Continuous Authentication in Secure Messaging

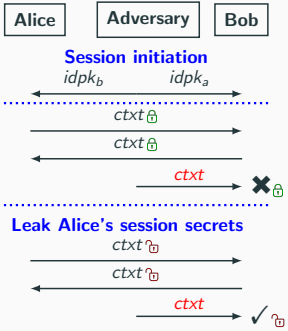
Benjamin Dowling ✉ b.dowling@sheffield.ac.uk
University of Sheffield
Felix Günther ✉ mail@felixguenther.info
ETH Zürich
Alexandre Poirrier ✉ alexandre.poirrier@polytechnique.org
École polytechnique

April 14th, 2022

Signal Security

Signal offers several security properties:

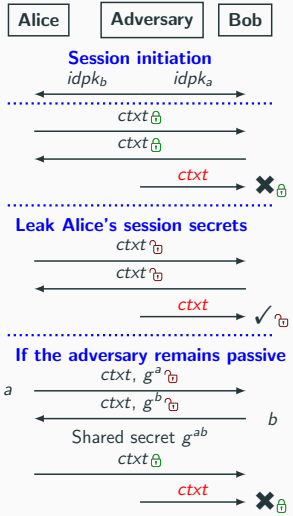
- Secrecy: Plaintexts cannot be deduced from ciphertexts.
- Authenticity: Accepted ciphertexts come from message keys holders.
- Forward secrecy: Messages received before a state compromise are still secret.



Signal Security

Signal offers several security properties:

- Secrecy: Plaintexts cannot be deduced from ciphertexts.
- Authenticity: Accepted ciphertexts come from message keys holders.
- Forward secrecy: Messages received before a state compromise are still secret.
- Post-compromise security: After a state compromise, if the adversary remains **passive**, secrecy and authenticity are restored.

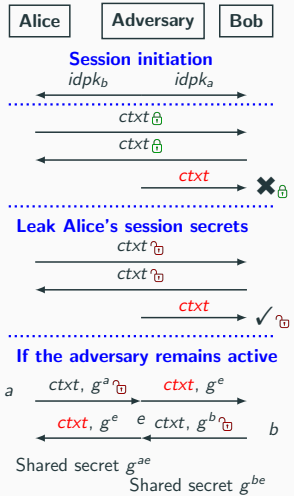


Signal Security

Signal offers several security properties:

- Secrecy: Plaintexts cannot be deduced from ciphertexts.
- Authenticity: Accepted ciphertexts come from message keys holders.
- Forward secrecy: Messages received before a state compromise are still secret.
- Post-compromise security: After a state compromise, if the adversary remains **passive**, secrecy and authenticity are restored.

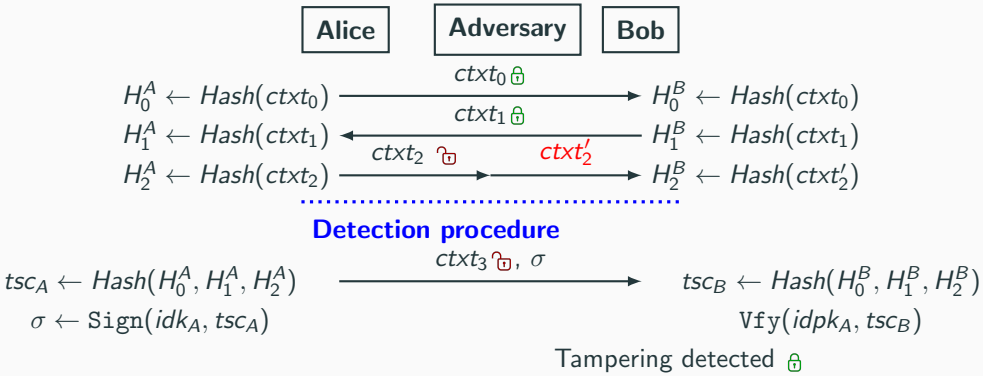
But if the adversary remains active, the communication stays compromised.



Contributions

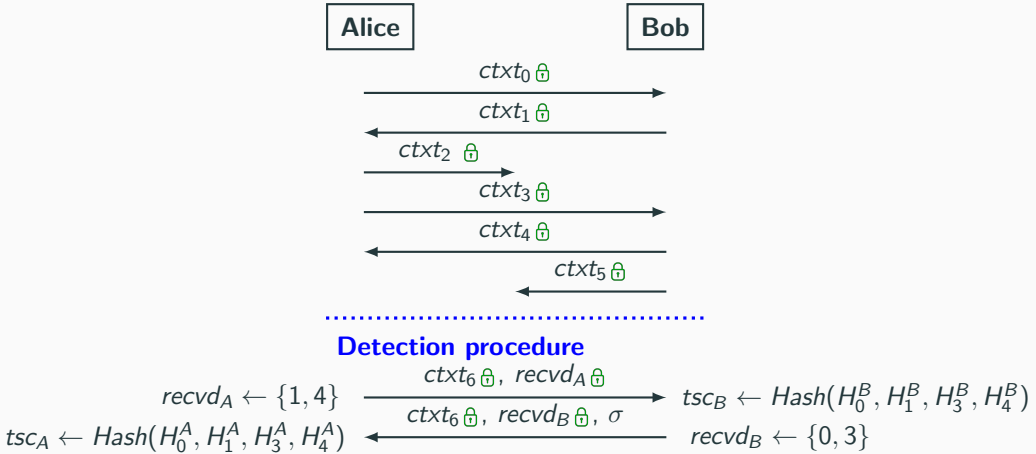
1. Formal security model for continuous authentication, capturing post-compromise security against active adversaries who have not compromised long-term secrets.
2. A generic extension for messaging protocols such as Signal to provide them with provably-secure continuous authentication.
3. A seamless implementation on top of the Signal Java library, with overhead analysis and benchmarks (not covered here).

Authentication steps (simplified)



Transcripts sent in the authentication step are authenticated with long-term keys. In this example, $H_2^A \neq H_2^B$ so the attacker is detected in-band.

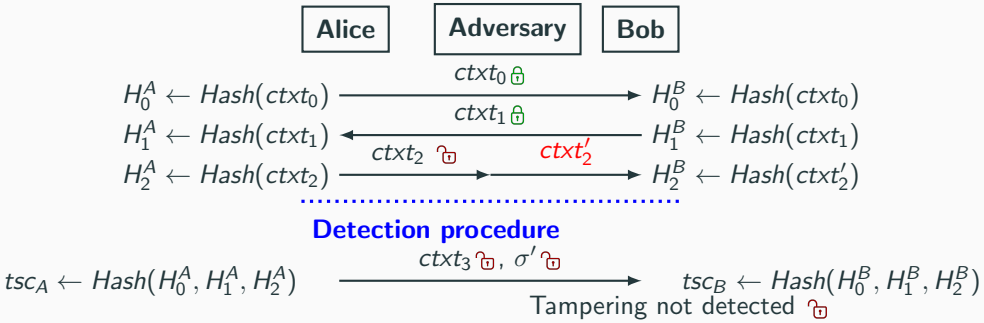
Working on an unreliable channel



One additional message is sent to inform parties of messages they have received, so they can compute transcripts only on common messages.

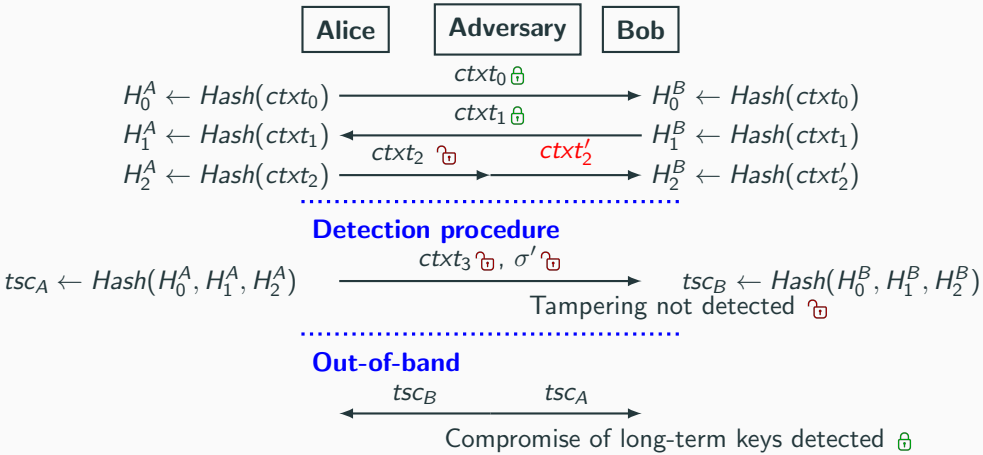
Bonus: long-term secret compromise detection using an out-of-band channel

What if long-term secrets are compromised?

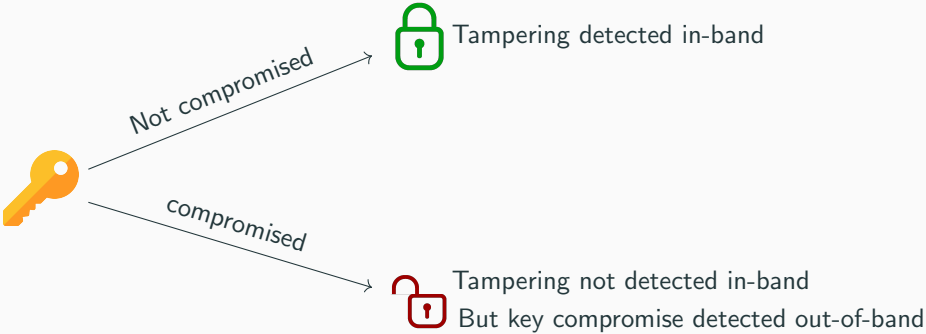


Bonus: long-term secret compromise detection using an out-of-band channel

What if long-term secrets are compromised?



Conclusion



A generic solution.

Proof of concept on top of the official Jave library.

Alternative solutions.