Four minutes of fast talking about order-preserving encryption

Paul Grubbs, Skyhigh Networks
What is OPE?

- Encryption which preserves the order of the plaintexts
- Boldyreva et al. formalized the problem in 2009
  - IND-OCPA
  - Impossibility (exponential-size ciphertext space)
  - The HGD connection
  - First construction, indistinguishable from ROPF
- ‘Revisited’
  - Window one-wayness and WDOW security for uniform messages, also built other schemes (MOPE, CEOE)
What is OPE? (cont’d)

• Popa et al. ideal-security OPE
  – Stateful scheme, mutable ciphertexts
  – Achieves IND-OCPA
  – Impossibility for non-mutable IND-OCPA

• Several other recent papers
What do we know?

• Ideal-security constructions are difficult to use in practice
• Boldyreva et al.’s construction is efficient and easy to use but its practical security is not well-understood
  – ‘Revisited’ paper gives upper and lower bounds for WOW and WDOW security
Why should I care?

• Use cryptographic reasoning to solve real-world problems
• Elegant/cool constructions, interesting connections between areas
• Lots of applications in protocol design
  – Use as black-box in other schemes
• Industry
• Cloud!
Open Problems

• Extend/adapt results of ‘Revisited’ paper to arbitrary message distributions
• Tight(er) lower bound on adversary’s advantage in WOW and WDOW game for large windows
  – Attack in the paper is simple application of tail bound for HGD (Can HGD connection be exploited further?)
• Efficient NHGD sampling (Not really crypto but still important to mention)
• Can we get more secure/efficient schemes when we don’t need to respect strict order?
• (More philosophical) When is relaxed security appropriate in practice?
Conclusion

• In this talk, I briefly discussed and motivated order-preserving encryption
• I described several open problems and invited discussion and collaboration on them