

IEEE Information Theory Society Newsletter



Vol. 69, No. 3, September 2019

EDITOR: Salim El Rouayheb

ISSN 1059-2362

The International Symposium on Information Theory (ISIT), our Society's flagship conference, took place a few weeks ago in Paris. It was there, in *la ville-lumière*, that many of us were able to discern some light at the end of the tunnel we felt we entered more than a year ago. But some have told me that they did not think we got completely out of the (Vail) woods yet. I am now at home, looking at the skyline of Manhattan, *the city that never sleeps*, and reflecting back on the ISIT and the time from the beginning of the year.

The ISIT was a great success by all measures. (Alright, I know, many would use different words for the banquet, and I will come back to that.) We had a record number of attendees and a very exciting plenary and regular program. We had five special sessions on information theory and related fields, as a part of this year's new initiative I wrote about in the March issue. The membership events were, as always, well attended and well received. We had a superb Shannon lecture, delivered flawlessly by Erdal Arıkan followed by a very lively discussion.

The annual Society's awards, listed later in this issue, were presented at the ISIT award ceremony. Our small Society (by

Robert J. McEliece and Elwyn Berlekamp who have recently passed away.

As a reminder, Announcements, news, and events intended for both the printed newsletter and the website, such as award announcements, calls for nominations, and upcoming conferences, can be submitted at the IT Society website <http://www.itsoc.org>. Articles and columns can be e-mailed to me at salim.elrouayheb@rutgers.edu with a subject line that includes the words “IT newsletter.”

The next few deadlines are:

Oct 10, 2019 for the issue of December 2019.

Jan 10, 2020 for the issue of March 2020.

April 10, 2020 for the issue of May 2020.

Please submit plain text, LaTeX, or Word source files; do not worry about fonts or layout as this will be taken care of by IEEE layout specialists. Electronic photos and graphics should be in high resolution and sent as separate files.

Salim El Rouayheb

IEEE Information Theory Society Newsletter

IEEE Information Theory Society Newsletter (USPS 360-350) is published quarterly by the Information Theory Society of the Institute of Electrical and Electronics Engineers, Inc.

Headquarters: 3 Park Avenue, 17th Floor,
New York, NY 10016-5997.

Cost is \$1.00 per member per year (included in Society fee) for each member of the Information Theory Society. Printed in the U.S.A. Periodicals postage paid at New York, NY and at additional mailing offices.

Postmaster: Send address changes to IEEE Information Theory Society Newsletter, IEEE, 445 Hoes Lane, Piscataway, NJ 08854.

© 2019 IEEE. Information contained in this newsletter may be copied without permission provided that the copies are not made or distributed for direct commercial advantage, and the title of the publication and its date appear.

1008 T(cial advamation c)TMT(amety 5Tvw 26.569 0 Td (-nnT008h 5v To 12 Td i 12 5 (b 12c.)i 3 (t 3 (0. 3i 12 3s 5v Td c 12 8d (-n23i 33em 35d i 33nation c)ar)- 5 (t 3nT008i69 0 908h 12 5 (nat.3d, o 3Twar)11 Td (-n33a 12 3s 5v 3v 3

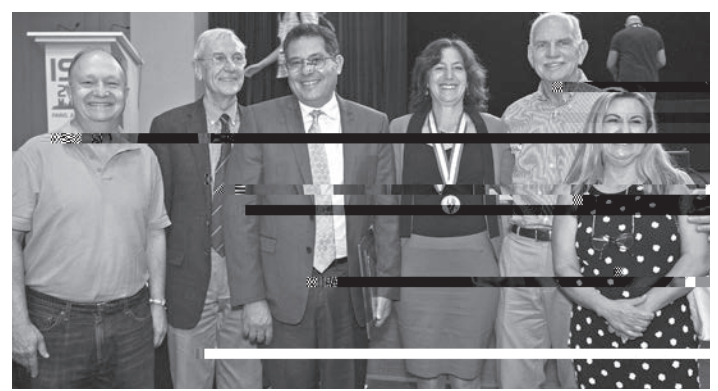
Table of Contents

President’s Column	1
From the Editor	2
Awards	3
From Sequential Decoding to Channel Polarization and Back Again	5
Tooting Our Horns: Practicing and Preparing Research Pitches	15
11th Asia-Europe Workshop (AEW11) on “Concepts in Information Theory and Communications”	15
40th Symposium on Information Theory in the Benelux	16
The Fifth London Symposium on Information Theory (LSIT)	17
In Memoriam: Robert J. McEliece (1942–2019)	19
In Memoriam: Elwyn Berlekamp (1940–2019)	21
Recent Publications	25
Call for Papers	30
Conference Calendar	36

Awards

Congratulations to the members of our community that have recently received recognition for their exceptional scholarly contributions.

ISIT 2019 Awards Ceremony



From Sequential Decoding to Channel Polarization and Back Again

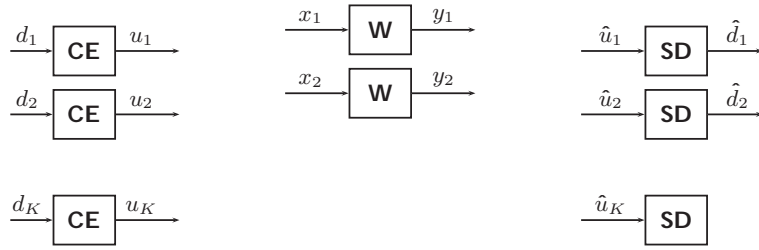
Güçer Çit'ın

Department of Electrical and Electronics Engineering
Bilkent University, Ankara, 06800, Turkey

II. CONVOLUTIONAL CODES AND SEQUENTIAL DECODING

Convolutional codes are a class of linear codes introduced by Elias [2] with an encoder mapping of the form $\mathbf{x} = \mathbf{dG}$ where the generator matrix \mathbf{G} has a special structure that corresponds to a convolution operation. An example of a convolutional code is

III. MASSEY'



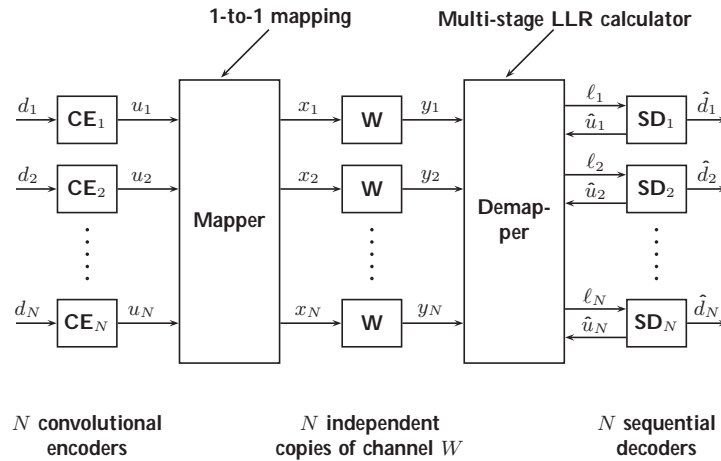
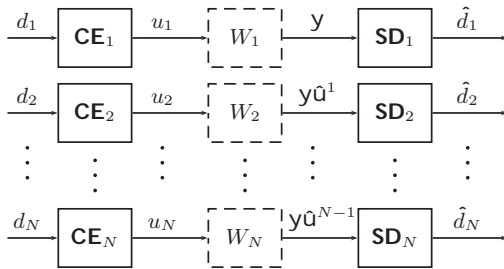


Fig. 8. Multi-level coding



Hki0 ;0 Dkv e jcpngmu etgcvgf d{ ONEIOUF

consider only this ideal case with no decision errors. Hence, from now on, we suppose that \mathbf{W} has this ideal form.

An important property of the MLC/MSD scheme is the conservation of capacity,

$$\sum_{=1}^N \mathbf{C} \mathbf{W} = \sum_{=1}^N \mathbf{I} \mathbf{U} \mathbf{Y} \mathbf{U}^{-1} = \mathbf{I} \mathbf{U} \mathbf{Y} = \mathbf{N} \mathbf{C} \mathbf{W} ,$$

where the second equality is obtained by writing $\mathbf{I} \mathbf{U} \mathbf{Y} \mathbf{U}^{-1} = \mathbf{I} \mathbf{U} \mathbf{Y} | \mathbf{U}^{-1}$ based on the assumption that \mathbf{U} and \mathbf{U}^{-1} are independent and then using the chain rule.

Vjg ONEIOUF uejgog eqpugtngu ecrcekv{ cv cp{ fpkvg construction size \mathbf{N} while Pinsker's scheme conserves capacity only in an asymptotic sense. Thus MLC/MSD uses informa- vkkp oqtg ghlekgnv{ cpf jgpeg oc{ dg gzrgevfg vq cejkgxg c given performance at a lower construction size (leading to a lower complexity).

On the other hand, unlike Pinsker's scheme in whi.4m)1o(ce)-30a0>3.90540n)65(c6t0>3..3(s)-48651lo)17l(w)-1.7e)4.22(i)-1o(ce)6.911

without any reference to their origin.

A *polar code* is a linear block code characterized by three parameters: a code block-length \mathbf{N} , a code dimension \mathbf{K} , and a data index set \mathcal{S} . The code block-length is constrained to be a power of two, $\mathbf{N} = 2^n$ for some $n \geq 0$. The code dimension can be any integer in the range $0 \leq \mathbf{K} \leq \mathbf{N}$.

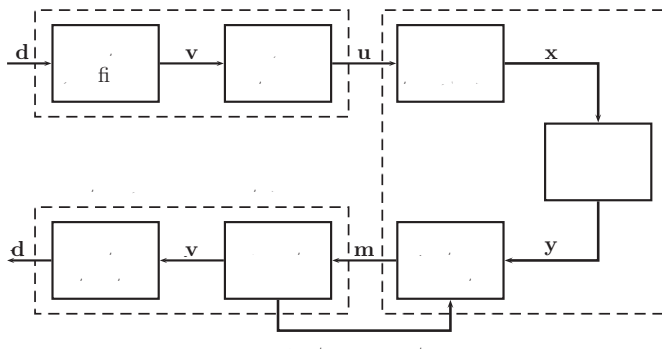


Fig. 13. PAC coding scheme.

polar transform. A low-complexity encoding alternative is to eq or wvg {tuv u vT and then x uP .

As usual, we characterize the convolution operation by an impulse response $c = c_0, \dots, c_{m-1}$, where by convention we assume that $c_0 \neq 0$ and $c_{m-1} \neq 0$. The parameter m is called the constraint length of the convolution. The input-output relation for a convolution with a given impulse response $c = c_0, \dots, c_{m-1}$ is

$$u_j = \sum_{i=0}^{m-1} c_i v_{j-i}$$

where it is understood that $v_{j-i} = 0$ for $j < i$. The same convolution operation can be represented in matrix form as $u = vT$ where T is an upper-triangular Toeplitz matrix,

$$T = \begin{bmatrix} c_0 & c_1 & c_2 & \dots & c_{m-1} & \dots & \dots \\ & c_0 & c_1 & c_2 & \dots & c_{m-1} & \dots \\ & & c_0 & c_1 & \dots & c_{m-1} & \dots \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & & & & c_0 & c_1 & c_2 \\ \vdots & & & & & c_0 & c_1 \\ \dots & \dots & \dots & \dots & & & c_0 \end{bmatrix}.$$

To illustrate the above encoding operation, consider a small example with $N = 8$, $K = 4$, $c = [1, 1, 1, 1]$, and $d = [d_1, \dots, d_4]$ into $v = [v_1, \dots, v_8]$

generates the well-known RM codes [22], [23] when \mathbf{T} is the identity transform.

We now turn to decoding of PAC codes. For purposes of

The first event we hosted as co-chairs of the Women in Information Theory Society (WITHITS) was a short lunch workshop at ISIT 2019 which focused on developing research pitches. Communicating our work and sharing our ideas with colleagues is a very important part of being a researcher, and yet this is a skill that is not often formally taught. In the process of brainstorming for this event, we reflected upon our journeys from graduate students to faculty, and recalled feeling nervous when describing and presenting one's research identity in casual conference networking events. Our aim with this workshop was to give participants an opportunity to practice communicating and promoting their own work in a safe and encouraging environment. As an additional goal, we hoped that being able to connect and meet other women and mentors on the first day of the conference would catalyze further conversations and provide relationships of support that would build confidence for participants to fully enjoy and engage in productive research conversations through the remainder of the conference.

The workshop started off with Tara Javidi sharing some guidelines on what makes a good research pitch. Plenary speaker Muriel Medard as well as Daniela Tuninetti and Lalitha Sankar shared examples of pitches as well—giving examples in different settings,

such as pitches to a funding agency, pitches about a conference talk, or pitches to a friend or family member. After hearing advice and examples, the rest of the event was dedicated to practicing in small groups to answer the following prompt: Suppose that you meet a new person at coffee break that greeted you with “Hello, nice to meet you! What do you work on?” The participants took turns to practice their response and give each other constructive feedback on their pitches. Senior members of the community were present to give feedback as well.

There were more than 120 people who attended the event. We received very positive feedback for the event—some groups discovered new research connections in their work, some participants were inspired to replicate the same event at their own university or lab group meetings, and other participants even commented that we should hold the exact same event every single year! Going forward, we are excited for hosting future events that support the mission of WITHITS—addressing the needs of and encouraging the participation of our underrepresented demographics, while being of interest and use to the community at large. We envision events that provide mentoring and build a support network, and provide training and practice for other similarly important but under-taught skills for flourishing as an academic.

The 11th Asia-Europe workshop on “Concepts in Information Theory and Communications” (AEW11) was held in Rotterdam-Netherlands on July 3-5, 2019. Thirty-three participants enjoyed the beautiful venue of the clubhouse of the Royal Maas Rowing and Sailing Club at the quay of a branch of the river Rhine, called the Maas in the very center of Rotterdam.

The workshop is based on a long-

of knowledge and ideas; 3) pay a tribute to a well-respected and special scientist.

For this workshop, Hiroyoshi Morita accepted the invitation to be the guest of honor and to be the key lecturer. Hiro is a well-known information theorist with many original contributions. We have also appreciated very much his many contributions to the Information theory community in general. Hiro gave an overview on 'Antidictionary and its Applications'.

The other sixteen presentations showed examples of concepts of error correcting codes, time series analysis, cryptography, multi-

server load balancing, convolutional codes, and coding for memories. The proceedings of the workshop can be found at <https://arxiv.org/abs/1907.02944>.

The workshop started with an informal get-together on Wednesday evening. On Thursday evening, after a reception in the garden near the river, a delicious dinner was served for attendees and spouses in the clubhouse's great hall. The workshop was concluded with a boating and hiking trip to Kinderdijk, a well-preserved Dutch polder with nineteen original windmills that have kept the Dutch feet dry for many centuries.

research fields were addressed, from quantum cryptography to biomedical signal processing to signal detection and estimation. The best student paper award was won by Simon Geirnaert (KU Leuven) for “Expected Switching Time: a Markov Chain Based Performance Metric to Evaluate Auditory Attention Decoding Algorithms”, joint work with T. Francart and A. Bertrand. The best student presentation award was won by Miao Sun (TU Delft), for “Atrial Activity Extraction Based on Graph-Time Signal Processing”, joint work with E. Isufi, N.M.S. de Groot, and R.C. Hendriks.

At the WIC General Assembly that took place during the symposium, Ludo Tolhuizen from Philips Research was awarded the honorary membership of the WIC for his extensive service to the WIC. In particular, he has served as a board member since 1998. During the years 1998-2006 and 2010-2019 he was the WIC secretary.

The symposium proceedings and slides of the keynotes are available via w-i-c.org. At this web site also future events will be an-



nounced. The 2020 Symposium on Information Theory and Signal Processing in the Benelux will be organized by TU Eindhoven, dates to be decided. Information theory in the Benelux is alive and kicking!

Two weeks after the end of post-war soap rationing, and a month after BBC's first overseas live TV broadcast (from France), a distinguished group of academics gathered at the Royal Society in London to talk about information theory. It was 1950—only two years after the publication of Shannon's seminal paper and of Wiener's “Cybernetics”—and the new ideas of information, control, and feedback were quickly making their way from engineering to the natural, social, and human sciences, begetting new insights and raising new questions.

This “cybernetic moment” [2] underpinned the first four editions of the London Symposium on Information Theory (LSIT), with the first meeting in 1950 followed by the symposia in 1952, 1955, and 1960. The program in 1950, shown in Fig. 1, featured two talks by Shannon on communications and coding, as well as a number of presentations on topics ranging from physics, statistics, and radar, to linguistics, neuroscience, psychology, and neu-

by Deniz Gündüz and Osvaldo Simeone from Imperial College

Guo (University of Bergen) on “Decryption failure attacks on post-quantum cryptographic primitives with error-correcting codes”; Leo Ducas (CWI) on “Polynomial time bounded distance decoding near Minkowski’s bound in discrete logarithm lattices”; and Thomas Prest (PQShield) on “Unifying leakage models on a Rényi day”. As the first, the second was not a rainy day and attendees were able to enjoy the view from the Bush House terrace with wine and mezes, while discussing results from poster sessions organised by Mario Berta (Imperial College London), and Kai-Kit Wong (University College London).

Videos of all talks are available on YouTube (<https://tinyurl.com/y5w92rga>).

Registration was free and more than 150 students, researchers, and academics were in attendance. Support was provided by the European Research Council (ERC) under the European Union’s Horizon 2020 Research and Innovation Programme (Grant Agreements No. 725731 and 677854).

LSIT has outlived the cybernetic movement, and it may well continue beyond the current “AI moment”. The organizers hope that we will not wait for another 60 years for the next information theory meeting in London, and would like LSIT to become a regular

biennial meeting of the information theorists and researchers from

He is survived by three daughters, a son and a step-daughter.

Below is a chronological list of some of Prof. McEliece's most important achievements.

- 1) McEliece's Theorem. This theorem, which identifies the largest power of p that divides all the weights in a p -ary cyclic code, and which contains the celebrated Ax divisibility theorem as a special case, is one of the deepest mathematical results to come out of coding theory. McEliece's theorem has inspired a large and impressive body of later work by Wilson, Calderbank, Katz, and others. Reference [R1] and [R2].
- 2) The Theory of Information and Coding. In print continuously since 1977, this classic textbook book has been compared to Richard Feynman's Lectures on Physics, as a standard and authoritative book in its field. Reference [R3]

3) Erdos number one: “Ramsey Bounds for Graph Products” (with Paul Erdos and Herbert Taylor), *Pac. J. Math.* 37 (1971), pp. 45–46.

4) NASA Group Achievement Award for Voyager Mission Opera-

President's Column

daily basis in areas which often require different kind of expertise than engineers usually possess.

Some other Society's members were also extremely busy in the months leading to the ISIT in Paris. We started this year with remarkably many new members at the key positions in the Society's governance, and that meant lot of learning, consulting with each other and with our predecessors, exchanging long and frequent e-mails. We got three new officers (ordinarily, there is only one), Frank Kschischang, Aylin Yener, and Wei Yu. We got a new Society's secretary, Lara Dolecek, a new conference committee chair, Vijay Kumar, a new online committee chair, Brian Kurkoski, a new external nominations committee chair, Dan Costello, a new thesis award committee chair, Christina Fragouli, a new young scholar award committee chair, Tom Fuja, a new fellows committee chair, Antonia Tulino, and new WITHITS chairs, Gireeja Ranade and Christina Lee Yu. Even people in their second year of service, like the Society's treasurer Aaron Wagner and the Newsletter editor, Salim El Rouyaheb, had entirely new types of challenges to deal with. I would like to wholeheartedly thank them all for stepping up to their respective roles when the Society needed them the most.

Most of these new appointments were made by the diligent 2018 Nominations and Appointments Committee, chaired by Alon Oriltsky. Thank you Alon and the committee. As if he did not deserve some time off after his long service to the Society, Alon continues to lead the activities related to the Shannon documentary *The Bit Player*. The movie premiered at the World Science Festival in New York City in May, and had four other screenings: at IBM, Yorktown Heights, in June, at the World Congress of Science Journalists in Lausanne and CineGlobe Festival at CERN, Geneva, in July, and at the Computer History Museum in Cupertino in August. All shows were extremely successful. You will hear about that in the next issue. For now, I recommend reading the recent review in *Physics Today* [2]. Yes, the physicists, again.

By the time this issue of the IT Newsletter reaches you, the IEEE annual elections will be in full swing. Please vote. Our Society is managed by the Board of Governors, and each year, one-third of the BoG gets replaced by new elected members. Please vote, and then, regardless of whether you like the outcome or not, put a serious effort to make our Society better for you and your colleagues, because leading our technical field and our technical community is too important to be left to the elected few. Is that too much to ask?

Each time there is an election of any kind, I think about the first US general elections I voted in. The year was 2004, and as usual, many were happy with the outcome and many got disappointed. The late Toni Morrison (the recipient of the 1993 Nobel Prize for literature) was among the latter. She was depressed, but eventually, inspired by a conversation with a friend, she wrote the following [3]: *This is precisely the time when artists go to work. There is no time for despair, no place for self-pity, no need for silence, no room for fear. We speak, we write, we do language. That is how civilizations heal. I know the world is bruised and bleeding, and though it is important not to ignore its pain, it is also critical to refuse to succumb to its malevolence. Like failure, chaos contains information that can lead to knowledge – even wisdom. Like art.*

References

- [1] Hilbert may have said *too hard*. Many human activities (including war, by Clemenceau) are said to be too important to be left to those seemingly in charge.
- [2] Toni Feder, "Review: *The Bit Player*, an Homage to Claude Shannon," *Physics Today*, July 2019.
- [3] Toni Morrison, "No Place for Self-Pity, No Room for Fear," *The Nation*, 150th Anniversary Special Issue, April 2015.

Recent Publications

<i>Q. Wang and M. Skoglund</i>	F, C, D, A	3183
<i>Q. Wang, H. S. n, and M. Skoglund</i>	C, E	3198
<i>Y.-P. Wei, K. Banawan, and S. Uluk</i>	F, C, A	3215

<i>S. V. S. Ranganathan, D. Di Alar, and R. D. We el</i>	September 2019
--	----------------

Deep Learning: Mathematical Foundations and Applications to Information Science

IEEE Journal on Selected Areas in Information Theory

<https://www.itsoc.org/publications/journal-on-selected-areas-in-information-theory-jsait>

Call for Papers

This special issue will focus on the mathematical foundations of deep learning as well as applications across information science. Prospective authors are invited to submit original manuscripts on topics within this broad scope including, but not limited to:

- Information theoretic methods for deep learning
- Robustness for training and inference
- Understanding generalization in over-parametrized models
- Efficient and compressed model representations
- Deep generative models and inverse problems
- Large-scale efficient training of large models
- Non-convex optimization in deep learning
- Deep learning for source and channel coding.

Guest Editors

Lead Guest Editor: Alex Dimakis: dimakis@austin.utexas.edu

Richard Baraniuk: richb@rice.edu

Sewoong Oh: sewoong@cs.washington.edu

Nati Srebro: nati@ttic.edu

Rebecca Willett: willett@uchicago.edu

Submission Guidelines

Prospective authors must follow the *IEEE Journal on Selected Areas in Information Theory* guidelines regarding the manuscript and its format. For details and templates, please refer to the *IEEE Journal on Selected Areas in Information Theory* [Author Information](#) webpage. All papers should be submitted through Scholar One according to the following schedule:

Important Dates

Manuscript Due: 1 October 2019

Acceptance Notification: 15 March 2020

Final to Publisher: 5 April 2020

Expected Publication: April/May 2020

**Princeton University - Department of Electrical Engineering
and Technical Co-sponsorship with the
IEEE Information Theory Society**

Authors are invited to submit previously unpublished papers describing theoretical advances, applications, and ideas in the fields of information sciences and systems including:

- | | | |
|------------------------|-------------------------|---------------------|
| ·Information Theory | ·Coding Theory | ·Image Processing |
| ·Communications | ·Signal Processing | ·Machine Learning |
| ·Big Data Analytics | ·Reinforcement Learning | ·Optimization |
| ·Statistical Inference | ·Security and Privacy | ·Energy Systems |
| ·Networking | ·Systems and Control | ·Biological Systems |

Electronic submissions of up to 6 pages (in Adobe PDF format) including 3-4 keywords must be submitted by **December 9, 2019**. Submissions should be of sufficient detail and length to permit careful reviewing. Authors will be notified of acceptance no later than **January 16, 2020**. Final manuscripts of accepted papers are to be submitted in PDF format no later than **January 30, 2020**. These are firm deadlines that will permit the distribution of electronic



The 2020 IEEE International Zurich Symposium on Information Theory will be held at the Hotel Zurichberg in Zurich, Switzerland, Wednesday, February 26, through Friday, February 28, 2020.

High-quality technical information is available at the following website:

Website	Official
Information	For the
Conference	Organization
Details	See
the	link
below	to

The information is available at the following website: <http://www.itis.ch/>. All the information is available at the website.

Please note that the information is available at the website (A4, page 5) of the conference. The information is available at the website (A4, page 5) of the conference. The information is available at the website.

The information is available at the website. Add the information to the website.

<http://www.itis.ch/>

We look forward to seeing you at IZS.

Andreas Hofmann, M. M. Chai

Conference on Information-Theoretic Cryptography (ITC) 2020: Call for Papers

June 17-19, 2020, Boston, MA, USA

The first *Information-Theoretic Cryptography (ITC)* conference will take place on June 17-19, 2020 in Boston, MA USA. ITC is a new conference dedicated to information-theoretic aspects of cryptography, broadly defined. See the website at <https://itcrypto.github.io/> for more information.

Areas of interest include, but are not restricted to:

- Randomness extraction and privacy amplification
- Secret sharing
- Secure multi-party computation
- Information theoretic proof systems
- Differential privacy
- Quantum information processing
- Oblivious data structures
- Idealized models (e.g. ideal channels, random oracle, generic group model)
- Bounded storage models
- Private information retrieval and locally decodable codes
- Authentication codes and non-malleable codes
- Adversarial and noisy channels
- Information-theoretic reductions
- Information-theoretic foundations of physical-layer security

Papers on all technical aspects of these and related topics are solicited for submission. Papers will be peer reviewed and accepted papers will be published in conference proceedings and presented at the conference.

The conference will have two tracks: a *publication track* and a *greatest hits* track. The publication track operates in the usual way, where authors submit their papers and the

Conference Calendar

DATE	CONFERENCE	LOCATION	WEB PAGE	DUE DATE
September 24-27, 2019	57th Annual Allerton Conference on Communication, Control, and Computing	Allerton, University of Illinois at Urbana-Champaign, Illinois, USA	https://allerton.csl.illinois.edu/	Passed
November 9-12, 2019	60th Annual IEEE Symposium on Foundations of Computer Science (FOCS)	Baltimore, Maryland, USA	http://focs2019.cs.jhu.edu/	Passed
November 11-14, 2019	IEEE Global Conference on Signal and Information Processing (GlobalSIP)	Shaw Center, Ottawa, Canada	http://2019.ieeeglobalsip.org/	Passed
December 9-13, 2019				