ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Tighter Security for Group Key Agreement in the Random Oracle Model

Bachelor Thesis

A. Ellison

January 19, 2038

Advisors: Prof. Dr. D. Hofheinz, Dr. K. Klein
Department of Computer Science, ETH Zürich

Abstract

TODO: How to adapt abstract? What should it contain?

The Messaging Layer Security (MLS) protocol, recently standardized in RFC 9420 [2], aims to provide efficient asynchronous group key establishment with strong security guarantees. TreeKEM is the construction underlying MLS and a variant of it was proven adaptively secure in the Ran- dom Oracle Model (ROM) with a polynomial loss in security in [1]. The proof makes use of the Generalized Selective Decryption (GSD) security game introduced in [6], adapted to the public-key setting. GSD security is closely related to the security of TreeKEM and the encryption scheme used in TreeKEM was proven to be GSD secure in the ROM under the standard assumption of IND-CPA security, implying a proof of security for TreeKEM (a sketch of this proof was provided in [1] for the TreeKEM variant).

TODO: describe results

Contents

Is there a predefined structure to the thesis?

Chapter 1

Introduction

TODO: more accessible introduction on why this is important We all rely on messaging applications like WhatsApp, Signal, etc. in our daily lives and take it for granted that our messages will be transmitted securely ("see it as a prerequisite" maybe better?). smoother transition to talking about protocols? For two parties, the Double Ratchet protocol is a common solution (true?) to transmit messages securely and efficiently. For more than two parties this problem was only solved recently with the MLS protocol.

The Messaging Layer Security (MLS) protocol, recently standardized in RFC 9420 [2], aims to provide efficient asynchronous group key establishment with strong security guarantees. The main component of MLS, which is the source of its important efficiency and security properties, is a protocol called TreeKEM (initially proposed in [3]). In essence, TreeKEM, as adopted from its predecessors, structures a group of users as a binary tree with the group key at the root and all group members as leaves. Group members may then compute the group key, update it or add/remove other members with a number of operations logarithmic in the group size.

As for any scheme, it is important to have formal security guarantees for TreeKEM based on precise hardness assumptions. Providing security definitions for the scheme already helps to describe exactly what assumptions are made on the capabilities of an adversary and what kind of security one should expect when using the scheme in practice. Moreover, proofs of (reasonably tight) security under these definitions serve as a guide to implementors on what values to choose for the security parameters of the scheme and provide strong justification that there are no flaws in its design. Given that a major vision for the MLS protocol is for it to be used by messaging applications and that it has support from several large companies ([4], [5]), it has the potential to be used by a huge number of users. Thus, it is important to better understand the security of MLS and hence also of TreeKEM.

One choice that can be made when defining the security of TreeKEM is whether the adversary is modeled as *selective* or *adaptive*. In the former case, the adversary must provide all the interactions it will have with the protocol and when it will attempt to break the scheme at the beginning of the security game, while in the latter case the adversary can make its decisions based on responses from previous interactions. Clearly, the adaptive setting is much closer to how an attack would unfold in practice, so it is desirable to prove security against adaptive adversaries. However, achieving this without too much of a blow-up in the security loss is a challenge since one often resorts to guessing actions performed by the adversary.

The Generalized Selective Decryption (GSD) security game ([6]) was introduced precisely to analyze adaptive security for protocols based on a graph-like structure (as is the case with TreeKEM). In [1], a variant of TreeKEM was proven adaptively secure in the Random Oracle Model (ROM) with a security loss in $\mathcal{O}((n \cdot Q)^2)$, where n is the number of users and Q the number of protocol operations performed by these users. The proof mainly relies on showing that the encryption scheme employed in TreeKEM, a slight modification of an arbitrary IND-CPA secure encryption scheme, is GSD secure in the ROM.

TODO: describe results and contribution in detail

Should all necessary concepts be explained in detail in "Preliminaries" and new contributions later?

Chapter 2

Preliminaries

TODO: add security definitions and explanations

TODO: define GSD game

TODO: define IND-CPA security

TODO: explain the ROM

Chapter 3

Example Chapter

Dummy text.

3.1 Example Section

Dummy text.

3.1.1 Example Subsection

Dummy text.

Example Subsubsection

Dummy text.

Example Paragraph Dummy text.

Example Subparagraph Dummy text.

Appendix A

Dummy Appendix

You can defer lengthy calculations that would otherwise only interrupt the flow of your thesis to an appendix.

Bibliography

[1] Joël Alwen, Margarita Capretto, Miguel Cueto, Chethan Kamath, Karen Klein, Ilia Markov, Guillermo Pascual-Perez, Krzysztof Pietrzak, Michael Walter, and Michelle Yeo. Keep the dirt: Tainted treekem, adaptively and actively secure continuous group key agreement. Cryptology ePrint Archive, Paper 2019/1489, 2019. https://eprint.iacr.org/2019/1489.

[2] Richard Barnes, Benjamin Beurdouche, Raphael Robert, Jon Millican, Emad Omara, and Katriel Cohn-Gordon. The Messaging Layer Security (MLS) Protocol. RFC 9420, July 2023.

[3] Karthikeyan Bhargavan, Richard Barnes, and Eric Rescorla. TreeKEM: Asynchronous Decentralized Key Management for Large Dynamic Groups A protocol proposal for Messaging Layer Security (MLS). Research report, Inria Paris, May 2018.

[4] Giles Hogben. An important step towards secure and interoperable messaging. https://security.googleblog.com/2023/07/an-important-step-towards-secure-and.html, 2023. Accessed: 2023-11-01.

[5] IETF. Support for mls. https://www.ietf.org/blog/support-for-mls-2023/, 2023. Accessed: 2023-11-01.

[6] Saurabh Panjwani. Tackling adaptive corruptions in multicast encryption protocols. In *Proceedings of the 4th Conference on Theory of Cryptography*, TCC'07, page 21–40, Berlin, Heidelberg, 2007. Springer-Verlag.

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Declaration of originality

The signed declaration of originality is a component of every semester paper, Bachelor's thesis, Master's thesis and any other degree paper undertaken during the course of studies, including the respective electronic versions.

Lecturers may also require a declaration of originality for other written papers compiled for their courses.

I hereby confirm that I am the sole author of the written work here enclosed and that I have compiled it in my own words. Parts excepted are corrections of form and content by the supervisor.

Title of work (in block letters):

Authored by (in block letters):
For papers written by groups the names of all authors are required.

Name(s):	**First name(s):**

With my signature I confirm that

- I have committed none of the forms of plagiarism described in the 'Citation etiquette' information sheet.
- I have documented all methods, data and processes truthfully.
- I have not manipulated any data.
- I have mentioned all persons who were significant facilitators of the work.

I am aware that the work may be screened electronically for plagiarism.

Place, date	**Signature(s)**

For papers written by groups the names of all authors are required. Their signatures collectively guarantee the entire content of the written paper.