2018/2019

Seminar Series

www.cs.unb.ca/seminarseries

EST. 1785 UNB UNIVERSITY OF NEW BRUNSWICK | Computer Science

Practical Backward-Secure Searchable Encryption from Symmetric Puncturable Encryption

Presenter:

Joseph Liu
Monash University, Australia

Symmetric Searchable Encryption (SSE) has received wide attention due to its practical application in searching on encrypted data. Beyond search, data addition and deletion are also supported in dynamic SSE schemes. Unfortunately, these update operations leak some information of updated data. To address this issue, forward secure SSE is actively explored to protect the relations of newly updated data and previously searched keywords. On the contrary, little work has been done in backward security, which enforces that search should not reveal information of deleted data. In this talk, we propose the first practical and non-interactive backward-secure SSE scheme. In particular, we introduce a new form of symmetric encryption, named symmetric puncturable encryption (SPE), and construct a generic primitive from simple cryptographic tools. Based on this primitive, we then present a backward secure SSE scheme that can revoke a server's searching ability on deleted data. We instantiate our scheme with a practical puncturable pseudorandom function and implement it on a large dataset. The experimental results demonstrate its efficiency and scalability. Compared to the state-of-the-art, our scheme achieves a speedup of almost 50× in search latency, and a saving of 62% in server storage consumption.

ALL STUDENTS ARE ENCOURAGED TO ATTEND

Friday, October 19th @ 3:30PM
Gillin Hall, Room C127