封闭阈下信道的理论模型*

李恕海, 王育民
(西安电子科技大学 ISN 国家重点实验室, 陕西 西安 710071)

摘 要: 提出了 2 个适用于封闭使用了随机数作为阈下信息载体的阈下信道的理论模型, 给出了该模型能够成功封闭阈下信道的几个条件, 并根据这 2 个模型分析并设计了几种封闭阈下信道的方案。总结得出封闭阈下信道的 2 个重要切入点——会话密钥的随机性和隐私性, 是封闭阈下信道成功与否的关键。

关键词: 阈下信道; 随机性; 隐私性
中图分类号: TN918.1 文献标识码: A 文章编号: 0529-6579 (2004) S2-0034-04

阈下信道作为信息隐藏的一个重要应用, 给信息安全带来了很大的挑战。自 Simmons[1-3] 提出阈下信道这一概念以来, 围绕建立与封闭阈下信道这两个相互矛盾、相互制约的技术, 信息安全界展开了广泛深入的讨论, 体现了人们对“安全”这一定义的深刻认识。在如今对信息安全要求越来越高的时代, 如何有效地封闭阈下信道, 使之不能为敌所用, 成为各种安全机构需要注意的问题。但是目前绝大多数签名体制中都可能存在阈下信道, 许多签名体制中的阈下信道在正常通信的意义下是受到保护的, 而且阈下信息一旦嵌入, 公开信道的监督方要提取通过阈下信道传送的信息, 在计算上是不可行的。这就给通信方的监督者合法地监控往来信息, 如政府的安全机关监控与敌对政府的通信造成了很大的困难。因此就需要有效地封闭阈下信道。

1 阈下信道的成因分析

1.1 必要条件——密文的冗余

众所周知, 自香农提出信息保密理论以来, 几乎所有的密码算法都是把对明文的混淆和扩散作为隐藏明文与密钥之间的依赖关系和统计特性的基本手段。现代加密体制, 尤其是双钥体制, 在明文加密或签名成密文时完成了混淆和扩散从而提供足够的安全性, 同时也增加了密文的冗余。密文长度要大于等于明文长度, 密文空间大于明文空间, 即一个明文可能对应几个不同的密文。通过这种方法密码分析者在密文空间里找到明文对应的密文的可能性小于在明文空间中猜测哪个是明文的可能性, 从而使得密文的安全性依赖于加密体制的难解性成为可能, 与此同时在密文空间也产生了冗余。这种做法在保密明文的安全意义下是完善的, 但是对于这些冗余信息的控制造成了一定的困难, 给不在意其明文安全性的潜在阈下信道使用者提供了安排阈下信息的空间。

1.2 阈下信息的载体——“随机数”

随机数在安全领域中重要性不言而喻, 它的存在保证了明文的统计特性不被密文泄漏。在各种典型的阈下信道存在的加密体制中, 如: ElGamal, DSS 等都是用了随机数作为会话密钥, 而该会话密钥又不能被其他任何人知道, 否则其私钥便有可能被破译。这样任何人都有足够的理由把这个会话密钥和私钥一样作为其隐私保护起来, 不让其他任何人知道, 即会话密钥具有“隐私性”。如果这个会话密钥确实是随机的, 那么阈下信道就不存在了。问题的关键在于: 阈下信息的嵌入者不会真正去选择随机数来作为会话密钥, 恰恰相反, 他们正是利用这个“随机的隐私”来传递阈下信息的。由于会话密钥的隐私性, 阈下信道的监督方不能解密出阈下信道中传送的信息, 甚至不知道阈下信道是否被使用; 而阈下信道的接收方则因为知道发送方的私钥可恢复出阈下信息。由此可见, 会话密钥的随机性得不到保护是产生阈下信道的根本原因。

由上述分析可以看出, 要封闭阈下信道有两种方法, 一是去掉密文的冗余; 二是在不影响加密方的私钥安全性的同时确保加密体制中的随机数真正随机, 即保证其隐私性和随机性。显然, 第一种方法在现有的体制中很难实现, 因为去掉密文的冗余的代价是牺牲加密体制的安全性, 这是任何人不能

* 收稿日期: 2004-09-11
基金项目: “十五”军事通信预研资助项目 (41001040303)
作者简介: 李恕海 (1980 年生), 男, 博士研究生; E-mail: lishuhai9811118@163.com

接受的，那么只有在第二种方法可供选择了。

2　封闭阈下信道的理论模型

从保证会话密钥的隐私性和随机性入手，构建了两种封闭阈下信道的理论模型：

2.1　无监督方的基于真随机数的封闭阈下信道模型

该模型是通过对真随机数的使用来封闭阈下信道的（图 1），这些真随机数不是来自于加密方，而是与之完全独立的公正的第三方（政府机构的安全部门）或者真随机数发生器（这里的真随机数是指任何人不能重新生成的真随机数，包括产生它的人）。

在实现中可以设置一个随机数产生机构或对加密方完全透明的随机数发生器来近似模拟真随机数发生器，保证每次加密时，加密方只能使用这个随机数产生机构或指定的随机数发生器所产生的随机数作为会话密钥。从而避免了阈下信道的发送方任意选择会话密钥的可能，确保了会话密钥的随机性；同时由于公正方的可信赖性或真随机数不能重新生成的特性来保障会话密钥的隐私性。这样便可以成功的封闭阈下信道。

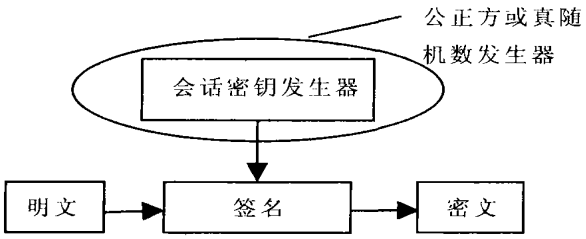

图 1　无监督方的封闭阈下信道模型

Fig 1　The models of closing the subliminal channels without supervision

2.2　有监督方参与的封闭阈下信道模型

加密方必须在监督方的“参与”下产生随机数作为会话密钥，同时必须满足“随机性”和“隐私性”，这里的随机性不但对加密方重要而且对监督方同样重要，因为要保证会话密钥的随机性，就像是两个人一起来生成一个随机数，有一个人是用随机数来生这个随机数就能保证这个随机数是随机的，同样加密方和监督方之间至少要有一个人真正用随机数参与会话密钥的生成（图 2）。

该模型的执行步骤如下：

(1) Alice 和 Carol 给 RNG 一个随机数作为种子，通过 RNG 协商生成会话密钥 k 来加密明文 m，得到密文 c。在这个过程中 Alice 同样可以监督

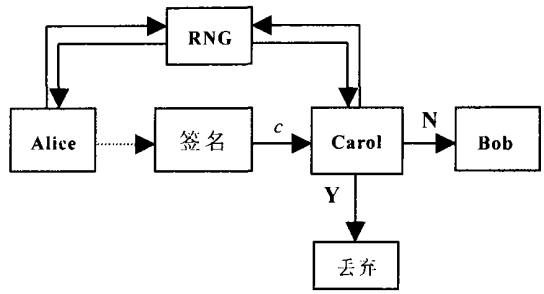

图 2　有监督方参与的封闭阈下信道模型

Fig 2　The model of closing the subliminal channels with supervision

Alice：加密或签名方；Bob：解密或验证方；
Carol：监督方；c：密文；RNG：会话密钥发生器；
N：Carol 验证 Alice 没有使用阈下信道；
Y：Carol 验证 Alice 使用阈下信道

Carol，若 Carol 在生成会话密钥的过程中建立了阈下信道，Alice 可以选择放弃加密，图中虚线表达了这个过程。

(2) Carol 检验该密文 c。若 Alice 使用 k 加密 m，则认为 Alice 没有使用阈下信道，将 c 送给 Bob；否则认为 Alice 使用了阈下信道，拒绝把 c 送给 Bob。

由上面的分析和模型的执行步骤可知 RNG 必须满足以下条件：

(1) 能够根据双方发送的密钥种子随机生成一个会话密钥，且不能被 Carol 知道；

(2) Carol 必须能够检验 Alice 是否真的使用了 RNG 生成的会话密钥；

(3) RNG 必须足够安全，不能被轻易分析；

(4) 不能让 Alice 和 Carol 任何一方有控制 k 的可能。

满足上述条件的 RNG 使得 Alice 和 Bob 在公平的状态下协商会话密钥，保证了“隐私性”和“随机性”。

3　应用封闭模型分析和设计实例

3.1　分析 Simmons 提出的一种封闭方案

以 DSS 签名算法为例，其体制描述：

公钥：一个大素数 p，长度在 512 和 1024 位（bit）之间，且为 64 的倍数，$p-1$ 具有一个 160 位的大素因子 q，计算 $g \equiv l^{(p-1)/q} \bmod p$，$l \in \{1, 2, \cdots, p-1\}$，$l$ 与 $p-1$ 互素；

私钥：$x \in \{1, 2, \cdots, p-1\}$；

验证密钥：$y \equiv g^x \pmod p$。

签名过程：Alice 首先把待签消息 m 杂凑成 $h = H(m)$，选择一个随机数 $k \in \{1, 2, \cdots, q-1\}$，$k$

是 Alice 随机选择的会话密钥，计算

$$r \equiv (g^k \bmod p) \bmod q,$$
$$s \equiv k^{-1}(h + xr) \bmod q$$

这里 $kk^{-1} \equiv 1 \pmod p$，三元组 (m, r, s) 作为签名消息被传了出去。

验证过程：Carol 收到 (m, r, s)，计算出 $h = H(m)$，$u_1 = hs^{-1} \pmod q$，$u_2 \equiv rs^{-1} \pmod q$，$v \equiv (g^{u_1} y^{u_2} \bmod p) \bmod q$。验证 $r = v$ 是否成立，若成立则认为签名有效。

DSS 阈下信道[4] 是利用会话密钥 k 来传递阈下信息的。过程如下：Bob 知道 Alice 的私人密钥 x，Alice 发出的签名消息 (m, r, s) 中，

$r \equiv (g^k \bmod p) \bmod q$，$s \equiv k^{-1}(h + xr) \bmod q$

q 是素数 $GF(q)$ 中所有非零元均有乘法逆元，假定 $w = h + xr \neq 0$，那么 $k \equiv s^{-1}w \pmod q$，即恢复出阈下信息 k。

3.2 Simmons 封闭方案

(1) 签名者 Alice 选择一个子密钥 k'，k' 是 $GF(q)$ 中的随机数，计算 $z \equiv g^k \pmod p$，把 z 送给 Carol；

(2) Carol 也选择一个子密钥 k''送给 Alice；

(3) Alice 计算会话密钥 $k \equiv k' \cdot k'' \pmod{p-1}$，用 k 来签名消息 m，得到三元组 $(H(m), r, s)$；

(4) Carol 验证 $r \equiv (z^{k''} \bmod p) \pmod q$，若成立则可验证 Alice 没有传递阈下信息。

分析：该方案的 (1)、(2) 两步完成的实际上就是前述第二个模型中 RNG 的功能。它用基于离散对数的求解困难性来使 Carol 无法了解 k'，从而不能得到 k，而且满足了安全性。同时 Carol 用它的随机种子 k''保证了 k 的随机性，并能够在第 (4) 步中检验 Alice 是否使用了 k 来加密。

但是这个方案也有缺陷，因为 Carol 可以通过在第 (2) 步中尝试 k''使 r 具有某些 Carol 想要的性质，便产生了“布谷鸟”信道[2]，也就是说 Carol 的“种子”——k''不随机，故该方案不满足第二个模型中 RNG 的条件 (4)。可以看出“布谷鸟”信道的产生其根本原因在于 Carol 可以“不随机”的控制由会话密钥 k 生成的 r，所以只要不能保证 k 的随机性便不能真正封闭阈下信道。

在文献[5—7] 中列举的几种封闭方法，同样可以用上述模型进行分析来确定是否能成功地封闭阈下信道，这里就不再赘述了。

3.3 两种基于有监督方参与的封闭阈下方案

针对上述方案不能禁止 Carol 可能操纵签名中的某些位的情况，一种基于单向散列函数的抛币协议[4] 的封闭方案可以解决这一问题，方案如下：

(1) Carol 选择 k''，将 $h = H(k'')$ 送给 A，其中 H 是公开的单项散列函数；

(2) Alice 选择 k'，将 $z \equiv g^{k'} \pmod p$，送给 Carol；

(3) Carol 将 k'' 送给 A；

(4) Alice 验证 $h = H(k'')$ 是成立来判断 Carol 是否使用了“布谷鸟”信道；若该等式成立则表示 Carol 没有使用“布谷鸟”信道，然后用 $k = k' \cdot k'' \pmod{p-1}$ 做会话密钥来签名消息 m，得到三元组 $(H(m), r, s)$；

(5) Carol 验证 $z^{k''} \equiv (r \bmod p) \bmod q$ 是否成立，若成立便认为 Alice 没有使用阈下信道；反之就表明 Alice 使用了阈下信道并拒绝 Alice 发送的消息。

在这个方案中，(1)、(2)、(3) 步为 RNG，其中 (1) 和 (4) 使用了单向散列函数来控制 Carol 选择 k''时的随机性，使之不能随意选择 k''来操纵签名中 r 的某些位，来建立自己的“布谷鸟”信道，因为如果 Carol 像前面的方案一样在第 (3) 步中任意尝试 k''来寻找想要的 r，那么 Carol 有 $(q-1)/q$ 的概率选择的 k'' 与在第 (1) 步中发送给 Alice 的 k''不同，这样 Alice 便可以通过检验 Carol 在第 (3) 步中发送的 k''的杂凑值 $H(m)$ 是否与第 (1) 步收到的 h 相等来判断 Carol 有没有使用“布谷鸟”信道。满足了 RNG 条件 (4)。(2) 和 (4) 确保了 Carol 监督并参与了 k 的生成，而且是基于离散对数的难解性满足了 RNG 条件 (1)，(2)，(3)。因此，它成功的封闭了阈下信道和“布谷鸟”信道。

这里还有一种方案可以封闭阈下信道和“布谷鸟”信道。

(1) Alice 发送 $H(z_1)$，$z_1 = g^{k'} \pmod p$ 给 Carol；

(2) Carol 发送 k''给 Alice；

(3) Alice 以 $k = k' + k'' \pmod{p-1}$ 为会话密钥来签名 m，把得到的三元组 $(H(m), r, s)$ 发送给 Carol；

(4) Carol 检查 $H(r \cdot g^{-k''} \bmod p) \equiv H(z_1)$ 是否成立来判断 Alice 有没有是用阈下信道。

同上面的方案一样，这里的 (1)、(2)、(3) 步为 RNG，Carol 也是通过 k''来封闭 Alice 的阈下信道，并且 (4) 能够判断 Alice 是否使用了双方协商的会话密钥 k，传送方法是基于离散对数的难解性及杂凑函数的安全性都可以满足 RNG 条件 (1)、(2)、(3)。这个方案与 Simmons 封闭方案类似，所不同的是在这里的 (1) 中 Alice 使用 $H(Z_1)$ 来确保 RNG 生成的会话密钥 k 的隐私性，同时由于 Carol

只知道 $g^{k'}$ 的杂凑值而不知道 $g^{k'}$ 的值就不能通过尝试 k'' 的方法来寻找其想要的 r，从而保证了会话密钥的“随机性”便不能使用“布谷鸟”信道。满足了 RNG 条件（4）。

4　结　语

作为当今信息隐藏的一个重要分支，阈下信道是近年来信息安全领域的一个热点问题。本文通过讨论阈下信道的形成原因，深入探讨了封闭阈下信道的关键问题——使用两类真随机数来保证会话密钥的隐私性和随机性。并以此建立了两个封闭阈下信道的理论模型及成功封闭阈下信道的条件。随着各种先进的通信方式的普及与应用，人们对信息安全的要求也越来越高，与此相对的是安全机构对信息的监管力度也随之加强，如何在不损伤人们隐私权的同时阻止有害信息的传递是信息安全发展的一个潜在方向，正如对阈下信道的封闭一样是值得我们进一步开展研究的重要问题。

参考文献：

[1] SIMMONS G J. Subliminal channels: past and present[J]. European Transactions on Telecommunications, 1994, 4(7/8): 459－473.

[2] SIMMONS G J. Cryptanalysis and protocol failures[J]. Communications of the ACM, 1994, 37(11): 56－65.

[3] SIMMONS G J. A secure subliminal channel (?) // WOLLIAMS H C. Advances in Cryptology[C]. Berlin: Springer-Verlag, 1986: 33－41.

[4] SCHNEIER B. 应用密码学、协议、算法与 C 源程序[M]. 吴世忠, 祝世雄, 张文政, 等译. 北京: 机械工业出版社, 2001: 62－63, 349－350, 382－384.

[5] 张彤. 信息隐藏与阈下信道技术研究[D]. 西安: 西安电子科技大学, 2001.

[6] 张彤, 杨波, 王育民, 等. 抵御分割选择法的阈下信道及其带宽分析[J]. 西安电子科技大学学报, 2000, 27(3): 344－347.

[7] 张彤, 杨波, 王育民, 等. 封闭阈下信道的若干方法研究[J]. 通信学报, 2002, 23(4): 17－21.

The Models of Closing the Subliminal Channels

LI Shu-hai, WANG Yu-min

(Information Security Institute in ISN, Xi'an University of Electronical Technology, Xi'an 710071, China)

Abstract: The article introduces why the subliminal channels exist, and generalizes two models of closing the subliminal channel using random numbers to carry subliminal information. Thus two models to closing the subliminal channels using the principle arpresented, and then according the two models several plans which are used to closing the subliminal are analyzed and devised.

Key words: subliminal; randomness; privacy