Distributed Multi-authority Attribute-based Encryption Using Cellular Automata

Ankit Pradhan, Kamalakanta Sethi, Shrohan Mohapatra, and Padmalochan Bera

Indian Institute of Technology (IIT) Bhubaneswar

October 26, 2019

Introduction

Cellular Automata (CA):

- Data parallelism
- Information scrambling
- No complex number theoretic operations

Introduction

Cellular Automata (CA):

- Data parallelism
- Information scrambling
- No complex number theoretic operations

Attribute-based Encryption (ABE):

- Fine-grained access control
- Scalability in large cloud applications
- Costly operations (like bilinear pairings, etc)

Introduction

Cellular Automata (CA):

- Data parallelism
- Information scrambling
- No complex number theoretic operations

Attribute-based Encryption (ABE):

- Fine-grained access control
- Scalability in large cloud applications
- Costly operations (like bilinear pairings, etc)

We employ Cellular Automata for achieving the diverse functionality provided by Attribute-based Encryption schemes:

- Encryption and attribute distribution $\rightarrow$ Reversible CA
- Policy satisfiability $\rightarrow$ Turing-complete CA

Basic CA motivation: Rule 110 CA

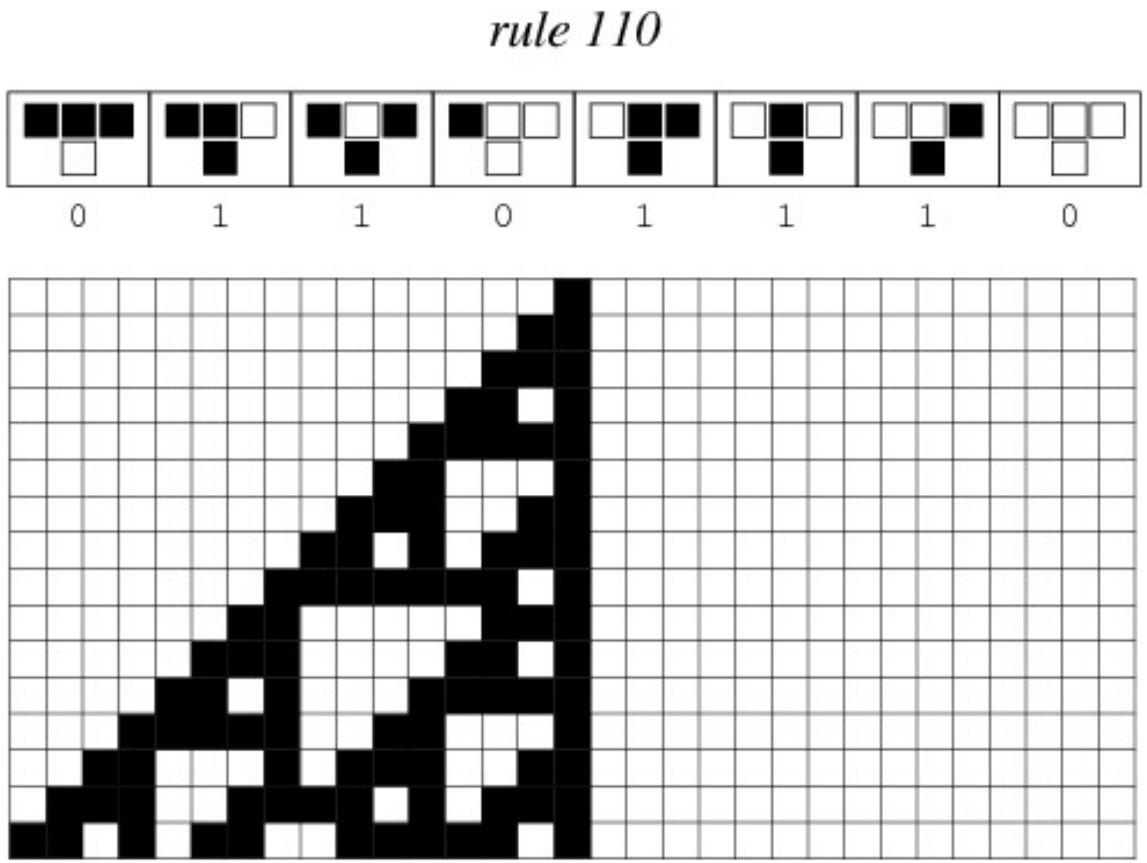


Figure 1: A demonstration of the rule 110 cellular automaton [1]. The first row shows the transition rules. It is noteworthy of the binary number formed of the outputs, whose decimal equivalent is rule 110. The subsequent grid shows the temporal evolution, where the initial seed consists of a single one and rest all zeroes.

Basic CA motivation: Conway's Game of Life

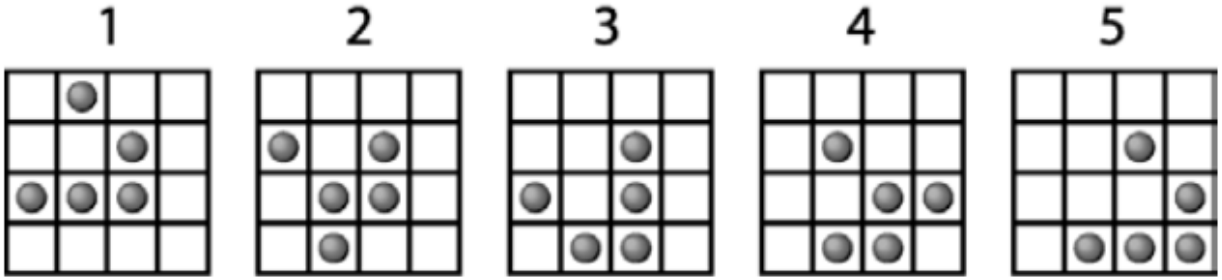


Figure 2: A demonstration of the Game Of Life cellular automaton [2]. The first grid shows the seed, and the subsequent grids show the temporal evolution of the same. This is known as a 'glider'.

Basic CA motivation: Conway's Game of Life

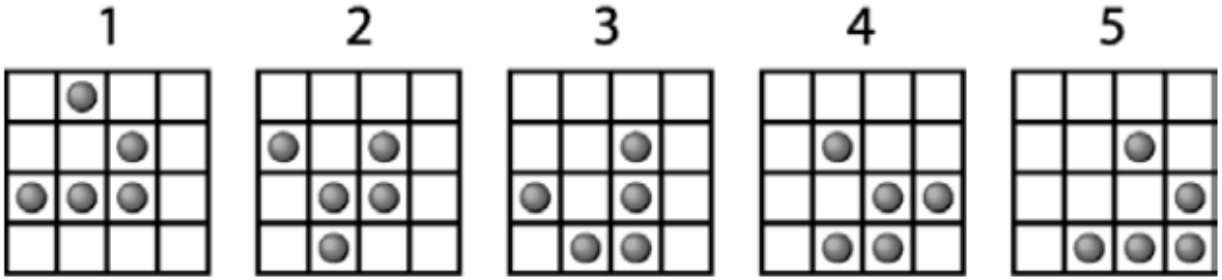


Figure 2: A demonstration of the Game Of Life cellular automaton [2]. The first grid shows the seed, and the subsequent grids show the temporal evolution of the same. This is known as a 'glider'.

Transition function of "Conway's Game of Life":

- Any live cell (state '1') with fewer than two live neighbours dies (state '0'), as if by under-population.
- Any live cell with two or three live neighbours lives on to the next generation.
- Any live cell with more than three live neighbours dies, as if by overpopulation.
- Any dead cell with exactly three live neighbours becomes a live cell, as if by reproduction.

Basic ABE motivation: Access Control

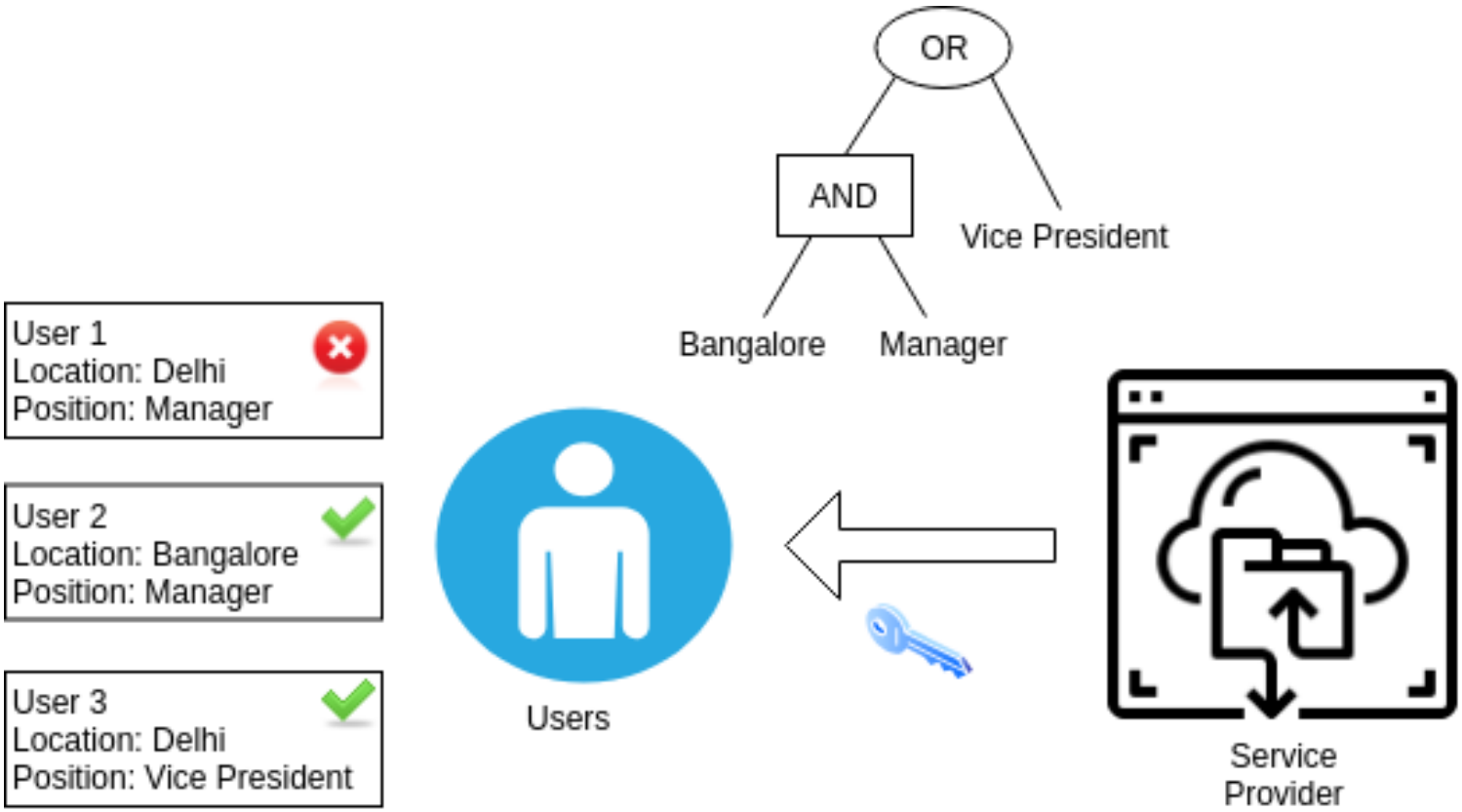


Figure 3: An example scenario demonstrating the principles behind Attribute-Based Encryption (ABE). Users possessing attributes which satisfy the access policy can decrypt the ciphertext.

Basic ABE motivation: KP-ABE vs CP-ABE

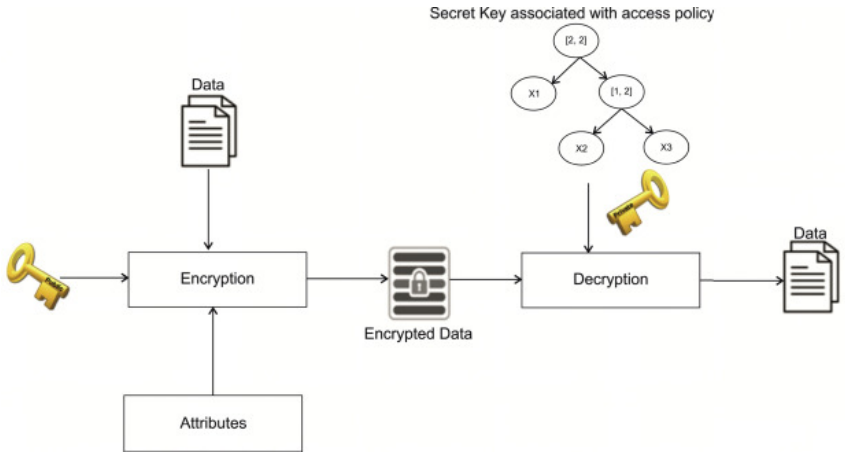


Figure 4: Key-policy Attribute-based Encryption (KP-ABE) [3]

Basic ABE motivation: KP-ABE vs CP-ABE

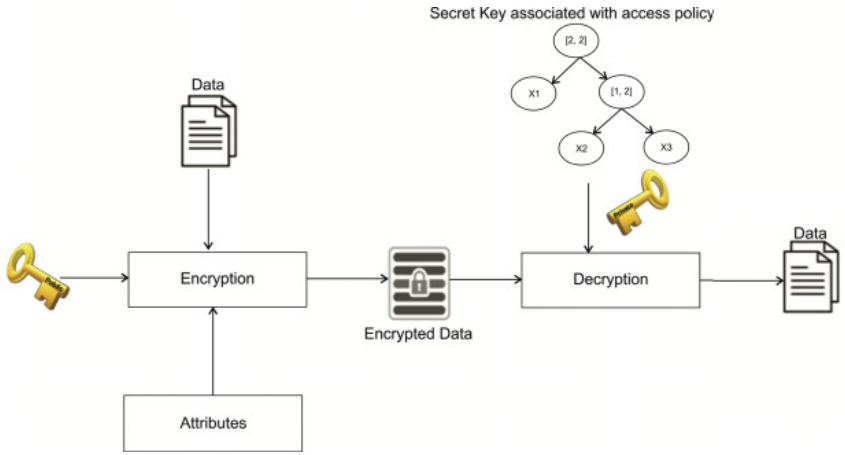


Figure 4: Key-policy Attribute-based Encryption (KP-ABE) [3]

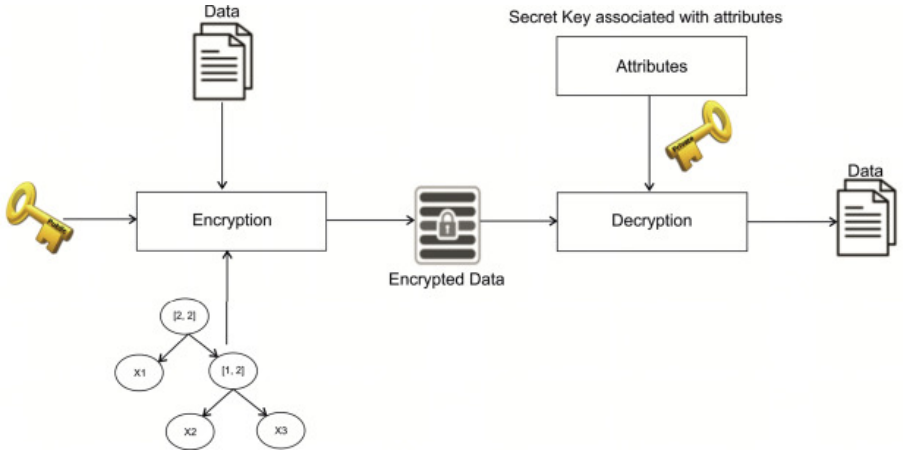


Figure 5: Ciphertext-policy Attribute-based Encryption (CP-ABE) [4]

Proposed Cryptosystem

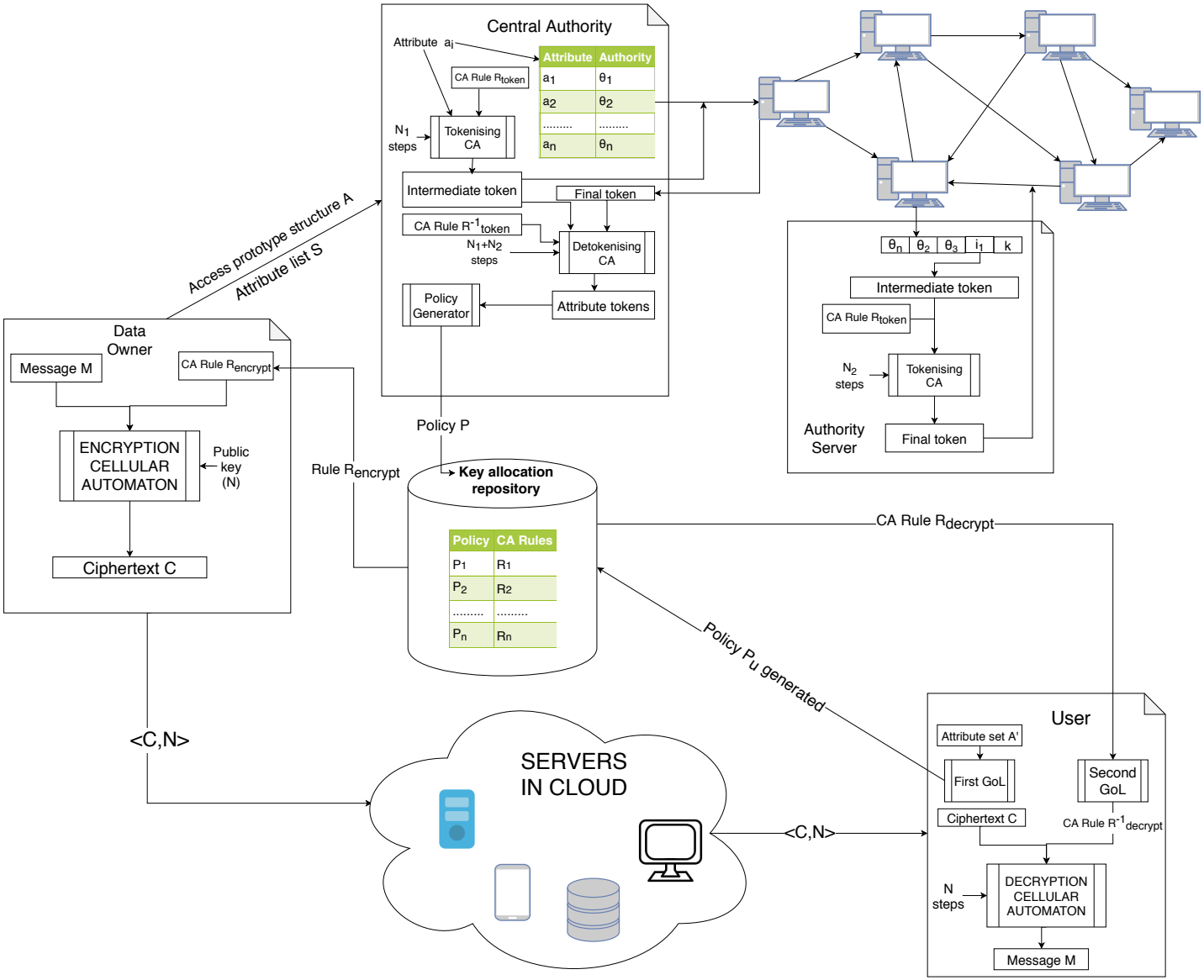


Figure 6: Architectural design of the proposed cryptosystem.

Security properties

Consider a CA with k states, r neighbours and grid size d. Also consider the cardinality of the attribute set A and n users of the system. We present some of the minimal brute force complexities making our cryptosystem robust.

Security properties

Consider a CA with k states, r neighbours and grid size d. Also consider the cardinality of the attribute set A and n users of the system. We present some of the minimal brute force complexities making our cryptosystem robust.

- Resistance to brute force attacks to discover the underlying CA rule being used: $\Omega\left((k^d)^{k^d} + k^{k^r}\right)$.

Security properties

Consider a CA with k states, r neighbours and grid size d. Also consider the cardinality of the attribute set A and n users of the system. We present some of the minimal brute force complexities making our cryptosystem robust.

- Resistance to brute force attacks to discover the underlying CA rule being used: $\Omega\left((k^d)^{k^d} + k^{k^r}\right)$.
- Resistance to brute force attack on the Game of Life CA: $\Omega(exp(n * 2^{2^A}))$.

Security properties

Consider a CA with k states, r neighbours and grid size d. Also consider the cardinality of the attribute set A and n users of the system. We present some of the minimal brute force complexities making our cryptosystem robust.

- Resistance to brute force attacks to discover the underlying CA rule being used: $\Omega\left((k^d)^{k^d} + k^{k^r}\right)$.
- Resistance to brute force attack on the Game of Life CA: $\Omega(exp(n * 2^{2^A}))$.
- Resistance to linear attacks: $\Omega\left(\binom{k^d}{d} d^3\right)$.

Security properties

Consider a CA with k states, r neighbours and grid size d. Also consider the cardinality of the attribute set A and n users of the system. We present some of the minimal brute force complexities making our cryptosystem robust.

- Resistance to brute force attacks to discover the underlying CA rule being used: $\Omega\left((k^d)^{k^d} + k^{k^r}\right)$.
- Resistance to brute force attack on the Game of Life CA: $\Omega(exp(n * 2^{2^A}))$.
- Resistance to linear attacks: $\Omega\left(\binom{k^d}{d} d^3\right)$.
- Resistance to attacks on attribute authorities: $\Omega(exp((k^d)!))$.

Security properties

Consider a CA with k states, r neighbours and grid size d. Also consider the cardinality of the attribute set A and n users of the system. We present some of the minimal brute force complexities making our cryptosystem robust.

- Resistance to brute force attacks to discover the underlying CA rule being used: $\Omega\left((k^d)^{k^d} + k^{k^r}\right)$.
- Resistance to brute force attack on the Game of Life CA: $\Omega(exp(n * 2^{2^A}))$.
- Resistance to linear attacks: $\Omega\left(\binom{k^d}{d} d^3\right)$.
- Resistance to attacks on attribute authorities: $\Omega(exp((k^d)!))$.
- Resistance to attacks by malicious attribute authorities: Timer-based solution at Central Authority.

Complexity of encryption and decryption

Testing environment is set up in Python and Wolfram languages. For comparisons with existing Attribute-based Encryption schemes, we use the efficient, statically-secure, large-universe, multi-authority Rouselakis-Waters scheme (RW-scheme) [5].

Complexity of encryption and decryption

Testing environment is set up in Python and Wolfram languages. For comparisons with existing Attribute-based Encryption schemes, we use the efficient, statically-secure, large-universe, multi-authority Rouselakis-Waters scheme (RW-scheme) [5].

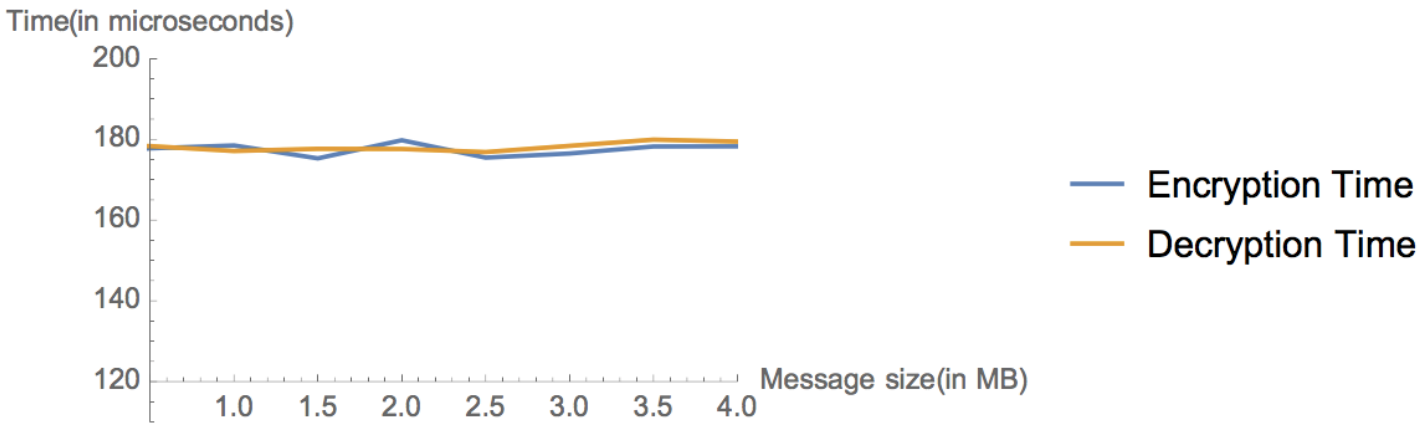
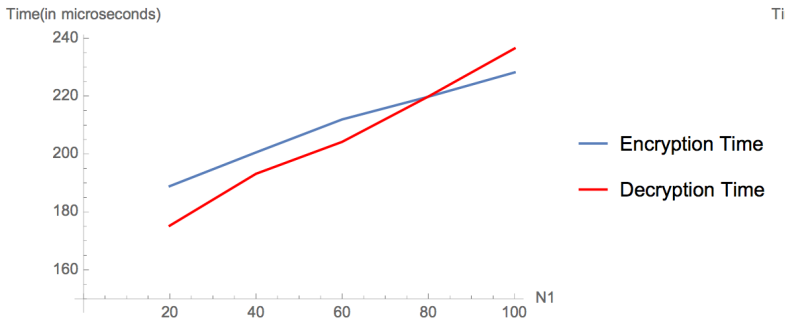
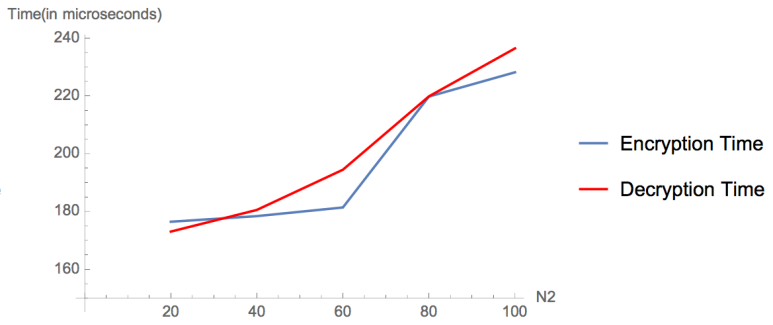


Figure 7: The plot of encryption and decryption time (in μs) against the message length l (in MB).

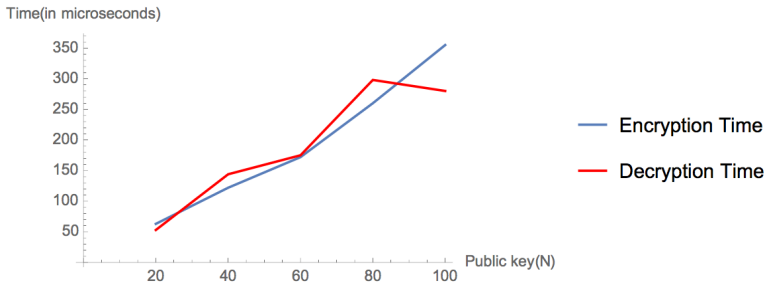
Complexity of encryption and decryption



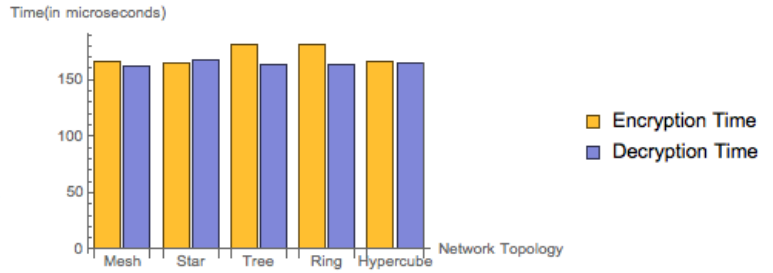
(a) vs number of steps N_1 in intermediate token generation



(b) vs number of steps N_2 in final token generation



(c) vs public key parameter N



(d) Variation across different topology of attribute authorities

Figure 8: Encryption and Decryption time (in μs) vs various parameters

Comparison with existing ABE schemes

Figure 9: Encryption time vs message length (in MB) for the proposed cryptosystem and the RW-scheme [5]. The blue curve shows the measure of time in μs whereas the red curve shows the same in ms

Comparison with existing ABE schemes

Figure 9: Encryption time vs message length (in MB) for the proposed cryptosystem and the RW-scheme [5]. The blue curve shows the measure of time in μs whereas the red curve shows the same in ms

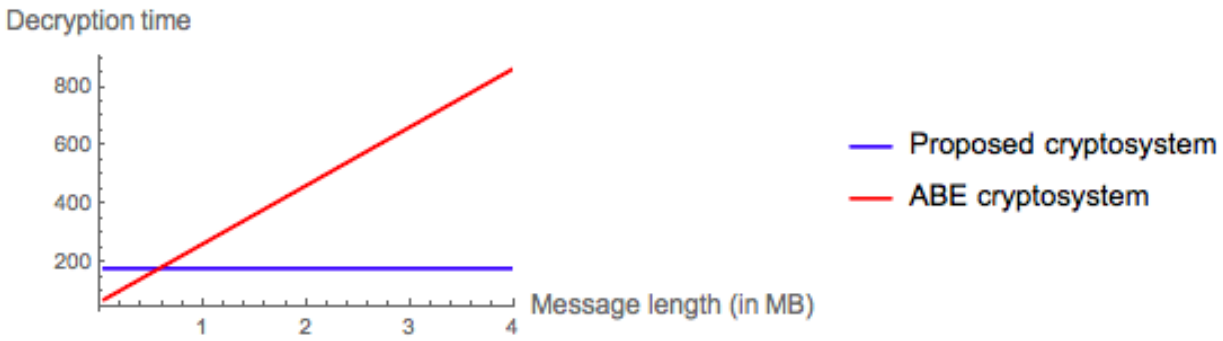


Figure 10: Decryption time vs message length (in MB) for the proposed cryptosystem and the RW-scheme [5]. The blue curve shows the measure of time in μs whereas the red curve shows the same in ms

Bibliography


T. Neary, D. Woods, *P-completeness of Cellular Automaton Rule 110*, in *International Colloquium on Automata, Languages, and Programming (ICALP)*, pp. 132-143, 2006.


J.P. Renard, *Implementation of logical functions in the Game of Life*, in *A. Adamatzky (Ed.), Collision-Based Computing*, pp. 491-512, 2002.


V. Goyal, O. Pandey, A. Sahai, B. Waters, *Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data*, in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 89-98, 2006.


J. Bethencourt, A. Sahai, B. Waters, *Ciphertext-Policy Attribute-Based Encryption*, in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pp. 321-334, 2007.


Y. Rouselakis, B. Waters, *Efficient Statically-Secure Large-Universe Multi-Authority Attribute-Based Encryption*, in Financial Crypto 2015.

Thank You!