第 34 卷 第 1 期 计 算 机 工 程 2008 年 1 月
Vol.34 No.1 Computer Engineering January 2008
·安全技术· 文章编号：1000—3428(2008)01—0158—03 文献标识码：A 中图分类号：TP393.08

一个安全高效的移动微支付协议

汪杨琴
(上海交通大学信息安全工程学院，上海 200240)

摘 要：提出了一个基于 Payword 的移动微支付协议，新协议对 Payword 的协议的不足之处进行了改进。为了使协议更好地应用到移动商务中，协议采用了对称加密算法，并且将多值 hash 链应用到与不同商家的交易中，降低了用户端的存储和计算开销。协议在保证安全性的前提下降低了微支付的交易成本。

关键词：移动商务；移动支付；微支付

Secure and Efficient Mobile Micropayment Protocol

WANG Yang-qin
(School of Information Security and Engineering, Shanghai Jiaotong University, Shanghai 200240)

【Abstract】 A Payword-based micropayment protocol is described in this paper. It overcomes Payword's several shortcomings. In order to make it suitable for m-commerce, only symmetry-encryption is used. Multiple Paywords which reduce customers' storage and computation can be applied to several vendors. The protocol minimizes the exchange cost of micropayment on the promise of security.

【Key words】 mobile commerce; mobile payment; micropayment

微支付主要应用在收费网页的浏览、mp3 及手机铃声的下载，即付即看视频等场合，应用前景非常广阔。在电子商务活动中，对不同的交易类型、不同的客户，需要采取不同的安全手段。由于微支付交易本身所具有的特点，必须满足下面一些条件：(1)匿名性：随着社会的进步，人们越来越注重自己的隐私。从顾客的角度来看，交易需要一个完全匿名的微支付系统。但是从政府的角度来看，完全的匿名性是不可取的。这是因为完全匿名的微支付系统将成为犯罪分子的天堂———进行非法交易和洗钱活动等。可以采取一种中庸的办法。在必要的情况下，可由可信的第三方揭示顾客的身份。(2)防止重复消费：在网络交易环境中，很容易复制电子货币。这就需要采用一种机制来发现货币的重复使用。(3)合理安全性，系统要满足这样的特性：一个心术不正的人破坏系统安全所花费的代价要大大高于他所获得的利益。(4)交易费用最小化：由于微支付本身的特点必须最大程度地降低成本。一方面采用较为低廉的单向散列数(如 MD5, SHA 等)来代替较为昂贵的公钥密码算法。另一方面，尽可能减少通信量；(5)易用性：顾客友好的界面是微支付的另一个重要特性。

1 基于 Payword 的研究

Payword[1]是一种基于信用方式的协议，其模型如图 1 所示。

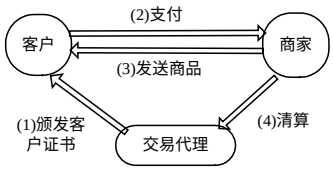

图 1 Payword 协议模型

该协议采用 hash 链的单向性保证了商家不能反向产生 Payword 链，但是可以检测 Payword 链的正确性，不需要代理的在线检测，减少了系统开销。Payword 协议中商家将收集的 Paywords 累计到一定的金额后再到代理 *B* 处兑现，因而也降低了交易费用。但是最初的 Payword 协议有很多的局限性。

鉴于Payword的多种缺陷，各位学者研究了多种改进方案。文献[2-3]改进了Payword，使客户的一条支付链应用到多个商家的交易中，部分解决了客户的恶意透支，但是还是没有解决重复消费等问题。文献[4]通过预支付(prepaid)来防止客户透支，基于对称加密来提高运行效率，但是因为每次交易顾客都要向代理*B*申请预支付，由代理来提供支付根W_n，如果客户的交易非常频繁，那么代理*B*将会成为系统的瓶颈。如果交易金额小，交易费用将超过交易的收益。文中虽然提出了一条支付链应用到多个商家的方案，但是此方案仅适合于客户在申请证书之前就决定要与哪些商家交易多少金额的情况，不具有通用性。并且存在一个商家合谋的问 题[5]。文献[6]中的方案保证了钱和信息商品的原子性，解决了客户透支和重复消费的问题，但是频繁应用公钥加密算法，开销大。文献[7]中的微支付协议是针对移动商务设计的，但是客户的每条支付链只能用于一个商户。并且当客户选择的支付链存在交叉重叠的时候，为商家的欺骗提供了途径。文献[8]中提供的一条支付链应用到多商户交易中的方案必须建立在各商户诚信并且乐意合作的基础之上，在现实中应用有一定的难度。

文中提出的微支付协议试图在保留 Payword 协议的优异性的同时改正 Payword 协议的缺点。新协议在保证安全性的前提下，更多地考虑到移动终端的特点。协议要达到的目标为：(1)较好的匿名性；(2)尽量用对称加密算法，同时减轻代理 *B* 的开销；(3)一条支付链可以应用于多次交易中；(4)公平

作者简介：汪杨琴(1981－)，女，硕士研究生，主研方向：网络安全，电子支付

收稿日期：2007-01-10 **E-mail：**wangyangqin_81@sjtu.edu.cn

性，尽量保证钱和信息商品的原子性；(5)避免透支和重复消费；(6)尽量避免 hash 链交叉。

2 协议描述

银行系统，包括技术系统和管理流程的系统，是专门为特别大额的款项支付而准备的。在实际应用中，微支付需要其他第三方机构来承担。新协议涉及到四方，客户 C、代理 B、商户 M 和银行 K。

2.1 符号说明

I_U, I_M, I_B 为客户、商家和代理的标识。K_{CB}, K_{CM}, K_{BM} 为客户和代理、客户与商家、代理与商家之间的共享密钥。$H^Y(X)$ 表示对 X 进行 Y 次 hash 运算。inf_1, inf_2 代表不同的信息商品。

2.2 注册阶段

进行交易前，客户和商家都要到代理B处注册。客户通过将自己的个人信息，包括自己的标识(经过代理的检测后必须唯一)、账户密码、银行卡号，身份证号等，通过预先建立的安全通道传送给代理B。B通过检测后发放客户标识和共享的密钥K_{CB}给客户，并建立一个客户账户。同理商家也通过此种方式在代理处建立一个账户和共享密钥K_{MB}，代理将商家的标识I_M与他的IP地址A_M唯一对应。

2.3 资金提取阶段

客户在首次发起交易前，为了获得支付链，首先要为账户充值，鉴于微支付每笔交易金额较小，代理预设了一个最低的充值金额 M。充值通过代理 B 与银行之间的专用网络安全操作。当客户充值完毕后，代理将选择

$$W_{N_1} = h(I_U, r_{B_1}, 1),\ W_{N_2} = h(I_U, r_{B_2}, 2),\ W_{N_3} = h(I_U, r_{B_3}, 5),\ W_{N_4} = h(I_U, r_{B_4}, 10)$$

其中，$W_{N_2}, W_{N_3}, W_{N_4}$ 分别代表人民币的一角、两角、五角、一元。代理根据系统的设定将每条支付链设为一定的长度，各条支付链代表的总金额从客户的账户上扣除。当支付链无法完成交易时，需要通过账户的可支配金额或银行卡充值重新构造支付链。设

$$W_{N_1} = h(I_U, r_{B_1}, 1),\ W_{N_2} = h(I_U, r_{B_2}, 2),\ W_{N_3} = h(I_U, r_{B_3}, 5),\ W_{N_4} = h(I_U, r_{B_4}, 10)$$

其中，$r_{B_1}, r_{B_2}, r_{B_3}, r_{B_4}$ 是代理产生的随机数，通过这种方法降低了客户支付链交叉的问题。代理计算

$$H^{N_2}(W_{N_2}) = W_{20}, H^{N_3}(W_{N_3}) = W_{30}, H^{N_4}(W_{N_4}) = W_{40}$$

然后代理将如下信息发送给客户：

$$B \to U\{N_1, W_{N_1}, W_{10}, N_2, W_{N_2}, W_{20}, N_3, W_{N_3}, W_{30}, N_4, W_{N_4}, W_{40}\}K_{CB}$$

客户在收到信息后可以通过计算

$$H^{N_1}(W_{N_1}) = W_{10},\ H^{N_2}(W_{N_2}) = W_{20},\ H^{N_3}(W_{N_3}) = W_{30},\ H^{N_4}(W_{N_4}) = W_{40}$$

来验证上述信息的正确性，并且导出 4 条支付链。

2.4 交易阶段

客户首先与商家A建立连接，了解订购产品的价格、单位商品价格、欲购单位数等。客户根据一个最优算法[9]选取电子货币，客户向代理发起如下交易请求信息：

$$(1)\ U \to B\{I_U, I_M, I_B, F, OI, h(I_U, I_M, I_B, F, OI)\}K_{CB}$$

其中，OI 为订单信息，包括交易时间、商品名称、商品数量、单位商品价格，总金额，以及各支付链与信息商品的对应情况等；$\boldsymbol{F}$ 是根据最优算法算出来的支付矩阵，总金额等于订单的价格

$$\boldsymbol{F} = (W_{1i_1}, K_1, i_1, W_{2i_2}, K_2, i_2, W_{3i_3}, K_3, i_3, W_{4i_4}, K_5, i_5)$$

其中，K_1, K_2, K_3, K_4 表示支付链的索引，取值从 1 到 4。引入索引的目的是便于代理和商家选择相应的支付链进行计算。当某条支付链没有用到时，就不必出现在 $\boldsymbol{F}$ 中。

代理验证 $\boldsymbol{F}$ 代表的总金额是否等于订单总金额，是的话分别发送信息给客户和商家 A 并且将客户这部分金额冻结，否则向客户发送错误信息：

$$(2)\ B \to U\{deal\text{-}ok, K_{CM}, E\}K_{CB}$$

$$(3)\ B \to V\{I_U, I_M, I_B, i_1, i_2, i_3, i_4, W_{10}, W_{20}, W_{30}, W_{40}, K_{CM}, E, OI\}K_{MB}$$

其中，K_{CM}是代理指定的商家和客户的共享密钥，用于加密交易信息；E表示商家清算的最后期限，也是密钥K_{CM}的有效期。当客户想要获得服务时，向商家发送如下信息：

$$(4)\ U \to V\ I_U, I_B, T, \{OI\}K_{CM}, W_{11}, \{W_{11}\}K_{CB}, 1, 1, W_{21}, \{W_{21}\}K_{CB}, 2, 1\cdots$$

其中，T表示当前时间。商家在自己的数据库中查找是否有代理I_B发来的对应I_U的没有过期的交易信息，如果是则验证 4 条支付链的正确性，并且保留收到的Paywords，用于下次验证或清算。引入 $\{W_{11}\}K_{CB}$ 等加密的Payword的目的是为了防止商家共谋，在交易阶段商家并不验证他们。

若验证错误，向客户发送错误信息，否则发送信息商品：

$$(5)\ V \to U\{inf_1, inf_2 \cdots\}K_{CM}$$

$$(6)\ U \to V\ W_{12}, \{W_{12}\}K_{CB}, 1, 2, W_{22}, \{W_{22}\}K_{CB}, 2, 2\cdots$$

$$(7)\ V \to U\{inf_3, inf_4 \cdots\}K_{CM}$$

交易未完时重复第(6)步、第(7)步。

根据最优算法[9]计算结果，顾客可以一次发送同一支付链中的多个Payword给商家A。比如一个商品的价格为 4 角，客户在第(6)步中发送W_{23},2,3 给商家A，表示一次支付两角。商家则验证$H^2(W_{23})=W_{21}$的正确性 。

客户与每个商户的交易步骤是相同的，当客户与商家 B 交易时，交易步骤将重复上述的(1)~(7)步。

$$(1)\ U \to B\{I_U, I_M, I_B, F, OI, h(I_U, I_M, I_B, F, OI)\}K_{CB}$$

$$(2)\ B \to U\{deal\text{-}ok, K_{CM}, E\}K_{CB}$$

$$(3)\ B \to V\{I_U, I_M, I_B, J_1, J_2, J_3, J_4, W_{1i_1}, W_{2i_2}, W_{3i_3}, W_{4i_4}, K_{CM}, E, OI\}K_{MB}$$

因为与商家A交易时一角的支付链用了i_1的长度，这次商家B的一角的支付链的根将从 W_{1i_1} 开始，同理可得其他支付链的根。

$$(4)\ U \to V\ I_U, I_B, T, \{OI\}K_{CM}, W_{1i_1+1}, \{W_{1i_1+1}\}K_{CB}, 1, 1, W_{2i_2+1}, \{W_{2i_2+1}\}K_{CB}, 2, 1\cdots$$

$$(5)\ V \to U\{inf_1, inf_2 \cdots\}K_{CM}$$

$$(6)\ U \to V\ W_{1i_1+2}, \{W_{1i_1+2}\}K_{CB}\ 1, 2, W_{2i_2+2}, \{W_{2i_2+2}\}K_{CB}, 2, 2\cdots$$

$$(7)\ V \to U\{inf_3, inf_4 \cdots\}K_{CM}$$

…

2.5 清算阶段

商家每隔一定的时间段，比如一个星期或一天在代理处兑换。

$$V \to B\ \{\{I_U, I_M, I_B, i_1, i_2, i_3, i_4, W_{10}, W_{20}, W_{30}, W_{40}, K_{CM}, E, OI\}K_{MB}, I_U, W_{1i_1}, \{W_{1i_1}\}K_{CB}, i_1, W_{2i_2}, \{W_{2i_2}\}K_{CB}, i_2, W_{3i_3}, \{W_{3i_3}\}K_{CB}, i_3, W_{4i_4}, \{W_{4i_4}\}K_{CB}, i_4\}K_{MB}$$

代理首先解密 $\{W_{1i_1}\}K_{CB}$ 等 4 个加密后的Payword，解密的结果与消息中对应的Payword相比较，比较的目的是为了防止商户之间的共谋。如果相等再验证 4 条支付链 $H^{i_1}(W_{1i_1}) \stackrel{?}{=} W_{10}$

$, H^{i_2}(W_{2i_2}) \stackrel{?}{=} W_{20}, H^{i_3}(W_{3i_3}) \stackrel{?}{=} W_{30}, H^{i_4}(W_{4i_4}) \stackrel{?}{=} W_{40}$，通过验证后将相应的金额划入商家账户。

一种情况就是商家实际收到的金额小于当初客户的订单金额。造成这种情况的原因是多方面的。包括：(1)网络中断；(2)客户进行一半交易后撤销了本次交易；(3)商家发送了错误的信息给客户，或者信息被篡改，客户因而没有继续发送 Payword 给商家。当是第(1)种或第(3)种情况时，必须有一个出错处理机制。其他的情形下在商家请求清算的时候将客户没有消费完的金额解冻，进入客户在代理处账户的可支配金额栏目。

2.6 出错处理子协议

网络可用的情况下客户向商家发送

$$U \rightarrow V: \{I_U, W_{1j_1}, \{W_{1j_1}\}K_{CB}, t_1, W_{2j_2}, \{W_{2j_2}\}K_{CB}, t_2, W_{3j_3}, \{W_{3j_3}\}K_{CB}, t_3, W_{4j_4}, \{W_{4j_4}\}K_{CB}, t_4, OI\}K_{CM}$$

商家在收到信息后将查找关于客户的交易记录，然后发送未发完的信息或重新发送信息。对于商家来说没有理由拒绝重新发送信息，因为重新发送的成本不高，并且可以保持良好的客户关系，所以客户钱丢失的可能性很小。关键在于如何防止黑客利用出错处理子协议对商家进行攻击。在此，当客户发送同一条出错信息的次数达到一定数量后，商家将拒绝为客户服务，并向代理报告此恶意客户。同时信誉良好的客户在完成一笔交易后可以向代理提交对商家的评价，这一评价指标出现在商家标识上，供用户交易前参考。

3 新协议性能评估

3.1 公平性

Payword 协议是基于信用的，因而客户可以透支，无法保证商家的利益。本协议采用预支付的手段，每次交易前通过代理冻结订单金额，保证了商家的利益。因为微支付的每笔交易利润小，只有加大用户群并且使每个用户的消费量增大，商家才能获得利润，所以客户钱丢失的可能性很小。当客户实际消费金额不满订单金额时，多余的金额在商家向代理提出清算请求的时候进入客户的可支配金额栏目，用于下次重新构造支付链。

3.2 效率性

新协议在效率方面有很好的表现，除了客户每次从银行提取不低于M的金额时通过安全通道提取金额，需要比较高的安全手段，交易的时候用的都是对称加密算法，加快了交易速度。采用多值hash链降低存储开销，减少hash运算的次数，避免过长hash链并可方便地并行进行多个信息服务的支付。关于代理的开销方面，新协议因为通过代理保全了交易金额，所以商家可以选择比较长的清算期，不同于代理并不需要每笔交易前都通过银行提取本次交易的金额[3]，因为每次从银行提取金额的最低限度为M，一般相当于多次交易的费用。再则新协议是预支付的，也就不存在由代理处理客户透支的额外开销。虽然每笔交易之前都要通过代理的审核，但是审核减少处理客户重复消费的开销，提前制止了欺骗。

3.3 扩展性

不同于文献[10]和 Payword 等协议中客户需要保留多条对应不同商家的 hash 链，新协议通过由代理构造通用的多值 hash 链应用于多个商家，减轻了客户端存储和管理方面的开销。不同于文献[4]中客户只能提前决定交易对象的特点，新协议使客户同时或者随时选择不同的商家交易。当然客户每发起一次交易需要给代理少量的手续费。并且支付根的选择是由代理来选择的，避免了支付链的交叉问题。如果支付根由客户随意选择，当用户数达到一定规模后，支付链的交叉问题将非常的明显，影响系统的扩展性能。新协议中有出错处理子协议，既保证了客户钱的原子性也避免了恶意客户对商家的攻击。代理为商家提供的信誉指标可以使商家提高服务质量，避免了商家的欺骗。

3.4 安全性

新协议的安全性也是非常高的。提取资金和清算资金的时候因为涉及到的资金比较大和银行卡号等机密信息，所以需用到专用的安全通道等一系列的安全手段，微支付时只用对称加密就可满足安全需求。当清算过后，代理将本次交易状态改为结束状态，商家不能重复清算。引入了加密的 Payword 后，新协议不存在两个商家共谋的问题，可以忽略客户将不正确的 Payword 加密后发送给商家的可能性，因为客户用于微支付的软件都是下载在客户端的，客户没有能力修改软件的操作细节。

3.5 匿名性

新协议提供了比较好的匿名性。只有代理知道客户和商家的详细信息。客户与商家交易的时候只是出示自己的代号I_U，商家也只是公布自己的IP地址A_M和代号I_M。

4 结束语

本协议在 Payword 协议的基础上提出了一种适合于移动商务的微支付协议。本协议的安全性完全适合微支付，具有比较强的可操作性。本协议优于 Payword 协议的地方就是没有用到公钥加密，具备更好的公平性和匿名性，避免透支和重复消费，更长的清算周期，多 hash 链扩展性好，并且可用于不同的商家。

参考文献

[1] Rivest R, Shamir A. Payword and Micromint: Two Simple Micropayment Schemes[C]//Proc. of International Workshop on Security Protocols. Berlin: Springer Verlag, 1996: 69-87.

[2] Kim S, Lee W. A Payword-based Micropayment Protocol Supporting Multiple Payments[C]//Proc. of IEEE International Conference on Computer Communications and Networks. Dallas: [s. n.], 2003: 609-612.

[3] Wang C, Chang C, Lin C. A New Micro-payment System Using General Payword Chain[J]. Electronic Commerce Research Journal, 2002, 2(1/2): 159-168.

[4] Yang Z, Lang W, Tan Y. A New Fair Micropayment System Based on Hash Chain[C]//Proceedings of IEEE International Conference on E-technology-commerce and E-service. Washington D. C.: [s. n.], 2004: 139.

[5] Yang C N, Lin T, Chen T S. Enhanced Fair Micropayment Scheme Based on Hash Chain to Avoid Merchant Collusion[C]//Proc. of the 9th International Symposium on Consumer Electronics. Macau: [s. n.], 2005: 39-42.

[6] Lee M, Lee H, Kim K. A Micro-payment System for Multiple Shopping[C]//Proc. of Symposium on Cryptography and Information Security. Shirahama: [s. n.], 2002: 229-234.

[7] 练　斌. 安全微支付系统的研究与设计[D]. 成都: 西南交通大学, 2005.

[8] 胡晓飞, 徐国华. 一种高效的 M-merchants 微支付方案[J]. 现代电子技术, 2006, 30(4): 33-35.

（下转第 172 页）