# OPTLS Rationale

- New to TLS: Forward secrecy (PFS), 0-RTT, ECC-centric instantiation
- Calls for:
  - DH as the essential primitive (PFS and ECC)
  - Server static DH key (to encrypt 1st flow data, signatures useless for 0-RTT)
  - Caching of static key at client (0-RTT and optimizations)
- Observation: Instead of using two different protocol logics for regular 1-RTT and 0-RTT/Caching, unify via static DH key:
  - Server signs static key; then uses it for session authentication, caching, and 0-RTT
  - Uniform spec, unified key derivation, single protocol analysis (also applies to PSK with and without PFS)
  - Performance optimization (esp. huge savings with RSA via static key caching)

# OPTLS Overview

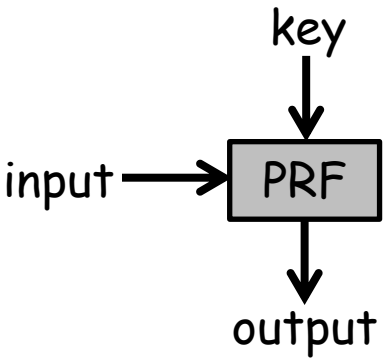
- C to S: C-hello, $g^x$, [C-ed]
- S to C: S-hello, $g^y$, [S-ske], S-fin = prf($g^{xs}$ ; session-hash)
- C to S: C-fin = prf($g^{xs}$ ; session-hash)

- C-ed (client early data): Enc($g^{xs}$ ; early-data)
- S-ske (server static key envelope): $g^s$, S-cert, Sig($g^s$, session-hash)

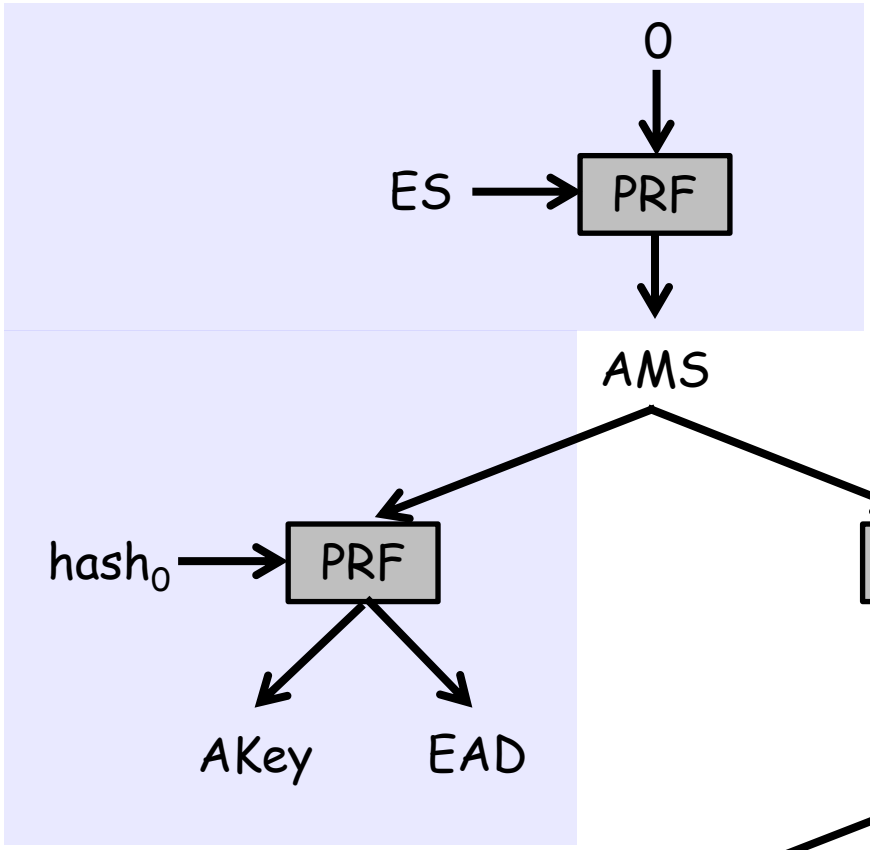
- Cases (all run Basic protocol plus possible additions)
  - Cached 1-RTT: Basic only; assumes C has $g^s$ but no C-ed (0 sig, 2 exp)
  - Cached 0-RTT: Basic + [C-ed], assumes C has $g^s$ (0 sig, 2 exp)
  - Transport 1-RTT: Basic + [S-ske], C caches $g^s$ (1 amortized sig, 2 exp)
  - Ephemeral 1-RTT: Basic + [S-ske] , ephemeral $g^s$, no caching (1 sig, 1 exp)
    - Ephemeral derives record keys from $g^{xy}$ only, others from both $g^{xy}$ and $g^{xs}$

# Notation

- Upper arrow: key
- Side arrow: input
- Down arrow: output




- ES: ephemeral-static $g^{xs}$ EE: ephemeral-ephemeral $g^{xy}$
- MS =Master Secret AMS = Authentication MS
- AKey = Authentication Key EAD = Early Application Data
- HTK = Handshake Traffic Keys ATK = Application Traffic Keys
- UMS = Update MS RMS = Resumption MS
- $hash_0$, $hash_1$, $hash_2$ = incremental session hash values




- 0-RTT: Full diagram
- PSK-DHE: AMS=PSK, no ES
- PSK: AMS=PSK, EE=0, no ES
- Resumption: AMS=RMS, EE=0
- 1-RTT (sig-based): AMS=0 and omit shadowed area