On Security Against Time Traveling Adversaries

Lúcás Críostóir Meier
lucas@cronokirby.com

December 7, 2022

Abstract

If you had a time machine, what cryptography would you be able to break?

In this work, we investigate the notion of time travel, formally defining models for adversaries equipped with a time machine, and exploring the consequences for cryptography. We find that being able to rewind time breaks some cryptographic schemes, and being able to freely move both forwards and backwards in time breaks even more schemes.

We look at the impacts of time travel on encryption and signatures in particular, finding that the IND-CCA and EUF-CMA security games are broken, while IND-CPA and UUF-CMA remain secure.

1 Introduction

[Mei22]

Definition 1.1 (Adversaries). An adversary is a cool thing.

Theorem 1.1 (Cool Beans). Woah mama

And that's what matters.

■

Lemma 1.2. Woah mama again!

Corollary 1.3. Woah mama again!

1.1 Relevance of Time Travel

IND-CCA
$x \leftarrow 4$

Protocol 1.2: Some Protocol

stuff

Γ^0

$x \leftarrow 3$
if $x + 2$:
  $y \xleftarrow{\$} \mathbb{F}_q$
$m \Rightarrow \langle \mathcal{P}_i, \mathcal{P}_j \rangle$ $\quad y \leftarrow 4$
$m \Leftarrow \langle \mathrm{OT}, \mathcal{P}_i \rangle$ $\quad x \leftarrow 3$

Foo(x, y):
  Bar(x, y)

(1)

Game 1.1: Some Game

IND-CCA
$x \leftarrow 4$

Protocol 1.3: Some Protocol

IND-CCA
$x \leftarrow 3$

Functionality 1.4: Encryption

References

[Mei22] Lúcás Críostóir Meier. MPC for group reconstruction circuits. Cryptology ePrint Archive, Report 2022/821, 2022. https://eprint.iacr.org/2022/821.