Sample Annotated Bibliography

October 17, 2019

References

[Hac12] Andrew Hacker. Is algebra necessary? New York Times, July 31 2012.

> This article was published in the New York Times. This is written by Andrew Hacker. The contents of this article is to argue whether algebra is necessary at all in terms of hacking. The conclusion provides pro and cons of with and without algebra.

[WM17] Xiaofen Wang and Yi Mu. Content-based encryption. In *Australasian Conference on Information Security and Privacy, Lecture Notes in Computer Science*, pages 57–72. Springer, Heidelberg, 2017.

> Content-centric networks have demonstrated an entirely new type of network topology, which offers a new way to distribute information in the data-driven network. Unlike the TCP/IP network topology, which is address-driven, content-centric networks do not require any address. Based on the content-to-consumer paradigm, content-centric networking architecture was proposed for the content to be provided efficiently with great convenience to users. As the content-centric network is not address-driven, when a data packet is delivered it cannot be encrypted with any encryption key of a node. Therefore, data confidentiality in content-centric network is a challenging problem. Motivated to solve this problem, the authors introduced a new

cryptosystem for content-based encryption, where the encryption key is associated with the content. They proposed a content-based encryption scheme (CBE), which is proven to be semantically secure in the random oracle model. They applied the CBE to construct a secure content delivery protocol in a content-centric network.

[WMC17] Xiaofen Wang, Yi Mu, and Rongmao Chen. One-round privacy preserving meeting location determination for smartphone applications. *IEEE Transactions on Information Forensics and Security*, 11(8):1712–1721, 2017.

With the widely adopted GPS technology in mobile devices, users enjoy many types of location services. As a recently proposed application, determining the optimal private meeting location with an aid of a location server has been an interesting research topic. The challenge in this paper is due to the requirements of security and privacy, because user locations should not be revealed to the honest-but-curious or semi-trusted location server. Adding the security and privacy protection to a location service will inevitably introduce computational complexity and communication overhead. In order to introduce robust location service and make this location service practical, the authors propose an efficient optimal private meeting location determination protocol, which needs only one round communication and light computation. Their proposed protocol satisfies the requirement of location privacy against outsiders, the semi-trusted meeting location determination server, and the semi-trusted group users. In order to study the performance of their protocol in a real deployment, their simulated the scheme on smartphones. The simulation results and the performance comparison with another scheme demonstrate its advantages in communication and computation efficiency.