CT Advanced Computing Center (CACC) Security Seminar Series 2022-2023

Speaker: Chloe Cachet, Doctoral Dissertation Proposal
Date: Wednesday, September 21
Time:12 - 1:30pm
Location: ITE 401
Remote Access: https://uconn-cmr.webex.com/uconn-cmr/j.php?MTID=m6e24b00880ea4a488adf302903cb9b63
Meeting number: 2621 780 2095
Password: EWt39phUyc4

Private Biometric Cryptosystems

Biometric records are collected and stored in large databases for identification purposes. Unfortunately, this is done with few cryptographic protection and database leakages are frequent. A solution to this issue would be to use proximity searchable encryption. Proximity searchable encryption handles proximity queries (finding all records within a bounded distance of the query point) over encrypted records. This work studies proximity searchable encryption applied to the iris biometric.

Inner product functional encryption was previously proposed to build proximity searchable encryption, as binary Hamming distance is computable using an inner product. However, this simple solution is flawed. First, the setup phase is highly inefficient for large input vectors for most inner product schemes. Second, this construction reveals the distance between the query and the stored records. Such leakage can be used to mount devastating attacks. Our work identifies and attempts to close these two gaps. We first propose a new technique to improve setup efficiency without harming the accuracy and security of the scheme. For 1024 bits input vectors this reduces setup runtime from approximately 23 days to 4 minutes. We then show that we can build proximity search from function hiding, secret key, predicate inner product encryption to avoid the distance leakage.

UCONN

CACC