SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

A Study of Non-malleability Definitions on Timed Commitments

Zehua Shang * Mehdi Tibouchi † Masayuki Abe ‡

Keywords: Time-release cryptography, Non-malleability, Timed Commitments

Abstract

Time-release cryptography has seen a recent surge of popularity in the research community, due to their wide array of applications. Timed commitments are one of the central primitives in time-release cryptography. Non-malleable commitment has also been a well studied primitive in cryptography for decades which ensures security in the presence of "man-in-the-middle" attacks. In this paper we conduct a survey on several existing constructions of non-malleable timed commitments, analyzing their security definitions and comparing them in CCA model. We hope this will motivate future research and provide new insights.

* Kyoto University, shang.zehua.23m@st.kyoto-u.ac.jp
† Kyoto University, NTT Secure Platform Laboratories, mehdi.tibouchi.br@hco.ntt.co.jp
‡ Kyoto University, NTT Secure Platform Laboratories, abe.masayuki.7a@kyoto-u.ac.jp