

文章编号:1001-9081(2009)09-2339-03

基于身份的结构化重签名方案

耿永军,张延红,崔雪冰

(河南城建学院 计算机科学与工程系,河南 平顶山 467001)

(geng-yong-jun@163.com)

摘要:双线性对易于实现复杂密码协议,为了简化公钥密码体制证书管理的负担,采用双线性对技术实现了一种结构化重签名方案并给出该方案的仿真结果。方案以用户的身份信息,如电子邮箱地址,IP 地址、电话号码等作为用户公钥,从而降低了建立和管理公钥基础设施的代价,避免了用户对公钥及其证书的存储和传递等问题,仿真结果显示其签名与验证签名时间开销是原方案 3/4。

关键词:数字签名;结构化重签名;公钥基础设施;双线性对

中图分类号: TP309 **文献标志码:** A

Identity-based structured multi-signature

GENG Yong-jun, ZHANG Yan-hong, CUI Xue-bing

(Department of Computer Science and Engineering, Henan University of Urban Construction, Pingdingshan Henan 467001, China)

Abstract: Bilinear pairs can easily realize complex cryptography protocol. In order to simplify the burden of certificate management of public key cryptography, a novel identity-based structured multi-signature was proposed by using bilinear pairing technology. The scheme took the user's identity information as public key such as e-mail address, IP address, telephone number so that it erased the cost of forming and managing Public Key Infrastructure (PKI) and avoided the problem of user's storing, receiving and sending his public key and certificate. The simulation results of the proposed scheme show that the cost of signing and verifying in the scheme is only 3/4 of the original scheme.

Key words: digital signature; structured multi-signature; Public Key Infrastructure (PKI); bilinear pairing

2001 年 Boneh 等人提出了基于双线性对的短签名^[1],双线性对构造密码协议其优势可归结为用双线性对可以构造一些用其他方法无法或难以实现的密码协议,所以双线性对一经提出就引起了广泛的关注,成为数字签名研究的热点之一^[2-5]。Shamir 于 1984 年提出了一种公钥密码体制^[6],该体制能大大减小公钥系统的复杂度,它选择任意比特串(通常是用户身份)作为公钥,由私钥生成中心(Private key Generator, PKG)生成对应的私钥,基于身份密码学(Identity-based Cryptography, IBC)最大的优势就在于它简化了传统基于证书的公钥体制负担最重的密钥管理过程,IBC 在密钥分发等方面远优于公钥基础设施(Public Key Infrastructure, PKI),它只需维护 PKG 产生用于认证的公开系统参数目录,这个开销将远低于维护所有用户的公钥目录所需开销。本文以文献[5]为基础采用双线性对技术提出了一种新的基于身份的结构化多重签名方案。该方案以用户的身份信息,如电子邮箱地址,IP 地址、电话号码等作为用户公钥,从而降低了建立和管理公钥基础设施的代价,避免了用户对公钥及其证书的存储和传递等问题。仿真结果表明其签名、验证时间开销是文献[5]的 3/4。

1 双线性映射

设 G_1, G_2 分别是同为 q 阶的加群和乘群, P 为 G_1 的生成元。假设在群 G_1, G_2 中,离散对数问题是难解的。可定义双线性映射对为 $e: G_1 \times G_1 \rightarrow G_2$, 并满足以下特性:

1) 双映射。

$$e(aP, bP') = e(abP, P') = e(P, abP') = e(P, P')^{ab}, \text{ 对}$$

所有的 $P, P' \in G_1$, 所有的 $a, b \in Z_q^*$ 成立。

2) 非退化性。存在 $P', Q \in G_1$, 使得 $e(P', Q) \neq 1$ 。

3) 可计算性。对所有的 $P', Q \in G_1$, 存在有效的算法可计算 $e(P', Q)$ 。

2 基于身份的结构化多重签名及其分析

2.1 方案的描述

1) 系统参数的初始化。

设 G_1 是由 P 生成的阶为素数 q 循环加群, G_2 是阶为 q 的循环乘群。 e 是一从 $G_1 \times G_1$ 到 G_2 的双线性对映射。 $U = \{u_1, u_2, \dots, u_n\}$ 表示 n 个参加签名成员的集合, H_1 是一个单向的 Hash 函数, $H_1: \{0, 1\}^* \rightarrow G_1$, H_2 也是一个单向的 Hash 函数, $H_2: \{0, 1\}^* \rightarrow Z_q^*$ 。密钥分发中心(PKG)随机选择一个主密钥 $x \in Z_q^*$, 计算 $Y = xP$, PKG 公开系统参数 $\{G_1, G_2, P, Y, q, e, H_1, H_2\}$, 保密主密钥 x 。

2) 成员密钥的生成。

给定签名成员的身份 ID_i , PKG 计算该用户的私钥 $x_i = xY_i$, 将此值秘密的发送给成员用户。其中, $Y_i = H_1(ID_i)$ 为该用户公钥。

3) 验证公钥的生成。

假设任一 $u_i \in U$ 同意签名结构 A , 对于每个 $u_i \in U$ 依据在签名结构 A 中的签名次序计算出自己的验证公钥 v_i 。

步骤 1 起点 u_s 进行初始化产生 v_s 的值:

$$v_s = 0$$

步骤 2 计算每个 $u_i (1 \leq i \leq n)$ 的验证公钥 v_i :

$$v_i = Y_i + \sum_{pre(i)} v_j$$

收稿日期:2009-03-09;修回日期:2009-05-05。

作者简介:耿永军(1971-),男,河南许昌人,博士,主要研究方向:现代密码学、数字签名;张延红(1969-),女,河南平顶山人,副教授,硕士,主要研究方向:电子商务;崔雪冰(1972-),女,河南新乡人,讲师,硕士,主要研究方向:电子商务。

步骤 3 在汇点计算多重签名的验证公钥:

$$v = \sum_{u_h \in \text{prev}(u_D)} v_h$$

4) 多重签名的产生。

设 M 为待签消息, 依据签名结构, 多重签名通过依次执行下列步骤完成。

步骤 1 起点 u_s 不参加签名, 进行初始化产生 $s_s = 0$, 将消息 M 、 B_s 和 s_s 发送给其直接后继节点。

步骤 2 假设 u_j 是 u_s 的直接后继节点。

u_j 随机选取 $k_i \in Z_q^*$, 根据消息 M 计算:

$$m = H_2(M)$$

$$s_j = mx_j + \sum_{u_s \in \text{prev}(u_j)} s_s$$

将 (M, s_j) 传给其后继节点 u_i 。

步骤 3 签名者 u_i 首先通过下式验证其直接前趋 u_j 签名的有效性。

$$e(s_j, P) = e(v_j, mY) \quad (1)$$

如果式(1)成立, 则继续; 否则, 结束签名。其中, P 为 q 阶的加群 G_1 的生成元, v_j 是用户 u_j 的验证公钥, s_j 为 u_j 对消息 M 的签名(后面将给证明)。计算下式:

$$m = H_2(M)$$

$$s_i = mx_i + \sum_{u_j \in \text{prev}(u_i)} s_j$$

将 (M, s_i) 传给其后继节点。重复执行步骤 3 直到汇点 u_D 。

步骤 4 汇点 u_D 进行多重签名最后阶段的汇总工作。首先对每个 $u_h (u_h \in \text{prev}(u_D))$ 的部分签名 (M, s_h) 利用式(1)进行验证。如果式(1)验证成立, 则计算下式:

$$s = \sum_{u_h \in \text{prev}(u_D)} s_h \quad (2)$$

最终, 以二元组 (M, s) 作为结构化重签名的结果。

5) 多重签名的验证。

签名的验证方计算

$$m = H_2(M)$$

$$e(s, P) \stackrel{?}{=} e(v, mY) \quad (3)$$

若式(3)成立, 则说明结构化多重签名有效。

2.2 安全性分析

下面证明本文提出的方案满足结构化重签名要求、能抵抗合谋攻击、伪造攻击。该改进方案的安全性基于下面困难性假设: 超奇异椭圆曲线离散对数难题、整数域离散对数难题和单向 hash 函数的不可逆性。先证明该方案的正确性, 然后证明其满足的安全性性质。

1) 方案的正确性证明。

定理 1 如果满足校验式 $e(s, P) = e(v, mY)$, 其中 $m = H_2(M)$, 则二元组 (M, s) 是有效的结构化重签名。

证明 应用递推证法。

① 当 $i = 1$ 时, 假设 u_1 是 u_s 的直接后继节点, $u_1 \in \text{next}(u_s)$, 可得 $s_1 = x_1 m, v_1 = Y_1$ 。

$$e(s_1, P) = e(x_1 m, P) = e(Y_1, x_1 m P) = e(v_1, mY)。$$

② 假设当 $i = j$ 时, 定理 1 成立, 其中 $u_j \in \text{prev}(u_k)$ 且 $(k \leq n)$ 。

③ 当 $i = k$ 时:

$$\begin{aligned} e(s_k, P) &= e(mx_k + \sum_{u_j \in \text{prev}(u_k)} s_j, P) = e(mx_k Y_k + \sum_{u_j \in \text{prev}(u_k)} s_j, P) = \\ &= e(mx_k Y_k, P) e(\sum_{u_j \in \text{prev}(u_k)} s_j, P) = e(Y_k, mY) e(\sum_{u_j \in \text{prev}(u_k)} v_j, \\ &= e(Y_k + \sum_{u_j \in \text{prev}(u_k)} v_j, mY) = e(v_k, mY) \end{aligned}$$

即证当 $k \leq n$ 时, $e(s_k, P) = e(v_k, mY)$ 。

④ 证明 $e(P, s) = e(v, mY)$ 。

$$\begin{aligned} e(P, S) &= e(P, \sum_{u_h \in \text{prev}(u_D)} s_h) = \prod_{u_h \in \text{prev}(u_D)} e(P, s_h) = \\ &= \prod_{u_h \in \text{prev}(u_D)} e(v_h, mY) = e(\sum_{u_h \in \text{prev}(u_D)} v_h, mY) = \\ &= e(v, mY) \end{aligned}$$

2) 方案满足的安全性。方案能抵制非法成员或部分合法成员的伪造攻击。

定理 2 除全体合法签名者外, 任何人伪造不出结构化重签名 (M, S) 满足校验式 $e(P, s) = e(v, mY)$ 。

证明 部分签名者合谋伪造多重签名将面临解决离散对数困难问题, 假设某一个签名者 $u_i (u_i \in U)$ 没有参与签名, 另外 $n - 1$ 签名人合谋伪造有效签名。首先, v 是由 n 个签名者事先联合产生的验证公钥, 没有 u_i 加入签名, 则 v 中不可能包含签名者 u_i 公钥信息。若在 s 中不用 u_i 的私钥来行使签名或编造一个值 (P, s_i) , 这将使验证方程式 $e(P, s_i) = e(v_i, mY)$ 不能成立, 是无效签名。如果想根据 $Y = xP$ 求出 x , 则遇到解椭圆曲线离散对数难题。恶意的外部攻击者无法根据 v 伪造出对消息 M 的多重签名。虽然攻击者很容易得到 P, Y, M 和 v 求出 $e(v, mY)$, 但解 $e(P, s) = e(v, mY)$ 中的 s 将面临计算 Diffie-Hellman 困难问题。攻击者若用另一消息 M' 的签名 S' 充当 M 的签名, 此时必须能给出合适的 m , 这也是困难的, 这是由 Hash 函数的性质决定的。同时, 结构化签名的先后次序是通过验证公钥 $v_i = Y_i + \sum_{u_j \in \text{prev}(u_i)} v_j$ 来保证的, 只有符合该次序的有效签名, 该验证公钥才能验证通过。

3 性能的理论分析和实验测试

3.1 性能分析

该方案是基于超奇异椭圆曲线构造的双线性对进行密码运算的, 方案重签名结构如图 1 所示。在基于双线性对的密码系统中, 算法的运算代价主要依赖于椭圆曲线标量乘运算和双线性对运算。方案中 3 个成员和一个签名合成者进行重签名, 3 签名成员共进行 3 次哈希, 4 次 G_1 群上的标量乘和 2 次双线性对操作运算, 签名合成者共进行 1 次哈希, 2 次 G_1 群上的标量乘和 4 次双线性对运算。重签名的验证需进行 4 次哈希和 6 次双线性对运算。带签名者意向的结构化签名 s 长度为 $|G_1|$ 。 $|G_1|$ 表示群 G_1 上一点坐标的长度。

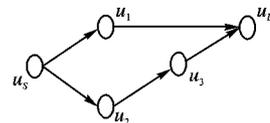


图 1 重签名签名结构 A

3.2 实验测试

编程实现该基于身份的结构化多重签名方案, 超奇异椭圆曲线的选取、双线性对的构造和椭圆曲线点群的运算采用 PBC 函数库, 该库函数可进行大整数、椭圆曲线点群和双线性对的运算。方案具体运行环境如下: Celeron 1.4 GHz + 760 MB RAM + Windows XP + VC8.0。方案中哈希运算采用 256 b 的 SHA-2, 加密算法采用 AES。PBC 函数库可操作的超奇异椭圆曲线分为 A、A1、D、E、F、G 六种类型, 本方案选用 A 型, 该类型曲线构造的点群运算速度快, 超奇异曲线方程为 $y^2 = x^3 + x$, 该方程基于域 $F_q, \#E(F_q) = q + 1$, 椭圆曲线点群的循环子群生成元为 p , 其阶为 r , 满足 $q + 1 = r \times h$ 。实验参数

值选取如下所示:

```

q = "87807107996633125224377819847540498158068831
994142082110286533992664756308802229570786251
794226622214231558587695823174592777133673174
81324925129998224791"
r = "73075081866545162136111924557150490140597655
9617"
r = 2159 + 2107 + 1 (Solinas 素数)
h = "12016012264891146079388821366740534204802954
401251311822919615131047207289359704531102844
802183906537786776"
p = "[3163580956772149639925912500766810073109666
440270410289968026398982380938528821100065051
990342893360704324303698244672599590418044198
150276814580345072723,18658758021481017841986
527657714984090278806241291719106485210842800
164749148463794325155471082092246281551679400
46585683527588501231517546468799494459083]"

```

实验测试模拟的重签名结构如图1所示,3个成员进行部分签名,最后由签名合成者完成重签名。实验测试结果为三个成员和重签名合成者完成重签名共耗时546 ms,验证重签名时间开销为141 ms。其签名和验证签名时间开销是文献[5]方案的3/4。

4 结语

企事业单位中,一个决议的通过要经过多个部门领导的

签名,要满足一定签名次序和结构,结构化多重签名就是对这类问题的一种解决方案。本文基于双线性对提出了一种基于身份的结构化多重签名方案,该方案以用户的身份信息,如电子邮箱地址、IP地址、电话号码等作为用户公钥,从而降低了建立和管理公钥基础设施的代价,避免了用户对公钥及其证书的存储和传递等问题。最后给出该种重签名方案的仿真实现。

参考文献:

- [1] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing [C]// Proceedings of Advances in Cryptology - Asia - crypt2001. Berlin: Springer-Verlag, 2001: 514 - 532.
- [2] BONEH D, BOYEN X, SHACHAM H. Short group signatures [C]// Proceedings of Cryptology - CRYPTO 2004. Berlin: Springer-Verlag, 2004: 41 - 59.
- [3] BOLDYREVA A. Efficient threshold signature, multi-signature and blind signature schemes based on the Gap-Diffie-Hellman-group signature scheme [C]// Proceedings of Practice and Theory in Public Key Cryptography. Berlin: Springer-Verlag, 2003: 31 - 46.
- [4] CHEN X, ZHANG F, KIM K. A new ID-based group signature scheme from bilinear pairings [C]// WISA 2003: Proceedings of the 2003 International Workshop on Information Security Applications. Berlin: Springer-Verlag, 2003: 585 - 592.
- [5] 吴克力. 一个带签名者意向的结构化多重签名方案[J]. 电子与信息学报, 2006, 28(5): 825 - 826.
- [6] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// Proceedings of Advances in Cryptology - Crypto'84. Berlin: Springer-Verlag, 1984: 47 - 53.

(上接第2338页)

数据权限实现了不同部门的用户只能操作本部门的数据,而传统的基于角色的访问控制模型只提供同类数据的过滤功能,不能实现同类数据在不同部门之间的过滤^[8]。相比而言,我们设计的新方案具有较高的数据安全保密性。

基于用户处理查询时,节点过滤技术需分解XML文档成DOM树,然后标记DOM树的各节点,再对标记后的DOM树剪枝,以便生成用户视图。且对每个用户的每次请求都需要进行重复的分解、标记和剪枝处理。而本文方案只需利用索引/标记值将需要访问的数据过滤出来即可,能减少和优化处理步骤,加快查询和查找速度,节省系统资源。

本文的快速更新方案在实现插入、删除等更新操作时不需改变DTD和XML文档结构,以浪费少量的空间来换取更新操作的时间,具有较快的处理速度。且不需要修改授权访问规则,减少了对授权访问规则的频繁访问,这是其他更新方案^{[2]82-83, [7]1100-1103}所不具备的。

5 结语

针对XML数据安全日趋重要的现实,本文提出了一种细粒度的同时支持读写权限的访问控制新方案。该方案以灵活有效的方法控制用户对XML数据库系统中不同安全等级数据的访问;利用空对象和备注子节点实现XML数据的删除和插入,确保了数据的有效性和安全性;结合动态索引/标记方案来实现查找,减少了处理步骤,加快了查找速度。

参考文献:

- [1] DAMIANI E, FANSI M, GABILLON A, *et al.* A general approach to securely querying XML [J]. Computer Standards and Interfaces,

2008, 30(6): 379 - 389.

- [2] DUONG M, ZHANG Y. An integrated access control for securely querying and updating XML data [C]// Proceedings of the 19th Conference on Australasian Database. Darlinghurst, Australia: Australian Computer Society, 2008: 75 - 84.
- [3] 李澜,何永忠,冯登国. 面向XML文档的细粒度强制访问控制模型[J]. 软件学报, 2004, 15(10): 1528 - 1537.
- [4] DAMIANI E, De CAPITANI di VIMERCATI S, PARABOSCHI S, *et al.* A fine-grained access control system for XML documents [J]. ACM Transactions on Information and System Security, 2002, 5(2): 169 - 202.
- [5] DUONG M, ZHANG Y. LSDX: A new labeling scheme for dynamically updating XML data [C]// Proceedings of the 16th Australasian Database Conference. Darlinghurst, Australia: Australian Computer Society, 2005: 185 - 193.
- [6] ZHAO G S, CHADWICK D W. On the modeling of Bell-LaPadula security policies Using RBAC [C]// Proceedings of the 17th IEEE International Workshops on Enabling Technologies. Los Alamitos, CA: IEEE Computer Science, 2008: 257 - 262.
- [7] DAMIANI E, FANSI M, GABILLON A, *et al.* Securely updating XML [J]. KES 2007: Proceedings of the 11th International Conference on Neural Networks, LNCS 4694. Berlin: Springer-Verlag, 2007: 1098 - 1106.
- [8] MASSACCI F, MYLOPOULOS J, ZANNONE N. Hierarchical hipocratic databases with minimal disclosure for virtual organizations [C]// Proceedings of the 12th ACM Conference on Computer and Communications Security in Computer Security. Heidelberg: Springer, 2005: 438 - 454.