IEEE Information Theory Society Newsletter

Vol. 68, No. 1, March 2018 EDITOR: Michael Langberg ISSN 1059-2362

President's Column

Elza Erkip

Do you believe in love at first sight? I didn't until I started graduate school. My goal was to get a Ph.D. in the general area of electromagnetics. That was the strength in my undergraduate institution, and that's what I had been trained in. But then one day a good friend, after hearing me constantly talk about how much I was enjoying Bob Gray's Random Processes course (think about sigma algebras in an introductory graduate engineering course!), gave me a spiral bound book to read. As I read theorem after theorem, I was fascinated by the elegance and depth of the results (even though I later realized what I had understood was only the tip of the iceberg), and I knew I had found my passion. The book was one of the final drafts of the first edition of "Elements of Information Theory" by Cover and Thomas, and within a few months I was a Ph.D. student in Tom Cover's group. As a fresh PhD student, I would not have imagined that I would be the President of the Information Theory Society a quarter century later. It is a great pleasure and honor to serve this society, which has a very special place in my heart.

Love may be forever, but a honeymoon doesn't last long. Shortly after I started my presidency on January 1, 2018, we had to prepare a long document for the five-year IEEE review of the Information Theory Society. Ruediger Urbanke (our Past President) and I rolled up our sleeves, and got major help from Prakash Narayan, Emina Soljanin, Daniela Tuninetti, Emanuele Viterbo, Aylin Yener and Matt LaFleur in completing a 14-section document on society activities and best practices. While being tedious, this process reminded me many of the recent accomplishments of our society:

- We have built a very strong Information Theory Schools program. We had 21 schools all around the globe in the last five years. This is a global educational initiative, with regular schools in the US, Europe, Australia, and Hong Kong. Other locations include India, Africa and South America. The number of participants during these five years significantly exceeds 1500. The tenth anniversary of the North American School of Information Theory was celebrated in 2017, with an accompanying article by Aylin Yener appearing in the December 2017 issue of the Newsletter.

- In celebration of Claude Shannon's 100'th birthday on April 30, 2016, the Information Theory Society sponsored and stimulated a large number of Shannon Centenary Celebrations around the globe. This initiative was a great success; details of all the events can be found on http://www.itsoc.org/resources/Shannon-Centenary

- Shannon's 100'th birthday celebrations also included a number of broad outreach projects, with the most ambitious one being the production of a feature length documentary on Shannon. This project was started in 2015 and is led by the director and producer Mark Levinson. I recently had the pleasure of meeting Mark in person and attending a small screening together with several movie enthusiasts and executives in New York. Who knew society presidency would also involve glamour moments like this? Mark plans to complete the documentary in the next few months and hopes to have screenings in several film festivals around the world.

- We also initiated several broad outreach activities aimed for school age children. The society, in collaboration with Britt Cruise (who also works for Kahn Academy), produced two short technical videos that explain some of the important technical contributions of our society to a broad audience, particularly to high school students. These videos covered network coding, MIMO and space time codes and can be found on

(continued on page 35)

From the Editor

Michael Langberg

Dear colleagues,

Our spring issue opens with Elza Erkip's first column as the IEEE Information Theory Society President. Please join me in warmly welcoming Elza and in wishing her and our community a fruitful and prosperous year. We continue with several exciting announcements of recent award winners from our community, a list of recent elevations of members of our community to the grade of IEEE fellow, a list of newly elected members to the IT Society Board of Governors, and a list of newly appointed IT Society Distinguished Lecturers. Congratulations to all! We are all honored as a community.

This issue includes an excellent survey article, "Information Theoretic Cryptography for Information Theorists", by Himanshu Tyagi and Shun Watanabe, which presents a historical perspective and high-level view of topics in the intersection between information theory and cryptography. The authors focus on the fundamental problem of secret key generation and conclude with an extremely useful student guide that can help a beginner ease into the area. Many thanks to the authors for their significant efforts in preparing this outstanding contribution!

The issue continues with a number of special columns and reports. We start with an ITSoc statement, that reaffirms the IEEE Code of Conduct, IEEE Code of Ethics, and IEEE Non-discrimination Policy. The ITSoc statement was recently approved by the society Board of Governors, and comes at a time of increasing awareness towards cases of harassment, bullying, and discrimination. The statement is followed by an awakening infographic summarizing the recent IEEE survey on women in tech. On a related note, we follow with our "Students' Corner" column presenting two intriguing interviews on "Career and Diversity in STEM", prepared by Mine Alsan, in which Andrea Goldsmith and Sarah Kate Wilson share experiences and thoughts on their successful career paths and on gender-related issues in our community. We continue with Tony Ephremides's Historian's column; the column "From the Field" of the IEEE Information Theory Society Brazil Chapter, by Sueli Costa, announcing the Latin American Week on Coding and Information; a report on the Munich Workshop on Physical Unclonable Functions (MPUF) 2017, by Onur Günlü, Michael Pehl, Tasnad Kernetzky, Georg Sigl, and Gerhard Kramer; a report on the 2017 IEEE Information Theory Workshop, by Stefano Rini and Po-Ning Chen; a societal call for nominations; minutes from the IEEE Information Theory Society Board of Governors meeting this fall in Chicago, by Stark Draper; and a list of recent articles published in

(continued on page 18)

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.

Table of Contents

Awards

Congratulations to the members of our community that have recently received prestigious awards and honors and to those that have been recently elevated to the grade of IEEE fellow!

We are all honored as a community!

IEEE Richard W. Hamming Medal: Erdal Arikan

The IEEE Richard W. Hamming Medal is awarded for exceptional contributions to information sciences, systems, and technology, sponsored by *Qualcomm, Inc.,* to **ERDAL ARIKAN** (FIEEE)—Professor, Department of Electrical Engineering, Bilkent University, Ankara, Turkey. *For contributions to information and communications theory, especially the discovery of polar codes and polarization techniques.*

IEEE Alexander Graham Bell Medal: Nambirajan Seshadri

The IEEE Alexander Graham Bell Medal is awarded for exceptional contributions to communications and networking sciences and engineering, sponsored by *Nokia Bell Labs,* to **NAMBIRAJAN SESHADRI** (FIEEE)— Professor ECE, University of California, San Diego, and consulting CTO, Quantenna Corporation, San Jose, California, USA. *For contributions to the theory and practice of wireless communications.*

IEEE Eric E. Sumner Award: Peter W. Shor

The IEEE Eric E. Sumner Award that recognizes outstanding contributions to communications technology—sponsored by *Nokia Bell Labs* is awarded to **PETER W. SHOR** (MIEEE)—Professor, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA. *For contributions to quantum communication and information theory.*

IEEE Kiyo Tomiyasu Award: J. Nicholas Laneman

The IEEE Kiyo Tomiyasu Award that recognizes outstanding early to mid-career contributions to technologies holding the promise of innovative applications— sponsored by *Dr. Kiyo Tomiyasu, the IEEE Geoscience and Remote Sensing Society,* and the *IEEE Microwave Theory and Techniques Society*—is awarded to **J. NICHOLAS LANEMAN** (FIEEE)—Professor of Electrical Engineering, University of Notre Dame, Notre Dame, Indiana, USA. *For contributions to wireless network communication theory, algorithms, and architectures.*

H. Vincent Poor has Been Elected a Foreign Member of the Chinese Academy of Sciences (CAS)

H. Vincent Poor, the Michael Henry Strater University Professor of Electrical Engineering at Princeton University, USA, a former Society President, and current member of the Board of Governors, has been elected a Foreign Member of the Chinese Academy of Sciences (CAS). In his letter informing Dr. Poor of his election, CAS President Chunli Bai cited his "*scientific achievements and contributions to the promotion of science and technology in China.*" The academic division of the CAS, which functions as a national academy of sciences of China, currently has 800 members and 90 foreign members.

2017 Johann-Philipp-Reis Award

Dr. Georg Böcherer of the Chair of Communications Engineering of the Technical University of Munich (TUM) was the recipient of the 2017 Johann-Philipp-Reis Award of the Information Technology Society (ITG) of the German Association of Electrical Engineering, Electronics, and Information Technology e.V. (VDE).

The award is given to engineers up to the age of 40 who have published an outstanding, innovative publication in the field of communications that have initiated, or are expected to have, an impact on the economy. The work being recognized is "Bandwidth Efficient and Rate-Matched Low-Density Parity-Check Coded Modulation" published in the IEEE Transactions on Communications in December 2015. This paper introduces a new layered architecture for coded modulation, that has received tremendous interest from the optical fiber community, including post-deadline papers and special sessions at the world's most influential optical communications conferences (OFC, ECOC). Nokia Bell Labs and Facebook have performed field trials with live traffic that verified the architecture's performance, and that demonstrated its agility. The method is being considered for the future ITU Multi-Gigabit Fast Access to Subscriber Terminals (DSL G.mgfast) standard. Nokia recently announced the first chipset (Photonics Service Engine 3) to implement Georg's shaping technique.

Johann Philipp Reis was born in 1834 in Gelnhausen and died in 1874 in Friedrichsdorf. He constructed the first device for sound transmission, the telephone. On October 26, 1861, he introduced the device for the first time in Frankfurt am Main, Germany.

The Johann-Philipp-Reis Award has been given biannually since 1986 by the VDE, the cities of Friedrichsdorf in the Taunus and Gelnhausen, and the Deutsche Telekom. The award is accompanied by a cash prize of 10.000 euro.

2018 Newly Elevated IEEE Fellows:

Erik Agrell
Chalmers University of Technology, Sweden.
for contributions to coding and modulation in optical communications

Emmanuel Candes
Stanford University, USA
for contributions to sparse and low-rank signal and image processing

Massimo Franceschetti
University of California San Diego, USA.
for contributions to random wireless networks

Pascal Frossard
École polytechnique fédérale de Lausanne, Switzerland.
for contributions to adaptive image and video representation, coding and communication

Martin Haardt
Ilmenau University of Technology, Germany
for contributions to multi-user MIMO communications and tensor-based signal processing

Aleksandar Kavcic
University of Hawaii
for contributions to signal processing and coding in data storage

Riccardo Leonardi
University of Brescia, Italy
for contributions to image and video compression and multimedia semantic content analysis

Olgica Milenkovic
University of Illinois at Urbana-Champaign, USA
for contributions to genomic data compression

Andrea Montanari
Stanford University, USA
for applications of statistical physics to coding theory

Mehul Motani
National University of Singapore, Singapore.
for contributions to wireless communications and sensor networks

Chandra Nair
The Chinese University of Hong Kong , Hong Kong
for contributions to network information theory

Girish Nair
The University of Melbourne, Australia
for contributions to control and information in networked dynamical systems

Lawrence Ozarow
Nokia
for contributions to capacity characterization of fading and feedback channels

Weifeng Su
University at Buffalo, USA.
for contributions to multi-input multi-output wireless communications and cooperative networks

Sergiy Vorobyov
Aalto University, Finland
for contributions to optimization in robust signal processing

---

Congratulation to our newly appointed Board of Governor member:

Tsachy Weissman
Stanford, USA.

Congratulations to our newly appointed Distinguished Lecturers:

Marco Dalai
University of Brescia, Italy.

Amos Lapidoth
ETH, Zurich, Switzerland.

Vincent Tan
National University of Singapore, Singapore.

Sennur Ulukus
University of Maryland, USA.

Information Theoretic Cryptography for Information Theorists

Himanshu Tyagi[†] and Shun Watanabe[‡]

At the IEEE International Symposium of Information Theory 2017, we gave a tutorial with the same title as this article. The current article summarizes the motivation for our choice of topic for those who missed our tutorial—the attendees required no such prodding. Instead of summarizing the results that we presented in the tutorial—they can be accessed from the notes we circulated during the tutorial— we provide a historical context to the topic. Furthermore, we provide a heuristic, high-level view of the results covered by us. Finally, we provide a list of references that we believe can help a beginner in the area or a student to gather the necessary background for following and contributing to the research in Informaton Theoretic Cryptography.

1. A historical Perspective

The study of cryptography in information theory started in Shannon's landmark paper [42]. It is no surprise that Shannon chose secrecy as a companion to communication for applying his newly formulated theory of information, which quantifies in bits the information contained by one random variable about

[†]Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore 560012, India. Email: htyagi@ece.iisc.ernet.in

[‡]Department of Computer and Information Sciences, Tokyo University of Agriculture and Technology, Tokyo 184–8588, Japan. Email: shunwata@cc.tuat.ac.jp

another—reliable communication of a message can be accomplished by sending sufficiently many bits and a secure communication is tantamount to curtailing the number of bits of information leaked to the adversary. Shannon's focus in [42], among other things, was on the *one-time-pad*, a basic cryptographic primitive that allows two parties sharing a secret key to send a message securely. The main result of [42] was that to send m bits of message securely over a public channel, the parties need to share a secret key comprising m random bits. The notion of secrecy used was that of *perfect secrecy*, namely the message must remain completely independent of the observations of the eavesdropper. Shannon used his newly crafted tools of entropy and conditional entropy to complete the proof, albeit for a restrictive class of encryption schemes.

In the following decade information theory was applied to fields ranging from genetics to economy, perhaps even to Shannon's surprise [41]. In all the excitement the thread of information theoretic cryptography was lost temporarily. A plausible reason for this is the negative connotation of Shannon's result: A fresh secret key of length equal to that of the message must be shared everytime a new message has to be sent securely. The lost thread was picked up by Wyner [49] who studied how inherent noise in the communication channel can be used to enable secure transmission without requiring an additional secret key. The model, termed the *wiretap channel*, entails two noisy communication channels, the first from transmitter to the legitimate receiver and the second from the transmitter to a (passive) eavesdropper. By this time, it was clear that Shannon's perfect secrecy requirement can be relaxed to the more nominal notion of secrecy where only a bound on the leaked information, as measured by the mutual information, is imposed. Wyner characterized the largest rate of a message that can be transmitted securely, the capacity, of a degraded wiretap channel, namely a wiretap channel where the eavesdropper observes a further noisy version of the observation of the legitimate receiver. The follow-up works of Csiszár and Körner [14] and Cheong and Hellman [30] extended these results to a general discrete wiretap channel and the Gaussian wiretap channel, respectively. These fundamental results underlie the effort in enabling security in the physical layer of a communication network, an area that has seen significant research interest over the last two decades (see [8] for a review).

But this revived interest in these classic works of information theory is a relatively new phenomenon. In the years following these works, another revolution was brewing in security circles which shifted the focus from these developments in information theory. Prior to World War II, construction of cyphers and cryptanalysis was largely based on ingenuity of expert cryptographers who used long tables to hand-compute the codes. In their effort, they were often supported by complicated mechanical constructs. Perhaps the most popular relic of this era is the infamous Enigma machine. But things changed rapidly after the war. As the available computation power improved rapidly, and the business demand for cryptographic primitives such as user authentication surfaced, the role of computers in enabling cryptography became clear. In fact, starting from the late 60's, an engineering wisdom emerged which made it clear that Shannon's perfect security might be an overkill for cryptography. Just like legitimate parties, the adversary, too, has a limited computation power. This engineering progress was coupled with a better understanding of the relationship between computationally difficult problems (see, for instance, Karp's seminal work [27]). Several bespoke security solutions surfaced that relied on inducing an asymmetry between the computational requirements of the legitimate parties and the adversary for solving certain algebraic problems. For an early example of a security solution that relied on the available computational resources of the time, see [36]. These efforts culminated in the landmark paper of Diffie and Hellman [18], where the concept public-key cryptography system based on the difficulty of computing discrete logarithm was proposed. A heuristic notion of a one-way-function, which can be easily computed, but requires formidable computational power for inversion, was given. Furthermore, a distinction was made between the information theoretic notion of security and the notion of computational security. From here on, practitioners security became computational, rather than information theoretic.

In a span of few years following the work of Diffie and Hellman, several new cryptographic primitives were proposed. Most were secure in the informal sense of computational security. However, a formal proof of security, or even a methodology for attempting such a proof, was missing. This gap was filled by [21] where a modern view of security proofs was proposed: A system can be deemed secure if an averasary who interacts with the system cannot distinguish it from an ideal secure system, with a sufficiently high reliability. Information theoretic security could now be viewed as allowing an adversary to have unbounded computation power, while computational security would limit the adversary's computational ability. A proof of computational security will involve showing that if the adversary can distinguish the real system from the ideal system, then he will be able to solve a computational problem, which is believed to be hard. This launched the formal area of theoretical cryptography.

Parallel to these developments, a better understanding of the role of randomness in enabling algorithms was emerging. In many computer science problems, including those related to cryptography and random number generation, it was important to quantize the amount of randomness that can be extracted. One of the goals was to characterize the power of a random source to yield uniform random bits. A key result of this line of research is the *leftover hash lemma* (*cf*. [25]) which relates the number of bits of randomness that can be extracted from a source to its min-entropy.

Another related thread from the 80s is that of *quantum key distribution* (QKD) introduced by Bennett and Brassard. This relied on using quantum resources to generate shared secret keys between two parties, with additional use of a public communication channel when noise is present. This led to the formulation of the secret key agreement problem with public discussion in [7]; interestingly, this formulation was under information theoretic secrecy. Partly in response to the threat posed on computational cryptography by quantum computing algorithms [43], QKD and related problems have been actively studied in the past few decades.

With these developments, the paths of information theoretic security and cryptography based on computational security, that had diverged temporarily, reunited. Randomness became an essential resource for cryptography, and information theoretic notions of information leakage and deviation from uniformity made regular appearances in cryptography papers. In fact,

many of the reduction steps in security proofs given in cryptography hold for even information theoretic security.

Following this confluence, in the information theory circles, a new formulation of the secret key agreement problem due to Maurer [31] gained prominance. Maurer studied the maximum rate of a secret key that can be generated by two parties observing correlated random variables and with access to a public communication channel. Both source and channel models were considered. Similar results were obtained independently, though inspired by a conference version of Maurer's work, in [1]. Subsequently, a multi-terminal variant of the secret key agreement problem was introduced in [16], [17]. These formulations and the results were closer in semantics to Wyner's wiretap channel formulation and revived the study of security in information theory community.

On the cryptography side, similar information theoretic formulations appeared. A specific example is that of *secure multiparty computation*, a multiparty extension of Yao's classic two-party formulation in [50]. When the number m of parties is larger than 2, it is known that information theoretically secure multiparty computation is possible if the number t of malicious parties is below a threshold [5], [10]—the threshold is $t < m/2$ when the malicious parties are passive and follow the prescribed protocol and $t < m/3$ for actively malicious parties. For two-party secure computation, only "trivial" functions are securely computable [4], [29] under information theoretic security. However, when certain additional resources are available, information theoretically secure computation is feasible. A commonly used resource is the *oblivious transfer* primitive, introduced in [37], [19]. In fact, any function can be securely computed, even information theoretically, once oblivious transfer is realized [28]. Interestingly, oblivious transfer itself can be realized from a noisy channel between the two parties [13]. A study of the rate at which instances of (randomized) oblivious transfer can be implemented using a noisy channel as a resource has been the subject of recent interest (see [34], [3]).

If an information theorist flips through the dense proceedings of a leading cryptography conference, he may be surprised to identify many of his favorite tricks utilized in a manner perhaps unfamiliar to him. The fields of information theory and modern cryptography are now intertwined. Our tutorial at ISIT 2017 was aimed at reviewing some of our favorite results at the intersection of these two fields. While we had the attention of the audience, we also took the opportunity to present our own recent results in this area. We summarize the results we covered for the secret key generation problem in the next two sections and close with a student's guide for navigating this area in the final section. We only provide a high-level description of the results; details can be found in the tutorial slides and the accompanying notes. A detailed review of all the results we discuss can be found alternatively in [33].

2. Protocols and Converses

In the secret key agreement problem, two parties observing correlated data want to share almost uniformly distributed bits. To that end, they communicate over a public channel, possibly using interactive communication. They need the shared bits to remain secure from an eavesdropper with access to the communication channel. We review the protocols for secret key agreement and the various strategies for proving the upper bounds, *i.e.*, the converse results.

Note that a proof of security in the modern cryptography literature entails relating the security of the system at hand to that of a more basic primitive. Such arguments are called *reduction* arguments. Typically, there are no converse results available in computational security. In contrast, the proof of security of a protocol in information theoretic cryptography typically entails showing a bound on the information leaked to the eavesdropper during the execution of the protocol. Interestingly, a converse proof that we show below involves reducing independence testing to secret key agreement.

Formally, the secret key agreement problem can be described as follows: Two legitimate parties $\mathcal{P}_1$ and $\mathcal{P}_2$ observe random variables X and Y taking values in $\mathcal{X}$ and $\mathcal{Y}$, respectively. Upon making these observations, the parties communicate interactively over a public communication channel that is accessible to an eavesdropper. At the end of the communication protocol, the parties generate secret keys K_1 and K_2, respectively. The transcript Π of the protocol is available to the eavesdropper; in addition, the eavesdropper observes a random variable Z. We require that the keys K_1 and K_2 agree with high probability (reliability) and are almost independent of the observations (Z, Π) of the eavesdropper (secrecy). These requirements are succinctly captured by the following equations: There exists a random variable K with range $\mathcal{K}$ such that

$$\begin{aligned} &\Pr(K_1 = K_2 = K) \geq 1 - \varepsilon, \\ &d(\mathrm{P}_{K\Pi Z}, \mathrm{P}_{\mathrm{unif}} \times \mathrm{P}_{\Pi Z}) \leq \delta, \end{aligned}$$

where $d(\cdot, \cdot)$ is the variational distance. When the above two conditions are satisfied, it is said that K constitues an (ε, δ)-secret key. Then, we are interested in characterizing the supremum length $S_{\varepsilon,\delta}(X, Y \mid Z)$ over the length $\log |K|$ of an (ε, δ)-secret key. Note that the security condition above can be viewed as a bound on the information leaked to the eavesdropper. Alternatively, it can be viewed to imply a bound on the statistical distance between an ideal protocol's view, captured by the distribution $\mathrm{P}_{\mathrm{unif}} \times \mathrm{P}_{\Pi Z}$ and the real protocol corresponding to $\mathrm{P}_{K\Pi Z}$. The choice of variational distance above is common in cryptography; but any other measure of distance between distributions could have been used here. We justify this choice with the clear dependence on δ that appears in the bounds that we discuss.

A secret key agreement protocol consists typically of two steps: *Information reconciliation* and *privacy amplification*. In the information reconciliation step, the parties engage in public communication to convert their correlated observations into shared random bits, termed *common randomness*. This is typically realized by using Slepian-Wolf codes [44], [11]. Heuristically, based on its observation Y, $\mathcal{P}_2$ forms a list of guesses for X. $\mathcal{P}_1$ applies a random hash function to its observation X and sends it to $\mathcal{P}_2$, which in turn compares the hash value with each entry in its list. Single-shot bounds for this scheme for Slepian-Wolf codes were derived in [32], [22], where an information spectrum approach was used to come-up with a guess list for $\mathcal{P}_2$ (see, also, [38] for a related approach using the smooth max-entropy). Note that this scheme is only a theoretical construct. Typically, the list formed at $\mathcal{P}_2$ is of exponential size, and the task of finding a matching hash over that list is of formidable computational

complexity. Practical variants of this scheme involve the use of efficient channel codes.

The common randomnes generated in the information reconciliation step need not be distributed uniformly. More importantly, a part of this information was revealed to the eavesdropper via the communication transcript. In the privacy amplification step, a secure randomness almost independent of the transcript and the eavesdropper's observation Z is extracted. This relates to a question of fundamental interest: How many bits of randomness independent from Z can be extracted from X? This second step is realized by using a randomly chosen member of a 2-universal hash family (2-UHF) [9], the simplest example of which is the class of all mappings with a given range set, *i.e.*, the popular random binning. The abstraction of a 2-UHF allows us to use more efficient constructions that serve essentially the same role as random binning. The required secret key is then obtained by applying a randomly chosen member of a 2-UHF (sampled using shared randomness) to the common randomness generated by the parties in the first step. A formal proof of security of the ensuing scheme requires a bound on the information leaked about the output of a 2-UHF to an observer of side-information Z. Several such bounds are available in the literature (*cf.* [7], [6]). Perhaps the most convenient form of this bound, termed the leftover hash lemma, appears in Renner's thesis [39], where it is shown that one can roughly extract as many bits of randomness from X independent of Z using a 2-UHF as the *smooth conditional min-entropy* of X given Z, denoted $H^{\varepsilon}_{\min}(\mathrm{P}_{XZ}|Z)$. Furthermore, when additionally the eavesdropper has access to an l bit function of X, such as the transcript Π, the amount of uniform randomness that can be extracted independent of (Z, Π) reduces to $H^{\varepsilon}_{\min}(\mathrm{P}_{XZ}|Z) - l$. This can be viewed as a simple extension of the classic form of leftover hash lemma derived in [25].

Note that there are several variants of the definition of smooth conditional min-entropy used in literature; one can simply choose a definition that is the most convenient for the use-case at hand. However, all these variants have the same limiting behavior—for i.i.d. X^n and Z^n, the rate of smooth conditional min-entropy convergences to $H(X|Z)$. In fact, it can be shown that the scheme above yields a secret key of rate $H(X|Z) - H(X|Y)$.

We now move to the proof of upper bounds for the secret key length possible. The first such bound appeared in [31], [1] where it was shown that roughly

$$S_{\varepsilon,\delta}(X,Y|Z) \lesssim \frac{1}{1-\varepsilon-\delta} \cdot I(X \wedge Y|Z),$$

which for the i.i.d. case yields an upper bound of $I(X \wedge Y|Z)$ for the secret key rate. In general, this upper bound deviates from the lower bound of $H(X|Z) - H(X|Y)$ achieved by the scheme above. However, the two bounds coincide for the case when the observation of the eavesdropper is a degraded version of that of a legitimate party, *i.e.*, when the Markov relation $X \multimap Y \multimap Z$ holds.

The proof of the bound above allows interactive communication. A property of interactive communication that is leveraged is that conditioning on interactive communication cannot increase the correlation between two random variables. Formally,

$$I(X \wedge Y|Z, \Pi) \leq I(X \wedge Y|Z).$$

An important consequence of this observation is that if X and Y are conditionally independent given Z, they remain conditionally independent when conditioned additionally on an interactive communication Π.

A shortcoming of the converse bound above is that it implies a multiplicative loss of $1/(1-\varepsilon-\delta)$. An alternative bound derived in [45], [46] using a different approach allows us to replace this multiplicative loss with an additive loss of $\log 1/(1-\varepsilon-\delta)$. This alternative bound is derived by using a reduction argument that relates secret key agreement to testing the conditional independence of X and Y given Z. Specifically, it can be shown that the length of the secret key is roughly bounded by the exponent of the probability of error of type II for the aforementioned conditional independence testing, when the probability of error of type I is less than $(1-\varepsilon-\delta)$. Heuristically, this reduction is appealing: The ability of the parties to generate a secret key of large length is related to how far the distribution P_{XYZ} is from $\mathrm{P}_{X|Z}\mathrm{P}_{Y|Z}\mathrm{P}_{Z}$, a distribution useless for generating a secret key. In the asymptotic regime with i.i.d. observations, this aleternative bound yields a strengthening of the bound above. For instance, it yields a strong converse theorem for secret key agreement and even a characterization of the second-order asymptotic term in the optimal secret key length.

A third approach for proving converse entails establishing a *monotone* for the protocol, namely a quantity that must decrease at every step of the protocol and satisfies some abstract properties. Such abstract bounds provide a general, unified view of both the bounds above and can even yield bounds that improve the ones obtained from the approaches outlined above (see, for instance, [20], [40]). A similar approach for proving bounds has found applications in other problems of cryptography as well; see [48], [35] for applications in secure multiparty computation.

3. Multiple Parties, Interaction, and Universality

A multiparty variant of the secret key agreement problem was formulated in [16]. There are m parties now, with the ith party observing X_i, and they can communicate to each other by broadcasting over a public communication channel. For simplicity, we assume that the eavesdropper observes only the communication and Z is a constant. As before, the parties seek to generate $K_1, \ldots, K_m$ that agree with large probability and remain concealed from an eavesdropper with access to the public communication. We only review secret key agreement protocols for multiple parties; the proof of converse bounds of the previous section extend to multiple parties.

The secret key agreement protocol we described earlier can be extended to this general case as well. However, it is unclear a priori what should the parties agree on in the information reconciliation step. An elegant solution to this problem was given in [16] where it was shown that a secret key of asymptotically optimal rate can be generated by agreeing on the collective observations of the party $(X_1, \ldots, X_m)$, termed attaining *omniscience*. Thus, if l bits of communication over the public channel are used to attain omniscience, we can generate a secret key of length roughly $H^{\eta}_{\min}(\mathrm{P}_{X_1 \ldots X_m}) - l$ can be extracted using the privacy amplification as before.

Till this point, we have only addressed the role of interaction in the converse bounds, but have not discussed if indeed the optimal protocols require interactive communication. In fact, for the two-party setting, when the Markov relation $X \multimap Y \multimap Z$ holds, a simple one round communication protocol yields a secret key of optimal rate. Even in the multiparty case described above, [16] used a standard, noninteractive Slepian-Wolf scheme to attain omniscience. On the other hand, [31] illustrated an interactive scheme that outperforms any simple noninteractive scheme when for a general distribution P_{XYZ}. Also, the aforementioned second-order asymptotic rate optimal secret key of [24] is attained using an interactive Slepian-Wolf code. A high-level description of the protocol is as follows. As for the standard Slepian-Wolf code, the party observing Y forms a guesslist for X. But now the size of the guesslist is not fixed. The party starts optimistically with a smaller guesslist and gradually increases the size of the list in each round of interaction when it cannot find any entry with matching hash. If no entry is found, a NACK is sent to the first party, who then sends additional bits of hash that are used to find the matching entry in the larger guesslist used in the next round.

In fact, the interactive Slepian-Wolf protocol described above is universal and does not even require the knowledge of the distribution (however, in the universal case, it is optimal only up to the first-order term and has a redundancy of $O(\sqrt{n \log n})$, where n is the observation length. In [47], building on this two-party protocol, a universal protocol for attaining omniscience in the multiparty setting was proposed. An interesting issue arises in the multiparty setting, which party must start the communication? The optimal protocol proceeds by first sharing the empirical entropies of the local sequences of all the parties. The party with the highest empirical entropy starts the communication and increases its rates in small steps. The party with the second highest empirical entropy starts communicating when the first has communicated a rate equal to the difference of their entropies. The subsequent parties join-in following the same principle. This ensures that the difference of rates of any two communicating parties is equal to the difference of their empirical entropies at all times, a principle that is heuristically appealing. Throughout, all the communicating parties are trying to decode the observations of any subset of the communicating parties using the form guesslist and find matching hash procedure described earlier. A key observation enabling our recursive protocol is that when a party i recovers the data of party j, j also recovers the data of i. Furthermore, at this point, the rates of parties are identical to those that would have resulted if the parties i and j were executing this protocol as a single party to begin with. Thus, from here on, we can simply continue the protocol pretending that the parties i and j are collocated. Owing to this recursive structure, this protocol is termed the *recursive data exchange* protocol.

4. A Student's Guide to Information Theoretic Cryptography

At its heart, information theoretic cryptography, especially in the multiparty settings, studies how can randomness be generated and shared across parties using communication. With this broad interpretation, it has applications way beyond security, including in problems of theoretical computer science and randomized algorithms. We strongly believe, with some confluence of interest, that it is one of the fundamental themes in information theory and must be pursued actively by researchers. However, many interesting ideas in this area are burried in the detailed calculations contained in cryptography papers and are in a language that can be daunting for a student of information theory. Nevertheless, with some effort, one can find resources that are palpable for an information theorist. We close our article with a list of resources that can help a beginner ease into this area and which, we believe, can be accessed easily by anyone with background in information theory. This is a bare-minimum reading list, curated mostly based on our background.

The first topic to pick-up is secret key agreement. The formulations with source and channel models in [1] are presented in the style of the popular information theory reference [15]. Upon reading [1], one may move to [16] for multiterminal models. In fact, the connection between secret key agreement and common randomness generation, in a broader sense, becomes apparent only in the view of the omniscience-based secret key agreement presented in [16]. At this point, a reader can move to single-shot formulations and see the paper [40]. Note that [1] uses the *balanced coloring lemma* for privacy amplification, as opposed to the perhaps more standard tool of leftover hash lemma. For the latter result, and the aforementioned single-shot formulations, a good resource is Renner's thesis [39]. However, the setting in his thesis is that of quantum information theory and some readers may prefer to avoid additional complications of quantum mathematics. Some of the important techniques developed for analysing quantum security are summarized in the language of classical information theory in [23, Sections II and III]. The single-shot converse bound in [46] is quite accessible. Many of these results on multiparty secret key agreement can be accessed from the recent published monograph [33]. With this basic background, one can access most of the literature on information theoretic key agreement from the 1990s and 2000s, and the companion literature on privacy amplification.

The next topic to consider is secure function computation. This is where the picture gets murky. Some folklore results published in this area published in the late 80s or early 90s have either incomplete or faulty proofs. Perhaps the most accessible reference for these results is a much recent work [26], although it only considers the completeness of oblivious transfer in a two-party setting, namely the fact that secure two-party computation for any function can be realized using oblivious transfer. If a reader wants to stay in his or her comfort zone of information theory, the oblivious transfer problem can be understood from [2], [3], [34]. However, we suggest that at this point one takes a leap and makes a foray into a paper written in the modern cryptography language, such as the aforementioned [26], which accomodates a broader class of adversaries. For the case with more than two parties, a thorough review of multiparty secure computation can be found in the recently published book [12].

References

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography–part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[2] ——, "On the oblivious transfer capacity," *IEEE International Symposium on Information Theory*, pp. 2061–2064, 2007.

[3] ——, "On oblivious transfer capacity," *Information Theory, Combinatorics, and Search Theory*, pp. 145–166, 2013.

[4] D. Beaver, "Perfect privacy for two party protocols," *Technical Report TR-11-89, Harvard University*, 1989.

[5] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," in *Proc. Symposium on Theory of Computing (STOC)*, 1988, pp. 1–10.

[6] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, November 1995.

[7] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM J. Comput.*, vol. 17, no. 2, pp. 210–229, 1988.

[8] M. Bloch and J. Barros, *Physical-Layer Security*. Cambridge University Press, 2011.

[9] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143—154, 1979.

[10] D. Chaum, C. Crépeau, and I. Damgård, "Multi-party unconditionally secure protocols," in *Proc. Symposium on Theory of Computing (STOC)*, 1988, pp. 11–19.

[11] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley-Interscience, 2006.

[12] R. Cramer, I. Damgård, and J. Nielsen, *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, 2015.

[13] C. Crépeau and J. Kilian, "Weakening security assumptions and oblivious transfer," in *Advances in Cryptology - Crypto 88*, 1990, pp. 2–7.

[14] I. Csiszár and J. Körner, "Broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[15] I. Csiszár and J. Körner, *Information theory: Coding theorems for discrete memoryless channels*. Academic Press, 1981.

[16] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, December 2004.

[17] ——, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2437–2452, June 2008.

[18] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[19] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," *Communications of ACM*, vol. 28, no. 6, pp. 637–647, Jun. 1985.

[20] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals: Part i," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3973—3996, August 2010.

[21] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270—299, 1984.

[22] T. S. Han, *Information-Spectrum Methods in Information Theory [English Translation]*. Series: Stochastic Modelling and Applied Probability, Vol. 50, Springer, 2003.

[23] M. Hayashi, "Security analysis of ε-almost dual universal$_2$ hash functions: Smoothing of min entropy versus smoothing of rényi entropy of order 2," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3451–3476, June 2016.

[24] M. Hayashi, H. Tyagi, and S. Watanabe, "Secret key agreement: General capacity and second-order asymptotics," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, May 2016.

[25] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proc. ACM Symposium on Theory of Computing (STOC)*, 1989, pp. 12–24.

[26] Y. Ishai, M. Prabhakaran, and A. Sahai, "Founding cryptography on oblivious transfer efficiently," *CRYPTO, LNCS*, vol. 5157, pp. 572–591, 2008.

[27] R. M. Karp, *Reducibility among Combinatorial Problems*. Boston, MA: Springer US, 1972, pp. 85–103.

[28] J. Kilian, "Founding crpytography on oblivious transfer," in *Proc. Symposium on Theory of Computing (STOC)*, 1988, pp. 20–31.

[29] E. Kushilevitz, "Privacy and communication complexity," *SIAM Journal on Math*, vol. 5, no. 2, pp. 273–284, 1992.

[30] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[31] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[32] S. Miyake and F. Kanaya, "Coding theorems on correlated general sources," *IIEICE Trans. Fundamental*, vol. E78-A, no. 9, pp. 1063–1070, September 1995.

[33] P. Narayan and H. Tyagi, *Multiterminal Secrecy by Public Discussion*. Hanover, MA, USA: Now Publishers Inc., 2016.

[34] A. C. A. Nascimento and A. Winter, "On the oblivious-transfer capacity of noisy resources," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2572–2581, 2008.

[35] V. Prabhakaran and M. Prabhakaran, "Assisted common information with an application to secure two-party sampling," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3413–3434, June 2014.

[36] G. B. Purdy, "A high security log-in procedure," *Communications of the ACM*, vol. 17, no. 8, pp. 442–445, August 1974.

[37] M. O. Rabin, "How to exchange secrets with oblivious transfer," Cryptology ePrint Archive, Report 2005/187, 2005, http://eprint.iacr.org/.

[38] J. M. Renes and R. Renner, "Noisy channel coding via privacy amplification and information reconciliation," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7377–7385, November 2011.

[39] R. Renner, "Security of quantum key distribution," *Ph. D. Dissertation, ETH Zurich*, 2005.

[40] R. Renner and S. Wolf, "Simple and tight bounds for information reconciliation and privacy amplification," in *Proc. ASIACRYPT*, 2005, pp. 199–216.

[41] C. E. Shannon, "The bandwagon," *IRE Transactions Information Theory*, vol. 2, no. 1, March.

[42] ——, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[43] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[44] D. Slepian and J. Wolf, "Noiseless coding of correlated information source," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, July 1973.

[45] H. Tyagi and S. Watanabe, "A bound for multiparty secret key agreement and implications for a problem of secure computing," in *EUROCRYPT*, 2014, pp. 369–386.

[46] ——, "Converses for secret key agreement and secure computing," *IEEE Trans. Inf. Theory*, vol. 61, pp. 4809–4827, 2015.

[47] ——, "Universal multiparty data exchange and secret key agreement," *IEEE Trans. Inf. Theory*, vol. 63, pp. 4057–4074, April 2017.

[48] S. Wolf and J. Wullschleger, "New monotones and lower bounds in unconditional two-party computation," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2792–2797, June 2008.

[49] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, October 1975.

[50] A. C. Yao, "Protocols for secure computations," in *Proc. Annual Symposium on Foundations of Computer Science (FOCS)*, 1982, pp. 160–164.

ITSoc Statement to Reaffirm the IEEE Code of Conduct, IEEE Code of Ethics, and IEEE Non-discrimination Policy

Elza Erkip
ITSoc President

The following statement was recently approved by the IEEE Information Theory Society Board of Governors. The statement is followed by an infographic summarizing the recent IEEE survey on Women in Tech.

IEEE members are committed to the highest standards of integrity, responsible behavior, and ethical and professional conduct. The IEEE Information Theory Society reaffirms its commitment to an environment free of discrimination and harassment as stated in the IEEE Code of Conduct, IEEE Code of Ethics, and IEEE Nondiscrimination Policy. In particular, as stated in the IEEE Code of Ethics and Code of Conduct, members of the society will not engage in harassment of any kind, including sexual harassment, or bullying behavior, nor discriminate against any person because of characteristics protected by law. In addition, society members will not retaliate against any IEEE member, employee or other person who reports an act of misconduct, or who reports any violation of the IEEE Code of Ethics or Code of Conduct.

Women's Experiences in Tech

In a recent IEEE survey, 4,579 women responded to questions on being a woman in tech. The detailed findings reveal discouraging experiences and perceptions within the industry.

Many women experienced the same negative incidents at alarmingly high rates...

73%
Have Experienced Negative Outcomes in Their Careers Attributed to Being a Woman

71% said questions or comments were addressed to males when questions should have been addressed to her

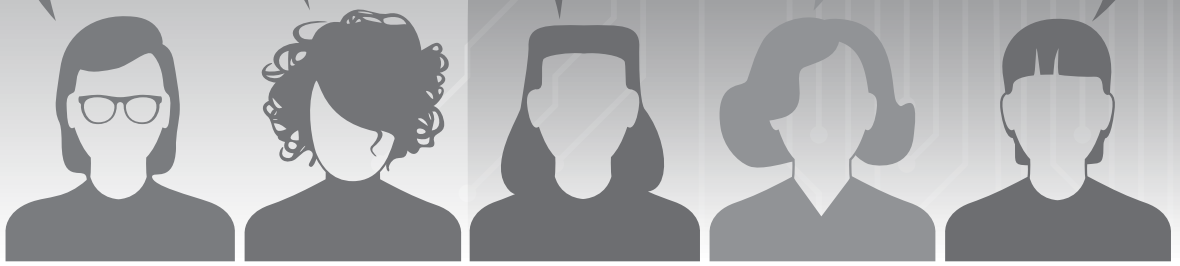
58% were asked inappropriate questions during interviews

39% were assigned lower-level tasks

37% were excluded from networking opportunities

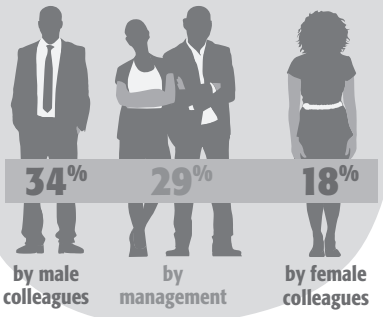
28% have experienced unwanted sexual advances

86% from colleagues | **58%** from a superior | **45%** from a client



WOMEN FEEL MISTRUSTED

Women report feeling a lack of trust from all levels across an organization.



GROUP DIFFERENCES

Those in the **US** have more **negative perceptions** and were more likely to experience **negative outcomes**

Those who work in **private industry** were more likely to have **negative perceptions** and experience **negative outcomes**

FAMILY MATTERS

51% felt need to speak less about family to be taken seriously

38% of mothers on maternity leave returned early for fear of negatively impacting career

For more information on this study, please contact women-in-tech-project@ieee.org

IEEE *Advancing Technology for Humanity*

Students' Corner: Career and Diversity Interview with Two Women in STEM

Mine Alsan

We are pleased to highlight experiences from two inspiring and serving members of the IEEE and our Society. We asked them several questions related to their career paths and diversity with an emphasis to reflect on the time when they were graduate students. They had no hesitation to share with us some of their experiences, thoughts, and advice. Meet the mastermind behind the Reviewer Appreciation Program of ComSoc, Prof. Sarah Kate Wilson, recently awarded the 2017 IEEE Communications Society Joseph LoCicero Award for Exemplary Service to Publications, and the first ever Chair of the IEEE committee on Diversity and Inclusion, Prof. Andrea Goldsmith, recently awarded the 2017 Comsoc WICE mentoring award.

Prof. Andrea Goldsmith, Stanford University

Part I: Career Oriented Questions

1. What was the subject of your Ph.D. thesis? If you were doing a Ph.D. thesis today, which topic would you chose?

My thesis investigated Shannon capacity limits as well as high-performance design of wireless communication systems. After working in the defense communications industry for 3 years before returning for my doctorate, I was enamored with wireless communications, and lucky enough to return to grad school to gain more knowledge of this area just as Wi-Fi and digital cellular systems were taking off. I was intrigued to study in my doctorate the fundamental performance limits for these emerging systems, and the designs needed to achieve performance close to these limits. Shannon theory was a beautiful and entrancing topic, while also providing practical design insights. How these practical designs performed relative to the Shannon limits provided insights into refining and expanding the wireless information theory problems I was investigating. This research trajectory between Shannon limits of wireless systems and designs to achieve those limits was far more satisfying for me than focusing on only one of those two research dimensions.

My choice of a Ph.D. topic today would be driven by the same philosophy I had at the time: find a topic you love that intrigues you, ideally in an area that has not yet received a lot of focus from other researchers. Working on the "hot topic" of the day is not typically a good strategy, as that hot topic may not be hot or may be saturated with other researchers by the time you graduate.

2. Can you tell us a result you derived when you were a Ph.D. student and you are most proud of?

My most satisfying result as a Ph.D. student was my derivation of the capacity of fading channels with perfect transmitter and receiver channel state information, and my companion result on achieving close to this limit using adaptive MQAM modulation. At the time there was no modulation that adapted the data rate to the instantaneous channel SNR in any wireless system, yet Shannon theory made it obvious that this was the right approach to maximize the data rate over fading channels. I was also inspired by the work of John Cioffi and his research group using adaptive modulation per OFDM subcarrier for twisted pair copper wire channels, which eventually became the ADSL standard. Today all Wi-Fi and cellular systems use adaptive MQAM modulation which I had proposed and analyzed as part of my doctoral research, yet I never could have foreseen that back in the early 1990s, when Wi-Fi was in its infancy and 2G cellular standards were focused on improving quality and user capacity for fixed-rate voice calls.

3. Do you remember which paper was your favorite when you were a student?

Shannon's 1948 paper was my favorite. It was so beautifully written, and so intuitive. At the time there were no classes on information theory at UC Berkeley, so I fell in love with the topic and also learned it starting from Shannon's paper and then reading Gallager's Information Theory book, which is my other favorite and most inspiring work from my graduate student days. Gallager's book, like Shannon's paper, is beautifully written and full of intuition along with the precise mathematics. It motivated and guided my Ph.D. work on both the capacity of fading channels and on the capacity of finite-state Markov channels.

4. What were you most passionate about as a graduate student?

I was most passionate about doing research. There was so much excitement at the time about how wireless systems would evolve and what applications they would support, it seemed there was an infinite number of challenging problems to formulate and try to solve around these questions. The process of doing research fascinated me also, which involved systematic learning through classes as well as reading papers that were almost indecipherable at first, but gradually I came to master as my knowledge base and ability to understand advanced research papers evolved. My research experience as a graduate student was atypical, as my adviser had not worked in my area of research, nor were there other professors or students at UC Berkeley working in communication/information theory. So I had to learn things more independently than might have been the case at a university with more faculty and students working in my research area. While I missed having a dynamic research climate with many really smart people working on similar or complementary problems to mine, that independence probably helped me in getting my first faculty job and launching my own research group.

5. What was the first conference you attended?

The first conference I attended was Globecom 1990 in San Diego. I did not have a paper there, but since there was no one at UC Berkeley working in information or communication theory at the time, I felt it was important that I attend and try to network with

people in these fields. Attending that conference was very fortuitous since I met my future Bell Labs mentor Larry Greenstein there, who invited me to apply for a summer job in his research group the following year.

6. ***What made you decide to pursue a Master's degree while working in industry after few years of your graduation from college? Similarly, what made you decide to pursue later a Ph.D. degree?***

Towards the end of my undergraduate degree, I focused on communications because I liked its rigorous mathematics applied to engineering, and developing a technology that significantly impacted people's lives. However, I didn't know if I wanted to be an engineer long term, or perhaps go into business or law or some other profession. In fact, I had no idea what engineers actually did. So I decided to work following my undergraduate degree while I figured out my professional ambitions. This was in 1986; the first cellular system had just been launched in Chicago, and Wi-Fi was still years away. Since commercial wireless technology was still in its infancy, there weren't really any engineering jobs in that space, especially for new graduates. I was fortunate to interview with a small defense communications startup, Maxim Technologies, that was working on multiple-antenna beamforming techniques and satellite communications. The company was very poorly run, and it generally only hired advanced Ph.D.s and engineers right out of college like me. As a result, us newly minted engineers had sole responsibility for solving really challenging problems, many of which were above our heads to solve. One of my earliest assignments was to develop direction-finding algorithms for antenna arrays. I went to Stanford's engineering library to research the topic, and found the beautiful papers by Kailath, Paulraj, and Roy on the MUSIC and ESPIRIT algorithms. While I was captivated by the elegance and rigor of the papers, I didn't have the technical background to understand the algorithms at a deep level. I also found that when I discussed technical problems with the Ph.D. engineers at Maxim, they approached problem formulation and solution through a completely different way of thinking than I was capable of. I realized that if I wanted to solve hard communication problems, particularly those in the emerging cellular and Wi-Fi systems, I would need to enhance my technical knowledge. So I decided to return to graduate school, thinking only that I would get an M.S. I initially applied to only two schools, UC Berkeley and Stanford, thinking that if both rejected me I would apply more broadly the subsequent year. Stanford rejected me but Pravin Varaiya, who was in charge of EE graduate admissions at UC Berkeley that year, saw something special about my application. He admitted me to UC Berkeley and to his research group even though I didn't have the strongest file in terms of GPA and test scores. I will always be grateful to him for that opportunity. Pravin was an inspiring adviser, teaching me how to formulate research questions and how to answer them with both mathematical depth and insight. I felt so privileged to be working with him, and was having so much fun doing research, that going on beyond the M.S. for a Ph.D. was a seamless decision.

7. Looking at your biography, it seems you worked several summers at AT&T Bell Labs during your graduate studies. How did this impact your doctoral research and later career? Do you recommend that graduate students work in industry during their studies?

After finishing my M.S. in 1991 I worked in Larry Greenstein's group at AT&T Bell Laboratories, which was a transformative experience. In contrast to UC Berkeley where no faculty or students were working in information theory, communications, or coding, some of the most prestigious people in these fields were in Larry's group or in the Information Theory and Signal Processing Bell Labs groups at Murray Hill. Moreover, Bell Labs was ramping up activities in wireless as cellular systems were starting to take off, so there was a lot of excitement about research in that area. Larry was a fantastic mentor in both research and the broader issues of how to be successful in a research career. He also introduced me to many of the luminaries in the wireless field. In the summer of 1992 I worked closely with both Larry and Jerry Foschini, another fantastic mentor and brilliant researcher. Jerry introduced me to his paper with Jack Salz on digital communications over fading channels. A key equation in that paper served as the basis for the optimal rate adaptation in MQAM I developed when I returned to UC Berkeley at the end of the summer. Overall my two summers at Bell Labs and the people who worked with and mentored me during those summers had a big impact on my research in the latter part of my Ph.D. and as I began my faculty career. It also introduced me to the culture in a research lab, which was very appealing. My decision as I neared graduation to apply for jobs in research labs as well as universities and companies was strongly influenced by my summers at Bell Labs during my doctorate. I highly recommend that my own graduate students spend at least one summer doing industrial research during their doctorate to learn about the application of research in technology development, and to benefit from the insights and experiences of people working in those environments.

8. ***Were your career choices all well planned, opportunistic, more of an exploration, included luck, or owing to your network?***

My career choices were not planned at all. I didn't know what I would major in when I started college, in fact I thought I would major in political science. I didn't know if I would pursue an engineering career when I graduated college. I didn't expect to get a Ph.D. when I returned to graduate school. And I certainly never expected to become an academic or startup founder. At each fork in the road, the career path I took was a combination of pursuing my passions, having the confidence to go after opportunities even if they seemed to be stretch goals, taking risks, and having colleagues and mentors who gave me the advice and support instrumental in my professional success.

9. Can you compare the job market today a graduate student is facing with the job market at the time of your graduation?

When I got my Ph.D. in 1994 there were very few faculty members in the U.S. working in wireless communications and wireless information theory. In fact, throughout the 1980s it was thought that there was little more research to do at the physical layer, as modems at the time were achieving rates close to the Shannon capacity limit of the 3 KHz telephone channel. The explosion of cellular usage in the late 1980s along with ADSL and Wi-Fi in the early 1990s initiated massive interest in wireless and wireline communication and information theory, so many universities, companies and research labs were looking to hire people in my field.

The last decade or so has seen a waning of interest in wireless communications and information theory among incoming Ph.D. students, perhaps in part due to the large numbers of doctoral students in these fields produced over the last few decades, and perhaps in part due to the explosion of interest in machine learning and related areas of statistical signal processing. Hence the job

market for Ph.D.s in these fields has been a bit less rosy than when I graduated, although all of my Ph.D. students have gotten great jobs in either academia or industry. However, I see momentum building again in these fields due to the new requirements and applications anticipated for 5G systems, connectivity requirements for the billions of sensors and small devices that will make up the "Internet of Things", along with interest in deploying new millimeter wave and LEO satellite systems. I believe this will lead to new and exciting opportunities for current Ph.D. students focused on wireless communications and information theory.

10. Would you suggest a graduating Ph.D. student or postdoc to work in industry even if they have a compelling offer in academia today?

I recommend graduating Ph.D. students apply broadly for any job that they think might be compelling. You learn a lot about your own aspirations and goals as well as different working environments in the process of applying and interviewing for positions in academia, industry, and research labs. When you have all the offers on the table, you can then decide which job is most desirable. If you are offered a compelling academic position and your desire is to be an academic, then I would recommend accepting the academic offer. That is because compelling academic jobs are harder to come by than industry jobs, and also depend on timing and luck as well as a candidate's qualifications. However, if you want industry experience to help in framing the research questions you will pursue as an academic, you can often request to delay the start of your academic job by a year and take that year to get industrial experience.

11. As a graduate student, did you imagine or consider you would write a book or start a company?

As a graduate student I never imagined I would write a book (let alone 3 books) or start a company (let alone 2 companies). My wireless book came about because I started teaching a graduate course in wireless communications to serve as a foundation for my incoming graduate students. The course began at Caltech in 1995 and moved to Stanford with me in 1999. There was no graduate level textbook throughout these years, so I started with a set of course notes that I kept expanding each year, hoping that someone would write a great book on wireless that I could then use instead of my course notes. By 2002 it appeared no one was going to write the textbook I wanted, so I decided to write one based on my course notes. It was another three years until it was done. I decided to write it as sole author since I had very set ideas on how I wanted to present the material, and I didn't want to compromise. The book took way longer to finish than I expected, as a book is never complete, perfectly-written, or error-free. The last four months were particularly brutal as I was already more than a year behind schedule, and the publishers were pushing me to wrap up in time for the next academic year sales season. My kids were 5 and 7 at the time, so I couldn't really get much work done at home. Hence I would order lunch and dinner from the café in my building, and stay at the office until just before the kids' bedtime. This was the first time in my career that my work/life balance became seriously out of whack. When I first received the published book, my reaction was that it wasn't worth it, as I would never get back those four months of dinners and evenings with my kids. Reflecting on that time now, it probably was worth it as the book has had a lot of impact, but I still think about those missed evenings, and I've tried to make it up to my kids ever since (and they are quite adept at exploiting my guilt from that period).

Starting a company was also not something I had thought about as a graduate student. There wasn't much of a startup culture at UC Berkeley in the early 1990s. Moreover, I had worked in a poorly run startup before graduate school and had seen many startups go under in Silicon Valley during the 1980s. Hence I was well aware of the challenges and likely failure of startup endeavors. In 2005 I was recently tenured and ready for a break from academic life. Around that time my Stanford colleague John Cioffi introduced me to Behrooz Rezvani, who would become my startup co-founder. Behrooz was interested in starting a company to build technology based on the emerging 802.11n Wi-Fi standard, which was the first to incorporate MIMO. At that point it had been 20 years since I had built technology during my days at Maxim. I was excited to see if all the research I had done as an academic over those 20 years could translate to a successful technology. Behrooz had previously started a successful VDSL company, so I thought we would make a good team; I would bring the general wireless and specific MIMO expertise as CTO, and he would bring the startup expertise as CEO. Quantenna was a wild ride with many ups and downs. The downs included almost running out of money several times, frequent executive and engineer turnover and, most difficult, my realization in 2009 that the friction between co-founders required me to leave the company as the best thing for its chance of success. Two CEOs later I was brought back to lead the company's Technical Advisory Board and to join the company executives and early employees in ringing the Nasdaq bell when Quantenna went public. While the Nasdaq bell ringing was the biggest "up" in my Quantenna experience, there were many others: recruiting and working with incredibly talented people, developing the adaptive physical layer algorithms for a 4×4 MIMO chipset, attending standards meetings where I learned that people in industry read our academic papers and implement our ideas, figuring out how to build and sell an advanced Wi-Fi chipset into a market that didn't exist, and bringing up Quantenna's first chipset which, magically, worked the first time.

12. Do you think any of your experiences during your time as a student or any characteristic that distinguished you already as a student have led to your winning of the Comsoc WICE mentoring award?

As a graduate student I benefited tremendously from the mentoring and support of my adviser as well as my Bell Labs summer supervisor and colleagues. As I moved through my academic career, I was fortunate to have other mentors and supporters at Stanford and in my professional societies (Comsoc and ITSoc). However, when I joined these societies in the early 1990s, there were no women mentors and few women comrades that faced some of the same issues I did as a female graduate student and later as an Assistant Professor. Our profession is still not very diverse, which means that women in communications and information theory face challenges that the guys don't have. It's not that we are not as good—in fact, I think in many cases we have to be better in order to overcome those extra challenges. That is why I believe that mentoring women in our profession is so important. It is a small contribution that I and others can make to help the next generation of superstars in the field reach their full potential and be recognized for their accomplishments.

13. Why did you choose to provide service to the Communications and Information Theory Society in the first place? When did you first get involved with "Society business"? Any advantages this brought to you?

I got involved in Comsoc service as a graduate student. Globecom was being held in San Francisco in 1994, and the Communications

Theory Technical Committee (CTTC) was planning to put on a mini-conference in addition to their regular conference sessions. This was controversial, and the CTTC leadership asked me in 1993 to serve as the local representative and push through the initiative. I made a lot of great connections with other Comsoc members through the conference planning process and that has been true of all my other Comsoc service as well. ITSoc was more difficult to penetrate as a volunteer. In 2002, after 8 years as a faculty member, I had not been asked to serve in any ITSoc volunteer role, not even on an ISIT TPC. I had pretty much given up on getting involved in ITSoc, but then Vijay Bharghava, who was ITSoc senior past president that year, asked me to run for the ITSoc BoG. I was sure I wouldn't win, but I did. Two years later I launched the ITSoc student committee and two years later I was elected an ITSoc officer. My service to both societies has been incredibly rewarding and valuable. I've met people through this service that inspire me with their ideas and accomplishments, and that became friends, collaborators, mentors, supporters, and mentees. I've been able to contribute to both societies in ways that make them better for current and future members. And I've given back to the professional societies that have formed the foundation on which my research career has been built.

Part II: Gender Diversity Oriented Questions

1. Any gender specific anecdotes/challenges you would like to share from your time as a graduate student?

I was fortunate that the people I worked with as a graduate student at UC Berkeley and Bell Labs judged me based on the quality of my research. But my sense at the time was that ITSoc was an "old boys club" where people of the right gender and pedigree, i.e. men studying with an adviser that was part of this club, were given the benefit of the doubt that they would do high quality research. The rest of us were not given that benefit of the doubt, and it seemed harder for the women to prove that their research was of high quality than for the men.

2. The women in Information Theory Society lists 19 women currently. Obviously there are more women and some might be against such lists. What is your stance on whether this is by itself a sort of self discrimination or not?

WITHITS was started by Muriel Medard when I was President of ITSoc to provide a peer group, mentoring, and events targeted to women members of the society. I'm not sure what motivates people to be on or off the WITHITS list: perhaps they don't wish to get bulk emails, or to self-discriminate. But the WITHITS events I have been to are very well attended and seem to be of value. I think that is more important as a metric of success then the number of people on the WITHITS mailing list.

3. Yet the list is very short. Among Shannon award winners there are 40 men and 1 women. Why do you think the Information Theory Society has been so unsuccessful in nurturing and retaining more female talent, with no disrespect to anyone?

Unfortunately, ITSoc does not have a good track record in recognizing its female members through awards and honors. Going by the names of authors, it seems that of the 64 papers that have won the ITSoc paper award, not a single one has a female author. Similarly, it appears that not a single female student has won the ISIT student paper award. Only five women have been elevated to IEEE Fellow through ITSoc, which is quite a small number given that approximately 3–5 members have been elevated annually to Fellow through ITSoc going back many decades. Finally, only one of the nine Padovani lecturers, who are selected as role models for current ITSoc graduate students, has been female. In my own experience serving on the ITSoc awards committees and Fellows committee, I rarely see women nominated for society awards and honors. When they are my sense is that their research, achievements, and impact are judged more harshly than that of the men. Perhaps that is why women are not well represented among the recipients of ITSoc's highest honors and awards.

4. As a graduate student, did you imagine you would be one day promoting gender equity? Today, there are probably more female graduate students in STEM fields than the time you were a student. Still, do you think the quality of experience improved or worsened?

When I was a graduate student there was one female professor and very few female graduate students, although my adviser had a particularly diverse group. I thought then that by the time my (hypothetical) children would be entering college, things would be much better in terms of the percentage of women in STEM and their experience working in these fields. Today, with my non-hypothetical daughter a college freshman interested in STEM, I am sad and disappointed that we have made far less progress than I would have thought by now. In particular, the percentage of women in STEM, particularly in electrical engineering, as students, graduate students, faculty, and in industry is far less today than I would have expected when I entered college. Perhaps even more demoralizing, there is ample evidence that these women encounter challenges and barriers to their success that the men don't have. The IEEE recently did a study with almost 5000 women members responding where a whopping 73% say they "have experienced negative outcomes in their careers attributed to being a woman". These statistics are one of the reasons I am now devoting quite a bit of my time to this issue by chairing the IEEE committee on diversity and inclusion, and by participating in an industry consortium of women in leadership positions.

5. We always talk about role models and the importance for "girls" to have female role models? Why not have male role models? Who were your role models?

I think it is important to have many role models and mentors, as each can serve a different purpose. I had wonderful male mentors and role models as a graduate student. My adviser Pravin Varaiya was an amazing role model in how to be a great researcher. My Bell Labs mentor Larry Greenstein was an amazing role model in how to be a great boss, supporter, and mentor of young people. Later in my career I had wonderful role models at Stanford in John Cioffi and A. Paulraj regarding how to be outstanding researchers, successful entrepreneurs, and great supporters of younger colleagues. Although there aren't really any women senior to me in communications and information theory, my female colleagues in these fields who started around the same time as me have served as wonderful role models as well as great supporters.

I believe that women need both male and female role models and mentors because there are so few women in the field. Hence, if we restrict ourselves to only have female role models and mentors, the pool is quite small and hence may not suffice. Female role models and mentors are important for women when they face gender-specific issues, such as having children pre-tenure. When I was an assistant professor I had several well-meaning senior male colleagues with stay-at-home wives tell me that I should not have children pre-tenure. I figured they couldn't possibly give me advice on this as it was so far from their own experience. I decided to go for it anyway,

and had both my kids pre-tenure. I believe that I and other women faculty with similar experiences can offer advice to women about this issue based on our own first-hand knowledge and perspective that would differ from what a male mentor might advise.

6. Recent harassment scandals in the US show that so many women endure terrible experiences in every industry including academia and there is a system which favors the exchange of support for sex. In a profession like academia where networking plays a very important role in building one's career, what is your suggestion to junior female graduate students and academics (hopefully about how not to compromise professionalism or lose hope about being respected as a professional) in the midst of such disturbing revelations?

Unfortunately, sexual harassment is fairly prevalent in academia and the hightech industry. The IEEE survey of its women described earlier indicated that 28% of the respondents had experienced sexual harassment. At my first ISIT conference in 1994, just before I finished my Ph.D. and after I had accepted a faculty job offer at Caltech, a very prominent member of our community, now deceased, tried to push his way into my hotel room. Fortunately I was able to push him out of my room. I told many people about this incident and who was responsible, at the conference and in the ensuing years. My female colleagues were sympathetic, but most people I told shrugged it off, with one telling me that this person had a reputation for acting similarly with his graduate students. There was no outrage, no one confronting him about these acts, and no efforts to stop him from this behavior.

Sexual harassment is not an easy problem to mitigate. It requires better reporting mechanisms and consequences when such behavior occurs. More importantly it requires a culture whereby such behavior is unacceptable and this is conveyed to the community from the highest echelons of power. Since the majority of people in ITSoc, particularly the senior people that hold the reins of power, are men, this can only happen if the men of ITSoc want it to and are proactive in creating this culture within the society.

My advice to junior women in the midst of disturbing revelations about sexual harassment is

1) Be informed about the nature of sexual harassment, which can range from the extreme of a physical attack to less extreme harassment.

2) Have mentors and people you trust, men and/or women, who can give you advice and support if you find yourself in a situation where someone makes you feel uncomfortable or acts improperly.

3) Act now to raise your own and your professional network's awareness about processes to handle sexual harassment complaints in your university, company, and/or the IEEE. If the processes in place appear inadequate, advocate for them to be improved.

As chair of the IEEE committee on Diversity and Inclusion, I am responsible for making recommendations to the IEEE on how they can mitigate sexual harassment within the IEEE and more broadly in the profession. I welcome the thoughts and suggestions of ITSoc members on how the IEEE can address this issue effectively.

Prof. Sarah Kate Wilson, Santa Clara University

Part I: Career Oriented Questions

1. What was the subject of your Ph.D. thesis? If you were doing a Ph.D. thesis today, which topic would you chose?

The subject of my Ph.D. thesis was OFDM and wireless broadcasting. If I were doing a Ph.D. thesis today I would try and do it on something fun that not so many people were working on. Back in the early 90's OFDM had a re-emergence due in part to Len Cimini's great paper, "Orthogonal Frequency Division Multiplexing" and the work on the European Digital Audio Broadcast System. So there was a lot of new ground to work. If I were a Ph.D. student today, I would read several papers, talk to my advisor and find a topic that was fun. I had a great advisor and I chose the advisor and the topic followed.

2. Can you tell us a result you derived when you were a Ph.D. student and you are most proud of?

When I was a Ph.D. student I looked at diversity in coded OFDM and also derivations of probability density functions for BER in the presence of channel estimation errors. Someone once told me that a Ph.D. is like a driver's license. It teaches you how to do research, but it's not necessarily the end result. It's a way of thinking and doing work. One of the great things about my Ph.D. experience was being asked sometimes unnerving questions by my advisor and the other members of my research group. At first I couldn't answer the questions and I was flustered. But getting those questions taught me to think more deeply about a result: does it make sense? do I trust it? what does it mean? what else can I do? I guess I'm most proud of the fact of what I learned and how I was able to continue contributing to knowledge.

3. Do you remember which paper was your favorite when you were a student?

That's a hard question to answer, but I really liked an old paper by Turin, On Optimal Diversity, 1961 from IRE Transactions on Information Theory. And there were follow ups on this by Mazo and Salz. The basic idea is if you have correlated receiver sources, these papers lay out a nice way of determining how much diversity you have.

4. What was the first conference you attended?

The first conference I attended was ICC '91. The dry runs of my talk had gone well, but I froze when I got up to speak. A very nice person in the audience (Mike Pursley as it turned out) started nodding at me in an encouraging way. I then relaxed and was able to continue. So that bit of kindness meant a lot.

5. What made you decide to pursue a Master's degree while working in industry after few years of your graduation from college? Similarly, what made you decide to pursue later a Ph.D. degree?

I moved out to California as I met a great guy from Palo Alto who is now my husband. While working at SRI I started taking

courses in Electrical Engineering. I really liked it and said to a fellow in my lab at SRI that I was thinking of applying to Stanford. He said to me, don't even bother applying. They'll never accept you. I went to Berkeley and they turned me down. So I got mad and applied to Stanford. After receiving my Master's I worked in industry and was somewhat unhappy and called John Cioffi. He said, would you like to come back to school and I said yes.

6. Can you explore a bit on your first job, where you worked as a programmer/analyst, after you graduated, and contrast with the expectations you had as a student?

When I graduated with a BA in math I had no idea what I wanted to do. While I was sort of looking for a job, I went back to working at the shoe store where I had worked summers. One day a friend of mine from high school came in and said, my dad would give you a job. And he did! I didn't know programming, but he said, you'll learn and I did. So I'm very grateful for that. As a student, I did not realize how much of work is actually work. That is some of it is wonderful and quite inspiring, but sometimes you just have to do unglamorous tasks that need to be done. That was a good lesson from my first job.

7. Were your career choices all well planned, opportunistic, more of an exploration, included luck, or owing to your network?

My career was not exactly planned, it was more accepting some opportunities, reaching out to networks and being in the right place at the right time (e.g. my current job at Santa Clara University). I've had setbacks and disappointments, but I've been very lucky to have a good network of friends and mentors.

8. Can you compare the job market today a graduate student is facing with the job market at the time of your graduation?

It's hard to say how the market is different. Specific fields go in and out of fashion. I can say that when I was a graduate student most everything was done by sending (and receiving) letters via the postal service. The online world of applications and references did not exist. As a result the number of applicants and the expected speed of responses has increased.

9. Would you suggest a graduating Ph.D. student or postdoc to work in industry even if they have a compelling offer in academia today?

I think a person should take a job that suits them. I learned a lot working in industry, e.g. real world constraints, practical concerns. I'm glad I worked in industry, but I'm very happy here at Santa Clara. I think industry experience informs my teaching and research. I know great academics who have not worked in industry. I wish I had done a postdoc before starting as an Assistant Professor back in the 90's. I think the time to really focus on research post-Ph.D. is invaluable.

10. As a graduate student, can you tell us about some initiatives you took that you believe significantly impacted your later career choices and progress?

When I was a graduate student I taught my advisor's course in Digital Communications when he was on sabbatical. I think that showed me how much I like teaching.

11. As a graduate student, did you imagine or consider you would write a book one day in your field?

When I was a graduate student just the thought of writing a Ph.D. thesis was kind of scary, so I'm not sure I ever imagined writing a book. However my book was an edited book and I was very lucky to have wonderful contributors who wrote the bulk of it.

12. Do you think any of your experiences during your time as a student or any characteristic that distinguished you already as a student have lead to your winning of the IEEE Communications Society Joseph LoCicero Award for Exemplary Service to Publications? Can you give us some examples of your innovative contributions in that respect? How much of your time did you allocate to your services to publications?

As a graduate student, my advisor gave us reviews to do. This experience was invaluable. And I'm relatively chatty, so when I became an Associate Editor, I discussed issues via email with the Editors-in-Chief. Eventually I worked as an Editor-in-Chief, then Director of Journals and finally Vice President of Publications. One of my contributions was the Reviewer Appreciation Program. Reviewers toil in obscurity and should be rewarded for continued thoughtful, insightful reviews. So I'm proud of that program. I'm also proud of implementing the "SWAT" reviewer program where we had an elite team of reviewers who could step in if some reviewers were missing in action.

I spent a fair amount of time on publications. Some of it was not very glamorous, but necessary, e.g. assigning reviews, dealing with plagiarism, things like that. However, I had the chance to shape and improve an important process in our area. And I'm very glad I had that opportunity.

Part II: Gender Diversity Oriented Questions

1. Any gender specific anecdotes/challenges you would like to share from your time as a graduate student?

I think the one thing that stands out for me here was being in the minority. I think like many women I was nervous about not doing well or asking questions as I felt like there was a big spotlight on me. We women graduate students hung out together. One night we did a "girls' night out" and went to see "Thelma and Louise." A male grad student wanted to come with us, so we made him an honorary girl that night. Just two weeks ago he asked me if we could do a girls night out reunion.

2. What is the comment addressed to you or to the public that you found most offensive in your career?

I think one of the ones that stands out was "You only got that job because they wanted a woman." So does that mean I'm not qualified? Does that mean I'm taking a job from a deserving man? Even if that statement were true, there has been job/admission preference in the other direction for years.

3. The women in Information Theory Society lists 19 women currently. Obviously there are more women and some might be against such lists. What is your stance on whether this is by itself a sort of self discrimination or not?

I think people differ on lists like that. Some are proud to be among such a list. Some people think why should we have

to have such a list? So my feeling is if such a list helps promote more women in the area it's good. If such a list mitigates the assumption that it's a male field, I'm happy to be on such a list.

4. Yet the list is very short. Among Shannon award winners there are 40 men and 1 women. Why do you think the Information Theory Society has been so unsuccessful in nurturing and retaining more female talent, with no disrespect to anyone?

I'm not sure why the Information Theory Society has not attracted more women. I can tell you that I only rejoined recently and two things led to it. Vince Poor said why aren't you a member? And a few years ago I was at a party and Tom Cover was there. He said to me, "Katie did I have you for Information Theory?" I said no I took it from someone else. Then in his inimitable Tom Cover voice he said, "Well I would have given you an A." Tom's comment made me feel better about fitting in with the Information Theory society. So I thought heck I can join IT.

5. As a graduate student, did you imagine you would be one day promoting gender equity? Today, there are probably more female graduate students in STEM fields than the time your were a student. Still, do you think the quality of experience improved or worsened?

I hoped I would be able to promote gender equity when I was a grad student. I'm grateful I have the kind of job where I can work on this issue. I think things are better than they were 20 years ago, but we're not there yet. We have more role models in the field now than we did in my day. Gradually we make progress, but there are still biases everywhere. We all have them. The goal is to overcome them and work for more equity.

6. We always talk about role models and the importance for "girls" to have female role models? Why not have male role models? Who were your role models?

I think that's an excellent point. Women role models are great for proof of existence, but there's more variety if one's role models and mentors are not limited to one gender. Most of my mentors have been men. When I was a graduate student I was at a large research university where many of the faculty started companies. That's not me. I like the "Teacher-Scholar" model where both teaching and research have equal weight. So in terms of the amount and sheer weight of research, I would say that my research style is different. I think everyone has to find their own style. Having a good advisor who asks good questions is a great start. As I've worked with more people through the years, the way I do research has evolved. I have several role models including my advisor, my mentors and my friends.

7. Recent harassment scandals in the US shows that so many women endure terrible experiences in every industry including academia and there is a system which favors the exchange of support for sex. In a profession like academia where networking plays a very important role in building one's career, what is your suggestion to junior female graduate students and academics (hopefully about how not to compromise professionalism or lose hope about being respected as a professional) in the midst of such disturbing revelations?

Fortunately I've not had to deal with men asking for sex. However I'm sure it's happened. I think one solution is to make friends of people you respect. The larger your support group is (both friends and mentors) the better off you are. If someone makes an inappropriate request, document it and tell someone you trust. Ask for help. This is not a bullet proof solution. If I had that I would shout it to the roof tops, but we can't be silent in the face of bad behavior.

From the Editor *(continued from page 2)*

the IEEE Transactions on Information Theory, in Foundations and Trends in Networking, and in Foundations and Trends in Signal Processing. Many thanks to all for their significant efforts in the preparation of their contributions!

On a personal note, with this issue I have completed my tenure as the Newsletter Editor. I truly enjoyed serving our society over the past three years and would like to take this opportunity to express sincere thanks to the many who supported the newsletter throughout this period. In particular, I would like to thank the Board of Governors for entrusting me with this role; the Newsletter Editorial Board for their significant support and help with each and every issue; Matt LaFleur, our Technical Community Program Coordinator, for his extremely valuable assistance in running the newsletter; and, of course, the many newsletter contributors for their significant (and selfless) efforts! Thanks all! I would also like to wish the incoming editor, Salim El Rouayheb, congratulations and the best of luck on his new appointment!

Please help to make the newsletter as interesting and informative as possible by sharing any ideas, initiatives, or potential newsletter contributions you may have in mind. 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 Salim El Rouayheb at salim.elrouayheb@rutgers.edu with a subject line that includes the words "IT newsletter."

The next few deadlines are:

April 10, 2018 for the issue of June 2018.

July 10, 2018 for the issue of Sep. 2018.

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.

With best wishes,
Michael Langberg
mikel@buffalo.edu

The Historian's Column

Anthony Ephremides

I was musing the other day about the number of technical conferences that surround our field. It is literally hundreds! How can a newcomer cope with the volume of (dis)information that is flooding the archives? We have entered, it seems, the era of "fake" papers?

So, I went back in time and recalled what the situation was when I graduated and entered the professional arena. There were exactly four (4) IEEE conferences and two (2) non-IEEE conferences available for someone working in the general field of Information and Communication Theory (there was no "Networks" field at that time). I may be leaving out a couple of other conferences tangential to the field. So, these were, of course, our own ISIT, the ICC (International Communications Conference) and NTC (National Telecommunications Conference) that later morphed into the Globecom, and the CDC (Conference on Decision and Control). The last one was sponsored by the Control Systems Society, while the preceding two were sponsored by the Communications Society. These three Societies had at the time a much greater affinity amongst them and belonged to the same Division of IEEE for a while. For reasons too complex and somewhat outside the scope of this article, things changed over time. Signal Processing and Networking came onto the scene, Computing became "big" and all kinds of "side"-disciplines emerged.

The other two conferences at that time, which were not IEEE-sponsored, were the CISS (only at Princeton) and the Allerton Conference in Urbana-Champaign. Later the CISS started alternating between Princeton and Johns Hopkins. Occasionally there would be a workshop with narrower focus that would be sponsored by one of these Societies. Gradually, as I am sure everyone knows, we started being bombarded by announcements touting "the First International Symposium/Conference/Workshop on….. (the topic of your choice)" to be held in (I better not mention any names). We are invited to organize a session of our fancy and sometimes we are offered to be excused from the usually steep registration fee if we agree to collaborate.

And, talking about registration fees, things have become really bad. Some of these conferences, including the "legitimate" ones, have surpassed the $1000 mark. In the early seventies they were even as low as $50. With "age", as we know, come some unforeseen benefits. So, in addition to having younger people offering their seats in buses and subways, I am thrilled when I can attend, say, the ICC as a Life Member for $50 (YES, you read right, FIFTY) while others pay over $1000! Of course, the $50 fee includes NOTHING except attendance at the sessions. Bypassing the dictum that says that "you get what you pay for", I note that the Banquet that is included in the regular registration has degenerated into a long, tasteless, and boring meeting in cavernous halls of "grand hotels". So, as far as registration fees are concerned I do not have much to complain about personally. But what about a young researcher who is struggling to obtain a grant of a mere $70K per year from one of the funding agencies and who would like to attend a conference along with a student?

Now, going to a conference requires not only payment of the registration fee. You need to, somehow, get there. In the new wonderful world of travel we know what this entails. In the old days you would pick up the phone and ask a travel agent to take you, say, from Washington DC to San Diego by using Eastern Airlines from DC to St. Louis and then connecting to Braniff Airlines from St. Louis to San Diego (if no non-stop existed). The choices were many and the costs were almost identical. Virtually every airline connected the cities it wanted to connect without the constraints of code-sharing, alliances, hubs, and the like. And the cost depended on origin and destination and not on the exact itinerary. Granted, there was no web to do early check-in or preselect your seats (assuming you are a frequent flier, of course). But things were predictable, simple, and, above all, the costs were commensurate with the size of your grant.

Today you have choices. In a recent search (for the DC to San Diego itinerary), I had about 34 possibilities. Yes, Thirty Four! I was tickled by some of the offerings. The non-stop option was offered for a whopping $900 (we are talking economy class, of course). But there were others. One of them (I am not making that up) would take me from DC to Chicago, then to Denver, then to Los Angeles, and then to San Diego (with an overnight stay in Denver) for $280! But the winner was the one that would take me from DC to Montreal (you read that right), then to Vancouver, then to San Francisco, and then to San Diego. You might think that this itinerary might be the cheapest. How wrong you would be! This one was offered for $1368! I guess the fare designers must have thought that if you were so stupid as to select this itinerary, you might as well be given a stiff financial penalty to add insult to injury.

So, this is the world of travel that we have to live with nowadays. I am not discussing hotels, car rentals, and related issues. The bottom line is that it is simply an onerous task to get yourself from place A to place B today. I am also not discussing the need to inspect carefully your socks for holes so as not to be humiliated in front of the TSA agents when you remove your shoes. Nor am I discussing the need to either check your light luggage if you happen to use a toothpaste. One time I had a German toothpaste with me that was half-empty and showed capacity of 75 ml. The TSA agent told me I had to give it up because it exceeded the 3 oz. limit. I noted to him that 1 oz. equals 27 ml. His response was "we are not mathematicians"! I had to invoke some form of Constitutional Amendment and talk to a supervisor to finally be allowed to carry it on board.

Imagine, therefore, after having endured these horrors to, finally, arrive at your destination where you would be flooded with "fake" results!

In the romantic era of my youth, one of the big hits was Bob Dylan's "The Times, they are a Changing". In addition to being a beautiful song with meaningful lyrics, it heralded the onset of the indignities outlined above. As the times are changing, unfortunately, the cloud of confusion about the reported scientific work at our meetings is increasing as well.

What is the solution, readers? What are your ideas? Tongue-in-cheek, I remind myself of another popular quotation during my revolutionary youth years. It was by Mao Zedong (then spelled Mao Tse Tung) that said: "Where do great ideas come from? Do they fall from the sky? No, they come out of the barrel of a gun"! ☺

From the Field

The Latin American Week on Coding and Information

The IEEE Information Theory Society Brazil Chapter is pleased to announce the LAWCI—Latin American Week on Coding and Information (http://www.dev.ime.unicamp.br/lawci/) to be realized in Campinas, SP Brazil (July 22nd to 27th , 2018). This event is composed by a School (July 22nd–24th) for graduate students and a Workshop (July 25th–27th) and has the support from the IEEE Information Theory Society and FAPESP foundation.

As in the previous international events we have organized (the IEEE- ITW 2011 and the SPCodingSchool 2015) the objective is, of course, to enhance the research area in this region. Confirmed lecturers for the School and the Workshop are Alexander Barg, Max Costa, Markus Grassl, Olgica Milenkovic, Daniel Panario, Moshe Schwartz, Gadiel Seroussi, Vinay Vaishampayan, Patrick Solé and Ram Zamir.

It will be a great honor for us to have such distinguished lecturers in this event and we would like to fully invite the IT Soc members to participate. This will certainly provide a broad view and perspective future interactions for the Latin American researchers. The school is planned for around 60 students (application deadline April 17th) and authors of accepted papers (submission deadline April 7th, 2018) for the Workshop can also submit a paper expanded version to a special edition of the journal Advances in Mathematics of Communications.

We are looking forward to meet you there!

Sueli Costa

Report on the Munich Workshop on Physical Unclonable Functions (MPUF) 2017

Organizers

Onur Günlü, Michael Pehl, Tasnad Kernetzky, Georg Sigl, and Gerhard Kramer

The TUM Chair of Communications Engineering (LNT) and the TUM Chair of Security in Information Technology (SEC) organized a Munich Workshop on Physical Unclonable Functions (MPUF 2017) on November 29, 2017. The technical program included talks by PUF researchers from TUM-LNT, TUM-SEC, the TUM Coding for Communications and Data Storage Group (COD), and the Fraunhofer Institute for Applied and Integrated Security (AISEC). The speakers were Michael Pehl, Lars Tebelmann, Robert Hesselbarth, Florian Wilde, Christoph Frisch, Matthias Hiller, Antonia Wachter-Zeh, and Onur Günlü. The workshop brought together researchers from the fields of information theory, coding theory, and hardware security to explore new ideas. The talk topics included:

- Information-theoretic Security and Privacy,
- Low-complexity Error-correcting Code Design,
- Hardware Optimization,
- Modeling and Evaluation of PUF Outputs,
- Side-channel Attacks on PUFs.

Researchers from 19 different groups from around the world attended the event, including delegates from Aalto Univeristy, CentraleSupélec, Chalmers, the Skolkovo Institute of Science and Technology, Tambov State University, and TU Eindhoven.

The social program included coffee and söbiyet (a Turkish dessert), and was followed by glühwein (a mulled wein) at the Cafe Altschwabing, which was built in 1887 in a historic architectural style.

Funding for the workshop was provided by the German Research Foundation (DFG), TUM-LNT, and TUM-SEC. The program, flyer, catchphrase, and photos are available at the web address http://www.lnt.ei.tum.de/en/events/2017-munich-workshop-on-physical-unclonable-functions-mpuf/

Report on the 2017 IEEE Information Theory Workshop

The 2017 IEEE Information Theory Workshop (ITW) took place in Kaohsiung, Taiwan, from November 6 to 10, 2017.

Kaohsiung is the third largest city in Taiwan, with 2.7 million inhabitants, and is the sixth largest harbor in the world. The event was hosted in the Kaohsiung Exhibition Center (KEC), which regularly hosts similarly world-renowned gatherings, such as the "Taiwan International Boat Show" and the "Kaohsiung International Food Show".

The event was attended by 176 participants, 57 of which were students. The participants were from 23 nations, the most represented being Taiwan (35), China (26), the USA (20) and Japan (18).

The conference had five invited sessions: Content Distribution, Coding for Memories, Coding for Memories (contributed by local industries), Information Theory and Biology, and Quantum Communications.

Among the 146 regular submissions, the most popular topics were Coding Theory and Practice (20), Network Communication Theory (15), Shannon Theory (13), and Multiple Terminal Information Theory (12).

The technical program also included four plenary talks: the plenary speakers and topics were (i) Prof. Michael C. Gastpar, *Caching—Strategies, Models, Bounds* (ii) Prof. Shu Lin, *A Novel Coding Scheme for Encoding and Iterative Soft-decision Decoding of Binary BCH Codes of Prime* (iii) Prof. Ilya Shmulevich, *Information-theoretic Perspectives on Stability-responsiveness Trade-offs in Biological Systems*, and, (iv) Prof. Mark Wilde, *Trading Communication Resources in Quantum Shannon Theory*.

The attendees were overwhelmingly elated by the conference banquet and the accompanying entertainment. The banquet menu offered a number of the much sought-after Taiwanese delicacies, such as steamed rice cake with prawns, mullet roe and smoked squid. The banquet entertainment was comprised of performances from Taiwanese aboriginal tribes, such as Thao, Rukai, Puyuma and Zuyun tribes. The "Zuyun Culture and Dance Company" performed beautiful and colorful dances with the accompaniment of bamboo and string instruments. Following, the orphaned children from highlands tribes, belonging the "Christian Mountain Children's Home", performed Italian Bel Canto traditional pieces.

The "Zuyun *Culture* and Dance Company"

Students at the poster session

Although the conference mostly followed the format of past ITWs, a few variations on the format were experimented.

Leading local industries that are actively investigating coding for memories were invited to present their newest developments at a specially arranged invited session. This session was well-received by the conference participants; it provided important insight on industrial efforts to develop ideas that emerged from academia.

A poster session gave the opportunity to junior researcher to present their work and receive feedback from the conference participants.

Lunch boxes were provided through the conference; coffees, tea, and snacks were provided all day. This ensured the utmost wellness and optimal caffeine intake of all participants. Finally, a 3-day Information Theory Society Student Special registration rate was offered.

We are grateful for the support of the local universities and the local students for their efforts in the local arrangements especially National Chiao Tung University (NCTU) and National Sun Yat-sen University (NSYSU).

We are also grateful for the Taiwanese Ministry of Science and Technology (MOST) and Ministry of Economic Affairs (MOEA) for their financial support.

We hope that all participants enjoyed Taiwan, its natural beauty and the cultural richness of its people. We sincerely hope that ITW has offered to many a better insight on the Taiwanese academic environment and culture.

The detailed program, proceedings, conference photos and videos of the plenary talks are all available online at the web address http://www.itw2017.org/

Stefano Rini, Publications Chair

Po-Ning Chen, General Chair

Call for Nominations

IEEE Information Theory Society Claude E. Shannon Award

The IEEE Information Theory Society Claude E. Shannon Award is given annually to honor consistent and profound contributions to the field of information theory.

NOMINATION PROCEDURE: Nominations and letters of endorsement must be submitted by **March 9, 2018**. All nominations should be submitted using the online nomination forms. Please see http://www.itsoc.org/shannon-award for details.

IEEE Information Theory Society Aaron D. Wyner Distinguished Service Award

The IT Society Aaron D. Wyner Service Award honors individuals who have shown outstanding leadership in, and provided long standing exceptional service to, the Information Theory community.

NOMINATION PROCEDURE: Nominations and letters of endorsement must be submitted by **March 9, 2018**. All nominations should be submitted using the online nomination forms. Please see http://www.itsoc.org/wyner-award for details.

IEEE Fellow Program

Do you have a colleague who is a senior member of IEEE and is deserving of election to IEEE Fellow status? If so, please submit a nomination on his or her behalf to the IEEE Fellow Committee. The deadline for nominations is **March 1, 2018**.

IEEE Fellow status is granted to a person with an extraordinary record of accomplishments. The honor is conferred by the IEEE Board of Directors, and the total number of Fellow recommendations in any one year is limited to 0.1% of the IEEE voting membership. For further details on the nomination process please consult: http://www.ieee.org/web/membership/fellows/index.html

IEEE Information Theory Society Paper Award

The Information Theory Society Paper Award is given annually for an outstanding publication in the fields of interest to the Society appearing anywhere during the preceding two calendar years. The purpose of this Award is to recognize exceptional publications in the field and to stimulate interest in and encourage contributions to fields of interest of the Society.

NOMINATION PROCEDURE: Nominations and letters of endorsement must be submitted by **March 15, 2018**. All nominations should be submitted using the online nomination forms. Please see http://www.itsoc.org/honors/information-theory-paper-award/itsoc-paper-award-nomination-form for details. Please include a statement outlining the paper's contributions.

IEEE Information Theory Society James L. Massey Research & Teaching Award for Young Scholars

The purpose of this award is to recognize outstanding achievement in research and teaching by young scholars in the Information Theory community. The award winner must be 40 years old or younger and a member of the IEEE Information Theory Society on January 1st of the year nominated.

NOMINATION PROCEDURE: Nominations and supporting materials must be submitted by **April 30, 2018**. All nominations should be submitted using the online nomination forms. Please see http://www.itsoc.org/honors/massey-award/nomination-form for details.

IEEE Awards

The IEEE Awards program pays tribute to technical professionals whose exceptional achievements and outstanding contributions have made a lasting impact on technology, society and the engineering profession. For information on the Awards program, and for nomination procedures, please refer to http://www.ieee.org/portal/pages/about/awards/index.html

IEEE Information Theory Society Board of Governors Meeting

Location: Chicago, USA

Date: 7 October 2017

Time: The meeting convened at 9am CDT (GMT-5); the meeting adjourned at 1:27pm.

Meeting Chair: Rüdiger Urbanke

Minutes taken by: Stark Draper

Meeting Attendees: Suhas Diggavi, Alex Dimakis, Stark Draper, Michelle Effros, Elza Erkip, Christina Fragouli*, Tara Javidi, Matt LaFleur#, Ubli Mitra, Pierre Moulin, Krishna Narayanan*, Alon Orlitsky, Anand Sarwate#, Emina Soljanin, Daniela Tuninetti, Rüdiger Urbanke, Michele Wigger*, Aaron Wagner#, Greg Wornell.

(Remote attendees denoted by *, non-voting attendees by #.)

Business conducted between meetings: Between the Jun. 2017 and Oct. 2017 Information Theory Society (ITSoc) Board of Governors (BoG) meetings, a number of items of business were conducted and voted upon by email. These items and results are summarized below:

1) Elza Erikp was elected to serve as President of ITSoc for 2018.

2) Emina Soljanin was elected to serve as first Vice-President of ITSoc for 2018.

3) Helmut Bölcskei was elected to serve as second Vice-President of ITSoc for 2018.

4) **Motion**: A motion was made to approve the revised budget for ISIT 2019. The motion passed.

At 9:00am local time, ITSoc president Rüdiger Urbanke called the meeting to order. He started by reviewing the agenda.

Motion: A motion was made to approve the agenda. The motion was passed unanimously.

Motion: A motion was made to approve the draft minutes of the Jun. 2017 ITSoc BoG meeting. The motion was passed unanimously.

1) **President's Report:** Rüdiger presented the President's report. He first reviewed the presidential chain, thanking retiring Second Past President Michelle Effros for her work and welcoming Helmut Bölcskei. BoG elections are ongoing and will conclude on 13 October. Rüdiger next reviewed the agenda, recapping the many ongoing initiatives and the review of Society bylaws that has been conducted by Michelle Effros. He discussed new Society chapters that have been formed and are in the process of being formed, as well as the upcoming 5-yearly review of the Society by the IEEE. In the review he expects two issues to be raised. The first of these is that there is no official "strategic plan" for the Society, a point also raised in the last review. The second is that there is no professional affiliations program, i.e., ITSoc has no outreach aimed at young professionals working in industry. He contrasted this with outreach efforts aimed at student and our mentoring programs targeted at young faculty. Rüdiger's penultimate item was a discussion of where and when the BoG meetings will be held in 2018. The first meeting will be held on the weekend prior to the UCSD ITA workshop, on Sunday 11 February. The second meeting will be held at the ISIT. The third, Chicago, meeting typically has the lowest attendance. So, a discussion ensued about whether we should conduct this meeting remotely, unless there are major topics to be discussed. Rüdiger concluded his report by discussing the process by which BoG members are nominated, and how it can be modified to broaden the geographic diversity of the BoG membership.

2) **Treasurer's Report:** Treasurer Daniela Tuninetti next presented her report. We still have money for new initiatives. Under the "50% rule" half of any surplus in year n can be used in year n+1 for new initiatives. This amounts to $4.6k USD for use in 2017, which to date is unused. Under the "3% rule" up to 3% of society reserves in year n can be used for new initiatives in year n+1. This latter spending is subject to IEEE approval. E.g., for 2017 the society asked for $140k USD for new initiatives and the IEEE approved $105k USD of spending. The $105k was targeted to continue the broad outreach efforts initiated in 2016. To date about $50k has been spent. Turning to the actuals of the budget, Daniela first noted that none of the 2017 events have yet closed their books. The net forecast for Q2 was negative $95k USD. (This wasn't a problem because it includes $105k USD of spending under the 3% rule so the operational net is positive, which is what the IEEE wants to see.) Due to under-spending on new initiatives, the forecast increased from negative $95k USD to negative $30k USD. A discussion ensued on how to increase spending on new initiatives by the end of 2017.

Daniela next turned to the 2018 budget. Hitting IEEE targets would result in a budget with a total net income of $22k USD. However, ITSoc has been working toward developing zero-surplus budgets. Therefore the draft ITSoc budget has a net income of $750. Drilling down into the budget Daniela noted that we asked for $100k USD for new initiatives. However, at the first level of IEEE review (of which there are two), that was reduced to $68k, which may be further reduced at the final review. All the new initiatives that are ongoing (outreach, book project, etc.) are three-year initiatives for which 2017 is year two. The BoG recalled that, as was also discussed at the ISIT meeting, schools are no longer new initiatives. (If the design or content of a school is materially changed it could then re-qualify as a new

initiatives.) A clarifying question was asked whether if we have an operational net, and don't make the IEEE's target that all societies deliver a 2.5% operational net profit, whether that would be a red mark. (Recall ITSoc aims for a zero-surplus.) As far as Daniela understands, only if a society has an operational net loss would IEEE have a problem. In conclusion, once the 2018 budget is approved, Daniela asked people to be ready to spend starting on new initiatives on 1 Jan. 2018.

3) **Conference Committee:** Due to communication difficulties this report, while on agenda, was not delivered.

4) **Nominations and Appointments Committees:** Nominations and Appointments (N&A) Committee Chair Michelle Effros first reviewed the current composition of the committee, the appointment process, and the duties thereof. She reviewed the process of forming committees while satisfying the constraints on appointments specified in the Bylaws and listed new appointments to the various committees.

5) **Constitution and Bylaws Committee:** Michelle Effros chairs this Committee as part of her duties as Second Past President. As Michelle outlined to the BoG at the June meeting, there are a number of confusing sections in the Constitution and Bylaws, and a number of internal inconsistencies. Michelle has been reviewing and cleaning up these documents, starting with the Bylaws. Her goal in the current round of changes was not to change any policy, but simply to clarify aspects of the documents that are difficult to decipher and to remove inconsistencies. Michelle walked through the proposed changes with the BoG. The BoG approved all proposed changes. She also raised two points that will need attention by next year's N&A committee: term limits (appointed vs elected), and whether paper award nominations should come from the Publications committee (consisting of the editors and associate editors of the Transactions, the editor of the Newsletter, and ex-officio members).

   There was problematic wording in the Bylaws regarding term limits. The prior Bylaws limit the number of terms BoG members can serve continuously to two; the only exception is for members serving in the presidential shift-register. However, appointed members of the BoG (secretary, treasurer, Conference Committee Chair) are appointed annually and traditionally serve for three years, i.e., three terms. Further, appointed members have often then been elected to the BoG as regular members after their appointed term(s). The proposed (and accepted) change to the Bylaws applies the two-term-limit only to elected members of the BoG, thereby making the document consistent with accepted and long-standing practice. There was discussion of changing term limits to a fixed number of years, or to removing term limits altogether. Since either of these ideas would mean a change in policy, they were not included in the revision but instead remain topics for further discussion.

   Michelle next turned to the question of how to improve the process of garnering nominations for paper awards, especially the ITSoc Paper Award. The current Bylaws put the onus of generating paper nominations on the Publications Committee. However, this Committee is heavily loaded with running the Transactions, and often the Awards committee receives few nominations. Michelle then led a discussion on how the nomination processes might be re-designed. An immediate clarifying question from the BoG asked how detailed nominations must be. Michelle responded that there is no formal requirement—even a one-sentence nomination is allowed—though Michelle certainly encourages nominators to submit solid, well-considered, and detailed nominations. Former members of the Awards Committee voiced the opinion that responsibility for fostering nominations should be moved from Publications to the Awards Committee. For example, once the Committee has completed its work surrounding the selection of that year's best paper they could then, in the second half of the year, foster nominations for the following year. This would be better than having the next year's committee foster nominations. The underlying logic here is that the Awards Committee is constituted on 1 January and must make its recommendation to the BoG by 1 March. Therefore there is not much time in-between to identify candidate papers.

6) **Online Committee:** Online Committee Chair Anand Sarwate update the BoG on his committee's work. One point of progress is getting the website colors to match IEEE standards (!). A second has been to get all sorts of letter accents displayed correctly. Anand reviewed the corpus of ITSoc members that subscribe to News & Events (roughly 25%) versus the mailing list of the Table-of-Contents (TOC) (100%). The former is an opt-in list while the latter is opt-out. He reminded the Awards Committees that he could really use a short blurb describing each award winner. He then could post this text on the website, the better to publicize the accomplishments of ITSoc members. Anand then reviewed upcoming goals of the committee, a number of which could be assisted by willing volunteers. If readers are interested in working with the Online Committee, please contact Prof. Sarwate (anand.sarwate@rutgers.edu).

7) **Outreach Committee Mentoring Program:** Outreach Committee Chair Aaron Wagner reviewed the activities of the committee. The Committee has two main charges. The first is running the mentoring program. The second is event planning. Aaron reviewed the current state of each.

   The mentoring program matches junior ITSoc members with senior members. After the initial match there are few formal follow-on activities. Based on anecdotal evidence the Committee inferred that matching works well in a few cases but, on the whole, there is little activity between pairings. To quantify the accuracy of such anecdotes, the committee recently conducted a survey of participants. While the survey showed a higher level of satisfaction among participants than than Committee anticipated, the survey results did indicate the need to reexamine the program. Generally, mentors are busy, its hard for pairings to find times to connect, and often a network of mentors is needed. In terms of event planning, the Committee is trying to move towards a set of recurrent events. For such events the template would be held constant, reducing the organizing effort required.

   The need for more mentoring and the desire to repeat events, led to the design of the Committee's activities at ISIT

2016 and ISIT 2017. At both ISITs the Committee organized round-table events. The goal was to provide the time and space for mentoring to occur. With the framework fixed, the topics can continue to evolve. Mentors only need to show up. Mentees have the opportunity to talk and connect with multiple senior people.

A question was raised whether it might help the Committee meet its objectives, and perhaps the need to expand outreach to young professionals, if each ISIT had a chair of outreach. It was additionally pointed out that the nascent restructuring of the Membership Committee (of which Outreach is currently a subcommittee) would leave fewer people focused on outreach. This makes the streamlining of activities that Aaron discussed very timely. A worry raised was whether termination of the mentor-mentee pairing program might be unfortunate for the, perhaps 20% of, pairings that work well. Aaron acknowledged that while there are pros and cons of the switch, the Committee feels that new version is both better focus and more sustainable. That said, there are still ways to try to foster one-on-one mentorship. For instance, there is an opportunity during the ISIT round-table for participants to sit down with members of the Outreach Committee to try to identify possible one-on-one mentors.

8) **Short Video Project Initiative:** Michelle Effros provided an update on the videos project. She reviewed the team working on the videos. Two videos have been produced. The first is on network coding, the second on space-time codes. There is funding for additional videos and the team is seeking proposals for additional topics. Selection guidelines include: broad appeal and demonstrated impact (established rather than future technologies). It goes without saying that this is not a venue to push one's own work but rather a mechanism to push community-wide ideas. A short section of the videos were played for the BoG. While the videos were not yet public at the time of the meeting, the plan was to make them public shortly thereafter. Both videos are now available on YouTube. The first is available at https://www.youtube.com/watch?v=B0ZcAWEvjCA. The second is available at https://www.youtube.com/watch?v=cbD4NsZQKYw. As discussed, once finalized, the videos were released in a concerted publicity effort, maximize attention: through the producer's (Brit Cruise's) YouTube channel, which connected the videos to his already large audience, as well as through ITSoc and other channels. To emphasize, the team actively encourages further proposals, with the understanding that the proposer should want to be involved in the development of the video.

9) **Online Talks Initiative:** Suhas Diggavi started by reviewing the five main goals of the initiative. The first is to develop a set of expository lectures. These talk would be by experts, could be based on plenary conference or tutorial talks, and might even be "named" to raise their profile. The second is to create an information theory "hall of fame". This would be a repository of historical reflections on impactful ideas by people in the community. The objective is not be simply to tell the technical story, but rather the stories behind the ideas, stories that capture the historical impact of information theory on technology and society. The third goal is to provide a forum to discuss nascent research ideas, something like a talk accompanying an ArXiv posting. A successful forum would provide a venue to disseminate new ideas within the ITSoc community with the object of enhancing collaboration. The intent is not to have a strongly curated forum, but rather to establish a distributed model like TCS+ or the new Shannon Channel on YouTube, the letter led by Salim El Rouayheb. Suhas told the BoG that the plan is to absorb the Shannon Channel into this new forum, with Salim being involved in this new effort as well. The fourth goal is to provide a venue for (invited) experts from outside the traditional information community to discuss new research directions that could benefit from cross-fertilization with ITSoc. The fifth and final goal is non-academic outreach. The final goal is to foster academic/industrial interaction, perhaps through short forums at conferences or workshops. Suhas then provided the BoG some updates. He, Salim El Rouayheb, and Anand Sarwate are organizing the "ArXiv talks" forum. They would appreciate help with this effort. They ran a test lecture on 13 June for the "Shannon Channel" using Google hangout. They identified numerous issues, most or all of which seem would be solved by instead using Webex. Another live test will occur in the near future (note: this second test occured in Nov. 2017). The target is to have at least one lecture completed prior to the Feb. 2018 BoG meeting. A question was raised as to which of the five goals is the current priority. Suhas responded that the curated lecture series is the current priority. Another recent update (as of Nov. 2017) is that two "hall of fame videos" are already under planning at Stanford and MIT, with resources allocated to them.

10) **Shannon Children's Book Initiative:** Christina Fragouli spoke about the children's book. A number of early hard copies were available at the meeting and were passed around. Feedback from a number of elementary school teachers and from Brit Cruise were incorporated. The last few issues are being resolved. There should be more copies available at the ITA meeting. Some of the remaining Funds of the $10k USD already allocated by the BoG will be used to print copies to distribute at ITA. Currently the price to print is about $10 USD per copy. If the book were distributed on Amazon, the cost to purchase the book (Amazon would handle the printing and distribution) would be $20 USD per copy. At this price point the book would generate no income for ITSoc. Some BoG members commented that $20 USD is expensive for a children's book. At the ITA BoG meeting Christina and Anna will present suggestions for further distribution, as well as exact details on the Amazon possibilities.

11) **Proposal for a new Magazine and/or Special Topics Journal and for a new Magazine:** Ad-hoc Committee Co-Chair Elza Erkip first reviewed progress with regards to the Journal on Special Topics in Information Theory. Following the ISIT BoG meeting, a letter-of-intent was submitted to the IEEE on 30 August. The letter will be reviewed at the next IEEE Technical Activities Board (TAB) meeting in mid-November. A steering committee has been formed, consisting of Robert Calderbank, Muriel Medard, Vincent Poor, and Rüdiger Urbanke, with Jeff Andrews serving as "shadow chair". The committee will be responsible for selecting the first EiC and steering the journal through its first few years. Feedback will be provided by the TAB in late 2017 with a formal proposal then to follow in 2018.

Elza then turned to the discussion of the IEEE Information Theory Magazine. A process similar to that described above for the special topics journal, and timeline, including a submission of a letter of intent to the IEEE TAB, is being followed. The steering committee for the magazine consists of Dan Costello, Christina Fragouli, and Ubli Mitra. Its tasks include developing the vision for the magazine and selection of the inaugural EiC and senior editors.

12) **Shannon Documentary:** Rüdiger Urbanke next provided the BoG an update on the Shannon Documentary. The documentary is progressing, additional shootings have occurred, and a rough first cut has been viewed by BoG members. Additional funds to the amount of over $400k USD has been raised. The total amount raised to date is about $900k USD. A short sequence was viewed at the BoG meeting. Rüdiger shared with the BoG some of the feedback provided to the director by those BoG members who have watched the rough cut. There was a discussion of how the director might get some clips of community members speaking about the contributions and impacts of Shannon for incorporation into the film. Some filming of community technical activities may occur.

13) **CloudComm:** Aaron Wagner next presented to the board on his hands-on approach to teaching digital communications at Cornell University. He noted that many digital communication classes are theory-oriented. This maybe, at least in part, because it is hard to develop, and expensive to maintain, hands-on labs for such courses. However, without a lab, it is difficult really to experience many real-world communication issues such as synchronization, and one looses the excitement of getting a system working in the real world. At the same time, even given an established lab, it is challenging to ensure everything works and that all student groups face the same channel because different lab stations in the same lab space will behave differently. To resolve these issues Aaron developed a lab-in-the-cloud approach. In this approach a single physical-layer experimental setup can be accessed by students over a network. Students interface with the channel through easy-to-develop WAV files. While the setup exists at Cornell University, it can be expanded to be available for use by students at other schools. In other words, a single instance of physical-layer hardware could be maintained for global use.

    The BoG asked what educational level this setup is aimed at. Aaron responded that, at Cornell, it is used in a fourth year course. Currently communications is over a baseband audio channel. He hopes to have an RF-band equivalent working by November for use in a first-year graduate course. Aaron made the point that the setup is flexible. It can be used to study a wide range of communication issues including how to combat inter-symbol interference, how to establish synchronization, and to test the efficacy of error-correction coding. In Aaron's experience students gain a huge amount from working with a real-world channel rather than an emulator thereof. A number of further questions and discussion the followed: whether this setup could be integrated into classes that use other types of hardware, e.g., Arduinos; whether supporting an initiative like this falls within the mandate of ITSoc; how widely such a setup would be used (a question that might be partially answered through surveys) and whether such a system might prove especially useful for under-resourced institutions across the world. One BoG member raised the issue of massively open online courses (MOOCs), whether this framework could fit into a MOOC, and the fact that something analogous is being done for a Georgia Tech MOOC on robotics. In that MOOC the robots are physically located at Georgia Tech, students only ever interact with them remotely. A discussion then followed as to whether ITSoc support for this initiative could factor into a larger educational outreach effort by the Society including the videos project and online learning of basic information theory. The final point of discussion surrounded sustainability: what would be needed to ensure the long-term availability of the resource. The next steps Aaron will be taking are two-fold. The first is to write an article for the Newsletter to help judge the interest amongst ITSoc member. The second is to consider how this idea might be integrated into larger outreach efforts.

14) **Recap of Bylaws:** Michelle Effros took a few minutes at the end of the meeting to discuss some aspects of the Bylaw changes she had not gotten to, especially regarding the reorganization of the membership committee. Some subcommittees of the Membership Committee (Outreach, WIHITS) are formed and even chaired by ITSoc members that are not members of the Membership Committee. This needs to be fixed in a future revision of the Bylaws. The relevant committee chairs were tasked with coming up with a proposal for the structure that they think would best serve these activities.

15) **Adjournment:** The meeting adjourned at 1:27pm local time.

Recent Publications

IEEE Transactions on Information Theory

Table of content for volumes 63(12), 64(1), 64(2)

Vol. 63(12): Dec. 2017.

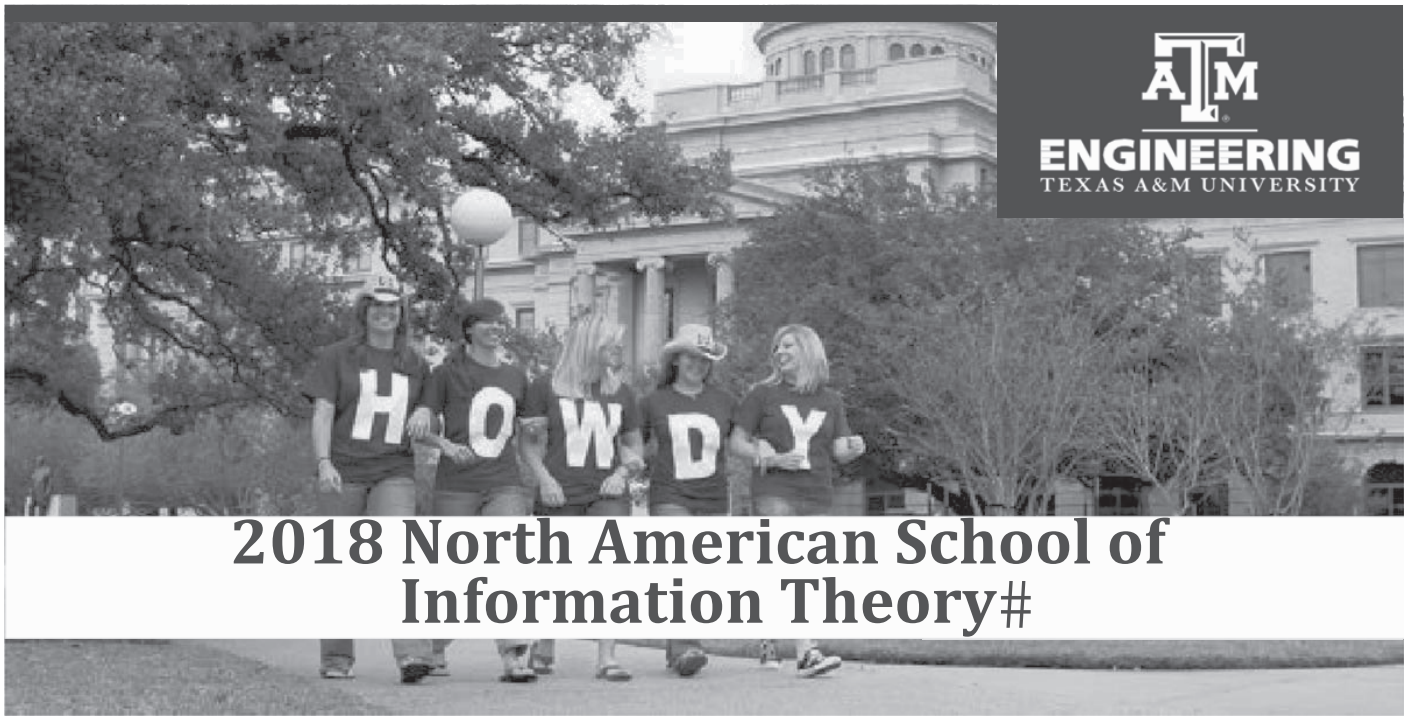
Vol. 64(2): Feb. 2018.

Foundations and Trends in Networking

Volume 12, Issue 3
Age of Information: A New Concept, Metric, and Tool
Antzela Kosta, Nikolaos Pappas and Vangelis Angelakis

Foundations and Trends in Signal Processing

Volume 11, Issue 34
Massive MIMO Networks: Spectral, Energy, and Hardware Efficiency
Emil Björnson, Jakob Hoydis, and Luca Sanguinetti



2018 North American School of Information Theory#

May 20-23, 2018

Hands-on machine learning workshop
by Alex Dimakis, UT Austin
Lectures by:
Frank Kschischang, University of Toronto (Padovani Lecture)
Olgica Milenkovic, UIUC
Yury Polyanksiy, MIT
Naftali Tishby, Hebrew University
Rajesh Sundaresan, Indian Institute of Science

Registration Deadline: May 1, 2018

Students who register before April 15 may be considered for
a limited number of travel grants
Schedule includes student research poster sessions and evening learning activities
Please contact Dr. Krishna Narayanan [krn@tamu.edu] for more information

http://shannon.tamu.edu

IEEE INFORMATION THEORY SOCIETY

NSF

Center for Science of Information
NSF Science and Technology Center

Welcome to ITW 2018 in Guangzhou! ITW 2018 solicits and welcomes original contributions on the frontiers of information theory, coding theory and their applications, as well as the frontiers with other fields such as data science, biology and signal processing. The conference structure consists of a daily plenary seminar followed by two parallel sessions throughout the day. Guangzhou is the third largest city in mainland China with a history of over 2,000 years. The conference will take place at the **Sun Yat-sen Kaifeng Hotel**, located within the university campus where the attendees can explore many historic architectures and artifacts, including the famous Swacey Hall, Xing Pavilion, Scholar Archway and many others. The conference also provides ample social events for better interactions among the participants. With appreciation and anticipation, we look forward to welcoming you in Guangzhou.

Scope of Submission

Original papers on **Information and Coding Theory** are encouraged for submission. The scope of submissions includes, but is not limited to

- Information Theory and its Applications
- Frontiers of Coding Theory and Practice
- Boundaries between Information Theory and Data Science, Biology and Signal Processing
- Network Information Theory
- Network Coding and Distributed Storage
- Information Theoretic Security

Important Dates

Paper submission : **May 18, 2018**
Acceptance notification : **August 13, 2018**
Final paper submission : **September 13, 2018**
Tutorial proposal submission: **March 1, 2018**
Tutorial acceptance notification: **March 15, 2018**

General Chairs

Pingzhi Fan - Southwest Jiaotong University, China
Aria Nosratinia - University of Texas at Dallas, USA
Li Chen - Sun Yat-sen University, China

Technical Program Chairs

Krishna Narayanan - Texas A&M University, USA
Dongning Guo - Northwestern University, USA
Pascal Vontobel - The Chinese University of Hong Kong, Hong Kong SAR, China
Daniela Tuninetti - University of Illinois at Chicago, USA

Publication Chairs

Shenghao Yang - The Chinese University of Hong Kong (Shenzhen), China
Qin Huang - Beihang University, China

Publicity Chairs

Xiaojun Yuan - University of Electronic Science and Technology of China, China
David Mitchell - New Mexico State University, USA

Financial Chair

Baodian Wei - Sun Yat-sen University, China

Chinese IT Society Liaison

Yunjiang Wang - Xidian University, China

Call For Papers

10th International Symposium on Turbo Codes & Iterative Information Processing
Hong Kong, China, December 3-7, 2018

Honorary General Chair:
Claude Berrou, Telecom Bretagne, France

General Co-Chairs:
Michel Jezequel, Telecom Bretagne, France
Li Ping, City University of Hong Kong, Hong Kong
Francis Lau, Hong Kong Polytechnic University, Hong Kong

Technical Program Committee Co-Chars:
Catherine Douillard, Telecom Bretagne, France
Werner Henkel, Jacobs University, Bremen, Germany

Technical Program Committee:
See http://www.istc2018.org/committes/

CALL FOR PAPERS

The 10th International Symposium on Turbo Codes & Iterative Information Processing will be held from Monday 3 December to Friday 7 December 2018 in Hong Kong. The symposium will be an opportunity to acquire a broad overview of the current status of advanced research in iterative information processing and its application to information theory and digital communications. All original contributions will be considered, in both theoretical and applied fields. Possible topics for submissions include, but are not limited to, the following:

- Error correcting coding
- Turbo, LDPC and polar codes
- Bit-interleaved coded modulation
- Interleaving and labeling
- Graph codes for compression
- Joint source-channel coding
- Coding for storage
- Iterative detection
- Multi-user and MIMO applications
- Turbo equalization
- Synchronization
- Cooperative communications
- Iterative processing over networks
- Bounds, performance, and convergence
- Iterative signal processing algorithms
- AMP and compressed sensing algorithms
- Bayesian inference and factor graphs
- Chip applications
- Applications in bio-informatics
- Data fusion

This symposium will have special sessions focused on the current and future trends in modern forward error control coding and iterative signal processing.

The symposium will include regular papers for oral and poster sessions as well as invited papers. Accepted and presented papers/posters will appear in the symposium proceedings as well as IEEEXplore (upon final decision by IEEE).

Submissions
Authors are invited to submit a full manuscript (not exceeding 5 pages) via the symposium website detailed below.

Submission of papers deadline: **June 15, 2018**
Notification of acceptance: **August 15, 2018**
Final papers and early-bird registration deadline: **September 15, 2018**

For further information regarding paper submission, registration, accommodation, and travel, please consult the symposium website at:

http://www.istc2018.org/

Entropy (ISSN 1099-4300) invites submissions to the special issue "Entropy and Information Inequalities".

The deadline for submission is June 29, 2018.

In recent decades, information theoretic inequalities have provided an interface with both neighboring and seemingly disparate disciplines. What is more, bridges built from these interactions have produced new and richer understandings of Information theory itself. Important connections have been established between information theoretic inequalities and subjects including, convex geometry, optimal transport, concentration of measure, probability, statistics, estimation theory, additive combinatorics, and thermodynamics, by way of inequalities; entropy power, Brunn–Minkowski, HWI, log-Sobolev, monotonicity in CLT, Sanov, sum-set, Landauer, and many more. Even within information theory, there has been renewed interest in developing inequalities in non-conventional settings such as convolution inequalities for Renyi or Tsallis entropy, inequalities for f-divergences, and entropy inequalities over discrete spaces.

In this Special Issue, we would like to invite contributions that establish novel information theoretic inequalities (broadly defined), extend the applications thereof, and deepen our understanding of information theory and related fields. Expository submissions are welcomed, and we envisage that these contributions will lead to an improvement of acumen in information theory, while also strengthening the growing bonds between the subject and the other areas outlined above, with the hope of generating further inter- field and interdisciplinary dialog.

Deadline for manuscript submissions is June 29, 2018.

Guest Editors: Dr. James Melbourne, Dr. Varun Jog

Multiple research positions in information theory and nonlinear fiber optics at TU Eindhoven

TU Eindhoven is hiring one postdoctoral researcher and one fully funded PhD student to work on the project FUNNOTCH: Fundamentals of the Nonlinear Optical Channel. Both positions are available for four years and are in the Signal Processing Systems (SPS) group at the Technical University of Eindhoven, The Netherlands.

FUNNOTCH is a 5 year research grant financed by the European Research Council (ERC Starting Grant). The PI is Dr. A. Alvarado and includes two fully-funded PhD students and two postdoctoral researchers. Some of the problems/topics that this project will address are discrete and continuous-time channel models in the highly nonlinear regime, information theory and channel capacity analysis of the nonlinear fiber optical channel, modulation, signal shaping, and error control coding.

TU Eindhoven offers an extensive package of fringe benefits (e.g., excellent technical infrastructure, the possibility of child care, and excellent sports facilities). TU Eindhoven also offers a competitive salary, the possibility of a salary boost via the so-called 30% tax benefit rule (if certain conditions are met), as well as an 8% holiday, and 8.3% end-of-year annual supplement.

More details about the positions can be found https://www.sps.tue.nl/ictlab/project/funnotch/

Alex Alvarado

President's Column *(continued from page 1)*

Brit's YouTube channel "Art of the Problem." Two more are in production and more are envisioned in the coming years. Anna Scaglione and Christina Fragouli co-authored and produced a wonderful children's book, "Information in Small Bits," aimed at elementary and middle school children. The book was distributed to the attendees of ITA this year and will soon be available for sale to the general public.

Looking into the future, we have several initiatives to expand the use of and exposure to Information Theory in the scientific community at large. Jeff Andrews is chairing the Steering Committee of a new Journal on Selected Topics in Information Theory. This will be a multi-disciplinary journal publishing special issues on the intersections of information theory with fields such as machine learning, statistics, genomics, neuroscience, theoretical computer science, and physics as well as on hot topics within information theory. Wojciech Spankowski is chairing the Steering Committee that is looking into revamping our beloved newsletter, and turning it into an archival publication that will include tutorial articles in core Information Theory topics as well as cross-cutting areas. Our Board of Governors had to prioritize the projects to make the best use of our finite resources, and decided to pursue the Selected Topics Journal first. Jeff plans to bring a detailed Phase 1 proposal for IEEE's consideration in the next few months. Wojciech will follow with the second project shortly thereafter.

As information theorists, we know very well the importance of diverse viewpoints: A channel with two independent looks at the output has higher capacity than a channel with two identical looks (see Problem 7.20, Second Edition of Cover & Thomas). Unfortunately, both our society and the IEEE still have a long way to go in terms of diversity. In terms of geographical diversity, Information Theory Society needs to increase membership and leadership from Region 10 (Asia-Pacific), which is one of the fastest growing regions of the IEEE. On the topic of gender diversity, according to a recent IEEE Survey on Women in Tech (summarized in page 11 of this Newsletter), 73% of women have experienced negative outcomes in their careers attributed to being a woman and 28% have experienced unwanted sexual advances. Sadly, our society is not immune to the types of events we are now accustomed to hearing in the recent #MeToo movement; Andrea Goldsmith shares an experience she had at her first ISIT in her interview in the Student's Corner (page 12 of this Newsletter).

Our Board of Governors, in its most recent meeting in February 2018, approved a statement to reaffirm the IEEE Code of Conduct, IEEE Code of Ethics, and IEEE Non-discrimination Policy, particularly in the context of harassment, bullying, discrimination and retaliation. You will find the complete statement on page 10 of this Newsletter. This statement will also be prominently displayed on our web site. The board also approved forming an Information Theory Society Ad-Hoc Committee on Diversity and Inclusion, the mission of which is to ensure contributions from and recognition of a diverse group of participants in our society. In addition to continuing the society's numerous technical and outreach activities, my goal as the President is to ensure a diverse and inclusive environment for everyone who chooses to pursue this beautiful field I fell in love with many years ago. I am happy to hear from all of you; please feel free to contact me at elza@nyu.edu.

Conference Calendar

DATE	CONFERENCE	LOCATION	WEB PAGE	DUE DATE
March 17–22, 2018	**IEEE Wireless Communications and Networking Conference (WCNC)**	Barcelona, Spain	http://wcnc2018.ieee-wcnc.org/	Passed
March 21–23, 2018	**52nd Annual Conference on Information Sciences and Systems (CISS)**	Princeton University, USA	http://ee-ciss.princeton.edu/	Passed
April 16, 2018	**The First Workshop on the Age of Information (AoI Workshop)**	Honolulu, HI, USA	https://www.eng.auburn.edu/AoIWorkshop/	Passed
April 25–26, 2018	**6th Iran Workshop on Communication and Information Theory (IWCIT)**	Sharif University of Technology, Tehran, Iran	http://iwcit.com/	Passed
May 7–11, 2018	**16th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)**	Shanghai, China	http://www.wi-opt.org/	Passed
May 7–11, 2018	**European School of Information Theory (ESIT)**	Bertinoro, Italy	http://www.itsoc.org/conferences/schools/2018-european-school-on-it	—
June 17–22, 2018	**IEEE International Symposium on Information Theory (ISIT)**	Vail, Colorado, USA	http://www.isit2018.org	Passed
June 25–28, 2018	**The 18th IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)**	Kalamata, Greece	http://spawc2018.org/	Passed
June 25–29, 2018	**50th Annual ACM Symposium on the Theory of Computing (STOC)**	Los Angeles, CA, USA	http://acm-stoc.org/stoc2018/	Passed
October 2–5, 2018	**56th Annual Allerton Conference on Communication, Control, and Computing**	Allerton, University of Illinois at Urbana-Champaign, USA	http://allerton.csl.illinois.edu/	—
October 28–31, 2018	**International Symposium on Information Theory and Its Applications (ISITA)**	Singapore	http://www.isita2018.org	April 6, 2018
November 25–29, 2018	**Information Theory Workshop (ITW)**	Guangzhou, China	http://www.itw2018.org/	May 18, 2018
December 3–7, 2018	**10th International Symposium on Turbo Codes & Iterative Information Processing (ISTC)**	Hong Kong, China	http://www.istc2018.org/	June 15, 2018

Major COMSOC conferences: http://www.comsoc.org/confs/index.html