On Security Against Time Traveling Adversaries

Lúcás Críostóir Meier
lucas@cronokirby.com

August 27, 2022

Abstract

In this work, we investigate the notion of time travel, formally defining a model for adversaries equipped with a time machine, and the subsequent consequences on common cryptographic schemes.

1 Introduction

[Mau09]

2 Defining Abstract Games

$G_b(\text{init}, \text{next})$

$s \leftarrow \text{init}()$

$\underline{\mathcal{O}(x):}$
$s, y \leftarrow \text{next}(b, s, x)$
`return` y

Game 1: $G_b(\text{init}, \text{next})$

References

[Mau09] Ueli Maurer. Unifying Zero-Knowledge Proofs of Knowledge. In *AFRICACRYPT 2009*, volume 5580 of *LNCS*, pages 272–286. Springer, Berlin, Heidelberg, 2009.