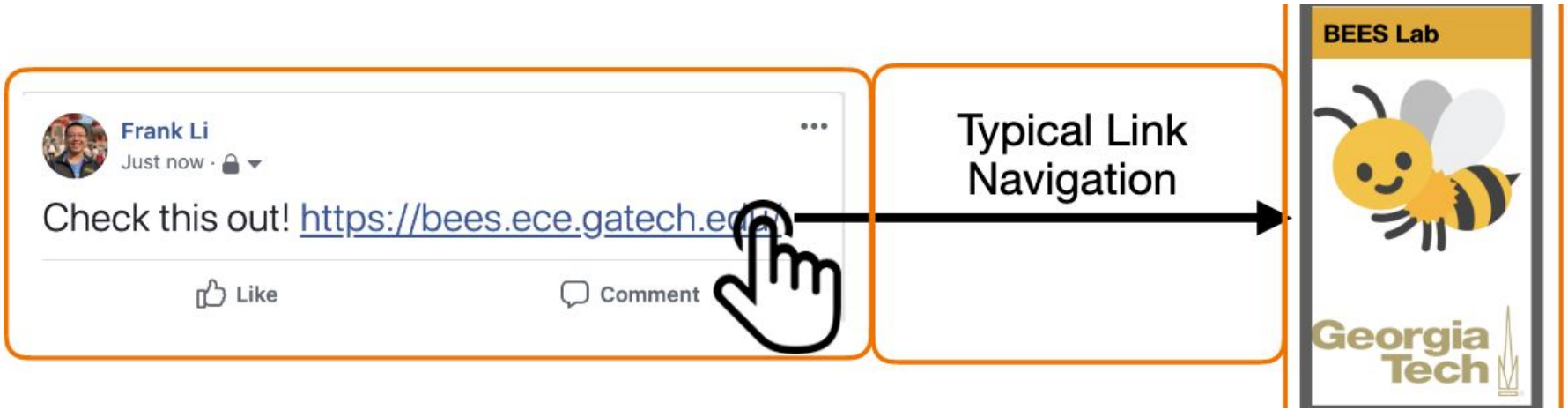
End-to-End Privacy for Link Shimming using Private Information Retrieval

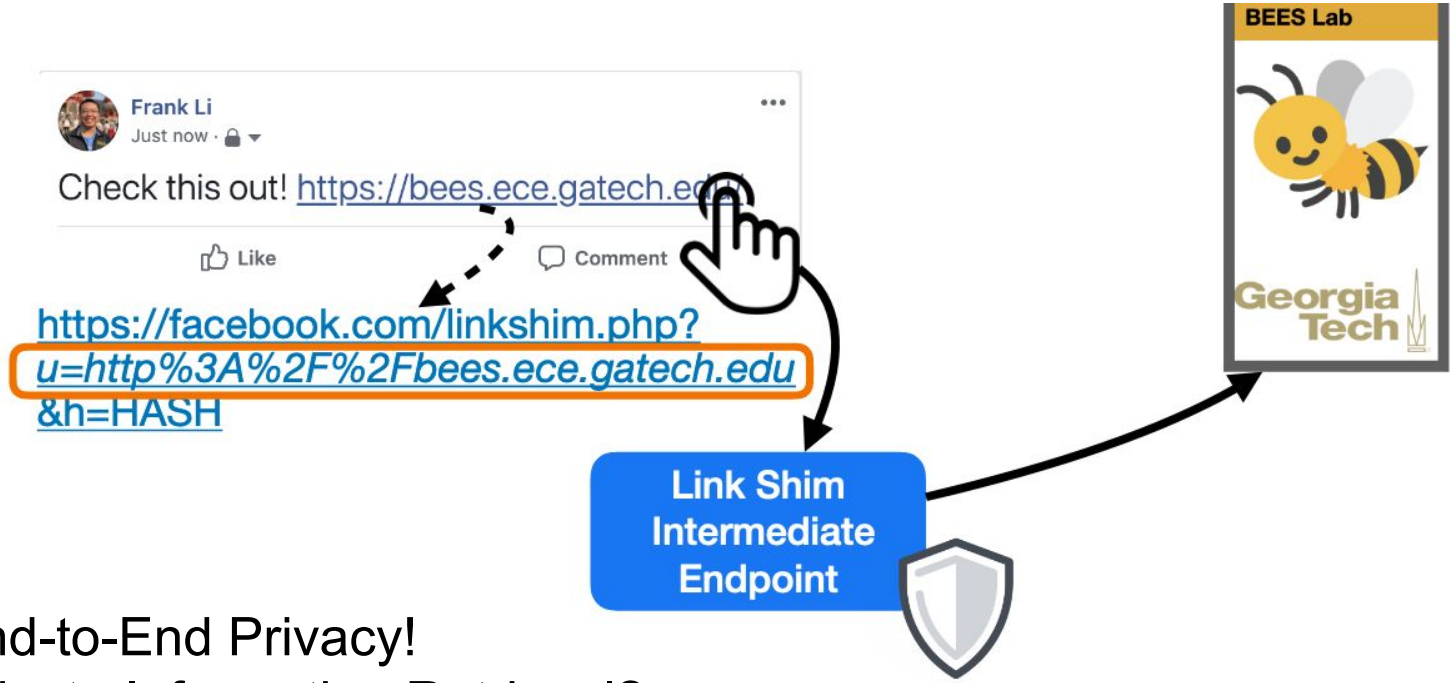
CSC 533
Group 2

How does a typical link navigation look like?



From Frank Li's slides, Georgia Tech

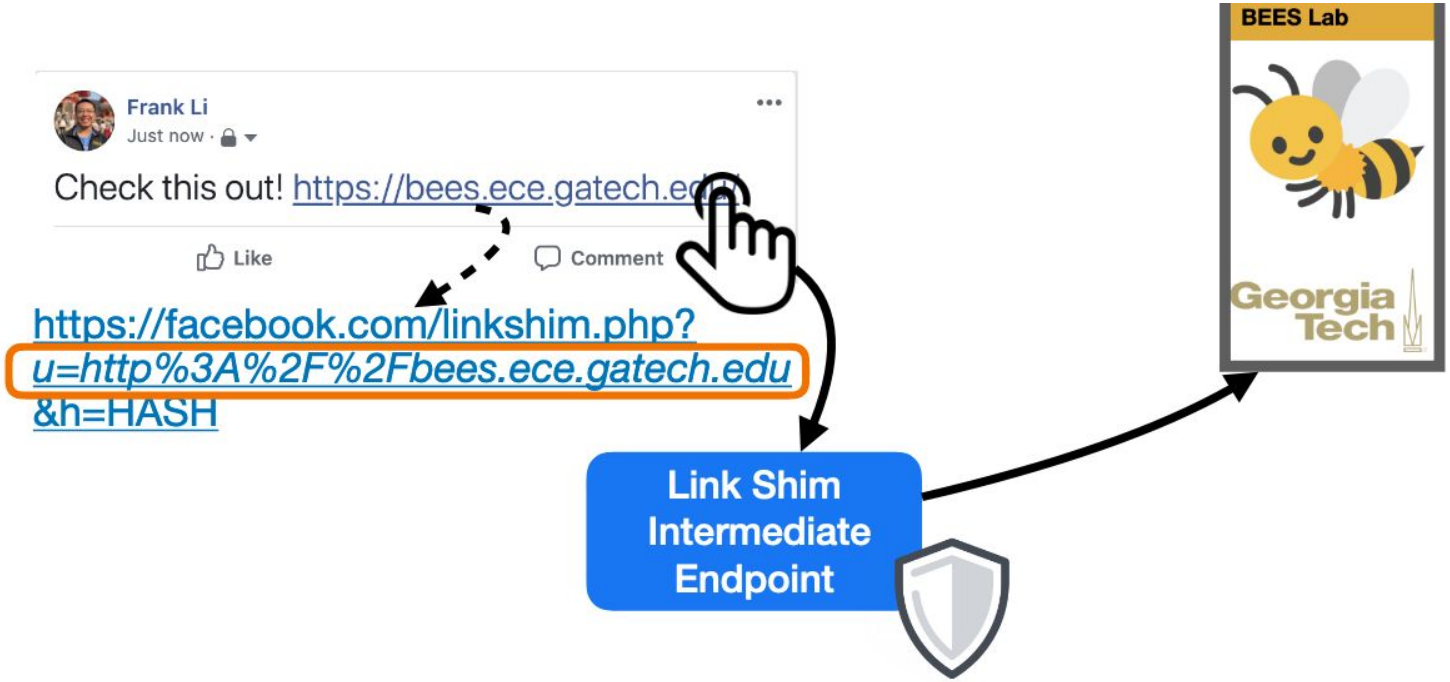
Should the server know which link you clicked?



End-to-End Privacy!
Private Information Retrieval?

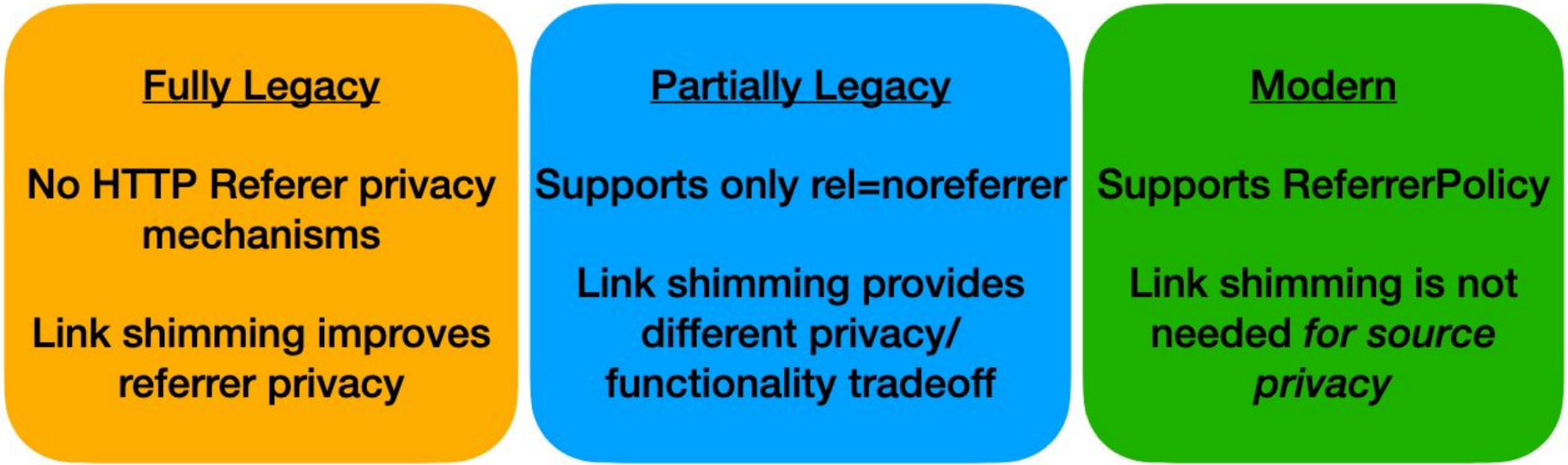
From Frank Li's slides,
Georgia Tech

What is link shimming?



From Frank Li's slides, Georgia Tech

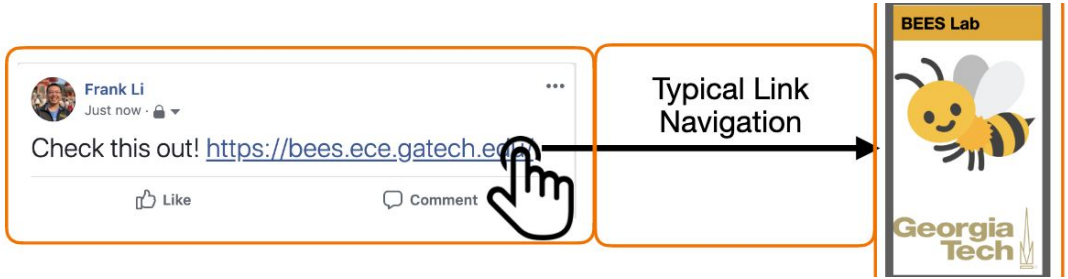
Privacy?



From Frank Li's slides, Georgia Tech

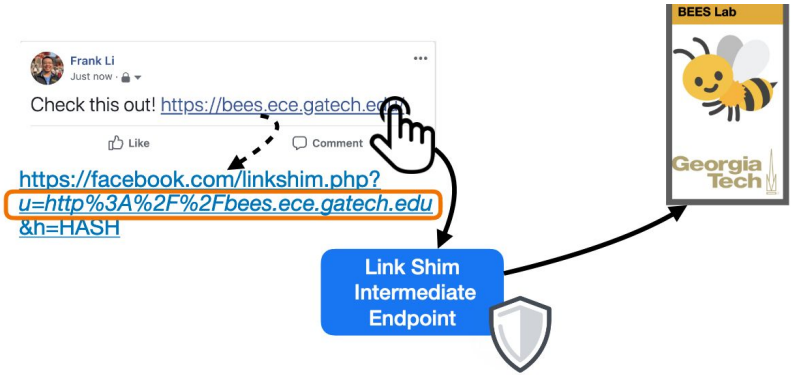
End-to-End Privacy for Link Shimming using Private Information Retrieval

Typical link navigation

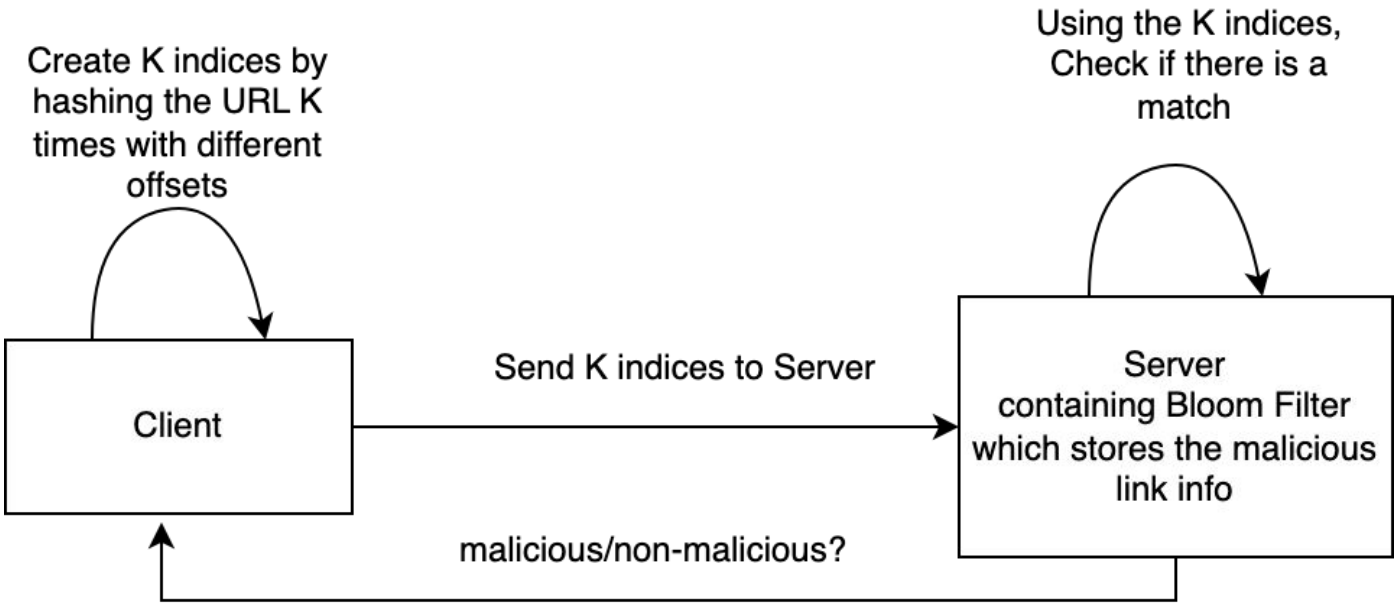


How to achieve end-to-end privacy?

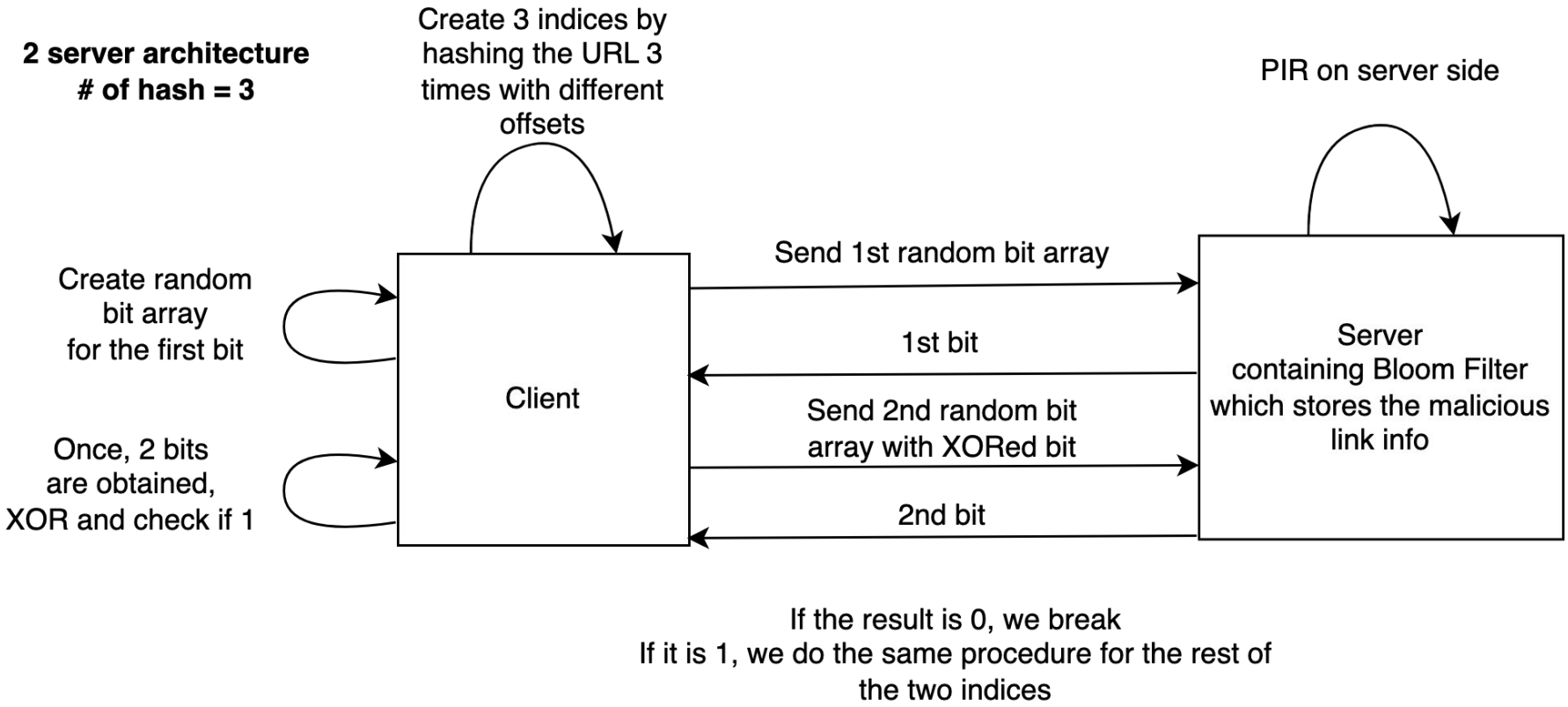
Link Shimming



How to detect malicious URLs using a bloom filter?

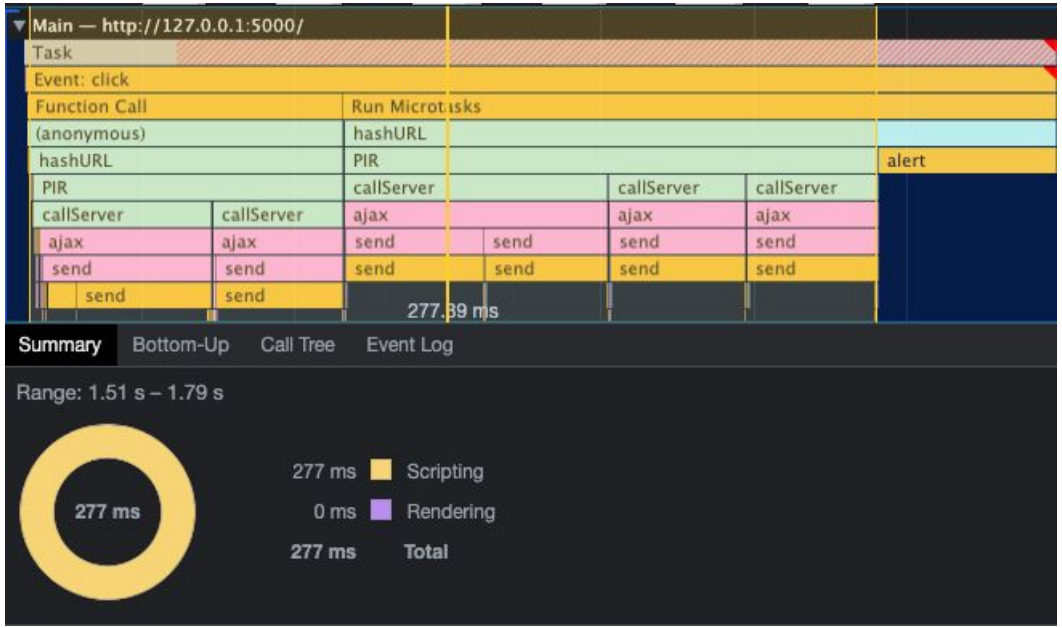


Our architecture (variant of 2-PIR - $O(n^{0.5})$ communication)

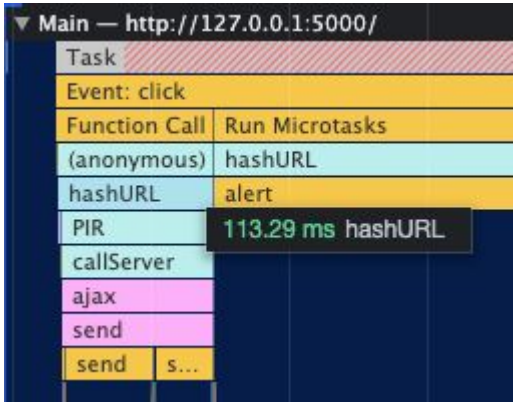


Performance

Better runtime performance than *Chielle et al. 2021, Real-time Private Membership Test using Homomorphic Encryption* - on dataset of size 2^{14} for False Positive of 0.0001.

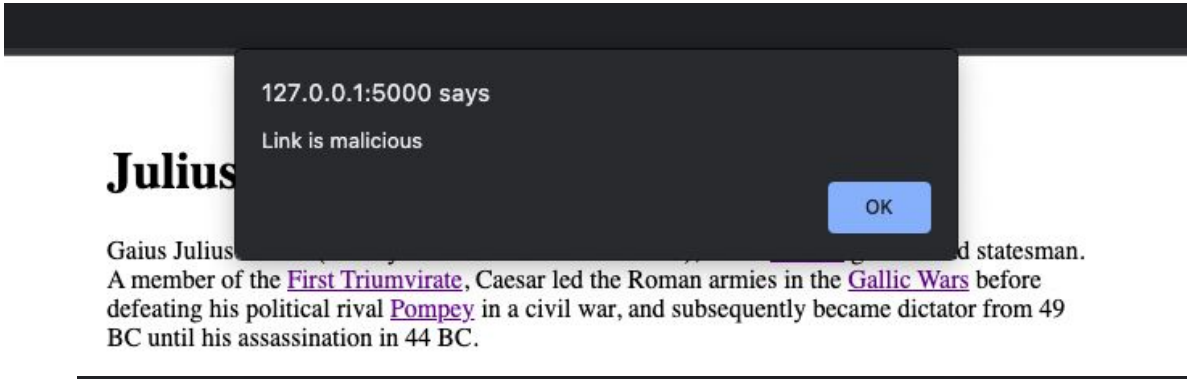


Malicious



Safe

Demo



https://github.com/pncnmnp/shimmey

Next Steps

- More extensive literature survey with comparison studies
- Performance improvements from Multi-bit PIR?
  - Researching the work done by Dr. Sennur Ulukus' lab - University of Maryland
- Show our findings in the report

Questions?

End of the Presentation