

Contents

1 Introduction

1.1 Security Amplification Theorems

Why security amplification is interesting topic in cryptography. Examples of the classical results – a weak one way function implying the strong ones. Hardness implication statements. Problems captured by weakly verifiable puzzles. Contribution of this thesis.

1.2 Organization of the Thesis

Overview of the content of the following chapters.

2 Preliminaries

2.1 Notation

Set up notation and terminology used in the Thesis.

2.2 Pairwise independent family of hash functions

Define efficient pairwise independent family of hash functions.

2.3 Oracle machines

Describe the way in which algorithms access the oracle, and the oracle queries are answered.

3 Weakly Verifiable Cryptographic Primitives

3.1 Weakly Verifiable Puzzles

Give a definition of dynamic, interactive weakly verifiable puzzles.

3.2 Examples

3.2.1 Message Authentication Codes

3.2.2 Public Key Encryption

3.2.3 Bit Commitments

3.2.4 CAPTACHs

3.3 Previous results

Give an overview of the previous works considering WVP. Present the approach of the authors, the contribution of the paper, give a sketch of the proof (e.g. the algorithm without the formal proof).

3.3.1 Results of R.Canetti, S.Halevi, and M.Steiner

3.3.2 Results of Y.Dodis, R.Impagliazzo, R.Jaiswal, V.Kabanets

3.3.3 Results of T.Holenstein and G.Scheonebeck

4 Security amplification for dynamic weakly verifiable puzzles

In this chapter I present my main result.

4.1 Main theorem

4.1.1 The k -wise direct product of weakly verifiable puzzle

4.1.2 Intuition

4.1.3 Domain partitioning

4.1.4 Amplification proof for the partitioned domain

4.1.5 Putting it together

4.2 Discussion

Discuss optimality of the result.