IJSR CSEIT

International Journal of Scientific Research in Computer Science, Engineering and Information Technology

© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Hidden Ciphertext Policy Attribute-Based encoding below customary Assumptions

Singampalli. Sankeerthi[*1], **Cherukuri Kiran**[2]

[*1]Assistant Professor, Department of MCA, St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

[2]PG Student, Department of MCA, St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

ABSTRACT

We advise new ciphertext policy attribute-based encryption (cp-abe) schemes in which the get entry to coverage is defined by using and-gate with wildcard. inside the first scheme, we present a brand new technique that uses only one organization element to represent an characteristic, while the prevailing abe schemes of the equal type want to use three one of a kind organization factors to represent an attribute for the three viable values (specifically, nice, negative, and wildcard). our new approach ends in a brand new cp-abe scheme with steady ciphertext size, which, however, cannot cover the get admission to policy used for encryption. the principle contribution of this paper is to endorse a brand new cp-abe scheme with the property of hidden get right of entry to policy by extending the approach we used inside the creation of our first scheme. specially, we display a way to bridge abe based totally on and-gate with wildcard with inner product encryption and then use the latter to obtain the purpose of hidden get admission to coverage. we show that our 2nd scheme is secure underneath the standard decisional linear and decisional bilinear diffie–hellman assumptions.

Keywords: Attribute based encryption, hidden policy, inner product encryption, Viète's formula

I. INTRODUCTION

Access control (i.e., authentication and authorisation) plays an critical function in many facts systems. amongst all the prevailing cryptographic gear, attribute based encryption (abe) has supplied an powerful way for finegrained get entry to manage. abe, that's an extension of identitybased encryption (ibe) [4], [23], permits an access structure/coverage to be embedded into the ciphertext (that is mentioned as ciphertext-policy abe, or cp-abe) or consumer mystery key (this is known as key-coverage abe, or kp-abe). in a cp-abe, the consumer's attributes used for key generation should fulfill theget entry to coverage used for encryption on the way to decrypt the ciphertext, even as in a kp-abe, the person can only decrypt ciphertexts whose attributes satisfy the policy embedded in the key. we will see that get admission to control is an inherent feature of abe, and via the usage of some expressive get entry to systems, we can efficaciously gain fine-grained get entry to control. seeing that its creation inside the seminal paintings of sahai and waters [21], abe has been significantly studied in recent years(e.g., [2], [3], [7], [8], [11], [12], [17], [26]). there are exclusive approaches to outline an get entry to structure/coverage for abe the bushy ibe given by using sahai and waters [21], which can be handled as the first kp-abe, used a specific threshold ccess policy. later, the linear secret sharing scheme (lsss) realizable (or monotone) get right of entry to structure has been followed by many next abe schemes [3], [11], [12], [26]. in [7], cheung and newport proposed any other way to define get entry to shape the use of and-gate with wildcard. to be greater unique, for each attribute inside the universe, there are two possible values: fantastic and terrible. a person's attributes are then defined through a series of tremendous and poor symbols w.r.t. every characteristic inside the universe (assuming that the attributes are located so as within the universe). an access structure is also described through a series of effective and bad symbols, plus a special wildcard (i.e., "don't care") symbol.

Cheung and newport confirmed that by using the usage of this easy get admission to shape, that is enough for many applications, cp-abe schemes may be constructed based on popular complexity assumptions. ultimately, numerous abe schemes [6], [9], [20], [28] have been proposed following this specific get right of entry to structure.

A. The Work

On this paintings, we discover new techniques for the construction of cp-abe schemes based totally at the and-gate with wildcard get right of entry to shape. the prevailing schemes of this kind want to use 3 different elements to symbolize the 3 viable values – wonderful, bad, and wildcard – of an attribute within the get right of entry to shape. on this paper, we recommend a new construction which makes use of handiest one element to represent one attribute. The most important concept at the back of our creation is to apply the "positions" of various symbols to carry out the matching among the access coverage and consumer attributes. specially, we positioned the indices of all of the wonderful, bad and wildcard attributes described in an get admission to shape into 3 units, and with the aid of the usage of theapproach of viète's formulas [22], we allow the decryptor to do away with all the wildcard positions, and carry out the decryption effectively if and best if the closing consumer attributes healthy the ones defined in the get right of entry to structure. our new method leads to a brand new cp-abe scheme with consistent ciphertext length.even though a comfortable abe can well defend the secrecy of the encrypted data against unauthorised get entry to, it does no longer protect the privacy of the receivers/decryptors by default. this is, given the ciphertext, an unauthorised person may also nevertheless be capable of achieve some facts of the statistics recipients. as an instance, a health organisation wants to send a message to all of the patients that deliver positive illnesses. then the attribute universe will incorporate all the diseases, and an get right of entry to coverage will have the format "++−∗∗+. . ." wherein "+" ("−") indicates high quality (terrible) for a selected disorder. if a cp-abe cannot cover the get admission to policy, then from the truth whether a person can decrypt the message or not, human beings can immediately study a few sensitive information of the person. therefore, it's also very import an to hide the get admission to coverage in such applications. but, most of the prevailing abe schemes based totally on and-gate with wildcard cannot achieve this belongings. to cope with this trouble, we further observe the trouble of hiding the get right of entry to policy for cp-abe primarily based on and-gate with wildcard. as the principle contribution of this work, we make bigger the method we've got used in the first production to bridge abe primarily based on and-gate with wildcard with internal product encryption (ipe) [1], [14], [24].

specially, we present a way to convert an get entry to coverage containing wonderful, terrible, and wildcard symbols into a vector x that's used for encryption, and the person's attributes containing effective and bad symbols into every other vector y that is utilized in key era, after which apply the approach of ipe to do the encryption. again, we use the positions of unique symbols and the viète's formulation [22] to carry out the conversion. the details are supplied in segment iv-a. in table i, we supply a comparison amongst cp-abe schemes that are primarily based on the and-gate get admission to shape or have constantsize ciphertext. we use p to denote the pairing operation, n the variety of attributes in an access shape or attribute listing, m the variety of all viable values for each characteristic, and w the range of wildcard in an get right of entry to shape. we are able to see that amongst all of the schemes which can guide wildcard and offer hidden get admission to coverage, our scheme 2 gives the greatoverall performance for the reason that ciphertext length and the decryption value rely most effective at the variety of wildcard in an get admission to shape.

B. Paper Organization

We present the preliminaries and safety definitions in section ii, that is followed by using our first scheme in phase iii.we then gift the second one scheme with security evidence in segment iv. the paper is concluded in segment v.

II. PRELIMINARIES

Bilinear Map and Its Related Assumptions

Let G and GT be two multiplicative cyclic groups of same prime order p. Let e : G × G → GT be a bilinear map with the following properties:

- *Bilineariry:* $e(u^a , v^b) = e(u^b, v^a) = e(u, v)^{ab}$. for any $u, v \in G$ and $a, b \in Z_p$.
- *Non-Degeneracy:* $e(g, g) = 1$.

Definition 1 : The Decisional Bilinear Diffie-Hellman

(DBDH) problem in G is defined as follows: given a tuple $(g, g^a, g^b, g^c, T) \in G^4 \times G_T$, decide whether $T = e(g, g)^{abc}$ or $T = e(g, g)^r$ where a, b, c, r are randomly selected from Z_p. An algorithm A has advantage in solving the DBDH problem in G if

$\mathbf{Adv}^{\mathrm{DBDH}}{}_{A}(k)$ = Pr[$A(1^k, g, g^a, g^b, g^c, Z) = 1 | Z = e(g, g)^{abc}$]

1. Pr[$A(1^k, g, g^a, g^b, g^c, Z) = 1 | Z = g^r$] ≤ .

We say that the DBDH assumptions holds in G if is negligible for any PPT algorithm A.

Definition 2: The Decisional Linear (DLIN) problem in G defined as follows: given a tuple $(g, g^a, g^b, g^{ac}, g^d, Z) \in$

$G^5 \times G_T$, decide whether $T = g^{b(c+d)}$ or Z in random in G. An algorithm A has advantage in solving the DLIN problem in G if

$\mathbf{Adv}^{\mathrm{DLIN}}{}_{A}(k)$

$$\Pr[A(1^k, g, g^a, g^b, g^{ac}, g^d, Z) = 1 | Z = g^{b(c+d)}] - \Pr[A(1^k, g, g^a, g^b, g^{ac}, g^d, Z) = 1 | Z = g^r] \leq$$

where $a, b, c, d, r \in_R Z_p$. We say that the DLIN assumptions holds in G if is negligible for any PPT algorithm A.

B. Access Structure

Let U = {Att1, Att2, . . . , AttL } be the universe of the attributes in the system. Each Atti is represented by a unique Value Ai . When a user joins the system, the user is tagged with an attribute list defined as S = {S1, S2, . . . , SL } where each symbol Si has two possible values: '+' and '−'. Let

W = {S1, S2, . . . , SL} denote an AND-gate with wildcard access policy where each symbol S
i has three possible values:

'+', '−', and '∗'. The wildcard '∗' means "don't care"(i.e., both positive and negative attributes are accepted).We use he notation S | W to denote that the attribute list S of a user
satisfies W.

For example, suppose U = {Att1 = CS, Att2 = EE,Att3 = Faculty, Att4 = Student}. Alice is a student in the CS department; Bob is a faculty in the EE department; Carol is a faculty holding a joint position in the EE and CS departments. Their attribute lists are illustrated in Table II. The access structure W1 can be satisfied by all the CS students without being in the EE department, while W2 can be satisfied by all CS students and faculties excluding those in EE.

C. CP-ABE Definition

A ciphertext-policy attribute based encryption scheme consists
of four algorithms: Setup, Encrypt, KeyGen, and Decrypt.

- Setup(λ,U): The setup algorithm takes security parameters and attribute universe description as input. It outputs the public parameters PK and a masterkey MSK.
- Encrypt(PK, M, W): The encryption algorithm takes as input the public parameters PK, a message M, and access structure W over the universe of attributes, and outputs aciphertext CT.
- Key Generation(MSK, L): The key generation algorithm takes as input the master key MSK and a set of attributesL ⊂ U, and outputs a private key SK.
- Decrypt(PK, CT , SK): The decryption algorithm takes as input the public parameters PK, a ciphertext CT, and a private key SK, and outputs a message M or a specialsymbol '⊥'.
- E. Security Definition for CP-ABE With Hidden Access PolicyWe define the Selective IND-CPA security for CP-ABE withhidden access policy via the following game.
- Init: The adversary commits to the challenge access policies W0,W1.
- Setup: The challenger runs the Setup algorithm and gives PK to the adversary.
- Phase 1: The adversary submits the attribute list L for a
- KeyGequery.If(L|W0∧L|W1)or(L|W0∧L| W1), the challenger gives the adversary the secret key SKL . The adversary can repeat this polynomiallymany times.
- **Challenge**: The adversary submits messages M0, M1 to the challenger. If the adversary obtained the SKL whose associated attribute list L satisfies both W0 and W1 in Phase 1, then it is required that M0 = M1. The challenger flips a random coin β and

passes the ciphertext Encrypt (PK, Mβ ,Wβ) to the adversary.

- Phase 2: Phase 1 is repeated. If M0 = M1, the adversary cannotsubmitLsuchthatL W0 ∧ L |W1.
- Guess: The adversary outputs a guess of β.

We say a CP-ABE scheme with hidden access policy is secure if for any probabilistic polynomial-time adversary A, AdvIND−CPA

A (k) = |Pr[β = β] − 12| is negligible in the security parameter k.

Full Security : In the above selective security model, the adversary is required to commit the challenge policy before seeing the system parameters. In the full security model, the adversary can choose the challenge policy in the Challenge phase, which makes the model stronger. However, similar to many other C P-ABE schemes given in Table I, we cannot directly prove the security of our schemes in the full security model. We should note that there are transformations from the selective security to full security [15], and we can apply the same transformation to our schemes presented in this paper. However, the transformed schemes will be based on composite Order pairing groups, and hencelessefficient.

III. OUR FIRST CONSTRUCTION

In this section, we present our first scheme based on than AND -Gate with wildcard access policy. Below is the main idea of our construction. We represent each attribute in the universe by an element Ai .

Given an access structure W, we first define three sets J ,V, and Z where J contains the positions of all the wildcard positions, and V and Z contain the positions of all the positive and negative attributes, respectively. We then represent eachpositive/negative attribute in an access structure.

The set J is attached to the ciphertext and sent to thedecryptor. In the decryption process, based on J , the decryptor can reconstruct the coefficients λwj , and generate

_j∈J(Ai)i j λwj = (Ai)_wj ∈J(i−wj)

according to the Viète's formulas, for each positive or negative attribute *Atti* associated with the secret key. In this way, all the wildcard positions will take no effect during decryption. Below are the details of our construction.

IV. CP-ABE WITH HIDDEN ACCESS POLICY

Despite the fact that the cp-abe scheme supplied in the previous segment can obtain consistent ciphertext size, it can't hide the access coverage because the wildcard positions need to be protected inside the ciphertext. on this section, we enlarge the method utilized in our first production to construct any other cpa-abe which can hide the access coverage. one manner to attain the attribute hiding property is to apply the internal product encryption technique within the production of cp-abe. such an method has been used in previous works on coverage hiding cp-abe [5], [15], [16]. however, for the reason that our cp-abe scheme is primarily based on the viète's components, we cannot at once use the preceding technique. in this paper, we propose a new transformation approach that could cope with the viète's formula.

A. OUR CONCEPT

Our fundamental concept is to transform the access policy and consumer attributes into vectors, after which observe the technique of inner product encryption to hide the get right of entry to coverage. much like the primary scheme, we separate the wonderful, negative, and wildcard symbols in an get right of entry to shape into three sets: v , z , and j . based totally on the set j , by using applying the viète's formulation,

we can construct a polynomial $\sum_{k=0}^{n} a_k i^k$ with coefficients $(a_0, a_1, \ldots, a_n)$.

Then we combine the set of positive positions V as:

$$\Pi_V = + \sum_{i \in V} \prod_{w_j \in J} (i - w_j)$$

and the set of negative positions Z as:

$$\Pi_Z = - \sum_{i \in Z} \prod_{w_j \in J} (i - w_j).$$

B. Our Second Construction

Setup(1k): Assume that we have *L* attributes in the universe,and each attribute has two possible values: positive and negative. In addition, we also consider wildcard (meaning

"don't care") in access structures. Let *N*1, *N*2, *N*3 be three upper bounds defined as:

*N*1 ≤ *L:* the maximum number of wildcard in an access structure;

*N*2 ≤ *L:* the maximum number of positive attribute in an attribute set *S*;

*N*3 ≤ *L:* the maximum number of negative attribute in an attribute set *S*.

C. Security Proof for Our Second Construction

Theorem 1: Assume the Decision Bilinear Diffie-Hellman assumption and Decisional Linear Assumption hold in group G, then our CP-ABE scheme is selective IND-CPA secure and policy hiding.

D. Indistinguishability Between Game0 and Game1

Suppose that there exists an adversary A which can distinguish the two games with a non-negligible advantage, we construct another algorithm B which uses A to solve the Decision Bilinear Diffie-Hellman problem also with advantage. On input (g, A = ga, B = gb,C = gc, Z) ∈ G4,
B simulates the game for A as follows.

- Setup: B selects random elements γ1, γ2, θ1, θ2,λ, {u1,i }ni=1, {t1,i }ni=1, {t2,i }ni=1, {w1,i }ni=1, {z1,i }ni=1,{z2,i }ni=1, in Zp.

E. Indistinguishability of Game2 and Game3

Suppose that there exists an adversary *A* which candistinguishthese two games with a non-negligible advantage _,we construct another algorithm *B* that uses *A* to solvehe Decision Linear problem with advantage . On input
(g, ga, gb, gac, gd , Z) ∈ G6, *B* simulates the game for *A* as follows.

- *Setup: B* selects random elements *γ*1, *γ*2, *θ*1, *θ*2,
λ, {*u*1,*i* }*ni*=1, {*t*1,*i* }*ni*=1, {*t*2,*i* }*ni*=1, {*w*1,*i* }*ni*=1, {*z*1,*i* } *ni*=1,
{*z*2,*i* } *ni*=1, in Z*p*. Then it selects a random _ ∈ Z*p* to obtain {*u*2,*i* }*ni*=1, {*w*2,*i* }*ni*=1,*w*2, *u*2 under the condition:
= *γ*1*u*2,*i* − *γ*2*u*1,*i*, _= *θ*1*w*2,*i* − *θ*2*w*1,*i* .

The rest of the proof is similar to the above proofs:

- *the indistinguishability between Game3 and Game4 can be proved in the same way as for Game2 and Game3;*
- *the indistinguishability between Game4 and Game5 can be proved in the same way as for Game1 and Game2;*
- *the indistinguishability of Game5 and Game6 can be proved in the same way as for Game0 and Game1*

V.CONCLUSION

In this paper, we provided two new buildings of ciphertext coverage attribute primarily based encryption for the and-gate with wildcard get entry to coverage. our first scheme achieves regular ciphertext length, but cannot conceal the access coverage. alternatively, our 2d scheme can even disguise the access coverage against the valid decryptors. we proved that our 2d production is comfy under the decisional bilinear diffie-hellman and the selection linear assumptions.one shortcoming of our 2d production is that its ciphertext length is no longer consistent, then proving this construction in absolutely comfy.we go away the solution for this trouble as our future work.

V. REFERENCES

[1]. M. Abdalla, A. De Caro, and D. H. Phan, "Generalized key delega-tion for wildcarded identity-based and inner-product encryption," IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1695-1706, Dec. 2012.

[2]. N. Attrapadung, B. Libert, and E. de Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6571. Berlin, Germany: Springer-Verlag, 2011, pp. 90-108.

[3]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secur. Privacy (SP), May 2007, pp. 321-334.

[4]. D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," in Proc. 21st Annu. Int. CRYPTO, 2001, pp. 213-229.

[5]. C. Chen et al., "Fully secure attribute-based systems with short cipher-texts/signatures and threshold access structures," in Topics in Cryptology (Lecture Notes in Computer Science), vol. 7779, E. Dawson, Ed. Berlin, Germany: Springer-Verlag, 2013, pp. 50-67.

[6]. C. Chen, Z. Zhang, and D. Feng, "Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-

cost," in Proc. 5th Int. Conf. Provable Secur. (ProvSec), 2011, pp. 84-101.

[7]. L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2007, pp. 456-465.

[8]. N. Doshi and D. Jinwala, "Hidden access structure ciphertext policy attribute based encryption with constant length ciphertext," in Proc. Int. Conf. Adv. Comput., Netw. Secur., 2012, pp. 515-523.

[9]. K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in Proc. 5th Int. Conf. ISPEC, 2009, pp. 13-23.

[10]. A. Ge, R. Zhang, C. Chen, C. Ma, and Z. Zhang, "Threshold ciphertext policy attribute-based encryption with constant size ciphertexts," in Proc. 17th Austral. Conf. Inf. Secur. Privacy, 2012, pp. 336-349.

[11]. V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in Proc. 35th Int. Colloq. Auto., Lang. Program. (ICALP), 2008, pp. 579-591.

[12]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryp-tion for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS), 2006, pp. 89-98.

[13]. J. Herranz, F. Laguillaumie, and C. Ràfols, "Constant size ciphertexts in threshold attribute-based encryption," in 13th PKC, 2010, pp. 19-34.

[14]. J. Katz, A. Sahai, and B. Waters, "Predicate encryption sup-porting disjunctions, polynomial equations, and inner products," in Proc. Theory Appl. Cryptogr. Techn. 27th Annu. Int. Conf. Adv. Cryptol. (EUROCRYPT), 2008, pp. 146-162.

[15]. J. Lai, R. H. Deng, and Y. Li, "Fully secure cipertext-policy hiding CP-ABE," in Proc. 7th Int. Conf. Inf. Secur. Pract. Exper. (ISPEC), 2011, pp. 24-39.

[16]. A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchi-cal) inner product encryption," in Proc. 24th Annu. Int. EUROCRYPT, 2010, pp. 62-91.

[17]. A. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques," in Proc. 32nd Annu. Conf. CRYPTO, 2012, pp. 180-198.

[18]. J. Li, K. Ren, B. Zhu, and Z. Wan, "Privacy-aware attribute-based encryption with user accountability," in Proc. 12th Int. Conf. Inf. Secur. (ISC), 2009, pp. 347-362.

[19]. 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, vol. 7646. Berlin, Germany: Springer-Verlag, 2012, pp. 146-159.

[20]. T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in Proc. 6th Int. Conf. Appl. Cryptogr. Netw. Secur. (ACNS), 2008, pp. 111-129.

[21]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. 24th Annu. Int. Conf. Theory Appl. Cryptogr. Techn. (EUROCRYPT), 2005, 457-473.

[22]. S. Sedghi, P. van Liesdonk, S. Nikova, P. Hartel, and W. Jonker, "Searching keywords with wildcards on encrypted data," in Security and Cryptography for Networks (Lecture Notes in Computer Science), vol. 6280. Berlin, Germany: Springer-Verlag, 2010, pp. 138-153.

[23]. A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. CRYPTO, 1984, pp. 47-53.

[24]. E. Shi and B. Waters, "Delegating capabilities in predicate encryption systems," in Proc. 35th Int. Colloq. Auto., Lang. Program. (ICALP), 2008, pp. 560-578.

[25]. T. V. X. Phuong, G. Yang, and W. Susilo, "Poster: Efficient ciphertext policy attribute based encryption under decisional linear assumption," in Proc. 21st ACM Conf. Comput. Commun. Secur. (CCS), Arizona City, AZ, USA, 2014.

[26]. B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. 14th Int. Conf. Public Key Cryptogr., 2011, pp. 53-70.

[27]. Y. Zhang, D. Zheng, X. Chen, J. Li, and H. Li, "Computation-ally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts," in Provable Security. New York, NY, USA: Springer-Verlag, 2014, pp. 259-273.

[28]. Z. Zhou and D. Huang, "On efficient ciphertext-policy attribute based encryption and broadcast encryption: Extended abstract," in Proc. 17th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2010, 753-755.