对Chen等人电子选举方案的密码学分析和修正

窦本年[1] 张 宏[2] 许春根[1] 韩 牟[2]
(南京理工大学理学院 南京 210094)[1] (南京理工大学计算机学院 南京 210094)[2]

摘 要 2004年,Chen等人提出一个安全的匿名网络选举方案。指出Chen等人给出的方案是不安全的;另外,给出一个满足电子选举安全要求的修正方案。

关键词 密码学分析,电子选举
中图法分类号 TP309 **文献标识码** A

Cryptanalysis and Modification of Chen et al.'s E-voting Scheme

DOU Ben-nian[1] ZHANG Hong[2] XU Chun-gen[1] HAN Mu[2]
(School of Science, Nanjing University of Science and Technology, Nanjing 210094, China)[1]
(School of Computer, Nanjing University of Science and Technology, Nanjing 210094, China)[2]

Abstract In 2004, Chen et al. proposed a secure internet e-voting. In this paper, we pointed out the security weaknesses of Chen et al.'s e-voting scheme. We gave a modification which satisfies the security requirements of an e-voting scheme.

Keywords Cryptanalysis, E-voting

1 引言

电子选举是近二十年被提出来用电子手段替代传统纸制选举的选举方案[1-6]。

一般来说,一个电子选举方案包括3个阶段:

初始阶段:在这个阶段,投票者在选举机构登记获得投票权,另外,一些系统参数被选取。

投票阶段:投票者通过一些通讯技术将自己填好的选票投出。

计票阶段:在此阶段,选票被统计,最终的选举结果被公布。

电子选举方案必须能提供至少和纸制选举方案相同的安全性。尽管电子选举方案的标准还没有提出来,但是在学者间达成共识的是,电子选举方案应该满足如下要求[4-6]:

正确性:所有有效选票应被正确统计。选票不能被修改、复制和删除。

公平性:计票结束前,没有人能知道选举结果。

合格性:只有合格的投票者才被允许投票。

唯一性:每个投票者最多只能投票一次。

不可强迫性:投票者不能向别人证明他投的是什么票以防止贿选。

匿名性:没有方法确定一张有效的选票是谁投的。

可验证性:每个投票者可以独立地验证他的选票已被正确地统计。

最近,Chen等人提出一个安全的网络选举方案,我们称之为CJC电子选举方案(后文简称CJC方案)[6]。在CJC等方案的基础上,Cao等人利用多项式函数构造了一个新的匿名网络选举方案[7]。文献[6,7]宣称CJC方案满足以上所列的电子选举方案的安全要求。在本文中,我们指出CJC方案不满足正确性、公平性、不可强迫性和可验证性。

本文第2节简要回顾CJC方案;第3节指出CJC方案的安全弱点;第4节给出CJC方案的一个满足电子选举安全要求的修正方案;最后是结束语。

2 CJC方案

本节回顾CJC方案。他们的方案基于RSA公钥密码体制和Chaum盲签名。CJC方案包括4个参与者:投票者V_i,认证中心AC,计票中心TC和监票中心SC。另外,证书机构CA和代理服务器也是需要的[6]。

需要下面一些记号描述他们的方案。PK是相应于RSA公钥体制中私钥SK的公钥。$E_{PK}(m)$是RSA中利用公钥PK对明文m的加密,而$D_{SK}(m)$是RSA中利用私钥SK对密文m的解密。$S_{SK}(m)$是利用私钥SK对消息m的签名。以下是CJC方案。

初始阶段:证书机构CA生成AC的RSA公私钥对(PK_{AC}, SK_{AC})并发给AC。另外,CA生成RSA公私钥对(PK_{TS}, SK_{TS})公布PK_{TS},而SK_{TS}由TC和SC秘密共享,s_{SC}是由SC分得的子秘密,s_{TC}是由TC分得的子秘密,$SK_{TS}=$

到稿日期:2009-12-04 返修日期:2010-03-12 本文受国家自然科学基金(No. 10771101),南京理工大学自主科研专项计划资助项目(No. 2010ZYTS067)资助。

窦本年(1976-),男,博士生,讲师,主要研究方向为密码学,E-mail:doubennian@yahoo.com.cn;张 宏(1956-),男,博士生导师,主要研究方向为信息安全;许春根(1969-),男,副教授,主要研究方向为信息安全;韩 牟(1982-),女,博士生,主要研究方向为密码学。

$s_{SC}+s_{TC}$。

认证阶段：在被 AC 认证后，投票者 V_i 选取随机数 v_i 作为自己的假名。然后，投票者 V_i 利用盲签名机制对 v_i 进行盲化，并把盲化后的 v_i 发给 AC。AC 对盲化后的 v_i 签名并把签名发给 V_i。投票者 V_i 对签名解盲从而获得签名 $S_{SK_{AC}}(v_i)$。

投票阶段：投票者 V_i 填好自己的选票 m 并选取随机数 β，计算 $E_{PK_{TS}}(m\oplus\beta)$。随后，$V_i$ 通过一个可信的代理服务器将$((v_i,S_{SK_{AC}}(v_i),E_{PK_{TS}}(m\oplus\beta),\beta)$发给 TC 和 SC。在收到$(v_i,S_{SK_{AC}}(v_i),E_{PK_{TS}}(m\oplus\beta),\beta)$后，$TC$ 和 SC 验证 v_i 和它的签名以防止重复投票。TC 和 SC 将$(v_i,S_{SK_{AC}}(v_i),E_{PK_{TS}}(m\oplus\beta),\beta)$存入自己的数据库。

计票阶段：TC 和 SC 合作对 $E_{PK_{TS}}(m\oplus\beta)$ 进行解密。为此，TC 和 SC 利用各自的子秘密 s_{SC} 和 s_{TC} 分别对 $E_{PK_{TS}}(m\oplus\beta)$进行解密。他们分别计算 $D_{s_{SC}}(E_{PK_{TS}}(m\oplus\beta))$和 $D_{s_{SC}}(E_{PK_{TS}}(m\oplus\beta))$，则最终的选票为：

$$m=(D_{s_{SC}}(E_{PK_{TS}}(m\oplus\beta))D_{s_{TC}}(E_{PK_{TS}}(m\oplus\beta)))\oplus\beta$$

3 CJC 方案的安全弱点

Chen 等人宣称 CJC 方案满足在引言中提到的电子选举的几个安全要求。在本节中我们指出 CJC 方案并不能完全满足引言中提到的几个安全要求。

在第 2 节中我们知道有两个机构即计票中心 TC 和监票中心 SC 会获得选民的选票。Chen 等人在他们的方案中并没有对这两个机构的可信性进行假设定义。我们可以假设 SC 是可信的，否则如果 TC 是可信的话，监票中心 SC 就不需要了。我们就是基于 SC 是可信的这个假设，来分析 CJC 方案的安全弱点。

3.1 CJC 方案不满足公平性

CJC 方案只使用了教科书式的 RSA 公钥密码方案来保证私密性。此 RSA 方案达不到 CPA，即在选择明文攻击下不安全[8]。投票者的真实选择可以被敌手确定：假如敌手有办法(比如与 TC 共谋)获得三元组$(v_i,S_{SK_{AC}}(v_i),E_{PK_{TS}}(m\oplus\beta),\beta)$，那他就可以加密所有可能的选票与 β 的异或来计算 $E_{PK_{TS}}(m\oplus\beta)$，并将这些加密与他获得的三元组进行比较，从而可以获得投票者的真实选择。因此，CJC 方案不满足公平性。

3.2 CJC 方案不满足匿名性

投票者通过一个可信的代理服务器将$(v_i,S_{SK_{AC}}(v_i),E_{PK_{TS}}(m\oplus\beta),\beta)$发送给 TC 和 SC。然而，代理服务器并不能提供匿名性，它只能去掉投票者电脑的 IP 地址。事实上，一个敌手可以对投票者的计算机与代理服务性之间的通信、代理服务器与 TC 之间的通信进行监听，然后他可以要求 TC 告诉他那张选票的内容，从而这个敌手就知道一个投票者投了什么样的票。因此，CJC 方案不满足匿名性。

3.3 CJC 方案不满足不可强迫性

在对一个选票的解密阶段，TC 知道$(v_i,S_{SK_{AC}}(v_i),E_{PK_{TS}}(m\oplus\beta),\beta)$，如此，它能知道选票 m 相应的假名 v_i，另外一方面，v_i 和投票者 V_i 是捆绑在一起的，因此在 TC 的帮助下，投票者 V_i 能向别人证明他投了什么票。从而，CJC 方案不满足不可强迫性。

3.4 CJC 方案不满足可验证性

在文献[6]中，作者们宣称他们的方案因为有了 SC 而满足可验证性。事实上，投票者无法获得证据以证明他们的选票被正确地统计了。

4 我们的修正方案

本节给出 CJC 方案的修正方案以满足电子选举的安全要求。

4.1 密码学准备

ElGamal 公钥加密方案为使用 ElGamal 密码体制，我们需要一个循环群 $G=\langle g\rangle$，在群 G 上离散对数是难解的。公钥是 $h=g^x$，x 是相应的私钥。对明文 m 的加密是(g^r,mh^r)，r 是一个随机数。密文(g^r,mh^r)的解密计算是$(mh^r)(g^r)^{-x}$。

ElGamal 密码体制的重加密[9]　ElGamal 密码体制下的密文(g^r,mh^r)可以被重加密而不影响解密。重加密的过程是这样的：(g^r,mh^r)被变换为$(g^s,mh^s)=(g^rg^t,mh^rh^t)$，$t$ 是一个随机数。容易看出重加密不影响解密，但是可以提供匿名性。

盲签名　盲签名也可以提供匿名性。在修正方案中我们使用 RSA 盲签名体制。签名者的私钥是 d，公钥是 e，$ed=1 \bmod \phi(n)$，n 是两个安全的大素数的乘积。一个用户若使用盲签名方案来获得签名者对消息 m 的签名，可按如下程序：首先，他随机选择一个随机数 r，并将 $r^eh(m)$发给签名者，这地方的 $h(m)$是消息 m 的 Hash 值；随后，签名者将$(r^eh(m))^d$ 发给这个用户；最后，用户获得消息 m 的签名是$(r^eh(m))^d/r$。

4.2 我们的修正方案

先给出一些记号。

V_i：投票者 i。

v_i：投票者 V_i 的假名。

CA：证书机构。

AC：认证中心负责对投票者进行认证。

TC：可信中心负责把从用户获得的密文重加密，并把这些重加密的密文随机打乱，另外可信中心还负责把投票者的假名公布在特定的网页上。可信中心在这些环节中是可信的。

SC：监票中心由 k 个政党 $SC_1,SC_2,\cdots,SC_k$ 组成。监票中心负责计票。

//：比特的串联计算。

方案中，我们使用投票站(即网络中的几个计算机终端)而不是代理服务器，利用投票站投票者可以匿名地将他们的选票投出去。另外我们使用 SSL(Secure Socket Layer 安全套阶层)保护投票站与那些投票中心机构之间的通信。先给出一些记号。

初始阶段：CA 生成 RSA 密钥对(PK_{AC},SK_{AC})和模数 N 给 AC。另外，CA 选择一个离散对数是难解的循环群 $G=\langle g\rangle$。CA 选取 ElGamal 密钥对$(x,h=g^x)$给 SC，h 是公钥，x 是相应的私钥。且 x 通过某个秘密共享机制由 $SC_1,SC_2,\cdots,SC_k$ 共享，$SC_1,SC_2,\cdots,SC_k$ 的子秘密分别是 $x_1,x_2,\cdots,x_k$；x 可以由 $t(<k)$个，或多于 t 个子秘密恢复出来[10]。N,PK_{AC}，G,g,G 的阶，h 公开。

认证阶段：在被 AC 认证后，投票者 V_i 选取随机数 v_i 作为自己的假名。然后，投票者 V_i 利用盲签名机制对 v_i 进行盲化，并把盲化后的 v_i 发给 AC。AC 对盲化后的 v_i 签名并

(下转第 125 页)

验证 Web 服务组合，则是一个新的研究方向。文献[7]指出在 Web 服务体系结构方面国际上仍然缺乏相关的研究；文献[8]提出需要从软件体系结构的角度研究 Web 服务组合及其验证的观点，并指出了组合服务体系结构的基本元素；文献[9]提出一种专门描述 Web 服务组合系统的体系结构描述语言 WSC/ADL，但与已有的软件体系结构描述语言相比，该语言还不够成熟，也未给出如何验证 Web 服务组合的工作。

本文从软件体系结构角度出发，并考虑到 Web 服务组合的实时特征，最后应用一种模型检测工具 UPPAAL 来实现对运行之前的 Web 服务组合的正确性验证。

结束语 由于 Web 服务处于一种分布式异构环境下，依靠实际运行发现其中错误的代价会较高，因此有必要从形式化角度验证 Web 服务组合的正确性。模型检测作为形式验证的一种重要技术，因其自动化程度高并且在不满足系统性质时能够给出反例，故应用越来越广泛。本文研究是模型检测在 Web 服务组合中的一个初步应用。本文未考虑到 Web 服务中涉及到多种复杂机制，如异常处理及补偿机制等以及如何缓解模型检测的 Web 服务组合状态空间爆炸问题，下一步工作将考虑解决这些问题。

参 考 文 献

[1] 唐稚松，等. 时序逻辑程序设计与软件工程[M]. 北京：科学出版社，2002

[2] 朱雪阳，唐稚松. 基于时序逻辑的软件体系结构描述语言 XYZ/ADL [J]. 软件学报，2003，14(4)：714-720

[3] 魏慧，戎枚，张广泉. 一种基于体系结构的 Web 服务组合描述方法[J]. 计算机工程与科学，2008，30(12)：5-8

[4] Behrmann G, David A, Larsen K G. A Tutorial on UPPAAL [C]// Int'l School on Formal Methods for the Design of Computer, Communication, and Software Systems. SFM-RT 2004, LNCS 3185, Springer-Heidelberg, 2004: 200-236

[5] Alur R, Dill D L. A Theory of Timed Automata[J]. Theoretical Computer Science, 1994, 126(2): 183-235

[6] 刘珊艳，张广泉. 实时时序逻辑语言 XYZ/RE 到时间自动机的映射[J]. 微计算机应用，2008，29(6)：69-75

[7] Vinoski S. WS-Nonexistent Standards [J]. IEEE Internet Computing, 2004, 8(6): 94-96

[8] Milanovic N, Malek M. Architectural Support for Automatic Service Composition[C]// Proc. IEEE Int'l Conf. Service Computing (SCC 2005). Washington, DC, 2005: 133-140

[9] 杨鑫，陈俊亮. WSC/ADL：Web Services 组合系统体系结构描述语言[J]. 软件学报，2006，17(5)：1182-1194

(上接第 98 页)

把签名发给 V_i。投票者 V_i 对签名解盲从而获得签名 $S_{SK_{AC}}(v_i)$。

投票阶段：V_i 选择两个随机数 r_i, y_i，并用 SC 的公钥 h 对他填好的选票 m_i 进行加密，并计算 $b_i = v_i // s_i // (g^{y_i}, m_i h^{y_i})$，$V_i$ 通过一个投票站将 b_i 发送给 TC。获得 b_i 后，TC 可以获取 v_i, s_i 和 $(g^{y_i}, m_i h^{y_i})$。TC 验证 v_i 的签名；它不允许假名 v_i 投两次票。TC 将 v_i 存入到只有 TC 可以编辑的一个网页中；这个网页对所有的投票者公开，投票者可以通过访问这个网页查看假名以确认自己的选票是否发给 TC。同时，TC 将 $(g^{y_i}, m_i h^{y_i})$ 重加密为 $(g^{z_i}, m_1 h^{z_i})$，并把这些 $(g^{z_i}, m_1 h^{z_i})$ 存入到它的被保护的数据库中。

计票阶段：投票阶段一结束，TC 把这些重加密后的密文 $(g^{z_1}, m_1 h^{z_1}), (g^{z_2}, m_2 h^{z_2}), \cdots, (g^{z_n}, m_n h^{z_n})$ 以随机顺序发给 SC。对于这些密文，首先，从 k 个政党 $SC_1, SC_2, \cdots, SC_k$ 中取出 t 个政党恢复私钥 x，接着利用 x 去解密每一个密文以获得选票。最后 SC 统计所有选票并公布此次投票结果。

4.3 安全性分析

下面说明我们的方案满足引言中所列的安全要求。

正确性：因为使用了 SSL，在我们的方案中选票在通过因特网传输时，不会被修改、复制和删除。TC 的可信与选票的门限解密保证了每一张选票会被正确地统计。

公平性：因为使用了 SSL，在选举结果出来前每一张选票都是被保密的。没有人能在选举中途知道选举结果。

合格性和唯一性：通过验证假名的签名，这两个要求可以被满足，只有合格的投票者才能投票，每个合格的投票者只能投一次。

不可强迫性：投票者只能出示从 TC 维护的网页中获得的他选取的假名，而 SC 只解密从 TC 处获得的打乱的重加密的密文，因此，投票者不能向别人证明他投的是什么票。

匿名性：在认证阶段我们的方案使用了盲签名，从而可以确保 AC 不能将假名与投票者联系起来；在投票阶段，选票是通过投票站投的，也可以提供匿名支持；在计票阶段，因为我们使用了重加密，所以 SC 不能将一个选票与投票者联系起来。

可验证性：投票者可通过访问 TC 管理的网页查看自己的假名是否在这个网页上以确认自己的选票是否被准确地统计。

结束语 在本文中，我们指出了 CJC 电子选举方案的安全漏洞，给出了一个修正方案，修正后的方案克服了 CJC 方案的安全漏洞。最后指出在我们的修正方案中可以用 Mixnet[1] 代替投票站以提高灵活性。

参 考 文 献

[1] Chaum D. Untraceable electronic mail, return addresses and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2): 84-88

[2] Fujioka A, Okamoto T, Ohta K. A practical secret voting scheme for large scale elections [C] // Proceeding of Cryptology-AUCRYPT'92. Springer, 1993: 15-19

[3] Okamoto T. Receipt-free electronic voting schemes for large scale elections [C] // Proceeding of Security Protocols Workshop. Springer, 1997: 25-35

[4] Dini G. A secure and available electronic voting service for a large-scale distributed system [J]. Future Generation Comput Syst, 2003, 19(1): 69-85

[5] Liaw H. A secure electronic voting protocol for general elections [J]. Computer & security, 2004, 23(2): 107-119

[6] Chen Y, Jan J, Chen C. The design of a secure anonymous internet voting system[J]. Computer & security, 2004, 23(4): 330-337

[7] Cao F, Cao Z. A secure anonymous internet electronic voting scheme based on the polynomial[J]. Wuhan University Journal of Natural Sciences, 2006, 11(6): 1777-1780

[8] Bellare M, Rogaway P. Optimal asymmetric encryption [C]// Proceeding of EUROCRYPT'94. Springer, 1995: 92-111

[9] Park C, Itoh K, Kurosawa K. Efficient anonymous channel and all/nothing election scheme[C]// Proceeding of EUROCRYPT'88. Springer, 1988: 177-182

[10] Pedersen T P. A threshold cryptosystem without a trusted party (extended abstract) [C] // Proceeding of EUROCRYPT'91. Springer, 1991: 522-526