

文章编号:1001-9081(2009)08-2220-03

## 标准模型下的高效短群签名

马海英,石振国,顾翔

(南通大学 计算机科学与技术学院,江苏 南通 226019)

(mhy8855@ntu.edu.com)

**摘要:**基于 SDH 假设下 BB 签名方案,构造了一个两层签名方案,通过应用合理的假设和非交互知识证明系统,提出了一种标准模型下完全匿名的动态短群签名方案,并证明了该方案满足 BSZ 模型的安全需求。与最近的其他方案相比,该方案具有较高的运行效率和较短的签名长度,且允许新成员的动态加入,群管理员不能伪造成员的签名。

**关键词:**短群签名;标准模型;完全匿名性;可追踪性;不可陷害性

**中图分类号:** TP393.08 **文献标志码:** A

### Short group signature with high efficiency under standard model

MA Hai-ying, SHI Zhen-guo, GU Xiang

(College of Computer Science and Technology, Nantong University, Nantong Jiangsu 226019, China)

**Abstract:** This paper constructed a two-level signature scheme based on BB signature based on SDH assumption. By making certain reasonable assumptions and applying the technique of non-interactive proof system, a full anonymous dynamic short group signature scheme with the standard model was presented. The scheme was proved to satisfy the secure request of BSZ model. Compared with the latest other schemes, the scheme is more efficient and of shorter length of group signature. It allows new member to join in the group dynamically, and the group manager cannot forge any member's signature.

**Key words:** short group signature; standard model; full anonymity; traceability; non-frameability

## 0 引言

群签名是一个非常有用的密码学工具。在一个群签名方案中,群中合法成员可以以匿名的方式代表整个群体对消息进行签名,并且在有争议的时候,群管理者可以确定签名者的身份。群签名方案有很多的应用场合,比如电子现金、投票协议等,然而在实际应用中群签名的运行效率和签名长度是其不能得到广泛应用的重要原因。

近年来,有很多种群签名方案被提出,Bellare 等人为群签名方案的安全性证明提供了标准模式<sup>[1]</sup>。Bellare, Shi 和 Zhang 针对动态群将 BMW 模型做了扩展,Bellare 等人在文献[2]中提出的动态群签名模型中引入了两个群权威,即群管理员和公开者,群管理员与加入的成员一起产生成员各自的签名私钥,群管理员还要维护一张注册表,该注册表能被公开者读取,公开者用于揭露签名者的真实身份。同时 BSZ 提出了一个动态群签名方案的标准模型,在该模型中给出了一个安全的动态群签名方案应该具备的正确性和三个安全需求的实验。2004 年文献[3]中提出了基于随机模型下的短群签名方案,由于随机模型在实际使用中存在安全隐患,2006 年,Boneh 和 Waters 采用新的非交互零知识证明技术提出一个基于标准模型下的群签名<sup>[4]</sup>,但该模型的完全匿名性被做了一定程度的弱化。

本文构造了一种标准模型下完全匿名的动态短群签名方案,通过应用合理的假设和非交互知识证明系统,证明了该方案满足 BSZ 模型的安全性需求,即正确性、匿名性、可追踪性和抗陷害性。

## 1 预备知识

双线性群:设  $G$  和  $G_T$  是阶为  $n$  ( $n$  为合数或素数) 的有限循环群,映射  $e: G \times G \rightarrow G_T$  称为双线性映射,且满足以下三个性质:双线性性、非退化性和可计算性。

**定义 1**<sup>[5]</sup> 如果不存在概率多项式时间算法解决子群决定问题,子群决定假设在合数阶群  $G$  上成立。

**定义 2**<sup>[6]</sup> 如果没有  $t$  时间算法以至少  $\epsilon$  优势解决  $(G_1, G_2)$  上的  $q$ -SDH 问题,则称群  $(G_1, G_2)$  上  $(l, t, \epsilon)$ -SDH 假设成立。

**定义 3**<sup>[5]</sup>  $(l, t, \epsilon)$ -OMSDH 假设。如果没有  $t$  时间算法以至少  $\epsilon$  优势解决  $G$  上的  $l$ -OMSDH 问题,则称  $G$  上  $(l, t, \epsilon)$ -OMSDH 假设成立。

**定义 4**<sup>[5]</sup>  $(l, t, \epsilon)$ -MOMSDH 假设。如果没有  $t$  时间算法以至少  $\epsilon$  优势解决  $G$  上的  $l$ -MOMSDH 问题,则称  $G$  上  $(l, t, \epsilon)$ -MOMSDH 假设成立。

## 2 二层签名方案

设  $\lambda$  为系统安全参数,用户身份  $id$  和消息  $M$  都取自  $\{0, 1\}^{\lambda}$ 。设乘法循环群  $G_1, G_2$  的阶为  $n = pq$  ( $p, q$  为素数),记  $G_1$  的  $p$  阶子群  $G_{1p} = \langle g_1 \rangle$ ,  $G_2$  的  $p$  阶子群  $G_{2p} = \langle g_2 \rangle$ ,双线性映射  $e_1: G_{1p} \times G_{2p} \rightarrow G_T$ 。

### 2.1 系统初始化

首先生成群管理员私钥  $\alpha, \beta \in Z_p^*$ , 计算群公钥  $u = g_2^{\alpha} \in G_{2p}, v = g_2^{\beta} \in G_{2p}, Z = e_1(g_1, g_2) \in G_T$ , 即  $PP = (g_1, g_2, u, v, Z)$ , 然后生成公开的抗联合攻击哈希函数  $H: \{0, 1\}^{\lambda} \rightarrow Z_p^*$ 。

收稿日期:2009-02-16;修回日期:2009-04-10。

基金项目:江苏省自然科学基金资助项目(08KJB520009;07KJB520096);南通大学引进人才科研启动基金资助项目(03080053;03080043)。

作者简介:马海英(1977-),女,河南卫辉人,讲师,硕士,主要研究方向:网络信息安全;石振国(1964-),男,江苏如皋人,副教授,博士,主要研究方向:网格计算、分布式智能信息处理;顾翔(1973-),男,江苏南通人,副教授,博士,主要研究方向:协议形式化技术、信息安全。

$$\pi' = e_2(g_1, g_2^{x+H(M)})^{t'3} \cdot e_2(\sigma'_3, h^{t'1} k^{t'2}) = \\ e_2(g_1, g_2^{x+H(M)})^{\frac{y+H(M)}{y+H(M)} \cdot \frac{\alpha+\beta x'+x'}{\alpha+\beta x} t_3} \cdot e_2(\sigma_3, h^{t_1+(x-x')/\eta} k^{t_2+\beta(r-r')/\theta}) =$$

$$\begin{aligned}
& e_2(\sigma_3, g_2)^{\alpha+\beta r'+x'} \cdot e_2(\sigma_3, h^{t_1} k^{t_2}) \cdot e_2(\sigma_3, h^{(x-x')/\eta_1} k^{\frac{\beta(r-r')}{\theta}}) = \\
& e_2(\sigma_3, g_2)^{\alpha+\beta r'+x'} \cdot e_2(\sigma_3, g_2)^{x-x'+\beta(r-r')} \cdot e_2(\sigma_3, h^{t_1} k^{t_2}) = \\
& e_2(\sigma_3, g_2)^{\alpha+\beta r+x} \cdot e_2(\sigma_3, h^{t_1} k^{t_2}) = \\
& e_2(g_1, g_2^{x+H(M)})^{t_3} \cdot e_2(\sigma_3, h^{t_1} k^{t_2}) = \\
& e_2(g_1, \rho_4)^{t_3} \cdot e_2(\sigma_3, h^{t_1} k^{t_2}) = \pi
\end{aligned}$$

因此,  $\pi = \pi'$ , 尽管模拟者用  $x$  产生了签名, 但签名却不能揭示签名者身份, 所以, 可以断定在模拟环境中, 敌手  $A$  在匿名性游戏中猜出身份的概率可以忽略不计。

#### 4.3 可追踪性

**定理 2** 如果存在一个  $(t, \varepsilon)$ , 敌手  $A$  可打破群签名方案的追踪性, 那么就存在一个  $(t', \varepsilon)$  选择性消息敌手打破二层签名方案的不可伪造性。

**证明** 假定存在一个和敌手  $A$  交互的模拟者  $B$ , 希望打破二层签名方案的可追踪性, 它执行以下算法。

在系统初始化阶段,  $B$  运行二层签名方案的初始化程序, 产生公共参数并公开它们, 然后,  $B$  把追踪私钥  $TK = q$  发送给  $A$ , 因此,  $A$  具有追踪权限。  $A$  向  $B$  询问身份  $id$  的私钥,  $B$  询问两层签名方案的用户私钥生成算法, 得到用户私钥  $K_{id} = (A, x, y, r)$ , 并发送给  $A$ 。  $A$  向  $B$  询问  $M$  以身份  $id$  的群签名,  $B$  直接询问二层签名方案的签名预言机, 得到  $\rho = (\rho_1, \rho_2, \rho_3, \rho_4)$ , 然后随机生成  $t_1 \in Z_n^*, t_2, t_3 \in Z_p^*$ , 计算群签名  $\sigma = (\rho_1 h^{t_1}, \rho_2 k^{t_2}, \rho_3^{t_3}, e_2(g_1, \rho_4)^{t_3} \cdot e_2(\rho_3^{t_3}, h^{t_1} k^{t_2}))$ , 显然上述为一个有效群签名,  $A$  可以用群公钥来验证上式的有效性, 并用  $q$  追踪它的身份。

在某时刻,  $A$  输出它的伪造签名  $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \pi^*)$ , 该签名被追踪到  $(id^*, M^*)$ , 要求  $A$  不能询问  $id^*$  的私钥, 并且上述签名不是通过预言机产生的。由  $\pi^*$  我们可得:

$$e_2(g_1, \rho_4)^{t_3} \cdot e_2(\sigma_3^*, h^{t_1} k^{t_2}) = e_2(\sigma_3^*, u\sigma_1^* \sigma_2^*)$$

由于

$$\begin{aligned}
e_2(\sigma_3^*, u\sigma_1^* \sigma_2^*) &= e_2(\rho_3^{t_3}, u\rho_1 h^{t_1} \rho_2 k^{t_2}) = \\
& e_2(\rho_3^{t_3}, u\rho_1 \rho_2) \cdot e_2(\sigma_3^*, h^{t_1} k^{t_2})
\end{aligned}$$

所以  $e_2(g_1^{t_3}, \rho_4) = e_2(\rho_3^{t_3}, u\rho_1 \rho_2)$ , 由于  $g_1^{t_3}$  和  $\rho_3^{t_3} \in G_{1p}$ ,  $\rho_4$  和  $u\rho_1 \rho_2 \in G_{2p}$ , 所以,

$$e_1(\rho_3^{t_3}, u\rho_1 \rho_2) = e_1(\rho_3^{\frac{y+H(M)}{x+\beta r+x} t_3}, g_2^{\alpha+\beta r+x}) =$$

$$e_1(\rho_3^{t_3}, g_2^{x+H(M)}) = e_1(\rho_3^{t_3}, \rho_4)$$

$e_1(\rho_3, u\rho_1 \rho_2)^{t_3} = e_1(g_1, \rho_4)^{t_3}$ , 由于  $G_T$  为素数阶  $p$  的循环群, 可得  $e_1(\rho_3, u\rho_1 \rho_2) = e_1(g_1, \rho_4)$ , 即  $(\rho_1, \rho_2, \rho_3, \rho_4)$  可以通过两层签名方案的验证等式, 所以它们是一个伪造的两层签名, 因此,  $B$  可打破二层签名方案的不可伪造性, 即定理 2 得证。

#### 4.4 不可陷害性

**定理 3** 如果存在一个  $(t, \varepsilon)$ , 敌手  $A$  可打破群签名方案的不可陷害性, 那么就存在一个  $(t', \varepsilon)$  选择性消息敌手打破二层签名方案的不可陷害性。

**证明** 假定存在一个和敌手  $A$  交互的模拟者  $B$ , 希望打破二层签名方案的不可陷害性,  $B$  执行算法同定理 3, 在某时刻  $A$  产生群签名  $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \pi^*)$  追踪到已存在的用户  $K_{id}^* = (A^*, x^*, y^*, r^*)$ , 同定理 2 的证明过程, 则有  $(\rho_1, \rho_2, \rho_3, \rho_4)$  为二层签名方案中用户  $K_{id}^* = (A^*, x^*, y^*, r^*)$  的签名, 因此打破了二层签名方案的不可陷害性, 即定理 3 得证。

#### 4.5 效率分析

从表 1 可以看出, 本文方案与 LCSL<sup>[5]</sup> 和 BW07<sup>[7]</sup> 群签名方案相比, 主要优势在于允许新成员的动态加入, 并且群管理员不能伪造任何成员的签名, 具有不可陷害性。特别的, 与 LCSL 方案相比, 我们的方案具有较高的运行效率和较短的签名长度, 并且满足 BSZ 动态群签名的安全需求。

表 1 与其他群签名方案中主要性能参数的比较

性能	IBW07 方案	LCSL 方案	本文方案
加入	$3T_{\text{Exp}}$	$T_{\text{Exp}}$	$5T_{\text{Exp}}$
签名	$12T_{\text{Exp}} + (m+10)T_{\text{Mul}}$	$11T_{\text{Exp}} + 8T_{\text{Mul}}$	$10T_{\text{Exp}} + 4T_{\text{Mul}} + 2T_{\text{pair}}$
验证	$6T_{\text{pair}} + 3T_{\text{Exp}} + (m+5)T_{\text{Mul}}$	$6T_{\text{pair}} + 4T_{\text{Mul}} + 3T_{\text{Exp}}$	$T_{\text{pair}} + 2T_{\text{Mul}}$
打开	$T_{\text{Exp}}$	$T_{\text{Exp}}$	$T_{\text{Exp}}$
签名长度	$6   G  $	$5   G  $	$4   G  $
加入新成员	否	否	能
群管理员陷害成员	能	能	否

## 5 结语

本文基于 SDH 假设下的 BB 签名方案<sup>[6]</sup> 构造了一个两层签名方案, 并在此基础上提出了一种标准模型下完全匿名的动态短群签名方案。与其他方案相比, 本文方案具有较高的运行效率和较短的签名长度, 且允许新成员的动态加入, 群管理员不能伪造成员的签名。但该方案依然是在合数阶群上实现的, 为了获得更好的效率, 模型的安全性被做了一定程度的弱化。下一步的工作是在素数阶群上实现标准模型下的短群签名方案, 并加强模型的安全性。

#### 参考文献:

- [1] BELLARE M, MICCIANCIO D, WARINSCHI B. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions [C]// Proceedings of EUROCRYPT 2003, LNCS 2656. Berlin: Springer-Verlag, 2003:

614-629.

- [2] BELLARE M, SHI H, ZANG C. Foundations of group signatures: The case of dynamic groups[C]// Proceedings of the Cryptographers' Track at the RSA Conference 2005. Berlin: Springer-Verlag, 2005: 136-153.
- [3] BONEH D, BOYEN X, SHACHAM H. Short group signatures [C]// Proceedings of the 24th Annual International Cryptology Conference, LNCS 3152. Berlin: Springer, 2004: 41-55.
- [4] BOYEN X, WATERS B. Compact group signatures without random oracles[C]// Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2006: 427-444.
- [5] LIANG XIAOHUI, CAO ZHENFU, SHAO JUN, et al. Short group signature without random oracles [C]// ICISC 2007, LNCS 4861. Berlin: Springer-Verlag, 2007: 69-82.

(下转第 2226 页)

```

 $\Gamma_{id} = \{Inst_{as}, SME_i, ME_m, Id: 1 \leq m \leq n\} \cup \{E_k, Id\}$ 
 $AS_k = (SME_i, TimeGap, \Gamma_{id}, \emptyset, \emptyset)$ 
if  $\exists AS \in Inst_{as}, \Gamma_{AS} \&\& \triangleright SubSeq(AS_k, AS)$ 
 $\Gamma_{inst}(E_k) = \Gamma_{inst}(E_k) \cup \{Inst_{as}\}$ 
end if
end for
 $Inst_k = Inst_{as} \in \Gamma_{inst}(E_k) \&\& \max(E_k, Time - Inst_{as}, Time)$ 
if  $\exists ME_i \in Inst_k, SME_i \&\& E_k, Id = ME_i, Id$ 
 $Inst_k, SME_i, ME_i, \Gamma_E = Inst_k, SME_i, ME_i, \Gamma_E \cup E_k$ 
else
 $Inst_k, SME_i, \Gamma_{ME} = Inst_k, SME_i, \Gamma_{ME} \cup AllocateME(E_k)$ 
 $Inst_k, \Gamma_{AS} = \{AS: \forall ME_i \in SME, \Gamma_{ME}, ME_i, Id \in AS, \Gamma_{id}\}$ 
CreateInstance( $\Gamma_s, \Gamma_{inst}, E_k$ )
 $\Gamma_{s1} = \{AS_j: AS_j \in \Gamma_s \wedge E_k, Id \in AS_j, \Gamma_{id}\}$ 
if  $\Gamma_{s1} \neq \emptyset$ 
 $SME_i = AllocateSME(E_k)$ 
 $\Gamma_{inst} = \Gamma_{inst} \cup \{(SME_i, \Gamma_{s1}, E_k, Time)\}$ 
Endif

```

### 3 实验评估

我们已经实现了系统的一个初步原型,并使用 Darpa99 数据集的第三周网内数据和 Darpa2000 数据集进行场景挖掘实验。实验环境是 Windows XP Professional SP2, Intel CPU 2.66 GHz, 512 MB 内存, 原始报警由 Snort 2.8.2 的 Win32 版本产生, 系统原型使用 VC++6.0 开发。

我们使用 DARPA99 数据来验证场景构建算法的性能。由于 Darpa99 每天的报警都大致为 3500~4000 条, 因此我们设定  $Thr. TimeThr$  为一天, 每条超报警序列和场景的 TimeGap 属性同样设置为一整天。对于 3000 多条报警, 场景构建算法所耗时间为 80~90 ms, 如果对整周数据分析, 时间在 400 ms 左右, 每天场景为 30~40 个。

我们应用 Darpa2000 中内网在阶段 1 到阶段 5 收集的数据来说明识别攻击场景。应用场景构建算法分析得出共有场景 16 个点表示每个场景的  $\Gamma_{id}$  集合。图 2 中序列长度最长的场景 2 勾画了一幅完整的攻击场景, 攻击者首先寻找是否存在 rpc sadmind 漏洞 (1:1957), 接下来对 RPC 请求解码 (1:12626, 1:585, 1:12628, 1:2256), 然后发起 exploit 攻击 (1:1911) 获得管理员权限, 最后调用 rsh 得到远程 shell (1:610), 此后攻击者可以在此基础上攻击其他机器。很容易看出, 图中最复杂的 4 个场景均有共同子序列, 因为在构建超报警序列时, 由于 1:585, 1:12626 和 1:12682, 1:2256 这些报警的优先级相同而且它们在报警序列中以不同时间顺序出现过, 在初始化时会被构建为不同的报警序列, 序列挖掘后则形成不同场景, 在实际应用过程中有可能造成场景数量过多, 因此需要进一步研究场景的表示方法, 将拥有共同子序列的多个场景合并为一个场景。

由于我们的实验仅使用 Snort 对 Darpa2000 的网络数据进行分析, 对 Snort 产生的原始报警做进一步聚合与关联处理, 因此实验结果只验证了 Darpa2000 数据的阶段 1 到阶段 4

的攻击场景关联, 而最后一步的 DDoS 攻击 (阶段 5), 由于 Snort 没有任何报警, 因此实验没有检测到该 DDoS 攻击。

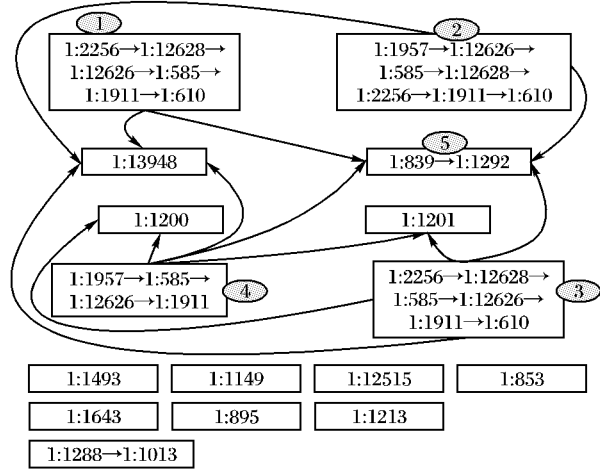


图 2 Darpa2000 数据的场景集合

### 4 结语

本文提出了一种基于闭频繁序列挖掘算法来进行入侵场景自动构建的方法, 并给出了所有相关算法的逻辑描述。该方法可根据设定的阈值从已有原始报警集合提炼出所有可能的攻击场景集合, 然后用这些场景去聚合与关联随后的原始报警。在 Darpa99 和 Darpa2000 数据集上的实验表明, 该方法适合在线运行, 并且不需要额外先验知识, 能有效发现复合攻击场景。未来工作主要包括: 1) 研究频繁模式更新算法, 解决场景集合的快速自适应更新问题; 2) 当前生成的场景还仅仅是报警序列, 导致场景集合中存在很多冗余信息, 需要进一步研究如何将这些具有相同子序列的场景合并为一个场景。

#### 参考文献:

- [1] 穆成坡, 黄厚宽, 田盛丰. 入侵检测系统报警信息聚合于关联技术研究综述[J]. 计算机研究与发展, 2006, 43(1): 1-8.
- [2] VALDES A, SKINER K. Probabilistic alert correlation[C]// The 4th International Symposium on Recent Advances in Intrusion Detection: RAID 2001, LNCS 2212. Berlin: Springer, 2001: 54-68.
- [3] CUPPENS F, ORATOL R. LAMBDA: A language to model a database for detection of attacks[C]// Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection. London: Springer-Verlag, 2000: 197-216.
- [4] NING P, CUI Y, REEVES D S. Analysing intensive intrusion alerts via correlation[C]// Recent Advances in Intrusion Detection 2002, LNCS 2516. Berlin: Springer-Verlag, 2002: 74-94.
- [5] QIN X, LEE W. Statistical causality of INFOSEC alert data[C]// Recent Advances in Intrusion Detection 2003, LNCS 2820, Berlin: Springer-Verlag, 2003: 73-94.
- [6] WANG J Y, HAN J W. BIDE: Efficient mining of frequent closed sequences[C]// Proceedings of 20th International Conference on Data Engineering. Washington, DC: IEEE Computer Society, 2004: 79-90.

(上接第 2222 页)

- [6] BONEH D, BOYEN X. Short signatures without random oracles and the SDH assumption in bilinear groups[J]. Journal of Cryptology, 2008, 21(2): 149-177.
- [7] BOYEN X, WATERS B. Full-domain subgroup hiding and constant-size group signatures[C]// Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography, LNCS 4450. Berlin: Springer, 2007: 1-15.
- [8] DELERABLEE C, POINTCHEVAL D. Dynamic fully anonymous short group signatures[C]// Vietcrypt'06, LNCS 4341. Berlin: Springer-Verlag, 2006: 193-210.
- [9] GROTH J. Fully Anonymous group signatures without random oracles[C]// Advances in Cryptology - ASIACRYPT 2007, LNCS 4833. Berlin: Springer, 2008: 164-180.