International Journal of Gender, Science and Technology
ISSN: 2040-0748
UGC Care Group I Journal.
Vol-12 Issue-02 Oct 2023
https://ijgst.com.2023.v12.i2.pp126-135

Protecting Personal Information with an Attribute-Based Encryption Framework

T CHAKRAVARTHI[1] MEKALA SANJEEV KUMAR[2] E.ADINARAYANA[3] N.TEAJA PRAKASH[4]
[1]ASST.PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[2] ASST. PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[3]ASSOC. PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[4] ASST. PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[1,2,3,4] SRI MITTAPALLI COLLEGE OF ENGINEERING

Abstract -

Each policy in Ciphertext Policy Attribute Based Encryption (CPABE) has a variety of characteristics that are used to implement expressive data access regulations. The ciphertext size of most current CP-ABE methods grows exponentially with the number of access policy characteristics. A construction of CPABE with constant ciphertext was recently suggested by Herranz et al. [1]. Nevertheless, the access controls are vulnerable to possible malevolent attackers, and the receivers' anonymity is not taken into account in [1]. Conversely, current privacy-preserving techniques [2], [3] guarantee anonymity but need ciphertext sizes that are large and grow linearly with time. To drastically decrease the ciphertext to a constant size with any given amount of characteristics, we provide a novel construction of CP-ABE in this study called Privacy Preserving Constant CP-ABE (PP-CPABE). To top it all off, PP-CP-ABE uses a concealed policy structure to effectively protect the receivers' privacy. We are unaware of any other structure that has these characteristics prior to PP-CP-ABE. Our team also came up with PP-AB-BE, an encryption system that preserves attributes while broadcasting. Being able to encrypt a broadcasted message using an expressive concealed access policy, with or without explicitly defining the recipients, makes PP-AB-BE more versatile than previous Broadcast Encryption (BE) methods. The storage and transmission overhead is reduced to an order of O(logN), where N is the system size, via PP-AB-BE. Additionally, we demonstrated that PP-AB-BE achieves a low constraint on storage cost for each user in order to cover all potential subgroups in the communication system by using information theoretical methodologies.

Keywords-- Attribute-based encryption, Privacy-preserving, Ciphertext-Policy, Constant ciphertext length, Broadcast encryption.

I. INTRODUCTION

Research on Ciphertext Policy Attribute-Based Encryption (CP-ABE) has been brisk as of late [4, 5, 6, 2]. Every object in CP-ABE may have several attributes, and each attribute is a descriptive string. To reach a group of receivers securely, message encryptors may set a policy for accessing shared data based on the common features that many entities share. In order to retrieve the message, the properties of the decryptor must match the access policy. For systems that need expressive data access control for numerous users, CPABE solutions are attractive due to their unique capabilities. The use of large, linearly growing ciphertext is a key issue with current CP-ABE systems. The size of a ciphertext grows exponentially with

respect to the amount of features contained in the CP-ABE methods described in [4, 6], [2]. For instance, according to BSW CP-ABE [4], the minimum message size is around 630 bytes, and a further 250-300 bytes are added for every extra property. The CP-ABE suggested by Herranz et al. [1] recently calls for a constant ciphertext size. Attached to the ciphertext in unencrypted form are the data access regulations, but it disregards the anonymity of data receivers. Eavesdropping on access policies allows passive attackers to follow a user or deduce the ciphertext's sensitivity. It is as important to safeguard the access controls in many settings as it is to safeguard the data itself. For instance, when the access policy is both "General" and "Pentagon," it reveals the recipient's status and suggests that the communication is sensitive.However, current privacy-preserving techniques [2], [3] safeguard the access rules at the expense of a massive, exponentially growing ciphertext size. We are unaware of any existing technique that simultaneously achieves privacy preservation and a constant ciphertext size. Our new Privacy Preserving Constant-size Ciphertext Policy Attribute Based Encryption (PP-CP-ABE) design uses wildcards to enforce concealed access rules and incurs constant-size conjunctive headers, irrespective of the amount of attributes. It is described in this work. There is a 100-byte limit on the number of bilinear group components needed for each conjunctive ciphertext header. How many parameters are used for the cryptosystem determines the true size of the bilinear group. With element compression, we use Type − D MNT curves in our approach [7]. Attaching many constant-size conjunctive headers to a single ciphertext message allows for disjunctive or more flexible access controls to be supported. It should be mentioned that in order to prevent confusion and maintain the anonymity of the receivers, we limited each ciphertext header to be conjunctive. Additionally, PP-CP-ABE is compatible with policies that include non-monotonic data access control. The only structure that we are aware of that accomplishes these properties—constant size conjunctive headers with wildcards and privacy preservation—is this one. We also provide a novel design called Privacy Preserving Attribute Based Broadcast Encryption (PP-AB-BE) that extends PP-CP-ABE. A sender encrypts a message for a defined group of receivers who are listening on a broadcast channel in current BE systems, for example, [8]. Nobody can decipher the message, no matter how much they conspire, except for the receivers in the chosen set. It is not a straightforward process to identify every recipient and acquire and store their public keys in a large-scale system. It might be a lengthy and costly procedure for the encryptor to query the CS department roster and get the public key of every student in the roster in order to broadcast a message to all CS students at a university.

II. RELATED WORKS

A fuzzy variant of IBE, Attribute Based Encryption (ABE) was first suggested in [10]. Every user's private key in CP-ABE is linked to a collection of properties, and an access policy encrypts every ciphertext [4, 5, 2, 11, 12, 13, 14]. In order to decipher the message, the user's private key properties must be in compliance with the access policy. The main distinction between identities and attributes is that identities are mapped to users many-to-one, while attributes are mapped to users many-to-many. Encrypting the message with the identity of each recipient and a gradually growing ciphertext

size simulates a constant size conjunctive header. With a fixed number of pairing operations and conjunctive headers of constant size, the authors of [15] presented a CP-ABE method. They obviously weren't trying to solve the problems with recipient anonymity. One issue with their plan is that since the model is still one-to-one, meaning that one attribute list or ID satisfies an access policy. Consequently, their plan may be efficiently and easily executed utilising IBE schemes by using the attribute lists of each user as their ID. The amount of possible combinations of characteristics in a system with n attributes is 2n, which should be noted. Consequently, all possible combinations need 2n access policies if wildcards are not to be used. One may describe numerous combinations of characteristics with a single access policy using wildcards. Separately, Herranz et al. [1] suggested a broader framework for CP-ABE that uses a constant ciphertext. With any monotonic threshold data access policy, such as n-of-n (AND), 1-of-n (OR), or m-of n, their suggested technique ensures constant ciphertext. Unfortunately, receiver anonymity isn't one of their design objectives, unlike our suggested PP-CP-ABE. Schemes such as KSW [2], NYO [3], RC [13] and YRL1 [16] were suggested for concealing the encryptor-specified access policy in order to safeguard its privacy. More specifically, the access policy makes the attribute names visible in both [13] and [16], but conceals the eligible attribute values. Another group key management technique that offers anonymity to group members is the YRL2 scheme, which was suggested in [17] and is based on the BSW scheme [4]. An innovative replacement for hidden policy attribute-based encryption techniques was suggested in [18] as a means of preserving both new and current systems. While all other hidden the conjunctive access rules do not work with wildcards or do-not-care. The characteristics of the decryptor must match those of the access policy in order to decipher ciphertext.The number of access rules grows exponentially

policy methods need ciphertext that grows linearly with the number of hidden policy characteristics, PP-CP-ABE drastically decreased the ciphertext size to constant. It should be mentioned that our previous work [14] suggested an ABE system with constant size ciphertext, and this paper's construction is an evolution of that scheme. First, we present the privacy-preserving requirements for ABE and integrate them into the prior approaches; second, we address the complexity of PP-AB-BE with an information theoretical analysis; and third, we perform a thorough performance evaluation. These three parts constitute the main improvements of this paper. Fiat and Naor presented Broadcast Encryption (BE) in [19], and ABE is an ideal cryptographic building component for making BE a reality. For a given communication, the encryptor in current BE systems must provide the recipient list. Knowing every potential recipient is a huge pain in many situations, therefore the ability to encrypt without knowing them all is a nice perk. Additionally, a basic receiver list is all that are currently supported by existing BE schemes [8], [20]. Access control rules that are both expressive and flexible are difficult to support. In lieu of the flat recipient list, an expressive attribute-based access policy was suggested for use in a broadcast encryption technique in [21]. Additionally, in order to minimise the amount of messages and provide expressive access controls, the authors suggested using a CP-ABE [4], [5] and flat-table [23] approach in [22], [5]. Our suggested approach

drastically cuts the ciphertext size in half, going from linear to constant, in comparison to these previous studies.

PROPOSED METHOD

Here, we showcase the PP-CP-ABE scheme that we built.

There are four main algorithms that make up the PP-CP-ABE scheme:

(1) **Setup(1^λ , k)**
A security parameter 1λ and the system's attribute count k are inputted into the Setup procedure. It gives you the master key MK and the public key PK. To encrypt data, one uses the public key, and to generate private keys, one uses the master key.

(2) **KeyGen(PK,MK,L)**
A security parameter 1λ and the system's attribute count k are inputted into the Setup procedure. It gives you the master key MK and the public key PK. To encrypt data, one uses the public key, and to generate private keys, one uses the master key.
.
(3) **Encrypt(PK,W,M)**
As input, the Encrypt algorithm requires the public key PK, the message M, and the given access policy W. Only an authorised user whose attribute list matches the access policy will be able to decipher the ciphertext CT that is generated by the algorithm. Aside from that, the ciphertext links the anonymised access policy W.

(4) **Decrypt(PK,SK,CT)**
Assuming the user's list of attributes is compatible with the access policy, the Decrypt algorithm will decode the encrypted data. As input, it requires the user's public key (PK), private key (SK), and ciphertext (CT), which consists only of the anonymised access policy (W). Where L is the user's attribute list and W is the access policy concealed from the ciphertext, it provides a valid plaintext M if and only if L |= W.
.

Algorithm 1 Construct local guess $\widetilde{W}$

Initialize $\widetilde{W} = \overline{W}$
for $i = 1$ to k **do**
  if $\overline{W}[i] ==$ ✠ **then**
    $\widetilde{W}[i] = L_u[i]$;
  end if
end for
return $\widetilde{W}$;

III. RESULTS AND DISCUSSION

Here we examine PP-AB-performance BE's and compare it to a number of similar solutions, including Subset-Diff [19], BGW [8], and FT-ABE [22], which is based on CP-ABE. In the tree-based multicast group key distribution domain, where a group controller may dismiss members by selectively multicasting key update messages to all remaining members, we also compared several works. Flat-Table (FT) schemes [23] and non-Flat-Table schemes (such as OFT [28], LKH [29], and ELK [30]) are the two main groups into which these solutions fall. In Table I, we can get a summary of the communication overhead complexity study for several methods. The communication overhead of the Subset-Diff scheme is O(t2 • log2t • logN), where t is the maximum number of users that may conspire to decipher the ciphertext. According to [8], the message size for the BGW system is O(N2). The degree of the access control polynomial, which is equal to the number of current receivers in the ACP

scheme, determines the size of the message. So, O(N) is the size of the message.Depending on the amount of keys in the tree that need to be changed, the communication cost for deleting members varies for non-flat-table tree-based multicast key distribution schemes like OFT [28], LKH [29], ELK [30], etc. When one member is eliminated, the centre must update the logN auxiliary keys that were distributed to that member, which results in O(logN) messages. When dealing with many leaves, several tree-based systems attempted to minimise the amount of messages needed to update all the impacted keys. The communication cost for several leaves in ELK [30], a very efficient tree-based system, is O(a − l), where a ≈ l logN is the number of impacted keys and l is the number of departing members. So, O(l logN) is a good way to express the complexity. Eliminating a single node from a flat-table tree-based approach [23] also has an O(logN) complexity. But the biggest advantage of flat-table is that it just takes a few messages to remove many members at once. The two schemes reached information theoretical optimality since ours and the flat-table strategy both used the same amount of messages.But flat-table may be taken down by conspirators. The authors suggested implementing flat-table utilising CP-ABE [4] to prevent collusion attacks in [22]. The amount of messages needed to control a set of receivers S using PP-AB-BE is directly proportional to the product word count in the fmin S. The authors established a maximum and minimum limit on the average product word count in a minimised SOPE in [32]. According to experiments, the typical amount of messages needed is around logN [22].

TABLE I: Examining the storage and transmission costs of various group key management and broadcast encryption methods

.

Scheme	Communication Overhead		Storage Overhead	
	single receiver	multiple receivers	Center	User
PP-AB-BE	$O(1)$	$\approx O(\log N)$	N/A	$O(\log N + m)$
Subset-Diff	$O(t^2 \cdot log^2 t \cdot \log N)$	$O(t^2 \cdot log^2 t \cdot \log N)$	$O(N)$	$O(t \log t \log N)$
BGW_1	$O(1)$	$O(1)$	N/A	$O(N)$
BGW_2	$O(N^{\frac{1}{2}})$	$O(N^{\frac{1}{2}})$	N/A	$O(N^{\frac{1}{2}})$
Flat-Table	$O(\log N)$	$\approx O(\log N)$	$O(\log N)/O(N)$	$O(\log N)$
Flat-Table-ABE	$O(\log N)$	$\approx O(\log^2 N)$	$O(\log N)/O(N)$	$O(\log N)$
Non-Flat-Table-Tree	$O(\log N)$	$O(l \cdot \log N)$	$O(N)$	$O(\log N)$

N: the number of group members; l: the number of leaving members; t: maximum number of colluding users to compromise the ciphertext.

With a 9 logN message limit for the 512-member group and an 18 logN message limit for the 024-member group, PP-AB-BE achieves about O(logN) complexity, as demonstrated in Figures 1, 2, 3, and 4.

https://ijgst.com.2023.v12.i2.pp126-135

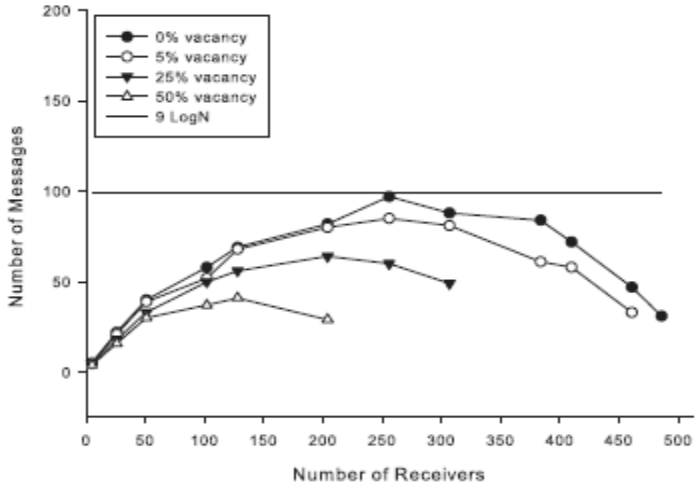

Fig. 1: Number of messages in a system with 512 users.

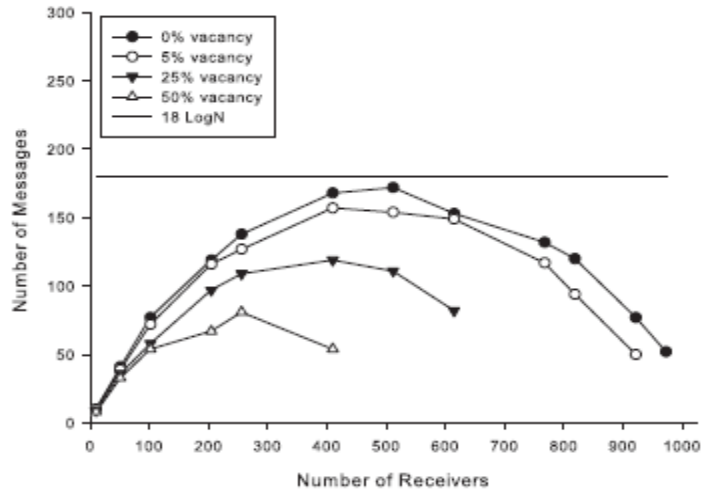

Fig. 2: Number of messages in a system with 1024 users.

International Journal of Gender, Science and Technology
ISSN: 2040-0748
UGC Care Group I Journal.
Vol-12 Issue-02 Oct 2023
https://ijgst.com.2023.v12.i2.pp126-135

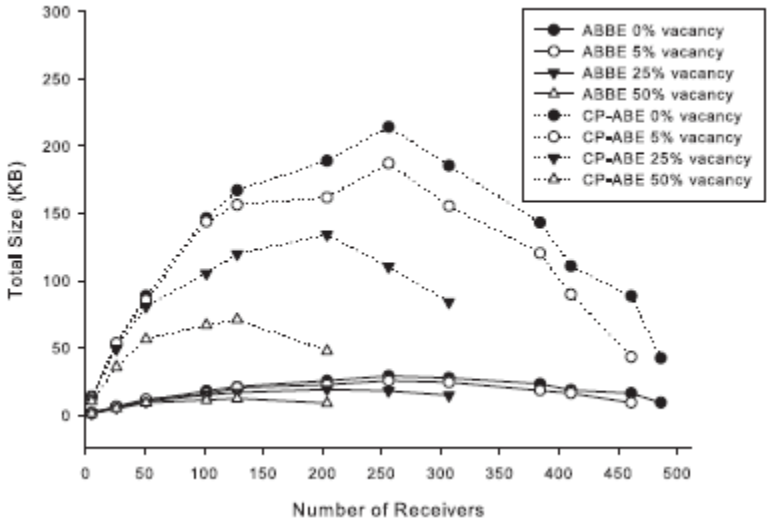

Fig. 3: Total Size of messages in a system with 512 users.

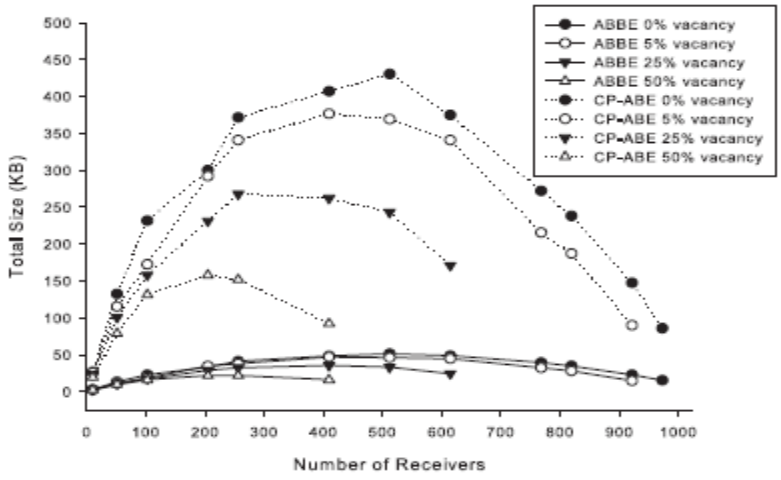

Fig. 4: Total Size of messages in a system with 1024 users.

IV. FUTURE SCOPE AND CONCLUSION

A policy attribute based encryption method called constant ciphertext encryption (PP-CP-ABE) was suggested in this work. In comparison to previous CP-ABE implementations, PP-CP-ABE enables expressive access controls and drastically decreases the ciphertext size from linear to constant. Because of this, PP-CP-ABE may be used in several settings where communication is limited. An Attribute Based Broadcast Encryption (PP-AB-BE) technique was presented, building on PP-CP-ABE, which achieves information theoretical low storage overhead. A user with limited storage space may nonetheless accomplish encryption and decryption by simply pre-installing all necessary key materials. We compared PP-AB-BE to several other BE systems using simulation and theoretical analysis, and we proved that PP-AB-BE achieves superior storage and communication overhead trade-offs.

Attackers using selected IDs are the foundation of PP-CP-ABE's security. Building secure constant CP-ABE against adaptive attackers remains an outstanding challenge.Another drawback of this work is that the PP-CP-ABE is built and shown using the BGW [8] model. We are on the hunt for brand-new buildings that provide the same degree of protection, if not more. On the topic of storage overhead, we only demonstrated that PP-AB-BE is minimalist in this work. Additional information theoretical analysis that considers storage-communication overhead in BE systems is now in the works. There will be two paths for further investigation into this work: This method just works with conjunctive access policies, to begin with. Improving access regulations to accommodate more flexible forms, such as non-monotonic and disjunctive normal forms, is a significant step in the right direction. Second, in order to keep things clear for the decryptor, the access policy does not conceal the wildcard attribute. It would be great if we could enable a fully concealed access policy without having to specify the wildcard attributes that are involved.

REFERENCES

[1] J. Herranz, F. Laguillaumie, and C. R`afols, "Constant Size Ciphertexts in Threshold Attribute-Based Encryption," *Public Key Cryptography–PKC* , pp. 19–34, 2010.

[2] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," *Advances in Cryptology-EUROCRYPT*, vol. 4965, pp. 146–162, 2008.

[3] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," *Applied Cryptography and Network Security*, vol. 5037, pp. 111–129, 2008.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pp. 321–334, 2007.

[5] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 456–465, 2007.

[6] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," *Theory of Cryptography*, pp. 535–554, 2007.

[7] B. Lynn, "On the implementation of pairing-based cryptosystems," Ph.D. dissertation, Stanford Univesity, http://crypto.stanford.edu/pbc/thesis.pdf, 2007.

[8] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *Advances in Cryptology–CRYPTO*. Springer, pp. 258–275, 2005.

[9] M. Abdalla, D. Catalano, A. Dent, J. Malone-Lee, G. Neven, and N. Smart, "Identity-based encryption gone wild," *Automata, Languages and Programming*, pp. 300–311, 2006.

[10] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," *Advances in Cryptology–Eurocrypt*, vol. 3494, pp. 457–473, 2004.

[11] R. Ostrovsky and B. Waters, "Attribute-based encryption with nonmonotonic access structures," in *Proceedings of the 14th ACM conference on Computer and communications security*. New York, NY, USA, pp. 195–203, 2007.

[12] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," *Automata,*

Languages and Programming. Springer, pp. 579–591, 2008.

[13] S. Roy and M. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Technical Report, Tech. Rep., 2009.

[14] Z. Zhou and D. Huang, "On efficient ciphertext-policy attribute based encryption and broadcast encryption," in *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 753– 755,2010.

[15] 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 5th International Conference on Information Security Practice and Experience*. Berlin, Heidelberg: Springer-Verlag, pp. 13–23, 2009.

[16] S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution with hidden policy," in *Proceedings of the 4th Workshop on Secure Network Protocols*, pp. 39–44, 2008.

[17] S. Yu, K. Ren, and W. Lou, "Attribute-based on-demand multicast group setup with membership anonymity," *Computer Networks*, vol. 54, no. 3, pp. 377–386, 2010.

[18] D. Huang, Z. Zhou, and Z. Yan, "Gradual identity exposure using attribute-based encryption," in *Proceedings of the 2010 IEEE Second International Conference on Social Computing (SocialCom)*, pp. 881– 888, 2010.

[19] A. Fiat and M. Naor, "Broadcast Encryption, Advances in Cryptology-Crypto93," *Lecture Notes in Computer Science*, vol. 773, pp. 480–491, 1994.

[20] C. Delerabl´ee, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys," *Pairing-Based Cryptography–Pairing*, pp. 39–59, 2007.

[21] D. Lubicz and T. Sirvent, "Attribute-based broadcast encryption scheme made efficient," in *Proceedings of the first International Conference on Cryptology in Africa (AFRICACRYPT)*. Springer, pp. 325–342,2008.

[22] L. Cheung, J. Cooley, R. Khazan, and C. Newport, "Collusion-resistant group key management using attribute-based encryption," in *Proceedings of the first International Workshop on Group-Oriented Cryptographic Protocols*, 2007.

[23] I. Chang, R. Engel, D. Kandlur, D. Pendarakis, and D. Saha, "Key management for secure lnternet multicast using boolean function minimization techniques," in *Proceedings of the Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom)*. IEEE, pp. 689–698, 1999.

[24] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," *Advances in Cryptology– EUROCRYPT*, pp. 440–456, 2005.

[25] E. McCluskey, "Minimization of Boolean functions," *Bell System Technical Journal*, vol. 35, no. 5, pp. 1417–1444, 1956.

[26] R. Poovendran and J. Baras, "An information-theoretic approach for design and analysis ofrooted-tree-based multicast key management schemes," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 2824–2834, 2001.

[27] T. Cover and J. Thomas, *Elements of information theory*. wiley, 2006. [28] A. Sherman and D. McGrew, "Key Establishment in Large Dynamic Groups Using One-Way Function Trees," *IEEE Transactions on Software Engineering*, pp. 444–458, 2003.

[29] C. Wong, M. Gouda, and S. Lam, "Secure group communications using key

[31] J. Snoeyink, S. Suri, and G. Varghese, "A lower bound for multicast key distribution," Computer Networks, vol. 47, no. 3, pp. 429–441, 2005.

[32] Muppavarapu, Rajasekhar, and Mastan Rao Kale. "An Effective Live Video Streaming System."

graphs," *IEEE/ACM Transactions on Networking*, vol. 8, no. 1, pp.16–30, 2000.

[30] A. Penrig, D. Song, and D. Tygar, "ELK, a new protocol for efficient large-group key distribution," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 247–262, 2001.

[33] LAKSHMI, MANNAM SWARNA, and KALE MASTHAN RAO. "Dynamic Audit Services for Cloud Outsourced Storages with Key Updates." (2017).