# 窃听信道下的认证信道容量

陈大江[1,2]，秦 臻[1,2]，秦志光[1,2]

(1. 电子科技大学信息与软件工程学院 成都 611731；2. 电子科技大学网络与数据安全四川省重点实验室 成都 611731)

【摘要】消息认证是合法发送方Alice传输消息$M$给合法的接收方Bob并向Bob认证$M$的交互过程。为了防止敌手Eve的攻击，Alice和Bob通常共享了一个安全密钥。该文考察如下认证框架：Alice首先通过无噪声信道将消息$M$发送给Bob；Alice接着利用消息$M$和安全密钥$K$生成一个认证标签；Alice再将认证标签转化为码字$X^n$；最后，Alice通过窃听信道模型将码字$X^n$传输给Bob。该文定义了固定标签率下的安全认证信道容量，并证明该认证信道容量等于$H(X|Z)$。特别地，证明了文献[15]提出的协议在该文的认证模型中是可达容量的。

**关 键 词** 消息认证； 认证信道容量； 信息论安全； 窃听信道

**中图分类号** TP309 **文献标志码** A doi:10.3969/j.issn.1001-0548.2015.04.017

# Authentication Capacity Over Wiretap Channel

CHEN Da-jiang[1,2], QIN Zhen[1,2], and QIN Zhi-guang[1,2]

(1. School of Information and Software Engineering, University of Electronic Science and Technology of China Chengdu 611731;
2. Network and Data Security Key Laboratory of Sichuan Provence, University of Electronic Science and Technology of China Chengdu 611731)

**Abstract** Message authentication is an interactive procedure that allows a legitimate sender Alice to send and authenticate a message M to a legitimate receiver Bob. To prevent the attacks from an adversary Eve, Alice and Bob usually share a secret key $K$. In this paper, we study a novel authentication framework as follows. Firstly, Alice sends a message $M$ to Bob over a noiseless channel; Secondly, Alice generates an authentication tag with the message $M$ and secret key $K$; Thirdly, Alice encodes the tag into a codeword $X^n$; Finally, Alice transmits the codeword $X^n$ to Bob over a wiretap channel. This paper defines an authentication channel capacity under a fixed tag rate, and show that it equals to $H(X|Z)$. Specifically, we prove that the authentication protocol proposed in Ref. [15] is capacity-achievable under our authentication model.

**Key words** authentication; authentication channel capacity; information-theory security; wiretap channel

消息认证是密码学和信息安全领域中一个最基础也是最重要的研究问题之一。其目的是，发送方Alice将消息 $M$ 发送给接收方Bob，并通过交互(或者非交互)的方式使得Bob能够确认消息 $M$ 是来自Alice的。要达到这个目的，Alice和Bob首先要共享一个密钥 $K$ 。为了确保协议的安全性，首先要考虑敌手模型，即敌手具有什么样的计算能力，能够发起什么形式的攻击。通常采用的敌手模型是敌手可以发起中间人攻击。即敌手可以冒充Alice(Bob)发送任何消息给Bob(Alice)。除此之外，敌手还可以插入、篡改和删除Alice和Bob之间的消息。

在经典消息认证模型中，Alice和Bob之间的通信信道是无噪声的[1-2]。然而，在无噪声的认证模型中，由于每一次认证都会降低密钥的熵，故而提高了敌手攻击成功的概率。文献[2]证明了使用相同密钥认证 $l$ 个消息后，敌手攻击成功概率的下界是 $2^{-H(K)/(l+1)}$ 。这说明当 $l$ 增大时，攻击成功的概率将会很快增加到1。噪声是通信中常见的物理现象。在安全领域，噪声却带来了诸多好处。文献[3]在窃听信道模型下利用噪声实现了合法用户间的密钥共享，同时使窃听者得不到任何关于密钥的信息。文献[4]将这一结果推广到了广播信道模型。从此，噪声信道下的密钥分配问题得到了理论和工业界的广泛研究[5-9]，但在噪声信道下的消息认证的相关工作却鲜有进展。如何实现信息安全下的多项式次的消息认证是一个值得关注的问题。

## 1 相关工作

本文将考察在噪声信道下的消息认证。文献[10]提到了利用噪声信道获得的相关性实现(无噪声)公

收稿日期： 2014 – 02 – 11；修回日期： 2014 – 12 – 15
基金项目：国家科技重大专项(20112X03002-002-03)；国家自然科学基金重点项目(61190110).
作者简介：陈大江(1982 – )，男，博士生，主要从事信息论安全、物理层安全、无线安全等方面的研究.

共信道的消息认证。该问题可归类为信源模型[11]的消息认证。文献[12]首次提出了窃听信道的消息认证：Alice和Bob共享一个密钥，当Alice发送 $X$ 时，合法接收者Bob通过主信道 $\boldsymbol{W}_1: X \to Y$ 收到 $Y$，窃听者通过窃听信道 $\boldsymbol{W}_2: X \to Z$ 收到 $Z$。当不等式 $I(X;Y) > I(X;Z)$ 成立时，文献[12]构造出一个能够多次进行消息认证的认证协议，并且认证次数的增加对敌手攻击成功的概率的影响是可以忽略的。而文献[2]的结论说明上述结果在无噪声信道下是不可能的。相关的研究工作还包括文献[13]提出的在MIMO衰落信道下的认证问题，该协议假设Alice和Bob之间没有共享密钥，并且假设攻击者只发起冒充攻击。该协议在文献[14]中得到了进一步的研究。

本文考察如下认证框架：Alice首先通过无噪声信道将消息 $M$ 发送给Bob，接着利用安全密钥生成一个认证标签，再将认证标签转化为码字 $X^n$，最后通过窃听信道模型将码字传输给Bob。本文定义了固定标签率下的安全认证信道容量，并证明该认证信道容量等于 $H(X|Z)$。这也进一步证明了文献[15]提出的协议在本文的认证模型中是可达容量的。

## 2 窃听信道模型与系统模型

### 2.1 窃听信道模型

一条输入字母表为$X$，输出字母表为$Y$的信道称为离散无记忆信道(discrete memoryless channel, DMC)当且仅当这个信道可以有随机矩阵 $\boldsymbol{W} = \{W(y|x)\}_{x\in X, y\in Y}$ 表示。其中，$W(\cdot|x)$ 是指当输入为 $x$ 时，在信道输出端的输出分布情况，即 $W(y|x) = P_{Y|X}(y|x)$。当输入为序列 $x^n = x_1x_2\cdots x_n$，输出为 $y^n = y_1y_2\cdots y_n$ 时，有：

$$P_{Y^n|X^n}(y^n|x^n) = \prod_{i=1}^{n} P_{Y|X}(y_i|x_i) = \prod_{i=1}^{n} W(y_i|x_i)$$

**定义 1** 把输入相同的两个离散无记忆信道 $\boldsymbol{W}_1: X \to Y$，$\boldsymbol{W}_2: X \to Y$ 称为窃听信道模型。其中，$\boldsymbol{W}_1$ 为主信道；$\boldsymbol{W}_2$ 为窃听信道。

### 2.2 系统模型

如图1所示，考虑两个离散无记忆信道 $\boldsymbol{W}_1: X \to Y$，$\boldsymbol{W}_2: X \to Z$。Alice和Bob共享一个对称密钥 $K$，其中 $K$ 是从一个有限集 $[\![K]\!]$ 中均匀的随机产生。他们由信道 $W_1$ 相连，当Alice传输 $X \in [\![X]\!]$ 时，Bob以概率 $P_{Y|X} = W_1(Y|X)$ 接收到 $Y \in [\![Y]\!]$(其中，对任意随机变量 $R$，$[\![R]\!]$ 定义为 $R$ 的事件域)。同时，$X$ 将在窃听信道 $\boldsymbol{W}_2$ 上传输。窃听者Oscar收到的信道输出变量为 $Z \in [\![Z]\!]$，其概率分布满足 $P_{Z|X} = \boldsymbol{W}_2(Z|X)$。Alice的目标是传输消息 $M$ 的同时并对消息进行认证。为此，定义认证模型为：记 $[\![M]\!]$ 为消息域，Alice将传输并认证消息 $M \in [\![M]\!]$。

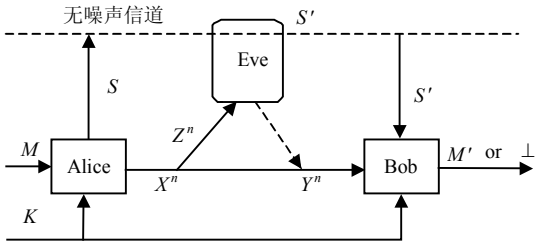


图1 系统模型

1) Alice通过无噪声信道发送消息 $M$ 给Bob；

2) Alice利用哈希函数 $h: [\![M]\!]\times[\![K]\!] \to [\![T]\!]$ 产生一个标签 $T = h_K(M)$；然后利用有密钥的编码函数 $f_K: [\![T]\!] \to [\![X]\!]^n$ 产生认证码 $X^n = f_K(T)$；最后在窃听信道 $(W_1, W_2)$ 上发送认证码 $X^n$。

3) Bob从无噪声信道接收到消息 $M'$，同时从信道 $\boldsymbol{W}_1$ 接收到失真的认证码 $Y^n$。Bob计算 $T' = h_K(M')$，并通过带密钥的函数 $\mathrm{g}_K: T \times Y^n \to \{0,1\}$ 认证 $(T', Y^n)$。如果函数 $\mathrm{g}_K$ 的输出是1，则接受消息 $M'$；否则，拒绝。

把满足上述模型的协议称为一个认证协议(记为 $\Pi$)，如果生成的认证码为 $X^n$，即认证码的长度为 $n$，用 $\Pi_n$ 表示 $\Pi$。

## 3 敌手模型

协议 $\Pi$ 的目的是认证消息 $M$。一个认证失败包含有两种可能性：完备性错误或者敌手攻击，其中，完备性错误是指没有敌手存在时发生了错误。在本文的模型中，从Alice到Oscar有一条DMC信道相连。Oscar可以插入和修改在无噪声信道的传输消息。假设从Oscar到Bob的信道是无噪声的，且敌手具有无限的计算能力。本文希望在敌手Oscar多次通过窃听信道 $W_2$ 得到认证的观察值并且多次动态地修改无噪声信道的消息的前提下，Oscar还是不能伪造一个可通过认证的消息。这里“多次”的上界是认证码长度的任意多项式。形式化地，Oscar可发起两类攻击。

1) 假设 Alice 已经认证了消息 $M_1, M_2, \cdots, M_{i-1}$。为了认证消息 $M_i$，Alice 在无噪声信道上发送消息 $M_i$，并且在信道 $(\boldsymbol{W}_1, \boldsymbol{W}_2)$ 上发送认证码 $X_i^n$。Oscar可以观察到 $M_i$ 并可以将其篡改为 $M_i'$。还可以观察到信道 $\boldsymbol{W}_2$ 的输出 $Z_i^n$。Bob 可以接收到无噪声信道

的消息 $M_i'$ 和信道 $\boldsymbol{W}_1$ 的输出 $Y_i^n$。Oscar 获得 Bob 的判定比特 $b_i := \mathrm{g}_k(T_i', M_i')$，这里 $T_i' = h_{\mathrm{k}}(M_i')$。当 $b_i = 1$ 并且 $M_i' \neq M_i$ 时，攻击成功。其中，$M_i'$ 的选取是基于 Oscar 的随机源 $R$，消息 $M_i'$ 和前 $i-1$ 阶段收集到的信息：$\{(M_j, Z_j^n)\}_{j=1}^{i-1}$；以及在第一型攻击下的判定比特 $\{b_j'\}$ 和在第二型攻击下的判定比特 $\{\hat{b}_j\}$。

如果 $M_t' = M_t$ (即不发起攻击)，$b_t = 1$ 是(几乎)可以确定的，因此可以将其从 $\{b_j'\}$ 中去掉。

2) Osca可以自适应地通过无噪声信道发送给Bob任何消息 $M_t \in [\![M]\!]$ 和 $\hat{Y}_t^n \in [\![Y]\!]^n$。Oscar将会学习到 Bob 的判定比特 $\hat{b}_i := \mathrm{g}_k(\hat{T}_t, \hat{Y}^n)$，其中，$\hat{T}_t = h_{\mathrm{k}}(\hat{M}_t)$。如果 $\hat{b}_i = 1$，则攻击成功。这里 $(\hat{M}_t, \hat{Y}_t^n)$ 的计算是基于Oscar的随机源 $R$ 和前 $i-1$ 阶段收集到的信息 $\{(M_j, Z_j^n)\}_{j=1}^{i-1}$、$\{b_j'\}$ 和 $\{\hat{b}_j\}$。

# 4　安全认证协议与安全认证容量

## 4.1　安全认证协议

在引入敌手模型后，开始形式化定义认证。认证的性质由完备性和认证性组成。完备性指敌手不存在时，Bob应当以很高的概率接受消息 $M$ 为合法的消息；认证性指在敌手存在的前提下，认证失败的可能性应该很小，其中，认证失败是指接受了敌手篡改过的消息。

**定义 2**　称一个函数 $f: \mathbb{N} \to \mathbb{R}$ 是可忽略的当且仅当对任意多项式函数 $\mathrm{Ploy}: \mathbb{N} \to \mathbb{R}$，存在一个自然数 $N_0$，当 $n \geqslant N_0$ 时，有：

$$\mathrm{f}(n) \leqslant \frac{1}{\mathrm{Ploy}(n)}$$

**定义 3**　给定一个窃听信道模型 $\boldsymbol{W}_1: X \to Y$，$\boldsymbol{W}_2: X \to Y$，称协议 $\Pi$ 是认证安全的当且仅当 $\Pi$ 满足下列条件：1) 完备性：如果敌手不存在，那么Bob将以指数(对于 $n$)小的概率拒绝合法的消息 $M$；2) 强安全性：记VIEW(Oscar)为窃听者Oscar的观察值，那么，互信息 $I(T; \mathrm{VIEW(Oscar)})$ 是可忽略的(对于 $n$)；3) 认证性：如果第二型攻击的次数不超过多项式(对于 $n$)，那么敌手攻击成功的概率 Pr(succ) 是可忽略的(对于 $n$)。

完备性说明合法消息有很高的概率通过认证；强安全性说明认证过程中的认证标签不会向敌手泄露；认证性说明敌手不能伪造一个消息并通过认证。

限制第二型攻击次数是不可避免的，这是因为敌手Oscar可以持续地选择同一个消息 $M$ 并选择所有可能的 $Y^n$，并通过无噪声信道发送给Bob。由于 $[\![Y]\!]^n$ 是有限集，Oscar总能够选中某些 $Y^n$ 使得攻击成功。限定第二型攻击的次数不超过多项式的原因是，每一次攻击都涉及接收方Bob，而要求Bob的复杂度超过多项式是不实际的。另外，由于第一型攻击的次数等于Alice发送消息的次数，故第一型攻击自然的被限定在多项式内。

## 4.2　安全认证容量

考虑到在窃听信道上通信是比较昂贵的资源，因此，希望尽可能少地利用这一昂贵的资源。针对有效性分析，定义了两类有效性测度。

第一类测度称为标签率，其定义是：

$$\ell_{\mathrm{auth}} = \log|M| / \log|T|$$

即消息源长度与标签长度的比值。

第二类测度称为标签的信道编码率，定义为：

$$\ell_{\mathrm{chan}} = \frac{1}{n}\log|T|$$

即标签长度和编码长度的比值。

事实上，$\ell_{\mathrm{auth}}$ 和 $\ell_{\mathrm{chan}}$ 都涉及信道的使用效率。一方面，对于固定的 $\ell_{\mathrm{chan}}$，更大的 $\ell_{\mathrm{auth}}$ 意味着同样的消息源具有更小的标签长度，因此，会更少使用窃听信道 $(W_1, W_2)$。另一方面，对于固定的 $\ell_{\mathrm{auth}}$，更大的 $\ell_{\mathrm{chan}}$ 意味着同样的 $n$，可以在信道上传输更长的标签，因此，消息源的长度也随之更长。也就是说，增加 $\ell_{\mathrm{auth}}$ 和 $\ell_{\mathrm{chan}}$ 的值都能够提高信道的使用率。本文协议主要关注如何提高 $\ell_{\mathrm{chan}}$ 的值，这是传统密码学解决的问题。

在窃听信道下安全认证信道容量的定义如下：

**定义 4**　给定一个窃听信道模型 $\boldsymbol{W}_1: X \to Y$，$\boldsymbol{W}_1: X \to Y$。对于任何以 $\ell_{\mathrm{auth}}$ 的标签率认证安全的协议 $\Pi$，可达的最大信道率 $\ell_{\mathrm{chan}}$ 称为以标签率为 $\ell_{\mathrm{auth}}$ 的安全认证信道容量，简记为 $C_{\mathrm{chan}}(\ell_{\mathrm{auth}})$。

# 5　主要结果

## 5.1　一个重要的定理

先引用一个重要的定理，该定理是构造一个可达安全认证容量的认证协议的基础。

**定理 1**[15]　记 $X, Y, Z$ 分别为 $[\![X]\!], [\![Y]\!], [\![Z]\!]$ 上的随机变量，且 $P_{Y|X} = \boldsymbol{W}_1$，$P_{Z|X} = \boldsymbol{W}_2$ 为两个DMC。有一个类 $P$ 使得 $X$ 的概率分布 $P_X = P$，且对于任意 $x \in [\![X]\!]$，有 $P(x) > 0$。若存在 $\tau > 0$，使得 $I(X;Y) > I(X;Z) + \tau$，那么，对于任意正整数 $I$、$J$ 满足条件：

$$0 \leqslant \frac{1}{n}\log J \leqslant H(X|Y)+\tau$$

$$0 \leqslant \frac{1}{n}\log I \leqslant I(X;Y)-I(X;Z)-\tau$$

则存在不相交的子集簇 $C_{ij} \subset T_P^n\ (i \in [I], j \in [J])$，使得对于足够大的 $n$，有下列3个性质成立：

1) 对于每一个 $j$，子集 $C_{\cdot j} \triangleq \bigcup_i C_{ij}$ 是信道 $\boldsymbol{W}_1$ 上一个信道编码 $(f_j, g_j)$ 的码本，并且该信道编码的平均解码错误率是指数(对于 $n$)小的。其中，$f_j$ 将消息 $m$ 映射到 $C_{\cdot j}$ 的第 $m$ 个码字。

2) 记 $J$ 为 $[J]$ 上的随机变量，$I$ 为 $[I]$ 上的随机变量，$\hat{Z}^n$ 为输入 $\hat{X}^n \leftarrow C_{IJ}$ 时信道 $\boldsymbol{W}_2$ 的输出。如果联合分布 $P_{IJ} = P_J / I$，那么，存在 $\beta_2 > 0$，使得 $I(I,J;\hat{Z}^n) \leqslant 2^{-n\beta_2}$ (该结果不依赖于 $P_J$)。

3) 对于 $[J]$ 上的任意随机变量 $J$，$[I]$ 上的任意随机变量 $I$，记 $\hat{Z}^n$ 为输入 $\hat{X}^n \leftarrow C_{IJ}$ 时信道 $\boldsymbol{W}_2$ 的输出。假设 $[J]$ 上的任意随机变量 $J'$ 使得 $J' \neq J$，且满足下列条件：

① $SD(P_{J'J}; P_{J'|I}) \leqslant \delta_1$；

② $J' \to IJ \to \hat{X}^n \to \hat{Y}^n$ 形成 Markov 链；

③ 对任意 $j', j$，有：

$$P_{J'J}(j', j) \leqslant \frac{2^{n^{\omega}}}{J(J-1)} + d(j', j)$$

且函数 $d(\bullet,\bullet)$ 满足不等式：

$$\sum\nolimits_{j',j} d(j', j) \leqslant \delta_2$$

那么，对于足够大的 $n$，有：

$$P(\hat{Y}^n \in T_{[W]_\varepsilon}(\boldsymbol{C}_{IJ'})) \leqslant 2^{-n\omega} + \delta_1 + \delta_2$$

式中，$\omega$ 是开区间 $(0,1)$ 上的常数。

### 5.2 可达性构造

文献[15]所构造的安全认证协议描述如下。

记 $\boldsymbol{W}_1 : X \to Y$，$\boldsymbol{W}_2 : X \to Y$ 为窃听信道模型。假设 $I(X;Y) > I(X;Z) + \tau$，其中 $\tau$ 为大于0的常数。$X$ 的概率分布 $P_X$ 为类 $P$，并且对任意的 $x \in X$ 有 $P(x) > 0$。记 $T_P^n$ 上的子集簇 $C_{ij}\ (i = 1,2,\cdots,I;\ j = 1,2,\cdots,J)$ 是通过定理1得到的。令 $K_1 = \{1,2,\cdots,I\}$，$h : [\![M]\!] \times [\![K_0]\!] \to [\![T]\!]$ 是一个 $\varepsilon$-ASU 哈希函数[15]，其中，集合 $[\![K_0]\!]$ 是密钥空间，$[\![T]\!] \subseteq \{1,2,\cdots,J\}$。Alice和Bob预先共享了对称密钥 $(K_0, K_1) \in [\![K_0]\!] \times [\![K_1]\!]$。如果 Alice 要传输消息 $M \in [\![M]\!]$ 给Bob，那么，执行下列步骤：

1) Alice计算 $T = h_{K_0}(M)$，并且从 $C_{K_1 T}$ 中随机地选出一个码字 $X^n$。Alice再将消息 $M$ 通过无噪声(无认证的)信道传给Bob。消息 $M$ 经过Oscar后，Bob收到 $M'$。最后，Alice通过信道 $(\boldsymbol{W}_1, \boldsymbol{W}_2)$ 传输 $X^n$。Oscar 通过 $W_2$ 收到 $Z^n$，Bob通过 $W_1$ 收到 $Y^n$。

2) 获得 $M'$ 和 $Y^n$ 后，Bob计算 $T' = h_{K_0}(M')$。如果 $\mathrm{g}(Y^n) \in C_{K_1 T'}$，Bob接受 $M'$；否则，拒绝。

在定理1中，$f_j$ 将消息 $l$ 编码成码本 $C_{\cdot j}$ 中的第 $l$ 个码字，$g_j(Y^n)$ 将 $Y^n$ 解码成 $\perp$ 或者 $C_{\cdot j}$ 中码字的编号。由于编号和码字是一一对应的，因此，在本文的构造中，$g_j(Y^n)$ 被定义为将 $Y^n$ 解码 $\perp$ 或者 $C_{\cdot j}$ 中码字。

**定理 2** 对于上述认证协议，存在一个恰当的参数输入，使得对任意的 $\ell_{\text{auth}}$，以及任意的 $\delta \in (0, H(X|Z))$，有 $\ell_{\text{chan}} = H(X|Z) - \delta$。

证明：该定理证明类似于文献[15]的定理3，这里将其略去。

### 5.3 理论上界

**定理 3** 给定窃听信道模型 $\boldsymbol{W}_1 : X \to Y$，$\boldsymbol{W}_2 : X \to Y$。对于任何以 $\ell_{\text{auth}}$ 的标签率认证安全的协议 $\Pi$，有 $\ell_{\text{chan}} \leqslant H(X|Z)$。

证明：由强安全性可知:

$$H(T) = H(T|Z^n) + I(T;Z^n) \leqslant$$
$$H(T|Z^n) + I(T;\text{View(Oscar)}) \leqslant$$
$$H(X^n|Z^n) + \varepsilon_n \leqslant nH(X|Z) + \varepsilon_n$$

式中，第 1 个不等式成立的原因是 $Z^n \in \text{VIEW(Oscar)}$；第2个不等式成立是因为 $T$ 可以由 $X^n$ 完全确定；第3个不等式成立是因为 $X^n$ 和 $Z^n$ 是独立同分布且窃听信道是离散无记忆的。

故有：

$$\ell_{\text{chan}} \leqslant H(X|Z)$$

证毕。

**定理 4** 给定窃听信道模型 $\boldsymbol{W}_1 : X \to Y$，$\boldsymbol{W}_2 : X \to Y$。对于任意 $\ell_{\text{auth}}$，认证信道容量为 $C_{\text{chan}}(\ell_{\text{auth}}) = H(X|Z)$。

证明：由定理2和定理3可以得出结论。

## 6 结 论

Alice在一个无噪声信道的辅助下，利用窃听信道 $\boldsymbol{W}_1 : X \to Y$，$\boldsymbol{W}_2 : X \to Y$ 来认证消息 $M$，其中，Alice和Bob事先共享一个对称密钥。在这个认证框架下，Alice利用无噪声信道来传输要认证的消息 $M$，然后在窃听信道上传输认证标签 $T$ 所对应的码字。证明了本文考虑的认证模型下的安全认证容量为 $H(X|Z)$。文献[15]提出了一个高效的消息认证

协议，本文的结果说明了该协议是可以达到认证容量的。将来的工作会探究怎样构造出一个计算有效的协议？

## 参 考 文 献


[1] SIMMONS G J. Authentication theory/coding theory[C]// Proc of CRYPTO'84. Berlin, Heidelberg: Springer, 1985: 411-431.

[2] MAURER U M. Authentication theory and hypothesis testing[J]. IEEE Trans Inf Theory, 2000, 46(4): 1350-1356.

[3] WYNER A D. The wire-tap channel[J]. Bell Syst Tech J, 1975, 54: 1355-1387.

[4] CSISZAR I, KORNER J. Broadcast channels with confidential messages[J]. IEEE Trans Inf Theory, 1978, 24(3): 339-348.

[5] MAURER U M, WOLF S. Secret-key agreement over unauthenticated public channels, part I: Definitions and a completeness result[J]. IEEE Trans Inf Theory, 2003, 49(4): 822-831.

[6] MAURER U M, WOLF S. Secret-key agreement over unauthenticated public channels, part II: the simulatability condition[J]. IEEE Trans Inf Theory, 2003, 49(4): 832-838.

[7] MAURER U M, WOLF S. Secret-key agreement over unauthenticated public channels, part III: Privacy amplification[J]. IEEE Trans Inf Theory, 2003, 49(4): 839-851.

[8] CHEN D J, QIN Z, MAO X F, et al. Smokegrenade: an efficient key generation protocol with artificial interference [J]. IEEE Transactions on Information Forensics & Security, 2013, 8(11): 1731-1745.

[9] CHEN D J, MAO X F, QIN Z, et al. Smokegrenade: a key generation protocol with artificial interference in wireless networks[C]//Proceedings of IEEE MASS. Hangzhou: IEEE, 2013: 200-208.

[10] KORZHIK V, YAKOVLEV V, MORALES L G, et al. Performance evaluation of keyless authentication based on noisy channel[C]//MMM-ACNS 2007. Berlin, Heidelberg: Springer-Verlag, 2007: 115-126.

[11] AHLSWEDE R, CSISZAR I. Common randomness in information theory and cryptography, part II: CR capacity [J]. IEEE Trans Inf Theory, 1998, 44(1): 225-240.

[12] LAI L F, ELGAMAL H, POOR H V. Authentication over noisy channels[J]. IEEE Trans Inf Theory, 2009, 55(2): 906-916.

[13] BARACCA P, LAURENTI N, TOMASIN S. Physical layer authentication over MIMO fading wiretap channels[J]. IEEE Transactions on Wireless Communications, 2012, 11(7): 2564-2573.

[14] FERRANTE A, LAURENTI N, MASIERO C, et al. On the achievable error region of physical layer authentication techniques over Rayleigh fading channels[EB/OL]. (2013-03-04). http://arxiv.org/abs/1303.0707.

[15] CHEN D J, JIANG S Q, QIN Z G. Message authentication code over a wiretap channel[EB/OL]. (2013-10-15). http://arxiv.org/abs/1310.3902.


编 辑 蒋 晓