Cryptography summary

D. Papaioannou, Prof. Ioannis Pitas
Aristotle University of Thessaloniki
pitas@csd.auth.gr
www.aiia.csd.auth.gr
Version 3.4

Artificial Intelligence &
Information Analysis Lab

Cryptography

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Hash Functions
- Secure Hash Algorithms
- Merkle Hash Binary Tree
- Homomorphic Encryption
- Zero Knowledge Proof

Cryptography

- ***Cryptography:*** Concerns the development and use of techniques to prevent third parties from gaining knowledge and access to private messages during a communication process.

Cryptography

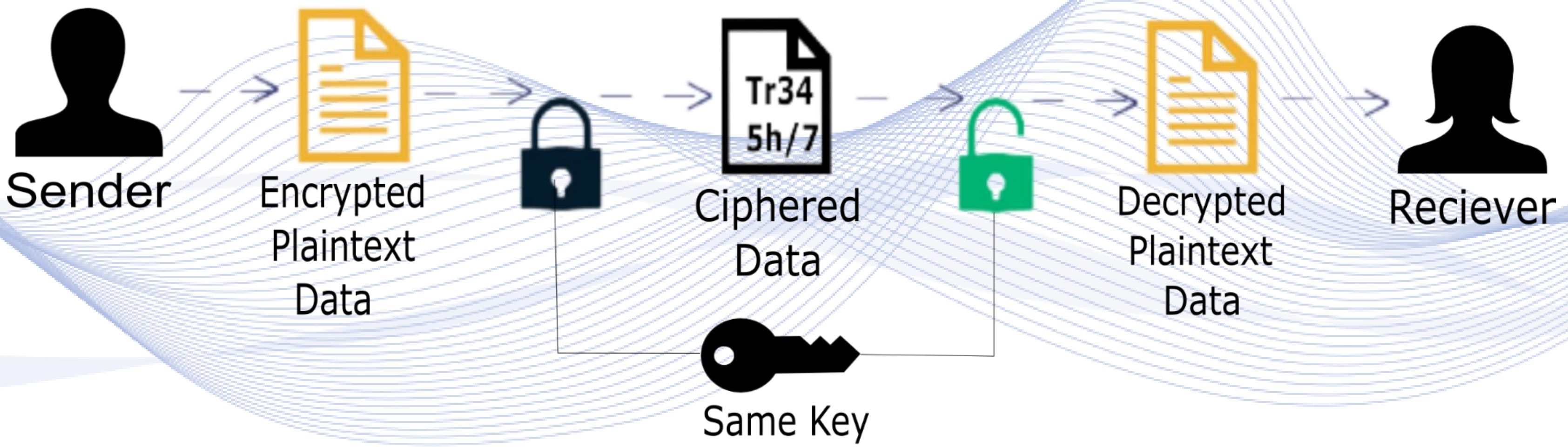
- ***Four pillars of Cryptography:***
  - ***Encryption:*** Method for converting normal texts (plaintext) into a sequence of random bits (ciphertext).
  - ***Decryption:*** Defined as the inverse task of encryption, transformation of ciphertext to plaintext.
  - ***Cipher:*** An algorithm for modifying plaintext to chiphertext or the inverse.
  - ***Key:*** A set of information which is fed as input in the encryption/ decryption operation to produce the desired output, the ciphertext or the plaintext, respectively.

Cryptography

- ***Types of Cryptography:***
  - ***Symmetric Key Cryptography***: Achieving encryption and decryption using a single-key, also known as private key cryptography.
  - ***Asymmetric Cryptography:*** Achieving encrypt and decrypt by using a public key for the first operation and a private key for the second operation, also called public key cryptography.
  - ***Hash Functions:*** Irreversibly "encrypt" information achieved by using mathematical transformations.

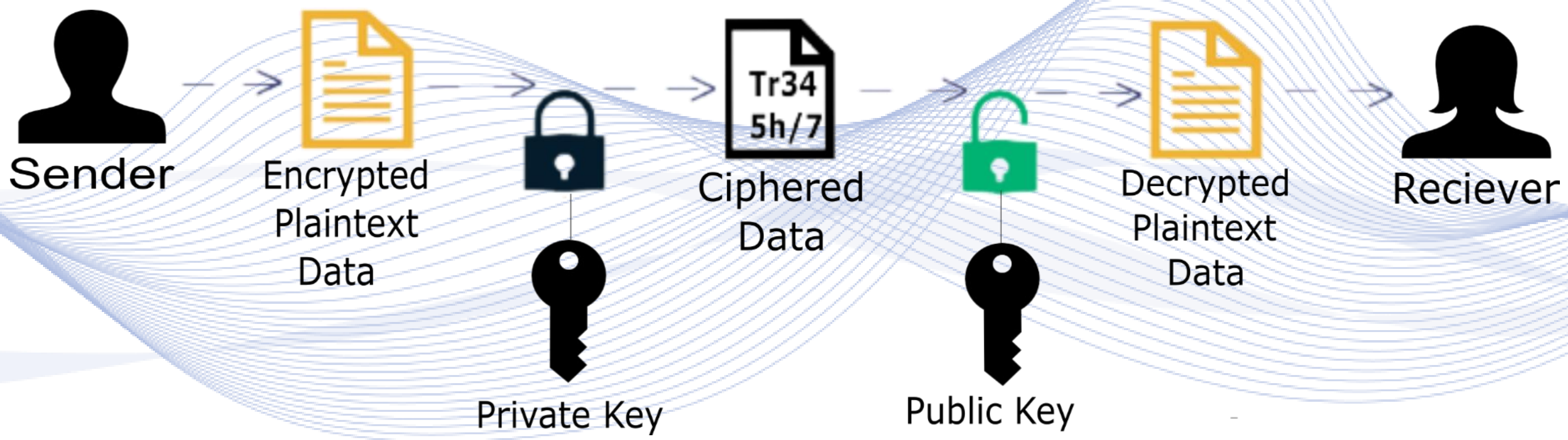
Symmetric Key Cryptography

- ***Encryption*** and ***decryption*** achieved by ***one single key.***
- Both, sender and receiver, have knowledge about the ***shared key***.
- Fast Symmetric encryption achieved.
- Less secure for sensitive data since key size is smaller.



Asymmetric Key Cryptography

- ***Public key*** is shared by ***everyone*** on the cryptographic scheme while ***Private key*** is known only by the ***authenticated user***.
- Private key is a result by a randomly generated number and the public key is the result of the irreversible algorithm.
- Less processing speed and encryption power.



Artificial Intelligence & Information Analysis Lab

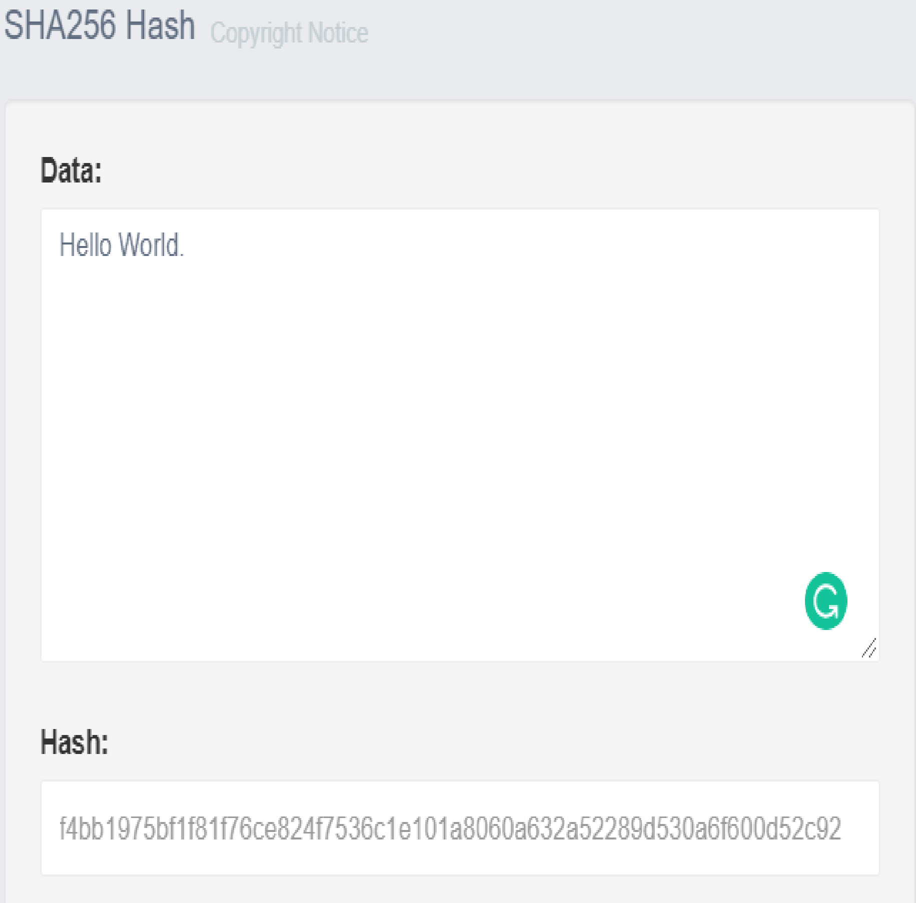
Hash Functions

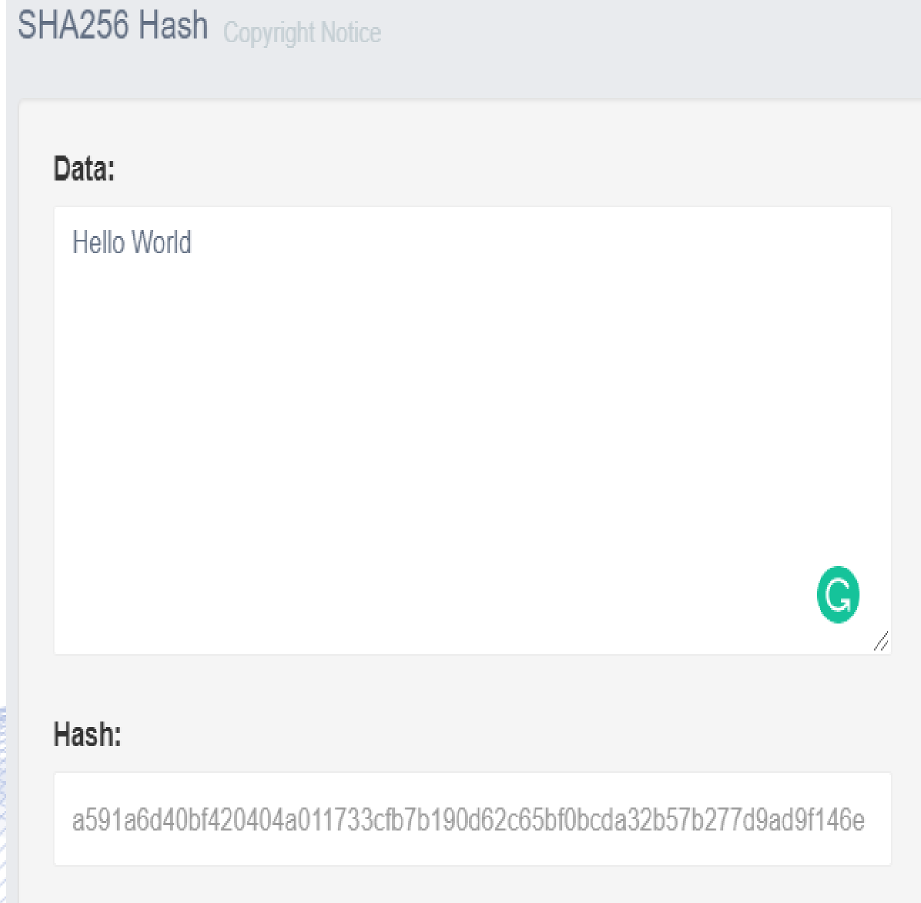
- ***Hash Function:*** Can be defined as a " ***digital fingerprint"*** (unique identifier) for every given piece of data.

- A process that receives as ***input*** a plaintext data $\boldsymbol{X}$ of any size and maps it into a ***unique output*** (chipertext) of a fixed size.

- The ***Secure Hash Algorithm SHA***, developed by NIST and NSA, is one of the most efficient and well-known hash function families.

Avalanche Effect

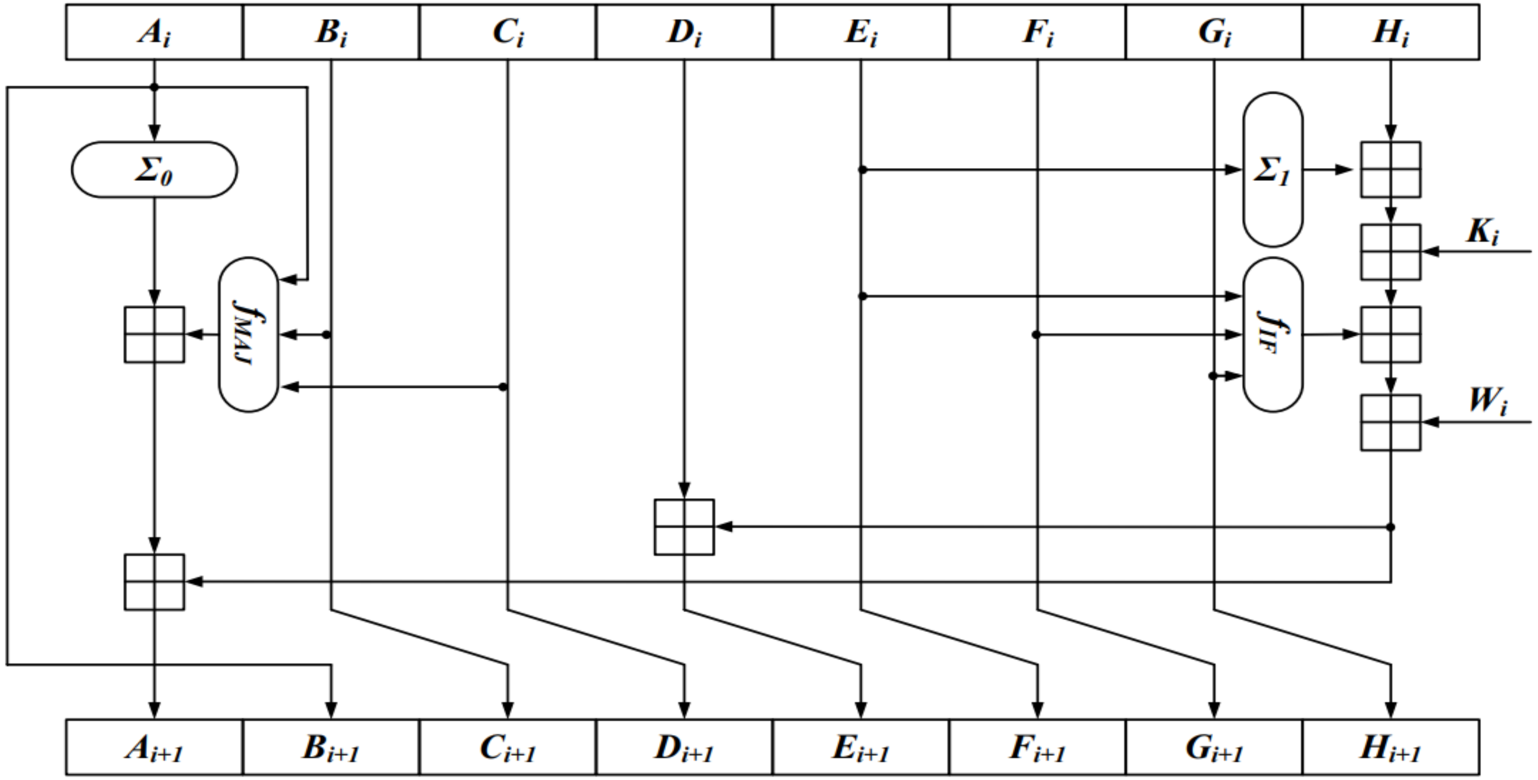




How the change of a single digit can affect radically the produced has value.

Source: https://tools.superdatascience.com/blockchain/hash

Secure Hash Algorithms



An example of one round of SHA-256 algorithm.

Source: [WOU2008]

Merkle Hash Binary Tree

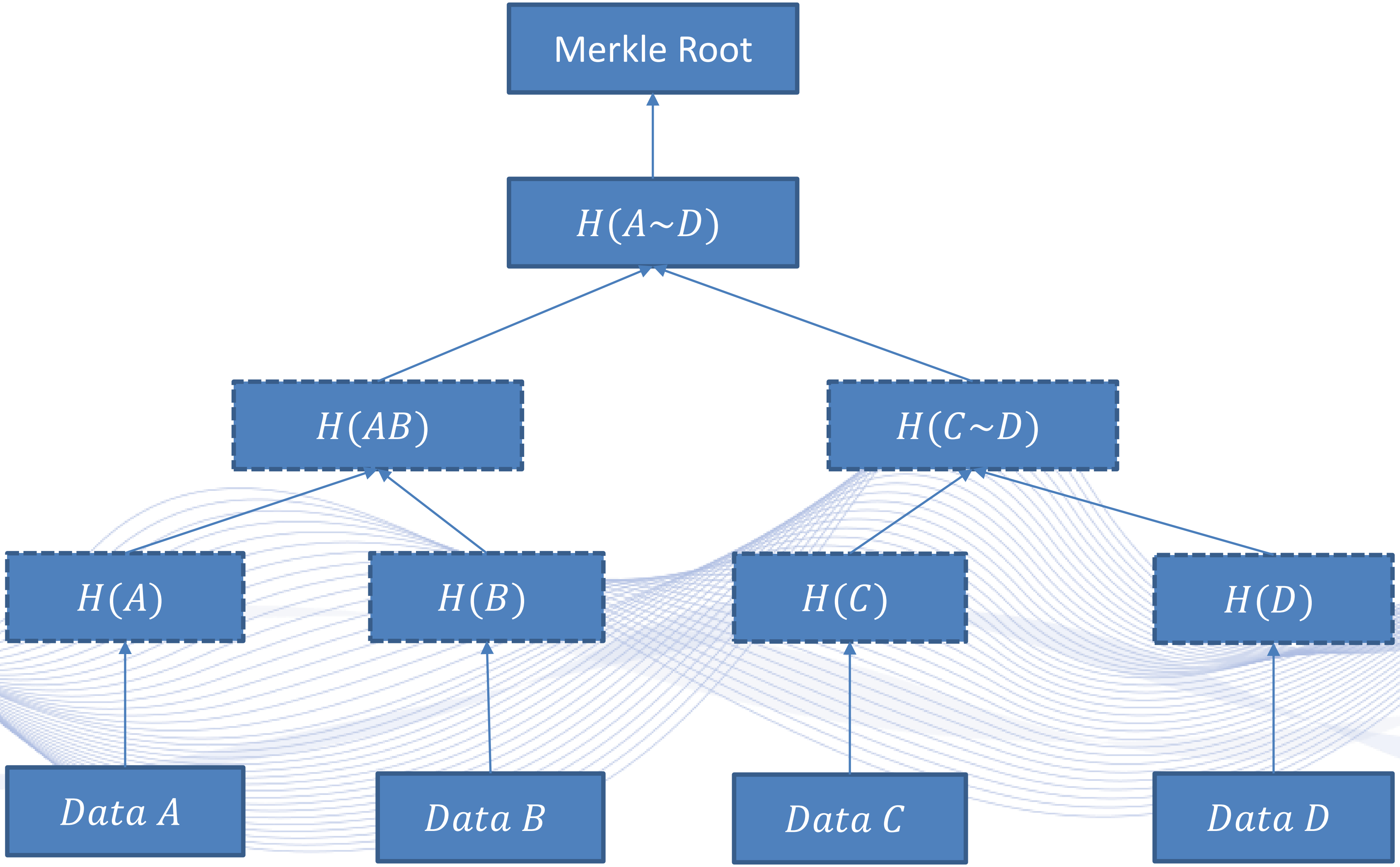
- Large-scale data requires an enchanted process for verification, the ***Merkle Hash Binary Tree***.

- A Merkle tree is a complete binary tree equipped with a hash function and an assignment, Φ, which maps the set of nodes to the set of k-length strings: $\Phi(n) \in \{0,1\}^k$. For two child nodes n_{left} and n_{right}, of any interior node n_{parent}, the assignment Φ is required to satisfy:

$$\Phi(n_{parent}) = hash\left(\Phi(n_{left}) || \Phi(n_{right})\right).$$

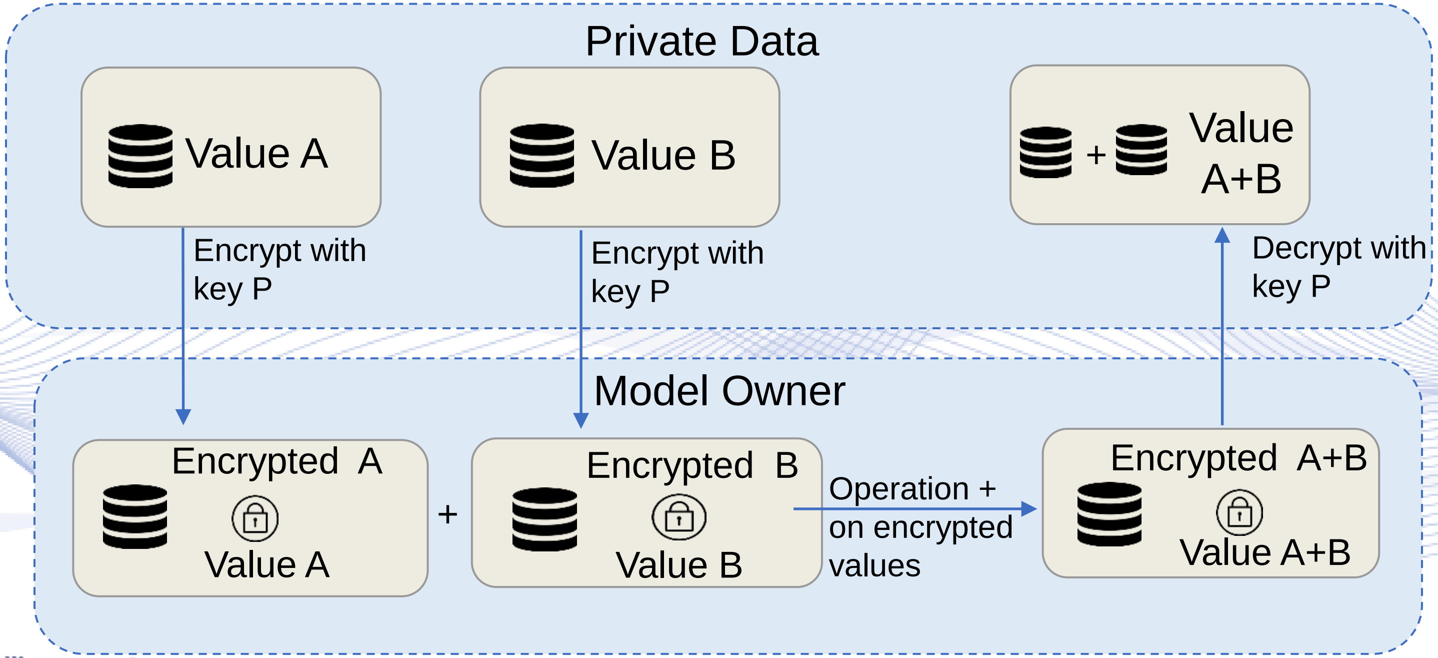
Artificial Intelligence & Information Analysis Lab

Merkle Hash Binary Tree



Homomorphic Encryption

- ***Homomorphic Encryption*** (***HE***) allows computation of encrypted data, creating encrypted results that, when decrypted, match the results of operations, as if they were originally executed.



Homomorphic Encryption

Partial Homomorphic Encryption

- Only one arithmetic operation can be protected, e.g., :

$$E(x+y)=E(x)+E(y).$$

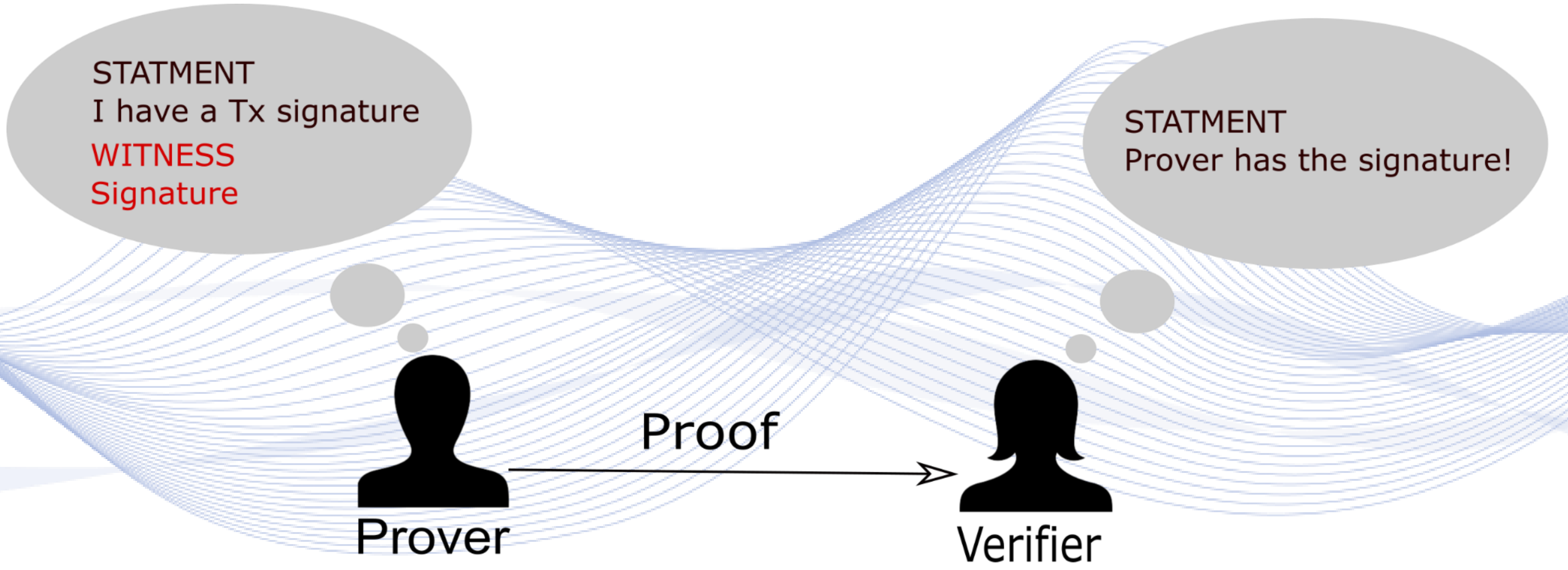
- $E(x)$: encrypted number.
- It can be used in averaging encrypted measurements.

Homomorphic Encryption

- It supports any arithmetic computation on cyphertexts (encrypted numbers).

Zero-knowledge Proof

Zero-Knowledge Proof (ZKP) is defined as a cryptography technique (protocol) where one party (prover) can convince another party (verifier) that he knows a certain statement (witness) without giving or leaking any additional clue except that he knows the statement.



Zero-knowledge Proof

Tokens of ZKP system:

- ***Complete:*** Verifier can be convinced by the prover if and only if the statement is True.
- ***Succinct Proof:*** proof is sort (logarithmic, bit-size).
- ***Fast Verification.***
- ***Efficient Proof Generation:*** Generating the proof in a linear time.

Security:

- If statement is false, then the prover cannot convince the verifier.
- Zero-Knowledge: Verifier does not learn anything about the witness.

Q & A

Thank you very much for your attention!

More material in
http://icarus.csd.auth.gr/cvml-web-lecture-series/

Contact: Prof. I. Pitas
pitas@csd.auth.gr