**REFERENCES**

[1] D. Song, E. Shi, I. Fischer, and U. Shankar, “Cloud data protection

for the masses,” Computer, vol. 45, no. 1, pp. 39–45, 2012.

[2] J. Yu, K. Ren, and C. Wang, “Enabling cloud storage auditing

with verifiable outsourcing of key updates,” IEEE Transactions on

Information Forensics and Security, vol. 11, no. 6, pp. 1362–1375,

2016.

[3] H. Yin, Z. Qin, J. Zhang, L. Ou, and K. Li, “Achieving secure,

universal, and fine-grained query results verification for secure

search scheme over encrypted cloud data,” IEEE Transactions on

Cloud Computing, 2017.

[4] K. Li, W. Zhang, C. Yang, and N. Yu, “Security analysis on one-tomany

order preserving encryption-based cloud data search,” IEEE

Transactions on Information Forensics and Security, vol. 10, no. 9, pp.

1918–1926, 2015.

[5] R. Zhang, R. Xue, and L. Liu, “Searchable encryption for healthcare

clouds: a survey,” IEEE Transactions on Services Computing,

vol. 11, no. 6, pp. 978–996, 2018.

[6] D. Boneh and M. Franklin, “Identity-based encryption from the

weil pairing,” SIAM Journal on Computing, vol. 32, no. 3, pp. 586–

615, 2003.

[7] J. Wei, W. Liu, and X. Hu, “Secure data sharing in cloud computing

using revocable-storage identity-based encryption,” IEEE

Transactions on Cloud Computing, 2016.

[8] D. He, N. Kumar, H. Wang, L. Wang, K.-K. R. Choo, and

A. Vinel, “A provably-secure cross-domain handshake scheme

with symptoms-matching for mobile healthcare social network,”

IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4,

pp. 633–645, 2018.

[9] C. Delerabl´ee, “Identity-based broadcast encryption with constant

size ciphertexts and private keys,” in International Conference on

the Theory and Application of Cryptology and Information Security.

Springer, 2007, pp. 200–215.

[10] H. Deng, Q.Wu, B. Qin,W. Susilo, J. Liu, andW. Shi, “Asymmetric

cross-cryptosystemre-encryption applicable to efficient and secure

mobile access to outsourced data,” in Proceedings of the 10th ACM

Symposium on Information, Computer and Communications Security.

ACM, 2015, pp. 393–404.

[11] J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, “Anonymous

identity-based broadcast encryption with revocation for file sharing,”

in Australasian Conference on Information Security and Privacy.

Springer, 2016, pp. 223–239.

[12] J. Lai, Y. Mu, F. Guo, and R. Chen, “Fully privacy-preserving

id-based broadcast encryption with authorization,” The Computer

Journal, vol. 60, no. 12, pp. 1809–1821, 2017.

[13] W. Susilo, R. Chen, F. Guo, G. Yang, Y. Mu, and Y.-W. Chow,

“Recipient revocable identity-based broadcast encryption: how

to revoke some recipients in ibbe without knowledge of the

plaintext,” in Proceedings of the 11th ACM on Asia Conference on

Computer and Communications Security. ACM, 2016, pp. 201–210.

[14] J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, “Fully privacypreserving

and revocable id-based broadcast encryption for data

access control in smart city,” Personal and Ubiquitous Computing,

vol. 21, no. 5, pp. 855–868, 2017.

[15] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and

atomic proxy cryptography,” in EUROCRYPT 1998. Springer

Berlin Heidelberg, 1998, pp. 127–144.

[16] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved

proxy re-encryption schemes with applications to secure distributed

storage,” Information and System Security (TISSEC), ACM

Transactions on, vol. 9, no. 1, pp. 1–30, 2006.

[17] B. Libert and D. Vergnaud, “Unidirectional chosen-ciphertext secure

proxy re-encryption,” in PKC 2008. Springer Berlin Heidelberg,

2008, pp. 360–379.

[18] Z. Cao, H. Wang, and Y. Zhao, “Ap-pre: Autonomous path proxy

re-encryption and its application,” IEEE Transactions on Dependable

and Secure Computing, 2017.

[19] H. Guo, Z. Zhang, J. Xu, N. An, and X. Lan, “Accountable

proxy re-encryption for secure data sharing,” IEEE Transactions on

Dependable and Secure Computing, 2018.

[20] M. Green and G. Ateniese, “Identity-based proxy re-encryption,”

in ACNS 2007. Springer Berlin Heidelberg, 2007, pp. 288–306.

[21] C. K. Chu and W. G. Tzeng, “Identity-based proxy re-encryption

without random oracles,” in ISC 2007. Springer Berlin Heidelberg,

2007, pp. 189–202.

[22] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, “An efficient cloudbased

revocable identity-based proxy re-encryption scheme for

public clouds data sharing,” in European Symposium on Research

in Computer Security. Springer, 2014, pp. 257–272.

[23] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, “Conditional identitybased

broadcast proxy re-encryption and its application to cloud

email,” IEEE Transactions on Computers, vol. 65, no. 1, pp. 66–79,

2016.

[24] K. Liang, M. H. Au, J. K. Liu,W. Susilo, D. S.Wong, G. Yang, Y. Yu,

and A. Yang, “A secure and efficient ciphertext-policy attributebased

proxy re-encryption for cloud data sharing,” Future Generation

Computer Systems, vol. 52, pp. 95–108, 2015.

[25] C. Ge, W. Susilo, L. Fang, J. Wang, and Y. Shi, “A cca-secure

key-policy attribute-based proxy re-encryption in the adaptive

corruption model for dropbox data sharing system,” Designs,

Codes and Cryptography, pp. 1–17, 2018.