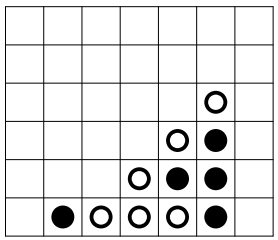
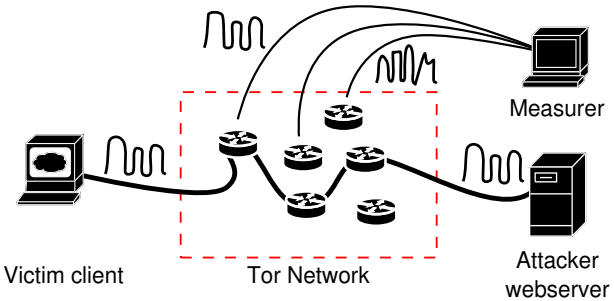
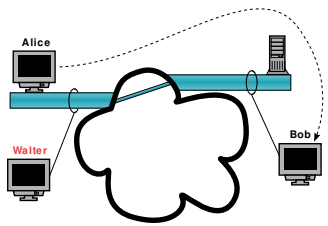
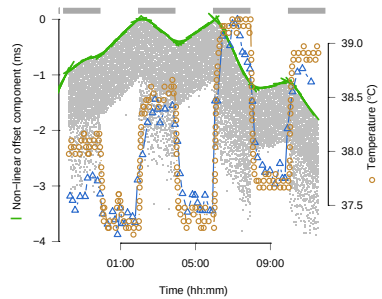
Covert channel vulnerabilities in anonymity systems









Steven J. Murdoch

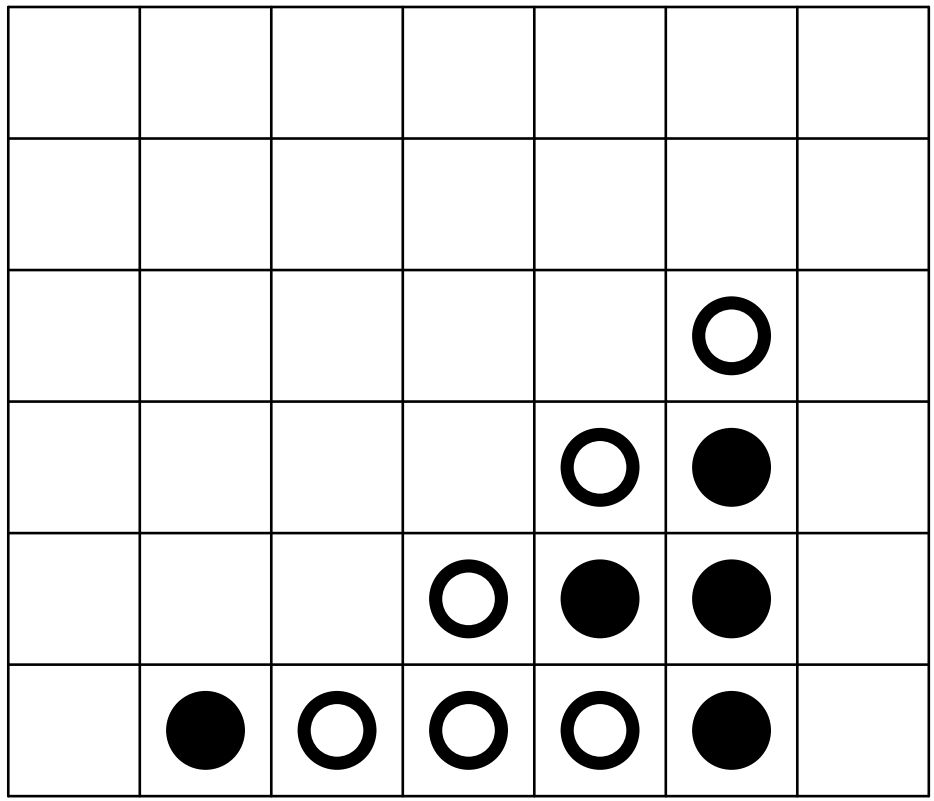
http://www.cl.cam.ac.uk/users/sjm217/

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

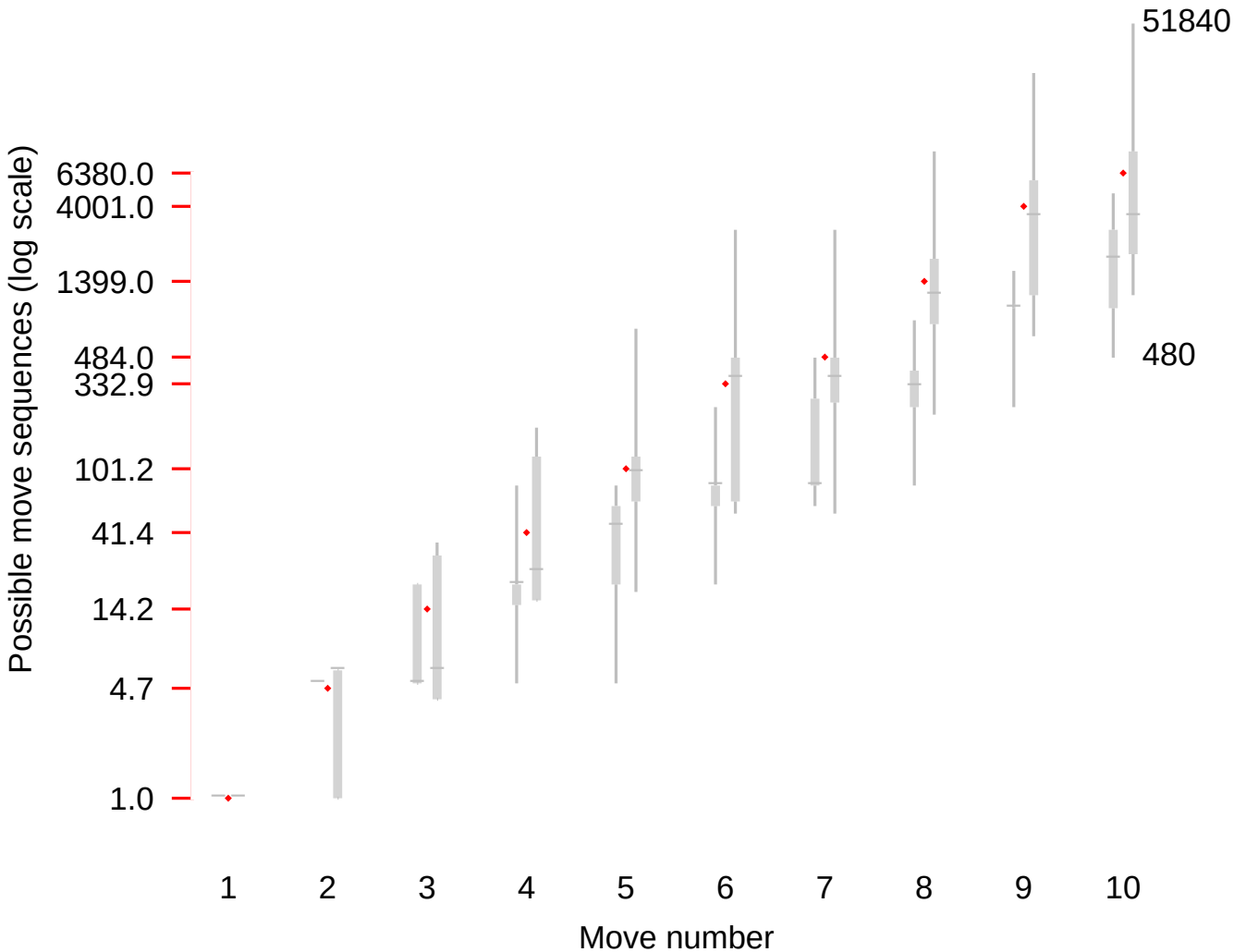
www.torproject.org

It all started with an Xbox

The competition was to play Connect-4

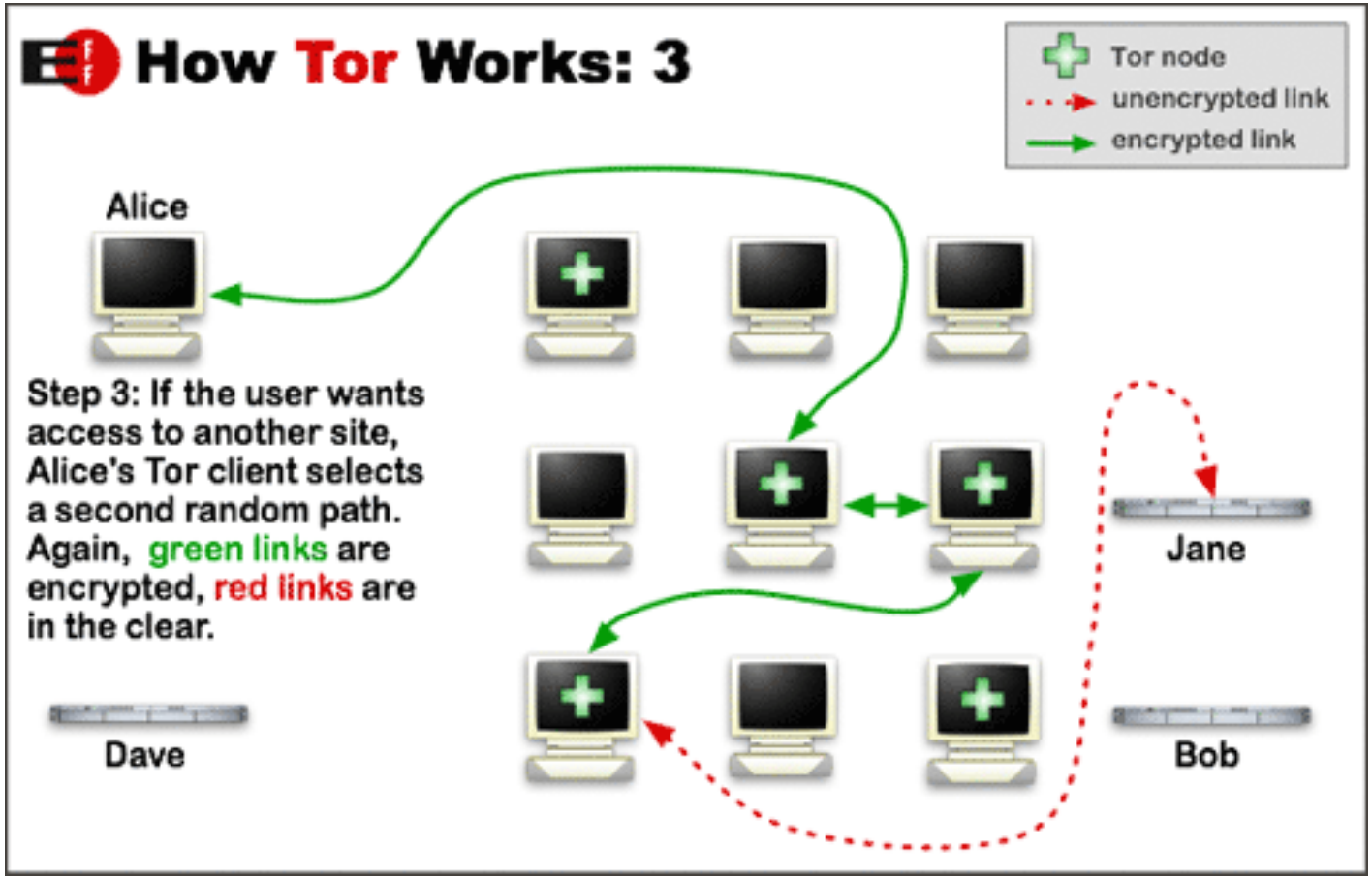


Our programs signalled identity through the moves they made

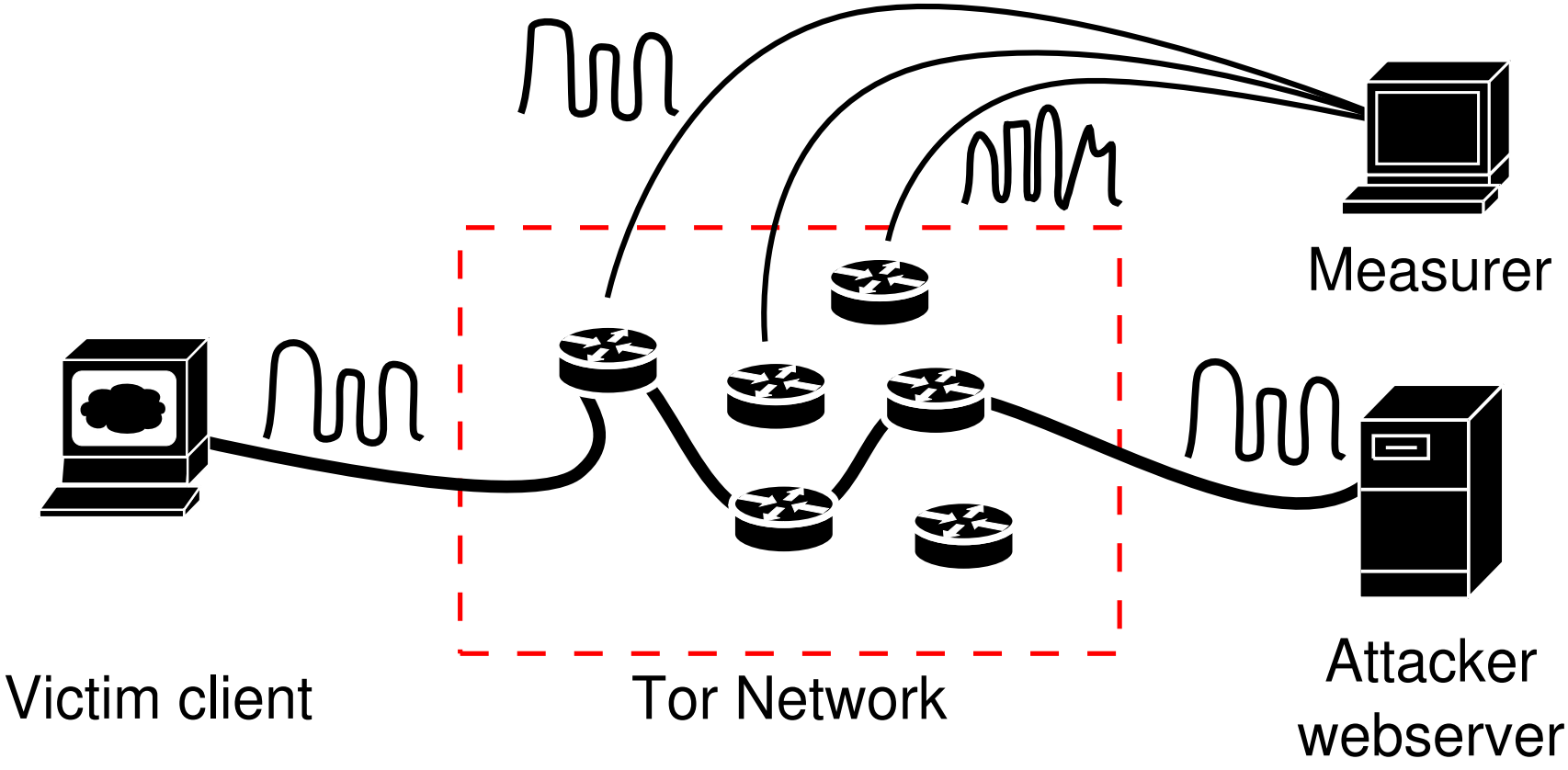


We wrote a paper for InfoHiding 2004

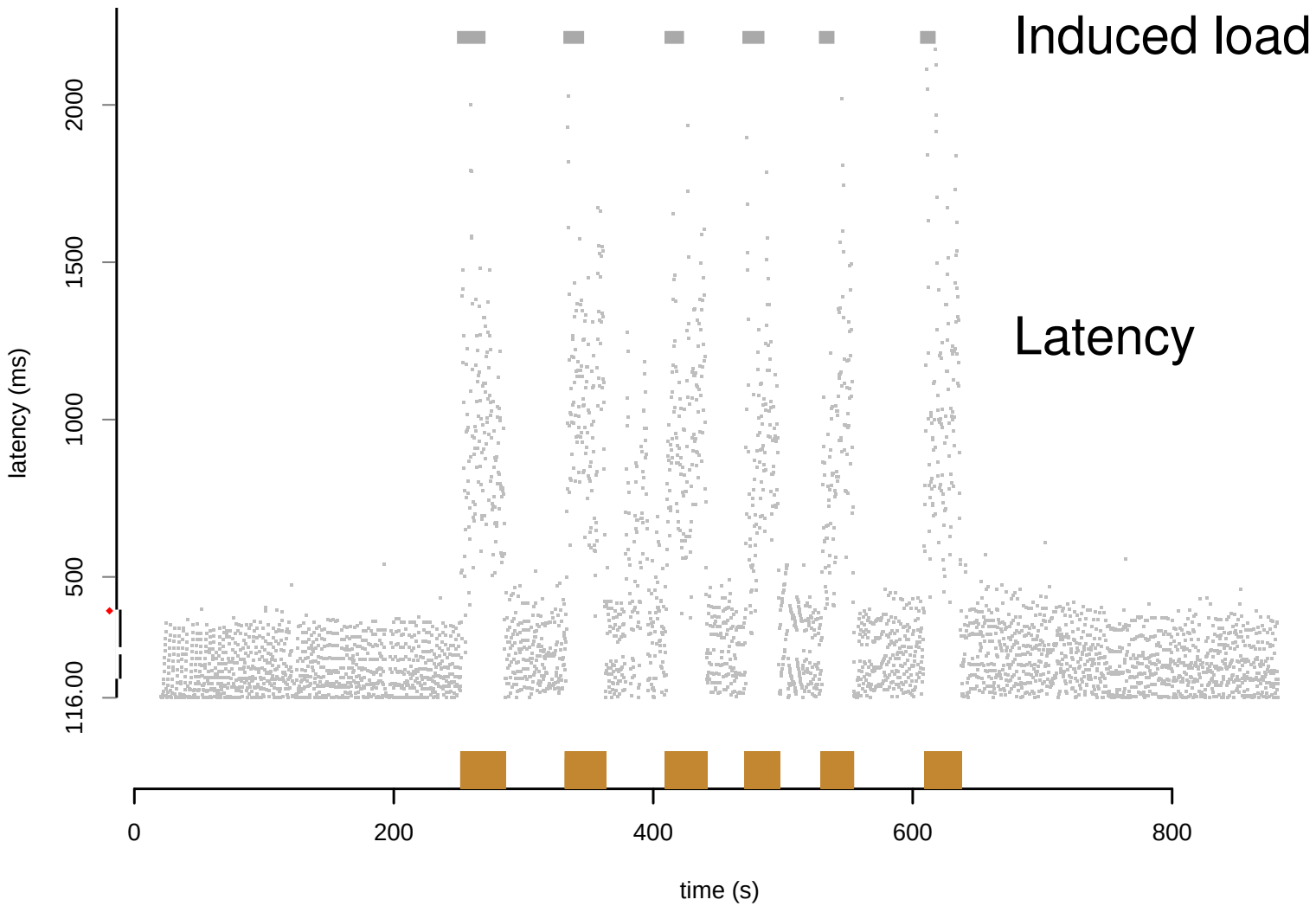
Following PET 2004, I operated a Tor node at Cambridge University



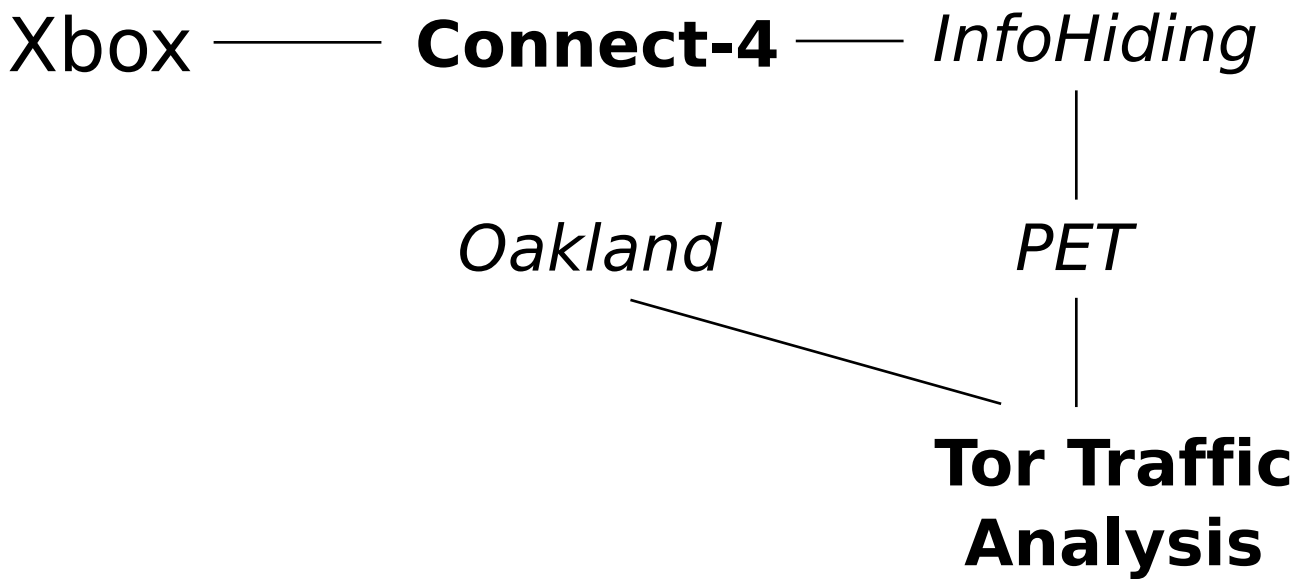
Our attack was to trace anonymous paths through the network



Latency measurements showed traffic load flowing through a node

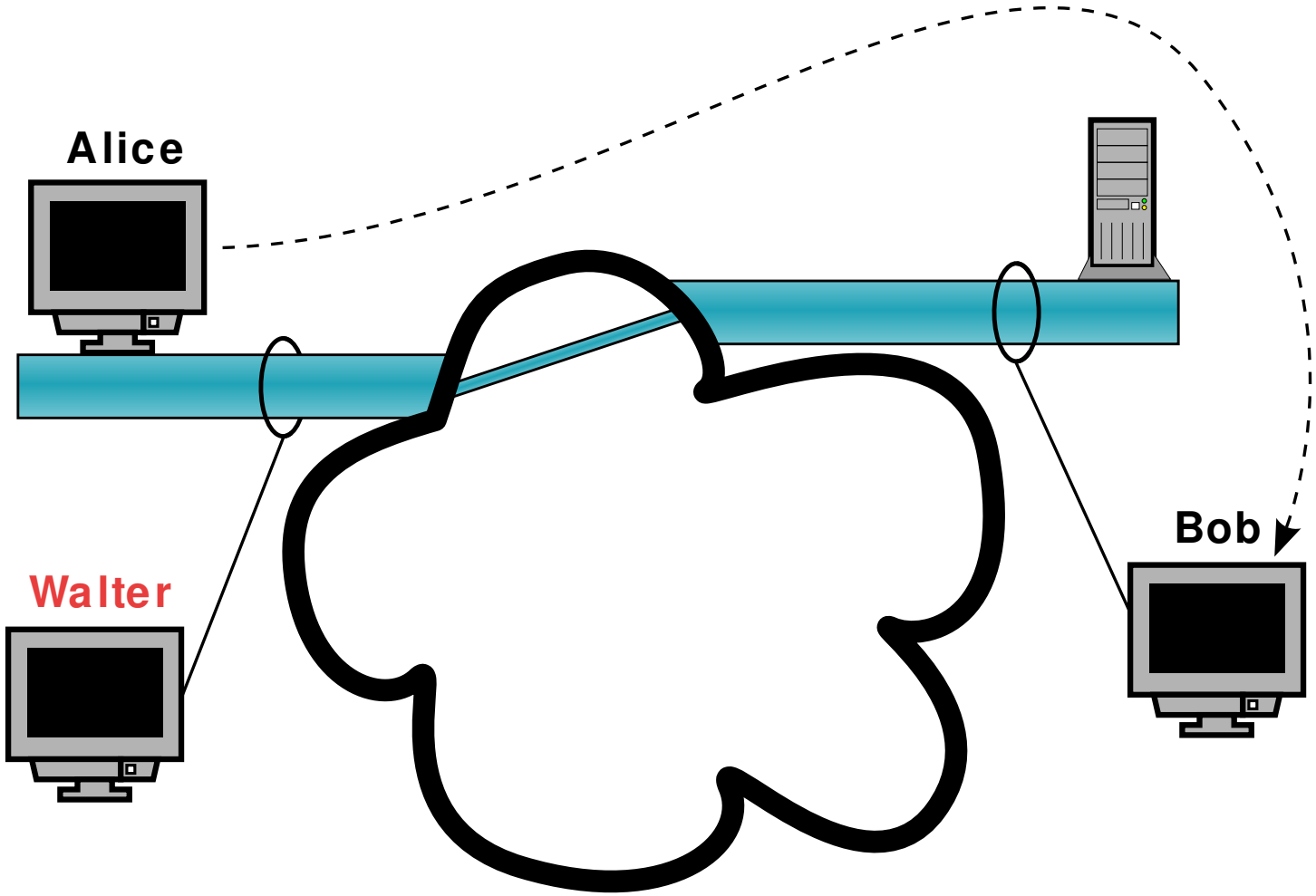


We wrote a paper for Oakland 2005



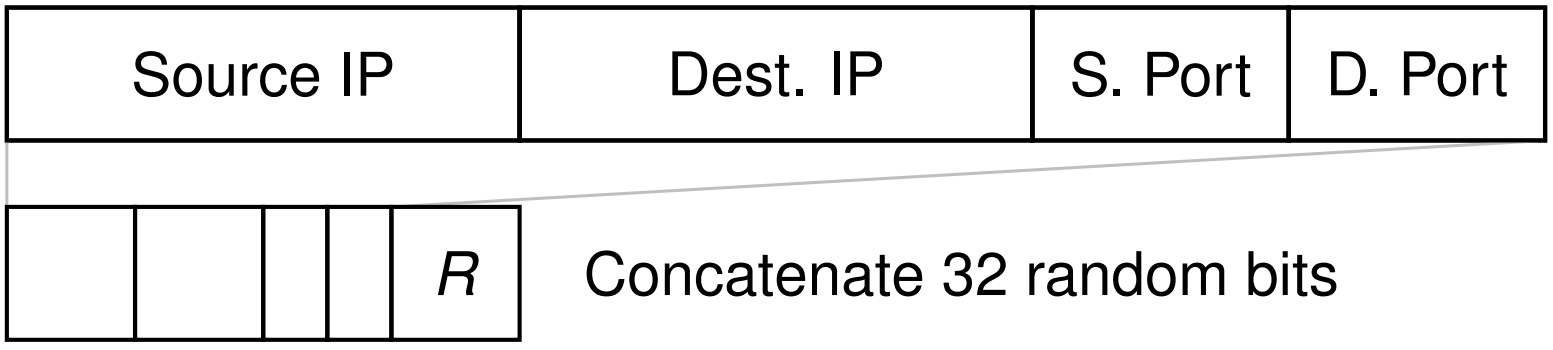
Following InfoHiding 2004, I also investigated currency watermarking

I presented my results at again 21C3, and attended a talk on Nushu

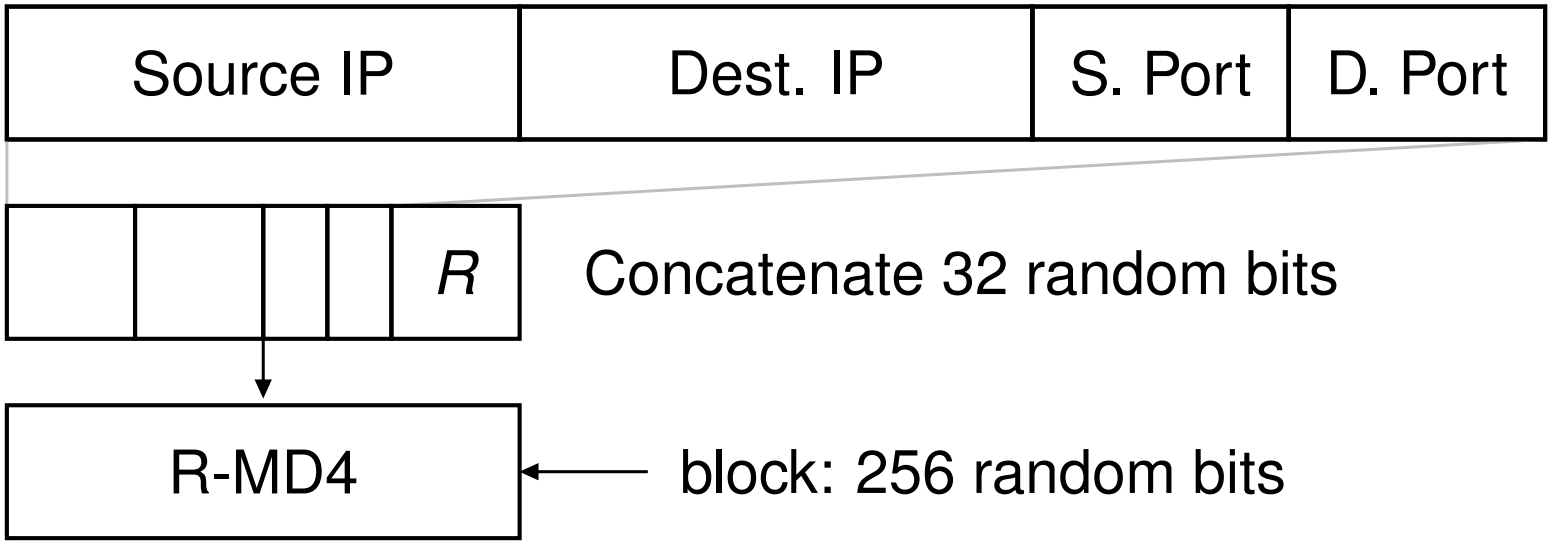


Initial sequence numbers have complex structure

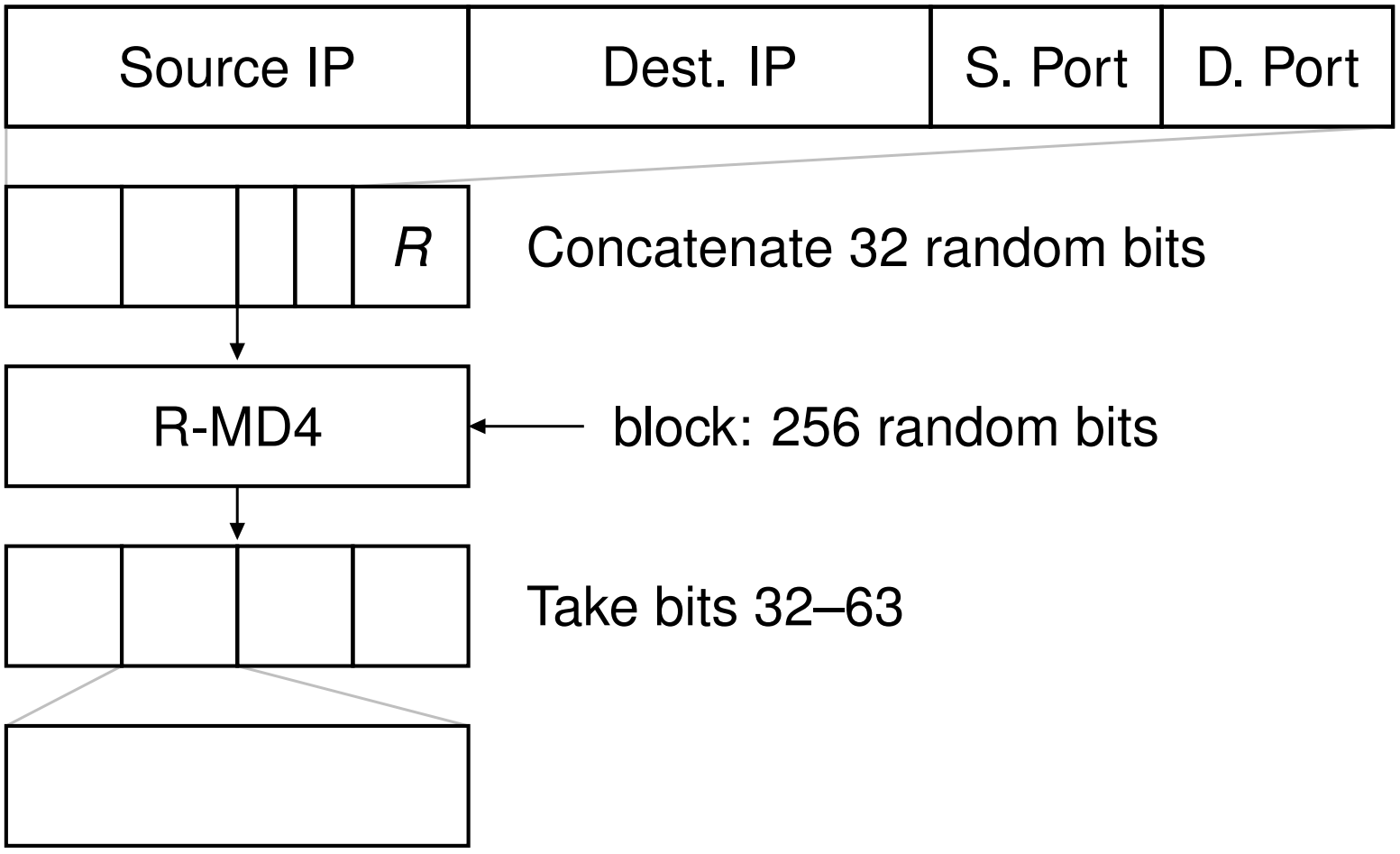
Initial sequence numbers have complex structure



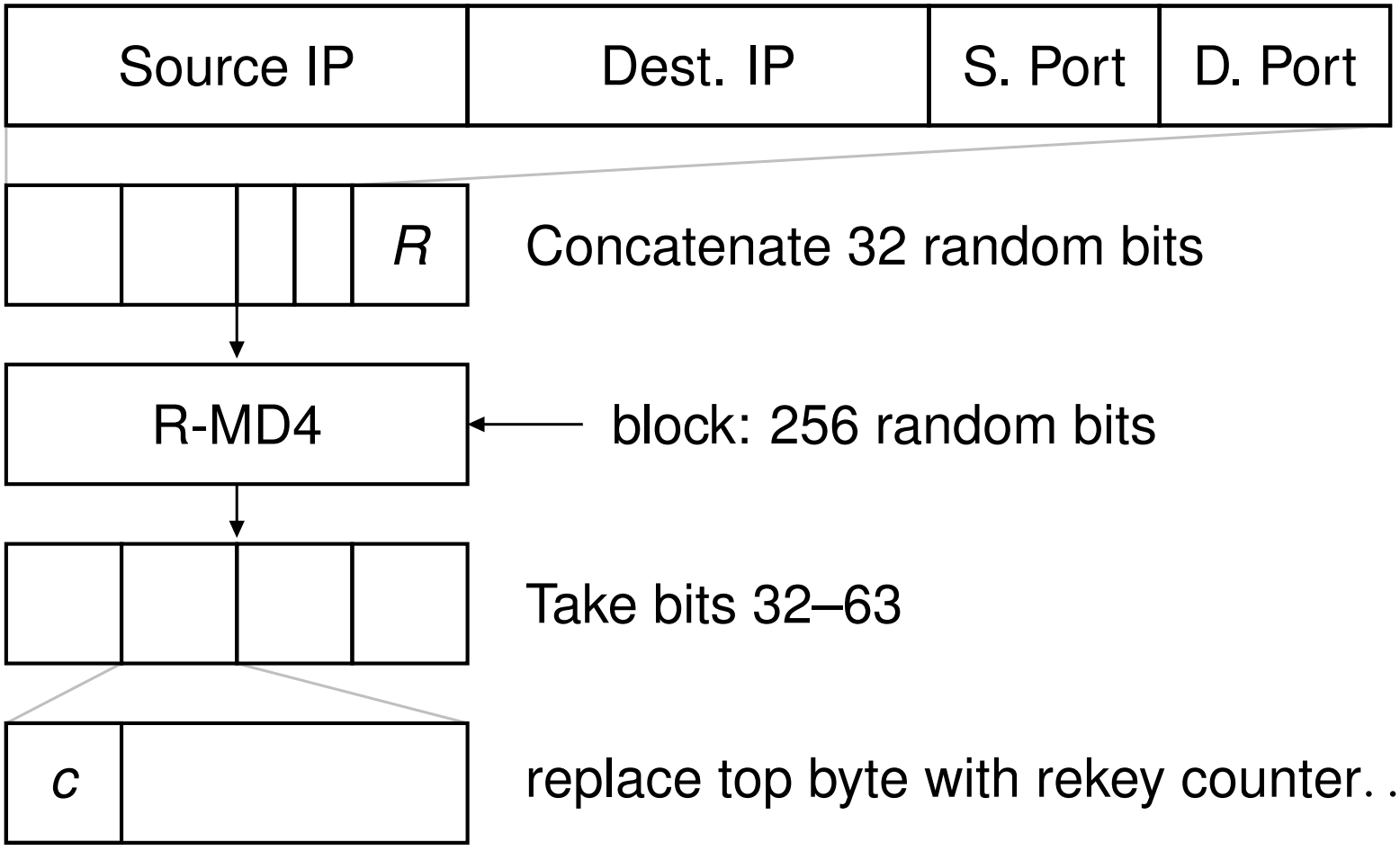
Initial sequence numbers have complex structure



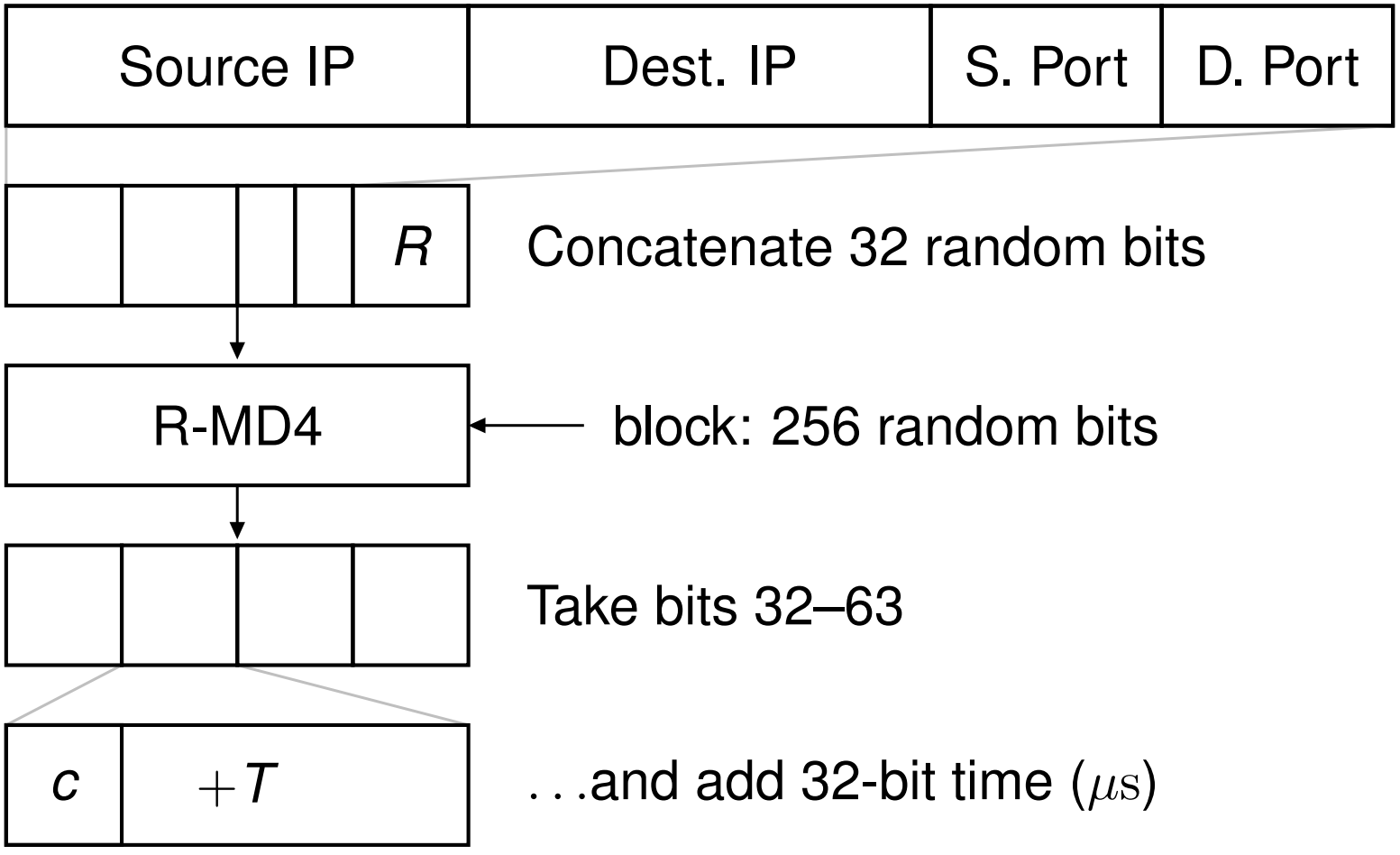
Initial sequence numbers have complex structure



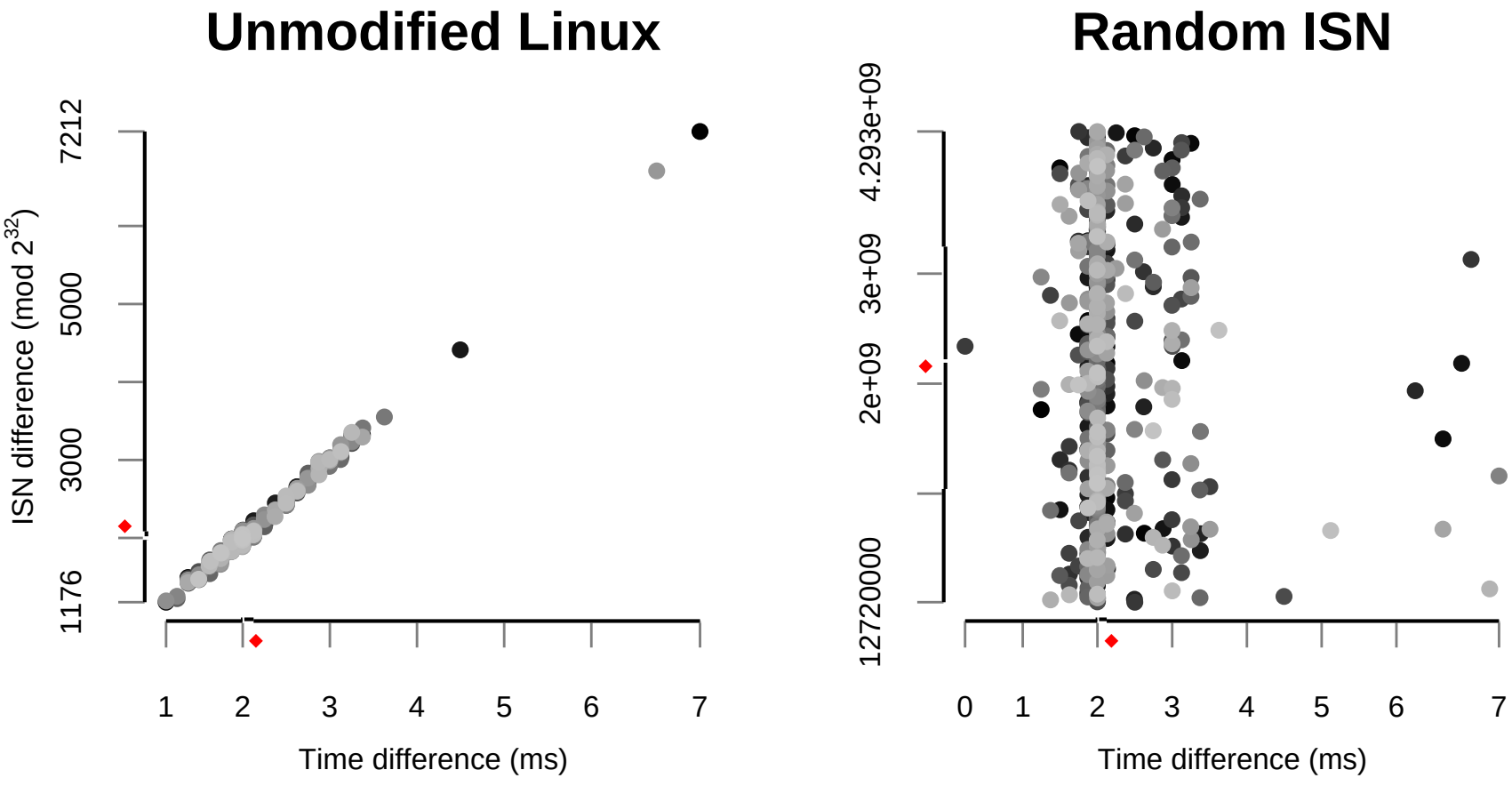
Initial sequence numbers have complex structure



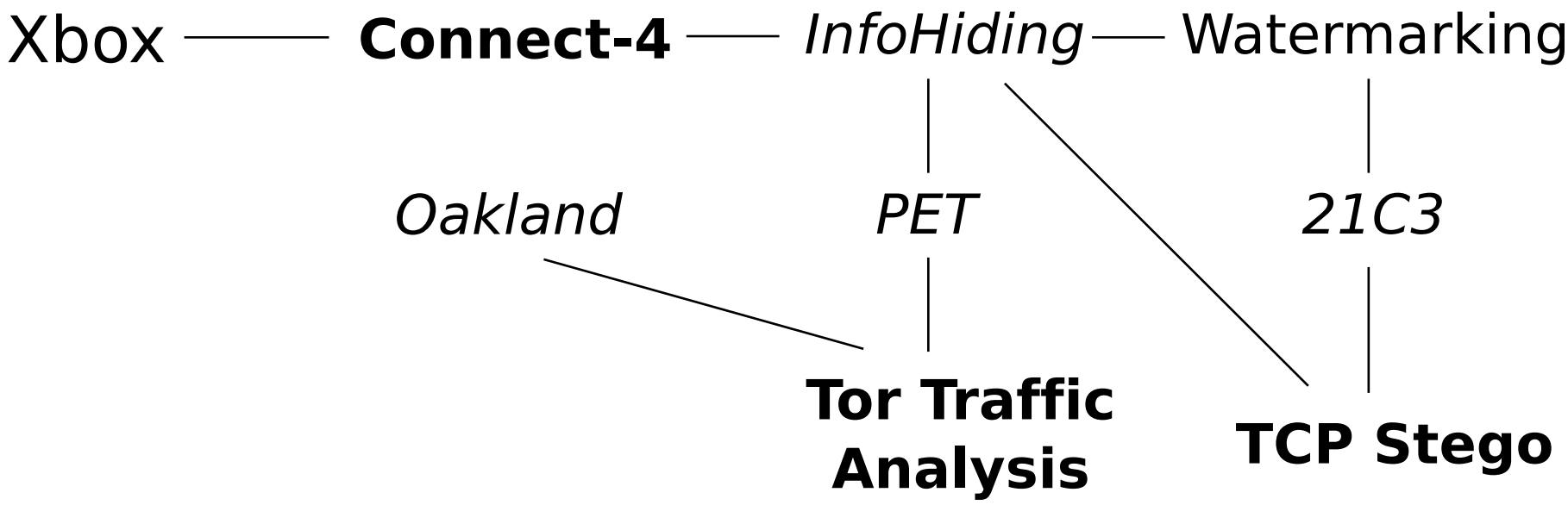
Initial sequence numbers have complex structure



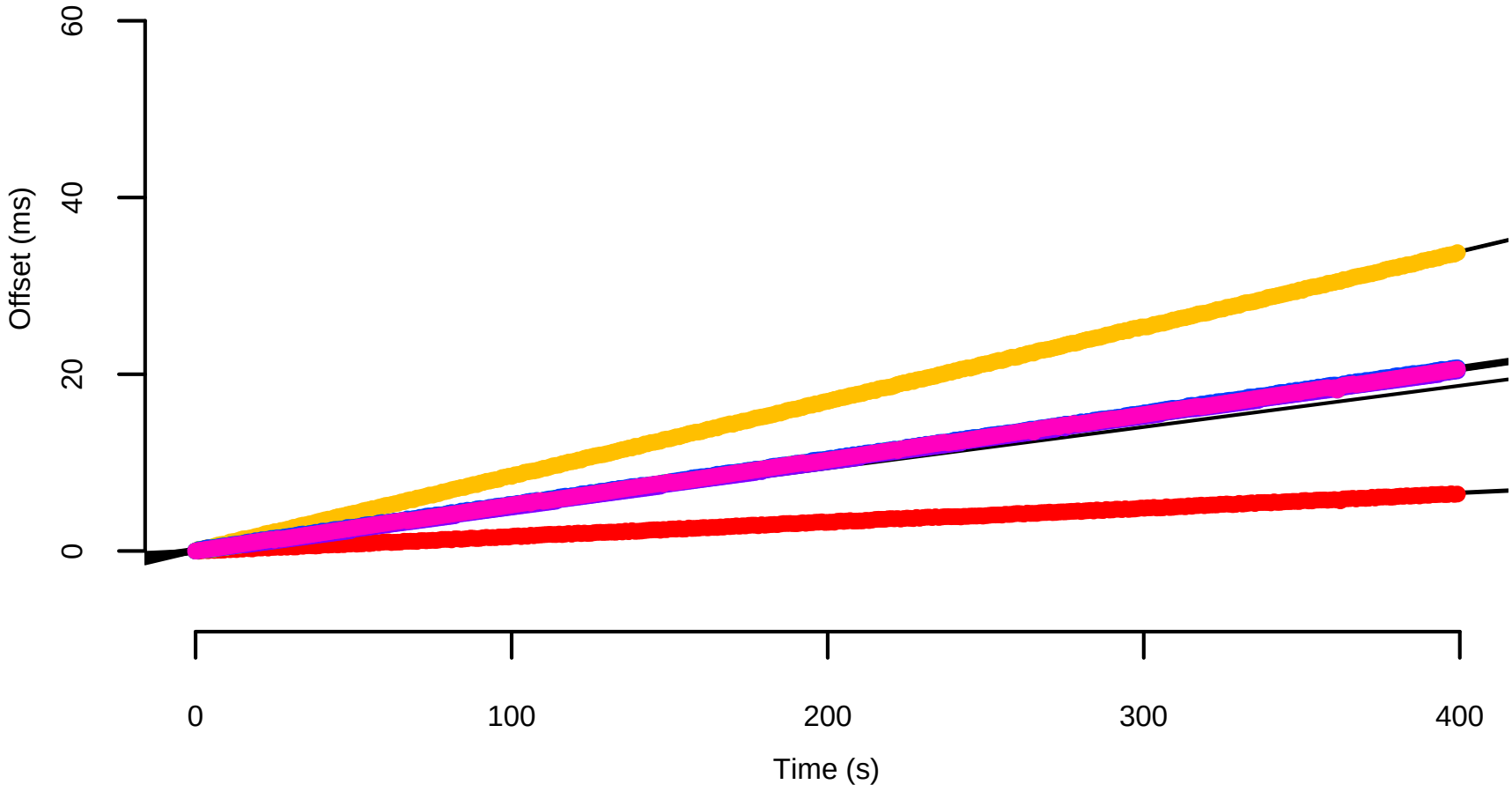
Even putting perfectly random ISNs will be detectable



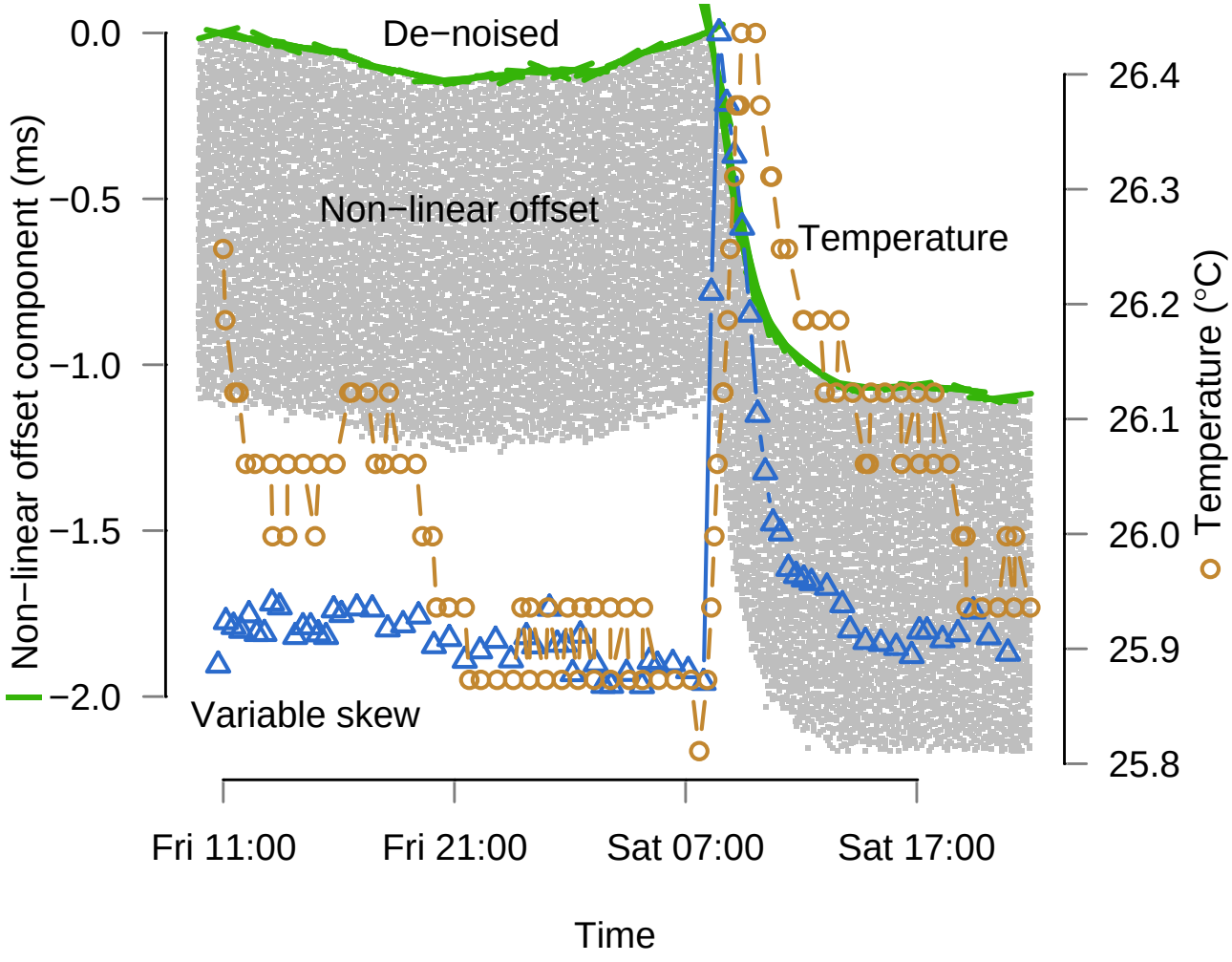
We wrote a paper on TCP steganography for InfoHiding 2005



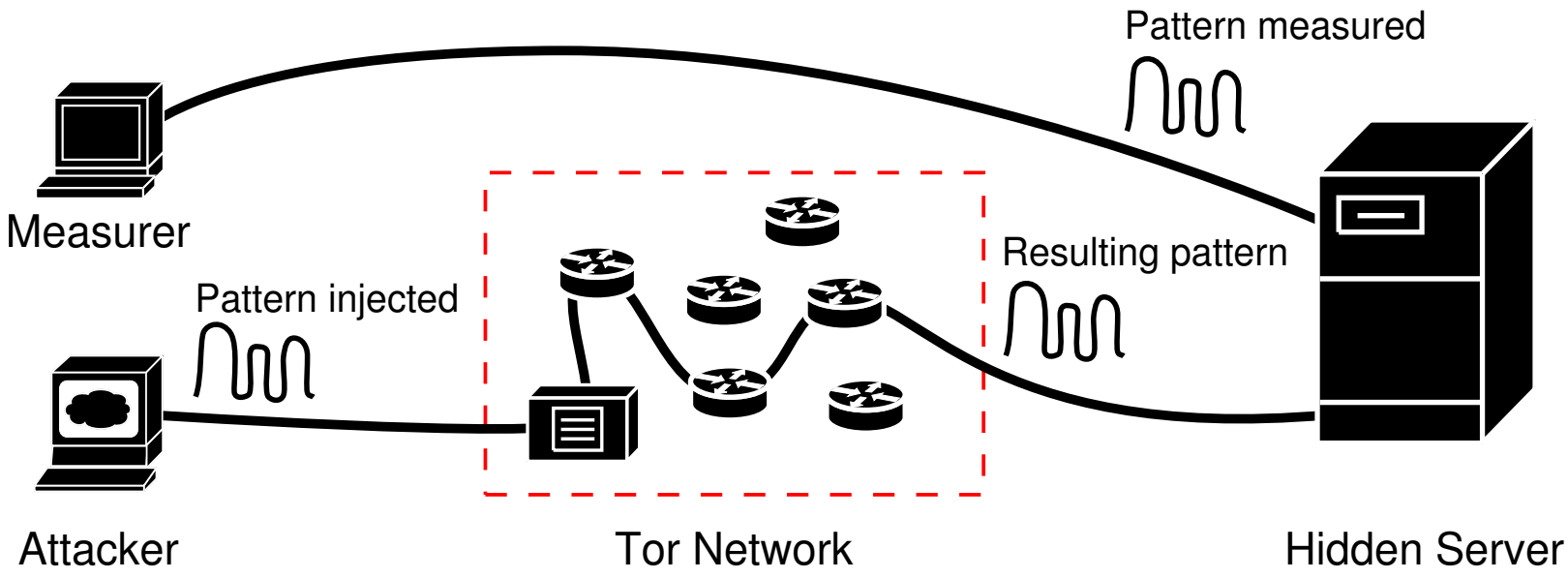
At Oakland 2005 I attended a talk on clock skew and security



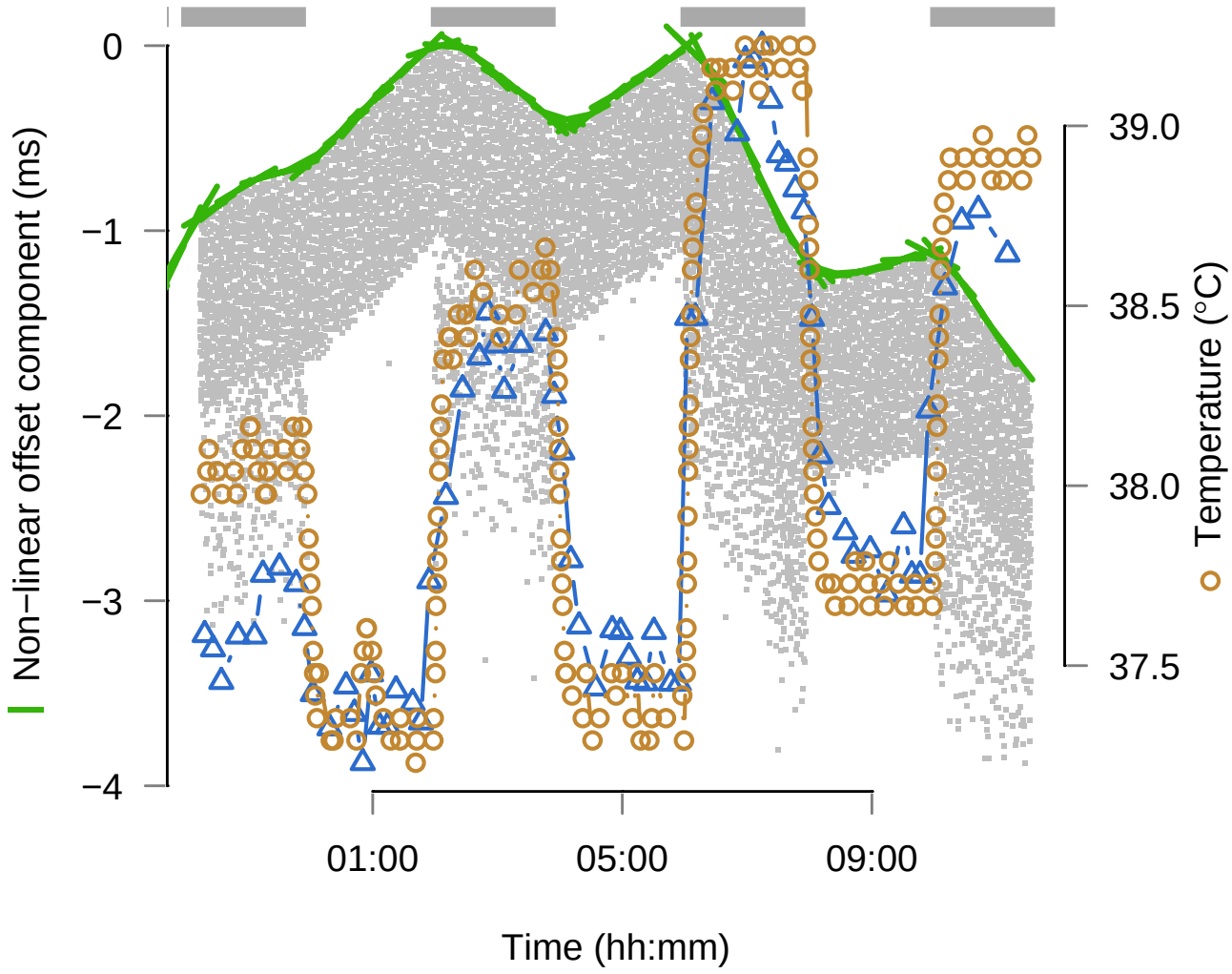
Clock skew changes with temperature



We can do the same attack on Tor, measuring skew rather than latency



The results show clear patterns



From these results, I wrote my thesis