REFERENCES

[1] Ian F Blake and Vladimir Kolesnikov. 2004. Strong conditional oblivious transfer and computing on intervals. In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 515–529.

[2] Ivan Damgård, Matthias Fitzi, Eike Kiltz, Jesper Buus Nielsen, and Tomas Toft. 2006. Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation. In *Theory of Cryptography Conference*. Springer, 285–304.

[3] Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. *Tor: The second-generation onion router*. Technical Report. Naval Research Lab Washington DC.

[4] Thomas Léauté and Boi Faltings. 2013. Protecting privacy through distributed computation in multi-agent decision making. *Journal of Artificial Intelligence Research* 47 (2013), 649–695.

[5] Daniel Lehmann, Liadan Ita Oćallaghan, and Yoav Shoham. 2002. Truth revelation in approximately efficient combinatorial auctions. *Journal of the ACM (JACM)* 49, 5 (2002), 577–602.

[6] Hsiao-Ying Lin and Wen-Guey Tzeng. 2005. An efficient solution to the millionairesâĂŹ problem based on homomorphic encryption. In *International Conference on Applied Cryptography and Network Security*. Springer, 456–466.

[7] John McMillan. 1994. Selling spectrum rights. *Journal of Economic Perspectives* 8, 3 (1994), 145–162.

[8] Silvio Micali and Michael O Rabin. 2014. Cryptography miracles, secure auctions, matching problem verification. *Commun. ACM* 57, 2 (2014), 85–93.

[9] David C Parkes, Michael O Rabin, Stuart M Shieber, and Christopher Thorpe. 2008. Practical secrecy-preserving, verifiably correct and trustworthy auctions. *Electronic Commerce Research and Applications* 7, 3 (2008), 294–312.

[10] Torben Pryds Pedersen. 1991. Non-interactive and information-theoretic secure verifiable secret sharing. In *Annual International Cryptology Conference*. Springer, 129–140.

[11] Stephen J Rassenti, Vernon L Smith, and Robert L Bulfin. 1982. A combinatorial auction mechanism for airport time slot allocation. *The Bell Journal of Economics* (1982), 402–417.

[12] Michael H Rothkopf, Aleksandar Pekeč, and Ronald M Harstad. 1998. Computationally manageable combinational auctions. *Management science* 44, 8 (1998), 1131–1147.

[13] Tuomas Sandholm. 1999. An algorithm for optimal winner determination in combinatorial auctions. (1999).

[14] Andrew C Yao. 1982. Protocols for secure computations. In *Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on*. IEEE, 160–164.

[15] Tatu Ylonen. 1996. SSH–secure login connections over the Internet. In *Proceedings of the 6th USENIX Security Symposium*, Vol. 37.