基于平滑熵的防主动攻击的无条件安全秘密钥的提取

杨 波, 张 彤, 王育民
(西安电子科技大学 ISN 国家重点实验室 106 信箱, 陕西西安 710071)

摘 要: 本文研究通信双方基于平滑熵在不安全且非认证的公共信道上实现防主动攻击的无条件安全秘密钥的提取. 首先讨论了在不安全且非认证的公共信道上根据部分保密的密钥实现认证的方法, 然后根据以上方法以抗击敌手在通信双方进行无条件安全秘密钥提取时的主动攻击, 得出了通信双方以一定概率所协商的秘密钥长度.

关键词: 平滑熵; 密钥协商; 认证
中图分类号: TN911.2 文献标识码: A 文章编号: 0372-2112 (2001) 10-1349-03

Distillation of Unconditionally-Secure Secret-Key Against Active Adversaries Based on Smooth Entropy

YANG Bo, ZHANG Tong, WANG Yu-min
(*National Key Laboratory on ISN of Xidian University, Xi'an, Shanxi 710071, China*)

Abstract: This paper investigates the distillation of unconditionally-secure secret-key against active adversaries over an insecure and not even authentic channel based on smooth entropy. First we discuss unconditionally secure authentication where the common key is only partially secret, then the authentication method is used to secret-key agreement against active opponents and obtains the size of the secret-key with some probability.

Key words: smooth entropy; secret-key agreement; authentication

1 引言

无条件安全秘密钥协商协议[1~5], 仅借助于有噪信道使通信双方 Alice、Bob 及敌手 Eve, 分别得到概率分布服从 P_{XYZ} 的三个随机变量 X, Y, Z 做为初始的相关信息, Alice 和 Bob 在公共信道上经过优先提取、信息协调可得一个部分保密的随机变量 S, 再经保密增强阶段, 就可以提取出通信双方间的秘密钥 S', 并使得敌手对 S' 几乎一无所知. 但以前的研究大都假定了公共信道是一个认证信道, 即敌手只能窃听信道上的通信内容而不能篡改. 防主动攻击的无条件安全的秘密钥协商, 必需防止敌手篡改通信双方在公共信道上的协商内容或冒充一方来执行密钥协商协议, 解决这一问题的最好方法就是认证. 传统认证技术的前提条件是通信双方间共享一个完全保密的认证密钥, 而无条件安全密钥协商的目的就是要产生共享密钥, 这是相互矛盾的, 如何解决这一矛盾是无条件安全密钥协商成功的关键. U. Maurer 在文[7]中利用最小熵研究了非认证信道上的保密增强, S. Wolf 在文[8]中利用二阶 Rényi 熵研究了非认证信道上的保密增强, 笔者在文[1]中利用平滑熵研究了认证信道上无条件安全秘密钥的提取, 本文在此基础上研究非认证信道上的无条件安全秘密钥的提取.

2 一些概念及结果

文中随机变量用大写字母表示, 取值集合用相应的手写体字母表示.

定义 **1**[6] 函数族 $\mathcal{F}: \mathcal{A}\to\mathcal{B}$ 称为 Universal$_2$ (简称 Universal) 的条件是对 $\forall x_1, x_2\in\mathcal{A}$ 且 $x_1\neq x_2$, $f(x_1)=f(x_2)$ 成立的概率最多为 $1/|\mathcal{B}|$, 其中 f 从 $\mathcal{F}$ 中均匀选择.

下面就是一个 $\{0,1\}^n\to\{0,1\}^r$ 的包括有 2^n 个不同函数的 Universal$_2$ 函数族; 设 $b\in GF(2^n)$, $x\in\mathcal{A}=\{0,1\}^n$ 也是 $GF(2^n)$ 中的一个元素. 考虑函数 $f_b:=(b\cdot x)_r$, 其中 $\cdot$ 代表域乘, 故 $b\cdot x\in GF(2^n)$, f_b 取的是 $b\cdot x$ 的前 r 个比特. 那么函数集 f_b ($b\in GF(2^n)$) 对所有的 $1\le r\le n$ 都是一个 Universal$_2$ 函数族.

定义 **2**[6] 如果下面的两个条件满足的话, 函数族 $\mathcal{H}: \mathcal{A}\to\mathcal{B}$ 就是一个 ε 几乎强 Universal$_2$ (或简记为 ε-ASU_2): (1) 对每一个 $a\in\mathcal{A}$, $b\in\mathcal{B}$ 满足 $h(a)=b$ 的函数 h 的个数为 $|\mathcal{H}|/|\mathcal{B}|$. (2) 对每个 $a_1, a_2\in\mathcal{A}$, $a_1\neq a_2$, $b_1, b_2\in\mathcal{B}$, $b_1\neq b_2$, 满足 $h(a_1)=b_1$ 且 $h(a_2)=b_2$ 的 hash 函数个数最多为 $\varepsilon\cdot|\mathcal{H}|/|\mathcal{B}|$.

定义 **3**[6] 一个 $(1/|\mathcal{B}|)$-ASU_2 函数族称为强-Universal$_2$ (或简称为 SU_2).

例如 $\mathcal{H}=\{h_{ab}: (a,b)\in(GF(2^n))^2\}$. 其中 $h_{ab}(x):=ax+b$, 则 $\mathcal{H}$ 是一个 $\{0,1\}^n\to\{0,1\}^n$ 的具有 2^{2n} 个元素的 SU_2 函数族. 有关 α 阶 Rényi 熵、相对熵及平滑熵的概念在文[1]中已做介绍, 本文不再赘述.

收稿日期: 2000-05-15; 修回日期: 2000-11-05
基金项目: 国家自然科学基金(No. 69972034); 国防科技重点实验室基金(No. 99JS06.3.1.DZ0112)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

引理 1[7] 设 $1<\alpha<2$, $r, t>0$, m 是满足 $m-\log(m+1)>\log|\mathcal{A}|+t$ 的整数, s 是平滑熵的安全参数, 则随机变量 X 在误差范围 $2^{-s}/\ln 2$(以相对熵度量)内的平滑滴 $\Psi(X)$ 以概率 $1-2^{-r}-2^{-t}$, 有以下关系: $\Psi(X)\geq H_\alpha(X)-\log(m+1)-r/(\alpha-1)-t-2$.

引理 2[1] 设 α, r, t, m, s 与引理 1 相同, 设 Eve 所知道的关于 W 的信息由 $V=v$ 表示; Alice 和 Bob 选择 $K=G(W)$ 作为其秘密钥, 其中 G 是从 $\mathcal{H}\{0,1\}^l$ 的 Universal hash 函数族中随机选取的一个函数, 则 K 的长度 l 以概率 $1-2^{-r}-2^{-t}$ 有以下关系: $l=H_\alpha(W|V=v)-\log(m+1)-r/(\alpha-1)-t-2-s$ 且 *Eve* 关于 K 的信息量 $\leq 2^{-s}/\ln 2$.

3 基于部分保密密钥的无条件安全的认证

本节考虑在敌手掌握密钥的部分信息情况下的无条件安全的认证.

引理 3[7] 设 $1<\alpha<2$, $r, t>0$, 对任意随机变量 X 和 Y, Y 取值 y 使得

$$H_\alpha(X|Y=y)\geq H_\alpha(XY)-\log|\mathcal{A}|-r/(\alpha-1)-t$$

成立的概率至少为 $1-2^{-r}-2^{-t}$. 设 S 是 Alice 和 Bob 共享的部分保密的密钥, 而 Eve 有 S 的部分信息(用 α 阶 Rényi 熵描述, $1<\alpha<2$), 设 X 是需要被认证的消息, Y 是认证符. 我们首先考虑在已知 X、Y 的情况下, S 的 α 阶 Rényi 熵减少的上界.

引理 4 设 $1<\alpha<2$, $r, t>0$, S, X 和 Y 分别是取值于集合 $\mathcal{S}$、$\mathcal{X}$ 和 $\mathcal{Y}$ 的任意随机变量, 并设 S 和 X 是相互独立的, 那么 $H_\alpha(S|X=x, Y=y)\geq H_\alpha(S)-\log|\mathcal{A}|-r/(\alpha-1)-t$ 成立的概率至少为 $1-2^{-r}-2^{-t}$.

证明 由引理 3 知, $H_\alpha(S|X=x, Y=y)\geq H_\alpha(SY|X=x)-\log|\mathcal{A}|-(r/(\alpha-1))-t$ 至少以概率 $1-2^{-r}-2^{-t}$ 成立.

因为当 X 给定时, Y 是 S 的确定性函数, 又 $\mathcal{S}$ 和 $\mathcal{X}$ 独立. 所以

$$H_\alpha(SY|X=x)=H_\alpha(S|X=x)=H_\alpha(S)$$

为方便起见, 以下令 $r=(\alpha-1)r_1 n$, $t=t_1 n$, 其中 $0<r_1<1$, $0<t_1<1$, 那么引理 4 变为 $H_\alpha(S|X=x, Y=y)\geq H_\alpha(S)-\log|\mathcal{A}|-(r_1+t_1)n$ 成立的概率至少为 $1-2^{-(\alpha-1)r_1 n}-2^{-t_1 n}$.

引理 5 设 X 是取值于集合 $\mathcal{X}$ 的随机变量, $p_{\max}=\max_{x\in\mathcal{X}}P_X(x)$, 则 $p_{\max}\leq 2^{-H_\alpha(X)+r_1 n}$ 至少以概率 $1-2^{-(\alpha-1)r_1 n}$ 成立.

证明 由 $H_\alpha(X)=1/(1-\alpha)\log\sum_{x\in\mathcal{X}}P_X(x)^\alpha$, 得 $(1-\alpha)H_\alpha(X)=\log\sum_{x\in\mathcal{X}}P_X(x)P_X(x)^{\alpha-1}$

即 $$E_X[P_X(x)^{(\alpha-1)}]=2^{(1-\alpha)H_\alpha(X)},$$

$$E_X[2^{(\alpha-1)\log P_X(x)-(1-\alpha)H_\alpha(X)}]=1,$$

取 r 为大于 0 的任一常数,

则 $E_X[2^{(\alpha-1)\log P_X(x)-(1-\alpha)H_\alpha(X)-r}]=2^{-r}$, 由不等式 $P[X\geq r]\leq E[e^{(X-r)t}]$, 其中 $t\in\mathcal{R}$, $r\in\mathcal{R}$

取 $t=\ln 2$, 则 $P[X\geq r]\leq E[2^{(X-r)}]$, 得 $P_X[(\alpha-1)\log P_X(x)-(1-\alpha)H_\alpha(X)\geq r]\leq 2^{-r}$. 即 $(\alpha-1)\log P_X(x)-(1-\alpha)H_\alpha(X)\leq r$ 至少以概率 $1-2^{-r}$ 成立,

两边同除以 $(\alpha-1)$ 得 $\log P_X(x)\leq -H_\alpha(X)+(r/(\alpha-1))$

所以 $P_X(x)\leq 2^{-H_\alpha(X)+r/(\alpha-1)}$ 至少以概率 $1-2^{-r}$ 成立,

因为 $P_X(x)$ 是 X 取任一 x 的概率, 所以 $p_{\max}\leq 2^{-H_\alpha(X)+r/(\alpha-1)}$, 取 $r=(\alpha-1)r_1 n$ 即得引理的结论.

定理 1 设 S 是 Alice 和 Bob 共享的随机变量, 为长 n(n 为偶数)的二元比特串, 作为认证方案的密钥, 设 $U=u$ 是 Eve 掌握的关于 S 的信息, 满足:

$$H_\alpha(S|U=u)\geq\left((1/2)+\tau+r_1\right)n,\text{ 其中 }\tau\geq r_1+t_1$$

又设 D 表示 *Eve* 成功实施假冒攻击或替换攻击这一事件, 则

$$P(D|U=u)\leq 2^{-(\tau-r_1-t_1)n}+2^{-(\alpha-1)r_1 n+1}+2^{-t_1 n}=2^{-\Omega(n)}$$

证明 首先考虑 Eve 假冒攻击成功的概率 p_{imp} 的上界. 对每一个可能的消息 $x\in GF(2^{n/2})$ 及每一个认证符 $y\in GF(2^{n/2})$, 存在 $2^{n/2}$ 个密钥使得认证正确. 所以在给定 $U=u$ 的条件下, 该密钥集的概率的上界可根据引理 5 由下式确定:

$$2^{n/2}[1-2^{-(\alpha-1)r_1 n}]p_{\max}\leq 2^{n/2}[1-2^{-(\alpha-1)r_1 n}]2^{-H_\alpha(S|U=u)+r_1 n}\leq 2^{-\tau n}$$

所以 Eve 猜测一个密钥成功的概率上界为 $2^{-\tau n}$, 因此 $p_{imp}\leq 2^{-\tau n}$. 在替换攻击中, Eve 看到一个消息认证对 $(X, Y)\in GF(2^{n/2})^2$, 其中在 $U=u$ 的条件下, S 和 X 是相互独立的. 由引理 4, $H_\alpha(S|X=x, Y=y, U=u)\geq H_\alpha(S|U=u)-\log|\mathcal{A}|-(r_1+t_1)n\geq\left(\frac{1}{2}+\tau+r_1\right)n-\frac{n}{2}-(r_1+t_1)n=(\tau-t_1)n$ 成立的概率至少为 $1-2^{-(\alpha-1)r_1 n}-2^{-t_1 n}$.

由引理 5, $p_{\max}(S|X=x, Y=y, U=u)\leq 2^{-H_\alpha(S|X=x, Y=y, U=u)+r_1 n}\leq 2^{-(\tau-t_1-r_1)n}$ 成立的概率至少为

$$[1-2^{-(\alpha-1)r_1 n}][1-2^{-(\alpha-1)r_1 n}-2^{-t_1 n}]\geq 1-2^{-(\alpha-1)r_1 n+1}-2^{-t_1 n}.$$

同时考虑 $p_{\max}(S|X=x, Y=y, U=u)\leq 2^{-(\tau-t_1-r_1)n}$ 不成立的情况, 可得替换攻击成功的概率的上界:

$$p_{sub}\leq 2^{-(\alpha-1)r_1 n+1}+2^{-t_1 n}+[1-2^{-(\alpha-1)r_1 n}-2^{-t_1 n}]2^{-(\tau-t_1-r_1)n}\leq 2^{-(\alpha-1)r_1 n+1}+2^{-t_1 n}+2^{-(\tau-t_1-r_1)n}$$

所以 $P(D|U=u)=\max(p_{imp}, p_{sub})\leq 2^{-(\tau-r_1-t_1)n}+2^{-(\alpha-1)r_1 n+1}+2^{-t_1 n}=2^{-\Omega(n)}$

4 基于平滑熵所能提取出的无条件安全秘密钥的长度

设 Alice 和 Bob 共享一个长度为 n 的部分保密的串 S, 他们在一个不安全且非认证的公开信道上进行协商以提取一个高度保密的串 S'. 基本思想如下: 将 S 分为 2/3 和 1/3 两部分, 用前 2/3 部分对他们选取的 Universal hash 函数进行认证, 再用后 1/3 部分作为 hash 函数的输入.

引理 6 说明了 Eve 关于 S 的子串的信息量的下界,

引理 6 设 $S=(s_1, s_2, \cdots, s_n)$ 是由 n 个二元随机变量构成的一个随机变量, 对任意 k 元组 $\underline{i}=(i_1, i_2, \cdots, i_k)$(其中 $1\leq i_1<i_2<\cdots<i_k\leq n$), 设 $S_{\underline{i}}$ 表示 S 的子串 $(S_{i_1}, S_{i_2}, \cdots, S_{i_k})$, 那么

$$H_\alpha(S_{\underline{i}})\geq H_\alpha(S)-(n-k)$$

证明 对固定的串 $s_{\underline{i}}=(s_{i_1}, s_{i_2}, \cdots, s_{i_k})$, S 可有 2^{n-k} 个值 $(s_1, s_2, \cdots, s_n)$ 与其对应, 设 $p_1, p_2, \cdots, p_{2^{n-k}}$ 是这些串的概率,

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

令 $p_0 = P_{S_{\underline{i}}}(s_{\underline{i}}) = \sum_{i=1}^{2^{n-k}} p_i$ 则 $\sum_{i=1}^{2^{n-k}} p_i^{\alpha} = p_0^{\alpha-1} \sum_{i=1}^{2^{n-k}} \left(\frac{p_i}{p_0}\right)^{\alpha-1} p_i \geq p_0^{\alpha-1}\left(\frac{1}{2^{n-k}}\right)^{\alpha-1} 2^{n-k} \sum_{i=1}^{2^{n-k}} p_i = \frac{p_0^{\alpha}}{2^{(n-k)(\alpha-1)}}$, $p_0^{\alpha} \leq 2^{(n-k)(\alpha-1)} \sum_{i=1}^{2^{n-k}} p_i^{\alpha}$.

所以 $\sum_{s_{\underline{i}} \in \{0,1\}^k} P_{S_{\underline{i}}}(s_{\underline{i}})^{\alpha} = \sum_{s_{\underline{i}} \in \{0,1\}^k} p_0^{\alpha} \leq 2^{(n-k)(\alpha-1)} \sum_{s_{\underline{i}} \in \{0,1\}^k} \sum_{i=1}^{2^{n-k}} p_i^{\alpha}$

$= 2^{(n-k)(\alpha-1)} 2^k \sum_{i=1}^{2^{n-k}} p_i^{\alpha} = 2^{(n-k)(\alpha-1)} \sum_{s \in \{0,1\}^n} P_S(s)^{\alpha}$

$$\log \sum_{s_{\underline{i}} \in \{0,1\}^k} P_{S_{\underline{i}}}(s_{\underline{i}})^{\alpha} \leq (n-k)(\alpha-1) + \log \sum_{s \in \{0,1\}^n} P_S(s)^{\alpha}$$

两边同除以 $1-\alpha$ 得: $H_\alpha(S_{\underline{i}}) \geq H_\alpha(S) - (n-k)$.

定理 2　设 $1<\alpha<2$, $0<r_1<1$, $0<t_1<1$, m 是满足 $m - \log(m+1) > \log(n/3) + t$ 的整数, $s \geq 0$ 是平滑熵的安全参数.

又设 Alice 和 Bob 共享一个长度为 n(n 是 3 的倍数, 否则增加或删除 1 个或 2 个比特) 的随机变量 S, $U=u$ 是 Eve 关于 S 的信息, 满足:

$$H_\alpha(S|U=u) \geq \left(\frac{2}{3} + \tau + r_1\right) n \quad (\text{其中 } r_1 + \frac{2}{3}t_1 < \tau < \frac{1}{3} - r_1)$$

则以下 3 个结论均以至少 $1 - 2^{-(\alpha-1)r_1 n} - 2^{-t_1 n}$ 的概率成立:

(1) Alice 和 Bob 可从 S 中提取的平滑熵 $\Psi(S) \geq \left(\tau + (2/3)r_1 - (1/3)t_1\right) n - \log(m+1) - 2$.

(2) Alice 和 Bob 可从 S 中提取高度保密的串 S', 其长度满足 $|S'| \geq \left(\tau + (2/3)r_1 - (1/3)t_1\right) n - \log(m+1) - 2 - s$.

(3) Eve 关于 S' 的信息量 $\leq 2^{-s}/\ln 2$.

又设 D 表示 Eve 成功实施假冒攻击或替换攻击这一事件, 则

$$P(D|U=u) \leq 2^{-(\tau - r_1 - 2/3t_1)n} + 2^{-2/3(\alpha-1)r_1 n + 1} + 2^{-2/3 t_1 n} = 2^{-\Omega(n)}.$$

证明　设 $n=3k$, S_1, S_2 分别是 S 的前 2/3 部分和后 1/3 部分, 长度为

$$|S_1| = n_1 = (2/3)n = 2k, \quad |S_2| = n_2 = (1/3)n = k,$$

将 S_1 看作 $GF(2^k)$ 中的一对元素 (A, B), 用于从 Universal hash 函数族中选取一个经认证的函数 G, 方法如下: Alice 随机选择 $X \in GF(2^k)$, 以 $Y = AX + B$ 作为认证符, 将 (X, Y) 发送给 Bob(如果 Eve 此时截获 (X, Y) 并将之删除, Bob 则不可能得到所希望的密钥, 因而终止协议的执行). Alice 和 Bob (Bob 在 $Y = AX + B$ 成立的情况下) 分别由 X 指定 Universal hash 函数 G. 由引理 6 得:

$$\begin{aligned} H_\alpha(S_1|U=u) &\geq H_\alpha(S) - (n - n_1) \geq (2/3 + \tau + r_1)n - (n - 2n/3) \\ &= (1/3 + \tau + r_1)n = (1/3 + \tau + r_1)3n_1/2 \\ &= [1/2 + 3/2(\tau + r_1)]n_1 \end{aligned}$$

由定理 1 得:

$$\begin{aligned} P(D|U=u) &\leq 2^{-(3\nabla/2 - 3r_1/2 - t_1)n_1} + 2^{-(\alpha-1)r_1 n_1 + 1} + 2^{-t_1 n_1} \\ &= 2^{-(3\nabla/2 - 3r_1/2 - t_1)2n/3} + 2^{-(\alpha-1)r_1 2n/3 + 1} + 2^{-t_1 2n/3} \\ &= 2^{-(\tau - r_1 - 2t_1/3)n} + 2^{-2/3(\alpha-1)r_1 n + 1} + 2^{-2/3 t_1 n} = 2^{-\Omega(n)} \end{aligned}$$

又由引理 6 得:

$$\begin{aligned} H_\alpha(S_2|U=u) &\geq H_\alpha(S) - (n - n_2) \\ &\geq \left(\frac{2}{3} + \tau + r_1\right) n - \left(n - \frac{1}{3}n\right) = (\tau + r_1) n \end{aligned}$$

以 S_2 作为 G 的输入, 即 $S' = G(S_2)$, 则由引理 1 和引理 2 得, 以下 3 个结论均以至少 $1 - 2^{-(\alpha-1)r_1 n - 2^{-t_1 n}}$ 的概率成立:

(1) Alice 和 Bob 可从 S 中提取的平滑熵 $\Psi(S) \geq H_\alpha(S_2|U=u) - \log(m+1) - r_1 n_2 - t_1 n_2 - 2 = \left(\tau + (2/3)r_1 - (1/3)t_1\right) n - \log(m+1) - 2$.

(2) Alice 和 Bob 可从 S 中提取高度保密的串 S', 其长度满足 $|S'| \geq H_\alpha(S_2|U=u) - \log(m+1) - r_1 n_2 - t_1 n_2 - 2 - s = \left(\tau + (2/3)r_1 - (1/3)t_1\right) n - \log(m+1) - 2 - s$.

(3) Eve 关于 S' 的信息量 $\leq 2^{-s}/\ln 2$.

5　结论

本文基于平滑熵研究了防主动攻击的无条件安全的秘密钥协商, 通信双方共享一个部分保密的随机变量, 在已知敌手关于该随机变量的 α 阶 Rényi 熵的下界的条件下, 得出了敌手攻击成功概率的上界, 以及通信双方以一定的概率所能提取的秘密钥长度.

参考文献:

[1] 杨波, 张彤, 王育民. 2001, 29(7): 930- 932.

[2] U M Maurer. IEEE Trans. Inform. Theory, 1993, 39(3): 733- 742.

[3] Charles H Bennett, et al. Generalized privacy amplification [J]. IEEE Trans. Inform. Theory, 1995, 41(6): 1915- 1923.

[4] Christian Cachin, Ueli Maurer. Linking information reconciliation and privacy amplification [A]. EUROCRYPT' 94 [C], Lecture Notes in Computer Science, Vol. 950, Springer-Verlag, 1995, 266- 274.

[5] Christian Cachin. Smooth entropy and Rényi entropy [A]. EUROCRYPT' 97 [C], Lecture Notes in Computer Science, Vol. 1233, Springer-Verlag, 1997, 193- 208.

[6] J L Carter, M N Wegman. Universal classes of hash functions [J]. J. Comput. Syst. Sci., 1979, 18(2): 143- 154.

[7] U M Maurer. Information-theoretically secure secret-key agreement by not authenticated public discussion [A], EUROCRYPT' 97 [C], Lecture Notes in Computer Science, Vol. 1233, Springer-Verlag, 1997, 209 - 225.

[8] S Wolf. Strong security against active attacks in information-theoretic secret-key agreement [A]. Advances in Cryptology-ACIACRYPT' 98 [C], Lecture Notes in Computer Science, Vol. 1514, Springer-Verlag, 1998, 405- 419.

作者简介:

杨　波　男. 1963 年 6 月生于陕西. 副教授, 1986 年在北京大学数学系获理学学士学位, 1993 年和 1999 年在西安电子科技大学计算机系和通信工程学院分别获得工学硕士和密码学博士学位. 目前从事信息隐藏和保密增强技术研究工作.

张　彤　(见本期第 1348 页)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

大的改变, 隐匿信息就不可能被修改.

例如对于一幅画有牛的数字图像, Alice 是发方, Bob 是收方, 如果主动攻击者 Wendy 只能改变 1% 的像素, 那么她就不可能把牛变成猪, 对于一个声像片段, 可以把某人说的一段清晰的话语作为宿主, Wendy 要想改变这些话, 须改变声音以及相应的人嘴的动作, 这是很难办到的. 我们把 U 称为宿主稳健成分的集合, $u\in U$, 函数 $f: u \rightarrow \{0,1\}^N$, 要在一个阈上信道中嵌入一个比特串 $x\in\{0,1\}^N$, Alice 选择一个宿主稳健成分 $u\in f^{-1}(x)$ 连同整个宿主信息通过阈上信道发送给 Bob, Wendy 可以怀疑隐蔽信道被使用, 她可以对宿主信息做小的改动以试图破坏噪声成分中可能嵌入的隐匿信息, 但却不能改变宿主稳健成分 u. Bob 收到 u 后, 应用函数 f, 可以恢复出 x, Wendy 要想把 u 修改成 u' 从而使 $f(u')\neq f(u)$ 是难于做到的, 即阈上信息具有稳健性. 函数 f 是公开的, 大家都容易得到, f 和 f^{-1} 是易于计算的. 使用阈上信道进行隐蔽通信, Alice 不能把一个具有明显意义的比特串直接传给 Bob, 因为 Wendy 可以用 f 很容易算出这一比特串(尽管她修改不了), 这样 Alice 和 Bob 之间的通信就会受到更加严密的控制和监视. 如果 Wendy 算出的是一个近似随机的数, 就不会产生怀疑.

阈上信道可用于完成一个隐蔽通信密钥交换的协议. Alice 生成一对公钥 y 和私钥 x, 选 $u\in f^{-1}(y)$, 送给 Bob, 根据阈上信道稳健性的特点, Bob 确信 Wendy 未改变 y, 这就克服了 Anderson 方案[7] 中可能出现的"中间人攻击". 假定 k 是 Alice 和 Bob 即将使用的隐蔽密钥, k 由 Bob 产生. Bob 收到 y 后, 选择 $u'\in f^{-1}(E_y(k))$ 发送给 Alice, Alice 恢复出 $E_y(k)$ 并用私钥 x 解密得到 k, 从而可以进行以数字图像或其它多媒体数据为载体的隐蔽通信. 一般来说, 数字图像中 5~10% 的成分为噪声数据. 可以把隐匿信息嵌入图像的噪声成分中, 以使人眼无法察觉到嵌入信息的存在. 嵌入了隐匿信息的宿主图像的数据量不变, 只是噪声成分的数据有了改变. 在一幅 1024* 1024 点阵像素的 8bit 灰度级图像中, 如果把 5% 的噪声数据用于嵌入隐匿信息, 则可传送 1024* 1024* 0.05= 51.2K 字节的隐匿信息, 远远大于对该图像数字签名中阈下信道的信息量.

下面用到的符号定义如下, 其余符号与前面定义的相同.

C 为所有可用的不含有隐匿信息的宿主信息的集合; U 为宿主信息中稳健成分的集合; k 为将隐匿信息嵌入宿主信息的密钥; K 为所有可能的 k 的集合; L 为把 K 加密后的密文的集合; Y 为公钥密码算法中公开密钥 y 的集合; X 为公钥密码算法中秘密密钥 x 的集合. 根据上述阈上信道的特点, 可以认为: $H(U|Y)=H(Y|U)=0$.

$$\because I((X,K);(L,U,Y))=H(L,U,Y)-H((L,U,Y)|(X,K))$$
$$=H(L,U)-H((L,U)|(X,K))$$
$$=I((X,K);(L,U))$$

又 $\because I((X,K);(L,U,Y))=H(L,U,Y)-H((L,U,Y)|(X,K))$
$$=H(L,Y)-H((L,Y)|(X,K))$$
$$=I((X,K);(L,Y))$$

$\therefore I((X,K);(L,U))=I((X,K);(L,Y))$

如果所用公钥密码算法是安全的, 即由 L 和 Y(或 U)得不到 X 和 K 的信息, 则

$$I((X,K);(L,Y))=H(X,K)-H((X,K)|(L,Y))$$
$$=H(X,K)-H(X|(L,Y))$$
$$-H(K|(L,Y,X))=0$$

$\because H(K|(L,Y,X))=0$

$\therefore H(X|(L,Y))=H(X,K)=H(K)+H(X|K)\geq H(K)$

由此可见, 攻击者由 L 和 Y(或 U)破译 X 的代价不低于直接攻击 K 的代价, 而 K 的安全性依赖于公钥算法本身的安全性, 所以攻击者通过破译 X 来得到 K 不会成功. 如果把隐匿信息 E 嵌入宿主的算法安全, 则 K 未知时便无法得到 E, 因而隐匿信息是安全的.

4 小结

利用数字签名中阈下信道传送隐匿信息时, 如果数字签名算法本身是安全的, 则隐匿信息是信息论上安全的, 但缺点是传输效率很低. 如果利用数字图像或其它多媒体宿主信息的噪声成分, 在其中建立隐蔽信道来传送隐匿信息, 则传输效率大大提高. 为了防止"中间人攻击", 引入阈上信道传递公开密钥, 如果所用的公钥密码算法是安全的, 则实际传送的隐匿信息是信息论上安全的.

参考文献:

[1] Anderson R J editor. Information hiding: first international workshop [A]. LNCS vol. 1174, Isaac Newton Institute, Cambridge [C], UK, May 1996. Springer-Verlag, Berlin, Germany.

[2] Aucsmith D editor. Information hiding: second international workshop [A]. LNCS vol. 1525, Portland Oregon [C], USA, April, 1998. Springer-Verlag, Berlin, Germany.

[3] 王育民, 刘建伟. 通信网的安全——理论与技术 [M]. 西安: 西安电子科技大学出版社, 1999, 4.

[4] Simmons G J. The subliminal channel and digital signatures [A]. Advances in cryptology - EUROCRYPT' 84 Proceedings [C], Berlin: Springer-Verlag, 1985, 364- 378.

[5] Simmons G J. Subliminal communication is easy using the DSA [A]. Advances in Cryptology - EUROCRYPT' 93 Proceedings [C], Berlin: Springer-Verlag, 1994, 218- 232.

[6] Craver S. On Public-key steganography in the presence of an active warden [A]. Information Hiding: second international workshop [C], LNCS vol. 1525, Berlin: Spinger-Verlag, April 1998, 355- 368.

[7] Anderson R J. Stretching the limits of steganography [A]. Information Hiding first international workshop [C], LNCS vol. 1174, Berlin: Springer-Verlag, May 1996, 39- 48.

作者简介:

张 彤 男. 1967 年 6 月生于陕西. 1988 年和 1991 年分别在西安交通大学信控系和西北核技术研究所获学士和硕士学位, 现为西北核技术研究所副研究员、西安电子科技大学通信工程学院博士生. 主要从事网络安全和信息隐藏技术方面的研究工作.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net