论 文

常规隐信道下可证明安全隐写术的有效构造方法

朱岩^{①②*}, 余孟扬^③, 胡宏新^④, Ahn Gail-Joon^④, 赵红佳^{①②}

① 北京科技大学计算机与通信工程学院, 北京 100083

② 北京大学计算机科学技术研究所, 北京 100871

③ 北京大学数学科学学院, 北京 100871

④ School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, AZ 85287, USA

* 通信作者. E-mail: zhuyan@ustb.edu.cn

收稿日期: 2011-03-15; 接受日期: 2011-10-14

国家自然科学基金 (批准号: 61170264, 10990011)、国家重点基础研究发展计划 (批准号: 2013CB329606)、美国国家自然科学基金 (批准号: NSF-IIS-0900970, NSF-CNS-0831360) 和美国能源部基金 (批准号: DE-SC0004308) 资助项目

摘要 隐写术是在看起来无害媒体中隐藏信息的科学. 文中为了解决在常规隐信道下可证明安全隐写术的有效构造问题, 在不依赖于任何采样假设的前提下, 提供了一种基于计算不可区分的安全隐写术构造. 文中结果表明, 隐信道采样器中影射函数的不可区分性是安全隐写系统抵抗自适应选择隐文攻击的必要条件. 在此基础上, 完整地证明了 $l(\epsilon_1 + 5\epsilon_2)$ —安全隐写系统能在 ϵ_1 伪随机函数和 ϵ_2 无偏采样函数下有效地被构造, 其中, ϵ_1 和 ϵ_2 是任意两个可忽略错误, l 是多项式的隐文长度. 更为重要的, 文中的研究不依赖于密码系统的密文伪随机性假设和完美采样假设, 因此, 我们的结果对于安全隐写系统的构造和隐写分析都具有现实意义.

关键词 密码学 隐写术 不可区分性 采样器 不可预测性 敌手模型

1 引言

隐写术是一种利用看似无害的消息或无关的媒介进行信息隐藏的科学, 例如, 匿名通信^[1]、匿名在线交易、计算机系统中的隐藏信道^[2]、隐藏或阉下通信以及知识产权保护中的隐形水印与数字指纹^[3], 等等. 显然, 假如我们期望通信是对于人或计算机来说是不可察觉的, 那么含有隐藏消息的通道 (被称为伪掩文或伪文, stegotext) 必须与无害载体通道 (被称为掩文, covertext) 是不可区分的. 因此, 本文研究工作的起点也是这种不可区分性 (indistinguishability).

安全性, 如同稳固性、不可知性一样, 是隐写术研究的一个关键方面. 1998 年, Cachin^[4] 使用信息论模型来研究隐写术的安全性, 该文首次引入“相关熵”(relative entropy) 作为量化观测信道中所含信息量的一种基本形式, 并以此定义了无条件安全的隐写系统. 直到 2002 年, Hopper、Langford 与 Ahn^[5,6] 才首次提出使用复杂性理论方法来研究隐写术. 但是, 该文中的安全性证明只适用于完美采样 Oracle 假设下. 这种假设需要信道样本相互独立, 这在大多数情形下是不实际的. 此外, 该文是在具有伪随机密文的 IND-CPA 安全密码系统与没有偏差的完美采样的强假设下证明了安全隐写术存在的前提, 然而, 这种假设在现有密码系统 (例如, RSA, Elgamel 加密系统) 和通信环境下并不成立^[7].

引用格式: 朱岩, 余孟扬, 胡宏新, 等. 常规隐信道下可证明安全隐写术的有效构造方法. 中国科学: 信息科学, 2013, 43: 657–669, doi: 10.1360/112010-1345

基于上述工作, 国内外学者开始研究各种保障隐写术语义安全的技术. 例如, Dedic 等人^[8]进一步降低了隐藏信道的要求, 并且提出了一种黑盒隐写术. 该文中基于拒绝采样编码器^[5]给出了两个改进算法. Von Ahn 与 Hopper^[9]创建了公钥隐写术与选择伪文攻击 (SS-CSA). Backes、Cachin^[10]与 Hopper^[11]研究了自适应选择伪文攻击. Lysyanskaya 与 Meyerovich^[12]讨论了在更弱的假设下的非完美样本的问题, 在这种假设下伪掩文分布被看作是一种马尔科夫 (Markov) 过程. 但是, 为了构造一个更实际的隐写系统, 仍需要对基本安全问题和有条件非完美采样信道做更进一步的讨论.

众所周知, 不可区分性是密码学安全分析的一个关键因素, 我们认为其也是隐写术安全分析的基础. 尽管这方面在之前的论文中已有所讨论^[5,8,11,12], 但是仍然缺乏对于不带任何样本采样假设下如何构造一个安全隐写系统的深入研究. 这是因为过强的假设致使敌手的攻击能力被低估, 从而导致实际应用的隐写系统易于被敌手攻破. 通常, 这种敌手假设是基于敌手缺少掩文分布的信息. 有许多方法来刻画这种能力: 独立分布的完美采样^[5]、Markov 过程中具有 α 阶的 α -无记忆的半自适应采样^[12]等等. 但是, 这些假设在实际应用中仍然太强. 因此, 削弱或者减少这些假设将是进一步研究的关键. 幸运的是, 现有复杂性理论中关于伪随机性、不可预测性与随机化无偏差样本函数的方法, 为处理在常规掩蔽信道 (不带样本采样假设) 中的此类问题研究提供了一个很好的途径.

在本文中, 我们专注于在不带任何样本假设下的常规掩蔽信道上构造安全隐写术. 通过构造一个更一般的隐写系统, 我们证明了隐信道采样器中影射函数的不可预测性 (unpredictability) 对于构造具有抗自适应选择隐文攻击下不可区分性 (IND-CHA) 的安全隐写系统是不可或缺的. 进一步, 我们证明如果存在 ϵ_1 -伪随机函数和 ϵ_2 -无偏差采样函数, 则计算安全的 $l(s_1 + 5s_2)$ 隐写术是可行的, 其中, ϵ_1 和 ϵ_2 是两个可忽略错误. 虽然先前的研究中已有类似的结论, 我们通过严格证明得到的结果可提供更完整的框架与更一般的结果. 特别地, 我们的研究剔除了强 IND-CPA 假设和完美采样假设, 从而避免在这种假设下用于构建隐写系统的密码系统的密文必须是伪随机的约束. 因此, 我们的构造揭示出安全隐写系统更一般性的构造, 并且所得结论也适用于应用到实际隐写系统的构造与分析中.

本文的组织结构如下: 我们在第 2 节中描述了隐写系统的一些基本概念及一般定义. 在第 3 节中, 我们基于 “left-right Oracle” 定义了一种 IND-CHA 安全的形式化隐写术模型. 在第 4 节中, 我们构造一个 IND-CHA 安全的隐写系统, 并且给出它的安全性分析. 最后, 我们在第 5 节给出结论.

2 预备知识

2.1 基本概念

在本文中, 我们用一个博弈过程来表述系统的安全性. 在这个博弈过程中, 敌手可以选择两个消息, 并由被测试系统随机选取其中一个进行隐藏, 并送给敌手猜测. 如果没有敌手可以比随机猜测更大的概率找出被隐藏的消息, 那么我们说该隐写系统被称作是安全的. 在我们陈述这个博弈过程之前, 我们先回顾可忽略函数的定义:

定义 1 (可忽略函数) 一个函数 $f: \mathbb{N} \rightarrow [0, 1]$ 称为可忽略的, 如果对任意多项式 $p(\cdot)$, 存在整数 N 使得 $|f(n)| < 1/p(n)$, 对任意 $n > N$.

也就是说, f 是渐近小于任何一个多项式的倒数. 本文将关注于有界错误概率多项式时间 (BPP, bounded-error probabilistic polynomial time) 语言, 并假设它可以被概率多项式时间 (PPT, probabilistic polynomial time) 图灵机以可忽略错误概率被识别.

计算不可区分性的定义是由 Goldwasser 和 Micali^[13]引入的, 并且由 Yao^[14]给出完整的一般性

定义. 其定义如下:

定义 2 (计算不可区分性) 两个概率集合, $X = \{X_n\}_{n \in \mathbb{N}}$ 和 $Y = \{Y_n\}_{n \in \mathbb{N}}$, 是计算不可区分的, 如果对任意概率多项式时间 (PPT) 区分器 D , 任意多项式 $p(\cdot)$, 及所有足够大的整数 n , 满足

$$|\Pr[D(1^n, X_n) = 1] - \Pr[D(1^n, Y_n) = 1]| < \frac{1}{p(n)}. \quad (1)$$

注意, $|X_n| = \Omega(n)$ 记为 X_n 中样本的长度. 很明显, 如果两个集合是统计接近的, 那么它们也是计算不可区分的. 反过来则不一定正确. 如果 U_n 为一个 n 比特串上的均匀分布, 则称该集合 $\{U_n\}_{n \in \mathbb{N}}$ 为均匀集合. 有了上述定义, 很容易如下定义伪随机性集合:

定义 3 (伪随机集合) 集合 $X = \{X_n\}_{n \in \mathbb{N}}$ 被称为伪随机的, 如果存在一个均匀集合 $U = \{U_n\}_{n \in \mathbb{N}}$, 使得 X 与 U 在多项式时间内计算不可区分.

更进一步, 记 $f: \{0, 1\}^s \times \{0, 1\}^L \rightarrow \{0, 1\}^l$ 为一族函数. 如果 f 是一个多项式时间确定算法, 并且集合 $\{f_k(U_n)\}_{n \in \mathbb{N}}$ 也是伪随机的, 那么我们称 f 是一个伪随机函数¹⁾.

另两个重要的概念是采样函数与无偏差函数. 给定一个复杂组合信道, 最简单的采样方法可能就是 Monte Carlo 方法, 或者被称为拒绝采样. 不失一般性, 我们在本文中也使用这个方法, 记为 $\text{Sample}_f^C(k, b)$ 函数. 该函数使用一个采样 Oracle, $\mathcal{O}^C$, 从隐蔽信道分布 $\mathcal{C}$ 中提取样本, 并根据一个函数 $f_k(\cdot)$ 将多比特字符 b 映射到该样本中, 其中, k 为密钥. 由于 Oracle 的存在, 使得该算法与一般的 Monte Carlo 算法有显著区别.

为了刻画采样空间中映射函数的统计性质, 我们定义无偏差函数如下:

定义 4 (无偏差函数) 函数 $f: \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{R}$ 被称为在分布 $\mathcal{K}, \mathcal{C}, \mathcal{R}$ 上的 (t_b, ϵ) - 无偏差函数, 如果对任意 $r \in \mathcal{R}$, 满足 $|\Pr_{x \leftarrow \mathcal{C}}[f_k(x) = r] - 1/|\mathcal{R}|| \leq \epsilon$, 其中 $|\mathcal{R}|$ 表示 $\mathcal{R}$ 中元素个数, t_b 表示 f 的时间复杂度.

如果 $\epsilon = 0$, 那么我们称函数 f 是无偏差的, 也就是说, $\Pr_{x \leftarrow \mathcal{C}}[f_k(x) = r] = 1/|\mathcal{R}|$. 一个函数被称为 ϵ - 偏差函数, 如果偏差 ϵ 是一个可忽略函数.

2.2 隐写系统的定义

假设存在这样一个公共信道 $\mathcal{C}$, 在该信道中发送方可以与接收方交流, 但敌手只能以只读形式访问. 同时, 我们也假设存在一个对任意消息可有效生成伪掩文的信源编码. 在此基础上, 一个隐写系统的模型^[5,6]可定义如下:

- $\mathcal{C}$ 为具有概率分布 $\Pr_{\mathcal{C}}$ 的隐蔽通道 (被称为掩文, coverttext). 假设 $\mathcal{C}$ 在采样后可被有限序列 $\{(c_1, \dots, c_l) | l \in \mathbb{N}, c_i \in \Sigma, 1 \leq i \leq l\}$ 表示, 其中, Σ 为有限源字母表²⁾.
- $\mathcal{P}$ 为具有概率分布 $\Pr_{\mathcal{P}}$ 的隐文 (hiddentext) 空间, 并且 $\Pr_{\mathcal{P}}$ 与 $\Pr_{\mathcal{C}}$ 统计独立.
- $\mathcal{S}$ 为具有概率分布 $\Pr_{\mathcal{S}}$ 的伪掩文 (stegotext) 空间. 为满足不可感知性, 我们让 $\mathcal{S}$ 与 $\mathcal{C}$ 相同 ($\mathcal{S} = \mathcal{C}$). 但某些情形, $\Pr_{\mathcal{S}}$ 与 $\Pr_{\mathcal{C}}$ 可能是不同的.

假设任何一个公共信道上的伪掩文序列是由伪掩文的独立重复组成. 与密码学类似, 我们记 $\mathcal{K} = \{0, 1\}^*$ 表示密钥空间. 基于上述 $(\mathcal{C}, \mathcal{P}, \mathcal{S}, \mathcal{K})$, 一个隐写系统 Φ 可定义如下:

1) 密码学中伪随机函数的拓展性质也许在隐写术中是非必要的, 因此可在实际中使用普通 Hash 函数作为伪随机函数.

2) 不失一般性, 我们也可把 Σ 中的 r_i 映射为有限域 $\mathbb{F}_q$ 中的元素 c_i . 例如, 图像水印中的像素操作可被看作是有限域 $\text{GF}(2^8)$ 中的模运算.

定义 5 (隐写系统^[11,12]) 一个有效的隐写系统是由概率多项式时间算法组成的三元组 $\mathcal{SS} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$, 其满足:

- 对于输入 1^n , 算法 $\mathcal{G}$ (密钥生成器) 输出比特串 k 作为私钥, 其中, n 为安全参数.
- 对于 $\mathcal{G}(1^n)$ 输出范围内的私钥 $k \in \mathcal{K}$, 隐蔽信道分布 $\mathcal{C}$, 以及所有隐文 $m \in \mathcal{P}$, 编码算法 $\mathcal{E}$ 输出伪掩文 $s \in \mathcal{C}$, 即 $s \leftarrow \mathcal{E}^{\mathcal{C}}(1^n, k, m)$.
- 对于 $\mathcal{G}(1^n)$ 输出范围内的私钥 $k \in \mathcal{K}$, 隐蔽信道分布 $\mathcal{C}$, 以及所有伪掩文 $s \in \mathcal{S}$, 译码算法 $\mathcal{D}$ 输出消息 $m \in \mathcal{P}$ 或者终止符 $\perp$, 即 $\{m, \perp\} \leftarrow \mathcal{D}^{\mathcal{C}}(1^n, k, s)$, 并且概率

$$\Pr[\mathcal{D}^{\mathcal{C}}(1^n, k, \mathcal{E}^{\mathcal{C}}(1^n, k, m)) \neq m]$$

是对于 n 可忽略的, 这里的概率是根据作为算法 $\mathcal{E}$ 和 $\mathcal{D}$ 输入的内部抛币, 以及信道分布 $\mathcal{S}$ 而得到的. 算法 $\mathcal{D}$ 或者返回表示失败的终止符 (空消息) $\perp$, 或者返回隐文 $m \in \mathcal{P}$. 特别地, 我们需要

$$\Pr[\mathcal{D}^{\mathcal{C}}(1^n, k, \mathcal{E}^{\mathcal{C}}(1^n, k, \perp)) = \perp] = 1$$

成立. 有时我们也把加密算法与解密算法简写作 $\mathcal{E}_k^{\mathcal{C}}(m)$ 与 $\mathcal{D}_k^{\mathcal{C}}(s)$. 在本文中, 我们更关注于检测隐文是否出现的有效算法, 而不是如何解密伪掩文. 这种情形下, 解密算法 $\mathcal{D}$ 也被称作判定算法, 如果 $\mathcal{D}$ 输出比特 $b \in \{0, 1\}$, 其中, $b = 1$ 表示出现隐藏信息, 否则 $b = 0$. 我们称这样的 $\mathcal{D}$ 为检测器.

根据文献 [5,8,11,12] 中的定义, 我们假设存在对于空消息可进行随机采样的加密算法 $c_n \leftarrow \mathcal{E}_{\mathcal{G}(1^n)}^{\mathcal{C}}(\perp)$. 基于此, 我们可定义计算隐藏性如下:

定义 6 (计算隐藏性^[5,12]) 我们称隐写系统 $\mathcal{SS} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ 具有计算隐藏性, 如果下述关系成立: 给定隐蔽信道分布 $\mathcal{C}$, 对于伪掩文 $c_n \leftarrow \mathcal{E}_{\mathcal{G}(1^n)}^{\mathcal{C}}(\perp)$ 及任意隐秘文 $s_n \leftarrow \mathcal{E}_{\mathcal{G}(1^n)}^{\mathcal{C}}(m)$ 是多项式时间内不可区分的, 也就是, 对于任意概率多项式时间算法 D , 任意隐文 $m \in \mathcal{P}$, 任意多项式 $p(\cdot)$, 以及充分大的整数 n , 都满足如下不等式:

$$\left| \Pr[D^{\mathcal{C}}(1^n, \mathcal{E}_{\mathcal{G}(1^n)}^{\mathcal{C}}(m)) = 1] - \Pr[D^{\mathcal{C}}(1^n, \mathcal{E}_{\mathcal{G}(1^n)}^{\mathcal{C}}(\perp)) = 1] \right| < \frac{1}{p(n)}.$$

这里的概率是根据算法 $\mathcal{G}, \mathcal{E}$ 输入的内部抛币以及分布 $\mathcal{C}$ 得到的.

3 IND-CHA 安全性定义

本文中的 IND-CHA 安全性可通过一个攻击者和挑战者之间的博弈过程来描述, 攻击者在该过程中可以选取两个消息, 其中一个消息被随机选取, 另一个为空消息, 挑战者则选择任意一个并由隐写系统进行隐蔽传输. 如果攻击者只能通过随机猜测来判断哪个消息被隐藏, 就称这个隐写系统是安全的. 或者不严格的说, 在此博弈过程中攻击者区分掩文和伪文是困难的.

下面我们将给出 IND-CHA 攻击的形式化定义, 定义中的不可区分性通过文献 [13] 中的 “left-or-right” 模型来度量. 定义 left-or-right Oracle 为 $\mathcal{E}_k^{\mathcal{C}}(\mathcal{LR}(\cdot, \cdot, b))$, 其中, $b \in \{0, 1\}$. 当输入为 (x_0, x_1) 时, 该 Oracle 操作如下: 若 $b = 0$, 它计算 $c_0 \leftarrow \mathcal{E}_k^{\mathcal{C}}(x_0)$ 并且返回 c_0 ; 否则 ($b = 1$), 它计算 $c_1 \leftarrow \mathcal{E}_k^{\mathcal{C}}(x_1)$ 并返回 c_1 .

相对我们的 IND-CHA 博弈过程而言, 攻击者的目的是判别他看到的是自己提供给编码器的隐文的加密, 还是简单的信道中的随机采样. 这种选择由 left-or-right Oracle $\mathcal{E}_k^{\mathcal{C}}(\mathcal{LR}(\cdot, \perp, b))$ 决定, 其中, 第二个分量是空串 $\perp$.

给定一个隐写系统 $\mathcal{SS} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$, 上述博弈过程可由以下四步组成:

1. 密钥生成: 通过密钥生成算法 $\mathcal{G}$ 来产生密钥 k .
 2. 学习阶段: Malice 准备一些隐文并发送给 Oracle $\mathcal{O}$, $\mathcal{O}$ 对其进行编码 $\mathcal{E}_k^C(m)$, 并将结果返回给 Malice. 经过许多次的重复之后, Malice 停止并选取一个消息 $m \in \mathcal{P}$;
 3. 挑战阶段: Malice 发送 m 给 $\mathcal{O}$. $\mathcal{O}$ 经过掷币得到 $b \in_U \{0, 1\}$, 然后计算 $c \leftarrow \mathcal{E}_k^C(\mathcal{LR}(m, \perp, b))$ 并发送给 Malice;
 4. 猜测阶段: 一旦接收到 c , Malice 必须输出一比特 b' 作为他对 $\mathcal{O}$ 中掷币 b 的猜测.
- 以此为基础, 我们定义在选择隐文攻击下的隐写系统安全性如下:

定义 7 (隐写系统的 IND-CHA 攻击) 令 $\mathcal{SS} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ 为一个对称的隐写系统, $b \in \{0, 1\}$, $n \in \mathbb{N}$, A_{cha} 是一个可以访问信道采样 Oracle 的攻击者. 我们定义如下实验:

Algorithm $\text{Exp}_{\mathcal{SS}, A_{\text{cha}}}^{\text{ind-cha-b}}(1^n)$
 $k \xleftarrow{R} \mathcal{G}(1^n)$
 $x \leftarrow A_{\text{cha}}^{\mathcal{E}_k^C(\mathcal{LR}(\cdot, \cdot, b))}(1^n)$
 Return x

我们约定询问 $\mathcal{E}_k^C(\mathcal{LR}(\cdot, \cdot, b))$ 的消息长度总是相等的, 其中, $\perp$ 表示消息为空. 根据上述实验, 我们定义攻击者的优势如下:

$$\text{Adv}_{\mathcal{SS}, A_{\text{cha}}}^{\text{ind-cha}}(1^n) = \left| \Pr \left[\text{Exp}_{\mathcal{SS}, A_{\text{cha}}}^{\text{ind-cha-1}}(1^n) = 1 \right] - \Pr \left[\text{Exp}_{\mathcal{SS}, A_{\text{cha}}}^{\text{ind-cha-0}}(1^n) = 1 \right] \right|.$$

进而, 我们定义密码体制下的优势函数: 对任意的整数 t , q_e 和 u_e ,

$$\text{InSec}_{\mathcal{SS}}^{\text{ind-cha}}(t, q_e, u_e) = \max_{A_{\text{cha}}} \{ \text{Adv}_{\mathcal{SS}, A_{\text{cha}}}^{\text{ind-cha}}(1^n) \},$$

其中, 最大值取遍所有的具有时间复杂度 t 的攻击者 A_{cha} , 每个攻击者对 $\mathcal{E}_k(\mathcal{LR}(\cdot, \cdot, b))$ 的查询次数至多为 q_e 次, 且查询的长度之和为至多 u_e 比特.

最后, 我们定义 IND-CHA 攻击下的隐系统安全性如下:

定义 8 (IND-CHA 安全性) 隐写系统 $\mathcal{SS} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ 在自适应选择隐文攻击下被称为 (t, q_e, u_e, ϵ) -不可区分的, 如果在上述隐写系统的 IND-CHA 攻击试验中, $\epsilon = \text{InSec}_{\mathcal{SS}}^{\text{ind-cha}}(t, q_e, u_e)$ 是可忽略, 其中, 攻击者可由具有任意 n 的多项式时间复杂度算法模拟.

4 安全隐写系统的构造

在这一部分, 我们将针对隐写存在性问题和计算复杂性下安全隐系统的构造方法展开研究. 直观地, 隐写对象越是不可预测, 在掩蔽信道中区分出它们就越困难. 基于这种想法, 为了得到通常信道下的安全隐系统构造, 我们重点讨论不可预测性和隐写性质的关系, 然后分析具体构造的安全性要求, 来解释 IND-CHA 隐写系统存在性的先决条件.

4.1 IND-CHA 安全的隐写系统构造

在这一部分, 我们把注意力转向具有计算隐藏性质的安全隐写系统构造上来. 在给出隐写系统具体构造之前, 我们首先给出一个采样算法 (sampler) 构造, 这是我们隐写系统构造中的一个关键部分.

在这个算法中, 仍然采用类似于文献 [5,6] 中的构造, 我们仅仅做了一个小的修改来满足在不完美采样 Oracle 模型下的要求. 该采样算法简要描述如下:

Algorithm $\text{Sample}_f^{\mathcal{C}}(k, b)$
 Require : a key k , a value $b \in \{0, 1\}^e$
 1 : repeat
 2 : $s \leftarrow \mathcal{O}^{\mathcal{C}}$
 3 : until $f_k(s) = b$
 4. Return s

在上述构造中使用了一种带有密钥 k 的映射函数 $f_k(\cdot) : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{R}$, 其中, $\mathcal{R} = \{0, 1\}^e$. 我们隐写方案构造中的编码算法就是基于这种拒绝采样算法 $\text{Sample}_f^{\mathcal{C}}(k, b)$ 的. 该算法能够从掩文分布 $\mathcal{C}$ 中根据 Oracle $\mathcal{O}^{\mathcal{C}}$ 采样出一个掩文符号, 并且一个 e 比特的信息能够对应到该掩文符号中. 为了简化表示, 该算法也被表示做为 $g_k^{\mathcal{C}}(b)$. 假定 $S = \{s_1, s_2, \dots, s_m\}$ 是在一次采样过程中的不同候选采样集合, 这些采样必须是人类视觉或听觉上不已感知差别的采样点. 而且, 采样 Oracle 算法随机选择它们直至 $f_k(s) = b$. 在其后的分析中, 我们的研究目标就是分析该映射函数 $f_k(\cdot)$ 的属性.

具体而言, 这种拒绝采样函数将满足如下特征用以在通常掩蔽信道中诱导出更大的可用性和灵活性: 我们并不假设完美采样 Oracle $\mathcal{O}^{\mathcal{C}}$ 的存在, 即 “一个人能够独立执行抽样, 另一个人也能重复该过程.” 这种独立采样假设由于太过严格, 而很少被现实应用所满足³⁾. 与之相反, 在我们拒绝采样算法中的采样 Oracle $\mathcal{O}^{\mathcal{C}}$ 能在任意信道中被执行, 因此在多采样过程中各采样点之间可以是彼此相关的. 我们不限上述假设的原因在于, 当分析多项式长度的两个采样序列的不可区分性时, 我们后续证明中并不依赖于采样的分布特征, 而是依赖于映射函数 $f_k(\cdot)$ 的随机选择能力.

<p>Algorithm $\mathcal{E}_k^{\mathcal{C}}(m)$</p> <p>1: $z \leftarrow \text{Encoder}(m)$</p> <p>2: Parse z as $\{z_1 \ z_2 \ \dots \ z_l\}$</p> <p>3: for $i = 1$ To l do</p> <p>4: $s_i \leftarrow g_k^{\mathcal{C}}(z_i)$</p> <p>5: end for</p> <p>6: Return $s \leftarrow \{s_1 \ s_2 \ \dots \ s_l\}$</p>	<p>Algorithm $\mathcal{D}_k^{\mathcal{C}}(s)$</p> <p>1: Parse s as $\{s_1 \ s_2 \ \dots \ s_l\}$</p> <p>2: bf for $i = 1$ To l do</p> <p>3: $z_i \leftarrow f_k(s_i)$</p> <p>4: end for</p> <p>5: $m \leftarrow \text{Decoder}(z_1 \ z_2 \ \dots \ z_l)$</p> <p>6: Return m</p>
---	---

最后, 我们描述隐写系统的具体构造. 该系统由编码算法 $\mathcal{E}$ 和译码算法 $\mathcal{D}$ 构成. 在上述算法, 算法 $\mathcal{E}$ 首先使用编码函数 Encoder 编码输入消息 m , 编码结果输出为 z . 然后, 它重复调用采样算法 Sample 来嵌入 z 得到一个伪掩文序列. 译码算法 $\mathcal{D}$ 的过程正好相反: 首先从隐蔽信道中抽取固定大小的掩文符号 s , 并采用映射函数 f 将其映射到符号序列, 然后这些符号序列被串联并送到译码函数 Decoder 获得隐藏的信息, 并把结果返回.

3) 正如文献 [5,6] 所述: “Our definitions (this assumption) do not rule out efficient constructions for channels where more is known about the distribution”, “In practice, this oracle is also the weakest point of all our constructions”, 以及 “A real-world warden would use this to his advantage”.

4.2 不可预测性与隐写术

本节中, 我们转移注意力到上述隐写系统的安全分析. 不难发现, 上述算法 ($\mathcal{E}$ 和 $\mathcal{D}$) 构成了一个有效的隐写系统. 不失一般性, 假设我们的分析是基于二值域 $\{0, 1\}$ 隐藏的, 也就是, Encoder 的输出是一个二进制串, 并且, 函数 $f_k(\cdot)$ 的输出为 $\{0, 1\}$ 中的一个值. 我们首先考虑 Encoder 的特征, 我们发现为了实现安全隐藏, Encoder 的输出应该是不可预测的 (unpredictable). 这种不可预测性可由 Goldreich^[15] 定义如下:

定义 9 (不可预测性^[15]) 集合 $\{X_n\}_{n \in \mathbb{N}}$ 被称为多项式时间 (t_p, ϵ) -不可预测的, 如果对于每个概率多项式时间算法 A 和一个忽略 ϵ ,

$$\Pr[A(1^{|X_n|}, X_n) = \text{Next}_A(X_n)] < \frac{1}{2} + \epsilon,$$

其中, 如果算法 A 的输入为 $(1^{|x|}, x)$ 并只读取 x 中的前 i 比特 ($i < |x|$), $\text{Next}_A(x)$ 返回 x 的第 $i+1$ 比特. 否则 (即, 当 A 读取整个串 x 时), 它返回一个在 $\{0, 1\}$ 上均匀选取的随机比特. t_p 表示算法 A 的时间复杂度.

在上述隐写系统中, 为了实现掩文与伪掩文的不可区分性, 我们要求每个伪掩文块是不可预测的. 同样地, 我们也要求编码块被隐藏到每个采样块中也是不可预测的. 不是一般性, 我们考虑二值隐藏问题, 也就是, 在 z 中的 $z_i \in \{0, 1\}$ 对任意 $i \in \{1, 2, \dots, l\}$. 我们有下面定理:

定理 1 (不可预测性暗示隐写安全) 如果编码算法 Encoder 的输出是 $(t_p, \frac{1}{p(n)})$ -不可预测的 (即它能够通过下一比特测试), 而且影射函数 f 的输出是 $(t_b, \frac{1}{q(n)})$ -无偏分布的, 那么对于足够大的 n , 在隐蔽信道 $\mathcal{C}$ 上的构造 $(\text{Sample}_f^{\mathcal{C}}, \mathcal{E}_k^{\mathcal{C}}, \mathcal{D}_k^{\mathcal{C}})$ 是一个 $(t_p - l(n)t_b, l(n), l(n)|\Sigma|, \frac{l(n)}{p(n)} + \frac{5l(n)}{q(n)})$ -安全隐写系统用于能够抵抗 IND-CHA 攻击, 其中, $l(n)$ 是一个 n 的多项式, 并且 $|\Sigma|$ 表示在 $\mathcal{C}$ 中样本字符表 Σ 的长度.

证明 假设存在一个概率多项式时间算法 $A^{\mathcal{C}}$, 它能以至少 $\frac{1}{p'(n)}$ 概率区分 $\mathcal{E}$ 的输出与隐蔽信道 $\mathcal{C}$ 的正常伪掩文 c . 因此, 对任意一个隐文 m 和足够大的 n , 我们去掉识别误差的绝对值并定义

$$\Pr[A^{\mathcal{C}}(1^n, \mathcal{E}_k^{\mathcal{C}}(m)) = 1] - \Pr[A^{\mathcal{C}}(1^n, \mathcal{E}_k^{\mathcal{C}}(\perp)) = 1] \geq \frac{1}{p'(n)}.$$

对任意多项式长度 $l(\cdot)$, 令隐文 m 在 Encoder 函数编码后的结果可表示为 $z = (z_1, \dots, z_{n'})$, 其中, 每个 z_i 为一个比特, z 的长度是 $n' = l(n)$. 同时, 我们将隐蔽信道采样序列 $c = \mathcal{E}_k^{\mathcal{C}}(\perp)$ 分割为 $\{c_1 \| c_2 \| \dots \| c_{n'}\}$. 对所有 $k \in \mathcal{G}(1^n)$, 我们考虑在符号集合 $\Sigma^{n'}$ 上的分布序列 $\{p_{k,0}, \dots, p_{k,n'}\}$ 如下:

$$\left\{ \begin{array}{ll} p_{k,0} &= \{c_1, c_2, \dots, c_{n'} : c \leftarrow \mathcal{C}\}, \\ p_{k,1} &= \{g_k^{\mathcal{C}}(z_1), c_2, \dots, c_{n'} : c \leftarrow \mathcal{C}, z \leftarrow \mathcal{P}\}, \\ &\dots\dots\dots \\ p_{k,r} &= \left\{ g_k^{\mathcal{C}}(z_1), \dots, g_k^{\mathcal{C}}(z_r), c_{r+1}, \dots, c_{n'} : c \leftarrow \mathcal{C}, z \leftarrow \mathcal{P} \right\}, \\ p_{k,r+1} &= \left\{ g_k^{\mathcal{C}}(z_1), \dots, g_k^{\mathcal{C}}(z_{r+1}), c_{r+2}, \dots, c_{n'} : c \leftarrow \mathcal{C}, z \leftarrow \mathcal{P} \right\}, \\ &\dots\dots\dots \\ p_{k,n'} &= \{g_k^{\mathcal{C}}(z_1), g_k^{\mathcal{C}}(z_2), \dots, g_k^{\mathcal{C}}(z_{n'}) : z \leftarrow \mathcal{P}\}. \end{array} \right.$$

在上述序列中, 开始序列为真实隐蔽信道采样序列 (见 $p_{k,0}$); 此后, 每一步我们从左用伪掩文中的一个伪掩文块替换其中一个采样, 这里, 每个被替换序列被称为 $g_k^{\mathcal{C}}$; 最后, 序列 $p_{k,n'}$ 已经变成一个

完全伪掩文分布序列. 因此, 我们有如下观测结果:

$$\begin{aligned}\Pr[A^C(1^n, \mathcal{E}_k^C(\perp)) = 1] &= \Pr[A^C(1^n, y^0) = 1 : y^0 \xleftarrow{p_{k,0}} \Sigma^{n'}], \\ \Pr[A^C(1^n, \mathcal{E}_k^C(m)) = 1] &= \Pr[A^C(1^n, y^{n'}) = 1 : y^{n'} \xleftarrow{p_{k,n'}} \Sigma^{n'}].\end{aligned}$$

根据我们的假设, 算法 A 有能力区分伪掩文分布 $p_{k,n'}$ 与隐蔽信道分布 $p_{k,0}$. 那么, 对于任意 $r \in \mathbb{N}$, 我们说算法 A 也有能力以如下概率区分两个分布序列 $p_{k,r}$ 和 $p_{k,r+1}$:

$$\begin{aligned}\frac{1}{p'(n)} &\leq (\Pr[A^C(1^n, \mathcal{E}_k^C(m)) = 1] - \Pr[A^C(1^n, \mathcal{E}_k^C(\perp)) = 1]) \\ &= \Pr[A^C(1^n, y^{n'}) = 1 : y^{n'} \xleftarrow{p_{k,n'}} \Sigma^{n'}] - \Pr[A^C(1^n, y^0) = 1 : y^0 \xleftarrow{p_{k,0}} \Sigma^{n'}] \\ &= \sum_{r=0}^{n'-1} \left(\Pr[A^C(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'}] - \Pr[A^C(1^n, y^r) = 1 : y^r \xleftarrow{p_{k,r}} \Sigma^{n'}] \right).\end{aligned}\quad (2)$$

由于我们注意到 $p_{k,r}$ 只在一个位置上与 $p_{k,r+1}$ 不同, 即第 $r+1$ 个采样, 因此, 对某些的 r , 算法 A 也能够用来从采样序列 $\{g_k^C(z_1), g_k^C(z_2), \dots, g_k^C(z_r)\}$ 中成功预测下一采样 $g_k^C(z_{r+1})$. 也就是, 对于任意随机选择的 r , 我们期望第 r 项采样被预测的概率和为 $\geq \frac{1}{n' \cdot p'(n)}$ ⁴⁾.

更为精确地讲, 对于近似无限多的 $k \in \mathcal{G}(1^n)$, 我们将从算法 A 中演变出一个新的概率多项式时间算法 D , 它能以较高概率从 $z = (z_1, \dots, z_{n'}) \in \{0, 1\}^{n'}$ 中预测下一比特. 据此, 我们开始一个更精确的算法 D 描述如下:

1. 在 $\{0, 1, \dots, n'-1\}$ 中均匀选择一个 r .
2. 在分布 $\mathcal{C}$ 中选择一个信道采样序列 $\{c_{r+1}, \dots, c_{n'}\}$, 然后设置

$$y^r = (g_k^C(z_1), \dots, g_k^C(z_r), c_{r+1}, \dots, c_{n'}).$$

3. 如果 $A^C(i, y^r) = 1$, 那么输出 $f_k(c_{r+1})$ 作为一个预测, 否则输出 $1 - f_k(c_{r+1})$ 作为预测, 即

$$D^C(r, z) = \begin{cases} f_k(c_{r+1}), & A^C(1^n, y^r) = 1, \\ 1 - f_k(c_{r+1}), & A^C(1^n, y^r) = 0. \end{cases}$$

不失一般性, 如果我们假设 $f_k(\cdot)$ 是一个 $\frac{1}{q(n)}$ -无偏函数 (函数的输出为一个可忽略偏差的近似为均匀分布), 进而根据引理 1, 我们假设 $\min(\Pr[f_k(c_{r+1}) = z_{r+1}], \Pr[f_k(c_{r+1}) = \bar{z}_{r+1}]) \geq \frac{1}{2} - \frac{1}{q(n)}$, 其中 $\bar{z}_{r+1} = 1 - z_{r+1}$. 因此, 根据算法 A 的定义, 我们得到如下等式:

$$\begin{aligned}s_D(n') &= \Pr[D^C(1^n, z) = \text{Next}_D(z) : z \leftarrow \{0, 1\}^{n'}] \\ &= \frac{1}{n'} \sum_{r=0}^{n'-1} \left\{ \Pr[A^C(1^n, y^r) = 1, f_k(c_{r+1}) = z_{r+1} : y^r \xleftarrow{p_{k,r}} \Sigma^{n'}] \right. \\ &\quad \left. + \Pr[A^C(1^n, y^r) = 0, 1 - f_k(c_{r+1}) = z_{r+1} : y^r \xleftarrow{p_{k,r}} \Sigma^{n'}] \right\} \\ &= \frac{1}{n'} \sum_{r=0}^{n'-1} \left\{ \Pr[A^C(1^n, y^r) = 1 : f_k(c_{r+1}) = z_{r+1}, y^r \xleftarrow{p_{k,r}} \Sigma^{n'}] \cdot \right. \\ &\quad \left. \Pr[f_k(c_{r+1}) = z_{r+1} : c_{r+1} \leftarrow \mathcal{O}^C] \right. \\ &\quad \left. + \Pr[A^C(1^n, y^r) = 0 : f_k(c_{r+1}) = \bar{z}_{r+1}, y^r \xleftarrow{p_{k,r}} \Sigma^{n'}] \cdot \right. \\ &\quad \left. \Pr[f_k(c_{r+1}) = \bar{z}_{r+1} : c_{r+1} \leftarrow \mathcal{O}^C] \right\}\end{aligned}$$

4) 注意, 上述概率是平均情况, 因此我们有如下不等式 $\Pr[A^C(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'}] - \Pr[A^C(1^n, y^r) = 1 : y^r \xleftarrow{p_{k,r}} \Sigma^{n'}] \geq \frac{1}{n' \cdot p'(n)}$, 这是由于一些采样项可能是 $\geq \frac{1}{n' \cdot p'(n)}$, 但是另一些并不满足上述条件.

$$\begin{aligned}
&= \frac{1}{n'} \cdot \sum_{r=0}^{n'-1} \left\{ \begin{array}{l} \Pr \left[A^C(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right] \cdot \\ \Pr[f_k(c_{r+1}) = z_{r+1} : c_{r+1} \leftarrow \mathcal{O}^C] + \\ \left(1 - \Pr \left[A^C(1^n, \overline{y^{r+1}}) = 1 : \overline{y^{r+1}} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right] \right) \cdot \\ \Pr[f_k(c_{r+1}) = \bar{z}_{r+1} : c_{r+1} \leftarrow \mathcal{O}^C] \end{array} \right\} \\
&\geq \frac{1}{2} - \frac{1}{q(n)} + \left(\frac{1}{2} - \frac{1}{q(n)} \right) \cdot \frac{1}{n'} \cdot \sum_{r=0}^{n'-1} \left\{ \begin{array}{l} \Pr \left[A^C(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right] \\ - \Pr \left[A^C(1^n, \overline{y^{r+1}}) = 1 : \overline{y^{r+1}} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right] \end{array} \right\} \\
&\geq \frac{1}{2} - \frac{2}{q(n)} + \frac{1}{2n'} \cdot \sum_{r=0}^{n'-1} \left\{ \begin{array}{l} \Pr \left[A^C(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right] \\ - \Pr \left[A^C(1^n, \overline{y^{r+1}}) = 1 : \overline{y^{r+1}} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right] \end{array} \right\}. \quad (3)
\end{aligned}$$

其中, $\overline{y^{r+1}} = (g_k^C(z_1), \dots, g_k^C(z_r), g_k^C(\bar{z}_{r+1}), c_{r+2}, \dots, c_{n'})$. 注意, $y^r \xleftarrow{p_{k,r}} \Sigma^{n'}$ 包括 $c_{r+1} \leftarrow \mathcal{O}^C$. 考虑到假设 $f_k(\cdot)$ 是一个 ϵ -无偏函数, 我们知道 y^r 是与 y^{r+1} 和 $\overline{y^{r+1}}$ 一致分布的, 其中, y^{r+1} 和 $\overline{y^{r+1}}$ 分别具有偏差概率 $\frac{1}{2} + \frac{1}{q(n)}$ 和 $\frac{1}{2} - \frac{1}{q(n)}$. 因此, 我们可得到下面等式

$$\begin{aligned}
&\Pr \left[A^C(1^n, y^r) = 1 : y^r \xleftarrow{p_{k,r}} \Sigma^{n'} \right] \\
&= \Pr \left[A^C(1^n, y^r) = 1 : f_k(c_{r+1}) = z_{r+1}, y^r \xleftarrow{p_{k,r}} \Sigma^{n'} \right] \Pr[f_k(c_{r+1}) = z_{r+1} : c_{r+1} \leftarrow \mathcal{O}^C] \\
&\quad + \Pr \left[A^C(1^n, \overline{y^r}) = 1 : f_k(c_{r+1}) = \bar{z}_{r+1}, \overline{y^r} \xleftarrow{p_{k,r}} \Sigma^{n'} \right] \Pr[f_k(c_{r+1}) = \bar{z}_{r+1} : c_{r+1} \leftarrow \mathcal{O}^C] \\
&\geq \left(\frac{1}{2} - \frac{1}{q(n)} \right) \left(\Pr \left[A^C(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right] \right. \\
&\quad \left. + \Pr \left[A^C(1^n, \overline{y^{r+1}}) = 1 : \overline{y^{r+1}} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right] \right), \quad (4)
\end{aligned}$$

这个等式暗示

$$\Pr \left[A^C(1^n, \overline{y^{r+1}}) = 1 : \overline{y^{r+1}} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right] \leq \left(\frac{\frac{1}{(\frac{1}{2} - \frac{1}{q(n)})} \cdot \Pr \left[A^C(1^n, y^r) = 1 : y^r \xleftarrow{p_{k,r}} \Sigma^{n'} \right] -}{\Pr \left[A^C(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right]} \right).$$

因此, 根据 (2) 式, 我们有如下关系:

$$\begin{aligned}
s_D(n') &= \frac{1}{2} - \frac{2}{q(n)} + \frac{1}{2n'} \sum_{r=0}^{n'-1} \left\{ \begin{array}{l} \Pr \left[A^C(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right] \\ - \Pr \left[A^C(1^n, \overline{y^{r+1}}) = 1 : \overline{y^{r+1}} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right] \end{array} \right\} \\
&\geq \frac{1}{2} - \frac{2}{q(n)} + \frac{1}{2n'} \sum_{r=0}^{n'-1} \left\{ \begin{array}{l} \Pr \left[A^C(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right] - \\ \left(\frac{\frac{1}{(\frac{1}{2} - \frac{1}{q(n)})} \cdot \Pr \left[A^C(1^n, y^r) = 1 : y^r \xleftarrow{p_{k,r}} \Sigma^{n'} \right] -}{\Pr \left[A^C(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right]} \right) \end{array} \right\} \\
&= \frac{1}{2} - \frac{2}{q(n)} + \frac{1}{2n'} \sum_{r=0}^{n'-1} \left\{ \begin{array}{l} \left(2 \Pr \left[A^C(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'} \right] - \right. \\ \left. 2 \Pr \left[A^C(1^n, y^r) = 1 : y^r \xleftarrow{p_{k,r}} \Sigma^{n'} \right] \right) - \\ \frac{4}{q(n)-2} \Pr \left[A^C(1^n, y^r) = 1 : y^r \xleftarrow{p_{k,r}} \Sigma^{n'} \right] \end{array} \right\}
\end{aligned}$$

$$\begin{aligned}
&\geq \frac{1}{2} - \frac{2}{q(n)} + \frac{1}{n'p'(n)} - \frac{2}{q(n)-2} \\
&\geq \frac{1}{2} - \frac{5}{q(n)} + \frac{1}{n'p'(n)},
\end{aligned}$$

其中, $q(n) \geq 6$. 这意味着, 对于长度 $n' = l(n)$, 在上述试验中算法 D 的猜测优势为至少 $\frac{1}{n'p'(n)} - \frac{5}{q(n)}$. 这是与我们的假设 (隐藏序列 z 是多项式时间不可预测的) 相矛盾的. 这里, 我们所提隐写系统构造的时间复杂性 t 至多为 $t_p - n't_b$, 因为 $t_p \geq t + n't_b$. 同时, 由于敌手可至多 $l(n)$ 次查询, 每次至多查询隐文中的 $l(n)|\Sigma|$ 比特, 因此, 敌手攻破我们所提隐写系统构造的优势为 $\frac{1}{p'(n)}$ 也是至少为 $\frac{l(n)}{p(n)} + \frac{5l(n)}{q(n)}$. 根据 $\frac{1}{p(n)} \geq \frac{1}{n'p'(n)} - \frac{5}{q(n)}$. 综上所述, 定理成立.

上述证明使用了所谓的“混杂”证明方法. 更重要的是, 这个证明提供了最坏情况下的预测性估计. 这意味着我们的安全隐写术构造对于隐文的所有比特都是不可预测的. 反之, 如果敌手能够成功预测伪掩文序列中的某些位, 这个隐写系统也将是不安全的. 事实上, 现实应用可能通过对这些比特的信息预测出隐文存在, 从而实现有效 (多项式时间的) 隐写分析^[16].

4.3 安全隐写系统存在的前提条件

为证明常规掩蔽信道中的计算隐藏性, 我们采用非完美采样 Oracle 实现了一个新的简单采样器构造: $(\text{Sample}_f^C, \mathcal{E}_k^C, \mathcal{D}_k^C)$. 在这个构造中, 样本之间不要求相互独立. 而且, 我们对上述隐写方案的安全进行了严格证明, 前述定理的结论对于隐写术分析是至关重要的, 其证明过程对于计算安全的隐写系统构造也具有特殊的意义.

在我们提出的隐写方案构造中存在两个核心部分: 影射函数 f 及加密函数 Encoder. 根据证明过程不难总结如下条件:

条件 1 影射函数 $f_k(\cdot)$ 对于密钥 k 是无偏差函数.

条件 2 加密函数 $\text{Encoder}(\cdot)$ 可生成一个不可预测序列.

条件 1 是由方程 (3) 和 (4) 的假设派生得到: 函数 $f_k(\cdot)$ 是一个具有多项式可忽略偏差 $\frac{1}{q(n)}$ 的 $\frac{1}{q(n)}$ -无偏差函数. 即, 关于分布 $\mathcal{C}$, 对任意 $b \in \{0, 1\}$, 有 $|\Pr_{c \leftarrow \mathcal{C}}[f_k(c) = b] - \frac{1}{2}| \leq \frac{1}{q(n)}$. 容易看出: $\frac{1}{2} - \frac{1}{q(n)} \leq \min\{\Pr_{c \leftarrow \mathcal{C}}[f_k(c) = b], \Pr_{c \leftarrow \mathcal{C}}[f_k(c) = \bar{b}]\}$ 以及 $\max\{\Pr_{c \leftarrow \mathcal{C}}[f_k(c) = b], \Pr_{c \leftarrow \mathcal{C}}[f_k(c) = \bar{b}]\} \leq \frac{1}{2} + \frac{1}{q(n)}$ 对任意分布 $\mathcal{C}$. 这些可由下述的引理得到:

引理 1 给定一个 ϵ -无偏差函数 $f: \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{R}$, 即, $|\Pr_{x \leftarrow \mathcal{C}}[f_k(x) = r] - \frac{1}{|\mathcal{R}|}| \leq \epsilon$. 设 S 为取值在 $\mathcal{R}$ 上的任意分布随机变量. 如果 S 和 f 相互独立, 则有 $\frac{1}{|\mathcal{R}|} - \epsilon \leq \Pr_{x \leftarrow \mathcal{C}}[f_k(x) = S] \leq \frac{1}{|\mathcal{R}|} + \epsilon$.

证明 由 ϵ -无偏差函数的定义, 我们有 $\frac{1}{|\mathcal{R}|} - \epsilon \leq \Pr_{x \leftarrow \mathcal{C}}[f_k(x) = r] \leq \frac{1}{|\mathcal{R}|} + \epsilon$. 由于 $f_k(x)$ 与 S 相互独立, 我们得到

$$\begin{aligned}
\Pr_{x \leftarrow \mathcal{C}}[f_k(x) = S] &= \sum_{r \leftarrow \mathcal{R}} \Pr_{x \leftarrow \mathcal{C}}[S = r | f_k(x) = r] \cdot \Pr_{x \leftarrow \mathcal{C}}[f_k(x) = r] \\
&\leq \left(\frac{1}{|\mathcal{R}|} + \epsilon \right) \sum_{r \leftarrow \mathcal{R}} \Pr[S = r] = \frac{1}{|\mathcal{R}|} + \epsilon.
\end{aligned}$$

同样地, 我们也可得到 $\Pr_{x \leftarrow \mathcal{R}}[f_k(x) = S] \geq \frac{1}{|\mathcal{R}|} - \epsilon$. 因此, 引理成立.

显然, 上述引理可得到影射函数 f 与掩文分布 $\mathcal{C}$ 相互独立⁵⁾. 在定理 1 中, 算法 D 预测的成功概率至少为 $\frac{1}{2} - \frac{5}{q(n)} + \frac{1}{n'p'(n)}$. 可以看出, 影射函数的偏差 $\frac{1}{q(n)}$ 降低了预测的成功概率. 进一步, 作为

5) 原因是对于无偏差函数 $f_k(x)$, 我们有 $\Pr[f_k(x) = r] = \sum_{c \in \mathcal{C}} \Pr[f_k(c) = r] \cdot \Pr_{\mathcal{C}}[c] = \frac{1}{|\mathcal{R}|} \sum_{c \in \mathcal{C}} \Pr_{\mathcal{C}}[c] = \frac{1}{|\mathcal{R}|}$.

该定理的一个特例, 当 $f_k(x)$ 是无偏差函数时, 则预测的成功概率至少为 $\frac{1}{2} + \frac{1}{n'p'(n)}$. 注意, 我们强调该函数应当使用密钥 k 来实现采样过程的随机性. 根据密码学理论, 我们可以使用预测困难的单向函数或者平衡布尔函数来构造一个无偏差函数.

条件 2 是如下密码学定理的直接推论. Yao 已经证明, 一个集合是伪随机的, 当且仅当它是多项式时间内不可预测的:

定理 2 (Yao 定理^[14,15]) 设 $I = (I_n)_{n \in \mathbb{N}}$ 是具有安全参数 n 的密钥集合, $G = (G_k : X_k \rightarrow \{0, 1\}^{l(n)})_{k \in I}$ 是具有多项式长度函数 l 的伪随机比特生成器, K 为密钥生成器. 则 G 是计算上完美伪随机的当且仅当 G 通过所有的下一比特测试.

Yao 定理说明, 如果存在一个伪随机比特生成器, 我们所提方案是有能力实现条件 2 中的计算安全隐写系统的. 此外, 根据单向函数和伪随机比特生成器的关系, 比计算安全隐写系统更弱的假设就是强单向函数的存在性, 由此就可导出伪随机比特生成器的存在性^[15].

将上述两个条件结合, 一个 IND-CHA 安全的 (基于块的) 隐写系统需满足如下性质:

推论 1 如果如下两条成立: 1) 存在具有可忽略错误的伪随机函数, 该函数可用于构造隐文消息的编码器; 2) 存在具有可忽略偏差的无偏差函数, 该函数用于构造拒绝采样函数, 那么, 存在一个抗 IND-CHA 攻击且计算安全的隐写系统.

注意到, 由定理 1 可知 IND-CHA 博弈过程中敌手的优势至多为 $\frac{l(n)}{p(n)} + \frac{5l(n)}{q(n)}$, 其中, 隐文长度 $l(n)$ 必须远小于多项式 $p(n)$ 和 $q(n)$. 也就是说, 敌手的优势与隐文长度 $l(n)$ 成正比, 与多项式 $p(n)$ 和 $q(n)$ 成反比. $l(n)$ 越小或者 $p(n)$ 、 $q(n)$ 越大, 那么这个隐写系统更安全.

5 结论

本文中, 我们不使用特定的信道分布假设, 构造了一个更一般性的安全隐写系统, 并证明了我们的构造是计算安全的, 对于自适应的选择隐文攻击具有不可区分性. 上述分析表明, 基于伪随机函数和无偏差采样函数的存在性, 计算安全隐写系统的构造是可行的. 类似地, 陷门单向函数和无偏差采样器也是构造安全私钥及公钥的隐写术方案的基础. 更重要的是, 这些结果对于隐写系统的构造和分析具有使用价值. 作为未来工作中的一部分, 我们将构造一个基于概念可证明的实验案例, 并且对其进行广泛地系统评估, 从而对上述理论进行试验证明.

致谢 非常感谢亚利桑那州立大学的 Stephen S. Yau 教授给出了非常有价值的建议.

参考文献

- 1 Feamster N, Balazinska M, Wang W, et al. Thwarting Web censorship with untrusted messenger discovery. In: Dingledine R, ed. Privacy Enhancing Technologies. LNCS, 2760. Berlin: Springer, 2003. 125–140
- 2 Serjantov A, Danezis G. Towards an information theoretic metric for anonymity. In: Dingledine R, Syverson P F, eds. Privacy Enhancing Technologies. LNCS, 2482. Berlin: Springer, 2002. 41–53
- 3 Boneh D, Shaw J. Collusion-secure fingerprinting for digital data. IEEE Trans Inf Theory, 1998, 44: 1897–1905
- 4 Cachin C. An information-theoretic model for steganography. In: Aucsmith D, ed. Proceedings of the 2nd Workshop on Information Hiding (IH 1998). LNCS, 1525. Portland: Springer, 1998. 306–318
- 5 Hopper N J, Langford J, Ahn L V. Provably secure steganography. In: Yung M, ed. Advances in Cryptology—CRYPTO 2002. LNCS, 2442. Santa Barbara: Springer, 2002. 77–92

- 6 Hopper N J, Ahn L V, Langford J. Provably secure steganography. *IEEE Trans Comput*, 2009, 58: 662–676
- 7 Bodo Möller. A public-key encryption scheme with pseudo-random ciphertexts. In: Samarati P, Ryan P Y A, Gollmann D, et al, eds. *Proceedings of the 9th European Symposium on Research in Computer Security, ESORICS 2004*. LNCS, 3193. Sophia Antipolis: Springer, 2004. 335–351
- 8 Dedic N, Itkis G, Reyzin L, et al. Upper and lower bounds on black-box steganography. In: Backes M, Cachin C, eds. *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005*. LNCS, 3378. Cambridge: Springer, 2005. 227–244
- 9 Ahn L V, Hopper N J. Public-key steganography. In: Cachin C, Camenisch J, eds. *Advances in Cryptology—EUROCRYPT 2004*. LNCS, 3027. Interlaken: Springer, 2004. 323–341
- 10 Backes M, Cachin C. Public-key steganography with active attacks. In: Kilian J, ed. *Theory of Cryptography, Second Theory of Cryptography Conference (TCC 2005)*. LNCS, 3378. Cambridge: Springer, 2005. 210–226
- 11 Hopper N J. On steganographic chosen coverttext security. In: Caires L, Italiano G F, Monteiro L, et al, eds. *Proceedings of the 32nd International Colloquium on Automata Languages and Programming (ICALP 2005)*. LNCS, 3580. Lisbon: Springer, 2005. 311–323
- 12 Lysyanskaya A, Meyerovich M. Provably secure steganography with imperfect sampling. In: Yung M, Dodis Y, Kiayias A, et al, eds. *Proceedings of the 9th International Conference on Theory and Practice of Public-Key Cryptography (PKC 2006)*. LNCS, 3958. New York: Springer, 2006. 123–139
- 13 Goldwasser S, Bellare M. *Lecture Notes on Cryptography*. 2008. [Http://www-cse.ucsd.edu/~mihir/papers/gb.html](http://www-cse.ucsd.edu/~mihir/papers/gb.html)
- 14 Yao A C. Theory and application of trapdoor functions. In: *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science (FOCS 1982)*. Chicago: IEEE Computer Society, 1982. 80–91
- 15 Goldreich O. *Foundations of Cryptography Volume I, Basic Tools*. London: Cambridge University Press, 2001
- 16 Luo X Y, Liu F L, Yang C F, et al. Image universal steganalysis based on best wavelet packet decomposition. *Sci China Inf Sci*, 2010, 53: 634–647

Efficient construction of provably secure steganography under ordinary covert channels

ZHU Yan^{1,2,*}, YU MengYang³, HU HongXin⁴, AHN Gail-Joon⁴ & ZHAO HongJia^{1,2}

1 *School of Computer & Communication Engineering, University of Science & Technology, Beijing 100083, China;*

2 *Institute of Computer Science and Technology, Peking University, Beijing 100871, China;*

3 *School of Mathematical Sciences, Peking University, Beijing 100871, China;*

4 *School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tempe, AZ 85287, USA*

*E-mail: zhuyan@ustb.edu.cn

Abstract Steganography is the science of hiding information within seemingly harmless messages or innocent media. This paper addresses the problems of efficient construction of secure steganography in ordinary covert channels. Without relying on any sampling assumption, we provide a general construction of secure steganography under computational indistinguishability. Our results show that unpredictability of mapping function in coverttext sampler is indispensable for secure stegosystem on indistinguishability against adaptive chosen hiddentext attacks. We completely prove that computationally secure steganography can be constructed on pseudorandom function and unbiased sampling function under ordinary covert channels, that is, its security is inversely proportional to the sum of errors of these two functions, as well as the length of hiddentexts. More importantly, our research is not dependent upon pseudorandom ciphertext assumption of cryptosystem or perfect sampling assumption. Hence, our results are practically useful for construction and analysis of secure stegosystems.

Keywords cryptography, steganography, indistinguishability, sampler, unpredictability, adversary models

ZHU Yan was born in 1974. He received the Ph.D. degree in computer science from Harbin Engineering University, Harbin, in 2005. He has been currently a Professor in the School of Computer and Communication Engineering at the University of Science and Technology Beijing since 2013. From 2007 to 2013, he was an Associate Professor of Computer Science at the Institute of Computer Science and Technology, Peking University. From 2008 to 2009, he was a visiting associate professor in the Department of Computer Science and Engineering, Arizona State University, Tempe. He was a visiting research investigator of the Department of Computer and Information Science, University of Michigan-Dearborn in 2012. His research interests include cryptography, network security, and steganography. Dr. Zhu is a member of CCF, IEEE and ACM.

HU HongXin received the Ph.D. degree in computer science from Arizona State University, Tempe, USA, in 2012. Currently, he is an Assistant Professor in the Department of Computer and Information Sciences at Delaware State University. His research interests include access control models and mechanisms, security and privacy in social networks, security in cloud and mobile computing, network and system security, and secure software engineering. Dr. Hu is a member of IEEE.

YU MengYang was born in 1991. He received the Ph.D. degree in Mathematics from the Peking University, Beijing, in 2010. Currently, he is a master student at Peking University. His research interests include cryptography and network security.

Ahn Gail-Joon received the Ph.D. degree in information technology from George Mason University, Fairfax, VA, in 2000. Currently, he is an Associate Professor in the Ira A. Fulton Schools of Engineering at Arizona State University. His research interests include vulnerability and risk management, access control, and security architecture for distributed systems. Dr. Ahn is a recipient of the U.S. Department of Energy Career Award and the Educator of the Year Award from the Federal Information Systems Security Educators Association. He is a senior member of IEEE and ACM.