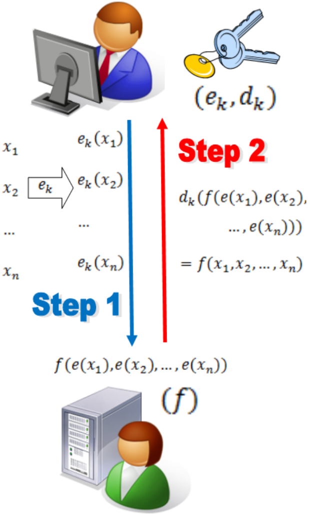
NTNU

October, 2014 COINS Seminar

Homomorphic Encryption

What is it?

- Privacy homomorphism – Rivest, Adleman, Dertouzos.

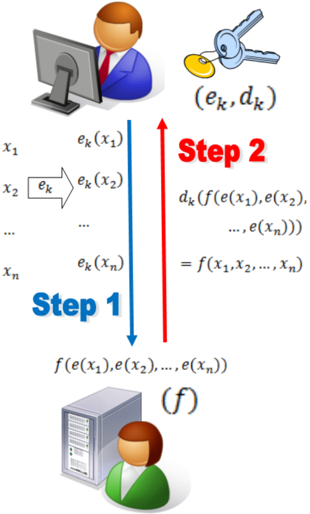


(e_k, d_k)
x_1
x_2
...
x_n
e_k
$e_k(x_1)$
$e_k(x_2)$
...
$e_k(x_n)$
Step 1
Step 2
$d_k(f(e(x_1), e(x_2), \ldots, e(x_n)))$
$= f(x_1, x_2, \ldots, x_n)$
$f(e(x_1), e(x_2), \ldots, e(x_n))$
(f)

Homomorphic Encryption

What is it?

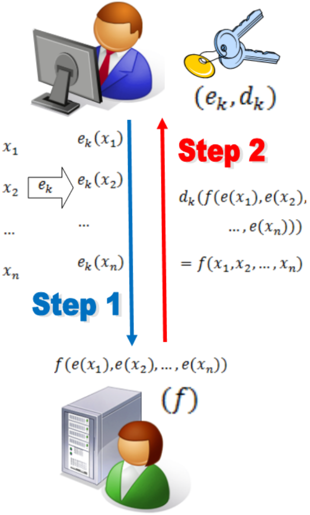
- Privacy homomorphism – Rivest, Adleman, Dertouzos.
- Multiplication – textbook RSA


(e_k, d_k)
x_1
x_2
...
x_n
e_k
$e_k(x_1)$
$e_k(x_2)$
...
$e_k(x_n)$
Step 1
Step 2
$d_k(f(e(x_1), e(x_2), \dots, e(x_n)))$
$= f(x_1, x_2, \dots, x_n)$
$f(e(x_1), e(x_2), \dots, e(x_n))$
(f)

Homomorphic Encryption

What is it?

- Privacy homomorphism – Rivest, Adleman, Dertouzos.
- Multiplication – textbook RSA
- Addition – Pailler's cryptosystem

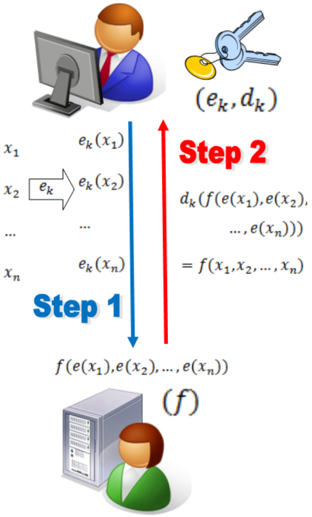


(e_k, d_k)
x_1
$e_k(x_1)$
Step 2
x_2
e_k
$e_k(x_2)$
$d_k(f(e(x_1), e(x_2), \dots, e(x_n)))$
...
...
x_n
$e_k(x_n)$
$= f(x_1, x_2, \dots, x_n)$
Step 1
$f(e(x_1), e(x_2), \dots, e(x_n))$
(f)

Homomorphic Encryption

What is it?

- Privacy homomorphism – Rivest, Adleman, Dertouzos.
- Multiplication – textbook RSA
- Addition – Pailler's cryptosystem
- Gentry and FHE.

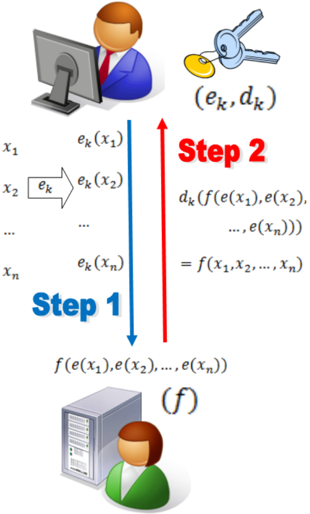


(e_k, d_k)
x_1
x_2
...
x_n
e_k
$e_k(x_1)$
$e_k(x_2)$
...
$e_k(x_n)$
Step 1
Step 2
$d_k(f(e(x_1),e(x_2),\ldots,e(x_n)))$
$= f(x_1,x_2,\ldots,x_n)$
$f(e(x_1),e(x_2),\ldots,e(x_n))$
(f)

Homomorphic Encryption

What is it?

- Privacy homomorphism – Rivest, Adleman, Dertouzos.
- Multiplication – textbook RSA
- Addition – Pailler's cryptosystem
- Gentry and FHE.
- The future...



(e_k, d_k)
x_1
x_2
...
x_n
e_k
$e_k(x_1)$
$e_k(x_2)$
...
$e_k(x_n)$
Step 1
Step 2
$d_k(f(e(x_1), e(x_2), \dots, e(x_n)))$
$= f(x_1, x_2, \dots, x_n)$
$f(e(x_1), e(x_2), \dots, e(x_n))$
(f)

Fully Homomorphic Encryption

General goal:

Further the developments of fully homomorphic encryption (FHE).

Fully Homomorphic Encryption

General goal:

Further the developments of fully homomorphic encryption (FHE).

Inevitable first question:

What is FHE?

Fully Homomorphic Encryption

General goal:

Further the developments of fully homomorphic encryption (FHE).

Inevitable first question:

What is FHE?

- Not immediately clear.
- We do have other types:

Fully Homomorphic Encryption

General goal:

Further the developments of fully homomorphic encryption (FHE).

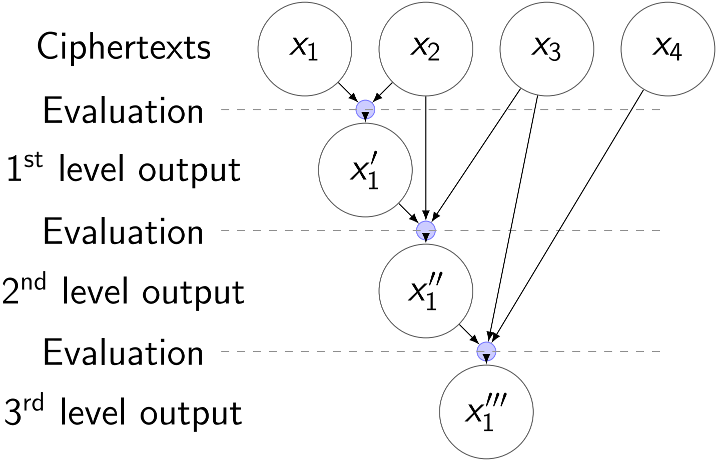
Inevitable first question:

What is FHE?

- Not immediately clear.
- We do have other types:
  - Somewhat
  - Levelled
  - Fully

FHE, appealing to intuition

Evaluating evaluation... by example



Ciphertexts

Evaluation

1st level output

Evaluation

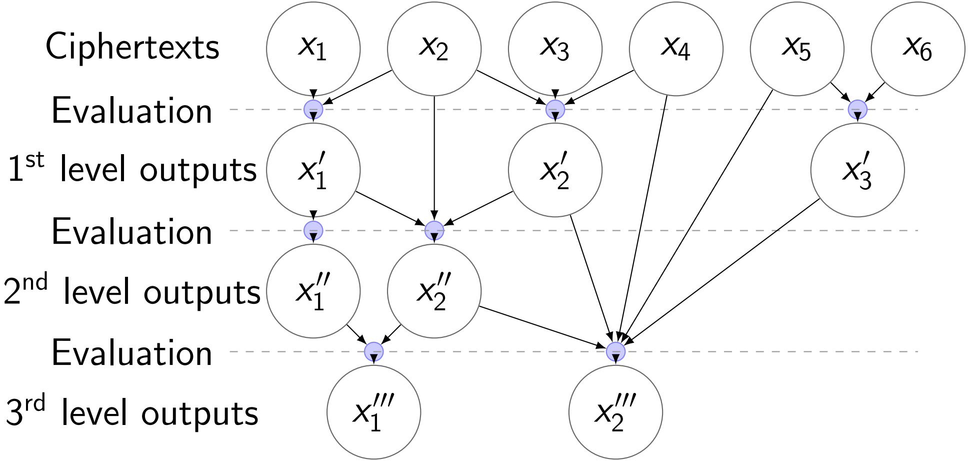
2nd level output

Evaluation

3rd level output

FHE, appealing to intuition

Evaluating evaluation... by example



Ciphertexts

Evaluation

1st level outputs

Evaluation

2nd level outputs

Evaluation

3rd level outputs

Abstract Homorphic Scheme

Three Musicians – Pablo Picasso

Our research

Or, what am I actually doing?

- Collaboration between NTNU and the University of Mannheim.

Our research

Or, what am I actually doing?

- Collaboration between NTNU and the University of Mannheim.
- Research direction:
  - What are the fundamentals of FHE schemes?

Our research

Or, what am I actually doing?

- Collaboration between NTNU and the University of Mannheim.
- Research direction:
  - What are the fundamentals of FHE schemes?
- Results:

Our research

Or, what am I actually doing?

- Collaboration between NTNU and the University of Mannheim.
- Research direction:
  - What are the fundamentals of FHE schemes?
- Results:
  - Generalisation of definitions.

Our research

Or, what am I actually doing?

- Collaboration between NTNU and the University of Mannheim.
- Research direction:
  - What are the fundamentals of FHE schemes?
- Results:
  - Generalisation of definitions.
  - Implications.

Our research

Or, what am I actually doing?

- Collaboration between NTNU and the University of Mannheim.
- Research direction:
  - What are the fundamentals of FHE schemes?
- Results:
  - Generalisation of definitions.
  - Implications.
  - Characterization of FHE.

Our research

Or, what am I actually doing?

- Collaboration between NTNU and the University of Mannheim.
- Research direction:
    - What are the fundamentals of FHE schemes?
- Results:
    - Generalisation of definitions.
    - Implications.
    - Characterization of FHE.
- Outcome: Paper due in November. Hurrah!

That's all Folks!