Errata for the BLACR Protocol

Errata

1. As Wang et al. [1] point out, the express pass $\mathtt{tk}_{\mathtt{pd}}$ does not contain information to link it to time period $\mathtt{pd}$. Consequently, it is possible for a malicious user to re-use an express pass obtained from period $\mathtt{pd}$ to make an authentication in period, say, $\mathtt{pd} + 3$ and thus skip all the misbehavior that might have been caught during period $\mathtt{pd} + 1$.

   The fix is rather straightforward, namely, to put the period information $\mathtt{pd}$ in the express pass $\mathtt{tk}_{\mathtt{pd}}$. In the express lane authentication at period $\mathtt{pd}$, the service provider will accept an express pass issued in the period $\mathtt{pd} - 1$. This fix has also been discussed by Wang et al. [1].

References

[1] W. Wang, D. Feng, Y. Qin, J. Shao, L. Xi, and X. Chu. ExBLACR: Extending BLACR system. In W. Susilo and Y. Mu, editors, *ACISP*, volume 8544 of *Lecture Notes in Computer Science*, pages 397–412. Springer, 2014.