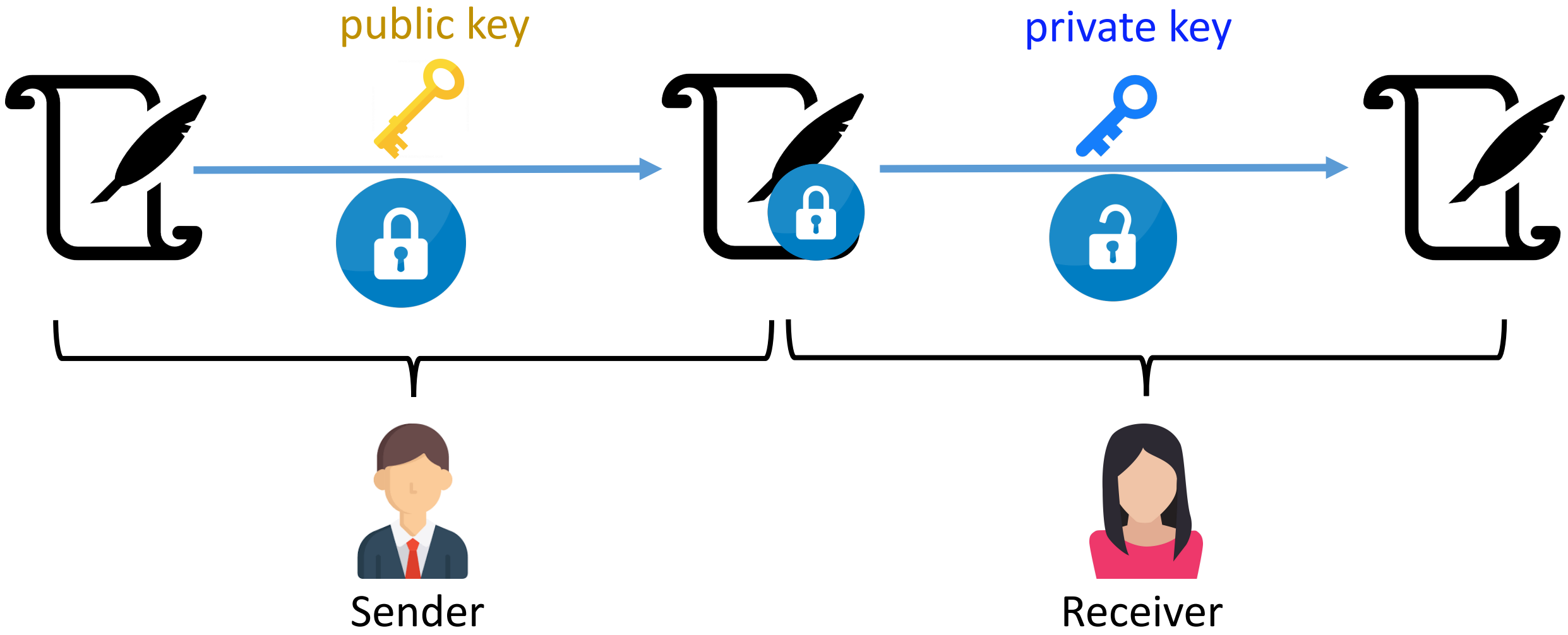
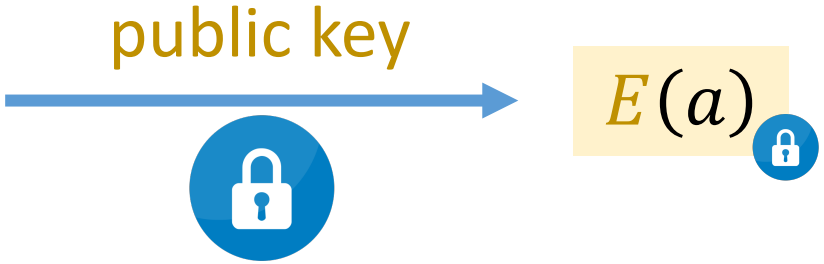
Homomorphic Encryption

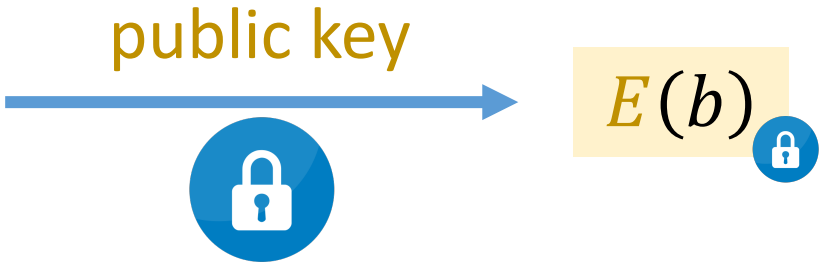
Shusen Wang

Revisit asymmetric encryption

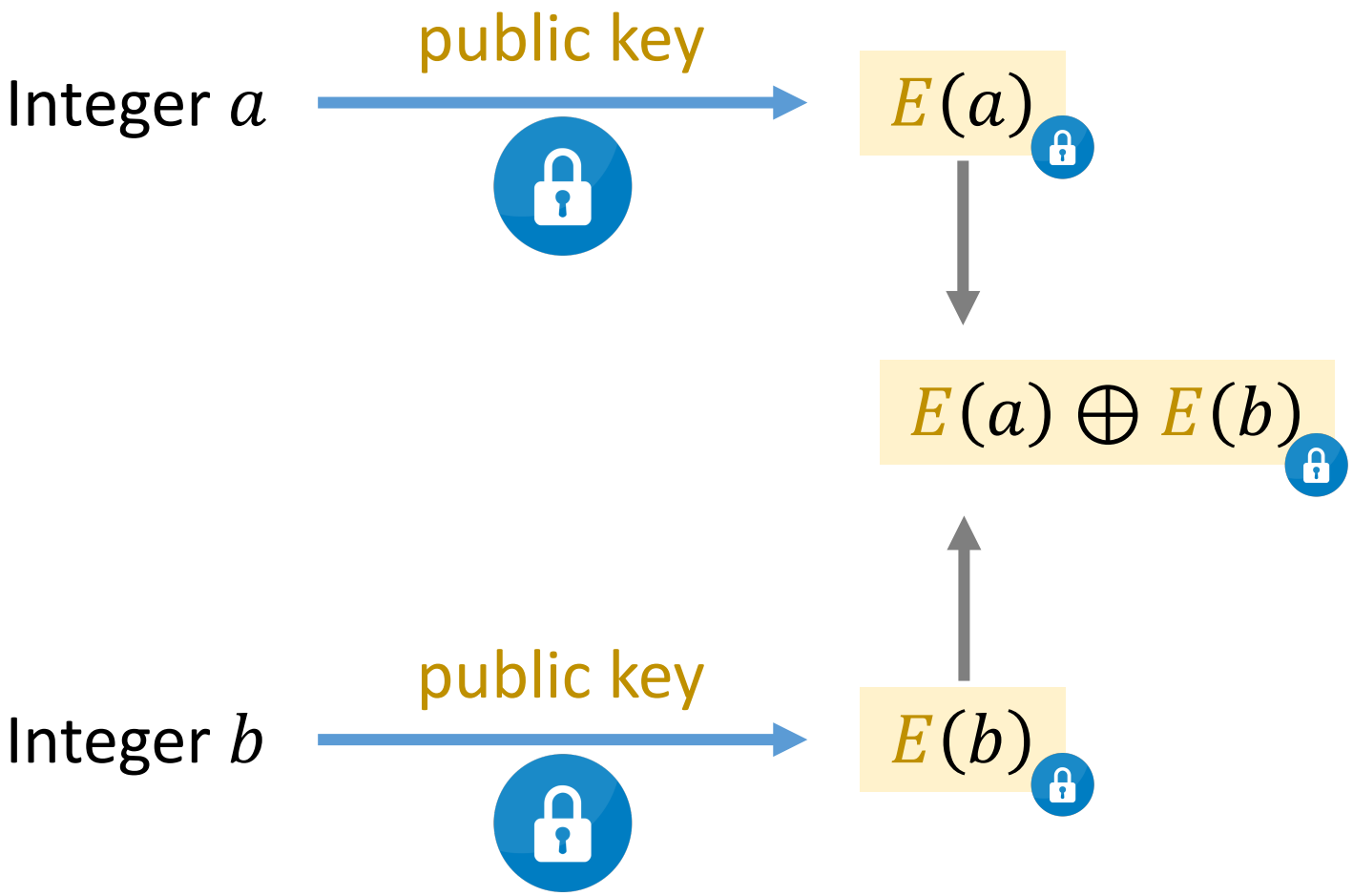


What is homomorphic encryption?

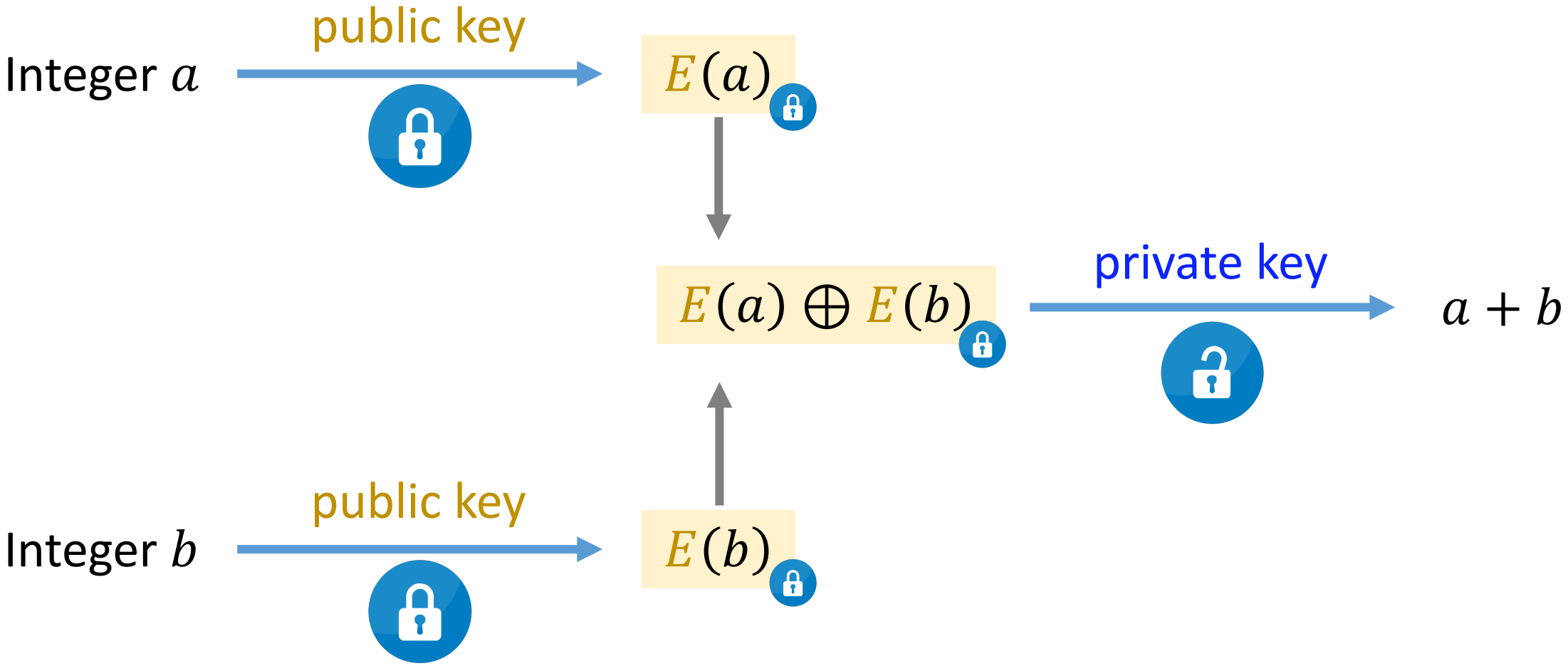
Integer a 

Integer b 

What is homomorphic encryption?



What is homomorphic encryption?



Partial Homomorphic Encryption

- Additive homomorphic cryptosystem (e.g., Paillier cryptosystem [1]):

$$E(a) \oplus E(b) = E(a + b).$$

Reference:

1. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, 1999.

Partial Homomorphic Encryption

- Additive homomorphic cryptosystem (e.g., Paillier cryptosystem [1]):

$$E(a) \oplus E(b) = E(a + b).$$

- Multiplicative homomorphic cryptosystem (e.g., RSA [2]):

$$E(a) \otimes E(b) = E(a \times b).$$

- Decryption: $D\big(E(x)\big) = x.$

Reference:

1. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, 1999.
2. Rivest, Shamir, & Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21 (2): 120–126, 1978.

Full Homomorphic Encryption

- Full homomorphic cryptosystem enjoys the 3 properties:
  1. $E(a) \oplus E(b) = E(a + b)$.
  2. $E(a) \otimes E(b) = E(a \times b)$.
  3. $D\big(E(x)\big) = x$.

Full Homomorphic Encryption

- Full homomorphic cryptosystem enjoys the 3 properties:
  1. $E(a) \oplus E(b) = E(a + b)$.
  2. $E(a) \otimes E(b) = E(a \times b)$.
  3. $D\big(E(x)\big) = x$.
- The first full homomorphic encryption is developed in 2009 [1].
- Read [2] to know more about homomorphic encryption.

Reference:

1. Gentry. Fully Homomorphic Encryption Using Ideal Lattices. In *ACM Symposium on Theory of Computing (STOC)*, 2009.
2. Acar, Aksu, Uluagac, & Conti. A survey on homomorphic encryption schemes: theory and implementation. *ACM Computing Surveys*, 51(4), 1-35, 2018.

Applications

Users' Data

Results

Users' Data

Cloud Server

Applications

Encrypted Data

Encrypted Results

Users' Data

Cloud Server

Thank You!