

基于二元仿射变换的广义 ELGamal 型盲签名方案

姚亦峰, 朱华飞, 陈抗生

(浙江大学信息与电子工程系, 杭州 310027)

摘 要: 利用广义 ELGamal 型签名方案或 DSS 构造盲签名(指强盲签名)方案, 是人们普遍关注但仍未解决的问题. 本文提出了利用二元仿射变换, 由 Ham 和 Xu 提出的十八种安全广义 ELGamal 型数字签名方案出发构造其盲签名方案的方法. 利用该方法得到十八种相应的盲签名方案. 进一步分析得到其中十二种方案是强盲签名方案, 而其余在该方法下只能得到弱盲签名方案.

关键词: 数字签名; 盲签名; 离散对数

中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2000) 07-0128-02

Generalized ELGamal Type Blind Signature Schemes Based on Affine Transform

YAO Yifeng, ZHU Huafei, CHEN Kangshen

(Dept of Information & Electronic Engineering, Zhejiang University, Hangzhou 310027, China)

Abstract: In this paper, a method constructing generalized ELGamal type blind signature schemes utilizing affine transform with two variables is developed. We show that among the 18 secure generalized ELGamal type schemes presented in [3] only twelve of them can be converted into strong blind signature schemes while the rest are weak ones.

Key words: digital signature; blind digital signature; discrete logarithm

1 引言

数字签名是一种实用的认证技术. 两个最重要的数字签名方案之一是由 ELGamal 提出的. Harn 和 Xu 提出了广义 ELGamal 型签名方案^[3], 并指出安全的 ELGamal 型签名方案共有 18 个. 为了缩短签名长度和提高签名方案的运行速度, 可以利用数字签名标准(DSS)中的技术对广义 ELGamal 型签名方案进行修改^[3].

盲签名的概念最早由 Chaum^[1]引进. 盲签名能完成这样的功能: 消息发送者 Bob 希望发送的消息能由签名者 Alice 进行签名并且其他用户可以验证该消息是由签名者签名的, 但发送者不希望签名者知道消息的真实内容.

假设 u, v 是定义在两个不同概率空间上的随机变量, 其概率分布分别为 $Pro(u)$, $Pro(v)$, 联合分布为 $Pro(u, v)$, 如果在多项式时间内无法区分概率分布 $Pro(u, v)$ 与 $Pro(u) * Pro(v)$, 则称 u, v 是不可联系的^[4]. 在签名方案中设 Alice 观察到的信息为 Σ 而 Bob 得到的消息-签名对为 $(m, sig(m))$, 如果两者是不可联系的, 则称该签名方案是盲签名方案.

若签名者存储盲消息及其签名 $(\tilde{m}, sig(\tilde{m}))$ 或其他有关数据, 待 $(m, sig(m))$ 公开后签名者可以找出它们之间的内在联系, 从而可以追踪消息 m , 则称为弱盲签名方案; 若签名者无法把这两者联系起来, 则称为强盲签名方案. 强盲签名可用于电子货币、电子投票等密码协议的设计. 目前存在的强盲签

名方案有盲 RSA 签名方案和盲 Schnorr 方案. 利用广义 ELGamal 型签名或 DSS 构造强盲签名方案是人们普遍关注但仍未解决的问题. 本文提出了利用二元仿射变换由 Harn 和 Xu 指出的十八种安全广义 ELGamal 型签名方案出发构造其盲签名方案的方法. 利用该方法得到十八种相应的盲签名方案. 进一步分析得到其中的十二个方案是强盲签名方案, 而其余的只能得到弱盲签名方案.

2 基于二元仿射变换的盲签名方案

下面考虑从广义 ELGamal 型签名方案构造相应盲签名方案的一般方法. 考虑到协议的运行速度, 从修改的广义 ELGamal 型签名方案出发. 设 Bob 希望 Alice 对消息 m 进行签名, 但不希望 Alice 看到消息 m . 因此 Bob 首先把消息盲化为 \tilde{m} , 让 Alice 对 \tilde{m} 进行签名, 签名方程为 $\tilde{r} = g^{\tilde{k}} \bmod p$ 和 $\tilde{\alpha}x = \tilde{b}\tilde{k} + \tilde{c} \bmod q$. 这里, $(\tilde{a}, \tilde{b}, \tilde{c})$ 是 $(\tilde{m}, \tilde{r}, \tilde{s})$ 的置换或数学组合. Bob 得到消息-签名对 $(\tilde{m}, (\tilde{r}, \tilde{s}))$ 后, 由 $(\tilde{m}, (\tilde{r}, \tilde{s}))$ 得到 $(m, (r, s))$ 使其满足签名方程 $r = g^k \bmod p$ 和 $\alpha x = bk + c \bmod q$. 即使得 $(m, (r, s))$ 是有效的消息-签名对. 不妨假设 $m = M(\tilde{m})$, $r = R(\tilde{r})$, $k = K(\tilde{k})$ 和 $s = S(\tilde{s})$. 由签名方程 $r = g^k \bmod p = g^{K(\tilde{k})} \bmod p = R(\tilde{r})$ 可知 $R(\tilde{r})$ 为 $K(\tilde{k})$ 所确定, 又有 s 为 m, k 所确定, 所以 $S(\tilde{s})$ 为 $M(\tilde{m})$ 和 $K(\tilde{k})$ 所确定. 因此只需考虑 $M(\tilde{m})$ 和 $K(\tilde{k})$.

在签名方程中 $\tilde{r} = g^{\tilde{k}} \bmod p$, $r = g^k \bmod p$, \tilde{k} 和 k 是 Alice 的秘密参数. 为了方便起见从 $K(\tilde{k})$ 的分析开始. $r = g^k \bmod p = g^{K(\tilde{k})} \bmod p$, 因此为了盲化 r , $K(\tilde{k})$ 只能是 \tilde{k} , x 的仿射函数. 不失一般性令 $K(\tilde{k}) = \alpha\tilde{k} + \tau_x + \beta \bmod q$, $\alpha, \beta, \tau \in \mathbb{Z}_q^*$, 是 Bob 随机选择的盲化参数, 那么 $R(\tilde{r}) = \tilde{r}^{\alpha} y^{\tau} g^{\beta} \bmod p$. 这里 $y = g^x \bmod p$ 是 Alice 的公钥, 因此 Bob 在不知 \tilde{k} 的情形下仍可以计算 r . 若 Bob 再确定 $M(\tilde{m})$, 那么 $S(\tilde{s})$ 也就唯一确定了. 不妨设 $\tilde{m} = f(m)$ 和 $s = S(\tilde{s})$, 根据盲签名方案的要求不难得到:

$f(m)$ 应满足以下要求: (1) $f(m)$ 不应该含有 x , 因为 x 是 Alice 的签名密钥; (2) $f(m)$ 应该含有随机参数 α, β, τ, r (至少有一个) 以实现对消息 m 的盲化; (3) $f(m)$ 不应该含有 \tilde{k} 和 k , 因为 \tilde{k} 和 k 是 Alice 的秘密参数; (4) $f(m)$ 不应该含有 s 和 \tilde{s} , 这一点由签名方案的安全性要求得到; (5) $f(m)$ 的计算是容易的; (6) $f(m)$ 可以含有 \tilde{r} 或 y .

$S(\tilde{s})$ 应满足以下要求: (7) $S(\tilde{s})$ 不应该含有 x , 因为 x 是 Alice 的签名密钥; (8) $S(\tilde{s})$ 应该含有随机参数 α, β, τ, r (至少有一个), 以实现对 \tilde{s} 的盲化; (9) $S(\tilde{s})$ 不应该含有 \tilde{k} 和 k , 因为 \tilde{k} 和 k 是 Alice 的秘密参数; (10) $S(\tilde{s})$ 的计算是容易的; (11) $S(\tilde{s})$ 可以含有 \tilde{r}, \tilde{m} 或 y .

假设对于一个签名方案存在上述的 $R(\tilde{r}), S(\tilde{s}), M(\tilde{m})$ 和 $K(\tilde{k})$, 由此可以得到下述的交互式盲签名方案:

(1) Alice 随机选择 $\tilde{k} \in \mathbb{Z}_q^*$, 计算 $\tilde{r} = g^{\tilde{k}} \bmod p$ 且发送 \tilde{r} 给 Bob. (2) Bob 随机选择 $\alpha, \beta, \tau \in \mathbb{Z}_q^*$, 计算 $r = R(\tilde{r}), \tilde{m} = f(m)$, 且发送 \tilde{m} 给 Alice; (3) Alice 对消息 \tilde{m} 签名, 即计算 \tilde{s} , 满足 $\alpha\tilde{s} = \tilde{b}\tilde{k} + \tilde{c} \bmod q$, 发送 \tilde{s} 给 Bob; (4) Bob 验证 $y^{\tilde{a}} = r^{\tilde{b}} g^{\tilde{c}} \bmod p$, 若方程不满足则 Bob 拒绝 Alice 的签名, 否则计算 $s = S(\tilde{s})$, 并将 (r, s) 作为 Alice 对消息 m 的签名.

对 Harn 和 Xu 指出的 18 个安全广义 ELGamal 型签名方案, 利用上述方法进行盲化得到相应的盲签名方案. 下面给出了一个具体的例子.

例 1 对修改的 Optimal Scheme(方案 7) 按上述方法盲化得到的一个强盲签名方案, 在变换时取 $k = K(\tilde{k}) = \alpha\tilde{k} + \tau_x + \beta \bmod q$, $\alpha, \beta, \tau \in \mathbb{Z}_q^*$:

(1) Alice 随机选择 $\tilde{k} \in \mathbb{Z}_q^*$, 满足 $\tilde{r} = g^{\tilde{k}} \bmod p$, $(\tilde{r}, q) = 1$, $\tilde{r}_q = \tilde{r} \bmod q$ 且发送 \tilde{r} 给 Bob; (2) Bob 随机选择 $\alpha, \beta, \tau \in \mathbb{Z}_q^*$, 计算 $r = (\tilde{r})^{\alpha} y^{\tau} g^{\beta} \bmod p$ $\bmod q$, $r_q = r \bmod q$, $\tilde{m} = \alpha^{-1} \tilde{r}^{-1} (rm - \tau) \bmod q$ 且发送 \tilde{m} 给 Alice; (3) Alice 对消息 \tilde{m} 签名, 即计算 \tilde{s} , 满足 $\tilde{r}_q \tilde{s} = \tilde{k} + \tilde{s} \bmod q$, 发送 \tilde{s} 给 Bob; (4) Bob 计算 $s = \alpha\tilde{s} - \beta \bmod q$, 并将 (r_q, s) 作为 Alice 对消息 m 的签名.

定理 1 (r_q, s) 是 Alice 对消息 m 的有效签名, 而且上述方案是一个强盲签名方案.

证明 根据协议的运行过程可以得到:

$$rmx = k + s \bmod q$$

$$\Leftrightarrow rmx = \tilde{k}\alpha + \tau_x + \beta + s \bmod q$$

$$\Leftrightarrow (rm - \tau)x = \tilde{k}\alpha + s + \beta \bmod q$$

$$\Leftrightarrow \alpha^{-1}(\tilde{r}m - \tau)x = \tilde{k} + \alpha^{-1}(s + \beta) \bmod q$$

$$\Leftrightarrow \alpha^{-1} \tilde{r}^{-1} (rm - \tau)rx = \tilde{k} + \alpha^{-1}(s + \beta) \bmod q$$

$$\Leftrightarrow \tilde{r}mx = \tilde{k} + \tilde{s} \bmod q$$

所以 (r_q, s) 是 Alice 对消息 m 的有效签名.

在该方案中 Alice 观察到的信息为 $\Sigma = (\tilde{k}, \tilde{m}, \tilde{r}_q, \tilde{s})$, Bob 得到的消息-签名对为 (m, r_q, s) , α, β, τ 为随机盲化参数. 类似 Harn^[4] 的分析: 若 Alice 在签名时存贮 $\Sigma = (\tilde{k}, \tilde{m}, \tilde{r}_q, \tilde{s})$, 待 Bob 公开 (m, r_q, s) 后, Alice 可以根据 $s = \alpha\tilde{s} - \beta \bmod q$, $\tilde{m} = \alpha^{-1} \tilde{r}^{-1} (rm - \tau) \bmod q$, $r = ((\tilde{r})^{\alpha} y^{\tau} g^{\beta} \bmod p) \bmod q$ 求解 α, β, τ , 从而 Alice 可以找出 $(\tilde{m}, \tilde{r}_q, \tilde{s})$ 和 (m, r_q, s) 的联系. 但从这三个方程不难知道 Alice 解出 α, β, τ 必须计算离散对数. 因此在难于计算离散对数的前提之下, 该方案是一个强盲签名方案.

3 盲签名方案的进一步分析

Harn 和 Xu 指出的 18 个安全广义 ELGamal 型签名方案中, 2、4、10、11、16、17 这六个方案, 按本文提出的方法进行盲化时只能使用一个随机参数, 即仿射变换只能取 $k = K(\tilde{k}) = \alpha\tilde{k} \bmod q$. 若已知 $(\tilde{m}, \tilde{r}_q, \tilde{s})$ 和 (m, r_q, s) , 可以根据 $m = M(\tilde{m})$, $r = R(\tilde{r})$ 和 $s = S(\tilde{s})$ 求解其中的随机参数 (在这三个方程中有两个线性方程). 故若 Alice 存贮 $\Sigma = (\tilde{k}, \tilde{m}, \tilde{r}_q, \tilde{s})$, 待 Bob 公开 (m, r_q, s) 后 Alice 可以找出 $(\tilde{m}, \tilde{r}_q, \tilde{s})$ 和 (m, r_q, s) 的联系. 因此这 6 个方案按本文提出的方法盲化得到的是弱盲签名方案. 而其他 12 个方案在盲化时可以使用三个随机参数, 即仿射变换可以取 $k = K(\tilde{k}) = \alpha\tilde{k} + \tau_x + \beta \bmod q$, 类似定理 1 可以证明这些方案是强盲签名方案. 若在盲化这些方案时使用的随机参数少于三个, 则相应的盲签名方案也为弱盲签名方案.

4 结束语

本文提出了利用二元仿射变换对广义 ELGamal 型签名方案进行盲化, 得到了 18 个广义 ELGamal 型签名方案的相应盲签名方案. 由 Camenisch^[7] 等人提出的弱盲签名方案是本文提出的方法得到的特例. 经分析指出了其中的六个盲签名方案为弱盲签名方案. 对于这些方案是否存在其他的盲化方法使其成为强盲签名方案有待进一步研究; 其他的 12 个方案在盲化时可引入三个随机参数, 从而盲化为强盲签名方案. 如果在盲化时减少随机参数将使得到的方案为弱盲签名方案, 对于这些方案的安全性也有待进一步研究.



姚亦峰 1971 年出生, 1997 年于华中理工大学获理学硕士学位, 现为浙江大学信息与电子工程系博士生, 研究方向计算机密码学, 电子商务.

朱华飞 浙江大学信息与电子工程系副教授, 主要研究方向计算机密码学, 电子商务等.

(下转第 134 页)

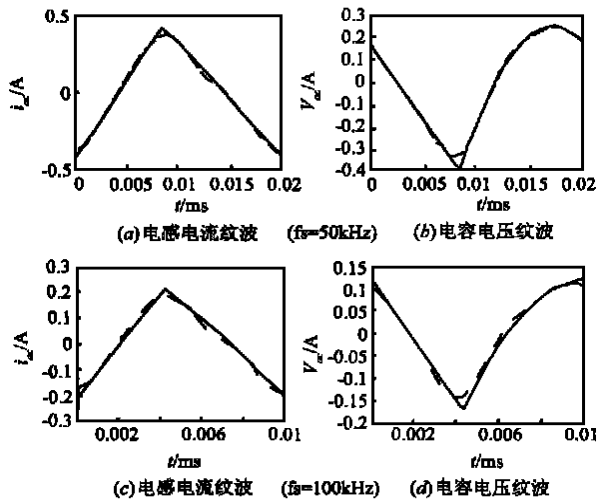


图4 例2状态变量稳态一周期内纹波比较图

之优点。所得结果都是符号表达式,易于掌握电路的工作机理,容易求得输出纹波,因而在工程设计及计算机符号分析中具有明显的应用价值。文中的方法原理及其所提供的两个实例证实:1)纹波对实用PWM开关功率变换器闭环系统(f_s 较高)的占空比的影响是相当小的;2)系统中存在的直流偏移可通过在反馈电路中加适当的积分补偿得到抑制;3)上文表2、表3中数据对比可说明本文算法用于分析反馈电路有补偿的系统时具有更高的准确性(实际应用电路一般属于这种情况)。

参考文献

- [1] R. D. Middlebrook and S. Cuk, A general unified approach to modelling switching converters power stages, IEEE PESC Rec. 1976: 18~ 34
- [2] P. T. Krein et al. On the use of average for the analysis of power electronics systems, IEEE Trans. on PE 5(2), 1990: 182~ 190
- [3] Seth R. Sanders et al. Generalized averaging method for power conversion circuits, IEEE Trans. on PE 6(2), 1991: 251~ 258

- [4] B. Lehman et al. Switching frequency dependent averaged models for PWM DG/DC converters, IEEE Trans. on PE 11(1), 1996: 89~ 98
- [5] Qiu. S. S., Filanovsky I. M. Calculation of steady state oscillations in nonlinear circuits, Int. J. Electronics, 1989, 67(3): 403~ 414
- [6] 丘水生. 非线性网络与系统. 成都, 电子科技大学出版社, 1990
- [7] 丘水生. 分析开关功率变换器的一种新方法. 华南理工大学学报, 1994, 22(3): 74~ 81
- [8] 林波涛, 丘水生. PWM 开关变换器的符号分析. 电子学报, 24(8), 1996: 83~ 87
- [9] 陈文, 丘水生. E 类放大器的符号分析法. 华南理工大学学报, 1997, 25(8): 88~ 92
- [10] 丘水生. 开关功率变换器符号分析方法的原理. 电子学报, 25(1), 1997: 5~ 10
- [11] Chen W, Qiu S. S. SAPNE: A symbolic analysis program for nonlinear differential equations, Proc. ICNNSP' 93, Guangzhou, 1993
- [12] Wamhaq P, et al. Symbolic network analysis method for practical analog integrated circuits: A survey, IEEE Trans. Circuits Syst. - II, 1998, 45(10): 1331~ 1341



陈艳峰 1995 年在武汉水利电力大学获电力电子技术专业硕士学位。现为华南理工大学电子与通信工程系 97 级博士生, 主要研究方向为非线性电路与功率电子学。



丘水生 教授, 博士生导师, 1966 年在华南理工大学非线性振荡理论专业研究生毕业。1984~ 1986 年为加拿大阿尔伯特大学访问学者。1990~ 1991 年先后任美国波特兰州立大学、加拿大阿尔伯特大学访问教授。现在华南理工大学电子与信息学院从事非线性电路与系统、功率电子学和混沌理论的教学、科研工作。

(上接第 129 页)

参考文献

- [1] D. Chaum. Blind signature systems, advances in cryptology, Crypto' 83, Plenum: 153
- [2] K. Nyberg, R. A. Ruepple. Message recovery for signature schemes based on discrete logarithm problem. Pre.-Proc. of Eurocrypt' 94, May, 1994: 175~ 190
- [3] L. Harn, Y. Xu, Design of generalized ElGamal type digital signature schemes based on discrete logarithm. Electron. Lett., 1993, 29(12):

1120~ 1121

- [4] L. Harn. Cryptanalysis of blind signature based on the discrete logarithm problem. Electron. Lett., 1995, 31(14): 1136
- [5] S. Goldwasser, S. Micali. Probabilistic encryption. Journal of Computer and System Science, 1984, 28(2): 270~ 299
- [6] S. Goldwasser, S. Micali, C. Rackoff. The knowledge complexity of interactive proof system Proc. 17th. ACM Symposium on the Theory of Computing (STOC), 1985: 291~ 304
- [7] J. Cramenisch, et al. Blind signature based on the discrete logarithm problem. Rump Session of Eurocrypt' 94, 1994