# TDP配对算法过程解释

1. **前提：基于椭圆曲线上的离散对数数学难题**

TDP配对过程的安全性由椭圆曲线上的离散对数数学难题保证，问题表述为：

***ECDHP：****设G1为椭圆曲线Fq上的循环加法群，其中P为基点，q为阶：*

*给定P，aP，bP，其中a、b为比q小的正整数，不能计算出abP的值。*

在TDP的设计中，我们认为ECDHP是不可解的。

1. **配对过程**

**设备注册**

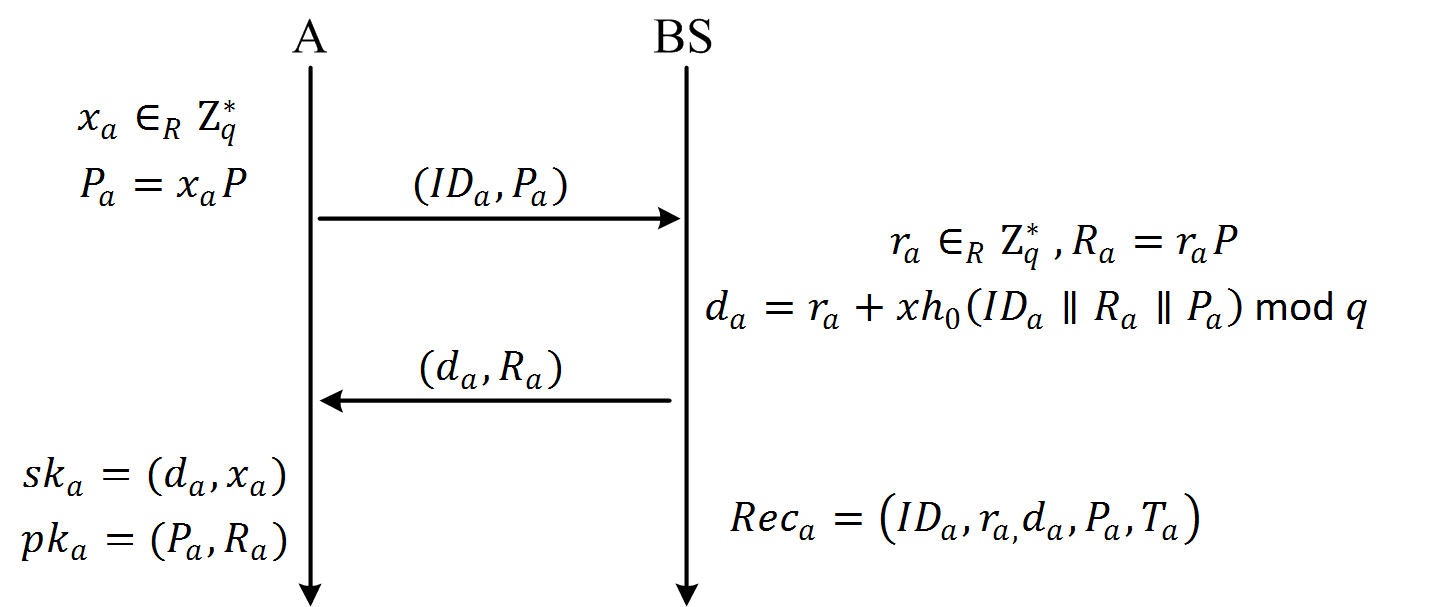


图1 设备注册过程

设备注册在参与设备A和后台服务器BS之间展开，设备通过安装群智应用获得椭圆曲线参数，之后：

1. A在本地选取小于q的随机正整数xa作为其本地部分私钥，并计算点Pa=xaP作为其本地部分公钥；
2. A将自身IDa与本地部分公钥Pa提交给BS；
3. BS收到注册请求后，在本地选取小于q的随机正整数ra，并计算点Ra=raP作为A的可认证补全公钥，之后利用BS持有的主私钥x、收到的IDa、Pa、以及本地确定的ra、Ra，计算da作为A的可认证补全私钥；
4. BS将da、Ra返回给A；
5. A将（da,xa）作为完整私钥、（Pa,Ra）作为完整公钥；同时BS在其本地建立A的存档Reca。

**设备配对**

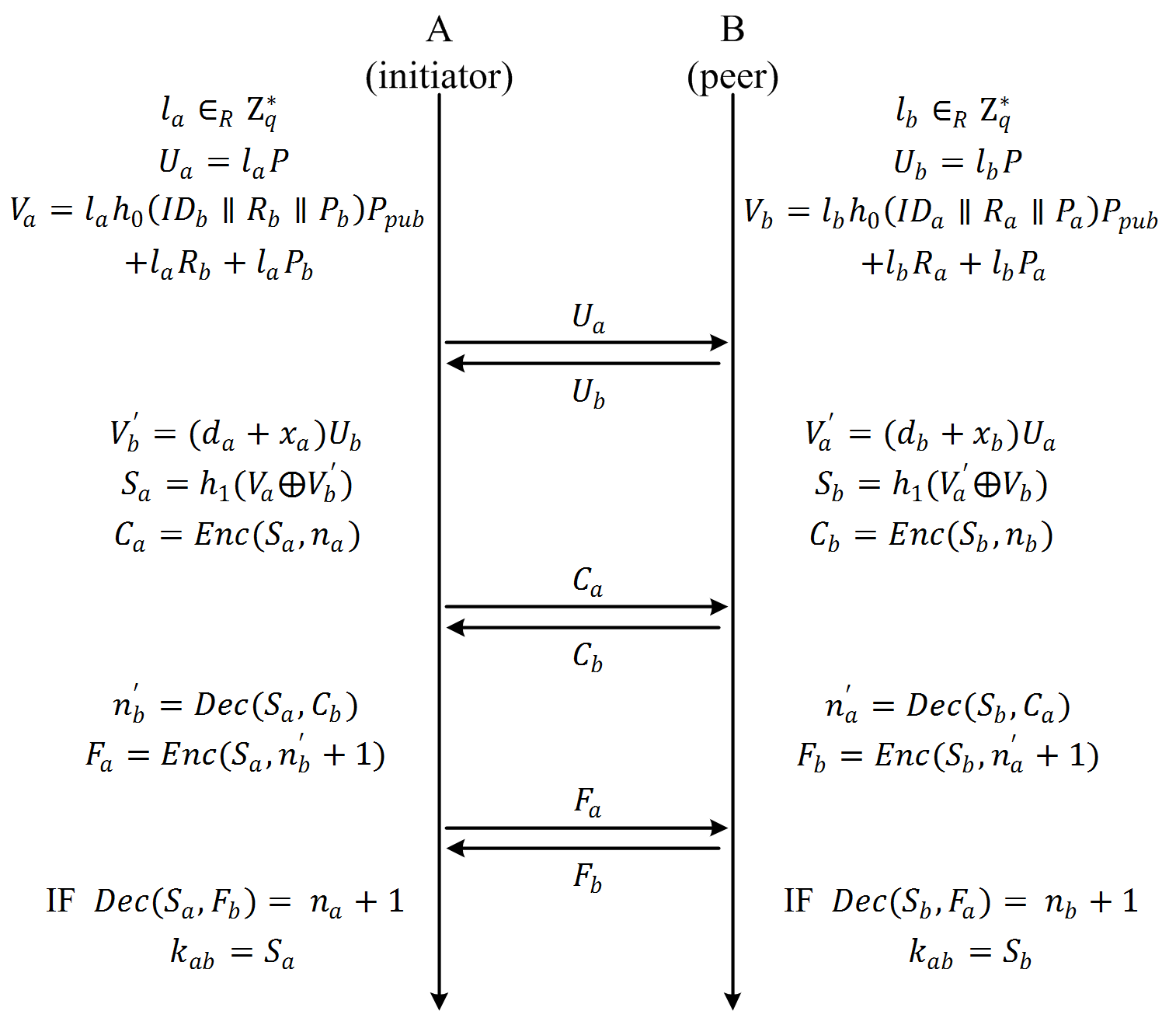


图2 设备配对过程

设备配对过程在机会主义相遇的设备A和B之间展开，由于A与B操作相同，下以A为例。确定需要进行D2D连接之后，

1. A在本地选取小于q的随机正整数la，并计算点Ua；
2. A根据la、B的公开信息（）和主公钥Ppub计算共享密钥协商材料Va；
3. A与B交换Ua和Ub；
4. A根据自己的私钥和Ub重建Vb；（把注册过程里d的定义带进去，U化成整数和基点的点乘，基点可以按分配率乘到括号里面去，乘出来展开就是Vb）

注：因为ECDHP，由Ub不能得到lb，而且Vb的计算使用了A在BS注册过的公开信息，因此只有持有A的相应私钥的设备能够通过图中方法重建Vb，保证了配对的安全性和可认证性。

1. A和B发起挑战应答操作，进行共享密钥认证。

# 实验总体内容：

在自动建立BLE/WiFi Direct连接的前提下，基于Android实现手机端的Trustworthy Device Pairing(TDP) app。

# TDP解决的问题：

1. 参与设备（Android手机）的注册：在安装TDP app之后，参与设备与后台服务器（PC端）基于Internet通信进行设备注册，协商配对凭据（公私密钥对）；
2. 参与设备配对：注册过的两个参与设备之间，根据配对凭据，依据已经建立的非安全BLE/WiFi Direct连接，协商共享秘密作为此次D2D会话密钥；
3. 设备可信度管理：在实现设备配对的前提下，根据每次D2D会话情况，由参与设备对此次会话设备（peer device，D2D会话的另一端）进行评价，产生D2D会话回执并向会话设备返回回执，收到回执的设备对回执有效性进行验证并保存回执，之后向后台服务器通过Internet连接返回有效回执，后台服务器验证有效性并进行设备可信度调整，对新的可信度进行签名并返回给被调整的设备。

# 初步实验目标

1. 实现设备注册：在PC端实现后台服务器BS，进行密钥系统的初始化（确定public parameters），为了实现简便，可以在BS端和参与设备中直接预置固定的public parameters，之后二者根据预置信息协商配对凭据（参与设备与BS协同生成的公私密钥对（sk，pk））；
2. 实现设备配对：对于两个已经获得配对凭据的参与设备，在已经自动建立非安全D2D连接的前提下，根据双方的配对凭据协商共享秘密作为D2D会话密钥。

# 技术细节

TDP app的实现基于JAVA，其中所使用的密码学操作原语来自Bouncy Castle Crypto API（https://www.bouncycastle.org/），主要使用ECC（椭圆曲线加密）原语和AES原语。

ECC为非对称密钥算法，即为实体分配的密钥由公钥（public key）和私钥（private key）组成，公钥可以公开，用来加密；私钥用来解密，需要保密。

AES为对称加密算法，即为实体分配的密钥只有单一的对称密钥，加密解密使用同一密钥。

关于ECC和AES的初步介绍如下：

ECC：<http://www.pediy.com/kssd/pediy06/pediy6014.htm>

AES：<https://en.wikipedia.org/wiki/Advanced_Encryption_Standard>

重点研究ECC过程，实验中需要实现的主要操作有：椭圆曲线初始化（包括确定椭圆曲线参数和确定生成元）和椭圆曲线上的点乘操作。