一个新的$(t,N-2)$弹性的 Mix Net

高虎明 陈晓峰 王育民

(西安电子科技大学 ISN 国家重点实验室 西安 710071)

摘 要 Mix net 是实现匿名通信、电子投票选举、电子支付以及电子投标的有力工具. 该文建立了$(t,N-2)$Mix net 模型,利用 Shamir 门限方案、ElGamal 公钥体制、零知识证明等密码技术设计了一个基于这个模型的 Mix net 协议. 该协议将同一密文组让不同的两个服务器组进行盲化解密示证和比较,从而使得该协议具有$(t-1,N-2)^{AA}$弹性及秘密性、正确性和可验证性等优点,同时通信量和计算量方面也少于已知的基于 ElGamal 公钥体制的可验证 Mix net 协议.

关键词 Mix net; 秘密性; 正确性; 可验证性

中图法分类号 TP309

A New $(t,N-2)$-Resilience Mix Net

GAO Hu-Ming CHEN Xiao-Feng WANG Yu-Min

(*National Key Laboratory of Integrated Serviced Networks, Xidian University, Xi'an* 710071)

Abstract A model of $(t, N-2)$-resilience Mix net is set up. A Mix net protocol based on the model is presented with the primitive cryptography tools of Shamir secret share scheme, ElGamal public key system, zero_knowledge and so on. Given an array of encrypt messages, two different groups of mix servers blind and decrypt the same array, then compare them, and finally publish the correct deciphered text on bulletin board. Our Mix net protocol mainly has the following properties: (1) The output of Mix net is$(t,N-2)^{AA}$-resilience that means the Mix net can also output right the decipher text and can not find the relationship between the input and output although there are $N-2$ malicious users among N senders and $t-1$ dishonest servers in t servers which may cooperate; (2) Because of the ElGamal public key system the input length of Mix net does not change with the number of Mix net servers; (3) The communication and computing cost is less than that of other verifiable Mix nets that we know presently due to the technique of dividing Mix net servers into two groups .

Keywords Mix net; confidentiality; correctness; verifiability

1 引 言

提供发送者匿名的基本密码协议 Mix net 的输入是一串加密的数据$(c_1,c_2,\cdots,c_N)$,输出是输入解密后得到的数据串$(m_1,m_2,\cdots,m_N)$的一个随机置换,隐藏了$(c_1,c_2,\cdots,c_N)$和$(m_1,m_2,\cdots,m_N)$之间的对应关系. Mix net 的简单实现是只用一个 Mix 服务器,其缺点是这要求用户对它的完全信任,容易招到各种攻击. Mix net 被认为是实现匿名通信、电子投票选举、电子支付以及电子投标的很好工具.

针对保护个人的通信隐私性,1981 年 Chaum 提

收稿日期:2002-04-23;修改稿收到日期:2002-10-29. 本课题得到国家自然科学基金(60073052)资助.**高虎明**, 男,1963 年生,博士研究生,副教授,主要研究方向为密码学及其应用、电子商务和网络安全. E-mail: gao_hmcn@cn. yahoo. com. **陈晓峰**,男,1976 年生,博士研究生,研究方向为电子商务、椭圆曲线密码. **王育民**,男,1936 年生,教授,博士生导师,研究领域为信息理论、编码及密码理论.

出了 Mix-networks 的思想和具体的方案,后来 Pfitzmann 给出了对这个方案的攻击;Chaum 方案的另一问题是他用 RSA 公钥体制,使得密文 c_i 的长度与 Mix 服务器的个数成正比例增长,带来了太多的额外通信量和加解密工作量. 1993 年 Park 等提出了用 ElGamal 公钥体制加密实现 Mix net 的方法,使得密文 c_i 为固定长度与 Mix 服务器的个数无关. 至此以后基于 ElGamal 公钥体制加密实现的 Mix net 成为研究的热点.

目前对 Mix net 的研究主要集中在:(1) 提高 Mix net 的可信度,包括正确性和秘密性. 为了增加可信度,一个 Mix net 由多个服务器组成,希望在一半以上的服务器诚实的情况下保证 Mix net 输出的正确性和秘密性. (2) 选择设计合适的算法和协议减少 Mix net 通信量和计算量. (3) 同时引入可验证性,让服务器公布一些计算过程,他人能用之证明其计算的正确性,约束他遵守协议工作. 利用 ElGamal 公钥体制加密是减少通信量的有效工具,增加预处理计算,减少在线计算是提高 Mix net 效率的有效方法.

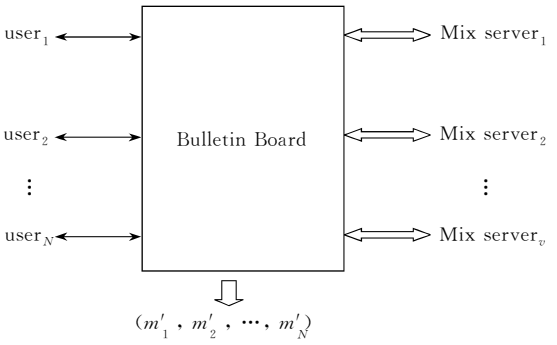
文献[7~10]中提出了不少可验证的高效的 Mix net 方案,但有的后来发现是不安全的,有的效率并不很高. 本文建立了 $(t,N-2)$ Mix net 模型,利用 Shamir 门限方案、ElGamal 公钥加密体制、零知识证明等密码技术设计了一个基于这个模型的 Mix net 协议. 我们的方法优于已有方案,其关键技术在于把同一密文组让两个不同的合法秘密共享组进行盲化解密,然后再进行对比. 这样既提高了解密的正确性,也减少了每个 Mix net 服务器的计算量和通信量. 我们的 Mix net 协议具有 $(t,N-2)^{AA}$ 弹性,密文长度与 Mix net 服务器个数无关,通过预计算可减少 Mix net 服务器的计算量,计算量和通信量都低于我们已知的可验证的 Mix net 协议,如文献[7~10]中的方案.

以下部分是这样展开的:首先引入 $(t,N-2)$ 弹性的 Mix net 模型,其次介绍协议使用的基本密码算法和协议,然后给出我们的 Mix net 协 议;在第 5 节进行协议的安全特性及其效率分析;最后是结束语.

2 $(t,N-2)$ 弹性的 Mix net 模型

2.1 Mix net 基本模型

在基于 ElGamal 公钥体制加密实现的 Mix net 基本模型中有三方参与者:用户 user,公布栏 Bulletin board,Mix net 服务器 Mix servers.



协议的基本模式是:

(1) 用户 i 发送加密的消息 $c_i=(a_i,b_i)=(g^{r_i}, m_i y^{r_i})$ 到 Bulletin Board,$i=1,2,\cdots,N$;

(2) Mix servers 对 $(c_1,c_2,\cdots,c_N)$ 进行盲化、解密和置换得到 $(m_1,m_2,\cdots,m_N)$ 的一个置换 $(m'_1,m'_2,\cdots,m'_N)$,并在 Bulletin board 上公布.

最为理想的是使得任何人无法得知 $(m_1,m_2,\cdots,m_N)$ 和 $(m'_1,m'_2,\cdots,m'_N)$ 的对应关系.

2.2 安全要求和攻击模型

假定最多有 $t-1$ 个不诚实的 Mix servers 和 $N-2$ 个恶意的用户试图发现 $(m_1,m_2,\cdots,m_N)$ 和 $(m'_1,m'_2,\cdots,m'_N)$ 的对应关系或者使得解密失败. 首先我们引入如下安全要求:

(1) $(t,N-2)$ 秘密性:能隐藏 $(m_1,m_2,\cdots,m_N)$ 和 $(m'_1,m'_2,\cdots,m'_N)$ 之间的对应关系的概率很大,使得发现其对应关系的概率不优于随机猜测.

(2) $(t,N-2)$ 正确性:Mix net 输出错误的 $(m'_1,m'_2,\cdots,m'_N)$ 的概率接近 0.

(3) $(t,N-2)$ 验证性:Mix net server 作弊成功即不按协议进行通信和计算的得逞的概率接近 0.

如果一个 Mix net 满足 $(t,N-2)$ 秘密性,$(t,N-2)$ 验证性和 $(t,N-2)$ 正确性,称它是具有 $(t,N-2)$ 弹性的.

根据攻击者的行为方式还可详细分为:

$(t,N-2)^{PP}$ 弹性的:即恶意的 $t-1$ 个服务器和 $N-2$ 个用户都是被动的攻击者;

$(t,N-2)^{PA}$ 弹性的:即恶意的 $t-1$ 个服务器是被动的攻击者和恶意的 $N-2$ 个用户是主动的攻击者;

$(t,N-2)^{AP}$ 弹性的:即恶意的 $t-1$ 个服务器是主动攻击者,恶意的 $N-2$ 个用户是被动的攻击者;

$(t,N-2)^{AA}$ 弹性的:即恶意的 $t-1$ 个服务器和 $N-2$ 个用户都是主动的攻击者.

3　基本协议和算法

1) 基于 ElGamal 的加密算法

令 $p=2q+1$，p 和 q 是大素数，G_q 是 Z_p^* 的 q 阶乘法子群，g 是 G_q 的生成元，$y=g^x$，x 是秘密钥，公开钥是(p,q,g,y)．用户对消息 m 的加密过程是，随机选择 $r\in_r Z_q$，加密消息是$(a,b)=(g^r,my^r)$，解密 $m=\frac{b}{a^x}$．

2) *Shamir* (t,v)门限方案

Mix net 服务器用 *Shamir* (t,v)门限方案共享秘密钥 x．S_i的秘密钥是 x_i，

$x=\sum_{i\in Q}x_i l_i \pmod q$，其中 $l_i=\prod_{j\in Q,j\neq i}\frac{j}{j-i}$，$Q$ 是参与者的一个子集，$|Q|=t$．

(p,q,$y=g^x$)是 Mix net 的公开钥．

3) 证明 $\log_{g_1} y_1=\log_{g_2} y_2$ 离散对数相等的非交互零知识证明

示证者 prover：

(1) 产生随机数 v，计算 $t_1=g_1^v$，$t_2=g_2^v$；

(2) $c=H(g_1,g_2,y_1,y_2,t_1,t_2)$；

(3) $r=v-cx$．

公布(c,r)．

验证者 verifier：

计算 $t_1=g_1^r y_1^c$，$t_2=g_2^r y_2^c$；验证 $c\overset{?}{=}H(g_1,g_2,y_1,y_2,t_1,t_2)$．

这个协议的安全性是建立在求离散对数的困难性和 Hash 函数的安全性上的．

4　(t,$N-2$)弹性的 Mix net 协议

4.1　系统建立

假定有 N 个用户(users)，其中最多有 $N-2$ 个不诚实用户；$2t$ 个 Mix net 服务器，其中最多有 $t-1$ 个 Mix net 服务器是不诚实的，$2t$ 个 Mix net 服务器利用 *Shamir* (t,v)门限方案共享秘密钥 x，$p=2q+1$，p,q 是质数，G_q 是 Z_p^* 的 q 阶乘法子群，g 是 G_q 的生成元，(p,q,$y=g^x$)是 Mix net 的公开钥，同时每个 Mix net 服务器 i 公布 $y_i=g^{x_i}$，x_i保密．

有一个公布栏 bulletin board，每个 Mix net 服务器和用户可以在 bulletin board 上正确读写，别人不能伪造特定 Mix net 服务器在 Bulletin board 公布信息，公布栏协议本文不作介绍．

假定 Bulletin board 公布有一组需要解密的密文

$$c=(c_1,c_2,\cdots,c_N),$$

其中 $c_i=(a_i,b_i)=(g^{r_i},m_i y^{r_i})$，$i=1,2,\cdots,N$．

4.2　基本协议描述

4.2.1　主协议描述

1．把 $2t$ 个 Mix servers 随机分成两组 $group_1=\{I_1,I_2,\cdots,I_t\}$，$group_2=\{II_1,II_2,\cdots,II_t\}$，$group_1\cup group_2=\{1,2,\cdots,2t\}$；

2．$group_1$ 对 $c=(c_1,c_2,\cdots,c_N)$ 执行盲化子协议 *groupblind*($group_1$,c)得 $B_1=L_N$；$group_2$ 对 $c=(c_1,c_2,\cdots,c_N)$ 执行盲化子协议 *groupblind*($group_2$,c)得 $B_2=L_N$；

3．$group_1$ 对 B_1 执行解密子协议 *Decryption*($group_1$,B_1)得 M_1；$group_2$ 对 B_2 执行解密子协议 *Decryption*($group_2$,B_2)得 M_2；

4．执行追查作弊者子协议 *verify*($group_1$)和 *verify*($group_2$)，如有作弊者返回步 1；

5．所有 Mix servers 比较 M_1 是否等于 M_2，若相等 Mix net 输出 M_1，结束；反之返回步 1．

4.2.2　子协议描述

(1) *groupblind*($group$,c)

令 $L_0=c=((a_{0,1},b_{0,1}),(a_{0,2},b_{0,2}),\cdots,(a_{0,N},b_{0,N}))$．

每个 Mix server$_i$ 随机选择 $r_{i,j}\in Z_q$，置换 π_i，$i\in group$，

计算 $L_i=\pi_i((a_{0,1}g^{r_{i,1}},b_{0,1}y^{r_{i,1}}),(a_{0,2}g^{r_{i,2}},b_{0,2}y^{r_{i,2}}),\cdots,(a_{0,N}g^{r_{i,N}},b_{0,N}y^{r_{i,N}})$，把 L_i在 Bulletin board 上公布；

(2) *Decryption*($group$,C)

令 $LL_0=C=((G_{0,1},H_{0,1}),(G_{0,2},H_{0,2}),\cdots,(G_{0,N},H_{0,N}))$，

Mix server$_i$，$i\in group$ 首先计算

$LL_i=((G_{i-1,1},H_{i-1,1}/(G_{i-1,1})^{x_i l_i}),(G_{i-1,2},H_{i-1,2}/(G_{i-1,2})^{x_i l_i}),\cdots,(G_{i-1,N},H_{i-1,N}/(G_{i-1,N})^{x_i l_i})$，$l_j=\prod_{j\in Q,j\neq i}\frac{j}{j-i}$，并且把 $((G_{i-1,1},H_{i-1,1}/(G_{i-1,1})^{x_i l_i}),(G_{i-1,2},H_{i-1,2}/(G_{i-1,2})^{x_i l_i}),\cdots,(G_{i-1,N},H_{i-1,N}/(G_{i-1,N})^{x_i l_i})$公布在 Bulletin board；

同时公布证明 $\log_{G_{i-1,j}} G_{i-1,j}^{x_i l_i}=\log_g y_i^{l_i}$，$i=1,2,\cdots,t$；$j=1,2,\cdots,N$．

(3) *verify*($group$)

令 $choice=hash(M_1,M_2,b_1,b_2)$，

对每个 Mix net 服务器 $i\in group$，在公布栏上给出集合 $G\subset\{1,2,\cdots,N\}$，

$|G|=|\{i;choice[i]=0\}|$，

$choice[i]$指把 $choice$ 看成二进制字符串的第 i 位．证明：

①存在数 G_i，Y_i满足：

ⓐ $G_i\cdot\prod_{\substack{choice[j]=0\\ j=1,2,\cdots,N}}a_{i-1,j}=\prod_{j\in G}a_{i,j}$；

ⓑ $Y_i \cdot \prod_{\substack{choice[j]=0 \\ j=1,2,\cdots,N}} b_{i-1,j} = \prod_{j \in G} b_{i,j}$;

ⓒ $\log_g G_i = \log_y Y_i$;

②存在数 G_i,Y_i 满足:

ⓐ $G_i \cdot \prod_{\substack{choice[j]=1 \\ j=1,2,\cdots,N}} a_{i-1,j} = \prod_{j \in group-G} a_{i,j}$;

ⓑ $Y_i \cdot \prod_{\substack{choice[j]=1 \\ j=1,2,\cdots,N}} b_{i-1,j} = \prod_{j \in group-G} b_{i,j}$;

ⓒ $\log_g G_i = \log_y Y_i$.

如果上述条件和等式有一不满足,说明 i 作弊,把 i 除名,添加一个 Mix net 服务器;直到每个服务器证明完毕.

5 安全特性及其效率分析

首先讨论我们的$(t,N-2)$弹性的 Mix net 协议的安全性,我们以定理的形式给出,并且予以简要的证明.

假定公布栏协议是安全的,即他人不能伪造篡改某人发布的信息,事实上只要使用加时戳的安全数字签字算法就能保证这一点.

定理 1. 本文给出的 Mix net 协议是具有$(t,N-2)^{PP}$弹性的.

证明. 用户和服务器都是被动攻击者.

他们受公布栏协议的限制不能篡改窃听他人消息,遵守协议正确计算,惟一的手段是恶意者勾结配合企图得知某些消息的发送者.这就保证了$(t,N-2)$正确性和$(t,N-2)$可验证性;由于 t 个服务器中至少有一个诚实者,他在盲化时使用的随机指数 $r_{i,j}$ 和随机置换 π_i 是秘密的,即使有 $t-1$ 个服务器和 $N-2$ 个用户勾结,也不能以高于平均概率得知未知消息的发送者,除非他们能攻破 ElGamal 的加密算法和 Shamir(t,v)门限方案,从而保证了$(t,N-2)$秘密性.

定理 2. 本文给出的 Mix net 协议是具有$(t,N-2)^{PA}$弹性的.

证明. 服务器是被动攻击者,用户是主动攻击者.

这时服务器是遵守协议的,他们不篡改窃听他人消息,由于公布栏协议的限制,用户的主动性很局限,惟一的手段也只是恶意者勾结配合.这与定理 1 条件相同,所以是具有$(t,N-2)^{PA}$弹性的.

定理 3. 本文给出的 Mix net 协议是具有$(t,N-2)^{AP}$弹性的.

证明. 服务器是主动攻击者,用户是被动攻击者.

由于公布栏协议的限制,他们不能篡改窃听他人消息.在 Decryption 和 verify 阶段由于零知识证明协议的执行以及主协议的步骤 5,所有 Mix servers 比较 M_1 是否等于 M_2 保证了解密的正确性和可验证性.

服务器发起的主动攻击只是不遵守协议,在 group-blind 阶段不按协议规定计算和置换,进行欺诈发起攻击.执行一次 verify 子协议以 1/2 的概率发现和替换欺诈者;同时由于 $group_1$ 和 $group_2$ 中存在诚实服务器,他们的随机指数 $r_{i,j}$ 和随机置换 π_i 是秘密的,即使欺诈者在执行子协议 verify 时相互配合得到$(m_1,m_2,\cdots,m_N)$和$(m'_1,m'_2,\cdots,m'_N)$之间的对应关系的概率也不大于随机猜测.极端情况下有 $t-1$ 个服务器和 $N-2$ 个用户配合,这时只要确定两个 m_i,m_j 和 m'_s,m'_k 的对应关系,随机猜对的概率是 1/2,$t-1$ 个服务器和 $N-2$ 个用户配合得逞的概率也只是 1/2.因而具有$(t,N-2)$秘密性.

定理 4. 本文给出的 Mix net 协议是具有$(t,N-2)^{AA}$弹性的.

证明. 服务器和用户是主动攻击者.

用户的主动攻击受 Bulletin 协议限制他们的手段与用户是被动攻击者时相同,所以是具有$(t,N-2)^{AA}$弹性的.

协议效率

用户只进行一次 ElGamal 的加密运算,要传输的数据量大约只是实际信息的两倍.这与已有的基于 ElGamal 公钥体制的 Mix net 协议相同.

我们把用户 i 的一个发送信息 m_i 看成一个信息,以对每个信息的计算量和通信量作为效率衡量标准.

在没有服务器作弊时,每个服务器对每个信息进行一次盲化,此时盲化因子可以通过预计算得到,实时计算只需要两次乘法;每个服务器在 verify 阶段对每个信息平均需要 $2t/N$ 个零知识证明验算;解密阶段,每个服务器对每个信息进行一次 ElGamal 解密运算、一次零知识证明、$t-1$ 次零知识证明验算.因此在计算量方面,我们的协议是优于 Miyako Ohkubo 和 Masayuki Abe 的 A Length-Invariant Hybrid Mix,Jakobsson 的 A practical mix. Jakobsson 的 Flash mixing.在没有服务器作弊时,我们只用了一次盲化运算和解密运算,使得通信量大大低于文献[7~10]中的方案.

在有服务器作弊时,我们的协议的计算量和通信量也低于文献[7~10]中的方案,这里我们不再做详细分析.

6 结束语

我们将同一密文向量让不同的两个服务器组进

行盲化解密,使该协议具有$(t,N-2)^{AA}$弹性及秘密性、正确性和可验证性等优点,同时通信量和计算量方面也少于目前我们已知的基于 ElGamal 公钥体制的 Mix net 协议.

我们的协议具有一定的鲁棒性,并且当有 Mix 服务器作弊时可以替换上新的服务器.与文献[7～10]一样,当不断的有服务器作弊时,Mix net 就成了死循环拒绝服务.在具体实现时要采取措施,避免每次盲化解密都有服务器作弊,如加重惩罚等.

Mix net 是解决匿名通信、电子投票选举、电子支付以及电子投标的很好工具,目前已有一些实用的 Mix net 实现,我们的协议在实现时需要设计一个高效安全的 Bulletin board 协议,它直接影响 Mix net 的性能.

参 考 文 献

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

2 Reiter M K, Rubin A D. Crowds: Anonymity for Web Transaction. ACM Transactions on Information and System Security, 1998, 1(1): 66～92

3 Syverson P F, Goldschlag D M, Reed M G. Anonymous connections and onion routing. IEEE Journal of Selected Areas in Commun., 1998, 16(4): 482～494

4 Pfitzmann A, Pfitzmann B. How to break the direct RSA-implementation of mixes. In: Advances in Cryptology——EUROCRYPT'89. Berlin: Springer-Verlag, 1989. 373～381

5 Pfitzmann A, Pfitzmann B, Waidner M. ISDN-mixes: Untraceable communication with very small bandwidth overhead. In: Proceedings of the GI/ITG Conference on Communication in Distributed Systems, Mannheim, Germany, 1991. 451～463

6 Ogata W, Kurosawa K, Sako K, Takatani K. Fault tolerant anonymous channel. In: Proceedings of ICICS'97, LNCS 1334, Berlin: Springer-Verlag, 1997, 440～444

7 Abe M. Universally verifiable mix-net with verification work independent of the number of mix-centers. In: Proceedings of EUROCRYPT' 98, LNCS 1403, Berlin: Springer-Verlag, 1998, 437～447

8 Abe M. A mix-network on permutation networks. In: Proceedings of ASIACRYPT'99, LNCS 1716, Berlin: Springer-Verlag, 1999, 258～273

9 Jakobsson M. A practical mix. In: Proceedings of EUROCRYPT'98, LNCS 1403, Berlin: Springer-Verlag, 1998, 448～461

10 Jakobsson M. Flash mixing. In: Proceedings of PODC'99, ACM, 1999. 83～89

11 Maashi Mitomo, Kaoru Kurosawa. Attack for flash MIX. In: Proceedings of ASIACRYPT2000, LNCS 1976, Berlin: Springer-Verlag, 2000, 192～204

12 Yvo Desmedt, Kaoru Kurosawa. How to break a practical MIX and design a new one. In: Proceedings of EUROCRYPT2000, LNCS 1807, Berlin: Springer-Verlag, 2000, 557～572

GAO Hu-Ming, born in 1963, Ph. D. candidate, associate professor. His main research interests include applied cryptography, E-commerce and network security.

CHEN Xiao-Feng, born in 1976, Ph. D. candidate. His main research interests include elliptic curve cryptography, E-commerce.

WANG Yu-Min, born in 1936, professor, Ph. D. supervisor. His research interests are in the general of communication, information theory, coding and cryptography.