**华 中 科 技 大 学**

**本科生课程报告**

**姓 名 MTX**

**学 号 U2021XXXX**

**学 院 网络空间安全学院**

**班 级 信安21XX班**

**课程名称 通信编码安全理论**

**报告日期 2024年06月04日**

**评 分**

|  |  |  |  |
| --- | --- | --- | --- |
| **题号** | **得分** | **题号** | **得分** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |
| --- | --- |
| **总分：** | **评卷人：** |

**注：1、无评卷人签名试卷无效。**

**2、必须用钢笔或圆珠笔阅卷，使用红色。用铅笔阅卷无效。**

基于反馈的极化码窃听信道保密编码方案

# 

# 摘 要

极化码可以用于实现退化窃听信道的保密容量。本文提出了一种基于反馈的极化码保密编码方案，适用于非退化窃听信道。通过引入反馈结构，所提出的保密编码方案可以显著提高正保密率。此外，极化码具有低复杂度的编码和解码特性，便于实现。仿真结果表明，该基于反馈的极化码保密编码方案可以可靠且安全地传输机密信息。同时，还分析了前向信道和反馈信道条件对所提保密编码方案性能的影响。

**关键词：**极化码；反馈；非退化窃听信道；保密编码

目 录

[**摘 要** I](#_Toc167462865)

[**1 引言 1**](#_Toc167462866)

[**2 问题表述 2**](#_Toc167462867)

[**3 提出的极化码保密编码方案 4**](#_Toc167462868)

[A. 保密编码方案 4](#_Toc167462869)

[B. 性能分析 4](#_Toc167462870)

[**4 仿真结果 4**](#_Toc167462871)

[**5 总结 8**](#_Toc167462872)

[**参考文献 8**](#_Toc167462873)

**1 引言**

随着无线网络的发展，安全问题变得越来越重要。在窃听信道上实现既可靠又安全的通信，近年来成为一个热门研究课题。许多保密编码方案被提出，用于在合法用户之间可靠地传输机密信息，并防止信息被窃听者截获。

1975年，Wyner提出了通用的退化窃听信道模型[1]。证明了在退化窃听信道上存在一个保密容量 ，即如果保密速率小于 ，则存在编码方案可以渐近实现既可靠又安全的通信。2007年，Arikan发明了极化码[2]，这是第一类被证明能够渐近实现离散无记忆信道对称容量且具有低编码和解码复杂度的码。由于这些优势，极化码被用于实现窃听信道的保密容量。基于极化码的退化窃听信道保密编码方案在[3][4][5]中提出，并证明了既可达到保密容量又可实现速率等价区域。

然而，在非退化窃听信道上，Wyner的编码方案不能提供任何正保密率以确保安全通信。在这种情况下，最近提出的一些机制可能用于等效地将非退化窃听信道转化为退化窃听信道。在[6]中，提出了一种反馈编码结构来达到这一目的，并实现了严格的正保密率，即使窃听信道比合法用户之间的信道噪声更小。然而，文献[6]中仅表明保密码存在，并未提出实现最大可能正速率的保密编码方案。

本文通过引入反馈结构和构建两级极化编码，提出了一种基于反馈的极化码保密编码方案，以在非退化窃听信道上实现正保密率。我们证明了所提保密编码方案的可靠性和安全性。仿真结果表明，所提保密编码方案可以实现可靠和安全的通信。并讨论了前向和反馈信道条件对所提保密编码方案性能的影响。

本文其余部分组织如下：第II部分介绍了非退化窃听信道上的反馈编码结构和正可达保密率。在第III部分中，我们提出了一种基于反馈的极化码保密编码方案，适用于非退化窃听信道。第IV部分通过仿真评估了所提保密编码方案。最后，第V部分给出了结论。

# 2 问题表述

本节回顾了文献[6]中的反馈编码结构。

如图1所示，在两个合法用户Bob和Alice之间建立了一个反馈信道。作为窃听者，Eve也可以访问从Bob到Alice的反馈信道。为了简化，我们将所有用户之间的信道视为二进制对称信道（BSC）。我们记从Alice到Bob的前向信道的交叉概率为，从Alice到Eve的交叉概率为 。反馈信道从Bob到Alice的交叉概率为 ，从Bob到Eve的交叉概率为 ​ 。由于前向窃听信道是非退化的，我们假设 ​ 。

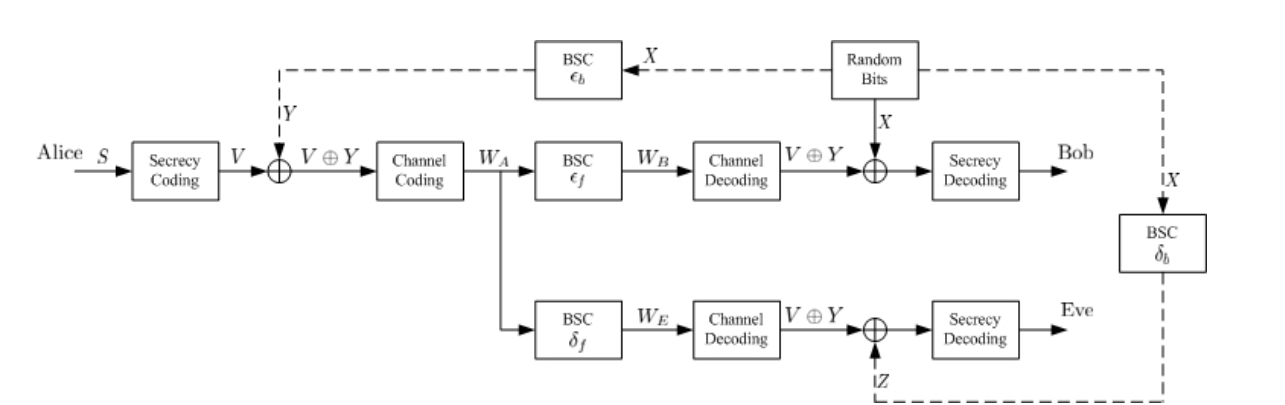


图1 反馈式保密编码模型在窃听信道中的应用

使用反馈保密编码结构传输机密信息的过程可以概念性地描述如下：

1. 当传输开始时，Bob向Alice反馈一个n比特序列x。序列x由期望为0.5的伯努利随机变量的独立实现生成n次。由于序列比特是独立同分布的，并且每个比特的错误概率对应于反馈信道的交叉概率，Alice和Eve分别接收到反馈序列y和z。
2. 假设从Alice到Bob和从Alice到Eve的前向信道都是无错误的。如果Alice想要向Bob发送一个n比特序列v，她必须发送 ，这里⊕表示模2加法。因此，Alice和Bob可以无误地接收到 。
3. 接收到 后，Bob恢复v的最优策略是计算 ，Eve的最优方式是计算 。

作为反馈保密编码结构的结果，Bob的等效比特错误概率记为 ，即 ,而Eve的等效比特错误概率 ,即 ​ 。由于 ，我们得到一个等效系统，其中解码后的窃听信道是主信道的退化版本，如图2所示。

要获得等效退化窃听信道，唯一的限制是前向信道并非真正无错误。然而，根据信道编码理论，如果n比特序列 以小于Alice到Bob信道容量的速率传输，则存在一种编码方案可以渐近实现无误传输。这里，由于 ， ，且 。因此，只要传输速率小于 ，就可以渐近实现可靠传输。

设 为保密编码后的最大保密速率，即：

(1)

在反馈保密编码结构中，我们使用 比特承载 个保密比特，然后将 比特编码为n比特序列v。假设Alice以速率 传输机密信息 ，并设 ​ 。因此，经过信道编码后，传输序列 为 比特。然后，我们得到一个整体保密速率 为：

(2)

在(2)中，引入反馈后的整体保密速率总是小于等效速率 ​ ，系数为 ​​。

为了实现尽可能大的保密速率 ​，我们应设计一种保密编码方案，使 ​ 和 同时最大化，其中 ​ 和 分别表示等效退化窃听信道的保密容量和从Alice到Bob的前向信道容量。

# 3 提出的极化码保密编码方案

## A. 保密编码方案

提出的保密编码方案分为两部分，即在等效退化窃听信道上的保密编码和在前向非退化信道上的信道编码。

首先，在生成机密消息v后，爱丽丝计算v⊕y，并使用信道编码编码器实现从爱丽丝到鲍勃的前向信道容量。所提出的信道编码方案是通过仔细选择适当的M = ，其中k是自然数，且< ，使得|{ i ∈ [M], Z() < }|= n成立。这里的记号|S|表示集合S的大小，Z(W)表示巴氏参数。

其次，我们将考虑在等效退化信道上的基于反馈的保密编码。在等效退化窃听信道模型中，假设主信道W\*是具有交叉概率的二元对称信道 (BSC)，而退化窃听信道W也是具有交叉概率+ - 2 的二元对称信道。对于任意固定的正常数 < ，我们定义良好信道集合 和坏信道集合如下:

(3)

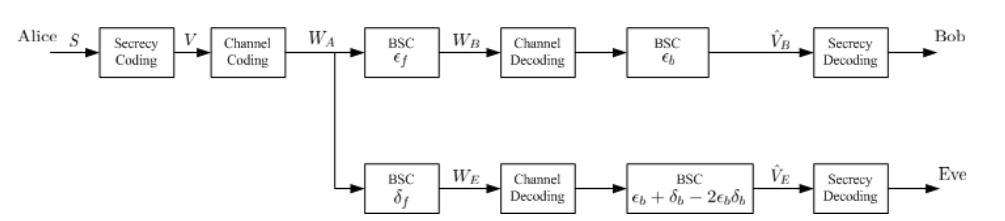


图2 等效退化窃听信道

由于极化码要求码长为2的指数，因此通道编码器的输入长度并不总是等于保密编码器的输出长度。由于我们需要找到一个足够大的整数s，使得s ≤ n，其中s =，n = s + n2，n2 < s，n1 ∈ N，n2 ∈ N。

对于给定的s和固定的< ，保密编码序列被划分为三个子集:

(4)

请注意。子集A代表对鲍勃有利但对伊芙不利的比特信道，R 是对鲍勃和伊芙都有利的比特信道集合，而B对应的是对鲍勃和伊芙都不利的比特信道集合。设，，保密序列 。我们定义，表示 **m**在集合S中坐标上的投影。

编码和解码算法描述如下:

**编码**：输入序列**m**被分成三部分：， 和 。携带从保密源生成的保密比特， 由爱丽丝从独立的 (0,1) 伯努利实验中均匀选择。被视为冻结比特集，已被鲍勃和爱丽丝知道。根据标准极化编码方法，输出序列

**解码**：形式上，连续消除 (SC) 解码算法用于在解码器处恢复机密消息。

由于保密序列和信道序列的长度是2的幂，有时我们不能充分利用前向信道中的 n个良好比特信道。这是基于反馈的极化码保密编码方案的限制。

编码和解码实现的复杂度是，保密编码是 ，而信道编码是 。

因此，整体基于反馈的保密编码方案使用两级极化编码。第一级实现保密编码，第二级实现信道编码。

## B. 性能分析

已经在[3]中证明了，在退化窃听信道上，保密编码方案可以实现保密容量。令保密率为，

***定理1 [7]***: 对于信道编码，如果我们选择适当的M，使得< ，并且满足|{() }|= 𝑛。将表示为从爱丽丝到鲍勃的前向信道，速率受到以下限制：

(5)

***命题2:*** 当保密序列的长度等于在前向信道上良好信道比特的总数n时，所提出的基于反馈的极化码保密编码方案实现了总体保密率

(6)

证明: 利用反馈保密编码结构，我们得到

(7)

随着码长渐近地趋向无穷大，保密率达到了保密容量，而信道传输率可写成：

(8)

总体保密率为：

(9)

由于保密码和信道码的长度都要求为2的指数，因此在分母中添加了系数。当趋近于1时，总体保密率的最大值为 ，其中s = n。因此，只有在一些特殊情况下，例如 = ，n ∈ N，才会达到最大保密率。

从命题2可以看出，所提出的保密编码方案总是可以实现正的保密率。作为一种保密编码方案，其可靠性和安全性需要在理论上得到证明。这里，我们使用两个指标来说明所提出的保密编码方案能够实现可靠性和安全性。

可靠性:

安全性： (10)

其中， 衡量的是可靠性。如果 = 0，表示机密信息在传输过程中没有错误。 表示混淆度，指的是窃听者在接收到从窃听信道估计的机密信息后，对机密信息的平均不确定性。如果混淆度等于零，意味着窃听者无法获得有效的机密信息。换句话说，传输是安全的。

***定理3：***所提出的基于反馈的极化码保密编码方案渐近地实现了可靠性和安全性。

证明：假设接收方使用连续消除解码器。设信道是从用户X到用户Y的信道，且。因此，信道中的块错误率为

(11)

令 , , 令为保密解码器的输出。因此，我们有：

(12)

然后，

(13)

其中，不等式(a)成立的原因是机密信息的块错误率不超过前向信道传输的块错误率加上前向信道传输正确但保密解码错误的块错误率。

在引入信道编码后，窃听者伊芙的混淆度增加，公式如下：

(14)

因此，不等式（b）成立是因为 s → → 形成马尔可夫链。因此，

(15)

设是窃听信道的输出， 也是窃听信道的输出，但被视为无噪声信道。如式（14）所示，。

定义 利用Fano不等式，我们有

(16)

其中,。然后，

(17)

然后，

= 0 (18)

因为 并且, 对，

(19)

# 4 仿真结果

在本节中，我们评估了所提出的基于反馈的极化码保密编码方案的性能。我们使用鲍勃和伊芙的比特错误率 (BER) 来展示该方案的可靠性和安全性。设 为鲍勃的 BER， 为伊芙的 BER。所提出的基于反馈的极化码保密编码方案的最佳条件是 ≈ 0 和 ≈ 0.5，其中 代表可靠性， 代表安全性。

对于二进制对称信道 (BSC)，我们采用文献 [8] 中提出的启发式方法来构建极化码。极化码的解码器使用连续消除算法来恢复消息。

图3展示了码长M对所提出的基于反馈的极化码保密编码方案的可靠性和安全性的影响，其中非退化窃听信道的参数为 = 0.05， = 0.03，反馈信道的参数为 = 0.01， = 0.2。随着M的增加，我们总能选择合适的和来获得保密率 ≈ 0.115625。从图3中可以观察到，当码长增加时，所提出的保密编码方案的可靠性 趋近于0，而其安全性趋近于0.5。因此，所提出的基于反馈的极化码保密编码方案可以实现可靠和安全的通信。

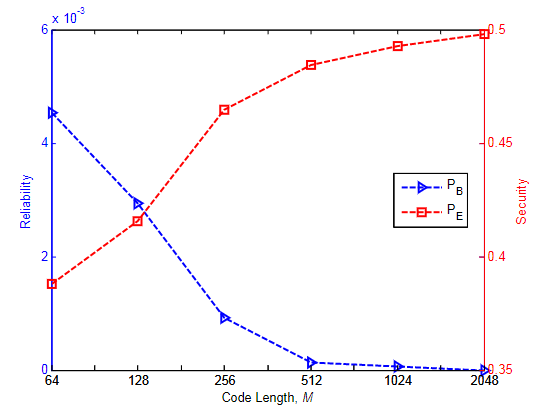


图3. 码长对所提出的保密编码方案的可靠性和安全性的影响，在此假设 = 0.05， = 0.03，= 0.01， = 0.2。

然后，讨论信道参数对所提出的保密编码方案性能的影响。表1展示了前向信道参数和对所提出的基于反馈的极化码保密编码方案的可靠性和安全性的影响，其中反馈信道的参数为 = 0.01， = 0.2，码长M = 128，保密率 = 0.197917。从表1可以观察到，当爱丽丝和鲍勃之间的前向信道变差，而爱丽丝和伊芙之间的前向信道 保持不变时，所提出的保密编码方案的可靠性变差，而安全性保持不变。此外，当保持不变而 变差时，所提出的保密编码方案的可靠性保持不变，而安全性变好。我们还观察到，当窃听信道 是的退化版本时，例如在= 0.04， = 0.05的情况下，可以实现良好的安全通信。

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| 0.02 | 0.01 | 0.001012 | 0.469424 |
| 0.04 | 0.01 | 0.006891 | 0.469424 |
| 0.04 | 0.04 | 0.006891 | 0.469720 |
| 0.04 | 0.05 | 0.006891 | 0.470209 |

表1 前向信道参数对所提出的保密编码方案的可靠性和安全性的影响

因此，当反馈信道已定时，所提出的基于反馈的极化码保密编码方案的可靠性随着爱丽丝和鲍勃之间前向信道状况的恶化而变差，而随着爱丽丝和伊芙之间前向信道状况的恶化，所提出的基于反馈的极化码保密编码方案的安全性则会变好。

表2列出了反馈信道参数 和 对所提出的基于反馈的极化码保密编码方案的可靠性和安全性的影响，其中前向信道的参数为 = 0.01， = 0.01，码长M = 256，保密率 = 0.190104。在表2中，和 分别表示具有反馈的等效退化窃听信道的参数。

当鲍勃和伊芙之间的反馈信道 变差时，所提出的基于反馈的极化码保密编码方案的可靠性和安全性都会变好。这一现象的原因在于，对于等效退化窃听信道，如果主信道和窃听信道之间的差距变大，我们可以选择更多对爱丽丝有利而对伊芙不利的比特信道。为了实现恒定的保密率，我们可以选择对鲍勃更好而对伊芙更差的比特信道，从而提高可靠性和安全性。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
| 0.01 | 0.18 | 0.01 | 0.1864 | 0.000393 | 0.479597 |
| 0.01 | 0.20 | 0.01 | 0.2060 | 0.000342 | 0.481942 |
| 0.01 | 0.22 | 0.01 | 0.2256 | 0.000300 | 0.486839 |
| 0.01 | 0.25 | 0.01 | 0.2550 | 0.000199 | 0.488551 |

表2 反馈信道参数对所提出的保密编码方案的可靠性和安全性的影响

图4展示了在不同反馈信道条件下，所提出的基于反馈的极化码保密编码方案的可达保密率，其中 = = 0.3，M=256，= 0.02， = 0.01。

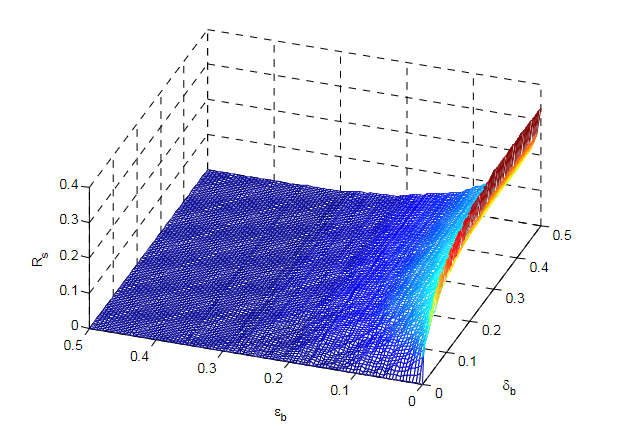


图4在不同反馈信道条件下，所提出的保密编码方案的可达保密率，其中 = = 0.3，M=256，= 0.02， = 0.01。

从图4中，我们观察到如果反馈信道 变好且 变差，那么所提出的基于反馈的极化码保密编码方案的可达保密率会变大，这表明反馈机制在我们提出的方案中起作用。为了在非退化窃听信道上实现更大的保密率，前向信道 和反馈信道 应该噪声较小，而反馈信道 应该较差，以便 和之间的噪声差距足够大，可以传输更多的机密信息。

# 5 总结

在本文中，我们提出了一种基于反馈的极化码保密编码方案，该方案适用于非退化窃听信道。在所提出的方案中，通过在非退化窃听信道中引入反馈并构建两级极化编码，可以实现严格正的保密率。同时，我们证明了在某些特殊情况下可达的最大保密率 。此外，我们还证明了所提出的基于反馈的极化码保密编码方案的可靠性和安全性。

仿真结果表明，所提出的基于反馈的极化码保密编码方案能够在非退化窃听信道上可靠且安全地传输机密信息。当爱丽丝和鲍勃之间的主信道状况改善以及鲍勃和伊芙之间的反馈信道状况恶化时，所提出的保密编码方案的可靠性得到提高。当爱丽丝和伊芙之间的窃听信道状况以及鲍勃和伊芙之间的反馈信道状况恶化时，所提出的保密编码方案的安全性得到增强。

**参考文献**

1. H. Liu, Y. Wang, J. Yang, and Y. Chen, “Fast and practical secret key extraction by exploiting channel response,” in Proc. INFOCOM, Turin,Italy, 2013, pp. 3048–3056
2. P. Barsocchi, S. Chessa, I. Martinovic, and G. Oligeri, “A cyber-physical approach to secret key generation in smart environments,”J. Ambient Intell. Humanized Comput., vol. 4, no. 1, pp. 1–16, 2013,doi: 10.1007/s12652-011-0051-5.
3. P. Barsocchi, G. Oligeri, and C. Soriente, “SHAKE: Single hash key establishment for resource constrained devices,” Ad Hoc Netw., vol. 11,no. 1, pp. 288–297, 2013, doi: 10.1016/j.adhoc.2012.05.013
4. C. Cachin and U. M. Maurer, “Linking information reconciliation and privacy amplification,” J. Cryptol., vol. 10, no. 2, pp. 97–110, 1997, doi: 10.1007/s001459900023.
5. T. K. Moon, Error Correction Coding: Mathematical Methods and Algorithms. Hoboken, NJ, USA: Wiley, 2005
6. R. G. Gallager, Low Density Parity Check Codes. Cambridge, MA, USA:MIT Press, 1963
7. S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik,Secret Key Extraction From Level Crossings Over Unauthenticated Wireless Channels. New York, NY, USA: Springer, 2010, pp. 201–230,doi: 10.1007/978-1-4419-1385-2\_9
8. P. Hoeher, “A statistical discrete-time model for the WSSUS multipath channel,” IEEE Trans. Veh. Technol., vol. 41, no. 4, pp. 461–468,Nov. 1992
9. P. Karadimas and D. W. Matolak, “Generic stochastic modeling of vehicle-to-vehicle wireless channels,” Veh. Commun., vol. 1, no. 4,pp. 153–167, 2014, doi: 10.1016/j.vehcom.2014.08.001.
10. H. Liu, Y. Wang, J. Yang, and Y. Chen, “Fast and practical secret key extraction by exploiting channel response,” in Proc. INFOCOM, Turin,Italy, 2013, pp. 3048–3056.
11. T. Wang, Y. Liu, and A. V. Vasilakos, “Survey on channel reciprocity based key establishment techniques for wireless systems,” Wireless Netw., vol. 21,