A Graphical Framework for Cryptographic Games

Lúcás Críostóir Meier
lucas@cronokirby.com

2023-07-30

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:

- two disjoint sets (of names): I, and O,
- a bijection $\varphi : [n] \leftrightarrow I \sqcup O$,
- 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 $f_i : \sigma_i \times T_i \to \sigma_{i+1}$, when $\varphi(i) \in I$,
  - and of type $f_i : \sigma_i \to \sigma_{i+1} \times T_i$ when $\varphi(i) \in O$.

□

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