可监管idmxier改进方案

1. 可监管id mixer方案简介

可监管idmixer方案在原idmixer方案的基础上结合群签名方案实现了用户身份监管的功能，通过CA对用户的身份进行强制性监管。方案参与方包括CA，用户和验证者，系统建立后，CA产生发行密钥对，追踪密钥以及群公钥。然后用户进行注册，CA为其分配一对私钥，同时CA根据用户提交的属性信息为用户颁发相关的证书。在用户出示证书时，验证者可指定用户证书上需要出示的属性，用户对证书进行签名，同时隐藏无需出示的属性值。验证者可对签名进行验证，若签名通过验证，则用户出示的证书有效，否则，用户出示的证书无效。

一个完整的可监管idmixer方案包含以下过程：

1. 生成发行方密钥对

输入安全参数，输出CA（发行方）的密钥对。发行方密钥对用户生成和验证用户的证书。

1. 生成群密钥

输入安全参数，输出追踪密钥和群公钥。追踪密钥由CA保存，用于从匿名证书中追踪用户的身份，群公钥用于出示和验证证书。

1. 用户注册

输入CA的私钥，输出用户私钥。用户私钥用于出示证书，CA也保存用户的私钥，在身份追踪时会将计算结果与用户的私钥比对进而确定用户身份。

1. 证书请求

输入用户秘密值和CA发送给用户的随机数，输出证书请求。用户将证书请求和属性值发送给CA，CA先对请求进行验证，若验证通过，则生成证书；否则，拒绝用户的请求。

1. 生成证书

输入CA的密钥对，证书请求，用户属性值，输出用户的证书。CA将证书发送给用户，用户进行验证，若通过验证，则证书有效，用户在本地存储证书；否则，证书无效。

1. 出示证书

输入用户私钥，用户秘密值，发行方公钥，群公钥，属性值，用户证书，输出一个签名。在出示证书时，验证者可指定用户需要出示的属性值，签名只暴漏需要出示的属性值，用户可在证书上对无需出示的属性值进行隐藏。然后验证者对签名进行验证，若通过验证，则出示的证书有效，否则出示的证书无效。

1. 身份追踪

输入出示的证书，CA的追踪密钥，输出匿名证书所对应的用户的私钥，CA将私钥和群内用户的私钥进行比对，从而追踪到用户的真实身份。

可监管的idmixer方案应满足不可伪造性、匿名性、无关联性、可追踪性等安全性质。

1. 可监管idmixer改进方案构造

可监管idmixer改进方案中主要利用到原idmixer方案和Dan Boneh 等人的“short group signatures”群签名方案。方案构造如下：

设，，为阶数为的循环群，为阶数为的整数群，为群的生成元，为群的生成元，存在可计算的双线性对，满足：

1. 双线性。对于任意，任意整数，都有。
2. 非退化性。。

方案包括以下步骤：

1. 生成发行方密钥对

选择随机整数，令发行方私钥，计算，设置属性名列表为，其长度为，CA通过属性名列表定义属性结构。

随机选择整数，计算一组长度为的随机数，然后随机选择整数，计算, , , 。

然后计算关于发行方私钥的零知识证明(Fiat-Shamir方案)

*ISK*:

,

,

.

}

最后输出发行方密钥对，

,

.

任何人可验证发行方密钥是否正确（验证零知识证明）：

首先计算

,

,

,

然后判断是否成立。

若公式成立，则发行方密钥正确，否则发行方密钥不正确。

1. 生成群密钥

随机选择整数，令，，，有CA设置群追踪密钥为，群公钥为。

1. 用户注册

对于用户，CA随机选择整数，计算，则用户的私钥为，同时CA将用户的私钥和对应的身份存储到一个表中。

1. 证书请求

用户选择一个随机整数作为自己的秘密值，然后随机选择整数，计算假名（可视为私钥的承诺），然后计算关于秘密值和随机数的零知识证明

:

, 其中和为随机整数。

，

其中为CA发送给用户的随机数

，

.

}

输出证书请求。

CA可验证证书请求是否正确（验证零知识证明）：

首先计算

，

，

，

然后判断是否成立。

若公式成立，则用户证书请求正确，否则用户证书请求不正确。

1. 生成证书（BBS+签名方案）

CA选择随机整数，然后计算。设用户提交的属性值为，则CA先计算，然后计算签名，最后得到证书，证书中包含一个签名，产生签名的随机数以及用户的属性值。

1. 出示证书（证书验证）

用户在交易时，需要出示证书，验证者可指定需要出示的属性值，用户对需要隐藏的属性值的下标进行标记，*HiddenIndices*=[]，其中为需要隐藏属性值的下标。用户先随机选择一个整数，计算一个新的假名，然后随机选择整数，对证书中的签名随机化，计算，，，。用户随机选择整数，计算两个辅助值，然后计算关于用户私钥，秘密值和随机数的零知识证明：

:

随机选择整数，设为一组随机整数，计算

，，

，

，

随机选择整数，计算

，

，，

，

， ，

设签名的消息为，用户产生一个随机数，然后计算

*,*

，

，

，

，

，

，

，

，

，

，

，

，

对于隐藏的属性值集合，计算

，

}

最终，用户出示的匿名证书（签名）为

。

验证者可对签名进行验证，首先计算双线性对,，若，则签名格式正确，然后验证零知识证明，计算

，，

，

，

需要出示的属性值下标集合记为，计算

，

，

，

，，

，

，

*,*

,

最后判断是否成立。

若公式成立，则用户出示的证书有效，否则用户出示的证书无效。

1. 身份追踪

若出现争端，验证者可将用户出示的证书发送给发行方或CA，请求仲裁。CA利用追踪密钥进行解密，计算

，

然后查找对比用户私钥的列表，最终追踪到用户的身份。

1. 效率分析

选择椭圆曲线上的群，阶数设为170bit的大整数，群内元素长度为171bit，（中离散对数的难度相当于普通1024bit整数群中离散对数的难度），大整数长度设为170bit，内元素长度为171bit。

改进后idmxier方案运行效率分析如表1所示，其中E为指数运算，H为哈希运算，P为双线性对运算，k为全部属性个数，为隐藏属性个数。

表 1 改进后idmixer方案运行效率

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 生成发行方密钥 | 生成群公钥 | 用户注册 | 证书请求 | 生成证书 |
| (11+k)E+2H | 3E | E | 5E+2H | (k+2)E |
| 出示证书 | 身份追踪 |  |  |  |
| ((k+)+48)E+4H+10P | 2E |  |  |  |

占用资源如表2所示。

表 2 改进后idmixer方案占用资源（单位：bit）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 发行方公钥 | 发行方私钥 | 用户私钥 | 追踪密钥 | 群公钥 |
| (5+k)171+340 | 170 | 513 | 340 | 513 |
| 证书请求 | 证书 | 出示证书 |  |  |
| 851 | 682 | 3407+170 |  |  |

改进后idmixer方案和原idmixer方案、SM2方案、ECDSA方案比较如表3所示。

表 3 改进后idmixer方案和几种方案的比较

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 改进后idmixer方案 | | | | | Idmxier方案 | | | SM2  方案 | ECDSA方案 |
| 生成密钥时间 | 发行方 | 群密钥 | | 用户注册 | (11+k)E+2H | | | E | | E |
| (11+k)E+2H | 3E | | E |
| 出示证书时间 | (+26)E+2H+3P  或26E+2H+3P(预计算) | | | | | (+14)E+2H或14E+2H(预计算) | | | E+2H | E+H |
| 验证证书时间 | (22+k)E+2H+7P  或(22+k-)E+2H+4P  (预计算) | | | | | (10+k)E+2H+2P或  (10+k-)E+2H+2P  (预计算) | | | 2E+H | 2E+H |
| 私钥长度(bit) | 发行方 | | 用户 | | | 发行方 | 用户 | 170 | | 170 |
| 510 | | 513 | | | 170 | 170 |
| 公钥长度(bit) | (5+k)171+853 | | | | | (5+k)171+340 | | | 171 | 171 |
| 签名长度(bit) | 3407+170 | | | | | 2044+170 | | | 340 | 340 |

改进后方案可通过预计算的方式提高运行效率，如，等计算可提前进行。在进行预计算后，方案可减少5次双线性对运算，次指数运算，但需增加bit存储量,其中为属性个数。

1. 功能分析
2. 可监管

相比原idmixer方案，增加了可监管的功能，CA可以为群内用户分配密钥，并通过追踪密钥追踪用户的身份，改进方案在原来用户出示证书的部分增加了群签名方案中的零知识证明技术，验证者在验证证书的同时也验证了用户匿名身份信息的正确性，如果出现争端，CA可追踪到用户的身份，因此改进的方案具有强制监管的作用。

1. 匿名性

改进方案在增加强制监管功能的同时还保证了用户的匿名性，相比一般身份监管方案，极大保护了用户的身份隐私。同时，用户在交易时，只需出示相应的属性值，对无需出示的属性值可以在证书中进行隐藏，符合用户的隐私保护需求。