一种新型群签名的分析与改进 *

王青龙[1,2], 魏艳艳[3]

(1. 长安大学 信息学院,西安 710064; 2. 北京交通大学 通信与信息系统北京市重点实验室,北京 100044; 3. 陕西交通职业技术学院,西安 710018)

摘 要: 最近提出的一种新型群签名方案,首先对 Boneh-Boyen 短签名提出了一种变形方案,然后在此变形方案的基础上构造一种群签名方案,使得它不依赖于可信第三方来为群成员产生证书。指出了此变形方案本身是错误的,故在此基础上的群签名也是不成立的。除此之外,所构造的群签名方案本身也存在签名长度过长、同一签名成员的签名存在关联性的缺陷。最后,给出了改进的方案。

关键词: 群签名; 短签名; 无关联性; 匿名性

中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2010)04-1464-02

doi:10.3969/j.issn.1001-3695.2010.04.072

Cryptanalysis and improvement on new type of group signature scheme

WANG Qing-long[1,2], WEI Yan-yan[3]

(1. *School of Information Engineering, Chang' an University, Xi' an* 710064, *China*; 2. *Key Laboratory of Communication & Information System, Beijing Jiaotong University, Beijing* 100044, *China*; 3. *Shaanxi College of Communication Technology, Xi' an* 710018, *China*)

Abstract: The recently proposed new type of group signature scheme was constructed on a new signature derived from the Boneh-Boyen short signature scheme. However, the new signature scheme was fault thus the group signature was flawed. Besides, the proposed group signature scheme was long in length and the signatures of the same signer are linkable. Further, this paper proposed an improved scheme.

Key words: group signature; short signature; unlinkability; anonymous

0 引言

群签名的概念最早是由 Chaum 等人[1]提出来的,这种签名体制是指多个成员组成一个群,每个成员都有互不相同的签名密钥,任意成员都可以代表这个群用自己的签名密钥匿名地产生签名。验证者用惟一的群公钥可以验证签名的合法性,但无法确定签名成员的身份。如果发生纠纷,群管理员(GM,在最新的一些研究中,有时将 GM 分为两个实体,即为成员生成签名密钥与打开签名)可以由签名追踪到签名成员的身份。这种签名合同制是一种面向多用户的签名体制,其目的主要是在于保护签名者的匿名性。

无论是在理论研究还是在实际应用中,群签名都有着非常重要的研究意义。理论方面,它与环签名既有联系又有区别,同时它还可以用来构造其他密码协议,如电子支付[2,3]、数字指纹[4,5]以及匿名证书等。在实际中,群签名有着非常广泛的应用背景,可用在电子选举、电子商务和交通安全通信体系[6]等方面。

群签名方案一般包括系统初始建立、新成员加入、签名生成算法、签名验证算法和打开签名算法。简单地说,群签名是每个群成员选择自己的成员密钥,用一个单向函数作用于该密钥生成其成员公钥;GM 对每个成员公钥进行签名,称做群成员资格证书。群签名,其本质就是成员对其拥有的成员资格证书和成员密钥的非交互式零知识证明。

Boneh-Boyen 短签名[7]是一篇重要文献,在此基础上,作者又先后构造两种群签名方案[6,8],其中文献[8]定义了本地验证的群签名概念。目前,设计具有向后无关性的本地验证群签名方案是其中一个重要的研究方向[9,10]。

基于 q-SDH 假设和判定 DH 假设,文献[11]提出了一种新型群签名方案。该方案首先是在 Boneh-Boyen 短签名[7]的基础上提出一种变形方案,然后在此变形方案的基础上构造了一种群签名方案。本文要指出的是,这一变形方案本身是错误的。除此之外,该群签名方案还存在签名长度过长、同一群成员的签名存在关联性的缺陷。

1 相关知识

1)双线性映射

(1)G_1、G_2、G_T 是阶为 p 的乘法循环群;g_1 是 G_1 的生成元,g_2 是 G_2 的生成元;

(2)φ 是从 G_2 到 G_1 的一个同态映射,满足 $\varphi(g_2)=g_1$;

(3)$e:G_1\times G_2\rightarrow G_T$ 是一个双线性映射,如果满足: a)双线性,对任意的 $u\in G_1, v\in G_2$ 和 $a,b\in Z$,都有 $e(u^a,v^b)=e(u,v)^{ab}$;b)非退化性,$e(g_1,g_2)\neq 1$。

2)记号 $\mathrm{SPK}\{(x_1,\cdots,x_t):R(x_1,\cdots,x_t)\}(M)$,表示签名者用秘密值 $x_1,\cdots,x_t$ 对消息 M 签名的一个知识证明,这里 $x_1,\cdots,x_t$ 满足关系 $R(x_1,\cdots,x_t)$。同文献[6, 10],文献[11]的签名的知识证明也采用 Fiat-Shamir 方法,即把哈希函数的输出值

收稿日期: 2009-07-11; **修回日期**: 2009-08-24 **基金项目**: 国家自然科学基金资助项目(60773175)

作者简介:王青龙(1970-),男,山西新绛人,博士,主要研究方向为数字签名、协议分析等(qlwang@live.cn); 魏艳艳(1979-),女,陕西西安人,讲师,硕士,主要研究方向为信息安全.

作为挑战的一种非交互的零知识证明。

2　方案回顾

下面简单回顾一下文献[11]中基于 BB 短签名提出的一种新型签名方案以及由此构造的群签名方案。

1)文献[11]提出的新型签名方案

签名　给定私钥 $x,y\in Z_p^*$ 和消息 $m\in Z_p^*$,签名者随机选择 $r\in Z_p^*$,计算 $\sigma\leftarrow(g_1^m)^{\frac{1}{x+g_1^m+yr}}$,生成的签名为$(\sigma,r)$。

验证　验证者收到签名(σ,r)后,分别计算两个双线性对 $e(\sigma,ug_2^{(g_1^m)}v^r)$,$e(g_1^m,g_2)$,如果这两个双线性对相等,则说明签名是对消息的合法签名。这里 $u=g_2^x,v=g_2^y$ 是签名公开。

2)文献[11]提出的群签名方案

系统参数为$(G_1,G_2,G_T,e,p,g_1,g_2,g_T,h,H)$。其中:$(G_1,G_2)$为第 1 章定义的双线性群,$e:G_1\times G_2\rightarrow G_T$ 是双线性映射;g_1,g_2,g_T 分别为 G_1,G_2,G_T 的生成元;$h\in G_T$;$H:\{0,1\}^*\rightarrow Z_p^*$ 是碰撞自由的哈希函数。

密钥生成　随机选取 $x,y\in Z_p^*$,计算 $u=g_2^x,v=g_2^y$。负责群成员加入群中的群成员身份管理者(GM),其群公私密钥对分别为 $sk_M\leftarrow(x,y)$,$pk_M\leftarrow(u,v)$。随机选择 $x_1,x_2,x_3,x_4,x_5\in Z_p^*$,计算 $y_1\leftarrow g_T^{x1}h^{x2}$,$y_2\leftarrow g_T^{x3}h^{x4}$,$y_3\leftarrow g_T^{x5}$。负责撤销群成员的撤销管理者(GR),其撤销公私密钥对分别为 $sk_R\leftarrow(x_1,x_2,x_3,x_4,x_5)$,$pk_R\leftarrow(h,y_1,y_2,y_3)$。群公钥为 $gpk\leftarrow(pk_M,pk_R,g_1,g_2,g_T)$。

群成员的加入　预加入的成员随机选取其私钥 $gsk\leftarrow k$ $(k\in Z_p^*)$,计算 $P=g_1^k$ 并发送给 GM,用签名的知识证明 SPK$\{(k):P=g_1^k\}$ 来证明其拥有私钥 k。验证通过后,GM 使用上面的签名方案对 P 进行签名,得到相应的(r,σ)作为成员的群资格证书发送给预加入的成员。GM 计算 $S\leftarrow e(P,g_2)$,存储 S 作为该成员的身份标签 ID。

签名　随机选择 $r_1,r_2\in Z_p^*$,计算 $\tilde{\sigma}\leftarrow\sigma^{r1}$,$\tilde{c}\leftarrow(ug_2^Pv^r)^{r2}$,$S=e(P,g_2)$,并用 pk_R 对 S 加密:$d_1\leftarrow g_T^u$,$d_2\leftarrow h^u$,$d_3\leftarrow y_3^uS$,$d_4\leftarrow y_1^uy_2^{uQ}$,其中,$Q\leftarrow H(d_1\parallel d_2\parallel d_3)$。然后对消息作知识签名:

$$\Delta\leftarrow \mathrm{SPK}\{(\mu,\theta,\gamma,\lambda):w_1=w_2^{\lambda}\wedge\tilde{\sigma}=\sigma^{\mu}\wedge\tilde{c}=(ug_2^Pv^r)^{\theta}\wedge d_1=g_T^{\gamma}\wedge d_2=h^{\gamma}\wedge d_3=y_3^{\gamma}w_3^{\lambda}\wedge d_4=(y_1y_2^Q)^{\gamma}\}(m)$$

这里 $w_1\leftarrow e(\tilde{\sigma},\tilde{c})$,$w_2\leftarrow e(g_1^{r1},g_2^{r2})$,$w_3\leftarrow e(g_1,g_2)$,最终输出的签名为$(\tilde{\sigma},r,d_1,d_2,d_3,d_4,\Delta)$。

验证　通过检验知识签名 Δ 的正确性来判断群签名的有效性。

打开 GM 可通过 GR 的私钥 $G_{msk}=sk_R$ 对群签名中的(d_1,d_2,d_3,d_4)进行解密获得成员的身份 S。步骤如下:计算 $Q\leftarrow H(d_1\parallel d_2\parallel d_3)$,验证 $d_4=d_1^{x1+x3Q}d_2^{x2+x4Q}$ 是否成立,若成立,则有 $d_3/d_1^{x5}=g_T^{x5u}S/g_T^{x5u}=S$。

3　方案分析

签名方案是建立在第 1 章中定义的双线性群和双线性映射上的,生成的签名为 $\sigma=(g_1^m)^{\frac{1}{x+g_1^m+yr}}$。在该签名中,指数的分母部分为 $x+g_1^m+yr$,其中,$g_1^m\in G_1$ 而 $x,y,r\in Z_p^*$,即 $x+g_1^m+yr$是两个不同域的元素相加。而在双线性群和双线性映射上,这两个域中元素相加的运算是没有定义的,故直接将这两个元素相加显然是不正确的,即文献[11]基于 BB 短签名提出的新签名方案是错误的。除上述提到的问题,文献[11]提出的签名方案还存在如下不足:

a)签名长度过长。文献[8](以下简称 BBS 方案)基于 q-SDH 假设构造了一种高效的群签名方案,文献[11]的群签名方案也是基于该假设的,作者指出其方案中得到的签名只比 BBS 签名方案多了一个 G_T 中的元素。

一般地,对于双线性群和双线性对,通常 φ 是迹映射的 MNT 椭圆曲线[12]。如果令 p 是长为 170 b 的素数,那么 G_1 中元素长为 171 b,则 G_T 中元素长为 1 020 b。按照此参数来统计,则文献[8]的群签名长度是 1 533 b,而文献[11]的长度则是 6 120(统计结果是根据作者在文献[11]中的签名统计——签名是 6 个 Z_p^* 中元素和 5 个 G_T 中元素),即为前者 399%,是目前建立在椭圆曲线上长度最长的签名方案,这与使用椭圆曲线构造密码协议的目的相背离。

b)签名存在关联性。关联性在某些特定的场景中有其实用价值,但更多的一个群签名应该具有无关联性,即同一个成员的任意签名之间不存在关联性。而文献[11]中的群签名方案恰恰又具有关联性。确定两个签名是否为同一成员所签,可以根据下面方法来判定:签名最后输出为$(\tilde{\sigma},r,d_1,d_2,d_3,d_4,\Delta)$,其中,$r$ 是包含在每个成员加入群时 GM 分配的群成员资格证书(σ,r)中的。这样,对同一个成员,他每次的群签名中都会包含相同的 r,签名的关联性显而易见。

4　改进方案

针对文献[11]中新型签名方案的错误,一种直接的改进方法是采用文献[13]中提出的修复方案方式,引入一映射 f:$G_1\rightarrow Z_p^*$,将签名变成 $\sigma\leftarrow(g_1^m)^{\frac{1}{x+f(g_1^m)+yr}}$,这样就不再存在不同域中元素相加的问题了。

借鉴文献[10]中的方式,此处给出另外一种方法来实现群签名的不可伪造性,这种方法不需要对 BB 短签名进行改造,而在群签名中成员加入时使用文献[7]中的技巧。为了节约篇幅,下面仅就主要变化的成员加入算法予以描述:

当加入群时,成员产生私钥 $gsk\leftarrow k(k\in Z_p^*)$,计算 $P=g_1^k$ 并发送给 GM,用签名的知识证明 SPK$\{(k):P=g_1^k\}$ 来证明其拥有私钥 k。验证通过后,GM 对 g_1h^{-k} 作 BB 短签名(建议使用 BB 短签名方案中的第二个更简单的签名方案),即得 $\sigma=(g_1h^k)^{\frac{1}{x+r}}$,于是$(\sigma,r,k)$就是成员的群资格证书。其余部分与文献[10]中类似,此处不再详细介绍。

5　结束语

文献[11]在文献[7]的基础上,提出一种基于 BB 短签名的变形签名方案,然后在此变形方案的基础上构造了一种新型群签名方案。本文则指出 BB 短签名的变形方案是不正确的;除此之外,所构造的群签名还存在签名长度过长和签名存在关联性的缺陷。同时,本文给出了改进的方案。

致谢　中国科学院信息安全国家重点实验室的魏凌波博士为本文提供了很多帮助,在此特予以感谢。

参考文献:

[1] CHAUM D, HEYST V E. Group signatures[C]//Proc of Eurocrypt '91, LNCS 547. Brighton:Springer-Verlag, 1991: 257-265.

[2] MAITLAND G, BOYD C. Fair electronic cash based on a group signature scheme[C]//Proc of ICICS'01, LNCS 2229. Berlin:Springer-Verlag, 2001:461-465.

(下转第 1488 页)

本文提出的冲突检测算法的冲突检测效率略优于改进前的算法,与理论分析结果一致。

表1　规则状态映射表

状态名	对应实数
休眠态	0
执行态	1
挂起态	2

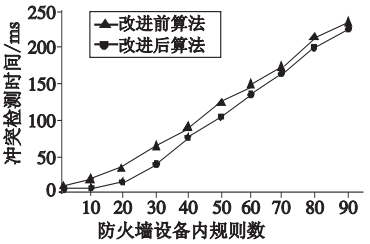

图5　改进前后冲突检测算法处理时间比较

5　结束语

本文提出了一种可扩展的安全设备内策略冲突检测算法。该算法采用规范化和离散化技术,将策略域的属性数据映射到实数集合,并将实数集上的规则属性数据划分为区间,以减少存储离散性规则属性数据所需的空间复杂度;然后通过定义实数区间的运算判断策略域属性数据之间的关系,实现了冲突检测算法的可扩展性;此外,通过加入规则过滤环节,提高了安全策略冲突检测算法的执行效率;最后,实验验证了冲突检测算法的效率,结果表明算法正确高效,具有实用价值。下一步工作将致力于研究安全设备内策略冲突检测算法的优化问题,进一步提高算法的效率。同时以设备内冲突检测为前提,研究如何检测安全设备之间的策略冲突。

参考文献:

[1] AL-SHAER E, HAMED H. Taxonomy of conflicts in network security policies [J]. IEEE Communications Magazine, 2006, 44(3): 134-141.

[2] EPPSTEIN D, MUTHUKRISHNAN S. Internet packet filter management and rectangle geometry[C]//Proc of the 12th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA). [S.l.]: ACM Computing Research Repository, 2001: 827-835.

[3] HARI A, SURI S, PARULKAR G. Detecting and resolution packet filter conflicts[C]//Proc of the 19th Annual Joint Conference of the IEEE Computer and Communications Society. Tel Aviv, Israel: IEEE, 2000: 1203-1212.

[4] ALFARO J G, CUPPENS F, BOULAHIA C N. Towards filtering and alerting rule rewriting on single-component policies [C]//Proc of Conference on Computer Safety, Reliability, and Security. Berlin: Springer, 2006: 182-194.

[5] 王卫平,陈文惠. 防火墙规则配置错误分析及其检测算法[J]. 计算机应用,2005,25(10):2269-2271.

[6] MAYER A, WOOL A, ZISKIND E. Fang: a firewall analysis engine [C]//Proc of IEEE Symposium on Security and Privacy. Berkeley, CA: IEEE, 2000: 177-187.

[7] WOOL A. Architecting the lumeta firewall analyzer[C]//Proc of the 10th USENIX Security Symposium. Berkeley, CA: USENIX Association, 2001: 7.

[8] ERONEN P, ZITTING J. An expert system for analyzing firewall rules, IMM-TR-2001-14 [R]. [S. l.]: University of Denmark, 2001: 100-107.

[9] GAO Zhuo-min. Conflict handling in policy-based security management [D]. Florida: The University of Florida, 2002.

[10] AL-SHAER E S, HAMED H H. Discovery of policy anomalies in distributed firewalls[C]//Proc of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies. [S. l.]: IEEE, 2004: 2605-2616.

[11] CUPPENS F, CUPPENS-BOULAHIA N, GARC'A-ALFARO J. Detecting and removal of firewall misconfiguration[C]//Proc of International Conference on Communication, Network and Information Security. Barcelona: Universitat Autonoma de Barcelona, 2005: 154-162.

[12] AL-SHAER E, HAMED H. Modeling and management of firewall policies [J]. IEEE Trans on Network and Service Management, 2004, 1(1): 2-10.

[13] WU Bei, CHEN Xing-yuan, WANG Yong-liang, *et al*. Network system model-based multi-level policy generation and representation [C]//Proc of IEEE International Conference on Computer Science and Software Engineering. 2008: 283-287.

[14] DAMIANOU N, DULAY N, LUPU E, *et al*. The ponder policy specification language[C]//Proc of the Policy Workshop on Policies for Distributed Systems and Networks. London: Springer-Verlag, 2001: 18-39.

(上接第 1465 页)

[3] CANARD S, TRAORE J. On fair e-cash systems based on group signature schemes [C]//Proc of ACISP'03, LNCS 2727. Berlin: Springer-Verlag, 2003: 237-248.

[4] CAMENISCH J. Efficient anonymous fingerprinting with group signatures[C]//Proc of ASIACRYPT'00, LNCS 1976. Berlin: Springer-Verlag, 2000: 415-428.

[5] CONSTANTIN P. Application of group signatures to anonymous fingerprinting schemes[C]//Proc of VIPromCom'02. [S. l.]: IEEE, 2002: 177-182.

[6] BONEH D, SHACHAM H. Group signatures with verifer-local revocation[C]//Proc of CCS'04. Washington: ACM Press, 2004: 168-177.

[7] BONEH D, BOYEN X. Short signatures without random oracles [C]//Proc of Eurocrypt'04. Heidelberg: Springer-Verlag, 2004: 56-73.

[8] BONEH D, BOYEN X, SHACHAM H. Short group signatures[C]//Proc of Crypto'04. California: Springer-Verlag, 2004: 41-55.

[9] NAKANISHI T, FUNABIKI N. A short verifer-local revocation group signature schemes with backward unlinkability[J]. IEICE Trans on Fundamentals of Electronics, 2007, E90(9): 1793-1802.

[10] 魏凌波,武传坤,周苏静. 具有向后无关性的本地验证撤销群签名方案[J]. 计算机研究与发展,2008,8:1315-1321.

[11] 钟军,何大可. 一种新型的群签名方案[J]. 电子与信息学报,2008,30(5):1214-1217.

[12] MIYAJI A, NAKABAYASHI M. TAKANO S. New explicit conditions of elliptic curve traces for FR-reduction [J]. IEICE Trans on Discrete Mathematics and its Applications, 2001, 84(5): 1234-1243.

[13] 钟军. 群数字签名方案的设计与研究[D]. 成都:西南交通大学,2007.