Journal of Information Systems Engineering and Management
2025, 10 (31s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Quantum Key Generation Integration with AES Encryption for Quantum Attack Resilience

*B S Spoorthi, S Pushpa Mala

[1]Research Scholar, DayanandaSagar University, Bangalore and Assistant Professor, Malnad College of Engineering, Hassan, India

[1]spoorthi.bs.136@gmail.com

[2]Dayananda Sagar University, Bangalore, India

[2]pushpasiddaraju@gmail.com

ARTICLE INFO

Received: 20 Dec 2024

Revised: 15 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

Quantum cryptography, with the chance of advancement offered by its basis on the single principle of quantum mechanics, constitutes a notable point of strength in the advancement of new cryptography research. Utilizing the distinctive properties of quantum mechanism, such as qubits, quantum cryptography offers enhanced protection against quantum computer attacks. This paper proposes a novel quantum cryptographic algorithm that integrates quantum key generation with the Advanced Encryption Standard (AES) technique to safeguard data from quantum threats. By combining quantum bit generation with AES encryption, the confidentiality of information exchanged between parties is preserved. The quantum bit generation technique exploits the inherent properties of quantum mechanics, particularly quantum superposition, to generate secure cryptographic keys. Leveraging the efficiency and robustness of the AES encoding standard, this approach offers heightened security against quantum attacks. Experimental analysis using MATLAB software validates the effectiveness of the proposed method.

Keywords: Quantum cryptography, quantum key generation, AES encryption, AES decryption, secret message

INTRODUCTION

Quantum cryptography is an innovative field that guarantees the principles of quantum mechanics for easy communication between parties. The term “quantum computer” refers to all types of quantum hardware based on their various functions, in many different ways. With the proliferation of qubits in quantum computers, there emerges a plethora of statistical matrices, leading to enhanced static stability and computational capabilities. Although quantum computing is still in its embryonic phase, its potential for a rapid revolution in classical infrastructure is heavily under consideration. According to a recent report[2], global investment in quantitative information media is predictable to reach $25 billion by 2021. A decade-long advertising campaign can do nothing but a decade-long campaign means the result is useless. Conversely, projections suggest that 40% of the surge in 2025 will stem from China's expanded adoption of quantum computing. Technology giants like IBM, Google, and Intel have already claimed numerous successes in the area of quantum computing.

The integration of quantum mechanics has taken a revolutionary turn in the ground of communication and the pursuit of quantum cryptography. While traditional cryptography methods largely claim their intelligent algorithms, quantum cryptography does rely on the essential principles

of quantum mechanics to guarantee the maximum probability possible. The notion of this question arises from the indifferent use of quantum properties in cryptographic solutions, a process identified as quantum key distribution (QKD). The generation of quantum states undergoes a transformative shift with the introduction of quantum mechanics principles, particularly the concept of superposition of states. The quantum wave generation process entails the transfer of the quantum bit of the qubit across a quantum channel, through which the photon can be used as a carrier of information. Although the generation of quantum bits guarantees a small amount of computational confusion, it is all necessarily worthy of practical interpretation. It includes a conventional encryption standard such as the Advanced Encryption Standard (AES), a generally used symmetric translation algorithm, noted for its reliability and efficiency. Through the amalgamation of quantum behavior generation and AES encryption within a unified framework, it becomes possible to harness the intrinsic characteristics of the quantum realm to enhance the reliability of classical translation methods. This approach provides not only the security of traditional cryptography methods but also the ability to advance quantum technology and risk a new prospect for easy communication in the digital age.

LITERATURE REVIEW

Quantum technology is rapidly developing in academia and industry. Continued progress in quantum computing is driven by different approaches. Over the past decade, we have seen dramatic changes in quantum cryptography research, from proof-of-principle experiments to building practical quantum key distribution (QKD) systems over proven fiber optic networks. Information and security are integrally linked to each other, because without security, various types of attacks like hacking, malware attacks, etc. are inevitable. Make it easier for hackers to gain unauthorized access to information [1]. In this case, cryptography, the science of creating and breaking codes, plays an important role in information security. A strong encryption algorithm can secure all information, while cryptanalysis can cause insecurity. Therefore, developing an algorithm that is effective against an adversary with unlimited resources may be the holy grail of cryptography. However, breakthroughs in cryptography came when Gilbert Sandford-Vernam first invented the One Time Pad (OTP) cipher in 1917 [2]. Claude Shannon proved that One-Time Pad (OTP) is secure because the random key is used only once [3]. Even though the OTP is unbreakable in theory, it may be unsafe in practice due to two phenomena that are not possible in classical physics. An event is really the generation of random numbers; The second is secure key distribution through insecure channels [4]. Symmetric key algorithms such as DES and AES must generate a shared key between the sender and receiver. Symmetric key algorithms use shorter keys to encrypt longer messages and therefore reduce the use of random keys. Therefore, these symmetric algorithms are not preserved as One-Time Pad (OTP). When the secret key is sent over an insecure channel, it is likely being copied or stolen by an intruder. This is a major problem in key distribution in case of symmetric key algorithm [4]. To solve the key distribution problem, asymmetric key algorithms, or public key algorithms, were invented. In the famous asymmetric key algorithm, the RSA scheme (named after its inventors, Ron Rivest, etc. Shamir and Leonard Edelman), the recipient, Bob, generates two keys: one is the public key, and the other is the private key. The public key is broadcast by Bob. The sender, Alice, encrypts her message with Bob's public key and sends it over an insecure channel. At the receiving end, Bob can decrypt the message using the corresponding private key [5]. Therefore, public key cryptography can solve the key distribution problem. To provide high security for financial transactions, military communications, emails, medical data, websites, etc., public key encryption systems such as RSA [5], Elliptic Curve Cryptography (ECC) [6], and Diffie-Hellman (DH)); are used. [7] Public key cryptography is based on several mathematical assumptions. For example, RSA security depends on the difficulty of parsing a large composite integer. If there is an algorithm that can efficiently parse an arbitrarily large integer, the security of the RSA algorithm will be compromised. Therefore, the possibility of the invention of fast factoring algorithms cannot be ignored, and if it does, the security of most public key encryption algorithms cannot be ignored. There is already a factoring algorithm known as the noise algorithm that can be applied to quantum computers. Shor's algorithm [9] requires polynomial time to solve integer multiplication problems (IFP) and discrete logarithm problems (DLP), thus advancing

quantum cryptanalysis. This suggests that in a few decades, when quantum computers become widely available, all public key encryption algorithms will collapse [10].

PROPOSED WORK

Traditional cryptographic methods, relying on sophisticated algorithms, may eventually succumb to advanced computing systems' decoding capabilities. In contrast, quantum cryptography forces the intrinsic principles of quantum mechanics, offering theoretically impregnable security. By generating quantum bits, this approach, when integrated with conventional cryptographic algorithms like the Advanced Encryption Standard (AES), ensures data security during communication. AES, a prevalent symmetric cryptography standard, serves both as an encoder and decoder. The fusion of indiscriminate quantum bits with AES cryptography renders quantum cryptography a potent and straightforward method for safeguarding valuable information. The proposed study outlines the implementation of a quantum key generation technique coupled with the AES algorithm to fortify data against quantum attacks. Within the proposed quantum cryptographic algorithm, an error correction mechanism is incorporated to rectify errors occurring during quantum key distribution. Subsequently, the quantum key generation technique, error correction method, and AES encryption algorithm is discussed in detail.

A. Quantum bits (qubits)

Qubit, short for quantum bit, is the basic unit of quantum information in quantum computing, corresponding to the classical bit in classical computing. While classical bits can exist in states 0 or 1, quit can exist in a superposition of both states simultaneously. This unique property allows qubits to perform complex calculations and solve problems that are not possible for classical computers. For example, in quantum cryptography, qubits can be used to create unbreakable codes due to their ability to exist in multiple states at once. Qubits are typically represented by two basis states, $|0\rangle$ and $|1\rangle$, which correspond to the classical 0 and 1 states. However, qubits can also be in a rectilinear combination of these states, known as superposition. This indicates that a qubit can be in a state represented as $a1|0\rangle + a2|1\rangle$, where a1 and a2 are complex numbers. The ability of qubits to exist in superposition allows for parallel processing and exponential speedup in quantum algorithms. Equation (1) gives the single qubit vector representation. “Ket” represents the quantum states and denoted by the symbol $|\rangle$. The value of ket 0 and ket 1 is represented in equation (2) and equation (3) respectively. Equation (4) gives the vector representation of two qubits.

$$|v\rangle = a1|0\rangle + a2|1\rangle \rightarrow \begin{pmatrix} a1 \\ a2 \end{pmatrix} \quad (1)$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (2)$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (3)$$

$$|vv\rangle = a1|00\rangle + a2|01\rangle + a3|10\rangle + a4|11\rangle \quad (4)$$

Table 1: Algorithm to generate qubits in MATLAB environment

Define ket 0 and ket 1 states. Define the superposition state Ψ= a1 |0> + a2 |1> In the superposition state based on amplitude of a1 and a2 the output received bit will be decided either as 0 or 1. Save the logic in step 3 as a single function this function is invoked whenever the qubit is called.

B. Quantum key generation

The quantum key distribution provides secure communication between the two known entities, Alice and Bob. Alice defines the required number of qubits for the generation of a secret key; these qubits are used by the random key generator function to produce the 2^n possible keys for n qubits. Equation (5) generates the 2^n random keys for n number of qubits. Table 2 shows the sharing of secret key. In the Table 2 “+” represents rectilinear basis and “×” represents designs basis.

randi([0, 1], 1, num_qubits) (5)

C. Error Detection and Correction

The quantum error correction method detects and fixes the errors occurred during the qubit transmission. Alice transmits a stream of qubits to Bob through a quantum channel in the form of zeros and ones. Qubits travel through the channel and reaches Bob. Upon reception, Bob scrutinizes the received bits to detect errors resulting from eavesdropping or Bob's improper application of the basis when receiving the qubits from Alice.

Alice transmits the qubit stream to Bob using various bases. Equation (6) illustrates the qubit stream transmitted from Alice to Bob, employing either a rectilinear or diagonal basis. at the receiver's end Bob checks the received bits and checks for the error that occurred due to eavesdropping and usage of the wrong basis by Bob while receiving the qubits from Alice. Alice sends the stream of qubits to Bob which are of different basis. Equation (6) shows the stream of qubits transmitted from Alice to Bob using either a rectilinear or diagonal basis.

$Q_s = (q_1, q_2, q_3, q_4 \ldots\ldots\ldots q_n)$ (6)

where,

Qs Є rectilinear basis 0(↑), rectilinear basis 1(→), diagonal basis 0( ) and diagonal basis 1( )

Table 2: Generation of Quantum Key

Random key of Alice	0	1	1	1	1	0	0	0
Sending basis of Alice	+	+	×	+	+	×	×	×
Alice sends bits using photon polarization	↑	→	↘	→	→	↗	↗	↗
Measuring basis of Bob	+	+	×	+	+	×	×	×
Bob measures the bits using Photon polarization	↑	→	↘	→	→	↗	↗	↗
Secret key shared by Alice and Bob	0	1	1	1	1	0	0	0
Qubit representation	ket 0	ket 1	ket 1	ket 1	ket 1	ket 0	ket 0	ket 0

The error detection method involves comparing the basis used by Alice with that used by Bob, as well as examining the qubits themselves. Equation (7) is employed to identify any discrepancies in the basis; if such mismatches occur, the correction method employs the key distillation process to rectify errors in the received bits. Should the number of error bits surpass the predetermined threshold value, equation (8) is applied to correct the errors.

error_indices =find(alice_bases ~= bob_bases) (7)

error_corrected_key(~ismember(1:num_qubits, error_indices)) =
bob_measurements(~ismember(1:num_qubits, error_indices)) (8)

D. AES Algorithm

The advanced encryption standard algorithm is integrated with the quantum key generation technique to provide security to data from quantum attacks. The key used in the algorithm is 128 bits. The inputs to the algorithm are quantum key generated using a quantum key generator and the secret message intended for encryption. Equation (9) shows the MATLAB function to encrypt the message using the AES algorithm. Table 3 shows the application of AES algorithm on qubits.

ciphertext = aesencrypt(plaintext, shared_secret_key_hex) (9)

Table 3: Application of AES algorithm on qubits

Initialize n cubits and generate 2^n random states using key generation method. One random state is selected among 2^n state and used as secret key for AES encryption-decryption method. Alice sends the secret key to bob using his basis format and Bob should use the same basis format to retrieve secret key. If bob uses different basis, an error occurs and this is corrected by error correction method. AES encryption and decryption algorithm is adopted to encrypt and decrypt the normal secret message using secret key.

E. Encryption-Decryption Process

The proposed method adopts advanced encryption standard algorithm and the random key generator technique to secure the information from quantum attacks. Quantum cryptographic algorithm enhances the security robustness of the proposed system, ensuring the system useful for both classical computing and the quantum era. Fig. 1 shows the complete model flow. The proposed method includes the following steps

Step 1: Alice randomly chooses the number of qubits and generates 2^n possible keys for n qubits.

Step 2: Alice sends a stream of qubits to Bob.

Step 3: Bob verifies the basis used at the receiving end with the Alice basis at the transmitting end. The error must be corrected using an error-correcting algorithm.

Step 4: Alice uses a secret key to encrypt the message using the AES algorithm.

Step 5: Bob receives the encrypted message transmitted from Alice.

During the Decryption Process, Bob applies the AES decryption algorithm and secret key same as that of the sender used for encryption to the cipher text to recover the original plaintext message.

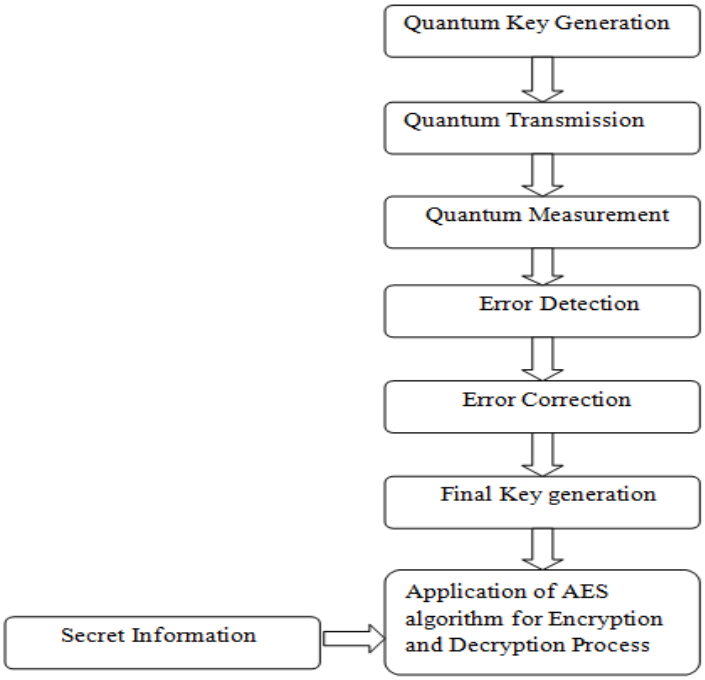

Figure 1: Design flow for the proposed method

RESULT AND ANALYSIS

Quantum cryptography, in particular the combination of quantum key generation techniques with the AES cryptography standard, represents a promising way to achieve unprecedented security in communication systems. Beyond the use of quantum principles such as the superposition of states, the generation of the quantum key provides guarantees of theoretically indestructible security. The communicating parties, Alice and Bob used quantum property as a statistical basis to generate a separate stream of quantum bits. MATLAB software is used to implement the proposed method, separate class for qubits is defined in MATLAB language and AES encryption and decryption is implemented. After obtaining a sufficient number of qubits, Alice and Bob continue measurements to determine the basic statistics used by the transmitting and receiving streams. Apply error correction technique to reconcile eventual differences. This hybrid approach draws on the strengths of quantum cryptography and the techniques of classical cryptography to guarantee the preservation and integrity of the data. Figure (4) shows the output of the proposed method. Parameters like error rate, key generation rate, security, and transmission probability are considered to assess the robustness of the proposed method. Figure (5) and Table 4 show the value of all the parameters considered for analyzing the strength of the proposed algorithm to withstand the quantum attacks. Figure (6) the GUI of the input and AES encryption dialogue box. The GUI conveys the secret message entered in the display icon, binary conversion of the secret information into 0s and 1s encryption result of the AES algorithm. In the proposed method, the combination of Quantum key Generation and AES encryption for message encryption offers a solid and secure communication solution, resistant to both classical and quantum attacks. Table 5 shows the execution time taken by each part of the propose method.

Table 4: Values of the parameters considered for analyzing the performance of the proposed method

Parameters	Values
Key generation rate	0.019608
Error rate	0
Security level	1
Transmission probability	0.67032

Table 5: Values of the parameters considered for analyzing the performance of the proposed method

Parts of the proposed method	Execution time
Quantum key generation	0.12s
AES encryption	0.06s
AES decryption	0.09s

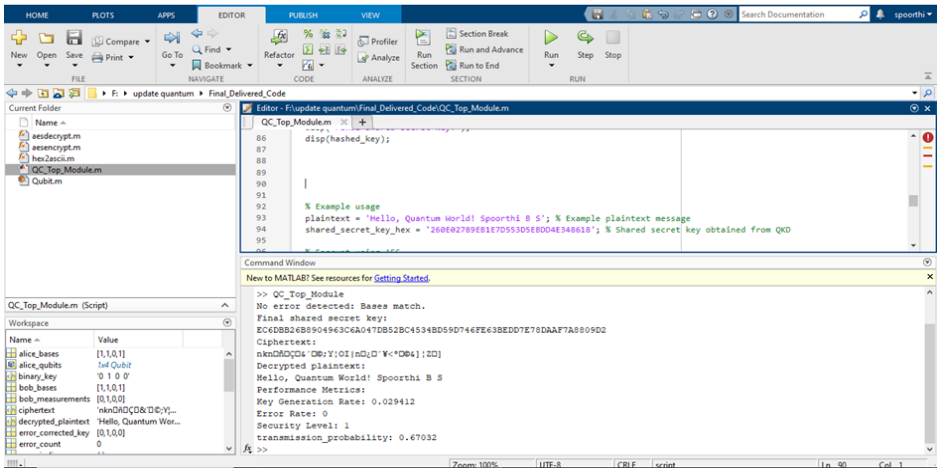

Figure 4: Output of the proposed method

Figure 5: Values of different output parameters

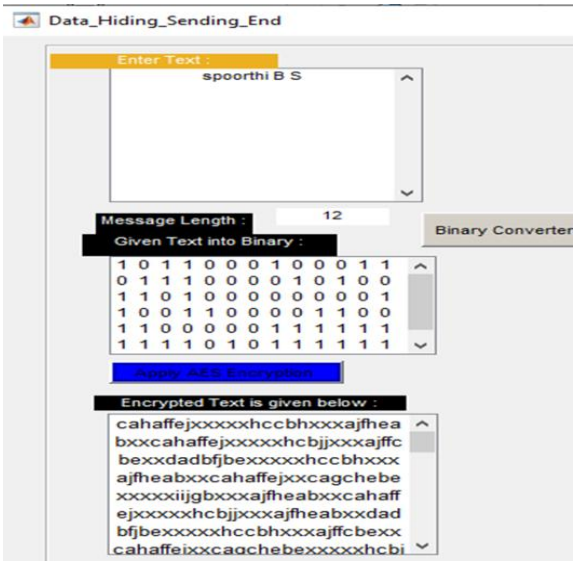

Figure 6: GUI of input and AES encryption dialogue box

CONCLUSION AND FUTURE SCOPE

Quantum cryptography, in actually the quantum key generation method, provides a promising methodology to secure communications based on the principles of quantum technology. The combination of the quantum key generation technique with the AES cryptography method increases the security of the communication between entities by making a secure mode for information exchange. The proposed combination attains the standard of classical cryptography and the strength of quantum cryptography and protects unauthorized access to secret information from quantum computer attacks. In conclusion, quantum encryption integrated with the AES encryption algorithm has great potential to provide secure communications. The proposed method provides security against quantum attacks and by the analysis of all the parameters values, we can conclude that the proposed method is robust enough among the entire quantum cryptographic algorithm.

Future research should focus on better security research, including investigating potential attacks and developing countermeasures to improve the effectiveness of quantum cryptography and emerging threats. Widespread adoption of quantum cryptographic technologies requires coordination and interoperability efforts. Future research should focus on the development of protocols and standards that facilitate communication between different quantum cryptographic systems and ensure compatibility with existing communication infrastructures.

CONFLICT OF INTERESTS

The authors declare no conflict of interests.

REFERENCES

[1] Manuela Weigold, Johanna Barzen, Frank Leymann, Marie Salm, “Expanding Data Encoding Patterns for Quantum Algorithms” IEEE 18th International Conference on Software Architecture Companion pp. 95-101, 2021

[2] Wenjie Liu, Yinsong Xu, Maojun Zhang, Junxiu Chen,and Ching-Nung Yang, “A Novel Quantum Visual Secret Sharing Scheme”, IEEE Access, volume 7, pp.114374-114384, 2019

[3] Xingbin Liu, Di Xia, Wei Huang, and Cong Liu, “Quantum Block Image Encryption Based on Arnold Transform and Sine Chaotification Model”, IEEE Access, volume 7, pp. 57188- 57199, 2019

[4] Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, Tel-Aviv and Umesh Vazirani, “Dense Quantum Coding and Quantum Finite Automata”, Journal of the ACM, vol. 49, pp. 496–511july 2002.

[5] M. Weigold, J. Barzen, F. Leymann, and M. Salm,“Data Encoding Patterns for Quantum Algorithms”, Hillside Proc. of Conf. on Patternlang, of Prog, 10 pages, October 2020

[6] Noam Elron and Yonina C. Eldar, “Optimal Encoding of Classical Information in a Quantum Medium”, IEEE Transactions on Information Theory, pp. 1-10, 2006

[7] Priti Sehgal, Sarvesh Rawat, Saurabh Kaushik, Shafaq Ali, Rohit Yadav, “Hiding Encrypted Text using Text and Image Steganography: A Dual Steganographic Technique”, International Journal of Electrical, Electronics and Data Communication, vol. 5, pp. 54-57, 2017

[8] Ahmed Al-Shaaby, Talal Alkharobi, “Cryptography and Steganography: New Approach”, Transactions on Networks and Communications, vol 5, pp. 25-38, 2017

[9] Jinyuan Tao, Sheng Li, Xinpeng Zhang, And Zichi Wang, “Towards Robust Image Steganography”, IEEE Trans. Circuits And Systems for Video Technology, pp. 1-7, 2018

[10] S. Song And M. Hayashi, "Capacity Of Quantum Private Information Retrieval with Colluding Servers," In IEEE Transactions On Information Theory, Vol. 67, No. 8, pp. 5491-5508, Aug. 2021

[11] K. Lee And S. O. Hwang, "High Throughput Implementation of Post-Quantum Key Encapsulation and Decapsulation on GPU for Internet of Things Applications," 2022 IEEE World Congress on Services, Barcelona, Spain, 2022, pp. 13-13.

[12] D. Chung, S. Lee, D. Choi And J. Lee, "Alternative Tower Field Construction for Quantum Implementation of the Aes S-Box," In IEEE Transactions on Computers, Vol. 71, No. 10, Pp. 2553-2564, 1 Oct. 2022.

[13] S. Alghamdi And S. Almuhammadi, "The Future of Cryptocurrency Blockchains in The Quantum Era," 2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, Australia, 2021, pp. 544-551.

[14] Y. Gao, J. Xu And H. Wang, "Cunh: Efficient GPU Implementations of Post-Quantum Kem New hope," In IEEE Transactions on Parallel and Distributed Systems, Vol. 33, No. 3, Pp. 551-568, 1 March 2022.

[15] H. -C. Cheng, E. P. Hanson, N. Datta And M. -H. Hsieh, "Non-Asymptotic Classical Data Compression with Quantum Side Information," In IEEE Transactions on Information Theory, Vol. 67, No. 2, pp. 902-930, Feb. 2021.

[16] Manuela Weigold, Johanna Barzen, Frank Leymann, Marie Salm, “Expanding Data Encoding Patterns for Quantum Algorithms” IEEE 18th International Conference on Software Architecture Companion pp. 95-101, 2021

[17] Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, Tel-Aviv And Umesh Vazirani, “Dense Quantum Coding and Quantum Finite Automata”, Journal of The Acm, Vol. 49, pp. 496–511july 2002.