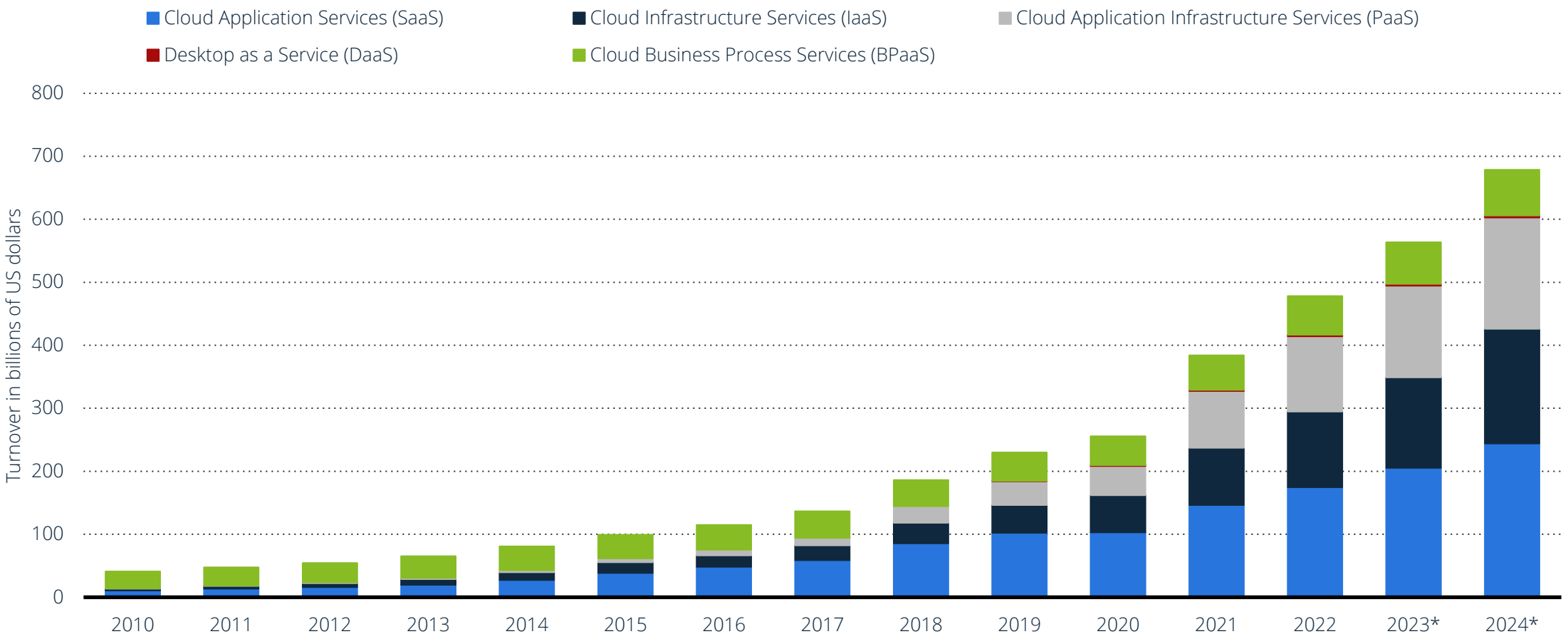
Introduction to Homomorphic Cryptosystems

Lecture 1

Cloud Computing

Global cloud computing revenue from 2010 to 2022 and forecast to 2024 by segment (in billions of US dollars)

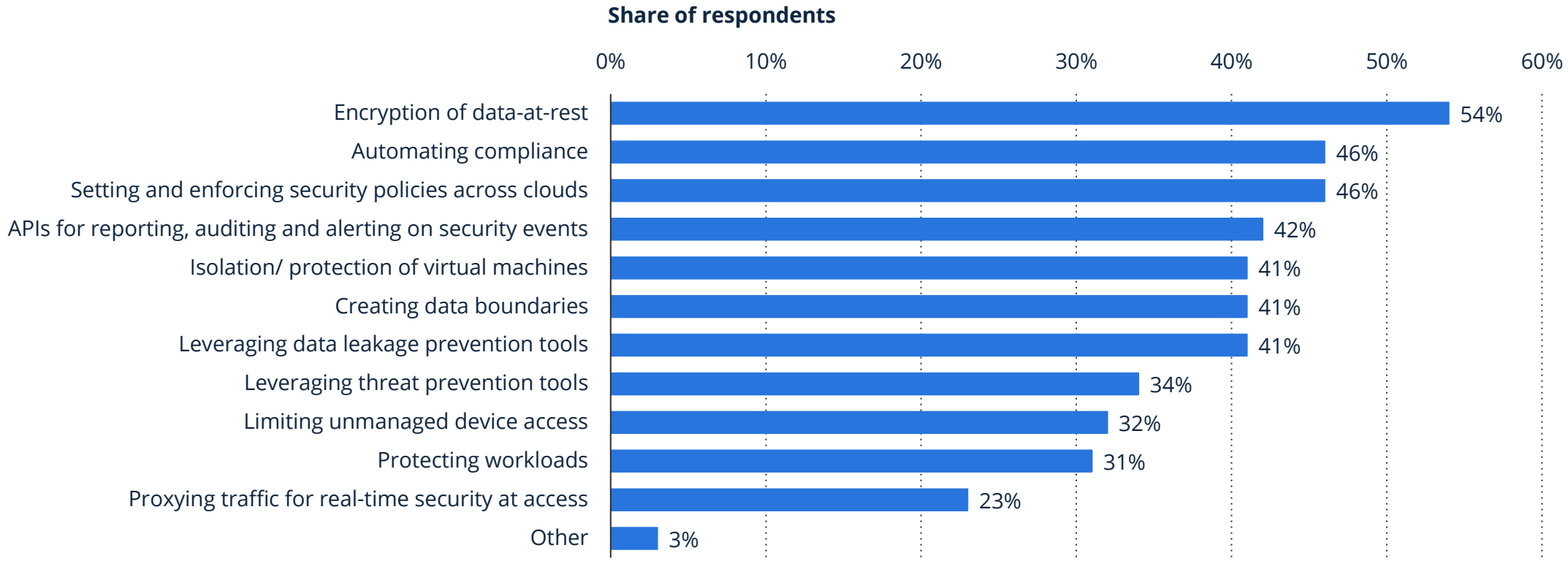


https://de.statista.com/statistik/daten/studie/195760/umfrage/umsatz-mit-cloud-computing-weltweit/

Whats a Limiting Factor of Cloud Computing?

Which of the following security controls would most increase your confidence in adopting public clouds?

Global security tools that would increase public cloud adoption worldwide 2022



Description: According to 54 percent of respondents, encryption of data-at-rest was the security tool that would increase their confidence in public cloud adoption in 2022. At the same time, 46 percent of respondents chose automating compliance as the best security tool to increase public cloud adoption worldwide. Read more
Note(s): Worldwide; March 2022; 823 respondents; Cybersecurity professionals
Source(s): Branden; Cybersecurity Insiders; Fortinet

Motivation

Cloud computing has grown over the last decade and is expected to become more important in the future.

The AI market size is projected to rise from 241.8 billion U.S. dollars in 2023 to almost 740 billion U.S. dollars in 2030, accounting for a compound annual growth rate of 17.3%. [1]

The number of digital crimes is increasing and causing ever greater losses.

In the E.U., 57% of large enterprises using the cloud reported the risk of a security breach as the main limiting factor in the use of cloud computing services. [2]

[1] https://www.statista.com/statistics/941835/artificial-intelligence-market-size-revenue-comparisons/
[2] Josep Domingo-Ferrer, et Al.; ”Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges” https://doi.org/10.1016/j.comcom.2019.04.011.

Data Privacy vs. Confidentiality vs. Data Integrity vs. Access Control

Data privacy

- The claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others

Confidentiality

- The protection of sensitive information from unauthorized access or disclosure.

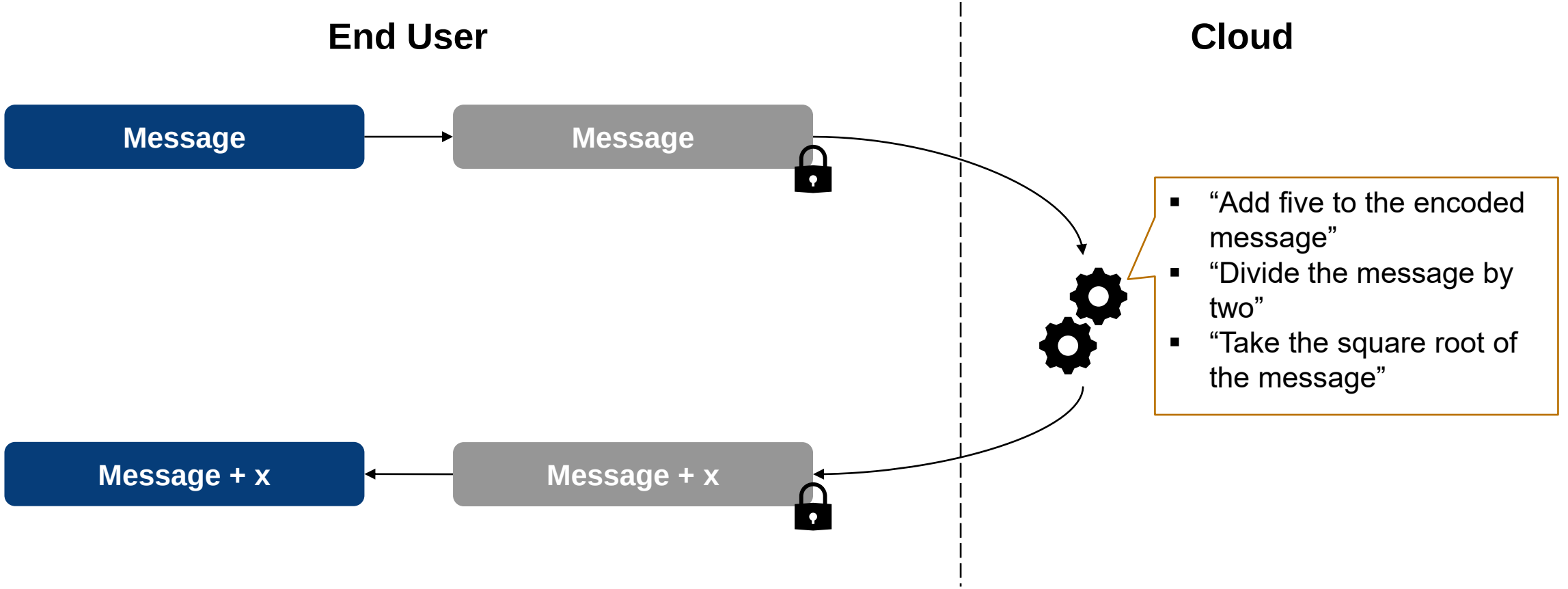
Data integrity

- Ensuring the accuracy, completeness, consistency, and validity of the data.

Access Control

- The selective restriction of access to a place or other resource (data).

Motivation – Basic Idea



- We can do calculations on encrypted numbers
- The party doing calculations does not know the outcome

Motivation - History

- Idea and name was first introduced by Rivest et al. in 1978
  - Assumption that cryptosystems with the homomorphic property are possible
  - But: no solution
- No fully homomorphic solution was found over the next 30 years
- Breakthrough in 2009 by Gentry et al.
  - First real homomorphic cryptosystem
  - Possible to do unlimited number of operations on the ciphertext

Homomorphic Encryption (HE) is a new and interesting topic, which is expected to undergo more breakthroughs in the future

Goals

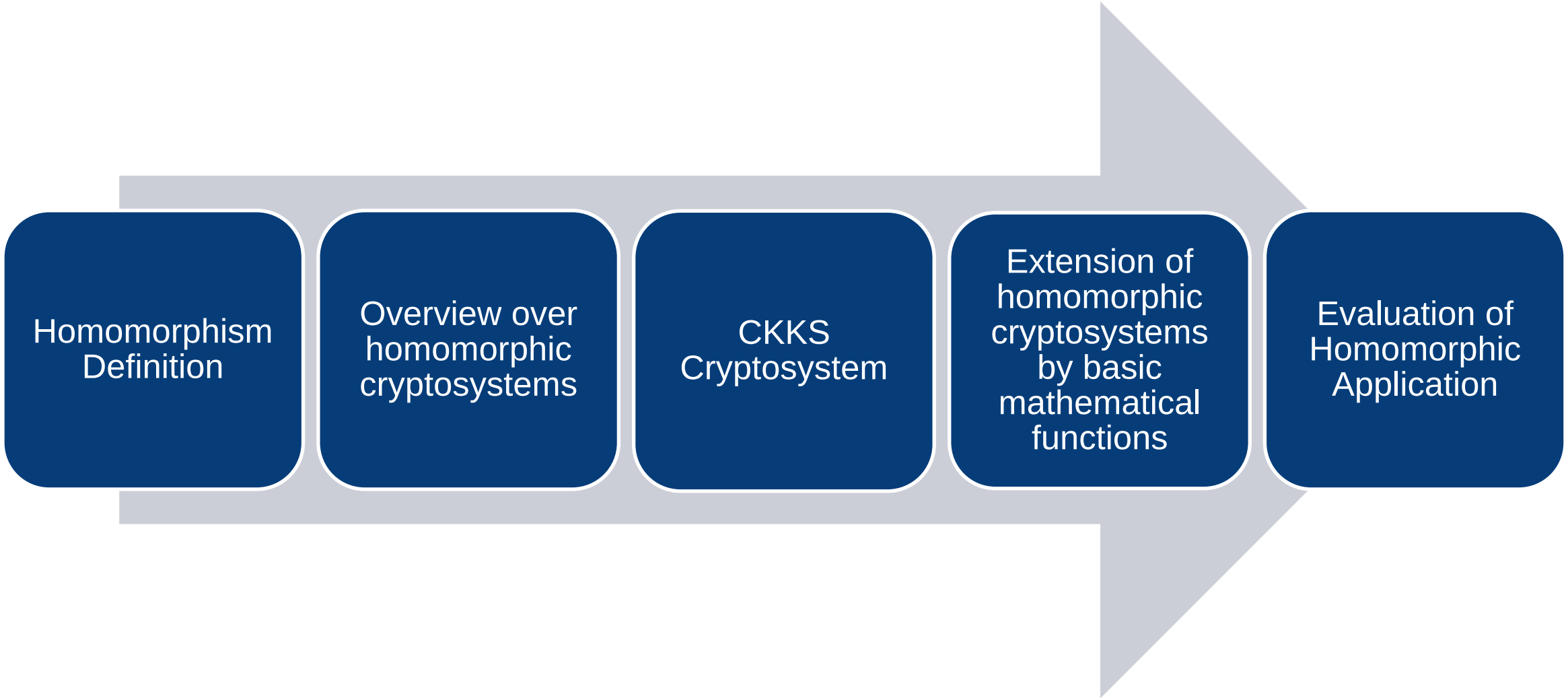
The idea and importance of Homomorphic Encryption

Mathematical background and differences of multiple HE cryptosystems

How to implement important functions with limited operations

What do we want to learn in this lecture?

Storyline of the Lecture



MATHEMATICAL BACKGROUND

Mathematical Background

Group

A group is a set G, combined with an operation $\circ$, such that

- The group contains an **identity**

  $$\exists e \in G: \forall a \in G: e \circ a = a = a \circ e$$

- The group contains **inverses**

  $$\forall a \in G: \exists b \in G: a \circ b = e = b \circ a$$

- The operation is **associative**

  $$\forall a, b, c \in G: (a \circ b) \circ c = a \circ (b \circ c)$$

- The group is **closed** under the operation

  $$\forall a, b \in G: (b \circ a) \in G$$

Example

The integers together with the operation $+$ build the Group $(\mathbb{Z}, +)$:

- **Identity** element

  $e = 0$

- **Inverse** element

  The inverse of a is $-a$

- The operation is **associative**

  Addition is associative

- The group is **closed**:

  Adding two integers always gives an integer

Mathematical Background

Homomorphism

A homomorphism is a map between two algebraic structures of the same type (that is of the same name), that preserves the operations of the structures.

- Group
- Monoid
- Ring
- Vector space
- Modul
- …

Group homomorphism

Given two groups $(G,*)$ and $(H,\circ)$, a group homomorphism is a function

$$f: G \to H$$

such that

$$\forall x, y \in G: f(x * y) = f(x) \circ f(y)$$

Observation

$$f(e_G) = e_H$$

(e_G is the identity element of G, e_H analog)

Group Homomorphism Example

$f(x) = \exp(x) = e^x$ yields a group homomorphism from the group $(\mathbb{R}, +)$ to the group $(\mathbb{R}^+, \cdot)$.

$\mathbb{R}^+$: The group of positive real numbers

This is needed because:
$exp\colon \mathbb{R} \to \mathbb{R}^+$

Proof

Trivial because of the rules of exponents:

$$z^m \cdot z^n = z^{m+n}$$

$\forall x, y \in G\colon f(x * y) = f(x) \circ f(y)$

So for all $x, y \in \mathbb{R}$ the exponential function fulfills the homomorphic property:

$$f(x + y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$$

HOMOMORPHIC PROPERTY OF RSA

Homomorphic property of RSA

The (textbook) RSA cryptosystem

Encryption of m: $E(m) = m^e \bmod N = c$

Decryption of c: $D(c) = c^d \bmod N = m$

- e: Public key
- d: Private key
- N: Public parameter

Short task

Does this cryptosystem fulfil homomorphic properties?

And if so: Which mathematical operation preserves the structure?

Homomorphic property of RSA

The (textbook) RSA cryptosystem

Encryption of m: $E(m) = m^e \bmod N = c$

Decryption of c: $D(c) = c^d \bmod N = m$

- e: Public key
- d: Private key
- N: Public parameter

RSA is homomorph with respect to multiplication

$$E(m_1) \cdot E(m_2) = m_1^e m_2^e \bmod n$$
$$= (m_1 m_2)^e \bmod n$$
$$= E(m_1 \cdot m_2)$$

OVERVIEW OVER HOMOMOPRHIC CRYPTOSYSTEMS

Homomorphic cryptosystems

We distinguish between three different homomorphic encryption approaches:

Partially Homomorphic Encryption (PHE)
Allows only one type of operation with an unlimited number of times

Additive or **Multiplicative**

RSA

Somewhat Homomorphic Encryption (SWHE)
Allows some types of operations a limited number of times

Additive and **Multiplicative**

Fully Homomorphic Encryption (FHE)
Allows an unlimited number of operations for an unlimited number of times

Additive and **Multiplicative**

Unlevelled
Encryption does not add an error to the message

Levelled
Encryption adds a (small) error to the message

We don’t know an unlevelled FHE scheme!

Levelled Homomorphic Encryption

- Performing operations increases the error
- **Addition** of two messages m, m':

$$E(m) + E(m') = (c + e) + (c' + e) = c + c' + 2e$$

- **Multiplication** of two messages m, m':

$$E(m) \cdot E(m') = (c + e) \cdot (c' + e) = cc' + ce + c'e + e^2$$

- The error e
  - It is usually negligible, but more operations (especially multiplications) increase the error significantly
  - After a certain limit is reached, decryption is no longer possible
  - We need methods to push this limit far away (Rescaling, Bootstrapping …)
  - Why is there an error anyway?
    It guarantees security. We will discuss this in the next lectures

Levelled
Encryption adds a (small) error to the message

Homomorphic Cryptosystems

- Domains:
  - Integer → Only Integer arithmetics
  - Boolean → Represents boolean circuits with typical gates (AND, OR, NOT)
  - Real numbers → Floating-point arithmetics

Name	Year	Domain
BGV	2011	Integer
BFV	2012	Integer
FHEW	2014	Boolean
TFHE	2016	Boolean
CKKS	2017	Real number

Homomorphic Encryption – The solution for everything?

- Homomorphic Encryption provides interesting new approaches in the IT security domain
- However, it's not a solution for everything:

Performance
Calculations on the (mostly) larger ciphertexts take much longer, then doing the same operation on the plaintext.

No verifiable computing
There is no way of verifying that the correct computations were executed in the cloud.

Malleability
An attacker could transform a ciphertext into another ciphertext which decrypts to a related plaintext.

Multiple parties
How can multiple parties privately input values for the computation?

Summary – What did we learn today?

A group is a set G, combined with an operation $\circ$. There are four requirements to fulfill.

Mathematical Background

What is a group?

What is the definition of “Homomorphism”?

Given two groups $(G,*)$ and $(H,\circ)$, a group homomorphism is a function $f: G \to H$ such that $\forall x, y \in G: f(x * y) = f(x) \circ f(y)$

Homomorphic property of RSA

RSA is homomorph with respect to multiplication

Overview over homomorphic cryptosystems

PHE vs. SWHE vs FHE

Levelled vs. unlevelled

We need methods like rescaling or bootstrapping to implement FHE schemes.