Sādhanā (2022) 47:221
https://doi.org/10.1007/s12046-022-02007-w

A novel traceability approach in IoT paradigm for CP-ABE proxy re-encryption

NISHANT DOSHI

Pandit Deendayal Energy University, Gandhinagar, Gujarat, India
e-mail: doshinikki.backup@gmail.com

MS received 18 January 2022; revised 31 July 2022; accepted 22 September 2022

Abstract. Internet of Things (IoT) is a technology aimed to provide the cost effective infrastructure for today's problems. Due to its plus points, it is widely deployed for various applications. Data generated from these applications need to be protected from prying eyes of the attacker. As identified in the research, CP-ABE (Ciphertext Policy Attribute Based Encryption) is a promising technique to provide the security of data with efficient multi casting. The naïve CP-ABE scheme suffers with issues like traceability, proxy re-encryption, constant length ciphertext, etc. Recently, In 2022, Jhang *et al* proposed the improved approach to improvise the basic CP-ABE scheme having traceability issues. However, it is yet to suffer from other issues like multi authority, proxy re-encryption and variable length ciphertext. One can use different schemes to achieve each of features which result in high computation overhead. Thus, we have improved the existing approach and proposed novel scheme which not only solve traceability but also provide proxy re-encryption as well as multi-authority and constant length ciphertext.

Keywords. IoT; attribute; multi-authority; traceability; constant length.

1. Introduction

Encryption mechanisms are accepting critical part in IoT (Internet of Things) to get the security and mystery. A standard symmetric based key scheme of transporter and beneficiary has identical key for correspondences. However, if single client is vulnerable than whole arrangement set out some reasonable compromise. To decide this issue, in [1] authors have mentioned public key scheme in which beneficiary can give public key to all for encoding of message, thus nobody is given an authority to recover the message. Nonetheless, this plan does not maintain the useful multicast considering the way that for multicast source expected to scramble the message, as many as identical to recipients. Also, transporter hope to maintain public key of a beneficiary, to beat this issue in [2] researchers propose the identity based called IBE scheme i.e. source scramble the plaintext considering gatherer's clever id like email id, Security Number, etc. In any case, the plan failed to help the multi cast so in [3] researchers propose fuzzy IBE structure wherein client with id X priority the choice to interpret the ciphertext entitled for X', if and gave that $|X - X'| > y$, where y is beginning threshold values.

To mitigate the issue of multi cast, in research, the authors have proposed the attribute based scheme called ABE in two variants i.e. KP-ABE [4] and CP-ABE [5]. Indeed, CP-ABE provides more flexibility to sender over KP-ABE based approaches for improvements. In [6], the researchers have proposed the CP-ABE from multi authorities.

As the ongoing philosophies oversee single authority, it is experiencing the overhead issues like regenerate of user's secret key, estimation overhead to make the secret key for all users. In [7–11], the researchers have mentioned the strategies considering multi authority system. More details on these procedures are given in next section.

All of the techniques referred to so far anticipates that IoT transporter should re-encode a comparative mandate for different methodology. It prompts the computation up which can be alleviating as a substitute for the cloud systems. Within proxy re-encryption scheme the proxy server re-scramble with basically no data on secret key of client. In [12–16], the researchers have proposed various ways of managing oversee proxy based re-encryption part.

All of the research work referred to so far have failed to achieve the key traceability issue, for instance anyone having the key (otherwise called secret key) cannot trace to follow the client from it. In this manner in [17–23], the researchers have proposed various ways to deal with the key traceability issue.

All of the approaches referred to has yet to oversee ciphertext length of variable size i.e. size of message

Published online: 01 November 2022

increased with more attribute numbers. Indeed, this makes overheads like computation and communication onto recipient side. In [24–27], the researchers have mentioned the strategies by considering constant length ciphertext.

1.1 *Our contribution*

Considering the ongoing work, it might be required to have a one arrangement having all features. Thus, in this research, we have a plot to incorporate CP-ABE with proxy re-encryption to make our arrangement proper circumstance having subverted client's spoofed secret key is followed and deleted. Indeed, key generation is one time process while encryption/decryption is multiple time process, which make the proposed scheme more suitable to IoT environments. Our arrangement works as follows i.e. attributes of policy is supposed to be subset of key attributes. We identified new scheme to determine this issue and the capability diverge from the ongoing shows. The hardness of this show that the reliance on DBDH assumptions as their predecessors approached.

2. Literature survey

In this fragment we have given the overview on the various procedures in CP-ABE.

2.1 *Multi authority*

Primary CP-ABE plot [5] is overseeing environment of single authority. As entire trust is on the one authority, thus it contains the drawbacks like overhead as well as key escrow. In [7], authors mentioned the chance of multi-authority based structure to tackle these issues of a single authority. This system consists of central authority (CA) and arbitrary Attribute Authority (AA). In [8–11, 28, 29] researchers proposed the different methods to deal with the multi-authority based approaches.

2.2 *Traceability*

As said previously, in CP-ABE, the client is given the secret key considering their qualities. This will lead to the issue of key duplicate as various clients would have the relative attributes of similar key. Finally, it will lead to the key traceability issue in which client's key is compromised/lost/taken and have to follow for reuse. Along these lines, there is a component wherein the delivered secret key will be followed to the given out client and further move will be started by the authority. In [17], the researchers have proposed the possibility of revised CP-ABE considering the improvement of [30, 31]. In this manner, in [18], the researchers have extended the approach for considering the advancement of [32]. Further, it will loosen up with liability in [19]. Afterwards, in [20–22], the researchers have proposed the move closer for additional CP-ABE plot. As all the previous approaches are centered around variable length ciphertext, in [23], the researchers have proposed the philosophy with short ciphertext with less decryption time. Nevertheless, it is limited to single authority with just traceability feature.

2.3 *Proxy re-encryption (PRE)*

Approaches so far failed to provide proxy re-encryption feature i.e. untrusted proxy can re-encrypt the message to minimize the user time. In [33] researchers present the prospect of PRE. In [34] researchers proposed the bidirectional PRE plot. In [35] researchers proposed the principal unidirectional PRE plot. In [36, 37] researchers proposed the identity based PRE plot which switches ciphertext encoded under Bob's key to the alice's key. In [38] researchers proposed the PRE plot which is bidirectional and taking into account key procedure scheme. In [39] researchers proposed the CP-ABE-PRE plot. In [40, 41] researchers mentioned the approach having constant length. In [12–16], the researchers have mentioned the approaches for improvements of PRE schemes.

2.4 *Ciphertext length*

In IoT paradigm, the size of ciphertext is one of the important features. All approaches mentioned earlier failed to provide the efficient ciphertext length. Due to this, there will be not only communication, but also the computation overhead on the involving entities. In [42], the researchers have firstly proposed the concept of constant length ciphertext approach. In [43], the researchers mentioned the improved scheme in ABE considering the strong edge encryption from [44]. In [24–27], the researchers have mentioned the different arrangement for the redesigns in constant length ciphertext.

Taking into account our composing study, traceability or multi-authority or consistent length ciphertext or proxy re-encryption are important features. In any case, none of the procedure available in the investigation to give this features as single arrangement. Likewise, to include the different arrangement for every component be overhead on structure clients. Thus, this paper mentions the approach by taking all of these features in a single scheme to eliminate the use of various schemes.

3. Preliminaries

In this part, we have given the hardness problems to be useful all through the paper.

3.1 *Bilinear group*

Bilinear map: Let G_1 and G_2 multiplicative group of prime order p and generators g_1 and g_2 respectively. A deterministic bilinear map function $e : G_1 \times G_1 \rightarrow G_2$ with following requirements.

- For all $a, b \in G_1, x, y \in Z_p, e(a^x, b^y) = e(a, b)^{xy}$.
- $e(g_1, g_1) \neq 1$.
- e will be computed in linear time complexity.

Decisional Bilinear Diffie Hellman (DBDH) Problem : Group G of prime order p having generator h, on input $h, h^i, h^j, h^k \in G$, check if $k = ij$ or not.

4. The proposed scheme

The simplified diagram is as shown in figure 1.

Set-up: Central Authority will run this algorithm.

- Chooses G_0 having generator g and prime order p.
- Selects exponents $y, \mathcal{E} \in_R Z_p$
- Gets $h = g^{\mathcal{E}}$ and $Y = e(g, g)^y$
- Gets general public parameters $MPK = G_0, g, h, Y$
- Gets general secret parameters $MSK = (\mathcal{E}, y)$

AA_i setup: Attribute Authority i will run this algorithm to generate parameters for attribute i.

- Chooses exponent $\alpha_i \in_R Z_p$.
- Gets general public attribute values $PK_i = g^{\alpha_i}$
- Choose general secret attribute values $SK_i = \alpha_i$

Keygen (MSK,u): Central Authority runs this algorithm. As the user do not require any confidential attribute parameters from CA, the proposed scheme is said to be key escrow free from the attackers.

- Chooses $r \in_R Z_p$
- Gets secret key $SK_u = g^{(y+rtrc)/\mathcal{E}}$,
- Gets public key $PK_u = g^{rtrc}$
- It chooses $trc \in_R Z_p$ as the trace parameter for the respective user.
- Gets $K' = trc$
- It stores the pair (u, trc) in the table T for traceability.
- Set attribute list $L_u = \emptyset$

Trace (u, T, SK_u): It runs by CA to trace the user u. It will check for K' in the trace table T. If corresponding entry found in table T it will output u else return null.

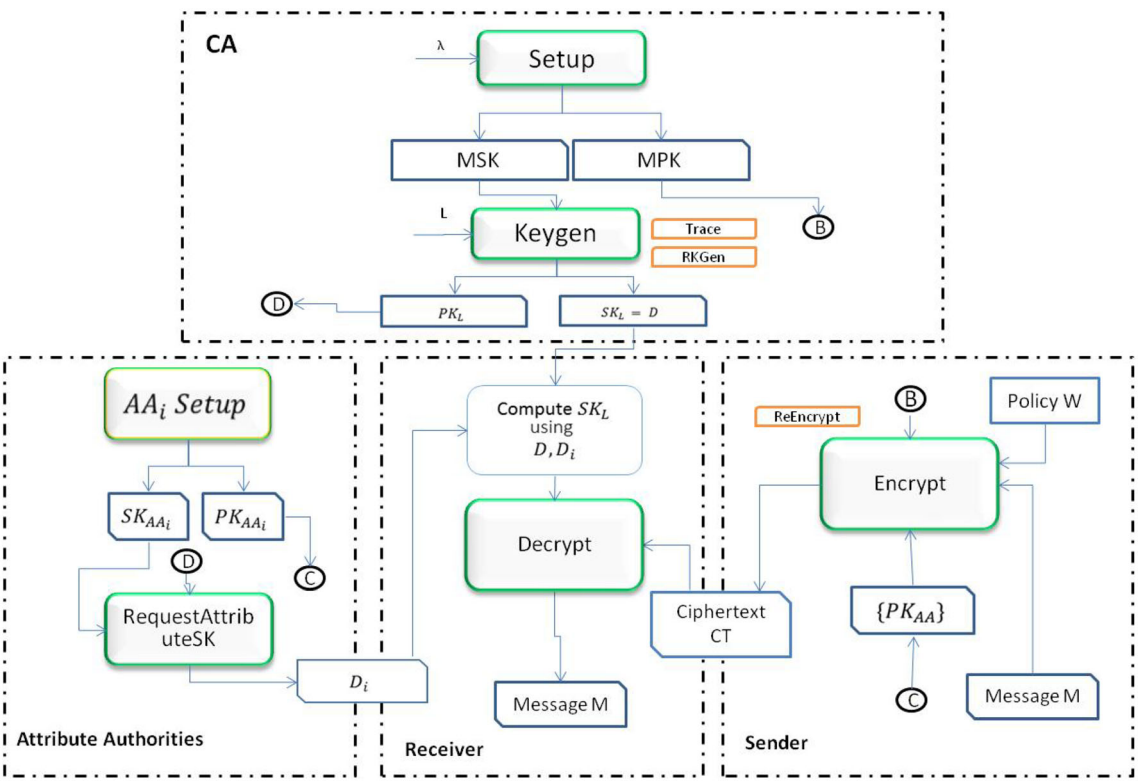

Figure 1. Simplified version of proposed scheme.

Table 1. Size based analysis of CP-ABE schemes.

Approach	Public parameters	Secret parameters	Secret key size	Ciphertext length	Type of policy
[9]	$O(1)\|\partial\|$	$O(1)\|\aleph\|$	$O(1)\|\partial\|$	$O(\mathbb{R}_1)\|\partial\|$	Any threshold gate
[10]	$O(n)\|\partial\|$	$O(n)\|\aleph\|$	$O(\mathbb{R}_2)\|\partial\|$	$O(\mathbb{R}_1)\|\partial\|$	AND gate
[11]	$O(1)\|\partial\|$	–	$O(\mathbb{R}_2)\|\partial\|$	$O(\mathbb{R}_1)\|\partial\|$	Any threshold gate
[28]	$O(1)\|\partial\|$	$O(1)\|\partial\|$	$O(\mathbb{R}_2)\|\partial\|$	$O(n')\|\partial\|$	Any threshold gate
[29]	–	–	$O(n)\|\partial\|$	$O(\mathbb{R}_1)\|\partial\|$	Any threshold gate
[17]	$O(n)\|\partial\|$	$O(n)\|\aleph\|$	$O(\mathbb{R}_2)(\|\partial\|)$	$O(\mathbb{R}_1)\|\partial\|$	Any threshold gate
[18]	$O(1)\|\partial\|$	$O(n)\|\aleph\|$	$O(\mathbb{R}_2)(\|\partial\|+\|\aleph\|)$	$O(\mathbb{R}_1)\|\partial\|$	Any threshold gate
[19]	$O(1)\|\partial\|$	$O(n)\|\aleph\|$	$O(\mathbb{R}_2)(\|\partial\|+\|\aleph\|)$	$O(\mathbb{R}_1)\|\partial\|$	Any threshold gate
[23]	$O(n)\|\partial\|$	$O(n)\|\aleph\|$	$O(\mathbb{R}_2)(\|\partial\|+\|\aleph\|)$	$O(\mathbb{R}_1)\|\partial\|$	Any threshold gate
[24]	$O(n)\|\partial\|$	$O(n)\|\aleph\|$	$O(\mathbb{R}_2)\|\partial\|$	$O(1)\|\partial\|$	AND gate
[25]	$O(1)\|\partial\|$	$O(1)\|\aleph\|$	$O(\mathbb{R}_2)\|\partial\|$	$O(1)\|\partial\|$	Any threshold gate
[26]	$O(n)\|\partial\|$	$O(n)\|\aleph\|$	$O(\mathbb{R}_2)\|\partial\|$	$O(1)\|\partial\|$	Any threshold gate
[27]	$O(1)\|\partial\|$	–	$O(\mathbb{R}_2)\|\partial\|$	$O(1)\|\partial\|$	AND gate
[12]	$O(1)\|\partial\|$	–	$O(\mathbb{R}_2)\|\partial\|$	$O(\mathbb{R}_1)\|\partial\|$	Any threshold gate
[13]	$O(1)\|\partial\|$	$O(1)\|\partial\|$	$O(\mathbb{R}_2)\|\partial\|$	$O(n')\|\partial\|$	Any threshold gate
[14]	–	–	$O(n)\|\partial\|$	$O(\mathbb{R}_1)\|\partial\|$	Any threshold gate
[15]	–	–	$O(n)\|\aleph\|$	$O(\mathbb{R}_1)\|\aleph\|$	Any threshold gate
[16]	–	–	$O(n)\|\aleph\|$	$O(\mathbb{R}_1)\|\aleph\|$	Any threshold gate
Our Work	$O(n)\|\partial\|$	$O(1)\|\partial\|$	$O(\mathbb{R}_2)\|\partial\|$	$O(1)\|\partial\|$	AND gate

Table 2. Time based analysis of the CP-ABE scheme.

Scheme	Encryption	Decryption
[9]	$O(\mathbb{R}_1)T_{Exp}+O(1)T_{Mul}$	$O(\mathbb{R}_1)\left(T_{Exp}+T_{Mul}+T_{Pairing}\right)$
[10]	$O(\mathbb{R}_1)\left(T_{Exp}+T_{Mul}+T_{Pairing}\right)$	$O(\mathbb{R}_1)\left(T_{Exp}+T_{Mul}+T_{Pairing}\right)$
[11]	$O(1)T_{Exp}+O(n)\left(T_{Mul}+T_{Pairing}\right)$	$O(n)\left(T_{Mul}+T_{Pairing}\right)$
[28]	$O(n'\mathbb{R}_1)T_{Exp}+O(\mathbb{R}_1)T_{Mul}$	$O(\mathbb{R}_1)T_{Mul}+O(1)T_{Pairing}$
[29]	$O(1)\left(T_{Exp}+T_{Mul}+T_{Pairing}\right)$	$O(\mathbb{R}_1)\left(T_{Mul}+T_{Pairing}\right)$
[17]	$O(\mathbb{R}_1)T_{Exp}+O(1)T_{Mul}$	$O(\mathbb{R}_1)\left(T_{Exp}+T_{Mul}+T_{Pairing}\right)$
[18]	$O(\mathbb{R}_1)T_{Exp}+O(1)T_{Mul}$	$O(\mathbb{R}_1)\left(T_{Exp}+T_{Mul}+T_{Pairing}\right)$
[19]	$O(\mathbb{R}_1)T_{Exp}+O(1)T_{Mul}$	$O(n)\left(T_{Mul}+T_{Pairing}\right)$
[23]	$O(n)T_{Exp}+O(\mathbb{R}_1)T_{Mul}$	$O(\mathbb{R}_1)T_{Mul}+O(1)T_{Pairing}$
[24]	$O(n)\left(T_{Mul}+T_{Pairing}\right)$	$O(1)\left(T_{Exp}+T_{Pairing}\right)$
[25]	$O(n)\left(T_{Mul}+T_{Pairing}\right)$	$O(1)\left(T_{Exp}+T_{Pairing}\right)$
[26]	$O(n)\left(T_{Mul}+T_{Pairing}\right)$	$O(1)\left(T_{Exp}+T_{Pairing}\right)$
[27]	$O(\mathbb{R}_1)T_{Exp}+O(1)T_{Mul}$	$O(\mathbb{R}_1)\left(T_{Exp}+T_{Pairing}\right)$
[12]	$O(1)T_{Exp}+O(n)\left(T_{Mul}+T_{Pairing}\right)$	$O(n)\left(T_{Mul}+T_{Pairing}\right)$
[13]	$O(n'\mathbb{R}_1)T_{Exp}+O(\mathbb{R}_1)T_{Mul}$	$O(\mathbb{R}_1)T_{Mul}+O(1)T_{Pairing}$
[14]	$O(1)\left(T_{Exp}+T_{Mul}+T_{Pairing}\right)$	$O(\mathbb{R}_1)\left(T_{Mul}+T_{Pairing}\right)$
[15]	$O(n)\left(T_{Mul}+T_{Pairing}\right)$	$O(n)\left(T_{Exp}+T_{Pairing}\right)$
[16]	$O(n)\left(T_{Mul}+T_{Pairing}\right)$	$O(n)\left(T_{Exp}+T_{Pairing}\right)$
Our work	$O(1)T_{Exp}+O(\mathbb{R}_1)T_{Mul}$	$O(\mathbb{R}_1)T_{Mul}+O(1)T_{Pairing}$

RKGen(MPK,W,W',SK_L): This will generate proxy re-encryption key by the user.

- Generates $d, g_1 \in_R Z_p$.
- Gets $C = Encrypt\left(MPK, g_1^{nd}, W'\right)$
- Gets $R = D \prod_{v_{i,j} \in AS} (D_{i,j} g_1^d)$
- $RK_{AS \to W'} = \langle C, R, g^r \rangle$

RequestAttributeSK(PK_u,u, L_u): Attribute Authority run this algorithm to generate the corresponding parameters of the user's secret key.

- It gets $D_i = (g^r)^{\alpha_i}$

Table 3. Feature based comparative analysis of CP-ABE schemes.

Approach	F1	F2	F3	F4
[9]	✔	×	×	×
[10]	✔	×	×	×
[11]	✔	×	×	×
[28]	✔	×	×	×
[29]	✔	×	×	×
[17]	×	✔	×	×
[18]	×	✔	×	×
[19]	×	✔	×	×
[23]	×	✔	×	×
[24]	×	×	✔	✔
[25]	×	×	✔	×
[26]	×	×	✔	×
[27]	✔	×	✔	✔
[12]	×	×	×	✔
[13]	×	×	×	✔
[14]	×	×	×	✔
[15]	×	×	×	✔
[16]	×	×	×	✔
Our scheme	✔	✔	✔	✔

Table 4. Time based analysis of CP-ABE Scheme (in ms).

Scheme	KeyGen	Encryption	Decryption
[9]	1125	27584	56857
[26]	2124	36548	63548
[27]	1325	25426	45639
[16]	2415	56254	75846
Our scheme	1054	11254	34562

- It gets $L_u = L_u + i$
- Give D_i and L_u to as output to the user

Encrypt(M,W,PK$_1$,PK$_2$,…,PK$_N$): Sender runs this algorithm to generate ciphertext.

- Chooses exponent $s \in_R Z_p$.
- Gets $C_1 = MY^s$
- Gets $C_2 = g^s$
- Gets $C_3 = \left(\prod_{t\in W} PK_i\right)^s = \left(\prod_{t\in W} g^{\alpha_i}\right)^s$
- Gets $C_4 = (h)^s = g^{\mathcal{E}s}$
- Ciphertext $CT = \{C_1, C_2, C_3, C_4, W\}$

RKEncrypt(CT_W,$RK_{AS\to W'}$**):** Proxy server converts CT_W to $CT_{W'}$ in this algorithm.

- $C' = \frac{C_1\ e(C_2,g^r)}{e(C_3,R)} = \frac{M}{e(g,g_1)^{nsd\mathcal{E}}}$
- $CT_{W'} = \langle C', C, C_3\rangle$

Decrypt(SK,CT): User runs to get decryption of the ciphertext

If **CT** is actual ciphertext then do

$$= \frac{C_1 \cdot e(g^r, C_2) \cdot e(C_3, g^r)}{e\left(C_4, g^{\frac{y+r}{\mathcal{E}}}\right) \cdot e\left(C_2, \left(\prod_{t\in AS} g^{\alpha_t}\right)^r\right)}$$
$$= M$$

If **CT** is generated from proxy server than user will follow

- $g_1^{nd} = Decrypt(SK, CT)$
- $= \frac{M\ e(C_3,g_1^{nd})}{e(g,g_1)^{nsd\mathcal{E}}}$
- $= M$

5. Performance analysis

In this part, we have analyzed the proposed scheme against earlier schemes on various parameters. In table 1, we have given the comparative analysis against size of various parameters. In table 1, $\mathbb{R}_1$ presents total CT attributes, $\mathbb{R}_2$ represents total SK attributes, $|\aleph|$ presents single Z element bit-length, $|\partial|$ presents single G element bit-length, $\boldsymbol{n}$ presents total system attributes and $\boldsymbol{n'}$ presents total gates in the policy. In table 2, we have given the practical analysis based on encryption and decryption time. In table 2, $\boldsymbol{T_{Exp}}$ presents single exponent time, $\boldsymbol{T_{mul}}$ presents single multiplication time, $\boldsymbol{T_{pairing}}$ presents single pairing time. table 3 represents the feature-based analysis where F1 represents Multi Authority, F2 represents Traceability, F3 represents Constant Length Ciphertext and F4 represents Proxy Re-Encryption. For practical implementation, we have implemented the proposed as well as earlier scheme using Pairing Based Cryptography (PBC) library with type A curve on the Intel Core i7 processor with 4GB RAM. Timings are as follows Bilinear Pairing (18 ms), Exponent in G (9 ms), Exponent in Z (2 ms), Multiplication/Division/Inversion (1ms), Hashing (3 ms) (table 4).

6. Conclusion

Attribute based technology is the compelling strategy for the multicasting. In any case, the naïve scheme encounters different problems like key delectability as well as ciphertext length. The authors have mentioned the various designs for all of the part (anyway arrangement gave these components). Thus, this paper mentioned arrangement to give various features (i.e. consistent ciphertext length, multi- authority, proxy re-encryption, traceability) which make the proposed scheme to be useful in various circumstances when compared to previous approaches. One

can improvise the mentioned approach to support the consistent length secret key.

References

[1] Rivest R L, Shamir A and Adleman L 1978 A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 21: 120–126.

[2] Shamir A 1984 Identity-based cryptosystems and signature schemes. In: *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, pp. 47–53

[3] Sahai A and Waters B 2005 Fuzzy identity-based encryption. In: *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques,* pp. 457–473

[4] Goyal V, Pandey O, Sahai A and Waters B 2006 Attribute-based encryption for fine-grained access control of encrypted data. In: *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 89–98

[5] Bethencourt J, Sahai A and Waters B 2007 Ciphertext-policy attribute-based encryption. In: *Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP'07),* pp. 321–334

[6] Garg S, Gentry C, Halevi S, Sahai A and Waters B 2013 Attribute-based encryption for circuits from multilinear maps. In: *Proceedings of the Annual Cryptology Conference*, pp. 479–499

[7] Chase M 2007 Multi-authority attribute based encryption. In: *Theory of Cryptography Conference*, pp. 515–534

[8] Muller S, Katzenbeisser S and Eckert C 2009 On multi-authority ciphertext-policy attribute-based encryption. *Bull. Korean Math. Soc.* 46: 803–819

[9] Gorasia N, Srikanth R R, Doshi N and Rupareliya J 2016 Improving security in multi authority attribute based encryption with fast decryption. *Procedia Comput. Sci.* 79: 110–116

[10] Božović V, Socek D, Steinwandt R and Villányi V I 2012 Multi-authority attribute-based encryption with honest-but-curious central authority. *Int. J. Comput. Math.* 89: 268–283

[11] Lin H, Cao Z, Liang X, and Shao J, 2008 Secure threshold multi authority attribute based encryption without a central authority. In: *Proceedings of the International Conference on Cryptology in India*, pp. 426–436

[12] Zhang X and Yin Y 2019 Research on digital copyright management system based on blockchain technology. In: *Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, pp. 2093–2097

[13] Xu Z, Shen J, Luo P and Liang F 2020 PVcon: localizing hidden concurrency errors with prediction and verification. *IEEE Access* 8: 165373–165386

[14] Shen J, Deng X and Xu Z 2019 Multi-security-level cloud storage system based on improved proxy re-encryption. *EURASIP J. Wirel. Commun. Netw.* 2019: 277–289

[15] Xu Z, Shen J, Liang F and Chen Y 2021 Fine-grained access control scheme based on improved proxy re-encryption in cloud. *J. Adv. Comput. Intell. Intell. Inform.* 25: 170–176

[16] Pareek G and Purushothama B R 2021 KAPRE: key-aggregate proxy re-encryption for secure and flexible data sharing in cloud storage. *J. Inf. Secur. Appl.* 63: 103009

[17] Liu Z, Cao Z and Wong D S 2012 White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. *IEEE Trans. Inf. Forensics Secur.* 8: 76–88

[18] Ning J, Cao Z, Dong X, Wei L and Lin X 2014 Large universe ciphertext-policy attribute-based encryption with white-box traceability. In: *Proceedings of the European Symposium on Research in Computer Security*, pp. 55–72

[19] Zhang Y, Li J, Zheng D, Chen X and Li H 2016 Accountable large-universe attribute-based encryption supporting any monotone access structures. In: *Proceedings of the Australasian Conference on Information Security and Privacy,* pp. 509–524

[20] Odelu V, Das A K, Rao Y S, Kumari S, Khan M K and Choo K-KR 2017 Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment. *Comput. Stand. Interfaces* 54: 3–9

[21] Odelu V, Das A K, Khan M K, Choo K-KR and Jo M 2017 Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts. *IEEE Access* 5: 3273–3283

[22] Odelu V and Das A K 2016 Design of a new CP-ABE with constant size secret keys for lightweight devices using elliptic curve cryptography. *Secur. Commun. Netw.* 9: 4048–4059

[23] Wang G, Li F, Wang P and Hu Y 2021 Traceable ciphertet-policy attribute-based encryption with constant decryption. *KSII Trans. Internet Inf. Syst.* 15: 3401–3420

[24] Doshi N 2022 An enhanced approach for CP-ABE with proxy re-encryption in IoT paradigm. *Jordan. J. Comput. Inf. Technol.* 1–10

[25] Zhang Z, Zhang W and Qin Z 2021 Fully constant-size CP-ABE with privacy-preserving outsourced decryption for lightweight devices in cloud-assisted IoT. *Secur. Commun. Netw.* 2021: 1–16

[26] Zhang Z and Zhou S 2021 A decentralized strongly secure attribute-based encryption and authentication scheme for distributed Internet of Mobile Things. *Comput. Netw.* 201: 108553

[27] Nishant D and Reema P 2022 An improved approach in CP-ABE with proxy re-encryption, in e-Prime-Advances in electrical engineering. *Electron. Energy* 100042

[28] Lewko A and Waters B 2011 Decentralizing attribute-based encryption. In: *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 568–588

[29] Müller S, Katzenbeisser S and Eckert C 2008 Distributed attribute-based encryption. In: *International Conference on Information Security and Cryptology*, pp. 20–36

[30] Lewko A, Okamoto T, Sahai A, Takashima K and Waters B 2010 Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 62–91

[31] Boneh D and Boyen X 2004 Short signatures without random oracles. In: *Proceedings of the International*

Conference on the Theory and Applications of Cryptographic Techniques, pp. 56–73

[32] Rouselakis Y and Waters B 2013 Practical constructions and new proof methods for large universe attribute-based encryption. In: *Proceedings of the ACM SIGSAC Conference on Computer & Communications Security*, pp. 463–474

[33] Blaze M, Bleumer G and Strauss M 1998 Divertible protocols and atomic proxy cryptography. In: *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 127–144

[34] Mambo M and Okamoto E 1997 Proxy cryptosystems: Delegation of the power to decrypt ciphertexts. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* 80: 54–63

[35] Ateniese G, Fu K, Green M and Hohenberger S 2006 Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Trans. Inf. Syst. Secur.* 9: 1–30

[36] Green M and Ateniese G 2007 Identity-based proxy re-encryption. In: *Proceedings of the International Conference on Applied Cryptography and Network Security*, pp. 288–306

[37] Matsuo T 2007 Proxy re-encryption systems for identity-based encryption. In: *Proceedings of the International Conference on Pairing-Based Cryptography*, pp. 247–267

[38] Guo S, Zeng Y, Wei J and Xu Q 2008 Attribute-based re-encryption scheme in the standard model. *Wuhan Univ. J. Nat. Sci.* 13: 621–625

[39] Liang X, Cao Z, Lin H and Shao J 2009 Attribute based proxy re-encryption with delegating capabilities. In: *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, pp. 276–28

[40] Ibraimi L, Asim M and Petković M 2010 An encryption scheme for a secure policy updating. In: *Proceedings of the International Conference on E-Business and Telecommunications,* pp. 304–318

[41] Luo S, Hu J and Chen Z 2010 Ciphertext policy attribute-based proxy re-encryption. In: *Proceedings of the International Conference on Information and Communications Security*, pp. 401–415

[42] Emura K, Miyaji A, Nomura A, Omote K and Soshi M 2009 A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In: *Proceedings of the International Conference on Information Security Practice and Experience*, pp. 13–23

[43] Herranz J, Laguillaumie F and Ràfols C 2010 Constant size ciphertexts in threshold attribute-based encryption. In: *Proceedings of the International Workshop on Public Key Cryptography*, pp. 19–34

[44] Delerablée C and Pointcheval D 2008 Dynamic threshold public-key encryption. In: *Proceedings of the Annual International Cryptology Conference,* pp. 317–334