阈下信道分类及边信息协商问题研究*)

董庆宽　肖国镇
(西安电子科技大学ISN综合业务网国家重点实验室　西安710071)

摘　要　在本文中我们首先给出了阈下信道的一般模型和含有阈下信道的密码系统的定义，讨论了信任度和安全度两个指标。然后我们对目前的构造技术进行了系统的分类，对各类方案的容量、计算复杂度及边信息量等进行较为深入的研究，并讨论了认证码中的阈下信道与一般阈下信道的差别。我们首次提出了边信息协商的概念，并给出了几个实现方案。

关键词　数字签名，阈下信道，边信息，信息隐藏

Research on the Classification of Subliminal Channels and Side Information Exchange

DONG Qing-Kuan　XIAO Guo-Zhen
(National Key Lab. of Integrated Services Networks of Xidian Univ. Xi'an Shanxi, 710071)

Abstract　A definition of cryptosystem with subliminal channels and a model of subliminal channels are given in this paper. And two index, confiding degree and security degree, are also discussed. Then a systemic classification of subliminal channels techniques is given. And a sound research on capacity, computational complexity and side information has also been done. We then discuss the difference between the subliminal channels in authentication codes and the one in other system. Finally, a concept of side information exchange is first presented and some schemes are given.

Keywords　Digital signature, Subliminal channel, Side information, Information hiding

1　引言

阈下信道(Subliminal Channel)，也称潜信道，最早由G. J. Simmons于1983年提出，是一种在密码数据中主要是签名或认证协议中建立起来的隐蔽信道[1]。Simmons通过在看守(Warden)的完全监视下两个囚犯如何协商一个逃跑计划的例子引入了该信道。阈下信道提出的最初目的是为了证明美国用于SAL-Ⅱ苏美战略核武器限制条约核查系统中的安全协议存在着漏洞[2]。随着计算机技术、电子技术和网络技术的不断发展，各类业务的网络化进程不断加快，如电子商务、电子政务等新兴应用技术。信息安全技术特别是签名和认证技术在实现和维系这些应用系统的过程中起到了至关重要的作用。而这些技术正是阈下信道技术赖以生存的环境，各类业务的网络化为阈下信道技术的发展拓展了新的应用空间，除了情报和隐私保密之外，有很多新的应用。比如可以在签名中嵌入身份验证信息以使收方能够识别签名是否被伪造和篡改，另外商家可以将用户的信任度嵌入到信用卡中，政府可以将违法记录嵌入到当事人的身份证中，交管部门可以将事故记录嵌入到司机的驾驶执照中等等。目前阈下信道技术的研究已经越来越引起人们的重视，但仍有许多问题没有解决。

比如，在信息隐藏技术的发展中，人们给出了若干信息隐匿的模型，并归纳了鲁棒性、透明性等重要的指标。但是阈下信道是信息隐藏技术中较为特殊的一种，还没有一个专门的模型及适合的指标来描述它。本文的第一个目的就是给出阈下信道的一般模型及两个重要指标，同时给出一个含有阈下信道的密码系统的定义。

迄今为止，人们已经构造了多种阈下信道[3~9]，研究主要集中于两个方面：一是寻求建立阈下信道的新方法，二是怎样最大限度地开发宿主系统的随机冗余比特，以扩大带宽。在目前人们开发的新型信道中，某些类型实质上没有什么分别[7~9]，在新近的研究中，新型信道的构造仍限于技巧性构造，甚至是重复性工作，这对该技术的进一步发展相当不利。因此本文的第二个目的就是对现有的构造技术进行系统分类，并讨论了容量、计算复杂度和所需的边信息量等问题，我们也将讨论认证码中的阈下信道与一般阈下信道的差别。

阈下信道的建立需要收发双方共享一定的秘密信息，称之为边信息，我们提出了边信息协商的概念，解决传统体制中必须共享较多秘密比特的矛盾，以及收发双方没有预先共享的秘密比特的问题，并且提出了已知秘密比特协商方案和未知秘密比特协商方案。

本文第2节讨论阈下信道的基本问题，包括模型、指标以及定义，第3节详细讨论分类问题，并且分析了容量、计算复杂度和边信息量等问题，第4节提出边信息协商概念及实现方案，最后给出小结。

2　阈下信道的基本问题

2.1　一般模型

图1给出了一个阈下信道的一般模型。其中原始数据 D 是指密码系统(比如认证或签名系统)的输入数据；嵌入算法 E 包含了宿主系统的密码算法；边信息 K 是指收发双方共享的全部秘密比特，包括了宿主系统泄漏给阈下收方的秘密信息和阈下消息随机化密钥信息。看守W检测隐匿数据 S(含有阈下消息的密码数据)，如果通过检测则转发至收方，否则将发方抓获。阈下收方对接收到的隐匿数据首先进行宿主系统验证，这样既可实现宿主系统原有的密码功能又可看作是对阈下消息的一种认证，如果宿主系统产生了安全问题，那么

*)基金项目：国家自然科学基金重大项目(No. 90104005)，97-3项目(No. G1999035804)。董庆宽　博士生。

阈下消息就失去了可信性。

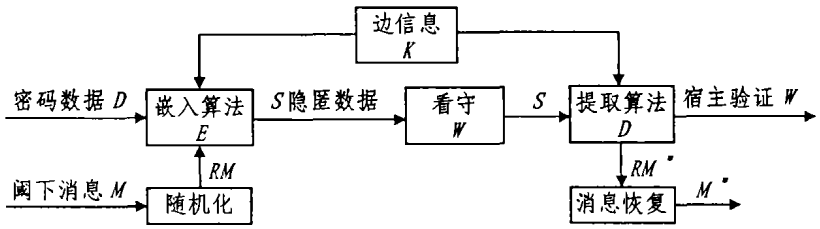

图1 阈下信道的一个基本模型

设原始密码系统为 C(即宿主系统),嵌入了阈下消息的密码系统为 C',并且 C' 满足如下要求:

(1)C' 的输入数据与 C 的输入数据的公开说明相一致;

(2)阈下消息嵌入算法包含于 C',并且该嵌入算法是透明的,即它只影响 C 中的秘密参数的选择,而不影响 C 中的算法;

(3)由嵌入算法秘密选择的参数集为 T',原始密码数据的随机参数集为 T,满足 $T'\subseteq T$;

(4)C' 的输出数据与 C 的输出数据的公开说明相一致;

(5)对除阈下收方以外的任何第三方,C' 保留了 C 的全部密码功能。

则含有阈下信道的密码系统定义为:

定义1 一个对秘密参数选取有附加限制的密码系统被称为是含有阈下信道的密码系统当且仅当 C' 与 C 的输出集合的概率分布是不可区分的,或是计算上不可区分的。

2.2 两个指标

由于阈下信道所依托的宿主系统的特殊性使得阈下信道的两个重要指标与一般的信息隐藏系统有所不同,区别于一般系统中的透明性(不可检测性)和鲁棒性指标,我们用安全度和信任度来定义阈下信道的指标。

安全度:与不可检测性相对应。看守通过对密码系统的输出进行检测来判断是否含有阈下消息。这主要是通过检验输出的统计特性来实现。阈下信道中的秘密随机参数一般是均匀选取的,如签名中的会话密钥等,设其概率分布为 U_r,相应地密码(陷门)单向函数 f 的输出满足分布 Q_r,设嵌入了阈下消息的秘密随机参数的分布为 U_t,相应地嵌入了阈下信道以后的密码(陷门)单向函数 f 的输出分布为 Q_t。如果 U_r 与 U_t 是同分布的,在同一函数作用下,输出的分布 Q_r 与 Q_t 亦为同分布,该阈下信道是无条件安全的。如果 U_r 与 U_t 的分布不同则 Q_r 与 Q_t 也不同,如果这种不同很明显,就会被看守检测出来,而使信道不安全。Cachin 在提出的基于假设检验的信息隐藏模型中[10]提出了相对熵的概念来描述安全度,张彤给出了进一步的结果[11]。

一般的阈下消息的分布与均匀分布的秘密随机参数是有很大的差别的,因此必须随机化以后再嵌入,以使 U_r 尽可能接近 U_t,获得较高的安全度。采用一次一密乱码本(one time padding,可用伪随机序列产生器来逼近)对消息进行随机化是很好的一种办法,伪随机序列具有良好的统计特性,副近真正随机秘密参数的分布。

信任度:这是我们首次提出的概念,阈下收方在提取阈下消息时可能出现错误,这主要来自于两种情况:一种是阈下发方嵌入消息时可能引人的错误,有些阈下信道方案中发方在嵌入时需要较大的搜索量,有可能在某些条件限制下出现嵌入不成功的情况而又无法让收方知道,另一种是发方没有嵌入阈下消息而收方却认为已经嵌入了阈下消息而引起的错误。收方对提取的阈下消息的可信程度被称为信任度,用嵌入成功的概率来描述它。我们可以在阈下信道中引入冗余度来标记阈下信道是否存在或阈下消息是否被正确嵌入来改善信任度,比如当某一固定秘密比特值为1时阈下消息存在,0时不存在。但这种策略要折中安全度和信道容量。因为,该固定比特必然影响随机参数的概率分布,同时也不能用于传递阈下消息。

2.3 ELGamal 签名[12]

为后面叙述方便我们简单回顾一下 ELGamal 签名方案。用户密钥的产生如下:p 是一个大素数,$g\in GF(p)^*$ 是一个生成元;签名秘密钥 $x\in\{1,\cdots,p-2\}$,相应的公开密钥 $y=g^x \bmod p$。签名者(signer)首先计算消息 m 哈希值 $H(m)$,H 为标准的哈希函数,简记 $H(m)$ 为 H,满足 $0\leqslant H<p-1$,随机选择 $k\in_R\{1,\cdots,p-2\}$ 且 $\gcd(k,p-1)=1$。签名者计算 $1\leqslant r<p$,以及

$$r=g^k \bmod p \tag{1}$$

$$s=k^{-1}(H-xr) \bmod (p-1) \tag{2}$$

(s,r) 即为有效的签名。接收者通过检验 $1\leqslant r<p$ 及 $g^H=r^r y^r \pmod p$ 来验证签名。

3 阈下信道的分类及相关问题

我们根据阈下信道的不同构造原理来讨论分类问题,现存阈下信道可以分为四类。

A. 宿主系统提供陷门信息 阈下信道在密码数据中的存在性与密码数据本身的随机成份是密切相关的,而这些随机成份引入的本来目的在于提供一个安全的密码系统,比如概率公钥加密系统。密码系统中的这些随机成份是阈下消息的载体,如签名中的会话密钥。如果收方共享了发方的部分或全部的密码秘密钥,那么收方就能够获得部分或全部的随机成份。有些阈下信道方案的建立就是依赖于密码秘密钥等陷门信息对阈下收方的泄漏。以下叙述中 $t \bmod q$ 的值记做 t_q。

以2.3节的 ELGamal 签名为例,该类信道的一般方案如下:设 q 是签名子群的阶 $p-1$ 的一个因子,且阈下收发双方可知,$x_q=x \bmod q$ 为收发双方所共享的部分秘密钥。待传阈下消息 $M<q$ 随机化后得 RM。在会话密钥中的嵌入如下:$k=k'q+RM^{-1}$。k' 是满足签名条件的任意整数。阈下收方获得签名后,对2.3节中的签名方程(2)两边求模 q 得到 $s_q=RM^{-1}(H_q-x_q r_q) \bmod q$,此即 $RM=s_q^{-1}(H_1-x_q r_q)$。q 最好选作素因子,以使 RM 的逆存在。

目前有多个这样的信道:Simmons 于1993年在 DSA[13]中建立的宽带信道[3],在收方与发方之间共享完全的签名秘密钥,被称为宽带信道。Jinn-Ke Jan 和 Yuh-Min Tseng[8],Harn Lein[8]以及张方国[9]等分别提出的阈下信道也属于该类,阈下信道的收发双方共享部分密码秘密钥比特,它们属于窄带信道。

Newdon 信道[5]是 Anderson 于1996年提出的 ElGamal 签名中的一种阈下信道，利用 $GF(p)^*$ 中的平滑阶子群上离散对数问题的可解性来构造的，见附录 A。事实上，该信道的收方不必根据平滑阶去直接求解阈下消息，因为平滑因子 m 已经泄漏了相应长度的密钥比特，收方或任何其他人可直接从签名验证公钥 $y=g^x \bmod p$ 中求解出因平滑成份而泄漏的部分签名秘密钥比特 $x_m=x \bmod m$，然后可用前述的提取方法提取阈下消息。可见实质上 Newdon 信道属于 A 类信道中的一种。

显然信道的可实现容量近似等于密码秘密钥的泄漏比特数，密码数据中关于随机秘密参数的某些限制，比如 ELGamal 签名中会话密钥要与模互素的条件或阈下信道本身带来的约束条件，对实际容量都有一定影响。

A 类信道最大的优点就是可以根据要求最大限度地利用随机参数来传递阈下消息，但这种容量的扩大要以牺牲密码数据的安全性为代价，泄漏的密码秘密钥比特越多，密码数据对发方来说可保留的安全性就越小，当泄漏足够的比特以使收方的计算能力能够求解单项函数的逆时，密码数据几乎无安全性可言，如 Simmons 的宽带信道，签名者不得不将其秘密钥与收方共享，他要冒收方滥用其签名权力的危险。A 类信道的实现复杂度非常小，几乎不需要增加宿主系统的计算负担。其边信息量除了随机化密钥外，还有共享的部分或全部密码秘密钥。A 类信息道是现有几类信道中带宽优势最大的一类。其中只泄漏部分密码秘密钥比特的方案可以保留发方原始密码系统的安全性。

B. *控制单向函数的输出比特*　这里的单向函数是指密码系统中的(陷门)单向函数，其单向性依托所用的数学难题。在该类信道的构造中，发方通过搜索适合的随机秘密比特(如签名中的会话密钥)，以使输出具有与阈下比特相适应的特性，而不必泄漏密码秘密钥信息，典型的如1993年 Simmons 提出的 DSA 中的三种阈下信道[4]，它们同样存在于 ELGamal 签名中，分别包括：1)通过搜索签名的会话密钥 k 来控制签名的输出成份 r 对某秘密模数的二次剩余特性，使之与阈下比特相适应来构造信道；2)通过搜索适合签名会话密钥 k，使签名的输出成份 r 的最后 u 比特($u\geqslant 1$)等于待传的 u 比特阈下消息所构造的信道，以及3)根据具有较短指数的离散对数的可解性构造的信道。其中 k，r 的意义参见2.3节。

该类信道的嵌入复杂度比较高，需要大量的搜索，因此容量受到了极大的限制，均系窄带信道，这是因为由单向函数的输入控制其输出特性需要很大的计算量，控制选择的输出比特越多，计算复杂度越高。影响容量的主要因素是发方或收方的计算能力。Imai 等人对容量进行了详细讨论[18]，他们把该类阈下信道简化为单向函数的输入和输出之间的信道。设单向函数的输入为密码数据 D，输出为 S 则 Imai 的信道容量定义为 $Capa(S,D)=\max\limits_{\Pr(D)} I(S;D)$。实际嵌入时由于计算能力和诸多方面的限制，嵌入不总是成功的，记错误概率为 SER 有 $SER=(1-1/|M|)^n$，n 表示搜索次数，M 表示嵌入的消息集，则嵌入成功的概率为 $\Pr(m^*=m|m)=1-SER$，如果阈下信道的未嵌入概率为 p，则信任度为 $1-p-(1-p)SER$。实际信道容量定义为 $Capa(M^*,M)=\max\limits_{\Pr(M)} I(M^*;M)$，随着嵌入方案不同而稍有不同，Imai 最终给出了可达信道容量 $\max\limits_{|M|}(Capa(M';M))\approx\log_2 n-1.44$，这就是说要嵌入 x 比特信息至少要进行 $n_x=2^{x+1.44}=2.71\cdot 2^x$ 次搜索。

该类信道的嵌入复杂度呈2的指数形式上升。容量受到计算能力的限制，也影响着其应用范围。一般的该类信道不影响密码系统的安全性。由于其嵌入的消息是暴露的，因此阈下消息嵌入前必须进行加密，即阈下消息的随机化。随机化密钥是该类信息中主要的边信息。信任度较之 A 类要小得多。

C. *失败停止式的风险信道*　该类机制与 B 类的不同之处是，如果输出数据恰好与阈下比特相适应，则嵌入成功，阈下消息将被传递，否则发方将终止协议，但这将引起看守的怀疑，因而有风险。该类信道实用性很差，容量小。它存在的价值在于阈下信道的封闭性研究当中。典型实例是 Y. Desmedt 于1998年在文[14]中的构造，其目的是为了说明 Simmons 的封闭协议[19]并没有完全封闭阈下信道的结论。设嵌入消息为 u 比特，则嵌入成功的概率 $p=1/2^u$，平均容量 $C=up$。容易求得 $u=1/\ln 2$ 时平均容量取最大值0.5307比特。

D. *冗余数据的汉明校验*　Reihameh S. Safavi-Naini 在1991年讨论与纠错码相对偶的认证码时，在编码的冗余度中引入了阈下信道[15]。认证码分为保密的和非保密的两种，显然在具有消息保密作用的认证码中引入阈下信道是没有意义的，因为其本身就有加密功能。

无保密的认证码的一般结构是在待认证的消息后面附上具有校验能力的冗余度。一种办法是采用带密钥的编码方法构造认证码，另一种方法是采用带密钥的单项函数，比如用带密钥的哈希函数来构造认证码。

嵌入时将阈下消息以噪声的形式加入到冗余比特中，在收方利用码字纠错能力来恢复阈下消息，当错误样本的汉明重量在码字的纠错能力之内时，收方仍可正确认证。在采用带密钥的哈希函数构造认证码时，在不影响哈希函数碰撞特性的前提下可以改变哈希值的几个比特来构造阈下信道，只要错误比特的汉明重量足够小即可。

该类信道中嵌入的消息具有自验证特性，看守亦可以引入额外的噪声，因此安全度很低。为改善此情况，阈下消息必须引入冗余度，这又极大地限制了容量。虽然原则上纠错的最大能力可以看作容量，但由于安全度问题实际上要小得多，不是一种好的办法。

严格地说该类方案与一般的阈下信道的概念有些差别，更像信息隐匿(Steganography)系统。一般的带有阈下信道的密码系统传输的数据是确定的不能被修改的，也不能引入噪声。而含有该类信道的密码系统中看守可能在认证码中引入少许错误，并且满足收方的正确验证条件，这表明码字相当于存在噪声的掩饰数据。下面两点说明该类信道归入信息隐匿系统中更适合：1)与信息隐匿系统中的掩饰数据一样，建立了阈下信道的认证体制中认证消息的冗余度使得少量噪声的引入不影响原系统的可懂性；2)存在主动的看守(Active Warden)，嵌入消息应该进行鲁棒的编码才能正确提取。该类信道的嵌入相当于把阈下消息以噪声的形式嵌入系统。该系统的信任度与阈下消息的编码有关，需要考虑鲁棒性等因素。而且一个频繁引入噪声的认证系统，其安全性也值得考虑。

4　边信息协商

阈下信道的建立离不开收发之间所共享的边信息，一方面嵌入之前要进行随机化，以达到较高的安全度，另一方面如 A 类信道，阈下收方必须与发方共享部分或全部密码秘密钥比特才能提取阈下消息。如 Simmons[1]提出的“囚犯问题”，通常假设 Alice 和 Bob 在被捕入狱前共享了一串秘密比特 R，这为他们将来建立阈下信道协商逃跑计划创造了先决条件。而在实际应用中，这一先决条件可能得不到满足，或者 R 与阈下信道所需的边信息无关。在这种情况下，就需要一个获得边信息的方案，这就是我们提出边信息协商这个概念的背景。

以下分未知秘密比特串协商和已知秘密比特串协商两方面进行讨论。

4.1 未知秘密比特协商

如果 Alice 和 Bob 没有共享的随机比特串 R，可以采用下面的办法来实现边信息协商：

Adam Yong[16]，Y. Desmedt[17]等人曾经详细讨论了密码系统的滥用问题，该类系统可称为受污染的密码系统，比如文[16]中的 SETUP 体制。这是一种很强的构造，要求发方能够完全控制密码系统操作及其各个参数的产生算法，我们可以用这种受污染的体制作边信息协商。其原理如下：设某一个阈下收方发布的公钥为 Y，发方要与收方协商一个秘密比特串 R，则发方首先用公钥 Y 对 R 加密得密文 C，然后选择一个适合的公钥 Y' 将 C 嵌入到其中，并发布。该阈下收方从发布的公钥 Y' 中提取密文 C，并解密得到 R。从而可以利用所协商得边信息建立各种阈下信道。采用此方案阈下发方可以利用感染了的密码系统将边信息即密钥信息泄漏给任何所期望的收方，只需利用收方的公钥即可，但这种体制要求发方有较高的权限，即控制公私钥对的产生，应用上有一定的限制。详细的方案见文[16]。

我们也提出了另一种采用多次协议的方案。假设 Alice 要给 Bob 发送阈下消息，并知道 Bob 的一个公钥密码算法的公钥 Y，以 ELGamal 签名中的构造为例，收发双方协商密钥 R 的过程如下。设 q 是签名子群的阶 $p-1$ 的一个因子，且收发双方可知。Alice 首先利用 Bob 的公钥密码算法对 R 加密得密文 c，记 $c=c_{i-1}q^{i-1}+c_{i-2}q^{i-2}+\cdots+c_0$，$i\approx\lfloor|c|/q\rfloor$，之后运行 i 次签名协议。其中对任意的第 j 次协议($0<j\leqslant i$)，我们把 c_{i-j}^{-1} 嵌入于随机会话密钥的逆元当中，即 $k^{-1}=k'q+c_{i-j}^{-1}$，如果某个 c_{i-j}^{-1} 不存在则可以重新选取至满足条件。在第 $i+1$ 次协议时，以 x_q^{-1} 嵌入。收方在得到这 $i+1$ 个签名方程(2)后，分别对方程两边模 q，则由第 $i+1$ 次协议所获方程容易解得 $x_q=s_{q,i+1}^{-1}H_{q,i+1}(1+s_{q,i+1}^{-1}r_{q,i+1})^{-1} \bmod q$，再由前 i 次方程解出 $c_{i-j}=s_{q,j}^{-1}(H_{q,j}-x_qr_{q,j})$，$0<j\leqslant i$，从而恢复密文 c，其中 $s_{q,j}$，$r_{q,j}$，$H_{q,j}$ 表示第 j 次协议中的签名参数 s_j，r_j，H_j 模 q。Bob 再对 c 解密获得协商的密钥 R。最佳的方案是选择一个大的素因子 q，以使以上方案中的逆元均存在。在 ELGamal 签名中 q 的长度可以大于模长的三分之一而不影响签名安全性。这时只需四次以内的协议就可以完成边信息交换。

4.2 已知秘密比特协商

此时收发双方共享的随机串 R 与阈下信道所需的边信息无关，为了由 R 获得相关的陷门信息。一种在 ELGamal 签名中的方案如下：设 q 是签名子群的阶 $p-1$ 的一个因子，且收发双方可知，设阈下消息为 m，则协议执行时置 $k^{-1}=k'q+R_q^{-1}$，s，H，x，r，R 模 q 后记为 s_q，H_q，x_q，r_q，R_q 收方对签名方程(2)两边求模 q 得到 $s_q=R_q(H_q-x_qr_q) \bmod q$，可得 $x_q=(H_q-s_qR_q)r_q^{-1} \bmod q$。必须注意 q 的比特长度选择，要使密钥的泄漏量不至于影响宿主系统的安全性。

小结 本文对阈下信道的构造、容量及其应用问题进行了系统的讨论，并对其进行了分类。建立了一个适合于阈下信道的一般模型，并给出了安全度和信任度两个指标和含有阈下信道密码系统的定义。提出了边信息协商的概念并讨论了实现方案。对以上问题的研究使我们对阈下信道中的基本问题有了更系统的认识，这有益于我们进一步开展研究工作。寻找合适的阈下信道的信息论模型，研究新型阈下信道的建立方法和如何构造好的边信息协商方案等问题，值得进一步的研究。

参 考 文 献

1 Simmons G J. The prisonner's problem and the subliminal channel. Advances in Cryptology: Proceedings of CRYPTO' 83, Plenum Press, N. Y., 1984. 51～67

2 Simmons G J. The History of Subliminal Channels. IEEE Journal On Selected Areas In Communication, 1998, 16(4): 452～462

3 Simmons G J. Subliminal communication is easy using the DSA. Advances in Cryptology: Proceedings of EUROCRYPT' 93, Berlin, Springer-Verlag, 1993. 218～232

4 Simmons G J. The subliminal channeal in the U. S. Digital Signature Algorithm (DSA). In: Proc. of 3rd Symposium on State and Progress of Research in Cryptography-SPRC'93, Rome, Italy, Feb. 1993. 35～54

5 Anderson R, Vandeney S, Preneel B, et al. the Newton Channel. Lecture Notes in Computer Science 1174. In: Proc. of Information Hiding: First International Workshop, Cambridge, UK, May 30-June 1, 1996, Berlin: Springer-Verlag, 1996. 151～156

6 Simmons G J. A secure subliminal channel (?)'. Crypto'85 Santa Barbara, CA, August 18-22, 1985, Advance in Cryptology, Ed. by H. C. Williams, Springer-Verlag, Berlin, 1986. 34～41

7 Jan J K, Tseng Y M. New Digital Signature with Subliminal Channels Based on the Discrete Logarithm Problem. In: 1999 Intl. Worshops on Parallel Processing, Wakamatsu, Japan, 1999. 198～203

8 Hain L, Gong G. Digital signature with a subliminal channel. IEE. Proc. Comput. Digit, Tec., 1997, 144(6): 387～389

9 Zhang Fangguo, Lee B, Kim K. Exploring Signature Schemes with Subliminal Channel. SCIS 2003, The 2003 Symposium on Cryptography and Information Security vol 1/2, Itaya, Japan, 2003. 245～250

10 Cachin C. An Information-Theoretic Model for Steganography. In: Proc. 1998 Workshop on Information Hiding Porland, Oregon, Lecture Notes in Computer Sciences, Springer-Verlag, 1998

11 Zhang Tong. Studies on Information Hiding and Subliminal Channels: [Doctor Dissertation]. Xidian Univ. P. R. China. Oct. 2001. 51～57

12 ELGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Information Theory, 1985, 31(4): 469～472

13 A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS) Federal Register, Aug. 1991

14 Desmedt Y. Simmons' Protocol is Not Free of Subliminal Channels [C]. In: proc. of the 9th IEEE computer security foundations workshop, County Kerry, Ireland, 1996. 170～175

15 Safavi-Naini R S, Seberry J R. Error-Correcting Codes for Authentication and subliminal channels. IEEE Trans. On IT, 1991, 37(1): 13～17

16 Young A, Yung M. The Dark Side of Black-Box Cryptography or: Should We Trust Capstone?. Advances in Crytology-CRYPTO' 96, Springer-Verlag, pages 89～103

17 Desmedt Y. Abuses in cryptography and how to fight them. Advances in Cryptology-Proc. of Crypto' 88, Springer-Verlag, 1990. 375～389

18 Kobara K, Imai H. On the channel capacity of narrow-band subliminal channels. In: Proc. of the second intl. conf. on information and communication security, Sydney, Australia, Nov. 1999. 309～324

19 Simmons G J. An introduction to the mathematics of trust in security protocols [C]. In: Proc. Computer Scurity Foundations Workshop VI, IEEE Computer Society Press, 1993. 121～127

附录 A. ELGamal 签名中的 Newton 信道[5]

消息的嵌入：令 $p=qt+1$ 其中 t 是平滑的(对于一个适合的界 B，如果整数 t 的任何一个素因子 q 都满足 $q<B$，则称 t 是 B-平滑的，这里 B 是一个素阶群的最大可能阶，在该群上的离散对数问题采用现有数学方法和计算能力是可解的)。会话密钥 k 用平滑因子 t 和阈下消息 c 表示为 $k=c+k't$，k' 是使 k 满足 ELGamal 数字签名方案中参数条件的任意整数。

消息的提取：我们看这样一个事实，对 $r=g^k \bmod p$ 两边 q 次幂得到 $r^q=(g^k)^q=(g^q)^k=(g^q)^{c+k't}=(g^q)^c \bmod p$，这就是说提取阈下消息即是求解方程 $(g^q)^x=r^q \bmod p$。而 g^q 的阶 t 是 B-平滑的，我们可以利用求解 DLP 问题的 Pollard-ρ 算法和 Pohlig-Hellman 分解算法求解 x，运算的时间复杂度为 $O(\sqrt{B})$。