SECRET KEY AGREEMENT: FUNDAMENTAL LIMITS AND PRACTICAL CHALLENGES

ZOUEIR REZKI, MARWEN ZORGUI, BASEL ALOMAIR, AND MOHAMED-SLIM ALOUINI

ABSTRACT

Despite the tremendous progress made toward establishing PLS as a new paradigm to guarantee security of communication systems at the physical layer, there is a common belief among researchers and industrials that there are many practical challenges that prevent PLS from flourishing at the industrial scale. Most secure message transmission constructions available to date are tied to strong assumptions on CSI, consider simple channel models and overlook the practical challenges that prevent PLS from flourishing. Therefore, PLS is regarded as a new approach that may complement existing cryptographic encryption techniques in order to achieve wireless network security. Perhaps arguably, the most likely way to leverage PLS in securing modern wireless communication systems is via secret-key agreement. In the latter setting, the legitimate parties try to agree on a key exploiting the characteristics of the channel, such as fading and/or noise, to secure communications via sophisticated channel coding schemes. For concrete examples how to exploit channel characteristics via received signal strength (RSS), channel phase estimation, or frequency domain characteristics, for key agreement, please see, for example, [1, 2]. Exploiting physical layer techniques such as cooperative communications can substantially enhance the key exchange rate, for example, [3]. Since then, PLS has been regarded as a new approach that may complement existing cryptographic encryption techniques in order to achieve wireless network security. Perhaps arguably, one of the promising applications of PLS is secret-key agreement in which the legitimate parties try to agree on a secret key. The concept of sharing a key between legitimate parties is formalized in [4]. Essentially, this concept relies on exploiting common randomness that the legitimate parties have in order to agree on a key. Mainly, two channel models for secret key agreement have been proposed [5]. The source model (SW) and the channel model (CW). The SW model depicts a scenario where common randomness is generated by an independent discrete memoryless source whose output is observed by two legitimate terminals and an eavesdropper. For instance, this model can be useful if the legitimate parties are sensors that measure vital parameters (temperature, pressure, humidity) and that need to communicate in order to control securely a nuclear station. The CW model, on the other hand, depicts a scenario where the source is monitored by a legitimate user. Essentially, this is closely related to the wiretap channel [6], but including a public channel. Specifically, in the CW model, two legitimate terminals want to agree on a key while keeping it secret against a third terminal, the eavesdropper. The legitimate terminals have at their disposal a one-way memoryless noisy channel and a two-way public channel with high capacity. Both channels are also available to the eavesdropper who can observe, but cannot tamper any of them. In this article, our focus is rather on the CW model. More precisely, we consider a CW model where the outputs at the destinations are independent given the input. The secret-key capacity in this case is known in both fast and quasi-static fading channel models [7, 8]. For an illustration, Fig. 1 depicts a high-level multiple-antenna secure communication model. In Fig. 1, Alice wants to communicate with Bob over a wireless channel, and an eavesdropper, Eve, is listening to their communication through...
another wireless channel. All terminals have multiple antennas. The channel state information (CSI) in Fig. 1 may be regarded as an indication of the quality of each wireless channel. Via a channel estimation mechanism, Alice has a measure of the main channel that is often designated as CSI-T. Bob, in turns, also has a measure of the main channel, that is, CSI-R. On the other hand, the eavesdropper is also able to obtain a measure of its channel to Alice designated in Fig. 1 as the eavesdropper channel. In wireless communication security, the aim is to investigate whether Alice can communicate with Bob in a secure manner, exploiting the property of the channel, while leaking a marginal amount of information to Eve.

On the other hand, incorporating multi-element antennas at the transceivers enhances both reliability and throughput of wireless communications. Generally, these performances are measured via the diversity and the multiplexing gains, respectively. Traditionally, multiple antennas have been used to increase diversity to combat channel fading. Another design point of view suggests that in a multiple-input multiple-output (MIMO) channel, fading can be beneficial, through increasing the degrees of freedom available for communication. Most communication systems have been designed with respect to one of these lines of thought to achieve either the maximum diversity gain, or the maximum multiplexing gain, but not both. This disconnect between the two design paradigms motivates the need for a unified metric to assess MIMO communication performance.

About 15 years ago, a novel interpretation of MIMO channels emerged. It advocates that both gains can actually be extracted simultaneously, but there is a fundamental trade-off between how much of each gain a coding strategy can get. For instance, if a design engineer wants to achieve a higher diversity gain, then he/she needs to sacrifice some multiplexing gain, and vice versa. This is the so-called diversity-multiplexing trade-off (DMT) [9]. The DMT is a high signal-to-noise ratio (SNR) metric that characterizes the optimal trade-off between these two gains. Essentially, the diversity gain depicts how steep the error probability is versus SNR, whereas the multiplexing gain measures how fast the transmission rate scales with SNR. Meanwhile, the outage probability is defined as the probability that the target transmission rate is higher than the channel mutual information. It turns out that at high SNR, the outage events are the main sources of error. That is, characterizing the outage event of a particular channel implies derivation of its DMT.

Since then, the DMT has attracted a lot of attention from researchers and industry due to its simplicity, and also because it represents the first unified guidelines to design space-time codes for MIMO communication systems. Naturally, this interest has expanded to include communication systems with a secrecy constraint.

The DMT has attracted a lot of attention from researchers and industry due to its simplicity, and also because it represents the first unified guidelines to design space-time codes for MIMO communication systems. Naturally, this interest has expanded to include communication systems with a secrecy constraint.

Figure 1. A high-level security model. Alice and Bob want to communicate securely over a wireless channel. Eve, an eavesdropper, is listening to their communication through a different wireless channel. All terminals have multiple antennas. Measurements of the channel quality (CSI) is obtained at the terminals through channel estimation mechanisms.

**Error Performances and Secret-Key DMT**

**Related Background**

As previously mentioned, the SW and CW models have been proposed for key generation in [5]. In this article, our focus is rather on the CW model. In this model, two legitimate terminals want to

---

**IEEE Wireless Communications • Accepted for publication**
The CW with public channel. Alice and Bob want to agree on a key while keeping Eve ignorant about it. Alice and Bob have access to a two-way public channel with infinite capacity that is also observed by Eve.

To distill a secret key from the codewords transmitted over the noisy channel, the transmitter and the receiver are allowed to communicate over a two-way authenticated public channel with infinite (very high in practice) capacity. In this definition, “public” implies that the eavesdropper, likewise the legitimate users, has access and thus can track all communications over this channel; “authenticated” means that the eavesdropper can listen, but cannot alter the transmitted messages. Concisely, key-agreement consists of transmissions over the noisy channel as well as exchanges of messages through the public link. As a result of this process, the source and the destination produce the keys $K$ and $L$, respectively, where $K$ and $L$ both belong to a finite set $\mathcal{K}$.

We are particularly interested in the behavior of the error probability at high SNR when the source and the destination are agreeing on a key at a target rate $R_{E}^{(1)}(\text{SNR})$ that is a function of SNR.

**Definitions:** The secret-key multiplexing gain $r_{k}$ is defined as the ratio of the secret-key rate $R_{E}^{(1)}(\text{SNR})$ to $\log(\text{SNR})$.

The key outage events are the events where the key rate at which the legitimate parties share a key is higher than the secret-key capacity of the channel. Intuitively, we qualify the secret-key outage events as the events where the target key rate is greater than what the channel can support. Accordingly, we define the key outage probability as the probability of occurrence of these events.

Similarly, the secrecy outage events are the events where the target secrecy rate at which the legitimate parties communicate, is higher than the secrecy capacity of the channel. The secrecy rate outage probability is the probability of occurrence of these events.

As defined above, the secret-key multiplexing gain gives an indication as to how fast the target key rate varies with increasing SNR, whereas the secret-key diversity gain depicts how the error probability decreases with increasing SNR.

**Secret-Key DMT Characterization**

In order to characterize the secret-key DMT, one needs to analyze the possible error events. For this purpose, let us consider a CW channel upon which the source and the destination agree on a key at a fixed (i.e., not adaptive with CSI) rate $R_{E}^{(1)}(\text{SNR})$. Then, the error events are due to three possible events:

- $E_{1}$: the key agreement between the legitimate parties is violated.
- $E_{2}$: the secret-key leakage is not arbitrarily low.
- $E_{3}$: the key is not uniformly distributed.

Thus, in order to characterize the error probability at high SNR, one needs to evaluate the probability of occurrence of each event $E_{i}$, $i \in \{1, 2, 3\}$. It turns out that at the scale of interest, event’s $E_{1}$ contributions are only marginal so that the error probability is essentially dominated by events $E_{1}$ and $E_{2}$. That is, $P_{E}(\text{SNR}) = \text{Prob}(E_{1} \cup E_{2})$. By properly choosing the rates of the involved codebooks, it can be verified that at high SNR, $\text{Prob}(E_{1} \cup E_{2}) = \text{Prob}(E_{2})$ and hence the CW channel is equivalent to a MIMO channel with

\[
\begin{align*}
    Y_{D} &= H_{D}X + N_{D} \\
    Y_{E} &= H_{E}X + N_{E}
\end{align*}
\]
[m_s - m_t]^* and m_0 transmit and receive antennas, respectively, from a DMT point of view. Details regarding the latter statement are too technical to be included here, but can be found in [11]. That is, the eavesdropper “steals” m_2 transmit antennas only, without affecting the destination. What is even more striking is that this result holds true regardless of whether the transmitter does or does not have CSI-T. This is different from the MIMO wiretap channel where CSI-T is very crucial in comparison with the safe DMT. However, the secrecy constraint and the secret-key constraint induce a loss in both the multiplexing and the diversity gains compared to the safe DMT. Nevertheless, the key DMT is higher than the secret DMT for any multiplexing gain.

Figure 3b displays the DMT of three communication scenarios and for (m_s, m_t, m_r) = (5, 3, 2). Here, we note that the safe DMT, the no CSI-T secret DMT, and the key agreement DMT are respectively equal to d_{5,3}(r), d_{3,1}(r), and d_{1,3}(r), respectively. As can be seen in Fig. 3a, the secrecy constraint and the secret-key constraint induce a loss in both the multiplexing and the diversity gains compared to the safe DMT. Nevertheless, the key DMT is higher than the secret DMT for any multiplexing gain.

In this section, we assume that the source has full CSI of both its channel to the destination and its channel to the eavesdropper, while acquiring CSI to the legitimate receiver is reasonable enough in regard of the fact that the source and the destination belong to the same network and thus may share their CSI. It is quite tenuous to assume CSI-T of the eavesdropper’s channel since the latter may not be part of the network. However, as we argue below, such an assumption is not always mandatory to design DMT-optimal key-agreement schemes. In the case of full CSI-T, the secret DMT is equal to secret-key DMT. Hence, there exists at least three strategies to agree on a key optimally in the high-SNR regime.

**Exploit the Public Channel by Creating a Virtual Wiretap Channel from the Legitimate Receiver to the Source:** The conceptual (virtual) wiretap channel can be described briefly as follows. First, Alice generates a sequence X^o of independent and identically distributed (i.i.d.) symbols from a message transmission is, in part, due to the availability of the high-capacity public channel that makes up for the lack of CSI at the transmitter. Furthermore, from a signaling design perspective, we note another advantage of coding for secret-key agreement. Indeed, we have found that allocating the power evenly among the source antennas is DMT-optimal, whereas it is strictly sub-optimal from a secret DMT perspective. In Fig. 4, we plot the secrecy rate outage and the secret-key rate outage performances, for (m_s, m_t, m_r) = (2, 2, 1). In both curves, the input covariance matrix is set to K_X = SNR I, and the target multiplexing gain is set to r_s = r_k = 0.8. Analytically, we expect the secret diversity gain to be equal to d_s = 0.2 and the secret-key diversity gain to be equal to d_k = 0.4. Figure 4 is consistent with our analytical derivation and shows that while simple signaling is optimal in key agreement transmission, it generally fails to achieve full performance in the case of secret message transmission.

**Comments on Secret-Key DMT-Achieving Schemes**

In this section, we assume that the source has full CSI of both its channel to the destination and its channel to the eavesdropper, while acquiring CSI to the legitimate receiver is reasonable enough in regard of the fact that the source and the destination belong to the same network and thus may share their CSI. It is quite tenuous to assume CSI-T of the eavesdropper’s channel since the latter may not be part of the network. However, as we argue below, such an assumption is not always mandatory to design DMT-optimal key-agreement schemes. In the case of full CSI-T, the secret DMT is equal to secret-key DMT. Hence, there exists at least three strategies to agree on a key optimally in the high-SNR regime.
wiretap channel. The outage probability of the hybrid scheme is expected to be lower than its corresponding secret DMT-achieving scheme.

**Effect of Transmit Correlation on Secret-Key Capacity and Optimality of Beamforming**

**Related Background**

Here, our focus is on secret key agreement over a fast-fading multiple antenna wiretap channel. Different from the quasi-static model, the fast fading channel model is good to capture low-rate delay-unconstrained communication such as text messaging. Furthermore, we assume that the fading associated with the transmit antennas are correlated, whereas those associated with the receive antennas (the destination and the eavesdropper) are uncorrelated. We note that Fig. 2 depicts a channel model for key agreement with fading, hence it is valid here too. The only precision that we should add is that while earlier the channel matrices are i.i.d., $H_D, H_E \sim \mathcal{CN}(0, I)$, in this section $H_D$ and $H_E$ are not i.i.d., that is, $H_D, H_E \sim \mathcal{CN}(0, R_I)$, where $R_I$ is the transmit correlation matrix. Recall that in [7], it is assumed that the channel matrices are uncorrelated. However, in practical systems, the antennas might be correlated at the transmit side and/or the receive side. This is the case, for instance, when there is not enough spacing between antennas.

There exists a panoply of work studying the effect of spatial correlation on wireless communications with no secrecy constraint (e.g. [12]). For instance, in [13, 14], the multiple input single output (MISO) is studied in the case of transmit correlation. It is indicated that the gain obtained through even partial knowledge of the channel can be substantial. In [15], the MIMO system with transmit correlation and imperfect feedback is studied. The optimal input covariance matrix is characterized and requires transmission of independent Gaussian symbols in the directions of the channel covariance eigenvectors, which parallels the result obtained in [13] for the MISO case. Furthermore, [15] investigates beamforming in the MIMO case and provides a sufficient and necessary condition for its optimality. Restricting the input covariance matrix to be rank one (a scheme also called beamforming) considerably simplifies the encoding/decoding at the transmitter and at the receiver. It is argued in [13] that beamforming can perform close to the optimal strategy in certain situations.

**System Model**

Our system model is similar to the one depicted in Fig. 2, with the difference that the channel gains now are not fixed, but vary from one symbol transmission to another. In addition, we assume that Alice is only aware of the statistics of both $H_D$ and $H_E$ and hence is aware of the transmit correlation matrix. Clearly, the (ergodic) capacity of this channel may be obtained along similar lines as in [7]. Furthermore, it may be easily shown that a circular-symmetric complex Gaussian input $\sim \mathcal{CN}(0, k_I)$ is here again optimal. However, while allocating the power evenly among the transmit antennas is optimal in case $H_D$ and $H_E$ are i.i.d. [7], we are interested in knowing how
Alice will exploit the correlation matrix in order to maximize the secret-key rate.

**Effect of the Transmit Correlation on the Capacity**

First, we note that the guidelines reported in this subsection are technically detailed in [16]. Indeed, one can show that the covariance matrix maximizing the key rate has the same eigenvectors as the channel covariance matrix. That is, transmitting independent complex Gaussian symbols along the eigenvectors of the transmit correlation is optimal. The strength of each eigenvector (i.e., the value of its corresponding eigenvalue) can be found numerically via an optimization procedure. Also, the trace constraint should be satisfied with equality as a consequence of the strict monotonicity of the capacity in $K_S$.

It is particularly appealing to see that the optimal input covariance matrix has the same structure as in the case of a MIMO communication without secrecy constraint [15]. A question of practical interest would be to know under which condition beamforming is optimal. Beamforming is the transmission strategy that exploits only the strongest eigenmode, to which the full amount of power is given. One can thus develop a necessary and sufficient condition for beamforming optimality. Technical details are similar to those used in [15] and can be found in [16]. We illustrate the region where beamforming is optimal in Fig. 5a via an example where the channels $H_D$ and $H_E$ have the same statistics. In Fig. 5a, the region under which beamforming is optimal is located below the curve, $P$ designates the transmit power budget, $\sigma^2$ represents the common variance of $H_D$ and $H_E$ entries, whereas $\lambda_1^2$ and $\lambda_2^2$ denote the strength and the second strongest eigenvalues of the transmit correlation matrix, respectively. Depending on the two dominant eigenvalues, the transmitter can determine whether beamforming is optimal or not.

In order to assess the effect of transmit correlation, we display in Fig. 5b the secret-key capacity with and without correlation. Also shown in Fig. 5b are the secret-key rate of beamforming and the secret-key rate when the power is split equally among the channel modes, an optimal strategy in the uncorrelated case [7]. For this configuration, we set $(m_s, m_D, m_E) = (2, 1, 1)$, and the (full rank) correlation matrix $\Delta^2 = \text{diag}(1.8, 0.2)$. As can be seen in Fig. 5b, in the high-power regime, a key capacity loss due to transmit correlation is observed. However, in the low-power regime, transmit correlation provides a key capacity higher than the one corresponding to the no-correlation case, which suggests that correlation may help increase the secret-key capacity. We also note that the key capacity in the no-correlation case scales as $\log(SNR)$ as $\text{SNR} \gg 1$, which confirms that the key multiplexing gain is equal to $\min(m_S - m_E, m_D) = 1$ as shown earlier. We also see that full rank transmit correlation does not affect the scaling law of the secret-key capacity, which also scales as $\log(SNR)$ at high SNR, as shown in Fig. 5b. Furthermore, beamforming is optimal in the low-power regime, whereas it is suboptimal in the high-power regime.

**Practical Challenges**

In the previous sections, we highlighted the importance of secret-key agreement mechanisms in establishing secure systems at the physical layer. However, the benefits of secret-key agreement mechanisms depend enormously on the existence of a free public channel whose capacity is unbounded. Naturally, this channel may not always be physically available due to spectrum scarcity and/or its high operating cost. However, and as we argue below, new technologies may be leveraged in order to create such a channel.

**Public Channel Through Relay Helpers:** In this architecture, the public channel can be a set of helpers from the source to the destination. As depicted in Fig. 6, the helpers $K_i$’s, $i = 1, \ldots, 6$, thus chosen, form a versatile public channel that can change depending on the helpers’ channel gains strengths.

**Public Channel Through a Fiber Optic Link:** In the case where Alice and Bob are an access point and a base station, respectively, a fiber optic link can be used as a public channel. In regard of its high data rate (10-100 Tb/s), the fiber optic link may not be necessarily dedicated to this role and could serve other purposes.

---

Figure 5. Effect of transmit correlation on the key agreement capacity: a) Regions where beamforming is or is not optimal. The source has 2 antennas, the destination has 4 antennas and the eavesdropper has a single antenna; b) The Secret-key rate versus SNR for different transmit schemes. In both figures, $(m_s, m_D, m_E) = (2, 4, 1)$. 
There is a consensus that wireless physical layer security is here to stay. We argued in this article that secret-key agreement is one of the most important tools to provide security mechanisms of data networks at the physical layer. This is mainly because their rate is generally higher than that of secret message transmission, as well as their inherent flexibility in terms of coding schemes.

Public Channel Through Ultra-Wideband (UWB) Communications: UWB wireless communication is a technology for transmitting large amounts of digital data over a wide frequency spectrum using short-pulse, low-powered radio signals. UWB communications transmit in a manner that does not interfere with conventional narrowband and carrier wave used in the same frequency band. Hence, while common randomness is exchanged between the legitimate parties at typical wireless narrowband frequencies (between 800 MHz and 2.1 GHz), all terminals may stretch their frequency range in order to achieve high data-rate UWB communications that will be utilized as a public channel. In order for this frequency expansion mechanism to work, all terminals should have UWB transceiver capabilities.

Obviously, in no way is the above list of examples exhaustive. It only gives a few ideas how engineers can leverage network features along with sophisticated physical layer techniques to make the public channel available. Nevertheless, availability of the public channel using resources at the physical layer may still be challenging as it requires sophisticated algorithms and protocols at the upper layers in order to identify the public channel, let alone issues related to authentication and active eavesdropping.

Furthermore, as with most fundamental limitations of communication systems, the performance limits established in this article rely on realistic assumptions such as the high-SNR analysis for secret-key DMT, and ignores issues related to the complexity of key-exchange mechanisms. In practice, for example, for cellular networks, wireless sensor networks, or optical communications, key exchange between the legitimate parties should happen while considering the budget limits at the transceivers (power, energy, etc.). Hence, the high-SNR assumption is not realistic in these cases; instead, considering the notion of DMT at finite-SNR is more appealing. The finite-SNR secret-key DMT would provide a measure of reliability of key-exchange communications, but for a given SNR value. Nonetheless, the high-SNR secret-key DMT studied in this article provides useful insights that translate into design guidelines for key-exchange communications.

On another note, the key-exchange schemes presented here and in related work ignore the encoding and decoding complexity. In several scenarios, the legitimate terminals have only limited computation capability (processor speed, memory, etc.). In these cases, it is of interest to study suboptimal key-exchange schemes in order to assess the loss induced by the complexity constraint.

CONCLUSION

There is a consensus that wireless physical layer security is here to stay. We argued in this article that secret-key agreement is one of the most important tools to provide security mechanisms of data networks at the physical layer. This is mainly because their rate is generally higher than that of secret message transmission, as well as their inherent flexibility in terms of coding schemes. We have highlighted such flexibility by focusing on two performance yardsticks.

First, in the quasi-static setting, we have shown that the key-agreement DMT is equal to the DMT of a reduced MIMO main channel with no secrecy constraint. Furthermore, we have highlighted the fact that key DMT is the same whether CSI-T is available or not. Consequently, the public channel is not essential to obtain full key DMT, and coding for secret message transmission over the wiretap channel is sufficient. In the CSI-T case, although without any effect on the DMT, the public channel is shown to improve the outage performance.

Second, in the fast fading setting, we have studied the effect of transmit correlation on secret-key agreement capacity. We have shown that, as with MIMO systems without secrecy, transmitting Gaussian signals along the covariance channel eigenvectors is optimal. Our framework highlights two facts: transmit correlation helps in the low-power regime, but may induce a secret-key loss in the high-power regime.

The benefits of coding for secret-key agreement are achieved at a cost and require the availability of a two-way publicly authenticated public channel with high-capacity. However, we have provided a few examples showing how to exploit network features along with resources at the physical layer in order to create a reliable public communication.

ACKNOWLEDGMENT

This work has been supported by a grant from King Abdulaziz City of Science and Technology (KACST), Riyadh, Saudi Arabia.

REFERENCES


**Biographies**

**Zouheir Rezki** [S’01, M’08, SM’13] received the diplôme d’ingénieur degree from the École Nationale de l’Industrie Minérale (ENIM), Rabat, Morocco, in 1994, the M.Eng. degree from École de Technologie Supérieure, Montreal, Quebec, Canada, in 2003, and the Ph.D. degree from École Polytechnique, Montreal, Quebec, in 2008, all in electrical engineering. From 2008 to 2009, he was a post-doctoral research fellow with the Data Communications Group, Department of Electrical and Computer Engineering, University of British Columbia. He has been a senior research scientist with the King Abdullah University of Science and Technology, Saudi Arabia, since 2012. He joined the University of Idaho as a faculty member in 2016. His research interests include performance limits of communication systems, physical-layer security, optical communications, cognitive and sensor networks, and low-complexity detection algorithms.

**Marwen Zorgui** [S’13] received the Eng. degree in electronic and communication engineering from the Ecole Polytechnique de Tunisie, Tunisia, in 2013, and the M.S. degree in electrical engineering from King Abdullah University of Science and Technology, Thuwal, Makkah Province, Saudi Arabia, in 2015. He is now pursuing his Ph.D. at the University of California at Irvine, CA, USA. His research interests include physical layer security, performance limits of communication systems, and coding theory.

**Basel Alomari** [S’10, M’11] is an assistant professor and founding director of the National Center for Cybersecurity Technology (C4C) in King Abdulaziz City for Science and Technology (KAUST), an affiliate professor, and co-director of the Network Security Laboratory (NSL), University of Washington-Seattle, Seattle, WA, USA, an affiliate professor at King Saud University (KSU), and a cryptographic consultant at various companies. He was the recipient of the 2010 IEEE/IFIP William Carter Award from the IEEE Technical Committee on Fault-Tolerant Computing (TC-FTC) and the IFIP Working Group on Dependable Computing and Fault Tolerance (WG 10.4) for his significant contributions in the area of dependable computing. He was the recipient of the 2012 Distinguished Dissertation Award from the Center for Information Assurance and Cybersecurity, University of Washington (UW CIAC), and the 2015 Early Career Award in Cybersecurity by the NSA/DHS Center of Academic Excellence in Information Assurance Research for his contributions to Modern Cryptographic Systems and Visionary Leadership.

**Mohamed-Slim Alouini** [S’94, M’98, SM’03, F’09] received the Ph.D. degree in electrical engineering from the California Institute of Technology (Caltech), Pasadena, CA, USA, in 1998. He served as a faculty member at the University of Minnesota, Minneapolis, MN, USA, then at Texas A&M University at Qatar, Education City, Doha, Qatar, before joining King Abdullah University of Science and Technology (KAUST), Thuwal, Makkah Province, Saudi Arabia, as a professor of electrical engineering in 2009. His current research interests include the modeling, design, and performance analysis of wireless communication systems.