**REFERENCES**

[1] M. Y. Becker, C. Fournet, and A. D. Gordon, “SecPAL: Design and Semantics of a Decentralized Authorization Language,” in Journal of Computer Security (JCS), 2010, pp. 597–643.

[2] M. Blaze, J. Ioannidis, and A. D. Keromytis, “TrustManagement for IPsec,” in ACM Transactions on Information and System Security (TISSEC), 2002.

[3] N. Li, B. N. Grosof, and J. Feigenbaum, “Delegation logic: A Logic-based Approach to Distributed Authorization,” in TISSEC, 2003.

[4] C. Soriente, G. O. Karame, H. Ritzdorf, S. Marinovic, and S. Capkun, “Commune: Shared ownership in an agnostic cloud,” ser. SACMAT ’15, 2015.

[5] “Amazon Simple Storage Service(S3),” http://aws.amazon.com/s3/.

[6] S. Ceri, G. Gottlob, and L. Tanca, “What you always wanted to know about Datalog (and never dared to ask),” in Knowledge and Data Engineering, IEEE Transactions on, 1989.

[7] Y. Gurevich and I. Neeman, “DKAL: Distributed-Knowledge Authorization Language ,” in CSF ’08.

[8] J. DeTreville, “Binder, a Logic-based Security Language,” in Proceedings of IEEE Symposium on Security and Privacy, 2002, pp. 105 – 113.

[9] “The Respect Network,” https://www.respectnetwork.com/.

[10] “WDMy Cloud,” <http://www.wdc.com/en/products/products.aspx?id=1140>.

[11] M. O. Rabin, “Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance,” in Journal of the Association for Computing Machinery.

[12] J. K. Resch and J. S. Plank, “AONT-RS: Blending Security and Performance in Dispersed Storage Systems,” in FAST, 2011.

[13] R. L. Rivest, “All-or-Nothing Encryption and the Package Transform,” in International Workshop on Fast Software Encryption (FSE), 1997.

[14] V. Boyko, “On the Security Properties of OAEP as an All-or-nothing Transform,” in Procedings of CRYPTO, 1999, pp. 503–518.

[15] J. Daemen, and V. Rijmen, “AES Proposal: Rijndael,” http:

//csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf.

[16] J. H. van Lint, Introduction to Coding Theory. Secaucus, NJ, USA:

Springer-Verlag New York, Inc., 1982.

[17] M. vanDijk,A. Juels,A.Oprea,R. L.Rivest, E. Stefanov, andN. Triandopoulos, “Hourglass Schemes: how to prove that cloud files are encrypted,” in CCS, 2012.

[18] A. B. Lewko and B.Waters, “Decentralizing Attribute-Based Encryption,” in EUROCRYPT, 2011.

[19] P. Rogaway and M. Bellare, “Robust computational secret sharing and a unified account of classical secret-sharing goals,” in CCS, 2007.

[20] C. Charnes, J. Pieprzyk, and R. Safavi-Naini, “Conditionally secure secret sharing schemes with disenrollment capability,” in CCS, 1994.

[21] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.”

[22] F. Armknecht, J.-M. Bohli, G. O. Karame, Z. Liu, and C. A. Reuter,

“Outsourced proofs of retrievability,” ser. CCS ’14.

[23] F. Armknecht, J.-M. Bohli, G. O. Karame, and F. Youssef, “Transparent data deduplication in the cloud,” ser. CCS ’15, 2015.

[24] Ethereum, “A Next-Generation Smart Contract and Decentralized

Application Platform,” White Paper, Tech. Rep., 2016. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[25] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, “Town Crier: An Authenticated Data Feed for Smart Contracts,” ser. CCS ’16, 2016.

[26] D. F. Ferraiolo and D. R. Kuhn, “Role-based access controls,” in Proc. of 15th NIST-NSA National Computer Security Conference, 1992.

[27] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse attacks on bitcoin’s peer-to-peer network,” ser. SEC’15. USENIX Association, 2015.

[28] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, “Tampering with the delivery of blocks and transactions in bitcoin,” in CCS, 2015.

[29] Y. Rouselakis and B. Waters, “Efficient statically-secure large-universe multi-authority attribute-based encryption,” in Financial Cryptography and Data Security, 2015.

[30] A. Beimel, “Secret-sharing schemes: A survey,” in Third International Workshop on Coding and Cryptology (IWCC), 2011, pp. 11–46.

[31] A. Shamir, “How to Share a Secret?” in Communications of the ACM, 1979, pp. 612–613.

[32] H. Krawczyk, “Secret SharingMade Short,” in International Conference on Advances in Cryptology, 1993.

[33] H. Xia and A. A. Chien, “RobuSTore: a Distributed Storage Architecture with Robust and High Performance,” in SC, 2007.

[34] M. Abd-El-Malek, G. R. Ganger, G. R. Goodson,M. K. Reiter, and J. J.Wylie, “Fault-Scalable Byzantine Fault-Tolerant Services,” in SOSP, 2005.

[35] J. Kubiatowicz, D. Bindel, Y. Chen, S. E. Czerwinski, P. R. Eaton, D. Geels, R. Gummadi, S. C. Rhea, H.Weatherspoon,W.Weimer, C.Wells, and B. Y. Zhao, “OceanStore: An Architecture for Global-Scale Persistent Storage,” in ASPLOS, 2000.

[36] M. K. Aguilera, R. Janakiraman, and L. Xu, “Using Erasure Codes Efficiently for Storage in a Distributed System,” in DSN, 2005.

[37] G. R. Blakley and C.Meadows, “Security of ramp schemes,” in Advances in Cryptology (CRYPTO), 1984, pp. 242–268.

[38] A. Desai, “The security of all-or-nothing encryption: Protecting against exhaustive key search,” in Advances in Cryptology (CRYPTO), 2000, pp. 359–375.

[39] G. O. Karame, C. Soriente, K. Lichota, and S. Capkun, “Securing cloud data in the new attacker model,” IACR Cryptology ePrint Archive, 2014.