[55] Wojciech Jamroga, Peter B. Rønne, Peter Y. A. Ryan, and Philip B. Stark. 2019. Risk-Limiting Tallies. In *E-Vote-ID 2019, Proceedings (LNCS, Vol. 11759)*. Springer, 183–199.

[56] A. Juels, D. Catalano, and M. Jakobsson. 2005. Coercion-Resistant Electronic Elections. In *Proceedings of Workshop on Privacy in the Eletronic Society (WPES 2005)*. ACM Press, 61–70.

[57] Sanket Kanjalkar, Ye Zhang, Shreyas Gandlur, and Andrew Miller. 2021. Publicly Auditable MPC-as-a-Service with succinct verification and universal setup. In *IEEE European Symposium on Security and Privacy Workshops, EuroS&P 2021, Vienna, Austria, September 6-10, 2021*. IEEE, 386–411.

[58] Aggelos Kiayias, Annabell Kuldmaa, Helger Lipmaa, Janno Siim, and Thomas Zacharias. 2018. On the Security Properties of e-Voting Bulletin Boards. In *SCN 2018, Proceedings*. 505–523.

[59] Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang. 2015. DEMOS-2: Scalable E2E Verifiable Elections without Random Oracles. In *CCS 2015*. 352–363.

[60] Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang. 2015. End-to-End Verifiable Elections in the Standard Model. In *EUROCRYPT 2015*. 468–498.

[61] Ahmed Kosba, Zhichao Zhao, Andrew Miller, Yi Qian, Hubert Chan, Charalampos Papamanthou, Rafael Pass, Elaine Shi, et al. 2015. C∅C∅: A Framework for Building Composable Zero-Knowledge Proofs. *Cryptology ePrint Archive* (2015).

[62] Ralf Küsters, Julian Liedtke, Johannes Müller, Daniel Rausch, and Andreas Vogt. 2020. Ordinos: A Verifiable Tally-Hiding Remote E-Voting System. In *IEEE EuroS&P 2020*.

[63] R. Küsters, J. Müller, E. Scapin, and T. Truderung. 2016. sElect: A Lightweight Verifiable Remote Voting System. In *CSF 2016*. 341–354.

[64] R. Küsters and T. Truderung. 2016. Security Analysis of Re-Encryption RPC Mix Nets. In *IEEE EuroS&P 2016*. IEEE Computer Society, 227–242.

[65] R. Küsters, T. Truderung, and A. Vogt. 2010. Accountability: Definition and Relationship to Verifiability. In *ACM CCS 2010*. 526–535.

[66] R. Küsters, T. Truderung, and A. Vogt. 2011. Verifiability, Privacy, and Coercion-Resistance: New Insights from a Case Study. In *IEEE S&P 2011*. 538–553.

[67] R. Küsters, T. Truderung, and A. Vogt. 2012. Clash Attacks on the Verifiability of E-Voting Systems. In *IEEE S&P 2012*. 395–409.

[68] R. Küsters, T. Truderung, and A. Vogt. 2014. Formal Analysis of Chaumian Mix Nets with Randomized Partial Checking. In *S&P 2014*. 343–358.

[69] Jiwon Lee, Jaekyoung Choi, Jihye Kim, and Hyunok Oh. 2019. SAVER: Snark-friendly, Additively-homomorphic, and Verifiable Encryption and decryption with Rerandomization. *IACR Cryptol. ePrint Arch.* 2019 (2019), 1270.

[70] Maine State Legislature. 2020. Ranked Choice Voting in Maine. http://legislature.maine.gov/lawlibrary/ranked-choice-voting-in-maine/9509.

[71] Mary Maller, Sean Bowe, Markulf Kohlweiss, and Sarah Meiklejohn. 2019. Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updatable Structured Reference Strings. In *Proceedings of the 2019 ACM CCS*. 2111–2128.

[72] David Mesten, Johannes Müller, and Pascal Reisert. 2022. To appear. How Efficient are Replay Attacks against Vote Privacy? A Formal Quantitative Analysis. In *IEEE 35rd Computer Security Foundations Symposium, CSF, 2022*.

[73] NSW Government. 2020. Constitution Act No 32. https://legislation.nsw.gov.au/~/view/act/1902/32.

[74] Katsuyuki Okeya and Kouichi Sakurai. 2001. Efficient Elliptic Curve Cryptosystems from a Scalar Multiplication Algorithm with Recovery of the y-Coordinate on a Montgomery-Form Elliptic Curve. In *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings (Lecture Notes in Computer Science, Vol. 2162)*. Springer, 126–141.

[75] Alex Ozdemir and Dan Boneh. 2021. Experimenting with Collaborative zk-SNARKs: Zero-Knowledge Proofs for Distributed Secrets. *IACR Cryptol. ePrint Arch.* (2021), 1530.

[76] Bryan Parno, Jon Howell, Craig Gentry, and Mariana Raykova. 2013. Pinocchio: Nearly Practical Verifiable Computation. In *2013 IEEE Symposium on Security and Privacy, SP 2013, Berkeley, CA, USA, May 19-22, 2013*. IEEE Computer Society, 238–252.

[77] Torben P. Pedersen. 1991. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In *Proceedings of the 11th Annual International Cryptology Conference (CRYPTO 1991) (Lecture Notes in Computer Science, Vol. 576)*. Springer, 129–140.

[78] Personal communication (email) with Philip Wright, Technical Director of CES. 2020.

[79] Kim Ramchen, Chris Culnane, Olivier Pereira, and Vanessa Teague. 2019. Universally Verifiable MPC and IRV Ballot Counting. In *Financial Cryptography and Data Security - FC 2019, Revised Selected Papers (LNCS, Vol. 11598)*. Springer, 301–319.

[80] Republic of Nauru. 2016. Electoral Act No. 15. http://ronlaw.gov.nr/nauru_lpms/files/acts/d83250a1ebdc56c1701fa7aa245af5b1.pdf.

[81] scipr-lab. 2017. libsnark. https://github.com/scipr-lab/libsnark.

[82] Society for Industrial and Applied Mathematics (SIAM). 2019. SIAM Announces New 2020 Leadership. https://sinews.siam.org/Details-Page/siam-announces-new-2020-leadership-1.

[83] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman. 2014. Security Analysis of the Estonian Internet Voting System. In *Proceedings of the 2014 ACM CCS*. 703–715.

[84] Alan Szepieniec and Bart Preneel. 2015. New Techniques for Electronic Voting. *USENIX Journal of Election Technology and Systems (JETS)* 3, 2 (2015), 46 – 69.

[85] The National Archives. 2011. Greater London Authority Act 1999. https://www.legislation.gov.uk/ukpga/1999/29/contents.

[86] Roland Wen and Richard Buckland. 2009. Minimum Disclosure Counting for the Alternative Vote. In *VoteID 2009. Proceedings (LNCS, Vol. 5767)*. Springer, 122–140.

[87] S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, V. Yagati, and R. Gonggrijp. 2010. Security Analysis of India's electronic Voting Machines. In *Proceedings of the 17th ACM CCS*. 1–14.