Notations for All Documents in this Project

Sammy

2017-09-22

Belows are some notations to ease descriptions in all other documents within the this project

- $H_s(\cdot)$: a hashing algorithm that returns a scalar (i.e., the hash output is interpreted as an integer and reduced modulo l, where l is the order of EC in the context)
- $H_p(\cdot)$: a hashing algorithm that returns a point on the EC for a given point on EC
- $x \in_u R$: generate/select a uniformly random scalar