EDL签名中可证明安全的阈下信道封闭协议

张应辉[1,2] 马 华[1] 王保仓[2]
(西安电子科技大学理学院 西安 710071)[1]
(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)[2]

摘 要 首先构造了EDL签名方案中的阈下信道,然后设计了一个交互式阈下信道封闭协议,完全封闭了EDL签名中由参数的随机性所引入的阈下信道,并在RO(random oracle)模型中给出了安全性证明。在CDH(computational Diffie-hellman)问题是困难的假设下,新协议被证明是安全的。在新协议中,看守虽然参与了签名的生成,但却不能伪造签名,从而保证了签名者的签名权力。在计算量方面,签名者和看守分别执行2次和3次模指数运算。

关键词 密码学,数字签名,信息隐藏,阈下信道,封闭协议,随机预言机模型
中图法分类号 TP309 **文献标识码** A

Provably Secure Subliminal-free Protocol in EDL Digital Signature

ZHANG Ying-hui[1,2] MA Hua[1] WANG Bao-cang[2]
(School of Science, Xidian University, Xi'an 710071, China)[1]
(Key Laboratory of Computer Networks & Information Security, Ministry of Education, Xidian University, Xi'an 710071, China)[2]

Abstract Subliminal channels in EDL signature were constructed firstly, then an interactive subliminal-free protocol was designed. It is shown that the proposed protocol can completely close subliminal channels existing in the random parameters in EDL signature. The proposed protocol is proved to be secure in RO(random oracle) model assuming the CDH(computational Diffie-hellman) problem is hard. In the new protocol, the warden participates the generation of signature, but can not sign messages. Thus, the signature authority of the signer is guaranteed. To generate a signature, it only needs to perform 2 and 3 modular exponentiation for the signer and the warden respectively.

Keywords Cryptography, Digital signature, Information hiding, Subliminal channel, Free protocol, Random oracle model

阈下信道最早是由G. J. Simmons于1978年在美国圣地亚国家实验室(Sandia National Labs)提出的[1]。通过引入囚犯模型,Simmons证明了当时美国用于核查系统的安全协议存在缺陷,由此正式命名了阈下信道。阈下信道分为宽带阈下信道和窄带阈下信道[2]。利用与阈下收方共享的秘密密钥,阈下发方对一个无害的消息进行签名,但在签名中隐藏阈下信息,阈下收方收到签名后,确认消息来自于阈下发方,然后忽略无害消息,用共享秘密密钥提取阈下信息。除收方外,任何其他人均不知道密码数据中是否有阈下信息存在[3,4]。

数字签名是实现认证这一密码技术的重要工具,它在信息安全,特别是在大型网络安全通信中的密钥分配、认证以及电子商务系统中具有重要作用。然而,已有的绝大多数签名体制中都可能存在阈下信道。Simmons指出ElGamal数字签名算法中存在阈下信道[5],还在DSA数字签名算法中成功地构造了一个宽带阈下信道。NTRU签名方案和基于椭圆曲线密码体制的阈下信道[6]也已被提出。阈下信道具有隐藏通信事实的特点,使得阈下信道可被合法用户用于传递秘密信息[7],又可使得犯罪分子传递信息而不被发现,这对信息安全是一个很大的挑战。

这样就提出一个亟待解决的密码学问题:设计一个安全的签名协议以满足认证性要求,同时必须保证协议中不存在阈下信道。Eu-Jin Goh等人基于Schnorr签名设计了EDL签名方案[8],在CDH(computational Diffie-Hellman)问题是困难的假设下,对EDL签名给出了规约很紧的安全性证明,这使得该签名方案得到了业界的广泛重视。然而,本文指出EDL签名协议中仍然存在阈下信道,并利用协议中的随机参数构造了2个阈下信道。为了解决上述密码学问题,必须建立基于签名方案的阈下信道封闭协议[9]。本文基于EDL签名方案,设计了一个交互式阈下信道封闭协议,并在RO(random oracle)模型[10]中给出了安全性证明。在CDH问题是困难的假设下,新协议被证明是安全的。

1 预备知识

本节介绍下文所使用的符号及相关定义。

1.1 符号说明

(1) $s \xleftarrow{R} S$:从集合S中随机选取一个元素s。

(2) l_t:元素t的二进制(比特)长度。

(3) $m||r$:比特串m和r的级联。

到稿日期:2009-10-26 返修日期:2010-01-24 本文受国家自然科学基金(60803149)资助。
张应辉(1985—),男,博士生,主要研究方向为密码学与信息安全,E-mail:prrd2007@163.com;马 华(1963—),女,教授,主要研究方向为密码学;王保仓(1979—),男,副教授,主要研究方向为密码学与信息安全。

(4) $G_{p,g}$：以 g 为生成元的 q 阶循环群，即 $G_{p,g}=\{g^0, g^1, \cdots, g^{q-1}\}$，它是有限域 $GF(p)$ 的乘法群 $GF^*(p)$ 的子群。这里 p,q 是两个大素数，满足 $q|p-1$。

1.2 安全性相关定义

定义 1(数字签名方案在适应性选择消息攻击下的安全性)[8]

对于一个数字签名方案，如果一个算法 F 能够在时间 t 内，任意作 q_H 次 Hash 询问(对应哈希函数 H)和 q_{sig} 次签名询问后，至少以概率 ε(概率取于算法 F，Hash 询问和签名询问的内部掷币之上)伪造出该签名方案的一个有效签名，则称算法 F 是该签名方案的一个$(t,q_H,q_{sig},\varepsilon)$-伪造者。

如果一个数字签名方案不存在$(t,q_H,q_{sig},\varepsilon)$-伪造者，则称该签名方案在 RO 模型中是$(t,q_H,q_{sig},\varepsilon)$-安全的。

定义 2(CDH 假设)[8]

对于一个概率多项式时间算法 A，如果以$((p,q,g),(g^a,g^b))$为输入，在时间 t 内，A 计算出 $DH_{p,g}(g^a,g^b)=g^{ab}$ 的概率至少为 ε(概率取于算法的内部掷币和随机变量(a,b)之上)，则称算法 A 在群 $G_{p,g}$ 中(t,ε)-解决 CDH 问题。

如果不存在(t,ε)-解决 CDH 问题的概率多项式时间算法 A，则称群 $G_{p,g}$ 是一个(t,ε)-CDH 群。

2 EDL 签名中的阈下信道

2.1 EDL 签名方案介绍

EDL 签名涉及到两个独立的安全 Hash 函数：$H:\{0,1\}^* \to G_{p,g}$ 和 $H':(G_{p,g})^6 \to \mathbb{Z}_q$。设签名者为 S，待签名的消息为 m，签名验证者为 V。则具体方案如下：

(1) 密钥生成

S 选取整数 $x \xleftarrow{R} (1,q)$，相应的签名公钥为 $y \equiv g^x \pmod p$。

(2) 签名生成

S 选取 $r \xleftarrow{R} \{0,1\}^{l_r}$，计算 $h=H(m||r)$，$z \equiv h^x \pmod p$，此时有 $DL_h(z)=DL_g(y)$。S 再选取 $k \xleftarrow{R} (1,q)$，计算 $u \equiv g^k \pmod p$，$v \equiv h^k \pmod p$，$c=H'(g||h||y||z||u||v)$ 和 $s \equiv k+cx \pmod q$。

对消息 m 的签名即为 $\sigma=(z,r,s,c)$，S 将签名消息(m,σ)发送给 V。

(3) 签名验证

V 收到(m,σ)后，计算 $h'=H(m||r)$，$u' \equiv g^s y^{-c} \pmod p$，$v' \equiv h^s z^{-c} \pmod p$，令 $c'=H'(g||h||y||z||u||v)$，最后根据 $c'=c$ 是否成立判定签名的有效性。

2.2 EDL 签名中阈下信道的构造

设阈下发方为 S，阈下收方为 V。我们利用参数的随机性，构造出以下 2 个阈下信道，说明了 EDL 签名方案的不足。

(1) 利用 $r \xleftarrow{R} \{0,1\}^{l_r}$：$S$ 选取 r，直到 r 的某些固定位比特为阈下比特，V 收到(z,r,s,c)后，就可从 r 中提取阈下信息。或者，对于确定的 m，S 选取 r，直到 $h(=H(m||r))$的某些固定位比特为阈下比特，则 V 收到(z,r,s,c)后，求解出 h 就可以提取阈下信息。

(2) 利用 $k \xleftarrow{R} (1,q)$：S 选取 k，直到 $u(\equiv g^k \pmod p)$的某些固定位比特为阈下比特，则 V 收到(z,r,s,c)后，根据 $u \equiv g^s y^{-c} \pmod p$解出 u，就可获得阈下信息。

3 阈下封闭协议的设计

为了封闭阈下信道，我们使阈下发方和阈下收方之间的看守 W 参与协议的执行。看守 W 选取整数 $t \xleftarrow{R} (1,q)$，则 $\gcd(t,q)=1$，计算 $T \equiv g^t \pmod p$，保密 t，公开 T。公开发布 3 个安全的哈希函数 H_0,H_1 和 H_2，其中 $H_0:\{0,1\}^* \to G_{p,g}$，$H_1:\{0,1\}^* \times G_{p,g} \to G_{p,g}$，$H_2:\{0,1\}^* \times (G_{p,g})^6 \to \mathbb{Z}_q$。

3.1 密钥生成

签名者 S 选取整数 $x \xleftarrow{R} (1,q)$，相应的签名公钥为 $y \equiv T^x \pmod p$。

3.2 交互式阈下封闭协议

设 $m \in \{0,1\}^*$ 为有意义的待签名消息，则签名者 S 和看守 W 之间的交互如下：

Step1 S 计算 $h_0=H_0(m)$，发送 h_0 给 W。

Step2 W 选取整数 $k_w \xleftarrow{R} (1,q)$，计算 $r \equiv y^{k_w^{-1}} \pmod p$，发送 r 给 S。

Step3 S 计算 $h_1=H_1(m||r)$，$z_1 \equiv h_1^x \pmod p$，则有离散对数等式 $DL_{h_1}(z_1)=DL_T(y)$。S 将(h_1,z_1)发送给 W。

Step4 W 计算 $z \equiv z_1^t \pmod p$，将 z 发送给 S。

Step5 S 选取整数 $k_A \xleftarrow{R} (1,q)$，计算 $\alpha_0 \equiv g^{k_A} \pmod p$，$\beta_0 \equiv h_1^{k_A} \pmod p$，发送$(\alpha_0,\beta_0)$给 W。

Step6 W 计算 $\alpha \equiv \alpha_0^{k_w} \equiv g^{k_A k_w} \pmod p$，$\beta \equiv \beta_0^{k_w} \equiv h_1^{k_A k_w} \pmod p$，发送$(\alpha,\beta)$给 S。

Step7 S 计算 $c=H_2(m||g||T||y||z||\alpha||\beta)$，发送 c 给 W。

Step8 W 计算 $\theta \equiv c \cdot t \cdot k_w^{-1} \pmod q$，发送 θ 给 S。

Step9 S 计算 $s' \equiv k_A + \theta \cdot x \pmod q$，发送$(m,s')$给 W。

3.3 签名生成

W 收到(m,s')后，检验 $h_0=H_0(m)$ 和 $h_1=H_1(m||r)$ 是否同时成立，若不成立，则终止协议；否则计算 $s \equiv k_w \cdot s' \equiv k_A k_w + xtc \pmod q$，从而得到对消息 m 的签名 $\sigma=(z,r,s,c)$，W 将其发送给签名验证者 V。

3.4 签名验证

当签名验证者 V 收到(z,r,s,c)后，计算 $h_1=H_1(m||r)$，$\alpha' \equiv g^s y^{-c} \pmod p$，$\beta' \equiv h_1^s z^{-c} \pmod p$，令 $c'=H_2(m||g||T||y||z||\alpha'||\beta')$，最后根据 $c'=c$ 是否成立判定签名的有效性。

3.5 签名的正确性

签名的正确性由以下两点保证：

(1) 当(z,r,s,c)是对消息 m 的有效签名时，一定有 $s \equiv k_A k_w + xtc \pmod q$。令 $h_1=H_1(m||r)$，从而得到

$$\alpha' \equiv g^s y^{-c} \equiv g^{k_A k_w + xtc} y^{-c} \equiv g^{k_A k_w} T^{xc} y^{-c} \equiv g^{k_A k_w} y^c y^{-c} \equiv g^{k_A k_w} \equiv \alpha \pmod p$$

$$\beta' \equiv h_1^s z^{-c} \equiv h_1^{k_A k_w} h_1^{xtcz^{-c}} \equiv h_1^{k_A k_w} z_1^{xc} z^{-c} \equiv h_1^{k_A k_w} z^c z^{-c} \equiv h_1^{k_A k_w} \equiv \beta \pmod p$$

因此 $c'=H_2(m||g||T||y||z||\alpha'||\beta')=H_2(m||g||T||y||z||\alpha||\beta)=c$。

(2) 如果 $c'=c$，则(z,r,s,c)一定是对消息 m 的有效签名，否则 $s \neq k_A k_w + xtc \pmod q$，从而 $\alpha' \neq \alpha \pmod p$，$\beta' \neq \beta \pmod p$，因此 $c'=H_2(m||g||T||y||z||\alpha'||\beta') \neq H_2(m||g||T||y||z||\alpha||\beta)=c$，这与前提条件 $c'=c$ 相矛盾。

4 安全性和性能分析

首先规划了协议的安全模型，然后给出了基于 RO 模型的安全性证明，最后讨论了协议的阈下封闭性和效率。

4.1 签名的安全性

4.1.1 安全模型规划

这里的安全性特指伪造签名。对于一般的数字签名方案，由于只有签名者和验证者参与了签名协议，因此，验证者和任意第三方伪造签名的能力没有差别，敌手就是任意第三方。在本文的协议中，由于看守参与了签名的生成，因此看守比协议外的任意第三方伪造签名的能力更强。基于以上考虑，我们认为看守就是敌手，这是与一般签名方案安全模型的主要区别。当敌手经过一系列 Hash 询问和签名询问后，如果能够以不可忽略的概率伪造出一个新的签名，就称敌手成功。为了能够使协议顺利执行，敌手必须按照协议的步骤与签名者进行交互。

4.1.2 安全性证明

上述协议的安全性由下面的定理 1 给出。

定理 1 如果 $G_{p,g}$ 是一个 (t',ε')-CDH 群，则在 RO 模型中，本文所给的方案是 $(t,q_{H_0},q_{H_1},q_{H_2},q_{sig},\varepsilon)$-安全的，这里 $t\leqslant t'-(q_{H_1}+4\cdot q_{sig})\cdot C_{exp}(G_{g,p}),\varepsilon\geqslant\varepsilon'+q_{sig}\cdot(q_{H_0}+q_{sig})\cdot 2^{-l_m}+q_{sig}\cdot(q_{H_1}+q_{sig})\cdot 2^{-l_r}+q_{sig}\cdot(q_{H_2}+q_{sig})\cdot 2^{-3l_q}+(q_{H_2}+1)\cdot 2^{-l_q}$，其中，$C_{exp}(G_{g,p})$ 表示群 $G_{g,p}$ 上的一次模指数运算所耗费的时间。

证明：基于文献[8,11]的基本思想，假设 F 是本文方案的一个 $(t,q_{H_0},q_{H_1},q_{H_2},q_{sig},\varepsilon)$-伪造者，则可以构造一个“模仿”算法 A，以 $((p,q,g),(g^a,g^b))$ 为输入，在时间 t 内，A 计算出 $DH_{p,g}(g^a,g^b)=g^{ab}$ 的概率至少为 ε，从而与 CDH 假设矛盾。

A 首先公布签名公钥 $y\equiv g^a \pmod p$（私钥 a 未知），然后向 F 模仿签名协议，并回答 F 的询问，最终目的是把 F 的一个可能的伪造签名 (m,σ) 转化成求解 $DH_{p,g}(g^a,g^b)=g^{ab}$ 的算法。A 把 F 作为子程序，并维护 L_0,L_1,L_2,L_s 4 张列表，这些列表开始都为空，L_0,L_1,L_2 分别用于跟踪 F 对预言机 H_0,H_1,H_2 的询问，L_s 用于模拟签名预言机。下面详细解释这些列表的建立。

H_0 询问：如果 (m,h_0) 在表 L_0 中，A 返回 h_0；否则选取 $h_0\xleftarrow{R}G_{p,g}$，将 (m,h_0) 添加到表 L_0 中，返回 h_0。

H_1 询问：如果 $((m,r),h_1)$ 在表 L_1 中，S 返回 h_1；否则选取 $d\xleftarrow{R}(1,q)$，令 $h_1=g^{bd}$，将 $((m,r),h_1)$ 添加到表 L_1 中，返回 h_1。

H_2 询问：如果 $((m,g,T,y,z,\alpha,\beta),c)$ 在表 L_2 中，S 返回 c；否则选取 $c\xleftarrow{R}(1,q)$，将 $((m,g,T,y,z,\alpha,\beta),c)$ 添加到表 L_2 中，返回 c。

签名询问：假设 F 询问对消息 m 的签名之前，已经对 m 执行了 H_0 询问。A 试图在不知道私钥 a 的前提下，构造有效的签名 $(m,\sigma)=(m,(z,r,s,c))$，详细过程如下：

(1) 如果 A 在表 L_0 中寻找到含有 m 的项，则放弃模拟；否则选取 $h_0\xleftarrow{R}G_{p,g}$，将 (m,h_0) 添加到表 L_0 中，令 $H_0(m)=h_0$。

(2) A 收到 $r(\equiv y^w \pmod p)$ 后，如果在表 L_1 中找到含有 (m,r) 的项，则放弃模拟；否则选取 $j\xleftarrow{R}(1,q)$，令 $z_1\equiv y^j \pmod p$，$h_1\equiv T^j \pmod p$，将 $((m,r),h_1)$ 添加到表 L_1 中，定义 $h_1=H_1(m||r)$，将 (h_1,z_1) 发送给 F。注意 $DL_{h_1}(z_1)=DL_T(y)$，即有 $h_1{}^a\equiv z_1 \pmod p$。

(3) A 收到 $z(\equiv z_1^t \pmod p)$ 后，选取 $s'\xleftarrow{R}(1,q)$，$c\xleftarrow{R}(1,q)$，取 $\alpha_0\equiv g^{s'}r^{-c} \pmod p$，$\beta_0\equiv h_1^{s'}z^{-c} \pmod p$，发送 (α_0,β_0) 给 F。

(4) A 收到 (α,β) 后，如果在表 L_2 中找到含有 (m,g,T,y,z,α,β) 的项，则放弃模拟；否则定义 $H_2(m,g,T,y,z,\alpha,\beta)\triangleq c$，并将 $((m,g,T,y,z,\alpha,\beta),c)$ 添加到表 L_2 中，这里 $\alpha\equiv\alpha_0^k w \pmod p$，$\beta\equiv\beta_0^k w \pmod p$。

(5) A 发送 s' 给 F，F 即得到对 m 的签名 $\sigma=(z,r,s,c)$，这里 $s\equiv k_w\cdot s'\equiv k_A k_w+atc \pmod q$。

解决 CDH 问题

对一个新的消息 m，A 调用 F，假设 F 以不可忽略的概率返回了有效的签名 $\sigma=(z,r,s,c)$。如果以下两个条件同时成立，A 就能以不可忽略的概率解决 CDH 问题。

(1) F 对 (m,r) 进行过 H_1 询问，即在表 L_1 中可以找到 (m,r) 的对应项；

(2) 离散对数等式 $DL_{h_1}(z_1)=DL_T(y)$ 成立，这里 $T^u\equiv y \pmod p$；

由(1)可得 $h_1=H_1(m||r)=g^{bd}$，由(2)可得 $h_1^a\equiv z_1 \pmod p$，从而 $z_1\equiv(g^{bd})^a\equiv(g^{ab})^d \pmod p$，因此 $z_1^{1/d}\equiv g^{ab} \pmod p$，这样 A 就求解出 $DH_{p,g}(g^a,g^b)=g^{ab}$。

A 解决 CDH 问题的概率分析

为叙述方便，我们用 ε_{abort} 表示 A 放弃模拟的概率；NH_1 表示 F 对 (m,r) 没有进行过 H_1 询问就伪造出 m 的有效签名这一事件；NQ 表示 F 伪造出 m 的有效签名，但 $DL_{h_1}(z_1)\neq DL_T(y)$ 这一事件；这样，A 解决 CDH 问题的概率就是 $\varepsilon-(\varepsilon_{abort}+\Pr(NH_1\cup NQ))$。

下面给出具体的求解过程。

(1) 签名询问可能在第一步失败，即 A 在表 L_0 中找到含有 m 的项。因为至多有 $q_{H_0}+q_{sig}$ 个这样的 m，故碰撞概率至多为 $(q_{H_0}+q_{sig})\cdot 2^{-l_m}$，这样对 q_{sig} 个签名询问而言，失败概率至多为 $q_{sig}\cdot(q_{H_0}+q_{sig})\cdot 2^{-l_m}$。

(2) 签名询问可能在第二步失败（假设已通过第一步确定了 m，现在只有 r 可变），即 A 在表 L_1 中找到含有 (m,r) 的项。因为至多有 $q_{H_1}+q_{sig}$ 个这样的 (m,r)，故碰撞概率至多为 $(q_{H_1}+q_{sig})\cdot 2^{-l_r}$，这样对 q_{sig} 个签名询问而言，失败概率至多为 $q_{sig}\cdot(q_{H_1}+q_{sig})\cdot 2^{-l_r}$。

(3) 签名询问可能在第四步失败，即 A 在表 L_2 中找到含有 (m,g,T,y,z,α,β) 的项。因为至多有 q_{H_2} 个这样的 (m,g,T,y,z,α,β)，其中 m,g,T,y 已经确定，$z\equiv y^{j\cdot t} \pmod p$，而 (j,α,β) 在 $\mathbb{Z}_q\times G_{p,g}^2$ 上均匀分布，且 H_2 至多被询问 $q_{H_2}+q_{sig}$ 次，故碰撞概率至多为 $(q_{H_2}+q_{sig})\cdot 2^{-3l_q}$，这样对 q_{sig} 个签名询问而言，失败概率至多为 $q_{sig}\cdot(q_{H_2}+q_{sig})\cdot 2^{-3l_q}$。

(4) 如果事件 $NH_1\cup NQ$ 发生，则 A 不能解决 CDH 难题。易知 $\Pr(NH_1\cup NQ)=\Pr(NH_1\cap\overline{NQ})+\Pr(NQ)$。对于 $\Pr(NH_1\cap\overline{NQ})$：这时事件 NH_1 和 $\overline{NQ}$ 同时发生，故对于一个有效的伪造签名而言，有等式 $z_1^{-x}=h_1=H_1(m||r)$ 成立，由

（下转第 93 页）

ference on Information, Communications & Signal Processing. Singapore, 2007: 1-5

[3] Bölcskei H, Duhamel P, Hleiss R. Orthogonalization of OFDM/OQAM pulse shaping filters using the discrete Zak transform [J]. Signal Processing, 2003, 83(7): 1379-1391

[4] TIA Committee TR-8. 5. Wideband Air Interface Isotropic Orthogonal Transform Algorithm(IOTA)-Public Safety Wideband Data Standards Project-Digital Radio Technical Standards [S]. TIA-902. BBAB(Physical Layer Specification, Mar. 2003) and TIA-902. BBAD(Radio Channel Coding(CHC) Specification, Aug. 2003

[5] Lele C, Siohan P, Legouable R, et al. Preamble-based channel estimation techniques for OFDM/OQAM over the powerline[C]// IEEE International Symposium on Power Line Communications and its Applications. Pisa, Italy, 2007: 59-64

(上接第 74 页)

于 H_1 是随机预言，故等式成立的概率至多为 2^{-l_q}。对于 Pr(NQ)：设 $\alpha\equiv g^k \pmod p$，$\beta\equiv h_1^{k'} \pmod p$，$y\equiv T^x\equiv g^{tx} \pmod p$，但 $z_1\equiv h_1^{x'}\neq h^x \pmod p$。由于签名是有效的，根据签名验证可知，$\alpha\equiv g^s y^{-c} \pmod p$，$\beta\equiv h_1^s z^{-c} \pmod p$，从而有 $k=s-ctx$，$k'=s-cx'$，这样就得到 $H_2(m||g||T||y||z||\alpha||\beta)=c=(k-k')/(x'-t\cdot x)$。由于 H_2 是随机预言，因此，F 在全部 H_2 询问中找到上述 c 的概率至多为 $q_{H_2}\cdot 2^{-l_q}$。

综上可知，A 成功解决 CDH 问题的概率至少为 $\varepsilon-(\varepsilon_{short}+\Pr(NH_1\cup NQ))=\varepsilon-(q_{sig}\cdot(q_{H_0}+q_{sig})\cdot 2^{-l_m}+q_{sig}\cdot(q_{H_1}+q_{sig})\cdot 2^{-l_r}+q_{sig}\cdot(q_{H_2}+q_{sig})\cdot 2^{-3l_q}+2^{-l_q}+q_{H_2}\cdot 2^{-l_q})$。

运行时间分析

A 的运行时间就是 F 的运行时间与群 $G_{p,g}$ 中的许多模指数运算时间之和。注意到一次 2 个指数幂乘运算大约相当于 1.2 次指数运算，从而运行时间为 $(q_{H_1}+4\cdot q_{sig})\cdot C_{exp}(G_{p,g})$。

因此原假设与 CDH 假设相矛盾，证毕。

4.2 协议的阈下封闭性

除了验证公钥 y 和 T 等公共参数外，接收者唯一能够获得的是签名消息$(m,(z,r,s,c))$，因此，签名者要传递阈下信息必须以签名(z,r,s,c)为载体。

由交互协议可以看出：尽管由 S 执行 $h_1=H_1(m||r)$，但他由于不知道 k_w 和秘密参数 t 的信息，因此不能控制 $r(\equiv y^{k_w^{-1}} \pmod p)$的取值，也就不能控制 h_1 的取值，而 $z_1\equiv h_1^x \pmod p$，$z\equiv z_1^t \pmod p$，因此也不能控制 z 的取值，从而不能控制 $c=(H_2(m||g||T||y||z||\alpha||\beta))$的取值。另外，尽管 S 能够得到 $\alpha(\equiv g^{k_A k_w} \pmod p)$，$\beta(\equiv h_1^{k_A k_w} \pmod p)$和 $\theta(\equiv c\cdot t\cdot k_w^{-1} \pmod q)$，但他由于不知道秘密参数 t，因此以不能获得关于 k_w，g^{k_w} 的任何信息，直至 W 完成最终签名之前，S 对 k_w，g^{k_w} 都是一无所知，因而不能控制 $s(\equiv k_w\cdot s' \pmod q)$的取值。特别地，如果 S 在 Step4 不使用 W 生成的 r，W 可以在签名生成时检测出来，从而终止协议。

由以上分析可知，发送者不能传送任何阈下信息给接收者，因此该协议封闭了由参数的随机性所引入的阈下信道。

4.3 计算复杂度及通信量

比起模指数运算，模乘和模加等运算的复杂度可以忽略，因此仅考虑模指数运算的复杂度。在本文的协议中，签名者和看守分别执行 2 次和 3 次模指数运算(不计预计算)，各进行 5 次数据传递，以此代价首次实现了 EDL 签名方案中由参数的随机性所引入的阈下信道的完全封闭，并确保了协议在 RO 模型中是安全的。

结束语 EDL 数字签名方案有着规约很紧的安全性证明，受到了业界的广泛重视。本文首先构造了 EDL 签名中的阈下信道，说明了 EDL 签名方案确实存在不足。接着，设计了一个交互式阈下信道封闭协议，它完全封闭了 EDL 签名中由参数的随机性所引入的阈下信道。基于 CDH 问题的困难性假设，在 RO 模型中证明了新协议是安全的。在新协议中，签名者签署的消息必须经过看守的审批方能生效。将来的目标是设计更有效的阈下信道封闭协议。

参 考 文 献

[1] Simmons G J. The 'prisoners' Problem and the Subliminal Channel[C]// Advances in Cryptology, Proc. Crypto'83. Springer Verlag, 1984: 51-66

[2] 董庆宽，肖国镇. 阈下信道分类及边信息协商问题研究[J]. 计算机科学，2004，31(5)：103-106

[3] Simmons G J. Subliminal Channels: Past and Present[J]. European Transactions on Telecommunications, 1994, 4(4): 459-473

[4] Simmons G J. Subliminal Communication Is Easy Using the DSA[C]// Proc. of Eurocrypt 93. 1994: 218-232

[5] Simmons G J. The Subliminal Channel and Digital Signature[C]// Advances in Cryptograph-Eurocrypt'84. Springer-Verlag, 1985: 364-378

[6] Xie Yuhua, Sun Xingming, Xiang Lingyun, et al. A Security Threshold Subliminal Channel Based on Elliptic Curve Cryptosystem[C]// Proceedings-2008 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP. 2008: 294-297

[7] Kobara K, Imai H. On the Channel Capacity of Narrowband Subliminal Channels [C] // Proc. of the Second International Conference on Information and Communication Security. Berlin: Springer-Verlag, 1999: 309-324

[8] Goh EJ, Jarecki S. A Signature Scheme as Secure as the Diffie-Hellman Problem[C]// Biham E, ed. Advances in Cryptology-EUROCRYPT 2003. LNCS 2656. Berlin: Springer-Verlag Publishers, 2003: 401-415

[9] Meng Tao, Wang Jianfeng, Sun Shenghe. Cover Communication Based on Subliminal Channel in Broadcast Multi Signature[C] // Proceedings-2008 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP. 2008: 309-1311

[10] Bellare M, Rogaway P. Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols[C] // Proc. of the 1st ACM Conf. on Computer and Communications Security. New York: ACM Press, 1993: 62-73

[11] 陈伟东，冯登国，谭作文. 指定验证方的门限验证签名方案及安全性证明[J]. 软件学报，2005，16(11)：1967-1974