Electromagnetic Side Channel Leakage Improvements Using Free-running Oscillator Clock Reference

Jacob N. Louie*, Sara Faour**, and David C. Burnett*
*Department of Electrical and Computer Engineering, Portland State University, Portland, Oregon, USA
**Inria, Paris, FR
Email: jlouie@pdx.edu, sara.faour@inria.fr, dburnett@pdx.edu

***Abstract*—Electromagnetic (EM) leakage can be seen near the radio's center frequency when a mixed-signal chip wirelessly transmits data. The undesired signal provides information that can be exploited to decode encrypted data on the chip. This paper looks into how a free-running RC oscillator affects the EM leakage that is being seen through the on-chip radio and compares these results to a clock reference that is similar to a traditional crystal. The purpose of testing a free-running oscillator is to see how a more inconsistent clock reference would affect EM leakage through the radio in hopes of finding an additional countermeasure. The inconsistency of this clock reference is small enough that it is still compatible with IoT communication standards like IEEE 802.15.4. Meaning that devices using this alternative clock reference may not sacrifice any functionality and will have the added benefit of an increase in scalability and a decrease in power consumption. Along with capturing the activity near the carrier, data at the 3rd harmonic (3X the center frequency) is taken. The results of the RC oscillator tests show a decrease in amplitude near the center frequency and no visible EM leakage at 3X the center frequency, with a maximum difference of approximately 6.48 dBm when compared to the crystal-like clock reference. The decrease in signal power causes a reduction in the distance at which the leakage can be exploited. It can be assumed that this type of clock source can be used as a countermeasure, improving the EM side-channel leakage.**

***Index Terms*—Electromagnetic leakage, mixed-signal chip, clock jitter, free-running.**

I. Background

Previous work [1] has shown that it is possible to intercept electromagnetic (EM) leakage through the radio's transceiver when it is sending 2.4 GHz modulated data like Bluetooth or Wi-Fi. This allowed them to decode the encrypted data being processed on the CPU at a greater distance than previously possible. Without the help of the transceiver, the amount of EM leakage would only be visible within millimeters of range for low-power devices [1]. EM leakage has been a known issue in the cybersecurity world [2]. Because of this, there are already methods in place to help prevent EM leakage from being exploited. These methods include shielding, filtering, and masking to dampen, hide, or isolate unwanted noise [3], [4].

Despite this, [1] highlights the increased vulnerability of System-on-Chip (SoC) devices that have their radio on the same die as the CPU. Having both analog and digital components on the same die is a mixed-signal chip. EM leakage is generated due to the sharp current transitions generated by digital activity. As the die sizes and the isolation between analog and digital components decrease, the signal strength of EM leakage increases. This signal is then amplified along with the desired message signal and broadcast by the radio [1]. Internet of Things (IoT) devices that are bound to have a mixed-signal design due to area constraints are especially prone to side-channel attacks.

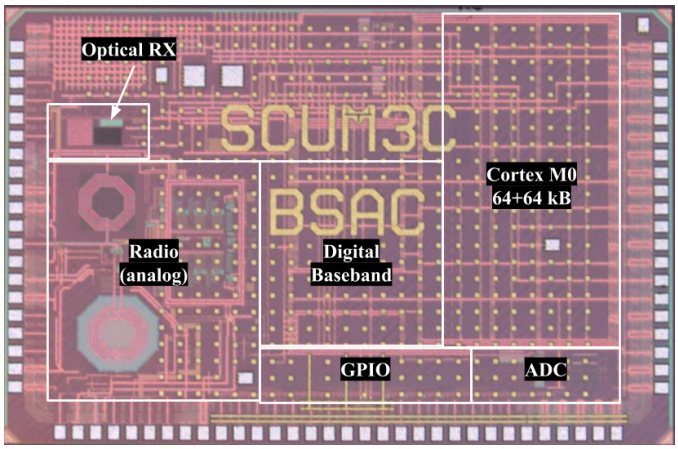


Fig. 1: Annotated die photo of Single-Chip micro-Mote (SCμM). The total die volume is $2 \times 3 \times 0.3mm^3$ [8].

II. Introduction

This paper explores the amount of EM radio leakage on a mixed-signal chip that uses a free-running LC oscillator as the RF local oscillator and a free-running RC oscillator as the CPU clock reference. These results are compared to the amount of EM leakage when using a traditional crystal-referenced CPU clock. The tests in this paper aim to find an alternative method to improve the amount of EM leakage broadcast through the radio. Because the leakage is coming from the radio, the signal is relative to the transmitted center frequency and the clock frequency. To determine what RF signals are being produced due to EM leakage, each clock reference is shown as the chip does a series of mathematical computations in software,

979-8-3503-6330-2/24/$31.00 ©2024 IEEE
DOI 10.1109/CrystalFreeIoT62484.2024.00006

overlaid with the RF data when the chip is doing nothing in a continuous loop (infinite while loop).

It is important to note that the amount of EM leakage into the radio is dependent on the chip's physical layout and design [1]. When the digital logic and radio are spatially closer, the amount of leakage into the radio will likely increase. In addition, the specific hardware implementations incorporated as countermeasures for standard EM leakage need to be accounted for. This means that any test comparing the difference in EM leakage is relative to the hardware on which the test is being run. For all tests, the Single-Chip micro-Mote (SCμM) [7], [8] is used. SCμM is uniquely suited for this experiment because of the amount of control over the clocks and filtering that most commercial devices don't allow. This chip ordinarily uses an internal free-running RC oscillator to clock the CPU but can also clock the CPU from an external clock source. The size and general layout of this chip can be seen in Figure 1.

The hypothesis is that the RC oscillator will have a diminished amount of leakage because of the amount of jitter and lack of "sharp" current transitions associated with this type of clock. A RC oscillator generally has an estimated ppm of 1000 while a crystal source can range from 50-100 ppm [6]. Any type of inconsistency coming from the source of the EM leakage could help reduce the peak signal strength on the RF spectrum. This would decrease the distance at which the side channel leakage can be exploited. Despite using a noisier clock reference compared to crystals, SCμM can still communicate wirelessly to commercial devices using the IEEE 802.15.4 communication standard and transmit Bluetooth LE data [5], [6], potentially revealing a standards-compatible SoC with reduced leakage issues compared to commercial products. From a design perspective, the biggest trade-off of implementing a free-running oscillator as the clock source would be a reduction in clock stability. The current benefits of doing so include the increase in total footprint scalability due to the removal of the crystal reference. There would also be a decrease in power consumption when using a free-running oscillator in comparison to a crystal oscillator.

III. Methods

Using SCμM on the Sulu V2 [9] development board, a 20 MHz external clock is provided from a function generator and is connected to the chip through the GPIO. Alternatively, the chip uses an internal 20 MHz free-running RC oscillator as the CPU's clock reference. A 20 MHz CPU clock is used due to the SCμM limitations on the CPU clock speed. Switching between the two clock references can be controlled in software. Both clock references are running to ensure consistency between the two clock reference tests and the external clock is physically connected to the GPIO throughout all tests.

The spectrum analyzer was configured with the settings used in Table I and was connected to SCμM with an SMA cable (for the general testing layout see Figure 2). The transmit frequency is centered at 2.4 GHz and the 3rd harmonic at 7.2 GHz ($3 \cdot f_{center}$). Looking at the 3rd harmonic is useful

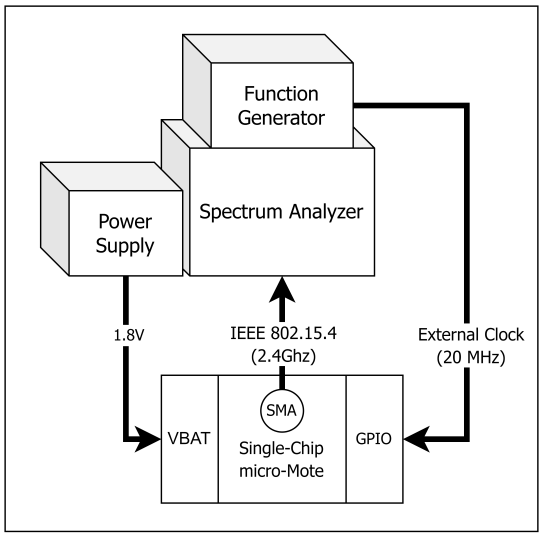


Fig. 2: Block diagram of the test setup including Agilent E3636A Power Supply, Tektronix AFG 3252 Function Generator, Agilent E4440A PSA Series Spectrum Analyzer, and Sulu V2 Development Board [9].

for avoiding interference from external signals. In software, the chip is configured to switch between doing computations and doing nothing by sitting in a loop. These computations are intended to simulate data that could be maliciously extracted and are intended to demonstrate the difference in activity levels when logic gates are switching. The software also controls the switching of the radio's functionality and the previously mentioned clock references. The following terms describe parameters for testing.

Doing Work/No Work: The chip is considered doing "No Work" when in an empty loop. When the chip is "Doing Work", the CPU runs simple computations comprised of integer multiplication, division, summation, and exponentiation. This can also be described as the CPU's activity level.

HF Clock: This is the internal free-running RC oscillator that is calibrated to 20 MHz. This is the typical CPU clock reference for this crystal-free chip.

External Clock: A Tektronix AFG 3252 Function Generator that is running at 20 MHz and is connected through SCμM's GPIO to the CPU as a substitute for a crystal clock reference.

Averaging/No Averaging: Averaging refers to the bandwidth averaging (BW/Avg) setting on the spectrum analyzer. When Averaging is on, the result is the average signal amplitude from consecutive sweeps.

No Data Transmitted: When the term "No Data Transmitted" is used, the chip has its transmitter on but it is not modulating/sending data. Even though this parameter does not represent a real-world configuration, this is done for testing purposes. All of the "Data Transmitted" figures are not included in this paper. These figures are excluded for clarification purposes to introduce the topic and to focus solely on CPU clock reference changes. The results from the data transmitted test may show that the phase noise from the RF

TABLE I: Spectrum analyzer configuration (Agilent E4440A PSA Series Spectrum Analyzer).

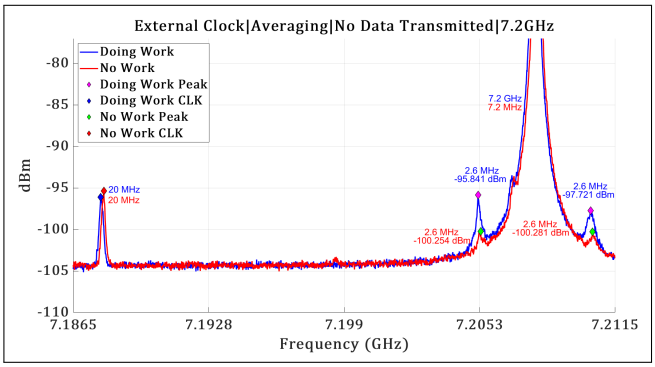
Setting	Value
Scale/Div	3 dB
Attenuation	0 dB
Average Count	100
Points	2000
VBW	10 kHz
RBW	100 kHz

local oscillator is capable of masking the EM leakage from the crystal-reference CPU. This is not the focus of this paper which is why those figures are not included.

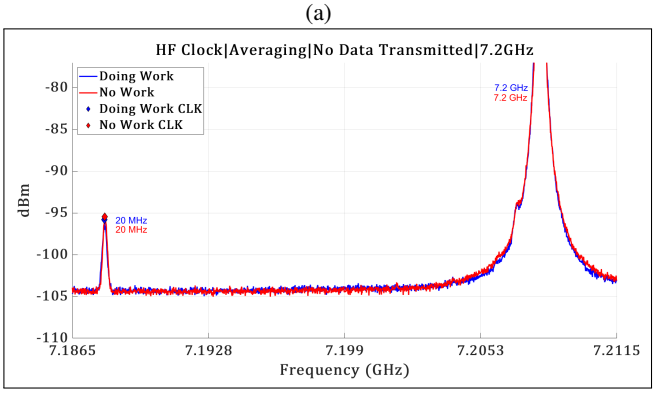
IV. Results

Figures 3 and 4 show the difference in the radio-amplified EM leakage between the external and RC oscillator clock references. Only half of the frequency spectrum is shown for demonstration purposes, being centered between the carrier frequency and the CPU clock offset. It can be expedited that almost all of the activity seen on one side is also mirrored on the other. All markers in these figures, excluding the 3rd harmonic (7.2GHz), are labeled as the frequency offset from the 3rd harmonic. The 20 MHz clock signal can be seen on the far left while the center frequency is shown on the right side of the graph as the signal with the highest power. The EM leakage can be seen at 1.6 MHz from the carrier (2.4GHz) and 2.6 MHz from the third harmonic (7.2GHz) of the carrier. It is known that these peaks are the result of EM leakage based on the floor set by the "No Work" signal in Figures 3-5. By purposefully removing the math computations in software for the "No work" data, the signals seen at 1.6MHz and 2.6MHz must be the activity factor of the logic gates switching.

At 3X the center frequency, when no data is transmitted and averaging is on, an ideal scenario is presented (Figure 3). The ideal scenario in this context means the configuration that would result in the most visible EM leakage. With the external clock reference, there is a noticeable difference in signal amplitude when comparing the chip activity data at 2.6 MHz (Figure 3a). It can be concluded that the expected EM leakage when using the external clock source is present. This data is the baseline when determining if a change in clock reference will make a difference. As shown in Figure 3b, the EM leakage spikes at 2.6 MHz using the external clock do not seem to be present with the RC oscillator. This shows a decrease in EM leakage at the 2.6 MHz offset of approximately 6.48 dBm. Despite not seeing any visible leakage when using the RC oscillator, this is inconclusive evidence of no EM leakage. This is because the observed leakage has a frequency delta of 2.6 MHz which is relatively close to the center frequency, making it likely that phase noise from the LC oscillator is hiding the EM leakage.



(a)

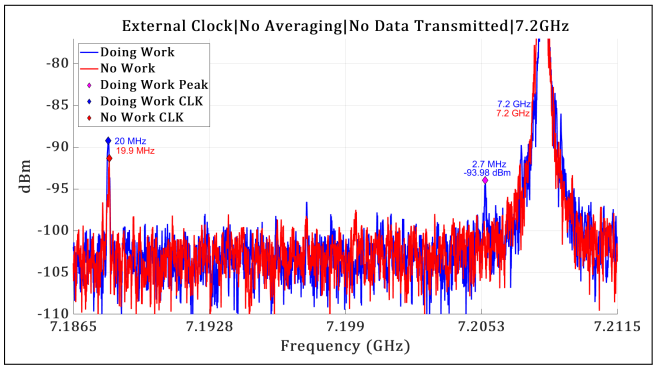


(b)

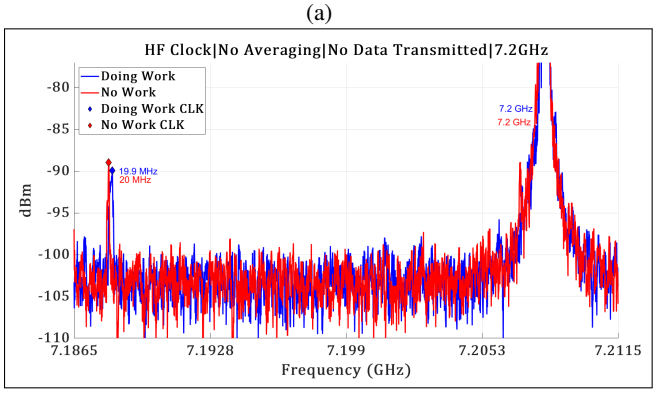
Fig. 3: The average amplitude at 3X the center frequency of 2.4 GHz. A comparison of EM signal strength between the crystal-like external clock reference (a) and the internal free-running RC oscillator (b). All makers, excluding the 3X center frequency, are labeled as the frequency offset from the 3X center frequency. The 20 MHz signal is the clock frequency. The 2.6MHz signal in (a) is the EM leakage. At 2.6 MHz offset, left of the center frequency, there is a difference of 6.48 dBm between the two oscillators when doing work. The max signal power of the 3X center frequency is -52.2 dBm.

The exclusion of averaging in Figure 4 is meant to represent a real-time snapshot of the amount of visible leakage without the noise being masked due to averaging. The external clock data with no averaging has a noticeable EM leakage spike when "Doing work" (Figure 4a). As for the internal clock data without averaging, there may be a small momentary spike around 2.7 MHz (Figure 4b). It is known from the averaged data in Figure 3b, that this can not be a consistent occurrence. Subsequent snapshots result in no noticeable CPU activity.

At 2.4 GHz, the external clock source exhibits EM leakage near 1.6 MHz from the center frequency (Figure 5a). CPU activity also seems to be present near the clock frequency. These activity spikes, on the left side of Figure 5a, are labeled as the frequency offset between themselves and the clock frequency. The unlabeled frequency spikes when the chip is doing "No Work" are echoes from the clock frequency. The switch to the RC oscillator at 2.4 GHz (Figure 5b) also indicates a decrease in EM leakage, similar to what is

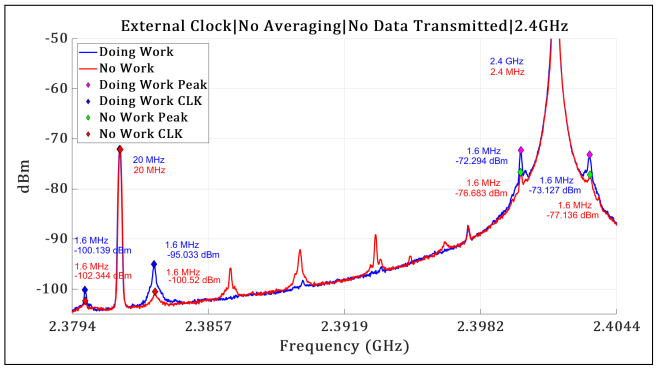


(a)

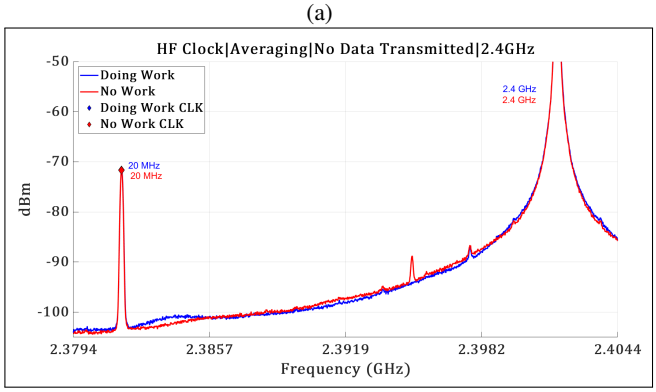


(b)

Fig. 4: A single snapshot taken of the signal amplitude at 3X the center frequency of 2.4 GHz. A comparison of EM signal strength between the crystal-like external clock reference (a) and the internal free-running RC oscillator (b). All makers, excluding the 3X center frequency, are labeled as the frequency offset from the 3X center frequency. The 20 MHz signal is the clock frequency. The 2.6MHz signal in (a) is the EM leakage. The max signal power of the 3X center frequency is -45.1 dBm.



(a)



(b)

Fig. 5: The average amplitude at the center frequency of 2.4 GHz. A comparison of EM signal strength between the crystal-like external clock reference (a) and the internal free-running RC oscillator (b). All makers, excluding the center frequency, are labeled as the frequency offset from the center frequency. The 20 MHz signal is the clock frequency. The 1.6MHz signal in (a) is the EM leakage. At 1.6 MHz offset, right of the clock frequency, there is a difference of 6.44 dBm between the two oscillators when doing work. The max signal power of the center frequency is -15.5 dBm.

shown at 7.2 GHz (Figure 3). However, there is now visible leakage relative to the clock frequency showing a difference in amplitude between CPU activity levels. This can be seen at approximately 1.6 MHz on the right side of the 20 MHz clock frequency (Figure 5b) with a difference between the two oscillators being approximately 6.44 dBm when the CPU is doing computations. A symmetrical response is expected on both sides of the clock frequency when there is activity. It is unknown why this is not the case in the experiment. The visible EM leakage has a decrease in signal amplitude but an increase in bandwidth compared to the external clock source. It is unknown if this signal can still be exploited using the existing methods for side-channel attacks. Based on the results at 2.4 GHz, the switch to an RC oscillator could reduce the distance at which a side-channel attack is possible. This can be an additional method for improving EM leakage.

V. Conclusion

The amplified EM leakage through a mixed-signal chip's radio was recreated using a function generator as a substitute for a crystal clock reference. The chip used for testing had an internal free-running RC oscillator for its CPU clock reference. When comparing the amount of EM leakage between the two there is a difference in amplitude when using the RC oscillator compared to the crystal-like clock reference, measured to be as much as 6.48 dBm. This may be due to the RC oscillator's increased amounts of jitter and lack of sharp current transitions compared to a more stable crystal-like clock reference. The chip used in testing uses a free-running LC oscillator as the RF local oscillator and can communicate using the IEEE 802.15.4 communication standard. This means that for certain applications there would be no change in functionality with the addition of an increase in total footprint scalability and a decrease in power consumption.

At the 3rd harmonic, there seems to be no noticeable EM

leakage. This is important because the 3X center frequency is what would most likely be used in a side-channel attack due to fewer interfering signals. Near the center frequency (2.4 GHz), using the free-running RC oscillator, there was a decrease in amplitude and an increase in bandwidth of the EM leakage. Even though the EM leakage is still present, the decrease in amplitude causes a reduction in the distance at which the leakage can be exploited. This makes it more difficult for a side-channel attack to take place.

With the continued shrinkage of designs, this type of clock reference can be an additional method for improving EM leakage on mixed-signal chips. The levels of improvement will vary between implementations because the amount of EM leakage into the radio depends on the physical layout and the use of existing countermeasures to standard EM leakage.

VI. Future Work

Further investigation into the limitations of using a free-running oscillator to improve EM leakage is needed. Increasing the amount of radio EM leakage, followed by introducing this alternative clock reference, could help in the understanding of the effectiveness of this method. As noted in the methods section, the clock rate for the experiments is limited by SCμM's hardware design. However, it was observed in the tests that the amplitude of the EM leakage would non-linearly increase as the clock frequency increased. Running the same test at a higher clock rate may give more insight into this implementation.

The testing in this paper only focused on the change in power between clock references. This means this paper did not attempt to implement any decoding used in previous work [1]. Further testing can be done by creating a more realistic signal comprised of encrypted data being computed on the chip. If other implementations of the free-running RC oscillator result in a measurable EM leakage signal, an attempt at decoding the signal can be made.

References

[1] Camurati, Giovanni, et al. "Screaming channels: When electromagnetic side channels meet radio transceivers." Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018.

[2] "Tempest: A Signal Problem," NSA, https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf.

[3] Agrawal, Dakshi, et al. "The EM side—channel (s)." Cryptographic Hardware and Embedded Systems-CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 2002 Revised Papers 4. Springer Berlin Heidelberg, 2003.

[4] R. M. Secareanu et al., "Physical design to improve the noise immunity of digital circuits in a mixed-signal smart-power system," 2000 IEEE International Symposium on Circuits and Systems (ISCAS), Geneva, Switzerland, 2000, pp. 277-280 vol.4, doi: 10.1109/ISCAS.2000.858742.

[5] F. Maksimovic et al., "A crystal-free single-chip micro mote with integrated 802.15.4 compatible transceiver, sub-mW Ble compatible beacon transmitter, and cortex M0," 2019 Symposium on VLSI Circuits, Jun. 2019. doi:10.23919/vlsic.2019.8777971

[6] D. C. Burnett et al., "CMOS oscillators to satisfy 802.15.4 and Bluetooth LE PHY specifications without a crystal reference," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Jan. 2019. doi:10.1109/ccwc.2019.8666473

[7] D. C. Burnett et al., "Two-Chip Wireless H2S Gas Sensor System Requiring Zero Additional Electronic Components," 2019 20th International Conference on Solid-State Sensors, Actuators and Microsystems & Eurosensors XXXIII (TRANSDUCERS & EUROSENSORS XXXIII), Berlin, Germany, 2019, pp. 1222-1225, doi: 10.1109/TRANSDUCERS.2019.8808294.

[8] T. Chang et al., "Industrial IOT with Crystal-free mote-on-chip," 2020 IEEE Symposium on VLSI Circuits, Jun. 2020. doi:10.1109/vlsicircuits18222.2020.9162981

[9] "scum-dev-board," GitHub, https://github.com/PisterLab/scum-dev-board/tree/master/sulu-reg.