DOI:10.14188/j.1671-8836.2008.05.029
第54卷 第5期 武汉大学学报(理学版) Vol.54 No.5
2008年10月 J. Wuhan Univ.(Nat.Sci.Ed.) Oct. 2008, 607~610

文章编号:1671-8836(2008)05-0607-04

多授权中心可验证的基于属性的加密方案

唐 强, 姬东耀†

(信息安全国家重点实验室/中国科学院研究生院, 北京 100049)

摘 要: 在本文构造的方案中, 将可验证的属性加密方案由单个授权中心推广到多个授权中心, 使得多授权中心的基于属性的加密在解密出错时, 可以检验出是哪个授权中心部分的密钥出错, 只需要去找该授权中心重发, 不用让所有授权中心均重发; 其次各个授权中心在被检查出错时, 也只需要重发对应部分的信息; 当密钥通过验证, 而解密依然出错, 说明是加密过程中或者密文跟随的消息属性出了问题, 不会出现无法判断哪里出错的情况. 同时证明了加入可验证性后, 在经过修正的安全模型下, 并不影响多授权中心基于属性加密的安全性.

关 键 词: 基于属性的加密; 多授权中心; 可验证秘密分享; 可证安全

中图分类号: TP 309 文献标识码: A

0 引 言

具有良好性质的密码学基本模块的研究对于密码学理论的发展和应用具有很重要的意义, 基于属性的加密(ABE)就是这样一类基本模块, 它是基于身份加密的一个延伸, 身份用一系列描述性的属性表示, 具有一些良好的性质. 传统的公钥加密如RSA, 通信双方确定, 而ABE最突出的优点是很适用于分布式环境下解密方不固定的情况, 加密方加密信息时不需知道具体是谁解密, 而解密方只要符合相应条件, 便可解密. 通过对它的研究, 可以利用它来构造一些具有相应良好性质的其他密码学模块.

在Shamir提出基于身份体制[1]的概念和Boneh构造出第一个实用的基于身份加密体制[2]后, Sahai和Waters提出模糊的基于身份的加密方案[3], 在该方案中, 身份由一组刻画用户的属性来描述, 经某一属性集加密的消息可以由和该属性集交集较大的一些属性集刻画的用户解密, 第一次利用秘密分享的思想, 引入了ABE的概念.

Goyal等人在文献[3]中提出的属性加密的基础上, 将解密条件扩展成一般的单调访问控制结构, 构造出可支持细粒度访问控制的密钥策略的ABE方案, 并引入一般秘密分享[4]的思想, 其访问结构为一般单调访问结构, 大大扩展了ABE的应用范围[5].

Bethencourt等针对Goyal等的密钥策略的属性加密方案, 提出了更接近于现实访问控制系统的密文策略的属性加密方案[6], 但是在证明中, 该方案的安全性假设基于的困难问题不是著名难题. 为了解决上述安全性的问题, Cheung等提出一个基于DBDH问题的密文策略的ABE方案[7], 但是访问策略没有达到一般的访问控制结构, 他的访问结构只是正负属性描述和AND操作.

以上所有的ABE方案都是单个认证授权中心来进行密钥的计算分发工作, 负担较重, 风险较大, 而且对密钥分发中心的信任要求是无条件的. 于是Chase提出了多授权中心的ABE系统[8], 密钥分发, 属性认证等分到各个部门, 各自维护各自部门属下的内容, 一方面更加细致准确地描述了属性, 一方面大大降低了单个认证中心的负担.

在多授权中心的属性加密的内容不能被合法用户解密时, 无法判定是密钥还是密文出了问题, 更不知道是哪个授权中心出了问题, 本文就是解决这个问题.

唐强, 姬东耀提出可验证ABE方案[9], 将可验证秘密分享[10]的思想引入, 使得在密钥分发中心分发密钥时, 如果检验出错, 可以让分发中心重新计算

收稿日期: 2008-03-20 † 通讯联系人 E-mail: dyji@gucas.ac.cn

基金项目: 国家重点基础研究发展计划(973)项目(2007CB311202); 国家高技术研究发展计划(863)项目(2006AA01Z427); 国家自然科学基金资助项目(90604010)

作者简介: 唐 强(1984-), 男, 硕士生, 现从事应用密码学与安全协议理论的研究. E-mail: qtang84@gmail.com

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

发送相应那部分的密钥,不用全部重新来算;并且如果密钥通过检验,而解出的密文仍有问题,就很可能是密文的问题,该去找加密方,而不会不知道是该找加密方还是分发中心.该方案给出了可验证 ABE 方案的形式化定义,并且在经过修正的选择属性集合模型里 DBDH 假设下也证明安全.

本文针对多授权中心的属性加密方案,提出了多授权中心的可验证的属性加密方案,它的好处除了具有单授权中心基于属性加密的上述优点外,在多密钥分发中心情况下,如果检测出错误,还能够找到是哪个分发中心出的错,这样就只需要与该分发中心联系重发,并不需要像 Chase 的多认证中心属性加密方案那样与所有分发中心联系重发.本文在给出具体的方案后,给出了安全模型和简单的安全性分析.

1 背景知识

双线性对与 DBDH 假设概念见文献[3].

由于下面设计的多授权中心的可验证的基于属性的加密方案中,各个授权中心需要用到文献[9]中的可验证的基于属性的加密,所以这里简要介绍该方案的密钥生成和验证算法.

其过程是用户根据属性对消息明文加密,接收方提交访问结构,授权中心审核后根据该访问结构生成解密密钥以及可供验证的信息,如果访问结构满足属性集,通过验证的密钥便可用于解密出这个属性集下加密的消息.

访问结构为树形,可参考文献[3]中的树形访问结构.

参考文献[9]中授权中心根据树形访问结构,生成私钥以及验证信息.

2 方案构造

2.1 算法步骤

多授权中心的可验证的基于属性的加密方案有 K 个授权中心和一个中央认证中心(CA),它们运行以下这些算法步骤:

● 系统初始化:由可信方(如中央认证中心)输入安全参数,运行一个随机算法,输出各个授权中心的公私钥对和中央认证中心的主密钥和系统公钥,输出公用参数,群 G_1, G_2,双线性对 e,生成元 g 等.

● 授权中心密钥及验证信息生成:每个授权中心运行一个随机算法,输入该中心的公私钥,授权中心需要使用的公共参数,可以标识用户的 Id,以及用户在该授权中心下的属性集,输出授权中心给用户的私钥和可供于验证的附加信息.

● 中央认证中心密钥及验证信息生成:中央认证中心运行一个随机算法,以自己的主密钥和公钥,标识用户的 Id 作为输入,输出中央中心给用户的私钥和可供验证的附加信息.

● 加密:发送方输入消息明文,每个授权中心赋予的属性集和公钥,执行一个随机算法,输出密文.

● 验证:接收方拿到各个授权中心给的密钥和供验证的附加信息,执行各认证中心的验证算法,检验该密钥是否正确;然后输入中央认证中心的密钥和附加信息,再执行中央认证中心的验证算法,检验中央认证中心的密钥是否正确.若都正确,输出 1,否则输出 0.

● 解密:当验证算法输出 1 时,输入密文,密钥,访问结构,属性集,当且仅当用户的访问结构满足消息的属性,则输出消息明文.

2.2 构造方法

假定授权中心个数为 K,每个授权中心的属性个数不超过 n.

● 系统初始化:由安全参数得到素数 p 阶群 G_1, G_2,双线性对 $e: G_1 \times G_1 \to G_2$, G_1 的一个生成元 g,生成伪随机函数簇 $\{F_{s_i}\}_{i=1,\cdots,k}$, s_1, …, s_k 分别为各授权中心的私钥种子,随机选择 y_0, $\{t_{k,i}\}_{k=1,\cdots,k,\ i=1,\cdots,n} \in Z_q$,并令 $Y_0 = e(g,g)^{y_0}$ 为系统公钥.

● 授权中心 k 密钥及验证信息生成:它的私钥为 s_k, $t_{k,1}$, …, $t_{k,n}$.它的公钥为 $T_{k,1}$, …, $T_{k,n}$,其中 $T_{k,i} = g^{t_{k,i}}$.对于 Id 为 u 的用户,计算 $y_{k,u} = F_{s_k}(u)$,以 $y_{k,u}$ 为该授权中心的私钥,在该授权中心管理的属性集 A_k 和访问控制结构 $\Gamma_{k,u}$ 下,运行可验证基于属性的加密的密钥生成算法,输出用户 u 的该授权中心颁发的私钥 $\{D_{k,i} = g^{p(i)/t_{k,i}}\}_{i \in A_{k,u}}$ 和验证信息 $C_{k,u}$:

$$\{\{h_x = e(g,g)^{q_x(0)}\}, \{e(g,g)^{a_i}\}\}$$

其中,a_i 为各多项式系数.

● 中央认证中心密钥及验证信息生成:它的私钥为 s_1, …, s_k 以及 y_0,对用户 u,中央认证中心给它的私钥为 $D_{CA,u} = g^{y_0 - \sum_{k=1}^{K} y_{k,u}}$,同时,该认证中心维护一张表,它有 $K+1$ 列,而每行对应一个用户,每个格子中,中央认证中心放入 $Y_{k,u} = e(g,g)^{y_{k,u}}$,最后一列放入 $D_{CA,u} = e(g,g)^{y_0 - \sum_{k=1}^{K} y_{k,u}}$.有一个新用户请

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

求解密密钥, 中央认证中心就添加一行.

● 加密: 用户对消息明文 M, 根据属性集 A_m, 随机选择 $s \in Z_p$, 加密得到密文为:

$$\{E = Y_0^s M, E_{CA} = g^s, \{E_{k,i} = T_{k,i}^s\}_{i \in A_{m,k}, k=1,\cdots,k}\}$$

● 验证: 得到每个授权中心的验证信息 $C_{k,u}$ 后, 执行可验证基于属性的加密的验证算法, 验算:

$$e(D_x, T_i) = h_x = h_{\text{parent}(x)} \times \prod_{i=1}^{k-1} (e(g,g)^{a_i})^{\text{index}(x)^i}$$

一直重复验算到顶点, 检查该授权中心的密钥有无差错, 如果有错, 要求这个授权中心重发对应部分; 如果所有授权中心的密钥都通过检验, 检查中央认证中心维护的那个表, 用各个授权中心的验证信息, 检查表中对应的内容, 并检查是否满足 $Y_0 = Y_{CA,u} \times \prod_{k=1}^{K} Y_k$, 若不满足, 要求中央认证中心重新计算密钥, 若满足, 验证算法输出 1, 其他情况都输出 0.

● 解密: 如果验证算法输出为 1, 解密方拿到密文、密钥后, 当且仅当用户的访问结构 Γ_u 满足属性集合 A_m 时, 可以输出消息明文 M. 解密过程如下: 对每个授权中心的私钥, 先从叶子结点 x 计算 $e(E_{k,i}, D_{k,i}) = e(g^{t_{k,i}}, g^{p_x(i)/t_{k,i}}) = e(g,g)^{p_x(i)s}$, 然后通过拉氏插值, 逐步往上插值, 最后到顶点得到 $Y_{k,u}^s = e(g,g)^{p(0)s} = e(g,g)^{y_{k,u}s}$. 对中央认证中心的私钥, 计算 $Y_{CA,u}^s = e(E_{CA}, D_{CA,u})$. 由所有这些信息, 用户可计算出 $Y_0^s = Y_{CA,u}^s \times \prod_{k=1}^{K} Y_k^s$, 那么消息明文 $M = E/Y_0^s$.

3　安全性分析

3.1　安全模型

初始化: 敌手公开他要攻击的属性集合 A, 分到每个授权中心, 并公开已经被攻击的一些授权中心, 不包括中央认证中心; 挑战者运行系统初始化算法, 产生公共参数和公钥给敌手, 这些信息包括系统公钥, 各授权中心公钥, 被攻击授权中心私钥.

密钥查询 1: 敌手向中央认证中心和各授权中心询问相关访问结构的密钥, 要求对每一个用户 u, 每次询问时至少有一个授权中心的属性不被访问结构满足, 也就是询问到的密钥不能直接用于解密要攻击的属性集合下加密的密文, 对于同一授权中心, 敌手不能查询同一个用户两次以上; 并且要求查询到供验证的信息并要求查询到的密钥通过验证.

挑战: 敌手随机选择两个消息明文 M_0 和 M_1, 挑战者随机掷币 b, 在属性集合 A 下加密 M_b, 并将密文发送给敌手.

密钥查询 2: 重复密钥查询 1 阶段的过程, 可以继续询问相关的其他密钥.

猜测: 敌手猜测挑战者加密的是哪个消息明文.

定义 **1**　如果不存在任何概率多项式时间计算能力的敌手能在上述游戏中以不可忽略的概率猜测出挑战者的随机掷币, 那么多授权中心可验证的基于属性的加密在该模型下达到语义安全.

3.2　本文构造方案的安全性

定理 **1**　如果多授权中心可验证的基于属性的加密方案中的所有验证过程均通过, 则产生的密钥可用来解密.

证　有两部分的检验过程, 第一部分是各个授权中心的验证算法, 第二部分是对中央认证中心的的验证. 而验证主要是验证分享的秘密没有错, 则可最终解密.

对各个授权中心的验证算法, 如文献[9] 中的证明, 检验:

$$e(D_x, T_i) = h_x = h_{\text{parent}(x)} \times \prod_{i=1}^{k-1} (e(g,g)^{a_i})^{\text{index}(x)^i}$$

检验在每个多项式的分享过程中, 对应的值是正确的按照规则由多项式计算出来的, 如果能够通过验证, 却不是正确的分享值的等式成立, 便能求出 $e(g,g)$的阶的一个倍数小于 p, 而它所在的群的阶为素数 p, 它的阶只能为 p, 造出一个矛盾来.

对中央认证中心的验证算法, 在各个授权中心验证到最后一环时, 有 $Y_{k,u} = e(g,g)^{y_{k,u}}$, 并作为验证信息的一部分, 拿该部分检查表中的值是否正确, 若这些都正确, 验证等式:

$$Y_0 = e(g,g)^{y_0} = e(g,g)^{y_0 - \sum_{k=1}^{K} y_{k,u}} \times \prod_{k=1}^{K} e(g,g)^{y_{k,u}} = Y_{CA,u} \times \prod_{k=1}^{K} Y_k$$

该等式通过, 若用户不能正常解密, 则用户收到的是中央认证中心发送的值 $Q = e(g,g)^y = e(g,g)^{y_0 - \sum_{k=1}^{K} y_{k,u}}$, (所有运算为模运算)则中央认证能求出 $e(g,g)$, 的阶为小于 p, 同上所述, 这是一个矛盾.

综上所述, 当验证算法在两个部分均通过, 最后输出为 1 时, 用户拿到的解密密钥的指数分母就是由系统私钥 y_0 正确分享而来, 便最终能恢复到 Y_0 从而解密.

定理 **2**　2.2 节中构造的多授权中心的可验证的基于属性的加密方案在 3.1 节构造的安全模型中语义安全.

证　该安全模型比文献[8] 中安全模型多了一

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

个密钥查询阶段的查询验证信息和要求密钥通过这些验证信息,在挑战者构造合法的密钥的时候,如文献[9]中的证明,多项式系数一定是有的,而且相应的 $g^{q_x(\cdot)}$ 也能被算出,因而各个授权中心模拟合法密钥时需要的验证信息都可以被计算出,并且能通过验证;用同样的方法可以算出中央认证中心表中的除最后一列外的所有信息,最后一列的计算类似于文献[8]中方法,可以计算出与 $g^{y_0-\sum_{k=1}^{K} y_{k,u}}$ 不可区分的值,同样可以计算出与 $e(g,g)^{y_0-\sum_{k=1}^{K} y_{k,u}}$ 不可区分的值并保证各个值之间的关系,即满足验证的等式.因而该安全模型下需要模拟出的信息都可以被挑战者模拟出,从而类似文献[8],该方案最后达到该模型下的语义安全.

4 结 论

本文介绍了基于属性加密的基本研究情况,构造了一个多授权中心的可验证的基于属性的加密方案,该方案是从可验证的基于属性的加密推广而来,并具有更好的性质,即除了可验证的基于属性的加密的优点外,还可以在出错时直接定位到出错的授权中心,使得在出错时不用去找所有授权中心核对,减轻了出错处理的负担,并且证明了加入验证信息不降低安全性.

参考文献:

[1] Shamir A. Identity-Based Cryptosystems and Signature Schemes[DB/OL].[2007-11-03]. *http://www.iseca.org/downloads/Shamir47.pdf*.

[2] Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing[J]. *SIAM Journal of Computing*, 2003, **32**: 586-615.

[3] Sahai A, Waters B. Fuzzy Identity-Based Encryption [DB/OL].[2007-11-20]. *http://www.springerlink.com/content/k0vd9xqjq4jyyp9m/fulltext.pdf*.

[4] Bonaloh J, Leicheter J. Generalized Secret Sharing and Monotone Functions[DB/OL].[2007-11-18]. *http://www.cs.cornell.edu/courses/cs754/2001fa/bena88.pdf*.

[5] Goyal V, Pandey O, Sahai A, *et al*. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data[DB/OL].[2007-11-15]. *http://portal.acm.org/ft_gateway.cfm?id=1180418&type=pdf&coll=GUIDE&dl=GUIDE&CFID=37198578&CFTOKEN=84478665*.

[6] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy Attribute-Based Encryption[DB/OL].[2007-11-22]. *http://www.cs.berkeley.edu/~bethenco/oakland07-cpabe.pdf*.

[7] Cheung L, Newport C. Provably Secure Ciphertext PolicyABE[DB/OL].[2007-11-23]. *http://people.csail.mit.edu/lcheung/papers/ccs100-cheung.pdf*.

[8] Chase M. Multi-Authority Attribute-Based Encryption [DB/OL].[2007-11-25]. *http://www.cs.brown.edu/~mchase/papers/multiabe.pdf*.

[9] Tang Qiang, Ji Dongyao. Verifiable Attribute Based Encryption[DB/OL].[2008-04-20]. *http://eprint.iacr.org/2007/461.pdf*.

[10] Beth T, Knobloch H J, Otten M. Verifiable Secret Sharing for Monotone Access Structures[DB/OL].[2007-01-05]. *http://www.springerlink.com/content/prxxadggmh97g8pt/fulltext.pdf*.

Multi-Authority Verifiable Attribute-Based Encryption

TANG Qiang, JI Dongyao

(State Key Laboratory of Information Security/Graduate University of Chinese Academy of Science, Beijing 100049, China)

Abstract: This paper generalizes the verifiable attribute-based encryption (VABE) with a single authority to the multi-authority scenario. When the authorized user could not decrypt the message in a multi-authority ABE, the user could figure out which authority's secret key has problem and ask this authority to resend the key. Secondly, when an authority's key did not pass the verification, it needs only to resend the corresponding part of the key instead of all the information for computing the key. Thirdly, if all keys are verified right, but the user still could not decrypt, then, something must be wrong with the ciphertext or the attributes. At last, we prove that adding the information for verification does not reduce the security of the multi-authority ABE.

Key words: attribute-based encryption; multi-authority; verifiable secret sharing; provable security

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net