

文章编号:1001-9081(2007)10-2456-03

基于身份的可截取签名方案

蓝才会,王彩芬

(西北师范大学 数学与信息科学学院,兰州 730070)

(lan_ch@lztu.edu.cn)

摘 要:根据批签名的思想,提出了一个新的基于身份的可截取签名(CES)方案,该方案不需要对消息的每个子消息进行签名,有效地提高了签名的效率,而且能够防止私钥产生机构(PKG)伪造签名。在随机预言模型下,证明了其在适应性选择消息攻击及身份攻击下都能抵抗存在伪造。

关键词:可截取签名;基于身份签名;批量签名

中图分类号: TP309.7 **文献标志码:** A

ID-based content extraction signature

LAN Cai-hui, WANG Cai-fen

(College of Mathematics and Information Science, Northwest Normal University, Lanzhou Gansu 730070, China)

Abstract: A new ID-based Content Extraction Signatures (CES) scheme based on the batch signature was proposed. In our scheme, the signer only needs to sign the whole message. But other schemes have to sign each partition of primitive formation, so it improved the efficiency. And the dishonest Private Key Generator can not impersonate any user at any time. The proposed signature scheme can defend existential forgery on adaptively chosen message and ID attack in the random oracle model.

Key words: Content Extraction Signatures (CES); ID-based signature; batch signatures

0 引言

可截取签名(Content Extraction Signatures, CES)^[1]与传统的标准签名体制不同,在可截取签名体制中,给定一个已签名的消息,允许任何人根据需要,针对原消息的一部分,截取一个可公开并可验证的签名,而无需和最初的签名者进行交互。文献[2]中通过在 XML 签名规范中引入可截取签名功能,对 XML 签名进行了扩展。在文献[1]的基础上,文献[3]提出一种采用分级的群组策略的可截取签名方案,可有效地应用于数字图书馆等环境。文献[4]结合了基于身份的密码系统,提出了基于身份的可截取的门限签名方案,但是这个可截取签名方案需要对消息 M 的每一个子消息进行签名,严重地影响签名速度,使得签名效率不高。

文献[5]中提出批签名的概念,并构造了基于 RSA 的批签名方案;之后又出现了基于 DSA 的批签名方案,但是和文献[5]中的方案一样具有对签名消息的数量有限制等缺点。文献[9]中提出了基于二叉树的 Bi-tree 批签名方案,该方案不仅克服了签名消息数量有限制的缺点,而且构造方法和文献[5,6]中构造方法相比,可以把普通的签名算法改造成批签名。

1984 年,Shamir 提出了一基于身份的密码系统的概念^[13]。在一个基于身份的密码系统里,个人公钥可由他公开的唯一身份信息(如邮件地址、IP 地址)很容易计算出来,而私钥由一个可信的密钥生成中心 PKG 来生成,不存在由 CA 颁发公钥证书带来的存储和管理开销问题。之后许多基于身份的密码系统相继被提出,文献[12]利用双线性对提出了第

一个高效、可证明安全的基于身份的密码方案。目前,基于双线性对的基于身份的密码体制存在密钥托管和效率等问题。

本文以文献[7]中的基于身份的签名方案为基础,结合可截取签名体制和批签名思想,提出了一个新的基于身份的可截取签名方案,和现有的其他可截取签名方案相比,不需要对每个子消息进行签名,可以把一般的签名方案推广为可截取签名方案,具有更广泛的应用价值,签名效率提高了很多。

1 相关概念和理论知识

1.1 可截取签名简介

可截取签名允许在多方参与的环境中,使用者针对原消息的一部分,截取一个公开并可验证的签名,而无需和签名者交互。假如一个签名者(如大学)需要对包括 k 个子消息的信息(如学生的出生日期、学号、学习成绩、在校表现等个人信息) $M = \{m_1, m_2, \dots, m_k\}$ 签名,截取者(如学生)需要把签名提供给相关的验证者(如用人单位),但是截取者可以根据签名者的要求把一些信息(如个人信息)删除,算出 M' 的签名,同时验证者能够验证 M' 的签名是签名者签发的。在这种应用环境中使用标准的数字签名,一种实现方式是签名者可以先对 M 和相关要求签名,待截取者验证后,在签名者要求下把要签名的消息 M' 发送给签名者,签名者再对 M' 签名后发送截取者,截取者验证后再传递给验证者,这种实现方式需要验证者和截取者间信息的多次签名、多次验证和多次传递;另一种实现方式是签名者对 k 个子消息的所有组合都签名,把这些签名都发送给截取者,截取者验证 M 和 M' 的签名后,把 M' 的签名给验证者,这种方式克服了签名者和截取者之间的多

收稿日期:2007-04-04;修回日期:2007-06-13。

基金项目:甘肃省自然科学基金资助项目(3ZS051-A25-042);甘肃省科技攻关项目(2GS064-A52-035-03)。

作者简介:蓝才会(1977-),男,江西永丰人,硕士研究生,主要研究方向:信息安全、现代密码学;王彩芬(1963-),女,河北安国人,教授,博士生导师,博士,主要研究方向:信息安全、电子商务协议的设计与分析。

次交互,但是签名数量达到了 2^k ;我们可以考虑对 M 的 k 个子消息都签名,再把签名给截取者,由截取后选择 M' 中包括的子消息签名传递给验证者,这种方式没办法控制截取者非善意的截取而导致的信息歧义、原意改变等问题;总之用标准的数字签名不合理或效率低下。相比之下,可截取签名体制能克服标准数字签名在上述环境中的不便,总的过程是签名者对消息 M 签名,截取者从 M 的签名中计算出 M' 的签名,截取者把 M' 的签名给验证者验证。在这个过程中为了防止截取者的恶意截取,引入了内容截取访问结构 CEAS,在 CEAS 中,对每一个子消息段规定了必须截取和可选截取两种方式,可分别用“1”和“0”表示。截取者根据 CEAS 生成截取子集 $CI(M')$ (标记 M' 中所包含子消息段的编号), M' 仍然包含 k 个子消息段,其中编号不在 $CI(M')$ 子消息段用别的信息填充(要求用填充的信息求不出对应的消息),但 M' 所有子消息段的编号必须与 M 一致。例如 $M = (m_1, m_2, m_3, m_4)$, $CEAS = \{1, 0, 0, 1\}$, $CI(M') = \{1, 4\}$ 和 $M' = (m_1, ?, ?, m_4)$ 是合法的, $CI(M') = \{1, 3, 4\}$ 和 $M' = (m_1, ?, m_3, m_4)$ 也是合法的,其中?为填充的子消息段。一个可截取签名体制具体步骤如下:

- 1) 密钥生成。生成一个公、私钥对 (S_k, P_k) 。
- 2) 签名。输入密钥 S_k ,消息和 CEAS,输出一个可截取的全局签名 δ_{Full} 。
- 3) 签名截取。输入消息 M 、全局签名 δ_{Full} 、截取子集 $CI(M')$ 和公钥 P_k ,输出子消息 M' 的签名 δ_{Ext} 。
- 4) 签名验证。输入子消息 M' 、截取的签名 δ_{Ext} 和公钥 P_k ,输出验证结果。

1.2 双线性对

设 $(G_1, +)$ 和 (G_2, \times) 是 q 阶循环群, q 为一大素数, P 为 G_1 的生成元,设在群 G_1 和 G_2 中离散对数问题是困难的。两个群之间的双线性对 $e: G_1 \times G_1 \rightarrow G_2$ 是满足以下条件的映射:

- 1) 双线性: $e(aP, bQ) = e(P, Q)^{ab}; \forall a, b \in \mathbb{Z}_q^*, \forall Q \in G_1$;
- 2) 非退化性: $\exists P, Q \in G_1$,满足 $e(P, Q) \neq 1$;
- 3) 可计算性:对于任意 $P, Q \in G_1$,存在高效的算法能计算出 $e(P, Q)$ 。

利用超奇异椭圆曲线或超椭圆曲线上的 Weil 对和 Tate 对可构造出满足以上条件的双线性^[11,12]。

1.3 一些困难问题

设群 G 为 q 阶循环加群, P 为 G 的生成元。

- 1) 决策 Diffie-Hellman 问题 (DDHP): 已知 P, aP, bP, cP , 其中 $a, b, c \in \mathbb{Z}_q^*$,判定 $c = ab \bmod q$ 是否成立。
- 2) 计算 Diffie-Hellman 问题 (CDHP): 已知 P, aP, bP , 其中 $a, b \in \mathbb{Z}_q^*$,计算 abP 。

定义 1 若在群 G 中,决策 Diffie-Hellman 问题是容易计算的,但计算 Diffie-Hellman 问题是困难的,则称群 G 为 Gap Diffie-Hellman 群。

2 基于身份的可截取签名

2.1 方案描述

2.1.1 系统初始化

G_1 为 q 阶的 Gap Diffie-Hellman 群, G_2 为 q 的循环乘群, H_1, H_2, H_3, H_4 是公开的哈希函数, $H_1: \{0, 1\}^* \times G_1 \rightarrow \mathbb{Z}_q^*$, $H_2: \{0, 1\}^* \times G_1 \rightarrow G_1$, $H_3: \{0, 1\}^* \rightarrow \{0, 1\}^{h_1}$, $H_4: \{0, 1\}^* \rightarrow \{0,$

$1\}^* \rightarrow \{0, 1\}^{h_2}$,其中 h_1 为安全参数,存在一个双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 。 P 为 G_1 中的生成元,私钥管理中心 PKG 选择一个随机整数 $s \in \mathbb{Z}_q^*$ 作为系统的主秘密保存,计算 $P_{pub} = sP$ 。

公开系统参数 $\{G_1, G_2, P, P_{pub}, e, q, H_1, H_2, H_3, H_4\}$ 。

2.1.2 用户密钥生成

假定 ID 表示用户签名者的唯一可识别的身份,PKG 对签名者进行鉴定确信 ID 具有惟一性。密钥生成如下:

1) 签名者任意选取 $r \in \mathbb{Z}_p^*$ 作为其长期私钥,并发送 rP 给 PKG;

2) PKG 计算 $Q_{ID} = H_2(ID, rP)$, Q_{ID} 是签名者基于身份的公钥,任何人都能在获取签名者的签名后从中提取出 rP ,通过系统的公开参数计算出签名者的公钥;

3) PKG 计算 $S_{ID} = sQ_{ID}$,并通过安全的信道发送给签名者,则签名者的私钥 (r, S_{ID}) 。

2.1.3 签名

假定 M 为所要被签名的消息,且按照需要被分成 k 个子部分。 m_u 表示消息 M 中的子消息段,其中 μ 为子消息段在消息 M 中的编号, $u \in \{1, 2, \dots, k\}$ 。 M' 表示截取后的子消息; $CI(M')$ 标记 M' 中所包含的子消息段的索引所构成的集合;CEAS 是内容截取访问结构。

1) 签名者计算 $Q_{ID} = H_2(ID, rP)$ 并按以下方法求总散列值 \bar{M} :首先计算每个子消息 m_i 连接 CEAS 对于 H_3 的散列值,并按消息 M 中的顺序从左向右级联;然后求级联后的对于 H_4 的散列值,这个散列值就是所求的 \bar{M} 。例如 $M = (m_1, m_2, m_3, m_4)$ 。

$$\bar{M} =$$

$$H_4(H_3(m_1 \parallel CEAS) \parallel H_3(m_2 \parallel CEAS) \parallel H_3(m_3 \parallel CEAS) \parallel H_3(m_4 \parallel CEAS))$$

2) 签名者随机选择 $l \in \mathbb{Z}_q^*$,计算 $U = lP$ 和 $h = H_1(\bar{M}, U)$;

3) 签名者计算 $V = lQ_{ID} + h(S_{ID} + rQ_{ID})$ 。

最后输出作为对消息 M 的签名 (M, U, V, rP) 。

2.1.4 签名截取

截取者收到消息 M 的签名 (M, U, V, rP) 后,按 2.1.3 中的 1) 求出总散列值 \bar{M} ,计算 $Q_{ID} = H_2(ID, rP)$ 和 $h = H_1(\bar{M}, U)$,验证 $e(P, V) = e(U + hP_{pub} + hrP, Q_{ID})$,成立则执行如下截取算法:

1) 根据 CEAS 构造 $CI(M')$

2) 用 $M' = (m_1', m_2', \dots, m_k')$ 去替代原来的 $M = (m_1, m_2, \dots, m_k)$ 。

$$m_i' = \begin{cases} m_i, & i \in CI(M') \\ H_3(m_i \parallel CEAS), & i \notin CI(M') \end{cases}$$

完成后,输出子消息 M' 的签名 $(M', CEAS, CI(M'), U, V, rP)$ 。

2.1.5 验证

1) 验证者先验证 $CI(M') \in CEAS$,若成立,则根据 $CI(M')$ 和 M' 恢复总的散列值 \bar{M} ,方法如下:首先判断 i 是否属于 $CI(M')$,若属于,则对应叶子的值为 $H_3(m_i' \parallel CEAS)$,相反,不属于则对应叶子节点的值为 m_i' ,并按消息 M' 中的顺序从左向右级联;然后计算级联后的对于 H_4 的散列值,这个散列值就是 \bar{M} 。

2) 计算 $Q_{ID} = H_2(ID, rP)$ 和 $h = H_1(\bar{M}, U)$,验证 $e(P, V) = e(U + hP_{pub} + hrP, Q_{ID})$ 成立,且 $CI(M') \in CEAS$,则签名为有效签名。

2.2 方案的正确性

引理 1 在上述基于身份的可截取签名方案中采用的基于身份的签名方案是正确的。

证明:

$$\begin{aligned} e(P, V) &= e(P, lQ_{ID} + h(S_{ID} + rQ_{ID})) = \\ &= e(P, lQ_{ID} + hsQ_{ID} + hrQ_{ID}) = \\ &= e(lP + hsP + hrP, Q_{ID}) = \\ &= e(U + hP_{pub} + hrP, Q_{ID}) \end{aligned}$$

引理 2 在上述基于身份的可截取门限签名方案中, 如果对总散列值 \bar{M} 的基于身份的签名方案正确, 则此基于身份的可截取门限签名方案也正确。

证明 要证明定理成立, 只需证明签名时计算出总散列值和验证时恢复的总散列值是相等即可, 其他的由签名算法的正确性来保证。根据截取算法, 有:

$$1) m_i' = \begin{cases} m_i, & i \in CI(M') \\ H_3(m_i \parallel CEAS), & i \notin CI(M') \end{cases}$$

再根据验证算法, 有:

$$2) \text{ 验证时的值} = \begin{cases} H_3(m_i \parallel CEAS), & i \in CI(M') \\ m_i', & i \notin CI(M') \end{cases}$$

由(1)和(2)可得到验证的值为 $H_3(m_i \parallel CEAS)$, 和签名时的值是一致的, 也就保证了前后总散列值相等。

定理 1 此基于身份的可截取签名方案正确。

证明 由引理 1 和引理 2 可得。

2.3 安全性分析

引理 3 在随机预言机模型下, 若此基于身份的签名在适应性选择消息攻击以及身份攻击下是存在可伪造的, 则 CDHP 困难问题在 Gap Diffie-Hellman 群 G_1 中可解。

证明 在上述方案, 签名算法是 $U = bP, V = bQ_{ID} + h(S_{ID} + rQ_{ID})$, 其中 $h = H_1(M, U)$, b 为随机数, r 和 S_{ID} 为签名密钥, 验证算法是 $e(P, V) = e(U + hP_{pub} + hrP, Q_{ID})$ 。而在文献[11]中的 $U = bP, V = bQ_{ID} + hS_{ID}$, 其中 $h = H_1(M, U)$, b 为随机数, S_{ID} 为签名密钥, 验证算法是 $e(P, V) = e(U + hP_{pub}, Q_{ID})$ 。显然只需把 $S_{ID} + rQ_{ID}$ 换成文献[11]中 S_{ID} , 其余的证明同文献[11]中定理 1。

定理 2 若所选的哈希函数 H_3, H_4 是强无碰撞和基于身份的签名方案是不可伪造的, 则此基于身份的可截取签名方案也是不可伪造的。

证明 假设定理不成立, 攻击者可以伪造有效签名, 通过询问随机预言器得到的有效签名和收集到签名者以前的签名(假设攻击者有 k 个有效签名, 记为 $\delta^i = (M_i, CEAS_i, U_i, V_i, rP)$, $(i = 1, 2, \dots, k)$)。设攻击者伪造 $\delta = (M^*, CEAS^*, U_i^*, V_i^*, rP)$ 为有效签名。由于所选的哈希函数是强无碰撞, 所以攻击者求的总散列值 \bar{M}^* 和 $\bar{M}_i (i = 1, 2, \dots, k)$ 相同的概率可以忽略, 这样, 攻击者得到了不同于 $(\bar{M}_i, U_i, V_i, rP) (i = 1, 2, \dots, k)$ 的有效签名 $(\bar{M}^*, U_i^*, V_i^*, rP)$, 这和我们要求的基于身份的签名方案不可伪造相矛盾。所以定理成立。

由于文献[4, 14]中的基于身份的可截取门限签名方案不能防止私钥管理中心 PKG 的伪造签名, 所以在本方案中我们添加了用户签名私钥 r 。对于私钥管理中心 PKG, 签名算法为 $U = bP, V = bQ_{ID} + h(sQ_{ID} + rQ_{ID}) = V = bQ_{ID} + h(s + r)Q_{ID}$, 其中 $h = H_1(M, U)$, b 为随机数, r 和 $S_{ID} = sQ_{ID}$ 为签名密钥, PKG 不可能知道 $(s + r)Q_{ID}$, 因此可以把签名密钥看成 $D_{ID} = (s + r)Q_{ID}$, 签名算法看成 $U = bP, V = bQ_{ID} + hD_{ID}$ 。根

据上面的安全性分析, 有以下推论:

推论 此基于身份的可截取门限签名方案能有效防止 PKG 的伪造签名。

2.4 效率分析

本方案和文献[4, 7]一样, 在签名过程中没有使用双线性对运算, 而文献[14]中在签名过程中使用了 4 个对运算; 在验证算法中比文献[7]少了一个对运算, 和文献[4]一样, 但是相对文献[4]只需签一次名, 不需要对每个子消息签名; 另外只需传输一个签名, 不需要传输每个子消息的消息, 节省了带宽。

3 结语

本文在文献[7]的基础上, 参照 Bi-tree 批量签名方案^[9], 结合可截取签名体制, 提出了一种新的基于身份的可截取门限签名方案, 并证明了其在随机预言机模型下能抵抗伪造, 与其他的可截取签名方案相比, 具有更高的签名效率, 在电子商务或电子政务系统中具有更高的实际应用价值。

参考文献:

- [1] STEINFELD R, BULL L, ZHENG Y. Content extraction signatures [C]// Proceedings of 4th international conference on information security and cryptology (ICISC 2001). Berlin: Springer-Verlag, 2001: 285 - 304.
- [2] BULL L, STANSKI P, MCG SQU RE D. Content extraction signatures using XML digital signatures and custom transforms on ³/demand [C]// Proceedings of the 12th international World Wide Webconference (WWW2003). New York: ACM Press, 2003: 170 - 177.
- [3] BULL L, MCG SQU RE D, ZHENG Y. A hierarchical extraction policy for content extraction signatures[J]. International Journal on Digital Libraries, 2004, 4(3): 208 - 222.
- [4] 刘军龙, 王彩芬. 基于身份的可截取的门限签名方案[J]. 计算机应用, 2006, 26(8): 1817 - 1820.
- [5] FIAT A. Batch RSA[J]. Journal of Cryptology, 1997, 10(2): 75 - 88.
- [6] HARN L. Batch verifying multiple DSA-type signatures[J]. Electronics Letters, 1998, 34(9): 870 - 871.
- [7] 刘颖, 胡子濮, 王飞, 等. 一个高效的基于身份的门限签名方案[J]. 西安电子科技大学学报: 自然科学版, 2006, 33(2): 311 - 315.
- [8] GOLDWASSER S, MICALI S, RIVEST RL. A digital signature scheme secure against adaptive chosen-message attacks[J]. SIAM Journal on Computing, 1988, 4: 281 - 308.
- [9] PAVLOVSHI C J, BOYD C. Efficient Batch Signature Generation Using Tree Structures[C]// Proceedings of Cryptec 99. Hong Kong: City University of Hong Kong Press, 1999: 70 - 77.
- [10] CHEON J H, KIM Y, YOON H J. A new ID-based signature with batch verification [EB/OL]. [2004 - 05 - 31]. <http://eprint.iacr.org/2004/131>.
- [11] GALBRAITH S D, HARRISON K, SOLDERA D. Implementing the Tate Pairings[C]// ANTS 2002: LNCS 2369. Berlin: Springer-Verlag, 2002: 324 - 337.
- [12] BONEH D, FRANKLIN M. Identity based Encryption from Weil pairing[C]// Advances in Cryptology-Crypto'01, LNCS 2139. Berlin: Springer-Verlag, 2001: 213 - 229.
- [13] SHAMIR A. Identity-based Cryptosystems and Signature Schemes [C]// Advances in Cryptology CRYPT'84: LNCS196. Berlin: Springer-Verlag, 1984: 47 - 53.
- [14] YOON H J, CHEON J H, KIM Y. Batch Verifications with ID-based Signatures [C]// ICISC 2004: LNCS 3 506. Berlin: Springer-Verlag, 2005: 233 - 248.