









## References

- [1] S. G. Akl and P. D. Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," *ACM Transactions on Computer Systems (TOCS)*, vol. 1, no. 3, pp. 239–248, 1983.
- [2] G. C. Chick and S. E. Tavares, "Flexible Access Control with Master Keys," in *Proceedings of Advances in Cryptology – CRYPTO '89*, ser. LNCS, vol. 435. Springer, 1989, pp. 316–322.
- [3] W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, vol. 14, no. 1, pp. 182–188, 2002.
- [4] G. Ateniese, A. D. Santis, A. L. Ferrara, and B. Masucci, "Provably-Secure Time-Bound Hierarchical Key Assignment Schemes," *J. Cryptology*, vol. 25, no. 2, pp. 243–270, 2012.
- [5] R. S. Sandhu, "Cryptographic Implementation of a Tree Hierarchy for Access Control," *Information Processing Letters*, vol. 27, no. 2, pp. 95–98, 1988.
- [6] Y. Sun and K. J. R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications," in *Proceedings of the 23th IEEE International Conference on Computer Communications (INFOCOM '04)*. IEEE, 2004.
- [7] Q. Zhang and Y. Wang, "A Centralized Key Management Scheme for Hierarchical Access Control," in *Proceedings of IEEE Global Telecommunication Conference (GLOBECOM'04)*. IEEE, 2004, pp. 2067–2071.
- [8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in *Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09)*. ACM, 2009, pp. 103–114.
- [9] J. Benaloh, "Key Compression and Its Application to Digital Fingerprinting," *Microsoft Research, Tech. Rep.*, 2009.
- [10] D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," in *Proceedings of Advances in Cryptology – CRYPTO '01*, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–229.
- [11] F. Guo, Y. Mu, and Z. Chen, "Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key," in *Proceedings of Pairing-Based Cryptography (Pairing '07)*, ser. LNCS, vol. 4575. Springer, 2007, pp. 392–406.