用户和每一个RP分别在IdP处有长期不变的ID，分别称为ID\_U和ID\_RP

**用户在每一个RP处都有长期不变的Account**

在每一次identity proof产生的过程中（也就是每一次log in rp），IdP会产生绑定了ID\_U和ID\_RP的identity proof。

in this paper, we propose xxxx；如图所示。

具体的，在我们的方案，，Account和ID\_U不同；同时，在每一次identity proof 产生的过程之中，

RP都会在IdP处动态地注册匿名ID，称为PID\_RP；同时，IdP会根据PID\_RP和IDU产生PID-U，并将PID\_RP和PID-U绑定在identity proof中；当RP验证了identity proof之后，会利用PID\_RP生成过程中存在的trapdoor得到不变的account。

(1) xxx

(2) xxx

相比PPID，我们是……

相比SPRESSSO，我们是……

相比BrowserID，他们是将binding的操作，由IdP和用户合作2个步骤完成，使得ID\_RP不泄露给IdP。用户的标识并没有什么变化