具有指定验证者的短签名方案

司光东[1], 辛向军[2], 陈 原[1], 肖国镇[1]
(1. 西安电子科技大学 ISN 综合业务网国家重点实验室, 陕西西安 710071;
2. 郑州轻工业学院信息与计算科学系, 河南郑州 450002)

摘 要: 基于双线性对运算, 提出了一个只能被指定验证者验证的新的短签名方案. 把消息的签名从基于 RSA 签名算法的 1024 比特下降到 170 比特左右, 降低了网络数据流量, 有效地避免了网络中常见的阻塞问题, 提高了网络使用率. 同时满足了只有签名者指定的验证人才能正确验证该签名的正确性, 可以有效防止对与签名人相关信息的泄露. 在计算性 Diffie-Hellman 问题困难假设下利用随机预言模型证明了该方案的安全性. 并且根据实际情况下的遗嘱签定, 给出了遗嘱签定协议的具体应用.

关键词: 短签名; 双线性对; 随机预言模型; 遗嘱协议
中图分类号: TN918.1 文献标识码: A 文章编号: 0372-2112 (2008) 01-0024-04

Short Signature for Specified Verifier

SI Guang-dong[1], XIN Xiang-jun[2], CHEN Yuan[1], XIAO Guo-zhen[1]
(1. *State Key Laboratory of Integrated Service Network, Xidian University, Xi'an, Shaanxi 710071, China;*
2. *Department of Information and Computing Science, Zhengzhou University of Light Industry, Zhengzhou, Henan 450002, China*)

Abstract: Based on bilinear pairings, a new short signature scheme is proposed which can only be verified by the specified verifier in this paper. The signature of messages is dropped from the 1024 bits for RSA signature algorithm to around 170 bits, which reduces the flow of data network, avoids the congestion efficiently and increases the usage of the network. The characteristic, the designated verifier only can verify the correctness of the message's signature, prevents the disclosure of the signer's any relevant information. Presumed the difficulty of Computational Diffie-Hellman Problem, the security proofs for the new signature scheme is given in the random oracle model and its application is put forward on will subscription.

Key words: short signature; bilinear pairings; random oracle model; will subscription

1 引言

Boneh, Lynn 和 Shacham 在 2001 年亚洲密码年会上提出了一个短签名方案[1]. 他们在(超)椭圆曲线上利用双线性对算法, 把对消息的签名降到 170 比特左右. 而利用 RSA 算法和 DSA 算法对消息签名时, 假设 RSA 算法中大整数模约为 1024 比特, 则 RSA 签名长度就是 1024 比特. 同样情况下, DSA 算法的签名长度约为 320 比特. 它的安全性是建立在 Gap Diffie-Hellman[2,3] 上. 由于短签名方案在现实的网络传输中将占有更大的优势, 受到了众多学者们的关注.

目前, 短签名都是利用(超)椭圆曲线来构造, 这样就会在不降低安全性的情况下缩短对消息的签名长度. 双线性对算法是利用(超)椭圆曲线进行签名的非常重要的一种算法, 此类方案[3~7] 被相继提出.

Jackobsson 等首先提出了具有指定验证者的数字签名方案[8,9], 除了签名者指定的验证者外, 任何人都无法验证该消息签名的正确性, 从而保证了该消息签名者的隐私权不被泄露.

在本文中, 我们提出了一个具有指定验证者的短签名方案. 本方案的优点是利用双线性对运算, 把消息的签名从基于 RSA 签名算法的 1024 比特下降到 170 比特左右, 降低了网络数据流量, 有效地避免了网络中常见的阻塞问题, 对提高网络使用率具有重要作用. 同时满足了只有签名者指定的验证人才能正确验证该签名的正确性, 可以有效防止对与签名人相关信息的泄露, 在现实生活中有潜在的应用前景. 在随机预言模型下, 证明了该方案的安全性. 最后, 提出了一个该方案的应用

收稿日期: 2006-10-19; 修回日期: 2007-05-28
基金项目: 国家自然科学基金(No. 60773033, No. 60603010)

实例——遗嘱签定协议.

2 基础知识

设 G_1 和 G_2 是两个阶为 q 的群, q 为一个大素数. G_1 是加法群, G_2 是一个乘法群. 两个群之间的双线性映射 $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 满足下面的属性[1]:

(1) 双线性: 对所有的 $P, Q, R \in G_1$ 有 $\hat{e}(P, Q+R) = \hat{e}(P, Q)\hat{e}(P, R)$.

和对所有的 $P, Q, R \in G_1$ 有 $\hat{e}(P+Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$.

从而, 对所有 $P, Q \in G_1$ 和所有的 $a, b \in Z$ 有 $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.

(2) 非退化: 存在 $P, Q \in G_1$ 有 $\hat{e}(P, Q) \neq 1_{G_2}$.

(3) 可计算: 对所有 $P, Q \in G_1$, 存在计算 $\hat{e}(P, Q)$ 的有效算法.

更一般地, 双线性映射是指 $\hat{e}: G_1 \times G_2 \rightarrow G_T$, 其中 G_1 和 G_2 是两个阶为 q 的群, 存在有效的同构映射 $\Psi: G_2 \rightarrow G_1$, $\Psi(g_2) = g_1$ 其中 g_1, g_2 是 G_1 和 G_2 的生成元. 上述定义就是 $G_1 = G_2$ 恒等映射这一特殊情况. (可以利用超奇异椭圆曲线上的Weil对来构造双线性映射.)

在群 G_1 上, 我们可以定义以下几个密码学问题:

离散对数(DL)问题: 给定 $P_1, P_2 \in G_1$, 找出整数 n, 使得 $P_1 = nP_2$. 在密码学上这是一个困难性问题.

计算性 Diffie-Hellman(CDH) 问题: 给定三摘组 $(P, aP, bP) \in G_1^3$, 这里 $a, b \in F_q^*$, 找出 abP. 如果离散对数问题可解, 则 CDH 问题可解. 反之, 不一定成立.

判断性 Diffie- Hellman(DDH) 问题: 给定四元组 $(P, aP, bP, cP) \in G_1^4$, 对 $a, b \in F_q^*$ 判断 $c = ab \pmod q$ 是否成立.

在双线性映射下, 判断性 Diffie- Hellman(DDH) 问题是易解的. 在目前为止, 还没有一个好的方法来解决计算性 Diffie- Hellman(CDH) 问题. 我们假定计算性 Diffie- Hellman(CDH) 问题是不可解问题.

3 具有指定验证者的短签名方案

(1) 系统建立: 系统参数由 $\{G_1, G_2, \hat{e}, h(), P, q\}$ 组成, 其中 G_1 和 G_2 是两个阶为 q 的群, q 为一个大素数. G_1 是超奇异椭圆曲线构成的加法群, P 是 G_1 的生成元. G_2 是一个乘法群. 两个群之间的双线性映射是 $\hat{e}: G_1 \times G_1 \rightarrow G_2$, $h(M) \in G_1$ 是一个把消息转化为 G_1 中元素的哈希函数.

(2) 密钥生成算法:

设签名者为 A, 验证者为 B.

A 随机选取签名密钥 $x_A \in Z_q^*$, 计算对应的公钥 $P_A = x_A P$, 验证者 B 随机选取密钥 $x_B \in Z_q^*$, 计算对应的公钥 $P_B = x_B P$, 然后分别公布 P_A, P_B 以及他们的身份信息.

(3) 签名算法:

对于任意消息 $M \in \{0, 1\}^*$, A 计算 $h(x_A P_B \| M) \in G_1$, 然后计算 $\sigma = x_A h(x_A P_B \| M)$, 输出消息 M 的签名 (σ, B).

(4) 签名的验证:

当验证者 B 接收到 M 的签名 σ 后, 作如下计算:

$S = x_B P_A$

$h = h(S \| M)$

验证 $\hat{e}(P, \sigma) \stackrel{?}{=} \hat{e}(P_A, h)$, 若成立, 接受签名.

4 安全性证明

定义 **1**(完备性)　对于指定验证者的数字签名方案, 如果签名人正确执行签名协议后输出签名 σ, 且对于指定的验证者, 以及对于任意常数 $c > 0$ 和充分大的 n, 签名 σ 通过验证的概率至少为 $1 - n^{-c}$, 则称此方案是完备的.

原方案具有完备性, 因为对于一个正确的签名, 有

$$\begin{aligned}\hat{e}(P, \sigma) &= \hat{e}(P, x_A h(x_A P_B \| M)) \\ &= \hat{e}(x_A P, h(x_A x_B P \| M)) \\ &= \hat{e}(P_A, h(x_B P_A \| M)) = \hat{e}(P_A, h)\end{aligned}$$ 成立.

定义 **2**(不可伪造性)[1]　如果一个敌手在时间 t 内, 用不超过 q_s 次签名询问和不超过 q_H 次哈希询问, 并且以大于 ε 的概率伪造一个新的可通过验证的签名, 则称这个方案是 $(t, q_s, q_H, \varepsilon)$-可伪造. 反之, 如果一个敌手在时间 t 内, 用至少 q_s 次签名询问和至少 q_H 次哈希询问下, 并且以小于 ε 的概率伪造一个新的可通过验证的签名, 则称这个方案是 $(t, q_s, q_H, \varepsilon)$-不可伪造.

定义 **3**((t', ε')-**CDH** 加群)　如果一个敌手花费至少 t' 时间, 还不能以大于 ε' 的概率来解决 CDH 问题的加法群被称为 (t', ε')-CDH 加群. 由于计算性 Diffie-Hellman(CDH) 问题的困难性, 利用椭圆曲线可以找到这样的群.

下面利用随机预言模型证明原方案在自适应选择消息攻击时, 具有存在性不可伪造性[10, 11].

定理　设 G_1 是 (t', ε')-CDH 加群, 在自适应选择消息攻击和随机预言模型下, 本文提出的方案对于存在性伪造是 $(t, q_s, q_H, \varepsilon)$-不可伪造的. 这里 $\varepsilon \geqslant \frac{e^2}{2}(q_s + 1)\varepsilon'$, e 是自然对数. $t \leqslant \frac{1}{q_s + 1}(t' - \eta(2q_s + q_H))$, η 是与算法 B 相关的一个参数.

证明: 假设攻击者 A 是 $(t, q_s, q_H, \varepsilon)$-可伪造签名的算法, 则我们可以构造 (t', ε')-CDH 算法, 可在最多花费 t' 时间内, 以大于 ε' 的概率来解决 CDH 问题. 这将与我们假定 G_1 是 (t', ε')-CDH 加群相矛盾.

设 P 是 G_1 的生成元, 对于任意的 $U, V\in G_1$, 这里 $U= aP$, $V= bP$, 通过与攻击者合作, 算法 B 的最终目的是输出 $bU= aV= abP$, 在这个过程中, 算法 B 将模拟签名者对攻击者进行回应.

以下是攻击的几个阶段:

建立参数: 算法 B 给出签名者的公钥 $P_A= U+ xP= (a+ x)P\in G_1$, $x\in_R Z_q^*$, 然后把公钥传给攻击者.

哈希询问: 在任何时候, 攻击者都可以询问随机预言模型 $h()$. 每一次询问和回答都将被加入到一个哈希链表中. 在未询问之前该链表将被清空, 然后每一次的询问都将被加入在这个链表中. 如果是对同一个消息进行询问, 算法 B 就直接从哈希链表中取出对应值进行回答, 这就保证了对同一个消息询问的一致性回答.

在本次攻击中, 我们假定攻击者是签名的接收者. 如果连签名的接收者都不能生成一个有效的签名, 即可证明本签名方案的安全性.

攻击者任取 $M_i\in\{0,1\}^*$, 要求算法 B 对之进行签名, 若指定的接收者是同一个人, 则 $S= x_BP_A$ 就是一个定值, 也就是相当于对 $(S\| M_i)$ 进行签名. 算法 B 作如下计算:

(1) 生成一个随机数 $c_i\in\{0,1\}$, 使 $\Pr(c_i= 0)= \frac{q_s}{q_s+1}$.

(2) 对消息 $M_i\in\{0,1\}^*$, 算法 B 任取 $r_i\in Z_p^*$, 令 $\omega_i= r_iP+ c_iV$, 然后把 ω_i 作为对 $M_i\in\{0,1\}^*$ 的哈希回应, 即 $h(S\| M_i)= \omega_i$.

(3) 把 $\{\omega_i, M_i, c_i\}$ 作为一个新出现的哈希回应添加在哈希链表中.

签名询问: 若攻击者要求算法 B 返回消息 M_i 的签名, 算法 B 按以下运行:

算法 B 首先生成 M_i 对应的哈希回应 ω_i, 然后从哈希链表中取出 $\{\omega_i, M_i, c_i\}$. 若 $c_i= 0$, 输出签名 $\sigma_i= r_iP_A$, 并把它发给攻击者 A.

攻击者验证 $\hat e(P,\sigma_i)= \hat e(P, r_iP_A)= \hat e(r_iP, P_A)= \hat e(\omega_i, P_A)_{c_i=0}= \hat e(h, P_A)$

若 $c_i= 1$, 则算法 B 回应"失败、放弃".

输出阶段: 我们假定攻击者可生成一个有效的且没有被询问过的签名 $(\overline M, \overline\sigma)$, 由于此签名要保证 $\hat e(P, \overline\sigma)= \hat e(h, P_A)$, 而 $\hat e(P_A, h)= \hat e((a+ x)P, \overline\omega)= \hat e(P, (a+ x)\overline\omega)$

故 $\overline\sigma= (a+ x)\overline\omega$.

这时, 算法 B 生成 $\{\overline M, \overline\omega, \overline c\}$. 若 $\overline c= 0$, 宣布放弃.

若 $\overline c= 1$, 即 $\overline\omega= \overline rP+ V$,

所以 $\overline\sigma= (a+ x)\overline rP+ (a+ x)V= \overline rP_A+ aV+ xV= (\overline rP_A+ xV)+ aV$

由于 $\overline r$, x, V 都是由算法 B 所选, 从而可计算出 $abP= aV= \overline\sigma- (\overline rP_A+ xV)$, 即解决了椭圆曲线上计算性 Diffie-Hellman 问题. 由于假定了计算性 Diffie-Hellman 问题是困难的, 从而证明了以上结论.

下面计算它们成功的概率:

要使攻击成功, 需要满足三个条件

(1) 算法 B 进行 q_s 次签名, 并且验证通过, 概率为 $\left(\frac{q_s-1}{q_s+1}\right)^{q_s}$

(2) 攻击者以 ε 的概率生成一个有效的且没有被询问过的签名 $(\overline M, \overline\sigma)$.

(3) 保证生成的签名中 $\overline\omega= \overline rP+ V$, 它的概率 $\Pr(\overline c= 1)= \frac{2}{q_s+1}$

由于 $\left(1+\frac{1}{q_s}\right)^{q_s}\to e, (q_s\gg 0)$

从而
$$\varepsilon'\leqslant\varepsilon\left(\frac{q_s-1}{q_s+1}\right)^{q_s}\left(\frac{2}{q_s+1}\right)$$
$$\varepsilon\geqslant\frac{1}{2}\left(1+\frac{2}{q_s-1}\right)^{q_s}(q_s+1)\varepsilon'$$
$$\varepsilon\geqslant\frac{e^2}{2}(q_s+1)\varepsilon'$$

成功计算出计算性 Diffie-Hellman 问题需要的时间为, 每次攻击者可生成一个有效的且没有被询问过的签名 $(\overline M, \overline\sigma)$, 直到 $\overline c= 1$, 即 $\overline\omega= \overline rP+ V$ 为止, 约为 $t(q_s+ 1)$. 再加上 $(q_s+ q_H)$ 次哈希提问和 q_s 次签名回应. 故
$$t'\geqslant(q_s+ 1)t+\eta(2q_s+ q_H)$$
$$(q_s+ 1)t\leqslant t'-\eta(2q_s+ q_H)$$
$$t\leqslant\frac{1}{q_s+1}(t'-\eta(2q_s+ q_H))$$

说明: 本方案的证明采用了选择消息攻击模型[11], 和文献[1]中证明类似, 但我们是归约在 CDH 之上, 并且概率和运行时间不同.

5 本签名方案的应用

根据本文提出的方案, 我们给出了一个遗嘱签定协议. 参加人有立遗嘱人、公证机关、代理律师组成. 共分成以下几个步骤:

(1) 立遗嘱人向公证机关出具遗嘱协议正文和财产合法性证明, 证明这些财产是自己合法所得, 并对上述材料进行签名和加密.

(2) 公证机关验证上述材料的合法性, 然后对此遗嘱协议进行公证, 并对公证材料备份. 然后把公证材料发送给立遗嘱人.

(3) 立遗嘱人验证公证材料的合法性后, 把材料交给自己的代理律师保存.

(4) 若立遗嘱人想修改遗嘱协议的某些条款, 可以

再按(1)~(3)的次序对这些内容的具体事项进行说明.

(5)当立遗嘱人去世后, 遗嘱协议生效. 由律师和公证机关公示遗嘱内容. 继承人可以根据立遗嘱人的公钥验证遗嘱内容的合法性.

设 G_1 阶为 q 的群, P 是 G_1 的生成元. 立遗嘱人为 A, 对应的签名密钥和公钥对为 (x_A, y_A). 公证人员为 B, 对应的签名密钥和公钥对为 (x_B, y_B). 代理律师为 C, 对应的签名密钥和公钥对为 (x_C, y_C).

立遗嘱人 A 生成并通过某一秘密信道发送 $\{x_A h(M \| T), M \| T\}$ 给公证人 B. 其中 M 表示遗嘱协议, T 表示自己财产的合法性证明, "‖"表示二进制比特串的级联, $h(\,)$ 是上文所述的哈希函数.

当 B 收到后, 验证 $\hat{e}(P, x_A h(M \| T)) = \hat{e}(P_A, h(M \| T))$ 是否成立.

若成立, B 对协议签名, 生成 $x_B x_A h(M \| T)$ 发送给 A.

A 验证 $\hat{e}(P, x_B x_A h(M \| T)) = \hat{e}(P_B, x_A h(M \| T))$ 成立.

设 $E_s(\,)$ 是以 s 为密钥的对称加密算法, 立遗嘱人 A 生成:

$$Q_1 = x_A h(M \| T)$$
$$Q_2 = x_B x_A h(M \| T)$$
$$Q = E_{x_A P_C}(Q_1 \| Q_2 \| (M \| T))$$

把 $\{x_A h(x_A P_C \| Q), Q\}$ 发给 C.

6 结束语

短签名方案具有高效和储存空间小的特点, 将会在数字签名中占有十分重要的地位. 本文中, 基于双线性对运算, 我们提出了一个具有指定验证者的短签名方案, 把消息的签名从基于 RSA 签名算法的 1024 比特下降到 170 比特左右, 降低了网络数据流量, 有效地避免了网络中常见的阻塞问题, 对提高网络使用率具有重要作用. 同时满足了只有签名者指定的验证人才能正确验证该签名的正确性, 可以有效防止对与签名人相关信息的泄露. 并且在随机预言模型中证明了它的安全性. 最后, 根据双线性对和短签名方案, 给出了一个遗嘱签定协议.

参考文献:

[1] D Boneh, B Lynn, H Shacham. Short signatures from the weil pairing[A]. C Boyd(Ed.). In Asiacrypt' 01[C]. Gold Coast, Australia: Springer Verlag, 2001. 514- 532.

[2] D Boneh, X Boyen. Short signatures without random oracles [A]. Christian Cachin, Jan Camenisch (Eds.). In Eurocrypt' 04[C]. Interlaken, Switzerland: Springer Verlag, 2004. 56- 73.

[3] S Mitsunari, R Sakai, M Kasahara. A new trator tracing[J]. IEICE Trans. Fundamentals, 2002, E85A(2): 481- 484.

[4] K G Paterson. ID-based signatures from pairings on elliptic curves[J]. Electron Lett, 2002, 38(18): 1025- 1026.

[5] N P Smart. An identity based authenticated key agreement protocol based on the Weil pairing[J]. Electron Lett, 2002, 38(13): 630- 632.

[6] X Huang, Y Mu, W Susilo, F Zhang. Short designated verifier proxy signature from pairings[A]. The First International Workshop on Security in Ubiquitous Computing Systems[C]. Berlin: Springer-Verlag, LNCS 3823, 2005. 835- 844.

[7] 顾纯祥, 张亚娟, 祝跃飞. 混合可验证加密签名体制及应用[J]. 电子学报, 2006, 34(5): 878- 882.
GU Chun-xiang, ZHANG Ya-juan, ZHU Yue-fei. A mixed verifiably encrypted signature scheme and it's Applications[J]. Acta Electronica Sinica, 2006, 34(5): 878- 882. (in Chinese)

[8] R Steinfeld, L Bull, H Wang, J Pieprzyk. Universal designated-verifier signatures[A]. Chi Sung Laih (Eds.). In Asiacrypt' 03[C]. Taipei, Taiwan: Springer-Verlag, LNCS 2894, 2003. 523- 542.

[9] R Steinfeld, H Wang, J Pieprzyk. Efficient extension of standard schnorr/RSA signatures into universal designated-verifier signatures[A]. Feng Bao, Robert Deng, Jianying Zhou (Eds.). In PKC' 04[C]. Singapore: Springer-Verlag, 2004. 86- 100.

[10] M Bellare, P Rogaway. Random oracles are practical: A paradigm for designing efficient protocols[A]. In ACM Conference on Computer and Communication Security[C]. Virginia, USA: ACM Press, 1993. 62- 73.

[11] S Goldwasser, S Micali, R L Rivest. A digital signature scheme secure against adaptive chosen-message attacks[J]. SIAM J Comput, 1988, 17(2): 281- 308.

作者简介:

司光东　男, 1975 年 9 月出生于陕西省榆林市, 2005 年 9 月至今在西安电子科技大学通信工程学院攻读密码学博士学位. 研究方向为: 信息安全与网络安全.
E-mail: siguangdong@126.com

辛向军　男, 1974 年出生于河南淇县, 郑州轻工业学院讲师, 博士, 主要研究方向为密码学与信息安全.
E-mail: xin_xiang_jun@tom.com

陈　原　女, 1978 年出生于新疆阿克兹, 博士. 主要研究方向为信息安全与密码学.

肖国镇　男, 1934 年 9 月生于吉林四平, 西安电子科技大学教授、博士生导师, 西安电子科技大学信息安全与保密研究所所长, 亚洲密码学会执行委员会委员.