Progress report

Yin-Hong, Hsu

07 27, 2017

Outline

Debug the experiment for proposed solution

In Verify function

- The output of Sign function M, N is not equal to the variable M’ and N’ in Verify function
- The description for these function are fuzzy so that I’m not sure the correct way to implement
  - $h_k = H_1(m||M||N||R_1||\rho||U_k)$
  - $\mu_0 = H_0(0||r_0||m||ring)$

Solution

- As the description on paper, the Verify function is run on the AS side
- So that it's can be removed from UE side program