The Quantum Random Oracle Toolbox

Hans Heum

NTNU - Norwegian University of Science and Technology, Trondheim, Norway.
hans.heum@ntnu.no

Abstract. The tricks of the trade.

Keywords: Provable Security · Quantum Random Oracles

Table of Contents

1 Introduction

Hans: Idea: Take the basic examples from "Random Oracles Are Practical" [BR93] as motivating examples running through the paper.

In the following and throughout, $\mathcal{H}$ is a random oracle.

1.1 Recording ROs (or, Random Oracles are Good PRFs)

We start with the simplest ROM proof imaginable: showing that random oracles are good pseudorandom functions. Specifically, we will show that $\mathsf{PRF}_k(x) = \mathcal{H}(k||x)$ is indistinguishable from a random function, provided the key k is hard to guess.

We will do this by showing that if an adversary $\mathbb{A}$ can distinguish the output of PRF_k from random, then a reduction $\mathbb{B}$ can recover the key k. Crucially, the reduction does this by *recording* the queries of the adversary $\mathbb{A}$ to the random oracle $\mathcal{H}$.

1.2 Reprogramming ROs (or, Random Oracles yield Simple PKEs)

1.3 Rewinding ROs (or, Random Oracles yield Efficient Signatures)

Experiment $\mathsf{Exp}^{\mathrm{ind}}_{\mathsf{PRF}}(\mathbb{A})$	Oracle $\mathcal{E}(x)$
$k \leftarrow\!\!\$\ \mathcal{K}$	**if** $b^* = 0$:
$b^* \leftarrow\!\!\$\ \{0,1\}$	$\quad y \leftarrow \mathcal{H}(k\|\|x)$
$\hat{b} \leftarrow\!\!\$\ \mathbb{A}^{\mathcal{H},\mathcal{E}}$	**else** :
return $b^* = \hat{b}$	$\quad y \leftarrow \mathcal{R}(x)$
	return y

Fig. 1. The pseudorandomness indistinguishability game.

Experiment $\mathsf{Exp}^{\mathrm{ku}}_{\mathsf{PRF}}(\mathbb{B})$	Oracle $\mathcal{E}(x)$
$k \leftarrow\!\!\$\ \mathcal{K}$	$y \leftarrow \mathcal{H}(k\|\|x)$
$\hat{k} \leftarrow\!\!\$\ \mathbb{B}^{\mathcal{H},\mathcal{E}}$	**return** y
return $k = \hat{k}$	

Fig. 2. The pseudorandomness key recovery game.

Reduction $\mathbb{B}^{\mathcal{H}}$	Oracle $\mathcal{E}(x)$
$\hat{b} \leftarrow\!\!\$\ \mathbb{A}^{\mathcal{H},\mathcal{E}}$	$y \leftarrow \mathcal{H}(k\|\|x)$
return $\hat{k}$	**return** y

Fig. 3. The pseudorandomness key recovery game.

References

BR93. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, November 1993.