**REFERENCES**

[1] Joseph A Akinyele, Christina Garman, Ian Miers, Matthew W

Pagano, Michael Rushanan, Matthew Green, and Aviel D Rubin.

Charm: a framework for rapidly prototyping cryptosystems. Journal

of Cryptographic Engineering, 3(2):111–128, 2013.

[2] Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata.

Innovative technology for cpu based attestation and sealing. In

Workshop on hardware and architectural support for security and privacy

(HASP), volume 13, page 7. ACM New York, NY, USA, 2013.

[3] Alexandros Bakas and Antonis Michalas. Modern family: A revocable

hybrid encryption scheme based on attribute-based encryption,

symmetric searchable encryption and SGX. In SecureComm

2019, pages 472–486, 2019.

[4] Amos Beimel. Secure schemes for secret sharing and key distribution.

PhD thesis, PhD thesis, Israel Institute of Technology, Technion,

Haifa, Israel, 1996.

[5] John Bethencourt, Amit Sahai, and BrentWaters. Ciphertext-policy

attribute-based encryption. In S&P 2007, pages 321–334. IEEE,

2007.

[6] Victor Costan and Srinivas Devadas. Intel sgx explained. IACR

Cryptology ePrint Archive, 2016(086):1–118, 2016.

[7] Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, and Sergey

Gorbunov. IRON: functional encryption using intel SGX. In

Proceedings of the 2017 ACM SIGSAC Conference on Computer and

Communications Security, CCS 2017, pages 765–782, 2017.

[8] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of

asymmetric and symmetric encryption schemes. In Advances in

Cryptology-CRYPTO 1999, pages 537–554. Springer, 1999.

[9] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters.

Attribute-based encryption for fine-grained access control of encrypted

data. In ACM CCS 2006, pages 89–98. ACM, 2006.

[10] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man

Ho Allen Au. Improving privacy and security in decentralized

ciphertext-policy attribute-based encryption. IEEE transactions on

information forensics and security, 10(3):665–678, 2015.

[11] Christofer Hoff. Cloud computing security: From ddos (distributed

denial of service) to edos (economic denial of sustainability).

http://www. rationalsurvivability.com/blog/?p=66.

[12] Joseph Idziorek, Mark Tannian, and Doug Jacobson. Attribution

of fraudulent resource consumption in the cloud. In IEEE CLOUD

2012, pages 99–106. IEEE, 2012.

[13] Simon Johnson, Vinnie Scarlata, Carlos Rozas, Ernie Brickell, and

Frank Mckeen. IntelR software guard extensions: Epid provisioning

and attestation services. White Paper, 1:1–10, 2016.

[14] Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon

Kim, and Marcus Peinado. Inferring fine-grained control flow

inside sgx enclaves with branch shadowing. In 26th USENIX

Security Symposium, USENIX Security, pages 16–18, 2017.

[15] Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. Ksfoabe:

outsourced attribute-based encryption with keyword search

function for cloud storage. IEEE Transactions on Services Computing,

10(5):715–725, 2017.

[16] Jiguo Li, Yao Wang, Yichen Zhang, and Jinguang Han. Full

verifiability for outsourced decryption in attribute based

encryption. IEEE Transactions on Services Computing, DOI:

10.1109/TSC.2017.2710190, 2017.

[17] Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong. Tmacs:

A robust and verifiable threshold multi-authority access control

system in public cloud storage. IEEE Transactions on parallel and

distributed systems, 27(5):1484–1496, 2016.

[18] Ben Lynn et al. The pairing-based cryptography library. Internet:

crypto. stanford. edu/pbc/[Mar. 27, 2013], 2006.

[19] Frank McKeen, Ilya Alexandrovich, Alex Berenzon, Carlos V.

Rozas, Hisham Shafi, Vedvyas Shanbhogue, and Uday R. Savagaonkar.

Innovative instructions and software model for isolated

execution. In HASP@ISCA 2013, page 10, 2013.

[20] Antonis Michalas. The lord of the shares: combining attributebased

encryption and searchable encryption for flexible data sharing.

In SAC 2019, pages 146–155, 2019.

[21] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma,

and Lifei Wei. Auditable \_-time outsourced attribute-based encryption

for access control in cloud computing. IEEE Transactions

on Information Forensics and Security, 13(1):94–105, 2018.

[22] Jianting Ning, Zhenfu Cao, Xiaolei Dong, and LifeiWei. White-box

traceable CP-ABE for cloud storage service: How to catch people

leaking their access credentials effectively. IEEE Transactions on

Dependable and Secure Computing, 15(5):883–897, 2018.

[23] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Lifei Wei, and Xiaodong

Lin. Large universe ciphertext-policy attribute-based encryption

with white-box traceability. In Computer Security-ESORICS 2014,

pages 55–72. Springer, 2014.

[24] Jianting Ning, Xiaolei Dong, Zhenfu Cao, and Lifei Wei. Accountable

authority ciphertext-policy attribute-based encryption

with white-box traceability and public auditing in the cloud. In

Computer Security–ESORICS 2015, pages 270–289. Springer, 2015.

[25] Jianting Ning, Xiaolei Dong, Zhenfu Cao, Lifei Wei, and Xiaodong

Lin. White-box traceable ciphertext-policy attribute-based encryption

supporting flexible attributes. IEEE Transactions on Information

Forensics and Security, 10(6):1274–1288, 2015.