一种新颖的可再生多 Hash 链的构造

赵源超 李道本
(北京邮电大学信息工程学院 北京 100876)

摘 要 作为一种能够提供不可否认性的密码学算法，由于计算效率较高，Hash 链被广泛应用于电子微支付方案中。为了进一步提高系统的效率，可以同时采用多个 Hash 链表示不同的面值进行微支付。由于 Hash 链存在有限长度的限制，系统的设计需要尽量降低再生 Hash 链时导致的额外开销。该文提出一种高效的基于一次性签名的可同时再生多个 Hash 链的构造方法，分析了这种构造内在的不可否认性和再生配置的灵活性，讨论了在多面值微支付中的应用。这种构造方法能够提高同时使用多个 Hash 链的系统的效率。

关键词 Hash 链，不可否认性，一次性签名
中图分类号：TP309.2 **文献标识码**：A **文章编号**：1009-5896(2006)02-0299-04

A Novel Construction of Re-initializable Multi-Hash Chains

Zhao Yuan-chao Li Dao-ben
(*Dept of Info. Eng., Beijing Univ. of Posts and Telecom., Beijing* 100876, *China*)

Abstract As a cryptography algorithm that can provide non-repudiability, hash chains are widely used in electronic micropayment schemes because of its efficiency. In order to further improve efficiency, multiple hash chains can be simultaneously used to represent different denominations in micropayment. Because of the limitation that hash chain has a limited length, system design has to reduce the overhead when hash chains are re-initialized. A efficient one-time-signature-based construction is proposed which can simultaneously re-initialize multiple hash chains and its intrinsic non-repudiability and flexibility of configuration in re-initialization are analyzed. The application of the construction in multi-denomination micropayment is illustrated. The proposed construction can improve the efficiency of systems with multiple hash chains.

Key words Hash chain, Non-repudiability, One-time signature

1 引言

随着互联网络的快速发展，人们越来越多地采用网上电子支付的方法购买各种商品，为此研究人员设计了各种支付方案。人们所要购买的商品可以不是物质商品，而是信息或者服务，前者如数据库查 询、股票报价浏览等，后者如互联网服务提供商(Internet Service Provider, ISP)为用户提供接入Internet的服务等。在这些情况下，用户为单次购买需要付出的金额往往很少，很可能只有一分钱到几分钱，那么为这种微量金额交易设计的支付方案就称为微支付方案。在电子支付中，需要加入安全手段实现支付信息的不可否认性，而这些又会导致额外的计算开销。与微支付相对而言的宏支付往往大量采用传统的公钥签名技术，这时签名和验证都要付出很大的计算代价。对于微支付来说，由于单次交易涉及的金额很小，所以如果大量采用传统的公钥签名技术将会使得为计算付出的代价接近或者超过交易本身的价值，因此这样的系统是不能用于微支付的。总之，微支付方案的设计原则就是效率。

Hash链的方法是由Lamport[1]提出的。尽管最初是用来保护一次性口令不被窃听和重放，但是由于Hash链同时拥有类似于公钥技术的性质和计算的高效率，因此，它很快就被广泛用于微支付方案中，如PayWord[2]，NetCard[3]和Pederson[4]的方案。这些系统中，将Hash链上的一个Hash值作为一个付费单位的支付信息。为了进一步提高系统的效率，有的微支付方案同时采用多条Hash链，如NetPay[5]，不同Hash链上的Hash值表示具有不同面值的付费单位，类似于人们使用的普通货币，通过不同面值的组合对所需支付的费用给出支付信息。

2004-07-16 收到, 2004-11-12 改回
国家自然科学基金重大项目(69931050)资助课题

然而，这些应用都受到一个共同的限制，即 Hash 链的长度是有限的。当 Hash 链用尽以后，系统必须重新初始化，即需要再生新的 Hash 链，而且 Hash 链的再生一般都还要和系统初次启动一样使用公钥签名技术，这严重有损于系统的效率。现有文献还没有为同时使用多条 Hash 链的应用研究出一种高效率的多 Hash 链再生技术。本文正是为了解决这个问题，提出一种新的构造方法，高效率地再生一个或者同时再生多个 Hash 链，避免了使用计算负荷大的公钥签名技术。

下面几节分别包括如下内容：第 2 节简要介绍 Hash 链和一次性签名的概念以及相关的工作；第 3 节基于一次性签名技术提出一种新的可再生多 Hash 链的构造；第 4 节分析了这种新的构造方法内在的不可否认关系和再生配置的灵活性；第 5 节讨论了该构造在多面值微支付中的应用；第 6 节给出了本文的结束语。

2 Hash 链和一次性签名

2.1 Hash 链简介

Hash 链是由称作“单向 Hash 函数”的一个公开函数 h 进行递归运算得到的。其中，h 将一个任意长度(或预先确定最大长度范围)的比特串映射为一个固定长度的比特串。而且，h 满足 3 个性质：(1)给定 x，容易计算 $h(x)$；(2)给定 $h(x)$，求出 x 在计算上是不可行的；(3)找到两个值 x 和 y，且 $x\neq y$，使得 $h(x)=h(y)$ 在计算上是不可行的。

构造长度为 N 的 Hash 链时，首先选取一个随机的种子值 s，然后对 s 重复计算 N 次，得到如下的序列:

$$s,\ h(s),\ h^2(s),\cdots,\ h^i(s),\ \cdots,\ h^{(N-1)}(s),\quad h^N(s)$$

其中 s 可记作 $h^0(s)$，$h^N(s)$ 称作 Hash 链的根节点，作用类似于公钥技术中的公开密钥，而 s 类似于公钥技术中的私有密钥。知道 $h^N(s)$，但不知道 s，则不能生成 $h^{(N-1)}(s)$；给定 $h^{(N-1)}(s)$，则它的正确性可以很容易用 $h^N(s)$ 进行验证。依此类推，知道 $h^i(s)$，但不知道 s，则不能生成 $h^{(i-1)}(s)$；$h^{(i-1)}(s)$ 的正确性可以很容易用 $h^i(s)$ 进行验证，其中 $i=N,N-1,\cdots,1$。

Hash 链应用于微支付时，购买方知道 s (从而，知道整个 Hash 链)，销售方仅仅知道 $h^N(s)$。链中的一个 Hash 值代表一个付费单位。购买方根据需要付出的付费单位数量，从 $h^{(N-1)}(s)$ 开始，对销售方依次释放 Hash 链中的元素，直到到达 $h^0(s)$，即 s。这时，Hash 链被用尽，系统需要用一个不同的 s 值重新初始化。

2.2 一次性签名的背景知识

首先值得注意的是，一次性签名与 Hash 链一样只是使用单向 Hash 函数，而没有使用传统的公钥方法，所以适用于对计算效率要求高的应用，包括微支付。

一次性签名也是由 Lamport 首先提出的，文献[6]转述了他的想法——对 1bit 消息签名：选择两个随机数 $x1$ 和 $x2$ 作为私有密钥，分别代表‘0’和‘1’；用单向 Hash 函数 h 分别计算 $y0=h(x0)$和 $y1=h(x1)$，将 $y0$ 和 $y1$ 发布作为公开密钥；对 1bit 消息签名时，如果消息是‘0’，就公开 $x0$，消息的接收者计算 $h(x0)$，并且将计算结果与 $y0$ 比较，二者相同则验证通过；如果消息是‘1’，就公开 $x1$，消息的接收者计算 $h(x1)$，并且将计算结果与 $y1$ 比较，相同则验证通过。对 n 个 bit 消息的签名则分别需要准备 $2n$ 个 x 和 y。

在对最初的一次性签名的各种改进措施中，出于本文的目的，这里只采用Merkle[7]提出的方法：对n个bit消息的每一个 bit 只生成一个随机数 $x_i(i=1,2,\cdots,n)$，计算 $y_i=h(x_i)(i=1,2,\cdots,n)$，而且发布所有 y_i；当消息的第i个bit为‘1’时，公开 x_i，若为‘0’，不公开任何值。为了防止接收者将收到‘1’伪称为收到‘0’，签名者需要也对消息中‘0’的个数进行签名，而且对消息中‘0’的个数的签名方法与对消息体的签名方法完全相同。因此，在Merkle的方法里，对n个bit消息的签名则分别需要准备 $n+\lceil\log_2(n)\rceil$ 个x和y。

2.3 解决 Hash 链有限长度限制的相关工作

为了解决Hash链的有限长度问题，Bicaki和Baykal[8]提出了一种基于公钥密码学的“无限长Hash链”。尽管，这种构造方法确实解决了Hash链的有限长度问题，但是由于公钥密码技术存在很重的计算负担，这恰好与微支付对高效率的要求矛盾，因此这种无限长Hash链是不能被微支付系统采用的。

最近，文献[9]提出一种新的 Hash 链构造，称作可再生 Hash 链(Re-initializable Hash Chain, RHC)。当一个 RHC 用尽以后，能够以不可否认的方式安全地再生，从而得到另一个 RHC。这一过程能够无限次继续，实质上是将无限多个有限长度的 Hash 链(通过一次性签名的方法)“打结”在一起。这种方法一次只能再生一条 Hash 链，而下面一节提出的构造方法可以同时再生多条 Hash 链，并且提供了额外的配置上的灵活性。

3 可再生多 Hash 链的构造

这里，仅仅利用单向Hash函数和Merkle的一次性签名方案构造可再生的多Hash链。设系统共需要同时使用M条Hash链，每个Hash链的长度都为N。同时，设Hash函数h的输出的长度为L(bit)(例如：MD5[10]算法的输出是 128bit)。下面分为

两种不同的阶段进行讨论：

3.1 首次启动多 Hash 链阶段

发送方选择 M 个随机种子值为 s_1，s_2，…，s_M，相应地计算 M 个根为 $h^N(s_1)$，$h^N(s_2)$，…，$h^N(s_M)$。同时，给长度为 L 个 bit 的消息准备一对一次性签名密钥的实例，包括 $L+\lceil \log_2(L) \rceil$ 个随机数的级联 S_U 以及这些随机数相应的 $L+\lceil \log_2(L) \rceil$ 个 Hash 函数值的级联 P_U，可以将 S_U 和 P_U 分别看作一次性签名的私钥元素和公钥元素。实际上该一次性签名密钥的实例并不是真正用于本次 Hash 链的启动，而是用于下次再生 Hash 链的。

为了方便下面的讨论，这里规定多 Hash 链的“复合根(Composite Root, CR)”如下式 $\mathrm{CR}=h(\mathrm{flag},h^N(s_1),h^N(s_2),\cdots,h^N(s_M),h(P_U))$ 其中 flag 是一个 Mbit 长的二进制串，它的第 i 位用于标志本次启动中是否包含第 i 个 Hash 链。因为是首次启动 Hash 链，所以这个 CR 需要以安全的方式分发给接收方，当然，使用传统的公钥数字签名技术是最直接的选择。CR 中携带一次性签名的信息正是为了在后续再生 Hash 链的时候避免开销大的公钥计算。在开始使用 Hash 链之前，发送方还要将 $\mathrm{flag},h^N(s_1),h^N(s_2),\cdots,h^N(s_M),h(P_U)$ 发给接收方，因为是首次启动 Hash 链，所以 flag 的值一定是全 1 串，即 $11\cdots1$，共 M 个 1，表示启动所有 Hash 链。接收方可以通过计算 CR 对这个消息进行验证。在此之后，就可以按照通常的方式使用这 M 个 Hash 链了。发送方使用各个链上的 Hash 值，直到到达其中一些 Hash 链的种子值，这时，这些被耗尽的 Hash 链就需要进行后续的再生了。

3.2 后续再生多 Hash 链阶段

设上次使用时耗尽的 Hash 链的个数是 $K(K\le M)$个，它们分别是第 $i_1,i_2,\cdots,i_K(1\le i_1<i_2<\cdots<i_K\le M)$ 条 Hash 链，从而本次需要启动的 Hash 链的个数为 K。发送方需要选择 K 个新的随机种子值 $s_{i_1}',s_{i_2}',\cdots,s_{i_K}'$，而且生成一对新的一次性签名密钥的实例 S_U' 和 P_U'。然后计算新的复合根：

$$\mathrm{CR}'=h(\mathrm{flag}',h^N(s_{i_1}'),h^N(s_{i_2}'),\cdots,h^N(s_{i_K}'),h(P_U'))$$

发送方现在向接收方发出 P_U (注意不是 P_U')，对 CR′ 签名所需公开的部分 S_U (注意不是 S_U')以及 CR′。接收方用上一次启动时接收到的 $h(P_U)$ 验证 P_U，通过 S_U 的公开部分验证 CR′。同时，发送方还要将 $\mathrm{flag}',h^N(s_{i_1}'),h^N(s_{i_2}'),\cdots,h^N(s_{i_K}'),h(P_U')$ 发给接收方，其中 flag′ 所有的第 $i_h(h=1,2,\cdots,K)$ 位等于‘1’，其他位都等于‘0’。接收方计算 CR′ 来验证这些信息的有效性。此时，这些经过再生的 Hash 链就可以加入使用了。

而且，这种再生过程能够以相同的方式无限次进行，即再生能力为无限次，而且每次再生时都避免了进行开销大的公钥计算。

4　可再生多 Hash 链的特点

第 3 节提出的可再生多 Hash 链的构造最大的特点就是在再生和使用 Hash 链的时候，逐层地提供并且保持了不可否认性，而且这种不可否认性的实现中避免了公钥计算(初始启动除外)。这种特点直接来源于构造中仅仅使用了单向 Hash 函数。图 1 中以一个具体的例子说明了该构造内在的不可否认性关系。例子中同时使用的 Hash 链数量是 2，首次启动阶段启动了全部两个 Hash 链，所以 flag = 11；第 1 次再生时，(设第一条 Hash 链还未耗尽)启动了一个，也就是第二条 Hash 链，所以 flag′ = 01；第 2 次再生时，(设两条 Hash 链都已经耗尽)又同时启动了全部两条 Hash 链。图中“→”的指出方为“→”的指入方提供不可否认的证据，而且这种证据关系具有传递的性质：

(1) 复合根证明标志位的不可否认性；

(2) 复合根证明启动/再生的各个 Hash 链的根的不可否认性；

(3) 复合根证明一次性签名公钥 Hash 值的不可否认性；

(4) 单个 Hash 链靠近根的节点证明远离根的节点的不可否认性；

(5) 一次性签名公钥的 Hash 值证明该公钥的不可否认性；

(6) 一次性签名公钥和相应私钥的公开部分联合证明下次再生时的复合根的不可否认性。

可见，该构造能够以不可否认的方式安全地再生多 Hash 链。

另外，该构造具有配置灵活的优点。由于使用了标志位，所以每次再生 Hash 链时，可以根据各条 Hash 链的使用情况，

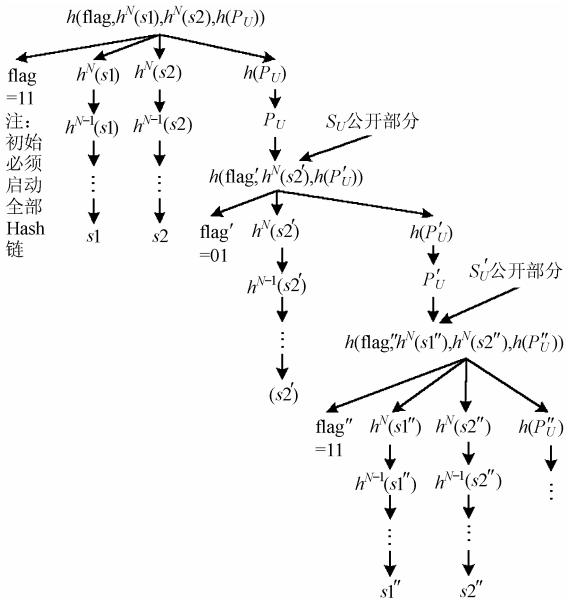

图 1　可再生多 Hash 链构造内在的不可否认关系

灵活地指定再生其中的一条或者多条 Hash 链，对于使用多 Hash 链的应用可能存在的不同使用模式提供了方便。

5 在多面值微支付中的应用

在较早的微支付方案[2－4]中，只生成和使用单一的支付信息Hash链，因此一个Hash值只能代表一个最低的付费单位。如果用户能够使用不同面值的Hash值进行付费，那么系统在计算上将变得更加有效率。例如：如果使用 1 条Hash链的付费单位为 1 分时，则使用 6 条Hash链时，每一条的付费单位可以分别是 1 分、2 分、3 分、4 分、5 分和 6 分。如果用户花费了 16 分，那么使用单Hash链的系统就要进行 16 次Hash值的计算，而使用多Hash链的系统可以按 6 分+6 分+4 分付费，从而只要进行 3 次Hash值的计算就可以了。而且，使用多个Hash链可以增加Hash链的使用时间长度。可见，微支付方案使用多个Hash链是有实用价值的。但是，在多Hash链的系统中，Hash链的再生效率仍然需要尽量提高。本文提出的方法，有效地解决了多Hash链的再生问题，一方面它避免了使用开销大的公钥技术，另一方面它可以同时再生多条Hash链，这要比一条一条地单独再生Hash链的效率有明显提高。

再有，该方法提供了再生配置上的灵活性，这一点可以与文献[11]提出的多 Hash 链的两种工作模式(进取模式和平衡模式)相结合进一步提高系统的效率。尤其是与平衡模式相结合时，各条 Hash 链的使用进度大致相同，可以减少再生操作的次数，从而提高了效率。

6 结束语

本文提出的可再生多 Hash 链构造避免了使用计算开销大的公钥技术，计算中只使用了计算效率高的单向 Hash 函数。而且，每次再生时都能够安全地以不可否认的方式启动多条 Hash 链。这里的效率和不可否认性都直接来源于单向 Hash 函数的性质。而且，提供了再生配置的灵活性，能够按实际需要再生不同数量的 Hash 链。这种方法可以明显提高同时使用多个 Hash 链的应用的效率，尤其有益于多面值微支付系统效率的提高。

此外，这种构造也可以用于移动通信环境中的实时不可否认计费。因为在移动通信中涉及归属运营商和服务运营商的计费，而且如果是数据通信的话，那么还要涉及 ISP 的计费。这些运营商的计费标准各不相同，则结合该构造的多个 Hash 链可以用于向他们分别付费。

参 考 文 献

[1] Lamport L. Password authentication with insecure communication . *Communications of the ACM*, 1981, 24(11): 770－772.

[2] Rivest R, Shamir A. Payword and MicroMint: two simple micropayment schemes. Proceedings of the 4th Security Protocols International Workshop (Security Protocols), Lecture Notes in Computer Science, Cambridge, UK, 1996, 1189: 69－87.

[3] Anderson R, Manifavas H, Sutherland C. NetCard – a practical electronic cash system. Proceedings of the 4th Security Protocols International Workshop (Security Protocols), Lecture Notes in Computer Science, Cambridge, UK, 1996, 1189: 49－57.

[4] Pedersen T. Electronic payments of small amounts. Proceedings of the 4th Security Protocols International Workshop (Security Protocols), Lecture Notes in Computer Science, Cambridge, UK, 1996, 1189: 59－68.

[5] Dai X, Lo B. Netpay-An efficient protocol for micropayments on the WWW. URL: http://ausweb.scu.edu.au/aw99/papers/dai/paper. html

[6] Diffie W, Hellman M. New directions in cryptography. *IEEE Trans. on Information Theory*, 1976, IT-22(11): 644－654.

[7] Merkle R. A digital signature based on a conventional encryption function. Proceedings of Advances in Cryptology – CRYPTO ’87, Lecture Notes in Computer Science, Santa Barbara, CA, USA, 1988, vol. 293: 369－378.

[8] Bicakci K, Baykal N. Infinite length hash chains and their applications. Proceedings of the 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE’02), Pittsburgh, USA, June 2002: 57－61.

[9] Goyal V. How to re-initialize a hash chain. URL: http:// eprint. iacr.org/ 2004/097.pdf

[10] Rivest R. The MD5 message digest algorithm. RFC 1321, April 1992.

[11] Yang Ching-Nung, Teng Hsu-Tun. An efficient method for finding minimum hash chain of multi-payword chains in micropayment. Proceedings of the IEEE International Conference on E-Commerce 2003 (CEC’03), Newport Beach, California, USA, June 2003: 45－48.

赵源超： 男，1971 年生，博士生，从事移动通信安全方面的研究.

李道本： 男，1939 年生，教授，博士生导师，主要从事 Las-CDMA 移动通信系统的研究.