Universitat Rovira i Virgili

Cryptography and Information Security

A cryptographically view on the [matrix] communication protocol

Justus Liam Vetter

January 4, 2026

UNIVERSITAT
ROVIRA i VIRGILI

Contents

Chapter 1

Introduction

The following chapter will introduce [matrix] and its implementation of `olm` and `megolm` which goes under the name vodozemac. Furthermnore it will also introduce the former implementation which were known under the name of libolm.
During this short introduction the report will elaborate the basic functionality of the [matrix] protocol as well as the philosphy behind [matrix] in general.

1.1 An introduction to [matrix]

[Matrix] is a open communication protocol with a strong focus on secure and decentralized communication. The Idea behind [matrix] is strongly influenced by the Matrix Manifesto which states that "The ability to converse securely and privately is a basic human right." and that "People should have full control over their own communication.". [1]

1.2 An introduction to libolm and vodozemac

1.3 Limitations and Constraints

Chapter 2

Schemes and Protocols

2.1 olm

2.2 megolm

2.3 Other aspects

Chapter 3

Conclusion and Results

3.1 Further needs for security

3.2 Conclusion

3.3 Outlook

Bibliography

[1] About [matrix] and the [matrix] consortium.
Last Checked: 2026-01-03
Available at: https://matrix.org/foundation/about/