Appendix -
On Transport Layer Security

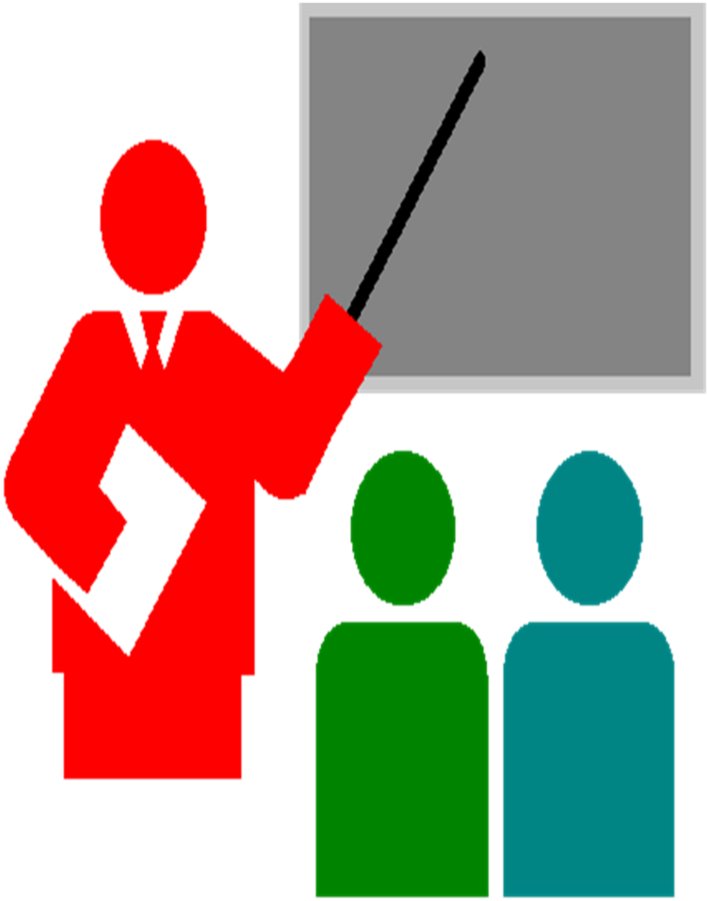
Roch Glitho, PhD

Professor and Canada Research Chair

My URL - http://users.encs.concordia.ca/~glitho/

Concordia University
Engineering and Computer Science
Concordia Institute for Information Systems Engineering

On Transport Layer Security Protocols



- Introduction
- Handshake protocols
- TLS 1.2 and TLS 1.3

Introduction

- Run at the transport layer and provide
  - Authentication
  - Integrity
  - Confidentiality

Introduction

- Evolution
  - 1994: SSL 1.0
  - 1995: SSL 2.0
  - 1996: SSL 3.0

Introduction

- Evolution
  - TLS 1.0 (IETF): 1999
  - TLS 1.2 (IETF) : 2008 - Most widely deployed
  - TLS 1.3 (IETF): 2018 (Used by QUIC)

Introduction

- Two categories of protocols
  - Handshake protocols
  - Record protocols

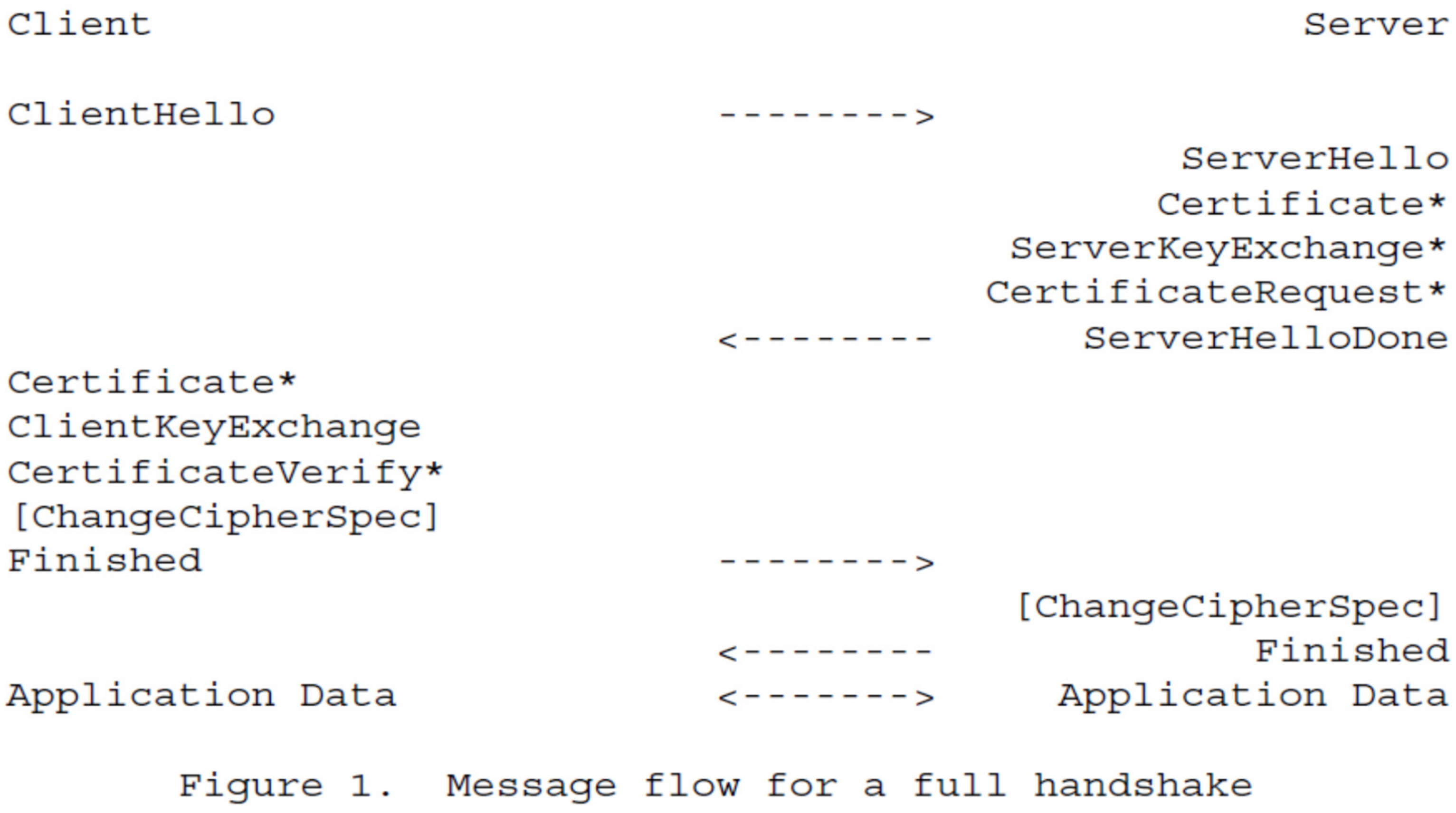
Focus: Handshake protocols

Handshake protocols

- Negotiation, e.g.
  - Cipher suite
  - Protocols versions
  - Compression method
  - Security keys
- Authentication
  - Server (if needed)
  - client

Handshake protocols

- TLS 1.2 (IETF RFC 5246)



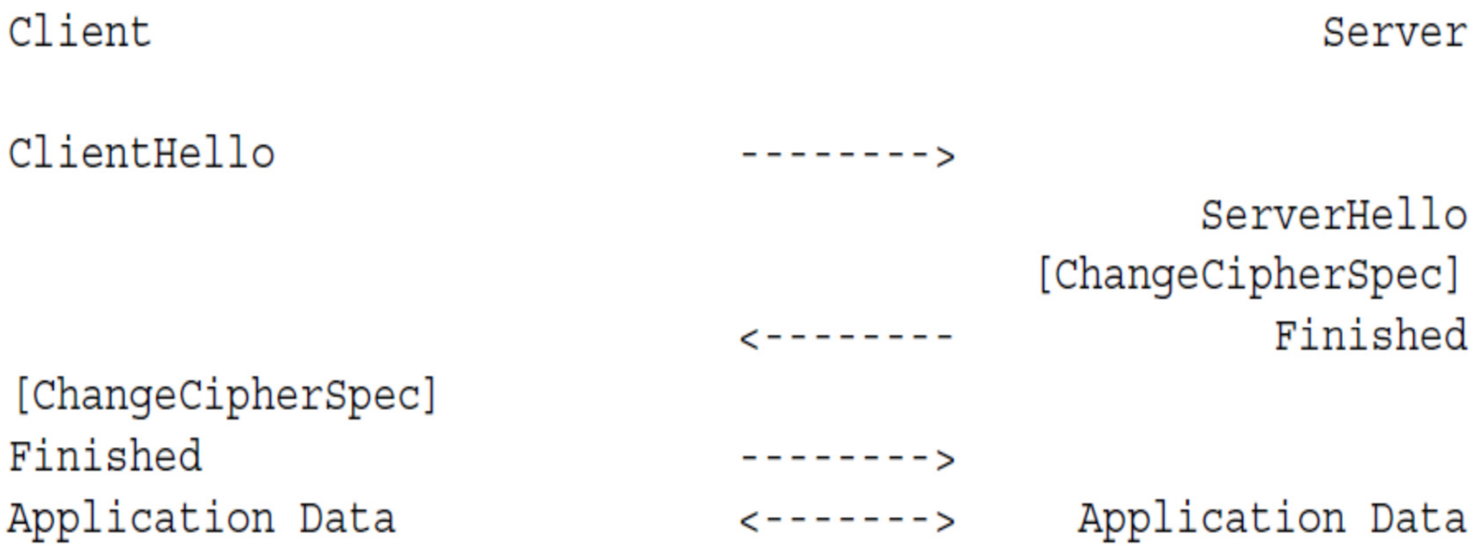
```
Client                                               Server

ClientHello                  -------->
                                                ServerHello
                                               Certificate*
                                         ServerKeyExchange*
                                        CertificateRequest*
                             <--------      ServerHelloDone
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished                     -------->
                                         [ChangeCipherSpec]
                             <--------             Finished
Application Data             <------->     Application Data

       Figure 1.  Message flow for a full handshake
```

Handshake protocols

- TLS 1.2 (IETF RFC 5246)



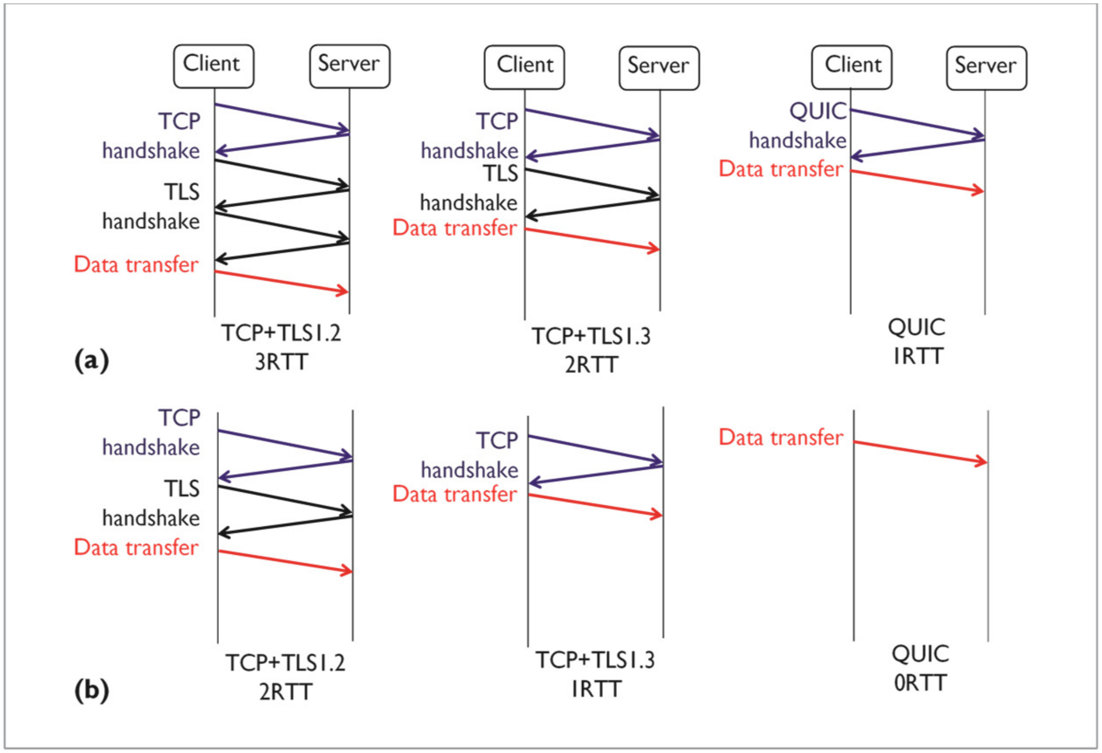
```
Client                                           Server

ClientHello                 -------->
                                            ServerHello
                                     [ChangeCipherSpec]
                            <--------          Finished
[ChangeCipherSpec]
Finished                    -------->
Application Data            <------->  Application Data
```

Figure 2. Message flow for an abbreviated handshake

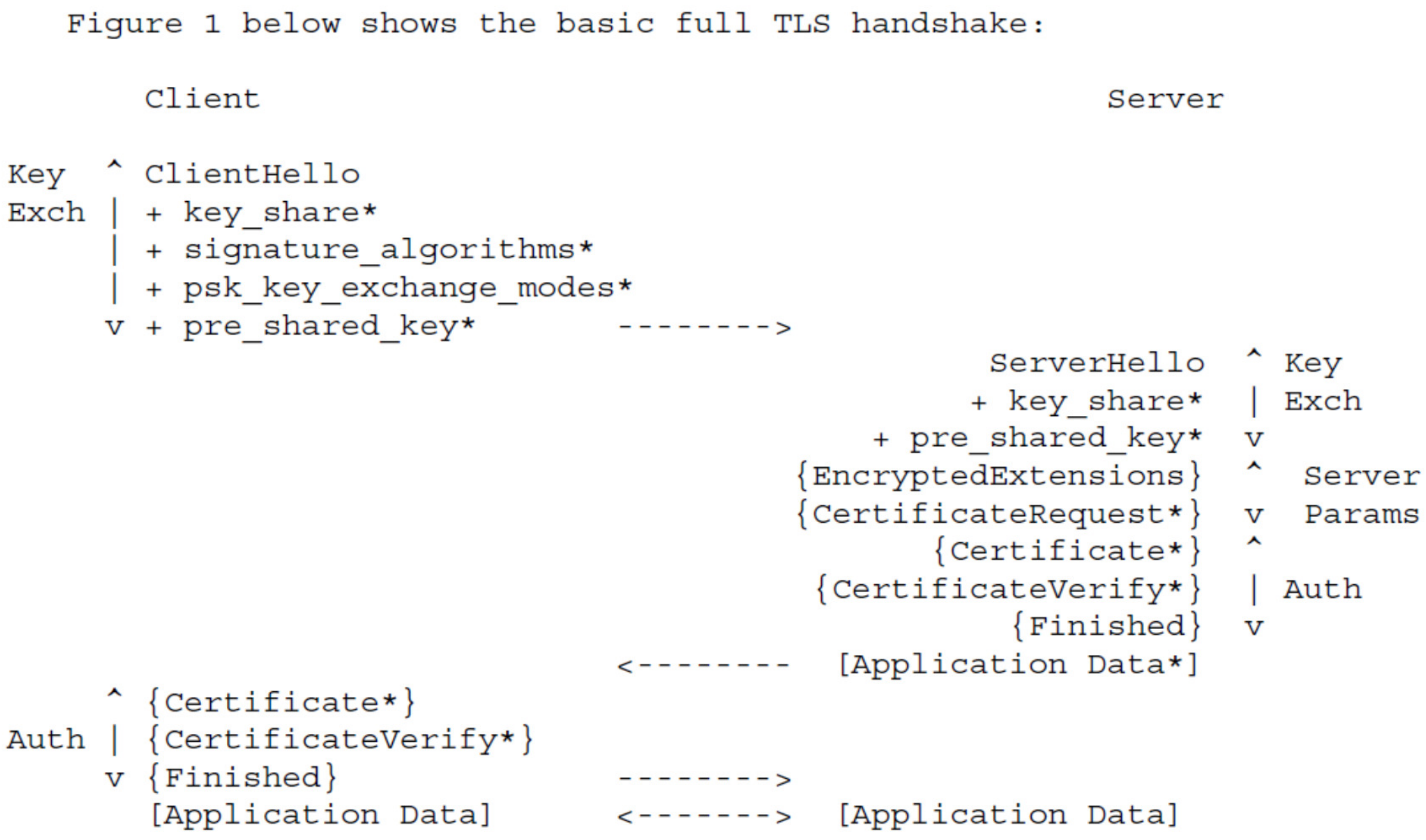
Quick UDP Internet Connection (QUIC)

Fast connection establishment



Handshake protocols

TLS 1.3 (IETF RFC 8446)



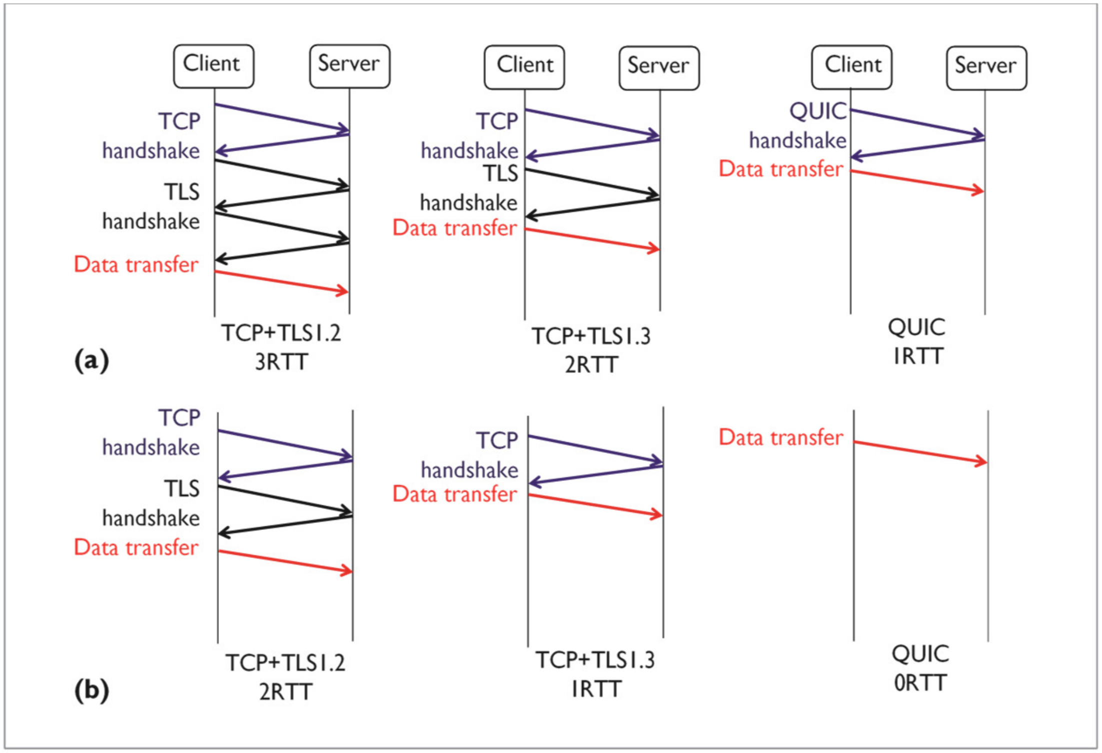
```
   Figure 1 below shows the basic full TLS handshake:

       Client                                           Server

Key  ^ ClientHello
Exch | + key_share*
     | + signature_algorithms*
     | + psk_key_exchange_modes*
     v + pre_shared_key*       -------->
                                                  ServerHello  ^ Key
                                                 + key_share*  | Exch
                                            + pre_shared_key*  v
                                        {EncryptedExtensions}  ^  Server
                                        {CertificateRequest*}  v  Params
                                               {Certificate*}  ^
                                         {CertificateVerify*}  | Auth
                                                   {Finished}  v
                               <--------  [Application Data*]
     ^ {Certificate*}
Auth | {CertificateVerify*}
     v {Finished}              -------->
       [Application Data]      <------->  [Application Data]
```

Quick UDP Internet Connection (QUIC)

Fast connection establishment



The End