International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 09 | Sep 2019 www.irjet.net p-ISSN: 2395-0072

Improved Identity-Based Anonymous Broadcast Encryption with Chosen Ciphertext Security

Iwuchukwu, Vitalis C.[1], Nwokorie, Euphemia C.[2], Okolie, Stanley A.[3], Obi, Uchenna M.[4]

[1]*Lecturer, Department of Computer Science, Federal University of Technology, Owerri, Nigeria*
[2]*Senior Lecturer, Department of Computer Science, Federal University of Technology, Owerri, Nigeria*
[3]*Lecturer, Department of Computer Science, Federal University of Technology, Owerri, Nigeria*
[4]*Lecturer, Department of Computer Science, Federal University of Technology, Owerri, Nigeria*

Abstract - *Anonymous receiver encryption is an important cryptographic primitive. It allows a sender to use the public identities of multiple receivers to encrypt messages so that only the authorized receivers or a privileged set of users can decrypt the messages, and the identities of the receivers are not revealed. The increasing need to protect users' identity in an era of improved digital technology and cyber crime is very crucial. As such, the idea of anonymity in all fields of modern cryptography is given due attention so as to improve users' experience and security. Generally, in broadcast encryption schemes, a broadcaster first chooses a set S of users who will be able to decrypt broadcast messages as authorized users' set and encrypts a computed secret broadcast as a part of a ciphertext. Pay televisions use the Conditional Access System (CAS) which is the bedrock of the anonymous broadcasting. This work will improve the Anonymous Identity-Based Encryption Schemes using security based on bilinear groups and decisional bilinear Diffie-Hellman problem in improving the ciphertext security. The methodology used is the Object-oriented System Analysis and Design Methodology and a design that focuses on reuses. Implementation of work was done using PHP programming language and Heidi Structured Query Language (HeidiSQL) in the Laragon platform as the backend.*

Key Words: Broadcast Encryption, Cryptography, Anonymity, Conditional Access System (CAS), Ciphertext security.

1. INTRODUCTION

The world is becoming very reliant on digital ideas and technologies, and a way to tackle the protection of users' privacy is becoming as important too. This is evident by the huge attention that is laid on anonymity in basically every aspect of cryptography in the modern area. Interesting angles such as network communication, pay satellite television and data management have been battling to make their users anonymous and independent on each other. Broadcast encryption (BE) as an idea was first propounded by Fiat and Naor in 1994, and it is a mode of communication where encryption of public-keys is sent to many recipients (multi-recipient broadcast). In many schemes of broadcast encryption, a broadcaster can encrypt a broadcast message and then sends them to a subset of users (S) who are users or listeners on the channel. In the set S, each user can utilize his/her private key decrypt the messages of the broadcast all at the same time. The notion of broadcast encryption has broad application areas such as management of digital rights, pay TV, video conferencing, communication through satellite radio and wireless sensor network [1].

Anonymity in the aspect of Public-key Encrytion (PKE), is usually termed as key-privacy [2]. PKE captures the features where a listerner of the channel is not capable of telling which particular key of many public keys that a ciphertext was designed. The importance of securing the privacy of receivers is paramount in very complex systems that involves Hierarchical Identity Based Encryption (IBE) for example [3] and Attribute-Based Encryption (ABE) also called Predicate Encryption [4], where improved anonymity achievement becomes a very hectic challenge. Moreso, in the aspect of digital signatures, several primitives effortlessly depend on anonymity: signature groups and anonymous credentials are peculiar examples of such system.

1.1 Definition of Broadcast Encryption

In the most general form of broadcast encryption models, a broadcaster first of all decides a set of S users who are capable of decrypting broadcast messages on a set of authorized users'. The message encrypts a private broadcast key computed into the header as an aspect of the ciphertexts. Next, the private key is used to encrypt broadcast messages in the way similar to symmetric encryption as a portion of the ciphertext also. Any listerner or user of the system that is using the broadcast channel could get the ciphertext with two portions [5], but then just users in the authorized set S can use their secret key to decrypt the ciphertext so as to read the broadcast message. A fully collusion resistant broadcast encryption model is one where considering that all unauthorized users of the set S colloude, they have no way of inferring any information about the broadcast messages [6]. Typically, schemes of identity-based encryption (IBE) allow users to determine public keys that relate to their common identities like telephone numbers, e-mails, names and other similar strings. Also, identity-based encryption decreases intercommunication, computational overhead and initialization. It also simplifies key management and removes the urgency for secret key databases.

1.2 Conditional Access System (CAS)

Broadcasting on televisions with paid subscriptions (pay TV) is made up of a system called Condtitional Access System whereby a broadcaster can encrypt two types of messages for any particular user: Entitlement Control Messages (ECM) and Entitlement Management Messages (EMM). ECM contains basic information availabale to all users while its transmission is same to the common broadcast encryption system where the private key of the user is used. On the other hand, EMM encloses contract or personal information of every individual user, in a encryption symmetric format, each user's secret key is engaged to encrypt the EMM. As such, the management of all user's secret and public keys is being done by the broadcaster. Typically, there is an increment in the cost of managing keys of the broadcaster compared to the general broadcast models as a result of the ultimate management of the secret key of all users. It is pertinent to ensure that the cost of management of of the broadcaster is reduced in the areas of low overhead and smooth communication of ECM and EMM.

A broadcast encryption scheme is said to be efficient in relation to four variables: key storage, decryption overhead, encryption overhead and transmission overhead [7]. In a broadcast scheme, the ciphertext overhead can be defined as the quantity of bits in the ciphertext above what is required for the authorized set of users to be fully described and the symmetric encryption of the plaintext payload [8]. This implies that a broadcast encryption scheme is more thorough and efficient provided that the secret key management is smaller and the ciphertext overhead is shorter, and it will also have a low overhead provided there is a logarithmic dependence of the ciphertext overhead and the number of users of the broadcast.

1.3 Anonymity in Broadcast Encryption

Anonymity is a very important aspect for encryption models. It only implies that no one can obtain the credentials of users from the ciphertexts. As an example: if a customer makes demand of a sensitive TV material, the user should expect no other user to know or be able to decipher his subscribed channels. Particularly, this problem is demanding very great attention in different aspects of cryptography recently, with key inputs in the "Key-Privacy Public Key Encryption Scheme" [2], "Anonymous Identity-Based Encryption Schemes" [9, 3], "Attribute-Based Encryption with Hidden Policy Schemes" [10], "Predicate Encryption with Hidden-Vector Scheme [4]. Also, two proposals of broadcast encryption systems with a security that is a chosen ciphertext and are fully anonymous were propounded in 2006. The first one is a general model construction, which relies on chosen-ciphertext security and anonymous "Public Key Encryption" schemes. Here, the cost of decryption has a linear relationship with the number of receivers [11]. The second one is an improvement of the first whereby the number of decryption activities is constant and its security depends on the "random oracle model". Libert et al. [12] also made contributions in anonymity of broadcast encryption designing with "adaptive chosen ciphertext" security in the standard scheme, and then formally highlighted the security definition of broadcast encryption models. Still in 2012, Fazio and Perera [13] propounded two new models called "Outsider-anonymous BE constructions with sublinear ciphertexts" and they went ahead to show that the model is secured adaptively to chosen-plaintext attack (CPA) and chosen-ciphertext attack (CCA).

Broadcast encryption is a broad field and "identity-based broadcast encryption" (IBBE) is a particular aspect of it, whereby the public key of the users' may be any string given that the string can be a unique identifier of the user, like name, phone number, passport number, etc. [14]. This field has been attracting a lot of attentions from researchers. An efficient "multi-receiver" IBBE model [15] was the first ever, as it is secured selectively against chosen ciphertext attacks in "random oracle model". It is worthy of note that identity based broadcast (IBE) models may be redesigned into IBBE schemes effectively. The very first IBBE scheme was proposed by Delerablee [16] which has an equal ciphertexts and secret key sizes and also secured in selective CCA in the random oracle scheme.

2. RELATED WORKS

In 2005, Boneh et al. [17] made a proposal of the first "stateless and fully-collusion resistant" broadcast encryption model with a chosen-ciphertext security. It was however tested to be secured only in selective security under "q-type" assumptions. The selective security needs an attacker to make a declaration on the targets of attack first before the common variables can be gotten.

Barth et al. [11] in 2006 proposed anonymous broadcast encryption designs that are fully anonymous and uses chosen-ciphertext security. The first one is a general design which relies on a chosen-ciphertext secured enough for anonymous public key encryption models. As a disadvantage, it has a linear relationship between the decryption cost and the size of the users. The second one is an improved model that needs a steady size of decryption activities, and the security adjustments are based on the "random oracle" scheme.

Delerablee also suggested the first identity based broadcast encryption model that has a steady number of ciphertexts and secret keys, while it also runs on secured selective chosen ciphertext attacks in random oracle model [16].

Libert et al. (2012) made a description of their scheme "Anonymous Broadcast Encryption: Adaptive Security and Efficient Constructions in the Standard Model". Formally, they defined the idea of anonymous broadcast encryption (ANOBE) while giving many designs for their idea. Also, they ahead to proof that their designs has space for

improvements through "anonymous hint systems" (to increase the performance of decryption) and reuse of randomness (which is to decrease the size of the ciphertext and the costs of computing encryption). A lot of work still should be done in this aspect, beginning from the improvement of the efficiency of the anonymous broadcast encryption models to improving all the extra features which can be found in standard broadcast encryption, including traitor tracing, dynamism or ease of new users to join the scheme, revocation of users' rights and letting them use the anonymous setting [12].

In 2012 also, Fazio and Perera [13] designed a two "outsider-anonymous" broadcast encryption scheme which uses sublinear ciphertexts and it was proven that the designs are secured against adaptive chosen-plaintext attack (CPA) and adaptive chosen-ciphertext attack (CCA) respectively in a standard scheme.

Another adaptive model was created by Zhang et al. (2012). They constructed some new scheme of IBBE in some subgroups. Their proposal ensured shorter ciphertexts size and secret keys. Additionally, it can achieve security fully under some simple "hardness assumptions". In their standard scheme, they used a two-way style to test run how secured the new model is. Their construction achieves O(1) – ciphertexts size and O(1) – secret keys size, and it can handle the trade-off of secret keys and ciphertexts [18]. The secret key of the design has a linear relationship to the maximum size of users. In addition, the proposal had a reduced security due to static assumptions. Their assumptions were a little natural than the ones in existing schemes. Furthermore, decryption cost of their model was dominantly two-pairing, which improves efficiency than in previous schemes.

A design proposed to oppose the one made by Zhang and his researchers was established by another Zhang et al. [19]. This model was a new anonymous scheme with multi-receiver encryption model and they suggested that this model has the ability to hide the identity of the receiver. In an unfortunate manner, in their proposal, they showed that the scheme by Zhang et al. in 2012 could not achieve the privacy of the receiver anonymously when they analyzed the security of the model. At similar periods, they also introduced an attack into the scheme. After due analysis of the reason to introduce the attack, a new anonymous "multi-receiver" encryption model was proposed to improve the anonymity of the identity of the receiver. Formally, they were able to prove that their proposed model is secured semantically to handle confidentiality and anonymity of receiver's identity as well as has better performance with robust security. The scheme has a security that relies on decisional bilinear Diffie-Hellman problem. They claimed that their model was very efficient in aspects of cost of computation and communication overhead. Yet, they focused more on security as a tradeoff to the number of receivers (S).

Ren et al. [20] also made a proposal of an IBBE model that is fully anonymous that relies on asymmetric bilinear groups, and has "adaptive-ID" security without random oracles. An attacker cannot be able to obtain the receivers' identities from the ciphertext, and each receiver is anonymous for any other receiver, and only the broadcaster knows the identities of all receivers. The scheme can simultaneously realize semantic security and recipient anonymity. The scheme achieved this without random oracles based on asymmetric DBDH assumption. Currently, the ciphertext size is not constant in all of fully anonymous BE or IBBE schemes, we expect to reduce the length of the ciphertext while maintaining its full anonymity properties in the future research.

Xu et al. [5] constructed an efficient Broadcast Encryption System with Personalised Messages (BEPM) model which uses multilinear maps. Their model was advantageous in several ways: the size of the public key in their scheme was shorter than in other previous systems, it also has a constant ciphertext length and constant private keys for users. Also, in comparison to other generic BE schemes, the broadcast centre cannot just send messages in a broadcast to all users but also compute personalized messages to all eligible users. Again, the Xu et al. model is secured statically and resistant against collusion if they exists a set of collusions. Lastly, their scheme is applicable efficiently to the conditional access system (CAS) that is the main area of the satellite TV system. However, their scheme did not lay so much emphasis on security and ciphertext attacks.

Kim et al. [21] also presented an adaptively CCA-secure IBBE scheme in standard model through employing dual system encryption technique.

A paper presented by He et al. [22] proposed IBBE model that is secured anonymously under the standard Decisional Bilinear Diffie-Hellman Assumption (DBDH). They claimed that their model is the first identity based broadcast encryption scheme which can satisfy simultaneously anonymity and confidentiality and secured against adaptive chosen-ciphertext (CCA) attacks. Again, their model is composed of some features that are desirable in stateless and fully collusion schemes. Next, their model is very efficient and the size of the public variables, secret key and decryption time are constant. Finally, they defined a new security idea for identity based broadcast encryption models that was called "weakly robust under chosen-ciphertext attacks" (WROB – CCA). However, the size of the ciphertext is linear with the size of the broadcast receivers and their anonymous IBBE model was without constant ciphertext size.

3. ANALYSIS OF EXISTING SYSTEM

Existing state-of-the art broadcast encryption schemes were anonymous and provided some sort of security to the users of the system. Most of them focused on the issue of anonymity at the expense of security and other problems such as running time and length of ciphertexts. There exists a thin space between the ciphertexts sizes in modern

broadcast encryption (BE) models and the scheme being proposed in this approach. The gap is found to hide in the constants in an asymptotic evaluation of the size of ciphertext (that is during measurement of the size of the ciphertexts) but in practice, it is significant enough. A huge problem will arise, therefore, when it is important to further reduce the ciphertexts size in this new research as well as maintaining properties of full anonymity.

Existing schemes may make provision for transmissions secured enough between a broadcast centre and a set of users and the broadcaster simply encrypts information by using public (or common) keys of the broadcast centre and the recipients. The cost of key management of these models is significantly smaller due to the availability of public keys. However, these models cannot be used to transmit personalized messages such that each personalized message is different for each user at any point in time.

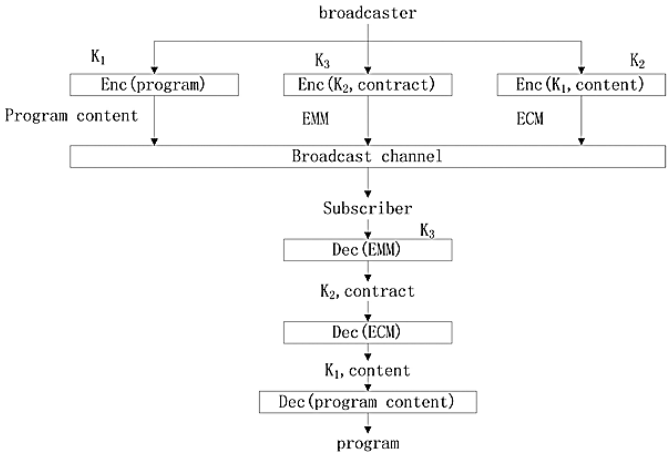

Figure –1: Model of the Existing System [5]

In Figure 1, the broadcaster must manage all users' key K_3. The Entitled Management Message (EMM) and the Entitled Control Message (ECM) are important aspects of the CAS as it initiates the broadcasting process. EMM manages the rights and authority of the viewers of the content while ECM controls the users or viewers of the channel or content. The encoding and decoding processes continue until the final broadcast content is decoded fully.

3.1 Analysis of the Proposed System

The model of the proposed system is incorporated into the Conditional Access System (CAS) as shown in Figure 2.

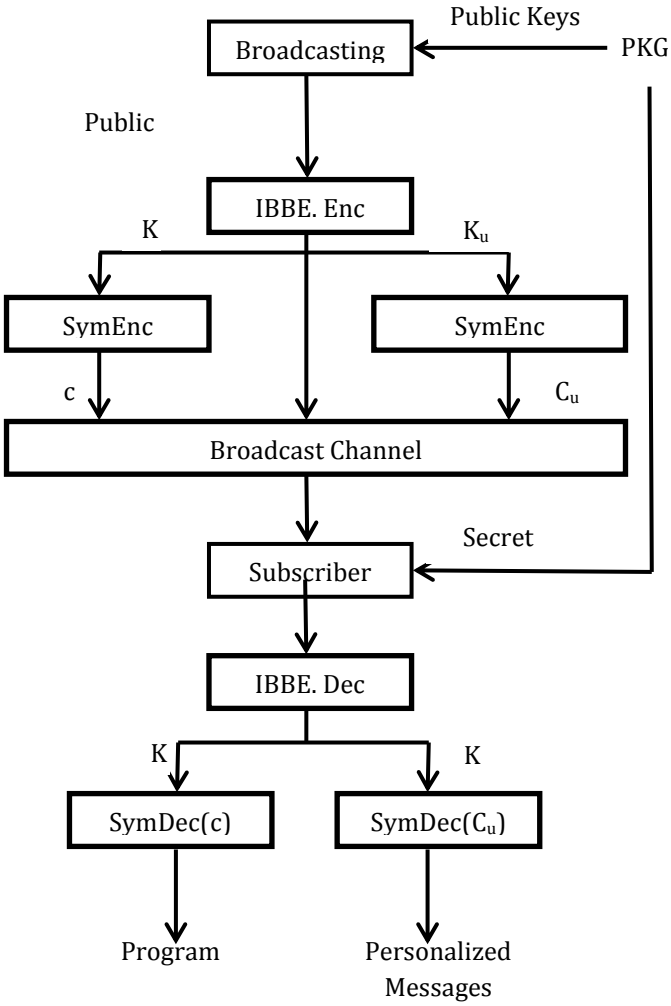

Figure -2: Model of the Proposed System

The proposed model in Figure 2 describes an identity-based broadcast encryption where a broadcaster initially processes the header, a key K for broadcast and K_u which is the key for personalized messages for any user $u \in S$. The K is then used to encrypt a program for broadcast as a ciphertext c and then transmits same. Same way, K_u is used to encrypt messages for personalization as c_u of any user $u \in S$ and then transmits it. An eligible member $u \in S$ (where S is a set of all subscribers or members of the program content) gets c and c_u, which are respectively decrypted using K and K_u to obtain the broadcast content and a eligibility information as personalized message. The Public Key Group (PKG) supplies the public keys for broadcasting and also the secret key to the subscriber for use in decoding the content. In this way, the scheme does not request the broadcaster to manage all users' private keys.

3.2 Algorithm of a Broadcast Encryption System

There are four algorithms that are used in any identity-based Broadcast Encryption model. These algorithms are as follows:

Setup (*ID*): Setting up of an identity space *ID* for a model of broadcast. The *ID* produces *params* as public parameters and *msk* as master secret key.

Extract (*msk*, *u*): A user $u \in ID$ and the master secret key *msk* are taken, and they produce a private key sk_u for any user *i* with identity *u*.

Enc (*params*, *S*): The public parameters *params* is used as input and $S \in ID$ as polynomial sized set of eligible recipients, and then outputs a pair (*Hdr, K*) and a set of personalised keys as K_u for the user $u \in ID$. *Hdr* is used to ensure the confidentiality of *K* which is the symmetrical encryption key that is used to encrypt the broadcast messages as *c* and also K_u as a personalized symmetrical encryption key of user *i* with identity *u* used to encrypt a personalized message as c_u. Finally, it outputs the set (*Hdr, c,* c_u $(u \in S)$) as a ciphertext.

Dec (*params*, *u*, sk_u, *Hdr*, *S*). The decryption algorithm uses inputs pairs *Hdr* and the private key sk_u of any user *i* with whose identity is $u \in ID$, and produces the pair of keys (*K,* K_u) for any user *i* with identity $u \in ID$. The decryption algorithm produces ⊥ if $u \notin$ S. Else, then any user *i* decrypts the *Hdr* with the use of its secret key sk_u to obtain *K* and K_u, and then, finally, the ciphertext *c* and c_u are decrypted respectively.

3.3 Architecture of the System

The proposed architecture of the broadcast encryption system begins with the data owner who has assigns privileges to authorized users and also main groups as shown Figure 3.

The data owner can be the administrator of the system or an agent that is responsible for collecting data from sellers and then allocating to permitted users. The remote user after registering and logging into the system will have a group authority that provides access to privy information and privileges (Figure 3).

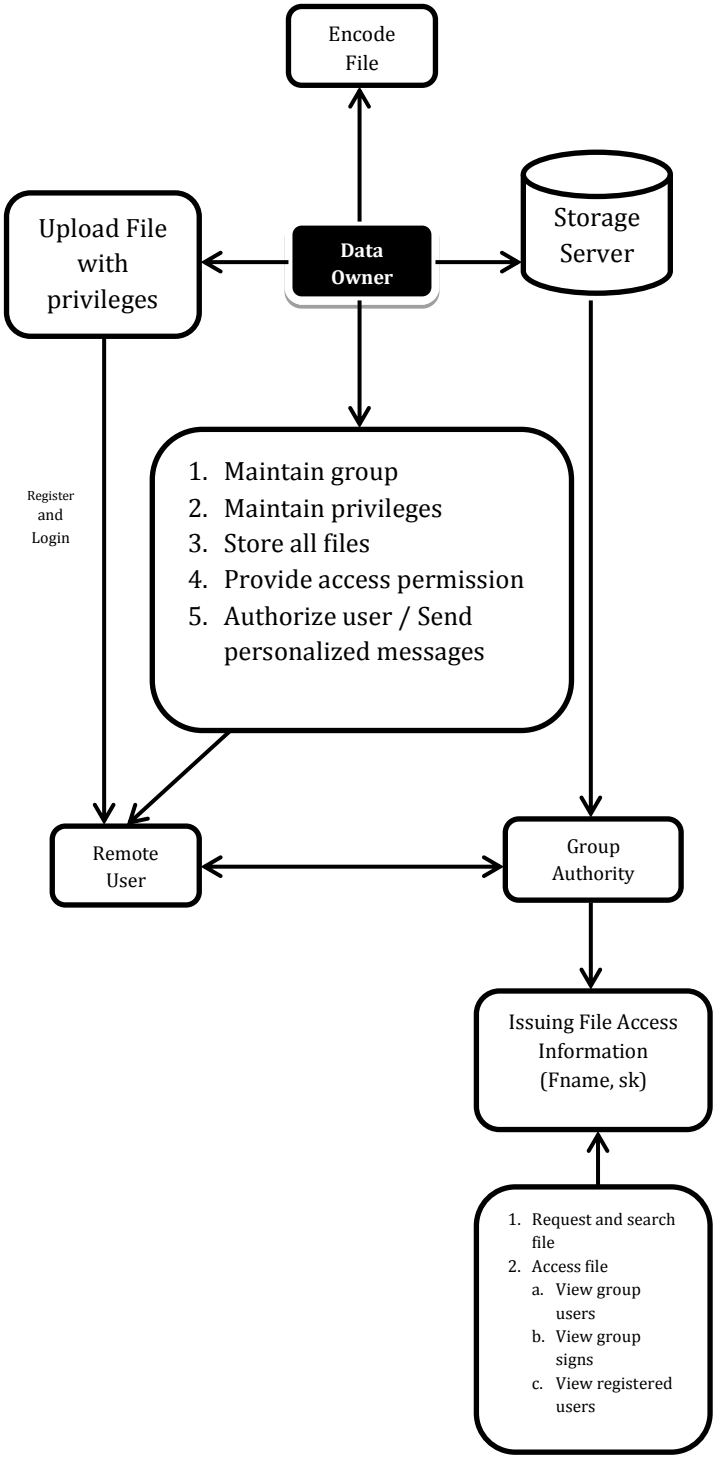

Figure -3: Architecture of the Broadcast System

4. ANALYSIS OF RESULTS

The results of the new model were analyzed and compared with the previous model presented by previous researchers.

i. Ciphertexts Length

The length of this new model is shorter and constant than previous general broadcast encryption schemes. For a message of about 20 characters, the ciphertexts length spans between 30 – 40 encrypted characters.

ii. Private key

The new scheme or model has constant private keys for any number of users to suit the users' mental ability to recall keys easily. This is unlike some generalized broadcast encryption schemes that provide different lengths of private keys to users.

iii. Intrusion Detection

A new mechanism was put in place to detect when an ineligible user tries to access the system or read messages by inputting a wrong key. BEPM is the Broadcast Encryption and Personalised Message Scheme.

Table -1: Comparison of results of the new and previous models.

Scheme	Intrusion Detection	Private Key Size	Ciphertext Size
BEPM	No	Varies (Logn)	Short
Our Model	Yes	Constant	Shorter

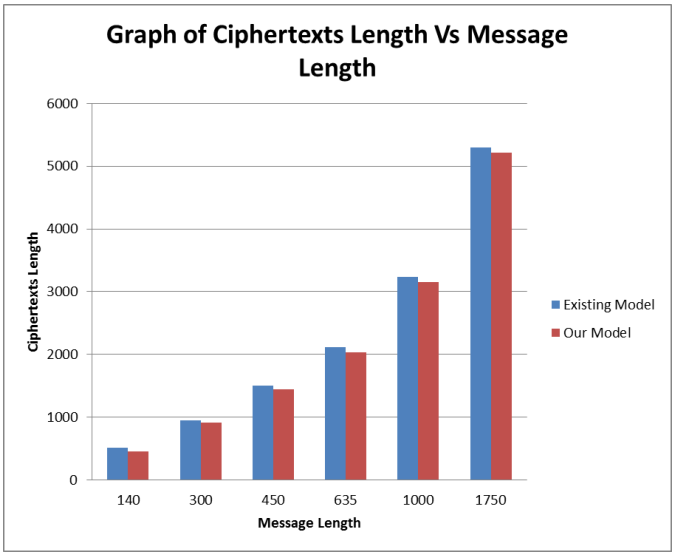

Figure -4: Graphical representation of the Ciphertexts Length against Message Length

Figure 4 shows the comparison of the length of the ciphertexts plotted against the message length of both the Broadcast Encryption and Personalised Messages (BEPM) scheme and our new model. It can be seen that the BEPM produces a little more encrypted characters than the new model. This adds a little advantage to the new system as less space will be occupied in memory.

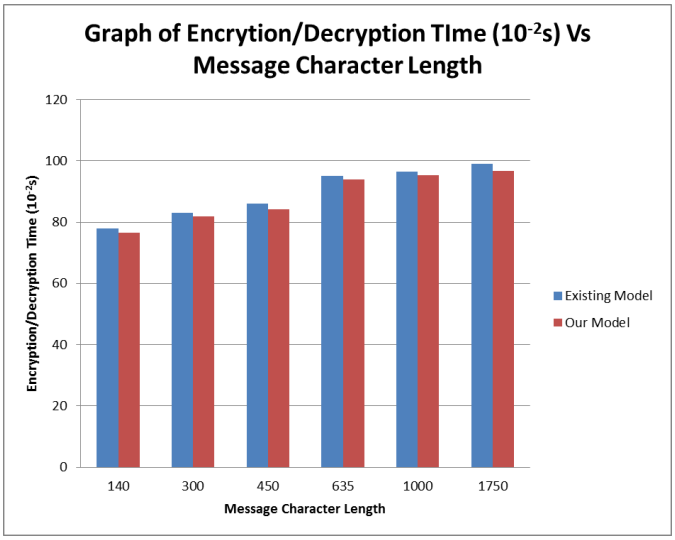

Figure -5: Graph of Encryption/Decryption Times against Message Character Lengths

The graphical illustration of the variations in encryption/decryption times between the test model and the existing model is well shown in figure 5. The times are read in microseconds and slightly increase with the length of the message sent.

5. CONCLUSION

This paper presents an anonymous Identity Based Broadcast Encryption scheme which achieves confidentiality and anonymity with adaptive Chosen Ciphertexts Attacks (CCA) secure under Decisional Bilinearity Diffie-Hellman (DBDH) assumption. In addition, this scheme allows stateless (anonymous) receivers and it is partially collusion-resistant. It is worthy of note that this new scheme is highly efficient, and has constant public parameters size, private key size and very fast decryption time. However, the ciphertext size is also constant and is not affected by the number of the receivers.

5.1 Recommendations

This research can be implemented in the Conditional Access System (CAS) which is currently being used as the model for satellite televisions. Therefore, this work is recommended for use in fields related to digital rights and signature, social media messaging services, satellite television and communication. Others are private messaging (PM), mailing and wireless radio networks.

References

[1] X. Zou and J. Xiang, "Dynamic broadcast encryption scheme with revoking user," Wuhan University Journal of Natural Sciences, Springer, Heidelberg, vol. 18, 499 – 503, 2013.

[2] M. Bellare, A. Boldyreva, A. Desai and D. Pointcheval, "Key-Privacy in Public-Key Encryption," In Advances in Cryptology – ASIACRYPT, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, 9-13(12), LNCS, Springer, Heidelberg vol. 2248, 566 –582, 2001.

[3] X. Boyen and B. Waters, "Anonymous Hierarchical Identity-Based Encryption (without random oracles)", Dwork, C. (ed.): In Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, 20-24(8), LNCS, Springer, Heidelberg,vol. 4117, 290–307, 2006.

[4] J. Katz, A. Sahai and B. Waters, "Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products", In Advances in Cryptology - EUROCRYPT, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, 13-17(4), LNCS, Springer, Heidelberg; vol. 4965, 146–162, 2008.

[5] K, Xu, Y. Liao, L. Qiao, Z. Liu and X. Yang, "An Identity-Based (IDB) Broadcast Encryption Scheme with Personalized Messages (BEPM)", PLoS ONE 10(12): e0143975, 2015. https://doi.org/10.1371/journal.pone.0143975

[6] B. Chor, A. Fiat and M. Naor, "Tracing Traitors", 14th Annual International Cryptology Conference on Advances in Cryptology, Springer-Verlag, London, 257–270, 1995.

[7] A. Kiayias and S. Pehlivanoglu, "Encryption for Digital Content", Springer, 978-1-4419-0044-9, 20-25, 2010. https://link.springer.com/chapter/10.1007/978-3-319-03584-0_19

[8] D. Boneh, B. Waters and M. Zhandry, "Low Overhead Broadcast Encryption from Multilinear Maps", CRYPTO 2014. LNCS, Springer, Heidelberg. vol. 8616, 206–233, 2014.

[9] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier and H. Shi, "Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions", In Advances in Cryptology – CRYPTO: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, 205 – 222, 2005.

[10] X. Li, D. Gu, Y. Ren, N. Ding and K. Yuan, "Efficient Ciphertext-Policy Attribute Based Encryption with Hidden Policy", In Internet and Distributed Computing Systems - 5th International Conference, IDCS, Wuyishan, Fujian, China, 21-23(11), 146 – 159, 2012.

[11] A. Barth, D. Boneh and B. Waters, "Privacy in Encrypted Content Distribution using Private Broadcast Encryption", In Financial Cryptography and Data Security, 10th International Conference, FC, Anguilla, British West Indies, 27(2) – 2(3), Revised Selected Papers, 52 – 64, 2006.

[12] B. Libert, K. Paterson and E. Quaglia, "Anonymous Broadcast Encryption: Adaptive Security and Efficient Constructions in the Standard Model", M. Fischlin; J. Buchmann; and M. Manulis (Eds): PKC 2012, LNCS 7293. International Association for Cryptologic Research, 206 – 224, 2012. https://link.springer.com/content/pdf/10.1007%2F978-3-642-30057-8_13.pdf

[13] N. Fazio and I. Perrera, "Anonymous Broadcast Encryption", GC Cryptography Student Seminar, 2012. https://milinda-perera.com/pdf/2012_06_22_GCCSS.pdf

[14] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes", In Advances in Cryptology, Proceedings of CRYPTO, Santa Barbara, California, USA, 19-22(8), LNCS, vol. 196, Springer, Heidelberg, 47–53, 1984.

[15] J. Baek, R. Safavi-Naini and W. Susilo, "Efficient Multi-Receiver Identity-Based Encryption and its Application to Broadcast Encryption", In Public Key Cryptography - PKC, 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, 23-26(1), 380-397, 2005.

[16] C. Delerablee, "Identity-Based Encryption with Constant Size Ciphertexts and Private Keys", Orange Labs – Caen, France. K. Kurosawa (Ed.): In Advances in Cryptology - ASIACRYPT, 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia LNCS 4833, 200 – 215, 2007. https://eprint.iacr.org/2008/268.pdf.

[17] D. Boneh, C. Gentry and B. Waters, "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys", In CRYPTO '05, LNCS 3621, pages 258–275, 2005.

[18] L. Zhang, Y. Hu and Q. Wu, "Adaptively Secure Identity-based Broadcast Encryption with Constant Size Private Keys and Ciphertexts from the Subgroups", Mathematical and computer Modelling 55, 12–18, 2012.

[19] L. Zhang, Q. Wu and Y. Mu (2013), "Anonymous Identity-Based Broadcast Encryption with Adaptive Security", In: Wang G., Ray I., Feng D., Rajarajan M. (eds) Cyberspace Safety and Security. Lecture Notes in Computer Science, vol 8300. Springer, Cham, 258 – 571, 2013. https://doi.org/10.1007/978-3-319-03584-0_19

[20] Y. Ren, Z. Niu, and X. Zhang. "Fully Anonymous Identity-based Broadcast Encryption without Random Oracles,. I. J. Network Security, 16(4):256–264, 2014.

[21] J. Kim, W. Susilo, M. H. Au, and J. Seberry, "Adaptively Secure Identity-based Broadcast Encryption with a Constant-sized Ciphertext", IEEE Transactions on Information Forensics and Security, 10(3):679–693, 2015.

[22] K. He, J. Weng, J.N. Liu, J.K. Liu, W. Liu and R.H. Deng, "Anonymous Identity-Based Broadcast Encryption with Chosen-Ciphertext Security". Proceedings of the 11th ACMon Asia Conference on Computer and Communications Security, Xi'an , 247-255, 2016.