

DOI: 10.3969/j.issn.1007-5461.2025.03.007

基于极化码的低复杂度星地量子密钥分发 实验密钥纠错方法

尹子欣, 刘尉悦*

(宁波大学信息科学与工程学院, 浙江 宁波 315211)

摘要: 纠错对于星地量子密钥分发 (QKD) 至关重要。在众多误码纠错算法中, 极化码有较高的编码效率和纠错速度。在基于极化码的星地 QKD 系统中, 不仅卫星面临体积和功耗等问题, 地面站也在不断追求设备的集成化。为了实现低成本的星地 QKD 设备, 本文提出了一种基于现场可编程门阵列 (FPGA) 的极化码连续删除 (SC) 译码器, 该译码器具有低硬件复杂度结构。分析表明, 该译码器在码长 N 为 1024 时, 能达到 29.7 Mbit/s 的吞吐率, 在硬件资源指标查找表 (LUT) 和触发器 (FF) 的消耗个数分别为线型结构译码器的 5.7% 和 10%。进一步的仿真实验表明, 在典型系统参数条件下, 该译码器在码长为 64 K 时, 其安全成码率达到 27.9 kbit/s。

关键词: 量子光学; 低硬件复杂度; 现场可编程门阵列; 极化码; 误码纠错; 成码率

中图分类号: TN927+.2

文献标识码: A

文章编号: 1007-5461(2025)03-00354-07

Key error correction method with low complexity for satellite-to-ground quantum key distribution experiment based on polar codes

YIN Zixin, LIU Weiyue*

(Faculty of Electrical Engineering and Computer Science, Ningbo University, Ningbo 315211, China)

Abstract: Error correction is crucial for satellite-to-ground quantum key distribution (QKD). Among many error correction algorithms, polar codes have higher coding efficiency and error correction speed. In the satellite-to-ground QKD system based on polar codes, not only satellites face the problems such as volume, quality and power consumption, but also ground stations is constantly pursuing the integration of equipment. Therefore, in order to realize low-cost satellite-to-ground QKD equipment, a field programmable gate array (FPGA) based on successive cancellation (SC) decoder with low hardware complexity is proposed. The analysis shows that the decoder can achieve a throughput of 29.7 Mbit/s when the code length N is 1024, and the consumption numbers of the hardware resource indicator lookup table (LUT) and flip-flops (FF) are 5.7% and 10% of that of the linear structure decoder,

基金项目: 浙江省自然科学基金 (LY21F050003)

作者简介: 尹子欣 (1998 -), 江西新余人, 研究生, 主要从事量子通信与应用方面的研究。E-mail: yinzx98@163.com

导师简介: 刘尉悦 (1978 -), 江西萍乡人, 博士, 副教授, 主要从事量子通信与应用方面的研究。E-mail: liuweiyue@nbu.edu.cn

收稿日期: 2023-09-21; 修改日期: 2023-10-23

*通信作者。

respectively. Further satellite-to-ground QKD data reconciliation simulation experiments show that under the conditions of typical system parameters, when the code length is 64 K, the security rate of the decoder can reach 27.9 kbit/s.

Key words: quantum optics; low hardware complexity; field-programmable gate array; polar codes; data reconciliation; bit rate

0 引言

在量子密钥分发 (QKD) 协议中, 通过产生、传输和测量量子信号, 通信双方 (Alice 和 Bob) 可以获取各自的原始密钥^[1]。借助卫星作为中继节点, QKD 可以突破地面光纤和自由空间的距离限制, 实现全球范围的量子密钥分发^[2-4]。2022年, 我国成功发射“济南一号”量子微纳卫星, 为构建高效、集成化、低成本化的天地一体化量子保密通信网络打下了基础^[5]。因此, 星地量子密钥分发已成为当前研究的前沿领域。

在 QKD 系统中, 由于实验设备不完善、外部环境干扰以及攻击者 (Eve) 的窃听影响, 会引起比特误码和信息泄露^[6-8]。因此, 纠正量子信道传输误码比特至关重要。BBSS^[9]和 Cascade 算法^[10]由于频繁的信息交互, 导致处理延时长、纠错速度慢; LDPC 码的校验矩阵依赖于误码率, 且采用迭代译码导致复杂度较高^[11]。然而, 自 2014 年极化码首次被应用于 QKD 的后处理误码纠错环节以来, 编码效率和纠错速度都有所提高^[12]。从此, 学术界对极化码在 QKD 中的应用展开了全面且深入的研究^[13-15]。

截至目前, 已经提出了不同的基于现场可编程门阵列 (FPGA) 的极化码连续删除 (SC) 算法译码结构, 以提升译码器的性能^[16]。例如, 树型结构^[17]通过建立 FPGA 上的树结构, 并利用并行处理能力, 对极化码进行有效译码; 线型结构^[18]在树型结构的基础上, 通过多路复用资源减少硬件复杂度, 同时保持吞吐率不变。尽管这些译码器结构能实现高吞吐率, 但由于其并行处理中使用的计算结构数量较多, 消耗了大量硬件资源。在高速星地 QKD 应用中, 卫星面临体积、质量和功耗等问题, 而地面站不断追求设备的集成化, 因此, 在满足纠错性能和吞吐率要求的同时, 降低 SC 译码器的硬件资源消耗, 对于星地 QKD 中的极化码具有重要意义。

本文将重点放在 SC 译码器硬件设计的优化上, 通过提前计算中间值、资源复用、减少计算结构的使用, 从而基于 FPGA 实现一种低硬件复杂度的 SC 译码器。在牺牲少量吞吐率的条件下, 该译码器大幅减少了其在硬件中的资源消耗。对设计的译码器结构进行星地 QKD 数据协商方案的仿真实验, 验证了其在星地量子密钥分发场景中的应用性能。

1 极化码译码算法

极化码的基本思想是通过信道极化, 选择优质子信道传输信息比特, 将传输能力较弱的子信道的编码比特作为冻结比特, 使其不参与信息传输。SC 译码通过对每个传输比特的对数似然比 (LLR) 进行计算, 进而译出比特。定义第 i 个比特的对数似然比为

$$L_N^0(y_1^N, \hat{u}_1^{i-1}) \triangleq \ln \frac{W_N^0(y_1^N, \hat{u}_1^{i-1} | 0)}{W_N^0(y_1^N, \hat{u}_1^{i-1} | 1)}, \quad (1)$$

式中: N 为码长, y_1^N 为接收序列, \hat{u}_1^{i-1} 为前 $i-1$ 个译码比特的估计值, $W_N^0(y_1^N, \hat{u}_1^{i-1} | 0)$ 为条件转移概率, 本研究计算对数似然比 LLR 值, 对比特进行估计值判决, 则有

$$\hat{u}_i = \begin{cases} u_i, & u_i \text{ 为冻结比特} \\ 0, & L_N^{(i)}(y_1^N, \hat{u}_1^{i-1}) \geq 0, u_i \text{ 为信息比特}, \\ 1, & L_N^{(i)}(y_1^N, \hat{u}_1^{i-1}) < 0, u_i \text{ 为信息比特} \end{cases} \quad (2)$$

式中: u_i 为当前 i 位原本比特, 译码按照 i 从 $1 \sim N$ 的顺序依次进行。Arikan^[16] 提出的 SC 译码结构类似于快速傅里叶变换结构, 其被划分为 $\log_2 N$ 个阶层的计算。并根据 (1) 式, 得到对数似然比的递推公式, 其分别为 f 函数和 g 函数, 可以表示为

$$\begin{cases} f(L_a, L_b) \triangleq \ln \left(\frac{e^{L_a+L_b} + 1}{e^{L_a} + e^{L_b}} \right), \\ g(L_a, L_b, \hat{u}_s) = (-1)^{\hat{u}_s} L_a + L_b \end{cases} \quad (3)$$

式中: L_a 、 L_b 表示上一层的对数似然比值, \hat{u}_s 表示已译出比特或者译码比特的模二和。但是 (3) 式中由于硬件实现 f 函数的乘法和除法过于复杂, 为了简化硬件, 使用最小和算法^[9], 将 f 函数近似为

$$f(L_a, L_b) = B_{MS}(L_a) B_{MS}(L_b) \min(|L_a|, |L_b|), \quad (4)$$

式中 B_{MS} (most significant bit) 表示最高有效位, 最小和算法简化了计算方式, 硬件实现容易, 通过比较器和加法器实现 f 函数计算, 而 g 函数不发生改变。

2 极化码译码器 FPGA 的实现

根据 SC 译码原理, 在整个极化码的译码过程中, f 函数和 g 函数的计算是核心部分, 由 (4) 式可知, 这两种函数的计算过程相互独立, 在硬件实现层面均需构建复杂运算模块。并且在线型译码结构中, LLR 值按照递归性进行计算, 待获得译码结果后, 再进行 g 函数计算。该结构采用多函数并行计算, 虽能实现高吞吐率, 但会显著增加 FPGA 的资源消耗。针对上述问题, 本文采用将 f 函数和 g 函数关联起来进行计算, 以及将 g 函数提前计算和复用计算结构的方法, 该方法基于 FPGA 的结构原理图, 如图 1 所示。

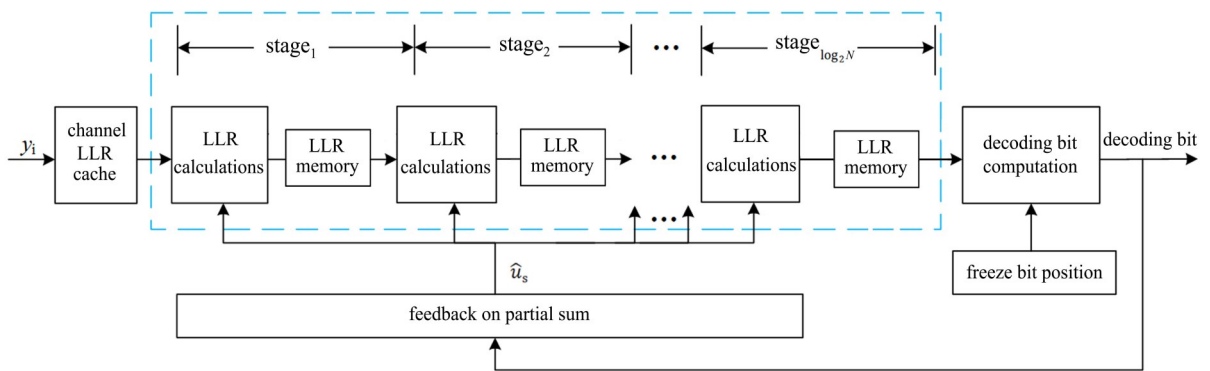


图 1 基于 FPGA 的低硬件复杂极化码译码器原理图

Fig. 1 Schematic diagram of a low hardware complex polarization code decoder based on FPGA

由图 1 可知, 在该译码器中将 y_i 作为输入, 进入信道缓存 LLR 模块, 转换为初始 LLR。LLR 计算模块对输入的 LLR 进行计算, 将计算结果用作下一阶段的输入, 或将计算结果传递到译码比特计算模块, 进行译码。LLR 存储模块用于保存 LLR 计算模块生成 f 函数和 g 函数的 3 个结果, 当下次需要数据时, 直接从该模块中取出, 无需重新计算。部分和反馈模块通过输入已译码比特, 进行部分和计算, 从而作为 g 函数的指数项 \hat{u}_s 。

译码比特计算模块用于计算最后一层的 LLR, 得到的结果根据冻结比特位模块输出的冻结比特位进行判决, 最终输出译码比特。

2.1 极化码 f 函数和 g 函数的关联计算

在常规的 f 函数^[20]中, $\min(|L_a|, |L_b|)$ 需要比较 LLR 值, 以确定最小绝对值, 再通过 LLR 值的最高位进行异或, 完成 $B_{MS}(L_a)B_{MS}(L_b)$ 的计算; 而 g 函数的计算将 LLR 值转换为补码形式, 在加减计算后, 将二进制补码形式的 LLR 值转换为有符号数^[20], 根据部分和 \hat{u}_s , 来选择 g 函数的似然值。然而, 由于 f 函数和 g 函数是分开计算各自的结果, 整体计算的效率较低, 而且 f 函数绝对值的比较部分在硬件实现上较为复杂, 因此, 采取 f 函数和 g 函数关联计算的方式: 1) 将输入的 LLR 相加和相减, 分别得到两个 g 函数的计算结果; 2) 对 g 函数计算出的 L_a+L_b 和 L_a-L_b 进行分析, 可以发现 $B_{MS}(L_a+L_b) \oplus B_{MS}(L_a-L_b)$ 与 $B_{MS}(L_a^2-L_b^2)$ 的大小一致, 并且 $L_a^2-L_b^2$ 的大小正好可以判决 L_a 和 L_b 的绝对值大小。因此, 可直接通过对 g 函数的计算结果的最高位进行异或计算, 将计算的结果作为判决 f 函数的绝对值大小的依据。直接利用 g 函数的计算结果, 得到 f 函数计算所需的绝对值, 再与输入的符号位进行运算, 得到 f 函数的计算结果。

这样, 在 f 函数的硬件设计中不需要设计对输出的 LLR 值进行比较的比较器, 如图 2 所示, g 函数以补码形式存储, 极大地减少了运算过程中的补码和有符号数值之间的转换。

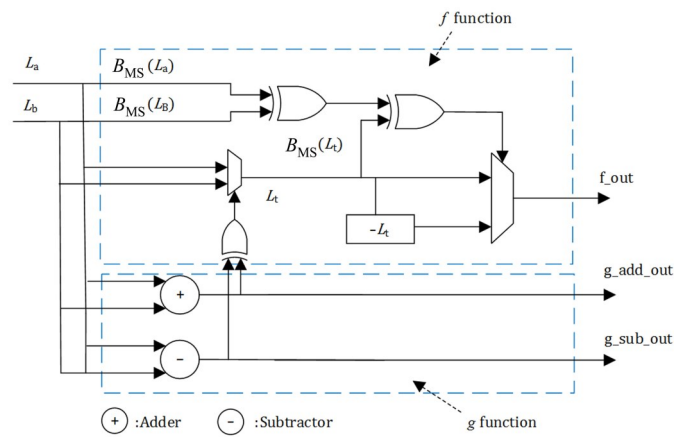


图 2 f 函数和 g 函数的硬件设计图

Fig. 2 Hardware design diagram of f function and g function

由图 2 可见, 该硬件模块由 L_a 、 L_b 作为输入, 输出分别有 f 函数计算结果、 g_add_out (表示 g 函数计算的加法结果)、 g_sub_out (表示 g 函数计算的减法结果)。使用加法器和减法器计算 g 函数的两个结果, 通过 g 复用函数结果的最高位进行异或运算, 生成用于选择最小绝对值的控制信号。最后, f 函数计算的输出结果由 L_a 、 L_b 和绝对值对应数据的符号位异或决定。

2.2 极化码 g 函数的提前计算

在线型结构的 SC 译码器计算 LLR 值的过程中, 通常只有其中一种函数 (f 函数或 g 函数) 被激活计算, 另一种函数并没有同时进行计算, 导致计算效率下降。其译码器在一个时钟周期内, 最多有 $N/2$ 个 f 函数或 g 函数同时进行计算^[18], 由此可见, 这种方式将导致资源浪费。

为了解决以上问题, 本文在提出的译码结构设计中提前计算 g 函数, 并与 f 函数同时计算之后进行存储。

这样,在后续的译码阶段,可以直接复用 g 函数的计算结果,无需重新计算。因此,该结构在FPGA的硬件实现中,设计 f 函数和 g 函数的计算模块和存储模块,用于提前计算和存储LLR的结果,减少了再次计算LLR需要的译码周期,并在整个译码结构上,大幅减少了计算 f 函数和 g 函数的硬件结构的使用,通过复用 f 函数和 g 函数结构来计算LLR值。该译码结构采用 $\log_2 N$ 个 f 函数和 g 函数复用设计,通过串行计算,实现了层间资源共享,同时利用层间并行计算提升吞吐率,从而显著提高了FPGA资源利用率。

2.3 极化码译码器的分析

为了更全面地评估两种结构的性能差异,对基于FPGA的本研究译码器与文献[18]中的SC译码器进行了综合结果比较。由于采用相同的芯片进行对比,可以更好地反映出两者的差异,因此,研究采用与文献[18]相同的Xilinx公司的Virtex-5系列XC5VFX70T芯片,并使用FPGA设计软件ISE 14.2进行分析。

如表1所示,该译码器结构在牺牲少量吞吐率(TH)的情况下,使用的查找表(LUT)、触发器(FF)的数量明显低于线型结构SC译码器,分别仅约为线型结构所使用个数的5.7%和10%,有效降低了译码器的资源消耗。

表1 编码长度为1024的综合资源结果

Table 1 Comprehensive resource results with encoding length of 1024

Decoder category	LUT	FF	Computation structure	TH/(Mbit·s ⁻¹)
SC decoder in this paper	2173	942	10	29.7
Linear structure SC decoder ^[18]	38152	9867	512	34.2

由于Virtex-5系列芯片为早期Xilinx公司旗下的Virtex系列,其计算能力和FPGA硬件板中资源的使用量有限。因此,采用了芯片型号Xilinx Virtex-7 XC7VX485T实现长码的译码器,并对本文译码器的综合结果进行了对比分析,结果如表2所示。

由表2可知,本文设计的低硬件复杂度译码结构在无需任何外接模块的条件下,能够实现编码长度为65536(64 K)的译码器,其译码吞吐率可达13.6 Mbit/s,因此,该译码结构在功耗受限的星地量子密钥分发卫星通信环境中具有适用性。由于芯片型号以及综合软件的差异,导致编码长度 N 为1024时,译码器资源的消耗和吞吐率与表1不同。因此,在硬件设备层面,选择更好的芯片也是提高性能的方法之一。

表2 不同码长下本文结构译码器的综合结果

Table 2 Comprehensive results of the decoder structure with different code length

N	LUT	FF	f /MHz	TH/(Mbit·s ⁻¹)
1024	1340	911	141.4	37.7
65536	53051	34372	67.6	13.6

3 实验仿真与验证

根据随机冻结位的极化码数据协调方案^[21],编写了基于极化码的实验仿真程序。实验过程中,对发送端(地面站)的编码序列进行比特随机翻转,以模拟量子信道引入误码,使接收端接收到包含误码的序列,将该序列与冻结序列一起输入到接收端(模拟卫星)译码器中,用于译码器译码之后进行编码,从而得到结果。

采用标准BB84协议,基矢比对因子 q 取0.5^[22]。设定实验参数发射频率为625 MHz,其中信号态、诱骗态

和真空态的比例为2:1:1, 信号态平均光子数和诱骗态平均光子数分别为0.8和0.1, 量子信道的链路衰减设置为30 dB, 接收端单光子探测器的暗计数为6250 counts/s。此外, 为了衡量系统的纠错性能, 引入 f 因子(FEC), 其越接近于1, 表明纠错性能越好。因此, 本实验在基于上述典型系统参数的设置下, 增加 f 因子为1时的安全成码率理论极限值作为对照标准, 得到量子比特误码率(QBER)与成码率的关系图, 如图3所示。

根据仿真结果, 当QBER为1%时, 系统的安全成码率在码长为65536 (64 K) 时达到27.9 kbit/s, 而在码长为1024 (1 K) 时为20.8 kbit/s, 而 f 因子为1时, 安全成码率理论极限值则达到36.7 kbit/s。相比之下, 即使在码长仅为1024的情况下, 系统的安全成码率也超出了该理论极限的50%。而当码长扩展到65536 (64 K), QBER上升到3%时, 系统仍能有效生成安全密钥, 其安全成码率仍保持在273 bit/s。因此, 结合表1的数据分析可知, 该译码器相对于线性结构, 其所需的硬件逻辑资源减少了90%以上, 这表明, 本研究设计的译码器在保持低硬件复杂度的前提下, 依然具有相对较高的纠错效率。这为资源受限的星地量子密钥分发场景的硬件设计提供了有效参考。

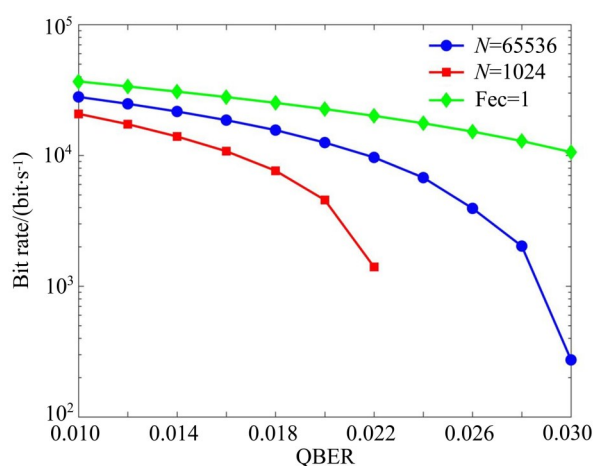


图3 量子比特误码率与成码率的关系

Figure.3 Relationship between quantum bit error rate and bit rate

4 结论

本研究提出了一个低硬件复杂度的SC译码器, 采用 g 函数提前计算和复用计算模块的方法, 优化了 f 函数和 g 函数结构, 从而降低了系统的复杂性和成本, 有利于实现星地量子密钥分发设备的小型化与集成化。通过Virtex-5系列XC5VFX70T综合分析, 该译码器在码长 N 为1024时, 吞吐率可达29.7 Mbit/s, 相较于线型结构译码器, 其对硬件资源指标的消耗更少。通过数据协调实验, 在典型系统参数条件下, 译码器在码长为64 K时, 安全成码率达到27.9 kbit/s, 验证了低硬件复杂度译码器的有效性。在量子通信领域, 本研究提出的译码器适用于高速实时星地QKD系统, 具有广泛的应用范围。

参考文献:

- [1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing [J]. *Theoretical Computer Science*, 2014, 560: 7-11.
- [2] Yin J, Li Y H, Liao S K, et al. Entanglement-based secure quantum cryptography over 1, 120 kilometres [J]. *Nature*, 2020, 582 (7813): 501-505.

- [3] Chen Y A, Zhang Q, Chen T Y, *et al.* An integrated space-to-ground quantum communication network over 4, 600 kilometres [J]. *Nature*, 2021, 589(7841): 214-219.
- [4] Ren J G, Xu P, Yong H L, *et al.* Ground-to-satellite quantum teleportation [J]. *Nature*, 2017, 549(7670): 70-73
- [5] 林梅, 王磊, 王海涵. 解密世界首颗量子微纳卫星的前世今生 [OL]. [2023-08-20]. http://https://zqb.cyol.com/html/2022-08/08/nw.D110000zgqnb_20220808_4-08.htm.
- [6] Kurtsiefer C, Zarda P, Halder M, *et al.* Quantum cryptography: A step towards global key distribution [J]. *Nature*, 2002, 419(6906): 450.
- [7] Li Y, Liao S K, Liang F T, *et al.* Post-processing free quantum random number generator based on avalanche photodiode array [J]. *Chinese Physics Letters*, 2016, 33(3): 030303.
- [8] Zhou X D, Wang S, Zhang T B, *et al.* Continuous-variable QKD data reconciliation protocol based on concatenated Polar coding and multistage decoding [J]. *Chinese Journal of Quantum Electronics*, 2022, 39(3): 411-417.
周晓东, 王晟, 张天兵, 等. 基于级联Polar码和多级译码方法的连续变量QKD数据协商协议 [J]. 量子电子学报, 2022, 39(3): 411-417.
- [9] Bennett C H, Bessette F, Brassard G, *et al.* Experimental quantum cryptography [J]. *Journal of Cryptology*, 1992, 5(1): 3-28.
- [10] Brassard G, Salvail L. Secret-key reconciliation by public discussion [C]. *Advance in Cryptology-Eurocrypt'93*, Berlin: Springer, 1994: 410-423.
- [11] Elkouss D, Leverrier A, Alleaume R, *et al.* Efficient reconciliation protocol for discrete-variable quantum key distribution [C]. *IEEE International Symposium on Information Theory*, 2009: 1879-1883.
- [12] Jouguet P, Kunz-Jacques S. High performance error correction for quantum key distribution using polar codes [J]. *Quantum Information and Computation*, 2014, 14(3&4): 329-338.
- [13] Zhao S M, Shen Z G, Xiao H, *et al.* Multidimensional reconciliation protocol for continuous-variable quantum key agreement with polar coding [J]. *Science China (Physics, Mechanics & Astronomy)*, 2018, 61(9): 090323.
- [14] Zhang M, Dou Y, Huang Y, *et al.* Improved information reconciliation with systematic polar codes for continuous variable quantum key distribution [J]. *Quantum Information Processing*, 2021, 20(10): 327.
- [15] Zhang M, Hai H, Feng Y, *et al.* Rate-adaptive reconciliation with polar coding for continuous-variable quantum key distribution [J]. *Quantum Information Processing*, 2021, 20(10): 318.
- [16] Arikan E. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels [J]. *IEEE Transactions on Information Theory*, 2009, 55(7): 3051-3073.
- [17] Leroux C, Tal I, Vardy A, *et al.* Hardware architectures for successive cancellation decoding of polar codes [C]. *International Conference on Acoustics*, Prague, Czech Public. IEEE, 2011: 1665-1668.
- [18] Deng Y Y, Qing L B, Wang Z Y, *et al.* The research and implementation of polarization code decoding based on FPGA [J]. *Application of Electronic Technology*, 2017, 43(6): 37-40.
邓媛媛, 卿粼波, 王正勇, 等. 基于FPGA的极化码译码研究及实现 [J]. 电子技术应用, 2017, 43(6): 37-40.
- [19] Fossorier M P C, Mihaljevic M, Imai H. Reduced complexity iterative decoding of low-density parity check codes based on belief propagation [J]. *IEEE Transactions on Communications*, 1999, 47(5): 673-680.
- [20] Yuan B, Parhi K K. Low-latency successive-cancellation polar decoder architectures using 2 bit decoding [J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2014, 61(4): 1241-1254.
- [21] Nakassis A, Mink A. Polar codes in a QKD environment [C]. *Quantum Information and Computation XII*, Baltimore, USA. SPIE, 2014.
- [22] Wei Z C, Wang W L, Zhang Z, *et al.* Decoy-state quantum key distribution with biased basis choice [J]. *Scientific Reports*, 2013, 3(6147):2453.