文章编号:1000-582X(2011)02-052-06

策略加密的信任协商隐私保护

喻 玲[a],陈蜀宇[b]
(重庆大学 a.计算机学院;b.软件工程学院,重庆 400044)

摘 要:自动信任协商隐私保护技术不断发展,隐藏证书是其中较为全面的解决方案。针对隐藏证书技术存在解密盲目性,造成解密运算执行代价高的弱点,提出基于策略的椭圆曲线双线性对加密算法的信任协商隐私信息保护(PBE-PP)方案。该方案在 BDH 问题困难的假设下,在随机预言模型中证明是 IND-Pol-CCA 安全的。与隐藏证书和其它基于策略加密方案相比,执行效率更高、安全性更好、密文长度更短。

关键词:自动信任协商;隐私;加密;双线性对;CDH-问题
中图分类号:TP309.2 **文献标志码**:A

Police-based encryption for privacy protection of trust negotiation

YU Ling[a], *CHEN Shu-yu*[b]
(a. College of Computer Science; b. College of Software Engineering, Chongqing University, Chongqing 400044, P. R. China)

Abstract: Privacy protection technologies of automated trust negotiation have witnessed great development, among which hidden credentials is an admittedly more satisfactory one. However, for hidden credentials, there exists fatal weakness of blindly decryption, which results decryption execution costly. To solve the problem, using bilinear pairings over elliptic curves, a policy-based encryption for privacy protection is proposed. Under the assumption of BDH problem, the scheme is proven to be IND-Pol-CCA safety in the random prediction model. Compared with hidden credentials and other encryption solutions based on policy, this scheme is more efficient, secure and of shorter length of cipher text.

Key words: automated trust negotiation; privacy; encryption; bilinear pairings; CDH-problem

随着计算机网络和通信技术的快速发展,网络环境已从原先的相对静止、面向特定组织和用户群体的封闭网络向具有动态性、异质性、广域性特点的开放网络发展。人们对资源共享和交互的需求日益增强。基于身份鉴别的集中式访问控制,不能有效地解决处于不同管理域的陌生体之间的信任建立。Winsborough 等人[1]提出自动信任协商(automated trust negotiation,ATN)技术为陌生体之间信任关系的建立提供了新的思路和方法。但当协商的双方逐步向对方提交信任证和访问控制策略信息,以期建立信息关系的过程中,存在信任证等敏感资源信息泄漏的风险和恶意攻击。如何有效保护协商者的隐私信息成为信任协商技术的研究热点。

隐私信息一般指协商双方的协商策略和证书中

收稿日期:2010-09-21
基金项目:重庆市自然科学基金 CSTC 资助项目(2008BB2307)
作者简介:喻玲(1972-),女,重庆大学博士,主要从事网络安全管理、网格计算方向研究。(Tel)023-65127610;
陈蜀宇(1962-),男,重庆大学博导,主要从事网格计算、容错与诊断、信息安全方向研究。(E-mail)443639424@qq.com。

所包含的、涉及到双方隐私甚至机密信息以及相关辅助信息。策略是为了保护资源所定义的一些规则。证书是协商者属性的集合体。信任协商技术中涉及的敏感、隐私对象可能是目标资源、服务、数字证书、访问控制策略甚至是资源请求。Seamons 等人[2]分析总结了信任协商过程中可能存在的 3 种隐私漏洞，一是敏感证书拥有与否的推断，二是敏感证书属性的探测，三是大量不相关证书信息的暴露，造成不期望的信息泄漏。Winsborough 等人[3]分析了可能造成敏感信息泄漏的协商过程中的 4 类非授权推测，即向前肯定推测、向前否定推测、向后肯定推测、向后否定推测。E. Bertino 等人[4]认为敏感证书可以通过选择性暴露其中的敏感属性而进行高效的隐私保护，同时分析了谁先（“go first”）问题带来的敏感信息泄漏。总体来说，目前研究的 ATN（自动信任协商）隐私信息主要分为 2 大类：一类是内容敏感，包括证书、证书中的某些属性、访问控制策略等，这些都属于显示敏感信息；另一类是拥有敏感，指协商方在响应和信息交互过程中隐式地暴露的敏感信息。

为了有效防止信任协商过程中各类敏感信息的泄露和免受恶意攻击，人们从不同保护对象入手进行研究。大体可分为 4 类。1）敏感证书保护。Seamons 等人[2]提出“non-response”方法，即拥有敏感证书时不应答来保护拥有敏感的证书，很明显这不是一个令人满意的解决办法，因为很容易造成协商没法成功建立。随后他们提出改进方案，让不拥有敏感证书的协商方假装应答拥有。虽然避免了先前问题，但需要预先部署多方协同对敏感证书的一致性假装拥有应答。Yu 等人[5]提出“策略迁移”和“策略滤波”方法，尽管在一定程度上解决证书的隐私问题，但有些情况下不能保持访问的成功，有时甚至会破坏协商成功的机会。此外，“策略迁移”方法可能会开来“循环策略依赖”问题。2）敏感策略保护。Seamons 等人[6]提出策略图（policy graphs）模型解决信任关系的逐步建立。Yu 等人在此基础上加以改进，提出 UniPro（unified scheme for resource protection）模式。该技术将策略作为最优资源看待，实现策略暴露的细粒度控制。3）敏感属性保护。证书属性的选择性暴露最先是由 Holt 等人[7]提出。Ryan Jarvis[8]加以改进提出基于位承诺和盲签名相结合的选择性暴露方案。E. Bertino 等[4]提出类似的方法但没有采用盲签名技术，称之为隐私增强证书（privacy-enhanced credentials）。尽管证书的选择性暴露技术给用户提供了更细致的暴露控制，但它并不能全面解决前面提到的很多其它隐私问题，特别是一旦证书被泄漏，敏感属性信息的保护就无从谈起。Winsborough 等人[3,9]提出属性确认策略（ACK policies），对需要保护的证书，使用 ACK 函数加以标记，表示不暴露或达不到暴露的目的；并研究了一种信任目标图算法（trust target graph algorithm，TTGA）增强 ACK 策略。虽然这种机制可以保护不同的入侵攻击，但过分依赖于证书链的前向查询结果，造成协商过程无法完成；而且这种方法的协商过程非常冗长，用户不得不定义大量的复杂策略，信任协商效率较低。4）相对全面、彻底的隐私保护方法。这类方法完全不同于前面介绍的隐私保护技术，它们试图从根本上全面解决信任协商的各种隐私保护问题。Camenisch 等人提出了匿名证书系统的一系列协议标准，并构建一个原型匿名证书系统，称之为 Idemix。匿名证书系统与传统证书系统相比，更好地保护证书在相关性推断方面的抗攻击能力。Holt 等人[10]在 2003 年首次提出隐藏证书（hidden credentials）技术，较为全面的解决了信任协商过程中涉及的资源请求、证书、访问控制策略以及资源等的隐私保护。Bradshaw 等人[11]在此基础上改进秘密分割机制，Frikken 等人[12]又在 Holt 和 Bradshaw 等人研究基础上加以改进，提出了一种完全隐藏策略的协议标准。

隐藏证书技术基于椭圆曲线加密的原理（即大素数相乘容易，因式分解困难），具有较好的安全保密性和数据完整性。是迄今为止公认的较为全面解决信任协商隐私保护问题的有效方法，但因为隐藏证书技术中认为策略也是敏感信息，所以解密操作存在严重的盲目性，即解密一方不得不尝试性提供自己拥有的每一个证书进行解密，并且要尝试性找出所需解密证书的正确组合关系。这就使隐藏证书技术耗费大量的解密计算成本。而实际上，隐藏证书技术并没能对访问控制策略进行有效保护，因为资源请求方在正确解密后，仍然可以获得资源提供方对资源的访问控制策略。所以，针对隐藏证书技术的不足，权衡不能有效保护策略而又付出高额运算成本的代价，提出利用双线性对的基于策略加密的隐私保护技术（PBE-PP），该方案优化了解密算法，缩短了密文长度，提升证书信息的安全性，从而提高了信任协商隐私保护的执行成效。

1　预备知识

1.1　双线性对（bilinear pairings）

双线性对的定义和性质详见参考文献[13]。这

里简要介绍一下双线性对的特点。令 G_1 是 P 生成的循环加法群，阶为 q，G_2 是具有相同阶 q 的循环乘法群，a，b 是 Z_q^* 中的元素。双线性对是指满足下列性质的一个映射 $\hat{e}:G_1\times G_2\to G_2$：

1)双线性(bilinear)。对于 $P,Q\in G_1$，$a,b\in Z_q^*$，$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$；

2)非退化性(non-degenerate)。存在 $P,Q\in G_1$，使得 $\hat{e}(P,Q)\neq 1$；

3)可计算性(computable)。对所有的 $P,Q\in G_1$，存在有效的算法计算 $\hat{e}(P,Q)$。

双线性映射 $\hat{e}$ 可以通过有限域上的超椭圆曲线上的 Tate 对和 Weil 对来构造。提出的加密方案依赖于以下的困难问题。

1)计算 DH 问题(CDHP)

定义 1 设 G_1,G_2 为阶数为素数 q 的 2 个循环群，$\hat{e}:G_1\times G_2\to G_2$ 为 1 个双线性映射，P 为 G_1 的生成元。则 $[G_1,G_1,\hat{e}]$ 上的(CDHP)问题是：对任意 a，$b\in Z_q^*$，由 $<P,aP,bP>$，计算 abP。

2)双线性 DH 问题(BDHP)

定义 2 设 G_1,G_2 为阶数为素数 q 的 2 个循环群，$\hat{e}:G_1\times G_2\to G_2$ 为 1 个双线性映射，P 为 G_1 的生成元。则 $[G_1,G_1,\hat{e}]$ 上的(BDHP)问题是：对任意 a，$b,c\in Z_q^*$，由 $<P,aP,bP,cP>$，计算 $\hat{e}(P,P)^{abc}$。

3)判定双线性 DH 问题(DBDHP)

定义 3 设 G_1,G_2 为阶数为素数 q 的 2 个循环群，$\hat{e}:G_1\times G_2\to G_2$ 为 1 个双线性映射，P 为 G_1 的生成元。则 $[G_1,G_1,\hat{e}]$ 上的(DBDHP)问题是：对任意 $a,b,c\in Z_q^*$，由 $<P,aP,bP,cP>$ 和 $h\in G_2$，判断 $h=\hat{e}(P,P)^{abc}$ 是否成立。

2 基于策略加密的形式化定义

2.1 相关术语及表示

$I=\{I_1,\ldots,I_N\}$ 表示证书发行者组；

R_k 表示 I_k，$k\in\{1,\ldots,N\}$ 的公钥，s_k 是相应的主密钥；

$\zeta(R_k,A)$ 表示证书发行者 I_k 基于有效的断言 A 而生成的证书；

$<I_k,A>$ 表示证书发行者 I_k 对断言 A 的判断，$A\in\{0,1\}^*$。

基于证书的策略是由 AND 和 OR 连接的单调布尔表达式，而 CNF 和 DNF 范式可以转换为 CDNF(conjunctive-disjunctive normal form)标准范式。因此策略 Pol 可以表示为 $\mathrm{Pol}=\wedge_{i=1}^{m}[\vee_{j=1}^{m_i}[\wedge_{k=1}^{m_{i,j}}<I_{k_{i,j,k}},A_{i,j,k}>]]$，其中 $I_{k_{i,j,k}}\in I$，$A_{i,j,k}\in\{0,1\}^*$，当 $\{m_{i,j}=1\}_{i,j}$ 时，CDNF 范式就是 CNF 范式；当 $m=1$ 时，CDNF 范式就是 DNF 范式。

2.2 形式化定义

1 个基于策略的加密机制是由 5 个算法构成，即 Setup，Issuer-Setup，CredGen，PolEnc 和 PolDec。

Setup 系统参数建立：输入安全参数 k，Setup 产生一组公共参数 P，信息空间 $\mathfrak{M}$，密文空间 C。

Issuer-Setup 证书发行者参数建立：证书发行者 $I_k\in I$ 产生随机主钥 s_k 和对应的公钥 R_k。

CredGen 产生证书：输入证书发行者 $I_k\in I$ 的公钥 R_k，以及断言 $A\in\{0,1\}^*$，该算法返回证书 $\zeta(Rk,A)$。

PolEnc 基于策略的加密：输入信息 $M\in\mathfrak{M}$、策略 Pol，该算法返回密文 $C\in C$，即采用策略 Pol 对信息 M 的加密密文。

PolDec 基于策略的解密：输入密文 $C\in C$，策略 Pol，满足策略条件的证书 $\sigma_{j_1,\ldots,j_m}(\mathrm{Pol})$，该算法返回信息 $M\in\mathfrak{M}$ 或 $\perp$。

上面的算法满足 $C=\mathrm{PolEnc}(M,\mathrm{Pol})\Rightarrow\mathrm{PolDec}(C,\mathrm{Pol},\zeta_{j_1,\ldots,j_m}(\mathrm{Pol}))=M$，存在 $\{j_i\in\{1,\ldots,m_i\}\}_{i=1}^{m}$。

3 基于策略加密的隐私保护方案(PBE-PP)

在具体描述基于策略的加密机制前，需定义算法 BDH-Setup：输入安全参数 k，产生 $(q,G_1,G_2,\bar{e},P)$，其中 $\bar{e}:G_1\times G_1\to G_2$。基于策略的椭圆曲线双线性对加密算法如下

Setup：输入安全参数 k，执行如下步骤

1)执行算法 BDH-Setup，产生 $(q,G_1,G_2,\bar{e},P)$；

2)令 $\mathfrak{M}=\{0,1\}^{n-n_0}$，$C=G_1\times(\{0,1\}^n)^*$，$(n,n_0\in\mathbf{N}^*$ 并且 $n_0\leqslant n)$；

3)定义 3 个 hash 函数：$H_0:\{0,1\}^*\to G_1$，$H_1:\{0,1\}^*\to Z_q^*$，$H_2:\{0,1\}^*\to\{0,1\}^n$；

4)定义 $I=(q,G_1,G_2,e,P,n,n_0,H_0,H_1,H_2)$。

Issuer-Setup：$I=(I_1,\ldots,I_N)$ 表示证书发行者组，每个证书发行者 $I_k\in I$ 随机选取一个主密钥 $s_k\in\mathbf{Z}_q^*$，产生相应的公钥 $R_k=s_k\cdot P$。

CredGen：输入证书发行者 $I_k\in I$，断言 $A\in\{0,1\}^*$，输出证书 $\zeta(R_K,A)=s_k\cdot H_0(A)$。

PolEnc：输入信息 $M\in\mathfrak{M}$，策略 pol，执行

1)随机选取 $M_i\in\{0,1\}^{n-n_0}$ (for $i=1,\ldots,m-1$)，计算 $M_m\oplus(\oplus_{i=1}^{m-1}M_i)$；

2)随机选取 $t_i \in \{0,1\}^{n_0}(i=1,\ldots,m)$；

3)计算 $r=H_1(M_1 \| \ldots \| M_m \| t_1 \| \ldots \| t_m)$，再计算 $U=r \cdot P$；

4)计算 $\pi_{i,j}=\prod_{k=1}^{m_{i,j}} e(R_{k_{i,j,k}}, H_0(A_{i,j,k}))$，$(j=1,\ldots,m_i, i=1,\ldots,m)$；

5)计算 $u_{i,j}=H_2(\pi_{i,j}^r \| i \| j)$，$v_{i,j}=(M_i \| t_i) \oplus u_{i,j}$，$(j=1,\ldots,m_i, i=1,\ldots,m)$；

6)返回 $C=(U,[[v_{i,j}]_{j=1}^{m_i}]_{i=1}^{m})$

从 PolEnc 加密算法可知，每个连接条件 $\wedge_{k=1}^{m_{i,j}} <I_{k_{i,j,k}}, A_{i,j,k}>$ 首先是和掩码 $u_{i,j}$ 相关，而 $u_{i,j}$ 依赖于特定条件的不同证书。加密信息 M 被划分为 m 个随机片段 $[M_i]_{i=1}^{m}$，对于每个 $i \in \{1,\ldots,m\}$，$M_i \| t_i$ 与条件 $\vee_{j=1}^{m_i} \wedge_{k=1}^{m_{i,j}} <I_{k_{i,j,k}}, A_{i,j,k}>$ 相关，其中 t_i 是一个随机选择的中间值。每个 $M_i \| t_i$ 都采用掩码 $u_{i,j}$ 加密 m_i 次。为了能够还原加密信息，对方需要利用策略 Pol 所设定的证书去获取所有的相关数据。

PolDec：输入密文 $C=(U,[[v_{i,j}]_{j=1}^{m_i}]_{i=1}^{m})$，策略 Pol 和满足策略的证书组 $\sigma_{j_1},\ldots,j_m(Pol)$，执行

1) 计算 $\tilde{\pi}_{i,j_i}=e(U, \sum_{k=1}^{m_{i,j}} \zeta(R_{k_{i,j,k}}, A_{i,j,k}))(\text{for } i=1,\ldots,m)$；

2)计算 $\tilde{u}_{i,j_i}=H_2(\tilde{\pi}_{i,j_i} \| i \| j_i)$，再计算 $(M_i \| t_i)=v_{i,j_i} \oplus \tilde{u}_{i,j_i}$；

3)计算 $r=H_1(M_1 \| \ldots \| M_m \| t_1 \| \ldots \| t_m)$；

4)如果 $U=r \cdot P$，那么返回 $M=\oplus_{i=1}^{m} M_i$，否则返回。

上述算法满足了标准的一致性约束，而实际上，这恰恰是双线性对的双线性特征。即 $\tilde{\pi}_{i,j_i}=e(r \cdot P, \sum_{k=1}^{m_{i,j_i}} s_{k_{i,j,k}} \cdot H_0(A_{i,j_i,k})) = \prod_{k=1}^{m_{i,j_i}} e(s_{k_{i,j,k}} \cdot P, H_0(A_{i,j_i,k}))^r = \pi_{i,j_i}^r$，所以基于对技术的加密操作本质上是对计算。

4　安全性分析

4.1　安全模型

安全模型是密码学机制的基础，密码学机制的安全性大多依赖某种数学难题的假设，在一定安全模型下达到某种安全强度。满足不可区分适应性选择密文攻击的安全性(IND-CCA)[14]是公钥加密机制的标准安全模型，基于身份的加密机制(IBE)是IND-ID-CCA，那么基于策略的加密机制就是 IND-Pol-CCA。

安全模型定义为挑战者和敌手之间的交互游戏。IND-ID-CCA 允许敌手获得所选择的任何身份对应的私钥，此外允许敌手选择希望挑战的身份，而在标准的 IND-CCA 模型中，敌手被随机选择的公钥挑战。那么，类似的，安全模型就应该允许敌手获得满足他所选择的任何策略的证书，而不是他被挑战的策略的对应证书。此外，敌手应该被允许指定挑战的策略。

游戏由 5 步骤构成：Setup，Phase-1，Challenge，Phase-2，Guess，具体如下

1)系统参数建立(Setup)。输入安全参数 k，挑战者首先执行 Setup 算法获得系统公共参数 P，然后，挑战者执行 Issuer-Setup 一次或多次以获得一组证书发行者 $I=\{I_1,\ldots,I_N\}$。最后，挑战者给敌手公共参数 P 以及 I 中不同的信任授权者的公钥。

2)阶段 1(Phase-1)。对手执行 1 个适应性预言查询多项式，每个查询可能依赖于前门执行过的查询。

3)挑战(Challenge)。一旦阶段 1 完成，敌手就会给挑战者 2 个等长的信息 M_0，M_1，以及它希望被挑战的策略 pol_{ch}。挑战者随机选取 $b \in \{0,1\}$，以 (M_b, Pol_{ch}) 为输入执行算法 PolEnc，将结果密文 C_{ch} 返回对手。

4)阶段 2(Phase-2)。对手再次执行一个适应性预言查询多项式。

5)猜测(Guess)。对手输出猜测 b'，如果 $b=b'$，那么赢得游戏。

阶段 1 和阶段 2，敌手执行了 2 个受控于挑战者的预言查询，一个是产生证书的预言，表示为 Cred-Gen-O，另一个是基于策略解密的预言，表示为 PolDec-O。2 个预言定义如下

CredGen-O。根据输入 (I_k, A)，其中 $I_k \in I$，$A \in \{0,1\}^*$，执行算法 CredGen，返回证书 $\zeta(R_k, A)$。

PolDec-O。根据输入 $c \in C$，策略 Pol，以及 $\{j_1,\ldots,j_m\}$，首先执行算法 CredGen 多次，获得符合条件的证书组 $\zeta_{j_1,\ldots,j_m}(\text{Pol})$，然后执行算法 $\text{PolDec}(C, \text{Pol}, \zeta_{j_1,\ldots,j_m}(\text{Pol}))$，返回结果。

定义 1　在 IND-Pol-CCA 游戏中，对手 A 赢得游戏的优势定义为 $Adv_A=\left|\Pr[b=b']-\frac{1}{2}\right|$。如果没有任何多项式有界的敌手以不可忽略的优势赢得游戏，那么称 PBE 机制是 IND-Pol-CCA 安全的。

4.2　PBE(policy-based encryption)的安全性

下面证明 PBE 机制在随机预言模型(random oracle Model，ROM)是 IND-Pol-CCA 安全的。

定理 1　设定 A° 是 1 个 IND-Pol-CCA 的敌手，

在攻击 PBE 机制时拥有优势 $Adv_{A^\circ} \geqslant \varepsilon$。假定 A° 已经运行 t_{A^0}，对预言 CredGen-O 产生至少 q_c 次的查询，对预言 PolDen-OCA 产生至少 q_d 次的查询，对预言 H_0 产生至少 q_0 次查询。那么，假如存在 1 个 IND-CCA 的敌手 A°，在攻击 NewBasicPub^{hy} 机制时，优势为 $Adv_{A^\circ} \geqslant F(q_c, q_d, q_0, N, m_{\wedge\vee}, m_\wedge, m_\vee) \cdot \varepsilon$，它的运行时是 $t_{A^\circ} = O(t_{A^\circ})$。文献[15,16]对该定理已做证明。

定理 2　基于双线性对 DH 问题(BDHP)的困难，PBE 机制在随机预言模式中是 IND-Pol-CCA 安全的。

证明　定理 2 遵循了图 1 的 1 个减少论据的顺序。

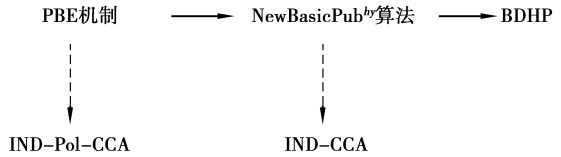

图 1　PBE 机制是 IND-Pol-CCA 安全的论证顺序

1)定理 2 表明，基于 PBE 机制的 IND-Pol-CCA 攻击能够转换成基于 NewBasicPub^{hy} 算法机制的 IND-CCA 攻击。

2)在文献[15]中，NewBasicPub^{hy} 算法证明了，假定 BDHP 问题困难，在随机预言模型(ROM)中是 IND-CCA 安全的。

综上所述，PBE 机制基于 BDH 问题困难的假设，在随机预言模型中可证明安全性。

4.3　性能分析

在表 1 中，对比分析了该隐私保护方案与文献[16]、[11]方案在加密、解密算法处理时间以及密文长度的对比，其中，l_1 代表双线性表示法的比特位长度。

表 1　3 种隐私保护机制的性能比较

隐私保护类型	加密	解密	密文长度
PBE-PP 机制	$\sum_{i=1}^{m}\sum_{j=1}^{m_i} m_{i,j}$	m	$l_1+(\sum_{i=1}^{m} m_i)\cdot n$
文献[14]的隐私保护机制	$\sum_{i=1}^{m}\sum_{j=1}^{m_i} m_{i,j}$	m	$l_1+(\sum_{i=1}^{m} m_i)\cdot n+n$
文献[11]的隐藏证书机制	$\sum_{i=1}^{m}\sum_{j=1}^{m_i} m_{i,j}$	$\sum_{i=1}^{m} m_{i,j_i}$	$l_1+(\sum_{i=1}^{m}\sum_{j=1}^{m_i} m_{i,j})\cdot n+n$

从对比分析可以看出，3 种机制的加密算法，计算量相同的，但 PBE-PP 和文献[16]的解密算法比文献[11]执行效率更高，因为 $m_{i,j_i} \geqslant 1, i=1,\ldots,m$。此外，PBE-PP 机制密文长度为 $l_1+(\sum_{i=1}^{m} m_i)\cdot n$，比其他 2 种机制的密文更短，而安全性更高。

5　结　论

隐藏证书技术尽管经过多人的不断优化，但因策略对解密方的未公开性，使得该技术存在运算成本高昂，执行效率低的缺点。基于策略对解密方公开，提出了一种采用双线性对的基于策略加密的信任协商隐私保护方案，并在随机预言模型中给予了安全性证明。在 BDH 问题是困难的假设下，该方案被证明是安全的。与目前的基于策略的加密方案和隐藏证书技术相比，PBE-PP 方案执行效率更高，安全性更强，密文长度更短。下一步工作重点放在提高信任协商隐私保护的执行效率、安全性以及兼顾各种敏感信息的全面保护研究上。

参考文献：

[1] WINSBOROUGH W, SEAMONS K, JONES V. Automated trust negotiation[C]//Proceedings of DARPA Information Survivability Conference and Exposition, 25-27 January 2000, Hilton Head, SC, USA. New York: ACM Press, 2000: 88-102.

[2] SEAMONS K, WINSLETT M, YU T, et al. Protecting privacy during on-line trust negotiation[C]//Privacy Enhancing Technologies. Second International Workshop, PET 2002, April 14-15, 2002, San Francisco, CA, USA. Berlin, Germany: Springer, 2003: 129-143.

[3] WINSBOROUGH W, LI N. Protecting sensitive attributes in automated trust negotiation[C]//Proceedings of the ACM Conference on Computer and Communications Security, November 18-22, 2002, Washingtion, DC, USA. New York ACM Press, 2002:41-51.

[4] BERTINO E, FERRARI E, SQUICCIARINI A. Privacy-preserving trust negotiations[C]//Privacy Enhancing Technologies. 4th International Workshop, PET 2004, May 26-28, 2004, Toronto, Canada. Berlin, Germany: Springer, 2004: 283-301.

[5] YU T, WINSLETT M. Policy migration for sensitive credentials in trust negotiation[C]//Proceedings of the ACM Workshop on Privacy in the Electronic Society, WPES 2003, October 30, 2003, Washington, DC, USA. New York: ACM, 2003:9-20.

[6] SEAMONS K, WINSLETT M, YU T. Limiting the disclosure of access control policies during automated

trust negotiation[C]//8th Annual Symposium on Network and Distributed System Security (NDSS01), February 8-9, 2001, Sand Diego, California, USA. [S.l.]: CiteSeer, 2001: 16-20.

[7] HOLT J, SEAMONS K. Selective disclosure credential sets[J/OL]. http://citeseer.nj.nec.com/541329.html.

[8] JARVIS R. Protecting sensitive credential content during trust negotiation[C]//Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society, November 21, Washington, DC, USA. [S.l.]: CiteSeer, 2002:41-51.

[9] WINSBOROUGH W, LI N. Towards practical automated trust negotiation[C]//Proceedings Third International Workshop on Policies for Distributed Systems and Networks, 5-7 June 2002, Monterey, CA, USA. [S.l.]: CiteSeer,2002:92-103.

[10] HOLT J, BRADSHAW R, SEAMONS K, et al. Hidden credentials[C]//Proceedings of the ACM Workshop on Privacy in the Electronic Society, WPES 2003, October 30, 2003, Washington, DC, USA. New York: ACM,2003: 1-8.

[11] BRADSHAW R, HOLT J, SEAMONS K. Concealing complex policies with hidden credentials[C]//Proceedings of the ACM Conference on Computer and Communications Security, CCS 2004, October 25-29, 2004, Washington, DC, USA. New York: ACM, 2004: 146-157.

[12] FRIKKEN K, ATALLAH M, LI J. Hidden access control policies with hidden credentials[C]//WPES'04: Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society, October 28-28, 2004 Washington DC, USA. New York: ACM, 2004:27-28.

[13] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[J]. SIAM Journal on Computing, Springer, 2003, 32(3): 586-615.

[14] RACKOFF C, SIMON D. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack [C]//Advances in Cryptology-CRYPTO '91, August 11-15, California, USA. Berlin, Germany: Springer, 1992: 433-444.

[15] GALINDO D, BONEH F. Identity based encryption revisited[C]//Automata, Languages and Programming. 32nd International Colloquium, ICALP 2005, July 11-15, 2005, Lisbon, Portugal. Computer Science, 2005: 791-802.

[16] BAGGA W, MOLVA R. Policy-based cryptography and applications[C]//Financial Cryptography and Data Security, 9th International Conference, FC 2005, February 28-March 3, 2005, Roseau, The Commonwealth Of Dominica. Computer Science,2005(3570): 72-87.

[17] CAI G, WANG Y, ZHU Z, et al. An improved trust negotiation protocol with hidden credentials[C]//International Conference on Computational Intelligence and Security Workshops, December 15-19, Heilongjiang, China. Washington, DC,USA: IEEE Computer Society, 2007: 510-513.

[18] JIN H, LIAO Z, ZOU D, et al. An asymmetrical encryption based automated trust negotiation model[C/OL]//Second IEEE International Conference on Digital Ecosystems and Technologies, Phitsanulok, Thailand, Febuary 26-29, 2008[2008-09-30]. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4635156.

[19] LU YANG, LI JI-GUO, XIAO JUN-MO. Constructing efficient certificate-based encryption with pairing[J]. Journal of Computers,2009,4(1):19-26.

[20] LI J G, HUANG X Y, MU Y, et al. Cryptanalysis and improvement of an efficent certificateless signature scheme[J]. Journal of Communications and Networks, 2008,10(1):10-17.

[21] WANG L, SHAO J, CAO Z, et al. A certificate-based proxy cryptosystem with revocable proxy decryption power[C]//Proceedings of the cryptology 8th international conference on Progress in cryptology, December 9-13, Chennai, India. Berlin, Germany: Springer-Verlag, 2007:297-311.

[22] LI JI-GUO, JIANG PING-JIN. An efficient and provably secure identity-based signature scheme in the standard model[J]. Journal of Computers, 2009, 32(11):2130-2136.

[23] LI F G, HU Y P, LI G. An efficient identity-based signcryption scheme[J]. Journal of Computers, 2006, 29(9):641-1647.

[24] TIAN Y, ZHANG Y J, LI Z C. A survey of identity-based cryptography using pairing[J]. Journal of Computer Research and Development, 2006, 43(10): 1810-1819.

(编辑　侯　湘)