基于时间约束的认证字典分类方法*)

周永彬[1] 卿斯汉[1] 薛 源[1] 刘 娟[2]

(中国科学院软件研究所 北京 100080)[1] (中国科学院信息安全技术工程研究中心 北京 100080)[1]

(云南民族大学历史系 昆明 650031)[2]

摘 要 认证字典是一类重要的数据结构,它在众多研究领域都具有重要的理论和应用价值,诸如科学数据挖掘、地理数据服务器、Internet 上的第三方数据发布以及 PKI 中的证书撤销等。本文介绍了认证字典的基本概念与原理;首次在认证字典模型中引入了时间约束,并据此给出了一种新的认证字典分类方法,探讨了认证字典的实现技术。最后,简要讨论了认证字典在 PKI/WPKI 中的应用。

关键词 认证字典,分类法,公钥基础设施

A Taxonomy of Authenticated Dictionary Based on Time Constraints

ZHOU Yong-Bin[1] QING Si-Han[1] XUE Yuan[1] LIU Juan[2]

(Institute of Software, Chinese Academy of Sciences, Beijing 100080)[1]

(Engineering Research Center for Information Security Technology, Chinese Academy of Sciences, Beijing 100080)[1]

(Department of History, Yunnan University for Nationalities, Kunming 650031)[2]

Abstract Authenticated Dictionary(AD) is one of the important data structures, and it is of great theoretic and applicable value in many research fields, including scientific data mining, geographic data servers, third-party data publication on the Internet and certificate revocation in public key infrastructure. Basic concept and principle of AD are examined. Time constraint is introduced into the model of AD for the first time, and a new taxonomy of AD is presented. Afterwards, implementation technologies of AD are given. Finally, applications of AD in PKI/WPKI fields are briefly described.

Keywords Authenticated dictionary, Taxonomy, Public key infrastructure (PKI)

1 引言

认证字典(Authenticated Dictionary, AD)是由 Naor 和 Nissim 提出的一类重要的数据结构[1],它在众多研究领域都具有重要的理论和应用价值,诸如科学数据挖掘、地理数据服务器、Internet 上的第三方数据发布以及 PKI 中的证书撤销等[2~4]。

认证字典所要解决的基本问题描述如下:设计一个协议,用于在一个不可信的示证者 P 和一个验证者 V 之间来对集合 S 进行隶属关系查询;这里,S 是由某个可信实体定义的一个有限集合,该集合对于 V 是未知的。信息源控制着用 S 来表示的认证字典所必需的信息。给定一个输入 x,P 可以证明 $x\in S$ 或者 $x\notin S$;同时,可信实体可以动态地改变集合的元素。

对于 AD,一般有这样的假设:在 P 和 V 交互作用时,S 是固定不变的。这一重要的假设在实际应用中具有现实意义。此外,还假定信息源是可信的;对于不可信的信息源,认证字典所要处理的实际情况将更加复杂,暂不在本文讨论的范围之内。

从参与模型的各个主体与信息流的角度出发,认证字典的基本模型可以如图 1 所示。

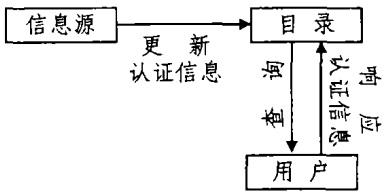

图 1 认证字典基本模型

在图 1 所示的认证字典的基本模型中,信息源就是问题描述中所指的可信实体,目录则为示证者 P,而用户就是验证者 V。示证者 P 可以访问用来表示 S 的数据结构以及关于 S 的一些公开信息,这些信息是由可信实体在设置 x 之前创建的。不可信的示证者 P 应该有一个高效的过程来对关于 x 的查询提供在线的短证明(例如:在 $|x|\cdot\log(S)$ 的多项式时间内)。这里需要特别说明的是:示证者 P 可以是一个(也通常是一个)非可信的实体。对于 AD 的实施而言,这一特点很让人费解,也常常给人造成错觉,但却是一个非常重要的特性:它大大地简化了 AD 的设计和实施。

证书撤销机制是 PKI/WPKI 中的一个核心性的基础问题。认证字典是实现这种机制的天然的数据结构。因此,认证字典在 PKI/WPKI 中具有十分广泛的应用基础。

*)国家重点基础研究发展规划资助项目(G1999035810、G1999035802)和国家自然科学基金资助项目(60083007)资助。**周永彬** 博士研究生,主要研究领域为应用密码学、网络与信息安全理论与技术;**卿斯汉** 研究员,教授,博士生导师,主要研究领域为信息安全理论与技术;**薛 源** 硕士研究生,主要研究领域为网络与信息安全理论与技术;**刘 娟** 硕士研究生,主要研究领域为民族经济与思想。

本文第2部分给出了认证字典的定义，分析了设计认证字典应该达到的目标；第3部分首次在认证字典模型中引入了时间约束，并据此给出了认证字典的一种新的分类方法；第4部分分析了实现AD的基本技术及其在PKI/WPKI中的应用；最后总结了全文。

2 认证字典的定义

记U为一个全集，S为一个集合，满足$S\subseteq U$。设D_S为表示集合S的一个数据结构。定义如下操作：

隶属关系查询 其形式为$\langle e\rangle$；对该查询的响应是一个字符串$\langle a\rangle$，满足$a\in\{YES,NO\}$，分别对应于$e\in S$和$e\notin S$。

认证的隶属关系查询 其形式为$\langle e\rangle$；对该查询的响应是一个字符串$\langle a,p\rangle$，满足$a\in\{YES,NO\}$，p是由示证者P给出的对a的真实性进行认证的一个证明。

更新操作 其形式有如下两种：

①插入操作$\langle$insert,e$\rangle$，这里$e\in(U\backslash S)$。设对D_S进行插入操作后所生成的新的数据结构为$D_{S'}$，则$S'=S\cup\{e\}$。

②删除操作$\langle$delete,e$\rangle$，这里$e\in S$。设对D_S进行删除操作后所生成的新的数据结构为$D_{S'}$，则$S'=S\backslash\{e\}$。

基于上述直观的理解，下面将对认证字典进行定义。

定义1(字典) 一个表示支持隶属关系查询和更新操作的集合S的数据结构D_S以及与所有这些操作相关的各种协议的总称。

定义2(认证字典) 一个表示支持认证的隶属关系查询和更新操作的集合S的数据结构D_S^{AU}以及与所有这些操作相关的各种协议的总称。

既然认证字典是动态的，那么就需要有一种机制来证明某个认证的证明已经是更新过了的。否则，非可信的目录就可能重放以前的旧证明。这里假定：要么由信息源按照预定的时间或者策略来对AD进行更新，要么发起查询请求的用户知道最新的更新是何时发生的。但是，无论在上述哪种情况下，验证者V都应该也必须能够检验证明p的新鲜度。

根据认证字典的定义及其基本模型，不难看出，在设计认证字典时，应该考虑达到如下目标：

计算量小。认证字典模型内的任何一个实体内部所要完成的计算都应该尽可能地简单、快速；同样，支持这些计算的数据结构所需要的内存空间应当尽可能小。

通信载荷小。数据源到目录(更新认证信息)之间的通信量以及目录到用户(查询认证信息)之间的通信量应该尽可能小。

安全性高。用户能够以很高的可靠性来验证目录所提供数据的真实性。

时间约束。如果可能，目录能够为用户提供在某个特定时刻t的信息真实性证明。

也就是说，在构造认证字典时，在保证安全性的前提下，对P的计算和验证应该尽可能高效，P要尽可能短；维护认证字典的操作所涉及的计算量和通信量应该尽可能小；如果可能，应该能够提供具有时间约束特性的认证查询。

3 认证字典的分类方法

依据认证字典所支持查询种类以及时间约束的不同，本文将AD分为三大类：①瞬时型认证字典(Ephemeral Authenticated Dictionary，EAD)；②持续型认证字典(Persistent Authenticated Dictionary，PAD)；③扩展型认证字典(eXtended Authenticated Dictionary，XAD)。这三种不同的认证字典的应用场合不尽相同，下面将逐一对其进行介绍。

3.1 瞬时型认证字典(EAD)

这种认证字典就是通常所说的认证字典。在这种类型的认证字典中，问题的基本形式为："(当前)，元素e(不)在集合S中吗？"。通常，对时间约束无需提及，问题隐含着查询是对当前时间而言的。

由问题的基本形式不难看出：这类认证字典一般用于对当前的操作数据而言。它一般仅仅保证当前的数据真实性。

该类型认证字典的基本模型如图1所示，它可以用于对待查询数据的实时性要求不是太高的场合。

3.2 持续型认证字典(PAD)

这种认证字典实际上是EAD在功能上的增强类型。在这种类型的认证字典中，问题的基本形式为："在t时刻，元素e(不)在集合S中吗？"。这种类型的认证字典可以对过去某个时刻数据的真实性进行证明。显然，当$t=0$(这里表示当前时间)时，有$PAD_{(t=0)}=EAD$。

与EAD相比，PAD的基本模型没有变化，都如图1所示。但是，PAD比EAD功能增强的一个主要方面就是它可以很方便地支持"历史查询"，以便于查询给定信息在过去某一时刻的真实性。这种功能在电子签名的验证过程中具有十分重要的作用。例如，假设有两个实体在过去某个时刻t签订一份电子合同；又假设在合同执行了一段时间后，合同的双方出现了和过去某个时刻t'有紧密关系的某种纠纷。这时，就需要验证在时刻t'时双方所争执数据的真实性问题。具体到PKI/WPKI中，自然就需要验证在t'时刻签名的有效性，也就需要验证时刻t'时的签名者证书的有效性问题。这是PAD的一类典型应用。此时，直接运用EAD是无法满足这种要求的。

3.3 扩展型认证字典(XAD)

XAD包含了EAD和PAD的所有功能；但是XAD不是EAD和PAD的简单叠加。即有：$(EAD\cup PAD)\subset XAD$；但是$(EAD\cup PAD)\neq XAD$。XAD的基本模型也和上述两种类型的认证字典的基本模型稍有不同，其模型如图2所示。在XAD中，信息源不再是一个单一的、固定的信息源，而是由多个信息源(这里，设信息源的数目为n)组成；这多个信息源共享同一个目录进行信息发布。任意的两个信息源之间相互独立，用户向该目录进行认证的隶属关系查询。

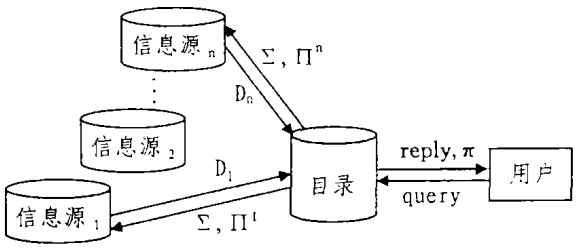

图2 扩展型认证字典(XAD)

由图2可以看出，对于XAD而言，问题的基本形式没有多大变化。但是，信息的发布和查询过程与上述两种类型的认证字典却有很大的不同，现分述如下：

信息发布：在该基本模型中，信息源为$O_i(1\leqslant i\leqslant n)$，其欲向目录发布的数据子集为$D_i(1\leqslant i\leqslant n)$。假设$P$在某一个特定时刻收集所有来自各信息源$O_i$的数据子集$D_i$，$P$首先对这些子集的和集$D=\bigcup_{i=1}^{n}D_i$计算摘要$\Sigma$；对于每一个信息源$D_i$，都有一个唯一的证明$\Pi^i$，用以证明数据源$D_i\in\Sigma$，$P$将$\Pi^i$和$\Sigma$发送给每一个信息源$D_i$，同时$P$将$\Sigma$公开，每一个信息源$D_i$都可以验证证明$\Pi^i$。

认证查询：用户User向P发送查询query。P计算对应

于查询 query 的响应 reply 以及其证明 π，并将二者发送给用户 User。用户检查 reply 和 π 的正确性，并据此来决定是接受还是拒绝响应 reply。

一般说来，在基本的 XAD 中，认证查询仍然是针对当前时刻而言的。很显然，这种类型的认证查询也可以加上时间约束从而扩展为更一般的基于时间约束的 XAD，本文不再赘述。该类型的认证字典在广义的基于 Internet 的真实信息发布中有众多重要应用场合。

4 AD 的基本实现技术及其在 PKI/WPKI 中的应用

实现认证字典的技术和方式各异，但是它们却几乎全部是基于密码学理论的应用[5]。一般说来，实现认证字典所需要的基本密码学基础结构主要有数字签名、单向无碰撞杂凑函数、链接式杂凑认证、树形杂凑认证，以及一些其他独特的密码学基础结构，例如单向累加器(One-Way Accumulator，简记为 OWA)等[5~8]。

假设要对一个全集为 U，待认证的数据集合为 S 的数据集合来构造一个认证字典 $D_S^{\mathcal{U}}$。对于一个小的全集 U 而言，构造 $D_S^{\mathcal{U}}$ 的计算量可以和 $|U|$ 成正比。使用上面所描述的基本的密码学结构，可以使用如下的方式来组织和实现认证字典。

线性列表法：如果 S 比较小，则可以使用该种方案：信息源对包含所有的 $s\in S$ 的列表的一个消息 M 签名。在 PKI/WPKI 中，最常用的证书撤销机制——CRL[3]机制就是采用了这种类型的认证字典。

单元素状态签名法：对于每一个元素 $e\in U$，信息源对相关的消息 $e\in U$ 或者 $e\notin U$ 进行签名。要更新 D_S，就必须提供个 $|U|$ 签名，这和 D_S 中变化元素的数目无关。例如，PKI 中的证书撤销系统 CRS[9]就是这样一种实现机制。

基于杂凑树的方法：信息源对“不在 S 内的有序元素间隔”签名，并使用 Merkle 杂凑树作为基础的数据结构来组织数据。这样的一个有序间隔是一个对 (s_1,s_2)；满足：对于所有的 $s_1\leqslant s\leqslant s_2, s\notin S$。例如，CRT/Skip-List/2-3 树等都是基于这种实现技术[9~11]。

基于单向累加器(OWA)的方法：单向累加器是可以用来实现认证字典的一种重要的密码结构，Goodrich 等给出了一种基于大整数环内的模幂运算的 OWA[8]，它基于 RSA 问题的难解性[12,13]。

需要指出的是：在上面给出的所有实现技术中，信息源都必须对所有的消息进行数字签名，而且在被签名的消息中同时也必须包含有认证信息的更新时间。实现认证字典所使用的具体数据结构的不同，实现上述基本操作的难易程度以及操作的效率也有很大的不同。

综上所述，无论实现认证字典基于何种数据结构，也不管采用何种实现技术，一个认证字典都应该至少支持以下四种基本操作：

- 创建操作 $create(S_0)$：给定一个初始集合 S_0，创建其相应的认证字典 D_{S_0}；
- 查找操作 $find(x,S)$：确定是否有 $x\in S$ 成立；对于 PAD，还需要增加一个时间参数 t，其形式变为 $find(x,S,t)$，即在时刻 t，是否有 $x\in S$ 成立。
- 插入操作 $insert(x,S)$：将 x 添加到集合 S 中，并更新 D_S；
- 删除操作 $delete(x,S)$：将 s 从集合 S 中删除，并更新 D_S。

在 PKI/WPKI 中，信息源就是通常所说的认证中心(即 CA，Certification Authority)。它向实体签发数字证书，用以证明实体的公钥和实体身份信息以及其他信息之间的绑定，从而来保证这些信息的真实性和有效性。每一个证书都有一定的有效期，有效期过后该证书便不再有效。然而，某些时候可能因为某种原因(例如，私钥的泄漏或者丢失、实体所属关系的变化等)需要在证书的有效期到达之前撤销证书。为了便于用户查询这些状态信息，就必须以一种认证的方式来发布这些真实的信息。显然，认证字典是解决这类问题的优选的数据结构，其思想也非常地直观。例如，在 PKI/WPKI 中占据极其重要地位的各种证书撤销和查询机制(如 CRL、CRS、CRT 等等)就是该数据结构的典型应用[12]。

结论 认证字典是一类重要的数据结构，它在众多研究领域都具有重要的理论和应用价值，诸如科学数据挖掘、地理数据服务器、Internet 上的第三方数据发布以及 PKI 中的证书撤销等。本文介绍了认证字典的基本概念与原理；在认证字典的基本模型中首次引入了时间约束，并据此给出了认证字典的一种新的分类方法，探讨了相关的实现技术。

认证字典在信息安全领域有着重要的应用价值，诸如 PKI/WPKI 中的证书撤销和验证机制问题。在应用这一重要的数据结构时，除了要使得构造出的认证字典具有安全、高效、简洁的特性，还必须要考虑到 AD 的具体应用背景因素，进行综合的分析比较。今后，将对基于不同的密码学结构的认证字典的效率进行量化分析，以指导对该数据结构的更好应用。

参 考 文 献

1 Naor M, Nissim K. Certificate revocation and certificate update. In: Proc. of the 7th USENIX Security Symposium (SECURITY-98), Berkeley, 1998. 217～228
2 Devanbu P, et al. Authentic third-party data publication. In: Fourteenth IFIP 11.3 Conf. on Database Security, 2000
3 Housley R, Ford W, Polk W, Solo D. Internet X.509 public key infrastructure: certificate and CRL profile. IETF RFC 2459, Jan. 1999
4 U.S. National Institute of Standards and Technology. A Public Key Infrastructure for U.S. Government unclassified but Sensitive Applications', September 1995
5 Stallings W. Cryptography and network security: principles and practice(Second Edition). Prentice Hall, New Jersey, 1998
6 Merkle R C. A Certified Digital Signature. In: Proc. of Crypto '89, Lecture Notes in Computer Science 435, Springer-Verlag, 1989. 234～246
7 Benaloh J, de Mare M. One-way accumulator: a decentralized alternative to digital signatures. Advances in Cryptology-Euro-Crypto93, LNCS 765, 1993. 274～285
8 Goodrich M T, Tamassia R. An efficient dynamic and distributed cryptographic accumulator. In: Proc. of Information Security Conf. (ISC 2002), Lecture Notes in Computer Science, vol. 2433, Springer-Verlag, 2002. 372～388
9 Micali S. Efficient certificate revocation. Technical Memo MIT/LCS/TM-542b, 1996
10 Goodrich M T, Tamassia R, Schwerin A. Implementation of an authenticated dictionary with skipl lists and commutative hashing. In: DARPA Information Survivablity Conf. and Exposition (DISCEX II), Volume 2, 2001
11 Goodrich M T, Tamassia R. Efficient authenticated dictionaries with skip lists and commutative hashing: [Technical Report]. Johns Hopkins Information Security Institute, 2000
12 Berkovits S, et al. Public key infrastructure study: final report. MITRE Corporation, April 1994
13 Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystem. Communications of the ACM, Feb. 1978