Adversarial Cooperation

S. Restrepo Ruiz

August 5, 2024

Contents

1 Introduction **1**
1.1 Section Title 1
1.2 Mathematics 1

2 Hash Functions **3**
2.1 Definition 3
2.2 Security Model 3
2.3 Examples 3

Appendix Title **5**

Chapter 1

Introduction

1.1 Section Title

This is an example of highlighted text using a custom command: **important**.

1.2 Mathematics

Text about vectors and sets: ${}^{b}_{a}\mathcal{C}^{e}_{d}$

- A vector: $\mathbf{v}$ and a set: $\mathcal{S}$.

Theorem 1 *If $a > b$, then $b < a$.*

Chapter 2

Hash Functions

2.1 Definition

Hashes are one-way functions $y = hash(x)$, —used to express x without revealing it.

2.2 Security Model

Hash function should be impossible to invert.

- First pre-Image resistance: Given $hash(\cdot), y$, the adversary knows not an inverse function $x = hash^{-}1(y)$.
- Second pre-Image resistance: Given $hash(\cdot), y, x_1$ where $y = hash(x_1)$, the adversary known not a second value such that $y = hash(x_2)$.
- Collision resistance: Given $hash(\cdot)$, the adversary knows not a pair $x_1 ! = x_2$ where $y = hash(x_1) = hash(x_2)$.
- Avalanche effect: Given $hash(\cdot), x, y$, any change δx, —however small, should produce an unpredictable and chaotic change δy.

2.3 Examples

```
~$ echo -n "Hello, World!" | md5sum
65a8e27d8879283831b664bd8b7f0ad4
```

```
~$ echo -n "ello, World!" | md5sum
d41d8cd98f00b204e9800998ecf8427e
```

Appendix Title

Details relevant to the appendix.