

文章编号:1001-9081(2013)02-0417-06

doi:10.3724/SP.J.1087.2013.00417

无随机预言的完全匿名多服务订购系统

柳 欣^{1,2*}, 雷文庆^{2,3}

(1. 山东青年政治学院 信息工程学院, 济南 250014; 2. 山东省高校信息安全与智能控制重点实验室(山东青年政治学院), 济南 250103;
3. 山东青年政治学院 继续教育学院, 济南 250014)
(*通信作者电子邮箱 lxonne@163.com)

摘要:最近,Canard 等(CANARD S, JAMBERT A. Untraceability and profiling are not mutually exclusive [C]// TrustBus 2010: Proceedings of the 7th International Conference on Trust, Privacy and Security in Digital Business, LNCS 6264. Berlin: Springer-Verlag, 2010: 117 – 128)提出了多服务订购的概念以及几个实例化的系统。然而,这些系统仅满足较弱的可撤销的匿名性且不适合于“按次付费”的服务。为此,通过对 Canard 等的系统进行扩展而提出一个改进的多服务订购系统。新系统利用 Liu 等(LIU J K, AU M H, SUSILO W, et al. Enhancing location privacy for electric vehicles (at the right time) [EB/OL]. [2012-08-01]. <http://eprint.iacr.org/2012/342>)的匿名支付技术实现了对“按次付费”的支持,利用 Peng-Bao 小区间证明技术实现了对“账户余额足以当前服务付费”的零知识证明。此外,通过将 Cramer 等的技术应用于底层 Σ 协议,实现了新系统的构造过程所需的知识证明协议。相对于已有的典型系统,新系统的优势体现在安全性方面:首先,在标准模型下满足可证安全;其次,实现了 3 个关键性质的最强安全等级,即支付令牌的不可分割性、用户的匿名性和底层证明系统的零知识性。

关键词:电子商务;增强隐私保护的机制;匿名访问;知识证明;标准模型

中图分类号: TP309.7 文献标志码:A

Fully anonymous multi-service subscription system without random oracles

LIU Xin^{1,2*}, LEI Wenqing^{2,3}

(1. School of Information Engineering, Shandong Youth University of Political Science, Jinan Shandong 250014, China;
2. Key Laboratory of Information Security and Intelligent Control in Universities of Shandong (Shandong Youth University of Political Science), Jinan Shandong 250103, China;
3. School of Continuing Education, Shandong Youth University of Political Science, Jinan Shandong 250014, China)

Abstract: Lately, Canard et al. (CANARD S, JAMBERT A. Untraceability and profiling are not mutually exclusive [C]// TrustBus 2010: Proceedings of the 7th International Conference on Trust, Privacy and Security in Digital Business, LNCS 6264. Berlin: Springer-Verlag, 2010: 117 – 128) introduced the notion of multi-service subscription and proposed several instantiations. Unfortunately, their systems only satisfied a weaker variant of anonymity called revocable-anonymity and they were not fit for "pay-per-use" services. To this end, a revised multi-service subscription system was put forward to extending Canard et al's system. The new system achieved pay-per-use subscriptions by incorporating the anonymous payment system raised by Liu et al. (LIU J K, AU M H, SUSILO W, et al. Enhancing location privacy for electric vehicles (at the right time) [EB/OL]. [2012-08-01]. <http://eprint.iacr.org/2012/342>). To allow users to prove in zero-knowledge that their account balance is enough for making a payment for the required access, it also utilized the Peng-Bao range proof for small ranges. Furthermore, it was constructed on several 4-round perfect zero-knowledge proofs of knowledge, which were obtained by applying a technique by Cramer et al. to the underlying Sigma-protocols. Compared with typical systems in the literature, the new solution gains advantages in terms of security. Concretely, it can be proved secure in the standard model. Moreover, it matches the strongest level of three crucial security notions, such as inseparability for spendable tokens, anonymity for users, and zero-knowledge for underlying proof systems.

Key words: e-commerce; privacy-enhancing mechanism; anonymous access; knowledge proof; standard model

0 引言

当前,能否较好地解决用户的个人隐私保护问题已经成为安全电子商务系统设计的关键。匿名订购系统^[1-6]允许用户预先订购所感兴趣的在线服务项目,此后以匿名、无关联的方式进行访问,从而确保个人敏感信息(如访问的服务类型、访问频率和账户余额等)不被泄露。根据具体应用环境,可以将已有的订购系统分为两种类型^[1]:第一类允许用户在固

定时段内不受次数限制地使用某项服务^[1-3],而第二类则要求用户“按次付费”^[4-6]。最近,Canard 等^[1]提出了多服务订购系统的概念,此类系统有利于在确保用户隐私的条件下,为服务供应商提供某种程度上的客户分析能力,从而确定最受欢迎的服务类型。然而,Canard 等^[1]的系统仅实现了较弱的“可撤销”的匿名性^[7]且并不适合于第二类应用环境(如根据下载次数付费的在线音乐以及根据检索次数收费的 DNA 数据库或专利数据库^[8]等)。尽管已有的多个系统^[4-6]支持按

收稿日期:2012-08-17;修回日期:2012-10-19。 基金项目:山东省高等学校科技计划项目(J11LG29)。

作者简介:柳欣(1978-),男,山东广饶人,讲师,博士,CCF 会员,主要研究方向:信息安全、密码学; 雷文庆(1964-),男,山东寿光人,副教授,主要研究方向:信息安全。

次付费,但是并不支持对多项服务的订购,即每订购一项新的服务就必须再次执行注册协议以申请新的支付令牌,从而增加了令牌管理的难度。此外,已有系统^[1-5]多数是在随机预言模型^[9]下设计的,尽管文献[6]的系统在标准模型下满足可证安全,但缺点是其底层证明系统实质上是知识论证系统而非知识证明系统。

本文在 Canard 等系统的基础上提出了改进的多服务订购系统。与已有系统相比,新系统的优点体现在以下方面:1)允许用户根据具体的服务类型和访问次数付费;2)用户可以利用一张支付令牌实现对多项服务的访问,而且允许多次进行匿名充值;3)用户的账户余额保存在支付令牌之中,从而可以向服务供应商隐藏该余额;4)支持令牌的过期,并且允许用户将账户余额转移至更新后的令牌;5)系统的安全性可以在标准模型下得到证明;6)与已有系统相比,本文系统同时满足多个理想性质,即令牌的强不可分割性、用户的完全匿名性以及底层证明系统的完全零知识性。

1 本文系统的描述

本文系统的设计思想如下:为了实现第二类的订购,采用了 Liu 等^[10]提出的匿名支付技术,即用户(U)最初向服务供应商(Service Provider,SP)申请一张支付令牌,并且预先存入系统规定的账户初始余额 D。此后,U 可以利用不同的子协议以匿名方式订购所感兴趣的服务,访问某项服务,追加订购服务项目,向账户中充值,并且在令牌过期后将账户余额转移至更新后的令牌。在这些子协议中,首先利用标准的 Σ 协议实现所需的知识证明,但是仅满足较弱的诚实验证者零知识性,而在现实应用中充当验证者的 SP 未必保持诚实。为此,采用 Cramer 等^[11]的技术将所得证明增强为完全零知识的知识证明协议。为了引入令牌过期机制^[10],将系统的运行过程划分为若干个时间周期,并假设当系统初始建立时进入周期 T_1 。为了在注册(或充值)协议中向 SP 支付, U 可以购买预先付费的信用卡^[8],且忽略了具体细节。此外,符号 $PK\{x\} : y = g^x$ 表示知识证明协议,其中位于圆括号内部的元素表示仅为证明者掌握的秘密元素,而其他的元素为证明者与验证者的共同输入。在系统描述中, $\pi_0, \pi_1, \dots, \pi_s$ 表示满足完全零知识性的知识证明协议,具体构造过程参见第 2 章。

系统建立 假设 SP 最多可以提供 f 项服务。

1) SP 产生对双线性映射 $\hat{e}: G_1 \times G_2 \rightarrow G_T$ 的描述,使得 $ord(G_1) = ord(G_2) = p, G_1 = \langle g_0 \rangle, G_2 = \langle h_0 \rangle$; 定义同构 $\psi: G_2 \rightarrow G_1$; 选取生成元 $g, h \in R^{G_1}$; 设置时间周期标识符 $T_i|_{i=1}$, 选取抗碰撞的散列函数 $H: \{0,1\}^* \rightarrow G_2$, 设置 $g_{i,j} = \psi(H(T_i \parallel j))|_{j=1,2,3}$ 。

2) SP 选取常量 $s_1, s_2, \dots, s_f \in R^{Z_p^*}$, 用于标识已经订购的服务; 选取常量 $n_1, n_2, \dots, n_f \in R^{Z_p^*}$, 用于标识尚未订购的服务; 选取生成元 $\tilde{g}_0, \tilde{g}_1, \dots, \tilde{g}_f \in R^{G_1}$; 选取证书签名方案^[12-13]的私钥 $\gamma \in R^{Z_p^*}$, 设置公钥 $w = h_0^\gamma$; 选取常数 u 以及适当的整数 n, 设置 $D = u^n$, 定义 D 为用户的初始和最大账户余额。

3) SP 发布公钥 $PK = (p, G_1, G_2, G_T, g_0, h_0, \hat{e}, \psi, g, h, T_i, H(\cdot), \{g_{i,j}\}_{i=1, j=1,2,3}, \{s_j\}_{j=1,2,\dots,f}, \{n_j\}_{j=1,2,\dots,f}, \{\tilde{g}_j\}_{j=1,2,\dots,f}; w, u, n)$ 。此外,SP 需要在系统进入新的周期后更新 PK 中的元素 $T_i, \{g_{i,j}\}$ 。

用户的密钥产生 U 选取个人私钥 $usk \in R^{Z_p^*}$, 设置

$$upk = g_{1,1}^{usk}$$

账户注册 假设当前处于第 i 个周期 T_i 。为了获得初始余额为 D 的支付令牌 token, 拥有密钥对 (usk, upk) 的 U 与 SP 执行以下过程:

1) U 设置 $g_{i,j} = \psi(H(T_i \parallel j))|_{j=1,2,3}$, 选取 $y', s \in R^{Z_p^*}$, 计算 $C = g_0^{y'} g_{i,1}^{usk} g_{i,3}^s$, 向 SP 发送 C, upk , 并且与 SP 执行知识证明 $\bar{\pi}_0 = PK\{(usk, y', s); upk = g_{1,1}^{usk} \wedge C = g_0^{y'} g_{i,1}^{usk} g_{i,3}^s\}$ 。 $\bar{\pi}_0$ 向 SP 证明: ① U 掌握与 upk 相对应的用户私钥 usk; ② C 是关于秘密元组 (usk, s) 的承诺。

2) 若 $\bar{\pi}_0$ 有效, 则 SP 选取 $y'', e \in R^{Z_p^*}$, 计算 $A = (g \cdot C \cdot g_0^{y''} \cdot g_{i,2}^D)^{\frac{1}{e+y}}$, 并且返回 (A, e, y'') 。

3) U 设置 $y = y' + y'' \bmod p$, 并验证是否满足 $\hat{e}(A, wh_0^e) = \hat{e}(gg_0^{y'} g_{i,1}^{usk} g_{i,2}^D g_{i,3}^s, h_0)$ 。若是, 则 U 保存支付令牌 $token = ((usk, D, s), (A, e, y))$ 。

订购 假设当前处于第 i 个周期 T_i 。假设 U 希望向 SP 订购标识为 $s_{i_1}, s_{i_2}, \dots, s_{i_k}$ 的 k 项服务, 且 $k \leq f$ 。定义 $I = \{i_1, i_2, \dots, i_k\} \subset \{1, 2, \dots, f\}$ 。具体过程为:

1) U 选取 $\tilde{y}' \in R^{Z_p^*}$, 计算 $C' = g_0^{\tilde{y}'} \tilde{g}_0^{usk}$ 。U 向 SP 发送 $C', \{s_{i_1}, s_{i_2}, \dots, s_{i_k}\}$, 并且与 SP 执行知识证明 $\bar{\pi}_1 = PK\{(A, e, y, usk, D, s, \tilde{y}'); \hat{e}(A, wh_0^e) = \hat{e}(gg_0^{\tilde{y}'} g_{i,1}^{usk} g_{i,2}^D g_{i,3}^s, h_0) \wedge C' = g_0^{\tilde{y}'} \tilde{g}_0^{usk}\}$ 。 $\bar{\pi}_1$ 向 SP 证明: ① U 拥有有效支付令牌; ② 承诺 C' 是以正确方式产生的。

2) 若 $\bar{\pi}_1$ 有效, 则 SP 选取 $\tilde{y}'' \in R^{Z_p^*}$, 计算 $\tilde{A} = (g \cdot C' \cdot g_0^{\tilde{y}''} \prod_{j \in I} \tilde{g}_j^{s_j} \prod_{j \in [1, f] / I} \tilde{g}_j^{n_j})^{\frac{1}{y''+e}}$, 并且返回 $(\tilde{A}, \tilde{e}, \tilde{y}'')$ 。

3) U 设置 $\tilde{y} = \tilde{y}' + \tilde{y}'' \bmod p$, 验证是否满足 $\hat{e}(\tilde{A}, wh_0^{\tilde{e}}) = \hat{e}(gg_0^{\tilde{y}'} \tilde{g}_0^{usk} \prod_{j \in I} \tilde{g}_j^{s_j} \prod_{j \in [1, f] / I} \tilde{g}_j^{n_j}, h_0)$ 。若是, 则 U 保存订购证书 $cert_{sub} = (usk, \{s_j\}_{j \in I}, \{n_j\}_{j \in [1, f] / I}, (\tilde{A}, \tilde{e}, \tilde{y}))$ 。

访问服务 假设当前处于第 i 个周期 T_i 。同时,假设订购了服务 $\{s_{i_1}, s_{i_2}, \dots, s_{i_k}\}$ 的用户 U 希望以匿名方式访问服务 s_{i_1} , 且访问该服务的费用为 v。此时, U 掌握 $token = ((usk, B, s), (A, e, y))$, $cert_{sub} = (usk, \{s_j\}_{j \in I}, \{n_j\}_{j \in [1, f] / I}, (\tilde{A}, \tilde{e}, \tilde{y}))$, 其中 B 表示 U 的账户余额。具体过程为:

1) U 检查是否满足 $B \geq v$, 若是, 则选取 $\bar{y}', \bar{s} \in R^{Z_p^*}$, 向 SP 发送 $C = g_0^{\bar{y}'} g_{i,1}^{usk} g_{i,2}^B g_{i,3}^{\bar{s}}$ 以及令牌序列号 s。同时, U 与 SP 执行知识证明 $\bar{\pi}_2 = PK\{(\bar{y}', \bar{s}, A, e, y, usk, B, \{s_j\}_{j \in I \setminus \{i_1\}}, \{n_j\}_{j \in [1, f] / I}, \tilde{A}, \tilde{e}, \tilde{y}); C = g_0^{\bar{y}'} g_{i,1}^{usk} g_{i,2}^B g_{i,3}^{\bar{s}} \wedge \hat{e}(A, wh_0^e) = \hat{e}(gg_0^{\bar{y}'} g_{i,1}^{usk} g_{i,2}^B g_{i,3}^{\bar{s}}, h_0) \wedge \hat{e}(\tilde{A}, wh_0^{\tilde{e}}) = \hat{e}(gg_0^{\bar{y}'} \tilde{g}_0^{usk} \prod_{j \in I \setminus \{i_1\}} \tilde{g}_j^{s_j} \prod_{j \in [1, f] / I} \tilde{g}_j^{n_j}, h_0)\} \wedge 0 \leq B - v \leq D\}$ 。 $\bar{\pi}_2$ 向 SP 证明: ① C 是关于秘密元组 (usk, B, \bar{s}) 的承诺; ② U 掌握有效的支付令牌; ③ U 已经订购了当前的服务; ④ U 的账户余额足以完成此次支付。

2) 若 $\bar{\pi}_2$ 有效且序列号 s 并未使用过, 则 SP 选取 $\bar{y}'' \in R^{Z_p^*}$, 设置 $\bar{A} = (g \cdot C \cdot g_0^{\bar{y}''} \cdot g_{i,2}^{\bar{v}})^{\frac{1}{\bar{y}''+e}}$, 返回 $(\bar{A}, \bar{e}, \bar{y}'')$, 并且保存 s。

3) U 设置 $\bar{y} = \bar{y}' + \bar{y}'' \bmod p$, $\bar{B} = B - v$, 并验证是否满足 $\hat{e}(\bar{A}, wh_0^{\bar{e}}) = \hat{e}(gg_0^{\bar{y}'} \tilde{g}_0^{usk} \tilde{g}_{i,2}^{\bar{v}} g_{i,3}^{\bar{s}}, h_0)$ 。若是, 则 U 保存更新后的令牌 $token = ((usk, \bar{B}, \bar{s}), (\bar{A}, \bar{e}, \bar{y}))$ 。

追加订购 假设当前处于第 i 个周期 T_i 。假设 U 已经订

购了 k 项服务,即 $\{s_{i_1}, s_{i_2}, \dots, s_{i_k}\}$,并且希望追加订购 l' 项服务,即 $\{s_{i_{k+1}}, s_{i_{k+2}}, \dots, s_{i_l}\}$,使得 $l = k + l'$ 。定义 $I = \{i_1, i_2, \dots, i_l\} = I \cup \{i_{k+1}, \dots, i_l\}$ 。此时, U 掌握 $token = ((usk, B, s), (A, e, y))$, $cert_{sub} = (usk, \{s_j\}_{j \in I}, \{n_j\}_{j \in [1, f] / I}, (\tilde{A}, \tilde{e}, \tilde{y}))$ 。具体过程为:

1) U 选取 $\bar{y}' \in {}_R\mathbf{Z}_p^*$, 计算 $C'' = g_0^{\bar{y}'} \tilde{g}_0^{usk} \prod_{j \in I} \tilde{g}_j^{s_j} \prod_{j \in [1, f] / I} \tilde{g}_j^{n_j} \circ U$ 向 SP 发送 C'' , $\{s_{i_1}, s_{i_2}, \dots, s_{i_k}\}$, $\{s_{i_{k+1}}, s_{i_{k+2}}, \dots, s_{i_l}\}$, 并与 SP 执行证明 $\bar{\pi}_3 = PK\{(\bar{y}', usk, A, e, y, B, s, \tilde{A}, \tilde{e}, \tilde{y})\}$:
 $C'' \prod_{j \in I} \tilde{g}_j^{-s_j} \prod_{j \in [1, f] / I} \tilde{g}_j^{-n_j} = g_0^{\bar{y}'} \tilde{g}_0^{usk} \wedge \hat{e}(A, wh_0^e) = \hat{e}(gg_0^y g_{i,1}^{usk} g_{i,2}^B g_{i,3}^s, h_0) \wedge \hat{e}(\tilde{A}, wh_0^e) = \hat{e}(gg_0^{\bar{y}'} \tilde{g}_0^{usk} \prod_{j \in I} \tilde{g}_j^{s_j} \prod_{j \in [1, f] / I} \tilde{g}_j^{n_j}, h_0)\}$ 。 $\bar{\pi}_3$ 向 SP 证明:① C'' 是关于秘密元组 $(usk, \{s_j\}_{j \in I}, \{n_j\}_{j \in [1, f] / I})$ 的承诺;② U 掌握有效的支付令牌;③ U 此前已经订购了服务 $\{s_{i_1}, s_{i_2}, \dots, s_{i_k}\}$ 。

2) 若 $\bar{\pi}_3$ 有效, 则 SP 选取 \bar{y}'' , $\bar{e} \in {}_R\mathbf{Z}_p^*$, 计算 $\bar{A} = (g \cdot C'' \cdot g_0^{\bar{y}''} \prod_{j \in I} \tilde{g}_j^{s_j - n_j})^{\frac{1}{\gamma + e}}$, 返回 $(\bar{A}, \bar{e}, \bar{y}'')$ 。

3) U 设置 $\bar{y} = \bar{y}' + \bar{y}'' \bmod p$, 验证是否满足 $\hat{e}(\bar{A}, wh_0^{\bar{e}}) = \hat{e}(gg_0^{\bar{y}} \tilde{g}_0^{usk} \prod_{j \in I} \tilde{g}_j^{s_j} \prod_{j \in [1, f] / I} \tilde{g}_j^{n_j}, h_0)$ 。若是, 则 U 保存更新后的订购证书 $cert_{sub} = (usk, \{s_j\}_{j \in I}, \{n_j\}_{j \in [1, f] / I}, (\bar{A}, \bar{e}, \bar{y}))$ 。

充值 假设当前处于第 i 个周期 $T_{i,0}$ 的账户余额为 B , U 希望向账户中充入金额 v , 使得 $\bar{B} = B + v \leq D$ 。此时, U 掌握 $token = ((usk, B, s), (A, e, y))$, $cert_{sub} = (usk, \{s_j\}_{j \in I}, \{n_j\}_{j \in [1, f] / I}, (\bar{A}, \bar{e}, \bar{y}))$ 。具体过程为:

1) U 选取 \bar{y}' , $s \in {}_R\mathbf{Z}_p^*$, 计算 $C = g_0^{\bar{y}'} g_{i,1}^{usk} g_{i,2}^B g_{i,3}^s$, 向 SP 发送 C 以及令牌序列号 s , 并且与 SP 执行证明 $\bar{\pi}_4 = PK\{(\bar{y}', usk, B, \bar{s}, A, e, y)\}$: $C = g_0^{\bar{y}'} g_{i,1}^{usk} g_{i,2}^B g_{i,3}^s \wedge \hat{e}(A, wh_0^e) = \hat{e}(gg_0^y g_{i,1}^{usk} g_{i,2}^B g_{i,3}^s, h_0) \wedge 0 \leq B + v \leq D$ 。 $\bar{\pi}_4$ 向 SP 证明:① C 是关于秘密元组 (usk, B, \bar{s}) 的承诺;② U 拥有有效的支付令牌;③ 在完成充值后,仍然不会超过最大账户余额 D 。

2) 若 $\bar{\pi}_4$ 有效且 s 未使用过, 则 SP 选取 \bar{y}'' , $\bar{e} \in {}_R\mathbf{Z}_p^*$, 计算 $\bar{A} = (g \cdot C \cdot g_0^{\bar{y}''} \cdot g_{i,2}^e)^{\frac{1}{\gamma + e}}$, 返回 $(\bar{A}, \bar{e}, \bar{y}'')$ 。

3) U 设置 $\bar{y} = \bar{y}' + \bar{y}'' \bmod p$, $\bar{B} = B + v$, 并验证是否满足 $\hat{e}(\bar{A}, wh_0^{\bar{e}}) = \hat{e}(gg_0^{\bar{y}} g_{i,1}^{usk} g_{i,2}^B g_{i,3}^s, h_0)$ 。若是, 则 U 保存更新后的令牌 $token = ((usk, \bar{B}, \bar{s}), (\bar{A}, \bar{e}, \bar{y}))$ 。

余额转移 假设当前系统进入第 $i+1$ 个周期 T_{i+1} 。掌握令牌 $token = ((usk, B, s), (A, e, y))$ 的用户 U 希望获得更新后的令牌,并且将原有的账户余额 B 转移至新的令牌。具体过程为:

1) U 设置 $g_{i+1,j} = \psi(H(T_{i+1} \| j))|_{j=1,2,3}$, 选取 \bar{y}' , $\bar{s} \in {}_R\mathbf{Z}_p^*$, 计算 $C = g_0^{\bar{y}'} g_{i+1,1}^{usk} g_{i+1,2}^B g_{i+1,3}^s$, 向 SP 发送 C 以及令牌序列号 s , 并且与 SP 执行知识证明 $\bar{\pi}_5 = PK\{(\bar{y}', usk, B, \bar{s}, A, e, y)\}$: $C = g_0^{\bar{y}'} g_{i+1,1}^{usk} g_{i+1,2}^B g_{i+1,3}^s \wedge \hat{e}(A, wh_0^e) = \hat{e}(gg_0^y g_{i+1,1}^{usk} g_{i+1,2}^B g_{i+1,3}^s, h_0)$ 。 $\bar{\pi}_5$ 向 SP 证明:① C 是关于秘密元组 (usk, B, \bar{s}) 的承诺;② U 拥有周期 T_i 内的有效支付令牌。

2) 若 $\bar{\pi}_5$ 有效且 s 未使用过, 则 SP 选取 \bar{y}'' , $\bar{e} \in {}_R\mathbf{Z}_p^*$, 计算 $\bar{A} = (g \cdot C \cdot g_0^{\bar{y}''})^{\frac{1}{\gamma + e}}$, 返回 $(\bar{A}, \bar{e}, \bar{y}'')$ 。

3) U 设置 $\bar{y} = \bar{y}' + \bar{y}'' \bmod p$, 并验证是否满足 $\hat{e}(\bar{A}, wh_0^{\bar{e}}) = \hat{e}(gg_0^{\bar{y}} g_{i+1,1}^{usk} g_{i+1,2}^B g_{i+1,3}^s, h_0)$ 。若是, 则 U 保存更新后的令牌

$$\overline{token} = ((usk, B, \bar{s}), (\bar{A}, \bar{e}, \bar{y})).$$

2 完全零知识的知识证明协议

本章将以 $\bar{\pi}_2$ 为例介绍本文知识证明的构造过程,且对其他证明的构造过程是类似的。 $\bar{\pi}_2$ 的构造分为两步。在第一步,需要采用标准技术实现 Σ 协议 π_2 。在第二步,需要利用 Cramer 等^[11]的技术将 π_2 增强为完全零知识的知识证明协议 $\bar{\pi}_2$ 。

2.1 利用 Σ 协议实现 π_2

在 π_2 的构造过程中,声明 $C = g_0^{\bar{y}'} g_{i,1}^{usk} g_{i,2}^B g_{i,3}^s$ 的证明方式较为直接。为了证明声明 $\hat{e}(A, wh_0^e) = \hat{e}(gg_0^y g_{i,1}^{usk} g_{i,2}^B g_{i,3}^s, h_0)$, 需要利用随机数 k_2 将秘密元素 A 盲化为 $A_1 = Ag^{k_2}$ 的形式,同时产生对 k_2 的辅助承诺 $A_2 = g^{k_1} h^{k_2}$ 。同样,为了证明声明 $\hat{e}(\bar{A}, wh_0^e) = \hat{e}(gg_0^{\bar{y}'} g_0^{usk} \tilde{g}_{i,1}^{s_{i_1}} \prod_{j \in I \setminus \{i_1\}} \tilde{g}_j^{s_j} \prod_{j \in [1, f] / I} \tilde{g}_j^{n_j}, h_0)$, 需要利用类似方式对 \bar{A} 进行隐藏。最后,为了证明声明 $0 \leq B - v \leq D$, 采用了文献[14]中的技术。具体地,需要产生对秘密元素 $B, B - v$ 的承诺 $E = g^B h^r, E' = E/g^v$ 。将 $B - v$ 写成 u 进制表达式的形式 $B - v = (x_n \cdots x_2 x_1)_u$, 使得 $B - v = \sum_{i \in [1, n]} x_i u^{i-1}$ 。同时,产生对每个数位 x_i 的承诺: $e_i = g^{x_i} h^{r_i}|_{i \in [1, n]}$ 。另外,计算秘密元素 $r' = (\sum_{i \in [1, n]} r_i u^{i-1}) \bmod p$ 。为了使用关于掌握“1-out-of-u”个秘密元素的证明技术^[13],对于 $i = 1, 2, \dots, n$,令 $e_i/g^{u-1} = Y_{i,1}$, $e_i/g^{u-2} = Y_{i,2}, \dots, e_i = Y_{i,u}$ 。通过对这些声明执行“AND”合成,可以将 π_2 实例化为如下形式:

$$\begin{aligned} \pi_2 = & PK\{(\bar{y}', usk, B, \bar{s}, k_1, k_2, -e, k_1 e, k_2 e, y, k_3, k_4, -\bar{e}, \\ & k_3 \bar{e}, k_4 \bar{e}, \bar{y}, \{s_j\}_{j \in I \setminus \{s_{i_1}\}}, \{n_j\}_{j \in [1, f] / I}, r, r', \\ & \{r_i\}_{i=1,2,\dots,n}): C = g_0^{\bar{y}'} g_{i,1}^{usk} g_{i,2}^B g_{i,3}^s \wedge A_2 = \\ & g^{k_1} h^{k_2} \wedge 1 = A_2^{-e} g^{k_1 e} h^{k_2 e} \wedge \frac{\hat{e}(A_1, w)}{\hat{e}(g, h_0) \hat{e}(g_{i,3}, h_0)^s} = \\ & \hat{e}(A_1, h_0)^{-e} \hat{e}(g, w)^{k_2 e} \hat{e}(g, h_0)^{k_2 e} \hat{e}(g_0, h_0)^r \hat{e}(g_{i,1}, h_0)^{usk} \hat{e}(g_{i,2}, h_0)^B \wedge A_4 = g^{k_3} h^{k_4} \wedge 1 = \\ & A_4^{-e} g^{k_3 e} h^{k_4 e} \wedge \frac{\hat{e}(A_3, w)}{\hat{e}(g, h_0) \hat{e}(\tilde{g}_{i,1}, h_0)^{s_{i_1}}} = \\ & \hat{e}(g_0, h_0)^r \hat{e}(\tilde{g}_0, h_0)^{usk} \prod_{j \in I \setminus \{s_{i_1}\}} \hat{e}(\tilde{g}_j, h_0)^{s_j} \\ & \prod_{j \in [1, f] / I} \hat{e}(\tilde{g}_j, h_0)^{s_j} \hat{e}(A_3, h_0)^{-e} \hat{e}(g, w)^{k_4 e} \hat{e}(g, h_0)^{k_4 e} \wedge \\ & E = g^B h^r \wedge \left(\prod_{i \in [1, n]} e_i^{u^{i-1}} \right) (E')^{-1} = \\ & h'^r \bigwedge_{i \in [1, n]} (Y_{i,1} = h'^i \vee Y_{i,2} = \\ & h'^i \vee \dots \vee Y_{i,u} = h'^i) \} \end{aligned}$$

π_2 的具体执行过程如下:

1) P 选取 $\rho_{\bar{y}'} \rho_{usk} \rho_B \rho_{\bar{s}} \rho_{k_1} \rho_{k_2} \rho_{-e} \rho_{k_1e} \rho_{k_2e} \rho_y \rho_{k_3} \rho_{k_4} \rho_{-e} \rho_{k_3e} \rho_{k_4e} \rho_{\bar{y}}$, $\{\rho_{s_j}\}_{j \in I \setminus \{s_{i_1}\}}$, $\{\rho_{n_j}\}_{j \in [1, f] / I}$, $\rho_r \rho_{r'} \in {}_R\mathbf{Z}_p$, 计算 $B_1 = g_0^{\rho_{\bar{y}'}} g_{i,1}^{usk} g_{i,2}^B g_{i,3}^s$, $B_2 = g^{\rho_{k_1}} h^{\rho_{k_2}}$, $B_3 = A_2^{\rho_{-e}} g^{\rho_{k_1} e} h^{\rho_{k_2} e}$, $B_4 = \hat{e}(A_1, h_0)^{\rho_{-e}} \hat{e}(g, w)^{\rho_{k_2} e} \hat{e}(g, h_0)^{\rho_{k_2} e}$, $\hat{e}(g_0, h_0)^{\rho_y} \hat{e}(g_{i,1}, h_0)^{\rho_{usk}} \hat{e}(g_{i,2}, h_0)^{\rho_B}$, $B_5 = g^{\rho_{k_3} h^{\rho_{k_4} e}}$, $B_6 = A_4^{\rho_{-e}} g^{\rho_{k_1} e} h^{\rho_{k_2} e}$, $B_7 = \hat{e}(g_0, h_0)^{\rho_y} \hat{e}(\tilde{g}_0, h_0)^{\rho_{usk}} \prod_{j \in I \setminus \{s_{i_1}\}} \hat{e}(\tilde{g}_j, h_0)^{\rho_{s_j}}$

$$\prod_{j \in [1, f] / I} \hat{e}(\tilde{g}_j, h_0)^{\rho_{ij}} \hat{e}(A_3, h_0)^{\rho_{-i}} \hat{e}(g, w)^{\rho_{k4}} \hat{e}(g, h_0)^{\rho_{k4}},$$

$$B_8 = g^{\rho_B} h^{\rho_r}, \quad B_9 = h^{\rho_r}$$

对于 $i = 1, 2, \dots, n$, 定义 $I_i = \{1, 2, \dots, u\}$ 。同时, 不失一般性地定义 $I'_i = I_i / \{1\}$ 。对于 $j \in I_i / I'_i$, 选取 $\rho_{i,j} \in {}_R \mathbf{Z}_p$, 计算 $B_{10,i,j} = h^{\rho_{i,j}}$ 。对于 $j \in I'_i$, 选取 $\tilde{c}_{i,j}, z_{i,j} \in {}_R \mathbf{Z}_p$, 计算 $B_{10,i,j} = Y_{i,j}^{\tilde{c}_{i,j}} h^{\tilde{c}_{i,j}}$ 。

2) P 向 V 发送 $(B_1, B_2, \dots, B_9, \{B_{10,i,j}\}_{i \in [1,n], j \in [1,u]})$ 。 V 返回挑战 $\tilde{c} \in {}_R \mathbf{Z}_p$, P 在 \mathbf{Z}_p 上计算

$$\begin{aligned} z_{\tilde{y}'} &= \rho_{\tilde{y}'} + \tilde{c}y', \quad z_{usk} = \rho_{usk} + \tilde{c}usk, \quad z_B = \rho_B + \tilde{c}B, \\ z_{\tilde{s}} &= \rho_{\tilde{s}} + \tilde{c}s, \quad z_{k_1} = \rho_{k_1} + \tilde{c}k_1, \quad z_{k_2} = \rho_{k_2} + \tilde{c}k_2, \\ z_{-e} &= \rho_{-e} + \tilde{c}(-e), \quad z_{k_1e} = \rho_{k_1e} + \tilde{c}k_1e, \\ z_{k_2e} &= \rho_{k_2e} + \tilde{c}k_2e, \quad z_y = \rho_y + \tilde{c}y, \quad z_{k_3} = \rho_{k_3} + \tilde{c}k_3, \\ z_{k_4} &= \rho_{k_4} + \tilde{c}k_4, \quad z_{-\tilde{e}} = \rho_{-\tilde{e}} + \tilde{c}(-\tilde{e}), \quad z_{k_3\tilde{e}} = \rho_{k_3\tilde{e}} + \tilde{c}k_3\tilde{e}, \\ z_{k_4\tilde{e}} &= \rho_{k_4\tilde{e}} + \tilde{c}k_4\tilde{e}, \quad z_{\tilde{y}} = \rho_{\tilde{y}} + \tilde{c}\tilde{y}, \\ \{z_{s_j}\} &= \rho_{s_j} + \tilde{c}s_j \}_{j \in I' / s_{i_1}}, \\ \{z_{n_j}\} &= \rho_{n_j} + \tilde{c}n_j \}_{j \in [1, f] / I}, \quad z_r = \rho_r + \tilde{c}r, z_{r'} = \rho_{r'} + \tilde{c}r' \end{aligned}$$

对于 $i = 1, 2, \dots, n$, P 采用如下方式定义 \mathbf{Z}_p 上的度数为 $u - 1$ 的多项式 $f_i(\cdot)$ 。方法是, 设置 $f_i(0) = \tilde{c}$, $f_i(j) = \tilde{c}_{i,j}, j \in I'_i$ 。在完成对 $f_i(\cdot)$ 的构造之后, 设置 $\tilde{c}_{i,j} = f_i(j), z_{i,j} = \rho_{i,j} + \tilde{c}_{i,j}r_i, j \in I_i / I'_i$ 。最后, 向 V 发送 $(z_{\tilde{y}'}, z_{usk}, z_B, z_{\tilde{s}}, z_{k_1}, z_{k_2}, z_{-e}, z_{k_1e}, z_{k_2e}, z_{\tilde{y}}, z_{k_3}, z_{k_4}, z_{-\tilde{e}}, z_{k_3\tilde{e}}, z_{k_4\tilde{e}}, z_{\tilde{y}})$, $\{z_{s_j}\}_{j \in I' / s_{i_1}}, \{z_{n_j}\}_{j \in [1, f] / I}, z_r, z_{r'}, \{f_i(\cdot), z_{i,j}\}_{i \in [1, n], j \in [1, u]}$ 。

5) V 验证是否满足 $g^v = E/E'$ 以及

$$\begin{aligned} B_1 &= g_0^{\tilde{x}''} g_{i,1}^{\tilde{z}_{usk}} g_{i,2}^{\tilde{z}_s} g_{i,3}^{\tilde{z}_B} C^{-\tilde{c}}, \quad B_2 = g^{\tilde{x}_1} h^{\tilde{x}_2} A_2^{-\tilde{c}}, \\ B_3 &= A_2^{\tilde{z}-\tilde{e}} g^{\tilde{x}_1e} h^{\tilde{x}_2e}, \\ B_4 &= \hat{e}(A_1, h_0)^{\tilde{z}-\tilde{e}} \hat{e}(g, w)^{\tilde{x}_2} \hat{e}(g, h_0)^{\tilde{x}_2} \hat{e}(g_{i,1}, h_0)^{\tilde{x}_1} \\ &\quad \left(\frac{\hat{e}(A_1, w)}{\hat{e}(g, h_0) \hat{e}(g_{i,2}, h_0)^{s_{i_1}}} \right)^{-\tilde{c}}, \\ B_5 &= g^{\tilde{x}_3} h^{\tilde{x}_4} A_4^{-\tilde{c}}, \quad B_6 = A_4^{\tilde{z}-\tilde{e}} g^{\tilde{x}_3e} h^{\tilde{x}_4e}, \\ B_7 &= \hat{e}(g_0, h_0)^{\tilde{x}_5} \hat{e}(\tilde{g}_0, h_0)^{\tilde{x}_{usk}} \prod_{j \in I' / s_{i_1}} \hat{e}(\tilde{g}_j, h_0)^{\tilde{x}_j} \prod_{j \in [1, f] / I} \hat{e}(\tilde{g}_j, h_0)^{\tilde{x}_{nj}} \hat{e}(A_3, h_0)^{\tilde{z}-\tilde{e}} \hat{e}(g, w)^{\tilde{x}_4} \hat{e}(g, h_0)^{\tilde{x}_4e} \\ &\quad \left(\frac{\hat{e}(A_3, w)}{\hat{e}(g, h_0) \hat{e}(\tilde{g}_{i,1}, h_0)^{s_{i_1}}} \right)^{-\tilde{c}}, \\ B_8 &= g^{\tilde{x}B} h^{\tilde{x}r} E^{-\tilde{c}}, \\ B_9 &= h^{\tilde{x}r'} \left(\left(\prod_{i \in [1, n]} e_i^{u_i-1} \right) (E')^{-1} \right)^{-\tilde{c}}, \\ \{B_{10,i,j}\} &= h^{z_i, j} Y_{i,j}^{f_i(j)} \}_{i \in [1, n], j \in [1, u]} \end{aligned}$$

2.2 将 π_2 增强为完全零知识的知识证明协议

在这一步, V (即服务供应商) 与 P (即用户) 顺序执行 Σ 子协议 π_2' 与 π_2'' 。首先, V 预先选取自己在子协议 π_2'' 中的挑战 \tilde{c} 。在 π_2' 中, V 充当证明者, 且 P 充当验证者。 π_2' 的作用是 V 向 P 证明自己产生了对挑战 \tilde{c} 的承诺 $(R_1, R_2, \dots, R_9, \{R_{10,i,j}\}_{i \in [1, n], j \in [1, u]})$ 。然后, P 与 V 执行子协议 π_2'' 。 π_2'' 的作用是 P 证明自己或者掌握该承诺的另一种打开方式, 或者掌握“访问服务”协议要求的那些秘密元素。在 π_2'' 中, P 充当证明者, 且 V 充当验证者。通过将 π_2' 的第 2, 3 轮与 π_2'' 的第 1, 2 轮合并, 可以获得如下的满足完全零知识性的 4 轮知识证明协议。

1) Round₁: V 预先选取证明 π_2'' 中的挑战 $\tilde{c} \in {}_R \mathbf{Z}_p$, 选取 $z_{\tilde{y}'}, z_{usk}, z_B, z_{\tilde{s}}, z_{k_1}, z_{k_2}, z_{-e}, z_{k_1e}, z_{k_2e}, z_y, z_{k_3}, z_{k_4}, z_{-\tilde{e}}, z_{k_3e}, z_{k_4e}, z_{\tilde{y}}, \{z_{s_j}\}_{j \in I' / s_{i_1}}, \{z_{n_j}\}_{j \in [1, f] / I}, z_r, z_{r'}, \{z_{i,j}\}_{i \in [1, n], j \in [1, u]} \in {}_R$

\mathbf{Z}_p 同时, V 以任意方式定义 \mathbf{Z}_p 上的度数为 $u - 1$ 的多项式 $\{f_i(\cdot)\}_{i \in [1, n]}$ 。然后, 向 P 发送 $(R_1, R_2, \dots, R_9, \{R_{10,i,j}\}_{i \in [1, n], j \in [1, u]})$ 以及自己在证明 π_2' 中的承诺 $(B_1, B_2, \dots, B_9, \{B_{10,i,j}\}_{i \in [1, n], j \in [1, u]})$, 其中

$$\begin{aligned} \pi_2' &= PK\{(\tilde{c}, z_{\tilde{y}'}, z_{usk}, z_B, z_{\tilde{s}}, z_{k_1}, z_{k_2}, z_{-e}, z_{k_1e}, z_{k_2e}, z_y, z_{k_3}, z_{k_4}, z_{-\tilde{e}}, \\ &\quad z_{k_3e}, z_{k_4e}, z_{\tilde{y}}, \{z_{s_j}\}_{j \in I' / s_{i_1}}, \{z_{n_j}\}_{j \in [1, f] / I}, z_r, z_{r'}), \\ &\quad \{f_i(\cdot), z_{i,j}\}_{i \in [1, n], j \in [1, u]}) : R_1 = \\ &\quad g_0^{\tilde{x}'} g_{i,1}^{\tilde{z}_{usk}} g_{i,2}^{\tilde{z}_s} g_{i,3}^{\tilde{z}_B} C^{-\tilde{c}} \wedge R_2 = g^{\tilde{x}_1} h^{\tilde{x}_2} A_2^{-\tilde{c}} \wedge R_3 = \\ &\quad A_2^{\tilde{z}-\tilde{e}} g^{\tilde{x}_1e} h^{\tilde{x}_2e} \wedge R_4 = \hat{e}(A_1, h_0)^{\tilde{z}-\tilde{e}} \hat{e}(g, w)^{\tilde{x}_2} \\ &\quad \hat{e}(g, h_0)^{\tilde{x}_2} \hat{e}(g_{i,1}, h_0)^{\tilde{x}_1} \hat{e}(g_{i,2}, h_0)^{\tilde{x}_2} \hat{e}(g_{i,3}, h_0)^{\tilde{x}_3} \hat{e}(g_{i,4}, h_0)^{\tilde{x}_4} \\ &\quad \left(\frac{\hat{e}(A_1, w)}{\hat{e}(g, h_0) \hat{e}(g_{i,4}, h_0)^{s_{i_1}}} \right)^{-\tilde{c}} \wedge R_5 = g^{\tilde{x}_3} h^{\tilde{x}_4} A_4^{-\tilde{c}} \wedge \\ &\quad R_6 = A_4^{\tilde{z}-\tilde{e}} g^{\tilde{x}_3e} h^{\tilde{x}_4e} \wedge R_7 = \hat{e}(g_0, h_0)^{\tilde{x}_5} \hat{e}(\tilde{g}_0, h_0)^{\tilde{x}_{usk}} \\ &\quad \prod_{j \in I' / s_{i_1}} \hat{e}(\tilde{g}_j, h_0)^{\tilde{x}_j} \prod_{j \in [1, f] / I} \hat{e}(\tilde{g}_j, h_0)^{\tilde{x}_{nj}} \hat{e}(A_3, h_0)^{\tilde{z}-\tilde{e}} \\ &\quad \hat{e}(g, w)^{\tilde{x}_4} \hat{e}(g, h_0)^{\tilde{x}_4e} \left(\frac{\hat{e}(A_3, w)}{\hat{e}(g, h_0) \hat{e}(\tilde{g}_{i,1}, h_0)^{s_{i_1}}} \right)^{-\tilde{c}} \wedge \\ &\quad R_8 = g^{\tilde{x}B} h^{\tilde{x}r} E^{-\tilde{c}} \wedge R_9 = h^{\tilde{x}r'} \left(\left(\prod_{i \in [1, n]} e_i^{u_i-1} \right) (E')^{-1} \right)^{-\tilde{c}} \wedge \\ &\quad \{R_{10,i,j}\} = h^{z_i, j} Y_{i,j}^{f_i(j)} \}_{i \in [1, n], j \in [1, u]} \end{aligned}$$

2) Round₂: P 选取在证明 π_2' 中的挑战 $\tilde{k} \in {}_R \mathbf{Z}_p$, 向 V 发送 \tilde{k} 以及自己在证明 π_2'' 中的承诺

$$(B_1', B_2', \dots, B_9', \{B_{10,i,j}'\}_{i \in [1, n], j \in [1, u]}),$$

$$(B_1'', B_2'', \dots, B_9'', \{B_{10,i,j}''\}_{i \in [1, n], j \in [1, u]})$$

其中

$$\begin{aligned} \pi_2'' &= PK\{(\tilde{c}', z_{\tilde{y}'}, z_{usk}', z_B', z_{\tilde{s}}', z_{k_1}', z_{k_2}', z_{-e}', z_{k_1e}', \\ &\quad z_{k_2e}', z_{\tilde{y}}', z_{k_3}', z_{k_4}', z_{-e}', z_{k_3e}', z_{k_4e}', z_{\tilde{y}}', \{z_{s_j}'\}_{j \in I' / s_{i_1}}', \\ &\quad \{z_{n_j}'\}_{j \in [1, f] / I}, z_r', z_{r'}, \{f_i(\cdot)', z_{i,j}'\}_{i \in [1, n], j \in [1, u]}'), \\ &\quad (\tilde{y}', usk, B, \bar{s}, k_1, k_2, -e, k_1e, k_2e, y, k_3, k_4, -\tilde{e}, \\ &\quad k_3\tilde{e}, k_4\tilde{e}, \tilde{y}, \{s_j\}_{j \in I' / s_{i_1}}, \{n_j\}_{j \in [1, f] / I}, r, r', \\ &\quad \{r_i\}_{i=1,\dots,n}) : statement_1 \vee statement_2 \} \end{aligned}$$

具体地, $statement_1$ 的表达式为:

$$\begin{aligned} R_1 &= g_0^{\tilde{x}'} g_{i,1}^{\tilde{z}_{usk}} g_{i,2}^{\tilde{z}'} g_{i,3}^{\tilde{z}_s} C^{-\tilde{c}'} \wedge R_2 = g^{\tilde{x}_1} h^{\tilde{x}_2} A_2^{-\tilde{c}'} \wedge \\ &\quad R_3 = A_2^{\tilde{z}-\tilde{e}'} g^{\tilde{x}_1e} h^{\tilde{x}_2e} \wedge R_4 = \hat{e}(A_1, h_0)^{\tilde{z}-\tilde{e}'} \\ &\quad \hat{e}(g, w)^{\tilde{x}_2} \hat{e}(g, h_0)^{\tilde{x}_2} \hat{e}(g_{i,1}, h_0)^{\tilde{x}_1} \hat{e}(g_{i,2}, h_0)^{\tilde{x}_2} \hat{e}(g_{i,3}, h_0)^{\tilde{x}_3} \\ &\quad \hat{e}(g_{i,4}, h_0)^{\tilde{x}_4} \left(\frac{\hat{e}(A_1, w)}{\hat{e}(g, h_0) \hat{e}(g_{i,4}, h_0)^{s_{i_1}}} \right)^{-\tilde{c}'} \wedge R_5 = \\ &\quad g^{\tilde{x}_3} h^{\tilde{x}_4} A_4^{-\tilde{c}'} \wedge R_6 = A_4^{\tilde{z}-\tilde{e}'} g^{\tilde{x}_3e} h^{\tilde{x}_4e} \wedge R_7 = \\ &\quad \hat{e}(g_0, h_0)^{\tilde{x}_5} \hat{e}(\tilde{g}_0, h_0)^{\tilde{x}_{usk}'} \prod_{j \in I' / s_{i_1}} \hat{e}(\tilde{g}_j, h_0)^{\tilde{x}_j} \\ &\quad h_0)^{\tilde{x}_j'} \prod_{j \in [1, f] / I} \hat{e}(\tilde{g}_j, h_0)^{\tilde{x}_j'} \hat{e}(A_3, h_0)^{\tilde{z}-\tilde{e}'} \hat{e}(g, w)^{\tilde{x}_4} \\ &\quad \hat{e}(g, h_0)^{\tilde{x}_4e} \left(\frac{\hat{e}(A_3, w)}{\hat{e}(g, h_0) \hat{e}(\tilde{g}_{i,1}, h_0)^{s_{i_1}}} \right)^{-\tilde{c}'} \wedge \\ &\quad R_8 = g^{\tilde{x}B} h^{\tilde{x}r'} E^{-\tilde{c}'} \wedge R_9 = \\ &\quad h^{\tilde{x}r'} \left(\left(\prod_{i \in [1, n]} e_i^{u_i-1} \right) (E')^{-1} \right)^{-\tilde{c}'} \wedge \{R_{10,i,j}\} = \\ &\quad h^{z_i, j} Y_{i,j}^{-f_i(j)} \}_{i \in [1, n], j \in [1, u]} \end{aligned}$$

$statement_2$ 的表达式为:

$$\begin{aligned} C &= g_0^{\tilde{x}'} g_{i,1}^{\tilde{z}_{usk}} g_{i,2}^{\tilde{z}'} g_{i,3}^{\tilde{z}_s} \wedge A_2 = g^{\tilde{x}_1} h^{\tilde{x}_2} \wedge 1 = A_2^{-\tilde{e}} g^{\tilde{x}_1e} h^{\tilde{x}_2e} \wedge \\ &\quad \frac{\hat{e}(A_1, w)}{\hat{e}(g, h_0) \hat{e}(g_{i,3}, h_0)^s} = \hat{e}(A_1, h_0)^{-\tilde{e}} \hat{e}(g, w)^{\tilde{x}_2} \\ &\quad \hat{e}(g, h_0)^{\tilde{x}_2} \hat{e}(g_{i,1}, h_0)^{\tilde{x}_1} \hat{e}(g_{i,2}, h_0)^{\tilde{x}_2} \hat{e}(g_{i,3}, h_0)^{\tilde{x}_3} \wedge A_4 = \end{aligned}$$

$$\begin{aligned} g^{k_3} h^{k_4} \wedge 1 &= A_4^{-\tilde{e}} g^{k_3 \tilde{e}} h^{k_4 \tilde{e}} \wedge \frac{\hat{e}(A_3, w)}{\hat{e}(g, h_0) \hat{e}(\tilde{g}_{i,1}, h_0)^{s_{i_1}}} = \\ \hat{e}(g_0, h_0) \tilde{y} \hat{e}(\tilde{g}_0, h_0) &\stackrel{usk}{\prod} \prod_{j \in I \setminus \{s_{i_1}\}} \hat{e}(\tilde{g}_j, h_0)^{s_j} \\ \prod_{j \in [1, J] \setminus I} \hat{e}(\tilde{g}_j, h_0) &{}^{s_j} \hat{e}(A_3, h_0) {}^{-\tilde{e}} \hat{e}(g, w)^{k_4} \hat{e}(g, h_0)^{k_4 \tilde{e}} \wedge \\ E &= g^B h^r \wedge \left(\prod_{i \in [1, n]} e_i^{u_i - 1} \right) (E')^{-1} = \\ h'^r \wedge \bigwedge_{i \in [1, n]} (Y_{i,1} &= h'^i \vee Y_{i,2} = h'^i \vee \cdots \vee Y_{i,u} = h'^i) \end{aligned}$$

在证明 π_2'' 中, 声明 $statement_1$ 部分是根据 $(R_1, R_2, \dots, R_9, \{R_{10, i, j}\}_{i \in [1, n], j \in [1, u]})$ 以模拟方式产生的, 而声明 $statement_2$ 部分是采用诚实方式产生的。

3) Round₃: V 返回预先选取的证明 π_2'' 中的挑战 \bar{c} 以及以诚实方式产生的证明 π_2' 中的应答 $(\xi_{z_y}, \xi_{z_{usk}}, \xi_{z_B}, \xi_{z_s}, \xi_{z_h}, \xi_{z_k}, \xi_{z_{-e}}, \xi_{z_{k1}}, \xi_{z_{k2}}, \xi_{z_j}, \xi_{z_{k3}}, \xi_{z_{k4}}, \xi_{z_{-e}}, \xi_{z_{k5}}, \xi_{z_{k6}}, \xi_{z_{-e}}, |\xi_{z_{-j}}|, j \in U \setminus \{i_1\})$ 以及 $(\{\xi_{z_{n_j}}\}_{j \in [1, f] \setminus I}, \xi_{z_r}, \xi_{z_r}, \{\xi_{f(j)}\}, \xi_{z_{i,j}} | i \in [1, n], j \in [1, u])$ 。

4) Round₄: P 验证 $(B_1, B_2, \dots, B_9, \{B_{10,i,j}\}_{i \in [1,n], j \in [1,u]}, \tilde{c}, \xi_{z_{\tilde{y}}}, \xi_{z_{usk}}, \xi_{z_B}, \xi_{z_s}, \xi_{z_{k_1}}, \xi_{z_{k_2}}, \xi_{z_{-e}}, \xi_{z_{k_1e}}, \xi_{z_{k_2e}}, \xi_{z_y}, \xi_{z_{k_3}}, \xi_{z_{k_4}}, \xi_{z_{-e}}, \xi_{z_{k_3e}}, \xi_{z_{k_4e}}, \xi_{z_{\tilde{y}}}, \{\xi_{z_{s_j}}\}_{j \in I \setminus \{s_{i+1}\}}, \{\xi_{z_{n_j}}\}_{j \in [1,n] \setminus I}, \xi_{z_r}, \xi_{z_r}, \{\xi_{f_i(j)}, \xi_{z_{i,j}}\}_{i \in [1,n], j \in [1,u]})$ 是否为证明 π_2' 的可接受副本, 若是, 则将 \tilde{c} 视为 V 在 π_2'' 中的挑战。然后, 向 V 返回自己在 π_2'' 中的应答 ($response_1, response_2$)。 $response_1$ 是模拟产生的, 而 $response_2$ 是采用诚实方式产生的, 即

$$\begin{aligned}
\text{response}_1 &= (\bar{c}_1, \xi_{z_y}'', \xi_{z_{usk}}'', \xi_{z_B}'', \xi_{z_{\bar{e}}}'' , \xi_{z_{k_1}}'', \xi_{z_{k_2}}'', \xi_{z_{-e}}'', \\
&\quad \xi_{z_{k_1e}}'', \xi_{z_{k_2e}}'', \xi_{z_y}', \xi_{z_{k_3}}', \xi_{z_{k_4}}', \xi_{z_{-\bar{e}}}', \xi_{z_{k_3e}}', \xi_{z_{k_4e}}', \xi_{z_{\bar{y}}}'', \\
&\quad \{\xi_{z_{i_j}}'\}_{j \in V|s_{i_1}|}, \{\xi_{z_{n_j}}'\}_{j \in [1, f]/I}, \xi_{z_r}'', \xi_{z_{r'}}'', \\
&\quad \{\xi_{f_i(j)}'\}, \xi_{z_{i,j}}'' \}_{i \in [1, n], j \in [1, u]}) \\
\text{response}_2 &= (\bar{c}_2, z_{\bar{y}}'', z_{usk}'', z_B'', z_s'', z_{k_1}'', z_{k_2}'', z_{-e}'', \\
&\quad z_{k_1e}'', z_{k_2e}'', z_{\bar{y}}'', z_{k_3}'', z_{k_4}'', z_{-\bar{e}}'', z_{k_3e}'', \\
&\quad z_{k_4e}'', z_{\bar{y}}'', \{z_{i_j}\}_{j \in V|s_{i_1}|}, \{z_{n_j}\}_{j \in [1, f]/I}, z_r'', z_{r'}'', \\
&\quad \{f_i(\cdot)\}, z_{i,j}'' \}_{i \in [1, n], j \in [1, u]})
\end{aligned}$$

同时, V 据此验证声明 $statement_1$ 与 $statement_2$ 是否成立, 以及是否满足 $\tilde{c}_1 \oplus \tilde{c}_2 \equiv \tilde{c}_0$

引理 π_2 是满足完全零知识的知识证明协议。

证明 首先证明 $\bar{\pi}_2$ 满足知识证明性质。为此,可以构造知识提取器 Ext 。 Ext 采用以下策略与可能为恶意的证明者 P^* 执行交互,并且自行充当诚实的验证者。在 Round₁ ~ Round₃ 部分, Ext 根据协议 π_2' 的要求自行产生关于承诺 $(R_1, R_2, \dots, R_9, \{R_{10, i, j}\}_{i \in [1, n], j \in [1, u]})$ 的一种打开方式。在 Round₄ ~ Round₄ 部分的末尾, Ext 对 P^* 执行重绕。根据 Cramer 等^[11] 的结论,可以在多项式时间内出现以下两种情况之一。情况 1): Ext 提取出承诺 $(R_1, R_2, \dots, R_9, \{R_{10, i, j}\}_{i \in [1, n], j \in [1, u]})$ 的另外一种打开方式,由于这些承诺是根据底层 Σ 协议 π_2 的验证等式构造的,因此 Ext 可以采用标准技术提取出所期望的秘密知识 $(\bar{y}', usk, \dots, \{r_i\}_{i=1,2,\dots,n})$; 情况 2): Ext 能直接提取出所期望的秘密知识 $(\bar{y}', usk, \dots, \{r_i\}_{i=1,2,\dots,n})$ 。

为了证明 $\bar{\pi}_2$ 满足完全零知识性, 可以构造模拟器 Sim 。
 Sim 并不掌握任何的秘密知识, 而是采用以下策略与可能为恶意的验证者 V^* 执行如下交互, 并且自行充当诚实的证明者。在 $Round_1 \sim Round_3$ 部分的末尾, Sim 对 V^* 执行重绕。在多项式时间内, Sim 可以提取出由 V^* 产生的关于承诺 $(R_1, R_2, \dots, R_9, \{R_{10, i, j}\}_{i \in [1, n], j \in [1, u]})$ 的一种打开方式。此后, 在 $Round_4$ 中, Sim 向 V^* 提供 \tilde{c}_1 以及以诚实方式产生的关于 π_1 的一种打开方式。

中 $statement_1$ 部分的应答, 同时提供 \tilde{c}_2 以及自己预先模拟产生的关于 π_2 ”中部分 $statement_2$ 的应答, 其中 $\tilde{c}_1 = \tilde{c} \oplus \tilde{c}_2$ 。

3 本文系统的安全性分析

定理 在群 (G_1, G_2) 上的 q -SDH (the q -Strong Diffie-Hellman) 假设和群 G_1 上的离散对数假设下, 本文系统是可证满足 Canard 等^[1] 要求的正确性、紧凑性、可靠性和匿名性。

证明 采用标准技术,不难验证账户注册、订购、访问服务、追加订购、充值和余额转移协议都是正确的,即只要用户(U)与服务供应商(SP)遵守协议,就能成功完成相应的子协议。此外,本文系统同样满足紧湊性,因为支付令牌的规模独立于 U 的账户余额,同时订购证书的规模独立于 U 订购的服务数量。下面,详细证明本文系统的可靠性和匿名性。

1) 可靠性。定义如下的在攻击者 Adv 和归约算法 B 间执行的可靠性实验。 Adv 在实验中充当欺诈用户, B 则充当诚实的服务供应商。最初, B 获得给定的双线性参数 $(p, G_1, G_2, G_T, g_0, h_0, \hat{e}, \psi)$ 和证书签名方案^[12-13] 的公钥 w 。以此为基础, B 自行产生 PK 中的其他元素。 B 初始化计数器 $W_1 = 0, W_2 = 0$ 和集合 $Query = \{\}$ 。 B 向 Adv 提供 PK 并且回答 Adv 提出的如下的预言询问:

账户注册询问 在该询问中, B 利用协议 π_0 的提取器 Ext_0 获得 Adv 的秘密知识 (usk, y', s) , 并且向底层的证书签名预言机 $O_x(\cdot)$ 提出询问 (usk, s) , 在获得签名 (A, e, y) 后, 向 Adv 返回 $(A, e, y'' = y - y')$ 。此外, B 在 $Query$ 中保存 $((usk, s), (A, e, y))$, 设置 $W_1 = W_1 + D_0$ 。

订购询问 在该询问中, B 利用协议 $\bar{\pi}_1$ 的提取器 Ext_1 获得 Adv 的秘密知识 (\tilde{y}', usk) , 并且向签名预言机 $O_s(\cdot)$ 提出询问 $(usk, \{s_j\}_{j \in I}, \{n_j\}_{j \in [1, f] \setminus I})$, 在获得签名 $(\tilde{A}, \tilde{e}, \tilde{y})$ 后, 向 Adv 返回 $(\tilde{A}, \tilde{e}, \tilde{y}'' = \tilde{y} - \tilde{y}')$ 。此外, B 在 $Query$ 中保存 $((usk, \{s_i\}_{i \in I}, \{n_i\}_{i \in [1, f] \setminus I}), (\tilde{A}, \tilde{e}, \tilde{y}))$ 。

访问服务询问 在该询问中, B 利用协议 $\bar{\pi}_2$ 的提取器 Ext_2 获得 Adv 的秘密知识 $(\bar{y}', usk, B, \bar{s})$ 。此外, B 还能提取出关于秘密元组 $(usk, \{s_j\}_{j \in I}, \{n_j\}_{j \in [1, f] \setminus I})$ 的签名 $(\bar{A}, \bar{e}, \bar{y})$ 。 B 检查是否满足 $((usk, \{s_j\}_{j \in I}, \{n_j\}_{j \in [1, f] \setminus I}), (\bar{A}, \bar{e}, \bar{y})) \in Query$, 若否, 则终止执行。 B 向签名预言机 $O_x(\cdot)$ 提出询问 $(usk, \bar{B} = B - v, \bar{s})$, 在获得签名 $(\bar{A}, \bar{e}, \bar{y})$ 后, 向 Adv 返回 $(A, e, \bar{y}'' = \bar{y} - \bar{y}')$ 。此外, B 在 $Query$ 中保存 $((usk, \bar{B}, \bar{s}), (\bar{A}, \bar{e}, \bar{y}))$, 设置 $W_2 = W_2 + v$ 。

追加订购询问 在该询问中, B 利用协议 $\bar{\pi}_3$ 的提取器 Ext_3 获得 Adv 的秘密知识 (\bar{y}', usk) , 并且向签名预言机 $O_x(\cdot)$ 提出询问 $(usk, \{s_j\}_{j \in I}, \{n_j\}_{j \in [1, f] \setminus I})$, 在获得签名 $(\bar{A}, \bar{e}, \bar{y})$ 后, 向 Adv 返回 $(\bar{A}, \bar{e}, \bar{y}'' = \bar{y} - \bar{y}')$ 。此外, B 在 $Query$ 中保存 $((usk, \{s_j\}_{j \in I}, \{n_j\}_{j \in [1, f] \setminus I}), (\bar{A}, \bar{e}, \bar{y}))$ 。

充值询问 在该询问中, B 利用协议 π_4 的提取器 Ext_4 获得 Adv 的秘密知识 $(usk, \bar{y}', B, \bar{s})$, 并且向底层的签名预言机 $O_s(\cdot)$ 提出询问 $(usk, \bar{B} = B + v, \bar{s})$, 在获得签名 $(\bar{A}, \bar{e}, \bar{y})$ 后, 向 Adv 返回 $(\bar{A}, e, y'' = \bar{y} - y')$ 。此外, B 在 $Query$ 中保存 $((usk, \bar{B}, \bar{s}), (\bar{A}, \bar{e}, \bar{y}))$, 设置 $W_1 = W_1 + v$ 。

余额转移询问 在该询问中, B 利用协议 π_s 的提取器 Ext_s , 获得 Adv 的秘密知识 $(usk, \bar{y}', B, \bar{s})$, 并且向签名预言机

$O_x(\cdot)$ 提出询问 (usk, B, \bar{s}) , 在获得签名 $(\bar{A}, \bar{e}, \bar{y})$ 后, 向 Adv 返回 $(\bar{A}, \bar{e}, \bar{y}'' = \bar{y} - \bar{y}')$ 。此外, B 在 $Query$ 中保存 $((usk, B, \bar{s}), (\bar{A}, \bar{e}, \bar{y}))$ 。

由于 Adv 借助 B 而间接向预言机 $O_x(\cdot)$ 提出的询问次数是受限制的, 因此上述游戏在有限次交互后结束。 Adv 在两种情况下获胜: 1) 满足 $W_2 > W_1$, 即在 Adv 游戏中支付的金额超过它通过付费而向账户中充入的金额, 表明 Adv 成功实现了对底层证书签名的伪造或攻破了底层准确区间证明协议^[14]的可靠性, 即违背了 q -SDH 假设或离散对数假设。2) B 在访问服务询问中终止执行, 表明 Adv 成功实现了对底层证书签名的伪造, 即违背了 q -SDH 假设。

2) 匿名性。定义如下的在攻击者 Adv 和归约算法 B 间执行的匿名性实验。 Adv 在实验中充当欺诈的服务供应商, B 则充当诚实用户。最初, Adv 自行产生 PK 中的所有元素。 B 向 Adv 请求 PK 并且回答 Adv 提出的账户注册(订购、访问服务、追加订购、充值、余额转移)询问。在相应的询问中, Adv 提供 $b \in_R \{0, 1\}$, 且 B 以诚实用户 U_b 的身份与 Adv 进行交互。

在挑战阶段, Adv 提出订购(访问服务、追加订购、充值、余额转移)询问。只要用户 U_0 与 U_1 均符合执行订购(访问服务、追加订购、充值、余额转移)协议的条件, B 就选取 $b' \in_R \{0, 1\}$, 并且以 $U_{b'}$ 的身份与 Adv 执行对应的协议。需要强调的是, 在执行相应的证明 $\bar{\pi}_1(\bar{\pi}_2, \bar{\pi}_3, \bar{\pi}_4, \bar{\pi}_5)$ 时, B 借助相应证明的零知识模拟器完成证明, 从而确保 Adv 并未在相应的证明过程中获得有关用户身份 b' 的任何信息。最终, 若 Adv 能正确猜中 b' 的取值, 则判定其获胜。显然, Adv 的获胜概率仅为 $1/2$ 。

4 本文系统的性能分析

相对于已有系统, 本文系统同时满足多个更具有吸引力的性质。在表1中对本文系统与已有的典型系统进行了安全

性质的对比。需要强调的是, 为了防止用户通过与他人共享令牌而损害服务供应商的商业利益, 需要提供令牌的不可分割性保护。文献[1-2, 4, 6]系统仅实现了弱不可分割性^[15], 然而当用户愿意将自己的令牌副本提供给他人时, 此类保护将失效。相反, 本文系统满足更理想的强不可分割性^[15], 即一旦共享令牌的其他用户获得了更新后的令牌, 则作为令牌原始拥有者的用户将无法继续使用自己的令牌。在匿名性保护方面, 存在无匿名性(即可关联)、可撤销的匿名性、有条件的匿名性和完全匿名性这 4 个等级^[7]。其中, 可撤销的匿名性表明允许系统权威对用户的匿名性进行撤销, 有条件的匿名性表明只要用户保持诚实就能确保自己的匿名性。本文系统满足完全匿名性, 因为包括 SP 在内的任何人都无法将用户的行为与他最初的注册过程进行关联, 即使用户有欺诈行为(即企图对账户透支或使用失效的令牌), SP 也仅能拒绝提供服务而无法揭示其身份。在底层证明系统的零知识强度方面, 文献[1-5]系统仅满足较弱的诚实验证者零知识性(Honest Verifier Zero-Knowledge, HVZK), 文献[6]系统满足更强的计算上的零知识性(Computational Zero-Knowledge, CZK), 而本文系统则满足最强的完全零知识性(Perfect Zero-Knowledge, PZK)。此外, 在安全模型的比较中, 本文采用 RO(Random Oracle)表示需要作出理想假设的随机预言模型, 用 Standard 表示更加接近实际应用环境的标准模型。

为了分析本文系统的运行效率, 在表2中对 U 与 SP 在几个主要子协议中的通信量和运算量进行总结。

假设初始(最大)账户余额为 1000, SP 至多提供 10 项服务, u 取 4, 于是可以用 5 位 4 进制数表示账户余额。在通信量比较过程中, 符号 $|G_1|, |G_T|, |\mathbf{Z}_p|$ 分别表示 G_1, G_T, \mathbf{Z}_p 上元素的比特长度, 符号 Exp_{G_1}, Exp_{G_T} 分别表示执行 1 次 G_1, G_T 上指数运算的耗费, 且 P 表示执行 1 次对运算的耗费。假设 U 与 SP 采用了双线性对的预先计算技术。

表1 各系统安全性质对比

系统	类型	支持多服务订购	支持令牌过期	支持账户充值	不可分割性	匿名性等级	零知识强度	安全模型
文献[1]系统	I	是	否	否	弱	可撤销	HVZK	RO
文献[2]系统	I	否	否	否	弱	可关联	HVZK	RO
文献[3]系统	I	否	是	否	强	完全	HVZK	RO
文献[4]系统	II	否	否	否	弱	可撤销	HVZK	RO
文献[5]系统	II	否	是	否	—	完全	HVZK	RO
文献[6]系统	II	否	否	是	弱	有条件	CZK	Standard
本文系统	II	是	是	是	强	完全	PZK	Standard

表2 几个主要子协议的性能分析

协议	通信量		运算量	
	U	SP	U	SP
注册	$6 G_1 + 10 \mathbf{Z}_p $	$4 G_1 + 5 \mathbf{Z}_p $	$8Exp_{G_1}$	$8Exp_{G_1}$
订购	$9 G_1 + 2 G_T + 24 \mathbf{Z}_p $	$6 G_1 + 2 G_T + 12 \mathbf{Z}_p $	$12Exp_{G_1} + 3Exp_{G_T} + 2P$	$12Exp_{G_1} + 4Exp_{G_T} + 2P$
访问	$61 G_1 + 4 G_T + 159 \mathbf{Z}_p $	$54 G_1 + 4 G_T + 79 \mathbf{Z}_p $	$88Exp_{G_1} + 6Exp_{G_T} + 4P$	$108Exp_{G_1} + 8Exp_{G_T} + 4P$
充值	$57 G_1 + 2 G_T + 107 \mathbf{Z}_p $	$50 G_1 + 2 G_T + 53 \mathbf{Z}_p $	$82Exp_{G_1} + 3Exp_{G_T} + 2P$	$100Exp_{G_1} + 4Exp_{G_T} + 2P$

5 结语

对 Canard 等的多服务订购系统作出改进, 提出了一个无随机预言的完全匿名多服务订购系统。与已有的典型系统相比, 新系统同时满足三个实用性质, 即允许利用同一张令牌对多项服务进行访问, 支持令牌过期和允许用户以匿名方式向账户充值。此外, 新系统在令牌的不可分割性、用户的匿名性和

底层知识证明系统的零知识性方面提供了最强的安全保护。

参考文献:

- CANARD S, JAMBERT A. Untraceability and profiling are not mutually exclusive [C]// TrustBus 2010: Proceedings of the 7th International Conference on Trust, Privacy and Security in Digital Business, LNCS 6264. Berlin: Springer-Verlag, 2010: 117–128.

(下转第 429 页)

二叉树节点处类别的分离顺序,提高分类准确率。实验结果表明该算法不仅保持了较高的分类精度,还在训练速度上体现了一定优势,具有一定的实用价值。与其他分类方法一样,BT-TWSVM 算法的性能与核函数的选取有关,对核函数进行优化以提高分类效果将是今后的研究内容。另外,该方法仅在特定的数据集 KDDcup99 上进行了实验,对于真实网络环境中的动态数据是否同样适用也是今后的研究内容。

参考文献:

- [1] 饶鲜,董春曦,杨绍全.基于支持向量机的入侵检测系统[J].软件学报,2003,14(4):798-803.
- [2] HOMG S J, SU M Y, CHEN Y H, et al. A novel intrusion detection system based on hierarchical clustering and support vector machines [J]. Expert Systems with Applications, 2011, 38(1): 306 - 313.
- [3] AMBWANI T. Multi class support vector machine implementation to intrusion detection [C]// Proceedings of the International Joint Conference on Neural Networks. Washington, DC: IEEE Computer Society, 2003: 2300 - 2305.
- [4] XU X, WANG X N. An adaptive network intrusion detection method based on PCA and support vector machines [C]// Proceedings of the 1st International Conference on Advanced Data Mining and Applications. Berlin: Springer-Verlag, 2005: 696 - 703.
- [5] SHON T, SEO J, MOON J. SVM approach with a genetic algorithm for network intrusion detection [C]// Proceedings of the 20th International Symposium on Computer and Information Sciences. Berlin: Springer-Verlag, 2005: 224 - 233.
- [6] VAPNIK V N. Statistical learning theory [M]. Berlin: Springer-Verlag, 1998: 123 - 167.
- [7] HSU C W, LIN C J. A comparison of methods for multiclass support vector machines [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002, 24(2): 216 - 229.
- [8] WESTON J, WATKINS C. Multi-class support vector machines [C]// Proceedings of European Symposium on Artificial Neural Networks'99. Mobile, Alabama: Factor Press, 1999: 233 - 265.
- [9] PLATT J C, CRISTIANINI N, SHAWE-TAYLOR J. Large margin DAGs for multiclass classification [C]// NIPS'99: Proceedings of Neural Information Processing Systems. Cambridge: MIT Press, 2000: 547 - 553.
- [10] SUYKENS J A K, VANDEWALLE J. Least squares support vector machine classifiers [J]. Neural Processing Letters, 1999, 19(3): 293 - 300.
- [11] KUMAR M A, GOPAL M. Binary classification using linear SVM pyramidal tree [C]// Proceedings of the 2010 International Conference on Data Storage and Data Engineering. Washington, DC: IEEE Computer Society, 2010: 54 - 58.
- [12] JAYADEVA, KHECHANDANI R, CHANDRA S. Twin support vector machines for pattern classification [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2007, 29(5): 905 - 910.
- [13] MANGASARIAN O L, WILD E W. Multisurface proximal support vector machine classification via generalized eigenvalues [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2006, 28(1): 69 - 74.
- [14] 谢娟英,张兵权,汪万紫.基于双支持向量机的偏二叉树多类分类算法[J].南京大学学报:自然科学版,2011,47(4):354 - 363.
- [15] SHAO Y H, DENG N Y, YANG Z M, et al. Probabilistic outputs for twin support vector machines [J]. Knowledge-Based Systems, 2012, 33(9): 145 - 151.

(上接第 422 页)

- [2] FUJII A, OHTAKE G, HANAOKA G, et al. Anonymous authentication scheme for subscription services [C]// KES 2007: Proceedings of the 11th International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, LNCS 4694. Berlin: Springer-Verlag, 2007: 975 - 983.
- [3] BLANTON M. Online subscriptions with anonymous access [C]// ASIACCS 2008: Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2008: 217 - 227.
- [4] 柳欣,徐秋亮.实用的匿名订购协议[J].计算机工程与应用,2009,45(4):93-97.
- [5] VASCO M I G, HEIDARVAND S, VILLAR J L. Flexible anonymous subscription schemes [J]. Communications in Computer and Information Science, 2012, 222(5): 203 - 219.
- [6] 柳欣.满足增强安全性的匿名订购系统[J].计算机工程与应用,2012,48(17):16-22.
- [7] TSANG P P, AU M H, LIU J K, et al. A suite of non-pairing ID-based threshold ring signature schemes with different levels of anonymity [C]// ProVSec 2010: Proceedings of the 4th International Conference on Provable Security, LNCS 6402. Berlin: Springer-Verlag, 2010: 166 - 183.
- [8] HENRY R, OLUMOFIN F, GOLDBERG I. Practical PIR for electronic commerce [C]// CCS 2011: Proceedings of the 18th ACM Conference on Computer and Communications Security. New York: ACM, 2011: 677 - 690.

- [9] 贾小英,李宝,刘亚敏.随机预言模型[J].软件学报,2012, 23 (1): 140 - 151.
- [10] LIU J K, AU M H, SUSILO W, et al. Enhancing location privacy for electric vehicles (at the right time) [EB/OL]. [2012-08-01]. <http://eprint.iacr.org/2012/342>.
- [11] CRAMER R, DAMGÅRD I, MACKENZIE P. Efficient zero-knowledge proofs of knowledge without intractability assumptions [C]// PKC 2000: Proceedings of the 3rd International Workshop on Practice and Theory in Public Key Cryptography, LNCS 1751. Berlin: Springer-Verlag, 2000: 354 - 372.
- [12] AU M H, SUSILO W, MU Y. Electronic cash with anonymous user suspension [C]// ACISP 2011: Proceedings of the 16th Australasian Conference on Information Security and Privacy, LNCS 6812. Berlin: Springer-Verlag, 2011: 172 - 188.
- [13] AU M H. Contribution to privacy-preserving cryptographic techniques [D]. Wollongong, Australia: University of Wollongong, 2009.
- [14] PENG K, BAO F. Batch range proof for practical small ranges [C]// AFRICACRYPT 2010: Proceedings of the 3rd International Conference on Cryptology in Africa, LNCS 6055. Berlin: Springer-Verlag, 2010: 114 - 130.
- [15] ARMKNECHT F, ESCALANTE B A N, LÖHR H, et al. Secure multi-coupons for federated environments: privacy-preserving and customer-friendly [C]// ISPEC 2008: Proceedings of the 4th International Information Security Practice and Experience Conference, LNCS 4991. Berlin: Springer-Verlag, 2008: 29 - 44.