基于 LDPC 的能源互联网安全通信研究

明阳阳，曹军威

清华大学信息技术研究院

摘要：能源互联网需要以先进的信息通信技术为支撑，实现对可再生能源的大规模消纳与利用，并通过高效的信息分析与决策，优化能源的使用效率，实现能源互联网的平稳高效运行。为此，能源互联网需要采集海量的信息。但这些信息大多具有一定的敏感性，需要对相关数据进行一定的保护，防止其在通信过程中泄露给非法的窃听者，避免给用户带来安全威胁或财产损失。除了传统的安全通信技术之外，本文建设性的提出一种基于 LDPC 编解码技术对相关信息进行保护的新方法，在少量增加编解码复杂度的情况下，实现对通信数据的有效保护。

关键字：能源互联网，安全通信，LDPC

Abstract: Energy Internet needs the support of advanced information and communication technologies (ICT), to realize the large scale absorbing and utilizing of renewable energy. And through high effective information analyzing and deciding ability, it can realize the steady and efficient running of Energy Internet. In order for that, Energy Internet needs to collect huge volume of information. But the information in Energy Internet has some extent of sensitivity, so the protection is necessary, to prevent it leaking to the illegal eavesdropper in the proceeding of communication, which can bring safety threat and property loss. Other than traditional safety communication technologies, this paper constructively advances a new protection method based on LDPC encoding and decoding to the information, in the price of slightly adding the complexity of encoding and decoding data, fulfilling the efficient protection of communication data.

Key Words: Energy Internet,safety communication,LDPC

1. 前言

基于能源系统在国家经济和社会正常运行的重要性，各国均非常重视对能源网络的安全性保护。但由于设施老化、设备容量接近极限等原因，传统能源网络（电网）出现区域性崩溃的事件并不少见。例如，美国和加拿大几次著名的电网瘫痪事件，大多由于某些重要发动机的故障，引起电网中发电设备的相继解列，导致了大范围的系统瘫痪。

通过有效利用信息通信技术，能源互联网的运行性能尤其是稳定性得到了极大的提升[1,2]，但这也给能源互联网的安全性带来了新的威胁。基于信息和能源的高度耦合，任何一方的故障或异常均可能影响到对方[3]，并可能进一步引发连锁反应，如多米洛骨牌一样，造成故障范围的不断扩大，并导致区域性的能源系统崩溃。基于此原因，能源互联网的信息网络极大可能成

为敌对势力或黑客的攻击对象。通过截获能源互联网的通信数据，可以实现对能源互联网的脆弱性分析，从而为黑客们的网络攻击提供突破口。同时，基于截获的能源用户的用能数据，能够非法获取用户的隐私，推断出用户的用能特征，甚至进一步了解用户的行动规律，从而为犯罪分子的作案提供帮助。这两种情况均会给社会经济的正常运行带来极大的危害，造成难以估量的损失。在此情况下，信息通信安全成为了能源互联网必须解决的关键性问题。

本文对基于 LDPC 码的能源互联网安全通信机制进行了研究。文章具体结构安排如下：第一章介绍了能源互联网通信安全的重要性；第二章将介绍传统信息通信安全技术；第三章将介绍能源互联网的安全特性；第四章介绍了 LDPC 编解码算法；第五章主要介绍基于 LDPC 的信息通信安全技术；第六章将介绍实验的主要过程及结果分析；第七章对全文进行总结。

2. 传统信息通信安全技术

对能源互联网通信系统的保护，首要工作是防止犯罪分子通过侦听等方式，获取有效的通信信息，并保证合法信息接收者能够从通信内容中获取有效数据。通常的通信安全保护技术包括：加解密技术、包头封装技术、安全多方技术和信息抖动（加扰）以及子采样技术，以上技术可以相互结合以进一步提高性能。

加解密技术[4,5]：数据加解密技术是目前普遍采用的信息保护技术。基于公私钥和加解密算法（如椭圆加密算法），可以实现对信息的加密、鉴权等功能。加解密技术目前已经相对成熟，但密钥的管理和分发仍是一项难题，需要耗费大量的计算、存储资源或建立公正有效的密钥管理机构。随着计算机处理能力的飞速提升，以及分布式算法的成熟，对公私钥的暴力破解能力不断加强，破解时间不断缩减，导致密码长度不得不随之增加，且编解码复杂度也大大增加。

包头封装技术：通过在原有报文之外，再嵌套一层相关协议的包头，导致信息截获者无法定位有效数据的起始位置，实现了对数据的有效保护。这建立在信息截获者无法了解报文结构的基础上。

安全多方技术：该类技术将数据划分为具有一定联系的数据片，或对数据片进行一定的处理后分别进行传输，当到达目的地时，通过对应的组合算法恢复出源信息。由于信息可以在不同路径或报文中传送，并经过了一定的处理。截获者即使获取部分报文也无法恢复出全部数据。其代表性方案有 SMART 算法[6]，PDA[7],iPDA[8]和 CDA[9]算法等。

信息抖动技术：通过在数据上添加一定概率分布的噪声，或者对数据值进行随机扰动，在保证大数据关联分析性能的同时，可以防止信息截获者获取有效的信息数据[10]，在一定程度上保护了用户的隐私。基于（成对）密钥的信息扰动也属于此类方法[11]。

子采样：通过子采样，减少数据的时间分辨率（例如从秒级减少为小时级别），在满足相关应用要求的同时，避免泄漏更多的用户信息。但对部分时间分辨率有严格要求的服务，子采样可能无法执行。

除了以上典型数据保护技术之外，网络编码技术[12]在一定上也可以保护数据安全，但其对通信拓扑具有一定的要求（可以还原解码相关数据），且需要与其它技术相结合（多路传输）以实现其功能。

以上技术均有各自的特点和优劣，也可以应用在能源互联网中。基于 LDPC 编解码技术[13,14]灵活、高效的特点，这里提出一种基于 LDPC 编解码的能源互联网信息安全保护技术。

3. 能源互联网的通信安全特性

目前的数据隐私保护研究一般基于无线传感器网络通信，在该通信场景下，数据传输节点在进行数据隐私保护的同时，也将完成数据集聚的功能，如最大、最小值聚合、平均值、方差等，以最大限度地保证数据安全，减少数据传输量，节省传感器的传输功率。

在能源互联网情况下，数据处理具有明显不同的特性，即隐私保护不必与数据聚集功能进行集合。一方面，能源互联网传感器所采集的数据大多互不相关，且所在的传感器网络(如家庭传感器网络)到达主干网的跳数并不多，其数据集聚功能可以转移到网关统一执行。而主干网络的稳定电源供应和嵌入式系统大大消减了节省通信能量消耗的需求。

另一方面，能源互联网将与大数据进行紧密结合以显著提高其运行性能，如典型的负荷预测、态势感知等。而大数据的产生将采集海量的原始数据，通过深度挖掘原始数据中的隐含特性为能源互联网运行创造价值，由此大大减少了对原始数据进行聚合处理的要求，聚合处理对能源互联网的整体性能并无多大影响。因此这里仅需对数据隐私进行保护处理。

4. LDPC 编解码

LDPC 即低密度（奇偶）校验码，该技术通过 tanner 图[15]对信息进行编解码，tanner 图一边是编码节点，另一边是校验节点，节点的值为 0 或 1。通过 tanner 图中不同类型节点的边连接可以形成校验矩阵，当部分节点的值存在错误时，基于相应的译码算法，可以恢复出相应节点的信息。为了保证译码的成功，tanner 图中的边连接具有一定的稀疏性，这也是低密度校验码的由来。

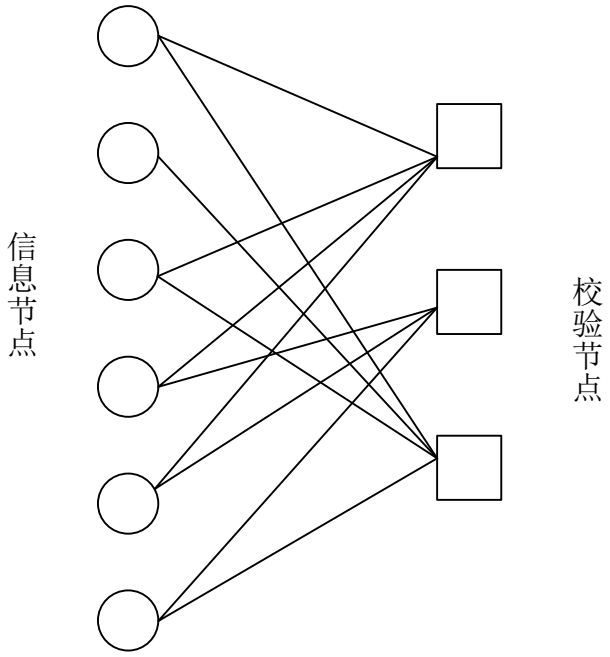

图 1 能源互联网 tanner 图

LDPC 有三种译码方式，硬判决[16]、软判决[17]和混合判决译码[18]。前者通过比特翻转或大数逻辑实现对节点的 0，1 值的直接判定。软判决这在译码中考虑了相关数据的置信度，该置信度既考虑了信源信息，也考虑了信道信息，通过置信传播技术和判决门限实现对节点值的分类。混合判决则结合了以上两种判决的优点，在硬判决译码的基础上，利用部分信道信息进行可信度计算。

在三种译码方式中，硬判决译码复杂度最低，但译码性能也最差。软判决译码复杂度最高，但译码性能也最好。混合判决的复杂度和性能居中。在本论文中，将采用软判决译码的方式。

LDPC 应用广泛，例如卫星通信，分布式视频编码[19]等，本文将其用于通信数据保护尚属首次。

5. 基于 LDPC 的信息通信安全技术

本文中假定相关数据已经经过了量化并形成了块状数据，一帧传送一块数据。且传输前已经经过交织等必要处理。

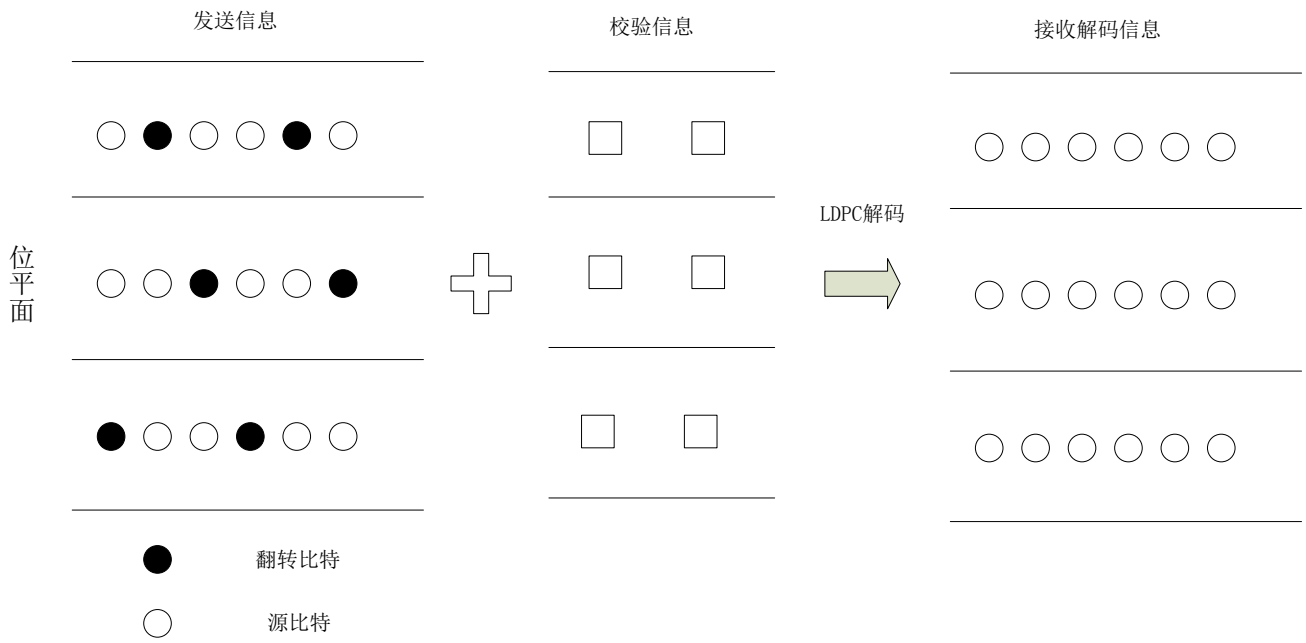

图 2 信息安全保护示意图

为了实现信息安全保护，根据量化阶数，对每一块数据进行 bit 面分层，即将每个数据的对应位比特提取出来并形成一个信息比特序列。根据该比特序列和对应的 tanner 图，生成校验比特序列。然后根据一定的概率，对每个信息比特序列的对应数据进行翻转（0 变成 1，1 变成 0），概率的选择与 tanner 图的解码能力有关。为了实现隐私保护效果的最大化，每个比特面的翻转位置需要相互错开。

对翻转后的序列，可以直接发送，或经过位平面重组后发送。在解码端，根据受损的信息比特序列和校验比特序列以及相关的误码概率（必要时可以考虑信道误码），通过 LDPC 解码，可以恢复出原有的信息。如果黑客仅获取信息比特序列，将无法恢复出有用信息。

为了保证信息安全，在传送信息比特序列和校验比特序列时，需要分开传送，对于信息序列，可以采用普通的传送信道，对于校验序列，可以采用与信息序列传输信道不同的传输路径，或通过安全信道传送，必要时，可以对其进行加密。通过这种方式，可以保证传输过程中有用的数据不被窃取，信息安全得到保障。

同时，需要对 tanner 图进行保护，可以将 tanner 图的结构数据进行加密，将其作为解码密钥传输到双方通信节点，从而实现有效保护。

基于 LDPC 为纠错码，所以这里可以将比特翻转与信道误码一起进行处理，系统得到一定的简化。

例如，在计算置信度时，需要同时考虑信源端主动改变产生的误码，也需要信道产生的误码，假定二者相互独立，可以得到以下的置信度计算公式。

$$belief(x) = \log p(source, channel \mid code = 1) \Big/ p(source, channel \mid code = 0)$$
$$= \log \frac{p(source \mid code = 1)}{p(source \mid code = 0)} * \frac{p(channel \mid code = 1)}{p(channel \mid code = 0)} \quad (1)$$

信源误码概率为翻转的比特数占块数据长度的比例。信道误码则可以通过通常的信道估计算法获得。

6. 实验过程与结果

这里假定为通过基带通信进行数据传送，码字类型采用双极性归零码，采集的不同类型数据将以帧为单位分别传送，数据采集频率根据实际情况确定。采集的数据可以在网关进行初步处理，在此情况下，由网关实现以上的数据安全保护；否则，由发送端进行以上数据保护。

为了实现基于 LDPC 的安全通信，主要需要研究 LDPC 码的解码能力。这里本文略去对具体通信过程的实验，仅对 LDPC 解码能力做初步研究。

实验具体分为两种情况，一种是不同平面分别进行编解码，另一种是将所有位平面的数据链接在一起，统一进行 LDPC 编解码保护。实验将计算不同翻转比特数量情况下，解码所需的校验位数。

解码比特数的计算基于 LDPCA 算法[20]，即先传输部分校验位进行解码，如果解码不成功，则增量传送校验位数，同时对 tanner 图进行相应修改，直到解码成功。

假定每个位平面包含 384 个比特，共有四个位平面。因此，下面就 384 比特和 1584 比特的 LDPC 解码性能分别进行仿真。

解码过程中，暂时只考虑信源置信度，尽管信道置信度可以很容易的加入其中。

对于翻转比特数，384 比特的情况选择从 1 到 100 个比特进行翻转，1584 比特的情况选择从 1 到 400 个比特进行翻转。根据每个翻转比特数，分别进行 25 次仿真。每次仿真随机选择比特翻转位置（服从均匀分布）进行编解码处理，选取所需的最大校验比特数（比例值）为初步仿真结果。

初步仿真结果具有一定的波动性，有时不满足单调递增的性质，为此，需进一步进行单调化处理。即从起始位置开始，如果当前校验比特数比例值比前一个值小，则将当前值设为前一比特值，如此直到数据结束或校验比特数比例达到 1。

具体仿真结果如下：

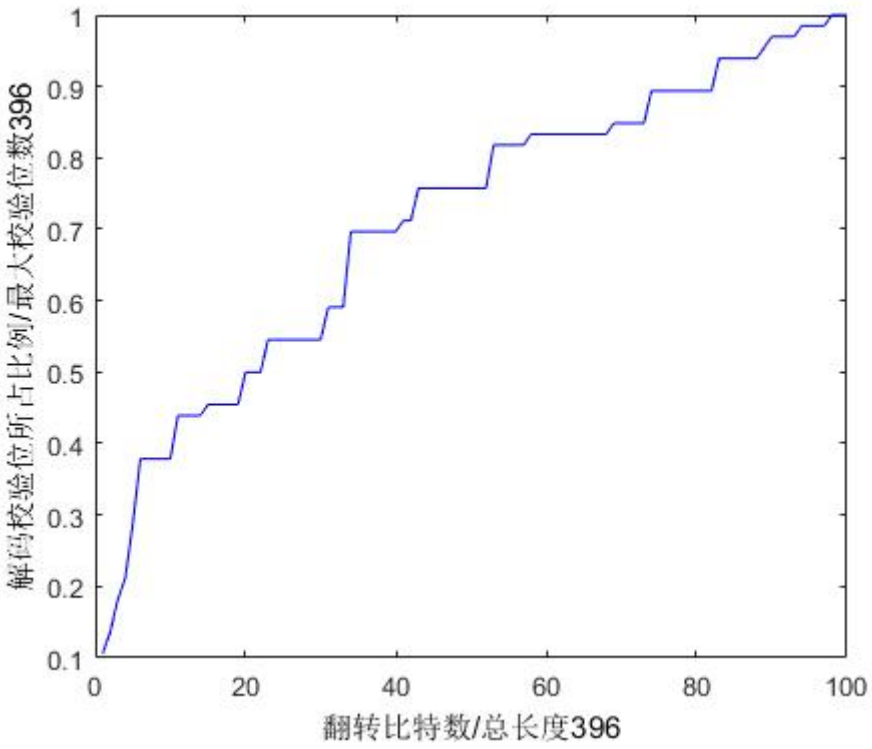

图 3 396 比特的编解码结果

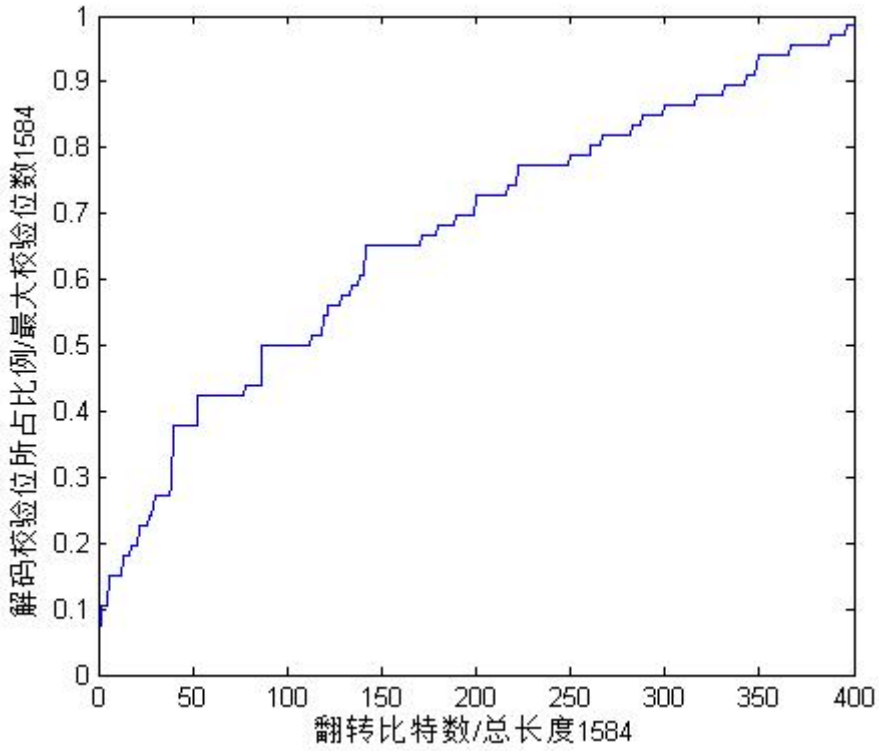

图 4 1584 比特的编解码结果

从图 3、4 中可以看出 1584 比特的 LDPC 解码结果略好于 396 比特的 LDPC 解码结果，这与预期的分析一致。比特数越大，翻转比特的分布就越均匀，特殊形状的比特分布出现的机会

也就越小（如形成环状拓扑），解码效果自然也就越好

当进行翻转比特数的选择时，过少的翻转比特数安全保护能力较弱，而翻转比特数过大，造成数据量的大幅增长，且有可能需要传输所有源比特，达不到安全保护的目的。初步选择翻转概率为 9%-16%，对应的校验比特数比例约为 0.55-0.8。对于 N 个比特平面，数值发生改变的信号比例最大为 N*翻转概率。

如果需要进一步加大安全保护能力（增加翻转比特概率，且校验比特数比例小于特定值），可以通过对信息位序列末尾添零，并扩展相应的 tanner 图实现。

如果需要规范反转比特数确定方式，可以采用线性优化算法，即，

$$bit\_num = \min(R1 - \lambda * R2)$$

$$\lambda \geq 0 \tag{2}$$

式中，$R1$ 代表翻转比特数，$R2$ 代表所需校验比特数，λ 为权重比例。通过调整权重，可以在信息安全保护效果和信息传输量中进行折中。

7. 总结

通过以上步骤，本文实现了一种基于 LDPC 编解码的通信安全保护算法，基于该算法，可以防止数据在传输过程中受到非法窃听。将其应用于能源互联网中，可以保证所采集数据的安全性，并有效的防止了信道干扰所产生的误码。

本算法在本质上是分布式编解码算法[21]的一种变形，比特翻转后的信息为与源信息相关的信息，而校验信息则为边信息，通过二者的结合，实现了对相关信息的隐私保护。

本文的下一步工作为将以上机制扩展为 LDPCA 码（累积低密度校验码），当出现解码失败时，可以实现对校验数据的增量传送，从而节省数据流量。

8. 参考文献

[1] 曹军威，杨明博，张德华，明阳阳，孟坤. 能源互联网——信息与能源的基础设施一体化. 南方电网技术，vol. 8，2014：1-10.

[2] 王继业，孟坤，曹军威，程志华，高灵超. 能源互联网信息技术研究综述. 计算机研究与发展，vol. 52，2015：1109-1126.

[3] DT Nguyen, Shen Yilin, MT Thai. Detecting Critical Nodes in Interdependent Power Networks for Vulnerability Assessment. IEEE Transaction on Smart Grid, Vol. 4, No.1, 2013:151-159.

[4] Rabindra Bista, Kim Hee-Dae and Jae-Woo Chang. A New Private Data Aggregation Scheme for Wireless Sensor Networks. 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010), 2010:273-280.

[5] Josep Domingo-Ferrer. A Provably Secure Additive and Multiplicative Privacy Homomorphism.Information Security, International Conference, Isc Sao Paulo, Brazil, September 30-october,2002:271-283.

[6] 王安琪. 适用于 WSN 的数据融合隐私保护算法研究.南京：南京邮电大学（硕士），2012.

[7] Wenbo He, Xue Liu, Hoang Nguyen, Klara Nahrstedt, Tarek Abdelzaher. PDA: Privacy-preserving Data Aggregation in Wireless SensorNetworks.Infocom IEEE International Conference on Computer Communications IEEE, Vol. 28, No.6, 2007:2045-2053.

[8] Wenbo He, Hoang Nguyen, Xue Liu, Klara Nahrstedt, Tarek Abdelzaher. iPDA: An Integrity-Protecting Private DataAggregation Scheme for Wireless Sensor Networks. Military Communications Conference, 2008:1-7.

[9] Joao Girao, Dirk Westhoff, Markus Schneider. CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks. IEEE 2005: 3044-3049.

[10] Alexandre Evfimievski, Ramakrishnan Srikant, Rakesh Agrawal, Johannes Gehrke. Privacy preserving mining of association rules. Information Systems 29, 2004: 343–364.

[11] Mauro Conti, Lei Zhang, Sankardas Roy, Roberto Di Pietro, Sushil Jajodia, and Luigi Vincenzo Mancini. Privacy-preserving Robust Data Aggregation in Wireless Sensor Networks. Security & Communication Networks, Vol. 2, No.2, 2009:195-213.

[12] 杨林, 郑刚, 胡晓惠. 网络编码的研究进展. 计算机研究与发展, Vol. 45, No.3, 2008:400-407.

[13] Seongkwon Jeong, Jaejin Lee. Iterative LDPC–LDPC Product Code for Bit Patterned Media. IEEE Transactions on Magnetics, Vol. 53, No. 3, 2017: 1-4

[14] Hua Li, Hong Ding, Linhua Zheng. An escaping scheme for gradient descent bit-flipping decoding of LDPC codes. 2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), 2016:2026-2030.

[15] 王单，LDPC 码编译码算法研究. 西安：西安电子科技大学（博士），2006.

[16] 邵湖, 赵恒凯. 基于改进型比特翻转准则的 LDPC 码硬译码算法.电子测量技术, Vol. 34, No.3, 2011:25-28.

[17] 甘毅. LDPC 码编译码算法研究. 南京：南京理工大学（硕士）， 2010.

[18] 陈紫强, 欧阳缮, 李民政, 臧岚, 肖海林. 一种基于改进线性规划的 LDPC 码混合译码算法.电路与系统学报，Vol.18, No.1, 2013: 107-112.

[19] Artigas X, Ascenso J, Dalai M, et al., The Discover Codec: Architecture, Techniques and Evaluation, Picture Coding, 2007, page(s):1-4.

[20] 李静, 王尊亮, 李学明.LDPCA 在分布式视频编码码率控制中的应用. 世界科技研究与发展, Vol.30, No.6, 2008:739-742.

[21] 胡涛,李峤,周宇. 基于信源编码的数据融合隐私保护技术.科技视界, 2016: 178, 235.