Thesis

Sergi Simón Balcells

February 27, 2023

Contents

1 PROJ RoadMap to write thesis

☒ What to include?

☒ Sections

1.1 Previous work

https://recsi2022.unican.es/wp-content/uploads/2022/10/LibroActas-978-84-19024-14-5.pdf

2 TODO Abstract

- ☐ Dunno, base it on previous work

An on-line forum is a platform which enables users to post messages which become available to any person with access to it. In this articles, we focus on forums which preserve the anonymity of a user while being authenticated. More concretely, in this paper we improve an existing scheme.

Index terms - cryptography, discussion board, privacy, ring signature

3 TODO Introduction

- ☒ Forum signature use case
- ☒ Signatures schemas: ring and group
- ☒ ~~Previous work~~ would be in caveats of previous approach

Enterprises, city halls and educators found a way to guarantee anonymous feedback by providing a mail box where people could post a message without specifying who it was. This enabled workers, citizens and students to provide feedback without any chances of having repercussions for critisizing them. At the same time, as the location of them was inside of the enterprise, city and eductional center, the readers could assert with some security that the writer was, in fact, an employee, a citizen, and a student.

With the arrival of the Internet, some of these activities could be totaly online, as a remote office, so it made appearent that there is a need for a security protocol that preserves the anonymity of the poster while it makes sure that the writer is an authenticated user. This use case will be refered as a forum in this paper.

Such cryptographic system should provide a means to authenticate, so only users can post messages. The users should remain anonymous, as the identity of the message author is not revealed. Additionally, messages from the same user should remain unlinkable.

For this cryptographic schemes, a Group signature [1] could provide the required security purposes. However, this cryptographic scheme includes a

trusted group manager, who is able to revoke the anonymity of the writer when required. To overcome this difficulty, the protocol described here will user a similar tool, namely ring signatures [2]. This does not require its users to trust the entity with the exception of certificate authorities issuing public key certificates.

4 Preliminaries

- ☐ Group signature
- ☐ Ring Signature
- ☐ Internet writer distribution

5 TODO Caveats of previous approach

- ☐ bad start makes different for weight
- ☐ bad if user changes habits
- ☐ depending on weight, bad for lurker or bad for super users

6 TODO Window approach

- ☐ window of last n messages
- ☐ simplified complexity if the forum grows larger
- ☐ computes weight based on that, so there is a maximum weight possible

7 TODO Results

- ☐ add graphic distribution of anonymity
  - ☐ explain that if users have the same amount of signatures but one has low anonymity while other high, then you have less chance to get the correct user
- ☐ add caveat of first message
  - ☐ explain that in simulations, it has even better anonymity than normal

☐ Add boxplots of anonymity of users.

8 TODO Conclusions

☐ Window is a superior approach to forum schemes.

9 TODO Acknowledgements

☐ I don't know if I have any

10 TODO References

☐ The eight references of my life.

☐ delete this, as the latex block takes care already

References

[1] E. b. H. D. Chaum, "Group signatures in advances in cryptology - eurocrypt'91, lecture notes in computer science," vol. 547, pp. 257–256, 1991.

[2] Y. T. R.L. Rivest, A. Shamir, "How to leak a secret, in intl. conf. on the theroy and application of cryptology and information security, lecure notes in computer science," vol. 2248, pp. 552–565, 2001.