Eluding Traffic Analysis with Multipath Spread Spectrum

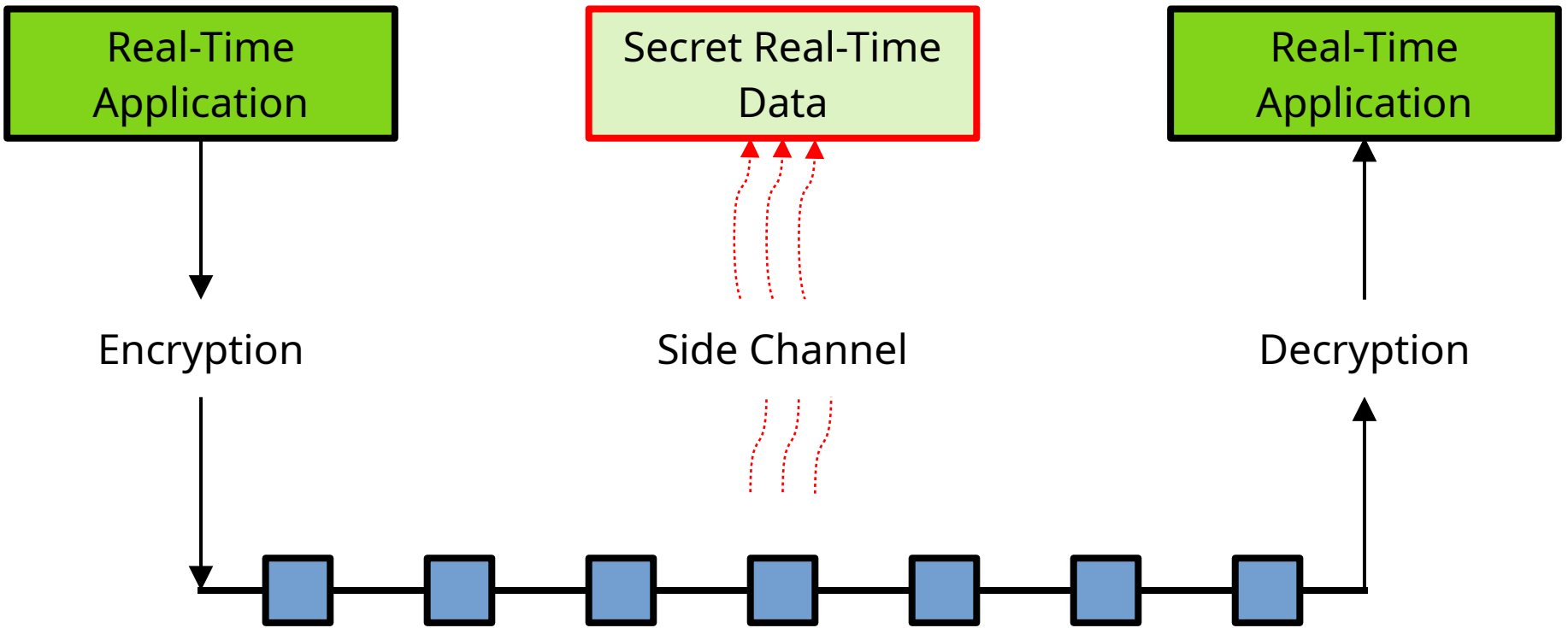
University of St Andrews

Gregor Haywood

PhD Student

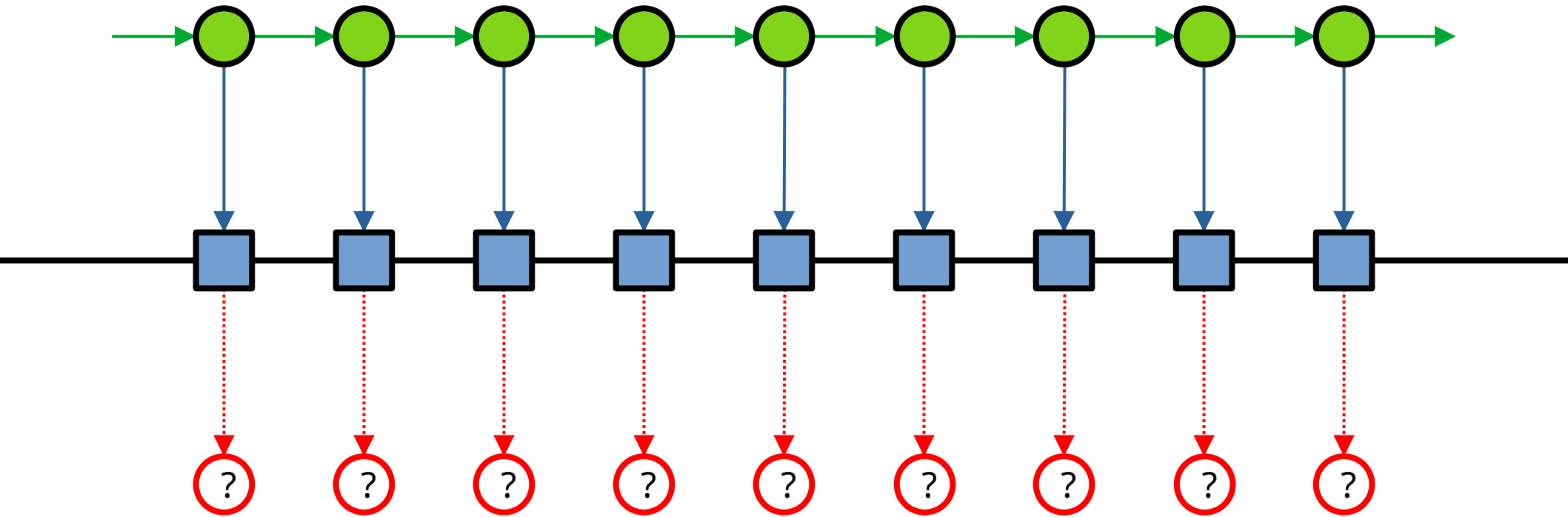
gh66@st-andrews.ac.uk

Traffic Analysis



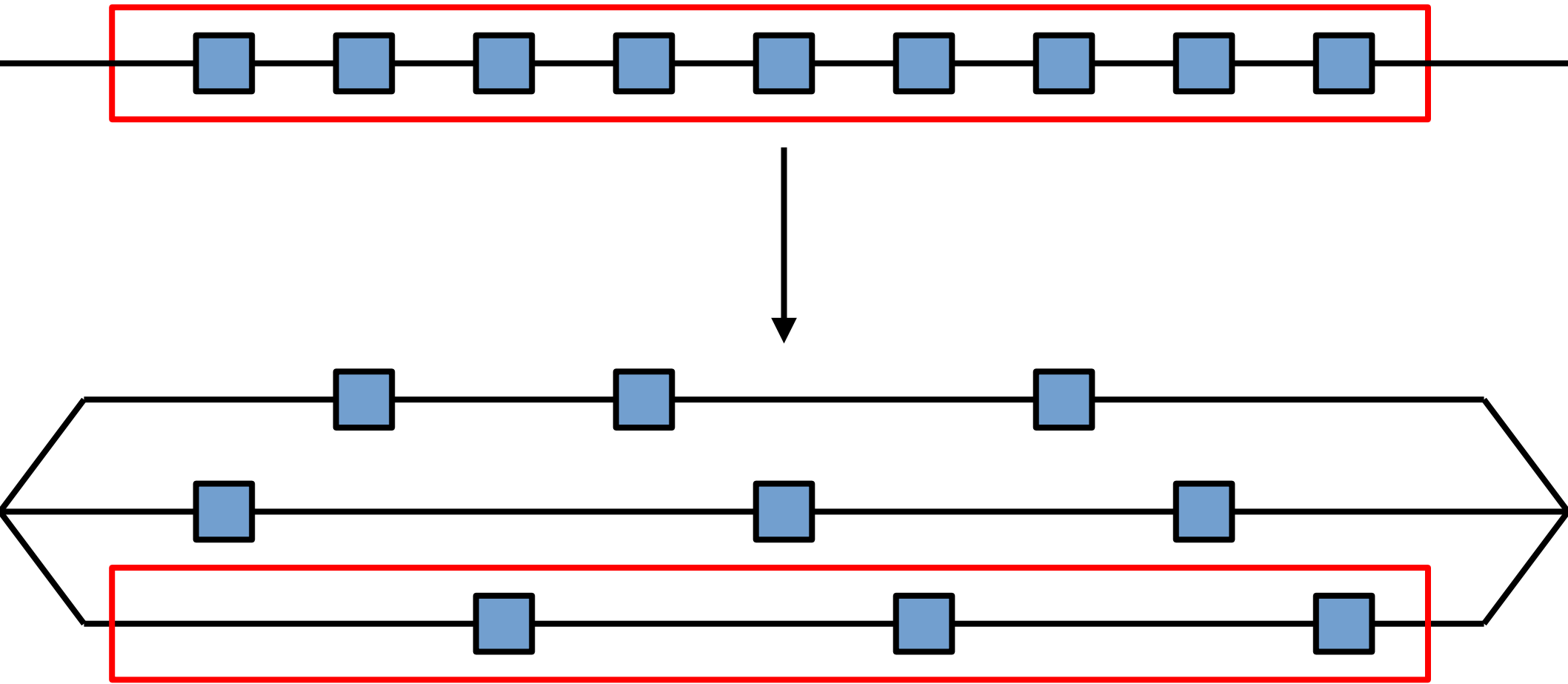
Hidden Markov Models

University of St Andrews



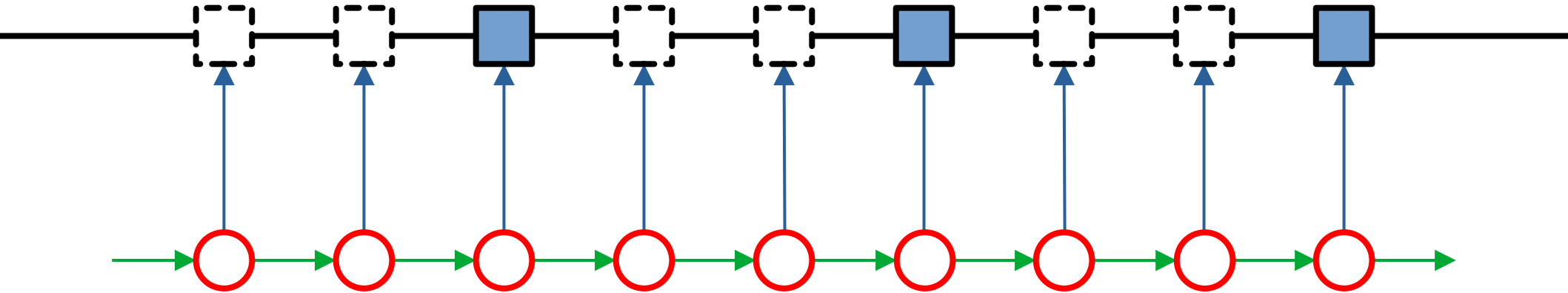
Spread Spectrum Defence

University of St Andrews

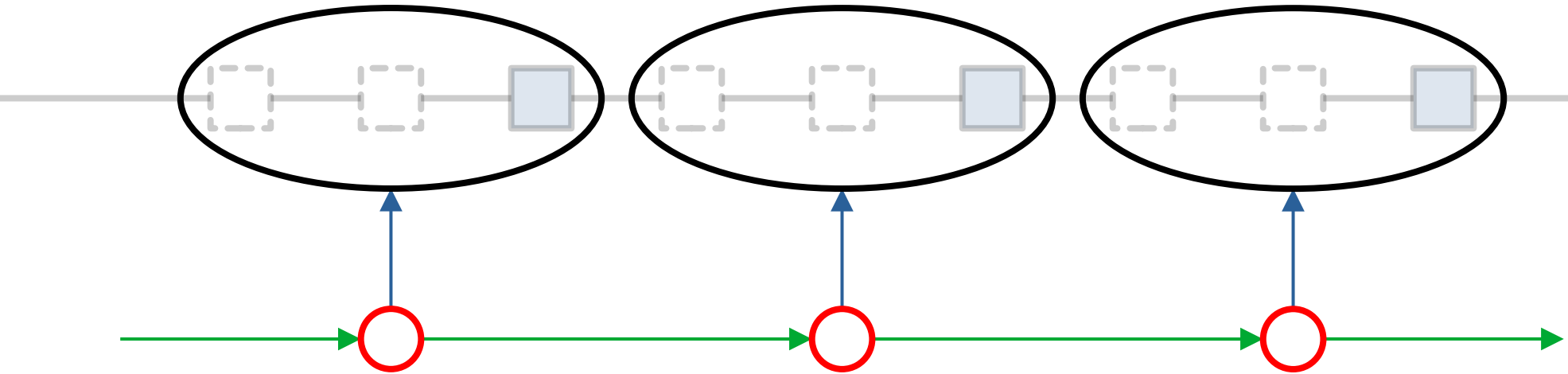


HMM Impact

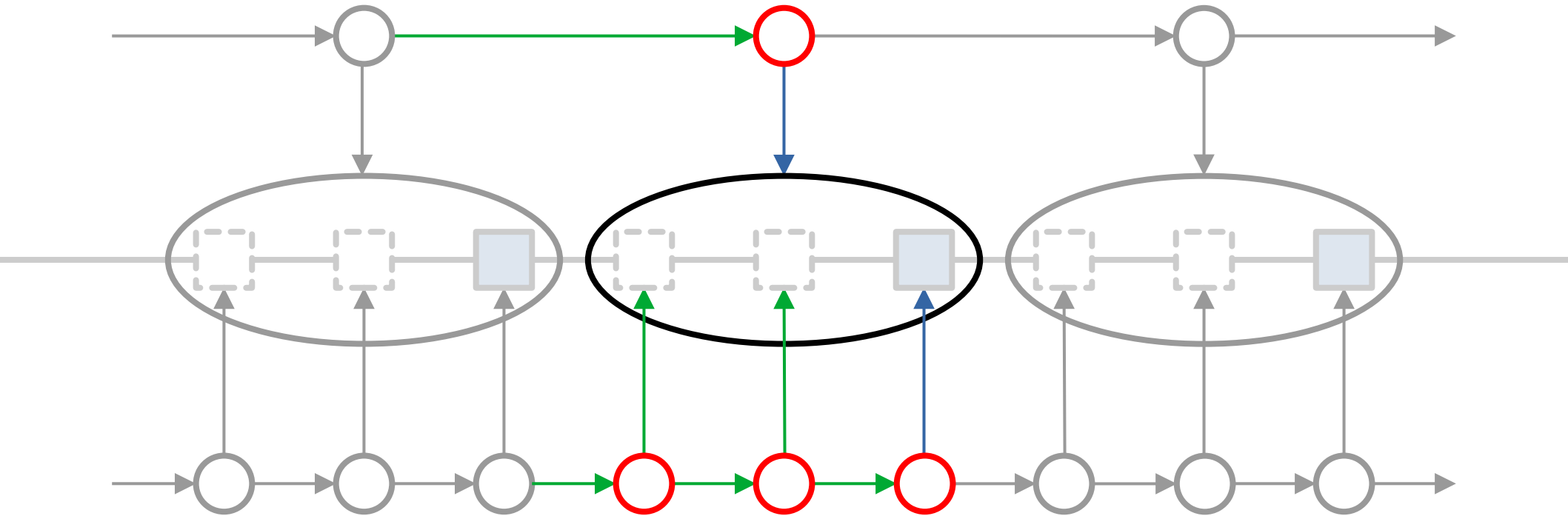
HMM Impact



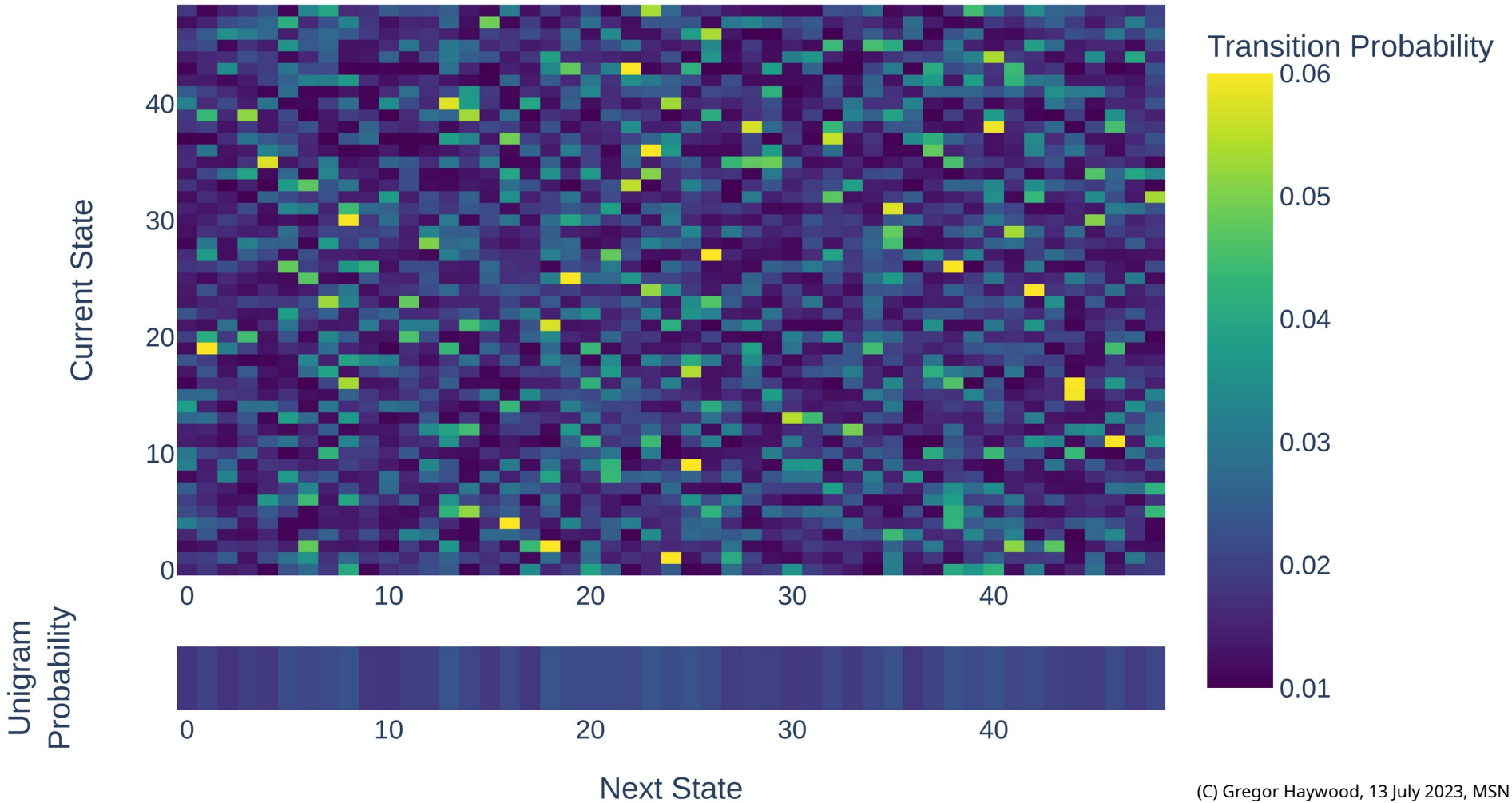
HMM Impact



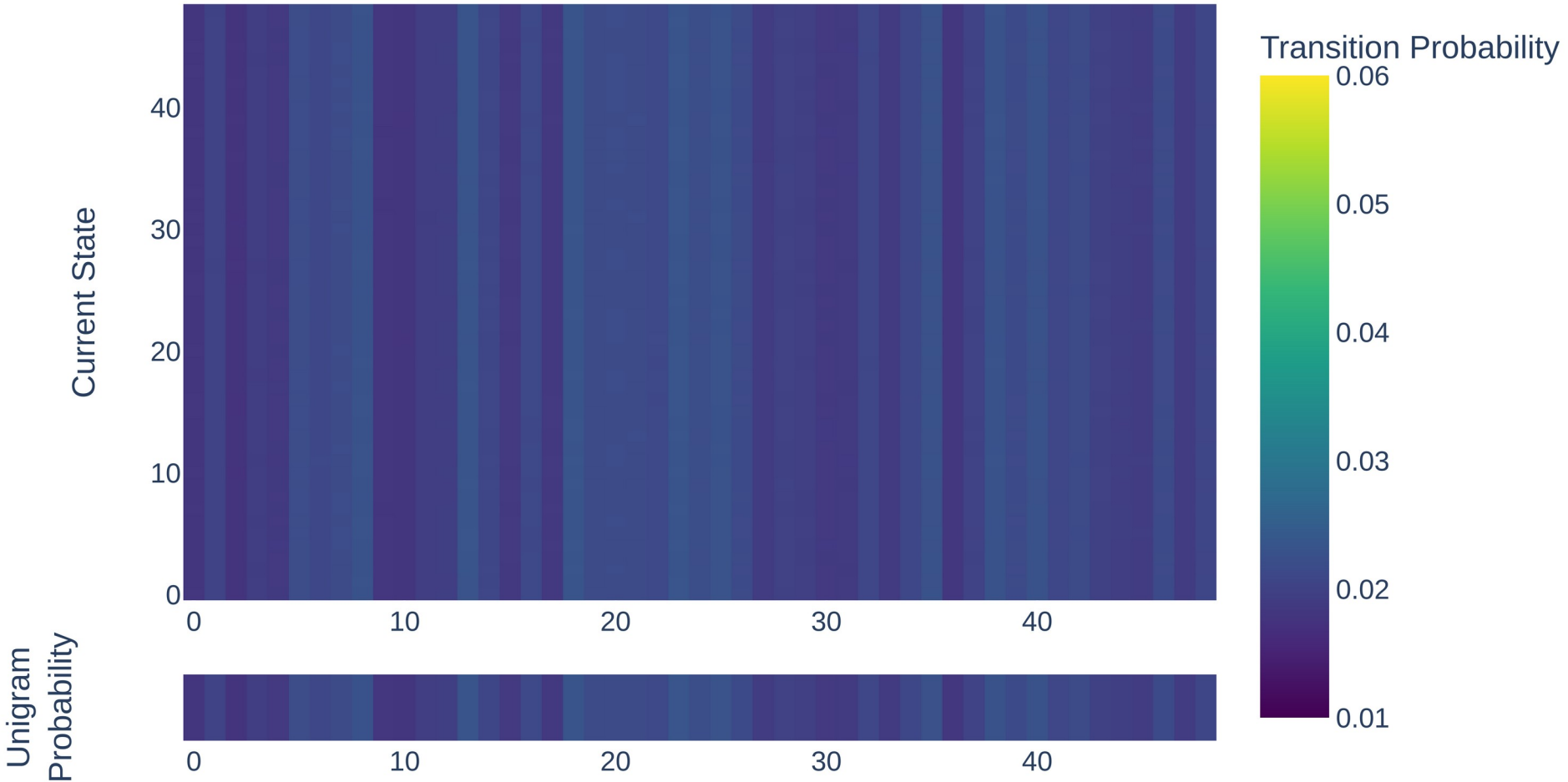
HMM Impact



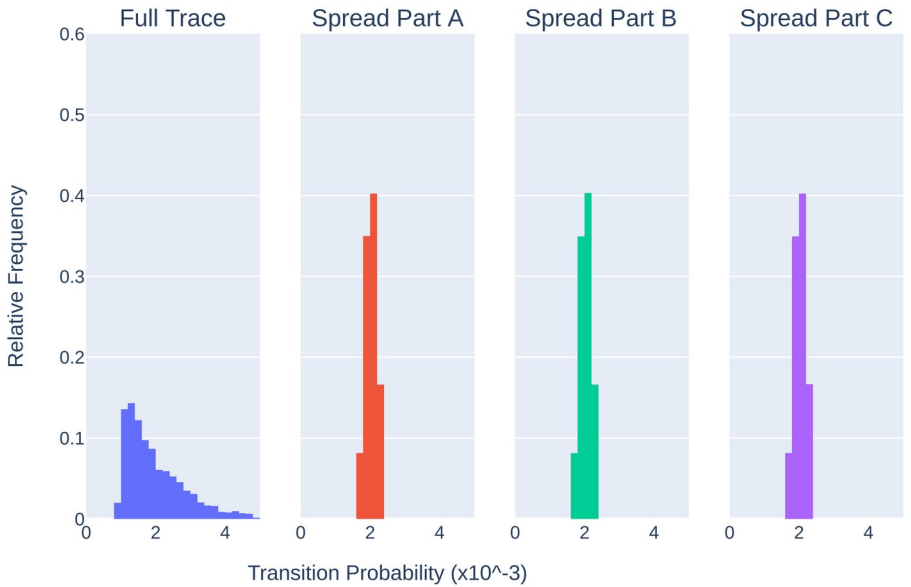
Single Path Probabilities



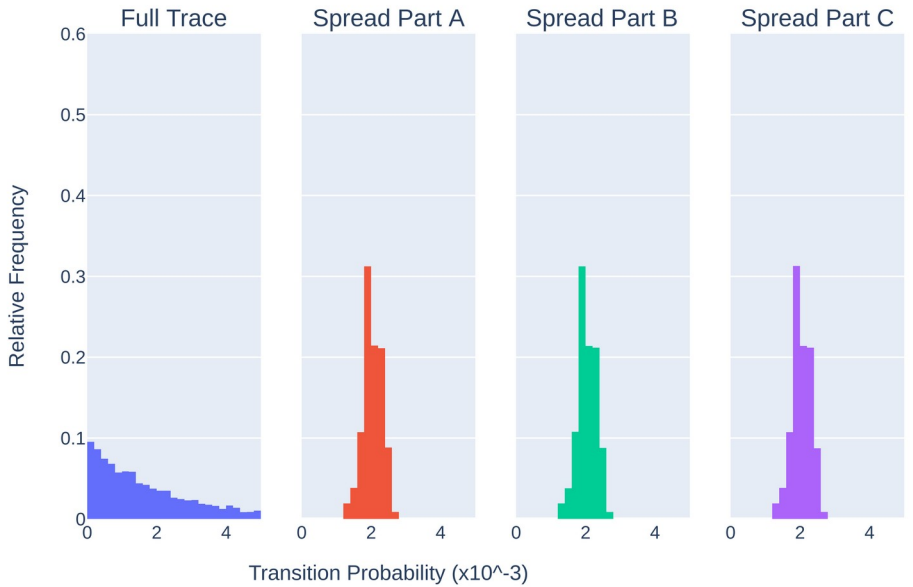
Multi-Path Probabilities



Transition Probability Distributions

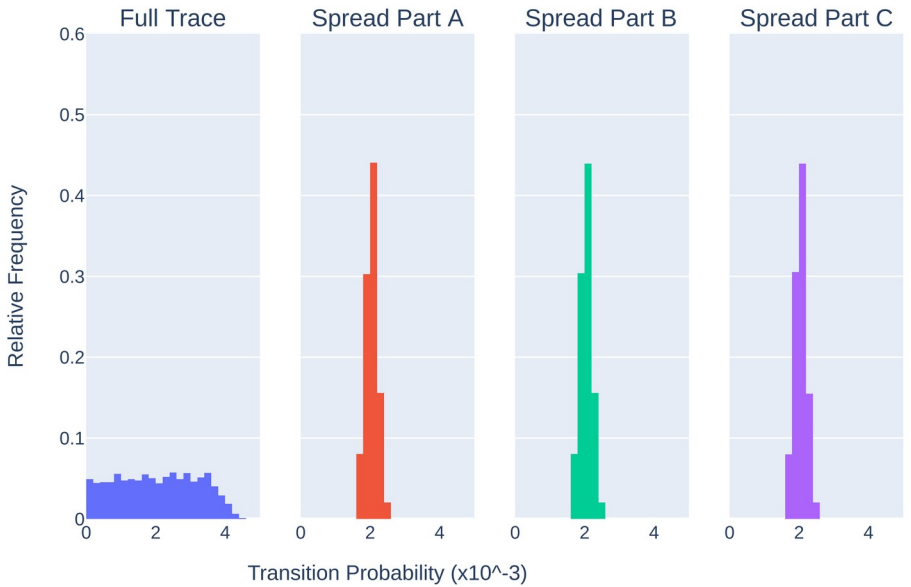


Non-Zero Exponential Markov Process

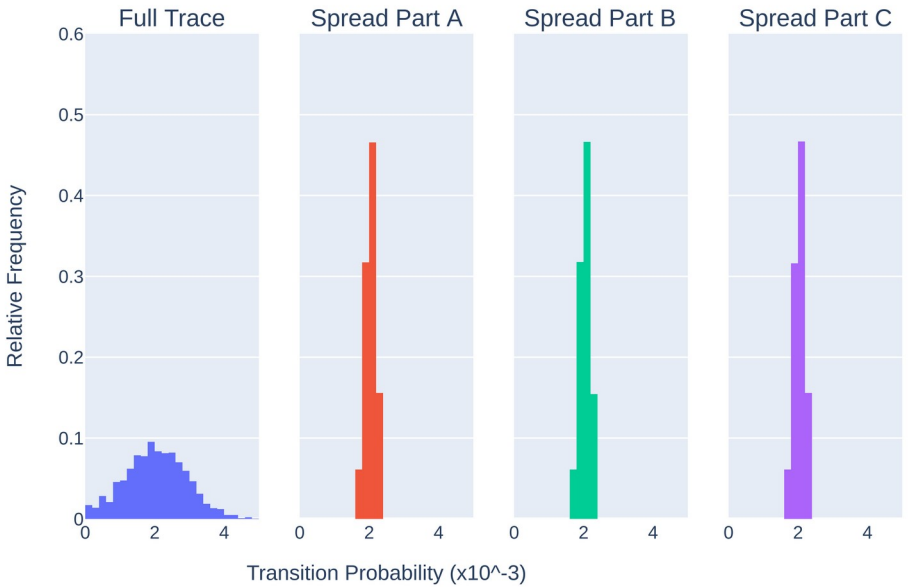


Exponential Markov Process

Transition Probability Distributions



Uniform Markov Process



Normal Markov Process

Summary

University of St Andrews

- **Multi-path communication can make side channel attacks harder**
- Round-Robin Spread Spectrum: Network Layer
  - Using ILNP
  - General Solution (no matter what happens above the network layer)
- Multipath congestion control: Transport Layer
  - MPTCP, QUIC, etc.
  - Competing goals!
- Future work:
  - New Congestion Controls
  - Performance Impact
  - Real Applications