



International Journal of Applied Technology & Leadership  
ISSN 2720-5215  
Volume 3, Issue 1, January 2024  
ijatl@org

# Understanding How System-on-a-Chip Data Can Leak over Radio Transmissions

**Tom Gallagher**

Capitol Technology University (USA)

## Abstract

The 2018 Screaming Channels research raised cybersecurity concerns about mixed-signal electronic devices. Fully appreciating those concerns requires background in electrical engineering, cybersecurity, and cryptography. This article provides the necessary foundation and presents the Screaming Channels phenomenon in a way that is understandable for the masses. Electronic devices are becoming smaller and denser, introducing risk that electronic noise from sensitive processing will leak into broadcasts from the device. The 2018 study showed that certain kinds of electronics, mixed-signal system-on-a-chip devices, are susceptible to this type of leak. Devices that leak digital data into their broadcasts jeopardize the security of their communication. This article will extend the Screaming Channels phenomenon to the context of small satellite communications.

## 1. Introduction

As wireless technology is increasingly adopted into commercial products and communication infrastructure, ensuring the security of those communications becomes more important. This article will explore a novel threat vector for wireless signals identified by Giovanni Camurati in the 2018 publication, Screaming Channels (Camurati et al., 2018, 163). Additionally, this article will extend Camurati's work by describing the phenomenon in common terms for individuals without a background in electrical engineering, cybersecurity, and cryptography. Additionally, the Screaming Channels phenomenon will be presented in the context of satellite communication, which will set a foundation for two subsequent articles to further explore this area.

It can be difficult to conceptualize the inner workings of electronics. The microscopic scale of computer chips makes it challenging to visualize millions of transistors (tiny electronic components) in a space no wider than an eyelash. Additionally, it is difficult to comprehend the speed at which processors operate to perform billions of calculations in a second. For these reasons, this article will employ real-world analogies to explain circuit behavior for individuals without an electrical engineering background. In particular, water flowing through pipes is generally easier to conceptualize than electricity moving through a circuit, and both flows exhibit similar high-level characteristics. While the water analogy breaks down in describing certain characteristics of electricity, such as the magnetic field associated with the flow of electricity (Nave, 2016), the parallels are frequently noted in textbooks (Theraja, 2022, 102) and are sufficient to explain core mechanics underpinning the Screaming Channels phenomenon.

In a circuit, voltage is analogous to the pressure exerted by water, such as when it is stored in a water tower. Voltage is the difference in electrical potential in one area, such as a battery, to another area, such as an electrical component. Current in a circuit is analogous to the flow rate of water through a pipe. Voltage drop (the decrease in electric potential along a circuit) and current have a relationship based on the resistance of the circuit. This relationship is akin to how a one-inch hose and a six-inch pipe can deliver the same volume of water over time, but the hose would have a faster flow (i.e., greater pressure) to keep pace with the pipe. Similarly, electronic components with smaller resistance can carry larger current than components with larger resistance given the same voltage. Mathematically, Ohm's law defines this relationship as  $\text{current} = \text{voltage drop} / \text{resistance}$ . This basic and core concept of electronics provides a backdrop for the discussion in this article.

Figure 1 helps to illustrate the Screaming Channels wireless signal concern in the context of the water analogy. Consider this contrived situation: a spy wants to know when a particular military base is mobilizing for an operation. The spy is aware that prior to mobilizing for an operation, the base always fills water trucks using massive pipes. Fortunately for the spy, the base shares a water tower with a nearby small town. The spy notices that filling the water trucks uses so much water that it causes the water pressure to drop in the nearby town. With this knowledge, the spy can continuously measure their faucet's water pressure to detect the water trucks being filled and thus impending troop deployment. Though this is not a realistic example, it illustrates how the sensitive operations of one component (e.g., the military base) on a shared supply (e.g., the water tower) can cause measurable impacts on other components (e.g., the spy's faucet) within the same circuit.

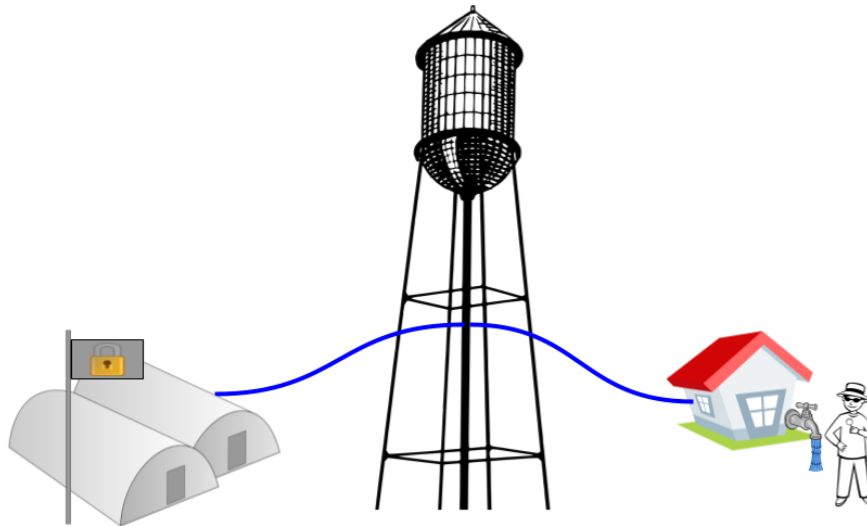


Figure 1: Screaming Channels information leak conceptualized in fictitious scenario.

Like the water system described above, an electronic device known as a mixed-signal circuit has multiple components that share a power source. As discussed in more detail later, mixed-signal circuits have digital components performing data processing and analog components that transmit and/or receive wireless signals. This article will explain how the sensitive operations within the mixed-signal circuit's processor can cause a voltage drop that impacts the radio components in the chip. This voltage drop may be propagated through the broadcast signal to the extent that sensitive information leaks across the broadcast.

## 2. Background

Though somewhat comical, the example of a spy sitting at their water faucet measuring water pressure is an example of a side-channel attack, where unintended effects leak sensitive information that is otherwise secure. Electronic side-channel attacks have been studied for decades. In 1985, Wim van Eck famously showed how electromagnetic emanations from computer monitors could be collected from an adjacent room and recreate the image on an attacker's screen (van Eck, 1985, 269). Despite extensive changes to computer architecture since van Eck's experiment, data leakage through unintentional electromagnetic (EM) "noise" is still a widespread issue being studied (Lavaud et al., 2021, 143-145).

### 2.1. A Tale of Two Signals

Since EM side-channel attacks have been studied for decades, it is understandable to question the significance of the 2018 Screaming Channels research. To understand the key difference between recent work and previous research, one must understand mixed-signal circuits and the difference between analog and digital signals.

Mixed-signal circuits are sets of electronic components intended to process digital signals and components intended to process analog signals (Das, 2021). Computers use a binary (0 or 1) digital signal to represent data being processed, such as when performing mathematical operations, running software applications, or processing images (Heddings, 2018). Analog signals are used whenever data is transmitted as radio signals over-the-air (i.e., wirelessly), such as over Wi-Fi, 5G, Bluetooth, and satellite communications (Agarwal & Lang, 2005, 41). Figure 2 illustrates the difference between digital and analog signals. The use of analog signals for broadcasting and digital signals for processing is not done out of convention or habit; the physics of these signals are such that they are the most practical choice for each use case. Because of this, circuits needing to both process data and communicate wirelessly use a mixed-signal architecture. Today, mixed-signal circuits are widely employed in consumer electronics, industrial control systems, and telecommunications in devices that use Wi-Fi, Bluetooth, 5G, and many other wireless protocols (Zhao & Hutchby, 2013, 157).

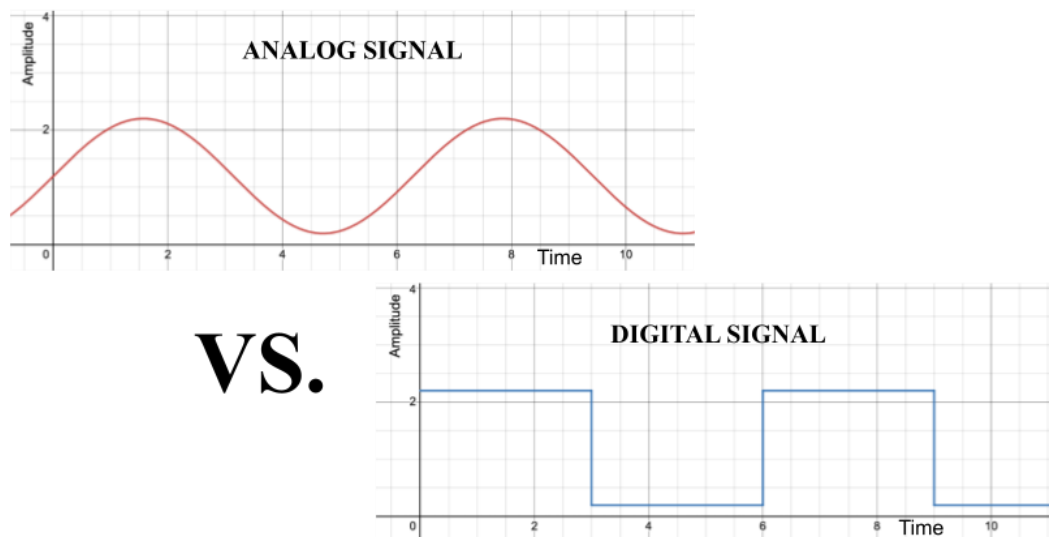


Figure 2: Digital vs Analog signals.

While the distinction between analog and digital may seem insignificant, different types of electronic components are used to process each type of signal and these components have different properties. Components processing analog signals tend to need high precision in measuring the signal (i.e., the “height” of the signal in the diagram) to accurately interpret the signal. Components processing digital signals have less need for precision since they ultimately interpret the signal as zero or one but are often focused on how quickly the signal can be sent or received. Because of the rapid transitions from zero (“off”) to one (“on”), digital components tend to be “noisy” in that they emit low-energy electromagnetic radiation. Analog components on the other hand are very sensitive to noise due to their requirement for precision (Marshall, 2022, 109). For this reason, mixed-signal circuits face the challenge of shielding analog components, such as radio transceivers, from the noise generated by digital processing. Often referred to as “crosstalk”, this design concern is a known issue (Peterson, 2019). This article will highlight the distinction between this problem and the Screaming Channels phenomenon.

## 2.2. Signal Modulation

It is conceptually straightforward how the 0's and 1's of digital signals represent arbitrary data through a variety of encoding techniques, such as the American Standard Code for Information Interchange (ASCII) representation of the letter "A" as 01000001 (Figure 3). Thus, it is straightforward to understand how these digital signals can be used within an electronic device or even over wired communication between devices. However, wireless communication is based on electromagnetic waves, which are inherently analog. Digital data is encoded onto an analog signal by modulating the analog signal in a way that the receiver can detect. To accomplish this, the transmitter alters an expected analog signal, known as a carrier signal, and the receiver can detect the differences, recreating the underlying digital signal used to create the transmission. There are three foundational analog modulation methods: frequency modulation (FM), amplitude modulation (AM), and phase modulation (PM) (Seçgin, 2023, 10-12). AM and FM are household acronyms made famous as the receiving modes of music radios; PM is not as widely known and has nothing to do with the afternoon indicator, post meridiem, bearing the same acronym.

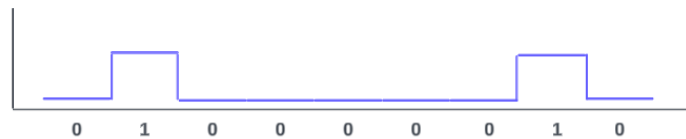


Figure 3: A digital signal representing the letter "A" in ASCII.

Each form of modulation makes perceptible changes to a specific aspect of the known carrier signal. Amplitude modulation modifies the "height" of the carrier signal; frequency modulation modifies the "period" of the carrier signal (i.e., how many times the signal repeats within an interval); and phase modulation modifies the "phase" of the carrier signal (i.e., where the carrier signal is in its cycle). Figure 4 below illustrates how FM, AM, and PM schemes would change a carrier signal given a particular data signal. Ultimately, when an electronic device broadcasts a signal, it is this modulated radio wave that carries the data.

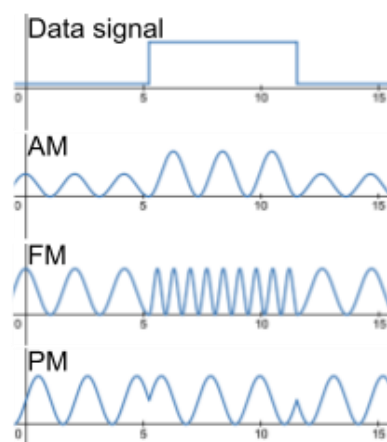


Figure 4: Comparison of AM, FM, and PM signal modulation.

Despite there being three foundational modulation schemes, amplitude modulation is not generally used alone in electronic communications because it is more susceptible to interference. Instead, wireless broadcasts generally use FM, PM, or a combination of the foundation schemes. For example, 5G cellular service may use Quadrature Amplitude Modulation (QAM), which is a combination of AM and PM, or Quadrature Phase Shift Keying (QPSK), which is based on PM (Thangamayan et al., 2022, 848). Different modulation techniques have different properties such as noise-resistance and data rate. For the purposes of this paper, it is sufficient to understand that there are three foundational modulation schemes and that modern wireless signals are designed to use one or more of them.

### **2.3. System-on-a-Chip**

A system-on-a-chip (SoC) is a single integrated circuit (a.k.a. computer “chip”) that contains the functionality of an entire electronic device (Gudivada et al., 2018, 173-179). For instance, a Bluetooth SoC includes the components necessary to transmit/receive a Bluetooth signal as well as a digital processor to perform application logic. SoCs can reduce the cost of manufacturing and assembling devices. In some cases, SoCs can reduce energy consumption and even increase performance. The benefits of SoCs come at the cost of increased design complexity (Rautakoura & Hämäläinen, 2023, 2-3). To accommodate the increased functionality, SoCs must fit many components into a small area. While circuit design is a mature field that has solved the operational challenges with SoCs, electronic components in close proximity and using the same power source can have subtle and unintended effects on each other as the remainder of this article will discuss.

## **3. The Screaming Channels Phenomenon**

### **3.1. Screaming Channels Analogy**

Returning to the analogy of water to understand electronics, consider valves on two pipes connected to the bottom of a large drum filled with water. Valve A is continuously being slowly adjusted from open to closed. Valve B is occasionally being switched, nearly instantly, between fully open and completely closed. With Valve B closed, if you were to measure the water pressure exiting Valve A, the flow would directly coincide with the changes to Valve A. However, consider what would happen if Valve B was suddenly opened; there would be a noticeable drop in water pressure because the water’s force would be distributed between the two pipes. Similarly, if Valve B was suddenly closed, water flowing out of Valve A would experience an observable increase in pressure. Figure 5 graphs this example. This example should make sense to anyone who has had an annoying sibling flush the toilet causing scalding water to pour out of the shower from the resultant drop in pressure from the shared cold-water supply.

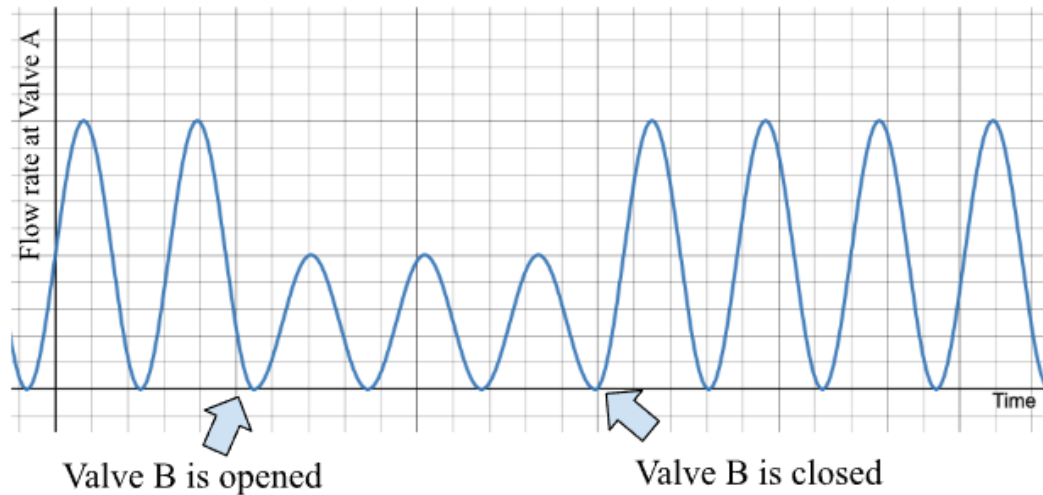


Figure 5: While flow rate is being constantly affected by Valve A, Valve B is suddenly opened and remains open for a short time before being suddenly closed. The graph shows the flow rate at Valve A.

### 3.2. Screaming Channels in a Circuit

Electricity flowing through mixed-signal circuits behaves like water pipes using a shared supply. In this example, Valve A represents the analog transceiver; Valve B, the digital processor; and the water drum, the shared power source. While there are several complexities abstracted by this analogy, the core concept is demonstrated. In a mixed-signal circuit, when there is a sudden drain/surge caused by state changes in the digital components (e.g., microscopic transistors switching from unpowered to powered to complete an operation), the analog components experience the voltage change as well.

Unlike the simple water tower example, voltage variations have more subtle effects on the underlying components. Digital components are designed to operate within a range of voltages and are operationally unaffected by slight variations; analog components are more sensitive to voltage variations (Patel, 2022). Voltage determines the strength (i.e., amplitude) of the broadcast from analog transceivers. Recall that wireless signals may exclusively use frequency modulation and/or phase modulation to encode data. In these cases, small amplitude modulations will not operationally affect the receiver's ability to interpret the intended signal. In other words, the receiver for these signals is only designed to detect variations in frequency and/or phase, so amplitude modulations are filtered out as noise. Returning briefly to the water analogy, someone getting a glass of water from their faucet is unlikely to notice if the water is fluctuating between 45 and 44 psi. Similarly, a radio receiver designed to demodulate based on phase and/or frequency is unlikely to "notice" small variations in the signal's amplitude. Essentially, these unnoticed variations in amplitude are the "Screaming Channel".

While this basic overview of Screaming Channels is sufficient to understand the concept, it hides some important complexities. Mixed-signal circuits are not composed of a single digital component and a single analog component; instead, billions of microscopic transistors make up

a digital processor. Each transistor changing state (unpowered to powered or vice versa) causes a small drop/surge in voltage and induces voltage changes in nearby components. Rather than the transistors chaotically changing at their own cadence though, the entire digital circuit triggers state changes based on a shared internal clock. Thus, the voltage changes in the digital circuit are tied to the clock signal which helps to abstract the problem from billions of components back to a single abstract source. In other words, it may not be clear what any specific transistor did at a given moment, but a clock trigger causing an overall drop in voltage could indicate a greater number of transistors “powering up” (i.e., switching from unpowered to powered). Billions of components abstracted into a simple metric of “surge” or “drain” may seem like a trivial amount of information; however, any information about the internal processor state can have drastic implications on data security (Randolph & Diehl, 2020, 1-2). In particular, this small leakage could potentially compromise private data transmitted from the device, described later in this article and in subsequent articles in the series.

### 3.3. Screaming Channels Example

A common mixed-signal circuit found in many consumer and commercial electronics is a chip used to send and receive wireless communications using the Bluetooth Low Energy (BLE) protocol (Cäsar et al., 2022, 1). BLE uses a form of frequency modulation, Gaussian Frequency Shift Keying (GFSK), to encode and decode digital information with a wireless carrier signal (Woolley, 2021). GFSK is a frequency modulation scheme, so minor amplitude fluctuations from a Screaming Channels leak would be filtered out by the intended receiver. Secure BLE communication uses encryption to secure transmissions necessitating a digital processor to perform the cryptography. With these conditions, a Bluetooth System-on-a-Chip (SoC) represents a potential environment where digital voltage fluctuations could impact the intended analog signal. Camurati showed that not only is such a leak possible but that the leak exists in real-world hardware and is sufficient to compromise the secured communication channel from the device.

BLE transmissions use GFSK modulation within the range of 2.54GHz to 2.56GHz. This means that over one second, the carrier signal repeats more than 2.5 billion times. The clock signal of a digital processor operates on a much slower frequency, generally 36-48MHz, or repeating approximately 40 million times per second. Figure 6 shows a 1/10,000,000 second (or 0.1 $\mu$ s) depiction of a 2.5GHz signal [green/top], a 40MHz signal [blue/middle], and a 2.5GHz signal that has been modulated by a 40MHz signal [red/bottom]. In this diagram, the green signal represents a signal exhibiting a Screaming Channels leakage. This depiction is theoretical as it shows flawless reception and zero noise/interference.



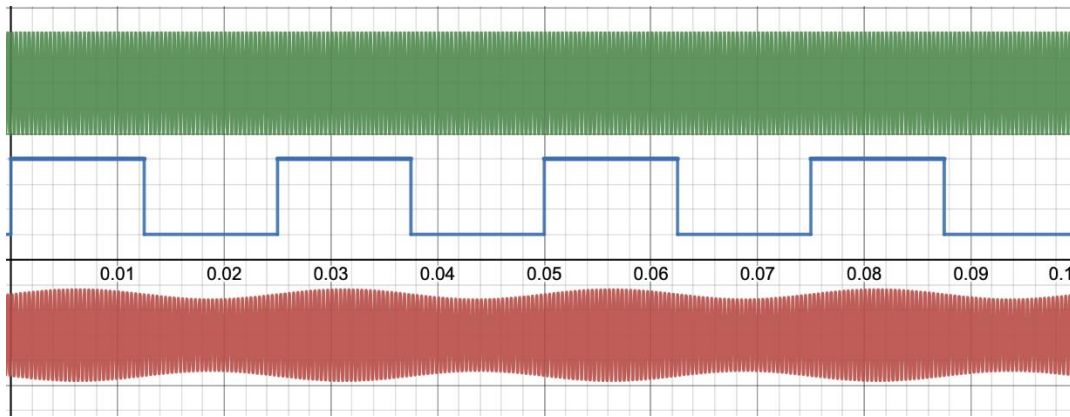


Figure 6: An idealized depiction over 0.1 microseconds of a 2.5GHz signal [top], a 40MHz signal [middle], and a 2.5GHz signal that has been modulated by a 40MHz signal [bottom].

In the real world, even within a radio frequency (RF) shielded enclosure, there is still background EM noise generated by the environment or other components on the device. Figure 7 shows an RF trace of a Bluetooth transmitter, Nordic Semiconductor PCA10040, where the digital processor is idle (a.k.a. sleeping) [top] and active [bottom]. The PCA10040 was shown to exhibit a Screaming Channels leak in Camurati’s published study (Camurati et al., 2020, 393). The top capture was taken by enabling the analog transmitter to continuously broadcast while the digital processor was configured to sleep. The bottom capture was taken by enabling the transmitter to continuously broadcast while the digital processor was tasked with continuous operations. The green line and red line show the average amplitude of the signal. As expected, when the digital processor is using power from the shared source, the amplitude of the signal is measurably lower. This is visible on the graphs as the green line [top graph] shows a slightly higher value than the red line [bottom graph]. Just like the water faucet example, this difference is not “noticeable” by a typical Bluetooth receiver.

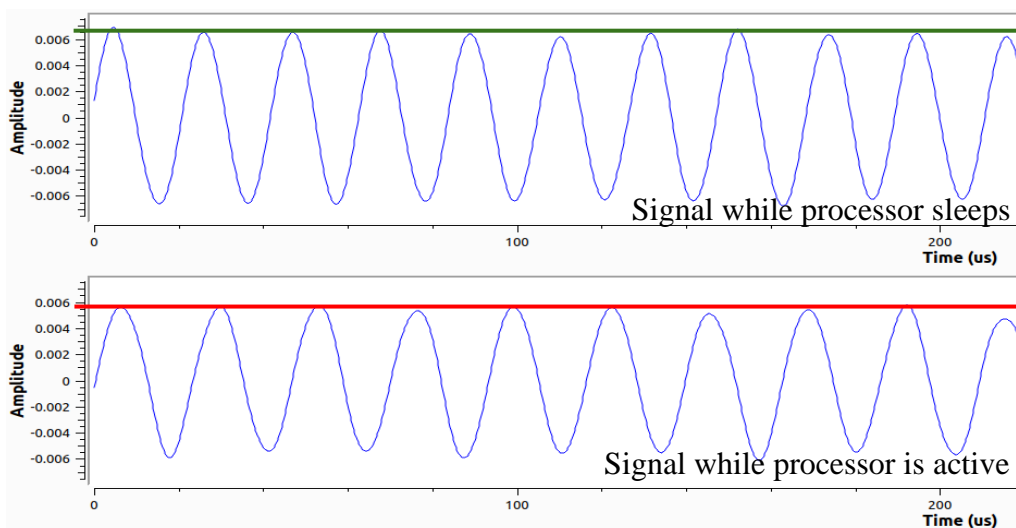


Figure 7: An RF capture from a Nordic Semiconductor PCA10040 Bluetooth transceiver [top] and the same device exhibiting a Screaming Channels leak [bottom].

These traces echo the findings of Camurati in showing the leakage from the digital processor into the analog signal. The Screaming Channels research further explored the leak during the

encryption process. Figure 8 below, taken from Camurati's work, shows the Bluetooth signal over time where the sensitive cryptographic processing is clearly affecting the analog transmission.

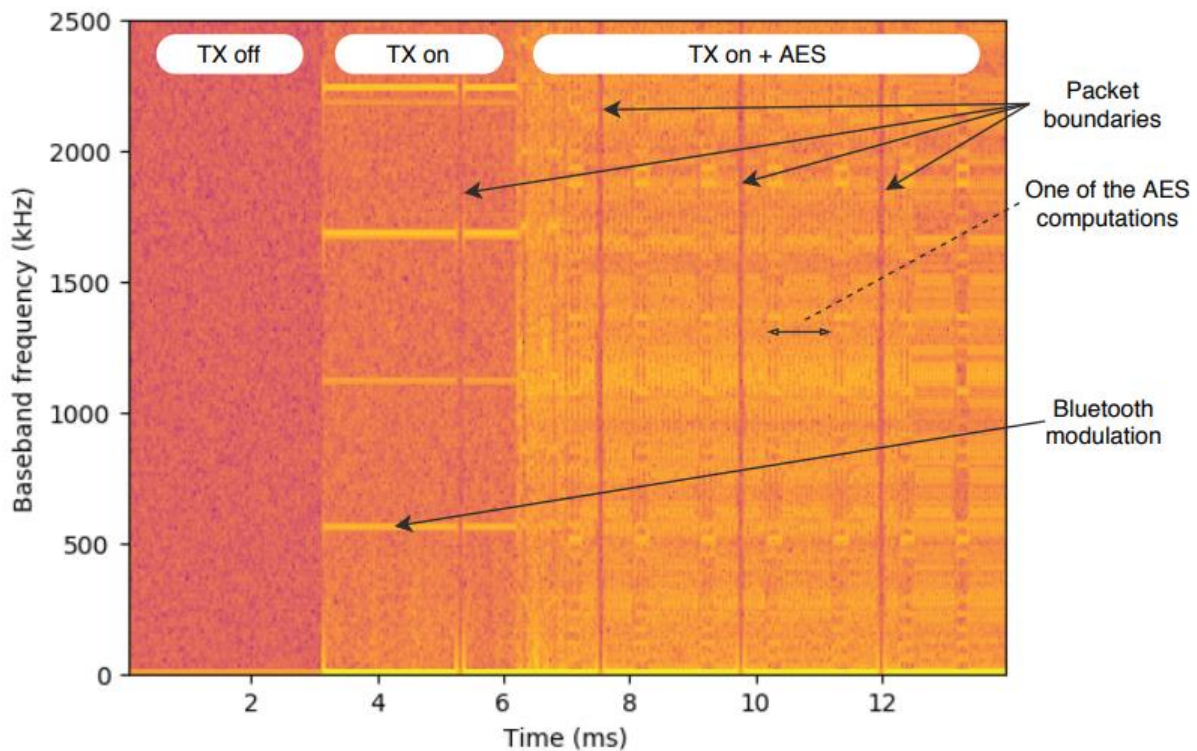


Figure 8: Frequency vs. Time plot of a Bluetooth transceiver while the device is off [TX off], transmitting [TX on], and transmitting while digitally processing [TX on + AES]. Image from *Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers*.

#### 4. Impact

With water flow, there isn't typically a significant need to hide whether a valve is open or closed. With a digital processor however, changes in power consumption can reveal details about the state of the internal processing, which can potentially be used to infer data being processed (Buiras et al., 2021, 579). This is extremely impactful if the data being processed is sensitive to security such as an encryption key. Secure wireless communications depend on the secrecy of the private key, so if such a key were to be compromised, then all communications using that key could be intercepted and decrypted. While the data leak could have additional implications on data security, the risk to cryptographic keys is likely the most impactful.

##### 4.1. Bluetooth Side-Channel Attack

Side-channel analysis is an attack enabled by a leak from a physical system, such as observable power consumption, acoustic emanations, or electromagnetic noise (NIST, 2020). For example, processing encryption algorithms, such as the widely adopted Advanced Encryption Standard (AES), can produce well-known patterns of EM noise (Wang & Dubrova, 2021, 4). Figure 9

shows a trace for a particular implementation of AES; each of the 16 rounds within the single encryption is observably similar. Using a side-channel attack on vulnerable AES processing emissions, attackers can potentially calculate the underlying cryptographic key (Yu et al., 2020, 410). Concern over these leaked transmissions led to the emergence of the emissions security (EMSEC) field, which focuses on preventing attackers from compromising unintentionally emitted signals (Anderson, 2020, 583). For the purposes of this article, it is sufficient to understand that comparing EM traces from known keys with traces from unknown keys could infer the unknown key. Side-channel cryptanalysis will be described in greater detail in the third article of this series.

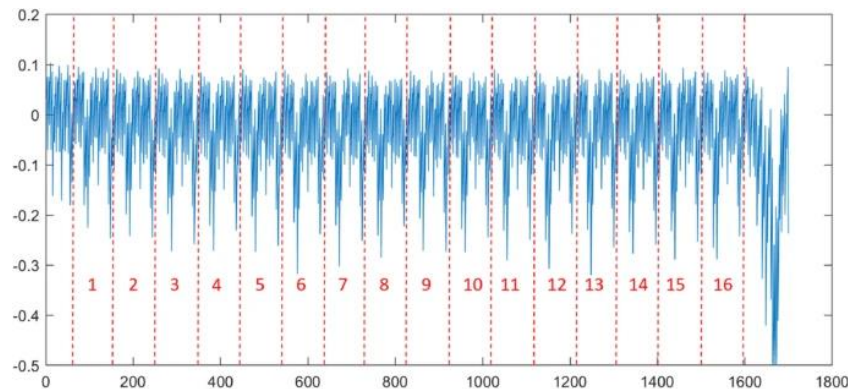


Figure 9: A signal trace showing the 16 rounds of AES encryption producing identifiable patterns (Wang & Dubrova, 2021, 4).

The 2018 Screaming Channels research analyzed three Bluetooth SoCs for leakage from the digital processor into the Bluetooth transmission. Bluetooth SoCs provide analog components for wireless transmission and digital processors making them potentially candidates for a Screaming Channels leak. By repetitively triggering specific functionality of a Bluetooth SoC, Camurati built a corpus of encryption traces with known keys. From that corpus, he was able to derive templates for traces based on known key values. He then collected traces from a device where the key was unknown and used cryptanalysis techniques to determine the secret key.

Figure 10 below shows how the Screaming Channels research could be leveraged to carry out a real-world attack. (1) An attacker develops firmware to exercise the cryptographic process in a piece of target hardware that the attacker owns. (2) The attacker records the signals from the device during the execution with both known keys. (3) The attacker develops a template of how data is leaked by the hardware. (4) The attacker interacts (potentially remotely) with a victim device that uses the same hardware recording the emanated signals. (5) The attacker correlates the captured signals with the leak model to determine possible values for the victim's key. Once an attacker has the victim's key, they can decrypt wireless communications protected by that key.

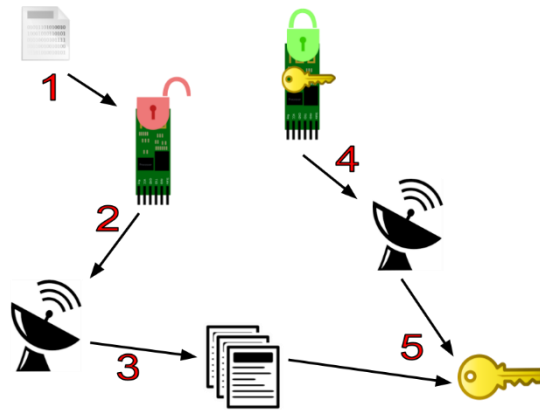


Figure 10: Attack scenario considered.

While the 2018 *Screaming Channels* attack against Bluetooth raised significant concerns, several implementation challenges made the tests less realistic. Custom firmware was created for both the attacker and victim devices rather than demonstrating an attack against an existing product. Additionally, the attack targeted a non-standard cryptographic library, tinyAES, that is known to be vulnerable to cryptanalysis and the device was configured to disable “frequency hopping”, a standard Bluetooth feature. Camurati postulated that frequency hopping could be defeated by other mechanisms, such as channel blacklisting or listening on all channels, which would make the attack more complex but not outside the realm of skilled actors (Camurati et al., 2020, 368). The use of tinyAES as a proof of concept provided a well-known cryptanalysis target to ease the burden on the researchers. Camurati performed analysis against the SoC’s innate cryptographic algorithms as well as a non-standard “masked” AES implementation<sup>1</sup>. In both cases, the attacks were unsuccessful in extracting the cryptographic key. In 2020, Camurati demonstrated successful *Screaming Channels* attacks against Google Eddystone Beacon devices (Camurati et al., 2020, 390-394) proving the real-world applicability of this issue.

## 4.2. Beyond Bluetooth

While the *Screaming Channels* research focused on Bluetooth devices, there is no reason why the phenomenon could not exist in similar circuits. Specifically, devices that communicate wirelessly and process sensitive data on the same chip are *potentially* vulnerable. Obvious and ubiquitous candidates are cellular devices (e.g., LTE, 3G, 5G) and electronics using IEEE 802.11 protocols (i.e., Wi-Fi). However, a more novel and potentially overlooked class of devices are satellites.

Satellites require wireless communication and perform digital processing, thus meeting part of requirements for the possibility of *Screaming Channels* leaks. However, the satellite would need to perform both operations on the same circuit to be vulnerable. Historically, satellites have been large platforms with separate dedicated circuits for handling transmissions, encrypting communications, and processing data (Linville & Bettinger, 2020, 43). Some

<sup>1</sup> Masked cryptographic algorithms include mitigations that reduce that exploitability of side-channel leaks.

satellites may eschew that practice in order to minimize size and weight, two important design considerations for satellites (Cobb, 2019). In fact, some modern satellite architectures have pushed minimization to the extreme in the production of “ChipSats” (example shown in *Figure 11*), which are functional satellites approximately the size of postage stamps (Abate, 2019). As the name implies, ChipSat architecture condenses the vast majority of functionality into a single integrated circuit (Umansky-Castro et al., 2021, 1). Thus, at a minimum, ChipSats have the preconditions for the possibility of a *Screaming Channels* leak. Other satellite architectures, such as CubeSats, may also leverage mixed-signal SoCs, but specific satellites would need to be reviewed on a case-by-case basis. The remainder of this series of articles will focus on ChipSats.

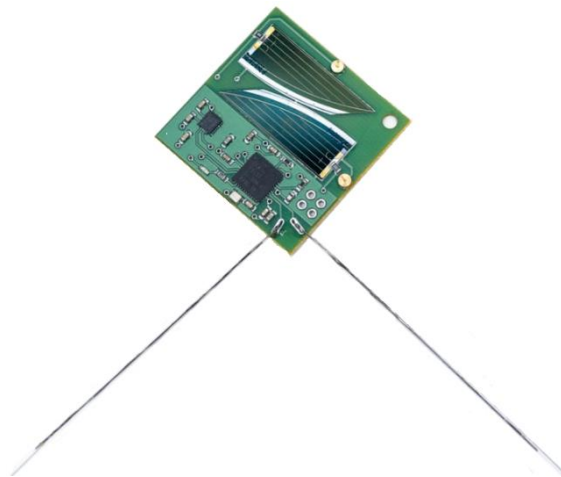



Figure 11: Example ChipSat that went into orbit. [Image credit: L.A. Cicero] (Abate, 2019).

To better understand ChipSat components, three publicized ChipSat initiatives were researched for this article. Specifically, Cornell University’s Monarch technology, the AmbaSat satellite kit, and Carnegie Mellon’s Tartan Artibeus platform published details regarding the hardware, including the radio transceiver SoC. *Table 1* below condenses those details and will provide the target of analysis for subsequent articles in this series.

Small Satellite	Identified SoC	Digital Processor	Analog broadcast	Visual
Monarch (Adams, 2020)	CC1310	48MHz ARM Cortex-M3	287-351, 359-439, 431-527, 718-878, 861-1054 MHz	





AmbaSat (Walls, 2020)	LoRa RFM95	48 MHz ARM Cortex-M4	868, 915 MHz	
Tartan Artibeus (Denby & Ruppel, 2022, 9)	CC1110	Intel 8051 CPU	300-348, 391-464, 782-928 MHz	

Table 1: Identified hardware in ChipSats.

## 5. Conclusion

The *Screaming Channels* phenomenon is an emerging threat to electronics that use mixed-signal SoCs, which are commonly used in a variety of consumer and enterprise electronics. While the Screaming Channels issue has been a known engineering challenge for decades, commonly referred to as crosstalk, the cybersecurity impact of this issue extends beyond device functionality. The phenomenon is potentially present when digital and analog components of a circuit share a power source. Digital components abruptly change state, which may cause miniscule voltage spikes and drops across the shared power substrate. Analog signals are sensitive to voltage changes, which may modulate the amplitude of the intended signal. If the intended signal uses frequency and/or phase modulation, the unintended amplitude modulation would be ignored as background noise. Because the information leak is broadcast alongside the device's intended analog signal, there is potential for an attacker to exploit the leak from anywhere that the signal reaches. The *Screaming Channels* leak was shown to be exploitable against some Bluetooth SoCs and is theorized to be exploitable across SoCs using other protocols. ChipSats and other small satellites that use mixed-signal SoCs could provide a novel attack surface for *Screaming Channels* analysis.

This article provided background on the *Screaming Channels* phenomenon, its known impact on Bluetooth devices, and its potential impact to small satellite communications. The next article in this series will present a framework for identifying potential *Screaming Channels* leaks in small satellite transceiver SoCs. The third and final article will provide methodology to measure the data leakage and explore the potential for cryptanalytic attacks against such leaks.

## References

1. Abate, T. (2019, June 3). Inexpensive chip-size satellites orbit Earth | Stanford News. *Stanford News*. <https://news.stanford.edu/2019/06/03/chip-size-satellites-orbit-earth/>
2. Adams, V. H. (2020, May). *Theory and Applications of Gram-Scale Spacecraft*. [https://ecommons.cornell.edu/bitstream/handle/1813/70469/Adams\\_cornellgrad\\_0058F\\_1\\_1878.pdf?sequence=1](https://ecommons.cornell.edu/bitstream/handle/1813/70469/Adams_cornellgrad_0058F_1_1878.pdf?sequence=1)
3. Agarwal, A., & Lang, J. (2005). *Foundations of analog & digital electronic circuits*. Elsevier Science. [https://neurophysics.ucsd.edu/courses/physics\\_120/Agarwal%20and%20Lang%20\(2005\)%20Foundations%20of%20Analog%20and%20Digital.pdf](https://neurophysics.ucsd.edu/courses/physics_120/Agarwal%20and%20Lang%20(2005)%20Foundations%20of%20Analog%20and%20Digital.pdf)
4. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley. <https://www.cl.cam.ac.uk/~rja14/book.html>
5. Buiras, P., Nemat, H., Lindner, A., & Guanciale, R. (2021). Validation of Side-Channel Models via Observation Refinement. *54th Annual IEEE/ACM International Symposium on Microarchitecture, Micro '21(MICRO-54)*, 578–591. ACM Digital Library. 10.1145/3466752.3480130
6. Camurati, G., Francillon, A., & Standaert, F.-X. (2020). Understanding Screaming Channels: From a Detailed Analysis to Improved Attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020(3), 358–401. 10.13154/tches.v2020.i3.358-401
7. Camurati, G., Poeplau, S., Muench, M., Hayes, T., & Francillon, A. (2018). Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers. *CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018(October), 163-177. 10.1145/3243734.3243802
8. Cäsar, M., Pawelke, T., Steffan, J., & Terhorst, G. (2022). A survey on Bluetooth Low Energy security and privacy. *Computer Networks*, 205(108712), 1-18. 10.1016/j.comnet.2021.108712
9. Cobb, W. W. (2019, March 1). *How SpaceX lowered costs and reduced barriers to space*. The Conversation. Retrieved June 29, 2023, from <https://theconversation.com/how-spacex-lowered-costs-and-reduced-barriers-to-space-112586>
10. Das, S. (2021, June 3). *Mixed Signal Circuit | Definition, Design, Examples*. Electronics Tutorial | Best Electronics Tutorial Website. Retrieved June 29, 2023, from <http://www.electronicandyou.com/mixed-signal-circuit-definition-design-examples.html>
11. Denby, B., & Ruppel, E. (2022). Tartan Artibeus: A Batteryless, Computational Satellite Research Platform. *Small Satellite Conference*, 2022. <https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=5213&context=smallsat>
12. Gudivada, V. N., Ramaswamy, S., & Srinivasan, S. (2018). Data Management Issues in Cyber-Physical Systems. In L. Deka & M. Chowdhury (Eds.), *Transportation Cyber-Physical Systems* (pp. 173-200). Elsevier Science. 10.1016/B978-0-12-814295-0.00007-1
13. Heddings, A. (2018, October 1). *What is Binary, and Why Do Computers Use It?* How-To Geek. Retrieved June 29, 2023, from <https://www.howtogeek.com/367621/what-is-binary-and-why-do-computers-use-it/>

14. Lavaud, C., Gerzaguet, R., Gautier, M., Berder, O., Nogues, E., & Molton, S. (2021, June 1). Whispering devices: A survey on how side-channels lead to compromised information. *Hardware and Systems Security*, 5(2), 143-168. 10.1007/s41635-021-00112-6
15. Linville, D., & Bettinger, R. A. (2020). An Argument against Satellite Resiliency Simplicity in the Face of Modern Satellite Design. *Air & Space Power Journal*, 2020(Spring), 43-53. [https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34\\_Issue-1/V-Linville\\_Bettinger.pdf](https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-1/V-Linville_Bettinger.pdf)
16. Marshall, A. (2022). Noise Effects in Analog Systems. In *Mismatch and Noise in Modern IC Processes* (pp. 109-117). Springer International Publishing. 10.1007/978-3-031-79791-0\_10
17. National Institute of Standards and Technology. (2020). *NIST SPECIAL PUBLICATION 1800-21 [Mobile Device Security]*. NIST Technical Series Publications. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-21.pdf>
18. Nave, C. R. (2016). *What's Wrong with the Water Circuit Analogy?* HyperPhysics Concepts. Retrieved June 29, 2023, from <http://hyperphysics.phy-astr.gsu.edu/hbase/electric/watcir3.html#c1>
19. Patel, S. (2022, April 21). *What's the Difference Between Analog and Digital Circuits in PCB Design?* Electronic Design. Retrieved July 31, 2023, from <https://www.electronicdesign.com/technologies/analog/article/21238481/mermar-electronics-whats-the-difference-between-analog-and-digital-circuits-in-pcb-design>
20. Peterson, Z. (2019, April 1). *How to Reduce and Remove Noise In Analog Signals From Your PCB*. Altium Resources. Retrieved July 30, 2023, from <https://resources.altium.com/p/removing-noise-analog-signals-your-pcb>
21. Randolph, M., & Diehl, W. (2020). Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman. *Cryptography*, 4(2), 1-33. 10.3390/cryptography4020015
22. Rautakoura, A., & Hamalainen, T. (2023, April 18). Does SoC Hardware Development Become Agile by Saying So: A Literature Review and Mapping Study. *ACM Transactions on Embedded Computing Systems*, 22(3), 1-27. 10.1145/3578554
23. Seçgin, S. (2023). *Evolution of Wireless Communication Ecosystems*. John Wiley & Sons, Incorporated. 10.1002/9781394182343
24. Thangamayan, S., Walunekar, M. D., Kumar Ray, D., Venkatesan, M., Banik, A., & Amrutkar, K. P. (2022). 5G Modulation Technique Comparisons Using Simulation Approach. *International Conference on Intelligent Engineering and Management (ICIEM)*, 2022(3rd), 848-856. 10.1109/ICIEM54221.2022.9853137
25. Theraja, B. L. (2022). *Fundamentals of Electrical Engineering and Electronics (LPSPE)*. S CHAND & Company Limited. [https://www.google.com/books/edition/Fundamentals\\_of\\_Electrical\\_Engineering\\_a/GbucEAAAQBAJ](https://www.google.com/books/edition/Fundamentals_of_Electrical_Engineering_a/GbucEAAAQBAJ)
26. Umansky-Castro, J. S., Yap, K. G., & Peck, M. A. (2021). ChipSats for Planetary Exploration: Dynamics and Aerothermal Modeling of Atmospheric Entry and Dispersion. *Frontiers in Astronomy and Space Sciences*, 8(July), 1-17. 10.3389/fspas.2021.664215
27. van Eck, W. (1985). Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? *Computers & Security*, 4(4), 269-286. ScienceDirect.



28. Walls, N. (2020, December). *AmbaSat-1: How To Guide*. AmbaSat. Retrieved July 8, 2023, from <https://ambasat.com/downloads/AmbaSat-1-How-To-Guide-MKII-Kit.pdf>
29. Wang, H., & Dubrova, E. (2021, July 9). Tandem Deep Learning Side-Channel Attack on FPGA Implementation of AES. *SN Computer Science*, 2(5), 1-12. 10.1007/s42979-021-00755-w
30. Woolley, M. (2021, Sep 9). *Bluetooth® Core Specification v5.0*. Bluetooth Technology. Retrieved July 31, 2023, from [https://www.bluetooth.com/wp-content/uploads/2019/03/Bluetooth\\_5-FINAL.pdf](https://www.bluetooth.com/wp-content/uploads/2019/03/Bluetooth_5-FINAL.pdf)
31. Yu, Q., Zhang, Z., & Dofe, J. (2020). Cyber-Physical Vulnerability Analysis of IoT Applications Using Multi-Modeling. In C. A. Kamhoua, S. Shetty, L. L. Njilla, & A. Kott (Eds.), *Modeling and Design of Secure Internet of Things* (pp. 407-433). Wiley. 10.1002/9781119593386.ch18
32. Zhao, B., & Hutchby, J. A. (2013). Mixed-Signal Technologies and Integrated Circuits. In J. N. Burghartz (Ed.), *Guide to State-of-the-art Electron Devices* (pp. 157-170). Wiley-IEEE Press. 10.1002/9781118517543.ch12