Resume on Lauri Tarkkala's Report

Oleg Mürk

In this short resume I will give my comments on Lauri Tarkkala's report about the article by Bellare-Impagliazzo and Lucks "A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP $\rightarrow$ PRF conversion".

In general Lauri has done a good work deciphering above mentioned article and presenting it in a comprehensible form. As I have not found any major faults (and didn't quite (bother to) understand the original article) I shall devote the rest of this writing to whining about the details.

- Spelling-checking could be of use.
- End of the first paragraph of Section 1: "expected time required to distinguish PRP from PRF is $2^{n/2}$ instead of 2^n" - 2^n for what? In general, one is interested in the advantage of distinguishing between PRP and RF, not expected time.
- Beginning of Section 2 - it would be nice to include a definition of statistical difference.
- Definition 2.1 - the first sentence after the definition is not very legible.
- Definition 2.2 - parenthesis problems.
- Definition 2.4 - parenthesis problems. Expression $\{1, q\}$ should be replaced with $\{2, \ldots, q\}$.
- Lemma 2.5 - what is a continuous probability distribution over R^q (and why)? It would be nice to pay more attention to formatting formulas so that they at least fit into column bounds. In this particular case \frac command could be of use.

- Section 3 - it would be nice to describe also general sum construction and not only it's modification that uses single key.

- Theorem 3.1 (and others) - I think it would be nice to keep preliminary definitions and comments out of the theorem environment.

- Figure - I would suggest making it 3x smaller. Also, it is not very nice to display page number 4 within the figure. I didn't quite understand why the domain of the functions $s(), t1(), t2(), t3()$ is (at least) $[0 \ldots 25]$. Further, I would suggest renaming functions $t1(), t2(), t3()$ so that a monotonic sequence would be formed: $t1 \leftrightarrow t2$.

- It would be interesting to know how author plotted graphs of functions that contain asymptotic terms $O(\ldots)$ - i.e. which constants were used and why?

- And a general comment: why all bounds for $InSec$ contain asymptotic terms $O(\ldots)$ when we are dealing with practical security? It's not the author's fault, of course.