IEEE 信息论学会广州分会季报

IEEE INFORMATION THEORY SOCIETY
GUANGZHOU CHAPTER NEWSLETTER

第七期, 2023 年 3 月 No. 7, Mar. 2023

主编序语

各位学者：

本期《分会季报》探讨了极化码研究的新动向，它可有效提升McEliece加密系统的信息传输速率和多址接入通信系统的吞吐率；面向6G通信网络，介绍了可支持Tbps吞吐率的快速极化码构造和性能优异的U-UV结构码。8月2-5日，“IEEE东亚信息论学校”在深圳人才研修院成功举办；8月11日，“面向未来无线网络的信息论与编码研讨会”在IEEE/CIC中国国际通信大会期间成功举办。华为黄大年茶思屋科技网站录制了“茶思屋三人行”畅谈香农信息论的发展和意义。

陈立

From the Editor-in-Chief

Dear Chapter Members,

This issue discusses some new directions of polar coding research. It is shown that polar codes can increase the information rate of McEliece's crypto systems and the throughput of multiple access communication systems. For 6G communication networks, this issue also introduces the fast construction of polar codes that can support Tpbs throughout and the good performing U-UV structural codes. From Aug. 2 to 5, the IEEE East Asian School of Information Theory took place in Shenzhen Institute for Talents Development. On Aug. 11, the Workshop on Information Theory and Coding for Future Wireless took place during the IEEE/CIC International Conference on Communications in China. Huawei Huang Danian Chaspark produced the Chaspark Trialogue on the progress and impact of Shannon Information Theory.

Li Chen

来稿请包含中英文题目、联系人、联系方式、拟投稿栏目，正文可以是中文或英文，不超过 800 字。
The submission should include the title in both Chinese and English, author contacts, and the column that the article belongs to. Content of the article can be both in Chinese or English, and is limited to 800 words.

投稿邮箱/Submission email：itguangzhou@163.com

目录 •Table of Content •

最新结果 • RECENT RESULTS •

交流活动 • RESEARCH ACTIVITIES •

新锐风采 • NEW TALENTS •

最新结果 • RECENT RESULTS •

基于极化码的改进 McEliece 加密方案
Improved Encryption Scheme Based on McEliece Scheme Using Polar Codes

夏冰，李金升，刘凌
深圳大学
Bing Xia, Jinsheng Li, Ling Liu
Shenzhen University.
2110276171@email.szu.edu.cn; lijinsheng2020@email.szu.edu.cn; liulingcs@szu.edu.cn

The rapid development of quantum computing threatens the traditional coding field, and the code-based encryption schemes are still considered to be resistant to quantum computing. Polar codes, introduced by Arıkan [1], have good error correction ability, low encoding and decoding complexity. Therefore, polar codes are applied to code-based encryption schemes to achieve better efficiency.

This paper originates from the direct improvement of McEliece scheme [2]. In [3], the authors use the added error vector to carry additional information bits to increase information rate. However, the system security was less guaranteed.

The new variant of the famous McEliece scheme in this work replaces the “XOR” operation between the codeword and noise vector with addition in the real number filed, i.e., a two-user multiple access channel (MAC) is formed in the encryption. Theoretically, the information rate can be increased to 1.5 bits/channel use.

A two-user MAC communication setup is depicted in Fig. 1.

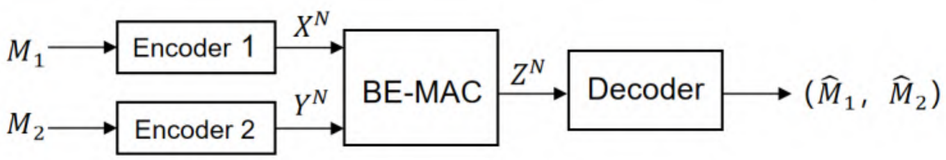


Fig.1 A two-user MAC communication setup.

According to the recent result for two-user MAC [4], when there is no time-sharing, the two-user decoding must obey the monotone chain rules to achieve a specific rate pair. And different expansions may affect the rate allocation of each user. Therefore, one may choose an appropriate decoding sequence according to a rate pair, and take the decoding sequence as the secret key since there are also different expansions to make the same rate pair.

According to the above knowledge, we proposed the following scheme:

Private Key: it consists of a set $\{G_1, S_1, P_1, G_2, S_2, P_2, b^{2N}\}$, where G_1 and G_2 are $K_1 \times N_1$ and $K_2 \times N_2$ generation matrices of polar code respectively, S_1 and S_2 are arbitrary $K_1 \times K_1$ and $K_2 \times K_2$ binary nonsingular matrices respectively, P_1 and P_2 are $N_1 \times N_1$ and $N_2 \times N_2$ random permutation matrices respectively, where $P_1 = P_2 = P$. P is $N \times N$ permutation matrix. And N_1 and N_2 are both equal to N. b^{2N} is the sequence of decoding corresponding to the monotone rate allocation scheme [4].

Public Key: it is composed of a set $\{G_{\mathrm{pub1}}, G_{\mathrm{pub2}}\}$, where $G_{\mathrm{pub1}} = S_1 G_1 P_1$ and $G_{\mathrm{pub2}} = S_2 G_2 P_2$. G_{pub1} and G_{pub2} are $K_1 \times N$ and $K_2 \times N$ binary encryption matrices respectively.

Encryption: Given matrix G_{pub1}, G_{pub2}, message m_1, m_2, and decoding path b^{2N}, the sender computes formulas as follows:

$$X = m_1 \times G_{\text{pub1}}$$
$$Y = m_2 \times G_{\text{pub2}}$$
$$Z = X + Y$$

Decryption: According to Z and P, the receiver can calculate ZP^{-1}.

$$ZP^{-1} = m_1 S_1 G_1 + m_2 S_2 G_2$$

Then he uses a 2-user MAC SC-decoder based on the monotone chain rule [4] to obtain $m_1 S_1$ and $m_2 S_2$. Finally, he can recover m_1 and m_2.

Table I

Comparison of key lengths.

Scheme	Code class	Parameter (unit: bits)	M_{pub} (unit: KB)	M_{sec} (unit: KB)
McEliece Scheme (BSC (0.05))	Polar	$N_M = 1024, K_M = 512,$	64	192
		$N_M = 512, K_M = 240,$	15	47
		$N_M = 256, K_M = 112,$	3.5	11.5
The proposed scheme	Polar	N=512, R_1'+R_2'=1.305,	41.76	133.13
		N=256, R_1'+R_2'=1.275,	10.2	32.77
		N=128, R_1'+R_2'=1.23,	2.46	8

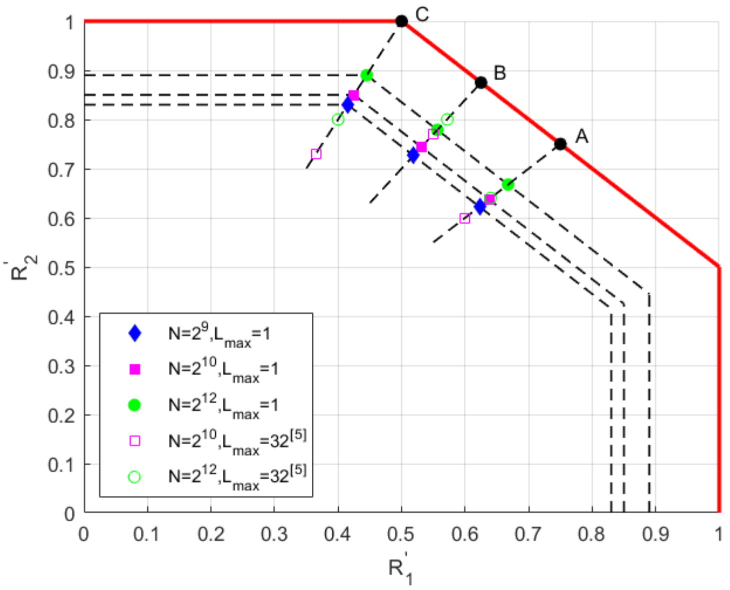


Fig. 2 Operating rates for the New Scheme at BLER = 10^{-4}.

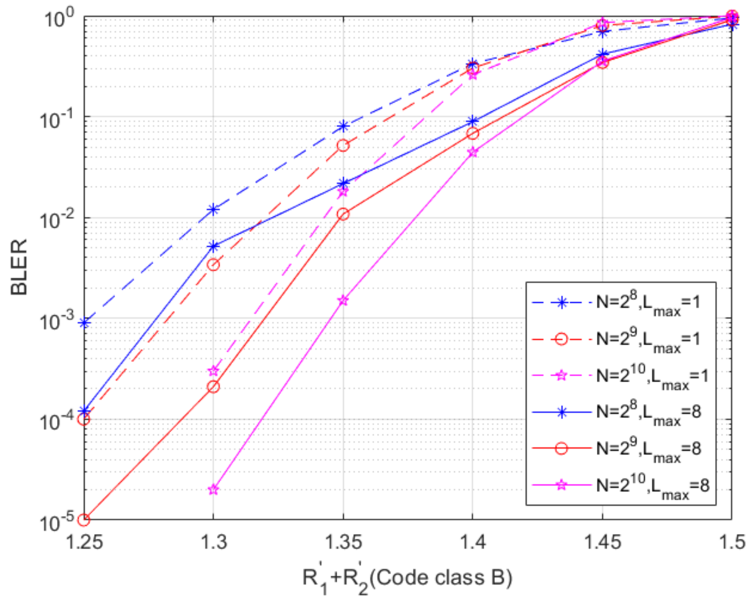


Fig. 3 BLER performance for the New Scheme w.r.t. sum rate.

Table I gives the comparison of key lengths between the two schemes. Fig. 2 shows that operating rates for the new scheme at BLER = 10^{-4}. The points in Fig. 2 compared with the points in [5], which shows that our results are better than theirs. Since we choose right decoding order, information set and frozen set, the decoding order obeys monotone chain rules. Therefore, our decoding achieves the rate pair of dominant face. The three points on the red line, A, B, and C, represent three different rate pairs (0.75, 0.75), (0.625, 0.875) and (0.5, 1), respectively. Fig. 3 shows BLER for the legitimate receiver w.r.t. sum rate for code class B in Fig. 2. We use a successive-cancellation MAC decoder and a successive-cancellation list MAC decoder to get the results. L_{max} denotes the maximum number of paths for decoding.

This paper proposed a new encryption scheme based on McEliece scheme using polar codes. Compared with the original McEliece scheme, where N_M = 1024, we increase the information rate to 1.305 bits/channel use with N = 512. In addition, the search space of proposed scheme is approximately $2^{5.7\times10^5}$ times that of McEliece scheme at N = 1024 when they are attacked by brute force. Compared with the original scheme, this scheme can transmit twice as much secret message when they consume the same public key size. In the future, we can consider adding artificial noises to improve security of the scheme.

References

[1] E. Arıkan, “Channel polarization: A Method for Constructing Capacity Achieving Codes for Symmetric Binary-input Memoryless Channels,” *IEEE Trans. Inf. Theory*, vol. 55, pp. 3051–3073, Jul. 2009.

[2] R. J. McEliece, “A Public-key Cryptosystem Based on Algebraic Coding Theory,” *DNS Progress Rep.*, Jet Propulsion Laboratory, CA, Pasadena, pp. 114-116, 1978

[3] H. M. Sun, “Improving the Security of the McEliece Public-Key Cryptosystem,” *Asiacrypt*, 1998.

[4] E. A. Bilkent, “Polar Coding for the Slepian-Wolf Problem Based on Monotone Chain Rules,” *IEEE Int. Symp. Inf. Theory (ISIT)*, in Proc., pp. 566-570, 2012.

[5] S. Önay, “Successive Cancellation Decoding of Polar Codes for the Two-user Binary-input MAC,” *IEEE Int. Symp. Inf. Theory (ISIT)*, in Proc., pp. 1122-1126, 2013.

最新结果 • RECENT RESULTS •

抗时隙擦除的极化时隙随机接入方法
Polar Slotted ALOHA over Slot Erasure Channel

牛凯，张志军
北京邮电大学
Kai Niu, Zhijun Zhang
Beijing University of Posts and Telecommunications.
niukai@bupt.edu.cn; zjzhang@bupt.edu.cn

With the blooming of uncoordinated wireless machine-type communications and the internet of things communication paradigms, efficient grant-free medium access control (MAC) protocols have attracted remarkable attention [1-3]. In these communication scenarios, the MAC protocols support massive low-power devices uncoordinated transmission to a common base station (BS) simultaneously with higher energy and spectral efficiency. Due to its simplicity and limited signal processing demand feature, the slotted ALOHA and its enhanced variants, such as contention resolution diversity slotted ALOHA, irregular repetition slotted ALOHA (IRSA) and coded slotted ALOHA (CSA) scheme (as a generalization of IRSA scheme) have been investigated. However, in the wireless transmission scenarios, the transmitted packets within the CSA scheme are often corrupted by the erasure channels, slot erasure channel (SEC) and packet erasure channel [4-6]. In [5], we derived the upper bound on load-threshold performance of CSA over SEC and that over PEC, respectively. The numerical results are shown in Fig.1 and which indicate that the asymptotic throughput of the CSA scheme over SEC is always worse than that over PEC with the identical transmission rate and erasure probability.

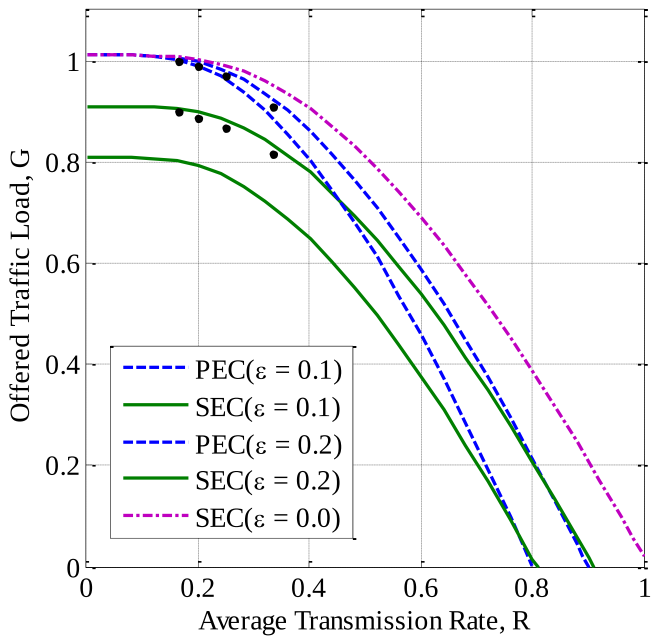


Fig. 1 The upper bounds on load-threshold of CSA with erasure probability ε = 0.1 or ε = 0.2, and target PLR = 0.01.

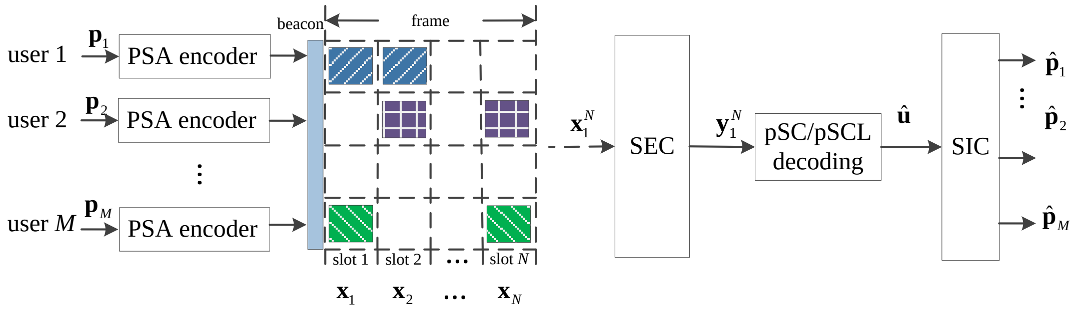


Fig.2 The PSA system model over slot erasure channel.

Polar Slotted ALOHA: Inorder to reduce the throughput loss caused by the SEC, a polar slotted ALOHA (PSA) framework is established [6], where the access process is decomposed into two-stage and jointly optimized under the slot polarization idea. The PSA system model is shown in Fig.2, and its random access and detection procedure can be described as follows:

1) PSA random access procedure: Based on the packet-oriented operation, we demonstrate that the symmetric SECs polarize under a recursive packet-based slot polarization transform (SPT) similar to Arıkan's [7], and prove that slot polarization phenomenon exists in SEC synthetic MAC channels [6]. Under the slot polarization idea, a PSA framework for the SEC is established where the random access is decomposed into a two-stage procedure. In the first stage, guided by the slot polarization, a slot subset is constructed at each active user side and the BS side. With an irregular degree distribution, each active user randomly selects slots within the slot subset to transmit the packet replicas. In the second stage, based on the SPT, the slotted packets of the slot subset are encoded by using a packet-level polar code. Each transmitted packet is encoded at each active user side. After receiving a beacon broadcasted from BS, each user sends the encoded packets simultaneously over slot erasure channel to form a transmission frame.

2) Multi-user detection procedure: As a generalization of Arıkan's SC decoder to the SEC case, a packet-oriented SC (pSC) and pSC list (pSCL) decoding algorithms are developed. At the BS side, the pSC/pSCL decoding algorithm is firstly performed to overcome the corruption caused by the SEC. And then, the success interference cancellation procedure is executed to recover the packet. As two critical issues affect the throughput of the PSA scheme, we optimize the degree distribution of active user nodes and derive the upper bound of the polar code rate. Given a maximum degree and an average transmission rate, the degree distribution is constrained by two linear equations. Therefore, the optimized irregular degree distribution can be found by searching the maximum within all the feasible solutions' traffic load threshold. And then, an upper bound of the polar-code rate for the PSA scheme is derived by using the optimized traffic load threshold. In the non-asymptotic regime of PSA schemes, the selection of the rate of packet-level polar code R_p is also affected by the finite-length pSC decoding performance. Therefore, we derive an upper and lower bounds of the pSC decoding for frame-error rate. Under different erase probabilities of the SEC, the pSC decoding performance curves and their upper and lower bounds are shown in Fig. 3. When ε increases from 0.1 to 0.3, it can be seen that the lower bound is getting looser, but the upper bound is getting tighter. However, in general, the upper/lower bound is still relatively loose. How to find a tighter bound of R_p, especially the bound of pSCL decoding for the medium and small N case, is a very interesting practical issue. Clearly, the perfect decoding performance of the pSC decoding is affected by the rate R_p. For ε = 0.1 and N = 1024, it is showed that the pSC decoding is in a perfect status without any decoding errors when R_p is less than around 0.8.

Results: The PSA schemes' throughput and packet loss rate are evaluated for the SECs under different parameters. Fig. 4 shows the throughput curves of the PSA and IRSA for the SEC with ε = 0.1 and the frame with N = 1024 slots. In Fig. 5, we make a comparison with respect to the packet-loss rates (PLRs) of the IRSA schemes and that of the PSA schemes. Simulation results indicate that the proposed PSA scheme can achieve an improved throughput over the IRSA scheme for the SEC. Moreover, compared to the IRSA scheme based on the same distribution, the results also show that the proposed PSA scheme is with a lower PLR error floor.

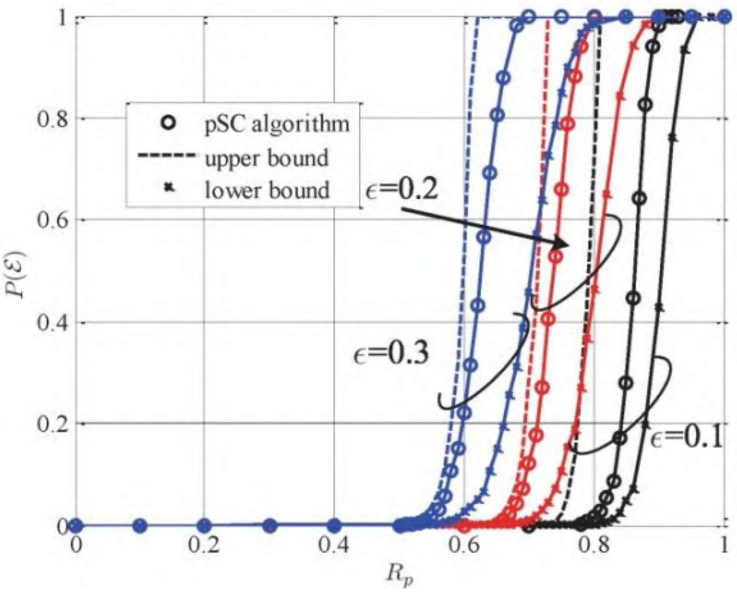


Fig. 3 The upper and lower bounds of frame-error rate for the pSC decoding versus the polar-code rate R_p over SECs under different slot erasure rates ε = 0.1, 0.2, 0.3 and N = 1024.

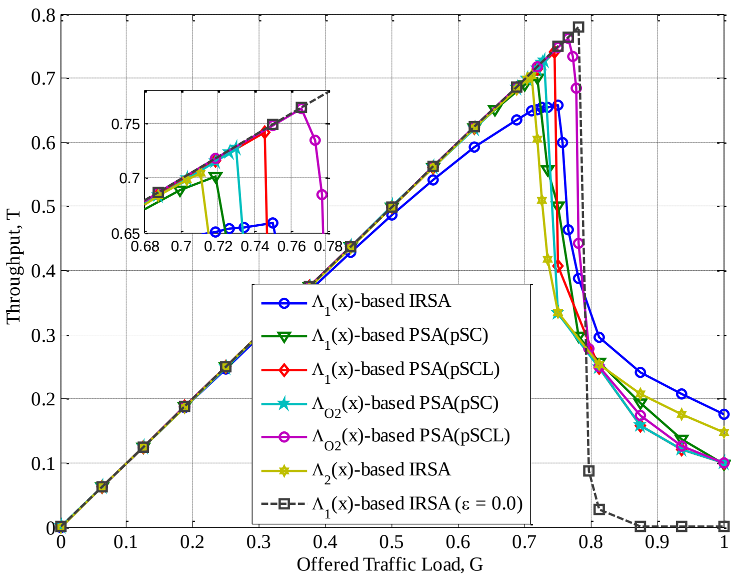


Fig. 4 The throughput T versus offered traffic load G of PSA schemes for the SEC with ε = 0.1 and N = 1024

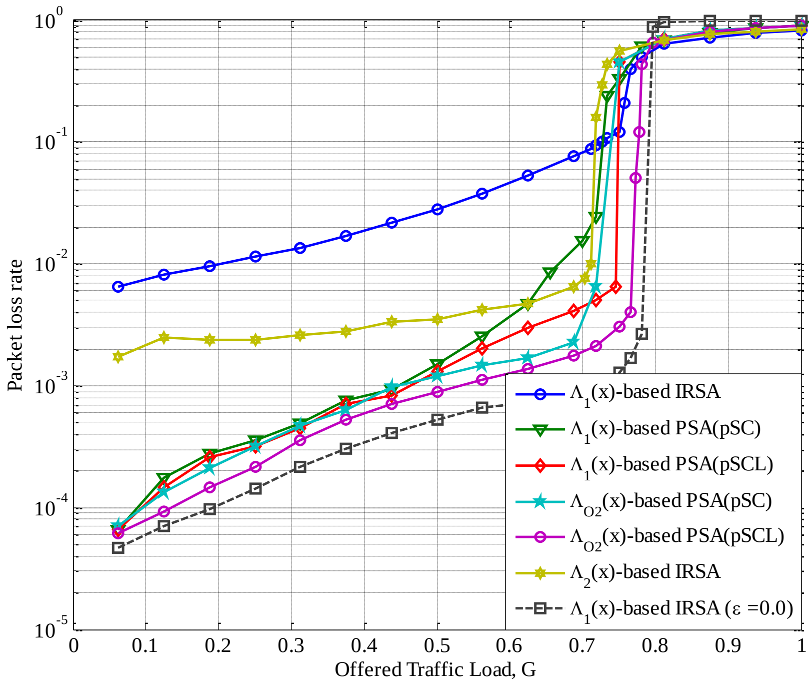


Fig. 5 Packet loss rates versus offered traffic load G for the PSA schemes of the SEC with ε = 0.1 and N = 1024.

Reference:

[1] E. Paolini, C. Stefanovic, G. Liva and P. Popovski, "Coded Random Access: Applying Codes on Graphs to Design Random Access Protocols," *IEEE Commun. Magazine*, vol. 53, no. 6, pp. 144–150, Jun. 2015.

[2] O. Ordentlich and Y. Polyanskiy, "Low Complexity Schemes for the Random Access Gaussian Channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aachen, pp. 2528-2532, 2017.

[3] Y. Wu, X. Gao, S. Zhou, W. Yang, Y. Polyanskiy and G. Caire, "Massive Access for Future Wireless Communication Systems," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 148-156, Aug. 2020.

[4] Z. Sun, Y. Xie, J. Yuan and T. Yang, "Coded slotted ALOHA for erasure channels: Design and throughput analysis," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 4817–4830, Nov. 2017.

[5] Z. Zhang, K. Niu and J. Dai, "Performance Bounds of Coded Slotted ALOHA Over Erasure Channels," *IEEE Trans. Veh. Technol.*, vol. 71, no. 11, pp. 12338-12343, Nov. 2022.

[6] Z. Zhang, K. Niu, J. Dai and C. Dong, "Polar-slotted ALOHA over Slot Erasure Channel," *IEEE Trans. Veh. Technol.*, early access, 2022.

[7] E. Arıkan, "Channel Polarization: A Method for Constructing Capacity-achieving Codes for Symmetric Binary-input Memoryless Channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

最新结果 • RECENT RESULTS •

用于Tbps 吞吐率通信的快速极化码
Fast Polar Codes for Terabits-Per-Second Throughput Communications

童佳杰[1]，王献斌[1]，张其蕃[2]，张华滋[1,2]，李榕[1]，王俊[1]
1 华为技术有限公司，2 华为加拿大技术有限公司
Jiajie Tong[1], Xianbin Wang[1], Qifan Zhang[2], Huazi Zhang[1,2], Rong Li[1], Jun Wang[1]
1 Huawei Technologies Co. Ltd., China, 2 Huawei Technologies Canada Co. Ltd., Canada.
tongjiajie@huawei.com; wangxianbin1@huawei.com; qifan.Zhang@huawei.com;
zhanghuazi@huawei.com; lirongone.li@huawei.com; justin.wangjun@huawei.com

Higher throughput has always been a primary targ*et al.*ong the course of mobile communications evolution. Driven by high data rate applications such as virtual/augmented reality (VR/AR) applications, the sixth generation wireless technology (6G) requires a peak throughput of 1 Tbp/s [2]. This is roughly a 50× ∼ 100× increase over the 10 ∼ 20 Gbp/s target throughput for 5G standards.

To support such a high data rate, we need to propose new physical layer design to further reduce implementation complexity, save energy, and improve spectral efficiency. This is particularly true when the peak throughput requirement is imposed on a resource constrained (limited processing power, storage, and energy supply etc.) device. Since channel coding is well-known to consume a substantial proportion of computational resources, it poses a bottleneck for extreme throughput. To this end, channel coding is one of the most relevant physical layer technologies in order to guarantee 1Tbp/s peak throughput for 6G.

Polar codes, defined by Arıkan in [3], are a class of linear block codes has been selected as the channel coding scheme for 5G NR. Successive cancellation (SC) is a basic decoding algorithm for polar codes.

This paper introduces a novel polar code construction method, coined as “fast polar codes”, to facilitate parallelized processing at an SC decoder. In contrast to some existing decoding-only techniques, we take a joint encoding-decoding optimization approach. Similar to existing methods, our main ideas could be better understood from the binary tree traversal perspective. They are (a) pruning more subtrees, (b) replacing some non-prunable subtrees with other fast-decodable short codes of the same code rates and then prune these “grafted” subtrees, (c) eliminating the remaining non-prunable subtrees by altering their code rates. As seen, both (b) and (c) involve a modified code construction. Consequently, we are able to fast decode any subtree (short code) of a certain size, without sacrificing parallelism.

The algorithmic contributions are summarized below:

1) Four new fast decoding modules are used to decode nodes with code rates $\{\frac{2}{M},\frac{3}{M},\frac{M-3}{M},\frac{M-2}{M}\}$. Here $M = 2^s$ is the number of leaf nodes in a subtree, where s is the stage number. These nodes are called dual-REP (REP-2), repeated parity check (RPC), parity checked repetition (PCR), dual-SPC (SPC-2) nodes, respectively. More importantly, these modules reuse existing decoding circuits for repetition (REP) and single parity check (SPC) nodes.

2) For medium-code-rate nodes that do not natively support fast decoding, we graft two extended BCH codes to replace the original outer polar codes. BCH codes enjoy good minimum distance and natively support efficient hard-input decoding algorithms, thus strike a good balance between performance and latency. The extension method is also customized to enhance performance.

3) We propose to re-allocate the code rates globally, such that all nodes up to a certain size support the above mentioned fast decoding algorithms. This approach completely avoids the traversal into certain “slow” nodes.

For code length N = 1024 and code rate R = 0.875, the proposed fast polar codes enable parallel decoding of all length-16 nodes. The proposed decoding algorithm reduces 55% node visits and 43.5% edge visits from the original polar codes, with a cost of within 0.3 dB performance loss. Two types of decoder hardware are designed to evaluate the area efficiency and energy efficiency.

Table I
Comparison with high throughput polar decoder.

Implementation	This Work (Unroll)	This Work (Recursive)	[4]	[5]	[6]
Construction	Fast-Polar	Fast-Polar	Polar	Product-Polar	Polar
Decoding Algorithm	Fast-SC	Fast-SC	SC	PDF-SC	OPSC
Code Length	1024	1024	32768	16384	1024
Code Rate	0.875	0.875	0.864	0.864	0.83
Technology	FPGA Converted to 16nm			In TSMC 16nm	
Clock Frequency (GHz)	1.20	1.00	1.00	1.05	1.20
Throughtput/Coded-bit (Gbps)	1229	25.6	5.27	139.7	1229
Area/Layout (mm^2)	0.30	0.045	0.35	1.00	0.79
Area Eff/Coded-bit (Gbps/mm^2)	4096	561	15.1	139.7	1555
Power (mW)	784	30.9	-	94	1167
Energy (pJ/bit)	0.63	1.21	-	0.67	0.95

We designed two types of hardware architectures to verify the performance, area efficiency and energy efficiency.

Recursive Decoder: It supports flexible code length and coding rates of mother code length N from 32 to 1024 with the power of 2. With rate matching, flexible code length with $0 < N \leq 1024$ and code rate with $0 < R \leq 1$ are supported. The $f_{+/-}$ functions in nodes are processed by single PE (processing element) logic, and one decision module to support all 9 patterns. The decoder processes one packet at a time.

Unrolled Decoder: It only supports a fixed code length and code rate. In our architecture we hard coded code length N = 1024, and code rate R = 0.875. This fully unrolled pipelined design combines exclusive dedicated PEs to process each $f_{+/-}$ function in the binary tree. Same to the decision modules that 21 dedicated node specific logic are implemented to support 21 nodes patterns. With 25 packets simultaneously decoding, thanks to the unrolled fully utilization of processing logic and storage, this decoder provides extreme high throughput with high area efficiency and low decoding energy.

The key performance indicators (KPIs) are reported in this section. First of all, we evaluate the area efficiency using equation

$$\text{AreaEff (Gbps/mm}^2) = \frac{\text{InfoSize(bits)}}{\text{Latency(ns)} \times \text{Area(mm}^2)} \ .$$

The recursive decoder takes 40 clock cycles to decoder one packet under fast polar code construction with code length N = 1024, and code rate R = 0.875. Thus the throughput is (1024 bits × 1 GHz)/40 cycles = 25.6 Gbps for coded bits, and ((1024 × 0.875) bits × 1 GHz)/40 cycles = 22.4 Gbps for information bits. Converting to 16nm process, the area efficiency for coded bits is 561 Gbps/mm^2.

The unrolled decoder takes 25 clock cycles to decoder one packet. It is fully pipelined, meaning a new packet of decoded results would be generated continuously every cycle after the first 25 clock cycles of the first packet processing time. The throughput is thus 1024 bits × 1.2 GHz = 1229 Gbps for coded bits, and (1024 × 0.875) bits × 1 GHz = 1075 Gbps for information bits. Converting to 16nm process, the area efficiency for coded bits is 4096 Gbps/mm^2.

We further evaluate the power consumption and decoding energy per bit through a simulation in which 200 packets are decoded. The process, voltage and temperature (PVT) condition of evaluation is TT corner, 0.8V and 20$^{\circ}C$, and the resulting of recursive decoder's power consumption is 30.9 mW, and decoding each bit costs 1.21 pJ of energy on average; while the unrolled decoder's power consumption is 784 mW, and decoding each bit costs 0.63 pJ of energy on average.

We also compare the decoding throughput, area efficiency and power consumption with several high-throughput decoders in literature, and present the results in Table I. From the KPIs, we conclude that unrolled decoders are more suitable for scenarios requiring extremely high throughput but only support fixed code length and rate; recursive decoders are much smaller, which are better for resource constrained devices, and at the same time provides flexible code rates and lengths - a desirable property for wireless communications.

These results indicate that fast polar codes can meet the high-throughput demand in the next-generation wireless communication systems. And the recursive hardware design and unrolled hardware design can be adopted to satisfy different system requirements.

References

[1] J. Tong, X. Wang, Q. Zhang, H. Zhang, R. Li, J. Wang, and W. Tong, "Fast Polar Codes for Terabits-per-second Throughput Communications," Available on arXiv https://arxiv.org/abs/2107.08600.

[2] W. Saad, M. Bennis, and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *IEEE Network*, 2019.

[3] E. Arıkan, "Channel Polarization: A Method for Constructing Capacityachieving Codes For Symmetric Binary-input Memoryless Channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051-3073, Jul. 2009.

[4] X. Liu, Q. Zhang, P. Qiu, J. Tong, H. Zhang, C. Zhao, J. Wang, "A 5.16Gbps Decoder ASIC for Polar Code in 16nm FinFET," *2018 15th Int. Symp. Wireless Commun. Systems (ISWCS)*, Lisbon, pp. 1-5, 2018.

[5] J. Tong, X. Wang, Q. Zhang, H. Zhang, S. Dai, R. Li, and J. Wang, "Toward Terabits-per-second Communications: A High-Throughput Implementation of GN-Coset Codes," *IEEE Wireless Communs. and Networking Conf. (WCNC)*, pp. 1-6, 2021.

[6] A. Süral, E. G. Sezer, E. Kolagasıoglu, V. Derudder, K. Bertrand, "Tb/s Polar Successive Cancellation Decoder 16nm ASIC Implementation," Available on http://www.polaran.com/documents/EPIC_Polar_Code_Paper.pdf.

最新结果 • RECENT RESULTS •

U-UV 码：一种好的中短码
U-UV Codes: The Good Short-to-Medium Length Codes

陈立 [1]，张华滋 [2]
1 中山大学，2 华为技术有限公司
Li Chen [1], Huazi Zhang [2]
1 Sun Yat-sen University, 2 Huawei Technology Ltd.
chenli55@mail.sysu.edu.cn; zhanghuazi@huawei.com

Background and Motivation: Future wireless communication networks will support various new applications that continue to realize the power of information technology. They include the extended reality, unmanned driving, wise information technology of medicine, factory automation, and etc. In these scenarios, transmission reliability is not the only key performance metric, but also the latency. Subsequently, the short-to-medium length (SML) channel codes whose codeword length n varies from tens of bits to at most a thousand will play an important role. The SML feature enables their low decoding latency. However, without a large codeword length as most modern codes, the code's minimum distance d shrinks, limiting its error-correction capability. Meanwhile, the iterative decoding for modern codes, such as the turbo codes and low-density parity-check (LDPC) codes, will not be effective for SML codes. For SML codes, the decoding independence assumption between codeword / information symbols falls further apart from reality. Consequently, designing good performing SML codes is an intriguing challenge. This article introduces a good performing SML code candidate – the U-UV codes.

So far, BCH codes, tail biting convolutional (TBC) codes, polar codes and the recent polarization adjusted convolutional (PAC) codes are the known good performing SML codes [1]. Their competent decoding performances are supported by powerful decoding algorithms. For example, the ordered statistics decoding (OSD) [2] and the successive cancellation list (SCL) decoding [3][4] enable the BCH codes and the cyclic redundancy check (CRC) concatenated polar (CRC-polar) codes to approach the normal approximation (NA) bound [5], respectively. The OSD is a near maximum likelihood (ML) decoding approach. Together with list decoding, they are often considered to be too complex for long codes. However, due to their limited size, SML codes can be decoded by these computationally expensive algorithms. On the other aspect, good performing SML codes can also be produced through structural coding. A number of small component codes can be structurally coupled in forming an SML code. Consequently, the decoding of a component code can be empowered by the a priori information gained from the decoding of other component codes. This has been demonstrated by the success of multilevel coding and its multistage decoding [6], in which the component codes are coupled through a constellation structure. This perception inspires our research into the (U | U + V) coding structure that was proposed by Plotkin in 1960 [7], in which the U code and the V code are component codes of equal length. We call this structure and its resulting codes the U-UV structure and the U-UV codes, respectively.

Construction and Design: Given a U code and a V code, both of which are linear block codes of length n and dimensions of k_{U} and k_{V}, respectively, they can be denoted by (n, k_{U}) and (n, k_{V}). Let d_{U} and d_{V} further denote the minimum distances of the U code and the V code, respectively. The U-UV code can be constructed by

$$\{(\boldsymbol{u} \mid \boldsymbol{u} + \boldsymbol{v});\ \boldsymbol{u} \in \text{U codebook and } \boldsymbol{v} \in \text{V codebook}\},$$

where $\boldsymbol{u}$ and $\boldsymbol{v}$ are codewords of the U code and the V code, respectively. It is a $(2n, k)$ linear block code with a dimension of $k = k_U + k_V$ and its minimum distance is $d = \min\{2d_U, d_V\}$. This construction can be extended recursively by involving more component codes, as shown in Fig. 1. In general, if there are H levels U-UV construction, it involves 2^H component codes and results in a U-UV code of length $2^H n$. This structural coding can be interpretated in two folds. An H levels U-UV code can be seen as a generalized concatenated code (GCC) with 2^H outer component codes of length n and n inner polar codes of length 2^H, which is shown as in Fig. 2. On the other aspect, polar coding is also founded on the U-UV structure. Fig. 3 shows the trellis that is commonly shared by a length 4 polar code and a 2 levels U-UV code. Polar encoding performs the symbol wise U-UV coupling, which would be vector wise for U-UV encoding. It is known channel polarization is realized under a large codeword length, in which the capacities of most subchannels are polarized to either 0 or 1. The subchannels with a capacity close to 1 will be utilized to transmit information, while other subchannels will be utilized to transmit redundancy which are called the frozen symbols known by both the encoder and decoder. But in the SML regime, channel polarization is incomplete. There is a significant portion of subchannels without a polarized capacity. Their transmission assignment becomes randomized, which affects the decoding. In the U-UV coding paradigm, each subchannel conveys a codeword instead of a symbol. If the component code rate does not exceed the subchannel capacity, reliable transmission over the subchannel can be achieved by the use of a channel code. Therefore, U-UV coding can be understood as an approach to overcome the incomplete polarization for SML polar codes.

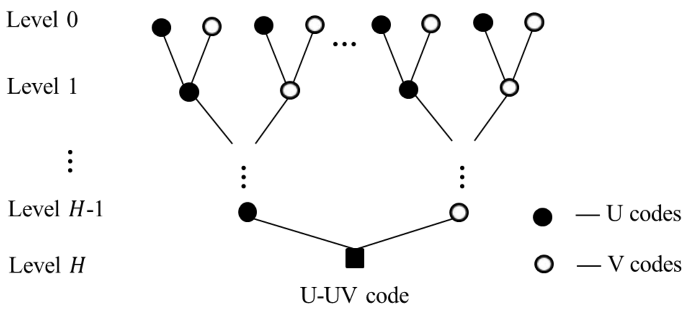


Fig. 1 Construction of U-UV codes.

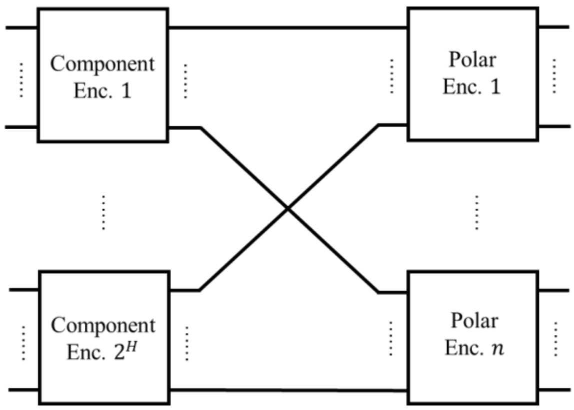


Fig. 2 GCC interpretation of U-UV codes.

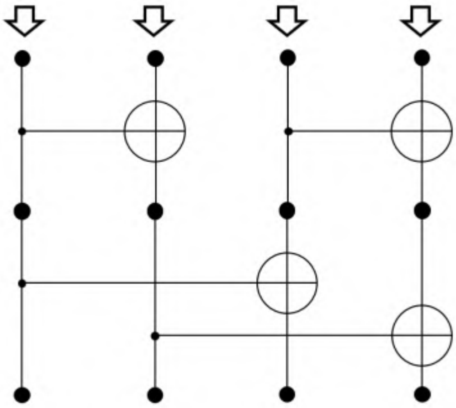


Fig. 3 The polar and U-UV trellis.

The above description implies that the U-UV codes can be designed based on the subchannel capacities, where the component code rates should be capped by the capacities. The subchannel capacities can be estimated by Gaussian approximation that assumes the log likelihood ratio (LLR) values of each decoding trellis layer are Gaussian distributed [8]. The use of small component codes and its multistage decoding mechanism lead to extra metrics to be considered in the design. First, SML codes are not capacity approaching codes. The finite length rates can be further calculated. They retreat from the estimated subchannel capacities, providing a more realistic limit for the component code rates. Secondly, since the component codes are decoded successively, performance of the U-UV code can be optimized by equaling their decoding error rates. This can be achieved by adjusting their rates so that their decoding error rates are better aligned. The decoding error rates can either be computed theoretically or through simulation. The former often requires knowledge of the component code's weight spectrum.

Decoding and Performance: Similar to CRC-polar codes, the U-UV codes can be decoded by the SCL algorithm in which the SC algorithm is a special case with the decoding output list size $l = 1$ [9]. In the decoding, estimations of the earlier decoded component codes participate into the upcoming decoding. SCL decoding of a U-UV code is also founded on the list decoding of its component codes, and consequently multiple decoding paths can be formed over the decoding tree. So far, BCH codes have been considered as the component codes and their OSD substantiate the SCL decoding of the U-UV code. In the successive decoding process, the number of decoding paths grows exponentially as it progresses, leading to an exponentially growing complexity. Therefore, path pruning is needed to curb the decoding complexity but meanwhile maintain the decoding performance. In the pursuit of finding the most likely estimation from the decoding output list, the correlation distance between a component codeword estimation and the received LLRs can be utilized as a metric to assess the codeword likelihood. This also becomes the SCL decoding metric that is accumulated along the decoding. It can be utilized to prune the decoding paths and identify the most likely U-UV codeword estimation from the decoding output list.

Fig. 4 compares the decoding performance of the (252, 139) U-UV code with the (256, 140) CRC-polar code and the (255, 139) BCH code over the additive white Gaussian noise (AWGN) channel using BPSK modulation. The U-UV code is resulted from a 2 levels construction of 4 BCH component codes, which are the (63, 57), (63, 39), (63, 36) and the (63, 7) BCH codes, respectively. The CRC-polar code is the 5G new radio standard code that contains a length 8 CRC concatenation. Both the U-UV code and the CRC-polar code are decoded by the SCL (incl. SC) algorithm that is parameterized by its decoding output list size l, while the (255, 139) BCH is decoded by the OSD that is parametrized by its order τ. Fig. 4 shows that the U-UV code can outperform the other two SML codes. With the same decoding output list size, SCL and SC decoding of the U-UV code can yield substantial coding gains over the CRC-polar code. But this is realized at the cost of higher decoding complexity. For example, with $l = 8$, SCL decoding of the U-UV code requires on average 1.3×10^6 binary operations

(BOPs) and 2.8 × 10^5 floating point operations (FLOPs) in decoding a codeword. SCL decoding of the CRC-polar code requires 1.6 × 10^4 BOPs and 1.9 × 10^4 FLOPs. However, note that the decoding performance gain can be exchanged for complexity gain. In comparison with the (255, 139) BCH code, the U-UV code's advantage becomes more significant. For example, OSD of the BCH with $\tau = 3$ would require on average 1.6 × 10^8 BOPs and 2.6 × 10^7 FLOPs to decode a codeword. This comparison implies that it is beneficial to couple a number of smaller BCH codes in replacing a large one. The U-UV is an effective coupling structure. The finite length transmission limit represented by the NA bound of a length 252 code also shows there is room to further optimize the SML code design.

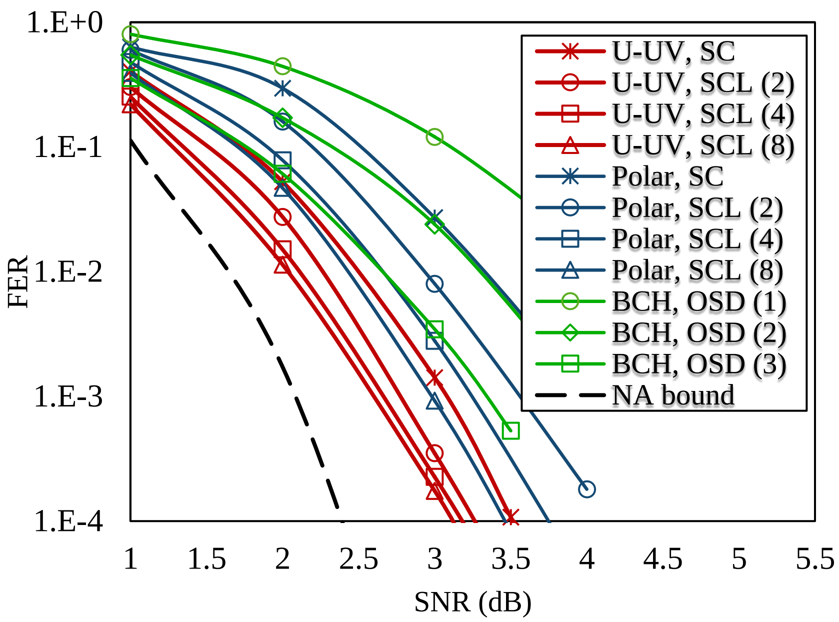


Fig. 4 Performance comparison between the U-UV, the CRC-polar and the BCH codes.

Merits and Challenges: Therefore, the U-UV codes are good performing SML codes, adding another candidate into this code family that is important for future wireless communication networks. In addition to this error-correction competency, it also has some special features that can be favored by future applications. Its codeword length can be adjusted through changing the number of construction levels, i.e., also the number of component codes. Since the U-UV decoding is substantiated by that of the component code decoding and the successive estimation through them, changing the number of component codes does not largely alter the decoder structure. In practice, an indicator for the number of component codes and their decoding status can keep up to the pace of changing the length of the U-UV code. This feature will be favorable when the more flexible channel coding is needed, where the coding block can be adapted to the size of the content. Secondly, it has more room to reduce the decoding latency. Due to the successive nature of the SC and SCL decoding, decoding latency of polar codes has also been a longstanding challenge. But for U-UV codes, its decoding latency optimization can be founded based on reducing the decoding latency of component codes. In particular, OSD may be supported by much simpler implementations in the future. It can also be parallelized to the level that can be supported by the hardware capacity. This will spin out interesting future research endeavors. Finally, the U-UV codes can also be constructed by other small component codes, which may lead to improved decoding performance. More than BCH codes, the binary subcodes of algebraic-geometric codes, the TBC codes, or other nonbinary codes can be considered. Non-binary U-UV codes that are competent in correcting burst errors can be naturally led to.

Postscript: A plenary talk of the same title was given in the 2022 IEEE Globecom Workshop on Channel Coding Beyond 5G. Its video and slides are available at: www.chencode.cn.

References

[1] M. Coskun *et al.*, "Efficient Error-correcting Codes in the Short Block-length Regime," *Phys. Commum.*, vol. 34, pp. 66–79, Mar. 2019.

[2] M. Fossorier and S. Lin, "Soft-decision Decoding of Linear Block Codes Based on Ordered Statistics," *IEEE Trans. Inf. Theory*, vol. 41, no. 5, pp. 1379–1396, Sept. 1995.

[3] K. Niu and K. Chen, "CRC-aided Decoding of Polar Codes," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1668–1671, Oct. 2012.

[4] I. Tal and A. Vardy, "List Decoding of Polar Codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2213–2226, Jul. 2015.

[5] Y. Polyanskiy, V. Poor, and S. Verdù, "Channel Coding Rate in the Finite Blocklength Regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[6] H. Imai, S. Hirakawa, "A New Multilevel Coding Method Using Error-correcting Codes," *IEEE Trans. Inf. Theory*, vol. 23, no. 3, pp. 371-377, May 1977.

[7] M. Plotkin, "Binary Codes with Specified Minimum Distance," *IRE Trans. Inf. Theory*, vol. 6, no. 4, pp. 445–450, Sept. 1960.

[8] P. Trifonov, "Efficient Design and Decoding of Polar Codes," *IEEE Trans. Commum.*, vol. 60, no. 11, pp. 3221–3227, Nov. 2012.

[9] J. Cheng and L. Chen, "BCH Based U-UV Codes and Its Decoding," in Proc. *IEEE Int. Symp. Inf. Theory (ISIT)*, Melbourne, Victoria, pp. 1433–1438, Jul. 2021.

交流活动 • RESEARCH ACTIVITIES •

第 11 届中国国际通信大会：面向未来无线网络的信息论与编码研讨会
11th IEEE/CIC International Conference on Communications in China: Workshop on Information Theory and Coding for Future Wireless

第 11 届中国国际通信大会(ICCC 2022)在佛山三水成功举办。本次大会由 IEEE、中国通信学会、中山大学、广东工业大学、佛山三水政府主办，由华为公司等赞助，口号为“智能互联，未来通信”。值得注意的是，本次大会的特色之一是聚焦基础研究，探讨“根技术”。信息论与编码作为通信技术中的底层核心技术，在本次ICCC得到了前所未有的重视。大会的主旨演讲包含 Polar 码发明人 Arıkan 教授和华为无线 CTO、首席科学家童文博士的报告，前者提出了信道编码在 6G 中的机会和挑战，后者展示了通往 6G 极致链接的最新研究成果。从理论到实践，提供了信息论与编码的盛宴，获得热烈反响。

依托于本次大会，华为无线技术实验室与 IEEE 信息论学会广州分会共同举办了名为面向未来无线网络的信息论与编码研讨会。本次研讨会邀请了童文博士、范平志教授、沈八中教授、白宝明教授、牛凯教授作为技术委员会主席，并邀请了国内信息论与编码领域的顶尖教授和学者作为技术委员会成员。

研讨于 8 月 11 日举行，由于疫情采用线上与线下结合的形式，并非常荣幸邀请到了沈八中教授、白宝明教授和大会主席陈立教授亲临会场，并先后做了开场致辞。三位教授都提到了需要进一步加大中国信息论与编码研究投入，并凝聚团结国内产学研研究人员和力量，提升信息论编码在国内和国际的认知度，非常令人鼓舞。

本次研讨会还邀请到了澳大利亚新南威尔斯大学的 Jinhong Yuan 教授与北京邮电大学的戴金晟教授作了主旨演讲。Yuan 教授介绍了 Turbo 码的进一步发展 - 广义空间耦合码；戴老师则介绍了语义通信的最新研究进展。报告结束后，观众踊跃提问并展开了热烈的讨论。

本次研讨会共有 12 篇技术论文报告，涉及 Polar 码、LDPC 码、代数码、波形、全双工、接收机、机器学习在信息论编码中的应用等，涵盖了信息论编码的诸多课题。参加研讨会的学生和老师（按发言顺序）来自于东南大学姜明、赵春明教授团队，浙江大学张朝阳教授团队、深圳大学刘凌教授团队、华为圣彼得堡研究所、华侨大学刘三亚教授团队、中山大学李聪端、陈立教授团队、西南交通大学范平志教授团队、代彬教授团队、山东科技大学崔建明教授团队、西安电子科技大学白宝明教授团队。

本次研讨会气氛活跃，学术讨论热烈，为信息论与编码、无线通信技术领域的老师和研究生、工程师们搭建了一个横跨学术界和工业界、专业性强、前沿学术成果分享和交流的平台。通过这次会议，优秀学者一起增进友谊，交流技术，共话信息论与编码的未来。

交流活动 • RESEARCH ACTIVITIES •

2022 IEEE 东亚信息论学校
2022 IEEE East Asian School of Information Theory

The 2022 IEEE East Asian School of Information Theory (EASIT) took place as a hybrid event from August 2 to 5, 2022 at Shenzhen Institute for Talents Development, co-organized by IEEE Information Theory Society Guangzhou, Tsinghua Shenzhen International Graduate School (SIGS), Sun Yat-sen University and the Chinese University of Hong Kong (Shenzhen). IEEE Information Theory Society and Huawei Technology Co., Ltd. are sponsoring this event. More than 100 students and researchers from about 26 Universities and Institutes registered for the school.

IEEE EASIT 2022 consisted of eight outstanding tutorials delivered by distinguished lecturers and covered the most cutting-edge research in information theory, including information theory and statistics, information theory and machine learning, coding for communications, and coding for storage. The school started with a tutorial on Neural Compression: Algorithms and Fundamental Limits presented by the IEEE Information Theory Society 2022 Goldsmith Lecturer Prof. Shirin Saeedi Bidokhti from the University of Pennsylvania. Prof. Bidokhti discussed the algorithm and theoretical advances of neural network compression. The first part of her presentation was an introduction to lossless and lossy compression and their theoretical limits. Then, she discussed neural compression based on deep generative models from two perspectives. There are techniques to make the compression rate close to the entropy of the source for lossless compression. For lossy compression, a simulation of a rate-distortion function was presented. Later, she discussed theoretically how it ensures rate and distortion in one-shot lossy compression.

In the afternoon, Prof. Erdal Arikan from Bilkent University gave a tutorial on polar codes. In the next decade, such techniques are likely to have a positive impact on the next generation of communication. This is due to the fact that polar code is the first scheme that can demonstrate channel capacity. During this tutorial, Prof. Arikan introduced the basic structure of the polar code and explained how this family of codes achieves the capacity of Binary Memoryless Symmetric channel. Such techniques can be future-embracing and reaching the channel capacity

The next day opened with a tutorial by Prof. Alexander Barg from the University of Maryland. Prof. Barg's tutorial topic was Information Coding under Communication Constraints. Prof. Barg overviewed the main problems in coding for distributed storage systems. His tutorial introduced some related methods and the associated results, including discussions on basic algebraic constructions of locally recoverable codes (LRC) and regenerating codes, problems of node recovery in systems where the connections between the nodes are constrained by a graph, and some new research directions.

In the afternoon of August 3rd, Prof. Xiaohu Tang from Southwest Jiaotong University presented his recent research on repairing maximum distance separable (MDS) code at a high rate. In actual big data storage systems, node failure is common. Therefore, it is very critical to design a reliable storage encoding scheme to recover data loss caused by node failure. As a result of their good properties, MDS codes are widely used in data storage systems under the backdrop of big data. Professor Tang introduces different schemes - aiming to cope with different node failure cases. These efficient designs can be applied to data recovery in different situations and provide rich coding schemes to improve the reliability of storage systems.

The morning of August 4th, Prof. Lizhong Zheng from Massachusetts Institute of Technology, gave us a tutorial on the machinery of simplified information geometry analysis and understanding deep learning with an information geometric method. When applying information theoretic analysis to machine learning problems, we often face the difficulty of describing the relation between a number of different distributions. It is a very effective way to describe this complex situation in a geometric approach. At the beginning of the tutorial, Prof. Zheng introduced several fundamental concepts in information theory including Kullback–Leibler divergence, Fisher information metrics, i-projection, information vector, and canonical dependence matrix. Later, Prof. Zheng discussed some learning theory applications of information geometric method in the analysis of strong data processing inequality, generalization error, and model selection. He also discussed more applied problems such as understanding deep neural networks, transfer learning, and multimodal learning.

On the afternoon of August 4th, Prof. Yao Xie from Georgia Institute of Technology, gave the tutorial on some recent advances in modern hypothesis tests. Hypothesis testing is an essential building block for machine learning and signal processing problems. In this tutorial, Prof. Yao Xie introduced: i) robust hypothesis tests utilizing modern optimization, as well as its application in classification and domain adaptation; ii) sequential hypothesis test and change point detection in multi-sensor sparse/subspace/robust setting, as well as methods utilizing deep learning that exploit low-dimensional structure; iii) continuous-time Hawkes network estimation/change point detection and discrete-time Hawkes network convex estimation. Such techniques enable us to leverage deep learning by developing efficient testing tools for modern data, a principled validation tool and a theoretical foundation for a deep learning model.

On the morning of August 5th, Prof. Tie Liu from Texas A&M University gave a tutorial about how to interpret the two fundamental problems in statistical data analysis and learning theory, i.e., concentration and generalization. In the first part, Prof. Liu focused on the concentration of a general function of independent variables. He presented the entropy method for leveraging various notions of functional stability into exponential tail bounds. In the second part, Prof. Liu focused on the generalization of a data-dependent query and proposes a systematic approach for relating it to various information-theoretic notions of algorithm stability.

On the afternoon of August 5th, Prof. Jinhong Yuan from The University of New South Wales presented a class of spatially coupled codes, namely partially information coupled (PIC) and partially parity coupled (PPC). There are two main characteristics of this class of codes. First, the code rate can be flexibly adjusted by varying the coupling ratio. Secondly, component encoders and decoders can adopt those off-the-shelf. Professor Yuan first introduced the background and concept of spatially coupled codes, and then introduced the main contents of this report in four parts: (1) Construction methods for PIC turbo codes and PPC turbo codes; (2) Generalized spatially coupled parallel concatenated codes (GSC-PCCs); (3) A new family of spatially coupled product codes called sub-block rearranged staircase codes; (4) Construction methods for PIC LDPC codes and PIC polar codes. These spatially coupled codes are compatible with current standards such that the underlying component code encoding and decoding can be kept uncharged. This improves the transmit spectrum and power efficiency.

The school also included poster sessions on days one through three of the event. A total of 60 student posters were received, and 20 were presented on-site. Poster authors are encouraged to communicate freely with other participants during the poster presentation. The organizing committee selected five posters from the 60 received posters for The Best Poster Awards on the last day before the summer school ended. Guodong Li *et al.* (Shandong University), Yuan Li *et al.* (Institute of Mathematics and Systems Science, Chinese Academy of Sciences), Chenhao Jin *et al.* (Sun Yat-sen University), Lijia Yang *et al.* (Sun Yat-sen University), Cheng Du *et al.* (Fudan University), were awarded student best poster awards for their poster content and presentation.

Our sincere thanks are extended to all lecturers who contributed to the development of science and education. We are also grateful to the IEEE Information Theory Society and Huawei Technology Inc. for the sponsorship of the whole event.

We would also like to thank all participants who attended despite the severe conditions of the epidemic. The epidemic forces many students to attend the conference online this year, but we hope to see you all at future events.

2022 IEEE 全球通信大会：5G 未来编码研讨会
2022 IEEE Global Communications: Workshop on Channel Coding beyond 5G

The 2nd Workshop on Channel Coding beyond 5G, was held on Dec. 4 in conjunction with the IEEE Global Communications Conference (Globecom) 2022, in Rio de Janeiro, Brazil.

Channel coding is a fundamental component in wireless communication. From 2G to 5G, wireless systems have been powered by state-of-the-art channel coding technologies. This workshop aims to galvanize academic and industrial researchers to discuss solutions on the coding techniques for wireless systems beyond 5G. The workshop adopted a hybrid format to provide the community interactions through on-site technical presentations and online keynote speeches. The workshop has received a total of 30 submissions. Among them, 12 papers were accepted for publication. The program included some latest research from the academia, and also received contributions from the industry, such as Huawei, Samsung, NVIDIA, and Infinera.

The in-person part of workshop was a half-day event, started with an opening speech by Dr. Huazi Zhang (Huawei Technologies Canada Co., Ltd.), who thanked the co-organizers and welcomed the attendees on behalf of the organizing committee of the workshop.



The in-person part of the workshop was featured by three keynote speeches:

- Prof. Jinhong Yuan (University of New South Wales) on generalized spatially-coupled turbo-like codes
- Prof. Michael Lentmaier (Lund University) on generalized LDPC codes with convolutional code constraints
- Prof. Li Chen (Sun Yat-sen University) on good short-to-medium length codes

The 12 accepted papers were categorized into three themes: coding schemes, coding theory and decoding. The papers cover areas including polar codes, LDPC codes, algebraic codes, decoding of short codes, neural networks for channel coding, and finite blocklength analysis. The in-person sessions provided a good opportunity for fruitful Q&A interactions between the presenters and the audience.

The workshop has achieved its success, realizing its motivation of promoting research on channel coding. In particular, the organizers managed to produce an in-person event with excellent technical presentations and face-to-face interactions. We would like to sincerely thank all the speakers and participants.

交流活动 • RESEARCH ACTIVITIES •

茶思屋三人行之香农信息论
Chaspark Trialogue on Shannon Information Theory

Shannon Information Theory laid the foundation for the modern information age. To help people, especially young professionals and students in engineering field, better understand the full picture and future directions of Shannon information theory, *Huang Danian Charspark Website* organized an in-person Trialogue on Shannon Information Theory on Aug. 4, 2022, at Shenzhen, China. The experts invited to participate include Prof. Xiaohu Tang from Southwest Jiaotong University, Prof. Li Chen from Sun Yat-sen University, and Dr. Li Sun from Huawei Technologies Co., Ltd. Dr. Li Sun hosted the trialogue.

Huang Danian Charspark Website (https://www.chaspark.net/#/home) is an online platform which aims at fostering an environment to explore and guide development and open thinking in the science and technology field. Since its foundation, the website has already organized multiple activities to exchange ideas and discuss technical opportunities to promote innovation and advance science.

The trialogue opens with a general introduction of the full picture of Shannon Information Theory. Prof. Chen and Prof. Tang summarized that Shannon Information Theory actually answers four fundamental questions: (1) What is information? (2) How to measure information? (3) How to represent information? (4) How to transmit information reliably and efficiently? For each of these questions, the two professors explained how Shannon and his successors have addressed.

Then, the experts continued to discuss the pioneering contributions of Shannon. Prof. Tang and Prof. Chen briefly introduced the seminal paper “A Mathematical Theory of Communication”, written by Claude E. Shannon in 1948, and elaborated on how this work guides the development of information and communications engineering in the past few decades. Dr. Sun mentioned another significant contribution by Shannon, i.e., the definition of perfect secrecy and the invention of one-time-pad approach, which greatly influences the cryptography.

Since the birth of Shannon Information Theory, various advanced coding, modulation, and multiple-access technologies have been devised, and the performance of the current communication systems is very close to the theoretical limit proposed by Shannon. In this situation, is information theory still worthy of further investigation? Are there unsolved and important problems in information theory research? Three experts had hot discussions on these topics. In Prof. Chen’s opinion, the capacity-achieving performance of various good codes relies on the assumption that the code length is large. However, this contradicts with the low-latency requirement in many applications. It is still unclear how to approach Shannon limit in the short code-length regime and satisfy both the ultra-reliability and low-latency requirements. Prof. Tang commented that diversified applications pose new constraints and requirements to the code design. Information and coding theories need to be upgraded to take into account these new constraints. “When talking about achieving the limits, we should focus on not only the performance but also the efficiency or the cost”, Dr. Sun said, “and it remains open how to incorporate energy, complexity, as well as delay into the theoretical framework”.

The fourth topic discussed by the experts is the impact of information theory on emerging applications, such as 6G, meta-verse, self-driving, smart factory, integration of communications, sensing, and computing, post-quantum security, etc. Prof. Chen indicated that it is necessary to extend the information theory to take into account the timeliness of the channel and the network topology. Moreover, he mentioned that in future machine-type communications, a priori knowledge is of vital importance for the connection of intelligence. Therefore, it is necessary to develop novel tools to exploit the a priori information for better signal processing and transmission scheme design. Prof. Tang mainly talked about the interplay between information theory and artificial intelligence. In particular, he pointed out several valuable directions, including the use of information theory towards explainable AI, and the development of network information theory to model and analyze the networked transmission environments. Dr. Sun mentioned that in the AI age, classical transmission-oriented information theory may evolve towards a computation-oriented or inference-oriented information theory.

The experts were also interested in information theory education. They reviewed Shannon’s famous disciples and followers, and introduced their groundbreaking contributions to the information theory field. Afterwards, using some interesting examples, Prof. Chen and Prof. Tang talked about how to train graduate students, how to motivate and maintain students’ desires for new knowledge, and how to guide them to seek for important problems.

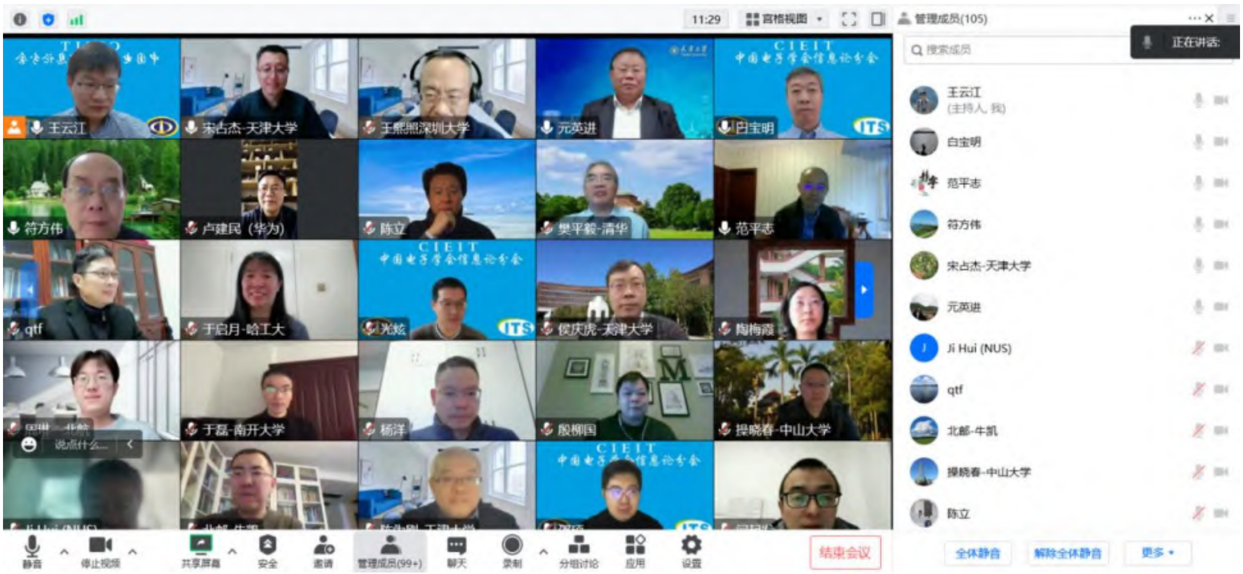
Finally, professors gave some advices to the younger generations in information theory research. Prof. Tang pointed out that a long-term dedication is a must for information theory studies, and he called for that more young faculty members should involve in this area. Besides that, Prof. Tang mentioned that many information theoretic top scholars, including Shannon himself, have a long experience in industries, which is beneficial for them to learn practical needs and find important problems. So, Prof. Tang suggested that information theorists have more exchanges with experts from industries. Prof. Chen emphasized the importance of interest. To be more specific, Prof. Chen said, “Follow your mind. Do pursue a problem if you think it has scientific values and you have interest in it as well”. Prof. Chen also stressed that advisors should create a good platform to promote communication between graduate students and leading experts.

We are grateful to *Huang Danian Charspark Website* for the sponsorship of the whole event. The video for this Trialogue (in Chinese) is available at https://www.chaspark.net/#/coffeeHours/media /790716910387302400. Interested readers are encouraged to visit this website for more details.

交流活动 • RESEARCH ACTIVITIES •

2022 年中国电子学会第二十九届信息论学术年会
29th Chinese Institute of Electronics Conference on Information Theory 2022

2022 年度全国信息论学术会议暨中国电子学会第 29 届信息论学术年会(CIEIT 2022)于 2022 年 12 月 2 日至 3 日在线召开。本届会议由中国电子学会信息论分会主办，天津大学和南开大学承办，西安电子科技大学通信工程学院和综合业务网理论及关键技术国家重点实验室协办，会议同时也受到华为技术有限公司和《Entropy》期刊的支持。本届会议邀请了包括元英进院士等 11 位海内外知名专家学者进行前沿学术报告。会议为国内信息与通信领域的专家学者和研究生搭建一个学术交流的平台，分享信息与通信领域的研究成果，探讨信息与通信的研究与应用所面临的关键性问题和研究方向。



会议组织

大会主席：

西安电子科技大学	白宝明
天津大学	宋占杰

程序委员会主席：

南开大学	符方伟
浙江大学	张朝阳
西南交通大学	唐小虎
北京邮电大学	牛凯
清华大学	樊平毅
中山大学	马啸
上海交通大学	陶梅霞

大会名誉主席：

西南交通大学	范平志

大会工业界主席：

华为技术有限公司	卢建民

组织委员会：

天津大学	宋占杰 陈为刚
南开大学	符方伟 光炫

学会轮值秘书长：

西安电子科技大学	王云江

新锐风采 • NEW TALENTS •

刘凡 (Fan Liu)，南方科技大学电子与电气工程系助理教授（副研究员），博士生导师。中国科协青年托举人才，广东省引进青年拔尖人才，玛丽·居里学者。2013 年于北京理工大学获工学学士学位，2018 年于北京理工大学获工学博士学位，师从国家最高科学技术奖获得者王小谟院士。曾于 2016 年-2018 年赴英国伦敦大学学院任访问学者，2018 年-2020 年在英国伦敦大学学院担任“玛丽·居里”研究员。2020 年回国后全职加入南方科技大学。主要研究方向为通信感知一体化，车联网与智能交通，毫米波通信等，获引 3000 余次。目前担任 IEEE Communications Letters 与 IEEE Open Journal of Signal Processing 编委，曾任 IEEE Journal on Selected Areas in Communications、IEEE Wireless Communications、《通信与信息网络学报》、《中国通信》、《信号处理》等期刊的客座编委。曾被列入 2021 和 2022 年斯坦福大学全球 2%顶尖科学家榜单，获得 2021 年 IEEE 信号处理学会青年作者最佳论文奖，2019 年中国电子学会优秀博士学位论文奖。刘凡博士牵头成立了 IEEE 通信学会通信感知一体化新兴技术倡议委员会 (IEEE ComSoc ISAC-ETI)，并担任首届学术主席。刘凡博士是华为技术有限公司独立顾问，以及 IMT-2030 (6G) 通信感知一体化任务组专家。

近年来的主要研究方向为通信感知一体化的基础理论与信号处理。主要贡献包括：揭示了高斯信道下通信感知一体化系统的信息论基本极限，包括确定-随机折衷与子空间折衷[1][2]；提出多种通信感知一体化波形及相应的信号处理方法，使系统同时具备优异的通信信息承载能力与稳健的环境感知能力[3][4][5]；提出感知辅助通信技术，将之应用于毫米波智能网联车辆场景，显著降低了车联网波束管理所产生的信令开销[6][7][8]；提出“感知即服务”的新型 6G 网络架构，构建了该架构下的资源分配理论与方法[9][10]。

部分重要学术论文：

[1] Y. Xiong, F. Liu, Y. Cui, W. Yuan, T.-X. Han, and G. Caire, “On the Fundamental Tradeoff of Integrated Sensing and Communications Under Gaussian Channels,” submitted to *IEEE Trans. Inf. Theory*. Available: https://arxiv.org/abs/2204.06938

[2] F. Liu, L. Zheng, Y. Cui, C. Masouros, A. P. Petropulu, H. Griffiths, and Y. C. Eldar, “Seventy Years of Radar and Communications: The Road from Separation to Integration,” submitted to *IEEE Signal Process. Mag*. Available: https://arxiv.org/abs/2210.00446

[3] F. Liu, Y. -F. Liu, A. Li, C. Masouros and Y. C. Eldar, “Cramér-Rao Bound Optimization for Joint Radar-Communication Beamforming,” *IEEE Trans. Signal Process.*, vol. 70, pp. 240-253, 2022.

[4] F. Liu, L. Zhou, C. Masouros, A. Li, W. Luo, and A. Petropulu, “Toward Dual-functional Radar-Communication Systems: Optimal Waveform Design,” *IEEE Trans. Signal Process.*, vol. 66, no. 16, pp. 4264-4279, Aug. 2018.

[5] F. Liu, C. Masouros, A. Li, H. Sun and L. Hanzo, “MU-MIMO Communications with MIMO Radar: From Co-existence to Joint Transmission,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2755-2770, Apr. 2018.

[6] F. Liu, W. Yuan, C. Masouros and J. Yuan, “Radar-assisted Predictive Beamforming for Vehicular Links: Communication Served by Sensing,” *IEEE Trans. Wireless Commun.*, vol. 19, no. 11, pp. 7704-7719, Nov. 2020.

[7] W. Yuan, F. Liu, C. Masouros, J. Yuan, D. W. K. Ng and N. G. Prelcic, “Bayesian Predictive Beamforming for Vehicular Networks: A Low-Overhead Joint Radar-Communication Approach,” *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 1442-1456, Mar. 2021.

[8] Z. Du, F. Liu, W. Yuan, C. Masouros, Z. Zhang, S. Xia, and G. Caire, “Integrated Sensing and Communications for V2I Networks: Dynamic Predictive Beamforming for Extended Vehicle Targets,” *IEEE Trans. Wireless Commun.*. Early Access.

[9] F. Liu, Y. Cui, C. Masouros, J. Xu, T.-X. Han, Y. C. Eldar, and S. Buzzi, “Integrated Sensing and Communications: Towards Dual-functional Wireless Networks for 6G and Beyond”, *IEEE J. Sel. Areas Commun.*, vol. 40, no. 6, pp. 1728-1767, Jun. 2022.

[10] F. Dong, F. Liu, Y. Cui, W. Wang, K. Han, and Z. Wang, “Sensing as a Service in 6G Perceptive Networks: A Unified Framework for ISAC Resource Allocation,” *IEEE Trans. Wireless Commun.*. Early Access.

新锐风采 • NEW TALENTS •

Zhen Mei (梅镇) received the B.Eng. degree in electronic and information engineering from Central China Normal University (CCNU), China, in 2012, and the M.Sc. degree in communications and signal processing and the Ph.D. degree from Newcastle University, U.K., in 2013 and 2017, respectively. He worked as a Post-Doctoral Researcher with the Singapore University of Technology and Design (SUTD) from 2017 to 2019, and a System Engineer with Huawei Technologies Co., Ltd from 2019 to 2021.

He joined Nanjing University of Science and Technology (NJUST) as an Associate Professor in 2021. His research interests include deep learning, channel coding and signal processing for communications and data storage systems. Recently, he has studied channel quantization and code design for emerging non-volatile memories with both model-driven and data-driven approaches. He is also investigating advanced machine learning algorithms for next-generation communication systems and non-volatile memories.

His key publications include:

[1] Z. Mei, K. Cai and X. He, "Deep Learning-Aided Dynamic Read Thresholds Design For Multi-Level-Cell Flash Memories," *IEEE Trans. Commun.*, vol. 68, no. 5, pp. 2850-2862, May 2020.

[2] Z. Mei, K. Cai, L. Shi and X. He, "On Channel Quantization for Spin-Torque Transfer Magnetic Random Access Memory," *IEEE Trans. Commun.*, vol. 67, no. 11, pp. 7526-7539, Nov. 2019.

[3] Z. Mei, K. Cai and G. Song, "Performance Analysis of Finite-Length LDPC Codes over Asymmetric Memoryless Channels," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11338-11342, Nov. 2019.

[4] Z. Mei, M. Johnston, S. Le Goff and L. Chen, "Performance Analysis of LDPC-Coded Diversity Combining on Rayleigh Fading Channels with Impulsive Noise," *IEEE Trans. Commun.*, vol. 65, no. 6, pp. 2345-2356, Jun. 2017.

[5] X. He, K. Cai, W. Song, and Z. Mei, "Dynamic Programming for Sequential Deterministic Quatization of Discrete Memoryless Channels," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 3638–3651, Jun. 2021.

[6] X. He, K. Cai, and Z. Mei, "On Finite Alphabet Iterative Decoding of LDPC Codes with High-order Modulation," *IEEE Commun. Lett.*, vol. 23, no. 11, pp. 1913-1917, Nov. 2019.

[7] B. Dai, R. Liu, C. Gao and Z. Mei, "Symbol Flipping Algorithm with Self-Adjustment Strategy for LDPC codes over GF(q)," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 7189-7193, Jul. 2019.

[8] Z. Mei, K. Cai and X. W. Zhong, "Neural Network-Based Dynamic Threshold Detection for Non-Volatile Memories," *IEEE Int. Conf. Commun. (ICC)*, pp. 1-6, May 2019.

[9] Z. Mei, K. Cai and L. Shi, "Information Theoretic Bounds Based Channel Quantization Design for Emerging Memories," *IEEE Inf. Theory Workshop (ITW)*, pp. 1-5, Nov. 2018.

[10] Z. Mei, M. Johnston, S. Le Goff and L. Chen, "Error Probability Analysis of M-QAM on Rayleigh Fading channels with Impulsive Noise," *IEEE Int. Workshop Signal Process. Advances Wireless Commun. (SPAWC)*, pp. 1-5, Jul. 2016.

新锐风采 • NEW TALENTS •

Ke Lai (赖恪) received the B.S. degree in communications engineering (hons), the M.S and Ph.D. degree in information and communications engineering all from National University of Defense Technology under the supervision of Prof. Jing Lei, Changsha, China, in 2016, 2018 and 2022, respectively. His research interest mainly focuses on the code domain non-orthogonal multiple access (CD-NOMA), in particular, the application and extension of sparse code multiple access (SCMA). He received the excellent master dissertation of Hunan province in 2021.

His thesis is entitled "Research on Efficient and Reliable Sparse Code Multiple Access Technique" which focuses on the design of high spectral efficiency and reliable SCMA system, and investigating the methods for further performances improvement. This thesis first proposes a novel analytical model for multi-cell SCMA, where several guidelines can be attained for the improvement of efficiency and reliability in the SCMA design. For the improvement of spectral efficiency, which is a topic that has rarely been discussed in SCMA, a framework of SCMA based on index modulation is proposed. In addition, this thesis designs SCMA and hybrid automatic repeat request (HARQ) jointly based on inter-packet network coding for high reliability.

His key publications include:

[1] K. Lai, J. Lei, Y. Deng *et al.*, "Analyzing Uplink Grant-Free Sparse Code Multiple Access System in Massive IoT Networks," *IEEE Int. Things Journal*, 9(7):5561-5577, 2022.

[2] K. Lai, W. Lei, J. Lei *et al.*, "Codeword Position Index Based Sparse Code Multiple Access System," *IEEE Wireless Communs. Letts*, 8(3):737-740, 2019.

[3] K. Lai, J. Lei, W. Lei *et al.*, "Codeword Position Index Modulation Design for Sparse Code Multiple Access System," *IEEE Trans. Veh. Technol.*, 69(11):13273-13288, 2020.

[4] 赖恪，雷菁，刘伟，文磊，基于网络编码的稀疏码多址HARQ方案，*通信学报*，43(9):57-69，2022。

[5] K. Lai, W. Lei, J. Lei, G. Chen, X. Pei, M. Amine, "Secure Transmission with Interleaver for Uplink Sparse Code Multiple Access System," *IEEE Wireless Commun. Lett.*, 8(2):336-339, 2019.

[6] K. Lai, Lei. W, J. Lei, G. Chen, W. Li, X. Pei, "Secure Transmission with Randomized Constellation Rotation for Downlink Sparse Code Multiple Access System," *IEEE Access*, 6:5049-5063, 2017.

[7] K. Lai, Liu Z, J. Lei *et al.*, "Sparse Code Multiple Access with Enhanced K-Repetition Scheme: Analysis and Design," *IEEE Trans. Wireless Communs.*, 2022. (Major Revision)