高效的在线/离线代理重签名方案

杨小东* 王彩芬
(西北师范大学数学与信息科学学院 兰州 730070)

摘 要：为了改善代理重签名的性能，该文提出在线/离线代理重签名方案。其基本思想是将重签名算法分成离线阶段和在线阶段。在签名消息到来之前，离线阶段进行重签名的大部分计算，并将这些运算结果保存起来；在签名消息到来时，利用离线阶段保存的数据能在很短的时间内生成消息的在线重签名。文中给出了在线/离线代理重签名方案形式化定义，在此基础上构造了具体实现的方案，并在随机预言模型下给出其安全性证明。该方案可将任意一个代理重签名方案转换为一个高效的在线/离线代理重签名方案。分析结果表明，新方案在效率上优于已有的代理重签名方案，在线重签名算法仅需要 1 次模减法运算和 1 次模乘法运算。

关键词：代理重签名；在线/离线；变色龙哈希函数；随机预言模型
中图分类号：TP309.7 **文献标识码**： A **文章编号**：1009-5896(2011)12-2916-06
DOI: 10.3724/SP.J.1146.2011.00406

Efficient On-line/Off-line Proxy Re-signature Schemes

Yang Xiao-dong Wang Cai-fen
(*College of Mathematics and Information Science*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

Abstract: To improve the performance of proxy re-signature schemes, the schemes of on-line/off-line proxy re-signature are proposed in this paper. The main idea is to split the re-signing procedure into two phases: the off-line and on-line phases. Most of the computations are performed in the off-line phase before seeing the message to be re-signed. The results of this precomputation are saved and then used in the on-line phase when the message must be re-signed. On-line/off-line proxy re-signature schemes are used in a particular scenario where the proxy must respond quickly once the message to be re-signed is presented. Based on the formal definition of on-line/off-line proxy re-signatures, an efficient construction of on-line/off-line proxy re-signature is presented. It can convert any proxy re-signature scheme into a highly efficient on-line/off-line one. Security is proved in the random oracle model. Compared wirh the existing proxy re-signature schemes, the new scheme is more efficient in the communication cost and the computational cost. It needs one modular subtraction computation and one modular multiplication computation in the on-line re-signing generation algorithm.

Key words: Proxy re-signature; On-line/off-line; Chameleon hash function; Random oracle model

1 引言

数字签名在保证数据的机密性、完整性和不可否认性等方面起着极为重要的作用，被广泛用于设计电子支付、电子投标、电子拍卖、电子彩票和电子投票等应用协议，是安全电子商务和安全电子政务的关键技术之一。根据实际应用背景的需要，人们提出了诸多特殊的数字签名方案，代理签名就是其中的一种。代理签名将签名者的某些权利委托给可靠的代理者，让代理者代表签名者行使相应的签名权利。但在代理签名中，委托者必须高度信任代理者。

为了分散代理者的签名权利，文献[1]提出了代理重签名的概念。在代理重签名中，一个拥有重签名密钥的半可信代理者(semi-trusted proxy)将受托者(delegatee)的签名(也称原始签名)转换为委托者(delegator)对同一消息的签名(也称重签名)，但这个代理者不能单独生成受托者或委托者的任何原始签名。所谓半可信，指的是仅仅相信这个代理者一定会按方案进行签名的转换。代理重签名在简化证书管理、管理群签名、提供遍历的路径证明、构造审查系统和数字版权管理系统等方面有广泛的应用前景[2]。

在线/离线签名[3]是把数字签名分成两个阶段的签名方式，它是为了提高签名方案的效率而提出来的一种解决方案。第 1 阶段是离线阶段，在未知签名消息的情况下进行签名预计算。由于此阶段有足够的时间，因而离线阶段签名算法并不影响消息的

2011-04-27 收到，2011-09-01 改回
国家自然科学基金(61063041)和西北师范大学青年教师科研能力提升计划(NWNU-LKQN-10-22)资助课题
*通信作者：杨小东 y200888@163.com

签名速度；第 2 阶段是在线阶段，这是在消息出现后开始的，由于离线阶段已做了预计算，所以此阶段签名速度非常快。在线/离线签名在现实中有广泛的应用，如智能卡等。

在已有的代理重签名方案中[1,2,4−7]，重签名生成算法中有幂指数运算，严重影响了代理重签名方案的签名效率。为了改善代理重签名的性能，本文基于变色龙哈希函数提出了一个在线/离线代理重签名方案。该方案将代理重签名的特性与在线/离线签名的特性进行了有效融合，能将已有的任意一个代理重签名方案转换为一个高效的在线/离线代理重签名方案。在线/离线代理重签名大大提高了代理重签名的实时性和安全性，可应用在重签名时间受限或重签名设备计算能力有限的场合，如无线传感器网络、无线路由器协议、PDA 等。如果是时间受限，在空闲时间进行离线阶段的运算，将计算结果保存，预备用于在线阶段的重签名运算；如果是设备的计算能力有限，让具有较强计算能力的设备进行离线阶段的计算，将计算结果存储在计算能力有限的设备上，用于在线阶段进行重签名。代理重签名是近年来密码学研究的一个热点，主要集中于研究代理重签名[1,2,4−7]、盲代理重签名[8]、无证书代理重签名[9]和门限代理重签名[10]等，但关于在线/离线代理重签名的公开文献几乎没有。

2　预备知识

2.1 椭圆曲线离散对数假设

选择大素数 t，$E(F_t)$ 是定义在有限域 F_t 上的一个椭圆曲线，$\#E(F_t)$ 是 $E(F_t)$ 中点的数目。点 $P\in E(F_t)$，P 的阶为素数 q，这里 $q\mid \#E(F_t)$。G 是 P 生成的一个 q 阶循环群。椭圆曲线离散对数问题(ECDLP)：给定 $(P,P_1)\in E(F_t)$，寻找一个整数 $a\in Z_q$，使得在 G 中有 $P_1=aP$。

定义 1 (椭圆曲线离散对数假设)　如果没有一个概率多项式时间算法在时间 T 内以至少 ε 的概率解决群 G 上的椭圆曲线离散对数问题，则称群 G 上的 (T,ε)-ECDLP 假设成立。

2.2 变色龙哈希函数

变色龙哈希函数 $\mathrm{CH}(\cdot,\cdot)$ 是一种特殊的哈希函数[3]，拥有一个门限密钥 TK 和一个公钥 HK，并且满足以下性质：

(1)有效性：给定公钥 HK，一个消息 m 和一个随机数 r，存在一个多项式时间算法计算 $\mathrm{CH}_{\mathrm{HK}}(m,r)$。

(2)抗碰撞性：输入公钥 HK，不存在任何一个概率多项式时间算法以一个不可忽略的概率输出 (m_1,r_1) 和 (m_2,r_2)，使得 $m_1\neq m_2$ 且 $\mathrm{CH}_{\mathrm{HK}}(m_1,r_1)=\mathrm{CH}_{\mathrm{HK}}(m_2,r_2)$。

(3)门限碰撞：给定门限密钥 TK，公钥 HK，两个不同的消息 (m_1,m_2) 和一个随机数 r_1，一定存在一个概率多项式时间算法输出一个值 r_2，使得 $\mathrm{CH}_{\mathrm{HK}}(m_1,r_1)=\mathrm{CH}_{\mathrm{HK}}(m_2,r_2)$；如果 r_1 服从均匀分布，则 r_2 服从的分布与均匀分布在计算上是不可区分的。

2.3 基于椭圆曲线离散对数假设的变色龙哈希函数

基于椭圆曲线离散对数假设，构造一个变色龙哈希函数，利用它构造在线/离线代理重签名方案。选择大素数 t，$E(F_t)$ 是定义在有限域 F_t 上的一个椭圆曲线，$\#E(F_t)$ 是 $E(F_t)$ 中点的数目。点 $P\in E(F_t)$，P 的阶为素数 q，这里 $q\mid \#E(F_t)$。G 是 P 生成的一个循环群。定义一个安全的哈希函数 $f: Z_q\times G\to Z_q$。具体描述如下：

(1)门限密钥生成算法：选择两个随机数 $k,x\in Z_q$，计算 $Y=xP$，$K=kP$，则门限密钥 TK=(k,x)，公钥 $\mathrm{HK}=(K,Y)$。

(2)哈希函数生成算法：对于公钥 $\mathrm{HK}=(K,Y)$，构造变色龙哈希函数 $\mathrm{CH}_{\mathrm{HK}}: Z_q\times Z_q\to G$，定义为 $\mathrm{CH}(m,r)=f(m,K)P+rY$。

定理 1　$\mathrm{CH}(m,r)=f(m,K)P+rY$ 是一个基于椭圆曲线离散对数假设的变色龙哈希函数。

证明　下面证明 $\mathrm{CH}(m,r)=f(m,K)P+rY$ 满足变色龙哈希函数的性质：

(1)有效性　给定公钥 $\mathrm{HK}=(K,Y)$，一个消息 $m\in Z_q$ 和一个随机数 $r\in Z_q$，在多项式时间内能计算出 $\mathrm{CH}(m,r)=f(m,K)P+rY$。

(2)抗碰撞性　给定公钥 $\mathrm{HK}=(K,Y)$，假设存在一个概率多项式时间算法以一个不可忽略的概率输出 (m_1,r_1) 和 (m_2,r_2)，使得 $\mathrm{CH}(m_1,r_1)=\mathrm{CH}(m_2,r_2)$ 且 $m_1\neq m_2$，则在多项式时间内能计算出 Y 的离散对数 x。即 $f(m_1,K)P+r_1xP=f(m_2,K)P+r_2xP$。

于是有

$$x=(r_2-r_1)^{-1}(f(m_1,K)-f(m_2,K))(\mathrm{mod}\,q)$$

因为椭圆曲线离散对数是个困难问题，而上述结论与椭圆曲线离散对数假设相矛盾，所以这个概率多项式时间算法不存在。即变色龙哈希函数满足抗碰撞性。

(3)门限碰撞　给定公钥 $\mathrm{HK}=(K,Y)$，门限密钥 TK=(k,x)，两个不同的消息 (m_1,m_2) 和一个随机数 r_1，寻找 r_2 使得 $\mathrm{CH}(m_1,r_1)=\mathrm{CH}(m_2,r_2)$。可通过下式在多项式时间内计算出 r_2，

$$r_2=r_1+x^{-1}(f(m_1,K)-f(m_2,K))(\mathrm{mod}\,q)$$

如果 r_1 在 Z_q 中服从均匀分布，那么 r_2 在 Z_q 中也服从均匀分布。　证毕

3 在线/离线代理重签名的形式化定义

定义 2 (代理重签名) 一个代理重签名方案 **PRS**=(**KeyGen**, **ReKey**, **Sign**, **ReSign**, **Verify**)由以下 5 个算法组成[2]：

(1)**KeyGen** 是密钥生成算法：输入一个安全参数 1^k，输出系统参数和用户的公私钥对(pk, sk)。

(2)**ReKey** 是重签名密钥生成算法：输入一个受托者的公私钥对(pk_A, sk_A)和一个委托者的公私钥对(pk_B, sk_B)，输出一个重签名密钥$rk_{A\to B}$。代理者使用$rk_{A\to B}$可将受托者的签名转换为委托者的签名。

(3)**Sign** 是签名生成算法：输入一个消息 m 和一个私钥 sk，输出一个消息 m 的签名σ。可用对应的公钥 pk 来验证签名σ的合法性。

(4)**ReSign** 是重签名生成算法：输入一个重签名密钥$rk_{A\to B}$，一个消息 m，一个公钥pk_A和一个签名σ_A，该算法首先验证σ_A的合法性，若 **Verify** (pk_A, m, σ_A)=1，则输出一个对应于公钥pk_B的消息 m 的签名σ_B；否则，输出$\perp$。

(5)**Verify** 是签名验证算法：输入一个消息 m，一个公钥 pk 和一个签名σ，如果σ是对应于公钥 pk 的消息 m 的合法签名，输出 1；否则，输出 0。

Ateniese 和 Hobenberger 定义了代理重签名的安全模型[2]：外部安全和内部安全。外部安全性可使用户免受来自系统外部的攻击者的恶意攻击，而内部安全性主要考虑来自系统内部的攻击，如代理者发起的攻击或他与委托双方中其中一方的合谋攻击。如果没有一个攻击者在多项式时间内以不可忽略的优势伪造 **PRS** 方案的合法签名，则称 **PRS** 方案在适应性选择消息攻击下是不可伪造的[2,4]。

定义 3 (在线/离线代理重签名) 一个在线/离线代理重签名方案 **OPRS**=(**Rekey**$^{\mathbf{On/Off}}$, **ReSign**$^{\mathbf{On/Off}}$, **Ver**)由以下 3 个算法组成：

(1)**Rekey**$^{\mathbf{On/Off}}$是重签名密钥生成算法：输入一个安全参数 1^k，输出系统参数 params、用户的公私钥对(pk, sk)和代理者的重签名密钥$rk_{A\to B}$。

(2)**ReSign**$^{\mathbf{On/Off}}$是重签名生成算法：该算法分以下两个阶段进行：

(a)离线阶段：输入私钥和重签名密钥，输出状态信息K_i。

(b)在线阶段：输入一个消息 m，一个公钥pk_A，消息 m 的签名ρ_A，状态信息K_i和私钥，首先验证ρ_A的合法性，若 **Verify** (pk_A, m, ρ_A)=1，则输出一个对应于公钥pk_B的消息 m 的重签名ρ_B；否则，输出$\perp$。

(3)**Ver** 是签名验证算法：输入一个消息 m，一个公钥 pk 和一个签名ρ，如果ρ是对应于公钥 pk 的消息 m 的合法签名，输出 1；否则，输出 0。

攻击模型：采用在静态攻陷模式下挑战者$\mathcal{C}$和攻击者$\mathcal{A}$之间的游戏来定义在线/离线代理重签名的安全性模型。攻击者$\mathcal{A}$在游戏开始前必须确定已被攻陷的用户，攻击游戏分 3 个阶段进行。首先是建立阶段，挑战者$\mathcal{C}$生成系统参数 params，并将 params 发送给攻击者$\mathcal{A}$。其次是查询阶段，攻击者$\mathcal{A}$可以适应性地向挑战者$\mathcal{C}$进行用户的公钥/私钥询问、重签名密钥询问、签名询问和重签名询问，挑战者$\mathcal{C}$通过相应的预言机(密钥预言机、重签名密钥预言机、原始签名预言机和重签名预言机)响应攻击者所发起的各种询问请求，并将询问结果返回给攻击者$\mathcal{A}$。这个阶段的安全性定义与一般的代理重签名的安全性定义[2,4]基本相同。最后是伪造阶段，攻击者$\mathcal{A}$输出一个伪造，即一个消息/签名对。

如果攻击者$\mathcal{A}$能生成一个新消息 m 的合法签名，那么我们就说攻击者$\mathcal{A}$伪造成功。攻击者$\mathcal{A}$在上面游戏中的优势可以定义 $\mathrm{Adv}_{\mathcal{A}}$= Pr[$\mathcal{A}$ succeeds]，这个概率完全取决于挑战者$\mathcal{A}$和攻击者$\mathcal{C}$之间的抛币概率。

定义 4 (不可伪造性) 如果没有一个攻击者在多项式时间内以不可忽略的优势赢得上述游戏，那么称在线/离线代理重签名方案 **OPRS** 在适应性选择消息攻击下能抵抗存在性伪造。

基于变色龙函数构造的在线/离线代理重签名方案，其安全性可归约为所关联的代理重签名的安全性或变色龙函数的安全性。如果攻击者输出一个在线/离线代理重签名的伪造，则可利用这个伪造构造一个所关联的代理重签名的伪造或找到变色龙函数的一个碰撞。因此，只要所基于的代理重签名方案是安全的且变色龙哈希函数具有抗碰撞性，则相应的在线/离线代理重签名方案也是安全的。

4 在线/离线代理重签名方案

基于变色龙哈希函数 $\mathrm{CH}(m,r)=f(m,K)P+rY$，本文提出了一个在线/离线代理重签名方案。该方案可将已有的任意一个代理重签名方案[1,2,5−8]转换为一个相应的在线/离线代理重签名方案，用 **PRS** 表示这些方案中的任意一个代理重签名方案。选择大素数t，$E(F_t)$是定义在有限域F_t上的一个椭圆曲线，$\#E(F_t)$是$E(F_t)$中点的数目。$P\in E(F_t)$, P 的阶为素数q, $q\,|\,\#E(F_t)$。G是P生成的一个循环群。签名的消息$m_i\in Z_q$，可通过哈希函数$g:\{0,1\}^*\to Z_q$延伸签名消息空间。选择安全的哈希函数$f: Z_q\times G\to Z_q$。

4.1 方案描述

假定 **PRS**=(**KeyGen**, **ReKey**, **Sign**, **ReSign**, **Verify**)是一个安全的代理重签名方案[2,5−8]，则相应的在线/离线代理重签名方案 **OPRS**=(**Rekey**$^{\mathbf{On/Off}}$, **ReSign**$^{\mathbf{On/Off}}$, **Ver**)由以下 3 个算法组成：

(1)**Rekey**$^{\mathbf{On/Off}}$：主要生成系统参数、用户的公私钥对和重签名密钥，具体描述如下：

(a)输入安全参数 1^k，运行 **PRS** 的 **KeyGen** 算法生成系统参数 params 和用户的公私钥对(pk, sk)。

(b)输入受托者的公私钥对(pk_A, sk_A)和委托者的公私钥对(pk_B, sk_B)，运行 **PRS** 的 **ReKey** 算法生成重签名密钥$rk_{A\to B}$。

(c)选择一个随机数 $x\in Z_q$，计算 $Y=xP$，$X=x^{-1}$，则 $\mathrm{TK}=x$，$\mathrm{HK}=Y$。

(d)选择一个随机数 $k^*\in Z_q$，计算 $h=k^*Y$。

(e)运行 **PRS** 的 **Sign** 算法生成受托者对 h 的原始签名 σ_A。即代理者请求受托者生成 h 的原始签名 σ_A，但代理者不知道受托者的私钥 sk_A 的任何信息。

(f)运行 **PRS** 的 **ReSign** 算法生成委托者对 h 的重签名 σ_B。即代理者使用 $rk_{A\to B}$ 将受托者对 h 的签名 σ_A 转换为委托者对 h 的重签名 σ_B。

公开参数 $(\mathrm{params}, pk_A, pk_B, E(F_t), G, t, q, f, g, \mathrm{CH}(\cdot,\cdot), \sigma_A, \sigma_B, Y, h)$，代理者的重签名密钥是$(rk_{A\to B}, x, X, k^*)$。

(2)**ReSign**$^{\mathbf{On/Off}}$：给定一个重签名密钥$(rk_{A\to B}, x, X, k^*)$，代理者进行如下操作：

(a)离线阶段：

(i)选择一个随机数 $k_i\in Z_q$，计算 $K_i=k_iP$；

(ii)保存状态信息 K_i。

(b)在线阶段：输入一个待签名的消息 $m_i\in Z_q$，一个公钥 pk_A 和消息 m_i 的签名 ρ_{Ai}，代理者进行如下操作：

(i)提取状态信息 K_i；

(ii)计算 $r_i=k^*-f(m_i,K_i)X(\mathrm{mod}\,q)$；

(iii)委托者对消息 m_i 的重签名 $\rho_B=(r_i, K_i, \sigma_B, \rho_{Ai})$；因为 σ_B 作为公开参数发布，所以 m_i 的重签名实际上是 $\rho_B=(r_i, K_i, \rho_{Ai})$。

(3)**Ver**：输入一个消息 m_i，委托者的公钥 pk_B 和一个签名 $\rho_B=(r_i, K_i, \rho_{Ai})$，为了验证 ρ_B 是对应于公钥 pk_B 的消息 m_i 的有效签名，进行如下操作：

(a)计算 $\mathrm{CH}(m_i,r_i)=f(m_i,K_i)P+r_iY$；

(b)运行 **PRS** 的 **Verify** 算法，如果 **Verify**(pk_A, m_i, ρ_{Ai})=1 且 **Verify**$(pk_B, \mathrm{CH}(m_i,r_i), \sigma_B)$=1，那么 ρ_B 是委托者对消息 m_i 的合法重签名，输出 1；否则，输出 0。

4.2 正确性分析

由于 $r_i=k^*-f(m_i,K_i)X(\mathrm{mod}\,q)$，于是有

$$\begin{aligned}\mathrm{CH}(m_i,r_i)&=f(m_i,K_i)P+r_iY=f(m_i,K_i)P\\&+(k^*-f(m_i,K_i)X)Y=f(m_i,K_i)P\\&+(k^*-f(m_i,K_i)x^{-1})xP=f(m_i,K_i)P\\&-f(m_i,K_i)x^{-1}xP+k^*xP=k^*xP=k^*Y=h\end{aligned}$$

因为 σ_B 是 **PRS** 中委托者对 h 的有效重签名，所以 σ_B 也是 **PRS** 中委托者对 $\mathrm{CH}(m_i,r_i)$ 的合法重签名。

4.3 安全性分析

定理 2　在随机预言模型下，如果循环群 G 上的(T,ε)-ECDLP 假设成立，代理重签名方案 **PRS**=(**KeyGen**, **ReKey**, **Sign**, **ReSign**, **Verify**)在适应性选择消息攻击下是不可伪造的，那么本文所提的在线/离线代理重签名方案 **OPRS**=(**Rekey**$^{\mathbf{On/Off}}$, **ReSign**$^{\mathbf{On/Off}}$, **Ver**)在适应性选择消息攻击下也是不可伪造的。

证明　假设 $\mathcal{A}$ 是在线/离线代理重签名方案 **OPRS** 的一个攻击者，**OPRS** 的挑战者将公开参数$(\mathrm{params}, pk_A, pk_B, E(F_t), G, t, q, f, g, \mathrm{CH}(\cdot,\cdot))$发送给 $\mathcal{A}$。q_S 表示 $\mathcal{A}$ 询问签名预言机(包括原始签名预言机和重签名预言机)的最大次数，q_f 表示 $\mathcal{A}$ 询问哈希函数预言机的最大次数。假设(m_i,K_i)是 $\mathcal{A}$ 第 i 次询问哈希函数预言机的输入，预言机返回相应的哈希函数值 e_i；m_j 是 $\mathcal{A}$ 第 j 次询问签名预言机的输入，预言机返回相应的签名(r_j', K_j', ρ_{Aj}')。攻击者 $\mathcal{A}$ 在适应性选择消息攻击下在时间 T 内以不可忽略的概率 ε 成功伪造 **OPRS** 的一个签名(m,r,K,ρ_A)，即

$$\begin{aligned}&\Pr[\mathrm{Verify}(pk_A,m,\rho_A)=1\wedge\mathrm{Verify}(pk_B,\mathrm{CH}(m,r),\\&\sigma_B)=1\wedge h=\mathrm{CH}(m,r)=\mathrm{CH}(m_i,r_i)]\ge\varepsilon\end{aligned}$$

给定系统参数 $(\mathrm{params}, pk_A, pk_B, E(F_t), G, t, q, f, g, \mathrm{CH}(\cdot,\cdot))$，定义一个概率多项式时间算法 $\mathcal{B}$，利用攻击者 $\mathcal{A}$ 的伪造解决一个椭圆曲线离散对数问题的实例。假设 $\mathcal{B}$ 收到的椭圆曲线离散对数问题实例是$(P,aP)\in G$，$\mathcal{B}$ 的目标是确定 aP 的离散对数 $a\in Z_q$。$\mathcal{B}$ 进行如下的操作：

(1)选择一个随机数 $b\in Z_q$，令 $Y=aP$，计算 $h=bY=abP$；运行 **PRS** 的 **Sign** 算法生成 h 的原始签名 σ_A；运行 **PRS** 的 **ReSign** 算法生成 h 的重签名 σ_B；公开(σ_A,σ_B,Y,h)。

(2)维持一个列表，记为 *f*-list，初始值为空。对于 $\mathcal{A}$ 的第 i 次哈希函数值询问(m_i,K_i)，$\mathcal{B}$ 首先检查列表 *f*-list 中是否存在(m_i,K_i)，如果存在，返回 e_i；否则，从 Z_q 中随机选取 e_i，将(m_i,K_i,e_i)添加到 *f*-list 中并返回 e_i。

(3) 对于 $\mathcal{A}$ 的第 j $(1 \le j \le q_S)$ 次签名询问 m_j，$\mathcal{B}$ 首先检查列表 f-list 中是否存在 (m_j, K_j', e_j')，若存在，则计算 $r_j' = Y^{-1}(h - e_j' K_j')$；否则，从 Z_q 中随机选取 (e_j', r_j')，计算 $K_j' = e_j'^{-1}(h - r_j' Y)$，将 (m_j, K_j', e_j') 添加到 f-list 中。然后询问签名预言机获得受托者对消息 m_j 的原始签名 ρ_{Aj}'。最后 $\mathcal{B}$ 返回消息 m_j 的签名 (r_j', K_j', ρ_{Aj}')。

挑战者 $\mathcal{B}$ 返回给攻击者 $\mathcal{A}$ 关于 m_i 的签名与攻击者 $\mathcal{A}$ 询问 **OPRS** 的签名预言机获得的签名，在计算上是不可区分的。最后，攻击者 $\mathcal{A}$ 以大于等于 ε 的概率输出 **OPRS** 的一个伪造 (m, r, K, ρ_A)，这里 $h = f(m,K)P + rY$，$m \ne m_i$，$i = 1, \cdots, q_S$。根据 Forking 引理[9]，假设对于不同的哈希函数值 $f(m,K)$ 和 $f'(m,K)$，攻击者 $\mathcal{A}$ 输出同一消息 m 的两个合法的 **OPRS** 签名 (m, r, K, ρ_A) 和 (m, r', K, ρ_A)，其中 $h = f(m,K)P + rY$, $h = f'(m,K)P + r'Y$，存在下面的等式：

$$f(m,K)P + rY = f'(m,K)P + r'Y$$

$$a = (r' - r)^{-1}(f(m,K) - f'(m,K))$$

于是，攻击者 $\mathcal{B}$ 以大于等于 ε 的概率解决了椭圆曲线离散对数问题的一个实例 $(P, aP) \in G$。如果循环群 G 上的 (T,ε)-ECDLP 假设成立，那么本文所提的在线/离线代理重签名方案 **OPRS**=(**Rekey**$^{\mathbf{On/Off}}$, **ReSign**$^{\mathbf{On/Off}}$, **Ver**)在适应性选择消息攻击下是不可伪造的。 证毕

4.4 有效性分析

在本文所提的在线/离线代理重签名方案中，重签名密钥生成算法的运算主要包括两次椭圆曲线点乘计算，一次代理重签名方案中的密钥生成算法的执行，一次重签名密钥生成算法的执行，一次签名算法的执行和一次重签名算法的执行。由于 σ_B 和 h 是公开参数，σ_B 是 h 的合法重签名，于是只需验证 $\mathrm{CH}(m_i, r_i) = f(m_i, K_i)P + r_i Y = h$，所以签名验证算法 **Ver** 的运算实际上是一次变色龙哈希函数值的计算和两次代理重签名方案中的签名验证算法 **Verify** 的执行。离线阶段重签名算法是一次椭圆曲线点乘运算。在线阶段的重签名算法是寻找变色龙哈希函数的一次碰撞，而寻找这样的一次碰撞仅需要一次模乘法算法和一次模减法运算。由于消息 m_i 的重签名 $\rho_B = (r_i, K_i, \rho_{Ai})$，所以本方案与大部分代理重签名方案[6,7,10]的重签名长度基本相同。

Ateniese 等人[2]指出代理重签名方案 BBS 是不安全的。在 BBS 方案中，任何人都能通过原始签名和重签名计算出重签名密钥并且成为恶意代理者；进一步，委托者(或受托者)可以从重签名密钥计算出受托者(或委托者)的私钥，所以本方案不与 BBS 方案进行签名效率的比较。一旦签名消息到来时，在线阶段生成实际消息的重签名，因此在线/离线代理重签名方案的重签名效率只考虑在线阶段。将已有的代理重签名方案和本方案的重签名算法进行签名效率比较，其结果见表 1。

表 1 重签名算法的性能比较

签名方案	减法运算	乘法运算	幂运算	配对运算
S_{md} 方案[5]	0	0	2	3
S_{uni} 方案[2]	0	1	3	2
Chow-phan 方案[6]	0	4	2	2
Libert-Vergnaud 方案[7]	0	2	6	3
改进的 S_{md} 方案[8]	0	1	4	3
本文的在线/离线方案	1	1	0	0

从表 1 中可以看出，在本文所提的在线/离线代理重签名方案中，在线重签名算法仅需要 1 次模减法运算和 1 次模乘法运算；当签名消息到来时，能在很短的时间生成消息的重签名。而模减法运算和模乘法运算相对于模幂运算和配对运算而言，其计算量是可以忽略不计的。所以，本文所提的在线/离线代理重签名方案大大改善了代理重签名方案的性能，更适用于网络安全应用。

5 结束语

结合门限代理重签名与变色龙哈希函数，本文提出了一个在线/离线代理重签名方案，该方案能将任意一个安全的代理重签名方案转换为一个相应的在线/离线代理重签名方案。在随机预言模型下证明了该方案在适应性选择消息攻击下是不可伪造的，并与已有的代理重签名方案进行了性能比较，其结果表明本方案重签名效率更高，仅需要 1 个模减法运算和 1 个模乘法运算就能生成消息的重签名，具有一定的实用性。将来的工作是设计在标准模型下可证安全的在线/离线代理重签名方案。

参 考 文 献

[1] Blaze M, Bleumer G, and Strauss M. Divertible protocols and atomic proxy cryptography [C]. Proceedings of EUROCRYPT'98, Helsinki, Finland, May 31–June 4, 1998: 127–144.

[2] Ateniese G and Hohenberger S. Proxy re-signatures: new definitions, algorithms, and applications [C]. Proceedings of the 12th ACM CCS, Alexandria, USA, Nov. 7–11, 2005: 310–319.

[3] Chen X, Zhang F, Tian H, *et al.*. Efficient generic on-line/off-line signatures without key exposure [C]. Proceedings of ACNS 2007, Zhuhai, China, June 5–8, 2007: 18–30.

[4] Shao J, Feng M, Zhu B, *et al.*. The security model of unidirectional proxy re-signature with private re-signature key [C]. Proceedings of the 15th Australasian Conference on Information Security and Privacy, Sydney, Australia, July 5–7, 2010: 216–232.

[5] Shao J, Cao Z, Wang L, *et al.*. Proxy re-signature schemes without random oracles [C]. Proceedings of INDO-CRYPT 2007, Chennai, India, Dec. 9–13, 2007: 197–209.

[6] Sherman C and Raphael P. Proxy re-signatures in the standard model[C]. Proceedings of the 11th International Conference on Information Security, Taibei, China, Sept. 15–18, 2008: 260–276.

[7] Benoit L and Damien V. Multi-use unidirectional proxy re-signatures [C]. Proceedings of the 15th ACM Conference on Computer and Communications Security, Alexandria, USA, Oct. 27–31, 2008: 511–520.

[8] Kiate K, Ikkwon Y, and Secogan L. Remark on shao et al'.s bidirectional proxy re-signature scheme in indocrypt'07 [J]. *International Journal of Network Security*, 2009, 9(1): 8–11.

[9] David P and Jacques S. Security arguments for digital signatures and blind signatures [J]. *Journal of Cryptology*, 2000, 13(3): 361–369.

[10] Deng Y, Du M, and You Z, *et al.*. A blind proxy re-signatures scheme based on standard model [J]. *Journal of Electronics & Information Technology*, 2010, 32(5): 1119–1223.

杨小东： 男，1981 年生，副教授，博士，研究方向为公钥密码体制、数字签名和网络安全.

王彩芬： 女，1963 年生，副院长，教授，博士生导师，研究方向为密码协议、网络编码和量子密码.