An Efficient Approach in Attribute-Based Encryption with Constant-Size Cipher text

Suga Priya. G [1]
[1] Department of Computer Science and Engineering
[1] Bharathidasan University, Trichy

Abstract- *Attribute-based encryption (ABE) is a cryptographic solves the problem security in data sharing. It changed the concept of public-key cryptography. Key-policy attribute-based encryption (KP-ABE) is a type of ABE, which enables senders to encrypt messages under a set of attributes and private keys are associated with access structures. Then this is used to specify which cipher texts the key holder will be allowed to decrypt. In most existing system of encryption the cipher text size grows linearly with the number of attributes attached to it. In this paper, we propose a new KP-ABE with constant cipher text size.*

I. INTRODUCTION

Cryptography is the science of writing in secret code and is an ancient art; the first documented of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any unfrosted medium, which includes just about any network, particularly the Internet.

In a key-policy attribute-based encryption (KP-ABE) system, ciphertexts are labeled by the sender with a set of descriptive attributes, while user's private key is issued by the trusted attribute authority captures an policy (also called the access structure) that specifies which type of ciphertexts the key can decrypt. KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents. Typical applications of KP-ABE include secure forensic analysis and target broadcast [5]. For example, in a secure forensic analysis system, audit log entries could be annotated with attributes such as the name of the user, the date and time of the user action, and the type of data modified or accessed by the user action. While a forensic analyst charged with some investigation would be issued a private key that associated with a particular access structure. The private key would only open audit log records whose attributes satisfied the access policy associated with the private key. The first KP-ABE construction was provided by Goyal et al. [5], which was very expressive in that it allowed the access policies to be expressed by any monotonic formula over encrypted data. The system was proved selectively secure under the Bilinear Diffie-Hellman assumption. Later, Ostrovsky et al. [6] proposed a KP-ABE scheme where private keys can represent any access formula over attributes, including no monotone ones, by integrating revocation schemes into the Goya et al. KP-ABE scheme.

In a ciphertext-policy attribute-based encryption (CP-ABE) system, when a sender encrypts a message, they specify a specific access policy in terms of access structure over attributes in the cipher text, stating what kind of receivers will be able to decrypt the ciphertext. Users possess sets of attributes and obtain corresponding secret attribute keys from the attribute authority. Such a user can decrypt a cipher text if his/her attributes satisfy the access policy associated with the ciphertext. Thus, CP-ABE mechanism is conceptually closer to traditional role-based access control method. The first CP-ABE scheme was proposed by Bettencourt et al. in [7], but its security was proved in the generic group model. Cheung and Newport [8] gave a CP-ABE construction under the Bilinear Diffie-Hellman assumption, but policies are restricted to a single AND gate. Later, Goyal et al. proposed a generic transformational approach to transform a KP-ABE scheme into a CP-ABE scheme using universal access tree in [9].

Within the context of any application-to-application communication, there are some specific security requirements, including:

- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously stud yak.)
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.

II. TYPES OF CRYPTOGRAPHIC ALGORITHMS

There are several ways of classifying cryptographic algorithms. For purposes of this study, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are (Figure 1):

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

Background

[1] In this setting, study presents the first key-policy ABE system where cipher texts can be decrypted with a constant number of pairings. Study show that GPSW cipher texts can be decrypted with only 2 pairings by increasing the private key size by a factor of Γ, where Γ is the set of distinct attributes that appear in the private key. Study discuss how these ideas can be translated into the cipher text-policy ABE setting at a higher cost.

In [2] the scheme is proved by using the dual system encryption argument and the four static assumptions which do not depend on the number of queries the attacker makes. The analysis results show that the scheme of this study is selective secure.

[3] Study describes a new efficient identity-based revocation mechanism that, when combined with a particular instantiation of our general monotonic construction, gives rise to the first truly expressive KP-ABE realization with constant-size cipher texts. The downside of these new constructions is that private keys have quadratic size in the number of attributes. It reduces the number of pairing evaluations to a constant, which appears to be a unique feature among expressive KP-ABE schemes.

III. REVIEW OF LITERATURE

Attribute-Based Encryption with Fast Decryption Susan Rosenberger and Brent Waters May 8, 2013: This work focuses on designing ABE schemes with fast decryption algorithms. Studies restrict our attention to expressive systems without system-wide bounds or limitations, such as placing a limit on the number of attributes used in a cipher text or a private key. In this setting, study presents the first key-policy ABE system where cipher texts can be decrypted with a constant number of pairings. Study show that GPSW cipher texts can be decrypted with only 2 pairings by increasing the private key size by a factor of the set of distinct attributes that appear in the private key. Study then present a generalized construction that allows each system user to independently tune various efficiency tradeoffs to their liking on a spectrum where the extremes are GPSW on one end and our very fast scheme on the other. This tuning requires no changes to the public parameters or the encryption algorithm. Strategies for choosing an individualized user optimization plan are discussed. Finally, study discusses how these ideas can be translated into the ciphertext-policy ABE setting at a higher cost.

A Key-Policy Attribute-Based Broadcast Encryption Jin Sun, Yupu Hu , and Leyou Zhang The International Arab Journal of Information Technology, Vol. 10, No. 5, September 2013: According to the broadcast encryption scheme with wide applications in the real world without considering its security and efficiency in the model simultaneously an “unbounded”, Key-Policy Attribute-Based Broadcast Encryption scheme(KP-ABBE) was proposed by combining with waters dual system encryption, attribute-based encryption and broadcast encryption system. Based on the standard model, the scheme can achieve constant-size public parameters, the public parameters do not impose additional limitations on the functionality of the systems (unbounded) and either a small universe size or a bound on the size of attribute sets avoid to fixed at setup. The scheme is proved by using the dual system encryption argument and the four static assumptions which do not depend on the number of queries the attacker makes. The analysis results show that the scheme of this study is selective secure.

Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts Nuttapong Attrapadung , Benoˆıt Libert , and Elie de Panafieu: This study proposes the first key-policy attribute-based encryption (KP-ABE) schemes allowing for non-monotonic access structures (i.e., that may contain negated attributes) and with constant ciphertext size. Towards achieving this goal, we first show that a certain class of identity-based broadcast encryption schemes generically yields monotonic KP-ABE systems in the selective set model. We then describe a new efficient identity-based revocation mechanism that, when combined with a particular instantiation of our general monotonic construction, gives rise to the first truly expressive KP-ABE realization with constant-size cipher texts. The downside of these new constructions is that private keys have quadratic size in the number of attributes. On the other hand, they reduce the number of pairing evaluations to a constant, which appears to

be a unique feature among expressive KP-ABE schemes.

Attribute Based Encryption with Privacy Preserving In Clouds M. Suriyapriya , A. Joicy International Journal on Recent and Innovation Trends in Computing and Communication Security and privacy are very important issues in cloud computing. In existing system access control in clouds are centralized in nature. The scheme uses a symmetric key approach and does not support authentication. Symmetric key algorithm uses same key for both encryption and decryption. The authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. A new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. The validity of the user who stores the data is also verified. The proposed scheme is resilient to replay attacks. In this scheme using Secure Hash algorithm for authentication purpose, SHA is the one of several cryptographic hash functions, most often used to verify that a file has been unaltered. The Paillier crypto system is a probabilistic asymmetric algorithm for public key cryptography. Pailier algorithm use for Creation of access policy, file accessing and file restoring process.

Ciphertext-Policy Attribute-Based Encryption John Bettencourt Carnegie Mellon University. In this study we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is unfrosted; moreover, our methods are secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

IV. METHODOLOGY

An (Key-Policy) Attribute Based Encryption scheme consists of four algorithms.

Setup - This is a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK. Encryption This is a randomized algorithm that takes as input a message m, a set of attributes γ, and the public parameters PK. It outputs the cipher text E.

Key Generation - this is a randomized algorithm that takes as input – an access structure A, the master key MK and the public parameters PK. It outputs a decryption key D.

Decryption - This algorithm takes as input – the cipher text E that was encrypted under the set γ of attributes, the decryption key D for access control structure A and the public parameters PK. It outputs the message M if $\gamma \in A$. We now discuss the security of an ABE scheme. We define a selective-set model for proving the security of the attribute based under chosen plaintext attack.

V. THE PURPOSE OF CRYPTOGRAPHY

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any entrusted medium, which includes just about any network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including:

- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously studyak.)
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn

(usually) be decrypted into usable plaintext.

In many of the descriptions below, two communicating parties will be referred to as Alice and Bob; this is the common nomenclature in the crypto field and literature to make it easier to identify the communicating parties. If there is a third or fourth party to the communication, they will be referred to as Carol and Dave. Mallory is a malicious party, Eve is an eavesdropper, and Trent is a trusted third party.

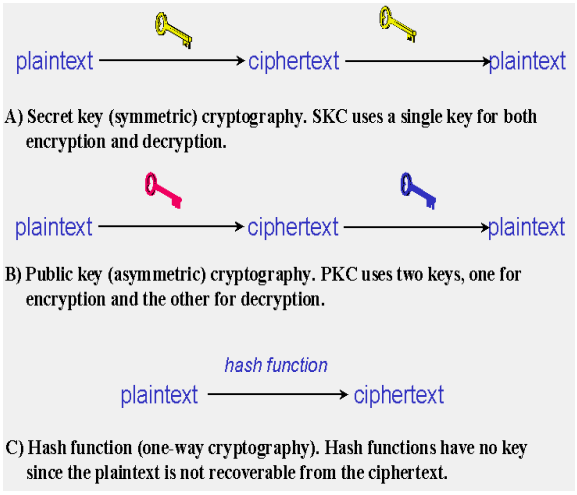

Figure 1.1: Three types of cryptography: secret-key, public key, and hash function

VI. TYPES OF CRYPTOGRAPHIC ALGORITHMS

There are several ways of classifying cryptographic algorithms. For purposes of this study, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are (Figure 1):

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

VII. ATTRIBUTE BASED ENCRYPTION DESCRIPTION

Attribute Based Encryption (ABE) is a novel technology that supports fine grained access control cryptographically. An ABE user can decrypt information, such as a file, only if he or she possesses a key that corresponds to attributes specified during the encryption process.

ABE has been proposed for secure information sharing in applications ranging from storage in clouds to social networks. This study proposes ABE as a part of the solution to secure information sharing in collaborative environments such as multinational operations.

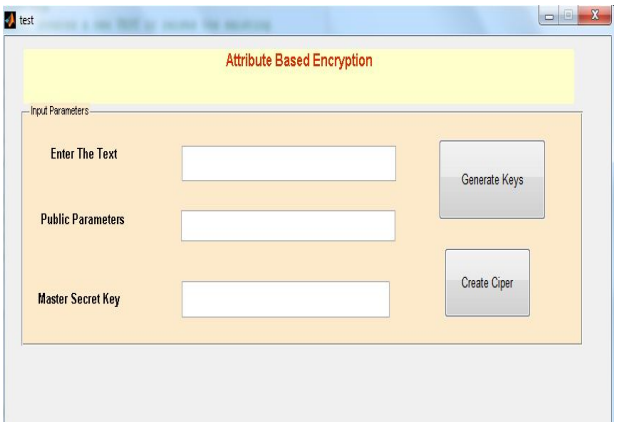

Fig 1 Attribute Based Encryption

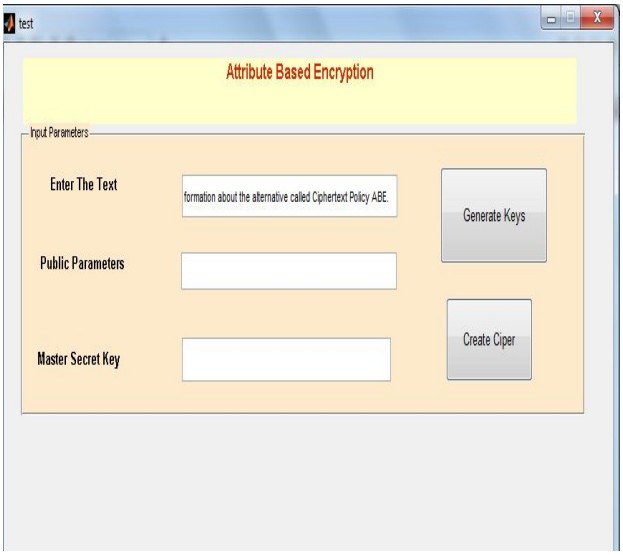

Fig 2 Attribute Based Encryption Gets a Input

Fig 3 Attribute Based Encryption Generates Keys

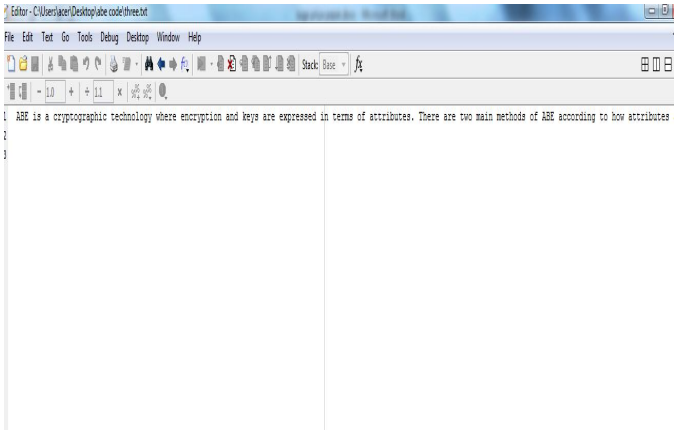

Fig 4 Attribute Based Encryption Generates Output

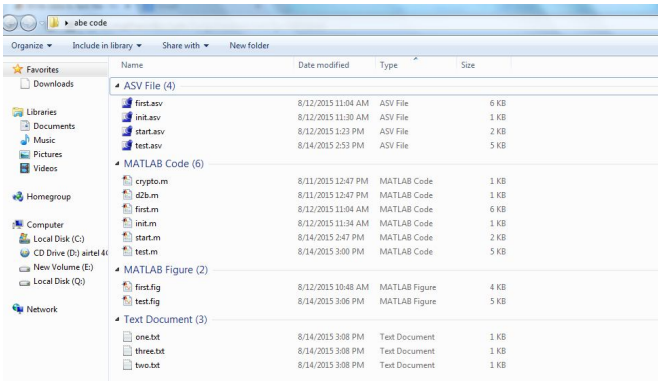

Fig 5 Attribute Based Encryption Outputs are stored in Text File

VIII. EXPERIMENTS & RESULT

SIMULATION ENVIRONMENT

MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

Typical uses include:

- Math and computation
- Algorithm development
- Modeling, simulation, and prototyping
- Data analysis, exploration, and visualization
- Scientific and engineering graphics
- Application development, including Graphical User Interface building

MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. This allows you to solve many technical computing problems, especially those with matrix and vector formulations, in a fraction of the time it would take to write a program in a scalar no interactive language such as C or Fortran.

The name MATLAB stands for matrix laboratory. MATLAB was originally written to provide easy access to matrix software developed by the LINPACK and EISPACK projects, which together represent the state-of-the-art in software for matrix computation.

MATLAB has evolved over a period of years with input from many users. In university environments, it is the standard instructional tool for introductory and advanced courses in mathematics, engineering, and science. In industry, MATLAB is the tool of choice for high-productivity research, development, and analysis.

MATLAB features a family of application-specific solutions called toolboxes. Very important to most users of MATLAB, toolboxes allow you to learn and apply specialized technology. Toolboxes are comprehensive collections of MATLAB functions (M-files) that extend the MATLAB environment to solve particular classes of problems. Areas in which toolboxes are available include signal processing, control systems, neural networks, fuzzy logic, wavelets, simulation, and many others.

Uses of MATLAB

MATLAB is widely used as a computational tool in science and engineering encompassing the fields of physics, chemistry, math and all engineering streams. It is used in a range of applications including −

- Signal Processing and Communications
- Image and Video Processing
- Control Systems
- Test and Measurement
- Computational Finance
- Computational Biology

The MATLAB System
The MATLAB system consists of five main parts:

IX. CONCLUSIONS

This paper has introduced secure multinational information sharing and Attribute Based Encryption (ABE) as basis of the solution.ABE is a recent cryptographic development in an area where further innovation is expected. The benefits of this approach are improved security within domains, mainly by minimising the attack surface for insiders and malware, and also by minimising dependency upon critical cryptographic servers. ABE reduces the impact of risks associated with errors in and compromise of data guards, and scenarios have been identified where ABE reduces the need to otherwise secure communications channels. These benefits

could lead to improved security and/or cost savings.

REFERENCES

[1] Attribute-Based Encryption with Fast Decryption Susan Hohenberger and Brent Waters May 8, 2013.

[2] A Key-Policy Attribute-Based Broadcast Encryption Jin Sun, Yupu Hu , and Leyou Zhang The International Arab Journal of Information Technology, Vol. 10, No. 5, September 2013

[3] Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts Nuttapong Attrapadung , Benoˆıt Libert , and Elie de Panafieu

[4] M. Li, S. C. Yu, Y. Zheng, K. Ren, and W. J. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013.

[5] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in Proceedings of the International Conference on Practice and Theory in Public Key Cryptography (PKC '11), vol. 6571 of Lecture Notes in Computer Science, pp. 53–70, Springer, 2011

[6] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy, attribute-based encryption scheme with constant ciphertext length," in Proceedings of the International Conference (ISPEC '09), vol. 5451 of Lecture Notes in Computer Science, pp. 13–23, Springer, 2009.

[7] "MIRACL Crypto SDK", Certivox, http://certivox.com/ index.php/solutions/miracl-crypto-sdk/

[8] Microsoft, "Digital Rights Management License Protocol Specification", March 2012, ref MS-DRM - v20120328

[9] T. Okamoto K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption", in Tal Rabin, editor, "CRYPTO", volume 6223 of Lecture Notes in Computer Science, Springer, 2010.