REFERENCES

[1] A. Fiat and M. Naor, “Broadcast Encryption,” in Proc. Crypto 1993, 1993, vol. LNCS 773, Lecture Notes in Computer Science, pp. 480- 491.

[2] I. Ingemarsson, D.T. Tang and C.K. Wong, “A Conference Key Distribution System,” IEEE Transactions on Information Theory, vol. 28, no. 5, pp. 714-720, 1982.

[3] Q. Wu, Y. Mu, W. Susilo, B. Qin and J. Domingo-Ferrer, “Asymmetric Group Key Agreement,” in Proc. Eurocrypt 2009, 2009, vol. LNCS 5479, Lecture Notes in Computer Science, pp. 153-170.

[4] http://en.wikipedia.org/wiki/PRISM %28surveillance program%29, 2014.

[5] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer and O. Farr`as, “Bridging Broadcast Encryption and Group Key Agreement,” in Proc. Asiacrypt 2011, 2011, vol. LNCS 7073, Lecture Notes in Computer Science, pp. 143-160.

[6] D. H. Phan, D. Pointcheval and M. Strefler, “Decentralized Dynamic Broadcast Encryption,” in Proc. SCN 2012, 2011, vol. LNCS 7485, Lecture Notes in Computer Science, pp. 166-183

[7] M. Steiner, G. Tsudik and M. Waidner, “Key Agreement in Dynamic Peer Groups,” IEEE Transactions on Parallel and Distributed Systems, vol. 11, no. 8, pp. 769-780, 2000.

[8] A. Sherman and D. McGrew, “Key Establishment in Large Dynamic Groups Using One-way Function Trees,” IEEE Transactions on Software Engineering, vol. 29, no. 5, pp. 444-458, 2003.

[9] Y. Kim, A. Perrig and G. Tsudik, “Tree-Based Group Key Agreement,” ACM Transactions on Information System Security, vol. 7, no. 1, pp. 60-96, 2004.

[10] Y. Mao, Y. Sun, M. Wu and K.J.R. Liu, “JET: Dynamic Join-Exit- Tree Amortization and Scheduling for Contributory Key Management,” IEEE/ACM Transactions on Networking, vol. 14, no. 5, pp. 1128-1140, 2006.

[11] C. Boyd and J.M. Gonz´alez-Nieto, “Round-Optimal Contributory Conference Key Agreement,” in Proc. PKC 2003, 2003, vol. LNCS 2567, Lecture Notes in Computer Science, pp. 161-174.

[12] W.-G. Tzeng and Z.-J. Tzeng, “Round Efficient Conference Key Agreement Protocols with Provable Security,” in Proc. Asiacrypt 2000, 2000, vol. LNCS 1976, Lecture Notes in Computer Science, pp. 614-627.

[13] R. Dutta and R. Barua, “Provably Secure Constant Round Contributory Group Key Agreement in Dynamic Setting,” IEEE Transactions on Information Theory, vol. 54, no. 5, 2007-2025, 2008.

[14] W.-G. Tzeng, “A Secure Fault-Tolerant Conference-Key Agreement Protocol,” IEEE Transactions on Computers, vol. 51, no.4, pp. 373-379, 2002.

[15] X. Yi, “Identity-Based Fault-Tolerant Conference Key Agreement,” IEEE Transactions Dependable Secure Computing vol. 1, no. 3, 170- 178, 2004.

[16] M. Burmester and Y. Desmedt, “A Secure and Efficient Conference Key Distribution System,” in Proc. Eurocrypt 1994, 1994, vol. LNCS 950, Lecture Notes in Computer Science, pp. 275-286.

[17] A. Joux, “A One Round Protocol for Tripartite Diffie-Hellman,” Journal of Cryptology, vol. 17, no. 4, pp. 263-276, 2004.

[18] D. Boneh and A. Silverberg, “Applications of Multilinear Forms to Crytography,” Contemporary Mathematics, vol. 324, pp.71-90, 2003.

[19] E. Bresson, O. Chevassut and D. Pointcheval, “Provably Authenticated Group Diffie-Hellman Key Exchange – The Dynamic Case,” in Proc. Asiacrypt 2001, 2001, vol. LNCS 2248, Lecture Notes in Computer Science, pp. 290-309

[20] E. Bresson, O. Chevassut and D. Pointcheval, “Dynamic Group Diffie- Hellman Key Exchange under Standard Assumptions,” in Proc. Eurocrypt 2002, 2002, vol. LNCS 2332, Lecture Notes in Computer Science, pp. 321-336.

[21] E. Bresson, O. Chevassut, D. Pointcheval and J.-J. Quisquater, “Provably Authenticated Group Diffie-Hellman Key Exchange,” in Proc. ACM CCS 2001, 2001, pp. 255-264.

[22] J. Snoeyink, S. Suri and G. Varghese, “A Lower Bound for Multicast Key Distribution,” in Proc. INFOCOM 2001, 2001, pp. 422-431.

[23] H.J. Kim, S.M. Lee and D. H. Lee, “Constant-Round Authenticated Group Key Exchange for Dynamic Groups,” in Proc. Asiacrypt 2004, 2004, vol. LNCS 3329, Lecture Notes in Computer Science, pp. 245- 259.

[24] M. Abdalla, C. Chevalier, M. Manulis and D. Pointcheval, “Flexible Group Key Exchange with On-demand Computation of Subgroup Keys,” in Proc. Africacrypt 2010, 2010, vol. LNCS 6055, Lecture Notes in Computer Science, pp. 351-368. [25] S. Jarecki, J. Kim and G. Tsudik, “Flexible Robust Group Key Agreement,” IEEE Transactions on Parallel Distributed Systetems, vol. 22, no. 5, pp. 879-886, 2011.

[26] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer and J. Manj´on, “Fast Transmission to Remote Cooperative Groups: A New Key Management Paradigm,” IEEE/ACM Transactions on Networking, vol. 21, no. 2, pp. 621-633, 2013.

[27] E. Bertino, N. Shang and S.S. Wagstaff Jr., “An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting,” IEEE Transactions on Dependable Secure Computing, vol. 5, no. 2, 65-70, 2008

[28] A. Shoufan and S.A. Huss, “High-Performance Rekeying Processor Architecture for Group Key Management,” IEEE Transactions on Computers, vol. 58, no. 10, 1421-1434, 2009.

[29] W. Gu, S. Chellappan, X. Bai and H. Wang, “Scaling Laws of Key Predistribution Protocols in Wireless Sensor Networks,” IEEE Transactions on Information Forensics and Security, vol. 6, no. 4, 1370-1381, 2011.

[30] M.-H. Park, G.-P. Gwon, S.-W. Seo and H.-Y. Jeong, “RSU-Based Distributed Key Management (RDKM) For Secure Vehicular Multicast Communications,” IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 644-658, 2011.