A Graphical Framework for Cryptographic Games

Lúcás Críostóir Meier
lucas@cronokirby.com

2023-08-01

Abstract

Ahoy

1 Introduction

1.1 Outline

2 An Informal Framework

3 A Formal Framework

3.1 Stacks

Definition 3.1: Stacks

A *stack* S consists of:

- a set $O \subseteq [n]$,
- types $T_1, ..., T_n$,
- types $\bullet = \sigma_1, \sigma_2, ..., \sigma_{n+1} = \emptyset$,
- functions $f_1, ..., f_n$, each of which is:
  - of type $f_i : \sigma_i \to \sigma_{i+1} \times T_i$ when $i \in O$,
  - of type $f_i : \sigma_i \times T_i \to \sigma_{i+1}$, when $i \notin O$.

□

Definition 3.2: Games

A *game* G consists of:

- a list of stacks $S_1, ..., S_m$,
- a set W,
- a function $\varphi : \bigsqcup_{i \in [m]} [n_i]^1 \to W$ whose restriction to the set $\bigsqcup_{i \in [m]} O_i$ is injective.

[1] By this, we mean that the domain of φ is the *disjoint* union of the individual index sets.

□

3.2 Diagrams

3.3 Efficient Diagrams

3.4 Randomized Diagrams

4 Some Basic Theory

5 Examples

5.1 Encryption from Pseudorandom Functions

5.2 The KEM-DEM Paradigm

5.3 IND-CPA Secure KEMs from Group Assumptions

6 Further Work

6.1 A Framework for Protocols

6.2 Categorical Structure

6.3 Alternative Interpretations

7 Conclusion