ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Modeling the Ideal Cipher in Linicrypt

Master Thesis

Frederik Semmel

April 22, 2022

Advisors: Fabio Banfi, Ueli Maurer

Institute of Theoretical Computer Science, ETH Zürich

Abstract

Todo

Contents

Chapter 1

Introduction

Chapter 2

Extending Linicrypt to Ideal Ciphers

Let $\mathcal{P}$ be a Linicrypt program. For each query to E of the form $y = E(k, x)$ we define the associated constraint $(E, \boldsymbol{k}, \boldsymbol{x}, \boldsymbol{y})$, where $\boldsymbol{k} \in \mathbb{F}^{\mathsf{base}}$ is the row vector corresponding to $k \in \mathbb{F}$ and similarly for $\boldsymbol{x}$ and $\boldsymbol{y}$. Each query to E^{-1} of the form $x = E^{-1}(k, y)$, is associated with the constraint $(E^{-1}, \boldsymbol{k}, \boldsymbol{y}, \boldsymbol{x})$

To capture the fact that $E(k, x) = y$ should be associated to the same constraint as $E^{-1}(k, y) = x$ for the same k, x and y, we introduce an equivalence relation on the constraints. For all $\boldsymbol{k}, \boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}^{\mathsf{base}}$ we define

$$(E, \boldsymbol{k}, \boldsymbol{x}, \boldsymbol{y}) \sim (E^{-1}, \boldsymbol{k}, \boldsymbol{y}, \boldsymbol{x}).$$

The set of constraints $\mathcal{C}$ corresponding to $\mathcal{P}$ is then a subset of

$$\Big(\{E, E^{-1}\} \times \mathbb{F}^{\mathsf{base}} \times \mathbb{F}^{\mathsf{base}} \times \mathbb{F}^{\mathsf{base}}\Big) \Big/ \sim$$

Todo: Include the idea that no constraint with the "same" input queries are used twice.

Todo: Maybe scrap the idea of the equivalence relation, it seems to hinder more than it helps.

Todo: Instead of doing weird things with equivalence relation in Collision structure definition, explicitly add data of reverse or forward direction.

Definition 2.1 (Collision structure)**.** *Let $\mathcal{P} = (\boldsymbol{M}, \mathcal{C})$ be a Linicrypt program. A **collision structure** is an index i^* and a tuple $(c_1, \ldots, c_n)$ for $c_i = (O_i, \boldsymbol{k}_i, \boldsymbol{q}_i, \boldsymbol{a}_i)$ and $O_i \in \{E, E^{-1}\}$, such that:*

1. *$[c_1], \ldots, [c_n]$ is an ordering of $\mathcal{C}$*
2. *The input or output corresponding to the query c_{i^*} can be fixed arbitrarily:*

$$\mathsf{span}\big(\{\boldsymbol{k}_{i^*}, \boldsymbol{q}_{i^*}\}\big) \nsubseteq \mathsf{span}\big(\{\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{i^*-1}, \boldsymbol{q}_1, \ldots, \boldsymbol{q}_{i^*-1}, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{i^*-1}\} \cup \mathsf{rows}\,(\boldsymbol{M})\big)$$

3. *For all $j \geq i^*$ the constraint c_j does not contradict previous constraints:*

$$\boldsymbol{a}_j \notin \mathsf{span}\big(\{\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{j-1}, \boldsymbol{q}_1, \ldots, \boldsymbol{q}_{j-1}, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{j-1}, \} \cup \{\boldsymbol{k}_j, \boldsymbol{q}_j\} \cup \mathsf{rows}\,(\boldsymbol{M})\big)$$

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Declaration of originality

The signed declaration of originality is a component of every semester paper, Bachelor's thesis, Master's thesis and any other degree paper undertaken during the course of studies, including the respective electronic versions.

Lecturers may also require a declaration of originality for other written papers compiled for their courses.

I hereby confirm that I am the sole author of the written work here enclosed and that I have compiled it in my own words. Parts excepted are corrections of form and content by the supervisor.

Title of work (in block letters):

Authored by (in block letters):
For papers written by groups the names of all authors are required.

Name(s):	**First name(s):**

With my signature I confirm that

- I have committed none of the forms of plagiarism described in the 'Citation etiquette' information sheet.
- I have documented all methods, data and processes truthfully.
- I have not manipulated any data.
- I have mentioned all persons who were significant facilitators of the work.

I am aware that the work may be screened electronically for plagiarism.

Place, date	**Signature(s)**

For papers written by groups the names of all authors are required. Their signatures collectively guarantee the entire content of the written paper.