International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-10, Jan 2019

Identity Based Encryption Schemes : A Survey

Khaleda Afroaz, Assistant Professor, Department of CS&IT, MANUU, Hyderabad, Telangana & India,khaleda.afroaz@gmail.com

ABSTRACT- Identity Based Encryption is an alternate to public key encryption, as it removes the necessity of digital certificates. Identity based encryption(IBE) is one of public key encryption scheme in which identity of a receiver is used as public key. Therefore, it eliminates the authentication of public key by digital certificates. In this paper we explain various IBE schemes such as IBE based on the quadratic residues, IBE based on weil pairing and Hierarchical IBE . IBE includes the applications such as give assistance to the deployment of public key encryption, public key revocation and decryption key delegation.

Keywords : Identity Based Encryption, IBE, Public Key Encryption and Hierarchical Identity Based Encryption

I. INTRODUCTION

In public key encryption if Alice wants to convey a message to Bob in an encrypted form he needs the public key of Bob. Digital certificates are used for the authenticity of that public key. Digital certificates are generated by Certificate Authorities(CAs), who are trusted and implement the process as follows: When Bob creates a key pair he presents PK_B and some valid identity to the CA. Then, CA generates a signature, under its verification key VK_{CA} which Bob appends to its public key. Here, signature is a sign of authentication to Bob's public key provided by CA[9,11]. Later, Alice can verify the signature of CA by using VK_{CA} . If it matches, he can gain the confidence that the key really belongs to Bob. However, in order to verify the signature Alice requires to know the true public key of CA[12,13]n . To make it practically possible there should be less number of CAs with wide publicity of their public keys. Though, the entire process is difficult, as all new public keys should be registered with CA[5].

In Identity Based Encryption, Alice can send encrypted data to Bob, by using any one of his identity, such as email id, name , finger print etc., After receiving the encrypted data Bob generates the private key of that identity with the help of private key generator[2,3,4]. Here, no need for Alice to get the public key or certificate. Here, notice that the private key generator has the knowledge of the private keys and it should be a trusted party[5].

In 1984 Shamir has raised a problem for a public key encryption scheme where an arbitrary string can be used as a public key. Since the problem was raised many IBE schemes were proposed. Here, we want to discuss various schemes[1].

In section 2, we give basic definition of IBE scheme. We then give an overview of various proposed schemes.

Identity Based Encryption

The model for Identity Based Encryption composed of a private key generator that generates a pms_i(system parameters) and a master secret key msk_i [5].

This scheme is specified by four polynomial time probabilistic algorithms[15,16].

1.Setup(1^k)
Input :*k* is the security parameter
Output : System parameters pms_i, master secret key msk_i.

2.Extract(pms_i,msk_i,*ID*)
Input : System parameters pms_i, master secret key msk_i,
ID $\{0,1\}^*$ is an IDentity of the receiver
Output: sk_{ID} secret key of the identity *ID*

3. Encryption (pms_i, *ID* ,*x)*
Input : System parameters pms_i, identity of the receiver *ID*, message to be encrypted $x \epsilon$ M
Output : Cipher text $y \epsilon$ C

4. Decryption (sk_{ID} ,y)
Input : Secret key corresponding to that identity *ID*, cipher text $y \epsilon$ C
Output : Message $x \epsilon$ M

II. IBE BASED ON THE QUADRATIC RESIDUES

Suppose q is a prime which is greater than 2 and b is an integer then b is a quadratic residue modulo q if $b \not\equiv 0 \pmod q$ and the congruence $l^2 \equiv b \pmod q$ has a solution $l \epsilon Z_q$. Here, the first practical IBE scheme was implemented by using quadratic residues. The security of this scheme is a dependant on the hardness of the quadratic residue problem. It consists of the following algorithms[6,2].

1. Setup()
The PKG generates a private key by using the following inputs.

 DOI : 10.18231/2454-9150.2018.1289

i. An RSA module n1 = rs, where n1 is a Blum integer which means r, s are two private distinct prime numbers which satisfy $r \equiv s \equiv 3 \pmod 4$
ii. A message space is indicated by $M = \{-1, 1\}$ and a cipher text space $C = Z_n$
iii. A secure common hash mapping $h1: \{0, 1\}^* \rightarrow Z_n$

2. Extract (*pms,msk,id*)
Input: parameters that are generated by Setup() and an arbitrary string ID
Output: the secret key sk_{id}

i. Generate b such that $\left(\frac{b}{n1}\right) = 1$ by a deterministic procedure ID.
ii. Let $sk_{id} = b^{\frac{n1+5-r-s}{8}} \bmod n1$ such that $sk_{id}^2 = \pm b \bmod n1$.

3. Encryption (*pms,id,x*)
Input: parameters that are generated by Setup (), ID of the sender and a message x
Output: Corresponding cipher text *C*

i. Choose a random q such that $x = \left(\frac{q}{n}\right)$, where x is an arbitrary bit of *x*.
ii. Let $y1 = q + bq^{-1} \bmod n1$ and $y2 = q - bq^{-1} \bmod n1$.
iii. Send $y = \langle y1, y2 \rangle$ to the recipient.

4.Decry
ption (sk_{id},y)
Input : Secret key corresponding to that identity *id*, cipher text yϵ C
Output : Message xϵ M

i. Let $\beta = y1 + 2sk_{id}$ if $sk_{id}^2 = b$, otherwise $\beta = y2 + 2sk_{id}$.
ii. Return $m = \left(\frac{\beta}{n1}\right)$

Correctness:
Since, $\beta = y1 + 2sk_{id}$
$= (q+bq^{-1})+2sk_{id}$
$= q(1+bq^{-2}+2sk_{id}q^{-1})$
$= q(1+sk_{id}^2 q^{-2}+2sk_{id}q^{-1})$
$= q(1+sk_{id}q^{-1})^2$

Take, $\left(\frac{\beta}{n1}\right) = \left(\frac{q(1+sk_{id}q^{-1})^2}{n1}\right)$
$= \left(\frac{q}{n1}\right)$
$= x$

III. IBE BASED ON THE WEIL PAIRING

This IBE scheme can be constructed from any bilinear map e:G1XG1→G2 where G1,G2 are two groups of order q,as the Bilinear Diffie-Hellman problem(Though <P,iP,jP,kP> is given, it is difficult to compute $e(P,P)^{ijk}$, where P be the generator in G1 and I,j,k ϵ Z_q^*) in G1 is hard. One of the examples for such map is Weil pairing on the elliptic curve. In this scheme admissible bilinear map is used. The following properties are satisfied by an admissible bilinear map [5,8,9,] .

a) Bilinear: The bilinear map is a map, if $e(cR,dS)=e(R,S)^{cd}$ for all R,S ϵ G1 and all c,d ϵZ.
b) Non-Degenerate: The map does not send all the pairs in G1 X G1 to the identity in G2.
c) Computable: There is an efficient algorithm to generate the mapping.

This scheme composed of the following four algorithms.
1. Setup (1^l)
Input: *l* is the security parameter
Output: System parameters pms_i, master secret key msk_i.

i. Run $G(1^l)$. G will generate a prime q and two groups G1,G2 of order q and a bilinear map which is admissible e:G1XG2→G2
ii. Select a random generator $g_r \epsilon$ G1
iii. Choose a random $r_m \epsilon Z_q^*$
iv. $J_p = r_m g_r$
v. Select a hash function $f1:\{0,1\}^* \rightarrow G1^*$,which is cryptographic
vi. Select a hash function $f2:G2 \rightarrow \{0,1\}^n$ which is cryptographic for some n
vii. Output $pms_i = <q,G1,G2,e,n, g_r, J_p,f1,f2>$
viii. $msk_i = r_m$

2. Extract (pms_i, msk_i, *ID*)
Input : System parameters pms_i, master secret Key msk_i, *ID*ϵ $\{0,1\}^*$is an identity of the receiver
Output: s_{kid} secret key of the identity *ID*.

i. Compute $R_{ID} = f1(ID) \epsilon G1^*$
ii. Set $e_{ID} = r_m R_{ID}$

3. Encryption (pms_i, *ID* ,*x*)
Input: System parameters pms_i, Identity of the receiver *ID*, message to be encrypted *x*ϵ M
Output: Cipher text yϵC

i. Compute $R_{ID} = f1(ID) \epsilon G1^*$
ii. Choose a random $t \epsilon Z_q^*$
iii. $v_{ID} = e(R_{ID}, J_p) \epsilon G2$
iv. $y = <tg_r, x \oplus f2(v_{ID}^t)>$

4. Decryption (sky_{ID},y)
Input : Secret key corresponding to that identity *ID*, cipher text *y*ϵ C
Output : Message *x*ϵ M

i. Let $y = <W,U> \epsilon C$
ii. Compute $x = U \oplus f2(e(e_{ID},W))$

Correctness:

Take,
$e(e_{ID},W) = e(r_m R_{ID}, tg_r)$
$= e(R_{ID}, t)^{r_m g_r}$

 DOI : 10.18231/2454-9150.2018.1289

$= e(r_m R_{ID}, J_p)^t$
$= v_{ID}^t$

Take, $U \oplus f2(e(e_{ID}, W))$
$= x \oplus v_{ID}^t \oplus f2(e(e_{ID}, W))$
$= x \oplus v_{ID}^t \oplus v_{ID}^t$
$= x$

IV. HIERARCHICAL IDENTITY BASED ENCRYPTION (H-IBE)

The Hierarchical IBE scheme is an expansion of IBE scheme based upon weil pairing. In H-IBE, every

user consists of an n-tuple ID in the hierarchy tree[14]. The n-tuple ID contains IDs of the user itself and its ancestors. The root is at level 0[7 8,10]. H-IBE contains following five algorithms: –

1. ***Root Setup***()

i. Based on l which is a security parameter l, generate a prime q using IG (BDH Parameter Generator).
ii. Use q to generate two fields G1 and G2, such that the map e : G1 × G1 → G2 which is bilinear holds.
iii. Pick an arbitrary element R_0 in G1, and then select a random number $T_0 \in Z/qZ$ as the master-key. Compute the system parameter $U_0 = T_0 R_0$.
iv. Generate two hash functions f1 : $\{0, 1\}^* \rightarrow G1$, f2 : $G2 \rightarrow \{0, 1\}^n$.
v. Lower-level Setup For each user $U_t \in Ll_t$, specify a random number $r_m \in Z/qZ$.

2.Extract()

i. For each user U_t with $ID = \langle ID_1, ID_2, \cdots, ID_t \rangle$, its father calculates $Ft = f1\langle ID_1, ID_2, \cdots, ID_t \rangle \in G1$, where r_0 is the identity of G1.
ii. Return the private key $R_m = R_{m-1} + r_{m-1}F_t = \sum_{i=1}^{m} s_{i-1}P_i$ of U_t and parameter $U_i = r_i R_0$.

3. Encryption ()

i. For a message x and $ID = \langle ID_1, ID_2, \cdots, ID_t \rangle$, calculate: $F_i = f1\langle ID_1, ID_2, \cdots, ID_i \rangle \in G1$
ii. 2. For any $s \in Z/qZ$, return the cipher text: $y = \langle sR_0, sR_2, \cdots, sR_t, x \oplus f2(h^s) \rangle$, $h = e(U_0, F_1) \in G2$

4. Decryption()

i. For cipher text $y = \langle Y_0, Y_2, \cdots, Y_t, W \rangle$ and $ID = \langle ID_1, ID_2, \cdots, ID_t \rangle$,
ii. return the message: $x = W \oplus f2\left(\frac{e(Y_0, R_m)}{\prod_{i=2}^{m} e(U_{i-1}, Y_i)}\right)$

Correctness:

Take, $\left(\frac{e(Y_0, R_m)}{\prod_{i=2}^{m} e(U_{i-1}, Y_i)}\right)$

$= \left(\frac{e(sF_0, \sum_{i=1}^{m} rm-1Fi)}{\prod_{i=2}^{m}(r_{i-1}F0, sR_i)}\right)$

$= e(U_0, F_1)^s$

$= h^s$

Take, $W \oplus f2\left(\frac{e(Y_0, R_m)}{\prod_{i=2}^{m} e(U_{i-1}, Y_i)}\right)$

$= x \oplus h^s \oplus f2\left(\frac{e(Y_0, R_m)}{\prod_{i=2}^{m} e(U_{i-1}, Y_i)}\right)$

$= x \oplus h^s \oplus h^s$

$= x$

V. CONCLUSION

Here we have discussed three basic identity based encryption schemes. In addition to algorithms, this paper clearly depicts the step by step correctness of each scheme.

REFERENCES

[1]. A. Shamir. Identity-based cryptosystems and signature schemes. In G. Blakley and D. Chaum, editors, Proceedings of Crypto 1984, volume 196 of LNCS, pages 47–53. Springer, 1984.

[2]. Adi Shamir. Identity-based cryptosystems and signature schemes. In Advances in Cryptology - Crypto 1984, volume 196 of Lecture Notes in Computer Science, pages 47–53, 1984.

[3]. A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems", in Advances in Cryptology – Crypto '86, Lecture Notes in Computer Science, Vol. 263, Springer-Verlag, pp. 186–194, 1986

[4]. Amos Fiat and Moni Naor. Broadcast encryption. In Douglas Stinson, editor, Proceedings of Crypto 1993, volume 773 of LNCS, pages 480–91. Springer, 1993.

[5]. Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In Joe Kilian, editor, Advances in Cryptology - CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 213–229. Springer, 2001.

[6]. C. Cocks, "An identity based encryption scheme based on quadratic residues", Eighth IMA International Conference on Cryptography and Coding, Dec. 2001, Royal Agricultural College, Cirencester, UK.

[7]. Craig Gentry and Alice Silverberg. Hierarchical ID-based cryptography. In Yuliang Zheng, editor, Proceedings of Asiacrypt 2002, volume 2501 of LNCS, pages 548–66, 2002.

[8]. Jeremy Horwitz and Ben Lynn. Towards hierarchical identity-based encryption. In Lars Knudsen, editor, Proceedings of Eurocrypt 2002, volume 2332 of LNCS, pages 466–81. Springer, 2002.

[9]. Dani Halevy and Adi Shamir. The LSD broadcast encryption scheme. In Moti Yung, editor, Proceedings of Crypto 2002, volume 2442 of LNCS, pages 47–60, 2002

[10]. Craig Gentry and Alice Silverberg. Hierarchical ID-based cryptography. In Proceedings of Asiacrypt 2002, volume 2501 of Lecture Notes in Computer Science, pages 548–566, 2002.

[11]. Ben Lynn. Authenticated identity-based encryption.

 DOI : 10.18231/2454-9150.2018.1289

Cryptology ePrint Archive, 2002.

[12]. Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. In Eli Biham, editor, Proceedings of Eurocrypt 2003, volume 2656 of LNCS. Springer, 2003.

[13]. Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity based encryption. In Christian Cachin and Jan Camenisch, editors, Proceedings of Eurocrypt 2004, volume 3027 of LNCS, pages 207–22. Springer, 2004.

[14]. Michael Goodrich, Jonathan Sun, and Robert Tamassia. Efficient tree-based revocation in groups of low-state devices. In Matthew Franklin, editor, Proceedings of Crypto 2004, volume 3152 of LNCS, pages 511–27. Springer, 2004.

[15]. Amit Sahai, Brent Waters, and Ronald Cramer. Fuzzy identity-based encryption. In Advances in Cryptology C EUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science, 2005.

[16]. Brent Waters and Ronald Cramer. Efficient identity-based encryption without random oracles. In Advances in Cryptology C EUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science, 2005.

 DOI : 10.18231/2454-9150.2018.1289