Binding Properties for Attested TLS

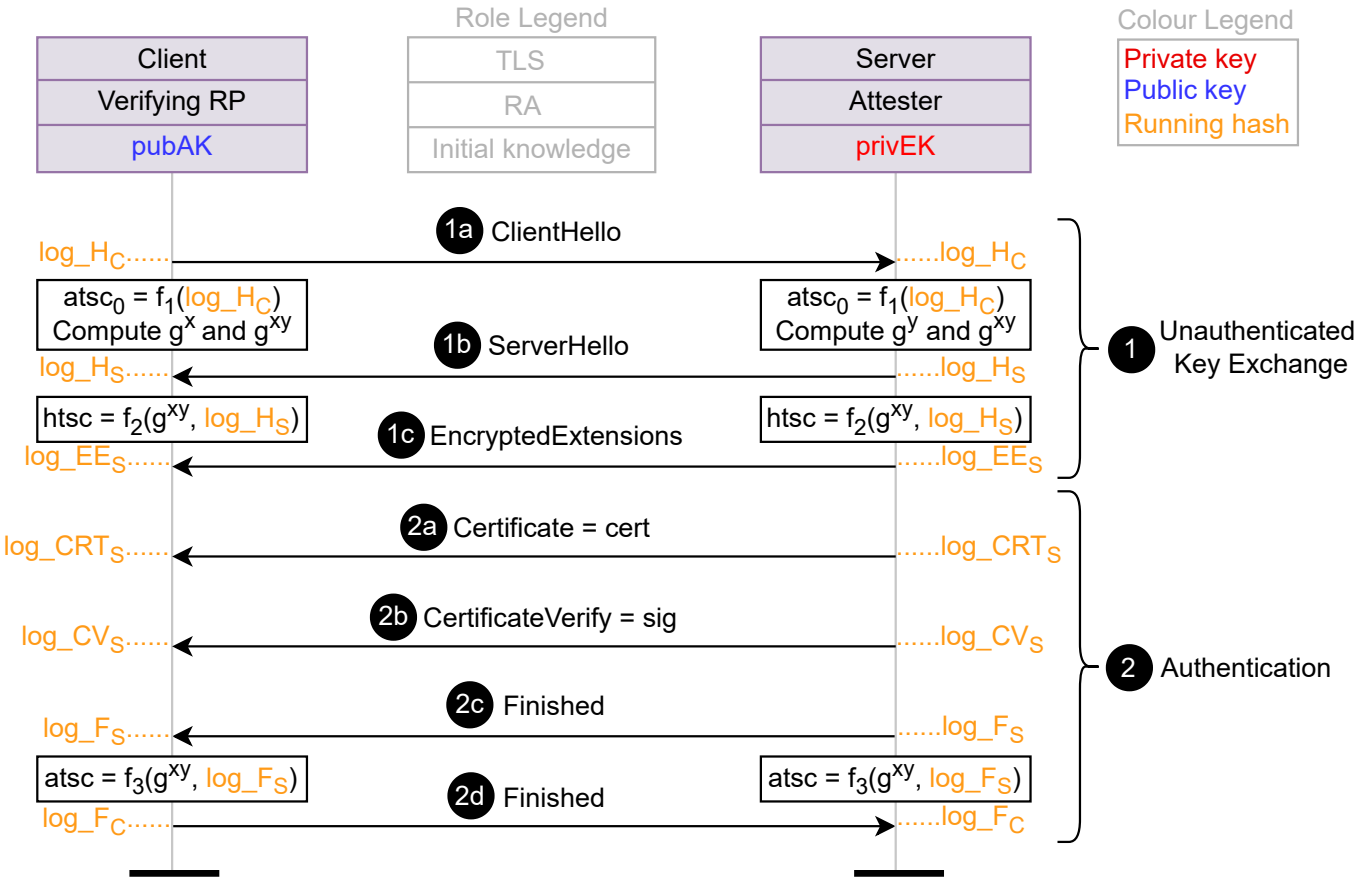
Muhammad Usama Sardar[1,2]

[1]TU Dresden, Germany

[2]Co-chair, Trusted Research Environment (TRE) Open Suite,
Global Alliance for Genomics and Health (GA4GH)

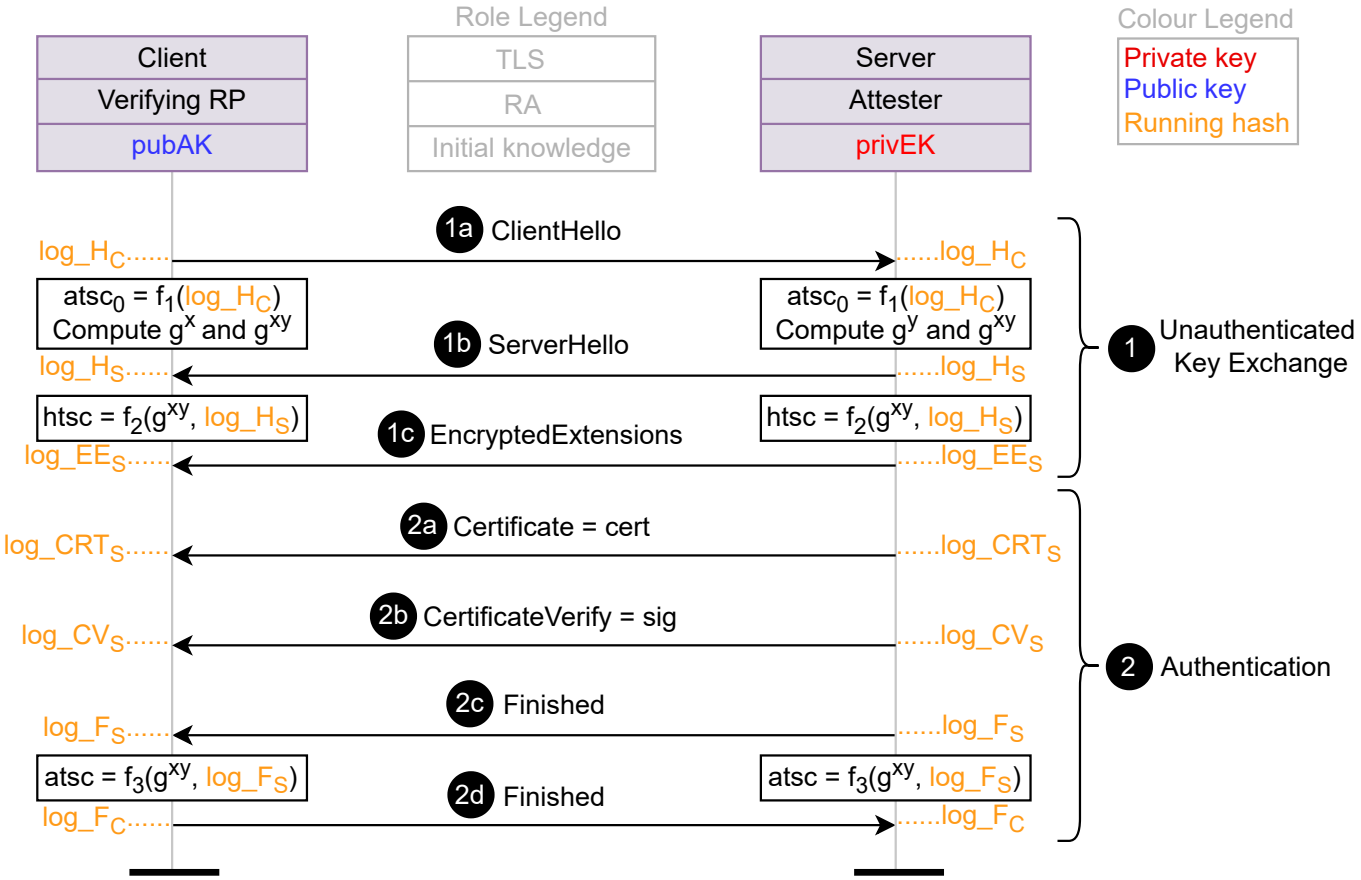
December 16, 2025

Strong Binding vs. Relay of Evidence (Abstracted)



- g^{xy}: Shared Diffie-Hellman key; f_1, f_2, f_3: Key derivation functions
- Discussion: Correlating Evidence to `htsc` vs. `atsc`
  - Running hash $\Longrightarrow$ `atsc` transitively includes all contributions in `htsc`
  - `atsc` provides stronger binding and avoids relay attacks.

Strong Binding vs. Relay of Evidence (Abstracted)



- `htsc`: used for encryption of clientFinished message (2d).
  - Irrelevant for security goals
- `atsc`: used for encryption of application data (client's secret, e.g., decryption key)
  - Relevant for security goals

Links to Resources

- Paper on identity crisis
  - https://www.researchgate.net/publication/398839141_Identity_Crisis_in_Confidential_Computing_Formal_Analysis_of_Attested_TLS
- Wiki page
  - https://github.com/EuroProofNet/ProgramVerification/wiki/AttestedTLS
- Formal proof of insecurity of pre- and intra-handshake attestation
  - https://github.com/CCC-Attestation/formal-spec-id-crisis
- Post-handshake attestation draft
  - https://datatracker.ietf.org/doc/draft-fossati-seat-expat/
- Attestation in Arm CCA and Intel TDX
  - https://github.com/CCC-Attestation/formal-spec-TEE
- Security considerations of remote attestation
  - https://datatracker.ietf.org/doc/draft-sardar-rats-sec-cons/
- IETF SEAT WG
  - https://datatracker.ietf.org/wg/seat/about/
- Technical Concepts
  - https://www.researchgate.net/publication/396199290_Perspicuity_of_Attestation_Mechanisms_in_Confidential_Computing_Technical_Concepts
- Validation of TLS 1.3 Key Schedule
  - https://www.researchgate.net/publication/396245726_Perspicuity_of_Attestation_Mechanisms_in_Confidential_Computing_Validation_of_TLS_13_Key_Schedule
- General Approach
  - https://www.researchgate.net/publication/396593308_Perspicuity_of_Attestation_Mechanisms_in_Confidential_Computing_General_Approach
- Weekly meetings
  - https://github.com/tls-attestation#meetings

ACK: Co-authors (in papers/IETF drafts)

- Jean-Marie Jacquet (University of Namur)
- Ionut Mihalcea (Arm)
- Thomas Fossati (Linaro)
- Arto Niemi (Huawei)
- Hannes Tschofenig (University of Applied Sciences Bonn-Rhein-Sieg and Siemens)
- Simon Frost (Arm)
- Ned Smith (Intel)
- Carsten Weinhold (Barkhausen Institut)
- Michael Roitzsch (Barkhausen Institut)
- Yogesh Deshpande (Arm)
- Yaron Sheffer (Intuit)
- Tirumaleswar Reddy K. (Nokia)
- Henk Birkholz (Fraunhofer SIT)
- Mariam Moustafa (Aalto University)
- Tuomas Aura (Aalto University)
- Liang Xia (Huawei)
- Weiyu Jiang (Huawei)
- Jun Zhang (Huawei)
- Houda Labiod (Huawei)
- Yuning Jiang (Huawei International)
- Meiling Chen (China Mobile)
- Peter Chunchi Liu (Huawei Technologies)
- Minghui Xu (Shandong University)
- Pavel Nikonorov (GENXT)
- Viacheslav Dubeyko (IBM)

ACK: Contributors

- Eric Rescorla (Independent)
- Laurence Lundblade (Security Theory LLC)
- Göran Selander (Ericsson AB)
- Marco Tiloca (RISE AB)
- Richard Barnes (Cloudflare)
- Giridhar Mandyam (AMD)
- Christopher Patton (Cloudflare)
- Dionna Amalie Glaze (Google)
- Bob Beck (Google)
- Mike Ounsworth (Cryptic Forest Software)
- John Preuß Mattsson (Ericsson Research)
- Cedric Fournet (Microsoft)
- Thore Sommer (TU Munich)
- Nikolaus Thümmel (Scontain)
- Jonathan Hoyland (Cloudflare)
- Jo Van Bulck (KU Leuven)
- Martin Thomson (Mozilla)
- Britta Hale (Naval Postgraduate School)
- Werner Staub (CORE Association)
- Christian Simmen (DENIC)
- Dennis Jackson (Mozilla)
- Peg Jones (Flashbots)
- Paul Wouters (Aiven)
- Matthias Wählisch (TU Dresden)
- Andrey Ruzhanskiy (Telekom MMS)
- Muuhh Ikede (Cybertrust)
- Mike Bursell (CCC)
- Ravi Sahita (Rivos)
- Samuel Ortiz (Rivos)
- Mathieu Poirier (Linaro)
- Hannes Reinecke (SUSE)
- Alexander Graf (AWS)
- Elena Reshetova (Intel)
- Jon Lange (Microsoft)
- Daniel Kiper
- David Woodhouse (AWS)
- David Kaplan (AMD)
- Tiziano Santoro (Google)
- Markus Rudy (Edgeless Systems)