A Graphical Framework for Cryptographic Games

Lúcás Críostóir Meier
lucas@cronokirby.com

2023-08-03

Abstract

Ahoy

1 Introduction

1.1 Outline

2 An Abstract Theory

3 A Concrete Model

3.1 Stacks

Definition 3.1: Stacks

A *stack* S consists of:

- a set $O \subseteq [n]$,
- types $T_1, \ldots, T_n$,
- types $\bullet = \sigma_1, \sigma_2, \ldots, \sigma_{n+1} = \varnothing$,
- functions $f_1, \ldots, f_n$, 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 $S_1, \ldots, S_m$,
- a set W ,
- a function $\varphi : \bigsqcup_{i \in [m]} [n_i]^1 \to W^?$ whose restriction to $\bigsqcup_{i \in [m]} O_i \to W$ is injective.

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

□

Definition 3.3: Literal Game Equality
Two games A, B are said to be *literally equal*, written $A \equiv B$, when $m_A = m_B$, and there exist bijections $\pi : [m] \leftrightarrow [m]$ and $\psi : W_A \leftrightarrow W_B$ such that $\varphi_A(i, x) = \psi(\varphi_B(\pi(i), x))$[2].

□

Definition 3.4: Game Composition
Given two games A , B , and an equivalence relation $\sim$ on $W_A \sqcup W_B$, such that $x = y$ implies $(i, x) \sim (i, y)$, and that

$$\nexists x \in \bigsqcup_i O_{A,i}, y \in \bigsqcup_i O_{B,i}.\ (0, \varphi(x)) \sim (1, \varphi(y))$$

, we can define their composition (relative to this relation) $A \diamond_\sim B$ as a game consisting of:

- the stacks $S_{A,1}, \ldots, S_{A,m_A}, S_{B,1}, \ldots, S_{B,m_B}$,
- the wire set $(W_A \sqcup W_B) / \sim$,
- the function

  $$\varphi(i, x) := \begin{cases} \varphi_A(i, x) & \text{if } i \le m_A \\ \varphi_B(i - m_A, x) & \text{if } i > m_A \end{cases}$$

  .

□

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

[2]Implicitly, $\psi(\bot) := \bot$ here.

6 Further Work

6.1 A Framework for Protocols

6.2 Categorical Structure

6.3 Alternative Interpretations

7 Conclusion