Homomorphic Encryption based E-Voting System

NT219.L21.ATTN

19522346 - Vương Minh Tiến
19521815 - Trần Đức Lương

REFERENCES

B. Raut, M. Jagtap, S. Ghule, K. Jadhav and P. S. P. Aundhakar, "Homomorphic Encryption Based Online Voting System," *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET),* vol. 6, no. 6, pp. 159-163, 2019.

S. M. Anggriane, S. M. Nasution and F. Azmi, "Advanced e-voting system using Paillier homomorphic encryption algorithm," *International Conference on Informatics and Computing (ICIC),* pp. 338-342, 2016.

S. Saproo, V. Warke, S. Pote and R. Dhumal, "Online Voting System using Homomorphic Encryption," in *International Conference on Automation, Computing and Communication 2020 (ICACC-2020)*, 2020.

Paillier, P. (1999, May). Public-key cryptosystems based on composite degree residuosity classes. In *International conference on the theory and applications of cryptographic techniques* (pp. 223-238). Springer, Berlin, Heidelberg.

Election Context

- Bất tiện khi phải bầu cử trực tiếp.
- Tính riêng tư của phiếu bầu không đảm bảo.
- Người tổng hợp có thể thay đổi kết quả phiếu của mình.

Online Voting

- **Ưu điểm:**

Tiện lợi, dễ dàng tham gia bầu cử.

Mỗi cử tri chỉ được quyền bỏ phiếu 1 lần duy nhất.

Giảm thiểu tối đa các khâu trung gian biết kết quả bầu cử.

Có thể mã hóa trước khi gửi kết quả

- **Nhược điểm:**

Cần phải giải mã trong quá trình tổng hợp phiếu bầu.

RESEARCH MOTIVATION

Giải quyết đồng thời 3 vấn đề:

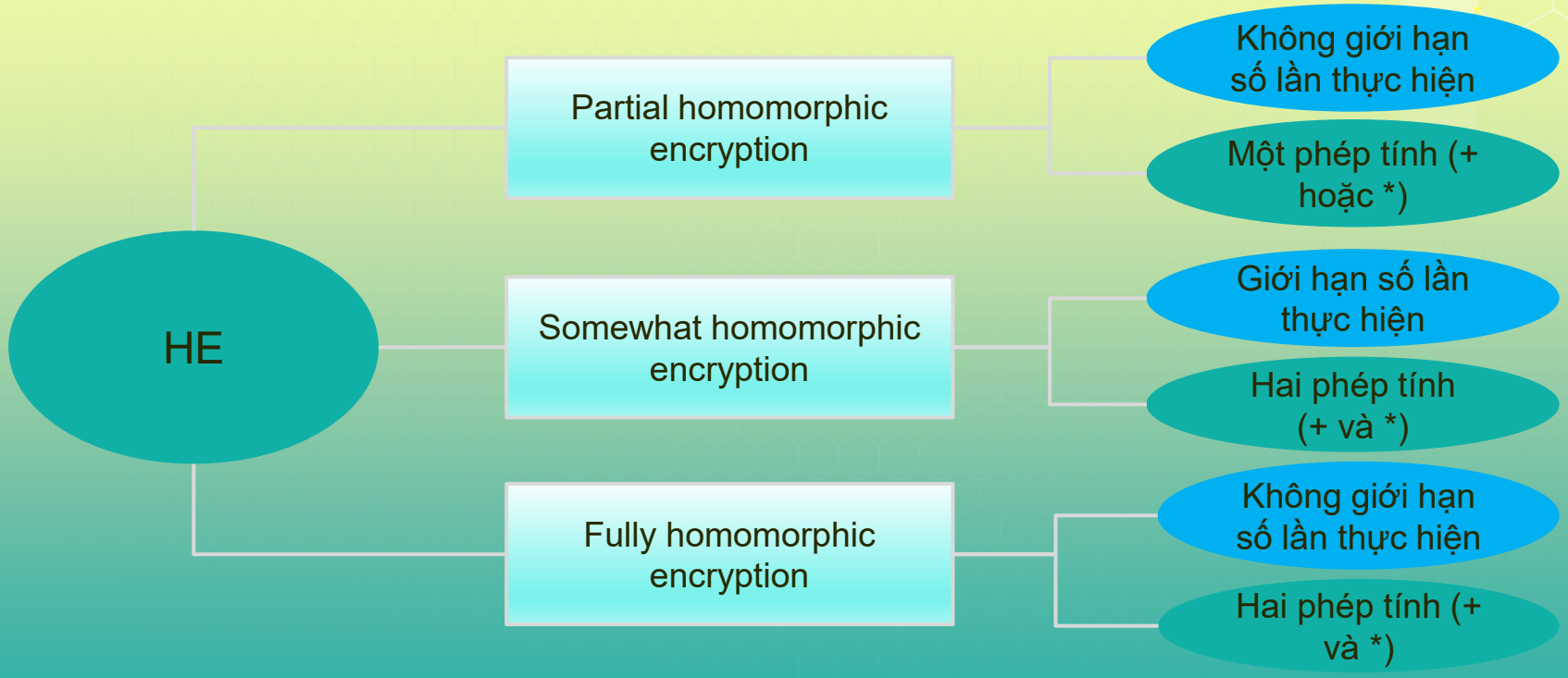
- Chỉ mỗi cử tri biết được mình bầu cho ai (mã hóa)
- Tính toán chỉ dựa trên bản mã
- Kết quả cuối cùng chỉ được giải mã khi quá trình bỏ phiếu hoàn tất.

SỬ DỤNG HOMOMORPHIC ENCRYPTION

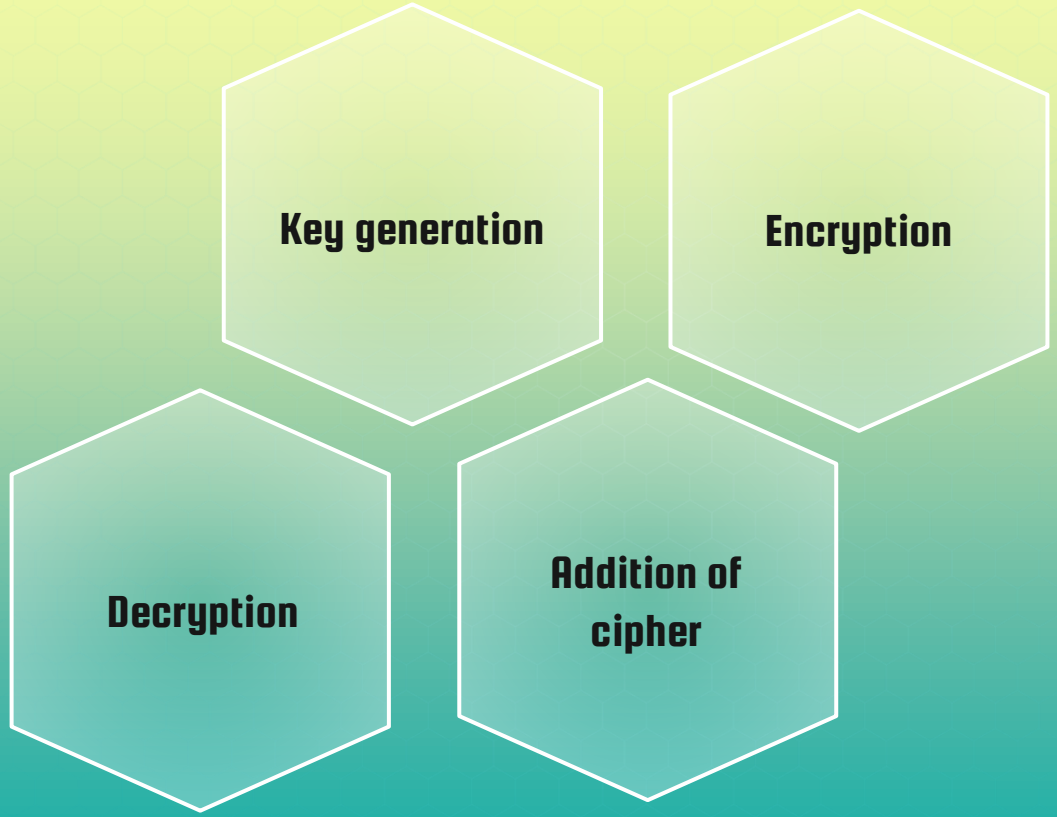
PROPOSED SCHEME

1. *HOMOMORPHIC ENCRYPTION*
2. *PAILLIER CRYPTOSYSTEM*
3. *VOTING PROCEDURE*

Homomorphic Encryption



PAILLIER CRYPTOSYSTEM



Paillier Cryptosystem

Key Generation

* Large prime number **p, q** (randomly & independent)
*GCD(p*q, (p-1)*(q-1)) = 1*
* Compute **n** = p*q
* Random **g** between 1 and n^2
* Compute **λ** as LCM(p-1, q-1)
*Compute **μ** = ($L(g^{\lambda} \bmod n^2)$)$^{-1}$
With L(x) = $\frac{x-1}{n}$

Public Key (n, g)

Private Key (λ, μ)

Paillier Cryptosystem

Encryption

With m is plaintext ($0 < m < n$)

Select random r where $0 < r < n$ and $GCD(r, n) = 1$

Encrypt: $c = g^m * r^n \bmod n^2$

Decryption

With c is ciphertext

Decrypt: $m = L(c^\lambda \bmod n^2) * \mu \bmod n$

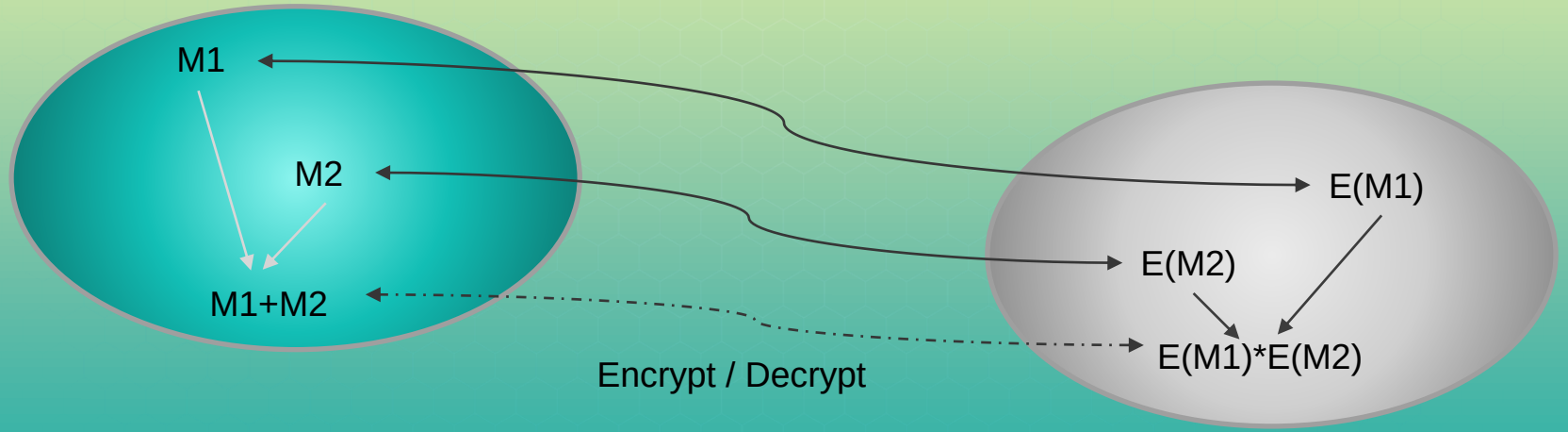
With $L(x) = \frac{x-1}{n}$

The role of the random *r* ensures that two equivalent value will encrypt to different ciphertexts.

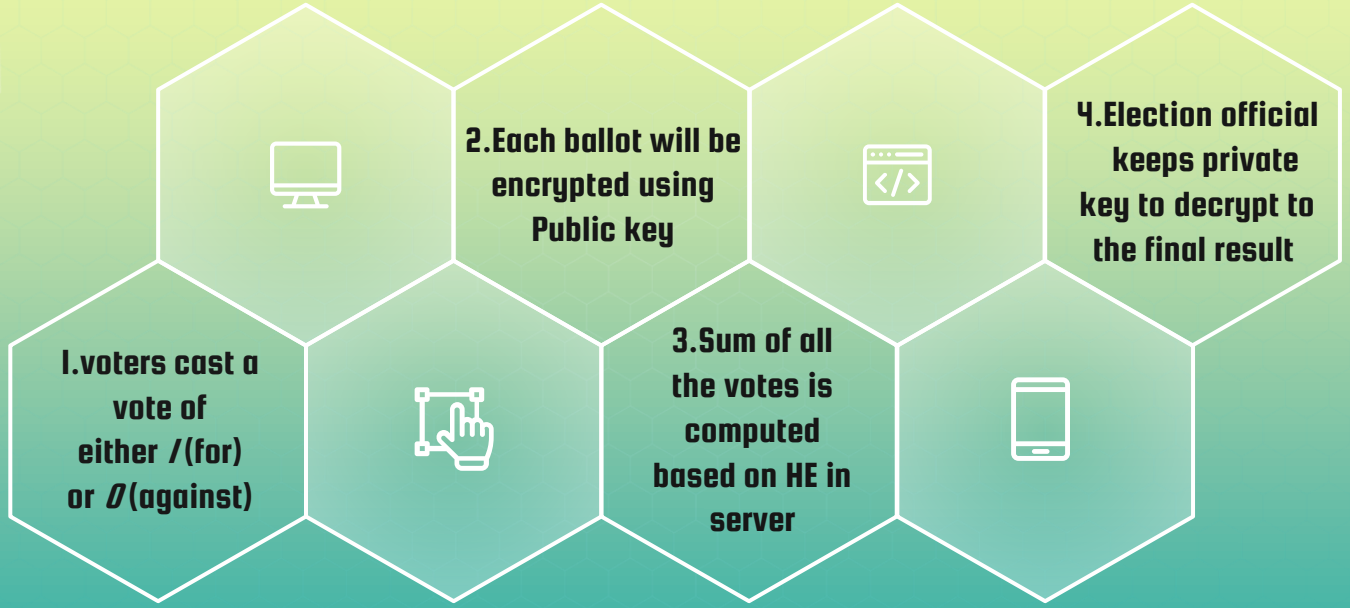
Paillier Cryptosystem

$$D(E(m1, r1) * E(m2, r2) \bmod n^2) = (m1 + m2) \bmod n$$

$$D(c1*c2 \bmod n^2) = (m1 + m2) \bmod n$$



Voting Procedure



CONTRIBUTIONS

- Dữ liệu của cử tri hoàn toàn được bảo mật, riêng tư thay vì bị toàn quyền kiểm soát bởi cơ quan bầu cử ở phương pháp truyền thống.
- Khả năng tính toán kết quả phiếu bầu trên bản mã của thuật toán Paillier mang lại tính công bằng trong cuộc bầu cử kín.
- Hiệu suất và tính ứng dụng cao hơn so với truyền thống.

COMMENT

Ứng dụng Homomorphic Encryption (HE) trong bầu cử trực tuyến giúp tính trung thực, công bằng và bảo mật của cuộc bầu cử được đảm bảo khi trải qua các khâu trung gian.

Tuy nhiên bầu cử trực tuyến cũng gặp phải một số khuyết điểm mà HE không thể xử lý được, chẳng hạn như vấn đề một cử tri tham gia bỏ phiếu nhiều lần (double-voting problem).

⇨ Nhóm đề xuất hướng khắc phục: Sử dụng ID Token trong công nghệ Blockchain

DEMO

ASSUMPTIONS

Key sharing is secured and trusted

First

Every voters signed in voting system before voting

Second

A citizen has only one turn to vote

Third

THANKS