Security Vulnerabilities of 0-RTT Data in TLS 1.3

DongHyeon Kim(wlswudpdlf31@kookmin.ac.kr), Future cryptography Design Lab

Table of Contents

TLS 1.3 Handshake Protocol

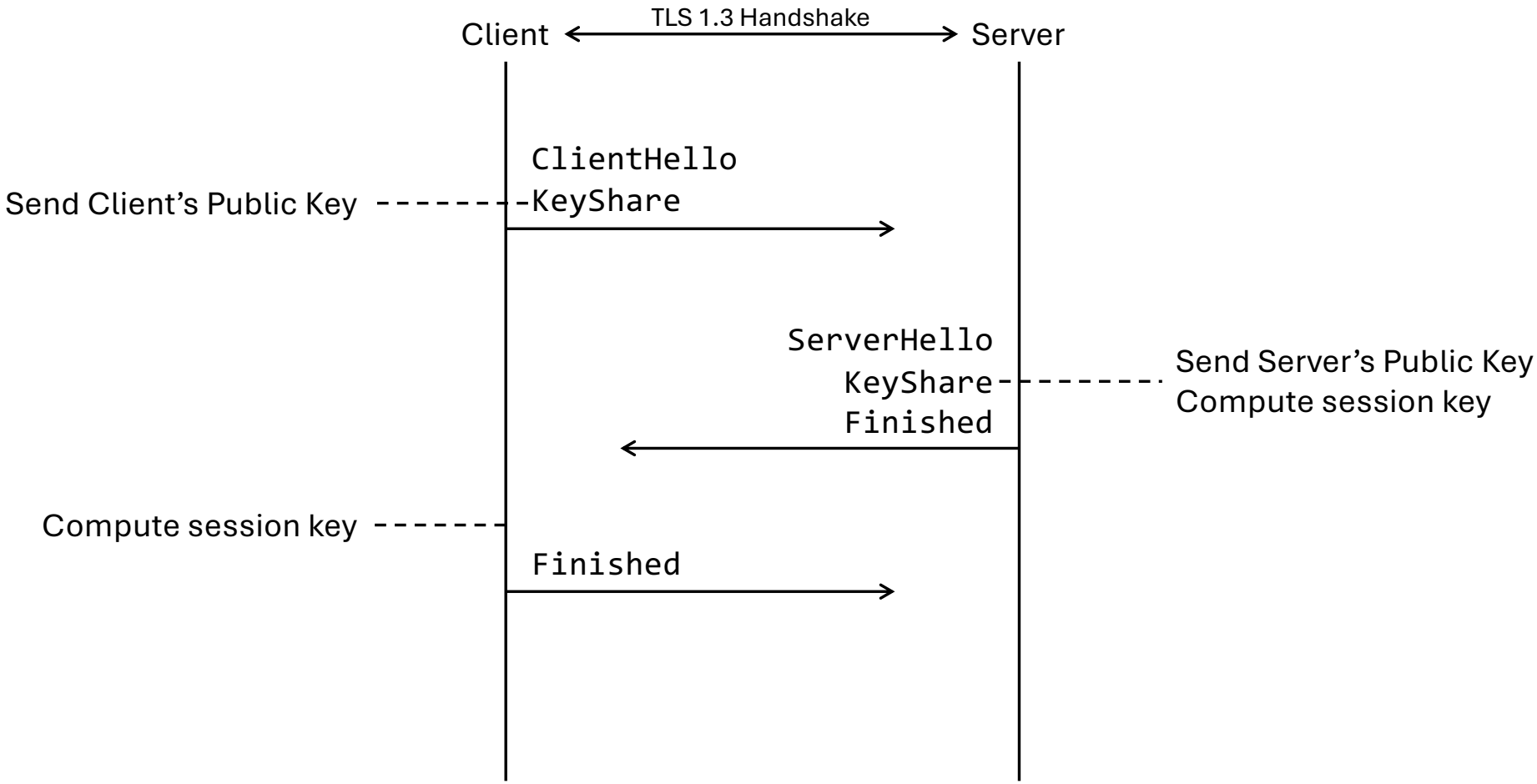

Goal of TLS(Transport Layer Security):
Client
Server
Provide secure channel

*“ The record protocol takes messages to be transmitted, fragments the data into manageable blocks, **protects the records**, and transmits the result. ”*

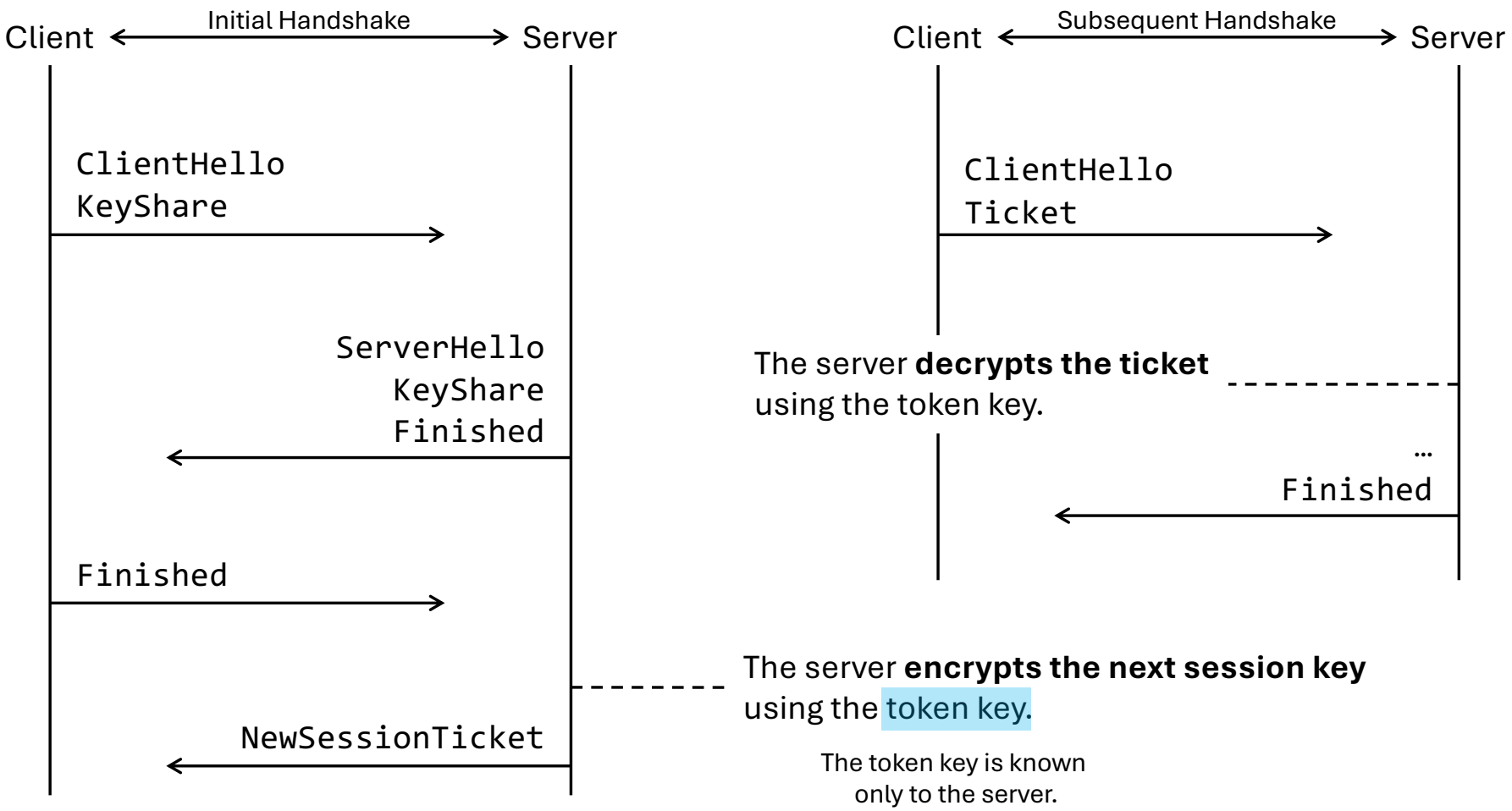
TLS: Handshake Protocol + Record Protocol

*“ The handshake protocol is used to **negotiate the security parameters** of a connection. ”*

TLS 1.3 Handshake Protocol

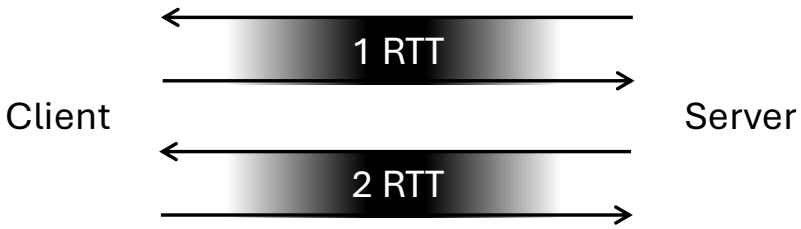


Pre-Shared Key(PSK) only mode



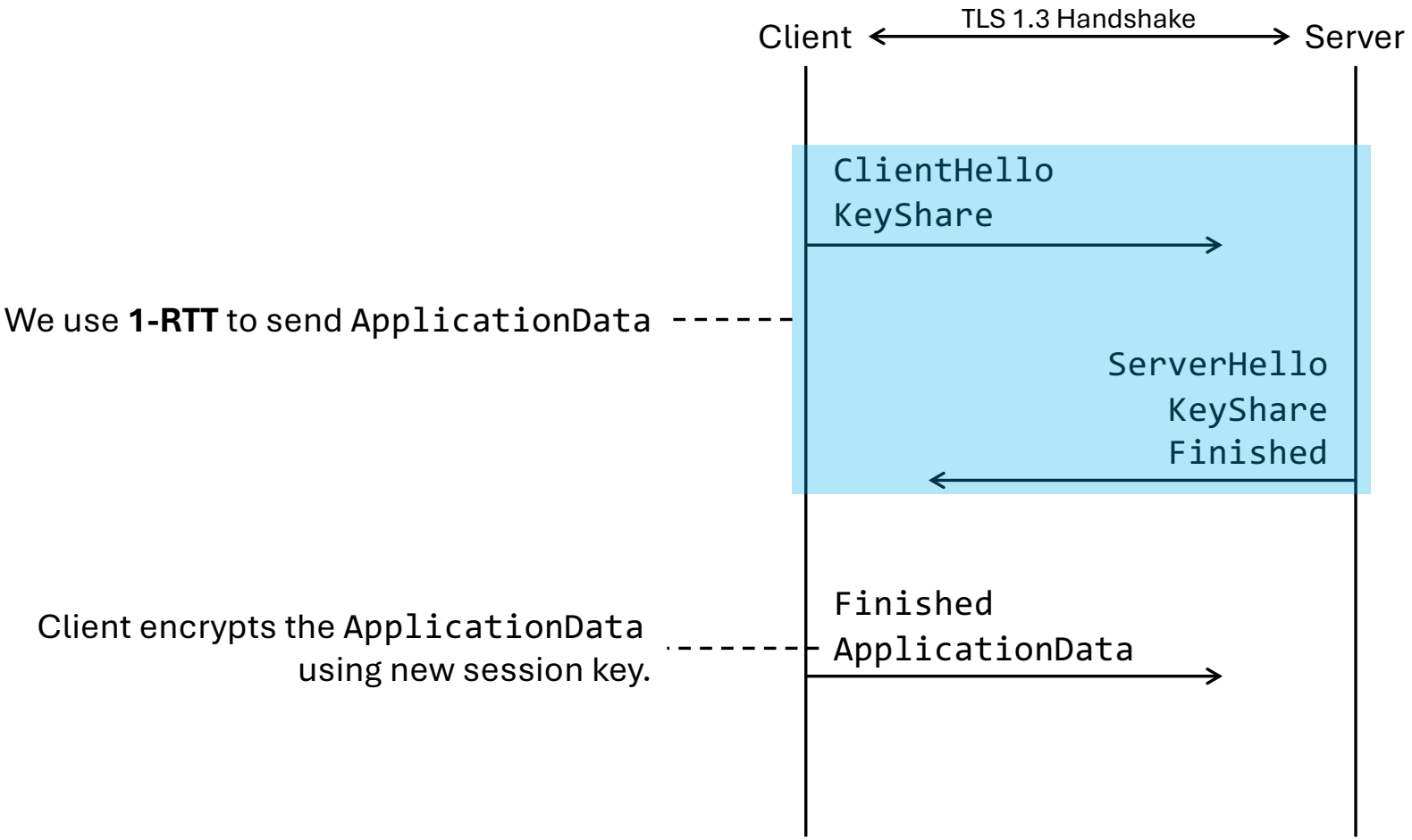
0-Round Trip Time

Round Trip Time, RTT for short

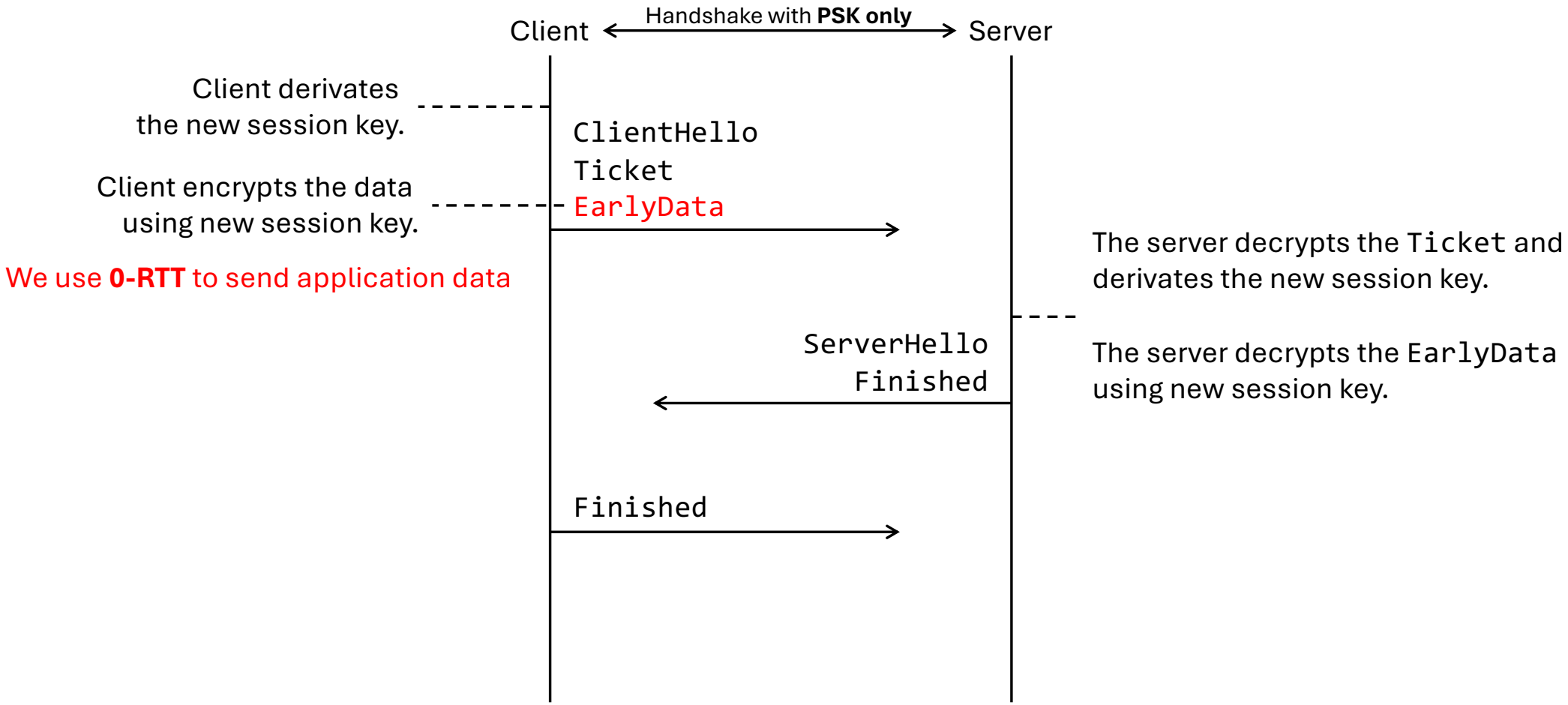


Fewer RTTs result in reduced time overhead.

0-Round Trip Time Mode

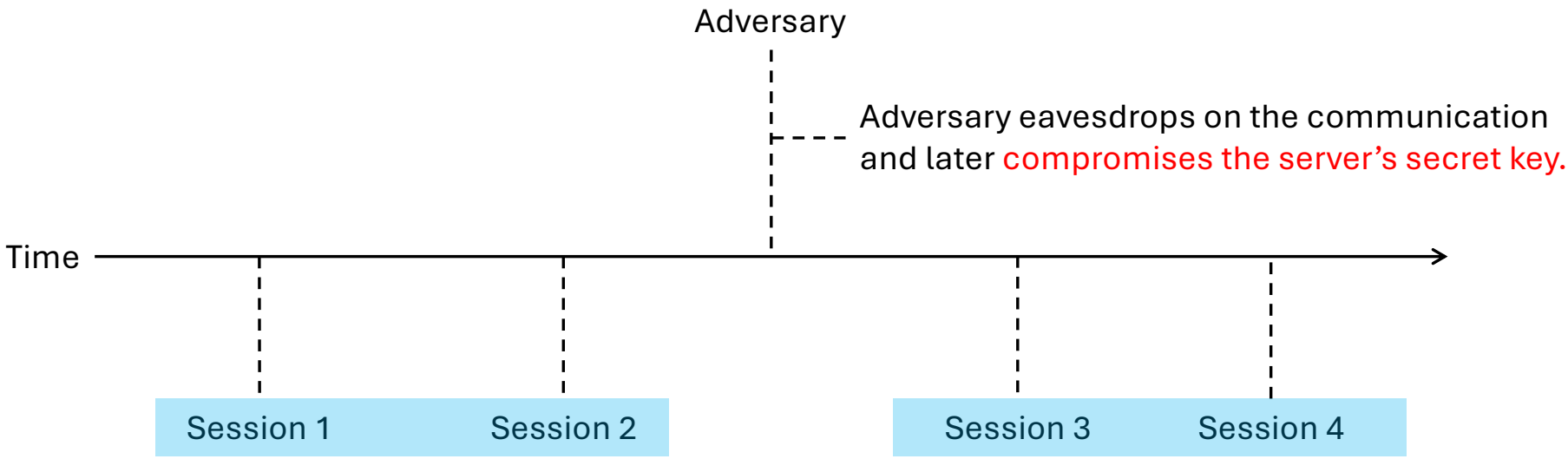


0-Round Trip Time Mode



Forward Secrecy

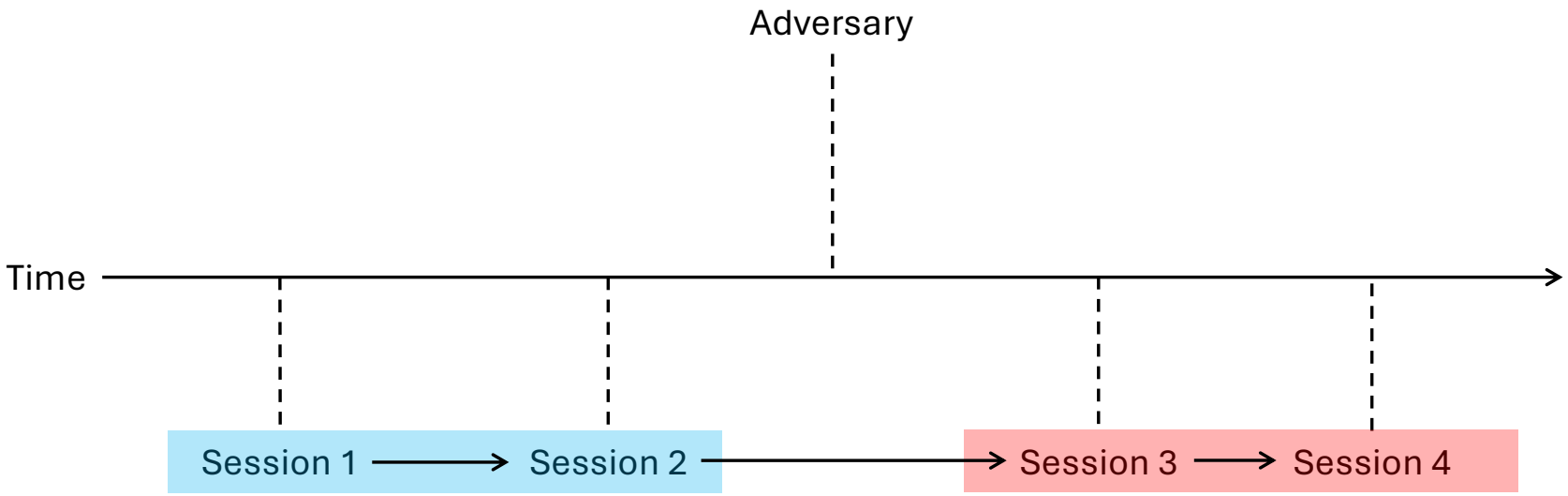
Forward Secrecy



In genaral,
adversary dose not know the others session key.

= Forward Secrecy

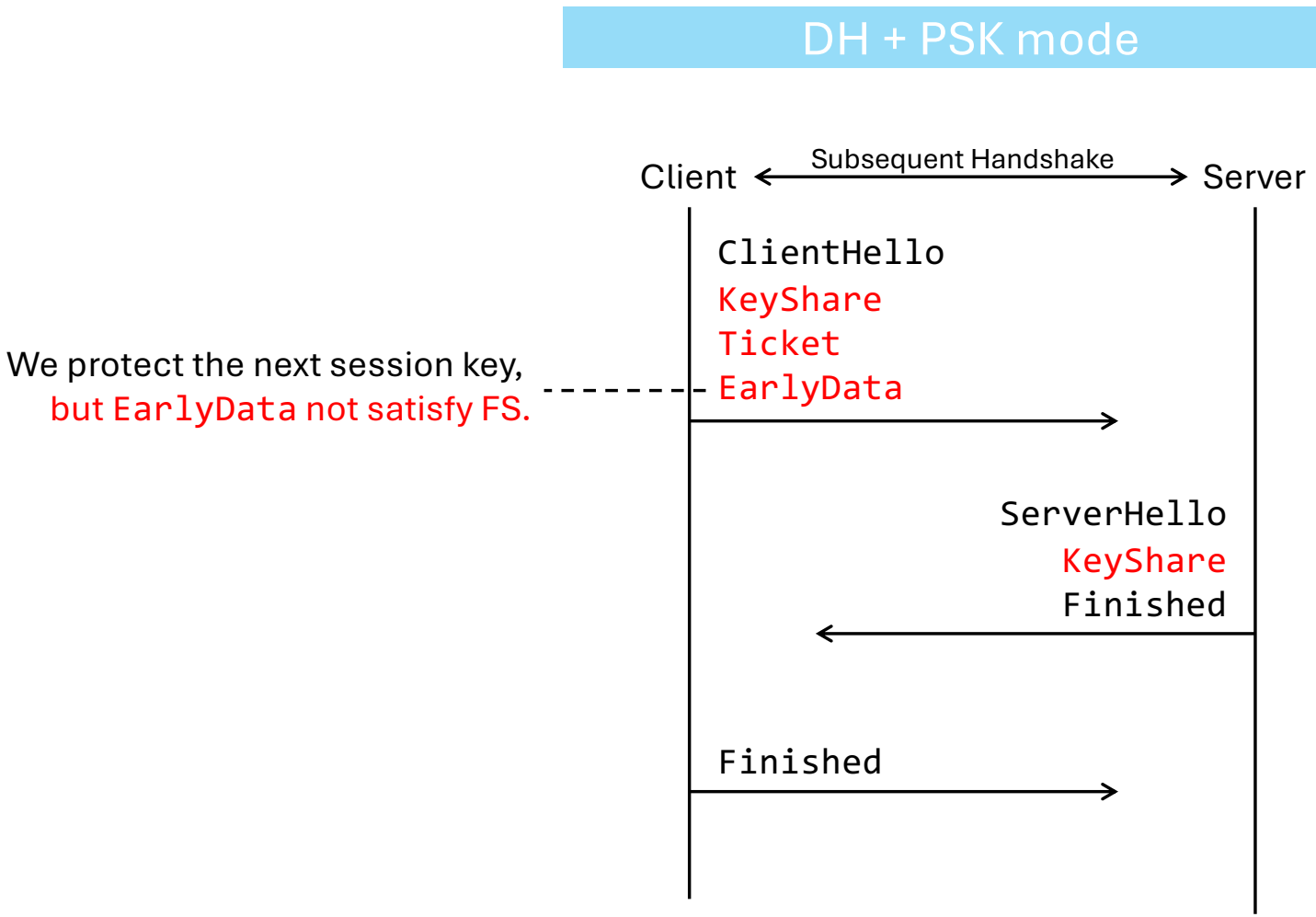
Forward Secrecy



In PSK only mode,
adversary knows the others session key

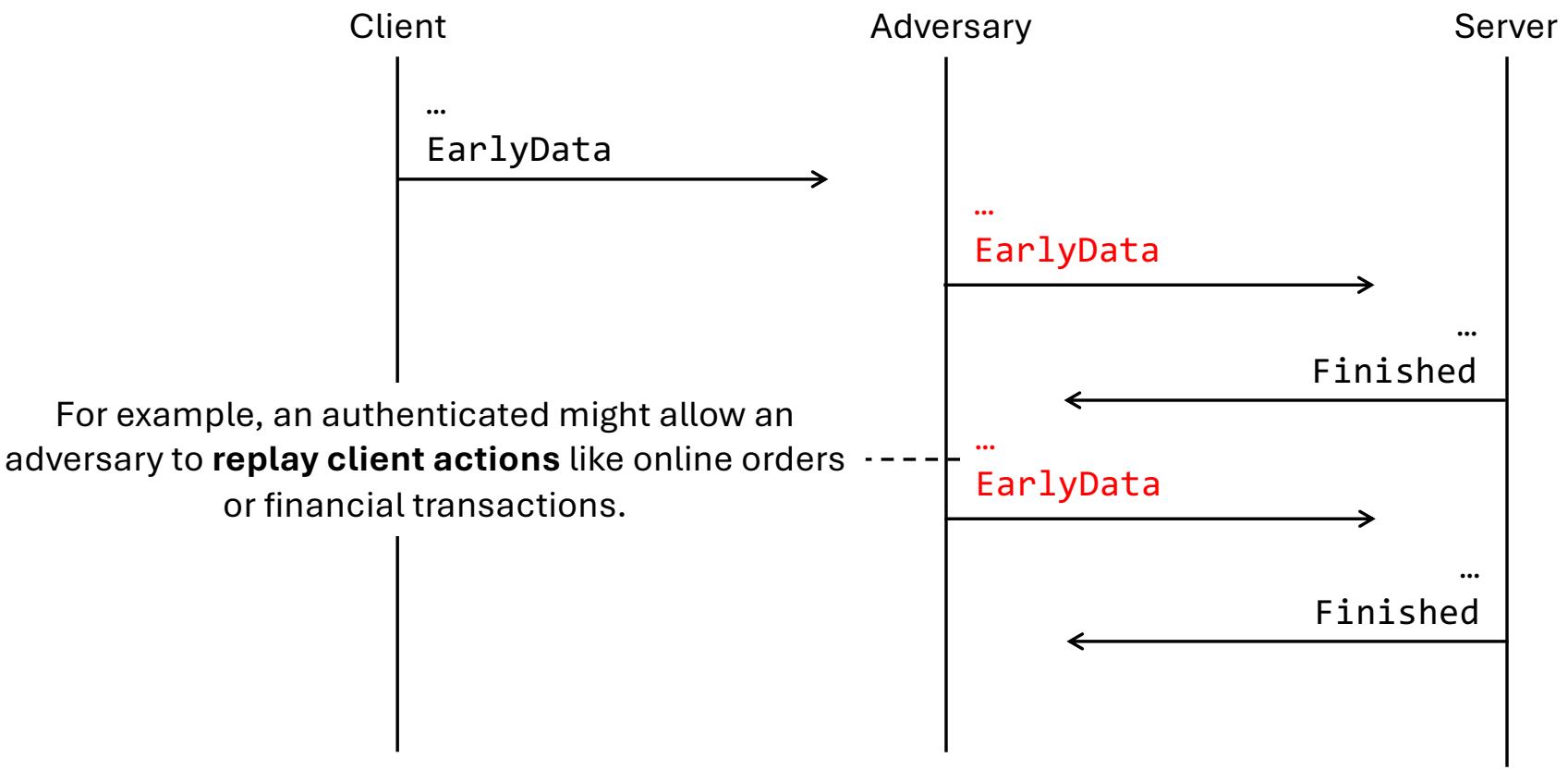
~~= Forward Secrecy~~

Forward Secrecy

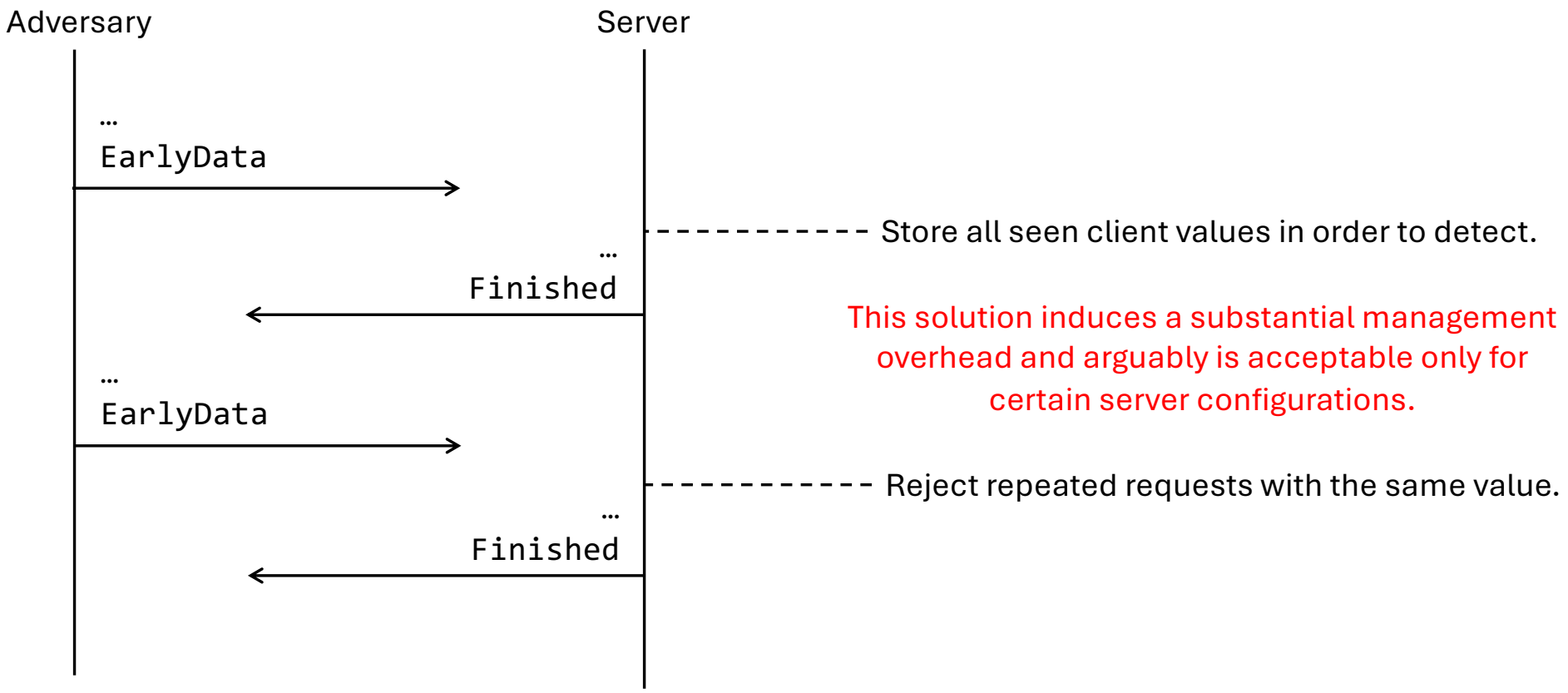


Replay Attack

Replay Attack



Replay Attack



“ 0-RTT data does not have forward secrecy and is vulnerable to replay attacks. ”

How can we solve this problem?

References

- Rescorla, E. (2018, August). The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446). RFC Editor. https://www.rfc-editor.org/info/rfc8446
- Günther, F., Hale, B., Jager, T., & Lauer, S. (2017). 0-RTT key exchange with full forward secrecy. In J.-S. Coron & J. B. Nielsen (Eds.), Advances in Cryptology – EUROCRYPT 2017 (pp. 519–548). Springer International Publishing. https://doi.org/10.1007/978-3-319-56617-7_18