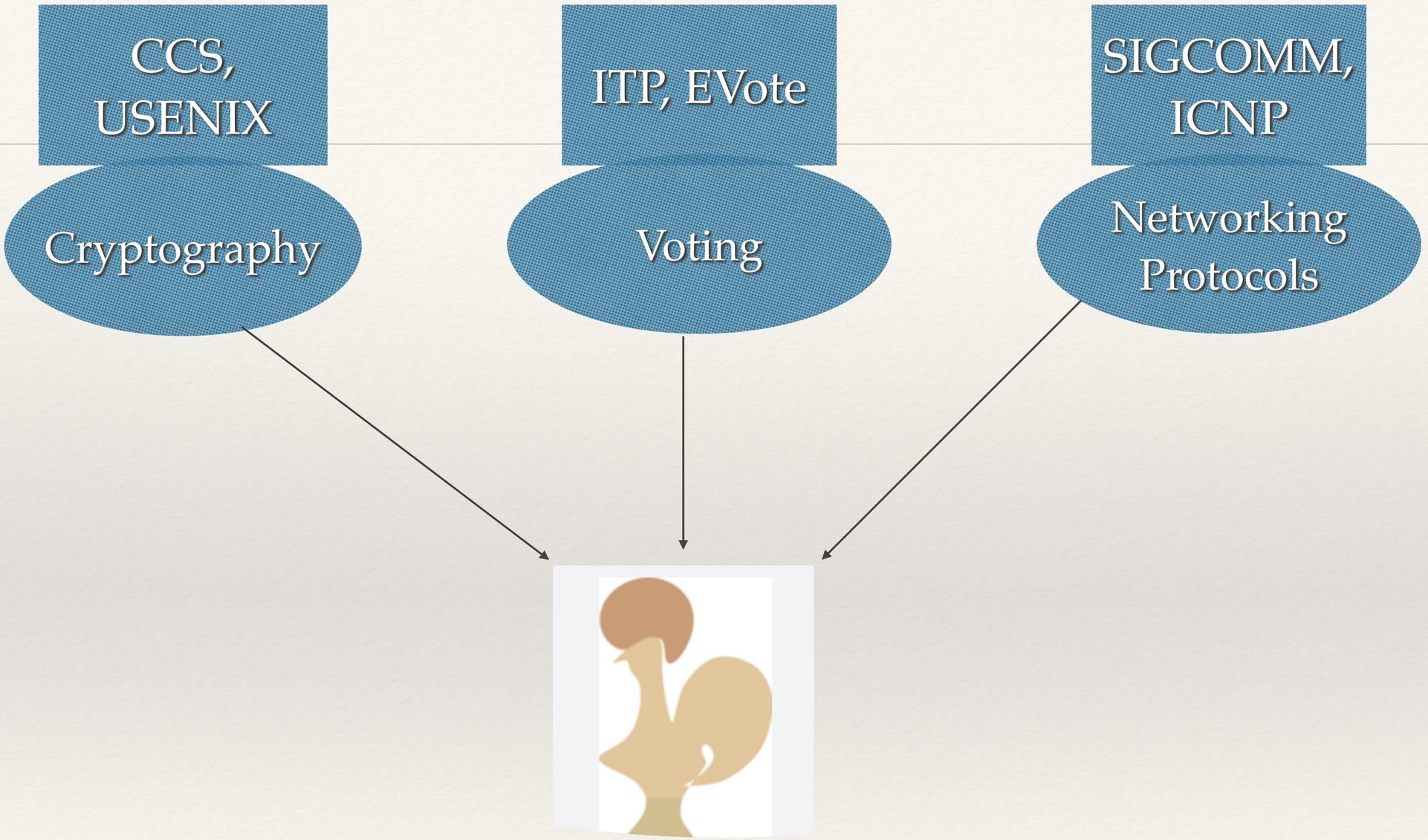
Projects (Past, Current, and Future)

Mukesh Tiwari,
University of Cambridge,
Cambridge

UNIVERSITY OF CAMBRIDGE


CCS, USENIX
ITP, EVote
SIGCOMM, ICNP
Cryptography
Voting
Networking Protocols

Schulze Voting as Evidence Carrying Computation

Dirk Pattinson & Mukesh Tiwari

Conference paper

948 Accesses | 6 Citations

Part of the Lecture Notes in Computer Science book series (LNTCS,volume 10499)

No More Excuses: Automated Synthesis of Practical and Verifiable Vote-Counting Programs for Complex Voting Schemes

Lyria Bennett Moses, Rajeev Goré, Ron Levy, Dirk Pattinson & Mukesh Tiwari

Conference paper | First Online: 06 October 2017

Modular Formalisation and Verification of STV Algorithms

Milad K. Ghale, Rajeev Goré, Dirk Pattinson & Mukesh Tiwari

RESEARCH-ARTICLE

Verified Verifiers for Verifying Elections

Authors: Thomas Haines, Rajeev Goré, Mukesh Tiwari Authors Info & Claims

Machine-checking Multi-Round Proofs of Shuffle: Terelius-Wikstrom and Bayer-Groth

Authors:
Thomas Haines, *Australian National University;* Rajeev Gore, *Polish Academy of Science;* Mukesh Tiwari, *University of Cambridge*

Submitted

Your Submissions

#784 Assume but Verify: Deductive Verification of Leaked Information in Concurrent Applications **Submitted**

Welcome to the SIGCOMM 2023 submissions site.

Your Submissions

#124 CAPP: Combinators for Algebraic Path Problems **Submitted**

The deadline for registering submissions has passed

Future Project

- Session Types for Voting (distributed voting centres, each collecting votes and sending it to a central server)
- Session Types for Information Flow Security (client/server not accidentally leaking a secret to other party, useful in differentially private Federated Learning)
- Session Types for computational model of cryptography (bounds of communication complexity)
- Session Types for Multi-Party Computation (combining votes without leaking individual ballots)
- Session Types for Smart Contracts

Questions?