# MPC triples provide

## 需求描述

1. 两方场景，提供`A\*B=C`

2. 支持同时服务多个应用

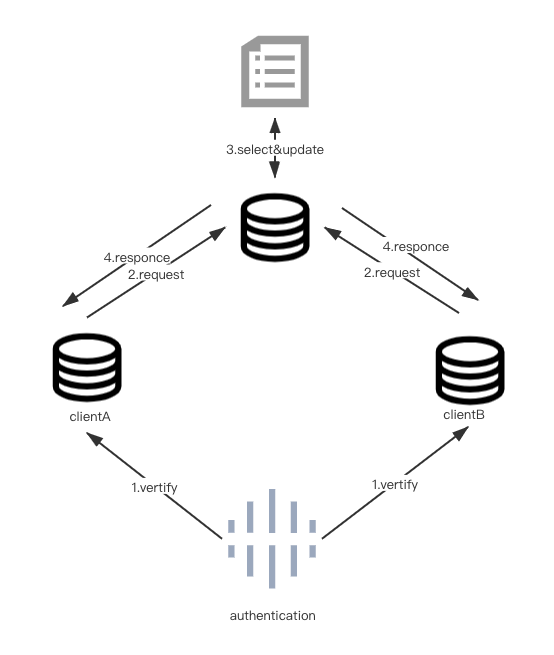
3. 提供int64的triple, 满足 (a1+a2) \* (b1+b2) = (c1+c2)

4. 提供bit的triple, 满足 (a1^a2) & (b1^b2) = (c1^c2)

5. 提供binary的triple, 参数为数据长度length, 满足 (a1^a2) & (b1^b2) = (c1^c2)

6. 服务通过grpc提供

## 需求方案



1. \*~~验证模块~~

技术方案1：使用 Google 的[iOS 登陆类库](https://developers.google.com/identity/sign-in/ios/)的 OAuth2 工作流代表用户发起身份验证 API 调用。

参考：<http://doc.oschina.net/grpc?t=61535>

技术方案2:基于 CA 证书的 SSL/TLS 认证方式

技术方案3: 使用golang实现用户登录注册模块(beego框架和beedb框架,数据库连接)，进行信息验证。

参考：https://www.cnblogs.com/rickiyang/p/14981374.html

2-4:创建grpc客户端和服务器服务并启动

Step1:从 .proto 的服务定义中生成 gRPC 客户端和服务器端的接口

Step2: 通过routeGuideServer服务方法，服务器端从客户端拿到request信息（主要为客户端本身Group，Role），然后连接数据库进行角色验证及triple生成。返回给客户端。

参考链接：<http://doc.oschina.net/grpc?t=60133#client>

Step3：搭建维护数据库和进行交互，具体参考生产环境及交互速度。