# Department of Computer Science

## Towards Next-Generation Password Protocols: A Cryptographic Perspective

**Jiayu Xu**
George Mason University

**Hosted by** Jing Li

**DATE:** Monday, April 19, 2021
**TIME**: 2:30 PM - 3:30 PM
**LOCATION:** https://njit.webex.com/njit/j.php?MTID=me2b470a51d8ff4e512d4236f4542d246

**https://cs.njit.edu/seminars**

**Abstract:** Passwords have long been the most ubiquitous method of authentication on the Internet. The current password authentication approach, "password-over-TLS," suffers from three major drawbacks: (1) the security of this protocol critically relies on the assumption that the server's public key is correctly distributed to the client; (2) the server obtains the client's password in the clear upon TLS decryption; and (3) an offline dictionary attack is inevitable upon server compromise. Recent years have witnessed an increasing number of attacks exploiting these deficiencies, leading to billions of password leakages.

In this talk, I will present two key findings from my cryptographic research towards eliminating the aforementioned weaknesses. First, I will present a new security analysis of the highly efficient SPAKE2 password-authenticated key exchange (PAKE) protocol, showing that its security preserves under arbitrary composition. Second, I will show my protocol OPAQUE that combines the security guarantees of PAKE and "password-over-TLS." Overall, these results contribute to the next-generation protocols for password authentication that achieve significantly stronger security. I will conclude with my long-term vision for password protocols from a multi-angle approach that combines cryptography, security, and social sciences.

**Bio:** Jiayu Xu is a postdoctoral researcher at George Mason University. His research spans theoretical and practical aspects of cryptography, as well as applications to network security. He obtained his Ph.D. degree in computer science from the University of California, Irvine in 2019, and his B.S. degree in mathematics from Peking University in 2013. His work was highlighted at Real World Crypto (RWC) conference in 2017 and 2019, and his password authentication protocol OPAQUE was recommended by the Crypto Forum Research Group (CFRG) for usage in IETF protocols in 2020.