# Communication Model and Capacity Limits of Covert Channels Created by Software Activities

Baki Berkay Yilmaz, *Student Member, IEEE*, Nader Sehatbakhsh, Alenka Zajić, *Senior Member, IEEE* and Milos Prvulovic, *Senior Member, IEEE*

***Abstract*— It has been shown that digital and/or analog characteristics of electronic devices during executing programs can create a side-channel which an attacker can exploit to extract sensitive information such as cryptographic keys. When the attacker modifies the software application to exfiltrate sensitive information through a channel, this channel is called a *covert channel*. In this paper, we model this covert channel as a communication channel and derive upper and lower capacity bounds. Because the covert channels are not designed to transmit information, they are exposed not only to the errors created by the transmission, but also by varying the execution time of computer activities, and/or by insertions from other activities such as interrupts, stalls, etc. Combining all of these effects, we propose to model the covert channel as an insertion channel where the transmitted sequence is a pulse amplitude modulated signal with random pulse positions. Utilizing this model, we derive capacity bounds of the covert channel with random insertion and substitution due to the noise and jitter errors, and propose a receiver design that can correctly detect the computer-activity-created signals. To illustrate the severity of leakages, we perform experiments with high clock speed devices at some distance. Further, the theoretical derivations are compared to empirical results, and show good agreement.**

***Index Terms*— Covert/Side Channels Wireless Communications, Electromagnetic Information Leakage, Information Security.**

## I. Introduction

Electronic devices may leak information through unintentional side-channels which are the by-products of computing. These side-channels can be created by exploiting the existing shared resources inside a computer (e.g., cache, DRAM, TLBs, etc.) and often called micro-architectural/digital side-channels, or alternatively, can be caused by the physical implementation of the system (e.g., electromagnetic, power, sound, temperature, etc.), which are known as physical/analog side-channels. Exploiting these side-channels, attackers can design *spy* software to transmit *sensitive* data to the outside world. This type of communication is referred to as a covert channel [1] because legitimate software instructions or other activities in a computer system are used to wirelessly transmit secret messages.

This work has been supported, in part, by NSF grant 1563991 and DARPA LADS contract FA8650-16-C-7620. The views and findings in this paper are those of the authors and do not necessarily reflect the views of NSF and DARPA.

Baki Berkay Yilmaz and Alenka Zajić are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA. Milos Prvulovic and Nader Sehatbakhsh are with the School of Computer Science, Georgia Institute of Technology, Atlanta, GA, USA.

Covert channels can be used to communicate sensitive data between two processes inside a processor - typically a *privileged* process that has access to secret data but no/limited access to the outside world and a *non-privileged* process with no access to the data but connected to the outside world, or alternatively, they can be used to "exfiltrate" data from an air-gapped computer which is physically and logically separated from public networks [2], [3], [4]. In both cases, the secret data can be *secretly* transferred to the outside world through a *wireless channel* which, in turn, breaks the existing assumptions about the security of sensitive data inside a system.

Covert channels are considered as a serious security threat [5] since they can circumvent and break existing defense mechanisms (e.g., memory isolation, partitioning, etc.) for protecting secrets inside a computer. Fortunately, in most side-channel attacks, e.g., power analysis [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], temperature analysis [16], [17], caches-based [18], [19], [20], etc., the "listener" still requires some degree of direct access to the system (to attach probes, run a "receiver" process that measures cache activity, etc.), with some (often significant) risk of detection. However, covert channel attacks based on the system's electromagnetic (EM) emanations only require physical proximity, allowing sufficiently motivated attackers to carry out numerous attacks wirelessly and with little risk of detection [21], [22], [23], [24], [25], [26]. Previous work [2], [25] confirms that modulated EM emanations from different devices such as laptops, FPGAs, etc. can be created by executing seemingly innocuous code, and that thousands of bits per second can be transmitted through an EM covert channel. For example, imagine a company which stores sensitive data (e.g., design IPs, client data, etc.), on a server that is well-protected, both physically (e.g., by using guards, locks, etc.) and electronically (e.g., by using intrusion detection, firewall, etc.). However, exploiting covert channels, a rogue employee and/or a malware/worm can infiltrate the server and inject a trojan (i.e., a piece of software that can find sensitive information inside the computer, e.g., list of clients), and then "transmits" this data from the server through a side-channel (e.g., EM), hence establishing a covert channel to exfiltrate the data. Leveraging an EM-based covert channel, the attacker can then receive this transmitted information several meters away (e.g., up to 80m as we will show in this paper) using an antenna and a receiver setup, while having no detectable footprint.

The detection probability of covert channels increases as the communication time increases. Therefore, higher bit-rates

can cause higher information leakages without raising any suspicion. Hence, the severity of any covert channel can be measured in terms of how fast it can transmit information. In other words, the transmission rate indicates how much information can be *leaked* in a limited amount of time. Consequently, finding lower and upper bounds for leakage in a given covert channel is a necessary step in securing systems.

Millen was the first to establish a connection between Shannon's information theory and information flow models in computer systems [27] and calculated the capacity of such a covert channel. However, the proposed model assumes a synchronous channel which is not a realistic assumption for wireless communication created via covert channels in computers. Typically, wireless communication is a carefully designed process that encompasses the coordinated design of transmitter and receiver and usually, the transmitted and received signals are well-synchronized. In contrast, covert channels lack these characteristics. Moreover, contrary to most communication systems, which are designed to avoid symbol loss and/or insertion with little or no overhead, covert channels are not designed to transfer information at all and their transmission is often corrupted by insertion, deletion, and erroneous transfer of bits. While there is a large number of papers discussing bounds on the capacity of channels corrupted with synchronization errors [28], [29], [30], [31], [32] and more recently, papers discussing bounds on the capacity of channels corrupted with synchronization and substitution errors [33], [34], none of them provide bounds for the capacity of the wireless covert channel which can be modeled as a cascaded insertion-substitution channel that suffers from random pulse position shifts, and that insertions occur with different probabilities for zero and one. To the best of our knowledge, there is no work that connects wireless communication created by computer activity with modulation/demodulation theory, nor there are capacity bounds for such a channel.

In this paper, to accurately model EM-based covert channels on electronic devices, we first study a covert wireless communication model for EM emanations created by a computer activity and provide a background on how this channel can be created and how information can be sent and received. We then mathematically model this system and introduce leakage limits which utilize capacity bounds proposed in [34].

Similar to traditional wireless communications, some errors in the covert channel occur due to variations in the propagation environment. However, in addition to channel errors, the software activity "transmitter" lacks precise synchronization, causing jitter that reduces the signal's effective bandwidth *and* increases the noise level. Also, the "transmitter" gets interrupted with other (system) activities, and the transmitted signal may go through a channel obstructed by metal, plastic, etc. To capture all effects of the observed behavior, we have modeled the transmitted sequence as a pulse amplitude modulated (PAM) signal with randomly varying pulse positions. From the model, we have derived the power spectral density and the bit error rate (BER) of the transmitted signal with only substitution errors. Finally, we derive capacity bounds of the covert channel with random insertions and substitutions due to noise and jitter errors. Both the model and capacity limits are very useful tools for modeling and characterizing the properties of the covert channels.

The organization of the paper is as follows: Section II describes software-activity-created signals and the modulation mechanisms, Section III describes the transmission model for a covert channel caused by EM emanations of the processor, Section IV explains reception model and BER for two case studies, Section V derives lower and upper bounds of the covert channel capacity, Section VI presents the experimental results to validate the proposed framework, and Section VII concludes this paper.

## II. Wireless Transmission via Covert Channels

In this section, we first describe how carrier signals can be created by software activities and then, describe a method to generate modulated signals. To create a carrier, we use repetitive variations in a software activity as described in [25], [35], [36]. We choose $T$, the period (duration) of each repetition, two types of activities (A and B), and write a small software code (i.e., a microbenchmark) shown in Fig. 1 that in each period does activity A in the first half and B in the second half. The intuition behind this is that if activity A and activity B result in non-identical EM fields around the processor (or the system), repetition of this A-then-B pattern will create oscillations (with period $T$) in this EM field, i.e., it will result in a "carrier" RF signal at frequency $1/T$. The period $T$ will be selected to correspond to a specific frequency, e.g., to produce a radio signal at 1 MHz, we should set $T = 1\mu s$. This carrier-generation approach is illustrated in Fig. 2.

```
1  while(1){
2  // Do some instances of activity A
3    for(i=0;i<n_inst;i++){
4      ptr1=(ptr1&~mask1);
5      // Activity A, e.g. a load
6      value=*ptr1;
7    }
8  // Do some instances of activity B
9    for(i=0;i<n_inst;i++){
10     ptr2=(ptr2&~mask2);
11     // Activity B, e.g. a store
12     *ptr2=value;
13   }
14 }
```

Fig. 1. The A/B alternation pseudo-code [36].

Next, the symbols are *amplitude modulated* by inserting intervals during which only activity B is performed in both half-periods which means any carrier signal produced by the differences between A and B should be absent when only B is used, resulting in the simplest form of AM modulation (on-off keying). This approach is illustrated in Fig. 3. Note that other modulations (e.g., frequency modulation or even some non-standard modulation) can just as easily be used to create a truly covert transmission. Also note that the assumption here is that the code for generating this software modulation and creating a covert channel is already injected to the system through advanced-persistent threat scenarios [37], or manually entered/created on the target system by a trusted insider (e.g., a rogue employee). Moreover, the transmission code itself is not responsible to find the sensitive data, but it is only *a mean*

*of communication for sending the sensitive data from trusted inside to the outside world.* The sensitive information (to this transmitter code) is supplied by an injected/created malware in the system (e.g., a worm that infiltrated to the system and found some sensitive documents in the system). Note that both of these assumptions are realistic and commonly used in the existing literature.

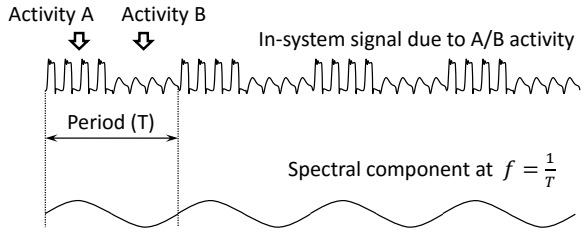



Fig. 2. Illustration of how microbenchmark induces emanations at a specific radio frequency by alternating half-periods of A and B activity.

Even an idle computer system produces RF signals that, after AM demodulation, result in clicking, whining, and other sounds (this can be confirmed by placing an AM radio receiver close to a computer). To confirm that the received communication sequence is indeed the transmitted message, we performed two experiments. First, we modulated our transmitted signal with the A5 note (880 Hz), and turned this tone on/off to transmit Morse code for "All your data belong to us" [25]. Second, we placed our microbenchmark code around the keyboard driver, which allowed us to transmit keystrokes wirelessly [38]. In both cases, we were able to correctly receive and demodulate transmitted signals.

However, we observed that the timing of the instructions was not perfectly synchronized. This issue confirmed that the baseband pulses generated with on-off keying do not have equal timing, and the created carrier is spread over several kilohertz in contrast to traditional communications where the carrier is well concentrated around a single frequency. This lack of synchronization in the transmitter causes significant jitter and has to be carefully modeled, as described in the following sections.

## III. Transmission Model for Software-Activity-Created Signals

In this section, we propose a model for covert channel communication systems. Before introducing the proposed model, we briefly review the baseband PAM signal and corresponding notations used in the rest of the paper.

The baseband PAM signal with a period of $\mathcal{T}$ can be written as [39]

$$x_p(t) = \sum_k x_k \delta(t - k\mathcal{T}) * p(t), \tag{1}$$

where $\delta(\bullet)$ is Dirac delta function, $*$ is the convolution operator, $\mathbf{x}_k = (x_k, x_{k-1}, x_{k-2}, \ldots)$ is the sequence of data symbols that are chosen from a finite alphabet, and $p(t)$ is a shaping pulse. The power spectral density (PSD) of $x_p(t)$ can be written as [39]

$$S_{xp}(f) = \frac{|P(f)|^2}{\mathcal{T}} S_x(f), \tag{2}$$

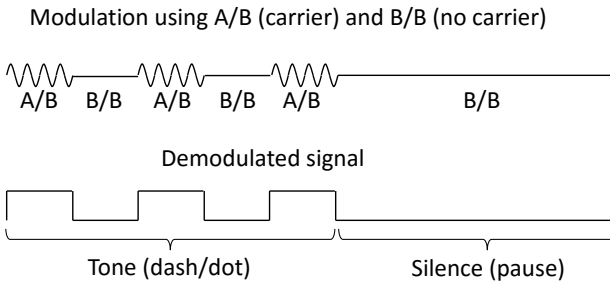



Fig. 3. Illustration of how microbenchmark modulates the signal into the carrier using on-off keying (bottom).

where $P(f)$ is the Fourier transform of the shaping pulse,

$$S_x(f) = \sum_{k=-\infty}^{\infty} R_x[k] e^{-j2\pi f k \mathcal{T}} \tag{3}$$

is PSD of the stationary sequence $\mathbf{x}_k$, and $R_x[k]$ is the autocorrelation function of sequence $\mathbf{x}_k$. Furthermore, if an impulse function is used as the shaping pulse, the power spectral density can be simply written as $S_{xp}(f) = S_x(f)/\mathcal{T}$.

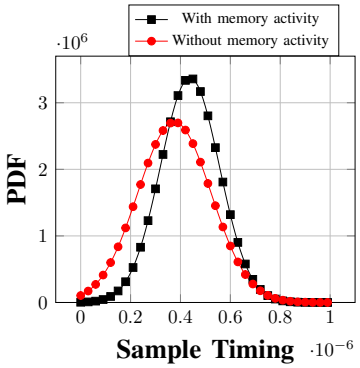



Fig. 4. Illustration of two timing distributions of symbols for an EM covert channel, one when memory activity is used and one with on-chip instructions is used.

The baseband signal shown in (1) assumes perfect symbol timing. However, the transmitted signals created by computer software activities are exposed to synchronization problems due to variations in symbol timing. As an example, Fig. 4 illustrates how the mean and the variance of the symbol timing vary with software activities when a covert channel is created based on emanated EM signals [25]. While the on-chip activities have a more concentrated distribution with a smaller variation, off-chip activities such as memory create more variations in symbol timing.

To deal with the pulse width variations and establish a connection using conventional communication theories, we assume the pulse width is fixed, but the center of the pulse changes due to the non-synchronous nature of the channel. Therefore, we propose to model the baseband signal as a pulse amplitude modulated (PAM) signal with a random pulse position. Then, the baseband received signal can be written as

$$y_p(t) = \sum_k x_k p(t - k\mathcal{T} - \mathbf{T_k}), \tag{4}$$

where $\mathbf{T}_k$ is a random shift associated with a particular pulse for the transmitted symbol, $x_k$, whose probability density function (pdf) is denoted by $f_{\mathbf{T}_k}(t_k)$. As illustrated in Fig.

3, the pulses are assumed to have a 50% duty cycle and the neighboring pulses do not overlap. Here, we need to note that although symbol timing varies as given in Fig. 4, our model contains a pulse function whose width is fixed and whose position is randomized. Also, the position of the pulse is chosen as the mid-point of the actual pulse width. This can be explained as follows: in traditional PAM modulation, pulse duty cycles are assumed to be fixed and do not vary. However, in a covert communication system, duty cycles generated by software activities can vary from one execution to another. Hence, to capture the variation in symbol timing in software activities and link the covert communication with the existing approaches, the transmitted signal is modeled as a PAM signal with a fixed pulse duty cycle.

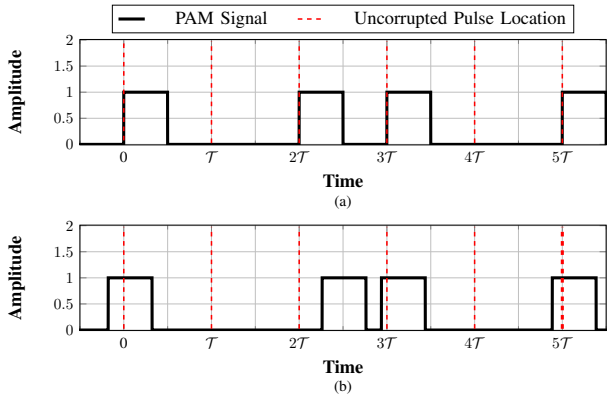



Fig. 5. (a) PAM with sequence $x_k$ and (b) distribution of pulses perturbed randomly in time and modulated in amplitude when the shaping pulse is a square wave.

To ensure that neighboring pulses do not overlap, the support set of $f_{\mathbf{T}_k}(t_k)$ is set to $\{t_k \in [-\mathcal{T}/4, \mathcal{T}/4)\}$. We also assume probability density functions, $\{f_{\mathbf{T}_k}(\bullet) \; | \forall k \in \{-\infty, \infty\}\}$, are identical and independent distributions (i.i.d.). As an example, Fig. 5 illustrates a typical PAM signal with 50% duty cycle and its randomly shifted version. We can observe that the time difference between neighboring pulses can increase or decrease, which mimics the variations in software activities and reflects the lack of synchronization.

To simplify (4) further, we will assume that $p(t)$ is an impulse function, $\delta(t)$, and the modulated baseband signal can be written as

$$y(t) = \sum_k x_k \delta(t - k\mathcal{T} - \mathbf{T_k}). \tag{5}$$

To evaluate the impact which the jitter introduces to the system due to the variation in symbol timing, we need to find PSD of baseband PAM signal with a random pulse position. The following theorem provides PSD of the signal with a random pulse position:

**Theorem 1.** *Let $\Phi(f)$ be the Fourier transform of $\phi(\tau)$ and*

$$\phi(\tau) = \int f_{\mathbf{T}}(\tau + t) f_{\mathbf{T}}(t) dt = f_{\mathbf{T}}(\tau) * f_{\mathbf{T}}(-\tau), \tag{6}$$

*where the subscript $k$ is removed to represent the random position distribution of the $k^{th}$ pulse since all distributions are assumed to be i.i.d. Then, PSD of the received signal, $y(t)$, in (5) can be written as*

$$S_y(f) = \frac{1}{\mathcal{T}} S_x(f)\Phi(f) + \frac{R_x[0]}{\mathcal{T}}(1 - \Phi(f)). \tag{7}$$

*Proof.* Please see Appendix I. □

Furthermore, for an arbitrary pulse shape, PSD of PAM signal with a random pulse position becomes

$$S_{y_p}(f) = \frac{|P(f)|^2}{\mathcal{T}} \left( S_x(f)\Phi(f) + R_x[0]\Big(1 - \Phi(f)\Big)\right). \tag{8}$$

This result shows that PAM with a random pulse position is equivalent to passing the PAM signal through a filter with power spectral density $\Phi(f)$, and having a jitter noise whose power is redistributed as a continuous wideband noise.

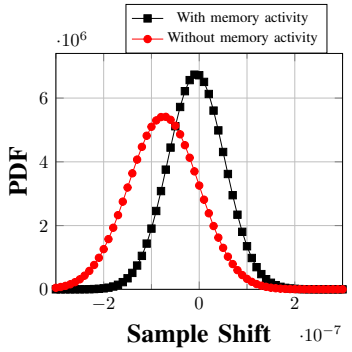



Fig. 6. Illustration of two distributions of pulse shift for an EM covert channel, one when memory activity is used and one with on-chip instructions is used.

The characteristics of the filter and the noise are completely determined by the probability distribution of the pulse positions. By fitting the measured samples of symbol duration into different probability distributions, we have found that the best fit for the pulse position variations is a Gaussian distribution with the mean $\mu$ and the standard deviation $\sigma$. Although fitting Gaussian distribution for the pulse positions contradicts our previous assumption that pulses can be only between $-\mathcal{T}/4$ and $\mathcal{T}/4$, we can still approximate the pulse positions with a Gaussian random distribution by assuming that the tail probability beyond $-\mathcal{T}/4$ and $\mathcal{T}/4$ is almost zero. Moreover, for the tractability of the derivations, we will assume that the means of these Gaussian distributions are equal. Fig. 6 plots the shift distributions of these pulse positions. We can observe that the pulse shift distributions are concentrated around zero. Therefore, (6) can be specified further for the memory and non-memory activities.

Given that Gaussian distribution has a Fourier transform

$$\mathfrak{F}\{f(t)\} = e^{-2\pi j f \mu} e^{-2\pi^2 \sigma^2 f^2}, \tag{9}$$

where $\mathfrak{F}\{\bullet\}$ takes Fourier transform of its argument and $f(t)$ is any Gaussian distribution with mean $\mu$ and standard deviation $\sigma$, we then combine (9) with (6) and obtain

$$\Phi(f) = e^{-2\pi^2 f^2 (\sqrt{2}\sigma)^2}. \tag{10}$$

Finally, inserting (10) into (7), we calculate PSD of PAM signal with Gaussian distributed pulse positions as

$$\begin{aligned} S_y(f) &= \frac{1}{\mathcal{T}} S_x(f) e^{-2\pi^2 f^2 (\sqrt{2}\sigma)^2} \\ &\quad + \frac{R_x(0)}{\mathcal{T}} \left(1 - e^{-2\pi^2 f^2 (\sqrt{2}\sigma)^2}\right) \\ &= S_{xt}(f) + S_{nt}(f), \end{aligned} \tag{11}$$

where $S_{xt}(f)$ denotes the spectrum of the transmitted sequence and $S_{nt}(f)$ denotes the noise spectrum due to random pulse position.

## IV. Quantifying the Information Leakage of Covert Channel Software-Activity-Created Signals

Traditionally, the performance of a communication system is evaluated by estimating symbol error rate or BER of the system. The error probability of pulse amplitude modulated signal (PAM) can be written as [39]

$$P_{PAM} = Q\left(\sqrt{\frac{P_s}{2P_n}}\right), \tag{12}$$

where $Q(\cdot)$ function denotes the tail probability of the standard normal distribution, $P_s$ is the averaged transmitted power of a symbol, and $P_n$ is the averaged noise power.

For the proposed scenario, BER represents the severity of the covert channel. Quantifying the information leakage in terms of BER reveals how fast we can transmit the information by establishing a reliable communication link using the computer systems. To estimate BER, we need PSD of the signal derived in (11). Then, we assume that the transmitted signal, $y(t)$, defined in (5) has been affected by the channel noise, and that received signal can be written as

$$r(t) = y(t) + n(t), \tag{13}$$

where $n(t)$ denotes the white Gaussian noise with zero mean and standard deviation, $\sigma_n$. We also assume that the noise and the transmitted sequence are independent. By observing that a communication system based on the covert channels described in Section II typically occurs at low frequencies ($\sim$ 1 MHz) where the multi-path effect does not play a significant role, it is reasonable to assume that the received signal is mostly impacted by noise and that inter-symbol interference (ISI) has almost negligible effect on the reliability of the covert communication. Here, we assume that the noise component contains both additive channel noise and all corruptive signals due to other activities in the system. Then, utilizing (11), the power spectral density of the received signal can be written as

$$S_r(f) = S_{xt}(f) + S_{nt}(f) + N_0/2, \tag{14}$$

where $N_0/2$ denotes the power spectral density of the additive white noise.

Obtaining PSD of the transmitted symbols facilitates the calculation of BER. To utilize (12), we need to know the signal and noise powers. Since our transmitted signal experiences jitter due to the variations in the symbol position, we start by calculating PSD of the jitter noise and the signal.

**Corollary.** *Considering the variation in the symbol position, PSD of the transmitted sequence for on-off keying (OOK) is given as*

$$\begin{aligned} S_y(f) &= \frac{R_x[0]}{\mathcal{T}} \left(\bar{S}_{xt}(f) + \bar{S}_{nt}(f)\right) \\ &= \frac{R_x[0]}{\mathcal{T}} \Bigg( \underbrace{\left(\frac{1}{2} + \frac{1}{2\mathcal{T}} \sum_m \delta(f - m/\mathcal{T})\right) \Phi(f)}_{\bar{S}_{xt}(f)} \\ &\quad + \underbrace{(1 - \Phi(f))}_{\bar{S}_{nt}(f)} \Bigg), \end{aligned} \tag{15}$$

*where $\bar{S}_{xt}(f)$ and $\bar{S}_{nt}(f)$ are the normalized signal and jitter noise powers.*

*Proof.* Please see Appendix I-A. □

Fig. 7 illustrates the behavior of the normalized signal and noise power when $\mathcal{T} \approx 15\sigma$.

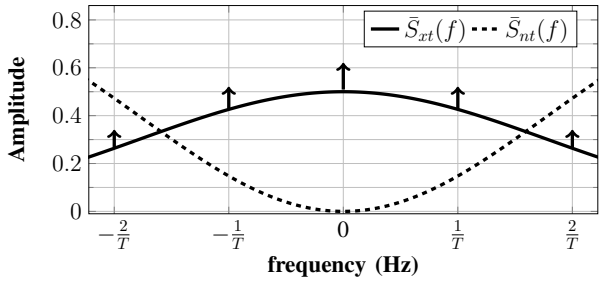



Fig. 7. PSD of normalized signal and jitter noise due to random pulse position when $\mathcal{T} \approx 15\sigma$.

Since the noise power due to jitter behaves like a white noise when $\Phi(f) \approx 0$, at the receiver front-end, we employ a low-pass filter whose bandwidth and magnitude are $1/2T$ and 1, respectively. The total signal power can be obtained as

$$\begin{aligned} P_{st} &= \frac{R_x[0]}{\mathcal{T}} \cdot \int_{-\frac{1}{2\mathcal{T}}}^{\frac{1}{2\mathcal{T}}} \bar{S}_{xt}(f) df \\ &= \frac{R_x[0]}{\mathcal{T}} \cdot \left(\frac{1}{2\mathcal{T}} + \frac{\sqrt{\pi}}{4\mathcal{T}} \mathrm{erf}\left(\pi\sigma/\mathcal{T}\right)/(\pi\sigma/\mathcal{T})\right), \end{aligned} \tag{16}$$

and total noise power due to jitter is equivalent to

$$\begin{aligned} P_{nt} &= \frac{R_x[0]}{\mathcal{T}} \cdot \int_{-\frac{1}{2\mathcal{T}}}^{\frac{1}{2\mathcal{T}}} \bar{S}_{nt}(f) df \\ &= \frac{R_x[0]}{\mathcal{T}} \cdot \left(\frac{1}{\mathcal{T}} - \frac{\sqrt{\pi}}{2\mathcal{T}} \mathrm{erf}\left(\pi\sigma/\mathcal{T}\right)/(\pi\sigma/\mathcal{T})\right), \end{aligned} \tag{17}$$

where erf($\bullet$) is the error function.

Having the power for both jitter noise and the received signal, we can estimate BER by using (12) assuming we have a channel without synchronization problems. However, this is not the case for a software-activity-based covert channels because synchronization can hurt the stealthy nature of these covert channels. Fortunately, after filtering the received signal at the receiver side, the jitter power becomes flat and behaves like an extra power source for the channel noise. Therefore, the receiver sees the channel noise with power $\hat{N}_0/2 =$

$N_0/2 + \mathcal{T}P_{nt}$. With that approximation, we can treat our communication system as a synchronized system with extra channel noise power. Hence, BER for the system can be approximated as

$$\text{BER} = Q\left(\sqrt{\frac{P_{xt}/\mathcal{T}}{\hat{N}_0}}\right). \tag{18}$$

The effect of varying jitter noise on BER is given in Fig. 8 where $\text{SNR}_i$ is defined as

$$\text{SNR}_i = R_x[0]/(N_0/2). \tag{19}$$

As the power of additive channel noise increases, the effect of the lack of synchronization on the erroneous transfer of bits becomes negligible. However, while the channel noise power decreases, the impact of jitter noise can be observed explicitly. In Section VI, we will demonstrate that assuming the jitter as an another source for the channel additive noise is a proper assumption to model the characteristics of BER of a covert channel.

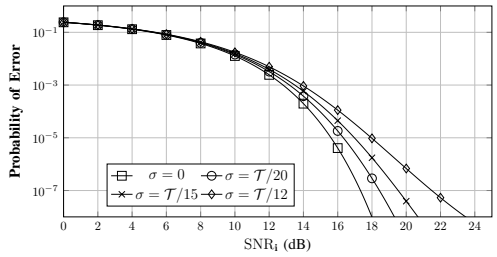



Fig. 8. BER for the covert wireless communication system with varying jitter noise power.

Finally, we investigate how the variation in the symbol position corrupts the transmitted sequence. The signal to jitter noise power ratio, $\text{SNR}_{jitter}$, at the transmitter side, due to random pulse positioning, can be written as

$$\text{SNR}_{jitter} = \frac{P_{st}}{P_{nt}} = \frac{\frac{1}{2} + \frac{\sqrt{\pi}}{4}\text{erf}\left(\pi\sigma/\mathcal{T}\right)/(\pi\sigma/\mathcal{T})}{1 - \frac{\sqrt{\pi}}{2}\text{erf}\left(\pi\sigma/\mathcal{T}\right)/(\pi\sigma/\mathcal{T})}. \tag{20}$$

Fig. 9 depicts how $\text{SNR}_{jitter}$ changes with respect to $\sigma/\mathcal{T}$. Since we assume $12\sigma \leq \mathcal{T}$, we limit $\sigma/\mathcal{T}$ to be between 0 and $1/12$ (due to the assumption that the distribution of the pulse shift has non-zero probability in the region $[-\mathcal{T}/4, \mathcal{T}/4)$ and considering three-sigma rule). As expected, as the variation in pulse position decreases, the distortion in the transmitted signal, due to jitter noise, decreases.

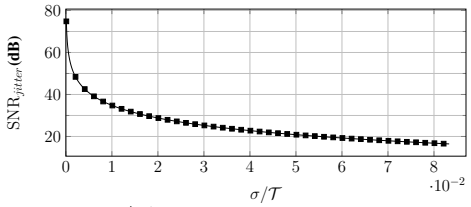



Fig. 9. $\text{SNR}_{jitter}$ vs. $\sigma/\mathcal{T}$.

## V. Capacity of the Covert Channel Created By a Computer Software Activity

The conventional method to assess the capacity of a communication system over Gaussian channels is to employ Shannon's capacity definition [39]. However, in addition to errors due to the Gaussian channel and pulse position, covert communication channels are exposed to insertion errors due to random software activities. We assume covert transmission occurs continuously, and the insertions are due to processor optimization, stalls, cache misses, queues, etc. These activities in a computer system can stall the covert channel communication and produce unintended signals. The receiver interprets these signals as ones or zeros, and these received bits are considered as the inserted symbols of the covert wireless communication. To model this covert channel, we assume binary discrete memoryless channel for the random insertions, as illustrated in Fig. 10. The channel parameters are $(p_{i0}, p_{i1}, p_e)$, where $p_{i0}$ denotes the probability that the random inserted symbol is 0, $p_{i1}$ denotes the probability that the random inserted symbol is 1, and $p_e$ denotes the probability of substitution error during transmission due to channel noise and jitter. To be able to calculate $p_e$, we follow the procedure given in Section IV, where we assume the jitter behaves like another power source for the additive channel noise. This model is a modified version of the channel model used by Davey and MacKay [29], where we additionally account for the fact that symbols for zero and one do not have equal probabilities of insertion, and the channel is noisy and jittery.

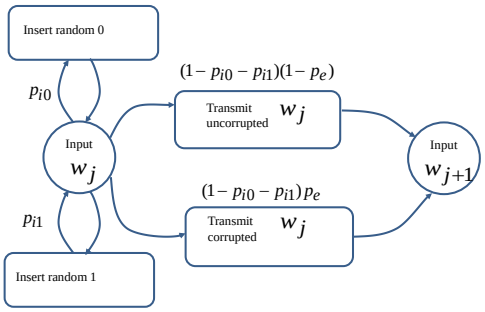



Fig. 10. Binary discrete memoryless noisy, jittery, synchronization channel.

With the model and the parameters defined above, the following theorem provides the upper and lower bounds of the covert channels which exhibit an OOK structure:

**Theorem 2.** *The covert channel capacity with probabilities* $(p_{i0}, p_{i1}, p_e)$ *and* $(p_{i0} + p_{i1}) < 0.5$ *is upper bounded by*

$$C \leq 1 - H_b(p_e), \tag{21}$$

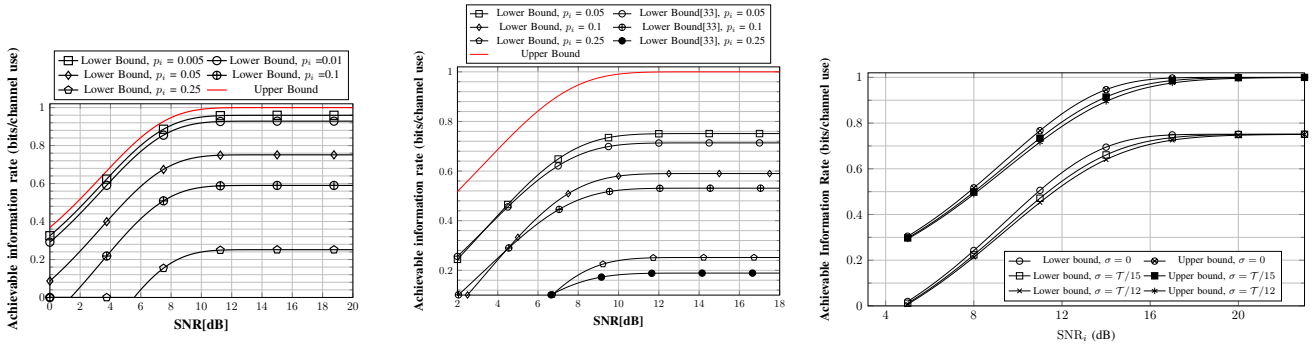
*and lower bounded by*

$$C \geq \max\left(0, \frac{1 - H_b(p_e) - H_b(p_{i0} + p_{i1})}{1 - p_{i0} - p_{i1}}\right), \tag{22}$$

*where* $H_b(\bullet)$ *is the entropy of a binary source.*

*Proof.* Please see Appendix II. □

Fig. 11(a) shows achievable information rates for the covert channel with various insertion probabilities. Here, we plot the upper bound derived in (21) and lower bound in (22) for several different insertion probabilities. We can observe that unless $p_{i0} = p_{i1} = p_i = 0$, the existence of insertions greatly limits the transmission capabilities, and reliable communication is not possible without channel coding even when SNR is high.




(a) (b) (c)

Fig. 11. a) Upper and lower bounds of information rates for deliberate side channel with several probabilities of insertion for a synchronized channel, b) Comparison of the lower bound of information rates for covert channel with no jitter and AWGN channel with insertions with the lower bound of information rate derived in [33], c) Upper and lower bounds of information rates of the covert channel with different jitter variances when $p_i = 0.05$.

Moreover, Fig. 11(b) compares the lower bound derived in (22) with a prior method [33] for several insertion probabilities. We observe that when the system is in the proper SNR regime for a reliable communication, the proposed lower bound is tighter than the one given in [33] for the capacity of a channel with insertion and substitution. We compare our results with work in [33] because it is the most similar channel scenario to the covert channels analyzed in this paper and their lower bound is shown to be tighter than all previously reported lower bounds for this type of a channel. We need to note that for Fig. 11(a) and Fig. 11(b), the jitter variance is set to zero for a fair comparison of the proposed bounds with the previous lower bound results because they are derived without considering the channels with jitter. However, assuming no jitter for a covert channel is not proper. Fig. 11(c) illustrates the relation between achievable information rates and jitter variance. Here, we assume the insertion probability is $p_i = 0.05$. We can observe that the achievable information rate increases with SNR and decreases with jitter variance. While the existence of jitter limits the transmission capabilities, with high enough SNR, reliable communication can be achieved.

## VI. Experimental Validation of the Proposed Model

In this section, we first demonstrate the existence of physical/analog covert channels generated by EM emanations, and then analyze this covert channel based on the proposed model, and also justify the assumption that the received signal is a PAM signal with insertions and substitutions for a variety of devices, i.e., FPGA, IoTs, laptops.

*1) Analysis of the Covert Channel:* To create a covert channel, we ran a microbenchmark (i.e., a *spy* application to transmit the sensitive data outside of the device) shown in Section II (also described in [35], [36]) on an Altera NIOS-II (soft) processor using a commercial Terassic DE1 SoC board [40]. This board is equipped with an Altera/Intel Cyclone-II FPGA chip and a variety of I/O protocols such as VGA, Serial, etc., and represents a popular class of embedded systems commonly used in the market. The application was written in standard C language and was compiled using the publicly available NIOS-II toolchain.

To receive the transmitted EM signals created by the *spy* application inside the system, we placed a magnetic probe, PBS-M [40], about 10 cm above the board so that it covers

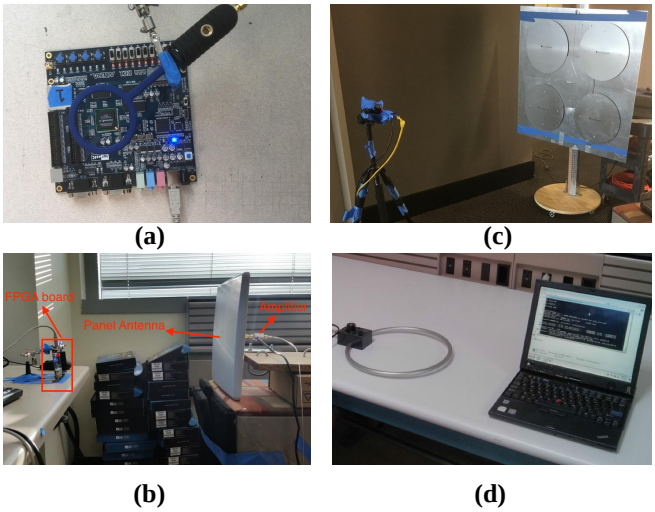



Fig. 12. The meausrement setup for devices: a) FPGA, b) FPGA, c) OLinuXino, d) Laptops with distance.

the processor area as shown in Fig. 12(a). We intentionally put the probe very close to the board to receive the EM signal with the highest achievable SNR to avoid the limitations due to low SNR. In the later sections, we will show how this covert channel performs under more realistic scenarios where the receiver is placed several meters away from the device.

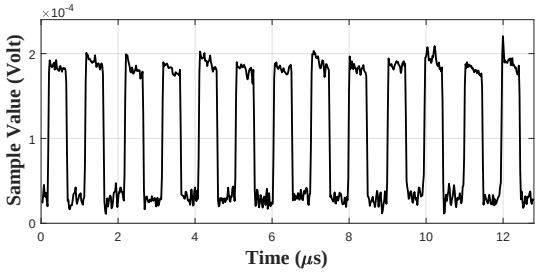



Fig. 13. The received baseband signal with period $\mathcal{T} = 1\mu s$.

The EM signals were recorded using a spectrum analyzer (Agilent MXA N9020A). We set the sampling rate to 10 MHz, and set the spectrum analyzer's center frequency to 50 MHz (i.e., the clock frequency of the FPGA chip), and the span to 4 MHz (i.e., 2 MHz for each side-band) since the designed microbenchmark creates periodic activities (i.e., A/B or A/A alternations) at 1 MHz so the device can pick up spikes from this periodic activity and its multiple harmonics.

The received signal is shown in Fig. 13 when the activity A and activity B of the microbenchmark are chosen as a load from main memory and load from an L1 cache, respectively. We can observe that the received signal has a shape of a PAM signal whose pulse width fluctuates due to uncertainties in the execution times of computer-software activities.

TABLE I

COMPARISON OF EXPERIMENTAL AND THEORETICAL RESULTS IN TERMS OF BER FOR NIOS PROCESSOR ON THE DE1 FPGA BOARD.

| | SNR (dB) | Experimental BER | Theoretical BER |
|---|---|---|---|
| 1 | 6 | 0.096 | 0.0829 |
| 2 | 13 | 0.0013 | 0.0016 |
| 3 | 14 | 0.0008 | 0.0009 |
| 4 | 24 | 0 | 0 |

To compare the theoretical results with the experimental results, we perform experiments with different activities and bandwidth. The estimated SNRs and the corresponding experimental and theoretical results are given in Table I. The activities and the corresponding bandwidth used for the experiments can be listed as follows: 1) Addition-Multiplication with 4 MHz bandwidth, 2) Addition-Multiplication with 2 MHz bandwidth, 3) Load from Main Memory-Load from L1 cache with 4 MHz bandwidth, and 4) Load from Main Memory-Load from L1 cache with 2 MHz bandwidth. The sampling frequency for all these experiments is 10 MHz. We need to note that we only provide these results because we do not control SNR of the communication, therefore, generation of a plot with various SNR values is hard and unreliable. These results illustrate that proposed model is a realistic model for covert channels and can be used as a simulation tool.

The second example illustrates the presence of jitter and why our assumption that the jitter power can be added as an extra power source of white noise to calculate the BER, i.e., why assumption in (18) is valid. The following discussion considers the jitter distributions given in Fig 6. First, we plot PSD of the information signal and jitter noise. Here, we study the scenario without memory activity and the baseband transmitted pulses are sent with period $\mathcal{T} = 1\ \mu s$. The standard deviation of the jitter noise is calculated as $\sigma = 5.91 \times 10^{-8}$. The theoretical PSD of the transmitted signal and the jitter noise are given in Fig. 14(a), and PSD of the filtered signal at the receiver side is given in Fig. 14(b). We observe that the jitter noise power dominates the transmitted signal for higher frequencies. Filtering the received signal removes this redundancy and helps to retrieve the information signal.

As the final step, to verify BER estimation given in (18) based on PSD of the transmitted signal and jitter noise, we design the following experiment: We create an impulse train with period $\mathcal{T}$ and apply jitter noise by altering the location of pulses based on the normal distribution with variance $\sigma^2$. Then, we disturb the signal further by adding white noise, whose distribution can be given as $\mathcal{N}(0, N_0/2)$. The received signal is filtered with an ideal low pass filter on the receiver side and sampled with frequency $1/\mathcal{T}$. Finally, the sampled outputs are thresholded to estimate the transmitted inputs. The

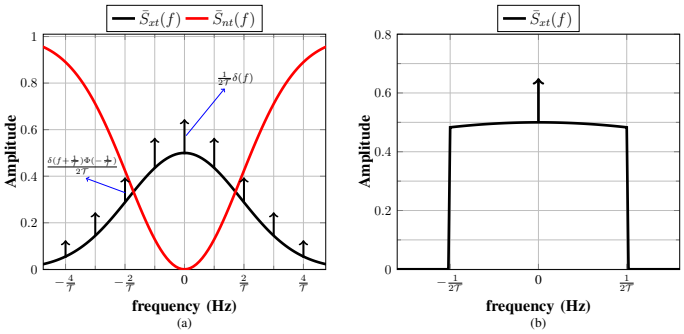



Fig. 14. PSD of a) the transmitted signal and b) its filtered version at the receiver side for the symbol without memory activity.

results are shown in Fig. 15. Here, we plot the simulation and theoretical BER results for the cases with and without memory activity. The results assert that simulated results agree with theoretically derived BER and verify the intuition that as the jitter variance increases, BER also increases.

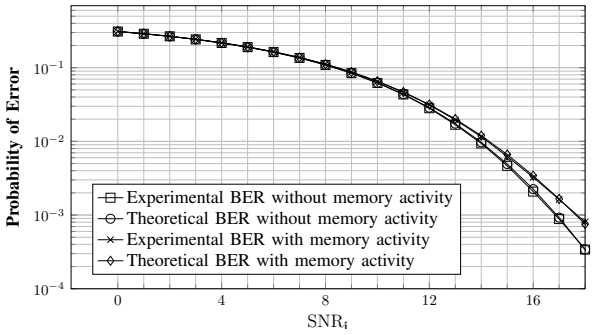



Fig. 15. Theoretical and experimental BER for the symbols with and without memory activity.

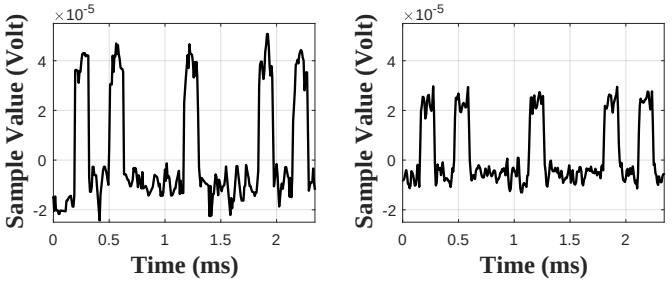
Please note that not only PAM, but also frequency shift keying (FSK) modulation scheme can be generated with the microbenchmark. However, the detection of FSK signals can be harder since the variations in execution time of the microbenchmark will cause scrambling of different frequencies and increase in BER. Therefore, more sophisticated receiver designs and more complex mathematical derivations are needed to achieve the same performance levels with the PAM case.

*2) Demonstration of the Analog Covert Channel on More Complex Systems:* In this section, we provide examples to show the practicality of the EM covert channel on more complex devices and more realistic distances.

We first study the impact of distance (i.e., the position of the probe/antenna and the receiving signal's SNR) on the bit-error-rate (BER). To measure the EM signals, we used a panel antenna [41]. We set the spectrum analyzer's center frequency to 2.3 GHz (i.e., the 46th harmonic of the FPGA's clock frequency, 50 MHz). This frequency is chosen to maximize the antenna's gain. We placed the board 50 cm and 1 m away from the board. The setup is shown in Fig. 12(b).

Fig. 16 shows the signal received from these distances. Please note that received signals preserve the square-wave-structure like the signals in Fig. 13. These experiments confirm that the proposed EM covert channel is not sensitive to the position of the probe, and can be exploited from longer

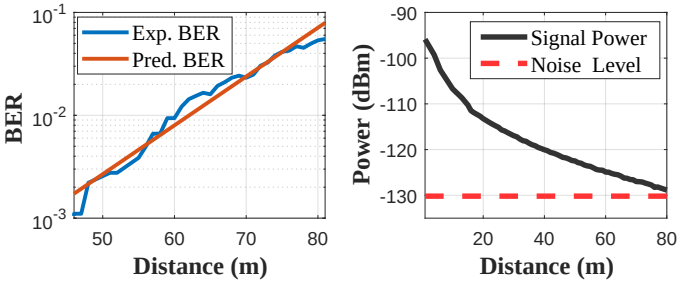
distances.




(a) (b)

Fig. 16. The received signal at distance of a) 50 cm, b) 1 m.

To further study the possible range of an EM covert-channel attack and investigate its possibility on other (more complex) types of devices, we perform another experiment, this time using an embedded single-board computer called OlinuXino [42]. This board is equipped with a modern Cortex A8 ARM core with two levels of caches, 4 MB main memory, and runs a Debian Linux operating system. OlinuXino represents a popular class of single-board computers widely used in the market to control a variety of critical and commercial tasks in factory lines, hospitals, etc.




(a) (b)

Fig. 17. a) BER vs. distance, b) The received signal power vs. distance where the noise level of the instrument sensitivity level is about -130dBm.

To receive the EM signals, we leveraged two different antennas: a commercially available horn antenna [43], and a high-gain custom-made disk-array based antenna [44]. Similar to the FPGA, we use our microbenchmark (written in C and compiled with Gnu-gcc tool) to establish the covert channel. We use the same spectrum analyzer for recording the signals with a center frequency set to 1 GHz (i.e., the clock frequency of the ARM core), and span of 5 MHz, while setting the microbenchmark to generate alternations at 2 MHz. Please note that Fig. 12(c) shows our measurement setup and demonstrates that communication is conducted in a realistic indoor environment.

The results for BER and the signal power are given in Fig. 17. In Fig. 17(a), we plot the BER of measurements when the distance is more than 45 m. For closer distances, the success rate of the measurements is almost 100% (i.e., BER $< 10^{-3}$). As can be seen from this figure, the success rate (BER) linearly decreases as the distance increases (as shown by the fitted line). From the results we note that covert channel can achieve more than 99.9% of success rate if the distance is less than 45 m and the signal level is at least 8 dB above the noise level of the measuring device (i.e., -130 dBm in this experiment).

Finally, to show that this EM covert channel can be created for complex computing systems such as laptops, we performed experiments on four different laptops with different processors, namely: AMD Turion X2 Ultra, Intel Core Duo T2600, Intel I7 2620M, and Intel Core 2 Extreme X9650.

In all these measurements, we use the same experimental setup given in [45] which utilizes a magnetic loop antenna with a radius of 30 cm [46] as shown in Fig. 12(d). The center frequency for the measurements is set to 1.024 MHz. The results are shown in Table II. In this table, we provide the maximum distances that we achieve a reliable communication (i.e., BER $\approx 10^{-3}$) when the transmission rate for the covert channel is 800 bits per second (bps). We observed that the signal power leaked from different platforms shows variation (depending on the packaging, board, etc.), and that affects the range of the covert channel. Compared to the state-of-the-art [3], [4], [47], our studied covert channel provides up to 5x higher data-rate and 5x lower bit-error-rate.

TABLE II

EXPERIMENTAL RESULTS FOR COMPUTER SYSTEMS WITH DISTANCE.

| Platform | CPU | Distance | BER |
|---|---|---|---|
| AMD Turion | 2.1 GHz | 2.5 m | $10^{-3}$ |
| Intel Core DUO | 2.16 GHz | 0.81 m | $10^{-3}$ |
| Intel i7 | 2.7 GHz | 1.75 m | $10^{-3}$ |
| Intel Core 2 | 3 GHz | 1.17 m | $10^{-3}$ |

## VII. CONCLUSIONS

A covert channel generated by program activities in a computer system is described and modeled. These covert channels experience jitter errors in addition to channel errors due to noise. This is a result of the computer activity "transmitter" which lacks precise synchronization. Also, the "transmitter" gets interrupted by other (system) activities, and the transmitted signal goes through a channel obstructed by metal, plastic, etc. To capture all these effects, we have modeled the transmitted sequence as a pulse amplitude modulated (PAM) signal with random varying pulse position. From the model, we have derived the power spectral density and the bit error rate of the transmitted signal with insertion and substitution errors. We have also derived capacity bounds of these covert channels with insertion and substitution errors due to interrupts, noise, and jitter. The theoretical derivations are compared to empirical results and show good agreements.

## APPENDIX I
## PSD OF PAM SIGNAL WITH RANDOM PULSE POSITION

The PAM signal with random pulse position $y(t)$ is given by $y(t) = \sum_k x_k \delta(t - k\mathcal{T} - \mathbf{T}_k)$. $y(t)$ is an impulse train whose amplitude is modulated by the sequence $x_k$ and the impulse positions are randomly shifted by $\mathbf{T}_k$. Furthermore, the autocorrelation function and the power spectral density of $x_k$ are denoted as $R_x[k]$ and $S_x(f) = \sum_k R_x[k] e^{-j2\pi f k\mathcal{T}}$,

respectively. Here, we note that the signals $x_p(t)$ and $y(t)$ in (1) and (5) are cyclostationary random processes if the amplitude modulating sequence $x_k$ and the random pulse position variation $\mathbf{T}_k$ are stationary [48]. For a cyclostationary random processes of period $\mathcal{T}$, the average autocorrelation function between 0 and $\mathcal{T}$ can be computed as [49]

$$R_y(\tau) = \frac{1}{\mathcal{T}} \int_0^{\mathcal{T}} R_y(t,\tau) dt, \tag{23}$$

where $R_y(t,\tau) = \mathrm{E}\Big[y(t), y(t-\tau)\Big]$ and $\mathrm{E}[\cdot]$ denotes the expectation. Here, $R_y(t,\tau)$ can be written as

$$\mathrm{E}\Big[\sum_i \sum_j x_i x_j \delta(t - i\mathcal{T} - \mathbf{T}_i)\delta(t-\tau - j\mathcal{T} - \mathbf{T}_j)\Big]. \tag{24}$$

It can be shown that $R_y(t,\tau)$ is also periodic in time with a period $\mathcal{T}$. Therefore, $y(t)$ is a cyclostationary random process. Using (23), we can rewrite the correlation function $R_y(\tau)$ as

$$\begin{aligned}
&= \frac{\int_0^{\mathcal{T}} \mathrm{E}\Big[\sum_{i,j} x_i x_j \delta(t - i\mathcal{T} - \mathbf{T}_i)\delta(t-\tau - j\mathcal{T} - \mathbf{T}_j)\Big] dt}{\mathcal{T}} \\
&= \frac{\sum_{i,j} \int_0^{\mathcal{T}} \mathrm{E}\Big[x_i x_j \delta(t - i\mathcal{T} - \mathbf{T}_i)\delta(t-\tau - j\mathcal{T} - \mathbf{T}_j)\Big] dt}{\mathcal{T}} \\
&= \frac{\sum_{i,j} \int_0^{\mathcal{T}} \mathrm{E}\big[x_i x_j\big] \mathrm{E}\Big[\delta(t - i\mathcal{T} - \mathbf{T}_i)\delta(t-\tau - j\mathcal{T} - \mathbf{T}_j)\Big] dt}{\mathcal{T}}
\end{aligned} \tag{25}$$

where (25) follows the assumption that $x_k$ and $\mathbf{T}_k$ are independent. Let $\lambda = t - i\mathcal{T}$. So, (25) can be written as

$$\frac{\sum_{i,j} \int_{-i\mathcal{T}}^{-(i-1)\mathcal{T}} \mathrm{E}\big[x_i x_j\big] \mathrm{E}\Big[\delta(\lambda - \mathbf{T}_i)\delta(\lambda-\tau - (j-i)\mathcal{T} - \mathbf{T}_j)\Big] d\lambda}{\mathcal{T}}.$$

Letting $j - i = m$, we can rewrite the correlation function as follows:

$$\begin{aligned}
R_y(\tau) = \frac{1}{\mathcal{T}} \sum_m \sum_i \int_{-i\mathcal{T}}^{-(i-1)\mathcal{T}} \Bigg( &\mathrm{E}\big[x_i x_{i+m}\big] \times \\
&\mathrm{E}\Big[\delta(\lambda - \mathbf{T}_i)\delta(\lambda - \tau - m\mathcal{T} - \mathbf{T}_{m+i})\Big]\Bigg) d\lambda.
\end{aligned} \tag{26}$$

Since $x_k$ is a stationary sequence, we can deduce $\mathrm{E}[x_i x_j] = R_x[i-j]$. Exploiting that $\{\mathbf{T}_k,\ \forall k \in (-\infty, \infty)\}$ are statistically identical and independent of each other, we can rewrite (26) as

$$\begin{aligned}
&\frac{1}{\mathcal{T}} \sum_{m,i} \int_{-i\mathcal{T}}^{-(i-1)\mathcal{T}} R_x[m] \mathrm{E}\Big[\delta(\lambda - \mathbf{T}_0)\delta(\lambda - \tau - m\mathcal{T} - \mathbf{T}_m)\Big] d\lambda \\
&= \frac{\sum_m R_x[m] \int_{-\infty}^{\infty} \mathrm{E}\Big[\delta(\lambda - \mathbf{T}_0)\delta(\lambda - \tau - m\mathcal{T} - \mathbf{T}_m)\Big] d\lambda}{\mathcal{T}}.
\end{aligned}$$

Taking the integration inside the expectation operator, $R_y(\tau)$ simplifies to

$$\begin{aligned}
&\frac{1}{\mathcal{T}} \sum_m R_x[m] \mathrm{E}\Big[\int_{-\infty}^{\infty} \delta(\lambda - \mathbf{T}_0)\delta(\lambda - \tau - m\mathcal{T} - \mathbf{T}_m) d\lambda\Big] \\
&= \frac{1}{\mathcal{T}} \sum_m R_x[m] \mathrm{E}\Big[\delta(-\tau - m\mathcal{T} + \mathbf{T}_0 - \mathbf{T}_m)\Big].
\end{aligned} \tag{27}$$

Considering that the pulse positions $\mathbf{T}_k$ are independent and identically distributed (i.i.d.), the autocorrelation function $R_y(\tau)$ can be calculated as

$$\begin{aligned}
&\frac{\mathrm{E}\Big[R_x[0]\delta(\tau)\Big] + \sum_{m\neq 0} R_x(m) \mathrm{E}\Big[\delta(-\tau - m\mathcal{T} + \mathbf{T}_0 - \mathbf{T}_m)\Big]}{\mathcal{T}} \\
&= \frac{R_x(0)\delta(\tau) + \sum_{m\neq 0} R_x(m) \mathrm{E}\big[\delta(-\tau - m\mathcal{T} + \mathbf{T}_0 - \mathbf{T}_m)\big]}{\mathcal{T}}.
\end{aligned} \tag{28}$$

To proceed further, let us introduce $z_m(\tau) = \mathrm{E}\big[\delta(-\tau - m\mathcal{T} + \mathbf{T}_0 - \mathbf{T}_m)\big]$. Therefore,

$$\begin{aligned}
z_m(\tau) &= \iint_{-\mathcal{T}/4+\mu}^{\mathcal{T}/4+\mu} \delta(-\tau - m\mathcal{T} + t_0 - t_m) f_{\mathbf{T}_0}(t_0) f_{\mathbf{T}_m}(t_m) dt_0 dt_m \\
&= \int_{-\mathcal{T}/4+\mu}^{\mathcal{T}/4+\mu} f_{\mathbf{T}_0}(\tau + m\mathcal{T} + t_m) f_{\mathbf{T}_m}(t_m) dt_m \\
&\overset{(a)}{=} \int_{-\mathcal{T}/4+\mu}^{\mathcal{T}/4+\mu} f_{\mathbf{T}}(\tau + m\mathcal{T} + t_m) f_{\mathbf{T}}(t_m) dt_m \\
&\overset{(b)}{\approx} \int_{-\infty}^{\infty} f_{\mathbf{T}}(\tau + m\mathcal{T} + t_m) f_{\mathbf{T}}(t_m) dt_m \\
&= f_{\mathbf{T}}(-\tau + m\mathcal{T}) * f_{\mathbf{T}}(\tau) \\
&= \delta(\tau - m\mathcal{T}) * f_{\mathbf{T}}(-\tau) * f_{\mathbf{T}}(\tau) \\
&= \delta(\tau - m\mathcal{T}) * \phi(\tau)
\end{aligned} \tag{29}$$

where (a) follows all distributions $\{\mathbf{T}_i | \forall i \in \{-\infty, \infty\}\}$ are i.i.d., (b) is due to support set assumption of distribution functions and $*$ denotes convolution. Plugging (29) into (28), we can write $R_y(\tau)$ as

$$\begin{aligned}
&\frac{R_x(0)\delta(\tau) + \sum_{m=0} R_x(m) \left(\delta(\tau - m\mathcal{T}) * \phi(\tau)\right) - R_x(0)\phi(\tau)}{\mathcal{T}} \\
&= \frac{\Big(\sum_m R_x(m)\delta(\tau - m\mathcal{T})\Big) * \phi(\tau) + R_x(0)\Big(\delta(\tau) - \phi(\tau)\Big)}{\mathcal{T}}.
\end{aligned} \tag{30}$$

The PSD $S_y(f)$ of the signal $y_p(t)$ is obtained by taking the Fourier transform of the above result. Using these results, we can write the spectrum of PAM signal with random pulse position as

$$S_y(f) = \frac{1}{\mathcal{T}} S_x(f)\Phi(f) + \frac{R_x(0)}{\mathcal{T}}(1 - \Phi(f)), \tag{31}$$

where $\Phi(f)$ is the Fourier transform of $\phi(\tau)$.

### A. PSD of "on-off" Keying (OOK) With Random Pulse Position

The power spectrum of the PAM with random pulse position has already been derived in (11). In this section, we specify the equation in (11) for OOK modulation case. As the first step, we need to calculate $S_x(f)$ to investigate the effect of random pulse position on the spectral power of the signal. We assume the amplitude of a symbol is $\mathcal{A}$ when the symbol is "on" and 0 otherwise. Therefore, autocorrelation of these symbols can be written as

$$R_x[m] = \begin{cases} \mathcal{A}^2/2 & \text{if } m=0, \\ \mathcal{A}^2/4 & \text{otherwise.} \end{cases} = \begin{cases} R_x[0] & \text{if } m=0, \\ R_x[0]/2 & \text{otherwise.} \end{cases}$$

If we convert this discrete signal into continuous signal with period $\mathcal{T}$, we have

$$R_x(\tau) = \sum_m R_x[m]\delta(\tau - m\mathcal{T}). \tag{32}$$

To obtain the power spectral density of the signal, Fourier transform of $R_x(\tau)$ can be calculated as follows:

$$\begin{aligned} S_x(f) &= \int_{-\infty}^{\infty} \sum_m R_x[m]\delta(\tau - m\mathcal{T}) e^{-j2\pi f\tau} d\tau \\ &= \sum_m R_x[m] e^{-j2\pi f m\mathcal{T}} \\ &= \frac{R_x[0]}{2} + \frac{R_x[0]}{2} \sum_m e^{-j2\pi f m\mathcal{T}} \\ &= \frac{R_x[0]}{2}\left(1 + \frac{1}{\mathcal{T}}\sum_m \delta(f - m/\mathcal{T})\right) \end{aligned} \tag{33}$$

If we insert (33) into (5), the power spectrum $S_y(f)$ can be written as

$$\begin{aligned} &\frac{R_x[0]}{2\mathcal{T}}\left(1 + \frac{\sum_m \delta(f-n/\mathcal{T})}{\mathcal{T}}\right)\Phi(f) + \frac{R_x(0)}{\mathcal{T}}(1-\Phi(f)) \\ &= \frac{R_x[0]}{\mathcal{T}}\left(\underbrace{\left(\frac{1}{2} + \frac{\sum_m \delta(f-m/\mathcal{T})}{2\mathcal{T}}\right)\Phi(f)}_{\bar{S}_{xt}(f)} + \underbrace{(1-\Phi(f))}_{\bar{S}_{nt}(f)}\right). \end{aligned} \tag{34}$$

Here, we need to note that since we assume that the random shift position is in the interval $\left(-\frac{\mathcal{T}}{4}, \frac{\mathcal{T}}{4}\right]$ that has a Gaussian distribution, we consider $\mathcal{T} \gtrsim 12\sigma$ to ensure our interval assumption holds with very high probability.

## Appendix II
## Covert-Channel Capacity Derivations

In this section, we provide the derivations for channel capacity bounds of the covert channel communications. In [50], it is shown that the capacity of a discrete memoryless synchronization channel exists and is given by

$$C = \sup_{\Xi} \lim_{n\to\infty} \frac{1}{n} \cdot I(W^n; Y^{\bar{N}n}), \tag{35}$$

where the supremum is taken over all stationary Markov chains $\Xi$ models of the input source, $n$ is the number of input bits, $W^n$ and $Y^{\bar{N}n}$ represent the input and observed sequence respectively. Here, $\bar{N}$ is the average number of received symbols per transmitted symbol. The number of insertions between consecutive input symbols are geometrically distributed and the average number of insertions per input symbol is

$$\begin{aligned} &(p_{i0}+p_{i1})(1-p_{i0}-p_{i1}) + 2(p_{i0}+p_{i1})^2(1-p_{i0}-p_{i1}) \\ &\qquad +3(p_{i0}+p_{i1})^3(1-p_{i0}-p_{i1}) + \dots \\ &= \frac{p_{i0}+p_{i1}}{1-p_{i0}-p_{i1}}. \end{aligned} \tag{36}$$

Hence, the average number of output symbols per input symbols is

$$\bar{N} = \frac{1}{1-p_{i0}-p_{i1}}. \tag{37}$$

In [34], [33], it is shown that channels with insertions and substitutions can be decomposed into a cascade of two channels, channel with insertions and channel with substitutions as shown in Fig. 18. Since both inputs and outputs of the covert channel are assumed to be equiprobable, it follows that

$$H(W^n) = n, \text{ and } H\left(X^{n/(1-p_i)}\right) = \frac{n}{1-p_i}, \tag{38}$$

where $n$ is the number of input bits, $p_i = p_{i0} + p_{i1}$, and $H(\cdot)$ denotes the entropy. From (35), it follows that we need to calculate mutual information $I\left(W^n, Y^{\frac{n}{1-p_i}}\right)$ between the input sequence and output of the second cascaded channel. This mutual information can be written as

$$\begin{aligned} I\left(W^n, Y^{\frac{n}{1-p_i}}\right) &= I\left(X^{\frac{n}{1-p_i}}, Y^{\frac{n}{1-p_i}}\right) \\ &\quad - I\left(X^{\frac{n}{1-p_i}}, Y^{\frac{n}{1-p_i}} | W^n\right). \end{aligned} \tag{39}$$

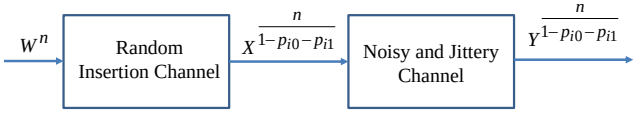



Fig. 18. Cascaded channels equivalent to the binary discrete memoryless noisy, jittery, synchronization channel with $n$ input symbols.

To find a lower bound for $I\left(W^n, Y^{\frac{n}{1-p_i}}\right)$, we are required to obtain an upper bound for $I\left(X^{\frac{n}{1-p_i}}, Y^{\frac{n}{1-p_i}} | W^n\right)$. Therefore,

$$\begin{aligned} 0 &\le I\left(X^{\frac{n}{1-p_i}}, Y^{\frac{n}{1-p_i}} | W^n,\right) \\ &= H\left(X^{\frac{n}{1-p_i}} | W^n\right) - H\left(X^{\frac{n}{1-p_i}} | W^n, Y^{\frac{n}{1-p_i}}\right) \\ &= H\left(X^{\frac{n}{1-p_i}}\right) - I\left(W^n, X^{\frac{n}{1-p_i}}\right) \\ &\quad - H\left(X^{\frac{n}{1-p_i}} | W^n, Y^{\frac{n}{1-p_i}}\right) \\ &\le H\left(X^{\frac{n}{1-p_i}}\right) - I\left(W^n, X^{\frac{n}{1-p_i}}\right). \end{aligned} \tag{40}$$

Combining (35), (39) and (40), $C$ can be written as

$$\begin{aligned}
&\sup_{\Xi} \lim_{n\to\infty} \frac{1}{n} \cdot I(W^n; Y^{\bar{N}n}) \\
=&\sup_{\Xi} \lim_{n\to\infty} \frac{1}{n} \Bigg( I\left(X^{\frac{n}{1-p_i}}, Y^{\frac{n}{1-p_i}}\right) \\
&\qquad -I\left(X^{\frac{n}{1-p_i}}, Y^{\frac{n}{1-p_i}} | W^n\right) \Bigg) \\
\geq&\sup_{\Xi} \lim_{n\to\infty} \frac{1}{n} \Bigg( I\left(X^{\frac{n}{1-p_i}}, Y^{\frac{n}{1-p_i}}\right) - H\left(X^{\frac{n}{1-p_i}}\right) \\
&\qquad +I\left(W^n, X^{\frac{n}{1-p_i}}\right) \Bigg) \qquad (41) \\
=&\sup_{\Xi} \lim_{n\to\infty} \frac{1}{n} \left( n\frac{I(X,Y)}{1-p_i} - \frac{n}{1-p_i} + I\left(X^{\frac{n}{1-p_i}}, W^n\right)\right) \\
=&\frac{I(X,Y)}{1-p_i} - \frac{1}{1-p_i} + \sup_{\Xi} \lim_{n\to\infty} \frac{1}{n} \left( I\left(X^{\frac{n}{1-p_i}}, W^n\right)\right) \\
=&\frac{I(X,Y)}{1-p_i} - \frac{1}{1-p_i} + C^i(p_i) \qquad (42)
\end{aligned}$$

where $C^i(p_i)$ is the channel capacity of insertion channel with insertion probability $p_i$ and (41) follows the assumption that the noisy substitution channel is a discrete memoryless channel (DMC). To obtain a lower bound for the insertion channel, we exploit the relation between deletion and insertion channels, and previous results for the capacity lower bound of deletion channels. In [34], the relation between deletion and insertion channels is given as

$$C^d(pi) = (1-p_i)C^i(p_i) \qquad (43)$$

where $C^d(p_i)$ is the information rate of a deletion channel with equiprobable iid inputs whose deletion probability equals to insertion probability of the insertion channel. Morover, in [51], the capacity lower bound for the deletion channel is given as

$$C^d(p_i) \geq 1 - H_b(p_i) \qquad (44)$$

where $C^d(p_i)$ represents the actual channel capacity of the deletion channel with deletion probability $p_i$ and $H_b(\bullet)$ denotes the binary entropy.

The equation given in (44) is valid for any deletion channel. Therefore,

$$\begin{aligned}
&1 - H_b(p_i) \;\leq\; C^d(p_i) \;=\; (1-p_i)C^i(p_i) \\
\Rightarrow \qquad &C^i(p_i) \geq \frac{1-H_b(p_i)}{1-p_i}. \qquad (45)
\end{aligned}$$

If we combine (42) and (45), we have

$$\begin{aligned}
C \;&\geq\; \frac{I(X,Y)}{1-p_i} - \frac{1}{1-p_i} + C^i(p_i) \\
&\geq\; \frac{I(X,Y)}{1-p_i} - \frac{1}{1-p_i} + \frac{1-H_b(p_i)}{1-p_i} \\
&=\; \frac{1-H_b(p_i)-H_b(p_e)}{1-p_i} \qquad (46)
\end{aligned}$$

where the last equation follows the assumption that the noisy channel is binary symmetric channel with substitution probability $p_e$. By definition, mutual information could not be less than zero, therefore, the lower bound can be written as

$$C \;\geq\; \max\left(0, \frac{1-H_b(p_i)-H_b(p_e)}{1-p_i}\right). \qquad (47)$$

To prove the upper bound for the covert-channel capacity, we consider a channel where the receiver is provided with the positions of all insertions caused by the covert channel and the sequence $Z^n = \{z_0, z_1 \;\cdots, z_n\}$ with

$$z_k = \begin{cases} 0 & \text{if the } k^{th} \text{ bit is inserted bit,} \\ 1 & \text{otherwise} \end{cases} \qquad (48)$$

which provides further information whether a bit is an information bit or an inserted bit. Therefore,

$$\begin{aligned}
I(W^n; Y^{\bar{N}n}) \;&\leq\; I(W^n; Y^{\bar{N}n}) + I(W^n; Z^{\bar{N}n} | Y^{\bar{N}n}) \\
&=\; I(W^n; Y^{\bar{N}n}, Z^{\bar{N}n}) \\
&=\; I(W^n; \hat{Y}^n) \qquad (49) \\
&=\; n(1-H_b(p_e)) \qquad (50)
\end{aligned}$$

where $\hat{Y}$ is the sequence obtained by removing the inserted bits. The equation given in (49) can be explained as follows: Knowing where the synchronization errors are located, the receiver can discard the inserted symbols. The capacity of this channel, therefore, is as large as the capacity of the channel with no synchronization errors. Finally, combining again (35) and (50), we can obtain the upper bound as

$$\begin{aligned}
C \;&=\; \sup_{\Xi} \lim_{n\to\infty} \frac{1}{n} \cdot I(W^n; Y^{\bar{N}n}) \\
&\leq\; \sup_{\Xi} \lim_{n\to\infty} \frac{1}{n} \cdot I(W^n; \hat{Y}^n) \\
&=\; 1 - H_b(p_e) \qquad (51)
\end{aligned}$$

which concludes the proof.

## REFERENCES


[1] B. W. Lampson, "A note on the confinement problem," *Commun. ACM*, vol. 16, no. 10, pp. 613–615, Oct. 1973. [Online]. Available: http://doi.acm.org/10.1145/362375.362389

[2] M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, and Y. Elovici, "Gsmem: Data exfiltration from air-gapped computers over gsm frequencies," in *24th USENIX Security Symposium (USENIX Security 15)*. Washington, D.C.: USENIX Association, Aug. 2015, pp. 849–864. [Online]. Available: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/guri

[3] ——, "Gsmem: Data exfiltration from air-gapped computers over GSM frequencies," in *24th USENIX Security Symposium (USENIX Security 15)*. Washington, D.C.: USENIX Association, 2015, pp. 849–864. [Online]. Available: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/guri

[4] M. Guri, M. Monitz, and Y. Elovici, "Usbee: Air-gap covert-channel via electromagnetic emission from USB," *CoRR*, vol. abs/1608.08397, 2016. [Online]. Available: http://arxiv.org/abs/1608.08397

[5] J. Millen, "20 years of covert channel modeling and analysis," in *Security and Privacy, 1999. Proceedings of the 1999 IEEE Symposium on*, 1999, pp. 113–114.

[6] A. G. Bayrak, F. Regazzoni, P. Brisk, F.-X. Standaert, and P. Ienne, "A first step towards automatic application of power analysis countermeasures," in *Proceedings of the 48th Design Automation Conference (DAC)*, 2011.

[7] D. Boneh and D. Brumley, "Remote Timing Attacks are Practical," in *Proceedings of the USENIX Security Symposium*, 2003.

[8] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound countermeasures to counteract power-analysis attacks," in *Proceedings of CRYPTO'99, Springer, Lecture Notes in computer science*, 1999, pp. 398–412.

[9] B. Coppens, I. Verbauwhede, K. D. Bosschere, and B. D. Sutter, "Practical Mitigations for Timing-Based Side-Channel Attacks on Modern x86 Processors," in *Proceedings of the 30th IEEE Symposium on Security and Privacy*, 2009, pp. 45–60.

[10] L. Goubin and J. Patarin, "DES and Differential power analysis (the "duplication" method)," in *Proceedings of Cryptographic Hardware and Embedded Systems - CHES 1999*, 1999, pp. 158–172.

[11] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Proceedings of CRYPTO'96, Springer, Lecture notes in computer science*, 1996, pp. 104–113.

[12] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis: leaking secrets," in *Proceedings of CRYPTO'99, Springer, Lecture notes in computer science*, 1999, pp. 388–397.

[13] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power analysis attacks of modular exponentiation in smart cards," in *Proceedings of Cryptographic Hardware and Embedded Systems - CHES 1999*, 1999, pp. 144–157.

[14] W. Schindler, "A timing attack against RSA with Chinese remainder theorem," in *Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2000*, 2000, pp. 109–124.

[15] D. Genkin, I. Pipman, and E. Tromer, "Get your hands off my laptop: Physical side-channel key-extraction attacks on pcs," in *Cryptographic Hardware and Embedded Systems CHES 2014*, ser. Lecture Notes in Computer Science, L. Batina and M. Robshaw, Eds. Springer Berlin Heidelberg, 2014, vol. 8731, pp. 242–260. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-44709-3_14

[16] M. Hutter and J.-M. Schmidt, "The temperature side channel and heating fault attacks," in *Smart Card Research and Advanced Applications*, ser. Lecture Notes in Computer Science, A. Francillon and P. Rohatgi, Eds. Springer International Publishing, 2014, vol. 8419, pp. 219–235. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-08302-5_15

[17] J. Brouchier, T. Kean, C. Marsh, and D. Naccache, "Temperature attacks," *Security Privacy, IEEE*, vol. 7, no. 2, pp. 79–82, March 2009.

[18] E. Bangerter, D. Gullasch, and S. Krenn, "Cache games - bringing access-based cache attacks on AES to practice," in *Proceedings of IEEE Symposium on Security and Privacy*, 2011.

[19] Y. Tsunoo, E. Tsujihara, K. Minematsu, and H. Miyauchi, "Cryptanalysis of block ciphers implemented on computers with cache," in *Proceedings of the International Symposium on Information Theory and its Applications*, 2002, pp. 803–806.

[20] Z. Wang and R. B. Lee, "New cache designs for thwarting software cache-based side channel attacks," in *ISCA '07: Proceedings of the 34th annual international symposium on Computer architecture*. ACM, 2007, pp. 494–505.

[21] D. Agrawal, B. Archambeult, J. R. Rao, and P. Rohatgi, "The EM side-channel(s)," in *Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2002*, 2002, pp. 29–45.

[22] ——, "The EM side-channel(s): attacks and assessment methodologies," in *http://www.research.ibm.com/intsec/emf-paper.ps*, 2002.

[23] M. G. Khun, "Compromising emanations: eavesdropping risks of computer displays," *The complete unofficial TEMPEST web page: http://www.eskimo.com/˜joelm/tempest.html*, 2003.

[24] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing keys from pcs using a radio: Cheap electromagnetic attacks on windowed exponentiation," in *Cryptographic Hardware and Embedded Systems – CHES 2015*, ser. Lecture Notes in Computer Science, T. Gneysu and H. Handschuh, Eds. Springer Berlin Heidelberg, 2015, vol. 9293, pp. 207–228. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-48324-4_11

[25] A. Zajic and M. Prvulovic, "Experimental demonstration of electromagnetic information leakage from modern processor-memory systems," *Electromagnetic Compatibility, IEEE Transactions on*, vol. 56, no. 4, pp. 885–893, Aug 2014.

[26] R. Callan, A. Zajic, and M. Prvulovic, "A Practical Methodology for Measuring the Side-Channel Signal Available to the Attacker for Instruction-Level Events," in *Proceedings of the 47th International Symposium on Microarchitecture (MICRO)*, 2014.

[27] J. K. Millen, "Covert channel capacity," in *Security and Privacy, 1987 IEEE Symposium on*, April 1987, pp. 60–60.

[28] Z. Wang and R. Lee, "Capacity estimation of non-synchronous covert channels," in *Distributed Computing Systems Workshops, 2005. 25th IEEE International Conference on*, June 2005, pp. 170–176.

[29] M. Davey and D. MacKay, "Reliable communication over channels with insertions, deletions, and substitutions," *Information Theory, IEEE Transactions on*, vol. 47, no. 2, pp. 687–698, Feb 2001.

[30] R. Venkataramanan, S. Tatikonda, and K. Ramchandran, "Achievable rates for channels with deletions and insertions," in *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, July 2011, pp. 346–350.

[31] A. Kirsch and E. Drinea, "Directly lower bounding the information capacity for channels with i.i.d. deletions and duplications," *Information Theory, IEEE Transactions on*, vol. 56, no. 1, pp. 86–102, Jan 2010.

[32] J. Hu, T. Duman, M. Erden, and A. Kavcic, "Achievable information rates for channels with insertions, deletions, and intersymbol interference with i.i.d. inputs," *Communications, IEEE Transactions on*, vol. 58, no. 4, pp. 1102–1111, April 2010.

[33] M. Rahmati and T. Duman, "Bounds on the capacity of random insertion and deletion-additive noise channels," *Information Theory, IEEE Transactions on*, vol. 59, no. 9, pp. 5534–5546, Sept 2013.

[34] H. Mercier, V. Tarokh, and F. Labeau, "Bounds on the capacity of discrete memoryless channels corrupted by synchronization and substitution errors," *Information Theory, IEEE Transactions on*, vol. 58, no. 7, pp. 4306–4330, July 2012.

[35] B. B. Yilmaz, R. Callan, M. Prvulovic, and A. Zajić, "Quantifying information leakage in a processor caused by the execution of instructions," in *Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE*. IEEE, 2017, pp. 255–260.

[36] B. B. Yilmaz, R. Callan, A. Zajic, and M. Prvulovic, "Capacity of the em covert/side-channel created by the execution of instructions in a processor," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 605–620, 2018.

[37] E. Cole, *Advanced persistent threat: understanding the danger and how to protect your organization*. Newnes, 2012.

[38] M. Prvulovic and A. Zajic, "Rf emanations from a laptop," 2012, http://youtu.be/ldXHd3xJWw8.

[39] J. Proakis, *Digital Communications*, ser. McGraw-Hill Series in Electrical and Computer Engineering. Computer Engineering. McGraw-Hill, 2001. [Online]. Available: https://books.google.com/books?id=sbr8QwAACAAJ

[40] DE1 FPGA on NIOS Processor, https://www.terasic.com.tw/cgi-bin/page/archive.pl?Language=English&CategoryNo=53&No=83&PartNo=2.

[41] Dual Polarized Panel Antenna, http://www.l-com.com/wireless-antenna-24-ghz-16-dbi-dual-polarized-panel-antenna-n-female-connectors.

[42] OlinuXino, https://www.olimex.com/Products/OLinuXino/A13/A13-OLinuXino/open-source-hardware.

[43] AH-118, "Double Ridge Horn Antenna," https://www.com-power.com/ah118_horn_antenna.html.

[44] P. Juyal, S. Adibelli, N. Sehatbakhsh, and A. Zajic, "A directive antenna based on conducting disks for detecting unintentional em emissions at large distances," *IEEE Transactions on Antennas and Propagation*, vol. 66, no. 12, pp. 6751–6761, 2018.

[45] R. Callan, N. Popovic, A. Zajić, and M. Prvulovic, "A new approach for measuring electromagnetic side-channel energy available to the attacker in modern processor-memory systems," in *2015 9th European Conference on Antennas and Propagation (EuCAP)*. IEEE, 2015, pp. 1–5.

[46] U. R. Inc., "Aor la390 wideband loop antenna," https://www.universal-radio.com/catalog/sw_ant/2320.html, 2014 (accessed Feb., 2019).

[47] R. J. Masti, D. Rai, A. Ranganathan, C. Müller, L. Thiele, and S. Capkun, "Thermal covert channels on multi-core platforms," in *24th USENIX Security Symposium (USENIX Security 15)*. Washington, D.C.: USENIX Association, 2015, pp. 865–880. [Online]. Available: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/masti

[48] A. Papoulis, *Probability, random variables, and stochastic processes*, ser. McGraw-Hill series in electrical engineering. New York: McGraw-Hill, 1991. [Online]. Available: http://opac.inria.fr/record=b1077486

[49] W. A. Gardner, "Two alternative philosophies for estimation of the parameters of time-series," *IEEE Transactions on Information Theory*, vol. 37, no. 1, pp. 216–218, 1991.

[50] R. L. Dobrushin, "Translated from problemy peredachi informatsii," *Probl. Inf. Transmiss.*, vol. 3, no. 4, pp. 11–26, 1967.

[51] S. Diggavi and M. Grossglauser, "On information transmission over a finite buffer channel," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 1226–1237, 2006.

**Baki Berkay Yilmaz** (S'16) received the B.Sc. and M.Sc. degrees in Electrical and Electronics Engineering from Koc University, Turkey in 2013 and 2015 respectively. He joined Georgia Institute of Technology in Fall 2016 and he is currently pursuing his PhD in School of Electrical and Computer Engineering, focusing on quantifying covert/side-channel information leakage. Previously, he worked on channel equalization and sparse reconstruction. His research interests span areas of electromagnetic, signal processing and information theory.

**Nader Sehatbakhsh** received his B.Sc degree in Electrical Engineering from University of Tehran in 2013 and the M.Sc. in Electrical Engineering from Georgia Institute of Technology in 2016. Since 2014, he has been a Graduate Research Assistant with CompArch and Electromagnetic Measurements in Communications and Computing (EMC2) Labs, pursuing the Ph.D. degree in the School of Computer Science, Georgia Institute of Technology focusing on Computer Architecture, Embedded System and Hardware Security. His work has received several awards including the Best Paper Award in MIRCO'49 for his work on using EM side-channel signals for software profiling.

**Milos Prvulovic** (S'97-M'03-SM'09) received the B.Sc. degree in electrical engineering from the University of Belgrade in 1998, and the M.Sc. and Ph.D. degrees in computer science from the University of Illinois at Urbana-Champaign in 2001 and 2003, respectively. He is a Professor in the School of Computer Science at the Georgia Institute of Technology, where he joined in 2003. His research interests are in computer architecture, especially hardware support for software monitoring, debugging, and security.

He is a past recipient of the NSF CAREER award, and a senior member of the ACM, the IEEE, and the IEEE Computer Society.

**Alenka Zajic** (S'99-M'09-SM'13) received the B.Sc. and M.Sc. degrees form the School of Electrical Engineering, University of Belgrade, in 2001 and 2003, respectively. She received her Ph.D. degree in Electrical and Computer Engineering from the Georgia Institute of Technology in 2008. Currently, she is an Associate Professor in the School of Electrical and Computer Engineering at Georgia Institute of Technology. Prior to that, she was a visiting faculty member in the School of Computer Science at Georgia Institute of Technology, a post-doctoral fellow in the Naval Research Laboratory, and a design engineer at Skyworks Solutions Inc. Her research interests span areas of electromagnetic, wireless communications, signal processing, and computer engineering.

Dr. Zajić was the recipient of the 2017 NSF CAREER award, 2012 Neal Shepherd Memorial Best Propagation Paper Award, the Best Student Paper Award at the IEEE International Conference on Communications and Electronics 2014, the Best Paper Award at the International Conference on Telecommunications 2008, the Best Student Paper Award at the 2007 Wireless Communications and Networking Conference, and the Dan Noble Fellowship in 2004, which was awarded by Motorola Inc. and the IEEE Vehicular Technology Society for quality impact in the area of vehicular technology. Currently, she is an editor for IEEE Transactions on Wireless Communications.