T-79.511 Special Course on Cryptology / Review of Vesa Vaskelainen's *Private Information Retrieval* survey

Xavier RONDE-OUSTAU

November 5, 2003

Overview

This paper is the review of a survey on Private Information Retrieval, written by Vesa Vaskelainen. This survey is mainly based on papers written by Y. Gertner et al. *Protecting Data Privacy in Private Information Retrieval Schemes* and by I. Kerenidis and R. de Wolf *Quantum Symmetrically-Private Information Retrieval*

The information given are quite complete, but the complex notation used makes difficult to understand how the systems practically work. Some schemas would have been very helpfull, at least for some non-initiated readers like me.

Some part of the surveys have been directly copied from the original papers.

Abstract

The word "writen" should be spelled "written".

1 Introduction

The sentence in the second paragraph "That is, every..." is not clear and could be rewritten as "This means that, in addition to maintaining the privacy of the user, every invocation of SPIT prevents the user..."

2 Notations and Definitions

Second line: "throughout" requires an attribute like "throughout this survey".
"denote" should be written "denotes".
There is a section "2.1" but no section "2.2".

3 The PIR schemes

The relation between the index bits $i_1 \ldots i_d$ and the final x_i is not clear, both in 3.1 and 3.2.

4 The SPIR Schemes

The first sentence needs to be rewritten, for example "In this section, it will be first shown that..."
Same paragraph: "a k-database".
In 4.2, I don't see what this function f is about, neither its use in the PSM.
Last lines of 4.2: "shown" instead of "showed" and there is a "e" missing for "schemes".
4.3: "there exsits" instead of "there exist".
At the end of the paragraph 4.3, "Intereterested reader is referred to read [3] more about proofs." should be rewritten as follows: "A reader interested in knowing more about proofs is advised to read [3]".
4.4 rewrite the introductory sentence in "The previous section delt with the SPIR scheme...".

5 Quantum Results

What is a and what is t? this is not explained in the survey. More generally, the notations are not introduced very well, it is difficult to see what they actually refer to.

line 16 of 5.1: "The user defines ... and sets up"
All the allusions to the "phase" should have been explained before, with the braket notations.
There is a section 5.1 and no section 5.2.

6 Conclusion

line 2: should be "transform into".