Negotiation Transparency in Configurable Protocols

A Case Study in the TLS Protocol and the Forward Secrecy Property

Eman Alashwali

October 2019

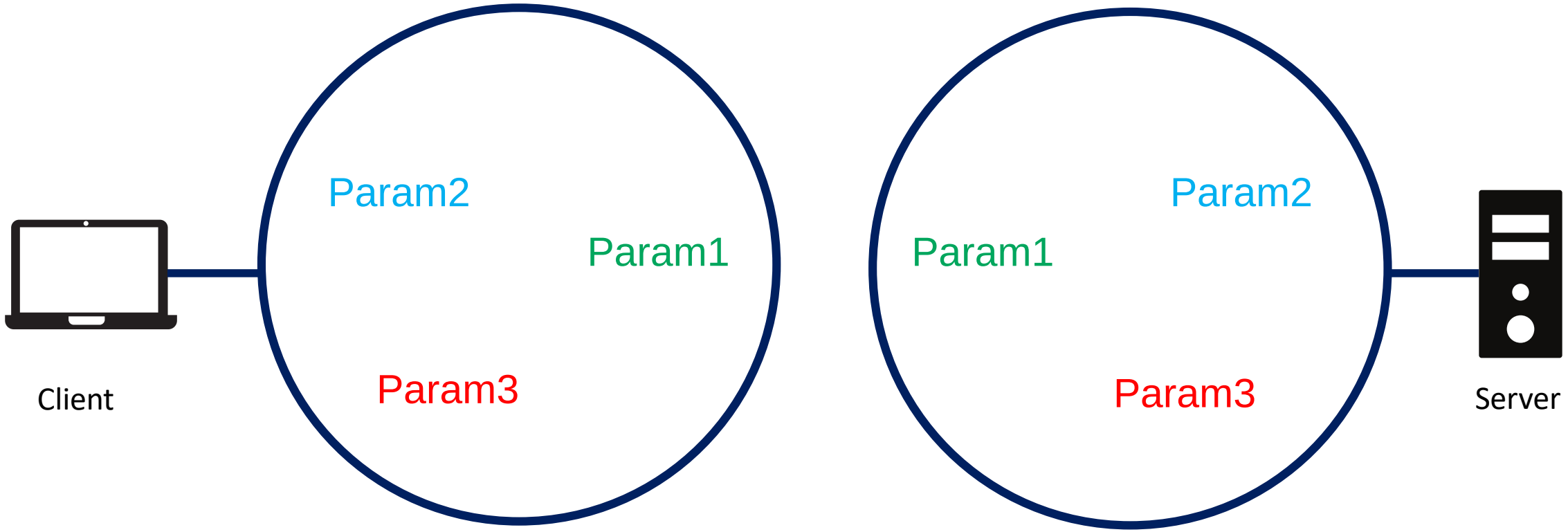
Outline

- Problem
- New adversarial model
- Experiment results
- Recommendations
- Conclusion

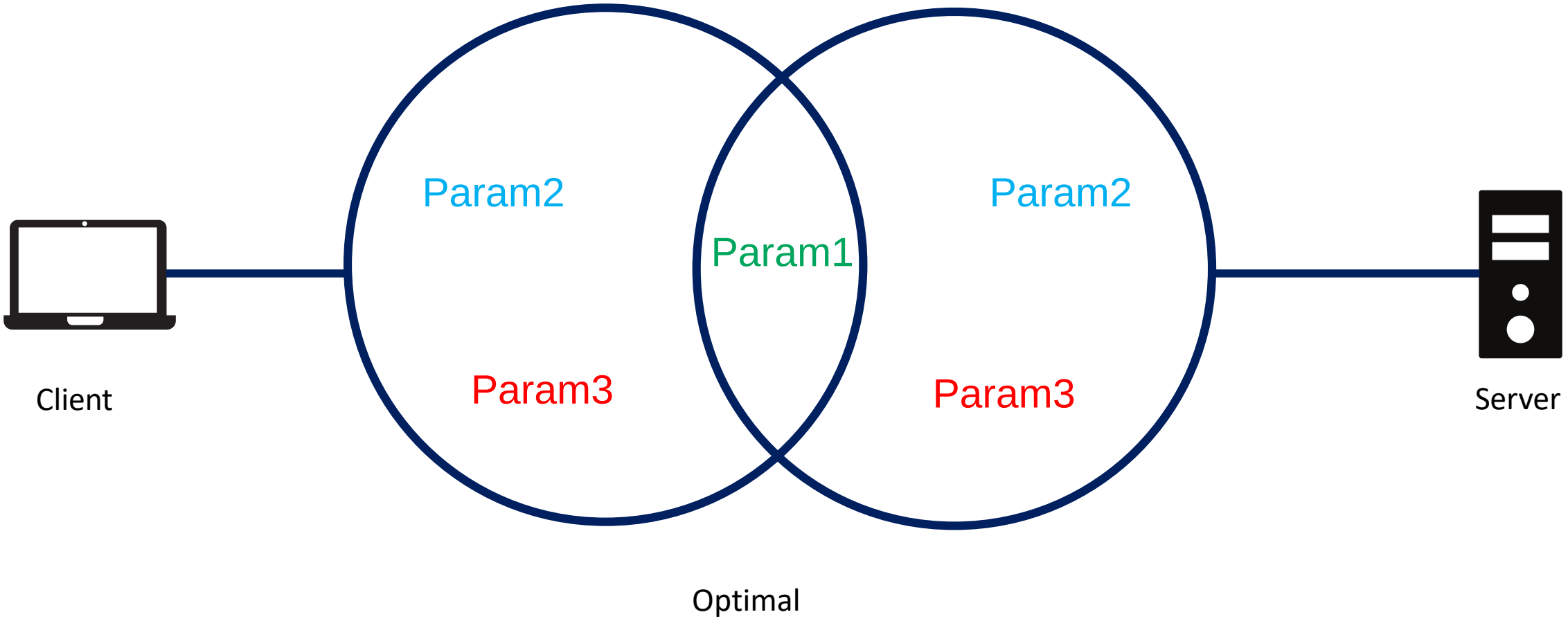
Negotiation

Security Parameters Negotiation

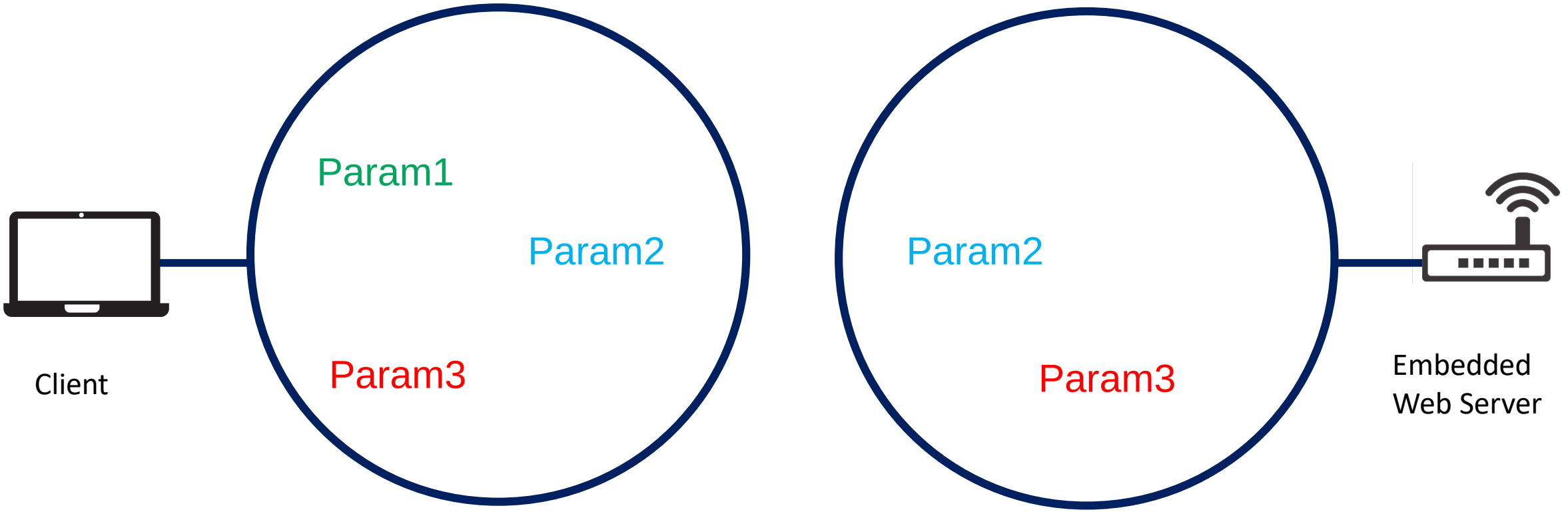
Security Parameters Negotiation



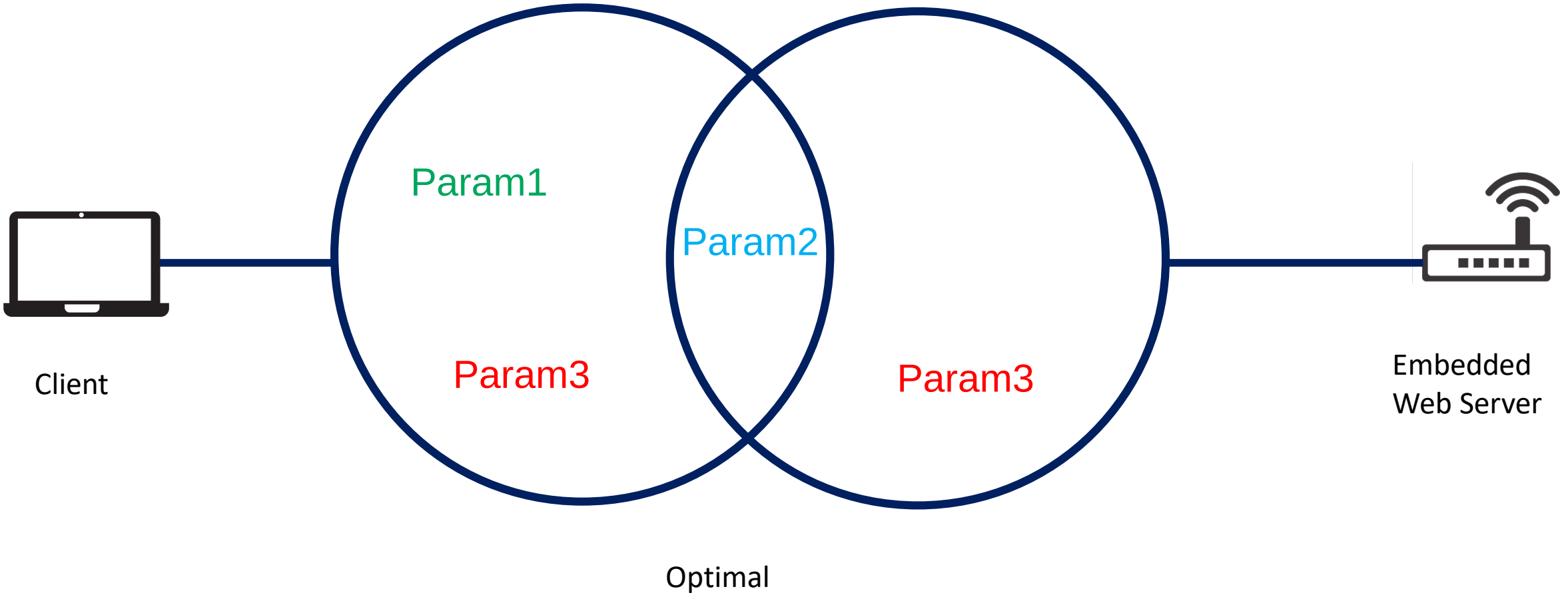
Security Parameters Negotiation



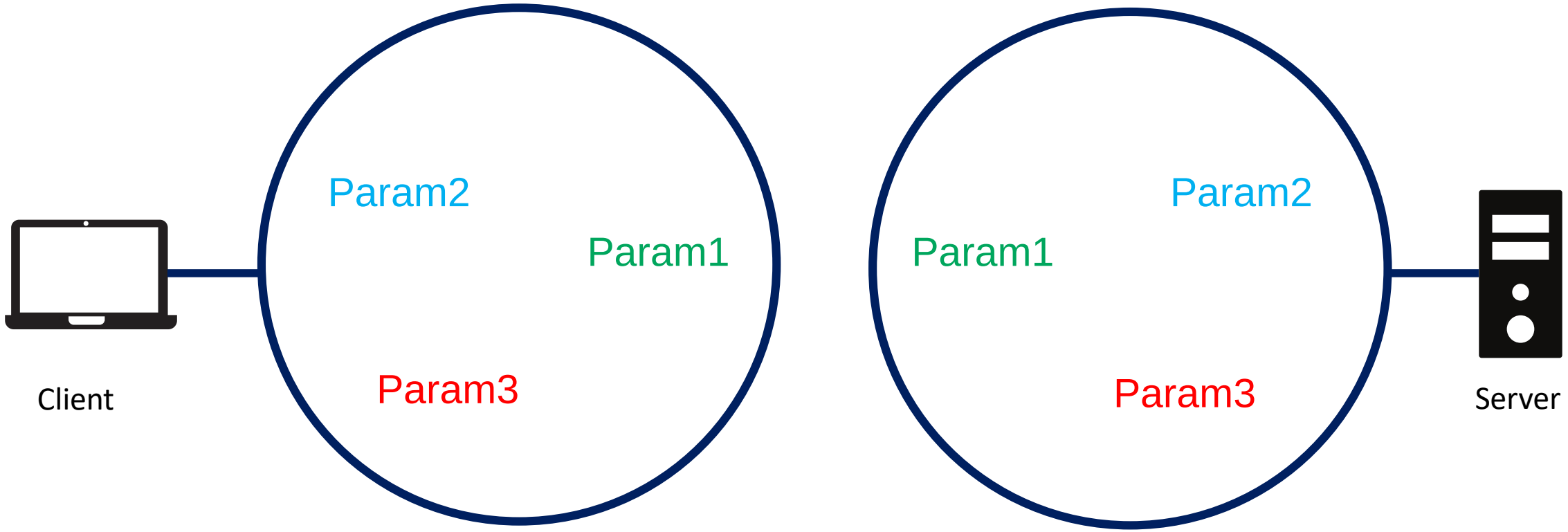
Security Parameters Negotiation



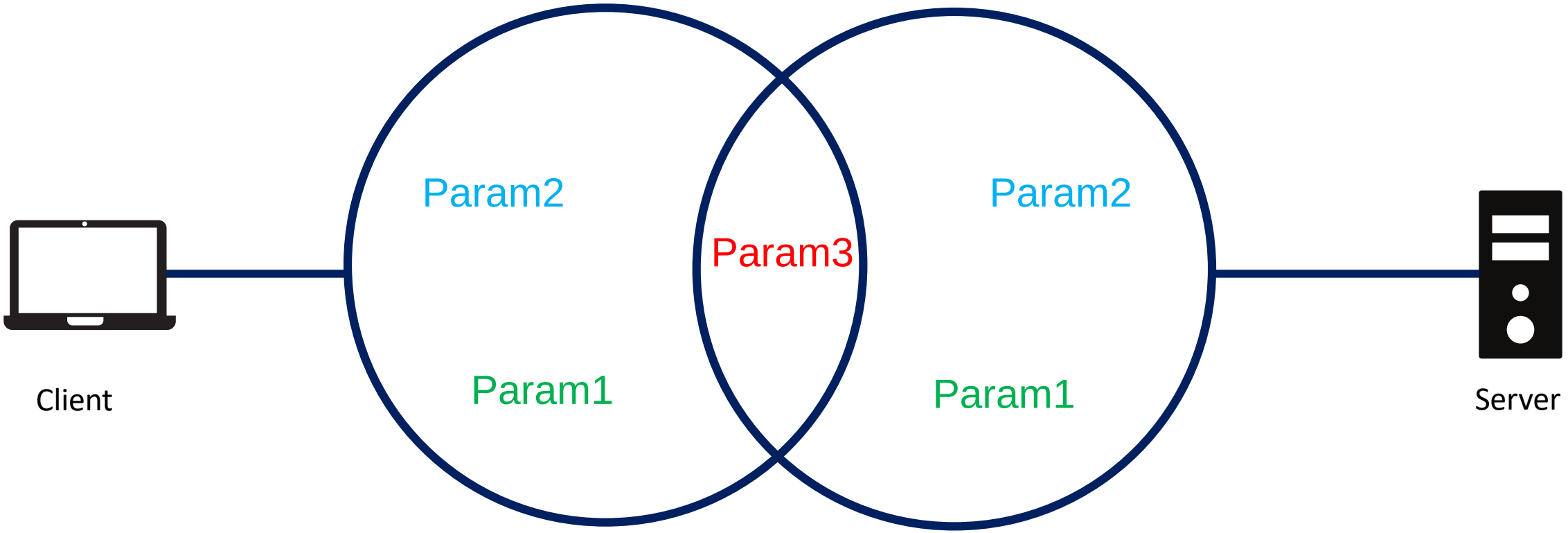
Security Parameters Negotiation



Security Parameters Negotiation



Security Parameters Negotiation



Less than Optimal / Downgrade

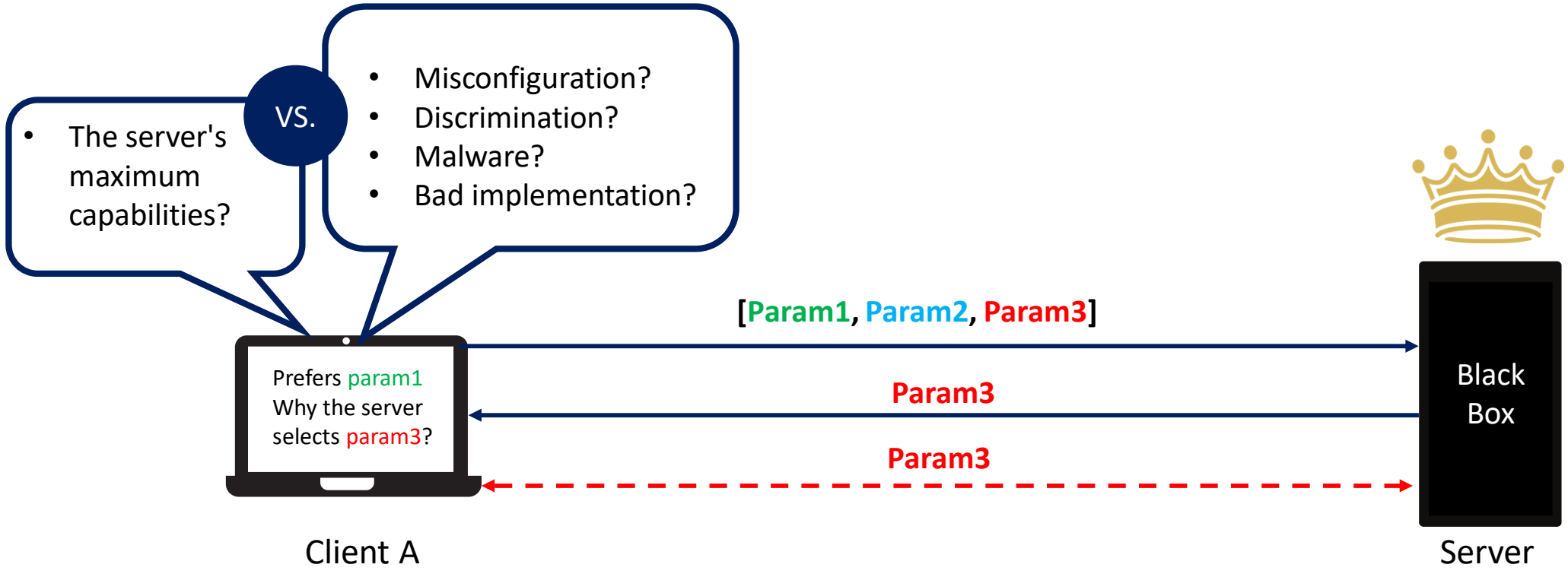
Questions?

- Are there unexplored adversarial models that result in a downgrade?
- To what extent such downgrades are prevalent in real-world protocols deployment?

Contributions

- Introduce a new adversarial model
  - The “discriminatory” adversarial model
- Empirical study on the Forward Secrecy property and the TLS protocol

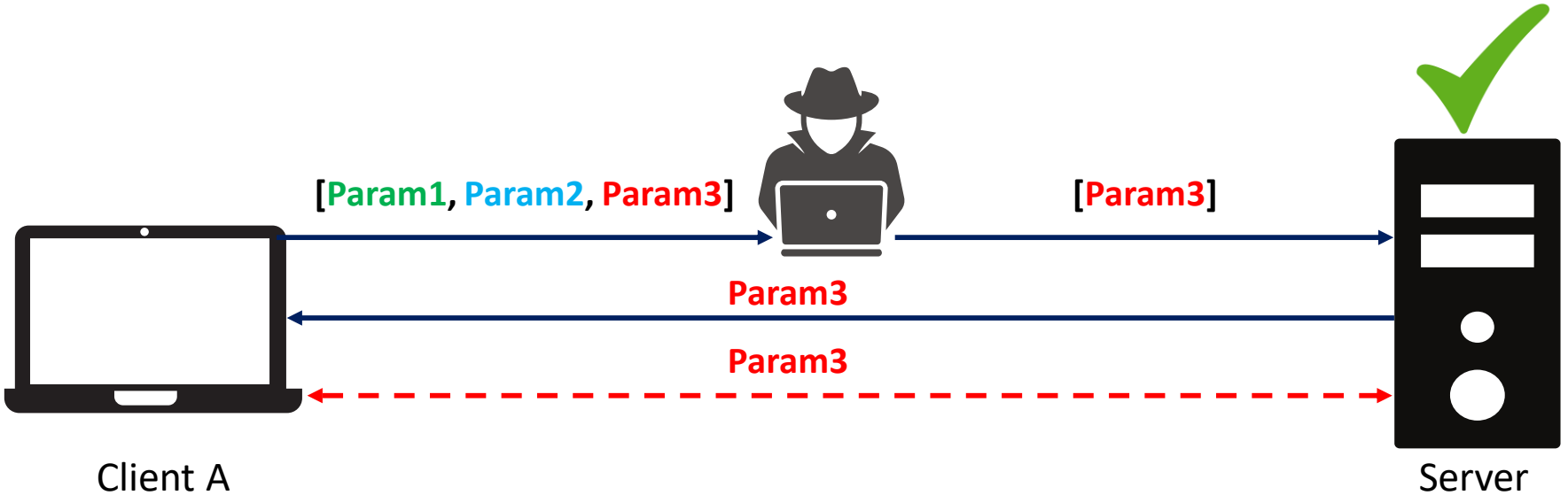
Ciphersuites Negotiation in TLS



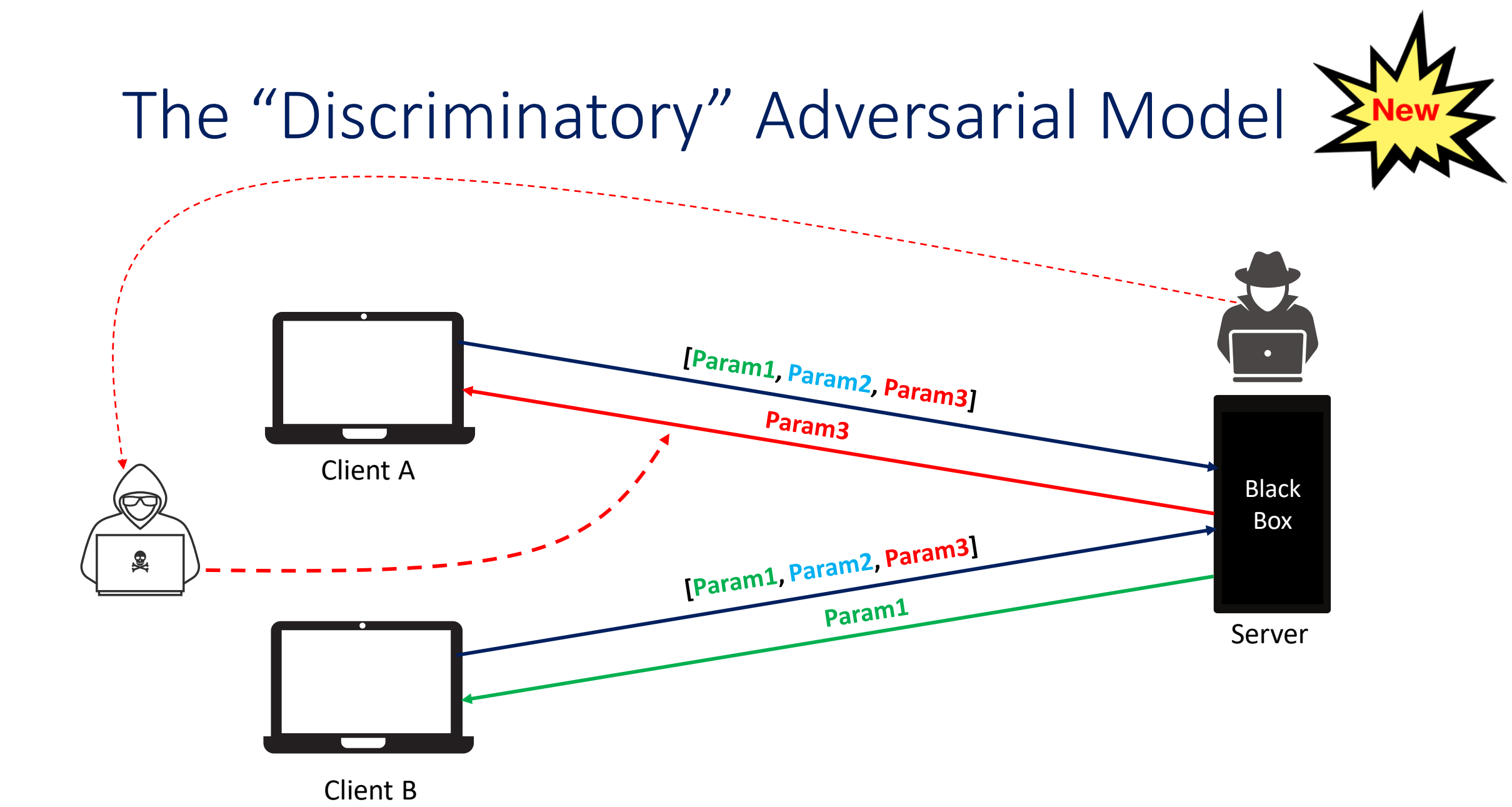
New

Server-dominant negotiation model

The Man-in-the-Middle Adversarial Model



The “Discriminatory” Adversarial Model



Realistic Model?

- In fact, it is inspired by real-life events
- Export-grade Cryptography

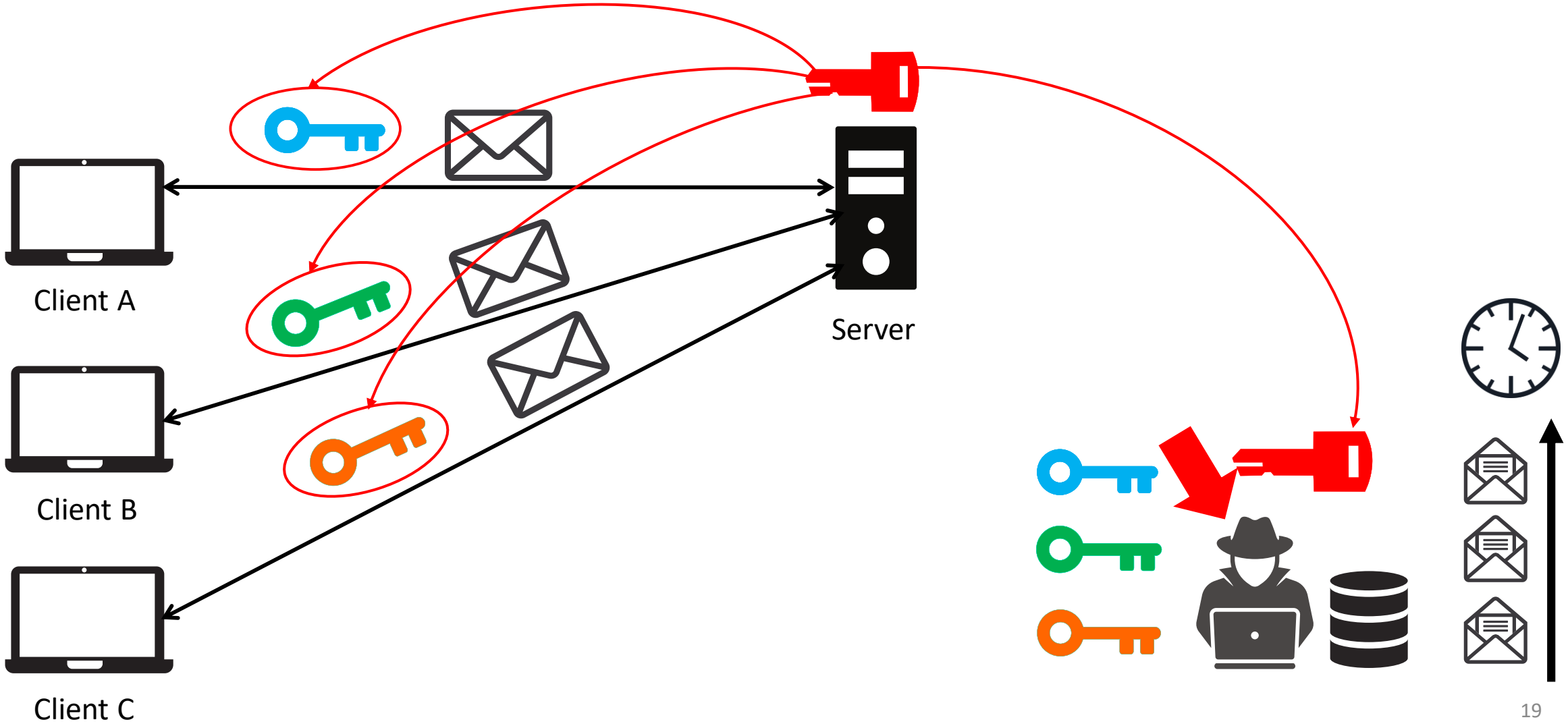
“…cryptography beyond a certain strength […] would not be licensed for export…”

- PRISM

Case Study

- TLS protocol
- Forward Secrecy property

Non-Forward Secrecy (Non-FS)

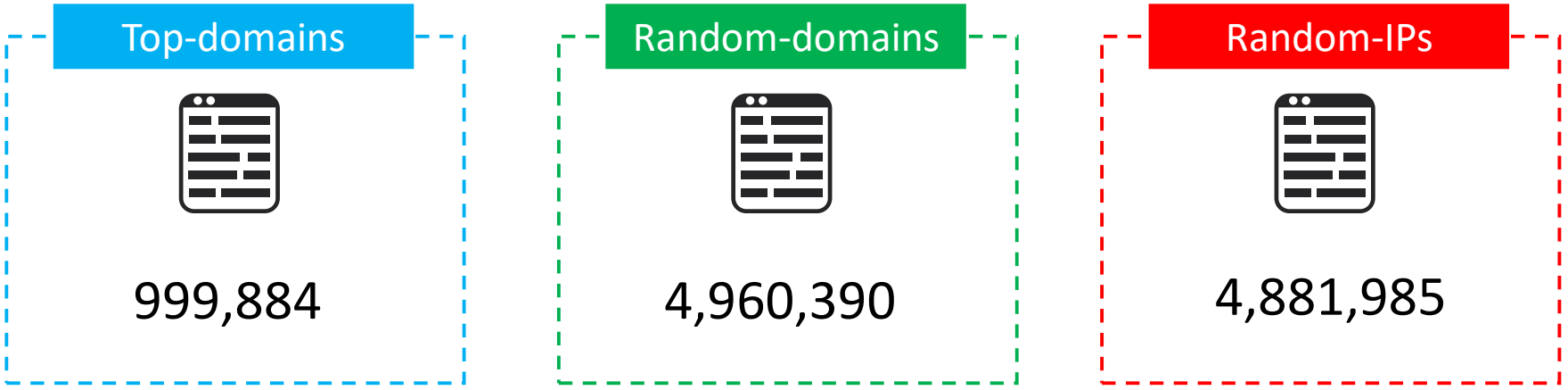


Empirical Study Question

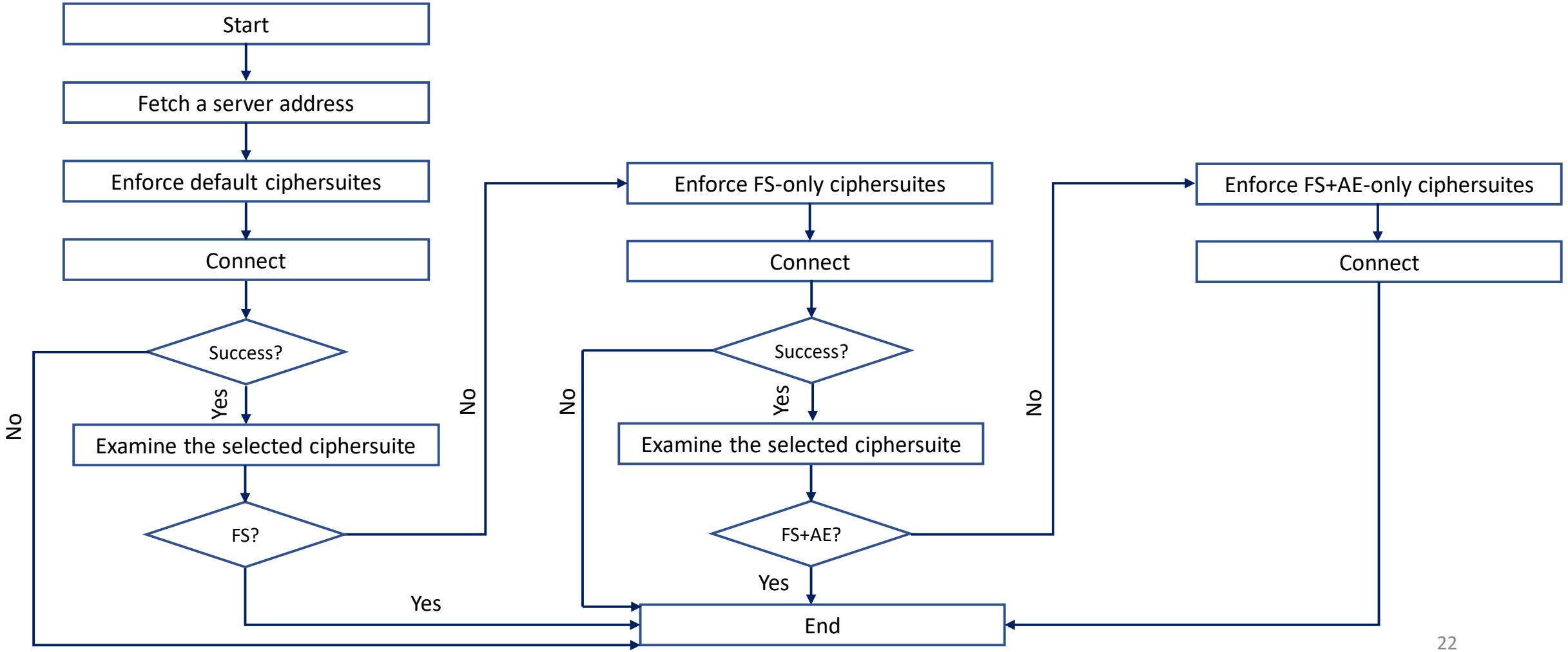
Do servers that select non-FS-ciphersuites support FS-ciphersuites?

Dataset

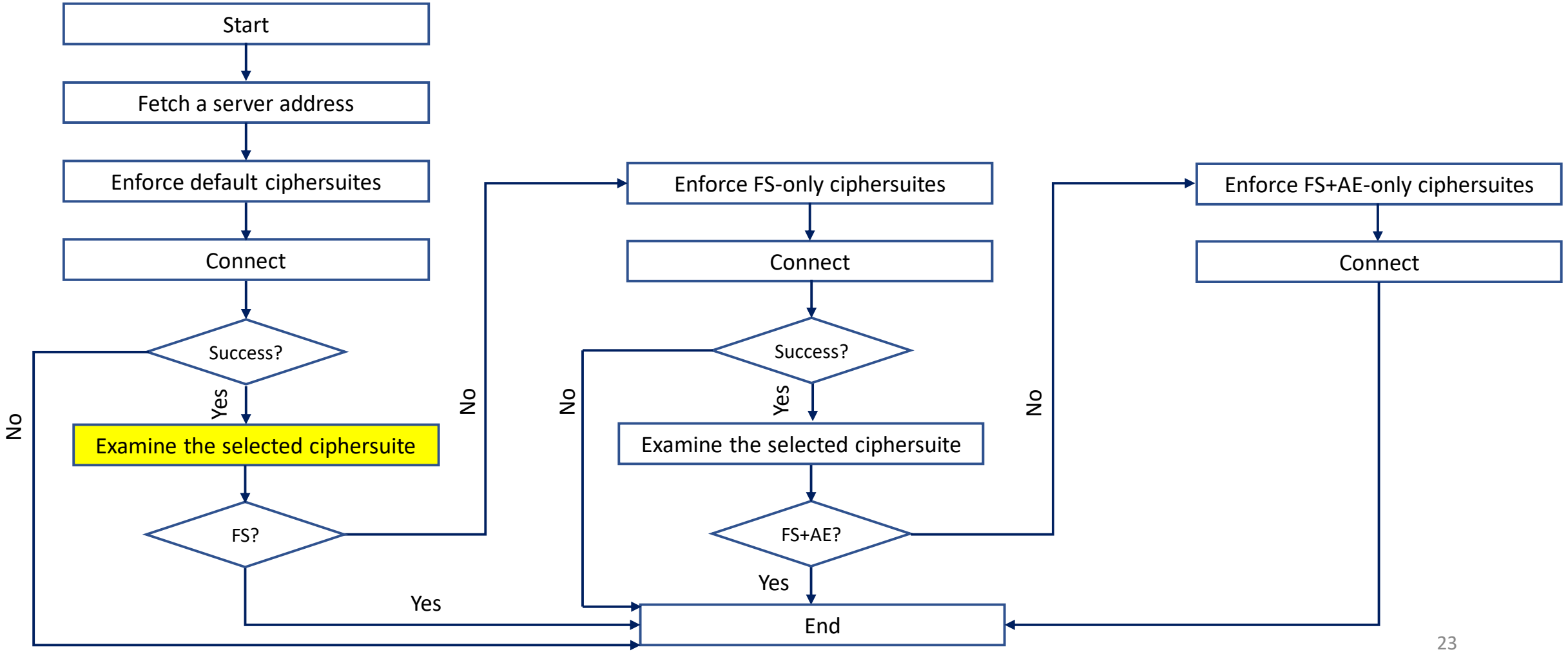
> 10 M


Top-domains
999,884
Random-domains
4,960,390
Random-IPs
4,881,985

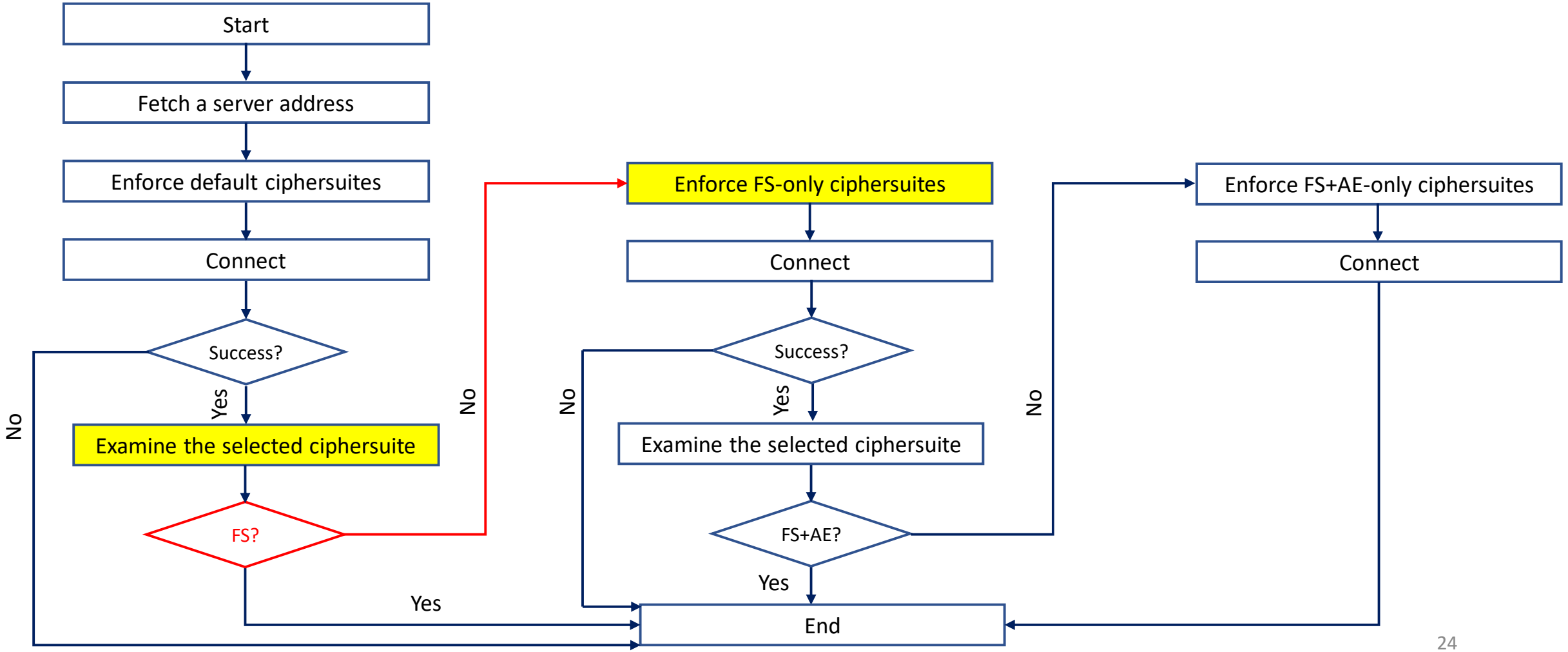
Heuristic Procedure



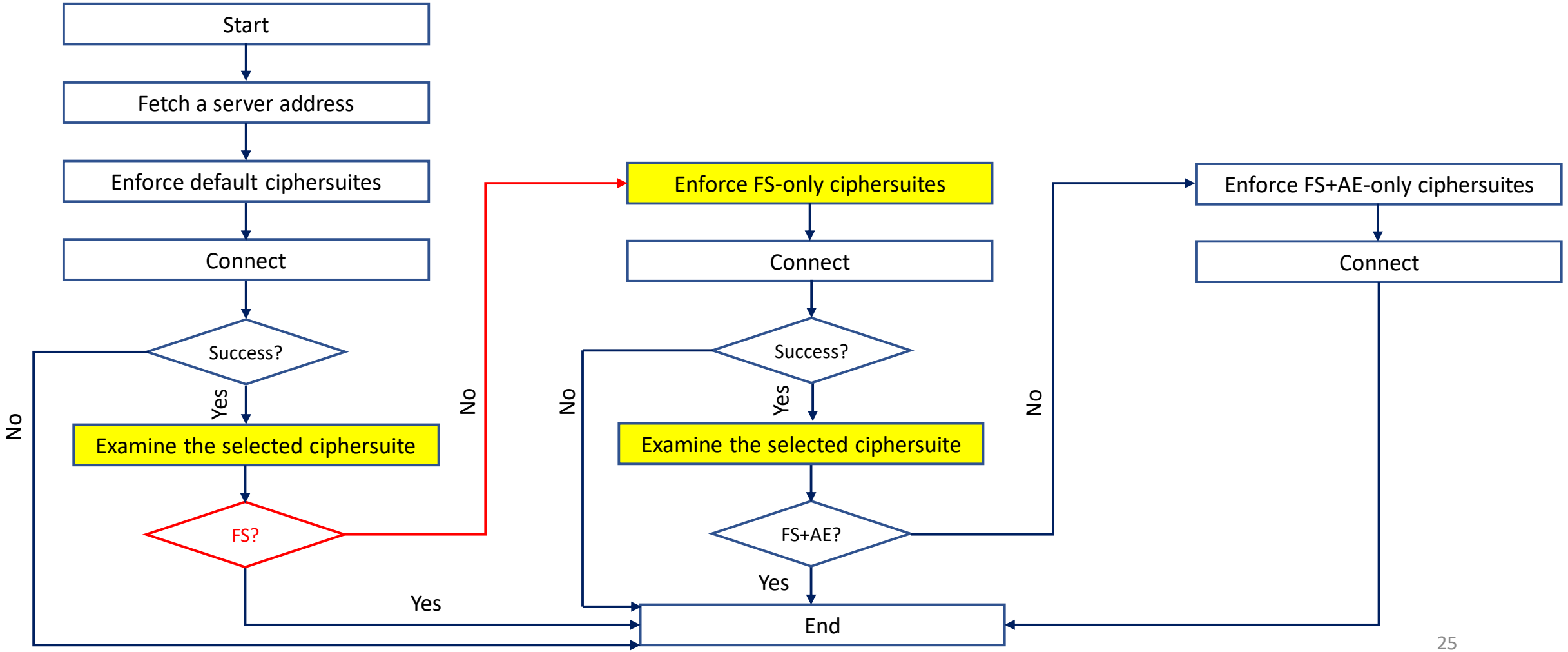
Heuristic Procedure



Heuristic Procedure



Heuristic Procedure



Results

	Dataset		
	Top-domain	Random-domain	Random-ips
Select non-FS	**5.37%**	**7.51%**	**26.16%**

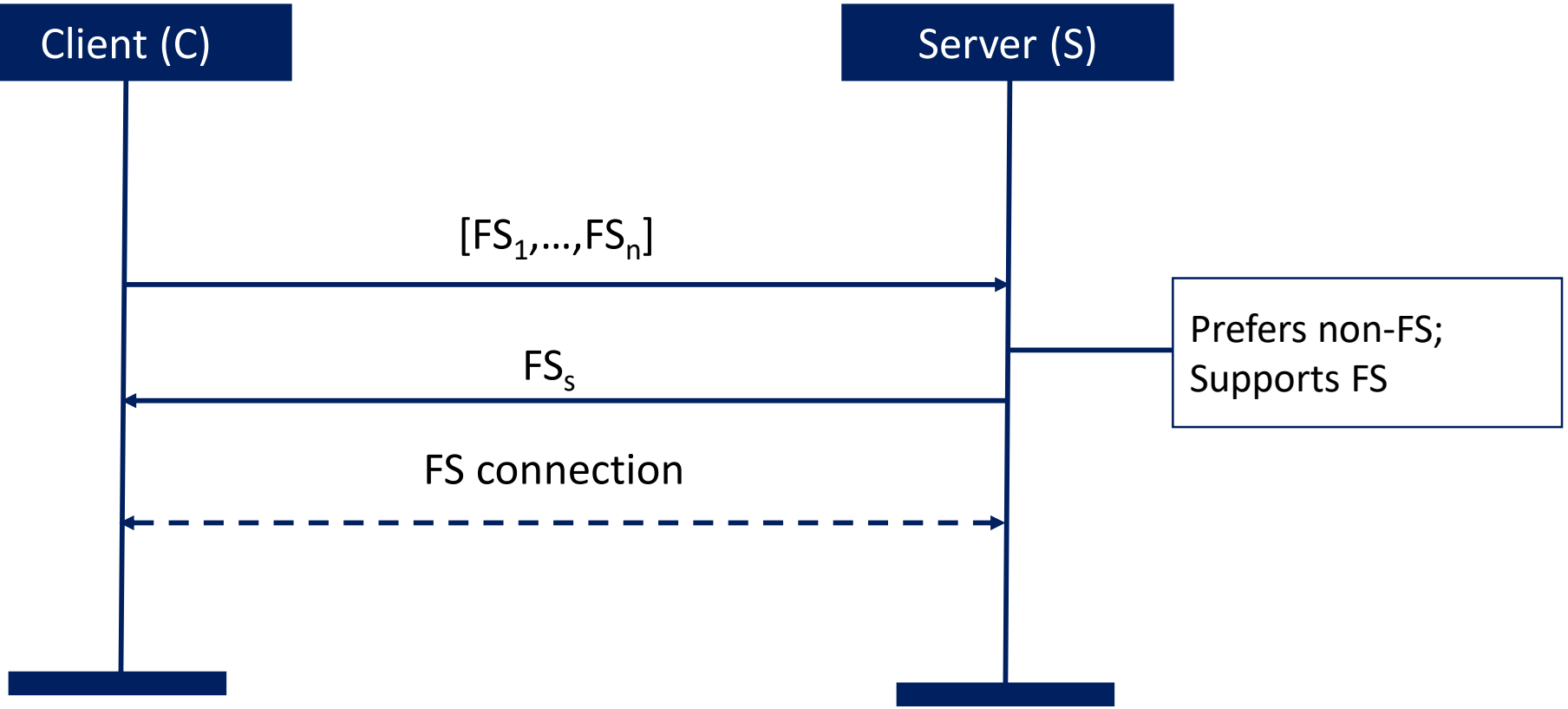
Results

	Dataset		
	Top-domain	Random-domain	Random-ips
Select non-FS	**5.37%**	**7.51%**	**26.16%**
Support FS	**39.20%**	**24.40%**	**14.46%**

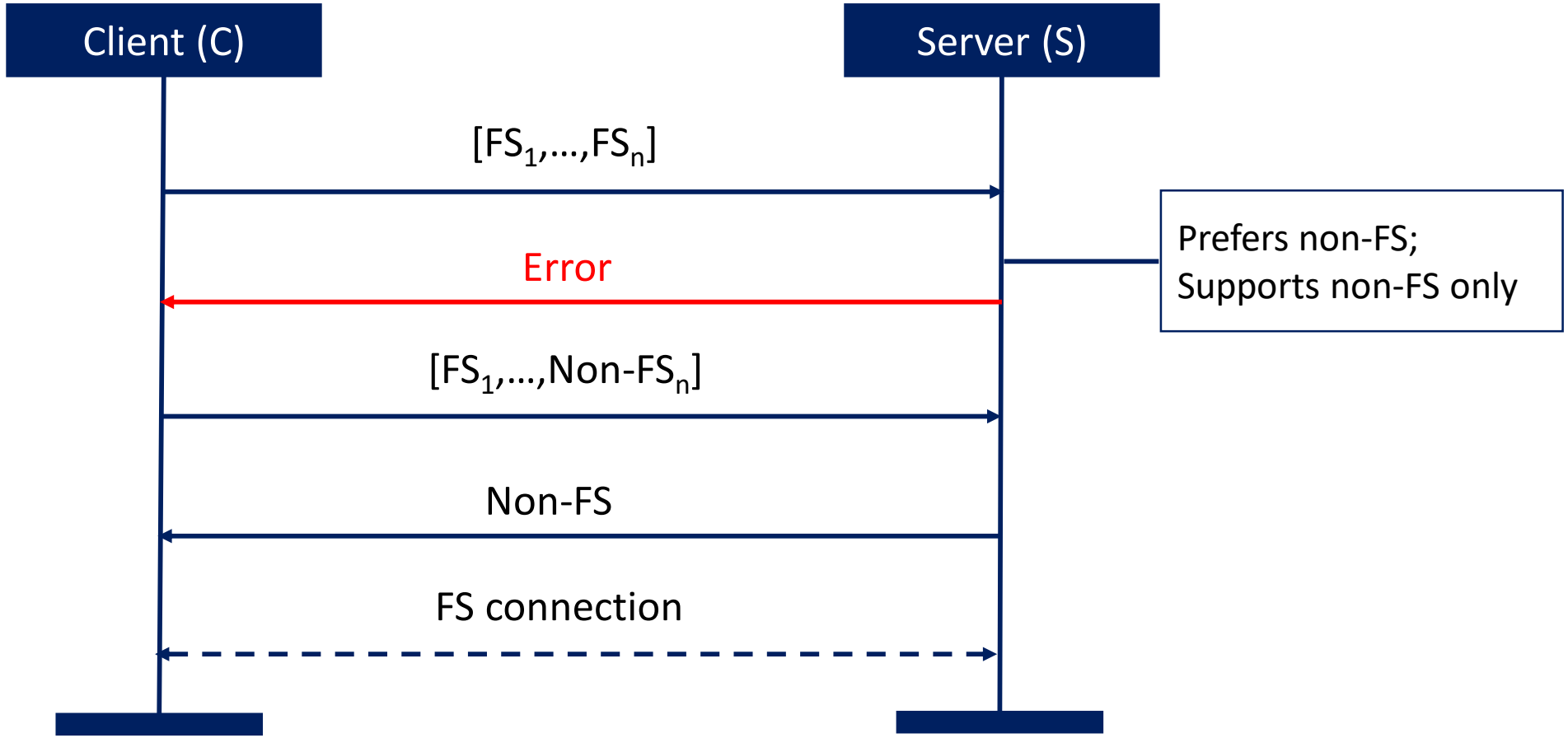
Towards Forward Secure Internet Traffic

- Deprecation
- Best effort approach

Best Effort Forward Secrecy



Best Effort Forward Secrecy



Conclusion

- The “discriminatory” adversarial model
- Empirical study on FS and TLS
- Best effort approach can add a value over the “all or nothing” approach

Towards Forward Secure Internet Traffic

Eman Salem Alashwali[1,2], Pawel Szalachowski[3], and Andrew Martin[1]

[1] University of Oxford, Oxford, United Kingdom
{eman.alashwali,andrew.martin}@cs.ox.ac.uk
[2] King Abdulaziz University (KAU), Jeddah, Saudi Arabia
[3] Singapore University of Technology and Design (SUTD), Singapore, Singapore
pawel@sutd.edu.sg

SecureComm 2019


thank
you