

一种基于有限域上的多项式分解定理的群签名方案

张 兴 兰

(北京工业大学 计算机学院, 北京 100124)

摘 要: 基于有限域上的多项式分解定理, 给出一种新的群成员撤销方案. 新方案的特点是: 不需要群管理员和成员的交互; 在成员增加和撤销过程中不改变成员的密钥; 签名算法等同于一个普通签名, 验证算法与撤销成员的个数无关. 并分析了提出方案的安全性和性能.

关键词: 因子分解定理; 群签名; 成员撤销

中图分类号: TN918

文献标识码: A

文章编号: 1000-7180(2010)03-0163-03

An Efficient Group Signature Scheme Based on Factorial Decompose Theorem of Polynomial with Factors in Finite Field

ZHANG Xing-lan

(College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China)

Abstract: Based the factorial decompose theorem of polynomial with factors in a finite field, a new group signature schemes is proposed. The solution is efficient in that it needs no communication between group manager and member, and the member's key is not need to change when the group manager adds or excludes the group members. The signing is same as a normal signature, and the computational cost of verifying is independent of the number of the revoked members. At last, the security is analyzed under factorial decompose theorem of polynomial and discrete logarithm problem assumption.

Key words: factorial decompose theorem; group signature; member revocation

1 引言

近年来, 人们也试图从其他侧面去研究群签名方案. 文献[1]提出了一种基于中国剩余定理的高效的群签名方案. 该方案简化了群签名算法的计算复杂性, 且保证了撤销成员的有效性. 尽管后来被证明其安全性存在问题^[2,3], 但它却给出了解决群签名方案的一种新途径. 此外, 对群签名的再电子商务等领域的应用也被广泛的研究^[4].

目前, 一些安全实用的群签名方案^[2,5]并不令人满意. 文中基于有限域上多项式分解定理提出了一种高效的成员撤销算法, 并基于新的成员标识进行签名使之满足群签名方案的需求, 不仅克服了目前一些基

于群签名撤销算法与群成员线性相关的缺点, 而且极大地降低了群签名的计算复杂度和通信代价. 与文献[1]以及其改进文献[3]相比, 文中的方案不仅减轻了群管理员的计算负担和保密任务, 而且取消了群管理员与成员之间的安全交互过程.

2 基于有限域上多项式分解定理的群签名方案

有限域上多项式分解定理: 有限域 F_q 上的一元多项式环是唯一因子分解整环.

(1) 系统的建立

群管理者选择满足离散对数假设的素数 p, q , 其中 $2^{L-1} < p < 2^L, 512 \leq L \leq 1024. q \mid p-1$, 且 2^{159}

收稿日期: 2009-02-03; 修回日期: 2009-05-22

基金项目: 国家“八六三”计划项目(2006AA01Z440); 国家“九七三”计划项目(2007CB311100); 北京市科技计划项目(207000100720706)

$< q < 2^{160}$. 生成元 $g \equiv h^{(p-1)/q} \pmod p, 1 < h < p-1$, 且 $g \not\equiv 1 \pmod p$. 成员 P_i 选择的 ELGamal 的公私钥为 (y_i, x_i) , 且 $y_i = g^{x_i} \pmod p$. 成员拥有各自的公私钥, 并且所有公钥公布于公开的目录. 为了描述简便, 约定在模 p 乘法运算在群 $\langle g \rangle$ 中进行, H 为一个理想的单向函数.

(2) 群公钥的生成

群管理者随机选择一个参数 $t \in Z_q^*, K \in Z_q$, 不可约多项式 $g(x) \in F_q(x)$ 和一个成员的代理子集 $\{P_1, P_2, \dots, P_n\}$, 计算 $\alpha = g^t \pmod p, f(x) = K + [\prod_{i=1}^n g(x)(x - y_i \pmod p)] \pmod q$. 同时, 群管理员通过扩展的 GCD 算法计算出 a, b 使得 $at + bq = 1$, 于是 $at \equiv 1 \pmod q$. 群管理者广播群公钥 $(\alpha, f(x), K)$, 保密恢复密钥 a .

(3) 成员证书的产生

成员 P_i 计算 $\alpha_i = \alpha^{x_i} \pmod p$, 验证 $f(\alpha_i) \pmod q = K$. 如果成立, P_i 就接受 α_i 为签名的群证书.

(4) 签名

P_i 计算 $r = \alpha^k \pmod p, s = k^{-1}(x_i - rh(m))$, 消息 m 群签名为 (m, r, s) .

(5) 验证

计算 $\alpha'_i = r^s \alpha^{H(m)} \pmod p$, 验证 $f(\alpha'_i) \pmod q = K$ 是否成立, 成立群签名有效, 否则, 群签名无效.

(6) 打开

对于有效的群签名, 群管理员通过计算 $\alpha'_i = r^s \alpha^{H(m)} \pmod p, y'_i = (\alpha'_i)^a \pmod p$ 最终确定成员身份.

(7) 新成员的加入

成员 $U_m, m > n$ 加入, 群管理者将 $f(x)$ 更新为 $K + [(f(x) - K)(x - y'_m \pmod p)] \pmod q$.

(8) 成员删除

删除成员 U_k , 群管理者将 $f(x)$ 更新为 $K + [(f(x) - K)/(x - y'_k \pmod p)] \pmod q$.

从上面的过程可以看到: 成员加入过程中并不需要传递秘密信息, 从而在群管理员和成员之间不需要安全信道; 在成员加入和撤销过程中, 合法成员不需要更新自己的密钥; 签名算法和验证算法与群成员个数和被撤销成员个数无关.

然而, 随着群组成员个数的增加, 证据多项式的次数将随之增加. 但相比安全参数而言, 群组成员个数远远小于安全参数的长度. 此外, 现有的具有删除功能的群签名方案都与群成员或被删除成员的个数

相关, 而与群成员个数相关要比与被删除成员个数相关的有效性高, 这是因为对于固定的群组织而言, 一般成员个数的变化不大, 而被删除成员的个数可能都难于计数. 如对于一个学校而言, 在校人数一般变化不大, 而离校人数将逐年增加.

3 安全性分析

在 BSZ 模型^[2]中, 将理想的动态群签名方案应满足的安全特性归纳为 4 点: (1) 正确性: 群成员所生成的签名验证有效, 打开算法能正确地揭示签名者的身份并且给出可接受的证明; (2) 匿名性: 对于一个指定消息的签名, 敌手不能判定是由他所选择的两个成员中哪一个成员所签署; (3) 可跟踪性: 敌手不能够生成一个 GM 不能揭示其身份的签名, 或者 GM 可以揭示其身份但是不能给出一个可接受的证明; (4) 抗陷害性: 如果一个成员没有生成某个签名, 敌手不能给出一个证明来认定该成员生成了此签名. 基于 BSZ 模型, 下面分析文中给出的群签名方案的安全性.

定理 1 如果合法成员忠实执行协议, 则方案满足正确性.

证明: 由 $\alpha = g^t \pmod p$, 则 $\alpha^{x_i} \equiv y_i \pmod p$. 因此, 群管理员认定的有效成员的群签名一定可以通过验证. 而且, 由 $at \pmod q = 1$, 群管理员利用打开算法密钥 a 计算 $(\alpha_i)^a \equiv (y_i)^a \equiv y_i^a \pmod p = y_i$. 因此, 方案的正确性成立.

定理 2 对于一个检验有效的签名, 打开算法一定可以揭示其签名者的身份, 即方案满足可跟踪性.

证明: 不失一般性, 假设敌手不能伪造 GM 发布的群签名公钥, 从而不能在组内添加无效的成员. 对于一个有效的签名 (m, r, s) , 对于 $\alpha'_i = r^s \alpha^{H(m)} \pmod p$, 有 $f(\alpha'_i) \pmod q = K$ 成立. 由有限域上多项式分解唯一性定理, α'_i 是唯一确定的. 又因为 $\alpha^{x_i} \equiv y_i \pmod p$, 由 $at \equiv 1 \pmod q$, 有 $(\alpha_i)^a \equiv (y_i)^a \equiv y_i^a \pmod p = y_i$ 成立, 所以任何揭示成员身份的证明是可以接受的.

定理 3 在离散对数假设下, 方案满足抗陷害性.

该定理由以下 3 个引理可得.

引理 1 在离散对数假设下, 签名的交互协议是关于成员私钥 x_i 的统计零知识证明.

证明: 构造模拟器 S : 随机选择 $\bar{k}, x \in Z_q^*$, 计算 $\bar{r} = g^{\bar{k}} \pmod p$, 调整 $H(m)$ 的值使关于 $\bar{s}$ 的方程 $\bar{k}\bar{s} = x - \bar{r}H(m)$ 有整数解 $\bar{s}$. 在离散对数问题假设下, 从观

察者的角度, $(\bar{r}, \bar{s})$ 与实际签名 (m, r, s) 中的 (r, s) 是统计不可区分的。

引理 2 从有限多个签名不能构造出一个新的签名。

证明:不失一般性,假设成员私钥是保密的。下面证明:如果敌手 A 可以构造出一个新的签名,则可以构造算法 B 破解离散对数问题。

设敌手可以访问签名 Oracle, 得到 q_s 个有效签名,但不可访问解密 Oracle。此时,如果敌手可以构造一个新的签名 (m, r, s) 使得 $\alpha'_i = r^s \alpha^{H(m)} \bmod p$ 成立,则存在算法 A 在给定条件下可求解二元方程 $\alpha'_i = x^y \alpha^{H(m)} \bmod p$ 。于是,设算法 B 给未定元 x 赋值 r , 构造一个新的一元方程 $\beta = r^y \bmod p$, 其中 $\beta = \alpha'_i \alpha^{-H(m)} \bmod p$ 。因为 $\alpha'_i = r^y \alpha^{H(m)} \bmod p$, 通过调用算法 A, B 就可以求解方程 $\beta = r^y \bmod p$ 。

引理 3 被撤销成员不能生成有效的签名。

证明:对于那些被撤销的成员,他们拥有自己的私钥 x_i ,但在有限域上多项式分解唯一性定理的条件下,对于撤销后的多项式 $f(x)$, $f(\alpha_i) \neq K$, 其中 $\alpha_i = \alpha^{x_i} \bmod p$ 。再根据引理 1 和引理 2, 被撤销成员不能签出有效的签名。

定理 4 方案部分满足匿名性,但不满足不可关联性。

证明:一个指定消息的签名,由于成员的身份 y_i 满足 $\alpha_i = y_i \bmod p$, $f(\alpha_i) = K$ 。在离散对数问题假设下,除群管理员外,任何人都不能获得成员的身份信息。但是,由于群证书是签名有效性检验的证据,敌手可以判定两个不同的签名是不是由同一个成员所签署,因此,群签名的不可连接性不能保持。

4 性能分析

系统建立阶段, GM 选择一个公钥密码系统,使得 GM 和成员各自独立生成自己的公私钥。在整个方案中, GM 的计算为一次模指数运算和若干次域 Z_q 上的多项式乘法或者除法运算。成员的签名算法与普通的签名算法相同。而验证过程多了一次多项式计算来检验成员的有效性。但是,文中方案的验证算法不及文献[3] 方案,因为合法性验证时需要计算一个多项式的取值,而文献[1] 方案仅需检验一个一次同余式即可。然而,在基于中国剩余定理的群签名方案中^[1,6], GM 需要为每个成员产生一对 RSA 密钥和一个素数,并且需要在 GM 和成员之间建立安全通道。相比而言,本方案简化了 GM 的计算负担和保密任

务,也不需要成员和管理者之间建立安全信道,并且在成员加入和撤销后,合法成员的签名密钥也不需要随之更新。设 E 表示模指数运算, M 表示模乘法运算, P 表示有限域上的多项式计算, En 为加密运算。如果将简单的整数运算代价忽略不计,文中方案与文献[3] 方案的性能比较见表 1。

表 1 文中方案与文献[3] 方案的性能比较		
	文中方案	文献[3] 方案
GM 的预计算	$nE + 1P$	$nE + 1P + nEn$
签名算法	$1E$	$1E$
验证算法	$2E + 1M + 1P$	$2E + 1M$

5 结束语

文中利用有限域上多项式分解唯一性定理给出了群成员的一种高效撤销方案,唯一性保证了用户的身份不可替代,并引入新的身份标识进行签名,使之适应群签名方案的需要。该方案解决了群签名方案的验证算法随撤销成员的个数线性增长的缺陷,而且由于签名密钥是成员自己选择,在离散对数问题假设下,任何伪造签名和窃取密钥的攻击行为是不可行的,因此克服了目前一些基于离散对数群签名方案容易伪造的缺点。该群签名方案具有以下的特点:不交互得到群证书; GM 的证据更新算法简单;签名算法简单;验证算法与撤销成员的个数无关;成员证据不随群公钥的变化而变化;不需要安全信道。因此,文中方案的安全性优于文献[3],并降低了群签名方案的计算复杂性和通信代价。

相比诸如 ACJT 等群签名方案复杂的模指数运算,文中给出的群签名在通信和计算代价上有着显著的优越性。

参考文献:

[1] 陈泽文, 张龙军, 王育民, 等. 一种基于中国剩余定理的群签名方案[J]. 电子学报, 2004, 32(7): 1062 - 1065.
[2] Li Jun, Cui Guohua, Liu Zhiyuan. Cryptanalysis and improvement of a group signature scheme[J]. ACTA Electronica Sinica 2007, 35(4): 778 - 781.
[3] Wang Fenghe, Hu Yupu, Wang Chunxiao. An attack and improve of a group signature scheme based on chinese remainder theorem[J]. Journal of Electronics & Information Technology, 2007, 29(1): 182 - 184.

(下转第 169 页)

在相同工艺条件下,文中对比了新型 2.5V/5V 双电源电压输出电路和采用厚栅氧晶体管的 2.5V/5V 双电源电压输出电路.在相同工艺下,电路中所有 MOS 晶体管的沟道宽度与沟道长度决定了电路的版图面积,所以文中选用了所有 MOS 晶体管的沟道宽度与所有 MOS 晶体管的栅面积两个指标来对比两电路的面积;另外,文中还对比了两电路在 100Mbps 传输速率下的延迟与功耗.其结果如表 1 所示.其中①表示采用厚栅氧晶体管的 2.5V/5V 双电源电压输出电路,②表示新型 2.5V/5V 双电源电压输出电路.由表 1 可以看出,新型 2.5V/5V 双电源电压输出电路在面积、延迟、功耗三方面都优于采用厚栅氧晶体管的 2.5V/5V 双电源电压输出电路.

表 1 采用厚栅氧晶体管的 2.5V/5V 双电源电压输出电路与新型 2.5V/5V 双电源电压输出电路的性能指标对比

		①	②
面积	所有晶体管的沟道宽度(μm)	841.5	790.5
	所有晶体管的栅面积(μm^2)	385.385	197.625
延迟	平均延迟 $T_d(\text{ns})$	3.18	2.34
	由 0 变为 1 时的传输延迟 $T_{d,\text{up}}(\text{ns})$	2.47	2.54
	由 1 变为 0 时的传输延迟 $T_{d,\text{down}}(\text{ns})$	3.88	2.17
功耗(mW)		27.6	26.3

4 结束语

文中基于 0.25 μm 标准 CMOS 工艺,提出一种新型 2.5V/5V 双电源电压输出电路,将摆幅为 0~2.5V 的内部信号转换为摆幅为 0~5V 的输出信号.此输出电路只使用耐压为 2.5V 的薄栅氧 MOS 器件,经过仿真,在 5V 电压下没有栅氧过压问题.相对

于采用厚栅氧晶体管的 2.5V/5V 双电源电压输出电路而言,文中提出的新型 2.5V/5V 双电源电压输出电路有着较好的性能.

参考文献:

[1] Scott R S, Dumin N A, Hughes T W, et al. Properties of high-voltage stress generated traps in thin silicon oxide[J]. IEEE Trans. Electron Devices, 1996,43(7):1133-1143.

[2] Iwai H, Momose H S. Ultra-thin gate oxides-performance and reliability[C]// IEDM. Tech. Dig. USA:San Francisco, 1998:163-166.

[3] 高丹,刘海涛. CMOS 数字电路低功耗的层次化设计[J]. 微电子学与计算机,2008,25(1):133-135.

[4] 李桦,宋李梅. 双栅氧 CMOS 工艺研究[J]. 微电子学与计算机,2005,22(11):5-7.

[5] Sanjay Dabral, Timothy Maloney. Basic ESD and I/O Design [M]. New York: Wiley, 1998.

[6] Annema A J, Geelen G, De Jong P C. 5.5V I/O in a 2.5V 0.25 μm CMOS technology[J]. IEEE J. Solid-State Circuits, 2001,36(3):528-538.

[7] Uyemura J P. Introduction to VLSI circuits and systems[M]. New York: John Wiley & Sons, Inc, 2002.

[8] Fotty D. MOSFET modeling with SPICE[M]. Boston: Prentice Hall Publishers, 1997.

作者简介:

苏强 男,(1983-),硕士.研究方向为专用集成电路设计.

吴龙胜 男,(1968-),研究员,硕士生导师.研究方向为 Soc 设计技术、微电子器件加固技术.

刘文平 男,(1957-),研究员,硕士生导师.研究方向为集成电路设计技术与 Soc.

(上接第 165 页)

[4] Lu Rongbo, Xuan Hengnong, He Dake. Cryptanalysis and improvement of a group signature scheme[J]. Journal on Communications, 2007,28(4):10-12.

[5] Zhang J H, Wu Q H, Zou J C,et al. An efficient group signature scheme[J]. Acta Electronica Sinica, 2005,33(6):1113-1115.

[6] Bellare M, Shi H, Zhang C. Foundations of group signatures; the case of dynamic groups[C]// CT-RSA 2005. Berlin: Springer-Verlag, 2005:136-153.

作者简介:

张兴兰 女,(1970-),博士,副教授.研究方向为信息安全.