基于承诺的可验证公平性微支付

刘忆宁*①② 赵全玉①
①(桂林电子科技大学数学与计算科学学院 桂林 541004)
②(桂林电子科技大学广西可信软件重点实验室 桂林 541004)

摘 要：微支付交易具有交易量极大且单次交易额极小的特点，使得复杂的认证协议不适用于微支付。Micali 等人(2002)提出的基于概率选择微支付方案，把微支付聚合成宏支付，大幅提高了微支付的效率。Liu-Yan 在(2013)提出了保证所有参与者的数据融入概率选择结果的生成, 而且使得所有参与者可以验证结果的公平性。然而，Liu-Yan 方案中银行可能获得额外利益，从而破坏了协议的公平性。该文首先分析了 Liu-Yan 方案的安全威胁，并且以“1 个用户-1 个商家”的模型代替 Liu-Yan 方案中“大量用户-1 个商家”的模型，以数据承诺技术为基础保障结果的公平性与可验证性。

关键词：微支付；承诺；公平性；可验证性
中图分类号：TP309 **文献标识码**：A **文章编号**：11009-5896(2017)03-0743-06
DOI: 10.11999/JEIT160300

Verifiable Fairness Micropayment Scheme Based on Commitment

LIU Yining①② ZHAO Quanyu①
①(*School of Mathematics and Computational Science*, *Guilin University of Electronic Technology*, *Guilin* 541004, *China*)
②(*Guangxi Key Laboratory of Trusted Software*, *Guilin University of Electronic Technology*, *Guilin* 541004, *China*)

Abstract: Due to the large transaction number and tiny value in micropayment, it is not practical to authenticate each transaction. Micali *et al.* (2002) propose a lottery-based micropayment to integrate multiple micropayment to one macro-payment that is worth using complicated authentication. Liu-Yan scheme (2013) guarantees the result is verifiable by involving all participants' data. However, there still exists a flaw that the malicious bank maybe obtain the illegal benefit by controlling the specific purchaser not be selected to execute the macro-payment, moreover, this attack can not be detected. In this paper, the flaw is firstly described, then, an improved version is proposed. Specifically the model "multiple purchasers to 1 merchant"in Liu-Yan's scheme is replaced with a new model "1 purchaser to 1 merchant", which guarantees the fairness and verifiability for all using the commitment technique.

Key words: Micropayment; Commitment; Fairness; Verifiability

1 引言

电子支付方案是电子交易中实现各方支付信息正确、安全、保密进行的规则和约定，通常包含 3 方参与：用户(U)，商家(M)，银行(B)[1] 。电子支付方案分为宏支付和微支付方案，宏支付交易金额较大、安全性要求高，通常使用数字签名、公钥加密等实现安全性；微支付交易金额小、效率性要求高，支付金额甚至远远小于支付能耗的成本。微支付交易对效率性要求高，因此并不能照搬宏支付方案来实施。

微支付是实现电子交易实时支付的一种技术[2]，应用非常广泛，如流量收费，歌曲下载等。交易所需支付的金额小，如果每次交易都采用常规计费方式(身份认证等)代价太大。微支付交易在满足一定安全性前提下，要求交易过程尽量简单，通讯能耗尽量低。因此微支付的一些性质被提出，如：安全性[3−5]， 高效性[6−8]，隐私性[9]，公平性[10,11]等。

1997 年，Rivest 等人[12]提出基于 Payword 的高

收稿日期：2016-03-31；改回日期：2016-07-29；网络出版：2016-10-09
*通信作者：刘忆宁 ynliu@guet.edu.cn
基金项目：国家自然科学基金(61363069, 61301166, 61662016)，桂林电子科技大学研究生教育创新计划(2016YJCX44)，广西研究生教育创新计划(YCSZ2015149)
Foundation Items: The National Natural Science Foundation of China (61363069, 61301166, 61662016), The Innovation Project of GUET Graduate Education (2016YJCX44), The Innovation Project of Guangxi Graduate Education (YCSZ2015149)

效微支付方案，但在该方案中，商家无法聚合不同用户的微支付进行兑换。Rivest 基于概率选择的微支付[13]中，大量用户和商家共同选择一个用户支付账单，实现大量用户的微支付以较小概率转化成某一用户的宏支付，如：每次交易时 1000 个用户和商家共同选择一个用户，每个用户被选中的概率是 0.001，那么每个用户平均 1000 次交易中有一次被选中，被选中后需要支付之前的账单。但文献[13]存在两个弱点：(1)如何保证用户被选择的公平性；(2)如何防止用户超额支付。文献[14]提出 MR1, MR2, MR3。MR1 保证了用户和商家公平的选择用户，但存在用户超额支付的情况；MR2 解决了超额扣除用户金额的风险，但恶意用户和商家会合谋攻击银行；MR3 把计算中心转移到银行，但并未解决超额扣除的问题。另外在 MR2 和 MR3 中，用户使用私钥对每次交易进行签名并发送给商家，可能会泄露用户身份，破坏协议的隐私性。同时数字签名计算比 hash 链和对称加密更加复杂，影响在移动终端中的使用。

Liu-Yan(2013)提出一种基于 hash 函数[15,16]和插值多项式的微支付方案[17]。该方案使用插值多项式生成可验证性随机数来选择支付用户，保护了隐私性，降低了计算负担。但该方案存在安全威胁。银行可以定向的选择用户，谋取非法利益；另外，Liu-Yan 方案很难实现大量用户同步操作，而且用户数增加时，计算负担会大幅度增加。本文提出基于承诺的可验证公平性微支付方案，商家和用户利用承诺协同生成一个小概率的结果，而且用户可以验证这个结果的公平性，该方案不仅满足其他安全特性，还具有更好的公平性。

2 Liu-Yan 方案

2.1 Liu-Yan 方案

在 Liu-Yan 方案中，有 3 个参与者：用户(U)，商家(M)，银行(B)，分为 4 个阶段：注册阶段，支付阶段，概率选择阶段，验证阶段。在方案中，每次交易值为 1 分，每个用户以 $s=0.001$ 的概率被选中去支付其账单，每次交易都在 1000 个用户中选择一个用户。

(1)注册阶段：

步骤 1 B 选择并公布一个大素数 p；并将数字证书 $\mathrm{Ct_U}=\{\mathrm{ID_B},\mathrm{ID_U},\mathrm{dt},\mathrm{ot}\}$ 和 $\mathrm{Ct_M}=\{\mathrm{ID_B},\mathrm{ID_M},\mathrm{dt},\mathrm{ot}\}$ 发送给 U 和 M，其中 $\mathrm{ID_B}$，$\mathrm{ID_U}$，$\mathrm{ID_M}$ 是 B, U 和 M 的身份信息，dt 和 ot 表示证书有效期和其他信息，证书保证 U 和 M 能够生成 hash 链[18]，M 能够利用 U 生成的 hash 链去 B 处兑换。设生成的每个 hash 值等于 1 分面额值；

步骤 2 U 选择随机数 w_n^{U}，并计算 $w_i^{\mathrm{U}}=h(w_{i+1}^{\mathrm{U}})$，$(i=n-1,n-2,\cdots,0)$ 得到 $w_0^{\mathrm{U}}\leftarrow w_1^{\mathrm{U}}\leftarrow\cdots\leftarrow w_n^{\mathrm{U}}$，$h(\cdot)$ 是 hash 函数。U 对 w_0^{U} 签名，将签名证书发给 B 和 M；

步骤 3 M 选择随机数 c_n，并计算 $c_i=h(c_{i+1})$，$(i=n-1,n-2,\cdots,0)$ 得到 hash 链 $c_0\leftarrow c_1\leftarrow\cdots\leftarrow c_n$，M 对 c_0 签名，并将签名证书发给 B。

(2)支付阶段： U 和 M 进行第 i 次交易，U 将 $\left(i,w_i^{\mathrm{U}}\right)_{\mathrm{PK_M}}$ 发送给 M; M 收到解密得到 w_i^{U}，并验证 $w_{i-1}^{\mathrm{U}}=h\left(w_i^{\mathrm{U}}\right)$ 是否成立，成立则继续完成交易。M 进行第 j 次兑换，M 将 $\left(j,c_j^{\mathrm{M}}\right)_{\mathrm{PK_B}}$ 发送给 B; B 接收解密得到 c_j^{M}，并验证 $c_{j-1}^{\mathrm{M}}=h\left(c_j^{\mathrm{M}}\right)$ 是否成立，成立则给 M 充值。

(3)概率选择阶段：

步骤 1 M 将 $\left(1,w_{i_1}^1\right),\left(2,w_{i_2}^2\right),\cdots,\left(1000,w_{i_{1000}}^{1000}\right)$ 和 $\left(0,c_i\right)$ 发给 B，1,2,…,1000 和 0 分别表示 1000 个用户和商家的身份。B 选择随机数 r_{B}，构造通过点 $\left(1,w_{i_1}^1\right),\left(2,w_{i_2}^2\right),\cdots,\left(1000,\ w_{i_{1000}}^{1000}\right)$，$\left(0,c_i\right)$ 和 $(1001,r_{\mathrm{B}})$ 的 1001 次多项 $A(x)=a_{1001}x^{1001}+a_{1000}x^{1000}+\cdots+a_0$；

步骤 2 B 计算 $R=h(a_0\|a_1\|\cdots\|a_{1001})\bmod 1000+1$，公布 $A(x)$ 和 R。B 从用户 R 账户中扣除 $i_R-\max_R$，给 M 充值 1000 分，并更新 $\max_R$ 为 i_R，i_R 和 $\max_R$ 分别是当前和上次支付序号。在长时间交易中，则 B 扣除用户 R 金额等于给 M 充值的金额。

(4)公平性验证阶段： U 和 M 通过验证方程 $w_{i_{\mathrm{U}}}^{\mathrm{U}}=A(\mathrm{U})$ 和 $c_i=A(0)$ 来验证随机数 R，如果两个等式都成立，则 R 是 U 和 M 共同参与生成的。

2.2 Liu-Yan 方案的分析

Liu-Yan 方案中被选择去支付的用户 U_R 和 M 都可以验证是否参与生成 R，但其安全性存在风险。1000 个用户中一些用户的账单 $i_R-\max_R>1000$，另外一些 $i_R-\max_R\le 1000$，B 每次选择其中一个用户支付账单，而给商家充值 1000 分。

命题 1 B 可以特定选择账单 $i_R-\max_R>1000$ 的用户，扣除 U 金额大于支付给 M 的金额，从中谋取利益。

证明 首先证明银行可以控制生成 R: B 根据 1001 个点计算得到线性方程式(1)：

$$\left.\begin{aligned}
&a_{1001}+a_{1000}+\cdots+a_0=w_{i_1}^1\\
&a_{1001}\cdot 2^{1001}+a_{1000}\cdot 2^{1000}+\cdots+a_0=w_{i_2}^2\\
&\qquad\qquad\cdots\\
&a_{1001}\cdot 1000^{1001}+a_{1000}\cdot 1000^{1000}+\cdots+a_0=w_{i_{1000}}^{1000}\\
&a_0=c_i
\end{aligned}\right\}\quad(1)$$

由式(1)得：$a_i=k_ia_{1001}+b_i$ $(i=1,2,\cdots,1000$，$k_1,k_2,\cdots,$

$k_{1000}, b_1, b_2, \cdots, b_{1000}$ 是常数)， $a_0 = c_i$ 。B 通过选择 a_{1001}，计算 $(a_0, a_1, \cdots, a_{1001})$ 和对应 R，令 $r_{\mathrm{B}} = A(1001)$，即 B 可以控制生成 R。

接下来证明银行通过多次控制生成 R，从而谋取利益。假设用户账单的金额值符合正态分布，期望值为 1000 分，那么大于 1000 分和小于等于 1000 分的概率分别是 1/2。B 通过 i 次选择 a_{1001}，计算得到 i 个 R，从中找到一个账单大于 1000 分 R 的概率如表 1。

表 1　i 次选择 a_{1001} 得到账单大于 1000 分用户的概率

i (次数)	1	2	3	4	5	6
概率	1/2	3/4	7/8	15/16	31/32	63/64

由表 1 可知：i 越大，B 挑选到账单大于 1000 分用户的概率趋近于 1。　　证毕

在 Liu-Yan 方案中，需要大量用户同步共同选择一个进行宏支付的用户，同步性要求太强，限制了方案的实用性。现实生活中更多是用户和商家之间的双方交易，如果每次选择 1000 个用户来生成多项式，交易时间不统一会使得完成交易的时间大幅度增加。Liu-Yan 方案中假设用户为 1000 个，则需要生产一个 1001 次多项式。现实生活中单笔商品或服务的价格极低，但交易量极大的微支付交易越来越多，也就需要更多用户的微支付才能以更小概率转化成某一个用户的宏支付，生成的多项式次数更高，计算复杂度增加，使得交易的开销大幅提升。为了降低计算复杂度，提高交易效率，降低同步性，并且防止银行通过选择特定用户来谋取利益，本文提出基于承诺的可验证公平性微支付方案。

3　基于承诺的可验证公平性微支付方案

3.1 承诺

承诺方案是密码学领域中的一个重要工具，承诺函数的性质使承诺在零知识证明，安全多方计算，身份认证等方面得到广泛的应用。通常承诺方案 $\mathrm{Com}(M)$ 应满足两个目标：

(1)对任意整数 M，由 M 计算 $\mathrm{Com}(M)$ 是容易的；由 $\mathrm{Com}(M)$ 计算 M 是不可能的。

(2)不可能找出两个整数 M_1，M_2，满足 $M_1 \neq M_2$ 且 $\mathrm{Com}(M_1) = \mathrm{Com}(M_2)$。

满足以上目标的承诺方案很多，其至少应该包括：承诺阶段和打开阶段。假设承诺双方为 Alice, Bob，承诺阶段：Alice 根据承诺函数计算 $C = \mathrm{Com}(M)$，并将 C 发给 Bob。打开阶段：当 Alice 需要打开承诺，Alice 公布消息 M , Bob 可以验证承诺值 C 是由 M 生成的。

3.2 基于承诺的可验证公平性微支付方案

基于承诺的可验证公平性微支付方案中，有 3 个参与者：用户(U)，商家(M)，银行(B)，对应的公钥、私钥分别为：$(\mathrm{PK_U}, \mathrm{SK_U})$，$(\mathrm{PK_M}, \mathrm{SK_M})$，$(\mathrm{PK_B}, \mathrm{SK_B})$。本文以 hash 函数作为承诺函数，这不影响基于其它承诺方案微支付协议的各项安全性质。交易过程分为 4 个阶段：注册阶段(与 Liu-Yan 方案相同)、概率选择阶段、支付阶段、验证阶段。具体步骤如下：

(1)概率选择阶段：用户 U_j 和 M 利用承诺协同生成随机数 R，R 决定第 i 次交易用户是否需要支付账单。

步骤 1　M 选择随机数 $r_{i_1}^{\mathrm{U}_j}$，计算 $y_{i_1}^{\mathrm{U}_j} = h\left(r_{i_1}^{\mathrm{U}_j}\right)$，并将 $y_{i_1}^{\mathrm{U}_j}$ 发送给 U_j；

步骤 2　U_j 接收并存储 $y_{i_1}^{\mathrm{U}_j}$，然后选择随机数 $r_{i_2}^{\mathrm{U}_j}$，并将 $\left\{r_{i_2}^{\mathrm{U}_j}, w_i^{\mathrm{U}_j}\right\}_{\mathrm{PK_M}}$ 发送给 M；

步骤 3　M 接收并解密得 $\left\{r_{i_2}^{\mathrm{U}_j}, w_i^{\mathrm{U}_j}\right\}_{\mathrm{PK_M}}$，验证 $w_{i-1}^{\mathrm{U}_j} = h\left(w_i^{\mathrm{U}_j}\right)$ 是否成立。如果成立，则计算 $R = h\left(r_{i_1}^{\mathrm{U}_j}, r_{i_2}^{\mathrm{U}_j}\right) \bmod 1000 + 1$，如果 $R = j$，M 将 $\left(\mathrm{ID_U}, \mathrm{ID_M}, w_i^{\mathrm{U}_j}\right)_{\mathrm{PK_B}}$ 发给 B 兑换金额。

(2)支付阶段：第 i_R 次交易时 $R = j$，U 被选中需要支付账单。B 收到 $\left\{\mathrm{ID_U}, \mathrm{ID_M}, w_{i_R}^{\mathrm{U}_j}\right\}_{\mathrm{PK_B}}$，解密得到 $w_{i_R}^{\mathrm{U}}$，并验证等式 $w_{i_R-1}^{\mathrm{U}} = h\left(w_{i_R}^{\mathrm{U}}\right), w_{i_R-2}^{\mathrm{U}} = h\left(w_{i_R-1}^{\mathrm{U}}\right), \cdots, w_{\max_R}^{\mathrm{U}} = h\left(w_{\max_R+1}^{\mathrm{U}}\right)$ 是否成立，如果这些等式都成立，则 B 从 U 账户扣除 $(i_R - \max_R)$ 分，并给 M 充值 1000 分。

(3)验证阶段：　U_j 需要验证 R 时，U_j 向 M 发送验证申请，M 将 $r_{i_1}^{\mathrm{U}_j}$ 发送给 U_j。U_j 收到 $r_{i_1}^{\mathrm{U}_j}$ 后，验证 $h\left(r_{i_1}^{\mathrm{U}_j}\right) = y_{i_1}^{\mathrm{U}_j}$ 和 $h\left(r_{i_1}^{\mathrm{U}_j}, r_{i_2}^{\mathrm{U}_j}\right) \bmod 1000 + 1 = j$ 是否成立，从而验证 R。

4　效率性及和安全性分析

4.1 效率性分析

微支付的效率性包括计算效率和通讯效率，没有使用复杂的数字签名进行认证的协议是高效的。方案中可验证性随机数 R 生成的主要运用 hash 运算，采用分层结构运算，大幅度降低了整体的计算量。本方案根据自己选择的随机数来生成可验证性随机数，降低了用户验证随机数的计算量，在普通的移动终端上也可以瞬间完成。

假设 1000 个人需要和商家完成交易，每个人和商家交易 1000 次，那么每人有一次被选中支付账单。假设 1000 个被选中的人中有 1 个人要求验证参与生成 R，比较 Liu-Yan 方案和本文方案中 1000 人每人交易 1000 次的总的计算量和通讯量，发现签名运算的次数、生成 hash 链的条数、验证 hash 运算的次数和数据通讯量相差不大。本文方案在生成 R 的时间和验证阶段计算上有很大优势，比较结果如表 2 所示。

表 2 1000 人每人交易 1000 次生成 R 的时间和验证阶段计算比较

	Liu-Yan 方案	本文方案
生成 R 的时间(ms)	15841.56	556.17
验证阶段计算	两次高次多项式计算	两次 hash 验证

由表 2 可知：本文方案在计算时间和验证计算上更加高效。另外 Liu-Yan 方案中用户人数成倍数增加时，生成可验证性随机数的计算负担大幅度增加。利用电脑参数为：系统：Ubuntu 14.04.3LTS, CPU: 2.50 GHz，内存：8 G 的电脑分别计算生成可验证性随机数的时间，得到表 3。本文中 hash 函数以 SHA-256 为例。

表 3 生成可验证性随机数 R 的时间(ms)

用户数(个)	Liu-Yan 方案	本文方案
1000	15.841	0.5562
10000	904.799	5.5617

4.2 安全性分析

4.2.1 SVO 逻辑语法和公理 安全性分析是安全协议的基本组成部分，本文利用 SVO 逻辑对方案进行安全性分析。SVO 逻辑定义了消息语言和公式语言。以 X，PK 和 SK 分别表示消息，公钥和私钥，P 和 Q 表示协议的实体。在消息语言中，以 X 表示消息。表 4 中介绍 SVO 逻辑使用的符号。

4.2.2 SVO 逻辑的形式化分析

(1) SVO 逻辑对安全协议给出了 4 种安全目标：

1:$\mathrm{M}|\equiv w_i$； 2:$\mathrm{B}|\equiv w_i$； 3:$\mathrm{M}|\equiv \mathrm{U}|\equiv R$； 4:$\mathrm{U}|\equiv \mathrm{M}\xleftrightarrow{R}\mathrm{U}$。

(2)初始化假设：

$\mathrm{P}_1:\mathrm{M}|\equiv \mathrm{U}\xleftrightarrow{\mathrm{PK}_M}\mathrm{M}$, $\mathrm{P}_2:\mathrm{M}\lhd w_0$, $\mathrm{P}_3:\mathrm{B}\lhd w_0$, P_4: $\mathrm{M}|\equiv \mathrm{U}\lhd w_n$, P_5: $\mathrm{U}|\equiv \mathrm{M}\xleftrightarrow{j}\mathrm{U}$, $\mathrm{P}_6:\mathrm{M}|\equiv \mathrm{U}\lhd w_0$, $\mathrm{P}_7:\mathrm{B}|\equiv \mathrm{U}\lhd w_0$, $\mathrm{P}_8:\mathrm{B}\lhd\left(\mathrm{ID}_C,\mathrm{ID}_D,w_{i_R}^{\mathrm{U}}\right)_{\mathrm{PK_B}}$, $\mathrm{P}_9:\mathrm{U}|\equiv \mathrm{M}|\Rightarrow\left(r_{i_1}^{\mathrm{U}_j},y_{i_1}^{\mathrm{U}_j}\right)$, $\mathrm{P}_{10}:\mathrm{U}\lhd\left(r_{i_1}^{\mathrm{U}_j},y_{i_1}^{\mathrm{U}_j}\right)$, $\mathrm{P}_{11}:\mathrm{M}|\equiv \mathrm{U}|\Rightarrow\left(r_{i_2}^{\mathrm{U}_j},w_i^{\mathrm{U}_j}\right)$, $\mathrm{P}_{12}:\mathrm{U}|\equiv\#\left(r_{i_1}^{\mathrm{U}_j},y_{i_1}^{\mathrm{U}_j}\right)$, $\mathrm{P}_{13}:\mathrm{U}|\equiv \mathrm{M}|\Rightarrow \mathrm{SK}_{\mathrm{M}}$, $\mathrm{P}_{14}:\mathrm{M}\lhd\left(r_{i_2}^{\mathrm{U}_j},w_i^{\mathrm{U}_j}\right)_{\mathrm{PK_M}}$, $\mathrm{P}_{15}:\mathrm{M}|\equiv\#\left(r_{i_2}^{\mathrm{U}_j},w_i^{\mathrm{U}_j}\right)_{\mathrm{PK_M}}$, $\mathrm{P}_{16}:\mathrm{M}|\equiv \mathrm{B}\xleftrightarrow{\mathrm{PK}_B}\mathrm{M}$, P_{17}:$\mathrm{M}|\equiv \mathrm{B}|\Rightarrow \mathrm{SK_B}$, $\mathrm{P}_{18}:\mathrm{B}|\equiv\#w_i^{\mathrm{U}}$。

(3)协议分析：

步骤 1 由 $\mathrm{P}_1,\mathrm{P}_{13},\mathrm{P}_{14}$ 可以得到：

$$\mathrm{M}\lhd w_i^{\mathrm{U}_j} \tag{2}$$

由式(2)，$\mathrm{P}_2,\mathrm{P}_4,\mathrm{P}_6$ 和 $\mathrm{M}|\equiv \mathrm{U}\xleftrightarrow{w_0=h^i(w_i)}\mathrm{M}$ 得到：

$$\mathrm{M}|\equiv \mathrm{U}|\sim w_i^{\mathrm{U}_j} \tag{3}$$

而由 P_{15} 可以得 $\mathrm{M}|\equiv\#w_i^{\mathrm{U}_j}$，所以

$$\mathrm{M}|\equiv \mathrm{U}|\equiv w_i^{\mathrm{U}_j} \tag{4}$$

由式(4)和 P_{11} 得 $\mathrm{M}|\equiv w_i^{\mathrm{U}_j}$，即证明目标 1: $\mathrm{M}|\equiv w_i$；

步骤 2 由 $\mathrm{P}_8,\mathrm{P}_{16},\mathrm{P}_{17}$ 可以得到 $\mathrm{B}\lhd w_i^{\mathrm{U}}$。由 $\mathrm{B}\lhd w_i^{\mathrm{U}}$，$\mathrm{P}_3,\mathrm{P}_7$ 和 $\mathrm{B}|\equiv \mathrm{M}\xleftrightarrow{w_0=h^i(w_i)}\mathrm{B}$ 得到：

$$\mathrm{B}|\equiv \mathrm{M}|\sim w_i^{\mathrm{U}_j} \tag{5}$$

由 P_{18} 和式(5)得：$\mathrm{B}|\equiv \mathrm{M}|\equiv w_i^{\mathrm{U}}$。而 $\mathrm{M}|\equiv w_i^{\mathrm{U}}$，即证安全目标 2：$\mathrm{B}|\equiv w_i^{\mathrm{U}}$；

步骤 3 由 $\mathrm{P}_1,\mathrm{P}_{14}$ 得：

$$\mathrm{M}|\equiv \mathrm{U}|\sim\left(r_{i_2}^{\mathrm{U}_j},w_i^{\mathrm{U}_j}\right) \tag{6}$$

再由式(6)，P_{15} 可知： $\mathrm{M}|\equiv \mathrm{U}|\equiv\left(r_{i_2}^{\mathrm{U}_j},w_i^{\mathrm{U}_j}\right)$，即得

$$\mathrm{M}|\equiv \mathrm{U}|\equiv r_{i_2}^{\mathrm{U}_j} \tag{7}$$

而由 P_{10}， $\mathrm{U}|\equiv \mathrm{U}\xleftrightarrow{y_{i_1}^{\mathrm{U}_j}=h\left(r_{i_1}^{\mathrm{U}_j}\right)}\mathrm{M}$ 得

$$\mathrm{U}|\equiv \mathrm{M}|\sim\left(r_{i_1}^{\mathrm{U}_j},y_{i_1}^{\mathrm{U}_j}\right) \tag{8}$$

再由 P_{12}，式(8)得

$$\mathrm{U}|\equiv \mathrm{M}|\equiv\left(r_{i_1}^{\mathrm{U}_j},y_{i_1}^{\mathrm{U}_j}\right) \tag{9}$$

表 4 SVO 逻辑语法的符号说明

符号	符号含义
$\mathrm{P}|\equiv X$	参与者 P 相信 X 或者 P 有资格相信 X
$\mathrm{P}\lhd X$	参与者 P 从其他参与者处收到 X 或包含 X 的消息，能够阅读和回复
$\mathrm{P}|\sim X$	参与者 P 曾经发送过包含 X 的消息
$\mathrm{P}|\Rightarrow X$	参与者 P 对消息 X 有管理权
(X,Y)	(X,Y) 包含 X 或者 Y
$\{X\}_{\mathrm{PK}}$ / $\{X\}_{\mathrm{SK}}$	用公钥 PK 加密的消息 X/用私钥 SK 签名的消息 X
$\mathrm{P}\xleftrightarrow{X}\mathrm{Q}$	参与者 P 和 Q 参与者共享消息 X
$\#(x)$	消息 x 是新鲜的

再由 P_9，式 (9) 得：$\mathrm{U}\models\equiv\left(r_{i_1}^{\mathrm{U}_j}, y_{i_1}^{\mathrm{U}_j}\right)$，即得 $\mathrm{U}\models\equiv r_{i_1}^{\mathrm{U}_j}$。再由 $y_{i_1}^{\mathrm{U}_j}=h\left(r_{i_1}^{\mathrm{U}_j}\right)$ 得：$\mathrm{M}\models\equiv\mathrm{U}\models\equiv r_{i_1}^{\mathrm{U}_j}$，而 $\mathrm{M}|\equiv\mathrm{U}\models\equiv r_{i_2}^{\mathrm{U}_j}$，并且 $R=h\left(r_{i_1}^{\mathrm{U}_j}, r_{i_2}^{\mathrm{U}_j}\right)\bmod 1000+1$，即证安全目标 3: $\mathrm{M}\models\equiv\mathrm{U}\models\equiv R$；

步骤 4　由 P_{11} 得：$\mathrm{U}\models\Rightarrow r_{i_2}^{\mathrm{U}_j}$，而 $\mathrm{U}\models\equiv r_{i_1}^{\mathrm{U}_j}$，并且 $R=h\left(r_{i_1}^{\mathrm{U}_j}, r_{i_2}^{\mathrm{U}_j}\right)\bmod 1000+1$，可以得到：$\mathrm{U}\models\equiv R$，再由 $\mathrm{U}\models\equiv\left(r_{i_1}^{\mathrm{U}_j}, y_{i_1}^{\mathrm{U}_j}\right)$，$\mathrm{U}\models\equiv R$，$\mathrm{P}_5$ 即证安全目标 4：$\mathrm{U}\models\mathrm{M}\overset{R}{\longleftrightarrow}\mathrm{U}$。

4.2.3 公平性分析　公平的目的在于确保协议参与各方的地位和作用平等，参与各方拥有的能力是相同的。微支付协议公平性指参与者在任何时刻都不会得到特别的好处。

命题 2　本文方案对 U, M 和 B 都是公平的。

证明　对于 U 而言，U 选择 w^{U}，并计算得 hash 链 A^{U}，再对 A^{U} 进行充值，不会出现透支消费。U 选择 $r_{i_2}^{\mathrm{U}}$，利用其和 M 共同生成决定是否需要支付账单的结果，并且 U 可以验证参与生成该结果。另 U 可以利用承诺值 $y_{i_1}^{\mathrm{U}_j}$ 验证 M 是否存在欺诈，对 U 而言协议是公平的。

对 M 而言，M 对 $r_{i_1}^{\mathrm{U}}$ 做出承诺, 再利用 $r_{i_2}^{\mathrm{U}}$ 和自己选择的 $r_{i_1}^{\mathrm{U}}$ 生成可验证性的 R，从而决定 U 是否需要支付账单。U 和 M 都参与生成 R，并且都可以验证参与生成 R。另外每次交易中，M 都要对 w_i^{U} 进行认证，认证不成立则拒绝交易，所以对 M 而言协议是公平性。

对 B 而言，B 不参与生成 R，所以 B 不能和其他参与者合谋。在 U 需要支付时，B 从 U 的账户扣除 $(i_R-\max_R)$，并且给 M 充值 1000 分，相应的亏空风险需要 B 承担。

在 Liu-Yan 方案中，B 可以特定选择用户，从中谋取利益，对 U 和 M 是不公平。在本文方案中 U, M 和 B 都是公平的参与交易，所以本文方案比 Liu-Yan 方案具有更好的公平性。　　证毕

4.2.4 隐私性分析　本文中，U 和 M 使用匿名化的 ID_{U} 和 ID_{M}，保护 U 和 M 的身份隐私。U 用来支付的 hash 值，U 和 M 利用 $r_{i_1}^{\mathrm{U}}$ 和 $r_{i_2}^{\mathrm{U}}$ 来生成的可验证性随机数 R，都不携带任何和 U, M 身份有关的信息。任何人无法通过 hash 值，$r_{i_1}^{\mathrm{U}}$ 和 $r_{i_2}^{\mathrm{U}}$ 得到和 U, M 有关的信息，保护了 U 和 M 的隐私。

5　结束语

本文对 Liu-Yan 基于插值多项式的微支付方案进行分析，提出了基于承诺的可验证公平性微支付方案。在本文方案中，用户和商家利用承诺协同生成概率验证性的结果，决定用户是否需要支付之前账单。用户和商家都可以验证是否参与生成结果，和 Liu-Yan 方案相比，本文方案除了满足安全性、隐私性、可验证性和高效性外，还具有更好的公平性。

参 考 文 献

[1] YANG Chingnung and WU Chihcheng. MSRC: Micropayment scheme with ability to return changes[J]. *Mathematical and Computer Modelling*, 2013, 58(1/2): 96–107. doi: 10.1016/j.mcm.2012.07.010.

[2] 王涛, 姚松涛, 郭荷清. 安全微支付技术应用于分布式系统安全审计的研究[J]. 通信学报, 2005, 26(5): 118–121.
WANG Tao, YAO Songtao, and GUO Heqing. Research on the application of secure micropayment technology in security auditing of distributed system[J]. *Journal on Communications*, 2005, 26(5): 118–121.

[3] GHAFOORI Z, DEHGHAN M, and NOURHOSEINI M. PPayWord: A Secure and Fast P2P Micropayment Scheme for Video Streaming[M]. Springer International Publishing Switzerland, Springer International Publishing, 2014: 79–91. doi: 10.1007/978-3-319-10903-9_7.

[4] HWANG Shinjia. Security Flaws of Off-Line Micro Payment Scheme with Dual Signatures[M]. Springer Science Business Media Dordrecht, Springer Netherlands, 2014: 905–909. doi: 10.1007/978-94-007-7262-5_103.

[5] CHA Byungrae, LEE Sanghun, PARK Soobong, *et al.* Design of micropayment to strengthen security by 2 factor authentication with mobile and wearable devices[J]. *Advanced Science and Technology Letters*, 2015, 109(7): 28–32. doi: org/10.14257/astl.2015.109.07.

[6] DECKER C and WATTENHOFER R. A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels[M]. Springer International Publishing Switzerland, Springer International Publishing, 2015: 3–18. doi: 10.1007/978-3-319-21741-3_1.

[7] CHEUNG Helen and YANG Cungang. A secure electronic payment protocol for wireless mesh networks[J]. *International Journal of Network Security and Its Applications*, 2014, 6(5): 1–22. doi: 10.5121/ijnsa.2014.6501.

[8] YEN Sungming, LIN Hsichug, CHEN Yenchang, *et al.* PayStar: A denomination flexible micropayment scheme[J]. *Information Sciences*, 2014, 259: 160–169. doi: 10.1016/j.ins.2013.07.031.

[9] BIRYUKOV A and PUSTOGAROV I. Proof-of-Work as Anonymous Micropayment: Rewarding a Tor Relay[M].

Springer Verlag Berlin Heidelberg, Springer Berlin Heidelberg, 2015: 445–455. doi: 10.1007/978-3-662-47854-7_27.

[10] 樊利民, 廖建新. 公平的移动小额支付协议[J]. 电子与信息学报, 2007, 29(11): 2599–2602.
FAN Limin and LIAO Jianxin. Fair mobile micropayment protocol[J]. *Journal of Electronics and Information Technology*, 2007, 29(11): 2599–2602.

[11] 万仁福, 李方伟, 朱江. 一种适用于移动环境的认证和支付协议[J]. 电子与信息学报, 2005, 27(3): 498–501.
WAN Renfu, LI Fangwei, and ZHU Jiang. An efficient authentication and payment protocol for mobile communication[J]. *Journal of Electronics & Information Technology*, 2005, 27(3): 498–501.

[12] RIVEST R L and SHAMIR A. Payword and micromint: Two simple micropayment scheme[C]. International Workshop on Security Protocols, Springer-Verlag, 1997, 1189: 69–87. doi: 10.1007/3-540-62494-5_6.

[13] RIVEST R L. Electronic lottery tickets as micropayments[C]. International Conference on Financial Cryptography, Springer Berlin Heidelberg, 1997: 307–314. doi: 10.1007/3-540-63594-7_87.

[14] SILVIO M and RIVEST R L. Micropayment Revisited[C]. Topics in Cryptology CT-RSA 2002, Springer Berlin Heidelberg, 2002: 149–163. doi: 10.1007/3-540-45760-7_11.

[15] RAFAEL M, HOMERO T, JOEL R, *et al*. P2PM-pay: Person to person mobile payment scheme controlled by expiration date[J]. *Wireless Personal Communications*, 2015, 85(1): 289–304. doi: 10.1007/s11277-015-2738-y.

[16] LIU Yining, HU Lei, and LIU Heguo. A micropayment scheme based on weighted multi-dimensional hash chain[J]. *Journal of Electronics* (*China*), 2006, 23(5): 791–794. doi: 10.1007/s11767-005-0219-2.

[17] LIU Yining and YAN Jihong. A lightweight micropayment scheme based on Lagrange interpolation formula[J]. *Security and Communication Networks*, 2013, 6(8): 955–960. doi: 10.1002/sec.643.

[18] SAZE G. Generation of key pre-distribution schemes using secret sharing scheme[J]. *Discrete Applied Mathematics*, 2003, 128(1): 239–249. doi: 10.1016/S1571-0653(04)00173-8.

刘忆宁： 男，1973 年生，教授，博士，博士生导师，主要研究方向为轻量级安全协议.

赵全玉： 男，1989 年生，硕士生，研究方向为微支付协议、电子投票协议.