T-79.511 Special Course on Cryptology / Zero Knowledge: Comments on "Statistical Difference is Complete for Honest-Verifier Statistical Zero Knowledge"

Johan Wallén

December 12, 2001

1 Introduction

In this document, we give some brief comments on Petteri Kaski's survey *Statistical difference is complete for honest-verifier statistical zero knowledge*. The main objective of the survey was to sketch a **HVSZK**-completeness proof of STATISTICAL DIFFERENCE (actually the survey only discusses the hardness part of the proof, since a HVSZK proof system for STATISTICAL DIFFERENCE was presented in a previous survey).

2 General

The main strength of the survey is that it makes the intuition behind the proof very clear. Especially Section 2 (Informal ideas) is good. After reading the survey, the reader has a clear picture of the ideas behind the elegant reduction, and gets a good intuition of why the result holds. The technical details of the reduction are also clarified nicely.

The survey is (due to lack of time) not as polished as some of the previous ones, and the technical parts of some proofs contain minor mistakes. The errors in the proofs are, however, not a major problem, since a careful reader easily can spot and correct them while reading. The technical parts of the proofs are further discussed in the next section.

As usual, the survey is very readable. It would, however, be nice to include a definition of statistical difference, for example, when the $\Delta(X, Y)$-notation is defined. This would make the survey almost independent from the previous survey on statistical zero knowledge.

3 Specific comments

3.1 The proofs

Lemma 3.1 Parenthesis are missing from the last summation.

Lemma 3.3 The last equality in the proof should be an inequality.

Lemma 4.1 The distributions X_i and Y_i have accidentally been swapped throughout the proof.

Lemma 4.2 The third displayed equation should be an inequality, that is

$$\Delta(\langle P_S, V\rangle_{2j+1}, S_{2j+1}) = \Delta(\langle P_S, V\rangle_{2j}, S_{2j})$$

should be

$$\Delta(\langle P_S, V\rangle_{2j+1}, S_{2j+1}) \leq \Delta(\langle P_S, V\rangle_{2j}, S_{2j}).$$

The same mistake also appears in the last displayed equation, and in the first row after the last displayed equation (if the equality indeed is an equality, this would need further explanation).

The bounds A "2" is missing from the bound for NO instances just after Lemma 4.5. The bound should be

$$\Delta(X, Y) \geq 1 - 2\exp\left(-\frac{4(12v)^2(1/12v)^2}{2}\right),$$

which is still greater than 2/3, so the typo does not affect the result.

3.2 Other comments

The bibliography The reference "[3]" is not (?) referred to in the text. In general, BibTeX is a highly recommended tool for managing bibliographies.