Internet 上的匿名技术研究

陆天波，方滨兴

（中国科学院计算技术研究所软件研究室，北京，100080）

（中国科学院研究生院，北京，100039）

摘 要： 近年来，人们对 Internet 上的隐私和匿名越来越关心，并做了很多工作。本文总结了匿名技术 20 多年来的研究进展情况，并对匿名技术的若干热点研究方向进行了归纳和总结。

关键词： 匿名；Mix；攻击

A Survey of Anonymity on the Internet

Tianbo Lu, Binxing Fang

(Institute of Computing Technology, Chinese Academy of Sciences, Beijing, 100080, China)

(Graduate School of the Chinese Academy of Sciences, Beijing, 100039, China.)

Abstract: The purpose of this article is to give an overview of existing and proposed techniques that can provide anonymity on the Internet, to analyze the current trends and developments in this area, and to propose a research agenda for anonymity systems.

key words: anonymity; Mix; attack

1 引言

近年来，Internet 迅猛发展，给人们的生活带来了极大的方便，但同时又给人们的隐私带来了很大的威胁。Internet 的用户通常并没有意识到他们在电子新闻组中所发的每张帖子，他们所发送的每封邮件，他们所访问的每个网页，以及他们在网上的购买行为等都可能被第三方监视和记录下来，例如美国的 Carnivore 系统和英国的 RIP 法案等。许多商家在收集、利用、出售和泄漏 Internet 用户的个人信息。

Internet 的一个缺陷是不提供匿名保护，攻击者可以根据通信流之间的关系对发送者和接收者进行追踪。随着 Internet 的快速发展并被人们广为接受，以及搜索引擎和数据挖掘等技术的发展，人们已经开始关注 Internet 上的隐私和匿名。隐私不仅意味着信息的机密性，而且意味着信息发布者身份的机密性。匿名技术是 Internet 上保护用户隐私的一种有效手段，它通过一定的方法将通信流中的通信关系加以隐藏，使攻击

基金资助：国家自然科学基金（60273016），国家"八六三"高技术研究发展计划基金（2001AA142110）。

作者简介：陆天波（1977-），男，贵州人，博士研究生，Email: lutianbo@software.ict.ac.cn。

者无法获知双方的通信关系或通信的一方。用户在通信过程中，通过隐藏自己的IP地址来保护自己的隐私。例如，用户访问了某个网站，但是由于用户使用了匿名技术，使得该访问活动无法与用户身份信息（指IP地址）关联起来，这在一定程度上保护了用户的隐私。

匿名技术在军事机构、执法机关、以及情报和反情报机关等安全性要求很高的环境中也有着很重要的用途。例如，在军事上，军事指挥中心和各个部门之间的通信，甚至其通信模式的变化本身已经暗含了很多有用的信息。而一封加密之后的电子邮件，如果它在毒贩和其他尚未被怀疑的人之间，或者国防建设的雇员与敌方大使馆官员之间传递，显然，它包含某种深意。军用通信系统不仅仅是使用加密技术来加密一条消息的内容，还力图隐藏消息的发送者、接收者，甚至是消息本身的存在。同样的技术也使用在移动电话系统、电子货币和电子选举方案中。

加密技术可以保护通信的内容，但是攻击者可以通过通信流分析(Traffic analysis)手段观察出谁和谁在通信，通信的时间以及通信流的多少等。因此，仅靠加密技术并不能保证通信的安全，尤其是在一个大的开放的环境中，保护通信者的身份就显得更加困难。通常，在匿名技术的研究中，通信者的身份是指其IP地址，因此发送者是指发送者的IP地址，同样，接收者是指接收者的IP地址。

2 背景与基本概念

匿名技术的研究可以追溯到1981年，在那一年，Chaum在其开创性的论文中首次提出了Mix的概念[1]。从此，很多研究工作致力于构建、分析和攻击匿名系统。1988年，Chaum根据密码学家就餐问题进一步提出了DC-Net的概念[2]。2000年7月在美国加州召开了以隐私保护为主题的第一届学术会议PET(Workshop on Privacy Enhancing Technologies)，更加促进了匿名技术的发展。

本节我们给出匿名技术的有关概念。首先我们假定发送者Alice通过一个通信网络向接收者Bob发送消息。攻击者Eve的目的是发现谁和谁在通信，通信的模式，或者控制该通信。在匿名技术的研究中，我们通常都假定密码系统是“完善”的，即攻击者不能破译密码系统。因此，通信的内容是不会泄漏通信者的身份信息的。下面给出的定义主要参考了Andreas Pfitzmann等人在文献[3]中给出的有关概念以及ISO/IEC标准[4]。

（1）匿名通信（anonymous communication）：它是研究发送者Alice和接收者Bob之间通信的秘密性。在Alice与Bob的通信中，如果Bob并不知道Alice的身份，并且第三方观察者Eve并不能把Alice和Bob关联起来，则称Alice匿名的与Bob通信。有时允许Bob知道Alice的身份，但Alice和Bob都会对Eve隐藏他们之间的通信。

（2）匿名（anonymity）：是指在一个实体（entity）集合——匿名集中的不可辨认性。匿名集是指执行某个行为（如发送一封电子邮件或者访问某个网站）的可能实体（如用户）的集合，匿名集的概念是研究匿名技术的基础。匿名是借助于其他实体的行为来隐藏自己的行为。

（3）不可关联性（unlinkability）：两个或多个对象（如实体、消息、事件、行为等）之间的不可关联性是指系统中的这些对象，相对于其先验知识（a-priori knowledge）的关联性（linkability）来说，其关联性没有发生变化。

（4）发送者匿名（sender anonymity）：指一个具体的消息不可关联到任何一个发送者，及对于一个具体的发送者来说，消息是不可关联的。

（5）接收者匿名（recipient anonymity）：指一个具体的消息不可关联到任何一个接收者，及对于一个具体的接收者来说，消息是不可关联的。

（6）关系匿名（relationship anonymity）：指不可推测出谁和谁通信，也就是指发送者和接收者之间（广播或组播中指接收者之间）的不可关联性。

3 重要的匿名协议

从 1981 年 Chaum 提出 Mix 的概念算起，匿名技术的发展已经历经 20 余年了。后来的很多工作都是沿着 Mix 的思想和 DC-Net 的思想进行的。我们可以把它们分成五类，分别为中心代理方式，组播（包括广播）方式，随机转发方式，分层加密方式和 P2P 方式。

3.1 代理

提供匿名保护的一种简单常用的方法是使用代理。用户和服务器之间的所有数据都通过一个代理服务器转发。这样，服务器所获知的只是代理服务器的地址。使用代理，发送者对接收者和位于代理和接收者之间的监听者来说是匿名的。基于这种方法的服务主要有 the Anonymizer[5], LPWA[6], Triangle Boy[7]。

这种方法的弱点是：第一，代理必须是可信的，否则，将成为系统的单失效点；第二，当用户和代理之间未使用加密时，它们之间的明文消息本身暴露了目的地址；第三，即使用户和代理之间使用了加密，使用通信流分析方法，如根据数据包的大小，通信的时间等进行分析，也可以很容易的知道目的地址。

3.2 组播

Chaum 于 1988 年提出了一个无条件安全的匿名通信协议 DC-Net[2]，这种机制的提出起源于“用餐的密码学家（Dining Cryptographer）”问题。DC-Net 可以取得发送者匿名和接收者匿名，即使是在计算能力无限的攻击者条件下。然而，Chaum 在 DC-Net 协议的安全性证明中的一个假设是可靠的广播，即每个诚实参与者所广播的消息都被其他参与者未经修改的接收到。Waidner 指出可靠的广播是一种不现实的假设，它不可能通过密码学的手段来获得[8]。

CliqueNet[9]是由 Cornell 大学设计的一个自组织的可扩展 P2P 匿名通信协议。它是对 DC-Net 协议的改进，目的是解决 DC-Net 效率低和可扩展性差的弱点。它采用分治（divide-and-conquer）的思想，把整个 DC-Net 分成多个小的 DC-Net（称为 Cliques）。CliqueNet 采用分治的思想，虽然在一定程度上缓解了广播通信流量大的问题，但是，它的路由层却带来了不必要的网络延迟。当网络规模比较大时，路由转发节点对包的转发量将急剧增加，成为网络的瓶颈。而且，它同样需要可靠的广播。

由 CMU 大学提出的 k-anonymity 协议[10]的思想与 CliqueNet 类似。它同样把整个网络分成许多小的类似于 DC-Net 的单元。每个单元至少有 k 个诚实的用户，这样攻击者最多知道消息的发送者（或接收者）在这 k 个用户中，但并不知道是哪一个。该协议匿名传递一个消息需要传递 $O(k^2)$ 个额外的消息，当 k 较大时，其通信流还是很大。而且它同样需要可靠的广播。

Maryland 大学提出的 P2P 匿名通信协议 P5[11]考虑了用户的匿名性和通信效率之间的平衡，这是它优于 Xor-Tree[12]协议的一个方面。P5 采用分级广播的思想来建立匿名通信网络，然而，它的可扩展性并没有作者所声称的那样好，当用户数很大（大约达到 1 万）时，该协议效率很低。但它的攻击模型却是比较强的。

可以看出，基于组播的匿名协议的匿名性较好，但通信开销很大。而且由于目前的 Internet 并不广泛支持组播（包括广播），因此这类协议并不实用。到目前为止，还没有一个实用的基于这类协议的匿名系统。

3.3 随机转发

由 Bell 实验室开发的 Crowds 系统[13]的目的是为用户提供匿名 Web 浏览。它使得用户能够匿名的从 Web 服务器取回信息而不对服务器和第三方泄漏用户自己的信息，如 IP 地址和域名等。其思想是“混在人群中”，意思是把自己隐藏在群体中。Crowds 把 Web 用户组织成一个称为 crowd 的群体，crowd 代表用户执行 Web 交易。crowd 中的用户用一个驻留在用户机器上的称之为 jondo 的代理表示。用户的请求通过本地的 jondo 随

机的转发给另一个 crowd 成员或者直接提交给终端服务器。当一个 crowd 成员收到另一个 crowd 成员送来的请求时，它会随机选择是把该请求转发给下一个 crowd 成员，还是把该请求提交给终端服务器。这样，Web 服务器和其他的 crowd 成员以及第三方观察者就不能确定该请求是由谁发起的。随后的所有请求及服务器端的应答都是沿着这条路径传递的。Crowds 采用随机转发，没有过多的消息开销，因而其效率高，可扩展性好。但是，Crowds 协议并不能抵御通信流分析，它设计的主要目的是抵制 Web 服务器获得访问者的真实地址，对于拥有监听网络流量能力的攻击者，它并不能维护足够的匿名性。

Purdue 大学提出的 Hordes 协议[14]是对 Crowds 的扩充和改进，克服了 Crowds 不能抵抗回溯攻击(traceback attack)的缺点。Hordes 在 Crowds 的回路阶段采用组播发送应答消息，一方面降低了延迟，但另一方面又降低了带宽利用率。组播在 Internet 上不是一种被广泛支持的技术，要在今天的 Internet 环境中实现 Hordes 将是一件非常困难的事情。

3.4 分层加密

这类协议都是在 Mix[1]的基础上发展而来的。Mix 的基本思想是通过使用中间节点来变换和混杂来自多个用户的消息，使窃听者无法确定输入消息和输出消息的对应关系，从而无法跟踪某条消息的传输路径，发现“谁跟谁通讯”的事实。通常把 Mix 所应用的逐层加密的方法称为分层加密。

Chaum 的论文主要目的是提出一种解决电子邮件匿名性的方法，该方法在当前的匿名电子邮件中得到了很好的应用和发展[15,16]。Mix 被后来的研究者扩展成了一种通用的通信匿名性保护技术，得到了广泛的应用。例如美国海军研究实验室主持的 Onion Routing[17]及 Free Haven 工程组设计开发的新一代 Onion routing 系统 Tor[18]；零知识系统开发的用于隐私保护的 Freedom 系统[19]；德累斯顿匿名社团（Dresden anonymity community）设计的 ISDN mixes[20]，Real Time mixes[21]和 Web mixes[22]；德国学者 Kesdogn 等人提出的 Stop-and-go mixes[23]，以及 MIT 的 Free Haven 项目[24]和 Purdue 大学设计开发的匿名发布系统 GNUnet[25]等。

3.5 P2P 网络

Chaum 在其奠基性工作中指出[1]，如果每个用户都是一个 Mix 节点，则网络的安全性将得到提高。近年来，P2P 技术的发展促使人们研究 P2P Mix 网络。P2P 系统要求每个匿名用户同时也是服务器，为其他用户提供匿名服务。这意味着经过一个节点的消息可能是源于该节点，也可能是源于其他节点，很难决定是这两种情况中的哪一种。P2P 系统的另一个特点是攻击者没有明确的攻击目标，在一个大规模的环境中，任何一次通信都可能包含许多潜在的用户。另外，P2P 系统具有较好的可扩展性和柔性，可以在节点之间进行负载均衡，不存在单失效点等优点。

Tarzan[26]是由 MIT 提出的一个网络层匿名协议，独立于应用层。它使用了掩饰流以抵抗通信流分析。MorphMix[27]是由瑞士联邦学院提出的一个应用层协议，节点间使用了 TCP 机制。它没有采用掩饰流，原因是它认为在一个大的动态环境中，攻击者进行通信流分析的难度很大。

我们所提出的 WonGoo 协议[28-30,49]是一个综合了 Mix[1]和 Crowds[13]的优点的可扩展点对点协议，提供三种形式的匿名保护：发送者匿名，接收者匿名和关系匿名。WonGoo 克服了 Mix 效率低和 Crowds 抗攻击性差的缺点，通过分层加密和随机转发取得了强匿名和高效率。其效率和匿名性介于 Crowds 和 Mix 之间，是两者的折中。

CliqueNet[9]是在 DC-Net 的基础上提出的一个 P2P 协议，其通信开销仍然很大。P5 是一个广播协议[11]。Freenet[31]起源于英国爱丁堡大学教授 Ian Clarke 主持的一个自适应点对点网络的项目，它由分散的多个节点组成，不存在中央服务器的概念。

4 可证明的匿名协议

Chaum 在其奠基性的工作中还建议一个邮件系统应该确保每个 Mix 节点都正确的对消息进行处理[1]。这在分层加密的系统中是很困难的，原因在于对称密钥算法很难分布式的应用，以及在其上进行零知识证明的不现实性。围绕着 Chaum 提出的这一属性，研究者提出了一系列可证明自己行为正确的 Mix 方案，称为重加密 mix 方案。这类方案主要利用了 ElGamal 加密算法可以对消息进行重复加密的性质，被广泛的应用于匿名投票。

Park 和 Itoh 等人[32]于 1993 年指出 Chaum Mix 方案的一个缺点是，密文数据包的大小随 Mix 节点数的增加而增加。为了克服这一问题，他们提出了基于 ElGamal 加密方案的重加密（re-encryption）Mix 协议，其密文数据包的大小与 Mix 节点数无关。Pfitzmann 在 1994 年发现了针对该协议的两个攻击[33]。Sako 和 Killian 在 1995 年提出了一个称为 receipt-free 的投票方案[34]，试图在文献[32]的基础上添加通用的可证明性（universal verifiability）。Michels 和 Horster1996 年发现了对该协议的一个攻击[35]。Ogata 和 Kurosawa 等人于 1997 年第一次提出了两个健壮的可证明的匿名通道方案[36]。一个是基于 r 轮剩余类问题，另一个是基于 ElGamal 方案。他们对前者进行了零知识证明。Abe 和 Jakobsson 于 1998 年分别提出了两个高效实用的可证明 Mix 协议[37,38]。其中后者被 Desmedt 和 Kurosawa 证明是不安全的[39]。为了减少方案[38]中乱序（mixing）的代价，Jakobsson 在 1999 年提出了 Flash Mix[40]。Mitomo 和 Kurosawa 后来发现了针对该方案的一种攻击并对其进行了完善[41]。Furukawa，Sako[42]和 Neff[43]在 2001 年分别提出了对 ElGamal 密文置乱的正确性进行有效证明的方案，但是他们的方案很难扩展到大规模的选举方案中。鉴于此，文献[44]提出了一种优化的 Mix 方案。如果没有检测到攻击，则该方案的效率很高，但是一旦有错误发生，则该方案不输出任何结果。

至今为止，上述协议没有一个得到了实现。其原因在于这类协议中，密钥的产生、分发和维护很复杂。可喜的是 2004 年，哈佛大学的 Golle 提出了一个新的实用的通用重加密方案（URE）[45]，它没有复杂的密钥产生，分发和维护。Fairbrother 对该方案进行了改进以便能高效的传输大文件[46]。Gomukiewicz 等人则对该方案进行了扩充（称为 EURE）并设计了一个新的 Onion Routing 协议[47]。然而，我们发现 URE 和 EURE 这两个方案都会遭受到 Pfitzmann 在 1994 年提出的一种选择密文攻击[33]。而且这两个方案中密文长度都是明文的四倍，而传统的重加密方案才两倍。我们在文献[48]中设计了一个实用的高效的匿名通道 rWonGoo，它采用了重加密和随机转发两种思想，其密文长度仅是明文的两倍。

5 展望

匿名技术发展到今天，虽然取得了一定的成就，但还有很多问题有待解决。首先，虽然基于消息的延迟不敏感系统在技术上已经很完善，但是基于虚电路的延迟敏感系统还很不成熟，需要进一步的发展。尤其是如何抵抗一些常见的攻击，如重放攻击和泄漏攻击等。第二是如何发现一些新的攻击手段，以进一步验证现有的匿名协议的安全性。第三是如何形式化的描述攻击者。对攻击者能力的描述将直接影响到协议的安全性。现有的形式化方法并不能很好的描述针对匿名协议的攻击者。第四是如何评估匿名系统的匿名性。至今为止，还没有一种合适的统一的评估匿名系统的方法，因此，现有的对匿名系统的比较都有很大的局限性。第五是如何对掩饰流的作用进行评价。目前最关键的问题就是不能从理论上说明掩饰流到底能不能提高系统的安全性。最后一点是如何构建类似于 Gnutella 的大规模的 P2P 匿名网络。即如何刺激用户自愿的为别人提供匿名保护，也就是匿名的经济问题。

参考文献：

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

February 1981.

[2] D. Chaum. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Journal of Cryptology, 1(1): 65 - 75, 1988.

[3] Andreas Pfitzmann and Marit Köhntopp. Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology; Draft v0.14. http://www.freehaven.net/anonbib/papers/Anon_Terminology_v0.14.pdf, May 2003.

[4] ISO/IEC 15408-2, 1999. http://csrc.nist.gov/cc/CC-v2.1.html/

[5] Lance Cottrell. The Anonymizer. http://www.anonymizer.com.

[6] E. Gabber et al. Consistent, yet Anonymous, Web Access with LPWA. Communications of the ACM, 42(2): 42-47, 1999.

[7] http://www.safeweb.com

[8] Michael Waidner. Unconditional Sender and Recipient Untraceability in spite of Active Attacks. Eurocrypt '89, LNCS 434, Springer-Verlag, Berlin 1990, 302 - 319.

[9] E. G. Sirer, M. Polte, and M. Robson. CliqueNet: A Self-Organizing, Scalable, Peer-to-Peer Anonymous Communication Substrate. http://www.cs.cornell.edu/People/egs/cliquenet/papers.html

[10] L. Ahn, A. Bortz, and N. J. Hopper. k-Anonymous Message Transmission. *In Proceedings of the 10th ACM conference on Computer and communication security (CCS-03)*, pages 122 – 130, 2003.

[11] R. Sherwood, B. Bhattacharjee, and A. Srinivasan. P5: A Protocol for Scalable Anonymous Communication. *In Proceedings of the 2002 IEEE Symposium on Security and Privacy*, 2002.

[12] S. Dolev and R. Ostrovsky. Xor-Trees for Efficient Anonymous Multicast and Reception. ACM Transactions on Information and System Security, 3(2):63 - 84, May 2000.

[13] M. K. Reiter and A. D. Rubin. Crowds: Anonymity for Web Transactions. ACM Transactions on Information and System Security, 1(1):66–92, November 1998.

[14] C. Shields and B. N. Levine. A Protocol for Anonymous Communication over the Internet. In Proceedings of the ACM Conference on Computer and Communications Security, pages 33 - 42, 2000.

[15] U. Möller, L. Cottrell, P. Palfrader, and L. Sassaman. Mixmaster Protocol—Version 2. Draft, July 2003.

[16] G. Danezis, R. Dingle dine, and N. Mathewson. Mixminion: Design of a Type III Anonymous Remailer Protocol. In Proceedings of the 2003 IEEE Symposium on Security and Privacy, May 2003.

[17] M. Reed, P. Syverson, and D. Goldschlag. Anonymous Connections and Onion Routing. IEEE Journal on Selected Areas in Communications, 16(4): 482–494, May 1998.

[18] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The Second-Generation Onion Router. In Proceedings of the 13th USENIX Security Symposium, August 2004.

[19] P. Boucher, A. Shostack, and I. Goldberg. Freedom Systems 2.0 Architecture. White Paper, http://www.freedom.net/info/whitepapers/Freedom_System_2_Architecture.pdf, 2000.

[20] A. Pfitzmann, B. Pfitzmann, and M. Waidner. ISDN-mixes: Untraceable communication with very small bandwidth overhead. In Proceedings of GI/ITG Conference on Communication in Distributed Systems, pages 451-463. Springer-Verlag, February 1991.

[21] A. Jerichow, J. MÄuller, A. Pfitzmann, B. Pfitzmann, and M. Waidner. Real-Time MIXes: A Bandwidth-Efficient Anonymity Protocol. IEEE Journal on Selected Areas in Communications, 16(4): 495-509, 1998.

[22] O. Berthold, H. Federrath, and S. KÄopsell. Web MIXes: A System for Anonymous and Unobservable Internet Access. In Proceedings of International Workshop on Design Issues in Anonymity and Unobservability, 2009 LNCS. Pages 115-129. Springer-Verlag, 2000.

[23] D. Kesdogan, J. Egner, and R. BÄuschkes. Stop-and-Go MIXes: Providing probabilistic anonymity in an open system. In David Aucsmith, editor, Information Hiding workshop (IH 1998), volume 1525 of LNCS, pages 83-98, April 1998. Springer-Verlag.

[24] http://www.freehaven.net

[25] D. Kügler. An Analysis of GNUnet and the Implications for Anonymous, Censorship-Resistant Networks. In Proceedings of Privacy Enhancing Technologies workshop (PET 2003), March 2003.

[26] M. J. Freedman and R. Morris. Tarzan: A Peer-to-Peer Anonymizing Network Layer. In Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS-02), November, 2002

[27] M. Rennhard and B. Plattner. Introducing MorphMix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection. In Proceedings of the Workshop on Privacy in the Electronic Society, November, 2002.

[28] Tianbo Lu, Binxing Fang, Yuzhong Sun, Xueqi Cheng. WonGoo: A peer-to-peer protocol for anonymous communication. Preceedings of the 2004 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA 2004), pages 1102-1106, June 2004.

[29] Tianbo Lu, Binxing Fang, Yuzhong Sun, Xueqi Cheng. Performance Analysis of WonGoo System. The 5th International Conference on Computer and Information Technology (CIT05). September 2005

[30] Tianbo Lu, Binxing Fang, Yuzhong Sun, Xueqi Cheng, and Li Guo. Building Scale-Free Overlay Mix Networks with Small-World Properties. The 3rd International Conference on Information Technology and Applications (ICITA05), pages 529-534 (Volume II), July 2005.

[31] I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong. Freenet: A Distributed Anonymous Information Storage and Retrieval System. In Proceedings of International Workshop on Design Issues in Anonymity and Unobservability, pages 46-66, July 2000.

[32] C. Park, K. Itoh, and K. Kurosawa. Efficient anonymous channel and all/nothing election scheme. *In Proceedings of Eurocrypt '93*, LNCS 765, Springer-Verlag, pages 248-259, 1994.

[33] B. Pfitzmann. Breaking efficient anonymous channel. In Proceedings of Advances in Cryptology (Eurocrypt'94), volume 950 of LNCS, pages 332-340, May 1994. Springer-Verlag.

[34] K. Sako and J. Kilian. Receipt-free MIX-type voting scheme | a practical solution to the implementation of a voting booth. In Proceedings of Advances in Cryptology (Eurocrypt 1995), volume 921 of LNCS, pages 393-403, May 1995.Springer-Verlag.

[35] M. Michels and P. Horster. Some remarks on a receipt-free and universally verifiable mix-type voting scheme. In Proceedings of Advances in Cryptology (Asiacrypt '96), volume 1163 of LNCS, pages 125-132, November 1996. Springer-Verlag.

[36] W. Ogata, K. Kurosawa, K. Sako, and K. Takatani. Fault tolerant anonymous channel. In Proceedings of ICICS '97, pages 440-444, LNCS 1334, 1997.

[37] M. Abe. Universally verifiable MIX with verification work independent of the number of MIX servers. In Proceedings Advances in Cryptology (Eurocrypt'98), volume 1403 of LNCS, pages 437-447, June 1998. Springer-Verlag.

[38] M. Jakobsson. A practical mix. In Proceedings of Advances in Cryptology - EUROCRYPT '98, volume 1403 of LNCS, pages 448-461, June 1998. Springer-Verlag.

[39] Y. Desmedt and K. Kurosawa. How to break a practical mix and design a new one. In Proceedings of Advances in Cryptology (Eurocrypt 2000), volume 1807 of LNCS, pages 557-572, May 2000. Springer-Verlag.

[40] M. Jakobsson. Flash Mixing. In Principles of Distributed Computing - PODC '99. ACM Press, 1999.

[41] M. Mitomo and K. Kurosawa. Attack for flash MIX. In Proceedings of Advances in Cryptology (Asiacrypt 2000), volume 1976 of LNCS, pages 192-204, December 2000. Springer-Verlag.

[42] J. Furukawa and K. Sako. An Efficient Scheme for Proving a Shuffle. In Proceedings of Crypto '01, pages 368-387, 2001.

[43] A. Neff, A verifiable secret shuffle and its application to e-voting. In Proceedings of ACM CCS '01, pages 116-125, 2001.

[44] P. Golle, S. Zhong, D. Boneh, M. Jakobsson, and A. Juels. Optimistic mixing for exit-polls. In Proceedings of Advances in Cryptology (Asiacrypt 2002), volume 2501 of LNCS, pages 451-465, December 2002. Springer-Verlag.

[45] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal Re-encryption for Mixnets. In Proceedings of RSA-Conference, Cryptographers' Track, pages 163-178, 2004.

[46] P. Fairbrother. An Improved Construction for Universal Re-encryption. Proceedings of Privacy Enhancing Technologies, 2004.

[47] M. Gomulkiewicz, M. Klonowski, and M. Kutylowski. Onions Based on Universal Re-Encryption – Anonymous Communication Immune Against Repetitive Attack. In Proceedings of Workshop on Information Security Applications, 2004.

[48] Tianbo Lu, Binxing Fang, Yuzhong Sun, Li Guo. Some Remarks on Universal Re-encryption and A Novel Practical Anonymous Tunnel. The 2005 International Conference on Computer Networks and Mobile Computing (ICCNMC05), volume 3619 of LNCS, pages 853-862, August 2005. Springer-Verlag.

[49] 陆天波，方滨兴，孙毓忠，郭丽. 匿名协议 WonGoo 的概率模型验证分析，小型微型机算机系统，已录用。