Errata for the BLACR Protocol

Errata

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

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

References