1-out-of-*n*不经意传输的变换及应用

张京良[1,2]，马丽珍[3]，王育民[1]

(1. 西安电子科技大学综合业务网国家重点实验室 西安 710071; 2. 中国海洋大学数学系 山东 青岛 266071;
3. 中国海洋大学物理系 山东 青岛 266100)

【摘要】提出了不经意传输的一个新应用——在群签名中的应用。首先给出了文献[1]的1-out-of-*n*不经意传输协议的一个变形，利用该变形协议提出了一种新的群签名成员资格撤销方法。该撤销方法是一个一般性的方法，可通用于任何群签名方案，而以前的撤销方法都是针对某一具体签名方案的，不具有通用性。在随机预言机模型以及计算Diffie-Hellman(CDH)假设下，可证明新协议是安全的。

关 键 词 1-out-of-n不经意传输; 群签名; 成员资格撤销; Schnorr签名
中图分类号 TP309 **文献标识码** A

Transformation of 1-out-of-*n* Oblivious Transfer and Its Application

ZHANG Jing-liang[1, 2], MA Li-zhen[3] , and WANG Yu-min[1]

(1. State Key Laboratory of Integrated Service Networks, Xidian University Xi'an 710071;
2. Department of Mathematics, Ocean University of China Qingdao Shandong 266071;
3. Department of Physics, Ocean University of China Qingdao Shandong 266100)

Abstract A new application to group signature on 1-out-of-*n* oblivious transfer is proposed. After introducing, the transformation of 1-out-of-*n* oblivious transfer protocol proposed by Ref.[1], a new membership revocation method in group signature is proposed by use of the transformation protocol. The proposed method is a universal method and can be applied to any group signature scheme; however, the previous revocation methods are only applicable to a specific group signature scheme. Under the random oracle model and computational Diffie-Hellman (CDH) assumption, the proposed protocol is provably secure.

Key words 1-out-of-*n* oblivious transfer; group signature; membership revocation; schnorr signature

不经意传输是可信密码学的一个基本工具，可分为比特不经意传输和字符串不经意传输；对应二者，又分别包含1-out-of-2、1-out-of-*n*、*k*-out-of-*n*等情形[1-2]。现在已发现，不经意传输有许多重要应用，如公平电子合同的签署、秘密信息检索、安全多方计算等[3]。本文给出了不经意传输的一个新应用——在群签名方面的应用。

1 1-out-of-*n*不经意传输协议

1-out-of-*n*不经意传输是指：发送者S有*n*个秘密消息 $m_1, m_2, \cdots, m_n$，根据接收者R的选择，将其中某个消息 m_α 发送给R，而S不知道发送给R的是哪个消息。文献[1]根据不同的安全需求，提出了3个高效的1-out-of-*n*不经意传输协议，其中第3个协议如下：

-System parameters (g, h, G_q)；

-S's input: $m_1, m_2, \cdots, m_n \in G_q$；

R's choice: α，$1 \leqslant \alpha \leqslant n$；

(1) R sends $y = g^r h^\alpha$， $r \in_R Z_q$。

(2) S sends $a = g^k$, and $c_i = m_i \oplus H((y/h^i)^k, i)$, $k \in_R Z_q$, $1 \leqslant \alpha \leqslant n$。

(3) By a and c_α， R computes $m_\alpha = c_\alpha \oplus H(a^r, \alpha)$。

这是一个高效的协议：R需要2个模指数运算——计算y和a^r；S需要3个模指数运算——计算a，y^k 和 h^k，而且a和h^k 还可以被预计算。

2 1-out-of-*n*不经意传输协议的变形

1-out-of-*n*不经意传输的变形定义：

定义 1 1-out-of-*n*不经意证明：验证者V有*n*个秘密消息 $m_1, m_2, \cdots, m_n$，示证者P向V证明他拥有这*n*

收稿日期：2007－06－29; 修回日期：2007－11－11
基金项目：国家自然科学基金(60473027)
作者简介：张京良(1973－)，男，博士生，主要从事密码学及其应用方面的研究.

个消息中的某一个消息 m_α，而不让V知道他拥有的是哪个消息。

1-out-of-n不经意证明可通过协议来实现。类似于1-out-of-n不经意传输，1-out-of-n不经意协议应满足下列要求。

正确性：如果P与V正确地执行协议，则协议的目标可实现。即P与V按照协议步骤执行，则在协议结束后，P可证明他拥有V的n个秘密消息中的某一个。示证者隐私(prover's privacy)：协议结束后，V除知道P确实拥有他的某个消息外，不知道他拥有的是哪个消息。即对应于P的不同消息 m_α 与 $m_{\alpha'}$ 的副本 $(\alpha \neq \alpha')$，V是不可区分的。如果副本是均匀分布的，则 m_α 是无条件安全的。验证者隐私(verifier's privacy)：P除知道 m_α 外，不知道V的其他消息。可在理想模型下证明此时可信第三方T作为中间代理，接收P的输入 m_α 和V的输入 $m_1, m_2, \cdots, m_n$，使V相信P有 m_α。要求对每一可能的具有恶意的P，都有一模拟器P′，通过与T交互使得P′的输出与P的输出是计算不可区分的。

可用文献[1]的1-out-of-n不经意传输协议的变形来实现1-out-of-n不经意证明：

-System parameters (g, h, G_q)；

-V's input: $m_1, m_2, \cdots, m_n \in G_q$；

P's input: m_α, $1 \leqslant \alpha \leqslant n$；

(1) P sends $y = g^r h^\alpha$, $r \in_R Z_q$。

(2) V computes $b = g^u h^t$, sends $a = g^k$, and $c_i = b \oplus H((y/h^i)^k, m_i)$, $u, t, k \in_R Z_q$, $1 \leqslant \alpha \leqslant n$。

(3) P sends $c = c_\alpha \oplus H(a^r, m_\alpha)$。

(4) V checks $b = c$。

正确性：$c = c_\alpha \oplus H(a^r, m_\alpha) = b \oplus H((y/h^\alpha)^k, m_\alpha) \oplus H(a^r, m_\alpha) = b \oplus H(a^r, m_\alpha) \oplus H(a^r, m_\alpha) = b$。

效率：P需要2个模指数运算——计算 y 和 a^r；V需要4个模指数运算——计算b、a、y^k 和 h^k。而且b、a 和 h^k 还可以被预计算。

定理 1　在随机预言机模型和CDH假设下，上述1-out-of-n不经意证明协议满足示证者隐私和验证者隐私的要求。

证明：示证者隐私。验证者从示证者那里获得到的关于 m_α 的信息是 $y = g^r h^\alpha$，但由于对 $\forall\ \alpha'$，都有 r' 使得 $y = g^{r'} h^{\alpha'}$，所以即使验证者有无限计算能力，也不能从 y 获得验证者的关于 α，进而 m_α 的任何信息。所以示证者的隐私是无条件安全的。

验证者隐私。(1) 有恶意的P不能以不可忽略的概率计算出 $(y/h^i)^k$ 和 $(y/h^j)^k$，$i \neq j$。如果P能计算2个值：$t_1 = (y/h^i)^k$ 和 $t_2 = (y/h^j)^k$，则他可计算出 $h^k = (t_1/t_2)^{1/(j-i)}$，这说明P能以如下方法求解CDH问题：给定 g、$g^{a'}$、$g^{b'}$，令 $h = g^{a'}$，$k = b'$，则P能计算 $h^k = (g^{a'})^{b'} = g^{a'b'}$，与CDH假设矛盾。(2) 在理想模型下，存在P的模拟器P′使得P′的输出与P的输出不可区分。

构造模拟器P′的步骤如下：

(1) 模拟P生成 $\bar{y}$。

(2) 随机选取 $\bar{b}$、$\bar{k}$、$\bar{c}_i$，计算 $\bar{a} = g^{\bar{k}}$。

(3) 模拟P输入 $\bar{a}$，$\bar{b}$，$\bar{c}_i$，并监听P对hash预言机的询问。当P询问 (a^r, m_j) 时，P′监听到 m_j，将 m_j 送给理想模型中的可信第三方T得到 j，并取 $h = b \oplus \bar{c}_j$ 作为hash值 $H((\bar{y}/h^j)^{\bar{k}}, m_j)$。

(4) P′的输出为 $\bar{c}_j \oplus H((\bar{y}/h^j)^{\bar{k}}, m_j)$。

易见，P′的输出是 $\bar{c}_j \oplus H((\bar{y}/h^j)^{\bar{k}}, m_j) = \bar{c}_j \oplus b \oplus \bar{c}_j = b$，而且由步骤(1)知，P不可能知道两个值 $(y/h^i)^k$ 和 $(y/h^j)^k$，$i \neq j$，即P的两次询问(a^r，m_j)与 (a^r, m_α) 是一样的，即 $j = \alpha$，从而说明P只拥有一个 m_α 且P′与P的输出是不可区分的。

3　1-out-of-n不经意证明的应用

本文以ACJT[4]群签名方案为例说明如何用1-out-of-n不经意证明设计成员撤销算法。这里仅简介各个步骤，具体参数的选取及签名过程可参见文献[4]。以下简称群管理员为GM。

建立：GM建立群公钥和GM的相应私钥。

加入：成员 P_i 通过与GM交互获得GM颁发的成员资格证书 v_i。

撤消：GM将成员证书保存在一个数据库中。若某个成员被删除，则将他的成员证书从该数据库中删除。

签字：一个群成员可用原方案中的方法进行签字，但需证明他没被撤消，具体如下：

设此时群中有n个成员，GM在数据库中保存的证书为 $v_{i_1}, v_{i_2}, \cdots, v_{i_n}$。成员 P_{i_α} 首先运用1-out-of-n不经意证明协议向GM证明他的证书 $v_{i_\alpha} \in \{v_{i_1}, v_{i_2}, \cdots, v_{i_n}\}$。若证明成功，GM对当前时间进行Schnorr签名 $\sigma = s_{\mathrm{GM}}(\mathrm{time})$，发送 (σ, time) 给 P_{i_α}。P_{i_α} 验证 σ 的正确性后，用原方案中的签字方法对用户消息 m 签字得到 S，则 P_{i_α} 的最终签字为 $(S, \sigma, \mathrm{time})$。

验证：用户首先验证 σ 的正确性，再检验time与当前时间是否相符；若相符，则再用原方案中的验证方法验证 S 的正确性。

打开：与原方案同。

由上可见，这种成员撤销方法不仅适用于ACJT方案，还适用于任何基于证书的群签名方案，如CS97[5]、NS'04[6]、NKHF'05[7]等。而且，若将撤销和签字过程中的成员证书换为成员身份，则这种撤销方法可适用于任何群签名，是一个通用方法。

安全性：方法的安全性基于原群签名、1-out-of-*n* 不经意证明协议及Schnorr签名的安全性。而由定理1知，1-out-of-*n* 不经意证明的安全性基于CDH假设；又Schnorr签名的安全性也基于CDH假设。所以，在CDH假设下本文的撤销方法的安全性与原签名方案的安全性相同。

效率比较：仅考虑花费较大的模指数运算。与原方案相比，在签名阶段，多了6个模指数运算(P_{i_α} 2个、GM4个，如果GM进行预计算，则仅需1个模指数运算)和1个Schnorr签名(1个模指数，也可以被GM预计算)；在验证阶段，多了1个签名Schnorr签名验证(1个模指数)。而文献[8]的方法在签名阶段需增加9个模指数运算，在验证阶段需增加5个模指数运算，而且每次撤销都需更新成员钥；文献[9-10]的方法在签名阶段需增加11个模指数运算，在验证阶段需增加8个模指数运算。所以，本文的方法更高效。而且，签名长度与当前成员个数和撤消的成员个数均无关，群公钥与成员资格证书也无需变动。

4 结 论

本文发现了不经意传输的一个新应用——用于群签名中成员撤销方法的设计中。所提出的撤销方法是一个一般性的方法，可通用于任何群签名方案，而以前的撤销方法都是针对某一具体签名方案的，不具有一般性。新方案的签名长度与当前成员个数和撤消的成员个数均无关，群公钥与成员资格证书也无需变动。

参 考 文 献

[1] TZENG Wen-guey. Efficient 1-out-of-*n* oblilvious transfer schemes with universally usable parameters[J]. IEEE Transactions on Computers, 2004, 53(2): 232-240.

[2] NAOR M, PINKAS B. Computationally secure oblivious transfer[J]. J Cryptology, 2005, 18: 1-35.

[3] 周明天, 谭 良. 可信计算及其进展[J]. 电子科技大学学报, 2006, 35(4): 686-697.
ZHOU Ming-tian, TAN Liang. Progress in trusted computing[J]. Journal of University of Electronic Science and Technology of China, 2006, 35(4): 686-697.

[4] ATENIESE G, CAMENISCH J, JOYE M, et al. A practical and provably secure coalition-resistant group signature scheme[C]//CRYPTO'2000, LNCS 1880. Berlin: Springer Verlag, 2000: 255-270.

[5] Jan Camenisch, Markus Stadler. Efficient group signature schemes for large groups[C]//CRYPTO'97, LNCS 1294. Berlin: Springer Verlag, 1997: 410-424.

[6] NAKANISHI T, SUGIYAMA Y. A group signature scheme with efficient membership revocation for reasonable groups[C]//ACISP 2004, LNCS 3108. Berlin: Springer Verlag, 2004: 336-347.

[7] NAKANISHI T, KUBOOKA F, HAMADA N, et al. Group signature schemes with membership revocation for large groups[C]//ACISP 2005, LNCS 3574. Berlin: Springer Verlag, 2005: 443-454.

[8] CAMENISCH J, LYSYANSKAYA A. Dynamic accumulators and application to efficient revocation of anonymous credentials[C]//CRYPTO'2002, LNCS 2442. Berlin: Springer Verlag, 2002: 61-76.

[9] CHEN Z W, WANG J L, WANG Y M, et al. An efficient revocation algorithm in group signatures[C]//ICISC 2003, LNCS 2971. Berlin: Springer Verlag, 2004: 339-351.

[10] ZHANG J L, WANG Y M. Efficient membership revocation in ACJT group signature[J]. Journal of Electronic Science and Technology of China, 2008, 6(1): 39-42.

编 辑 漆 蓉