Zone Encryption with Anonymous Authentication for V2V Communication

Jan Camenisch, Manu Drijvers, Anja Lehmann, Gregory Neven and Patrick Towa

Gautam Singh

Indian Institute of Technology Hyderabad

April 23, 2024

1. Introduction
2. Preliminaries
3. Zone Encryption
4. Group Signatures with Attributes
5. Conclusion

What is V2X?

1. Introduce V2X-related terms like pseudonym, RSU, CAM, etc.
2. Mention US/Europe standards for V2X.

V2X and Cryptology

1. 100/20 pseudonyms per week
2. 300 byte per CAM bandwidth constraint
3. Crypto implications of the above

Motivation and Goals

1. Aim to tackle the problem of privacy.
2. Address the problem of authenticity and confidentiality in combination *for the first time* (important to mention this?).
3. Meet (bandwidth) requirements.
4. Efficient encryption scheme (symmetric-key crypto).
5. Better security guarantees (privacy, authenticity, confidentiality).

Preliminaries

This is a slide with the list of preliminaries needed to understand ZE. We pick up the ones not covered (top down approach, start from ZE and then explain these if needed). Must list purpose of each preliminary here.

1. Pairing Groups
2. Hardness Assumptions (lot of notation, may be hard to grasp)
    1. SDL
    2. q-MSDH-1
3. Deterministic Authenticated Encryption (how much to cover?)
4. PS Signatures
5. DGS+A

Syntax of ZE Scheme

1. Define zone, payload, epoch.
2. Explain all the algos used.

Security Properties

Attack game and definitions 3-6 (are theorems 4-8 needed?)

Instantiation of ZE and Efficiency

(Is it worth mentioning section 4.4.1 or can we leave this?)

Summary of ZE

Table 2 of the paper.

DGS+A

Sub-headings

1. Syntax
2. Security properties (no proofs)
3. Instantiation from PS
4. Can be extended to threshold opening (should be a slide or only a mention during talk?)

Challenges in Deploying ZE

Section 4.6

Future Improvements

Section 4.6, brief and top-level idea of mini-project if time permits.