A Template for Cryptologic Papers

Author 1[1], Author 2[2], and Author 3[3]

[1] Institute 1
a1@iacr.org
[2] Institute 2
a2@iacr.org
[3] Institute 3
a3@iacr.org

Abstract. Convince everyone that your work is exciting and worthwhile for a in-depth read in a single self-contained paragraph.

Keywords: Cryptology · Research · Papers

1 Introduction

Introduction goes here.

2 Technical Overview

Summarize your work so that non-experts can get the main ideas by reading the Introduction and Technical Overview alone. They should be self-contained and within a 10-page limit. The original two-party authenticated garbling paper [1] serves as an example for a good technical overview.

3 Preliminaries

We list the notations of this paper in Section 3.1.

3.1 Notation

We use λ to denote the computational security parameter. We use log to denote logarithms in base 2. We define $[a, b) = \{a, \ldots, b-1\}$ and write $[a, b] = \{a, \ldots, b\}$. We write $x \leftarrow S$ to denote sampling x uniformly at random from a finite set S. We use $\{x_i\}_{i \in S}$ to denote the set that consists of all elements with indices in set S. When the context is clear, we abuse the notation and use $\{x_i\}$ to denote such a set.

We use bold lower-case letters like $\boldsymbol{a}$ for column vectors and bold uppercase letters like $\mathbf{A}$ for matrices. We let a_i denote the i-th component of $\boldsymbol{a}$ (with a_0 the first entry) and $\boldsymbol{a}[i, j]$ denote the sub-vector of $\boldsymbol{a}$ with indices $[i, j]$.

4 The Main Construction

Explain your constructions in detail in this section.

5 Performance Evaluation

Evaluation goes here.

References

1. Wang, X., Ranellucci, S., Katz, J.: Authenticated garbling and efficient maliciously secure two-party computation. In: Thuraisingham, B.M., Evans, D., Malkin, T., Xu, D. (eds.) ACM CCS 2017. pp. 21–37. ACM Press (Oct / Nov 2017). https://doi.org/10.1145/3133956.3134053