安全电子投票系统

郭灿林

2023 年 4 月 13 日

目录

1 符号说明

表 1: 符号说明

符号	表示含义
V	投票者
A	管理中心
C	计票中心
ID	投票者的用户名
IDC	随机生成的申诉标识
pk_x	x 持有的公钥
sk_x	x 持有的私钥
$Cert(x)$	x 持有的证书
N_A	A 生成的 RSA 大整数，用于 RSA 盲签名
$Enc_{pk}(m)$	对消息 m 公钥加密，密钥为公钥 pk，默认 RSA 算法
$Sig_{sk}(m)$	对消息 m 数字签名，密钥为私钥 sk，默认 RSA 算法
$Vrfy_{pk}(m)$	对消息验证签名，密钥为公钥 pk，默认 RSA 算法
$Hash(m)$	对消息 m 散列变化，默认 SHA-512 算法
$f(v_i, k_i)$	对消息 v_i 位比特承诺方案，密钥为第二个参数 k_i，默认 AES 算法

2 电子投票系统设计与分析

2.1 假设与前提

1. 本协议是基于 FOO 投票协议做的改进。主要借鉴了 FOO 投票协议中的盲签名使用，在此基础上完善了匿名性和可验证性，而且新增了无收据性、弃权性，以及证书的使用和部分消息的加密，防止投票过程中的中间人攻击。

2. 本协议假定 ID 和 $Cert$ 为投票者实际的个人信息，因此如果泄露这两者并且能将其与明文的投票结果对应上，就视为不安全，即不满足匿名性。因此以下的设计会围绕如何避开这样的问题展开。

3. 本协议的实现由三方共同完成，分别为投票者 V、管理中心 A 和计票

中心 T，管理中心 A 主要是来认证投票者的，其拥有合法参与投票的用户的 ID 和相关个人信息，计票中心 T 只是负责把得到的票进行统计并且公示，以及对投票者 V 身份的鉴定。

4. 本协议分为四个阶段，分别为注册阶段、投票阶段、计票阶段和公示阶段。

5. 任何需要使用公钥验证签名或者进行加密的步骤中，我们都加上了证书 $Cert$ 的使用，依靠颁布证书的可信第三方来防止中间人伪造公钥，保证了公钥的正确性。在发送一次公钥及其证书后，后续相同路径的传输就不必加上该信息了，默认其能将该信息存在本地。

6. 使用签名保证了消息的认证性，进行签名前对消息进行哈希，提高签名效率。

2.2 注册阶段分析

1. 该阶段分为两步，分别为获取 ID、IDC 和盲签名。

2. 我们做的是将投票者的个人信息和投票结果割裂开来，使得管理中心和计票中心都无法将两者联系起来，尽管他们都持有投票者的部分信息。对于 A，V 使用盲签名让持有用户个人信息的 A 进行签名，以此作为 V 的合法认证，而利用盲签名的特点，可以让 A 在不知道 V 的投票结果的情况下进行签名，尽管 A 知道 V 是谁。对于 T，它可以验证 V 从 A 那里获得的签名是否合法，以此判断是否接受它的投票，但是 T 不能知道该投票结果对应的 ID。

3. 为了让 V 知道有投票者在 A 处完成注册，但是又不能让 V 知道其 ID，因此我们设计了在 A 完成签名后，同时向 T 发送 ID 的哈希值，以此隐去投票者的信息，又可以让计票中心知道有投票者完成注册了，防止投票者用多个 IDC 进行多次投票。

4. 之所以 A 发送 ID 前要对 ID 使用 V 的公钥进行加密，是为了防止中间人窃听到 ID 后泄露了投票者的投票结果。因此需要加密，使用 V 的公钥使得只有 V 可以解开该密文得到 ID，因为只有一次传输，所以没有先协商密钥之后再使用对称密码。

5. 盲签名之前使用了位比特承诺方案对投票内容进行加密，一方面是为了防止传输过程中有中间人窃听，另外也是为了让 T 在投票阶段结束前不能看到该结果，根据位比特承诺的特点，在计票阶段 V 可以把密钥发送给 T 进行解密，从而可以完成计票。

6. A 公布 ID 的哈希值及其对应签名可以让 T 知道该哈希值对应的用户完成了签名，公布并不影响系统安全性。

7. 该阶段完成后，V 在 A 处完成了注册，获得了 ID，并且获得 T 生成的 IDC，此时 A 持有 V 的公钥和证书，T 持有 A 的公钥和证书，V 持有 T 和 A 的公钥和证书。

2.3 投票阶段分析

1. 在 FOO 投票协议中，该阶段 V 发送给 T 只是粗略地用 “匿名地发送” 来实现匿名性，这里由于我们设计的 IDC，T 此时是不知道 V 的 ID 的，也即 T 只能知道 IDC 和对应的加密投票内容，而 IDC 和 ID 并没有关系，因此这样就是匿名的了。并且此处 T 是可以去 A 公布的消息中验证该 IDC 对应的 ID 哈希值是否在公布的消息中，以确认 V 确实完成了签名。

2.4 计票阶段分析

1. 该阶段利用了随机数 (u, v)，是为了实现无收据性，具体分析见后述安全性分析。并且 T 公布处理后的加密结果，是为了 V 可以验证自己的投票结果。注意只有 V 自己知道哪个 IDC 是自己的，因此公布并不影响安全性。

2. 到该阶段 k 不必隐藏了，此时 T 已经可以知道投票结果了，尽管如此，T 也无法将投票结果与 V 的 ID 对应起来。

3 电子投票系统协议

3.1 注册阶段

该阶段完成 V 的注册登记工作，注册登记由 V 提出申请，由 A 和 T 共同完成。具体的过程为：

3.1.1 获取 ID、IDC

(1) V 向 A 提出申请，发送自己的证书和公钥 $(pk_V, Cert(V))$;

(2) A 收到证书后对照自己的合法投票者名单，在名单中若找到与证书中的信息一致的投票者,则发送 $(Enc_{pk_V}(ID), Sig_{sk_A}(Hash(Enc_{pk_V}(ID)), pk_A, Cert(A))$，否则返回申请失败的信息。该 ID 值存放在合法投票者名单中。同时向 T 发送 $(Hash(ID), Sig(Hash(ID)), pk_A, Cert(A))$;

(3) T 收到 $Hash(ID)$,生成随机数 IDC,向 V 发送 $(IDC, Sig(Hash(IDC)), pk_T, Cert(T))$。

3.1.2 盲签名

(1) V 随机生成密钥 k，用位比特承诺方案 f 对投票内容 v 进行加密得到 $x = f(v, k)$，对 x 进行 RSA 盲签名，随机生成盲因子 r,$e = r^e x(mod\ N_A)$，发送 ($Hash(ID)$,e,$Sig_{sk_V}(Hash(e))$) 给 A。

(2) A 遍历整个合法投票者名单中的每个 ID，分别做哈希计算后可以判定 (1) 的发送者是否合法，若合法，则接受，否则返回签名失败的信息。并公布 $(Hash(ID), e, S)$。同时，A 向 V 发送对 e 的签名结果 $d = Sig_{sk_A}(e) = e^d(mod\ N_A)$

3.2 投票阶段

该阶段主要是 V 获取 A 的签名并向 T 发起投票。具体的过程为:

(1) V 对注册阶段收到的 d 进行去盲化，得到 $y = r^{-1}d(mod\ N_A)$，将 (x, y, IDC) 发送给 T。

(2) T 验证 y 是否为 A 对 x 的签名以及 IDC 是否是自己生成的，若是，则接受该投票结果，否则舍弃该票。

3.3 计票阶段

(1) 多个 V 完成了上述两个阶段后,T 对于每一个投票结果,生成随机数对 (u, v), 将 (u, v) 发送给 V，并计算 $(x^*, y^*) = (u, v) * (x, y) = (ux, vy)$。最后，T 公布每个 V 的 $(IDC, (x^*, y^*))$;

(2) V 将注册阶段生成的密钥 k 发送给 T;

(3) T 得到 k 后就可以对 x 解密得到 v，即投票结果，从而完成投票结果的统计。

4 安全性分析

完整性 通过设置唯一的投票编号，每个 V 都可以在 T 的公告板上跟踪自己的选票是否已经被 T 正确统计，同时 T 也可以验证所有选票是否合法，确保了最终选票结果是真实可靠的。

合法性 依靠加密、数字签名和证书等技术提供保密性和认证性，防止第三方非法用户的冒充。

唯一性 每个 V 持有的 ID 和 IDC 都是唯一的，如果出现重复的 ID 和 IDC 就视为弃票。

公正性 本协议将投票阶段和计票阶段分开进行，并且 A 和 T 都无法伪造投票结果，投票结果在计票阶段之前不会泄露。

匿名性 一方面在注册和投票阶段 A 和 T 分别无法知道 V 投了什么票或者这个票是由哪个 V 投的，另一方面若计票结果没有被正确计入，在原始的 FOO 投票协议中，V 需要出示自己的盲化因子 r，这样会导致 V 的身份泄露，在本协议中，只需要出示 IDC 即可，而 IDC 和 ID 没有关系，因此不会泄露 V 的身份。

弃权性 T 在投票阶段结束后，可以对照自己已有的 $Hash(ID)$ 表，若有某个 $Hash(ID)$ 没有对应的投票结果，则将其视为弃权票。

可验证性 每个 V 都可以根据 T 的公布栏中的 $(IDC,(x^*,y^*))$，用自己持有的 (u,v) 进行如下验证：若 $f(v,k)*u=x^*, Vrfy(\frac{y^*}{v})=x^*$，则公示结果无误，否则，V 可以提出申诉。

无收据性 在本协议中，最终公示的结果是 $(IDC,(x^*,y^*))$，其他人是看不到 (u,v) 的，那么假设存在买票行为，第三方希望某个 V 投他期望的票，但是如果 V 要让第三方相信他确实投了他所期望的票是没办法的，这

是因为：对于公示的投票结果 $(IDC, (x^*, y^*))$，存在至少以下两种可能，即 $(x^*, y^*) = (u_1, v_1) * (x_1, y_1)$ 或 $(x^*, y^*) = (u_2, v_2) * (x_2, y_2)$，而 (u, v) 没有公示，第三方无法确定 V 是否在欺骗他，(u, v) 的作用实质上是起一个盲化的效果，V 可能投了选项 1，实际上投了选项 2，只是最终盲化后的结果是一样的。