基于属性加密的隐藏证书扩展模型

葛维进 程 权 胡晓惠 詹芊芊
(中国科学院软件研究所 北京 100190)

摘 要 当前基于身份加密体系的隐藏证书无法实现一对多的信息传输,对身份信息不具备容错功能,且密文容易被共谋破解,这些缺点导致其在实际应用中受到诸多限制。提出了基于属性加密的隐藏证书扩展模型,解决了原隐藏证书技术存在的上述问题,并在信任协商过程中保留了隐藏证书技术对于证书、资源和策略的隐藏和保护功能。在扩展模型中加密和解密都是基于属性集合的,因此提升了交互双方的信息安全级别。另外,通过对属性集证书发放过程的随机性控制,消除了共谋破解的可能。同时,分析了该扩展模型的性能、安全性和应用场景等,最后指出了今后的研究方向。

关键词 基于属性加密,隐藏证书,信任协商,共谋破解
中图法分类号 TP393.0,N945.23 **文献标识码** A

Attribute Encryption Based Hidden Credentials Extended Model

GE Wei-jin CHENG Quan HU Xiao-hui Zhan Qian-qian
(Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

Abstract The current identity-based encryption based hidden credential can not support 1-N communication, endures no identity fuzzy and lefts open to conspiracy crack, which brings great limitation to its availability. In this paper, an attribute-based encryption based hidden credentials extended model was presented which solves those dilemmas of basic hidden credential system, meanwhile, the extended model keeps the advantages in protecting all the certificates, resources and strategies safe in trust negotiation. Since in ABE system, each participant has and only has one attribute-set certificate, the extended model significantly improves the efficiency of decryption process. On the other hand, through the random control in certificate issue process, the possibility of conspiracy crack is also eliminated. In addition, we described their performance, security and applications in detail. Finally, the farther research directions were suggested.

Keywords Attribute-based encryption, Hidden credentials, Trust negotiation, Conspiracy crack

1 引言

Winsborough 等人在 2000 年提出了自动信任协商(automated trust negotiation, ATN)的概念,它"通过信任证、访问控制策略的交互披露,资源的请求方和提供方自动地建立信任关系"[1-3]。在 ATN 体系里,为解决访问控制中对敏感属性和敏感策略的保护问题,最初由 Holt 等人在 2003 年基于身份标识的加密算法(Identity Based Encryption, IBE)[4]提出了隐藏证书的概念[5];Bradshaw 等人提出了使用隐藏证书(Hidden Credential)来隐藏复杂策略的解决方案[6]。Frikken 等人继而提出了使用隐藏证书来保护访问控制策略[7]。隐藏证书实现了对敏感的请求、资源、证书以及策略的保护,具有单轮回证书交换、低网络开销等优点,大大提高了信任协商的效率。但现有的隐藏证书技术在下列方面存在明显缺点:

1)在开放的环境如 Internet 中,与陌生方进行合作时(如准许对于资源的访问),经常是基于请求方的一些模糊的特性集合,而不是基于请求方的明确身份;IBE 技术无法支持针对模糊特性的加解密,从而导致现有的隐藏证书技术在加密时,需要基于明确的接收方身份特征。

2)由于在加密时就需要明确规定接收方的身份特征,因此现有的隐藏证书技术无法支持一对多的信息交互,只能支持一对一的信息交互,也就是只支持双方信任协商,无法支持多方信任协商。

3)由于 IBE 体系中,每个身份特征都对应一个特征证书,导致接收方在解密时,存在特征证书组合爆炸的问题,大大降低了解密的效率。

4)每个用户持有多个特征证书,给共谋破解提供了有利之机。互不相关的两个参与方 B 和 C,可能共享他们的某些特征证书,从而"制造"出一个实际上并不存在的虚拟人员 D,D 可能实现对发送方密文的破解。

本文提出了基于属性加密(Attribute Based Encryption)的隐藏证书扩展模型,与现有的基于 IBE 的隐藏证书相比,新模型支持模糊属性匹配、多方信任协商($1-N$),并大幅提高了解密的效率,同时根除了共谋破解的可能性。

2 基于属性加密的隐藏证书扩展模型

2.1 相关技术研究现状

A. Sahai 和 B. Waters 等在 2005 年提出了基于属性加密

到稿日期:2010-08-19 返修日期:2010-11-09 本文受国防预研项目"网络互操作技术体制与平台研究"资助。
葛维进(1976—),男,博士,高级工程师,主要研究方向为综合信息系统集成及访问控制,E-mail:weijin_ge@hotmail.com。

的概念[8]。在他们构造的基于模糊身份的加密系统中，由一系列描述用户特性的属性构成一个模糊的身份，用于加密信息；用户的解密密钥由一系列的密钥组件构成，每一个密钥组件对应一个身份中的属性。一个拥有身份 ω 的密钥的用户能够解密用公钥 ω' 加密的密文，当且仅当集合 ω 和 ω' 有一定的重叠，即它允许加密信息的公钥和接收方的身份之间有一定的差别。图 1 示出基于模糊身份加密的过程。

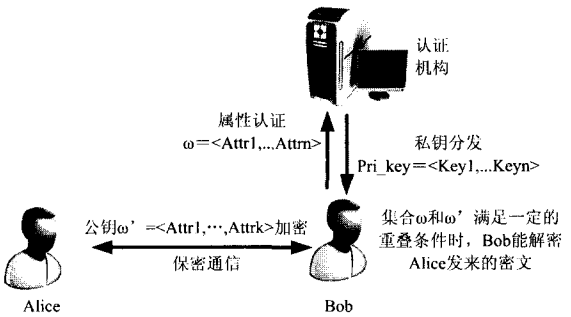

图 1　基于模糊身份加密的过程

基于模糊身份加密有两个主要的应用：

1)基于生物特征加密

使用若干属性来描述用户的生物特征，然后使用生物特征作为身份来加密信息。因为生物特征的测量是有干扰和误差的，所以不能采用先前的 IBE 系统。而文献[8]的系统具有一定容错能力，能够在用同一个生物特征加密但测量时有轻微误差的情况下解密密文。

2)基于属性加密 ABE

在这类应用中，用户希望能给拥有一系列确定属性的所有用户传送加密信息，即一对多的传输。信息发送者指定一个属性集合，只有拥有了指定属性集合中至少 d 个属性的用户才能解密信息。接收者收到消息后，向认证机构证明他拥有指定的属性，然后认证机构给他发放这些属性的密钥组件，构成解密密钥，接收者收到密钥后解密信息。例如，在一个计算机科学部门，主任希望给委员会的所有成员发送加密信息，则使用{"计算机科学部门","委员会成员"}作为身份来加密文件。任何一个包含以上属性的用户都能解密该信息。

在 A. Sahai 和 B. Waters 提出的原始 ABE 构造中，认证机构发放的密钥只能用门限来表示访问策略，即用户拥有密文中指定属性中的一定数量的属性就能解密密文。Goyal 等人在 2006 年提出了一个改进的 ABE 方案[9]，其中密钥能表示任何由"与"、"或"逻辑和门限表示的单调的访问规则。为了抵抗共谋攻击，即多个用户通过组合他们的密钥来解密密文，每个属性认证机构都有一个伪随机函数 PRF 用于随机化发放密钥。通过这种方式，从根本上消除了共谋破解的可能性。

2.2　模型架构和协议

2.2.1　扩展模型的体系架构

在基于 ABE 的隐藏证书扩展模型中，认证机构用于发放证书，用户的证书就是用户的解密密钥。每个用户有且仅有一个证书，即解密密钥。该证书由一系列证书组件(证书组件就是密钥片段)构成，每一个证书组件对应用户的一个属性，所以我们可以将这种证书称为属性集证书。在进行信任协商时，发送方基于自身的保密要求，选择确定接收方的属性集合 A_c 来加密信息。如果接收方的属性集证书 A_u 与加密信息时要求的属性集合 A_c 存在指定精度的匹配，接收方即能成功解密并获得信息。基于 ABE 的隐藏证书扩展模型的体系架构如图 2 所示。

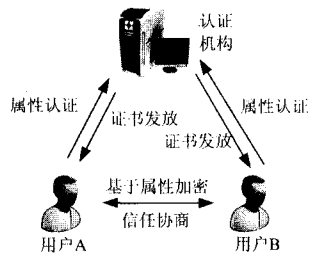

图 2　基于 ABE 的隐藏证书体系架构图

由图 2 可知，本文提出的基于 ABE 的隐藏证书扩展模型是基于单认证机构的，在开始信任协商前，用户 A 和用户 B 分别用其各自的全局身份 GID，向认证机构申请属性证书。由于不同用户的属性集证书是由不同的随机多项式产生的，因此即使多个用户相互串通，他们也无法联合他们的证书组件。假设用户 A 选择属性集合 (X,Y) 作为加密属性，并向用户 B 和用户 C 发送加密后的信息，而用户 B 拥有属性 X、用户 C 拥有属性 Y。由于 $B.Y$ 的密钥不同于 $C.Y$ 的密钥，因此 $B.X$ 的密钥无法和 $C.Y$ 的密钥共同使用，来共谋破解 A 的信息。

2.2.2　系统构造

本节将详细介绍基于 ABE 的隐藏证书扩展模型的系统构造。我们用 A_u 来表示用户 u 拥有的属性集合，用 A_c 来表示加密密文的属性集合。

一个基于 ABE 的隐藏证书扩展模型包括：

1)系统参数设置函数 *Setup*：由认证机构运行，产生系统公开参数 params 和主密钥 master-key；

2)证书发布函数 *CA_Issue*：由认证机构运行，随机选择多项式为每一个用户创建和发布一个证书，该证书由一系列证书组件构成，每一个证书组件对应用户的一个属性；用户在向认证机构获取证书时可以采用全局唯一的假名 nym；

3)加密函数 $CT=HCE(R,nym,A_c)$：由发送方运行，用属性集合 A_c 作为公钥来加密资源 R，R 的接收者为 nym，CT 为加密后的密文，A_c 作为访问策略包含在密文 CT 中；

4)解密函数 $R=HCD(CT,Cred)$：由接收方运行，对密文 CT 进行解密，证书 Cred 对应的公钥为 A_u，当且仅当 $|A_c \cap A_u| \geqslant d$ 时能解密资源 R，d 为一个确定的门限。

值得注意的是，这个系统并没有给用户的每一个属性发放一个证书，而是给每一个用户发放一个证书，每一个证书组件对应用户的一个属性。因为如果采用"每一个属性发放一个证书"的方式，多个用户将很容易串通，结合他们的属性证书来解密那些他们无法单独解密的密文，系统将很容易遭受共谋攻击。

2.2.3　双方信任协商协议

图 3 示出双方信任协商协议。使用基于 ABE 的隐藏证书实现双方信任协商的过程(用户 A 请求访问用户 B 的一份文件 R)如下：

1)A 向 B 发送请求 $Ta=HEs(request,Prequest)$；

2)B 的证书集合为 CB，如果 B 满足 $Prequest$，就能还原 $request=HDs(Ta,CB)$；

3)B 向 A 发送资源 $Tb=HEs(R,PR)$；

4)A 的证书集合为 CA，如果 A 能够满足 PR，就能还原 $R=HDs(Tb,CA)$。

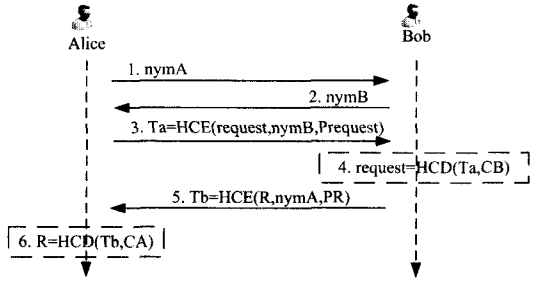

图 3　双方信任协商协议

2.2.4　多方信任协商协议

图 4 示出多方信任协商协议。使用基于 ABE 的隐藏证书来实现多方信任协商过程(用户 A 请求访问满足访问策略 $Prequest$ 的所有用户的文件 R_k)：

1)A 向系统中所有的用户发送请求 $Ta=HEs(request, Prequest)$；

2)接收到请求的用户如果不满足 $Prequest$，则不能还原请求，并且不会获得任何关于访问策略的信息；B 的证书集合为 CB，D 的证书集合为 CD，如果 B 和 D 都满足 $Prequest$，就都能还原 $request=HDs(Ta,CB)=HDs(Ta,CD)$；

3)向 A 发送资源 $Tb=HEs(Rb,PRb)$，D 向 A 发送资源 $Td=HEs(Rd,PR\,d)$；

4)A 的证书集合为 CA，如果 A 能够满足 PRb，就能还原 $Rb=HDs(Tb,CA)$；如果 A 能够满足 PRd，则也能还原得到 $Rd=HDs(Td,CA)$。

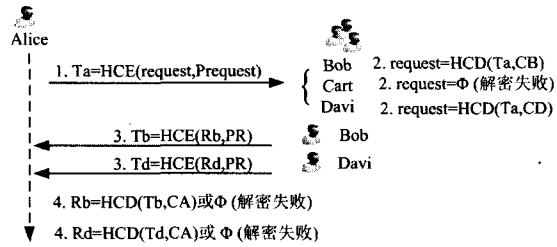

图 4　多方信任协商协议

双方信任协商和多方信任过程中的请求加密和解密、资源加密和解密都采用了基本 ABE 技术。与基于 IBE 的隐藏证书相似，本扩展模型也实现了证书隐藏和资源隐藏，在信任协商过程中避免了获取资源前的多次证书交换，减少了网络花销，同时也保护了证书的安全性。此外，在信任协商中，为了保护敏感策略，发送方在加密信息时只需要给出加密的公钥集合，而无需指明他具体使用了哪些公钥。在基于 IBE 的隐藏证书系统中，接收方需要用自己的每一个证书去尝试解密，这样做虽然实现了策略隐藏，但效率不高。而在基于 ABE 的隐藏证书扩展模型中，由于每个用户只拥有一个证书，在解密信息时只需要进行一次尝试，大幅提高了系统的效率。

3　扩展模型性能分析

假设 G_1 是素数 p 的双线性群，g 用于产生 G_1，$e:G_1\times G_1\rightarrow G_2$ 表示双线性映射，安全参数 κ 决定群的大小。

对 $i\in Z_p$ 和 Z_p 中的一组元素 S 定义拉格朗日系数 $\Delta_{i,s}$[8]：

$$\Delta_{i,s}(x)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$$

定义元素总体 U，为简单起见，我们取 Z_p^* 中的前 $|U|$ 个元素作为总体，即整数 $1,\cdots,|U|$(对 p 取余)。接着，随机地从 Z_p 中均匀选取 $t_1,\cdots,t_{|U|}$，最后随机地从 Z_p 中均匀选取 y。系统公共参数为

$$T_1=g^{t_1},\cdots,T_{|U|}=g^{t_{|U|}},Y=e(g,g)^y$$

主密钥为

$$t_1,\cdots,t_{|U|},y$$

产生一个证书需要随机选择一个 $d-1$ 阶的多项式 q，使得 $q(0)=y$。证书由证书组件 $(D_i)_{i\in A_u}$ 组成，对每一个 $i\in A_u$，有 $D_i=g^{\frac{q(i)}{t_i}}$。

使用公钥 A_c 加密信息 $M\in G_2$ 时，选取随机值 $s\in Z_p$，则加密密文为

$$E=(A_c,E'=MY^s,\{E_i=T_i^s\}_{i\in A_c})$$

解密时，任意选取一个 $|A_c\cap A_u|$ 的 d 元素的子集 S，则解密为

$$E'/\prod_{i\in S}(e(D_i,E_i))^{\Delta_{i,s}(0)}=Me(g,g)^{sy}/\prod_{i\in S}(e(g,g)^{sq(i)})^{\Delta_{i,s}(0)}$$
$$=M$$

由以上公式可以看出，在基于 ABE 的隐藏证书扩展模型中，加密时需要进行的幂运算次数与加密公钥中包含的属性数目呈线性增长；解密时所需要的花销则与 d 个双线性映射的计算量相关，d 为解密时的属性门限。

系统公共参数中的组元素数目与系统中所有的属性数目呈线性关系；用户证书中组元素的数目与他拥有的属性数目呈线性关系；密文中组元素的数目则与加密密文所采用的公钥的大小呈线性关系。

4　扩展模型安全性分析

在模糊选择身份安全模型[8](Fuzzy Selective-ID security model)下，本文证明了基于基本 ABE 的隐藏证书扩展模型的安全性。

模糊选择身份安全模型如下：

初始化：对手表明他想挑战的模糊身份 α；

系统设置：挑战者运行 setup 算法，并且告诉对手系统公共参数；

第一阶段：对手可以查询很多身份 Y_j 的私钥，对所有 j 有 $|Y_j\cap\alpha|<d$；

挑战：对手提交两个相同长度的信息 M_0,M_1。挑战者掷一个随机硬币 b，使用 α 加密 M_b，并将密文传送给对手。

第二阶段：重复第一阶段的过程；

猜测：对手输出 b 的猜测值 b'；

在此次博弈中对手的优势定义为 $\Pr[b'=b]-\frac{1}{2}$。

在模糊选择身份安全模型中，如果所有的时间多项式对手在博弈中至多有一点微不足道的优势，则系统是安全的。系统的安全性基于与决策性 BDH 假设类似的决策性 MBDH 假设。

定理 1　一个对手如果能在模糊选择身份安全模型中打破系统安全性，则能构建一个在决策性 MBDH 博弈中有无法忽略优势的假装者(具体证明见文献[8])。

(下转第 79 页)

Springer-verlag,2005:17-36

[4] Aumasson J P, Henzen L, Meier W, et al. Sha-3 proposal blake [EB/OL]. http:// 131002. net/blake/blake. pdf,2009-08-11

[5] Bernstein D J. CubeHash specification(2. b. 1)[EB/OL]. http://ehash. iaik. tugrazat/wiki/CubeHash,2009-08-11

[6] Ferguson N, Lucks S, Schneier B, et al. The Skein hash function family[EB/OL]. http://www. skein-hash. info/sites/default/files/skein1. 1. pdf,2009-12-20

[7] Li Ji, Xu Liang-yu. Attacks on Round-reduced BLAKE [EB/OL]. http://ehash. iaik. tugraz. at/wiki/The _ SHA-3 _ Zoo, 2009-11-08

[8] Aumasson J P, Guo Jian, Knellwolf S, et al. Differential and invertibility properties of BLAKE[EB/OL]. http://ehash. iaik. tugraz. at/wiki/BLAKE,2010-05-15

[9] Bernstein D J. The Salsa 2 0 encryption function [EB/OL]. http://cr. yp. to/snuffle. html,2010-02-23

[10] Paul S, Preneel B. Solving systems of differential equations of addition[C]// ACISP'05. Berlin: Springer-verlag,2005:75-88

[11] Khovratovich D, Nikoli I. Rotational Cryptanalysis of ARX [EB/OL]. http://www. skein-hash. info/sites/default/files/ARX. pdf,2010-04-15

[12] Brier E, Khazaei S, Meier W, et al. Linearization Framework for Collision Attacks: Application to CubeHash and MD6(Extended Version)[C]// ASIACRYPT 2009: Advances in Cryptology. Berlin: Springerverlag,2009:560-577

(上接第 57 页)

另外,本文选择对分布式系统而言具有代表性的两种攻击方法,分析探测攻击和中间人攻击。

1)探测攻击

敌意方通过试探的方法来获取私密的策略或属性内容。由于本方案采取交互加解密措施,如果敌手随机提交请求,基于隐藏证书的协商流程,对方将无法猜测到我方的策略。由于我方在发送信息时已经采取了加密措施,即使敌手有非法获取的正确请求方式也无法解密,除非对方有正确的信任证书,这一点确保了敌方无法采取探测攻击。

2)中间人攻击

敌手可能通过证书伪造来发起中间人攻击。在本文的方案中,双方传输的敏感证书和策略都已经进行了基于属性的加密,只具有理论上进行破解的可能性。

结束语 本文提出了基于 ABE 的隐藏证书扩展模型,详细描述了扩展模型的体系架构、系统构造、双方信任协商过程、多方信任协商过程、性能分析、安全性分析和实际应用场景示例。在开放的环境如 Internet 中,与陌生方进行信任协商时,经常是基于请求方的属性特性,而不是请求方的身份。因此,相对基于 IBE 的隐藏证书而言,基于 ABE 的隐藏证书有着更为广泛的应用。此外,由于 ABE 技术能灵活地实现一对多的加密特性,因此基于 ABE 的隐藏证书不仅能用于双方信任协商,还能用于多方信任协商。由于在 ABE 体系中,加密及解密都是基于集合及阈值,因此发送方和接收方都可以保证自己的具体信息不被泄漏。而且,由于每个用户只有一个属性集证书,在各发证机构采用不同的随机多项式进行发布的情况下,共谋攻击无法实施,从而消除了很多隐患。

同时,我们也清楚地认识到,本文提出的基于 ABE 的隐藏证书扩展模型是单认证中心架构的,在实际应用中还有一定的局限性。在后续研究中,基于多认证中心的 ABE 隐藏证书技术将是研究的主要方向[10,11]。另外,鉴于现实世界中各类属性一般都是分层的,基于分层属性 ABE 的隐藏证书技术将是另外一个研究方向[12-14]。

参 考 文 献

[1] Winsborough W, Seamons K, Jones V. Automated Trust Negotiation[C]// Proceeding of DARPA Information Survivability Conference and Exposition. ACM Press,2000:156-182

[2] Winsborough W H, Jacobs J. Automated trust negotiation in attribute-based access control[C]//DARPA Information Survivability Conference and Exposition. Proceedings of Volume 2. April 2003:252-257

[3] Li N H, Winsborough W H, Mitchell J C. Distributed credential chain discovery in trust management[C]// Proc. of the 8th ACM Conf. on Computer and Communications Security. New York: ACM Press,2001:156-165

[4] Boneh D, Franklin M. Identity-based Encryption from Weil Pairing[A]// Kilian J CRYPTO 2001[C]. Berin: Springer-Verlag, 2001:213-229

[5] Holt J E, Bradshaw R, Seamons K E, et al. Hidden credentials [C]//Proceedings of 2nd ACM Workshop on Privacy in the Electronic Society. ACM Press,2003:1-8

[6] Bradshaw RW, Holt J E, Seamons K E. Concealing complex policies with hidden credentials[C]// ACM Conf. on Computer and Communications Security. New York: ACM Press, 2004: 146-157

[7] Frikken K, Atallah M, Li J T. Hidden access control policies with hidden credentials[C]// ACM Workshop on Privacy in the Electronic Society. New York: ACM Press,2004:27-28

[8] Sahai A, Waters B. Fuzzy Identity Based Encryption[C]// Advances in Cryptology-Eurocrypt. volume 3494 of LNCS. Springer,2005:457-473

[9] Goyal V, Pandey O, Sahai A, et al. Attribute-based Encryption for Fine-grained Access Conrol of Encrypted Data[C]// ACM Conference on Computer and Communications Security (ACM CCS). 2006

[10] Chase M. Multi-authority Attribute-based Encryption [C]// TCC. volume 4392 of LNCS. Springer,2007:515-534

[11] Chase M, Chow S S. Improving Privacy and Security in Multi-authority Attribute-based Encryption[C]// CCS '09: Proceedings of the 16th ACM Conference on Computer and Communications Security. New York, NY, USA: ACM,2009:121-130

[12] Li J, Wang Q, Wang C, et al. Enhancing attribute-based encryption with attribute hierarchy[C]// 4th International Conference on Communications and Networking in China (Chinacom). To appear ACM MONET,2009

[13] Gentry C, Silerberg A. Hierarchical ID-based Cryptography[A]// Zheng Y ASICCRYPT 2002[C]. Berlin: Springer-Verlag,2002: 548-566

[14] Horwitz J, Lynn B. Toward Hierarchical Identity-based Encryption[A]//Knudsen L EUROCRYPT 2002[C]. Berlin: Springer-Verlag,2002:466-481