

P2P 中基于无证书的认证及密钥协商协议

冯新泉, 黎忠文

(厦门大学 信息科学与技术学院, 福建 厦门 361005)

摘要:目前 P2P 网络得到了迅猛发展, 但由于其本身的结构特点使之面临很多的安全问题。网络安全极大地阻碍了 P2P 系统的发展。文中在比较传统公钥基础设施(PKI), 基于身份的公钥密码系统(ID-PKC)和无证书公钥密码系统(CL-PKC)各自优缺点的基础上, 提出了混合 P2P 中一种基于 CL-PKC 的域内和跨域双向认证和密钥协商协议, 并进行了安全性分析。本方案克服了 P2P 网络中 PKI 繁琐的证书管理和 ID-PKC 的密钥托管等问题, 提高了双向认证和密钥协商的速度, 具有较高的效率, 能较好地解决混合 P2P 网络的安全问题。

关键词: P2P; CL-PKC; 双向认证; 密钥协商协议

中图分类号: TP393.08

文献标识码: A

文章编号: 1673-629X(2009)02-0165-04

Authenticated and Key Agreement Protocols Based on Certificateless in P2P Network

FENG Xin-quan, LI Zhong-wen

(School of Info. Sci. & Tech., Xiamen University, Xiamen 361005, China)

Abstract: Now P2P network has been rapidly developed, but it faces a lot of security problems because of the structural characteristics. Network security has greatly hampered the development of P2P systems. Based on the respective analysis of the advantages and disadvantages of the traditional public key infrastructure(PKI), identity-based cryptography(ID-PKC) and certificateless public key cryptography(CL-PKC), proposes one kind of bidirectional authenticated and key agreement protocols in one domain and across multiple domains based on CL-PKC for hybrid P2P network. At last analyses its security. The scheme overcomes the problem of complicated management of PKI certificates and the key escrow of ID-PKC in P2P network. It speeds up the time of bidirectional authenticated and key agreement protocols, proved to be more efficient, and can better solve the security problems in hybrid P2P network.

Key words: P2P; CL-PKC; bidirectional authentication; key agreement protocols

0 引言

自 1998 以来, P2P 网络得到了迅猛发展。P2P 系统消除了传统 C/S 模式下服务器的单点失败和可扩展性差等问题, 目前已广泛应用于对等协作、资源共享、知识管理等领域, 拥有良好的发展前景。但是由于 P2P 系统的开放性和匿名性, 恶意用户可以散布虚假、伪劣, 甚至是恶意的内容和服务^[1], 如 VBS、Gnutella 蠕虫病毒, 女巫攻击, “freeriding”现象^[2,3]等, 这些问题极大地阻碍了 P2P 系统的应用, 因而研究高效可行

的安全签名认证及其密钥协商协议成为当前 P2P 研究热点之一。

现有在 P2P 网络中的签名认证^[4-8]和密钥协商协议^[9-13]绝大部分都是基于非对称密码技术的公钥基础设施(PKI)^[4,5]或者是基于身份加密(IDE)^[9-11]来实现的。PKI 中的认证、数据的机密性、完整性和不可抵赖性等机制虽然在 P2P 网络中是适用的, 但传统 PKI 证书管理的过程需要很大的计算量和很强的存储能力, 如证书的撤销、更新、存储、分发以及验证等。此外, 静态的集中化控制和固定的证书内容是传统 PKI 固有的不足。这些问题妨碍了 PKI 在 P2P 环境实施的高效性。基于身份的公钥密码系统(ID-PKC)提供用户方便的验证签名的机制, 不需要交换公钥和私钥, 不需要管理证书。因此, 在密钥协商协议、加密、签名和认证等场合得到广泛的应用^[9-11]。ID-PKC 存在一个私钥生成器(KGC), 由 KGC 的主密钥和用户身份信息生成用户私钥。公钥是从用户的身份信息中导

收稿日期: 2008-06-12

基金项目: 福建省自然科学基金项目(A0410004); 厦门大学院士基金(0630-E23011); 厦门大学新世纪优秀人才支持基金(0000-X07116)

作者简介: 冯新泉(1978-), 男, 福建三明人, 硕士研究生, 研究方向为网络安全; 黎忠文, 博士, 教授, CCF 会员, 研究方向为实时系统高安全和高可靠技术。

出(通常是用户身份信息的哈希值)。ID-PKC 存在的主要缺点如下:

(1)固有的密钥托管性质。KGC 知道所有用户的私钥,可以解密任何用户的信息,可以伪造任何实体的签名。

(2)KGC 必须通过安全的信道发放用户私钥,使得私钥的发放比较困难。

(3)KGC 的主密钥是 ID-PKC 系统的薄弱点。一个有能力获取 KGC 主密钥的敌人可以伪装成任意实体威胁系统的安全。

(4)ID-PKC 一般适用于小的群体或者关系密切的环境而不是大的结构。

无证书的公钥密码体制(CL-PKC)^[7,8,12~16],最早由 Sattam S. Al-Riyami 和 Kenneth G. Paterson 在文献[12]中提出。此后,文献[17]又对文献[12]中的方案进行了改进,提出了一个新的基于双线性 Diffie-Hellman(BDHP)的 CL-PKE 方案。Tarjei K. Mandt 在文献[9]、文献[12]和文献[17]的基础上,提出了无证书认证的双方密钥协商协议^[13],它不仅解决了 PKI 和 ID-PKC 存在的问题,又兼具有它们各自的优点,提高了运行的效率和安全性,并且允许在不同域中的用户快速有效地建立一个共享密钥。文中把基于 CL-PKC 的签名作为身份认证加入到文献[13]的双方密钥协商协议,提出了在混合 P2P 网络中建立基于 CL-PKC 的双向认证和密钥协商协议。此协议能有效地解决 P2P 网络中的安全问题,并且消除了传统 PKI 繁杂的证书管理、ID-PKC 的密钥托管等问题,减少了通信次数,从而提高双向认证的速度和运行的效率。

1 基于 CL-PKC 的双向认证及密钥协商协议

1.1 CL-PKC 的基本概念

CL-PKC 不需要使用证书来保证公钥的可靠性,但依赖于一个拥有主密钥的可信机构,称为私钥生成中心(KGC)。KGC 不直接生成用户的私钥,它只产生与用户身份对应的部分私钥,并将其安全地传送给用户。然后由用户自己把部分私钥和一些秘密信息值结合从而获得实际的密钥。用户的公钥是用户利用 KGC 的公开参数和他本身的秘密值产生的。由于不需使用任何证书,与基于证书的认证相比节省了开销,同时也避免了基于身份认证中固有的密钥托管问题。

1.2 CL-PKC 的具体实现

现有无证书加密的方案是基于双线性对的,具体的 CL-PKC 的签名认证方案如下:

1)Setup: KGC 初始化系统参数:

(1)选取加法群 G_1 和乘法群 G_2 , 满足 $|G_1| = |G_2| = p$, p 为素数;

(2)选取双线性对 $\hat{e}: G_1 \times G_1 \rightarrow G_2$;

(3)选取安全的 Hash 函数 $H_1: \{0,1\}^* \rightarrow G_1, H_2: G_2 \rightarrow \{0,1\}^n$;

(4)选择系统主私钥 $s \in Z_q^*, P \in G_1$, 系统公钥 $P_0 = sP$;

系统公开参数为: $\{G_1, G_2, \hat{e}, n, P, P_0, H_1, H_2\}$, 主密钥 $s \in Z_q^*$ 。

2)Set-Secret-Value: 节点 ID_A 选择一个秘密值 $\chi_A \in Z_q^*$;

3)Set-Public-Key: 计算公钥 $P_A = \chi_A P$, 并公布 P_A ;

4)Partial-Private-Key-Extract: KGC 根据公钥 P_A 和 ID_A 计算 $Q_A = H_1(ID_A, P_A) \in G_1^*, D_A = sQ_A \in G_1^*$, 节点能够通过计算 $\hat{e}(D_A, P) = \hat{e}(Q_A, P_0)$ 来验证其正确性;

5)Set-Private-Key: 节点在得到部分私钥 D_A , 并通过 $\hat{e}(D_A, P) = \hat{e}(Q_A, P_0)$ 验证后, 计算私钥 $S_A = \langle D_A, \chi_A \rangle$;

6)签名: 一个节点 B 使用 S_B 对 T_B (随机数) 进行签名, 具体经过以下步骤:

(1)要先随机生成 T_B , 计算 $f = H(T_B)$ 得到文件摘要 f ;

(2)使用 S_B 对 f 进行加密, 形成数字签名 $\text{Sign}(T_B)$;

(3)将 $C = (T_B, P_B, \text{Sign}(T_B))$ 一并发送给 A 。

7)验证: 节点 A 对 $C = (T_B, P_B, \text{Sign}(T_B))$ 进行认证:

(1)检验 P_B 是否属于 G_1^* ;

(2)计算 $f_1 = H(T_B)$, 并用 B 的公钥 P_B 对数字签名 $\text{Sign}(T_B)$ 进行解密, 得到 f_2 ;

(3)验证 $f_1 = f_2$ 是否成立, 如果成立则表示通过认证, 不成立则认证失败。

1.3 混合 P2P 中基于 CL-PKC 的域内双向认证和密钥协商协议

在混合 P2P 网络中, 首先对新加入 P2P 网络中的节点 A , 通过 KGC 注册来产生公钥 $P_A =$ 和私钥 S_A 。当节点通过 KGC 成功注册后, 以后再跟其他节点进行通信时, 就不需要再经过 KGC, 而只要直接跟通信的节点进行双向认证和协商共享密钥即可。

通过改进文献[13]的无证书认证的双方密钥协商协议, 并应用在混合 P2P 网络中, 这样可以有效地提高 P2P 网络的安全性。具体协议如下: 如果同一个域中

两个节点 A, B 想要进行双向认证,从而相互通信,节点 A 首先选择一个随机数 $a \in \mathbb{Z}_q^*$, 计算 $T_A = aP$, 并用私钥 S_A 对 T_A 进行签名 $\text{Sign}(T_A)$ 。节点 A 再把 $\langle T_A, P_A, \text{Sign}(T_A) \rangle$ 发送给 B 。节点 B 首先检查对方公钥的正确性,如果不正确,则拒绝;否则,使用 T_A 和 P_A 对 A 的签名 $\text{Sign}(T_A)$ 进行验证 $\text{Verify}(T_A)$, 如果验证不通过,则停止通信;否则,节点 B 也同样选择一个随机数 $b \in \mathbb{Z}_q^*$, 并且计算 $T_B = bP$, 使用私钥 S_B 对 T_B 进行签名 $\text{Sign}(T_B)$, B 把确认消息 $\langle T_B, P_B, \text{Sign}(T_B) \rangle$ 返回给 A 。 A 收到此确认消息后,首先检测 P_B 的正确性,如果不正确,则停止与 B 节点的通信;否则,使用 T_B 和 P_B 对 B 的签名 $\text{Sign}(T_B)$ 进行验证,如果验证失败,则停止通信。这样节点 A 和 B 就完成了双向的身份认证。在不需要再次通信交换参数的同时,就可以分别计算出 $K_A = \hat{e}(Q_B, P_0 + P_B)^a \cdot \hat{e}(S'_A, T_B)$, $K_B = \hat{e}(S'_B, T_A) \cdot \hat{e}(Q_A, P_0 + P_A)^b$, $K = K_A = K_B = \hat{e}(Q_B, P)^{a(s+\chi_B)} \cdot \hat{e}(Q_A, P)^{b(s+\chi_A)}$, 这样节点 A 和节点 B 就可以通过计算, $FK = H_2(K \parallel abP \parallel \chi_A \chi_B P)$, 得出双向协商的共享密钥 FK 。节点 A 和节点 B 就可以通过双方共享密钥 FK 进行安全的数据传输。此双向认证和密钥协商协议具体如图 1 所示。

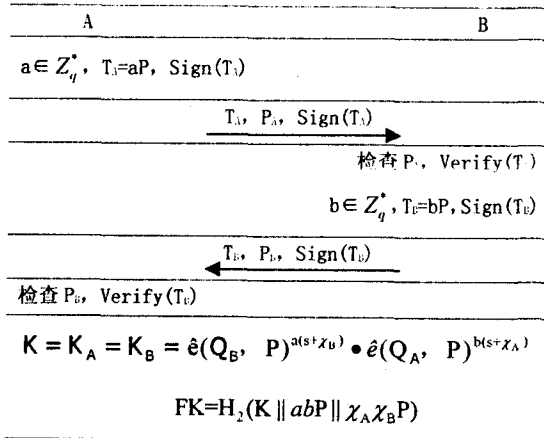


图1 双向认证及密钥协商协议

在混合 P2P 网络中,由每个域中的 KGC 对域中所有节点的状态进行维护。如节点被清除后, KGC 将删除其公钥和相关的参数,并公告整个域中的节点,被清除的节点将不能再与此域中的其他节点进行通信。

1.4 混合 P2P 中基于 CL-PKC 的跨域双向认证和密钥协商协议

假如有两个不同的域,如图 2 所示。

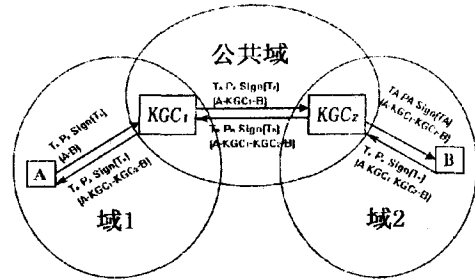


图2 基于 CL-PKC 跨域的双向认证和密钥协商协议

域 1 中有节点 A 和 KGC_1 , 域 2 中有 KGC_2 和节点 B , $s_1, s_2 \in \mathbb{Z}_q^*$ 分别为 KGC_1, KGC_2 的主密钥。则 KGC_1, KGC_2 的系统公钥分别为 s_1P, s_2P , P 为公共参数。则此跨域的双向认证和密钥协商协议具体如图 3 所示。

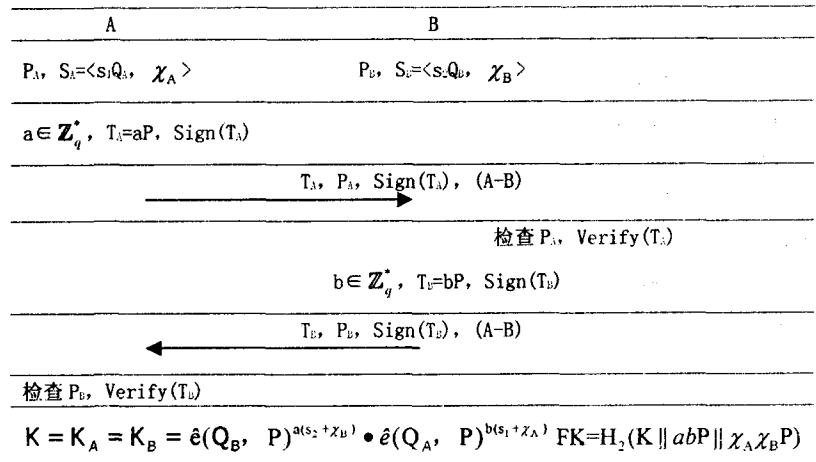


图3 跨域的双向认证和密钥协商协议

节点 A 想和不同域中的节点 B 通信,经过系统参数初始化后, A 把认证和密钥协商的参数信息 $\langle T_A, P_A, \text{Sign}(T_A) \rangle$ 和链路消息 $(A-B)$ 发送给 KGC_1 。 KGC_1 收到后,对 A 公钥和签名进行检查以防恶意节点。如果检查通过后, KGC_1 修改链路信息 $(A-KGC_1-B)$, 并向公共域中其他 KGC 发送 $\langle T_A, P_A, \text{Sign}(T_A) \rangle$ 和 $(A-KGC_1-B)$, KGC_2 对 A 的签名 $\text{Sign}(T_A)$ 用 P_A 进行验证,验证通过后, KGC_2 修改 $(A-KGC_1-KGC_2-B)$, 再把 $\langle T_A, P_A, \text{Sign}(T_A) \rangle$ 和 $(A-KGC_1-KGC_2-B)$ 发给节点 B , B 同样要对 A 的签名 $\text{Sign}(T_A)$ 用 P_A 进行验证,验证通过后,节点 B 初始化参数 $T_B, \text{Sign}(T_B)$, 再把 $\langle T_B, P_B, \text{Sign}(T_B) \rangle$ 按照链路 $(A-KGC_1-KGC_2)$ 逐个反向地发送给 KGC_2 , KGC_1, A 。最终节点 A, B 实现了双向的身份认证,并在不需要额外通信的同时,分别计算 $K_A = \hat{e}(Q_B, s_2P + P_B)^a \cdot \hat{e}((s_1 + \chi_A)Q_A, T_B)$, $K_B = \hat{e}(Q_A, s_1P + P_A)^b \cdot \hat{e}((s_2 + \chi_B)Q_B, T_A)$, 就得出, $K = K_A = K_B = \hat{e}(Q_B, P)^{a(s_2+\chi_B)} \cdot \hat{e}(Q_A, P)^{b(s_1+\chi_A)}$, 这样, A, B 就通过

$FK = H_2(K \parallel abP \parallel \chi_A \chi_B P)$, 得出双方协商的共享密钥 FK。在不同域中的节点 A、B 就完成了双向认证和密钥协商协议, 双方可以通过 FK 进行安全的数据传输。

1.5 协议的安全性分析

基于 CL-PKC 双向认证和密钥协商协议不仅可以抵抗被动攻击, 同时因为采用基于签名的双向认证, 所以也能抵抗主动攻击。此协议具有在文献[13]中 L. Law 等定义的五个性质:

1) 前向保密性(Forward secrecy)。由于双方共享密钥 FK, 其中 K 为临时的会话密钥, a 、 b 为节点生产的随机数, 所以每次会话双方共享密钥都不同, 这样即使节点某时刻把 FK 泄漏了, 也不会导致旧的共享密钥泄漏。

2) 已知会话密钥的安全性(Known session key security)。每执行一次协议, 每个节点都会生成一个唯一的共享会话密钥。因此一次会话密钥的泄漏不会导致其他时间段该协议运行生成的会话密钥泄露。

3) 未知密钥共享安全性(Unknown key share)。由于通信的双方在生成共享密钥之前, 都要对对方的公钥和签名进行检查, 这样保证了通信双方不被第三方冒充。

4) 密钥泄漏安全性(Key-compromise impersonation)。假如协议中节点 A 的私钥 S_A 泄漏, 攻击者又截获了节点 B 的 T_B , 然后把假的 T_B' 传给 A, 但是由于不知道临时的 a 和 B 的私钥 S_B , 所以攻击者仍然不能计算出 K_A 或 K_B 。

5) 密钥控制安全性(key control)。密钥的产生是由双方共同建立的, 双方都要给出临时的 a 、 b 来计算 $T_A = aP$, $T_B = bP$, 最终计算唯一的会话密钥 FK, 所以任何一方都不能事先决定会话密钥的建立。

2 结束语

P2P 网络中节点管理和访问控制存在许多安全和效率问题。针对这些问题, 提出了混合 P2P 网络域内和域间基于 CL-PKC 的双向认证和密钥协商协议, 并进行了安全性分析。解决了在 P2P 网络中双向实体认证效率过低, PKI 系统建设和维护成本太高, ID-PKC 密钥托管问题等不足, 具有较高的效率和安全性。

今后将在此基础上研究基于 CL-PKC 的信誉的访问控制模型, 这样就可以在混合 P2P 中建立一整套基于 CL-PKC 的访问控制机制, 从而实现基于双向认证、密钥协商、信任策略的授权机制和访问控制策略。

参考文献:

- [1] Divac-Krnic L, Ackermann R. Secure-related issues in peer-to-peer networks[M]//In: P2P Systems and Applications, Lecture Notes on Computer Science 3485. Berlin: Springer-Verlag, 2005: 529-545.
- [2] Dinger J, Hartenstein H. Defending the Sybil Attack in P2P Networks: Taxonomy, Challenges, and a Proposal for Self-Registration[C]//Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06). [s.l.]: IEEE Computer Society Press, 2006.
- [3] 王鹏, 王琳, 祝跃飞. 在 P2P 网络下 Sybil 攻击的研究与防范[J]. 微电子学与计算机, 2006, 23(4): 162-165.
- [4] 赵翠华. 基于 PKI 的 P2P 信任授权问题研究[D]. 西安: 西安电子科技大学, 2006.
- [5] 李芸波. P2P 下认证授权体系的研究[D]. 昆明: 昆明理工大学, 2007.
- [6] 孙鹏, 黄鑫, 庄雷. 认证技术在 P2P 网络中的应用研究[J]. 计算机应用与软件, 2005, 22(6): 115-118.
- [7] Gorantla M C, Saxena A. An Efficient Certificateless Signature Scheme[C]//In: Advances in Computer Science - ASIAN 2006, Lecture Notes in Computer Science 4435, 2008, 37-44. Proc of CIS'05. Berlin: Springer-Verlag, 2005: 110-116.
- [8] Wang Changji, Huang Hui. An Efficient Certificateless Signature from Pairings[C]//In: Data, Privacy, and E-Commerce, 2007. ISDPE 2007. [s.l.]: IEEE Computer Society, 2007: 236-238.
- [9] Chen L, Kudla C. Identity Based Authenticated Key Agreement Protocols from Pairings[C]//In Proc. 16th IEEE Security Foundations Workshop. [s.l.]: IEEE Computer Society Press, 2003: 219-233.
- [10] Xie G. An ID-based key agreement scheme from pairing. Cryptology ePrint Archive, Report 2005/093[EB/OL]. 2005. <http://eprint.iacr.org/2005/093>.
- [11] McCullagh N, Barreto P S L M. A new two-party identity-based authenticated key agreement[C]//In Menezes A J. Cryptographers' Track at RSA Conference - CT-RSA 2005, volume 3376 of Lecture Notes in Computer Science. [s.l.]: Springer-Verlag, 2005: 262-274.
- [12] Al-Riyami S S, Paterson K. Certificateless Public Key Cryptography[C]//In Lai C S. Advances in Cryptology - Asiacrypt 2003, volume 2894 of Lecture Notes in Computer Science. [s.l.]: Springer-Verlag, 2003: 452-473.
- [13] Mandt T K. Certificateless Authenticated Two-Party Key Agreement Protocols[M]. [s.l.]: Gjøvik University, 2006.
- [14] 肖自碧, 杨波, 温巧燕. 发展安全的公钥密码系统的新方法研究[J]. 计算机应用, 2007, 24(10): 5-8.
- [15] Al-Riyami S S, Paterson K G. CBE from CL-PKE: A Generic Construction and Efficient Schemes[C]//Proceedings

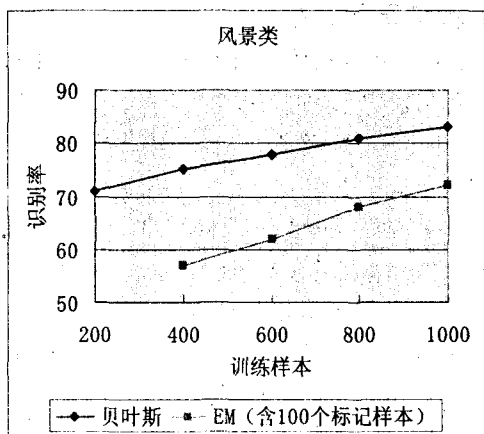


图3 F5测试结果(b)

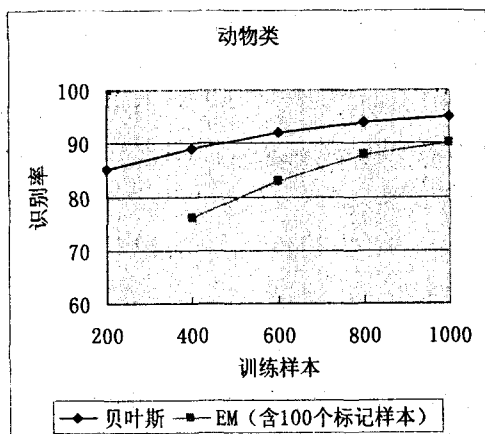


图4 Outguess测试结果(a)

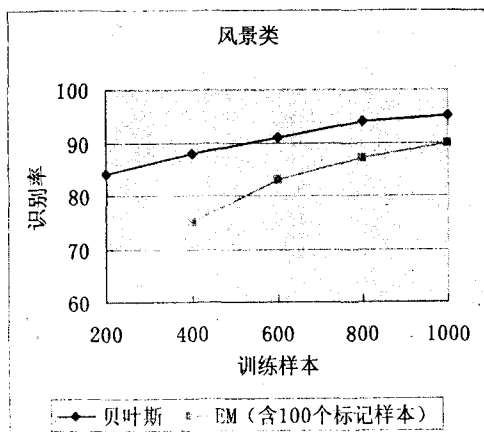


图5 Outguess测试结果(b)

JPEG 图像隐写分析中的分类器设计。该方法在缺少大量标记样本的情况下,通过有效地利用未标记样本,在一定程度上提高分类性能,也更符合实际情况。

(上接第168页)

of PKC 2005 (LNCS 3386), Jan 23 - 26, 2005, Les Diablerets, Switzerland. Berlin, Germany: Springer - Verlag, 2005:398 - 415.

[16] Shi Y, Li J. Provable efficient certificateless public key encryp-

参考文献:

- [1] Avci I, Memon N, Sankur B. Steganalysis using image quality metrics[J]. IEEE Trans on Image Processing, 2003, 12(2):221 - 229.
- [2] Farid H. Detecting hidden message using higher - order statistical models[C]// In Proc. IEEE Int. Conf. on Image Processing. New York: [s. n.], 2002:905 - 908.
- [3] Fridrich J. Feature - based steganalysis for JPEG images and its implications for future design of steganographic schemes [C]// In: 6th International Hiding Workshop. Toronto, Ontario, Canada: Springer - Verlag, 2005:67 - 81.
- [4] 黄 聪, 宣国荣, 高建炯, 等. 基于 DCT 域共生矩阵的 JPEG 图像隐写分析[J]. 计算机应用, 2006, 26(12):2863 - 2865.
- [5] Nigam K, McCallum A. Text Classification from Labeled and Unlabeled Documents using EM[J]. Machine Learning, 2000, 39(2):103 - 134.
- [6] Zhou Y, Goldman S. Democratic co - learning[C]// In: Proceedings of the 16th IEEE International Conference on Tools with Artificial Intelligence (ICTAI'04). Boca Raton, FL: [s. n.], 2004:594 - 602.
- [7] Zhou Z - H. Learning with unlabeled data and its application to image retrieval[C]// In: Proceedings of the 9th Pacific Rim International Conference on Artificial Intelligence (PRICAI'06). Guilin, China: [s. n.], 2006:5 - 10.
- [8] Hsu C T, Wu J L. Hidden Digital Watermarks in Images[J]. IEEE Trans. On Image Processing, 1999, 8:58 - 68.
- [9] Westfeld A. F5 a steganographic algorithm: High capacity despite better steganalysis[C]// In: 4th International Workshop on Information Hiding. Pittsburgh, PA, USA: [s. n.], 2001:289 - 302.
- [10] Provos N. Defending against statistical steganalysis[C]// In: 10th USENIX Security Symposium. Washington DC, USA: [s. n.], 2001:323 - 336.
- [11] Miller D J, Uyar H S. A mixture of experts classifier with learning based on both labelled and unlabelled data[C]// In: Mozer M, Jordan M I, Petsche T, eds. Advances in Neural Information Processing Systems 9. Cambridge, MA: MIT Press, 1997:571 - 577.
- [12] Dempster P, Laird N M, Rubin D B. Maximum likelihood from incomplete data via the EM algorithm[J]. Royal Stat. Soc., 1977, 39(1):1 - 38.

tion. Cryptology ePrint Archive, Report 2005/287[EB/OL]. 2005. <http://eprint.iacr.org/2005/287>.

- [17] Cheng Z H, Comley R. Efficient Certificateless Public Key Encryption. Cryptology ePrint Archive, Report 2005/012, 2005 [EB/OL]. 2005 - 12. <http://eprint.iacr.org/2005/012/>.