Books

1. Katz, Jonathan, and Yehuda Lindell. ***Introduction to modern cryptography*****.** CRC press, 2020.

Papers

1. Bellare, Mihir, and Phillip Rogaway. "**Random oracles are practical: A paradigm for designing efficient protocols.**" In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 62-73. 1993.
2. Ben-Efraim, Aner, Yehuda Lindell, and Eran Omri. "**Optimizing semi-honest secure multiparty computation for the internet.**" In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 578-590. 2016.
3. Bloom, Burton H. "**Space/time trade-offs in hash coding with allowable errors.**" *Communications of the ACM* 13, no. 7 (1970): 422-426.
4. Boneh, Dan, Eu-Jin Goh, and Kobbi Nissim. "**Evaluating 2-DNF formulas on ciphertexts.**" In *Theory of cryptography conference*, pp. 325-341. Springer, Berlin, Heidelberg, 2005.
5. De Cristofaro, Emiliano, Paolo Gasti, and Gene Tsudik. "**Fast and private computation of cardinality of set intersection and union.**" In *International Conference on Cryptology and Network Security*, pp. 218-231. Springer, Berlin, Heidelberg, 2012.
6. Debnath, Sumit Kumar, Pantelimon Stănică, Nibedita Kundu, and Tanmay Choudhury. "**Secure and efficient multiparty private set intersection cardinality.**" *Advances in Mathematics of Communications* 15, no. 2 (2021): 365.
7. ElGamal, Taher. "**A public key cryptosystem and a signature scheme based on discrete logarithms.**" *IEEE transactions on information theory* 31, no. 4 (1985): 469-472.
8. Fan, Junfeng, and Frederik Vercauteren. "**Somewhat practical fully homomorphic encryption.**" *IACR Cryptol. ePrint Arch.*2012 (2012): 144.
9. Fiat, Amos, and Adi Shamir. "**How to prove yourself: Practical solutions to identification and signature problems.**" In *Conference on the theory and application of cryptographic techniques*, pp. 186-194. Springer, Berlin, Heidelberg, 1986.
10. Ion, Mihaela, Ben Kreuter, Erhan Nergiz, Sarvar Patel, Shobhit Saxena, Karn Seth, David Shanahan, and Moti Yung. "**Private Intersection-Sum Protocol with Applications to Attributing Aggregate Ad Conversions.**" *IACR Cryptol. ePrint Arch.* 2017 (2017): 738.
11. Lv, Siyi, Jinhui Ye, Sijie Yin, Xiaochun Cheng, Chen Feng, Xiaoyan Liu, Rui Li, Zhaohui Li, Zheli Liu, and Li Zhou. "**Unbalanced private set intersection cardinality protocol with low communication cost.**" *Future Generation Computer Systems* 102 (2020): 1054-1061.
12. Pedersen, Torben Pryds. "**Non-interactive and information-theoretic secure verifiable secret sharing.**" In *Annual international cryptology conference*, pp. 129-140. Springer, Berlin, Heidelberg, 1991.