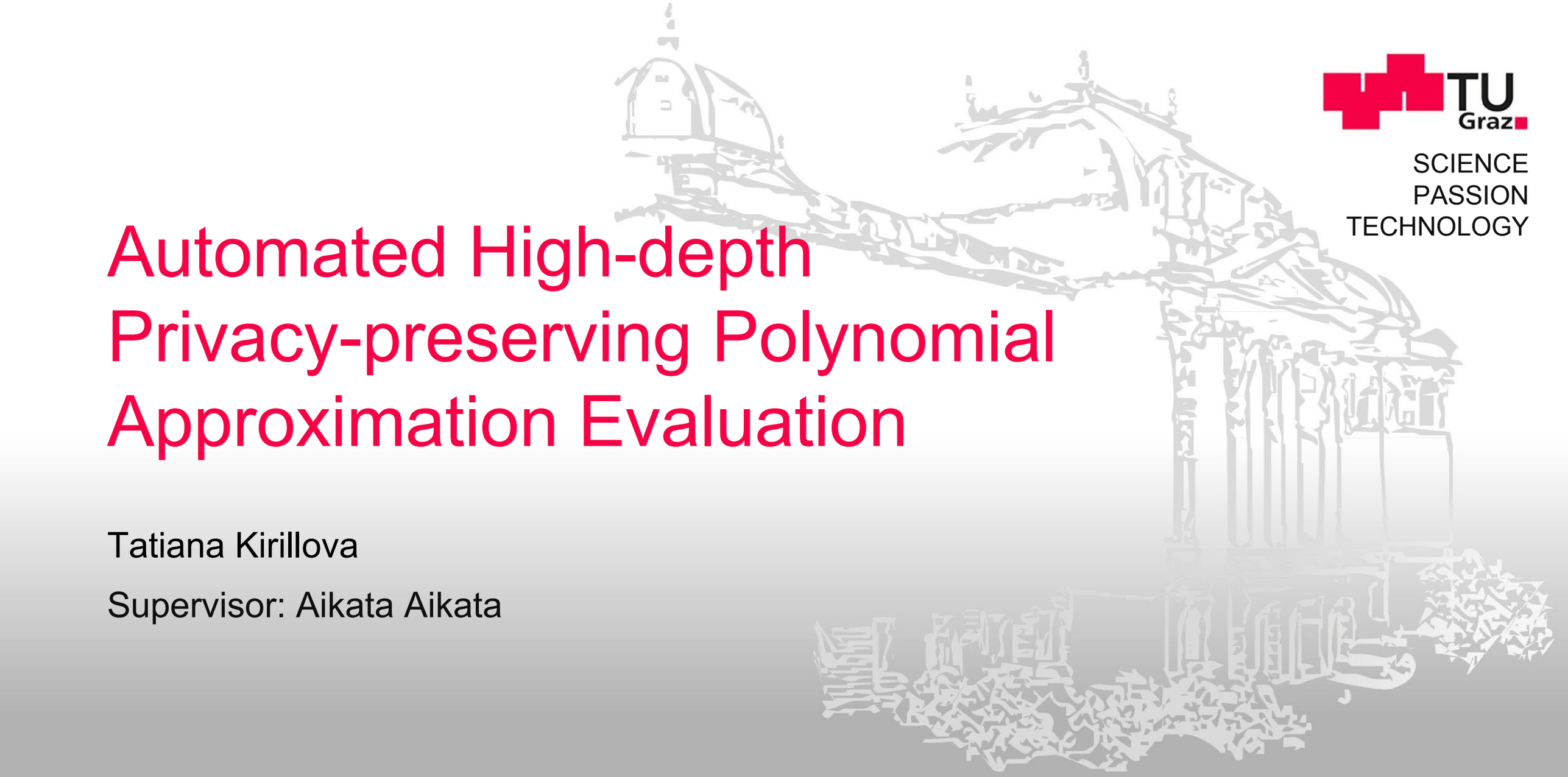


SCIENCE
PASSION
TECHNOLOGY

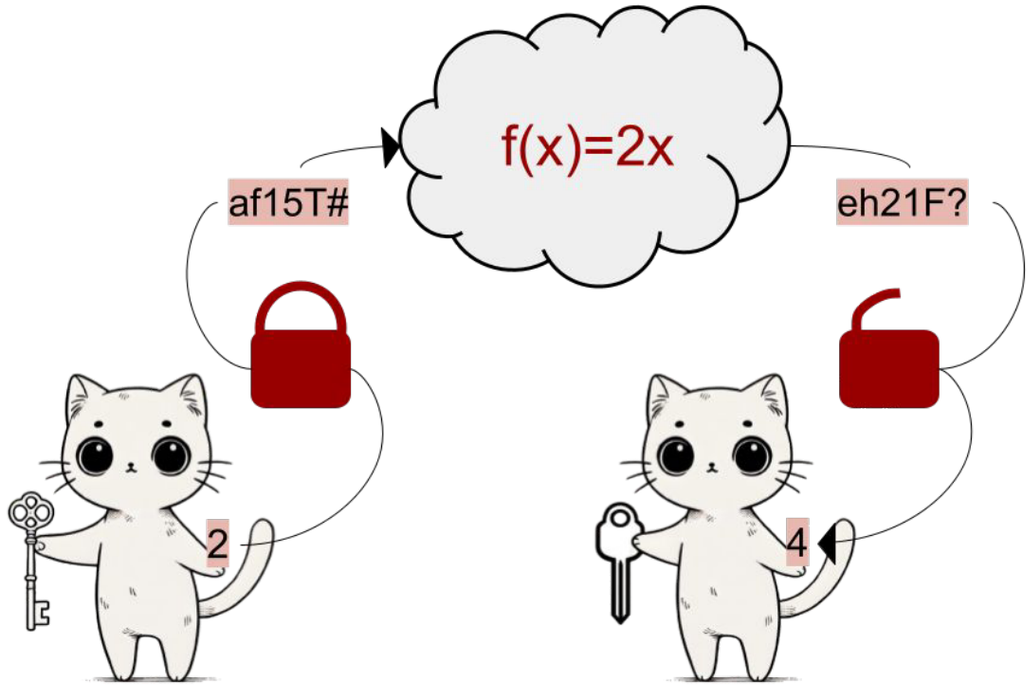
Automated High-depth Privacy-preserving Polynomial Approximation Evaluation

Tatiana Kirillova

Supervisor: Aikata Aikata

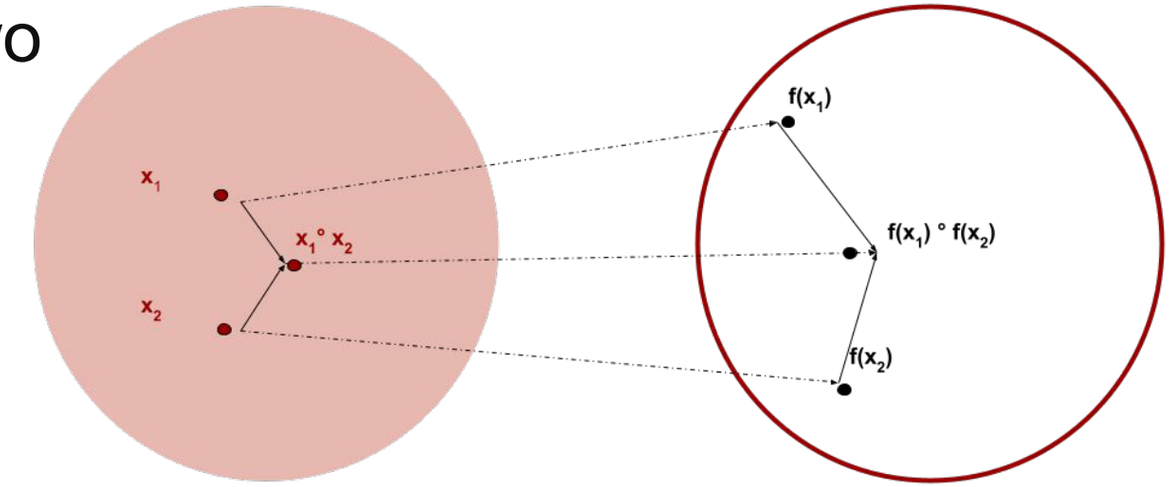
September, 2024

Homomorphic encryption



Homomorphism

Homomorphism = map between two algebraic sets if the same type.



An encryption scheme is homomorphic if:

$$E(m_1) \circ E(m_2) = E(m_1 \circ m_2), \forall m_1, m_2 \in M$$

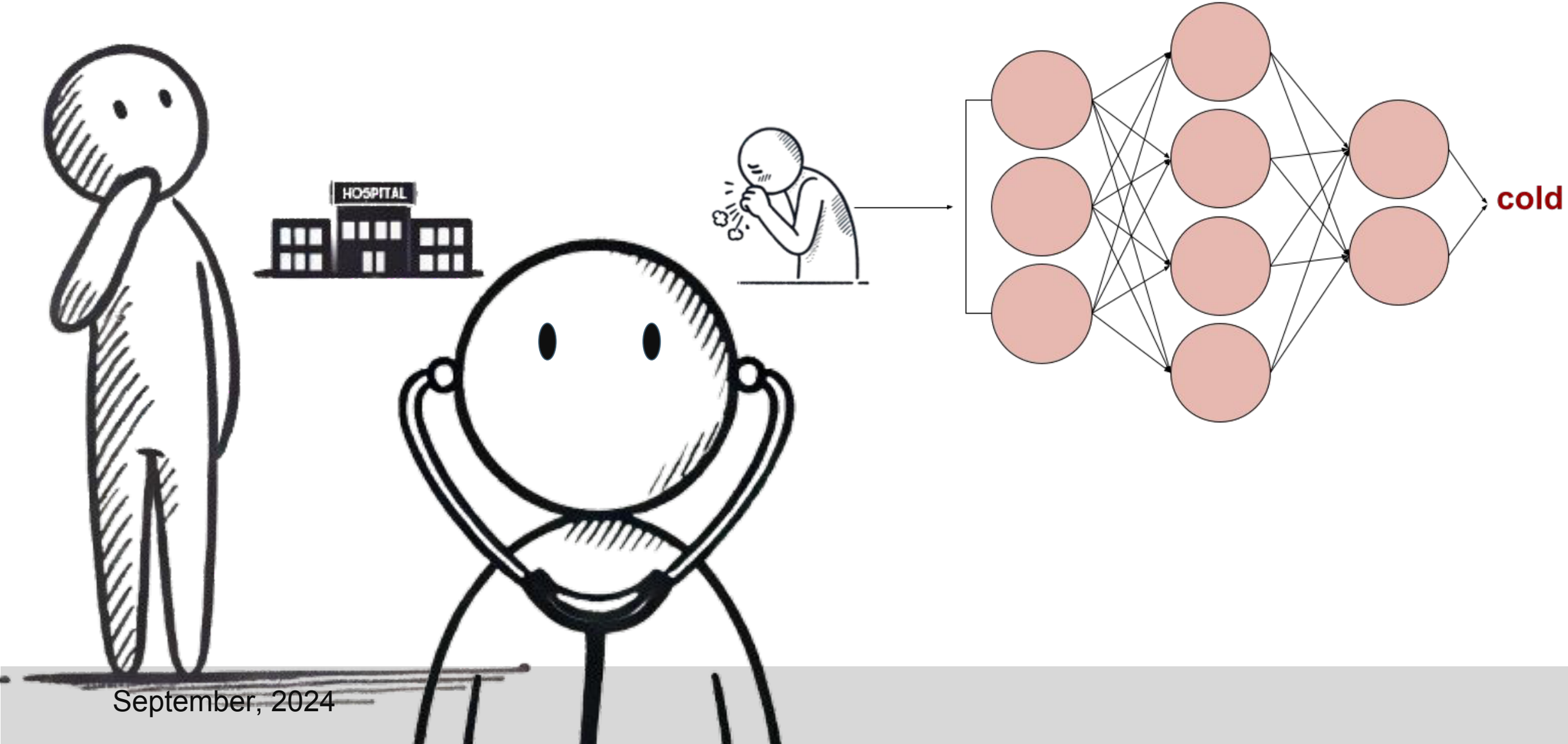
OpenFHE

- Framework
- Has all of the schemes
- User-friendly
- Tutorials

CKKS Scheme

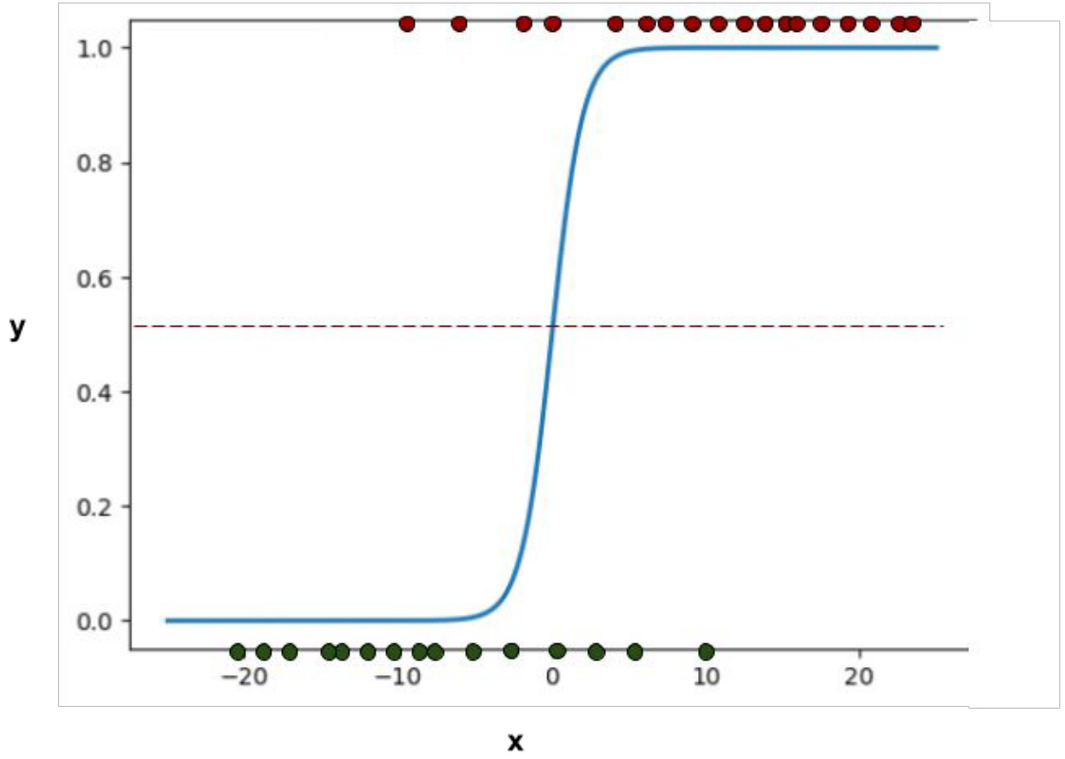
- approximate FHE
- supports computations of real numbers
- applicable for Privacy-Preserving Machine Learning

Privacy-preserving Machine Learning



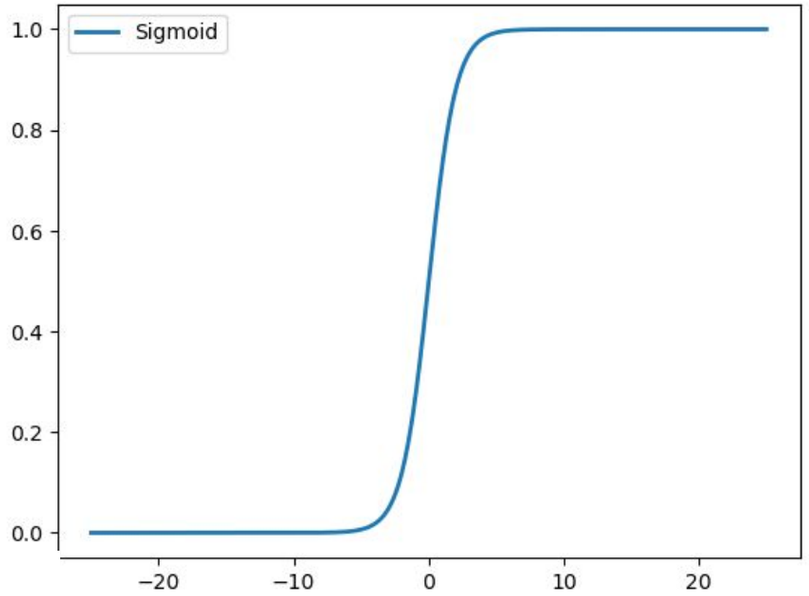
Logistic regression

- x is combination of all learned parameters: ex.
  = w1 * color + w2 * shape + b
- learned parameters, weights, affect the position of the sigmoid on the x axis



Sigmoid Function

- activation function in logistic regression
- cannot be represented as a polynomial and needs to be approximated



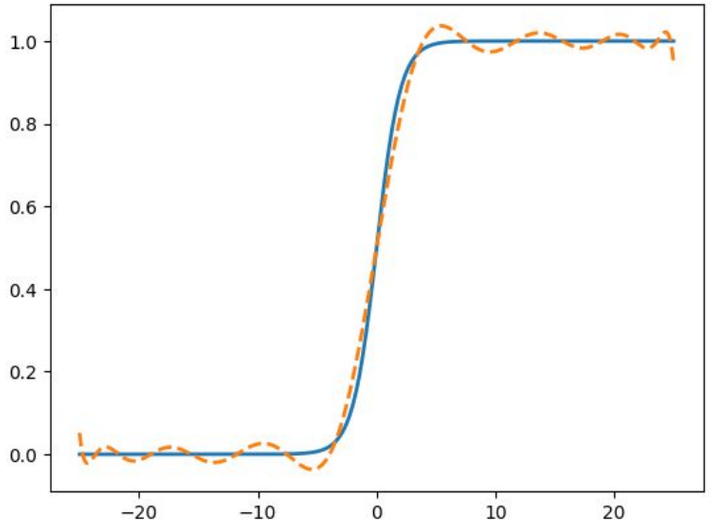
$$f(x) = \frac{1}{1 + e^{-x}}$$

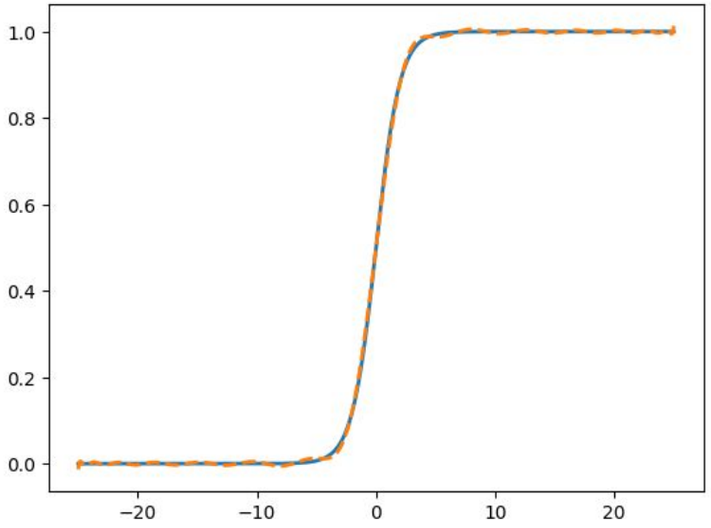
Sigmoid - Polynomial Approximation

$$f(x) = \frac{1}{1 + e^{-x}}$$

$$c_d x^d + c_{n-1} x^{d-1} + \ldots + c_0$$

- Numpy Polynomial.fit()
- least-squares fit





FHERMA Challenges

SIGN Challenge

The article details the solution provided by the winner of the Sign Function Challenge.

Author: Aikata, Ph.D. student at TU Graz

On this page:

The sign function, also known as signum, determines the sign of a value. It has significant applications in machine learning, serving as a foundational element for non-linear activation functions like the Rectified Linear Unit (ReLu) or Max Pooling. This is attributed to the ability of the sign function to facilitate comparison or max operations in the following manner:

Logistic Function Challenge

The article details the solution provided by the winner of the Logistic Regression Challenge.

Author: Aikata, Ph.D. student at TU Graz

On this page:

Test case #1

Test case #2

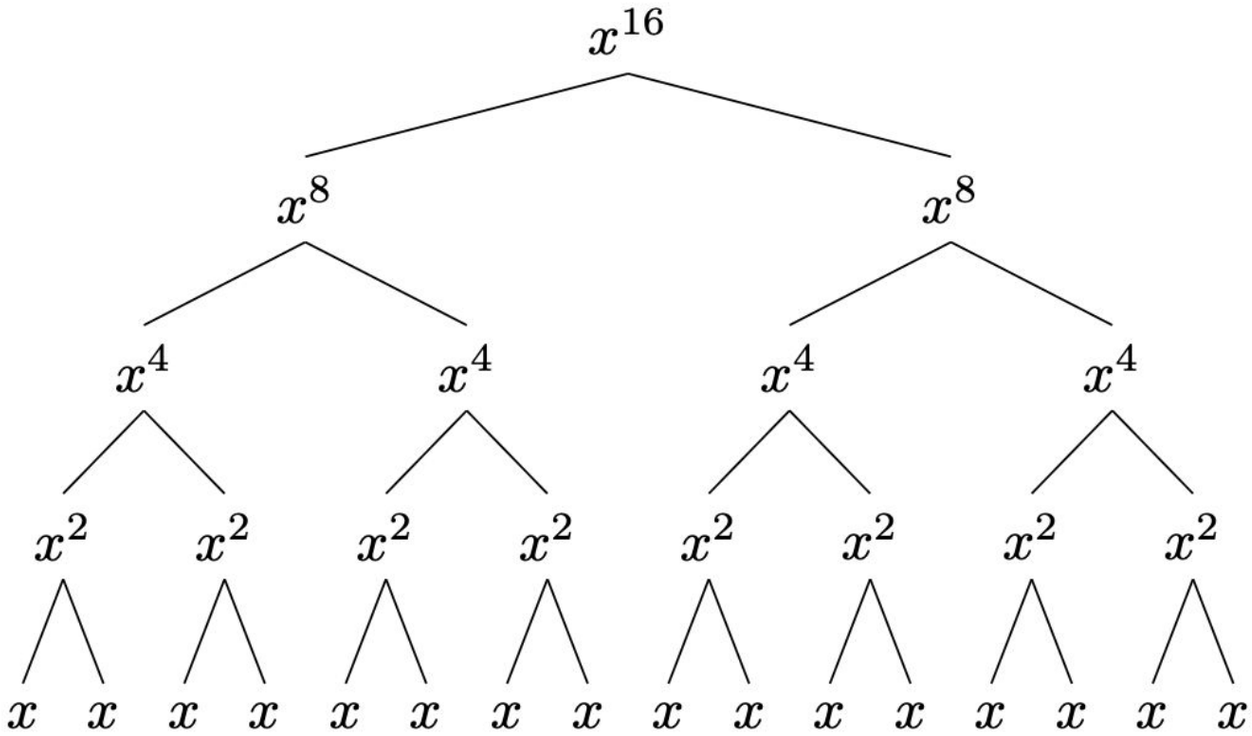
The logistic (a.k.a., sigmoid) function forms the basis for logistic regression-based machine learning. It is commonly employed as a non-linear activation function in neural networks. Homomorphic schemes like CKKS only support polynomial arithmetic operations, and expressing the sigmoid function as a polynomial is not feasible. Various series, such as the Taylor series or the Chebyshev series, are utilized to approximate

Multiplicative Depth

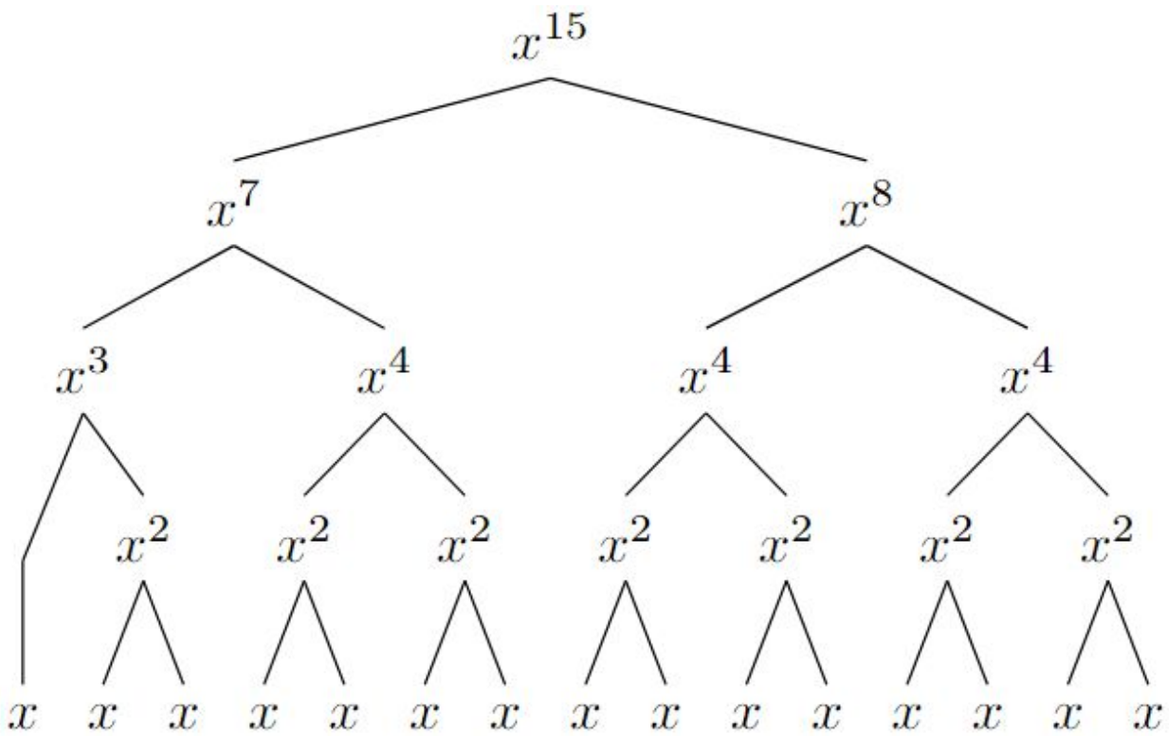
$$((x * x)x)x = (x * x)(x * x) = x^4$$

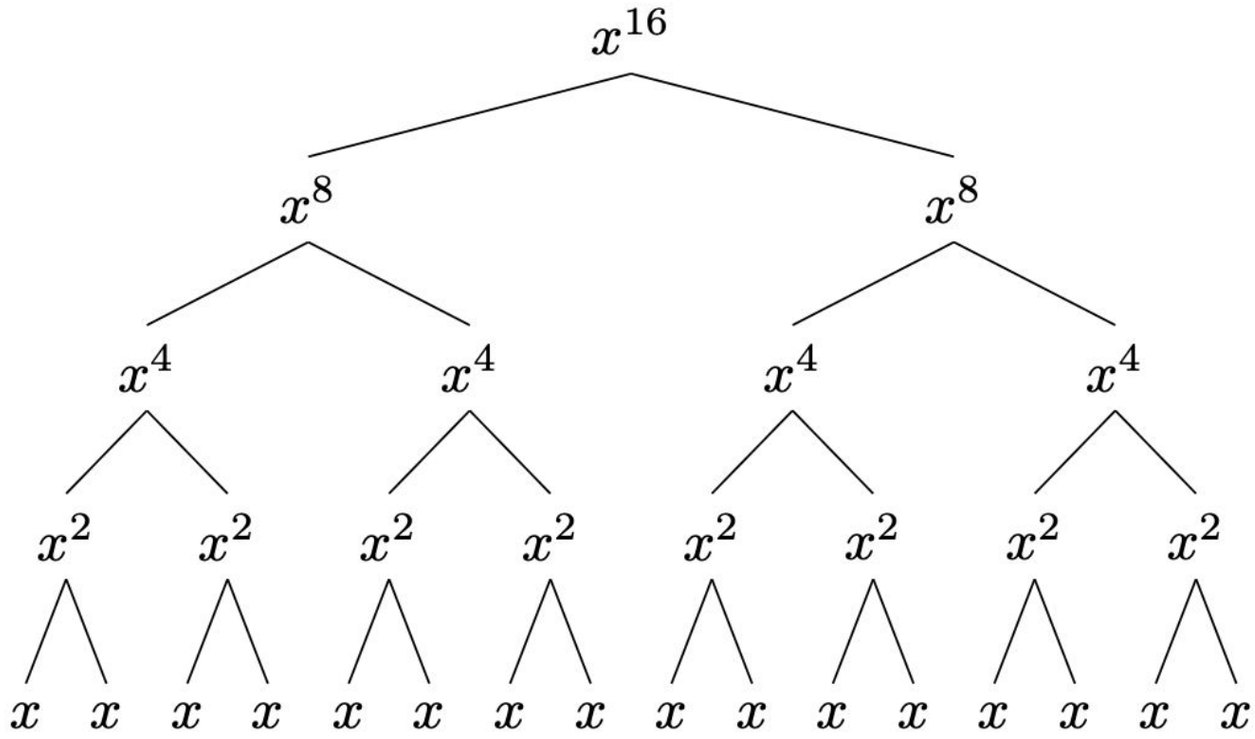
Multiplicative Depth

- binary tree decomposition technique



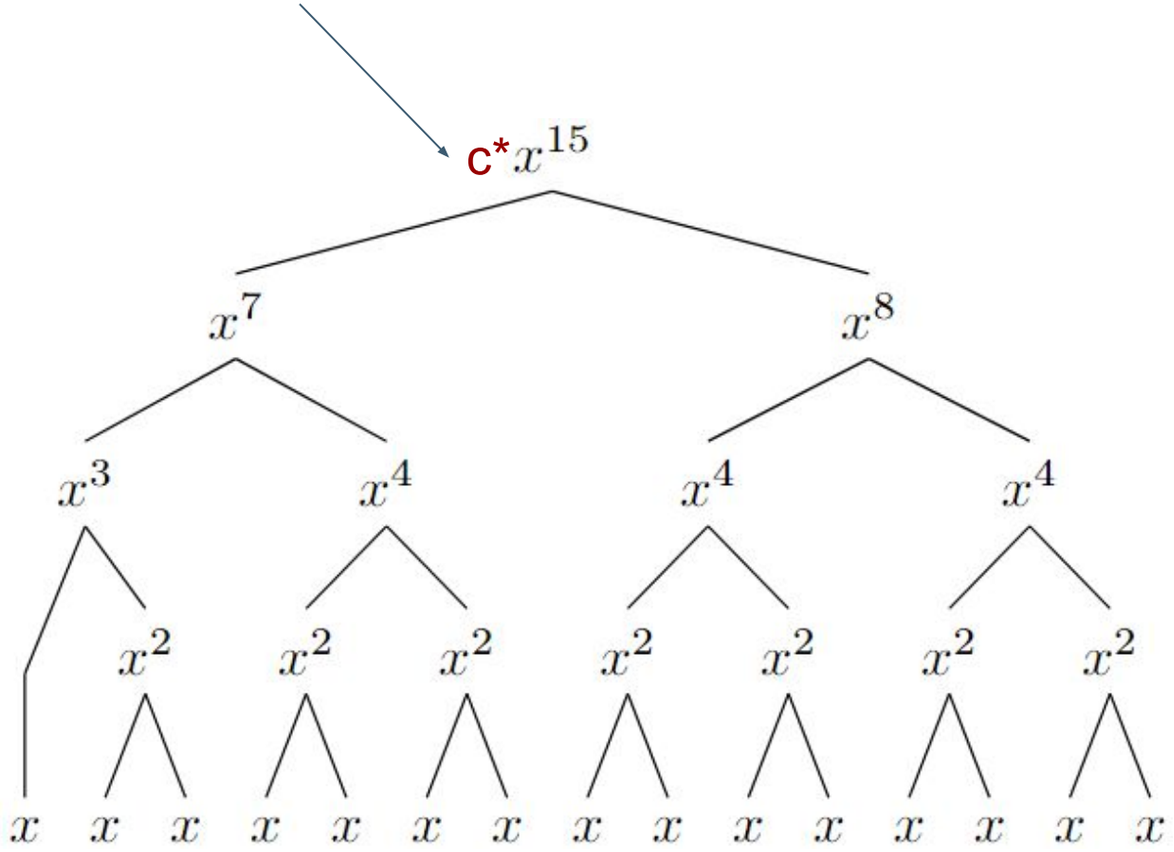
Multiplicative Depth

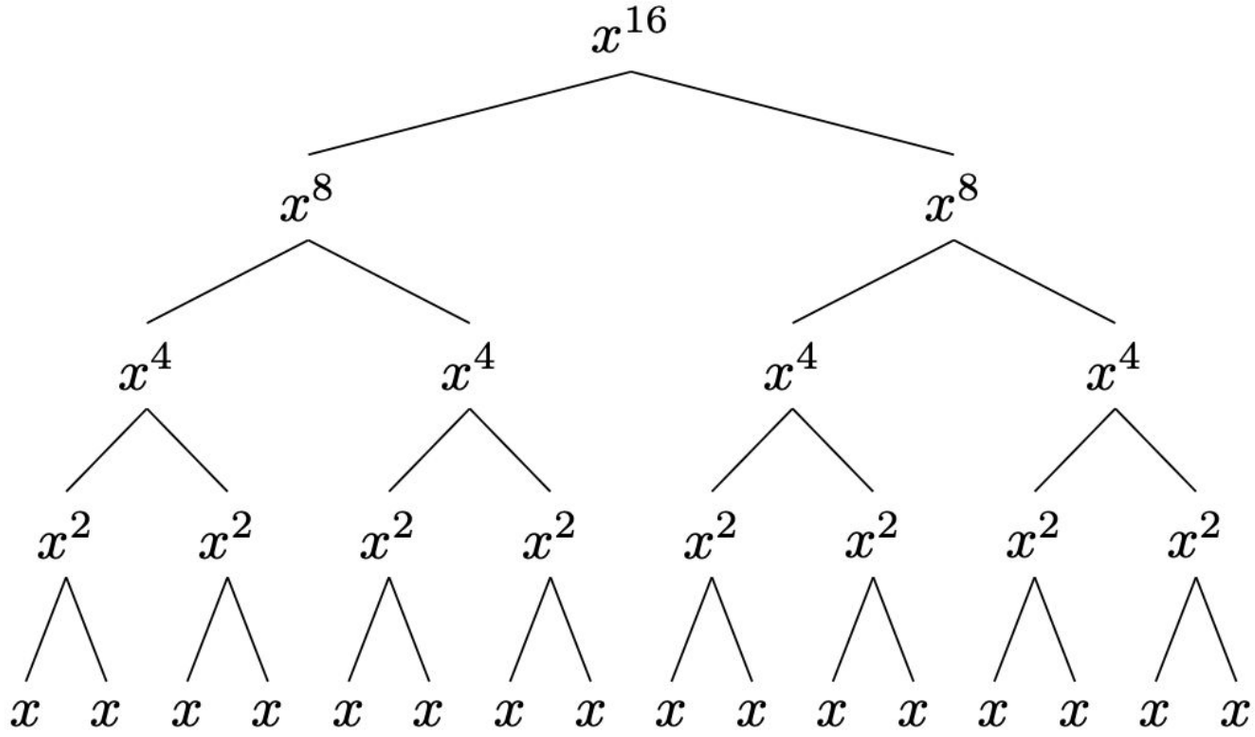




depth = 4

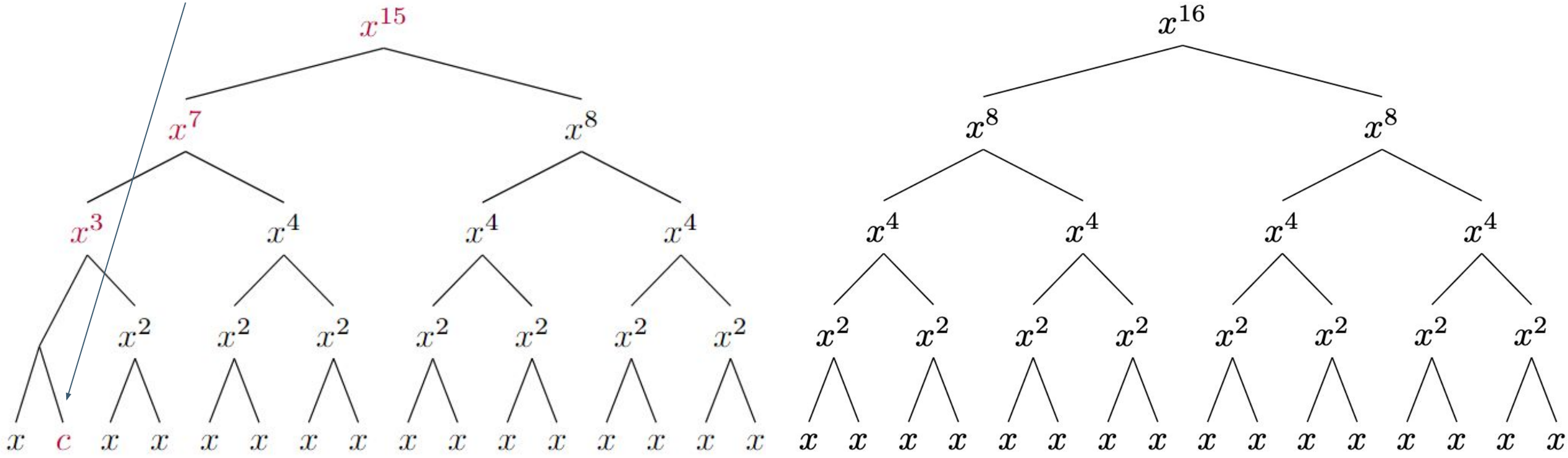
Multiplicative Depth





depth = 5

Multiplicative Depth



depth = 4

EvalPoly

```
auto result = cc->EvalPoly(ciphertext1, coefficients1);
```

Our Implementation

- sum
- recursive tree evaluation
  - **base case**: power = 1 with a flag coeffUsed set to true
  - if power odd => eval()

$$c_d x^d + c_{n-1} x^{d-1} + \ldots + c_0$$

Coefficient Splitting

```
array([ 5.00000000e-01,  2.26806207e-01,  7.10213751e-11, -1.07117796e-02,
       -1.41439692e-12,  3.52123146e-04,  1.27758476e-14, -7.05240408e-06,
       -4.73856319e-17,  8.99429984e-08, -2.05300071e-18, -7.61584637e-10,
        5.04075306e-20,  4.39092971e-12, -5.50984144e-22, -1.73238634e-14,
        3.58582142e-24,  4.55363924e-17, -1.51640495e-26, -7.13526075e-20,
        4.28088613e-29,  3.14409283e-23, -7.95812290e-32,  1.26765549e-25,
        9.05003211e-35, -3.19383668e-28, -4.70167613e-38,  3.58641738e-31,
       -1.54055379e-41, -2.09459946e-34,  3.37570182e-44,  5.15557487e-38,
       -1.31014816e-47])
```

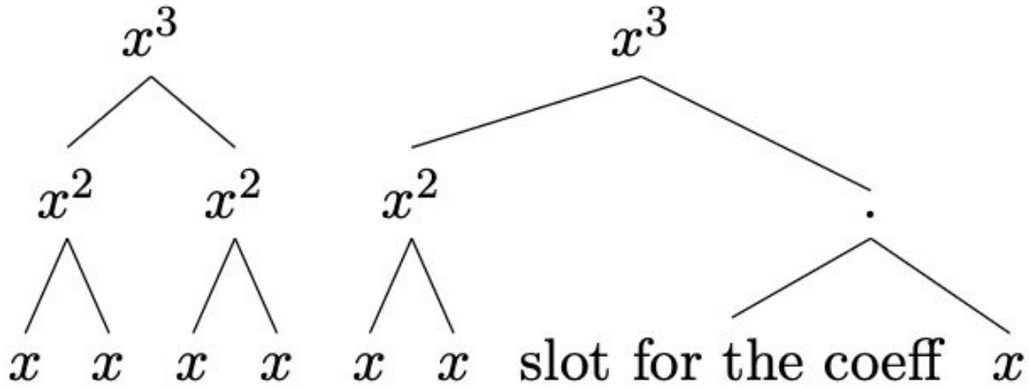
Coefficient Splitting - Thresholds

10^{-10} -> {c*10^{10}, 10^{-5}, 10^{-5} }

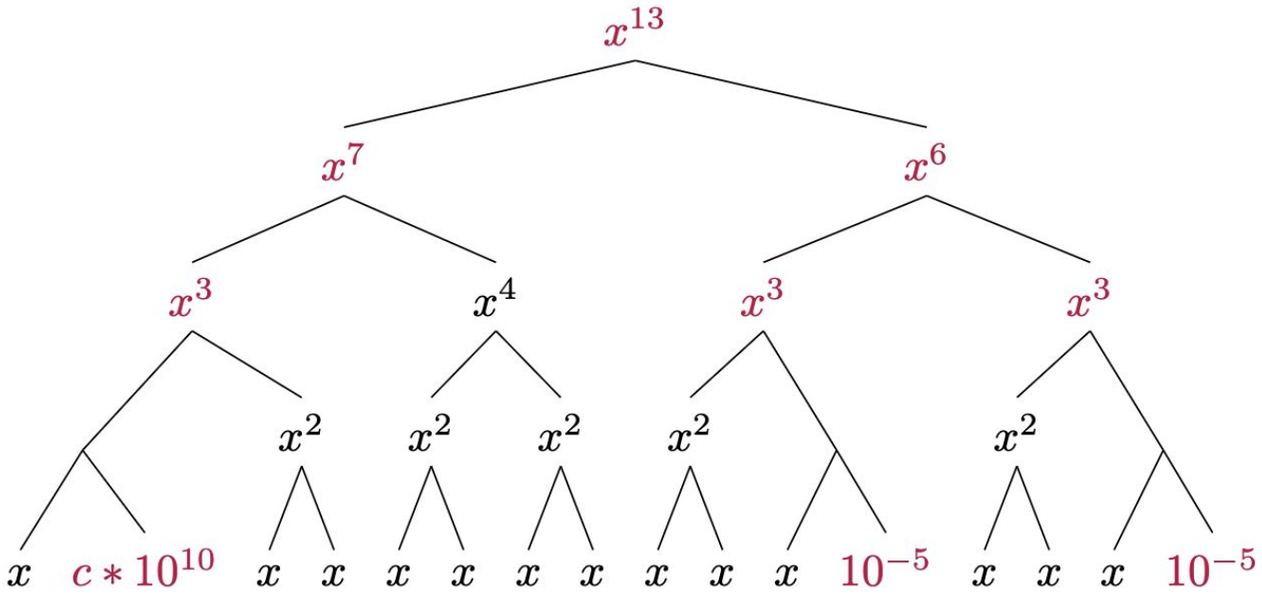
10^{-20} -> {c*10^{20}, 10^{5}, 10^{5}, 10^{5}, 10^{5}}

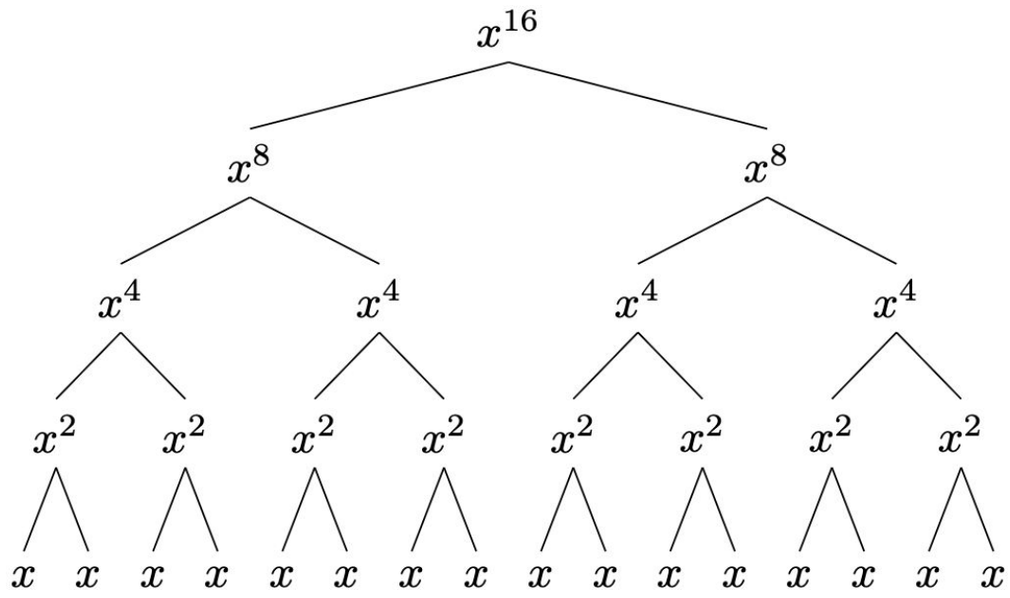
10^{-40} -> {c*10^{40}, 10^{5}, 10^{5} …}

10^{-80} -> {c*10^{80}, 10^{5}, 10^{5} … }



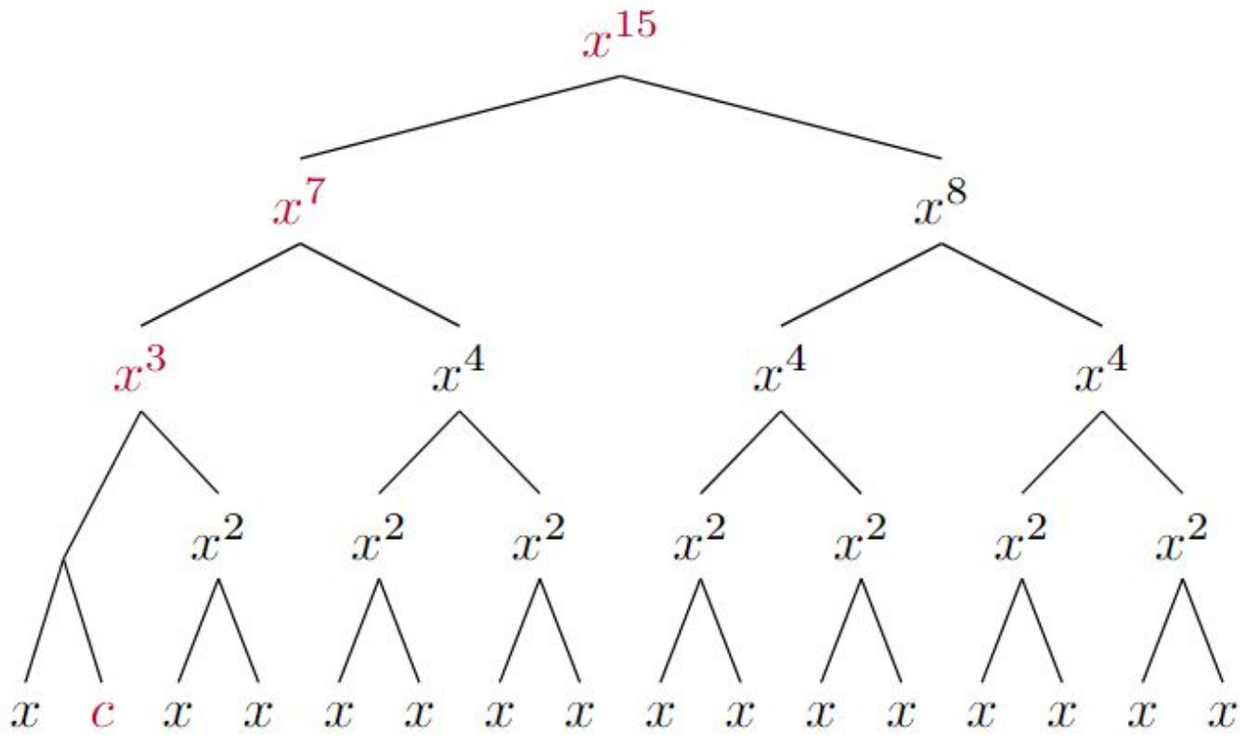
Coefficient Splitting

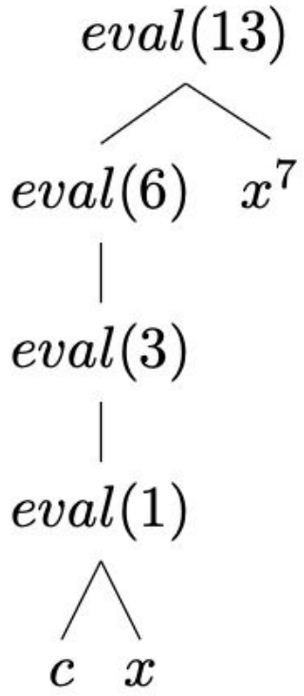




depth = 4

Term pre-generation



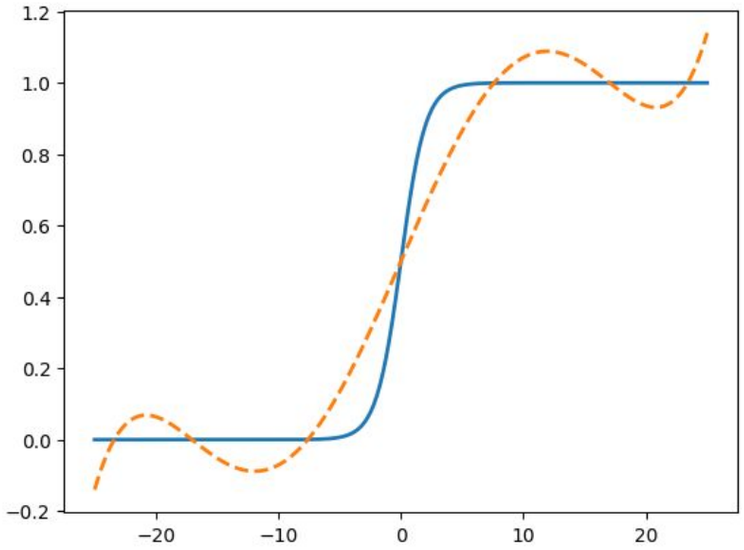


Results

Depth	**EvalPoly** - max. available degree	**Our Implementation** - max. available degree
3	5	7
4	13	15
5	27	31
6	60	63

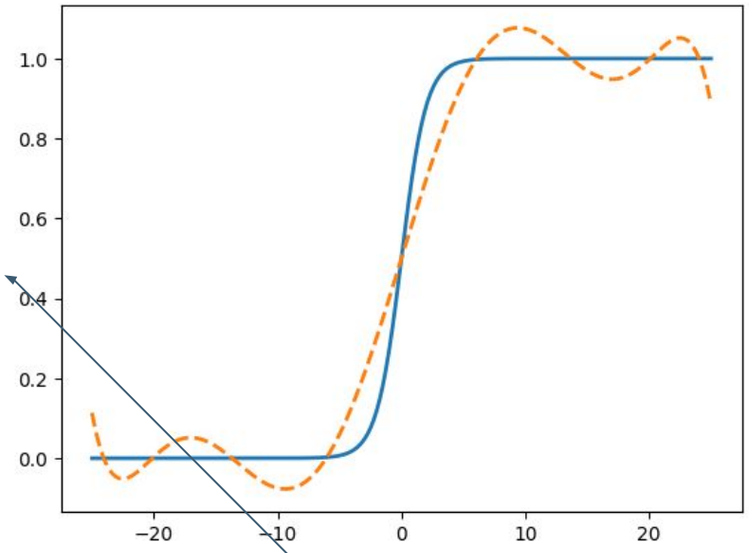
Results

99.04%



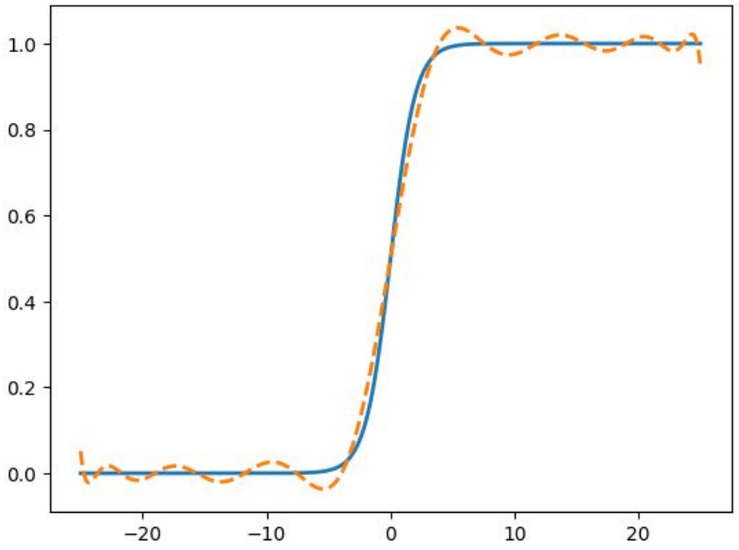
Degree 5

99.47%



Degree 7

99.94%

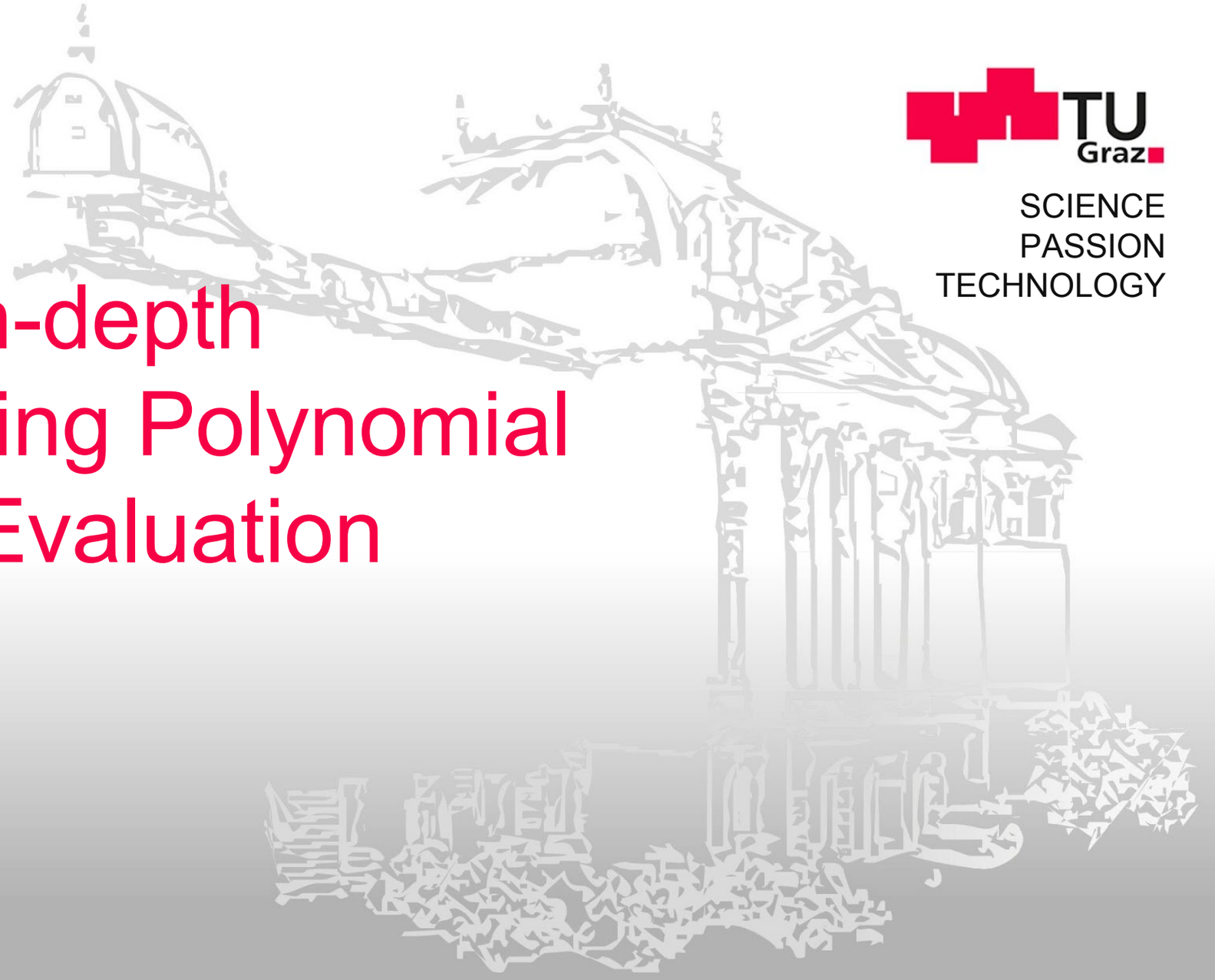


Degree 15

Results

Degree 27: 99.9977%
Degree 31: 99.9969% -> +0.0008%
Degree 63: 99.9985% -> +0.0016%

> jump from degree 28 to 31 half as significant as the jump from degree 31 to 63.



SCIENCE
PASSION
TECHNOLOGY

Automated High-depth Privacy-preserving Polynomial Approximation Evaluation

Tatiana Kirillova

Supervisor: Aikata Aikata

September, 2024