文章编号:1001 - 9081(2008)11 - 2827 - 02

依托 BLS 签名的基于身份盲签名方案

高 伟[1],李 飞[1],徐邦海[2]
(1. 鲁东大学 数学与信息学院,山东 烟台 264025; 2. 鲁东大学 计算机科学与技术学院,山东 烟台 264025)
(sdgaowei@ yahoo. com. cn)

摘 要:依托 Boneh 等人提出的签名(BLS 签名)算法、BLS 签名的盲生成算法和 BLS 签名的聚合算法,提出了一种高效的基于身份盲签名方案。该方案具有轮复杂度最优的特点,即盲签名的生成协议只需用户和签名者依次发送一次信息。它的安全性基于 one-more CDH 假设,而其他方案则依赖于一个更强的假设——ROS 假设。另外,它还具有计算效率高,签名长度短等特点,特别适合电子现金、网络投票等具体应用。

关键词:BLS 签名;基于身份盲签名;双线性对
中图分类号: TP309.7 **文献标志码**:A

Identity-based blind signature scheme based on BLS signatures

GAO Wei[1], LI Fei[1], XU Bang-hai[2]
(1. *College of Mathematics and Information, Ludong University, Yantai Shandong* 264025, *China*;
2. *College of Computer Science and Technology, Ludong University, Yantai Shandong* 264025, *China*)

Abstract: Depending on BLS signing algorithm, blind signing algorithm of BLS signatures, and aggregating algorithm of BLS signatures, a new efficient identity-based blind signature scheme was proposed. First, the round complexity of this scheme was optimal, i. e. it was enough for the user and the signer to respectively transmit only one message during each blind signing process. Second, its security was based on the so-called one-more Computational Diffie-Hellman Assumption (CDH) assumption, while the security of the other similar identity-based signature scheme was based on the stronger assumption - ROS assumption. Additionally, this scheme was computationally efficient and had very short signature length. Therefore, it was very suitable for the applications such as e-cash and e-voting.

Key words: BLS signature; identity based blind signature; bilinear pairing

0 引言

盲签名[1]广泛应用于电子投票和电子现金等安全协议的构造中。一般地,一个盲签名应满足以下两个条件:1)不可见性:被签名的消息对签名者是盲的。2)不可追踪性:签名人事后不能追踪签名的消息。

双线性对[2]是构造基于身份密码方案[3]的主要数学工具。结合盲签名和基于身份密码学这两个密码学概念,人们提出了基于身份盲签名的概念,并利用双线性对构造了相应方案[4-6]。文献[7]则粗略地讨论了如何用一般的数字签名构造基于身份盲签名的通用方法。

BLS 签名是利用双线性对构造的一种短签名方案[8],在基于身份密码学和基于双线性对密码学中具有非常广泛的应用。围绕 BLS 签名,人们先后扩展了高效的盲签名算法[9]、门限签名算法[9]和聚合签名算法[10]等。根据现有的 BLS 签名算法,BLS 签名的盲生成算法,BLS 签名的聚合算法,提出了一种新的基于身份盲签名方案,并比较和分析了在通信效率、计算效率、数论假设强度、签名长度等方面均具有比以往同类方案更好的特性,适合电子现金、网络投票等具体应用。

1 预备知识

定义 1 双线性对:令 G_1 和 G_2 是分别是阶为 q(q 是大素数)的加法群和乘法群,P 是群 G_1 的生成元。称 $e: G_1 \times G_1 \rightarrow G_2$ 为双线性对,它满足如下性质:

1) 双线性:对于任给的 $a, b \in Z_q^*$,$e(aP, bP) = e(P, P)^{ab}$;

2) 非退化性:存在 $(R, S) \in G_1 \times G_1$,使得 $e(R, S) \neq 1$,1 表示中 G_2 的单位;

3) 可计算性:对于任意的 $(R, S) \in G_1 \times G_1$,存在有效的多项式算法计算 $e(R, S)$。

下面简要回顾文献[8]的短签名(BLS 签名)方案。令参数 e, G_1, G_2, P 如上所述,m 为待签名的消息,$H: \{0,1\}^* \rightarrow G_1$ 是一个密码学安全的哈希函数。BLS 签名方案由如下三个算法组成:

密钥生成:随机选择 $x_L \in Z_q^*$,计算 $Y_L = x_L P$。Y_L 作为公钥,x_L 作为私钥。

签名生成:输入信息 m,计算签名 $\sigma_L = x_L H(m)$。

签名验证:输入信息 m 和签名 σ_L,判断 $e(H(m), Y_L) = e(\sigma_L, P)$ 是否成立。

文献[9]给出了 BLS 签名的一种盲生成算法(后面称 Boldyreva 盲签名):首先,用户随机选取 $r \in Z_q^*$ 作为盲因子,计算 $m' = rH(m)$ 作为消息 m 的盲化结果,并将 m' 发送给签名者。接着,签名者计算 $\sigma' = xm'$,并将 σ' 发送给用户。最后,用户计算 $\sigma_1 = r^{-1}\sigma'$ 作为最终签名。

文献[10]指出:两个签名者 L 和 L' 在不同的消息上的 BLS 签名(此处分别记做 $\sigma_L = x_L H(m)$,$\sigma_{L'} = x_{L'} H(m')$)可以通过 $\sigma_{L,L'} = \sigma_L + \sigma_{L'} = x_L H(m) + x_{L'} H(m')$ 聚合为一个签名

收稿日期:2008 - 07 - 21;**修回日期**:2008 - 09 - 03。

作者简介:高伟(1978 -),男,山东泰安人,讲师,博士,主要要研究方向:公钥密码学、信息论和网络安全; 李飞(1977 -),女,山东烟台人,助教,主要研究方向:安全密码协议; 徐邦海(1974 -),男,重庆璧山人,副教授,博士,主要研究方向:计算机网络、信息安全。

(BGL 聚合签名),而且可以通过验证 $e(\sigma_{L,L'},P) = e(H(m),x_LP)e(H(m'),x_{L'}P)$ 来判断该聚合签名的合法性。

2 依托 BLS 签名的基于身份盲签名方案

2.1 系统设置

PKG 首先选择 q,G_1,G_2,e,其含义与上一章相同。然后,选择 $P \in G_1$ 作为生成元,定义哈希函数 $H:\{0,1\}^* \rightarrow G_1$。最后,PKG 随机选择 $s \in Z_q^*$,计算 $P_{pub} = sP$,将 s 秘密保存,公开参数 $params = \{q,G_1,G_2,e,P,P_{pub}\}$。

2.2 密钥提取

签名人把其身份信息 ID 提交给 PKG。PKG 随机选取 $x \in Z_q^*$,并计算 $pk = xP, Q_{ID} = H(ID \| pk), C_{ID} = sQ_{ID}$。最后,PKG 把 x,pk,C_{ID} 发送给签名者。

2.3 盲签名协议

假设用户需要得到消息 m 的盲签名,基于身份的盲签名由以下步骤组成:

1) 用户随机选取 $r \in Z_q^*$ 作为盲因子,计算 $m' = rH(m)$ 作为消息 m 的盲化结果,并将 m' 发送给签名者。

2) 签名者计算 $\sigma' = xm'$,并将 σ',pk,C_{ID} 发送给用户。

3) 为了去除盲因子,用户计算 $\sigma_1 = r^{-1}\sigma'$。

4) 用户计算 $\sigma = \sigma_1 + C_{ID}$,并把 (σ,pk) 作为消息 m 的签名。

2.4 签名的验证

验证者判断等式 $e(\sigma,P) = e(H(ID \| pk),P_{pub})e(H(m),pk)$ 是否成立。若成立,则 (σ,pk) 是签名者 ID 在消息 m 的签名。

3 安全性分析

综上所述,我们显然有如下结论:

引理 1 $C_{ID} = sQ_{ID}$ 是公钥为 $P_{pub} = sP$,私钥为 s,被签名消息为 $(ID \| pk)$ 的 BLS 签名。

引理 2 $\sigma_1 = r^{-1}\sigma'$ 是公钥为 $pk = xP$,私钥为 x,被签名消息为 m 的 BLS 签名。

引理 3 $\sigma = r^{-1}\sigma' + C_{ID}$ 可以看做 $C_{ID} = sQ_{ID}$ 和 $r^{-1}\sigma'$ 这两个 BLS 签名的 BGL 聚合签名。

引理 4 2.3 节中的 1) ~3) 构成 Boldyreva 盲签名协议。

对于 BLS 签名方案,Boldyreva 盲签名方案,BGL 聚合签名方案,相应文献[7-10]有如下安全性结论:

1) 在 CDH(Computational Diffie-Hellman)假设和随机预言模型下,对于适应性选择消息攻击,BLS 短签名是存在性不可伪造的[8]。

2) 在 chosen-target CDH 假设(又称 one more CDH 假设)成立的前提下,Boldyreva 盲签名方案在随机预言模型下可以抵抗选择消息攻击下的多一伪造(one more forgery)[9]。

3) 在 CDH 假设和随机预言模型下,BGL 聚合签名方案在聚合式选择密钥攻击模型下是存在性不可伪造的[10]。

另外,文献[7]指出,在基本签名方案和盲签名方案安全的前提下,采用其通用的构造方法所得到的基于身份盲签名方案也是安全的。本文所提出的具体方案与文献[7]中的方法密切相关,是受文献[7]的通用构造方法启发下,在通信复杂度、计算复杂度、签名长度、数论假设强度等方面做了进一步优化的结果。

根据上述引理及相关论述,显然有如下结论:

定理 1 在 BLS 签名方案、Boldyreva 盲签名方案、BGL 聚合签名安全的前提下,本文所提出的基于身份盲签名方案也是安全的(满足盲性和多一不可为造型)。

4 比较

从表 1 可以看出,在轮复杂度、计算复杂度、签名长度和假设强度等方面,本文方案均达到了最优。我们需要说明的是:

1) 文献[7]并未给出具体的盲签名方案,表 1 中是将其通用方法套用到 BLS 签名时的结果。

2) 盲签名的最优轮复杂度为两次通信,即双方各发一次信息,故本文所提方案达到了最优轮复杂度。而对于电子现金和网络投票等应用,轮复杂度是最关键的效率瓶颈。如果考虑通常情况下,是用户而非签名者发起盲签名协议,文献[4-6]的方案实际要 4 次通信(首次信息是由用户发起)。

3) 文献[4-6]中,作者指出其安全性需要 ROS 假设,但是却不能够给予证明。特别地,ROS 假设需要的安全参数至少为 1 600 b,对应地,如果要达到紧凑的可证明安全性,文献[4-6]中的签名长度则是 3 200 b。而上述比较中,我们仅假设其签名长度为 320 b。

4) One more CDH 作为一种 one more one-way function 研究较多,且与 CDH 问题密切相关,故该假设比较合理。而 ROS 假设则相反,文献[4]提到已经找到的攻击 ROS 问题的算法迫使其安全参数提高到了 1 600 b。

5) 在基于双线性对密码学中,双线性对运算往往是最耗时的运算部分,文献[4-6]在签名过程中均需要设计双线性对运算,而本文方案则不需要该运算。

表 1 几种方案的比较

方案	轮复杂度	签名长度/b	数论假设	签名是否需对运算
本文方案	2 次	320	One-more CDH 假设	不需要
文献[4]方案	3 次或 4 次	320	ROS 假设	需要
文献[5]方案	3 次或 4 次	320	ROS 假设	需要
文献[6]方案	3 次或 4 次	320	ROS 假设	需要
文献[7]方案	3 次(默认优化后)	480	One-more CDH 假设	不需要

5 结语

提出了一种新的基于身份签名方案,克服了以往同类方案在通信效率、计算效率、安全性证明、签名长度等方面的不足,故具有更为广泛的适用性。

参考文献:

[1] CHAUM D. Blind signature for untraceable payments[C]// Advance in Cryptology - Crypto'82. Berlin: Springer-Verlag, 1983: 199-203.

[2] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]// Advances in Cryptology - Crypto 2001, LNCS 2139. Berlin: Springer-Verlag, 2001: 213-229.

[3] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// Advances in Cryptology - Crypto 1984, LNCS196. Berlin: Springer-Verlag, 1984: 47-53.

[4] ZHANG F, KIM K. ID-based blind signature and ring signature from pairings [C]// Advances in Cryptology - Asiacrypt 2002, LNCS 2501. Berlin: Springer-Verlag, 2002: 533-547.

[5] ZHANG F, KIM K. Efficient ID-based blind signature and proxy signature from bilinear pairings[C]// Proceeding of the 13th Australasian Conference on Information Security and Privacy. Berlin: Springer-Verlag, 2003: 312-323. (下转第 2831 页)

计算机病毒检测是一个二分类问题。对于样本空间的每一个样本可以看作是 n 维空间的一个点 $X=(x_1,x_2,\cdots,x_n)$,其中 $x_1,x_2,\cdots,x_n$,分别为行为事件属性 $a_1,a_2,\cdots,a_n$ 的取值。D 为样本类别属性,$D=\{d_0,d_1\}$, d_1 表示病毒,d_0 表示正常程序。依据朴素贝叶斯定理,病毒检测判别式表示为:

$$C(X)=\operatorname{argmax}_d\left(\frac{p(d)p(x\mid d)}{p(x)}\right) \tag{4}$$

根据朴素贝叶斯理论各条件属性相互独立的基本假设和 $p(x)$ 在判别式中对具体样本而言为常数,判别式可简化为:

$$C(X)=\operatorname{argmax}_d\left(p(d)\prod_{i=1}^{n}p(x_i\mid d)\right) \tag{5}$$

4.3　试验及结果

为保证检测方法对典型病毒的检测效率,训练和测试仅对发生恶意行为事件数大于 1 的黑白样本进行。如表 2 所示,黑样本集合 O 按比例 4∶1 随机划分为集合 A 和集合 B,白样本集合 O^0 随机划分成集合 A^0 和 B^0,其中 A^0 的样本数等于集合 A。集合 A 和 A^0 用于训练朴素贝叶斯分类器,集合 B 和 B^0 作为测试集。模型检测效果由检出率(True Positive Fraction, TPF)和误报率(False Positive Fraction, FPF)评价。检出率为黑样本中正确检测为黑样本的样本比例,误报率为白样本中误报为黑样本的比例。检出率和误报率结果取 5 次随机试验的平均结果。

表 2　试验中的样本

样本类别	总样本数	事件数大于 1 的样本数	训练集
黑样本	1 865	1 200(O)	960(A)
白样本	2 821	2 444(O^0)	960(A^0)

阈值 *TMID* 和 *TPD* 取值原则上应保持属性约简前后模型检测效果相当,在试验中,分别取 0.12 和 15,表 3 列出属性约简前后的试验结果。

表 3　属性约简前后的试验结果　%

测试集	维数为 35		维数为 20	
	TPF	*FPF*	*TPF*	*FPF*
$B\cup B^0$	83.82	7.87	86.14	7.96

从表中可以看出,经过约简后的维数从 35 维降到 20 维,在减少运算量的同时,模型检测效果基本保持不变,且对发生事件数大于 1 的样本有着较高的检出率和较低的误报率。

表 4 列出的是属性约简后保留的 20 个属性中 ISDEBUG, WRITE_FILE, DELETEFILE 和 CREATE_PROCESS 四个属性,其中 MI1 表示行为事件属性与类别病毒的互信息,MI0 表示行为事件属性与正常程序的互信息。

这四个属性的共同特点是其与正常程序的互信息要高于病毒程序。在实际的启发式病毒检测中,应降低这类行为在病毒判定中的决策权重,以减少误报率。

表 4　部分保留属性

行为属性	MI1	MI0	MID	PD
ISDEBUG	0.54	0.93	0.39	1.58
WRITE_FILE	0.12	0.30	0.19	1.85
DELETEFILE	-0.06	0.95	1.01	4.66
CREATE_PROCESS	0.27	0.51	0.24	1.64

5　结语

本文提出了一个基于行为特征向量的未知病毒检测方法。特征向量的每一维用于表示一种恶意行为事件,每一事件由相应的 Win32 API 调用及其参数表示。该方法通过监视程序运行行为获取恶意行为特征,其特征提取不依赖于文件内容,可克服基于特征码扫描法在病毒检测上的不足。对于已定义的行为属性,利用互信息理论进行评价和约简,对专家经验进行反馈,去掉专家经验中区分能力较弱的行为属性。实验结果表明,属性约简后的模型仍保持原有模型的检测效果,对于发生事件数大于 1 的样本,有着较高的检出率和较低的误报率。另外,从信息论角度对行为特征的评价也为启发式病毒检测中病毒行为决策权重大小的选取提供了一定的参考。今后的工作将关注以下两个方面:增加特征向量维数,定义更多在病毒和正常程序中具有区分能力的行为特征,使得程序在理论上能被捕获到更多的事件,增加模型可检测样本范围;另一方面,对于被删除的属性,探究其删除的原因,是因为参数定义的不够准确还是该 API 函数本身在黑白样本中就不具有区分度。

参考文献:

[1] XU J Y, SUNG A H, CHAVEZ P, *et al*. Polymorphic malicious executable scanner by API sequence analysis[C]// Proceedings of the 4th International Conference on Hybrid Intelligent Systems. Washington, DC: IEEE Computer Society, 2004: 378 - 383.

[2] KOIKE R, NAKAYA N, KOI Y. Development of system for the automatic generation of unknown virus extermination software[C]// Proceedings of the 2007 International Symposium on Applications and the Internet. Washington, DC: IEEE Computer Society, 2007: 8 - 8.

[3] 张波云,殷建平,蒿敬波,等. 基于多重朴素贝叶斯算法的未知病毒检测[J]. 计算机工程,2006,32(10):18 - 21.

[4] 张文良,黄亚楼,倪维建. 基于差分贡献的垃圾邮件过滤特征选择方法[J]. 计算机工程,2007,33(8):80 - 82.

[5] 伍建军,康耀红. 基于改进的互信息特征选择的文本分类[J]. 计算机应用,2006,26(S2):172 - 173.

[6] 王卫玲,刘培玉,初建崇. 一种改进的基于条件互信息的特征选择算法[J]. 计算机应用,2007,27(2):433 - 435.

(上接第 2828 页)

[6] HUANG Z, CHEN K, WANG Y. Efficient identity-based signatures and blind signatures[C]// Proceeding of the 4th International Conference on Cryptology and Network Security. Berlin: Springer-Verlag, 2005: 120 - 133.

[7] GALINDO D, HERRANZ J, KILTZ E. On the generic construction of identity-based signatures with additional properties[C]// Advances in Cryptology - Asiacrypt 2006, LNCS 4284. Berlin: Springer-Verlag, 2006: 178 - 193.

[8] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[C]// Advances in Cryptology - Asiacrypt 2001, LNCS 2248. Berlin: Springer-Verlag, 2001: 514 - 532.

[9] BOLDYREVA A. Efficient threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme[C]// Proceeding of the 6th International Workshop on Theory and Practice in Public Key Cryptography. Berlin: Springer-Verlag, 2003: 31 - 46.

[10] BONEH D, GENTRY C, LYNN B, *et al*. Aggregate and verifiably encrypted signatures from bilinear maps[C]// Advances in Cryptology - Eurocrypt 2003, LNCS 2656. Berlin: Springer-Verlag, 2003: 416 - 432.