In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Shielding Modern Collaboration for Privacy, Performance, and Purpose

by

Prof. Sherman S. M. Chow

The Chinese University of Hong Kong, Hong Kong

Date : 26th September, 2025 (Fri)

Time : 11:30am – 12:30pm

Venue : Room 801, Ho Sin Hang Engineering Building, CUHK

Abstract

Secure collaboration must satisfy multiple criteria: systems deliver scalability and sustainability, users keep control of privacy and anonymity, analytics comply with privacy law, and actions remain accountable despite insider compromise. Motivated by real-world constraints mostly overlooked in prior work, this talk presents cryptosystems that turn these goals into provable guarantees for governing, sharing, and learning.

Shared governance: ECDSA underlies critical infrastructure. Threshold ECDSA splits a signing key across n parties so any t can sign. Prior designs optimized communication but assumed no dropouts; any dropout forced a restart, wasting preprocessing and enabling denial-of-signing. We initiate the study of threshold ECDSA with best-of-both-worlds security, achieving true t-of-n liveness, so the signing continues without a restart (NDSS'23, '24). Signatures also act as credentials, making revocation on misbehavior and reputation for Sybil deterrence necessary. Earlier anonymous systems either required full-history proofs or stayed fast until a dispute, after which they could freeze everyone. Our scored anonymous credentials are free from system-wide halts caused by a single dispute (ACNS'23, EuroS&P'23).

Shared data space: Long-lived anonymity should not flood systems with ever-growing, unlinkable records. Most ring-based credential/payment systems let state grow without bound. We give "anonymity that compresses with time": the system reclaims space from obsolete records without introducing linkability (CSF'23). Switching to confidentiality, access-control encryption blocks policy-violating leakage via an egress verifier that enforces the read/write policy without learning the message, parties, or policy. We give the first constructions that compress fine-grained policies into short ciphertexts using pairings or lattices and the first information-theoretic scheme (S&P'21, ACNS'21, ISIT'23).

Shared discovery: Many contributors encrypt to a common store that must stay searchable. For two decades, the area was split: sublinear search came from single-writer symmetric schemes, while multi-writer public-key schemes needed linear scans. Hybrid and delegatable searchable encryption reconciles both worlds (Usenix Sec.'22, NDSS'24). We then align private machine learning (ML) with current practice: TEE+GPU+crypto co-design (Usenix Sec.'21, AAAI'21), crypto-ML co-design for LLMs (NDSS'25), and DP-Forward, which shifts privacy noise to the sensitive forward pass (CCS'23).

Stepping beyond these pillars, strategic control for blockchains (ICDCS'23, FC'25) and scalable verifiable analytics (AsiaCrypt'25) will be briefly discussed. Spanning all these areas, the long-term goal is to formalize and enforce societal rules with cryptography, so coalitions can govern, interoperate, and discover with privacy, performance, and purpose.

Biography

Sherman S. M. Chow joined The Chinese University of Hong Kong in late 2012 and received the Early Career Award (2013/14). He has taught nearly all—and co-developed many—security courses at CUHK, taught Cyber Security in the Business School's MSc programme, and is founding Co-Director of the MSc in Information Science and Technology Management. He has published in and served on PCs for AsiaCrypt, CCS, EuroCrypt, NDSS, PETS, PKC, S&P, The Web, and Usenix Security. His service includes Area Chair (Real-World Cryptography) for AsiaCrypt 2025, Senior PC for AAAI, IJCAI, PETS, and The Web, and the Caspar Bowden PET Award committee (2019). Editorial roles span IEEE TIFS (Senior Area Editor), IEEE TDSC, ACM TOPS, ACM DLT, IJIS, and IET Information Security (past deputy editor). Recognitions include the World's Top 2% Scientists list (2018–2024), inclusion in the CORE ranking's expert pool (2021–present), and AMiner's Security and Privacy Top 100 (2018, ranked 43rd). He is an EAI Fellow (2019, inaugural).

**** ALL ARE WELCOME ****

Host: Prof. Pascal Vontobel (Tel: 3943-8390, Email: pascal.vontobel@ie.cuhk.edu.hk)

Enquiries: Department of Information Engineering, CUHK (Tel.: 3943-8385)