Dual-Receiver Encryption and Deniable Authentication

Youngtae Youn and Adam Smith

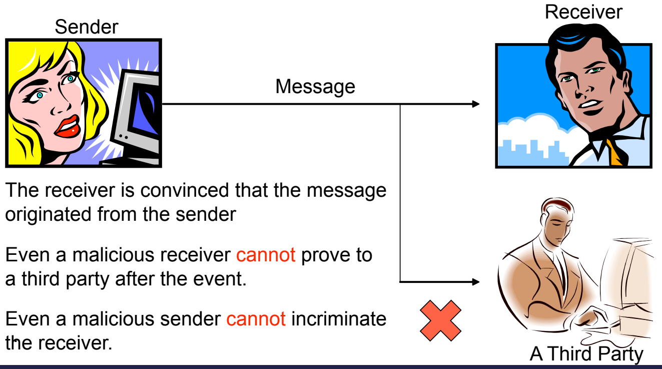
Research Goal

Deniable Authentication guarantees seemingly *paradoxical* security constraints.

- The receiver can verify that the message is from the sender.
- But it cannot be proved to a third party after the event.
- The receiver cannot be incriminated as having been involved.

Deniable authentication can be applied to many situations, such as:

- Off-the-record in journalism sourcing
- Whistle-blowing
- Espionage



The receiver is convinced that the message originated from the sender

Even a malicious receiver cannot prove to a third party after the event.

Even a malicious sender cannot incriminate the receiver.

Contributions

- Efficient deniable authentication with on-line deniability.

Deniability should hold even when one of the parties colludes with a third party *during execution of the protocol.*

Off-line setting: A malicious party records the transcript and shows it to a third party after the fact.

- Main Tool: An efficient Dual-Receiver Encryption scheme

Efficient DRE construction

- Ciphertexts of Kiltz' Tag-based Encryption (TBE) consist of five group elements.
- If two ciphertexts contain the same plaintext, *five* linear equations on *eight* variables always hold.
- We construct Groth-Sahai (GS) Proof on these equations.
- The GS proof on these equations results with 34 group elements in bilinear group.
- The naïve approach use general NP-reduction to some NP languages such as *Circuit Satisfiability,* which ends up with thousands of gates – prohibitively expensive.
- In addition to space efficiency, this construction is also *provably secure* in the standard model.

Building Blocks

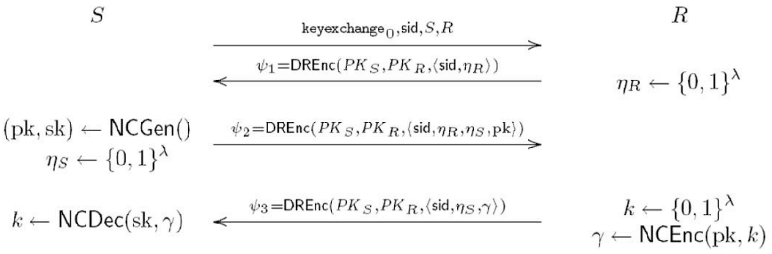
Non-Committing Encryption (NCE): `NCEnc`, `NCDec`

- It operates just like the usual encryption scheme.
- But can generate indistinguishable rigged public keys and ciphertexts
- such that the ciphertexts can be made to appear as if they contain any desired plaintext.

Dual-Receiver Encryption (DRE): `DREnc`, `DRDec`

- It encrypts a message to two parties with a *single* ciphertext
- Two receivers are guaranteed to recover the same message.

Deniable Authentication Protocol



$\mathsf{keyexchange}_0, \mathsf{sid}, S, R$

$\psi_1 = \mathsf{DREnc}(PK_S, PK_R, \langle \mathsf{sid}, \eta_R \rangle)$

$\eta_R \leftarrow \{0,1\}^\lambda$

$(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathsf{NCGen}()$

$\eta_S \leftarrow \{0,1\}^\lambda$

$\psi_2 = \mathsf{DREnc}(PK_S, PK_R, \langle \mathsf{sid}, \eta_R, \eta_S, \mathrm{pk} \rangle)$

$k \leftarrow \{0,1\}^\lambda$

$\gamma \leftarrow \mathsf{NCEnc}(\mathrm{pk}, k)$

$\psi_3 = \mathsf{DREnc}(PK_S, PK_R, \langle \mathsf{sid}, \eta_S, \gamma \rangle)$

$k \leftarrow \mathsf{NCDec}(\mathrm{sk}, \gamma)$

- sid, η_R, η_s are nonces.
- The key *k* is encrypted by non-committing encryption.
- We combine Kiltz' Tag-based Encryption (TBE) with Groth-Sahai (GS) proof to construct an efficient DRE scheme.

Conclusion and Future Works

- **Conclusion**
  - *First* practical implementation of On-Line Deniable Authentication.
  - *Provably secure* in the standard model without resort to any heuristics such as random oracle model.
  - The DRE scheme can be applied to other crypto protocols.
- **Future works**
  - Use other encryption schemes to *improve* performance of DRE.
  - Rigorously define the notion of deniability in various settings.
- **References**

- Dodis, Katz, Smith and Walfish, *Composability and On-Line Deniability of Authentication*, TCC 2009
- Damgaard and Nielsen, *Improved Non-committing Encryption Schemes Based on a General Complexity Assumption*, Crypto 00
- Kiltz, *Chosen-Ciphertext Security from Tag-Based Encryption*, TCC 06
- Groth and Sahai, *Efficient Non-interactive Proof Systems for Bilinear Groups*, Eurocrypt 08

Sponsored by the National Science Foundation