指定验证方的门限验证签名方案及安全性证明*

陈伟东[1,2+], 冯登国[3], 谭作文[4]

[1](信息安全国家重点实验室(中国科学院 研究生院),北京 100049)

[2](中国科学院 电子学研究所,北京 100080)

[3](信息安全国家重点实验室(中国科学院 软件研究所),北京 100080)

[4](中国科学院 数学与系统科学研究院 系统科学研究所,北京 100080)

Signature Scheme for Specified Threshold Verifiers and Security Proofs

CHEN Wei-Dong[1,2+], FENG Deng-Guo[3], TAN Zuo-Wen[4]

[1](State Key Laboratory of Information Security (Graduate School, The Chinese Academy of Sciences), Beijing 100049, China)

[2](Institute of Electronics, The Chinese Academy of Sciences, Beijing 100080, China)

[3](State Key Laboratory of Information Security (Institute of Software, The Chinese Academy of Sciences), Beijing 100080, China)

[4](Institute of Systems Science, Academy of Mathematics and System Sciences, The Chinese Academy of Sciences, Beijing 100080, China)

+ Corresponding author: Phn: +86-10-62645407, Fax: +86-10-62645000, E-mail: wsy@163.net, http://www.tsinghua.edu.cn

Received 2004-03-23; Accepted 2005-06-02

Chen WD, Feng DG, Tan ZW. Signature scheme for specified threshold verifiers and security proofs. *Journal of Software*, 2005,16(11):1967−1974. DOI: 10.1360/jos161967

Abstract: The problem called “constructing signature schemes for specified verifiers” is proposed by Laih, and such a scheme is also given by Laih. It is shown that this scheme is not secure and a scheme called SV-EDL is put forward. Furthermore, the provable security theory is used to analyze such schemes, i.e. the security of SV-EDL scheme is proved in RO (random oracle) model. The security against forgery is tightly related to the Computational Diffie-Hellman problem, i.e. the forgery is almost as difficult as solving CDH (computational Diffie-Hellman) problem. Especially, for anyone except the specified verifiers, the ability of verifying signature is tightly related to DDH (decisional Diffie-Hellman) problem. Since the hardness of the CDH and DDH problem is widely believed to be closely related to the hardness of the DL (discrete logarithm) problem, the scheme offers better security guarantees than the existing schemes. In addition, it offers non-repudiation in a very straight-forward manner. Finally, the concept of threshold verification is proposed and a (t,m)-threshold verification protocol is constructed, and its security is proved in the standard model. Especially, the scheme does not ask for the existence of the trusted center.

* Supported by the National Natural Science Foundation of China under Grant No.60253027 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802 (国家重点基础研究发展规划(973))

作者简介: 陈伟东(1969－),男,四川中江人,博士生,高级工程师,主要研究领域为密码学及其应用;冯登国(1965－),男,博士,研究员,博士生导师,主要研究领域为信息与网络安全;谭作文(1967－),男,博士,主要研究领域为密码学及其应用.

Key words: signature scheme; provable security; computational Diffie-Hellman assumption; decisional Diffie-Hellman assumption; random oracle model

摘 要: Laih 提出了指定验证方的签名方案设计问题,并给出一种解决方案.首先分析指出该方案存在严重安全缺陷,然后提出了签名方案 SV-EDL,解决了如上密码学问题.同时,把可证明安全理论引入这类方案的分析设计,并在 RO(random oracle)模型中证明:SV-EDL 的抗伪造安全性和计算 Diffie-Hellman(computational Diffie-Hellman,简称 CDH)问题紧密关联,亦即伪造 SV-EDL 签名几乎和解决 CDH 问题一样困难;除指定方以外,任何人验证签名的能力都与决策 Diffie-Hellman(decisional Diffie-Hellman,简称 DDH)问题密切相关.由于 CDH 问题和 DDH 问题的困难性与离散对数(discrete logarithm,简称 DL)问题紧密相关已成为广泛共识,因此与当前同类方案比较,该签名方案提供了更好的安全性保证.此外,上述签名方案还以非常简明、直接的方式满足不可否认要求.最后提出并构造了验证服务器系统的门限验证协议,并在标准模型中给出了安全性证明.该方案不要求可信中心的存在.

关键词: 数字签名方案;可证明安全性;计算 Diffie-Hellman(CDH)假设;决策 Diffie-Hellman(DDH)假设;随机预言模型

中图法分类号: TP309 文献标识码: A

数字签名方案是主要认证机制之一.普通签名的一个共同特点是,任何一方都可以验证签名的合法性.但是在某些特定情况下,要求只有预先指定的一个或一组验证方可以验证签名的合法性,除此之外的任何第三方都无法验证签名的合法性.例如,电子投标就是一个这方面的应用实例[1].

这样就提出了一个密码学问题:设计一个签名方案,确保只有指定的验证服务器(specified verification server,简称 SVS)(集合)可以验证签名是否合法.1996 年 Laih 提出了一个满足上述要求的多签名方案[1],但在 2002 年,文献[2]指出其存在严重安全缺陷:SVS 集合中的 Clerk 可以自己验证几乎所有签名.以上方案不具有不可否认性质,Clerk 的权限也过大.事实上,核心验证信息必须经其广播才能让每一验证服务器得到,这就要求 Clerk 必须完全可信.此外,在网络环境下验证服务器易受攻击(如 Hacker 攻击),因此,如果某些验证服务器被破坏,系统就不能正常工作.

本文采用文献[3]的设计思想提出了一种指定验证方的签名方案,并利用安全多方计算思想提出了安全协议.其主要特点如下:

(1) 签名方案实现效率较高,具有可证明安全性;

(2) 提出了“验证安全性”概念和“门限验证”思想,并证明门限验证协议满足“验证安全性”;

(3) 系统不设 Clerk,即不依赖于可信第三方的存在;

(4) 因其非常简明而直接的方式而具有不可否认性质.

安全证明依赖于 RO 模型(random oracle model)[4]、CDH(计算 Diffie-Hellman)假设以及 DDH(决策 Diffie-Hellman)假设.需要指出,这是一种应用可证明安全理论证明安全性的方案.

1 对 Laih 方案的简要分析

1.1 文献[1]所提出的方案简介

KeyGen(密钥生成). 设 $G_s=\{U_{s_1},\ldots,U_{s_n}\}$ 为签名方群,群私钥、公钥对为 $\left(-\sum_{i=1}^{n}s_i, Y_s=\prod_{i=1}^{n}g^{-s_i} \bmod p\right)$;

$G_V=\{U_{v_1},\ldots,U_{v_m}\}$ 为验证方群,群私钥公钥对为 $\left(-\sum_{i=1}^{m}v_i, Y_v=\prod_{i=1}^{m}g^{-v_i} \bmod p\right)$;每个群里有一个 clerk;单个用户的公私钥对应以上分量,都由可信中心生成.

Multisign(多签名). 设待签消息为 m ,步骤如下:1) 每个 U_{s_i} 随机选择 $r_i \in Z_q$, 计算 $x_i = Y_v^{r_i}$,并发送 x_i 给 clerk_s;2) clerk_s 计算 $x = \prod_{i=1}^{n} x_i \bmod p$,在 G_s 中广播 x ;3) 每个 U_{s_i} 计算 $e = h(x, m)$ 和 $w_i = r_i + es_i \bmod q$, 将 w_i 交给 clerk_s;4) clerk_s 计算 $e = h(x, m)$, $w = \sum_{i=1}^{n} w_i \bmod q$, 输出多签名 (e, w, m).

Verification(验证). G_v 中成员协同计算:1) 每个 U_{v_j} 计算 $x_j = [g^w Y_s^e]^{-v_j} \bmod p$, 传送给 clerk_v;2) clerk_v 计算 $x = \prod_{i=1}^{n} x_i \bmod p$,广播 x;3) 每个 U_{v_j} 验证 $e = h(x, m)$ 是否成立.

1.2 分 析

文献[2]指出,以上方案存在如下安全缺陷:clerk_v 只要参与过一次验证协议,以后就可以单独验证所有签名.原因在于,由 verification 容易计算出:

$$g^{\sum_{i=1}^{n} s_i \sum_{i=1}^{m} v_i} = [xY_v^{-w}]^e, \quad x = Y_v^w g^{-e\sum_{i=1}^{n} s_i \sum_{i=1}^{m} v_i}.$$

因此,只要 clerk_v 计算过一次 x ,就可以得到固定值 $g^{\sum_{i=1}^{n} s_i \sum_{i=1}^{m} v_i} = [xY_v^{-w}]^e$, 以后也就可以验证任一签名 (e, w, m) 是否合法.

1.3 我们的观点

实际上,不仅 clerk_v,每个验证方都可以在一次验证成功后具有验证以后所有签名的能力(无须 clerk 或其他验证方的配合);而且即使设法克服以上缺陷,每次验证时,clerk_v 仍可先于各验证方确认签名是否合法.以文献[1]为例,关键验证信息 x 是由 clerk_v 控制的.

上述系统要确保安全,必须维持多个可信中心,诸如 KAC(密钥认证管理中心),clerk_s 及 clerk_v.

最后,即使有一个验证服务器被破坏(如 Hacker 攻击),整个系统的验证工作就会限于瘫痪(“计算机系统的安全性低于协议本身的安全性”是已经证实的广泛共识).

此外,目前的这类方案都没有从理论上严格证明签名是不可伪造的,也未严格证明除指定方外的第三方没有验证签名的能力并提供不可否认功能.

2 指定验证方的门限验证签名方案

我们对上述密码学问题的解决方案主要包括指定验证方的基础签名方案 SV-EDL、多方(门限)签名协议和门限验证协议.但事实上只着重探讨指定验证方的基础签名方案和门限验证协议,因为对于多方(门限)签名协议而言,目前已有非常完备的结果.例如,文献[5–8]等,特别是文献[8]已证明,其设计的一类基于离散对数问题的 El Gamal 类型门限签名协议和相应单签名协议的输出及安全性是等价的.本文还针对指定验证方的签名方案提出了门限验证签名思想,同时在第 3 节和第 4 节定义并给出协议的安全性证明.

2.1 基础签名方案SV-EDL

我们利用 Eu-Jin Goh 等人提出的签名方案 EDL[3]的基本设计思想提出指定验证方的签名方案 SV-EDL.

SV-EDL 涉及两个独立的安全 Hash 函数:

$$H: \{0,1\}^* \to G_{p,g} = \{g^0, ..., g^{q-1}\}, H': G_{p,g}^8 \to Z_q.$$

设验证服务器 SVS 的群公、私钥为 $y_v = g^{x_v} \bmod p$, g 的阶为 $q \mid (p-1)$.

SV-EDL 签名方案描述如下:设待签署消息为 m .

KeyGen. 签名方私钥 $x \xleftarrow{R} Z_q$, 公钥 $y \longleftarrow g^x \bmod p$

Sign. 1) $r \xleftarrow{R} \{0,1\}^{n_r}$, 利用 Hash 函数 H 计算 $h = H(m, r)$;

2) 计算 $z = h^x$ (注意离散对数 $DL_g(y) = DL_h(z) = x$);

3) $k \xleftarrow{R} Z_q$, 计算 $u = g^k$, $v = h^k$;

4) $l \xleftarrow{R} Z_q$, $w = g^l$, $w' = g^{lx_v}$;

5) 利用 Hash 函数 H' 计算 $c = H'(g,h,y,z,u,v,w,w')$;

6) 计算 $s = k + cx$,输出 m 的签名 $\sigma = (z,r,s,w,c)$.

$\mathbf{Ver_{SVS}}$. SVS 计算 $h = H(m,r)$, $u = g^s y^{-c}$, $v = h^s z^{-c}$, $w' = w^{x_v}$,最后验证等式 $c' = H'(g,h,y,z,u,v,w,w') = c$ 是否成立以决定签名真伪.

与文献[3]相比,SV-EDL 的签名长度稍长,这主要是考虑到安全性证明,因为指定验证方签名方案的安全模型有其特殊性,参见第 3 节,因此适当延长签名长度是一种合理选择;而实现效率则几乎完全一样.

2.2 门限验证协议

所谓门限验证,是指验证 SV-EDL 签名的能力被 m 个验证服务器按门限方式共享,这主要是为了抵抗 Hacker 的入侵攻击:即使少数服务器瘫痪,系统仍能完成验证签名任务.

设 $SVS = \{SVS_1,...,SVS_m\}$,群公钥为 $y_v = g^{x_v} \bmod p$.

密钥分配协议 **DL-Key-Gen**. 不妨直接采用文献[6]提出的 DL-Key-Gen 作为密钥分配协议.其基本思想是:以公开参数 (p,q,g,h) 为输入,主要利用 *Joint-RVSS*(t)(无须 Dealer 或 KDC 的可验证秘密共享协议,参见文献[6]的引述),使每一服务器得到自己的私钥 share,并公开输出群公钥 $y_v = g^{x_v} \bmod p$.该协议具有可证明的适应性语意安全性(adaptively semantic security),即协议不会泄漏除群公钥以外的任何信息.

门限验证协议 **TVP**. 输入:SV-EDL 签名 $\sigma = (z,r,s,w,c)$、每一服务器的私有输入(shares)、群公钥及其他公开参数.执行:无妨设恰好前 t (门限值)个验证方参与.

1) SVS_i(i=1,2,…,t)计算并广播 $w_i' = w^{x_{v_i}} = g^{lx_{v_i}}$,这里 x_{v_i} 是各 SVS 执行 DL-Key-Gen 协议后得到的 Shamir 秘密共享 share;

2) SVS_i(i=1,2,…,t)计算 $w' = \prod_{i=1}^{t} w_i'^{\lambda_i} = g^{l\sum_{i=1}^{t}\lambda_i x_{v_i}} = g^{lx_v}$, λ_i 表示 shamir 秘密共享方案的 Lagrange 系数,是公开可计算的.其余验证步骤同第 2.1 节的 $\mathrm{Ver_{SVS}}$.

系统恢复协议.一般来说,系统服务器遭受 Hacker 入侵破坏很快会被察觉[6].如果发现已有超过门限值 t 个服务器被破坏,就意味着群私钥已遭破坏,则必须重新启动 DL-Key-Gen,生成新的群公私钥.然而多数情况是 Hacker 只侵入了少数(少于门限值)服务器,即系统私钥未遭破坏,但敌手也具备了验证签名的能力.为此,我们提出 ReKeyGen 协议,其基本思想是,在 DL-Key-Gen 的基础上,利用 *Joint-ZVSS*(t)(不存在可信 Dealer 或 KDC,对 0 值的可验证(Shamir)秘密共享方法[6])方法随机化子密钥 shares:

设预先执行 DL-Key-Gen 以后,各 SVS_i 得到的 shares 分别为 x_{v_i} ($i = 1,2,...,m$).

1) 执行 *Joint-ZVSS*(t),设各 SVS_i 得到的 shares 分别为 0_i ($i = 1,2,...,t$);

2) 每个 SVS_i 计算 $x_{v_i} + 0_i$ 作为自己的 share,显然这时系统公钥不变.

上述方法的优势在于,在只有少数验证服务器遭受 Hacker 攻击的情况下,恢复系统时只需随机化子密钥即可,公钥仍保持不变.其优点是显而易见的:不必频繁更换群公钥,方便签名方群体的认证等.

因为 SV-EDL 签名方案指定了验证方,因此存在对签名方“不可否认”性质的潜在需求(对普通签名而言,由于签名是公开可验证的,所以不存在这个问题).这里,我们以一种非常简明、直接的方式确保方案具有不可否认性质:当发生争执时(亦即 Signer 是否曾经签署了某份消息),Verifier 只需向第三方 T(裁定方)提供对应消息 $w' = g^{lx_v}$, T 易于验证本次签名是否合法.这避免了较繁琐的不可否认协议设计.这也是我们方案的一个突出优点.注意,T 不会因此获得验证其他签名的能力.

3 基础签名方案的安全性证明

3.1 SV-EDL签名的不可伪造性

首先给出基础假设:CDH 假设[3].

定义 **1**(**CDH** 假设). 称一个 ppt(概率多项式时间)算法 A 在子群 t $G_{p,g}=\{g^0,...,g^{q-1}\}$ 中(t,ε)-解决 CDH 问题,如果满足:以 $((p,q),(g^a,g^b))$ 为输入,在至多运行 t 步后, 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).如果不存在(t,ε)-解决 CDH 问题的 ppt 算法 A,则称群 $G_{p,g}=\{g^0,...,g^{q-1}\}$ 是一个(t,ε)-CDH 群.

下面规划安全模型.对于指定验证方签名方案,除签名方私钥外,签名算法还用到了接收方 SV 的公钥,而只有 SV 知道对应私钥,因此接收方 SV 和任意第三方在伪造签名能力上可能有差别.基于以上考虑,我们假定敌手可以获得 SV 的私钥,因此他是可以验证签名的,这是与一般签名方案安全模型的主要区别.当敌手经过一系列询问 Hash oracle 以及签名 oracle 之后,如果能够提出一个未经询问消息的合法签名,就称敌手成功.

定理 **1**. 如果 G 是一个(t',ε')-CDH 群,则在 RO 模型中,SV-EDL 是 $(t,q_H,q_{sig},\varepsilon)$-安全的(即不存在如下有效算法:在 t 步内,任意作 q_H 次 Hash 询问和 q_{sig} 次签名询问之后,至少以概率 ε 伪造一个合法签名),这里,

$$t\approx t'-(q_H+6.4q_{sig})C_{\exp}(G_{p,g}),\varepsilon\geq\varepsilon'+(q_{sig}q_H2^{-n_r}+q_{sig}(q_{sig}+q_H)2^{-3n_q}+2^{-n_q}+q_H2^{-n_q}).$$

注:算法的主要时间代价为 Z_q 上的指数运算,因此只考虑实现该运算的成本,设一次指数运算耗时 $C_{\exp}(G_{p,g})$.

证明:基本思想类似于文献[3].即假设 F 是 SV-EDL 的一个 $(t,q_H,q_{sig},\varepsilon)$-伪造者,即在 t 步内,任意作 q_H 次 Hash 询问和 q_{sig} 次签名询问之后, F 至少以概率 ε 伪造一个合法签名.构造这样一个“模仿”算法 S,以 $((p,q),(g^a,g^b))$ 为输入,至多 t' 后,至少以概率 ε' 计算出 $DH_{g,p}(g^a,g^b)=g^{ab}$,从而与 CDH 假设矛盾.

首先 S 运行 Key-Gen,生成签名方公钥 $y=g^a$ (私钥 a 未知);然后 S 向 F 模仿签名协议,并回答 F 的 Hash oracle(H,H') 询问、签名 oracle 询问,目的是把 F 的一个可能伪造 (m,σ) 转化成计算 $DH_{g,p}(g^a,g^b)$ 的算法.下面构造回答 oracle H, H', Sig 的算法,亦即 H_{sim}, H'_{sim} 和 Sig_{sim}.

H_{sim}:如果 F 的询问 (m,r) 是新的, S 随机选择 d,回答 $g^{bd}=(g^b)^d$;

H'_{sim}:对新的询问随机回答;

Sig_{sim} :1) $r\xleftarrow{R}\{0,1\}^{n_r}$, 如果 (m,r) 已问过,放弃;2) 否则,取 $j\xleftarrow{R}Z_q$, $z=y^j$, $h=g^j$, 定义 $h=H(m,r)$; 3) 随机选 $s,c\in Z_q$,取 $u=g^sy^{-c}$, $v=h^sz^{-c}$;4) 随机选 $l\in Z_q$,计算 $w=g^l$, $w'=(g^{x_v})^l=g^{lx_v}$;5) 如果 H' 已经被问过 (g,h,y,z,u,v,w,w'),放弃,否则定义 $c=H'(g,h,y,z,u,v,w,w')$,返回对 m 的签名 $\sigma=(z,r,s,w,c)$.

解决 CDH 问题:1) 调用 F,以不可忽略概率输出一个合法签名 (m,σ) ((m,r) 必然是新的);2) 如果 F 没有向 H 询问过 (m,r),放弃;否则有 $h=H(m,r)=g^{bd}$,则 S 输出 $z^{1/d}$ (若满足 $DL_g(y)=DL_h(z)$, $z^{1/d}=g^{ab}$).

概率分析:1) Sig_{sim} 可能在 Step 1 即失败:亦即 (m,r) 已经询问过 H oracle;因为至多有 q_H 个这样的 r,故碰撞概率至多 $q_H2^{-n_r}$,这样对 q_{sig} 个签名询问而言,失败概率至多为 $q_{sig}q_H2^{-n_r}$.

2) Sig_{sim} 也可能因 (g,h,y,z,u,v,w,w') 已询问过 H' oracle 而失败:该字符串可以写成 $(g,g^j,y,y^j,u,u^j,g^l,g^{lx_v})$,而 (u,j,l) 注意在 $G_{p,g}\times Z_q^2$ 上均匀分布,且 H' oracle 至多被问过 (q_H+q_{sig}) 次,故碰撞概率不超过 $(q_H+q_{sig})2^{-3n_q}$,对 q_{sig} 个签名询问而言,失败概率至多为 $q_{sig}(q_H+q_{sig})2^{-3n_q}$,这与文献[3]有所不同.

3) 在事件 $NH\cup NQ$ 发生时将无法解决 CDH 难题:这里, NH 表示 F 未经询问 H_{sim} 就伪造合法签名的事件; NQ 表示 F 伪造了一个合法签名但 $DL_g(y)\neq DL_h(z)$ 的事件.易见有 $\Pr[NH\cup NQ]=\Pr[NH\cap\overline{NQ}]+\Pr[NQ]$.

首先估计 $\Pr[NH\cap\overline{NQ}]$:这时事件 $\overline{NQ}$ 发生,故对于一个成功的伪造签名而言,有等式 $z^{-x}=h=H(m,r)$,由于 H 是随机预言,故成立概率至多为 2^{-n_q};

其次估计 $\Pr[NQ]$:设 $u=g^k$, $v=h^{k'}$, $y=g^x$,但 $z=h^{x'}\neq h^x$.由于签名是合法的,故 $u=g^sy^{-c}$, $v=g^sz^{-c}$,从而有

$k=s-cx,k'=s-cx$,这样得到 $H'(g,h,g^x,h^{x'},g^k,h^{k'},g^l,g^{lx_v})=c=(k-k')/(x'-x)$,由于 H' 是随机预言,因此,F 在全部 $H-oracle$ 询问中找到上述 c 的概率至多为 $q_H 2^{-n_q}$.

综上, S 至少以概率 $\varepsilon-(q_{sig}q_H 2^{-n_r}-q_{sig}(q_{sig}+q_H)2^{-3n_q}-2^{-n_q}-q_H 2^{-n_q})$ 成功解决 CDH 难题.至于时间估计,只需注意 S 的运行时间就是 F 的运行时间和许多 Z_q 中的指数运算,一次 2 个指数幂乘运算相当于约 1.2 次指数运算,略.因此原假设和 CDH 假设矛盾,证毕. □

与一般签名方案分析的重要区别在于,下面我们还要严格证明,除指定的 SVS 以外,任意第三方是不能验证 SV-EDL 签名的.

3.2 SV-EDL的验证安全性证明

定义 2(验证安全性). 称指定验证方的签名方案(KeyGen,Sign,Ver_{SVS})满足验证安全性,如果满足条件:对任意敌手 VA(概率多项式算法),有效签名(随机变量) σ 与结构相同的随机变量 σ' 是计算不可分辨的,亦即对任意多项式 $p(\cdot)$,任意 PPT 算法 D 及所有辅助输入 $z\in\{0,1\}^{poly(n)}$,$|\Pr[D(\sigma,1^n,z)=1]-\Pr[D(\sigma',1^n,z)=1]|<1/p(n)$.

以上定义即:如果以概率 1/2 随机给予敌手一个有效签名或某随机数,除了可以忽略优势以外,敌手猜对(哪一个是合法签名)的概率恰是 1/2.有关不可分辨概念,可以参见文献[9].注意,根据文献[9],以上定义中所含的绝对值符号是不必要的.为简单起见,以下均省略辅助输入和绝对值符号.

首先引入决策 Diffie-Hellman 假设(DDH 假设[6]).

定义 3(**DDH** 假设). 对满足前述条件的参数,对任意 ppt 算法 A 定义概率:

$$P_1=\Pr ob_{a,b,c\in_R Z_q}[A(p,q,g,g^a,g^b,g^c)=1],$$

$$P_2=\Pr ob_{a,b\in_R Z_q}[A(p,q,g,g^a,g^b,g^{ab})=1].$$

如果满足:对任意这样的 A,任意的多项式 $p(\cdot)$,只要 n 足够大,

$$|P_1-P_2|<1/p(n),$$

则称 DDH 假设成立.其涵义是,随机变量 (g^a,g^b,g^c) 和 (g^a,g^b,g^{ab}) 计算不可分辨.

SV-EDL 的验证安全性即基于"DDH 假设".

定义 $Adv(DDH)=\max_D\{\Pr_{a,b,c\in_R Z_q}[D(p,q,g,g^a,g^b,g^c)=1]-\Pr_{a,c\in_R Z_q}[D(p,q,g,g^a,g^b,g^{ab})=1]\}$,显然在 DDH 假设意义下这是可忽略函数.

首先规划安全模型.这里,敌手是任意第三方,仅知道 Signer,SV 的公钥,具有 Random Oracle H, H', Sig.当敌手经过询问 Oracle 后,能以不可忽略概率区分一个新的签名和一个随机值,就称敌手成功.

定理 2. SV-EDL 满足验证安全性,亦即除了可忽略概率以外,

$$Adv(\sigma,\sigma')\le Adv(DDH)/(1-q_{sig}(q_{sig}+q_H)2^{-3n_q}).$$

这里, $Adv(\sigma,\sigma')=\max_D\{\Pr[D(\sigma)=1]-\Pr[D(\sigma')=1]\}$,表示 σ 和 σ' 的最大区分优势.

证明:基本思想是,对于敌手 VA 的任何一个分辨真伪签名的 ppt 算法,我们可以在 RO 模型中构造一个模仿算法 S,以 (p,q,g,g^l,g^{x_v},w') 为随机输入($w'=g^j(j\in_R Z_q)$ 或 g^{lx_v}),输出一个模仿签名;若 VA 以不可忽略概率辨别真伪,则以 VA 为子程序就可以构造出以不可忽略概率区别 $(p,q,g,g^l,g^{x_v}g^{lx_v})$ 和 (p,q,g,g^l,g^{x_v},g^j) 的概率多项式算法,从而与 DDH 假设矛盾.主要困难在于: S 要在不知签名方的私钥 x 及验证方私钥 x_v 的条件下,仅根据 (p,q,g,g^l,w') 及双方公钥等公开参数给出一个模仿签名.下面首先给出(我们)回答各 oracle 的算法.

H_{sim}:如果 VA 的询问 (m,r) 是新的,则随机选择 $b\in Z_q$,定义 $h=H(m,r)=g^b \bmod p$ 作为回答;否则从过去保留的回答记录中找到相应的询问,给出过去的回答;

H'_{sim}:对所有新的询问给出随机回答.

Sig_{sim}:1) $r\xleftarrow{R}\{0,1\}^{n_r}$,调用 H_{sim},设得到 $h=g^b$,取 $z=y^b$;2) 随机选 $s,c\in Z_q$,取 $u=g^s y^{-c}$, $v=h^s z^{-c}$;3) 随机选 $l\in Z_q$,计算 $w=g^l$, $w'=(g^{x_v})^l=g^{lx_v}$;4) 如果 H' 已经被问过 (g,h,y,z,u,v,w,w'),放弃,否则定义 $c=H'(g,h,y,z,u,v,w,w')$,返回对 m 的签名 $\sigma=(z,r,s,w,c)$.

设 D 是 VA 关于签名变量 σ 和随机变量 σ' 的任意区别算法,下面构造解决 DDH 难题的区别算法 D'.

输入: (p,q,g,g^l,g^{x_v},w') 为随机输入($w'=g^j(j\in_R Z_q)$ 或 g^{lx_v}).

执行:1) $r\xleftarrow{R}\{0,1\}^{n_r}$,调用 H_{sim},设得到 $h=g^b,z=y^b=(g^x)^b$;

2) 随机选 $s,c\in Z_q$,取 $u=g^s y^{-c},v=h^s z^{-c}$;

3) 取 $w=g^l$;

4) 如果 H' 已经被问过 (g,h,y,z,u,v,w,w'),放弃,否则定义 $c=H'(g,h,y,z,u,v,w,w')$.

若模仿成功,输出 $D(\sigma)$,这里 $\sigma=(z,r,s,w,c)$ (模仿签名或随机变量),否则输出 0.

分析:令 $a(w')=(p,q,g,g^l,g^{x_v},w')$,令 S 表示模仿成功的事件,则有

$$\begin{aligned}\Pr[D'(a(w')=1]&=\Pr[D'(a(w')=1\mid S]\Pr[S]+\Pr[D'(a(w')=1\mid \bar{S}]\Pr[\bar{S}]\\&=\Pr[D(\sigma)=1]\Pr[S]+0\cdot\Pr[\bar{S}]\\&=\Pr[D(\sigma)=1]\Pr[S],\end{aligned}$$

因此易知

$$\Pr[D(\sigma)=1]-\Pr[D(\sigma')=1]=(\Pr[D'(a(g^{lx_v}))=1]-\Pr[D'(a(g^j))=1])/\Pr[S]\le Adv(SDDH)/\Pr[S].$$

根据 D 的任意性,易知 $Adv(\sigma,\sigma')\le Adv(SDDH)/\Pr[S]$. 下面估计 $\Pr[S]$ 的下界.

显然,仅在 Step3 有可能失败,亦即 (g,h,y,z,u,v,w,w') 已询问过 H' oracle,由定理 1 证明的概率分析部分易知, $\Pr[S]=1-\Pr[\bar{S}]\ge 1-q_{sig}(q_{sig}+q_H)2^{-3n_q}$,证毕. □

依据 DDH 假设易知,对任意敌手而言, $Adv(\sigma,\sigma')$ 是可忽略函数,因此对敌手而言, σ,σ' 是不可分辨的.

4 门限验证协议的安全性证明

如果敌手 VA 控制了任一验证服务器,就可以参与合法签名验证,因为这时 $w'=g^{lx_v}$ 可以通过 VA 和其他诚实服务器合作执行 TVP 得到.但根据文献[6],一般遭受入侵的情况会很快被察觉,然后根据情况采取必要的措施(如执行 ReKenGen).这里我们考虑如下的安全性定义:对于静态敌手 VA(由文献[6],对多数应用只需考虑静态敌手,而且也可以利用文献[8]的技术转化成动态敌手情况),如果其控制的验证服务器数目小于门限值 t,则敌手 VA 不会获得除了 (g^l,g^{x_v},g^{lx_v}) 之外的任何信息.这时系统可执行 ReKeyGen 协议,不必更换群公钥.

定理 **3**. 在上述安全性意义下,TVP 是安全的.

证明:基本思想是采用模仿论断:即构造一个除了 (g^l,g^{x_v},g^{lx_v}) 及其他公开参数之外一无所知的模仿者 Simulator,他以 VA 已控制的服务器(bad player)的输入输出、 g^{lx_v} 为输入,与 VA 联合执行 TVP,使得在 VA 看来,从和 Simulator 交互得到的观察与从和真正服务器交互得到的观察是不可分辨的,因此 VA 不会得到任何信息.这里所谓观察(view)是指协议执行期间 VA 所收发的所有信息.下面构造模仿协议 Sim-TVP.不妨设前 $(t-1)$ 个 SVS 已被破坏(corruped).1) 对于 bad players,计算并广播 $g^{lx_{v_i}}$ $(i=1,2,...,t-1)$;2) 随机选取 $x_{v_i}\in Z_q(i=t,t+1,...,m-1)$ 计算并广播 $g^{lx_{v_i}}$;3) 计算并广播 $g^{lx_{v_m}}=\left(g^{lx_v}/\prod_{i=1}^{m-1}g^{lx_{v_i}\lambda_i}\right)^{\lambda_m^{-1}} \bmod p$.

不难看出,由于 DL-Key-Gen 是安全的(VA 不会得到除群公钥 g^{x_v} 之外的任何信息),再考虑到 DDH 假设,因此在 VA 看来,从模仿协议得到的信息和从实际的 TVP 得到的信息是不可分辨的.证毕. □

当然,以上协议还有不足之处:不能证明稳健性(robustness),亦即如果敌手消极破坏(即提供假的 shares),则会导致认证系统失效.但是根据前面的叙述,这不是一个主要缺点.

References:

[1] Laih C, Yen SM. Multisignature for specifical group of verifier. Journal of Information Science and Engineering, 1996,12(1): 143−152.

[2] He WH. Weakness in some multisignature schemes for specified group of verifiers. Information Procesing Letters, 2002,83(2): 95−99.

[3] Goh EJ, Jarecki S. A signature scheme as secure as the Diffie-Hellman problem. In: Biham E, ed. Advances in Cryptology—EUROCRYPT 2003. LNCS 2656, Berlin: Springer-Verlag Publishers, 2003. 401−415.

[4] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In: Proc. of the 1st ACM Conf. on Computer and Communicatuions Security. New York: ACM Press, 1993. 62−73.

[5] Micali S, Ohta K, Reyzin L. Accountable-Subgroup multisignatures. In: Sander T, ed. Proc. of the 8th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2001. 245−254.

[6] Raimondo MD, Gennaro R. Provably secure threshold password—Authenticared key exchange. In: Biham E, ed. Advances in Cryptology—EUROCRYPT 2003. LNCS 2656, Berlin: Springer-Verlag, 2003. 507−523.

[7] Wu QH, Wang JL, Wang YM. *t*-out-of-*n* ring signatures from discrete logarithm public keys. In: Chen KF, Li X, eds. Advances in Cryptology—Chinacrypt 2004. Beijing: Science Press, 2004. 209−214 (in Chinese with English abstract).

[8] Canetti R, Gennaro R, Jarecki S, Krawczyk H, Rabin T. Adaptive security for threshold cryptosystems. In: Wiener M, ed. Advances in Cryptology—CRYPT'99. LNCS 1666, Berlin: Springer-Verlag, 1999. 98−115.

[9] Goldreich O. Foundations of Cryptography: Basic Tools. Beijing: Publishing House of Electronics Industry, 2003. 35−107.

附中文参考文献:

[7] 伍前红,王继林,王育民.基于离散对数公钥的 *t*-out-of-*n* 环签字.见:陈克非,李祥,编.密码学进展——ChinaCrypt 2004.北京:科学出版社,2004. 209−214.

Call for Papers for the 3rd Annual Conference of Theory and Applications of Models of Computation

May 15th to 20th, 2006, Beijing, China
http://gcl.iscas.ac.cn/accl06/TAMC06_Home.htm

TAMC 2006 is a new annual conference focusing on theory and applications of computation. It is organized as part of the Grand China NSF International Joint Project after which the conference is named, and is supported by the Chinese National Science Foundation, and the Institute of Software, the Chinese Academy of Sciences. Previously two annual meetings were held in 2004 and 2005, with enthusiastic participation from researchers all around the world. TAMC 2006 will be a much larger international conference. The scope of the conference will include algorithms, complexity, models of computation, and computability. The conference will be interdisciplinary in nature, and bring together researchers and students with an interest in computer science, mathematics and logic, and applications to the physical sciences. More information on the conference is available on the TAMC 2006 website.

Submission and publication

Submitted papers must describe work not previously published. They must not be submitted simultaneously to another conference with refereed proceedings. Research that is already submitted to a journal may be submitted to TAMC 2006, provided that (a) the PC chair is notified in advance that this is the case, and (b) it is not scheduled for journal publication before the conference. Accepted papers will be published in the conference proceedings (within the LNCS series of Springer), which will be available at the conference. Selected papers will also be published in a Special Issue of the journal Theoretical Computer Science. Authors of accepted papers are expected to present their work at the conference.

Abstract submission

Authors are strongly required to submit their extended abstracts electronically. A detailed description of the electronic submission process is available at http://gcl.iscas.ac.cn/accl06/TAMC06_Submission.htm.

Abstract format

Authors should submit an extended abstract (not a full paper). The submission should contain a scholarly exposition of ideas, techniques, and results, including motivation and a clear comparison with related work. The length should not exceed ten (10) letter-sized pages (not including the bibliography and figures).

Important dates

Submission deadline: December 17, 2005 Notification: January 20, 2006 Final versions: February 15, 2006.

Notification

Authors will be sent notification of acceptance or rejection by e-mail on or before January 20, 2006. A final copy of each accepted paper is required by February 15, 2006. Again this is a firm deadline. An author of each accepted paper must attend the conference and present the paper.