Secure Communication Channel Establishment
TLS 1.3 (over TCP Fast Open) vs. QUIC

ESORICS 19
Full version accepted to JoC

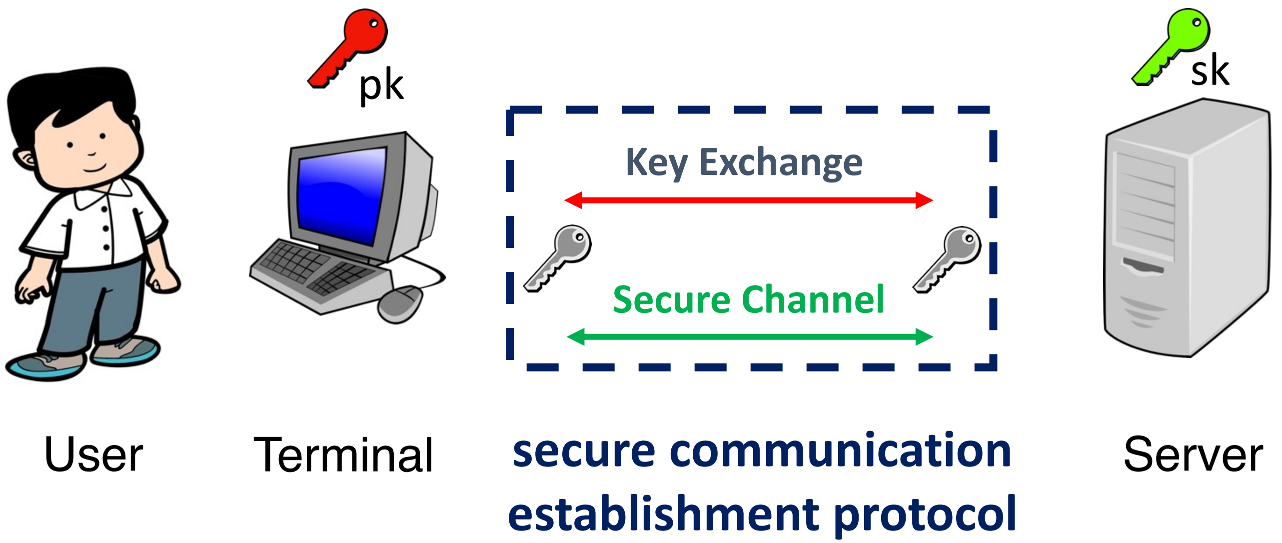
Shan Chen Samuel Jero Matthew Jagielski
Alexandra Boldyreva Cristina Nita-Rotaru

Georgia Tech MIT Lincoln Laboratory Northeastern University

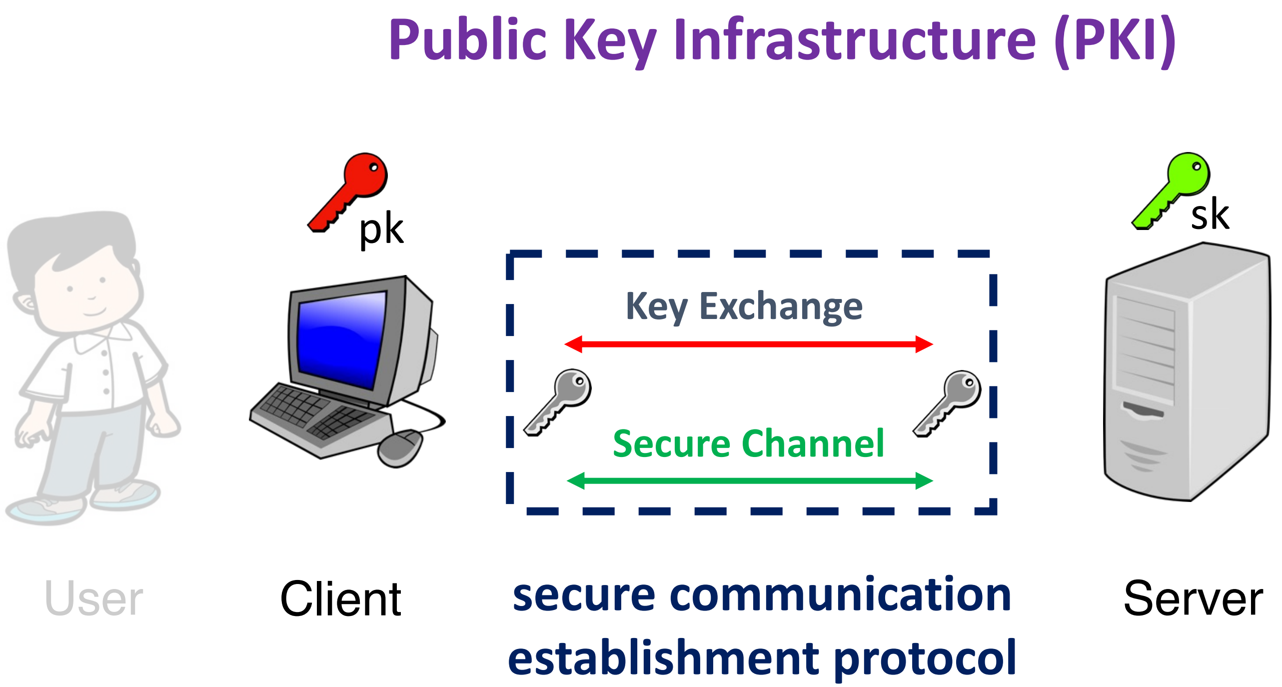
Motivation

Secure Communication and Authentication

Public Key Infrastructure (PKI)

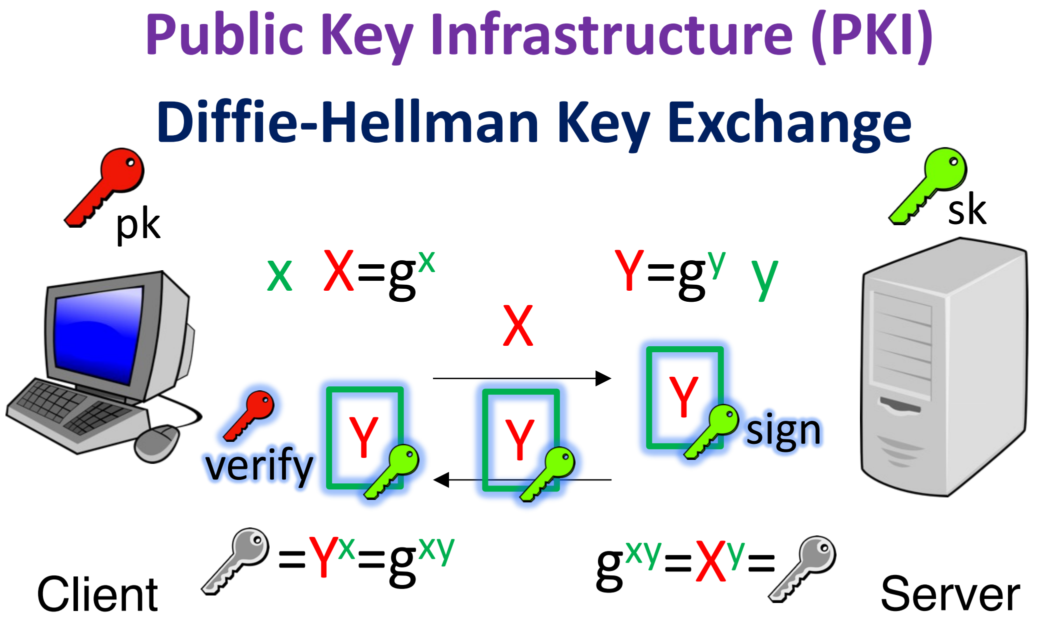


Secure Communication and Authentication



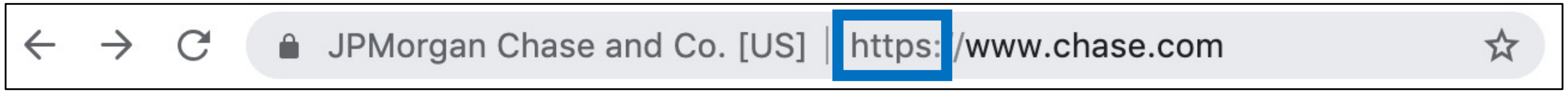
- The user is not involved in the secure channel establishment.

Secure Communication and Authentication

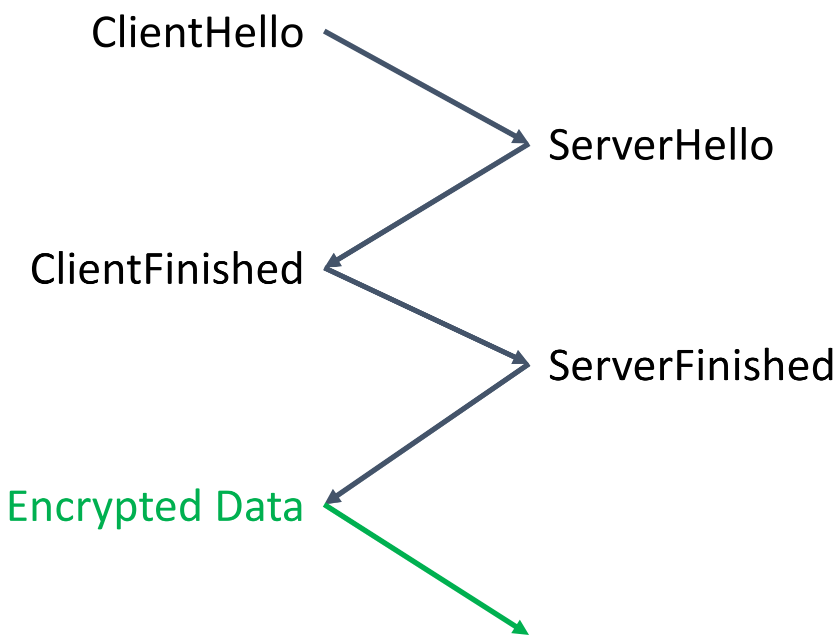


- In the real world, secure channel establishment is more complicated:
  - session resumption, key exchange encryption, channel protocol composition…

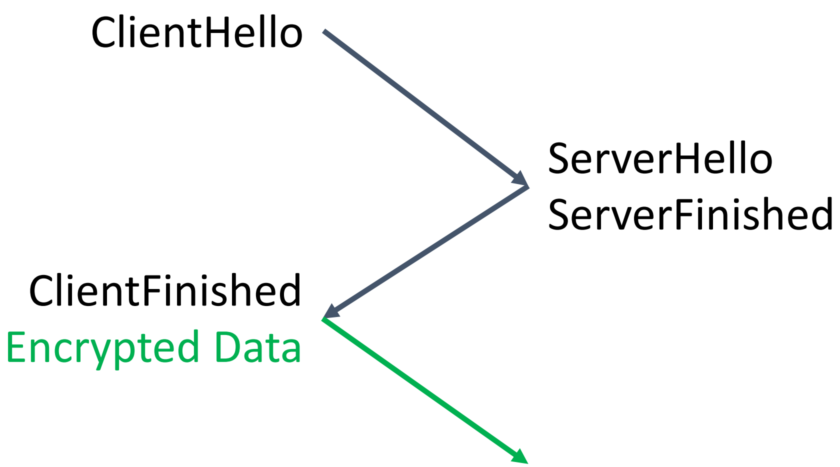
Current Deployed Standard: TLS 1.2



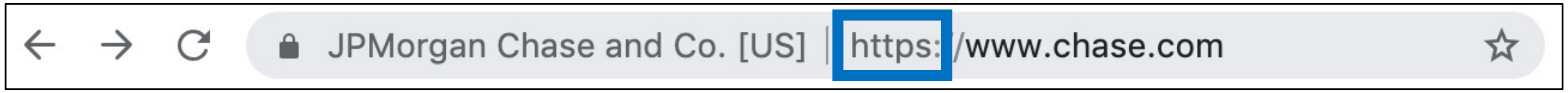
Initial Full Handshake (2-RTT)



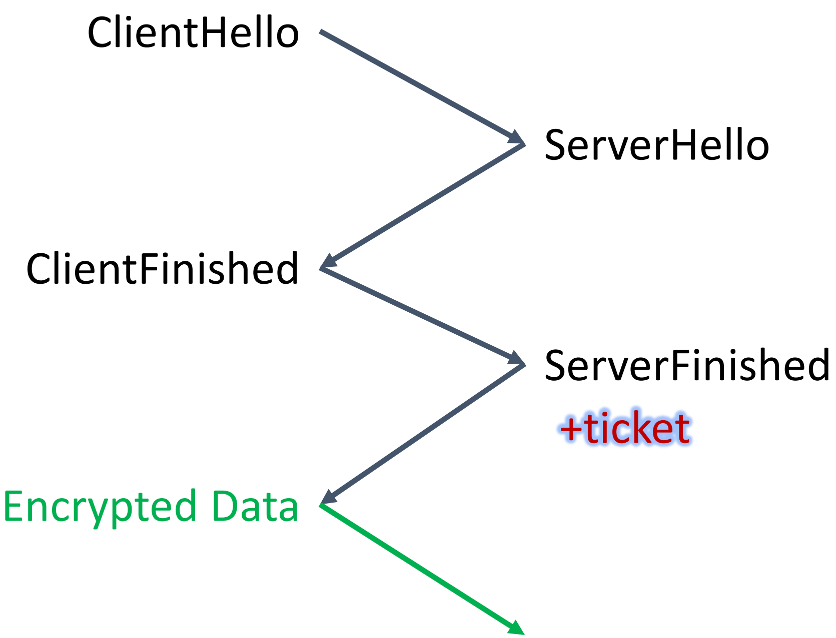
Resumption (1-RTT) **reduce latency**



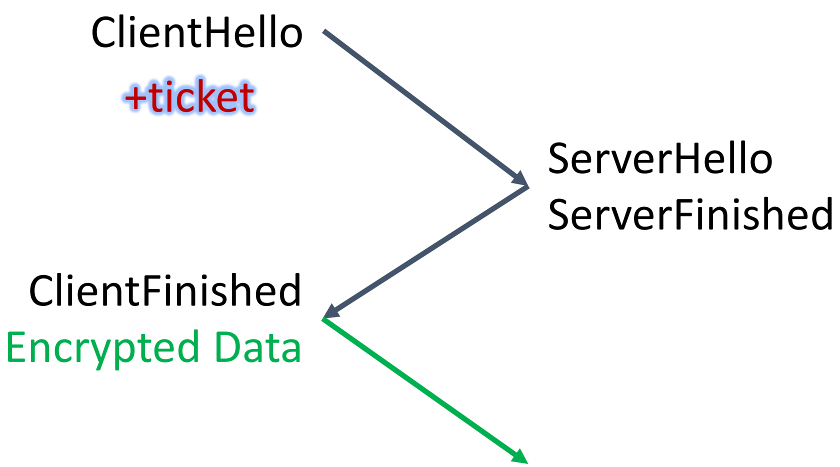
Current Deployed Standard: TLS 1.2



Initial Full Handshake (2-RTT)



Resumption (1-RTT) **reduce latency**



Why Low Latency?

- Every **100ms** of latency cost Amazon 1% in sales. [Linden06]
- Every **100ms** delay in website load time can hurt conversion rates by 7% – that is a significant 6% drop in sales [Akamai17]

…

[1 RTT from New York to London takes ~**70ms**]

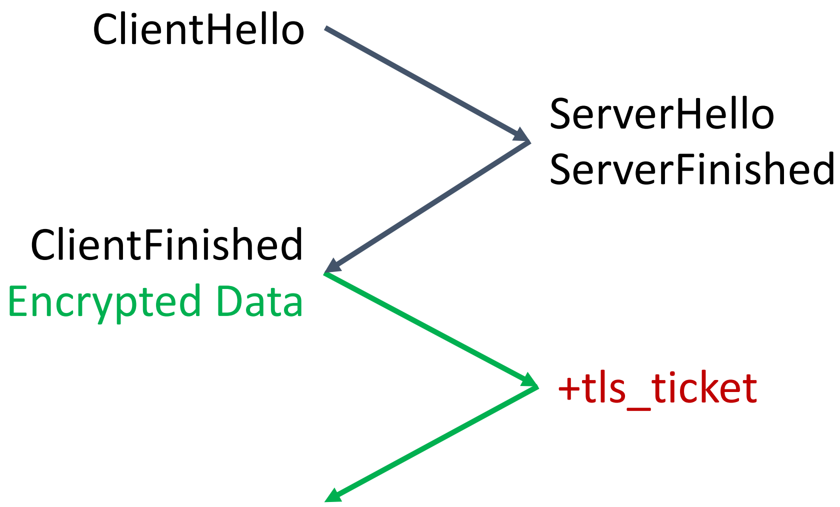
Important Low-Latency Protocols

- TLS 1.3 (over TCP)
  - new standard: proposed in 2018 to replace TLS 1.2
- QUIC (over UDP)
  - designed by Google and implemented in Chrome since 2012
- QUIC[TLS] (over UDP)
  - IETF-draft: new QUIC design by Mozilla that uses TLS 1.3's key exchange but keeps QUIC's transport functionalities

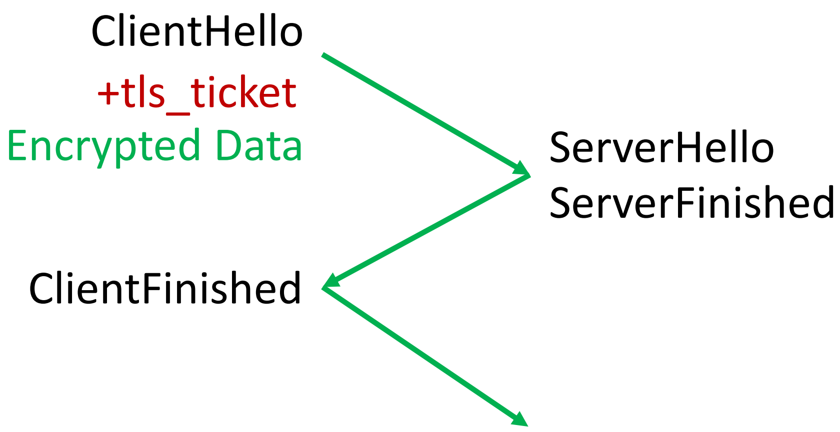
Protocol Description

TLS 1.3

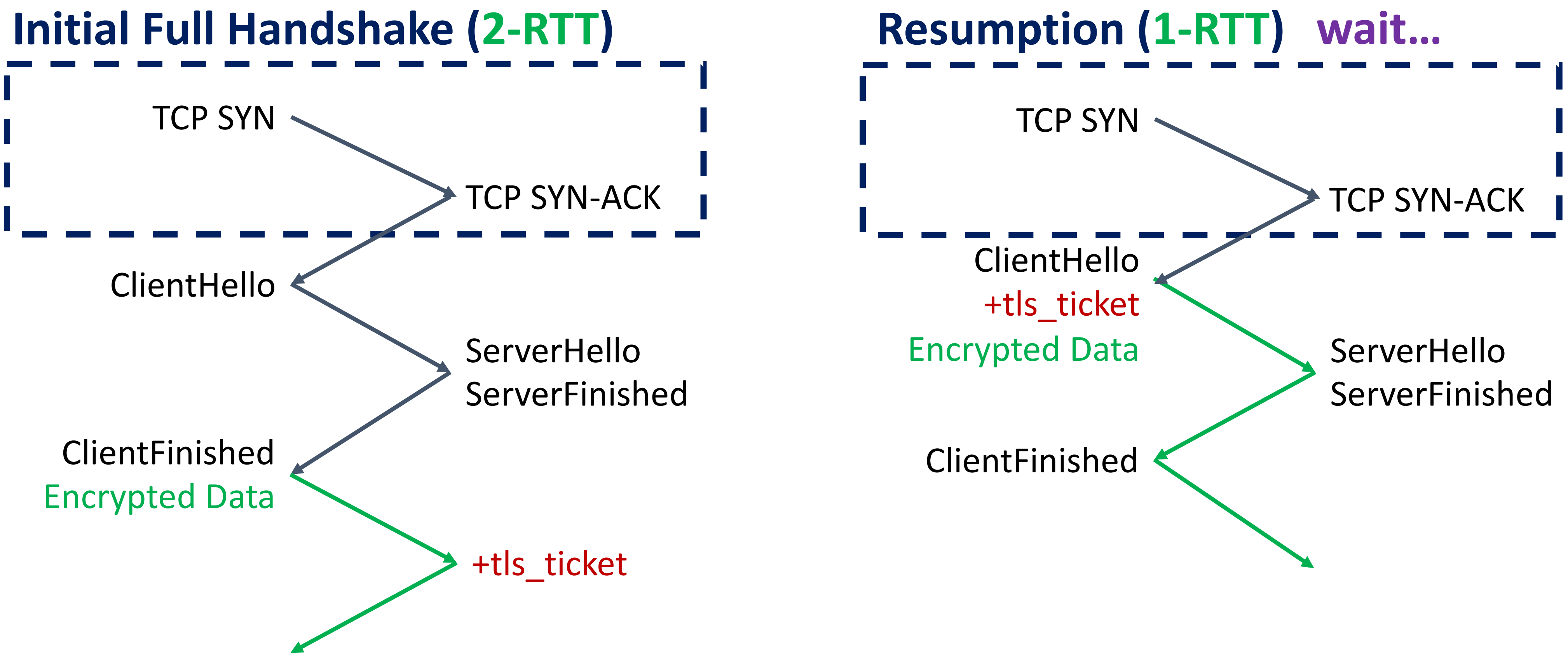
Initial Full Handshake (1-RTT)



Resumption (0-RTT) 0 latency 😀



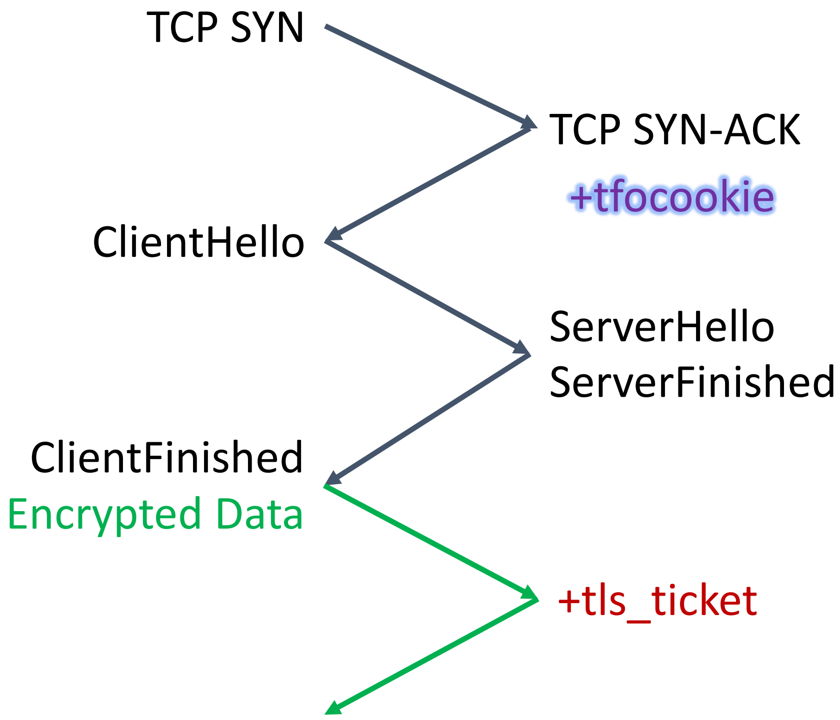
TLS 1.3 / TCP



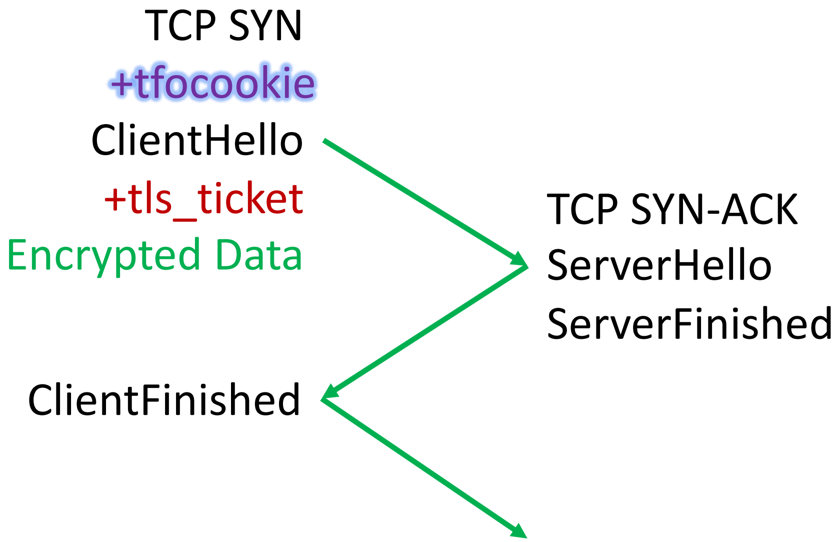
Initial Full Handshake (2-RTT)
TCP SYN
TCP SYN-ACK
ClientHello
ServerHello
ServerFinished
ClientFinished
Encrypted Data
+tls_ticket
Resumption (1-RTT) wait…
TCP SYN
TCP SYN-ACK
ClientHello
+tls_ticket
Encrypted Data
ServerHello
ServerFinished
ClientFinished

TLS 1.3 / TCP Fast Open (TFO)

Initial Full Handshake (2-RTT)

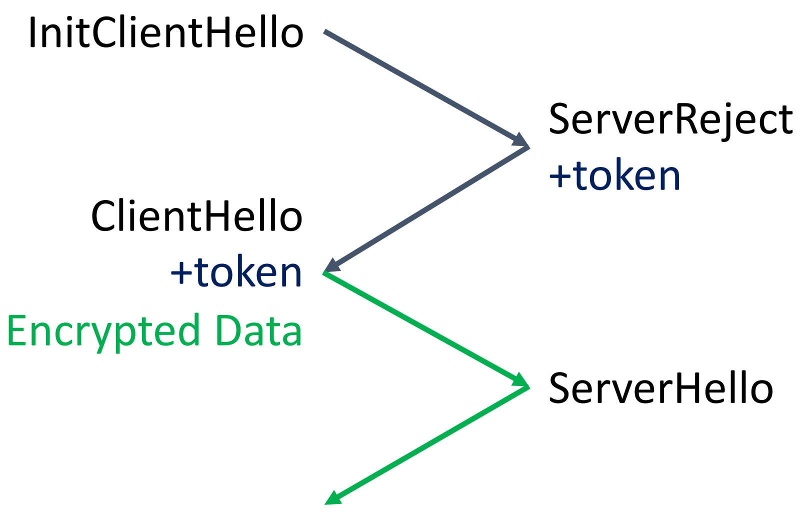


Resumption (0-RTT) 0 latency again!

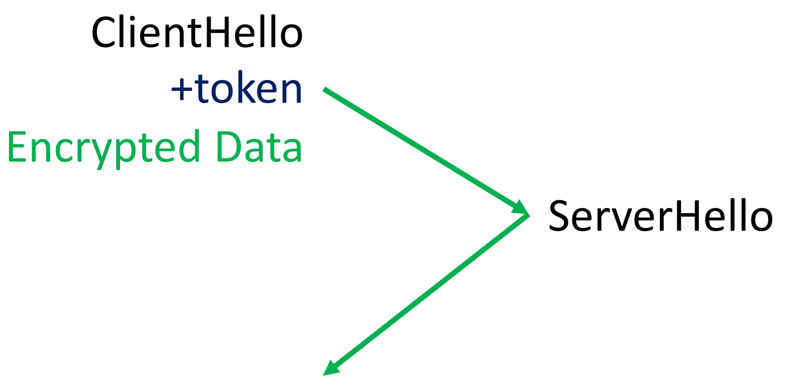


QUIC

Initial Full Handshake (1-RTT)

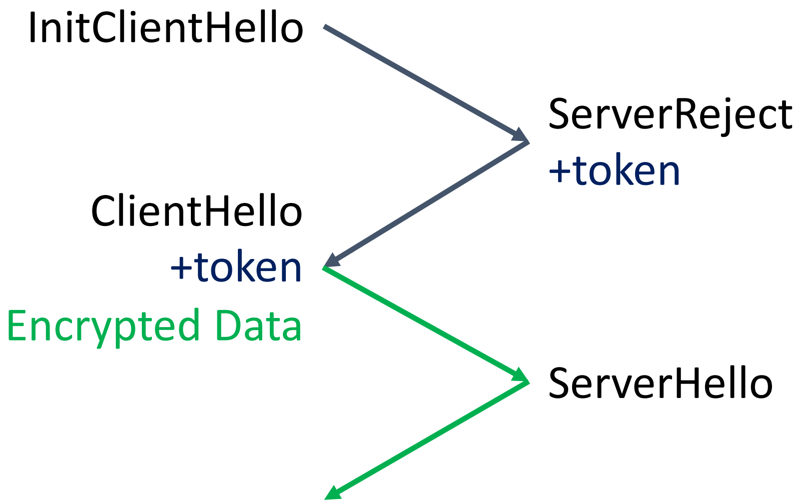


Resumption (0-RTT) 0 latency 😀

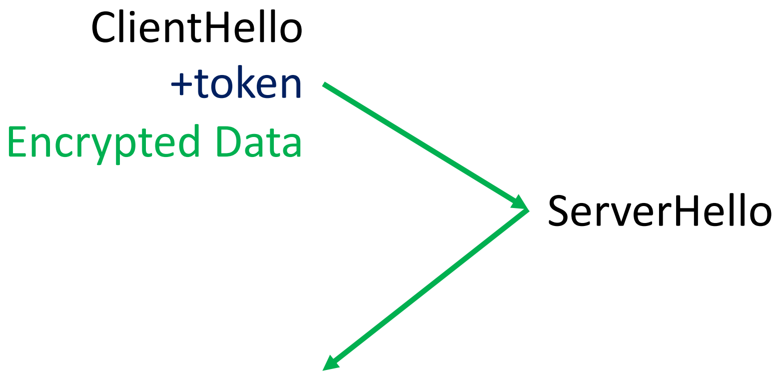


QUIC / UDP

Initial Full Handshake (1-RTT)



Resumption (0-RTT) 0 latency 😀



Latency Comparison

Layered Protocols	Full Connection	Resumption Connection
TLS 1.2 / TCP	3-RTT	2-RTT
TLS 1.3 / TCP	2-RTT	1-RTT
TLS 1.3 / TFO	**2-RTT**	**0-RTT**
QUIC / UDP	**1-RTT**	**0-RTT**
QUIC[TLS] / UDP	**1-RTT**	**0-RTT**

Latency Comparison

Layered Protocols	Full Connection	Resumption Connection
TLS 1.2 / TCP	3-RTT	2-RTT
TLS 1.3 / TCP	2-RTT	1-RTT
TLS 1.3 / TFO	**2-RTT**	**0-RTT**
QUIC / UDP	**1-RTT**	**0-RTT**
QUIC[TLS] / UDP	**1-RTT**	**0-RTT**

How to compare the security of the low-latency protocols?

Prior Works: TLS 1.3 vs QUIC

- TLS 1.3 security:
  - secure in the Multi-Stage Key Exchange (MSKE) model [FG14] [DFGS15] [DFGS16] [LXZFH16] [FG17]
  - composition: secure key exchange + secure symmetric-key channel
    - caveat: does NOT work for the full handshake due to phase dependency
- QUIC security:
  - secure in the MSKE model [FG14]
    - similar composition issue
  - secure in the Quick Authenticated and Confidential Channel Establishment (QACCE) model [LJBN15]

Motivation

- TLS 1.3 vs QUIC: similar security guarantees
- However…

Motivation

- TLS 1.3 vs QUIC: similar security guarantees
- However…
- What about security of **layered** protocols? TLS 1.3/TFO vs QUIC/UDP
  - no **universal model** to compare "layered" security

Motivation

- TLS 1.3 vs QUIC: similar security guarantees
- However…
- What about security of **layered** protocols? TLS 1.3/TFO vs QUIC/UDP
- **No formal understanding** of their **availability security**, i.e., any malicious attacks except packet dropping should be **detected**...
  - no security model to capture availability properties
  - TCP Fast Open (TFO) has not been formally analyzed

Motivation

- TLS 1.3 vs QUIC: similar security guarantees
- However…
- What about security of **layered** protocols? TLS 1.3/TFO vs QUIC/UDP
- **No formal understanding** of their **availability security**, i.e., any malicious attacks except packet dropping should be **detected**...

How to compare the availability security of low-latency layered protocols?

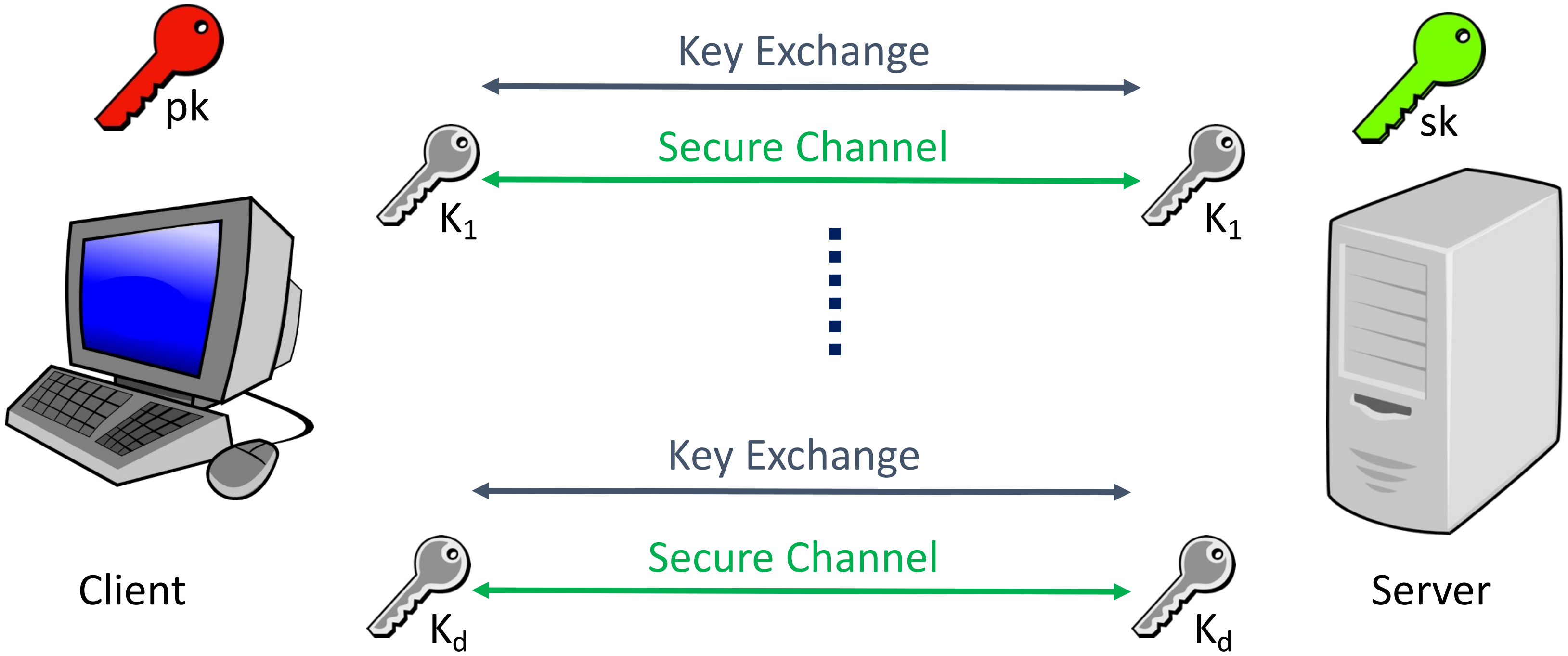
Security Comparison

Recall: Provable Security Approach

- How to analyze the security of a protocol?
  - Define **protocol syntax**, i.e., what is a protocol.
    - general enough to fit TLS 1.3/TFO, QUIC/UDP, QUIC[TLS]/UDP
  - Define **security model**, i.e., adversarial abilities and security goals.
    - security goals to capture availability properties
  - **Prove security** by reduction or identify **attacks**.

Step 1: Protocol Syntax

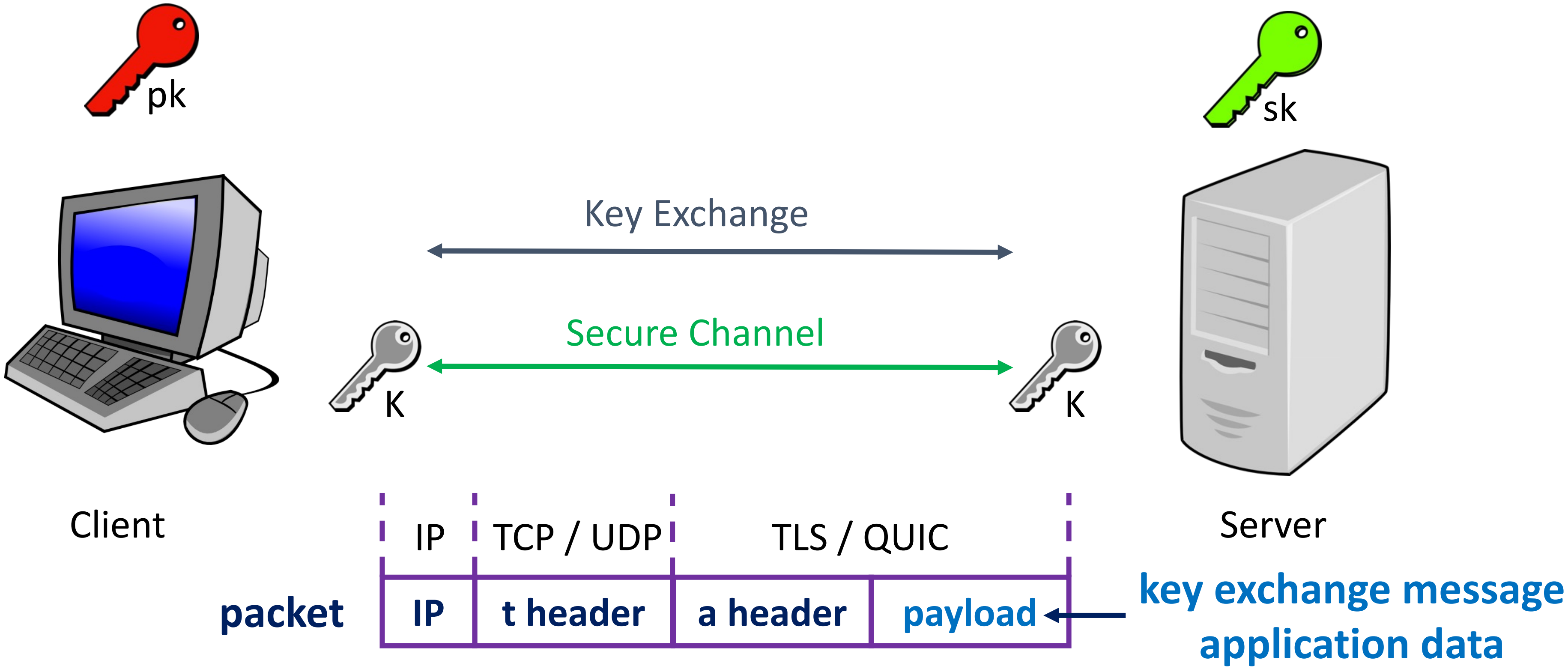
Multi-Stage ACCE (msACCE)



Step 2: Security Model

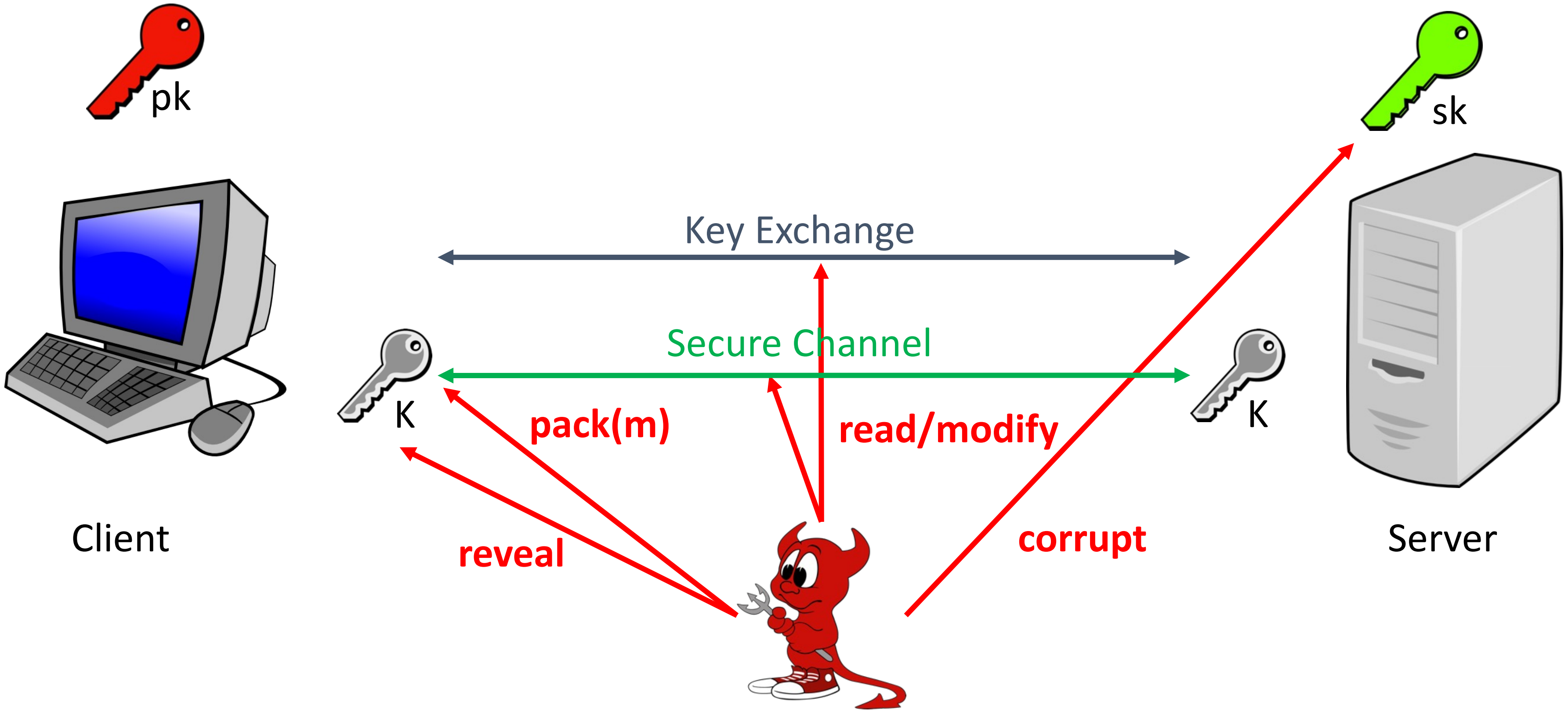
msACCE Security Model

- Messages are transmitted over the network via **packets**:



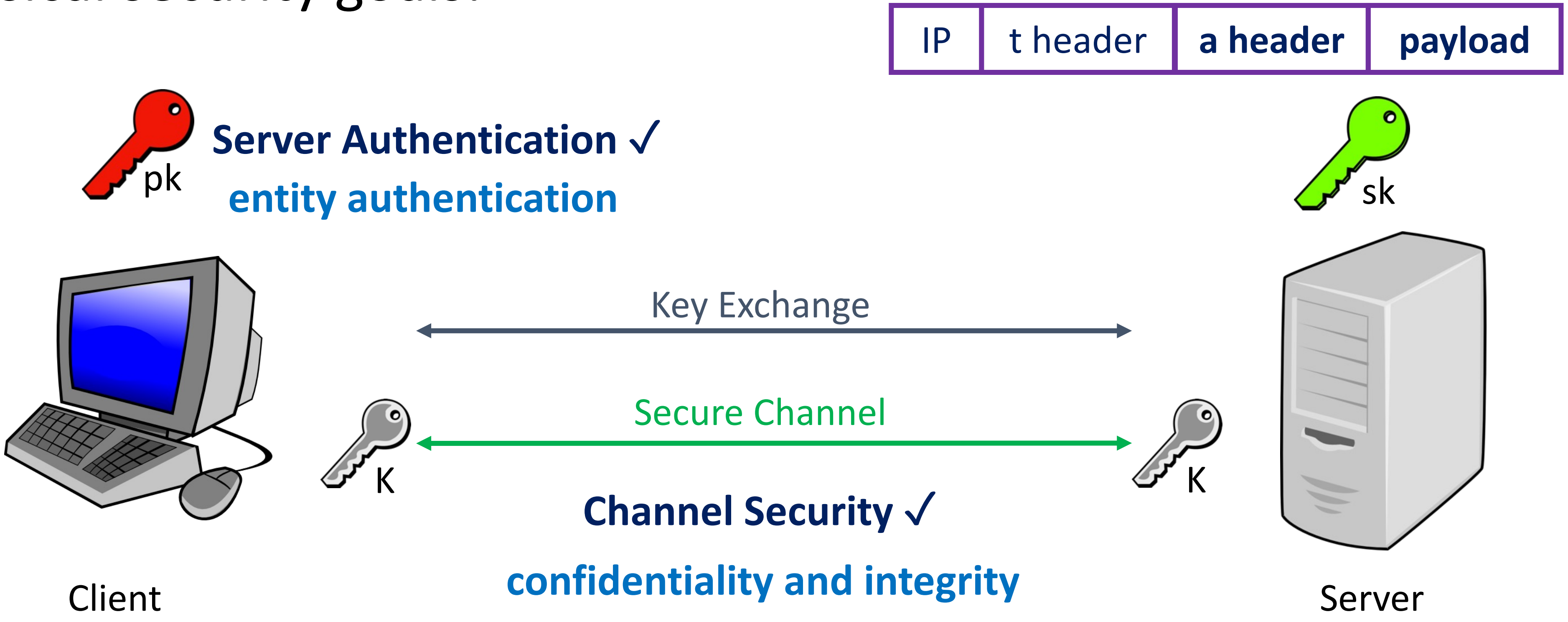
msACCE Security Model

- What are the adversarial abilities?



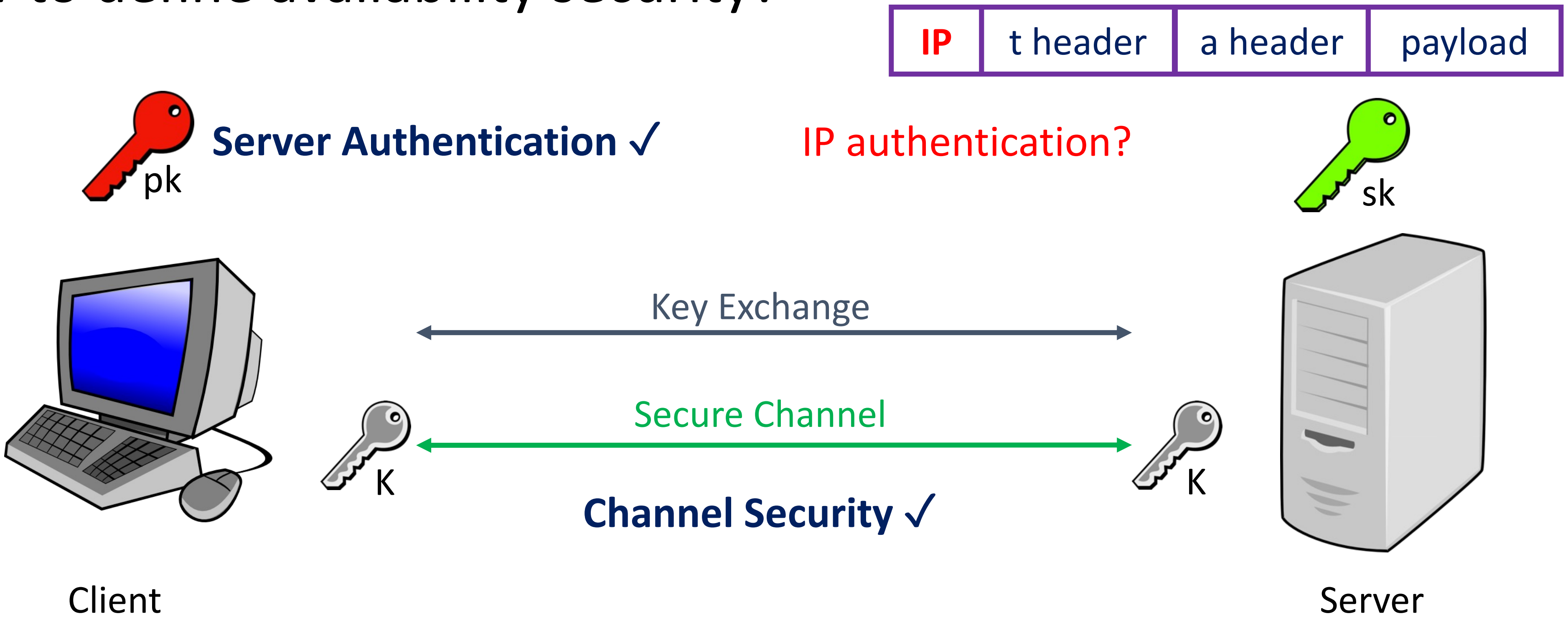
msACCE Security Model

- Classical security goals:



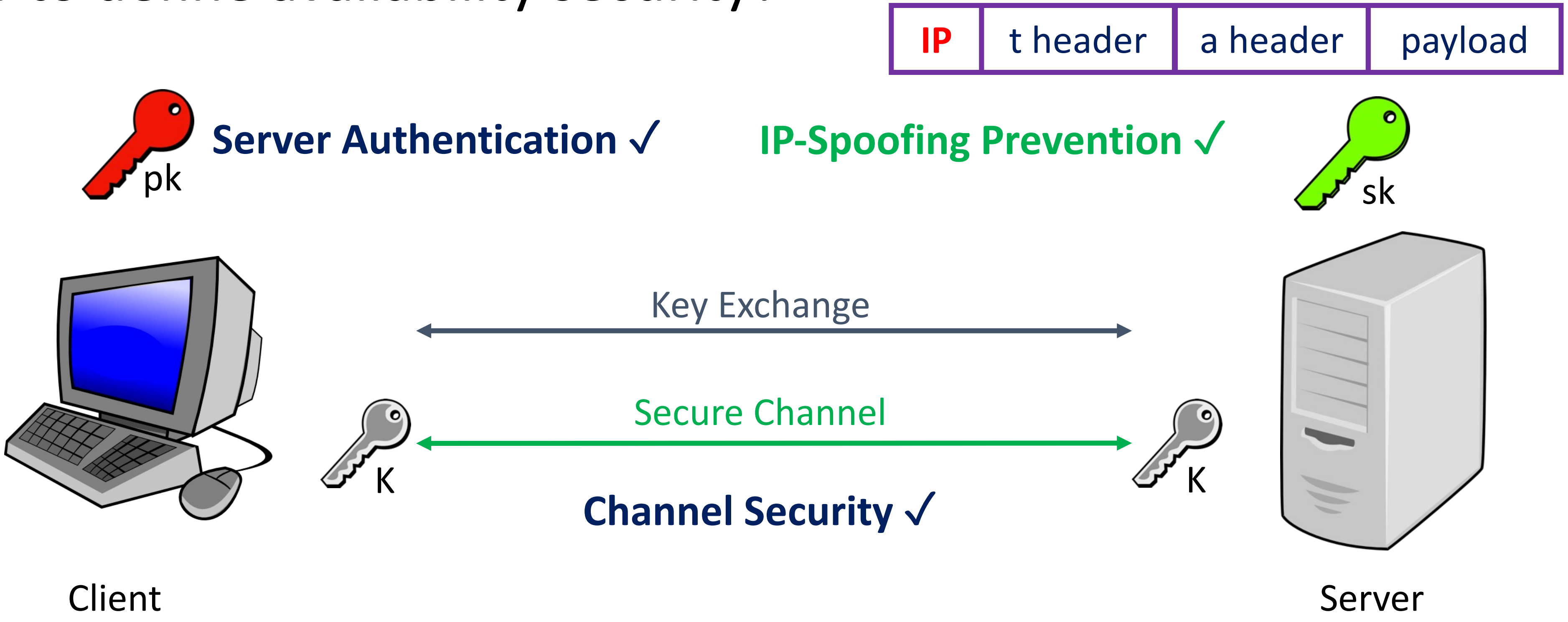
msACCE Security Model

- How to define availability security?



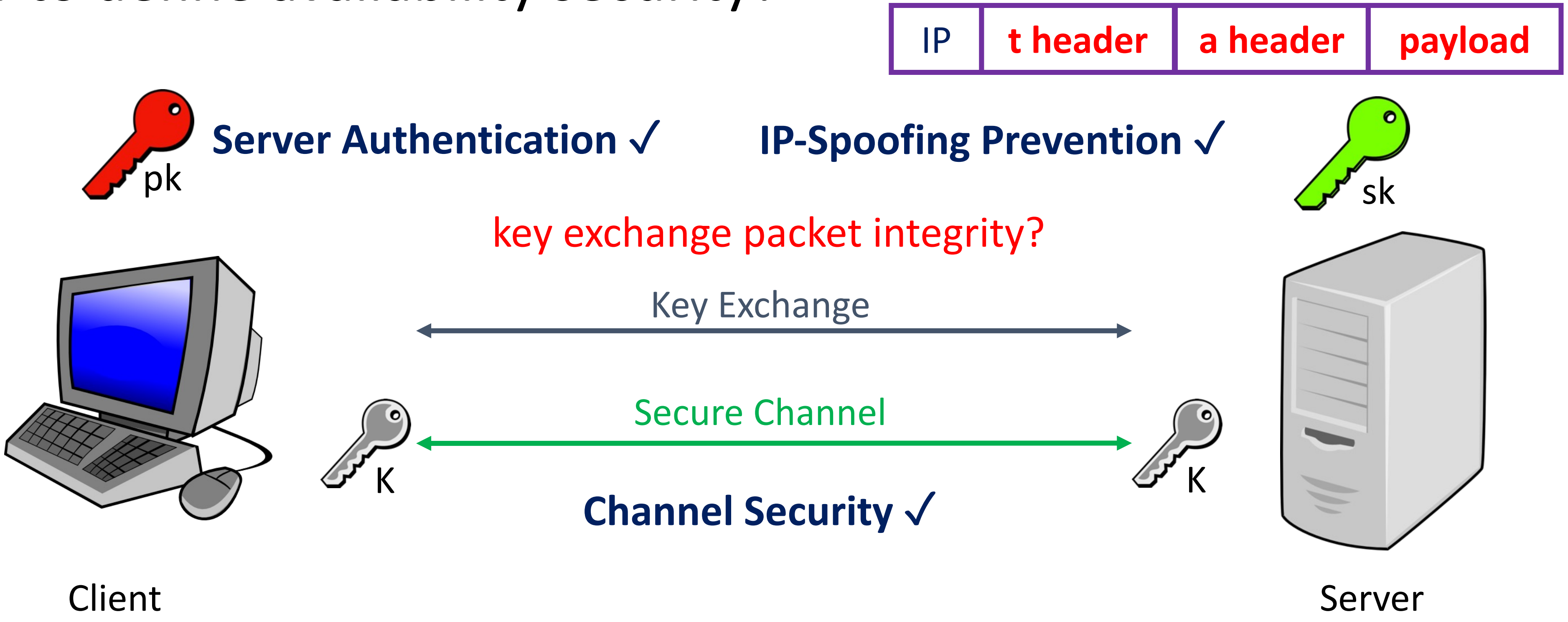
msACCE Security Model

- How to define availability security?



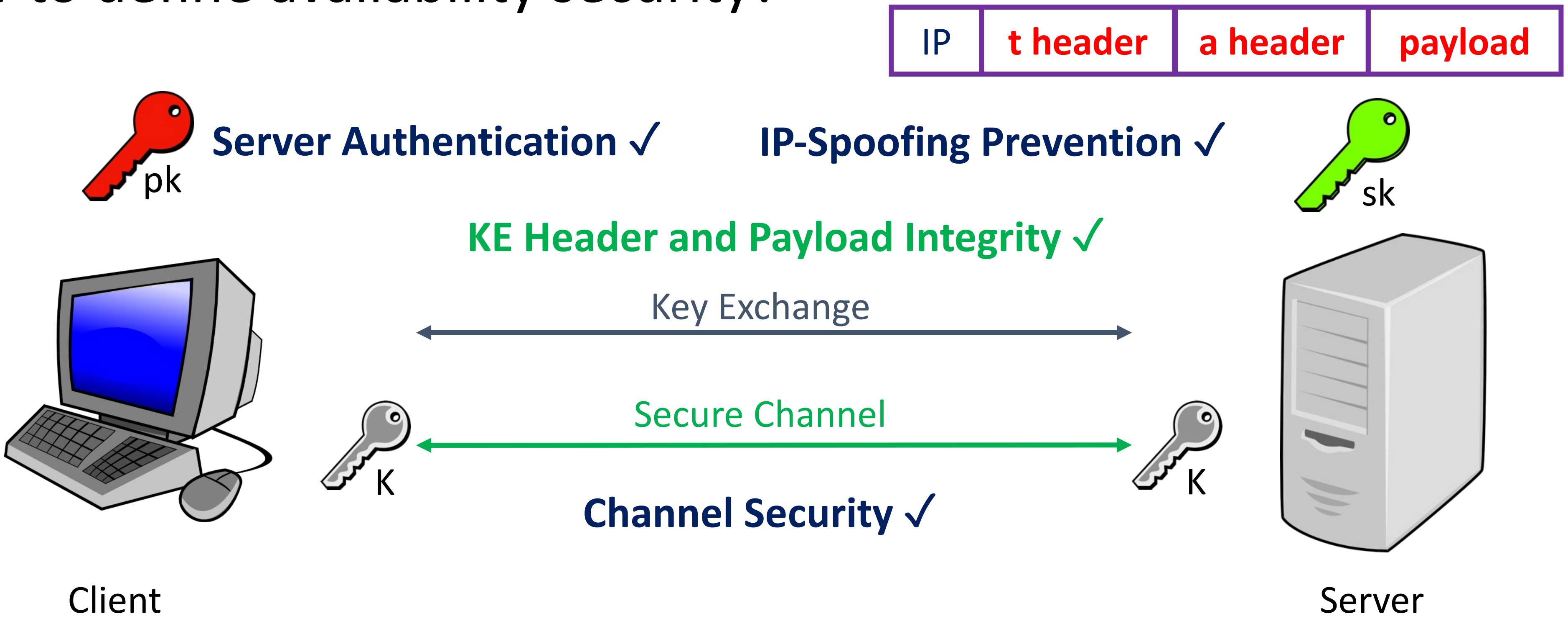
msACCE Security Model

- How to define availability security?



msACCE Security Model

- How to define availability security?

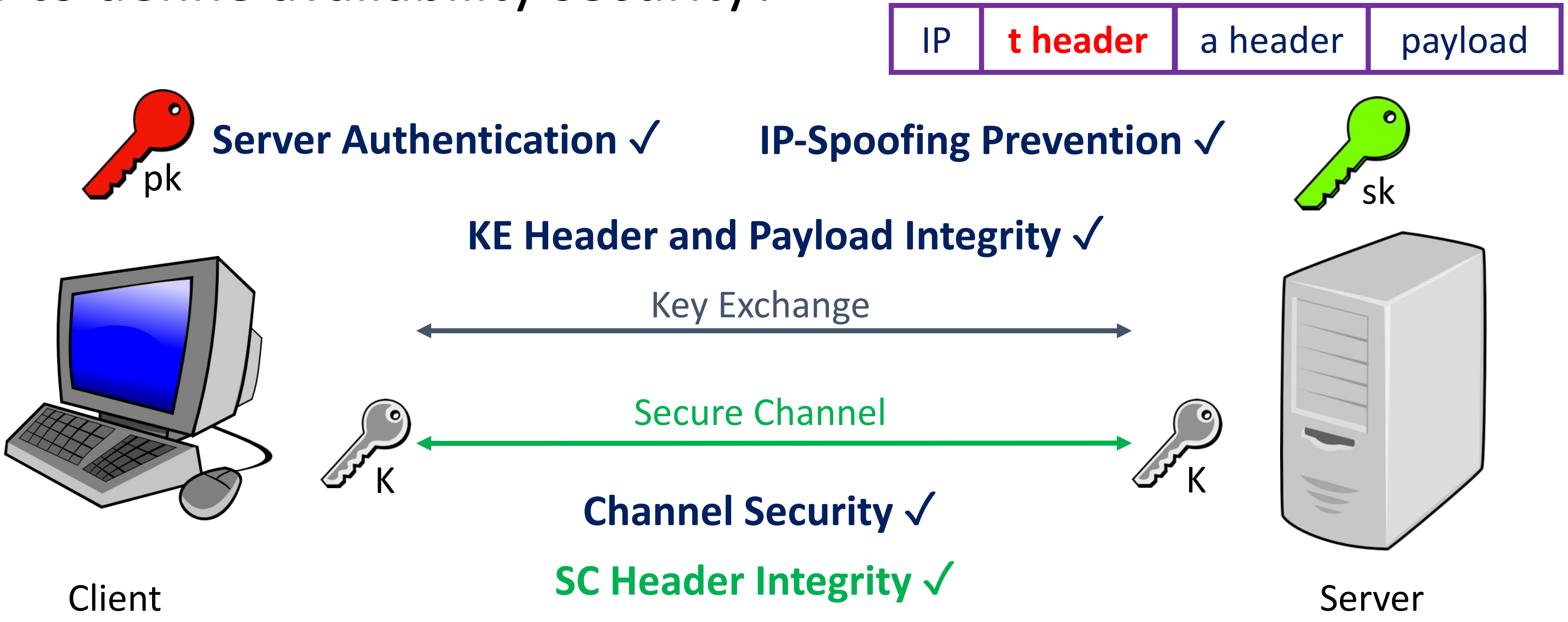


msACCE Security Model

- How to define availability security?

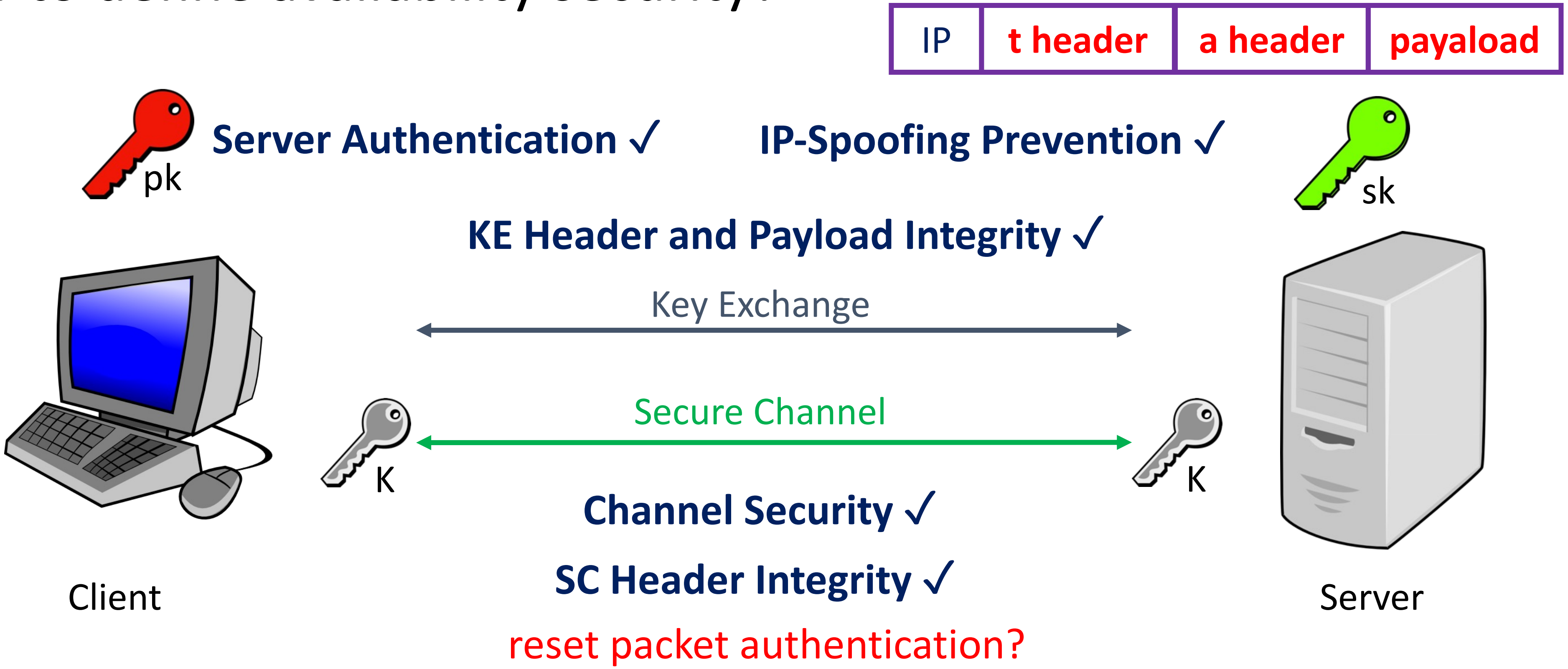
msACCE Security Model

- How to define availability security?



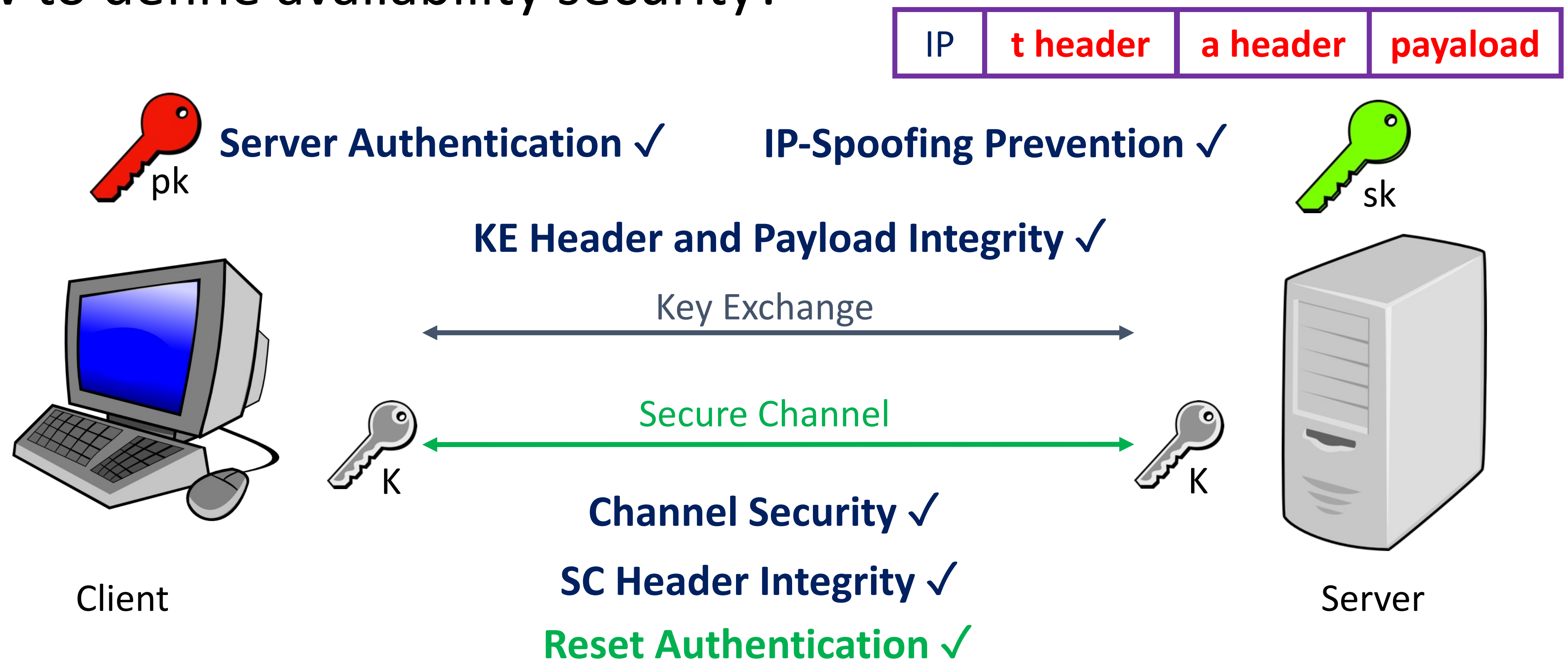
msACCE Security Model

- How to define availability security?



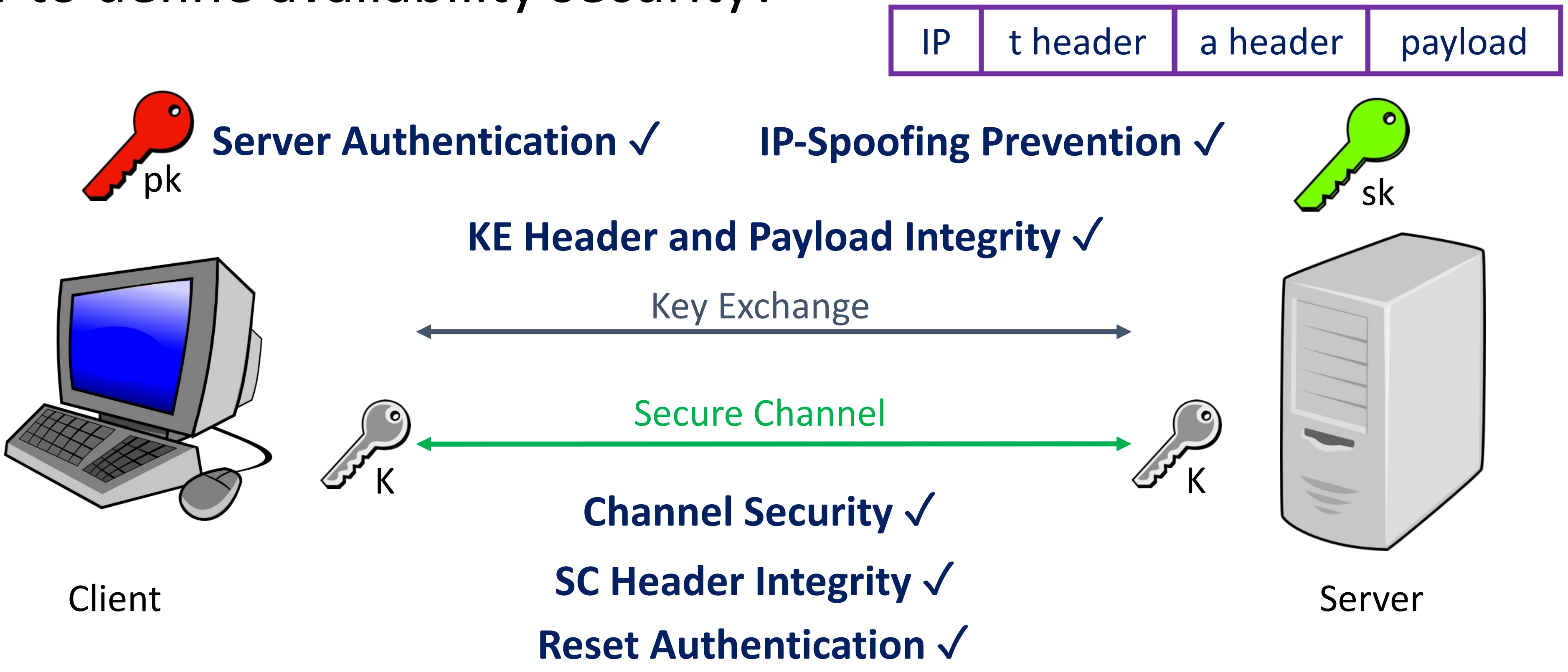
msACCE Security Model

- How to define availability security?



msACCE Security Model

- How to define availability security?



Step 3: Provable Security Results

Summary of Security Results

Layered Protocols	TLS 1.3 TFO	QUIC UDP	QUIC[TLS] UDP
Server Authentication	✓	✓	✓
Channel Security	✓	✓	✓
IP-Spoofing Prevention	✓😀	✓	✓
KE Header Integrity	✗😭	✗	✗
KE Payload Integrity	✓	✗😭	✗😭
SC Header Integrity	✗	✓	✓
Reset Authentication	✗	✗	✓😀

Summary of Security Results

Layered Protocols	TLS 1.3 TFO	QUIC UDP	QUIC[TLS] UDP
Server Authentication	✓	✓	✓
Channel Security	✓	✓	✓
IP-Spoofing Prevention	✓😀	✓	✓
KE Header Integrity	✗😭	✗	✗
KE Payload Integrity	✓	✗😭	✗😭
SC Header Integrity	✗	✓	✓
Reset Authentication	✗	✗	✓😀

Summary of Security Results

Layered Protocols	TLS 1.3 TFO	QUIC UDP	QUIC[TLS] UDP
Server Authentication	✓	✓	✓
Channel Security	✓	✓	✓
IP-Spoofing Prevention	✓😀	✓	✓
KE Header Integrity	✗😭	✗	✗
KE Payload Integrity	✓	✗😭	✗😭
SC Header Integrity	✗	✓	✓
Reset Authentication	✗	✗	✓😀

TCP Fast Open (TFO) Security Result

- **Theorem.** TLS 1.3 over **TFO** achieves **IP-Spoofing Prevention** if
  - cookie generation function is a **PRF** (AES-128)
  - TCP sequence number size is big enough **against online guessing attacks**

Summary of Security Results

Layered Protocols	TLS 1.3 TFO	QUIC UDP	QUIC[TLS] UDP
Server Authentication	✓	✓	✓
Channel Security	✓	✓	✓
IP-Spoofing Prevention	✓😀	✓	✓
KE Header Integrity	✗😭	✗	✗
KE Payload Integrity	✓	✗😭	✗😭
SC Header Integrity	✗	✓	✓
Reset Authentication	✗	✗	✓😀

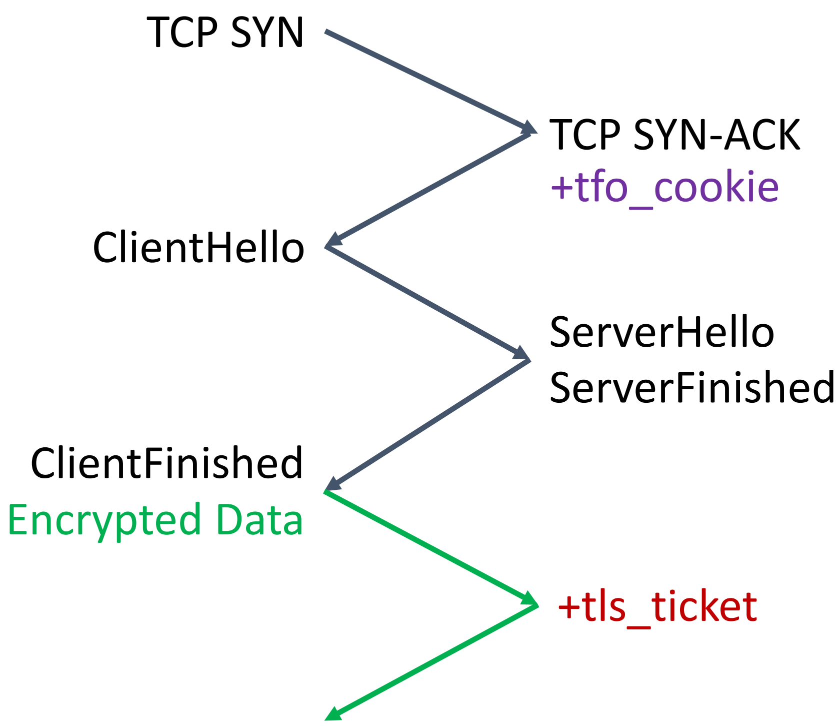
Summary of Security Results

Layered Protocols	TLS 1.3 TFO	QUIC UDP	QUIC[TLS] UDP
Server Authentication	✓	✓	✓
Channel Security	✓	✓	✓
IP-Spoofing Prevention	✓😀	✓	✓
KE Header Integrity	✗😭	✗	✗
KE Payload Integrity	✓	✗😭	✗😭
SC Header Integrity	✗	✓	✓
Reset Authentication	✗	✗	✓😀

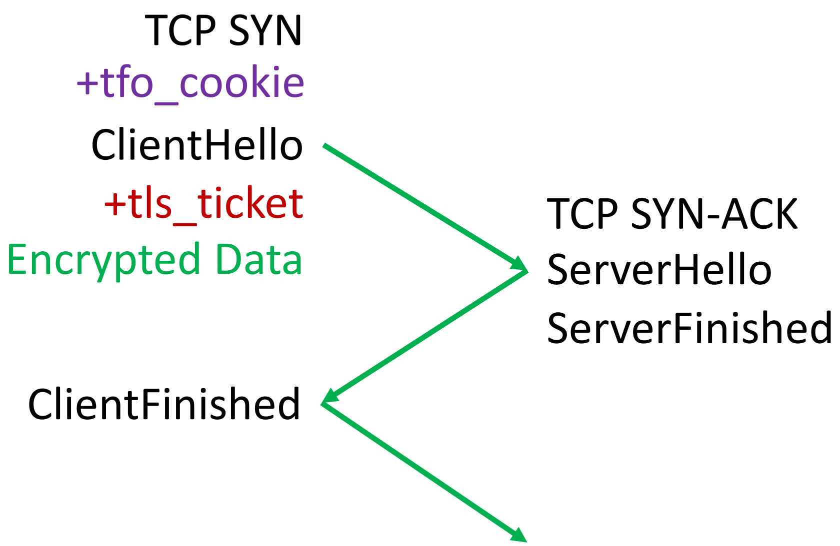
TFO Cookie Removal

Layered Protocols	TLS 1.3 TFO	QUIC UDP	QUIC[TLS] UDP
KE Header Integrity	✗😭	✗	✗

Initial Full Handshake (2-RTT)



Resumption (0-RTT)

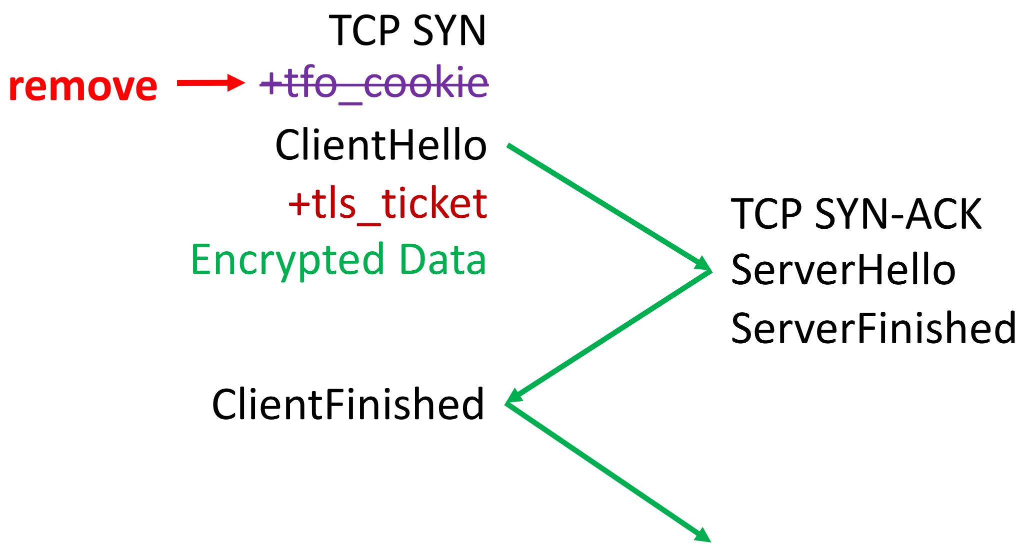


TFO Cookie Removal

Layered Protocols	TLS 1.3 TFO	QUIC UDP	QUIC[TLS] UDP
KE Header Integrity	✗ 😭	✗	✗

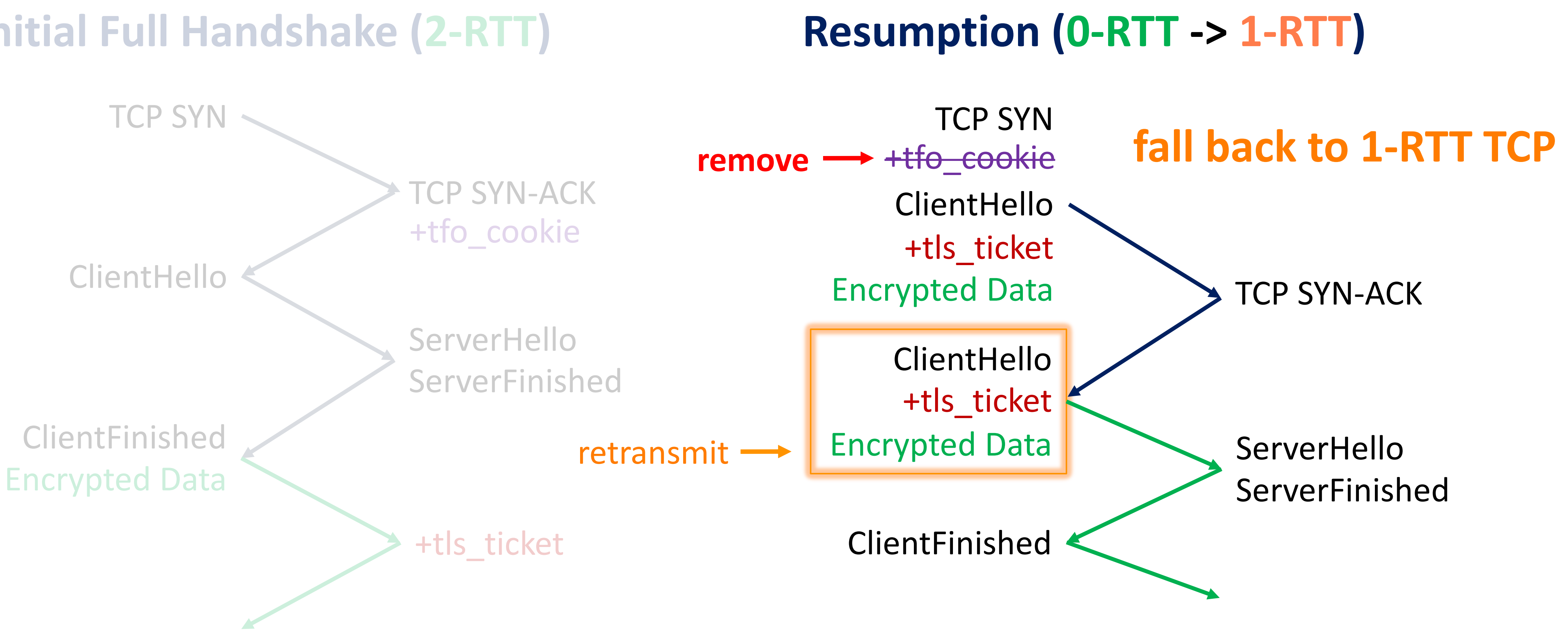
Initial Full Handshake (2-RTT)

Resumption (0-RTT)



TFO Cookie Removal

Layered Protocols	TLS 1.3 TFO	QUIC UDP	QUIC[TLS] UDP
KE Header Integrity	✗😭	✗	✗

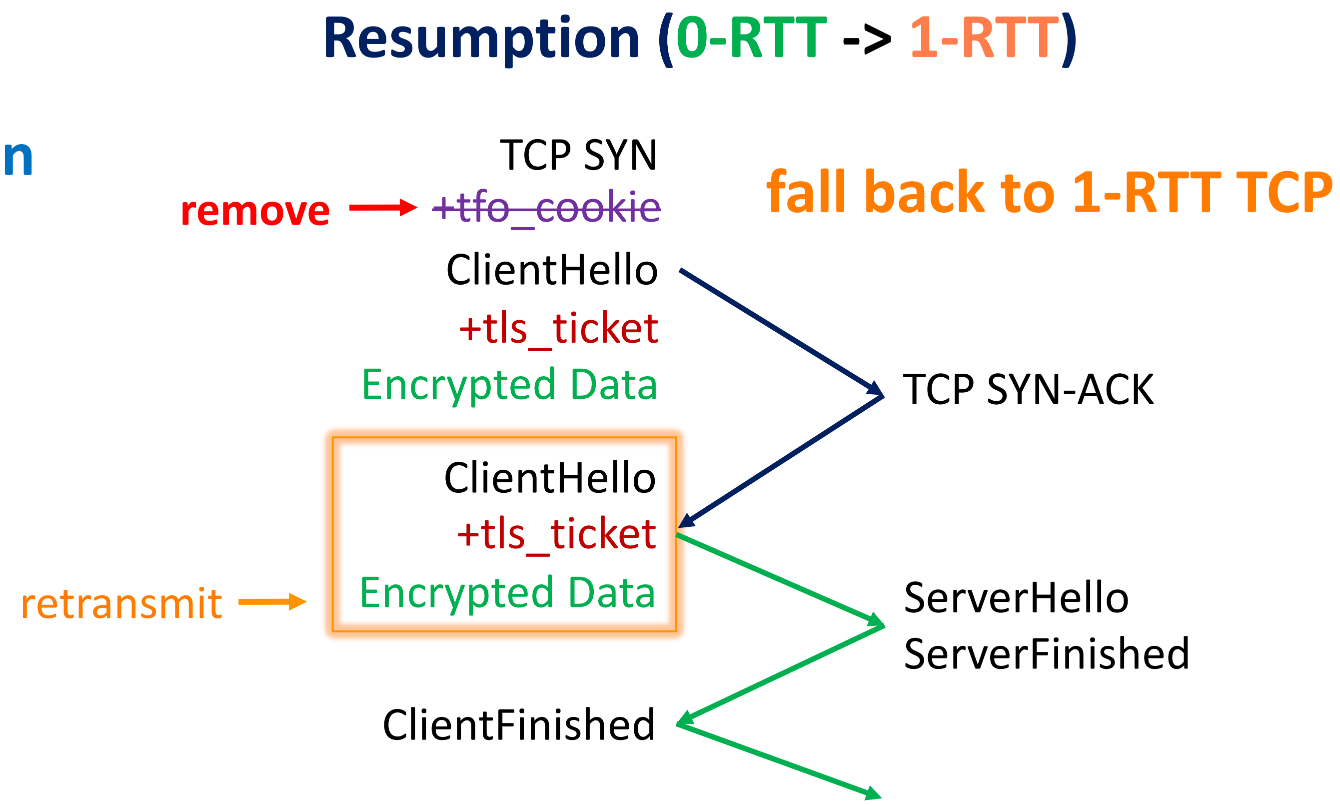


TFO Cookie Removal

Layered Protocols	TLS 1.3 TFO	QUIC UDP	QUIC[TLS] UDP
KE Header Integrity	✗ 😭	✗	✗

Our attack is more harmful than simply dropping packets:

- client thinking server does NOT support TFO
- TFO disabled for a long time



Summary of Security Results

Layered Protocols	TLS 1.3 TFO	QUIC UDP	QUIC[TLS] UDP
Server Authentication	✓	✓	✓
Channel Security	✓	✓	✓
IP-Spoofing Prevention	✓😀	✓	✓
KE Header Integrity	✗😭	✗	✗
KE Payload Integrity	✓	✗😭	✗😭
SC Header Integrity	✗	✓	✓
Reset Authentication	✗	✗	✓😀

Summary of Security Results

Layered Protocols	TLS 1.3 TFO	QUIC UDP	QUIC[TLS] UDP
Server Authentication	✓	✓	✓
Channel Security	✓	✓	✓
IP-Spoofing Prevention	✓😀	✓	✓
KE Header Integrity	✗😭	✗	✗
KE Payload Integrity	✓	✗😭	✗😭
SC Header Integrity	✗	✓	✓
Reset Authentication	✗	✗	✓😀

QUIC[TLS] Security Result

- **Theorem. QUIC**[TLS] over UDP achieves **Reset Authentication** if
  - reset token generation function is a **PRF** (AES-128)
  - **Channel Security holds**
  - reset token size is big enough **against online guessing attacks**

Summary of Security Results

Layered Protocols	TLS 1.3 TFO	QUIC UDP	QUIC[TLS] UDP
Server Authentication	✓	✓	✓
Channel Security	✓	✓	✓
IP-Spoofing Prevention	✓😀	✓	✓
KE Header Integrity	✗😭	✗	✗
KE Payload Integrity	✓	✗😭	✗😭
SC Header Integrity	✗	✓	✓
Reset Authentication	✗	✗	✓😀

Summary

Summary

- Propose the **first** security model that comprehensively capture **availability** properties of **layered** protocols.
- Provide **thorough** provable security comparison of **low-latency** layered protocols: TLS 1.3/TFO, QUIC/UDP, QUIC[TLS]/UDP.
- Identify **new availability attacks** based on our model.
- Help understand the advantages and limitations of novel secure channel establishment protocols.