doi:10.3969/j.issn.1000-436x.2012.12.011

EAEBHCM：一种扩展的基于属性加密的隐藏证书模型

葛维进，胡晓惠
（中国科学院 软件研究所，北京 100190）

摘 要：基于身份加密体系的隐藏证书原始模型存在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等缺点。提出的基于属性加密的隐藏证书扩展模型通过引入属性集合证书技术、基于加解密精度阈值等特性，解决了上述三个问题。在分析国内外相关研究进展的基础上，对扩展模型在体系架构、系统构造、双方信任协商协议、多方信任协商协议以及扩展模型解决复杂逻辑访问策略的方法等进行了详细的阐述，并对扩展模型的安全性进行了分析。通过一个典型的应用场景，对比分析了新旧隐藏证书技术在性能和安全性上的区别，阐明了扩展模型的优点。

关键词：属性；加密；隐藏证书；信任协商；共谋
中图分类号：TP393.0 **文献标识码**：A **文章编号**：1000-436X(2012)12-0085-08

EAEBHCM: an extended attribute encryption based hidden credentials model

GE Wei-jin, HU Xiao-hui
（Institute of Software, Chinese Academy of Sciences, Beijing 100190, China）

Abstract: The identity-based encryption based hidden credentials has three problems that it can not supports 1-*N* communication, endures no identity fuzzy and lefts open to conspiracy crack. An extended attribute encryption based hidden credentials model (EAEBHCM) was presented in to solve these three issued which making use of attribute-set certificates and decryption accuracy threshold characteristics. After analyzed the relevant research, the architecture, the system structure, the two sides trust negotiation protocol, multi-party trust negotiation protocols and how the model to solve complex logical access policies of the extended model were described in detail. And the security of extended model was also analyzed. Through a typical access control scenario, the difference between old and new hidden credentials technology on the performance and security were analyzed, which clarified the advantages of the extended model.

Key words: attribute; encryption; hidden credentials; trust negotiation; conspiracy

1 引言

自动信任协商(ATN, automated trust negotiation)的概念是 Winsborough 等人在 2000 年提出的[1~4]。这一概念是指资源的请求方和提供方通过一个自动化的过程逐步披露属性证书，最终建立信任关系。众多研究人员继承 Winsborough 等人的研究，以自动信任协商协议体系为基础，对如何在访问控制中保护敏感策略和敏感属性等问题进行了深入研究。例如，Holt 等人提出了隐藏证书 (hidden credential)技术[5]。Bradshaw[6,7]设计并实现了如何利用隐藏证书隐藏复杂安全策略。诸多研究人员相继对隐藏证

收稿日期：2012-04-15；修回日期：2012-11-21
基金项目：国家高新技术研究发展计划（“863”计划）基金资助项目（SS2012AA010106）
Foundation Item: The National High Technology Research and Development Program of China (863 Program)(SS2012AA010106)

书及其扩展技术进行了深入研究[8~16]。然而现有的隐藏证书技术在以下几个方面仍然存在明显不足。

1) 不支持多方信任协商。鉴于隐藏证书技术在加密时就得明确规定接收方的身份特性，导致它只支持一对一信息交互，并不支持 1-*N*(一对多)信息交互。

2) 不支持对模糊特性的加密和解密处理。隐藏证书技术需要基于明确的接收方身份特征实施加密，而在分布式网络中进行信任协商时，一般不是针对某个确定的身份特征，而是针对一些模糊的特性集合。

3) 存在被共谋破解的风险，安全性不足。在 IBE 系统中，每个用户有多个特征证书，两个参与方有共享双方的特征证书的可能性，进而有可能实现对发送方密文的破译。

针对上述问题，本文设计了一种扩展的基于属性加密的隐藏证书模型。该模型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；基于属性集合的加密和解密方式提升了交互双方的信息安全级别；对属性集证书发放过程进行随机性控制，消除了共谋破解的可能。

2 相关研究

目前，基于模糊身份的密码体制成为密码学界的一个研究热点。2005 年，Sahai 和 Waters 首次提出了这种密码体制[8]。在他们的方案中，引入了模糊身份（fuzzy identity）的概念并提出了一个基于模糊身份的加密（fuzzy identity based encryption）方案，将生物特性直接作为身份信息应用于基于身份的加密体制中。在这种基于模糊身份的加密系统中，用于加密信息的是由一系列描述用户特性的属性构成的一个模糊身份特征；而密钥组件则构成用户的解密密钥，密钥组件和身份的属性一一对应。例如，当且仅当集合 ω 和有一定的重叠时，一个拥有属性集合 ω 的用户能够解密用属性集合 ω' 加密的密文。即它允许发送方用于加密信息的特征集合和接收方用于解密的特征集合之间可以存在一定的差别。该过程的示例如图 1 所示。

基于模糊身份的密码体制有两个主要的应用领域：基于生物特征的识别技术和基于属性的加解密技术。

生物特征识别技术综合运用密码学、纠错编码技术和模糊生物特征加解密技术，将秘密数据与生物特征模板有机融合，有效地提高了秘密数据的安全性和生物特征的隐私性。但该技术存在的问题是图像的噪声使得生物特征不够稳定、可变性增强。而且，这种可变性导致了生物特征加密/解密过程成为不确定过程。因此，这项技术目前还不够成熟，有待进行广泛深入的研究。

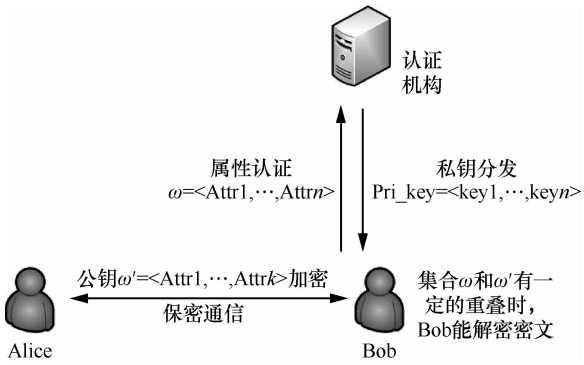

图 1 基于特征集合的加解密示例

把生物特征识别和 ABE 相结合是一个重要的研究领域。该领域的一般做法是：首先，描述用户的生物特征，确定这些特征的属性集合；然后，用确定的生物特征加密信息。由于噪音干扰会导致这种方法存在较大的误差，从而引起人们对于该系统适用性的怀疑。可喜的是，已经有研究人员设计出了具有一定容错能力的信息系统[8]。

基于属性的加密技术主要有下列 4 个方面的特点。

1) 只有符合密文属性要求的群体成员才能解密消息，从而保证了数据的机密性。

2) 资源提供方无需考虑群体中成员的数量和身份，只需要依据属性加密消息，提高了数据加密效率并保护了用户隐私。

3) 基于属性的加密机制中用户密钥与随机多项式或随机数相关，不同用户的密钥无法联合，因而从根源上杜绝了共谋破解的可能。

4) 基于属性的加密机制支持基于属性的访问控制策略，可以实现属性的与、或、非和门限操作。

ABE 的上述特征使得其具有高效性、抗合谋和策略表示的灵活性等，因此在细粒度访问控制[9](审计日志、付费电视系统等)、定向广播[7]、组密钥管理[11,12]、隐私保护[13,14]等领域具有良好的应用前景。而这些应用的共同特点是：信息发送方希望能传送加密信息给拥有一系列确定属性的所有用户，即采用一对多的方式传送信息。具体地，由加密信息的发送方确定属性集合，并且规定只有被证明具有指

定属性集合中至少 d 个（d 是事先确定的阈值精度）属性的用户才能解密信息。

在 Sahai 等提出的 ABE 方案的基础上，陆续有研究人员对该方案进行了改进。Goyal[9]等构造了改进的 ABE 方案。该方案中的密钥可以用于描述“与”，“或”及和门限结构的访问控制策略。2008 年，Nishide 等人[15]提出了一个可以隐藏访问结构的加密方案，实现了同时保护消息和访问结构私密性的功能，但是该方案的安全模型较弱。2011 年，Lai 等人[16]利用子群判定假设在合数阶群中提出了一个新的可以隐藏访问结构的加密方案，并证明是完全安全的。但是为了达到一定的安全级别，合数群的阶会取得比较大。

3　扩展的基于属性加密的隐藏证书模型

本文设计实现了一种基于属性加密的隐藏证书模型（EAEBHCM, extended attribute encryption based hidden credentials model）。该模型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；基于属性集合的加密和解密方式提升了交互双方的信息安全级别；对属性集证书发放过程进行随机性控制，消除了共谋破解的可能。以下分别介绍模型组成、模型架构、双方信任协商协议及多方信任协商协议。

3.1　EAEBHCM 的组成

本节介绍 EAEBHCM 的组成，其中，A_u 表示信息接收方的属性特征集合，A_c 表示发送方用来加密信息时所用的属性特征集合。

EAEBHCM 有下列 4 个主要的功能函数。

1) 系统初始化函数 *Init*：由证书发放机构运行。用于初始化整个体系的公共参数*params*和主密钥*key*。

2) 证书发放函数 *Issue_AC*：由证书发放机构运行。对于每一个用户，证书发放机构选择一个指定阶数的随机多项式用于创建属性证书。

3) 加密函数 $CT=\mathrm{HC_E}(R,nym,A_c)$：信息发送方在发送敏感信息前，根据对敏感信息 R 的具体访问控制策略的要求，选择接收方的指定属性子集 A_c 作为密钥来加密该敏感信息 R，密文的接收方由 *nym* 指定，*CT* 是加密得到密文；加密是可以指定解密精度要求，设其大小为 d。特别地，如果不指定接收者的 *nym* 信息，则该加密函数的结果可以被任一满足 A_c 要求的接收方正确解密。

4) 解密函数 $R=\mathrm{HC_D}(CT,\ Cred)$：由接收方运行，使用接收方拥有的各个匹配精度的属性证书对密文 *CT* 进行解密尝试，证书 *Cred* 对应的密钥为 A_u，当且仅当 $|A_c \cap A_u| \geqslant d$ 时能成功解密资源 R，d 为加解密的精度阈值。

在加密函数 *CT* 和解密函数 *R* 中：

$$\mathrm{HC_E}(R,nym,A_c)=\mathrm{Encrypt}(Params,nym \| A_c,R)$$

$$\mathrm{HC_D}(CT,\ Cred)=\mathrm{Decrypt}(Params,CT,A_u)$$

其中，

$$A_c=\{PKG_{pub},attr_1,attr_2,\cdots,attr_n\}$$

$$Params=\{params,PKG_{pub}\}$$

Cred 是由 *PKG* 发放的属性元素 $attr_i$ 的证书片段组成的综合属性证书。

证书发放机构在发布证书时，根据用户的属性特征集合，发放一个整体属性证书，可以理解为属性集证书。其中一个证书元件对应用户的一个属性元素。

为方便理解，下面以涉及一个属性的访问控制逻辑为例来描述本模型的工作流程。复杂逻辑访问策略的处理方式请参见本文第 4 节的内容。

设主客体之间的访问控制逻辑描述如下。

如果服务提供方的属性 *Name* 的值为 Alice，则可以获知访问请求方的本次访问请求，请求的具体内容为访问服务提供方的资源 *R*。

这是对访问请求方的访问请求 *Request* 的保护策略，可以记为 *P_Request*。其中，这个访问请求是敏感的，对于姓名不为 Alice 的服务提供方，并不能获知这个访问请求。

如果访问请求方的属性 *Name* 的值为 Bob，则可以访问服务提供方的资源 *R*。

这是对服务提供方的资源 *R* 以及对 *R* 进行保护的访问控制策略 *P_Response* 的保护性措施。其中这个访问控制策略本身也是敏感的，对于访问请求方姓名为 Bob 之外的人员，并不能获知这个访问控制策略。

针对上述访问请求双方之间的请求、策略和资源的保护措施，本扩展模型采用如下步骤实现对敏感信息的保护。

1) 访问请求方 *requester* 向 PKG 申请属性证书，其中包括属性 *Name* 的属性证书片段，且 *Name* 的值为请求方属性 *Name* 的实际取值，如 Bob、Mark 等。

2) 服务提供方 *provider* 向 PKG 申请属性证书，其中包括属性 *Name* 的属性证书片段，且 *Name* 的值为服务提供方属性 *Name* 的实际取值，如 Alice、Monica 等。

3) 访问请求方以 Alice 这个属性值、辅助以 PKG 的全局变量，一起加密本次访问请求 *Request*，并将加密后的结果 CT={$\mathrm{HC_E}$(*Request*, *provider*, P_{Request}), *rsize*}发送给服务提供方。

4) 服务提供方以自身的属性证书 *Gred* 来尝试解密这个访问请求，如果服务提供方拥有的属性证书满足访问请求方对服务提供方属性 *Name* 的取值要求，则能正确解密 $Request = \mathrm{HC_D}(CT, Cred)$；否则服务提供方无法获知访问请求方的请求内容，双方的交互流程随之结束。

5) 如果服务提供方能正确获知 *Request*，则需要使用 $P_{\mathrm{Responese}}$ 对资源 *R* 进行保护，并将施加了保护措施后的结果发送给访问请求方。由于资源 *R* 本身的大小和占用的字节空间不定，为了方便制定主客体之间的实际传输协议，需要由服务提供方来随机产生一个固定长度的密钥 *key*，并使用全局唯一的对称加解密算法，如 AES 加密算法，对资源 *R* 进行加密。并对这个随机产生的 *key*，使用 $P_{\mathrm{Responese}}$ 进行加密保护，从而达到间接保护资源 *R* 的目的，即 CT′={$\mathrm{HC_E}$(*key*, *requester*, P_{Response}), $\mathrm{E_{key}}(R)$}。

访问请求方接收到这个 CT′ 后，使用访问请求方的属性证书 *Cred′* 进行解密尝试，如果满足服务提供方对访问请求方属性的要求，则能正确解密获得服务提供方的随机加密密钥。$key = \mathrm{HC_D}(CT', Cred')$；从而根据全局唯一的对称加解算法，如 AES 加密算法，对最后的资源进行解密获得 $D_{key}(E_{key}(R)) = R$。如果访问请求方不满足服务提供方的访问控制策略的要求，则访问请求方无法获知服务提供方的资源 *R* 以及保护 *R* 的访问控制策略 $P_{\mathrm{Responese}}$。

3.2 EAEBHCM 的架构

EAEBHCM 的体系架构如图 2 所示。

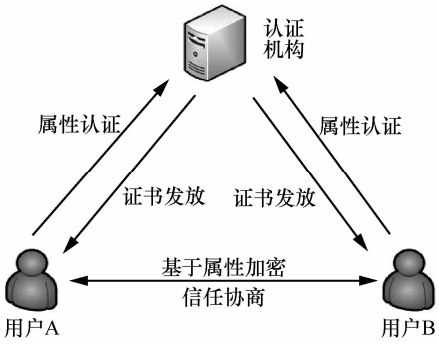

图 2 EAEBHCM 的体系架构

图 2 所示的 EAEBHCM 是基于单认证机构的，即只有一个证书发放机构。在开始交互信息前，各个用户选择一个全局身份 GID 并以此向证书发放机构申请证书。根据基于属性的加密技术的要求，在发放属性证书时，需要选择一个属性匹配的精度 Ω 的具体数值大小 *d*。认证机构在发放属性证书时，将根据这个匹配精度 *d* 的数值，针对不同的用户，选择一个($d-1$)阶的随机多项式来发放属性集证书。

一般地，为了方便访问请求双方之间的交互，每个用户可以认证结构申请 *N* 个属性证书，其中每一个证书对应一个不同的属性匹配的精度。设某用户有 *N* 个属性元素，那么他可以根据属性匹配精度从低到高的递增序列（公差为 1），以精度为 1, 2, 3,…,（$N-1$）和 *N*，相应地申请到和当前匹配精度相对应的 *N* 个属性证书 $Cred_{\mathrm{i}}$，从而形成一个匹配精度呈等差数列形式的属性证书的集合 $\bigcup_{i=1}^{N} Cred_{\mathrm{i}}$。

3.3 EAEBHCM 的信任协商协议

3.3.1 EAEBHCM 的双方信任协商协议

EAEBHCM 的双方信任协商过程如图 3 所示，假设用户 Alice 请求访问用户 Bob 的一份文件 R。

1) A 向 B 发送请求 $T_{\mathrm{a}} = \mathrm{HC_E}(request, P_{\mathrm{request}})$；其中，$P_{\mathrm{request}}$ 包含访问请求方 A 要求的精度匹配数值。

2) 服务提供方 B 使用其所拥有的不同匹配精度的属性证书集合 $\bigcup_{i=1}^{N} Cred_{\mathrm{i}}$，逐一尝试解密 T_{a}，如果 B 的某个匹配精度下的属性证书 $Cred_{\mathrm{i}}$ 满足 P_{request}，则能还原 $request = \mathrm{HC_D}(T_{\mathrm{a}}, Cred_{\mathrm{B}})$；如果所有 $Cred_{\mathrm{i}}$ 都无法解密成功，则交互结束。

3) 服务提供方 B 向访问请求方 A 发送资源 $T_b = \mathrm{HC_E}(R, P_r)$；其中，$P_{\mathrm{r}}$ 是对资源 *R* 的访问控制保护策略。P_{r} 中包含有服务提供方 B 的策略所要求的精度匹配数值。

4) 访问请求方 A 使用其所拥有的不同匹配精度的属性证书集合 $\bigcup_{j=1}^{M} Cred'_{\mathrm{j}}$，逐一尝试解密 T_b，如果 A 的某个匹配精度下的属性证书 $Cred'_{\mathrm{j}}$ 满足 P_{r}，则能解密还原 $R = \mathrm{HC_D}(T_b, Cred'_A)$；如果所有 $Cred'_{\mathrm{j}}$ 都无法解密成功，则交互结束。

其中，信息加密一方可以选择将匹配精度 Ω 的数值以明文方式附在加密结果之后，以进一步提升对方解密时的效率。

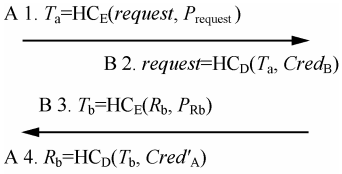

图 3　基于 EAEBHCM 模型的双方信任协商协议

3.3.2　EAEBHCM 的多方信任协商协议

本文提出的 EAEBHCM 模型的多方信任协商过程如图 4 所示，假定 Alice（A）请求访问所有用户的文件 R_x，这些文件满足访问策略 P_{request}。

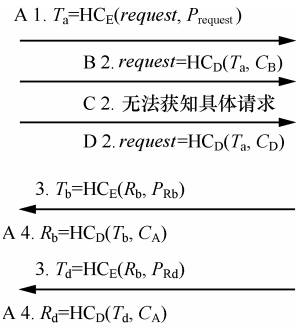

图 4　基于 EAEBHCM 模型的多方信任协商协议

1) A 向系统中所有的用户发送相同的加密请求 $T_a = \text{HC}_E(request, P_{\text{request}})$。

2) 用户 X 如果不满足 P_{request}，则无法解密获得请求的内容，从而也就无法获知访问请求方的任何有效信息；B、C、D 各自用自己拥有的各个匹配精度的属性证书尝试解密 T_a。设 B 的属性证书 C_B 解密 T_a 成功，C 的所有精度级别的证书解密全部失败，D 的属性证书 C_D 解密 T_a 成功，则 B、D 能解密还原 $request = \text{HC}_D(T_a, C_B) = \text{HC}_D(T_a, C_D)$；而 C 由于无法满足 P_{request} 的要求，从而无法获得 A 的请求信息。

3) B 向 A 发送资源 $T_b = \text{HC}_E(R_b, P_{Rb})$，D 向 A 发送资源 $T_d = \text{HC}_E(R_d, P_{rd})$。

4) A 用自己拥有的各个匹配精度的属性证书 CA_i 尝试解密收到的信息，若 A 的某个匹配精度级别的属性证书 CA_i 能够满足 P_{Rb}，则能解密 $R_b = \text{HC}_D(T_b, CA_i)$ 成功获得 B 的资源信息；相同地，假如 A 的某匹配精度级别的属性证书 CA_i' 能够满足 P_{Rd} 的要求，则也能成功解密 $R_d = \text{HC}_D(T_d, CA_i')$ 并获得用户 D 发来的资源。

相同地，信息加密一方可以选择将匹配精度 Ω 的数值以明文方式附在加密结果之后，以进一步提升对方解密时的效率。

4　复杂逻辑访问策略的解决方式

现实世界中，逻辑“与”和逻辑“或”是相辅相成的。类似下述访问控制策略“男教师或校长可以参加会议”可谓比比皆是。在这个策略中，可以定义涉及到的属性包括如下内容。

性别属性 *Sex*，取值可以为男、女和未知。

岗位属性 *Post*，取值可以为教师、学生和校长。

则“男教师或校长可以参加本次会议”这个策略，可以定义为

If ((*Sex*=“男” and *Post* =“教师”) or *Post* =“校长”) then

他可以参加本次会议。

为解决复杂逻辑下的加密问题，本节先讨论只涉及一个属性 *attr* 的访问控制策略的加密函数 $\text{HC}_{\text{simpleE}}$。根据上文可知，

$$\text{HC}_E(R, nym, A_c) = \text{Encrypt}(Params, nym \| A_c, R)$$

由于 $\text{HC}_{\text{simpleE}}$ 已经确定只涉及一个属性元素 *attr*，所以上述公式中的 A_c 可以简化为该属性元素本身的标识 *attr*。故：

$$\text{HC}_{\text{simpleE}}(R, nym, attr) = \text{Encrypt}(Params, nym \| attr, R)$$

在上述公式的基础上，定义复杂逻辑的加密函数 HC_E 如下。

1) 如果 P 是只涉及到一个属性元素的简单策略，则

$$\text{HC}_E(R, P) = \text{HC}_{\text{simpleE}}(R, P) \tag{1}$$

2) 如果 $P = (P_1 \vee P_2)$，则

$$\text{HC}_E(R, P) = \{\text{HC}_E(R, P_1), \text{HC}_E(R, P_2)\} \tag{2}$$

3) 如果 $P = (P_1 \wedge P_2)$，则

$$\text{HC}_E(R, P) = \{\text{HC}_E(\text{HC}_E(R, P_2), P_1)\} \tag{3}$$

4) 如果 P 是门限类型，即 $P = MofN(m, P_1, P_2, \cdots, P_n)$，则

$$\begin{aligned}\text{HC}_E(R, P) = MofN(R, m, n, &\text{HC}_E(s_1, P_1),\\ &\text{HC}_E(s_2, P_2), \cdots, \text{HC}_E(s_n, P_n))\end{aligned} \tag{4}$$

其中，*MofN* 是针对 R 的门限加密算法，这类策略表示需要满足 n 个策略中的至少 m 个，才算满足策略 P。$s_1, s_2, \cdots, s_n$ 是由所选择的门限模式定义的门限算子。

根据式(1)~式(4)，可以组合形成各种复杂的逻辑表达式。如对于

$$P=(P_1\wedge P_2)\vee(P_3\wedge P_4\wedge P_5)\vee P_6$$

则根据上述访问控制策略对敏感信息加密后的结果序列为

$$\begin{aligned}&\mathrm{HC_E}(R,P)=\{\mathrm{HC_E}(\mathrm{HC_E}(R,P_2),P_1),\\&\mathrm{HC_E}(\mathrm{HC_E}(\mathrm{HC_E}(R,P_5),P_4),P_3),\\&\mathrm{HC_E}(R,P_6)\}\end{aligned}\tag{5}$$

5 EAEBHCM 的安全性分析

假设 G_1 是素数 p 的双线性群，g 用于产生 G_1. $e:G_1*G_1\to G_2$ 表示双线性映射。

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]：

$$\Delta_{i,s}(x)=\prod_{j\in s,j\neq i}\frac{x-j}{(i-j)}\tag{6}$$

定义元素总集 V，为简单起见，对素数 p 取余后，选择 Z_p^* 中的前$|N|$个元素作为集合内容，即整数 1，…，$|N|$。然后随机地从 Z_p 中均匀选取 t_1，…，$t_{|N|}$，最后随机地从 Z_p 中均匀选取 y。系统公共参数为

$$T_1=g^{t1},\cdots,T_{|N|}=g^{t|N|},Y=e(g,g)^y\tag{7}$$

主密钥为

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

选取证书发布时所需的$(d-1)$阶随机多项式 q 使得 $q(0)=y$。证书由证书组件 $(D_i)_{i\in A_u}$，对每一个 $i\in A_u$ 有 $D_i=g^{\frac{q(i)}{t_i}}$。

使用特征集合 A_c 对信息 $M\in G_2$ 进行加密时，选取随机值 $s\in Z_p$，则加密密文为

$$E=(A_c,E'=MY^s,\{E_i=T_i^s\}i\in A_c)\tag{8}$$

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

$$\begin{aligned}M&=E'/\prod_{i\in s}(e(D_i,E_i))^{\Delta_{i,s(0)}}\\&=Me(g,g)SY/\prod_{i\in s}(e(g,g)^{sq(i)})^{\Delta_{i,S(0)}}=M\end{aligned}\tag{9}$$

分析上述公式可知，在加密时，EAEBHAM 需要进行的计算次数与 A_c 中包含的属性数量之间的关系为一阶线性函数关系；而解密时所需耗费的时间，则与加解密时选取的门限阈值 d 呈双线性映射。

根据模糊选择身份安全模型[8]可知，$\mathrm{HC_E}(R,nym,A_c)=\mathrm{Encrypt}(params,nym\|A_c,R)$，即密文是使用 ECC 椭圆曲线算法进行加密，破解该加密在理论上存在 WDH (Weil Diffie-Hellman)困难。在可见的时间内，挑战方无法攻破或获得可见的优势。

根据上述结果可得出如下推理：一个挑战者在可以预见的时间内，无法伪造一个有效的属性证书，用于破解加密后的内容。因此 $\mathrm{HC_E}$ 加密算法在面对任意一个非授权的属性证书时，都是安全的。

6 应用研究

本节选择一个实际场景，对 EAEBHCM 技术和基于身份加密的隐藏证书技术进行模拟分析。

场景：用户 A 是一个病人，希望能向多个医生或医疗机构成员 B 发送加密邮件请教问题 R，越多医护人员能看到她的病情，给以建议就会越好。Alice 将采用 UDP 广播或多播的方式，向所有可能接收到这个加密信息的人员发送请求。如果 B 至少能够满足下列 4 个条件中的任意 3 个，那么 B 就可以被允许获知 A 的具体问题 R，否则 B 将不能获取到任何邮件信息。这 4 个条件分别是：

B 是医疗机构 H 的成员；

B 是女医生；

B 年龄大于 40 岁；

B 是中国人。

与此同时，B 的身份（是否为医疗机构 H 的成员）、B 的性别、B 的年龄以及 B 的国籍，对于 B 本身而言，也都是需要保密的敏感信息，是不能向未经认证的陌生人透露的。

对于这个场景，可知访问请求方 A 对服务提供方 B 的属性元素的要求至少有下列 4 个：身份、性别、年龄和国籍，以 M、S、Age 和 C 来分别表示。根据访问控制要求，资源 R 的访问控制策略 S_r 为

$$S_r=C_4^3\wedge(P_1,P_2,P_3,P_4)+C_4^4\wedge(P_1,P_2,P_3,P_4)$$

其中：

$$P_1=(m\in H)$$

$$P_2=(S==Female)$$

$$P_3=(Age>40)$$

$$P_4=(C\ \text{is}\ \text{中国})$$

根据组合原理可知，当原子策略个数为 N，所需满足的最小策略个数为 M 时，访问控制组合数目为：$C_N^M+C_N^{M+1}+\cdots+C_N^N$。

6.1 使用隐藏证书原始模型的情况

对于这种 1 对 N 的场景，原始的隐藏证书模型

是无法实现的，A 只能依次向所有可能的人员集合进行一一的简单身份交互后，再发送相应的加密信息。当前交换了身份信息的人员 B 是否能正常获取她的问题并返回信息，她依然是不知道的，这种实现方式将大大降低应用的灵活度和效率。

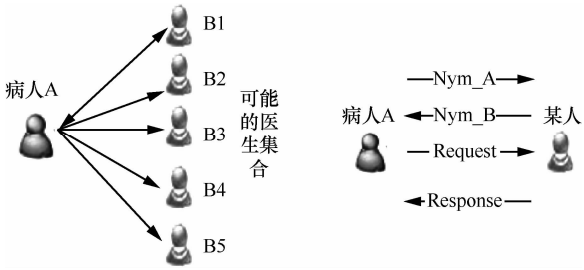

图 5　原始模型对多方信任协商的模拟

使用基于身份加密的隐藏证书原始模型时，上述的访问控制策略将细分为下列 4 个。

$$Sr_1 = P_1 \wedge P_2 \wedge P_3$$
$$Sr_2 = P_1 \wedge P_2 \wedge P_4$$
$$Sr_3 = P_1 \wedge P_3 \wedge P_4$$
$$Sr_4 = P_2 \wedge P_3 \wedge P_4$$
$$Sr_5 = P_1 \wedge P_2 \wedge P_3 \wedge P_4$$

根据上述的访问控制策略顺序。采用隐藏证书原始模型的加密结果也有 4 个，分别为：

$$\mathrm{HC_E}(R,Sr_1) = (\mathrm{HC_E}(\mathrm{HC_E}(\mathrm{HC_E}(R,P_3),P_2),P_1)$$
$$\mathrm{HC_E}(R,Sr_2) = (\mathrm{HC_E}(\mathrm{HC_E}(\mathrm{HC_E}(R,P_4),P_2),P_1)$$
$$\mathrm{HC_E}(R,Sr_3) = (\mathrm{HC_E}(\mathrm{HC_E}(\mathrm{HC_E}(R,P_4),P_3),P_1)$$
$$\mathrm{HC_E}(R,Sr_4) = (\mathrm{HC_E}(\mathrm{HC_E}(\mathrm{HC_E}(R,P_4),P_3),P_2)$$
$$\mathrm{HC_E}(R,Sr_5) = \mathrm{HC_E}(\mathrm{HC_E}(\mathrm{HC_E}(\mathrm{HC_E}(R,P_4),P_3),P_2),P_1)$$

在解密时，对应策略 P_1、P_2、P_3、P_4 的 4 个身份证书，将一一用于尝试去解密这几个加密信息。可以看到，原始模型在完成这类工作时，需要进行多次相对重复的信任协商工作，当访问策略涉及的属性元素个数增加时，这种情况将导致严重的资源消耗。

设原子策略匹配个数要求为 3 个，且区域内可请求的服务提供方 B 的个数为 10，则基于原始隐藏证书模型，访问请求方要完成对所有这些服务提供方的访问请求的信任协商次数情况如图 6 所示。

6.2　使用 EAEBHCM 的情况

使用 EAEBHCM 时，无需一一获取各个可能服务提供方的身份信息，而是直接采用属性证书片段 {*M*、*S*、*Age*、*C*} 并选取匹配精度 Ω=3 即可，使用该指定匹配精度的属性证书加密函数 $CT = \mathrm{HC_E}(R, A_C)$ 来加密所需保护的信息 *R* 后，可以 UDP 广播或多播的形式，发给所有可能的服务提供人员。根据 ABE 算法，当 B 根据使用其所拥有的属性证书（该属性证书由 *M*、*S*、*Age*、*C* 以及其他更多可能存在的属性元素证书片段组成），选择证书片段{*M*、*S*、*Age*、*C*}进行解密，当 B 能够完成匹配精度大于等于 3 的解密时，B 即能正确获取到 A 的请求信息并进行反馈。如果反馈的信息也需要进行访问控制保护，那么就进行一次反向的 1 对 1 的双方信任协商协议过程即可。

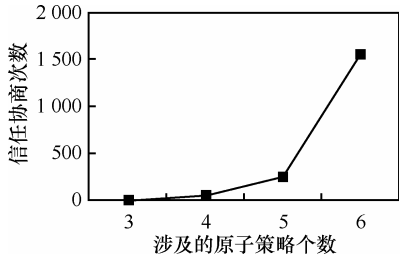

图 6　基于隐藏证书原始模型的一对多协商次数增长情况

除上述性能优势外，相比隐藏证书原始模型，使用 EAEBHCM 扩展模型拥有下列安全优势。

B 无从得知 A 具体的访问控制策略。因为在属性集合增大时，可能的策略组合数目将非常大。B 只能知道他自己是具体使用哪些属性证书来满足 A 对请求保护这个访问控制要求，而不清楚 A 访问控制策略的全貌。如 B 不是一个中国人，但她满足 A 的其他 3 个条件，那么她依然能够获取 A 的这个访问请求。但 B 无法知道，实际上 A 同时设置了一个国籍条件作为访问控制元素之一。

与此同时，A 也无从得出 B 是具体使用了哪些属性证书元素来解密自身对请求的保护，即 A 无从得知 B 具体满足哪些子策略。A 只能知道自己收到了 B 的反馈，从而得知 B 已经满足自己对请求的访问控制要求。但 B 具体是什么身份，A 依然无从猜测。如对 A 而言，B 可能是中国人，也可能不是中国人。但使用扩展前的技术，A 将很清楚 B 是什么样的身份，虽然 A 也只能获知 B 的部分身份信息。如 B 不满足 Sr_1 但是满足 Sr_2，那么显然地，对 A 而言，B 就是一个医疗机构 *H* 中，年龄小于 40 岁的中国女医生，而没有其他可能。这显然将导致 B 的敏感信息遭到不必要的暴露和侵犯。

7 结束语

本文设计了基于属性加密技术的隐藏证书扩展模型 EAEBHCM。首先对相关研究进行了分析，指出了存在的问题。然后详细描述了 EAEBHCM 的系统组成、系统架构、信任协商过程等，并对其性能和安全性进行了分析，进而构建了实际应用场景示例，进行了新旧模型之间的对比分析。表明了本文提出的扩展模型 EAEBHCM 克服了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等缺点。在信任协商过程中保留了原隐藏证书技术对于证书、资源和策略的隐藏和保护功能；基于属性集合的加密和解密方式提升了交互双方的信息安全级别，增强了策略保护的强度。

同时，由于本 EAEBHCM 是基于单认证中心架构实现的，因而其实际应用存在一定的局限性。今后将基于多认证中心对该模型展开进行进一步的研究[17,18]。

参考文献：

[1] WINSBOROUGH W, SEAMONS K, JONES V. Automated trust negotiation[A]. Proceedings of DARPA Information Survivability Conference and Exposition[C]. ACM Press. 2000. 156-182.

[2] WINSBOROUGH W H. J J: Automated trust negotiation in attribute-based access control[A]. DARPA Information Survivability Conference and Exposition[C]. 2003. 252 - 257.

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

[4] HOLT J E, BRADSHAW R, SEAMONS K E, *et al*. Hidden credentials[A]. Proceedings of 2nd ACM Workshop on Privacy in the Electronic Society[C]. ACM Press, 2003. 1- 8.

[5] BONEH D, FRANKLIN M. Identity based encryption from weil pairing[A]. Kilian J CRYPTO 2001[C]. Berin: Springer-Verlag, 2001. 213-229.

[6] BRADSHAW R W, Holt J E, SEAMONS KE. Concealing complex policies with hidden credentials[A]. ACM Conf on Computer and Communications Security[C]. New York: ACM 2004. 146-157.

[7] FRIKKEN K, ATALLAH M. LI JT. Hidden access control policies with hidden credentials[A]. ACM Workshop on Privacy in the Electronic Society[C]. New York: ACM Press, 2004. 27-28.

[8] SAHAI A, WATERS B. Fuzzy identity based encryption[A]. Advances in Cryptology-Eurocrypt, volume 3494 of LNCS[C]. Springer, 2005. 457-473.

[9] GOYAL V, PANDEY O, SAHAI A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proc of the 13th ACM Conf on Computer and Communications Security[C]. New York: ACM Press, 2006. 89-98.

[10] YU S C, REN K, LOU W J. Attribute-Based content distribution with hidden policy[A]. Proc of the 4th Workshop on Secure Network Protocols (NPSec)[C]. Orlando: IEEE Computer Society, 2008. 39-44.

[11] TRAYNOR P, BUTLER K, ENCK W, MCDANIEL P. Realizing massive-scale conditional access systems through attribute-based cryptosystems[A]. Proc of the 15th Annual Network and Distributed System Security Symp[C]. San Diego: USENIX Association, 2008. 1-13.

[12] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE[A]. Proc of the ACM Conf on Computer and Communications Security[C]. New York: ACM Press, 2007. 456-465.

[13] CHEUNG L, COOLEY J A, KHAZAN R, NEWPORT C. Collusion-resistant group key management using attribute-based encryption[EB/OL]. http://eprint.iacr.org/2007/161.pdf.

[14] YU S C, REN K, LOU W J. Attribute-based on-demand multicast group setup with membership anonymity[J]. Computer Networks, 2010, 54(3):377-386.

[15] NISHIDE T, YONEYAMA K, OHTA K. Attribute-basedencryption with partially hidden encryptor-specified access structures[A]. ACNS[C]. 2008. 111-129.

[16] LAI J, DENG R H, LI Y. Fully secure cipertext-policy hiding CP-ABE[A]. ISPEC 2011[C]. 2011. 24-39.

[17] CHASE M. Multi-authority attribute based encryption[A]. TCC, volume 4392 of LNCS[C]. Springer, 2007. 515-534.

[18] CHASE M, CHOW S, Improving privacy and security in multi-authority attribute-based encryption[A]. CCS '09: Proceedings of the 16th ACM conference on Computer and communications security[C]. ACM, New York, NY, USA, 2009. 121-130.

作者简介：

葛维进（1976-），男，浙江临海人，中国科学院软件研究所博士生，主要研究方向为综合信息系统集成及访问控制。

胡晓惠（1960-），男，河北保定人，中国科学院软件研究所研究员、博士生导师，主要研究方向为综合信息系统集成与仿真。