Ultra Freezing Attacks and Clock Glitching of Clock Oscillator Circuits

Jonathon Durand
Yale University
jonathon.durand@yale.edu

Anisul Abedin
Yale University
anisul.abedin@yale.edu

Jakub Szefer
Yale University
jakub.szefer@yale.edu

***Abstract*—This paper introduces novel ultra freezing attacks on clock oscillator circuits. The new attacks leverage liquid nitrogen to rapidly freeze quartz crystal oscillators and MEMS-based oscillators to temperatures approaching $-195\,^{\circ}\mathrm{C}$ ($-320\,^{\circ}\mathrm{F}$ or $77\,\mathrm{K}$). When the oscillators freeze to these temperatures, they begin to exhibit behavior outside of their specification, behavior which can especially be used to launch clock glitching like attacks on the target devices. In particular, when liquid nitrogen is poured over the devices, or when they are dipped in liquid nitrogen, the clock frequencies generated by the oscillator circuits become unstable, drift from their specification, or even stop oscillating for a period of time, creating glitches. The ultra freezing attacks presented in this work are the first type of clock glitching attacks on clock oscillator circuits that do not require physical connection to the target circuit, but can simply be deployed by pouring liquid nitrogen over the target device. The attacks are further very low cost. This paper highlights a new physical attack threat that designers should be aware of and defend against.**

I. Introduction

Secure, trustworthy, and reliable integrated circuits for computing and communications systems can only be created when physical security is considered. While numerous physical attacks require sophisticated equipment and may not easily be deployed in the wild, liquid nitrogen (LN_2) attacks are very inexpensive and can be readily performed in many settings. The ultra freezing attacks presented in this work are the first type of attacks on clock oscillator circuits that do not require physical connection to the target circuit, but can be simply deployed by pouring liquid nitrogen over the target device, or dipping the target device in liquid nitrogen.

The new type of physical attack is applied to quartz crystal oscillators and MEMS-based oscillators, which are often used to generate clock signals for computing and communications systems. As this work demonstrates, liquid nitrogen can rapidly freeze quartz crystal oscillators and MEMS-based oscillators to temperatures approaching $-195\,^{\circ}\mathrm{C}$ ($-320\,^{\circ}\mathrm{F}$ or $77\,\mathrm{K}$), at which point they begin to exhibit undesired behavior. The signal frequencies generated by the oscillator circuits become unstable, the signal frequencies drift from their specification, or the oscillators even stop oscillating for a period of time. The last behavior can be especially used to launch a new type of clock glitching attack that does not require physical connection to the device, but only physical proximity to pour the liquid nitrogen on the target device.

This work demonstrates that the new ultra freezing attacks are a new type of physical attack, and they can affect not just discrete clock circuits, but can affect computing platforms such as Android UNO or Google's Edge TPU. To address the threats, this paper also discusses a number of defenses that designers should consider to protect their devices from the ultra freezing attacks.

This work was supported in part by NSF grant 1901901.

978-1-6654-4185-8/21/$31.00 ©2021 IEEE

II. Background and Related Work

This work focuses on physical attacks, and in particular new attacks that abuse electronic device behaviors at very low temperatures. Prior security attacks based on rapidly cooling computer components are exemplified by the Cold Boot attack [1], which focused on the internal capacitors found in the data cells of Dynamic Random Access Memory (DRAM) modules. The authors showed that by cooling DRAM chips, the decay rate of the capacitors used to store data bits in DRAMs is reduced. This extends the time for which data persists in a powered-off chip, and allows malicious adversaries to transfer the cooled DRAM to a different computer to read the DRAM cells before the data is lost. The Cold Boot attacks focused on using up-side-down compressed air cans which leak compressed gas when used up-side-down and cool the DRAM. Authors in [1] also showed dipping DRAM chips in LN_2 to extend the time of the DRAM retention. The Cold Boot attack and its related work, e.g., [3], [4], has focused on cooling computer memories only, and did not consider clock oscillator circuits, and also did not focus on LN_2, except for one demonstration in [1].

More recent cooling-based attack work demonstrated the Chill Out attack [2], which focused on evaluation of behavior of capacitors and DC/DC converters when exposed to cooling sprays. The authors showed that there is a decrease in capacitance when capacitors are cooled to about $-55\,^{\circ}\mathrm{C}$, and that DC/DC converter behavior changes if the cooling is applied to the output electrolytic capacitors. The authors used off-the-shelf electronic cooling sprays and, similar to Cold Boot attack, up-side-down compressed air cans.

Our work differs from such prior research by considering the security implications of ultra freezing of clock oscillator circuits. Neither did existing work extensively evaluate using LN_2. Although extra care is needed to transport LN_2, the

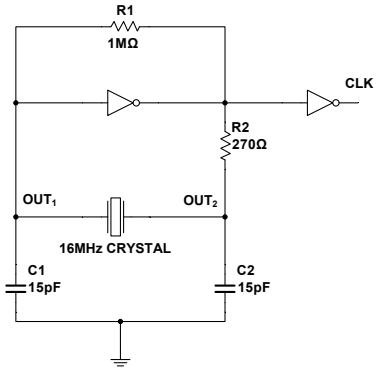

Fig. 1. Example schematic of a 16 MHz Pierce oscillator used in the experiments in this work.

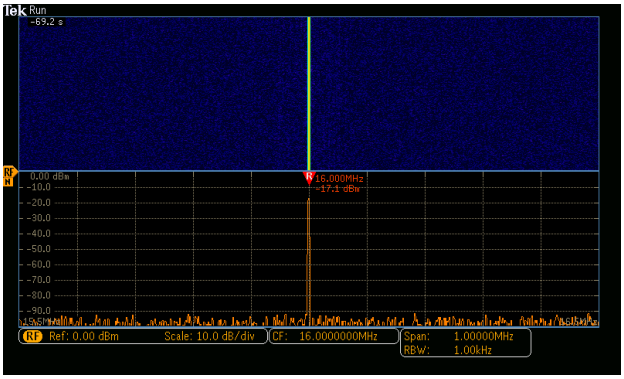

Fig. 2. Spectrogram of the quartz crystal output at room temperature before the attack.

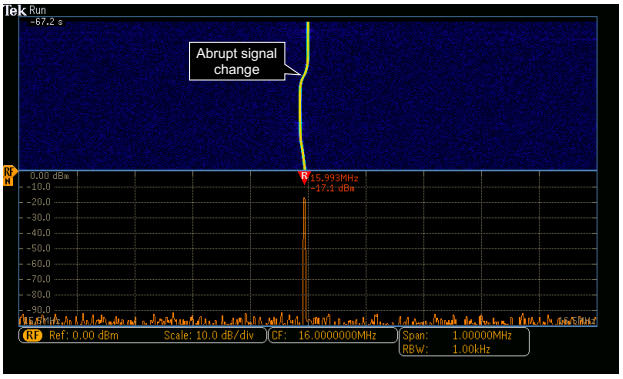

Fig. 3. Spectrogram showing that when dipping the quartz crystal in LN_2 the output signal deviates from specified frequency, but slowly begins to return towards specification as the crystal warms up after removal from LN_2.

attack cost can actually be lower than using cooling sprays or up-side-down compressed air cans. Cooling spray cans cost about \$20 per 10 oz can, electronic duster compressed air cans cost about \$5 per 3.5 oz can, while a liter of LN_2 needed for each attack costs about \$0.10 when purchased in bulk from our university cleanroom. Thus the new LN_2 attacks can be less expensive and bring devices to much lower temperatures compared to other cooling approaches.

III. Threat Model

This work assumes a malicious attacker who has physical access to the target device, but cannot modify or probe the target device, which could be easily noticed or detected by on-board circuitry. Instead, the attacker has a brief window of time to make changes to the environment in which the device operates, such as by pouring liquid nitrogen over the device or dipping the device in liquid nitrogen. We assume the attacker can control the time of the LN_2 pouring or time of dipping in the LN_2. We assume the attacker has access to device for no more than about 30-60 s, making this a very fast attack.

While the attack could be detected by use of thermal sensors, to best of our knowledge, existing circuits targeted in this work, such as in Arduino UNO or Google's Edge TPU, do not use thermal sensors or other defenses today. Section VIII has a more detailed discussion of the potential defenses and other considerations, such as thermal diodes or temperature-compensated crystal oscillators.

IV. Evaluation of Pierce Oscillators

Pierce oscillator is one of the most common designs for generating a square wave clock signal used for processors, microcontrollers, or other computer systems. It uses a very simple design, which is built around a quartz crystal resonator, has a very low cost due to limited number of components needed to build it. Figure 1 shows an example schematic of a Pierce oscillator used in our experiments. The values of capacitors and resistors can be adjusted depending on the frequency of the crystal.

In our evaluation, we evaluated number of quartz crystals. A 16 MHz crystal, part number `9B-16.000MAAE-B` from TXC Corporation, rated to −20 °C. A 16 MHz crystal, part number `ATS16A` from CTS-Frequency Controls, rated to −20 °C A 16 MHz crystal, part number `AS-16.000MAHK-B` from TXC Corporation, rated to −40 °C. A 32 MHz crystal, part number `9B-32.000MAAJ-B` from TXC Corporation, rated to −20 °C. The results and spectrograms are shown for the `ATS16A` crystal from CTS-Frequency Controls, but are representative of all the crystals tested.

A. Attack Setup

In the experiments, all components were initially at room temperature. Then, the quartz crystals were dipped in LN_2 for 30 s. The crystals were attached to long jumper wires to allow for their dipping in LN_2, while the rest of the circuit could remain unaffected by freezing. After dipping, the crystal was removed from LN_2 at which point it would naturally start to warm back up. At all times, the clock signal was measured between `GND` and one of the `OUT` connections shown in Figure 1.

B. Baseline Measurements

Figure 2 shows the spectrogram of the quartz crystal at room temperature. All the spectrogram figures are screen-captures

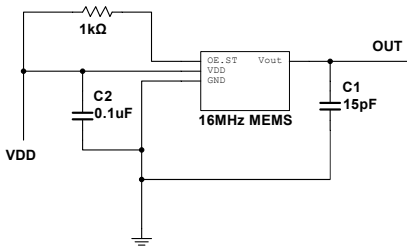

Fig. 4. Example schematic of a 16 MHz MEMS-based oscillator used in the experiments

of Tektronix MDO3104 Mixed Domain Oscilloscope, and TPP1000 1 GHz passive probes were used for data acquisition. The circuit was designed to give 16 MHz signal, which is confirmed by the scope reading, and the crystal generates very clean signal when undisturbed.

C. Ultra Freezing Attack Results

Figure 3 shows the spectrogram during and after the attack. An abrupt signal change is detected when the ultra freezing attack begins with the crystals being dipped in LN_2. The signal frequency jumps by about 15-20 kHz. The dipping is finished after 30 s and signal begins to return towards the target frequency, as shown at the end of the spectrogram. The initial abrupt jump can be used, e.g., to generate unstable clock signal that can affect the operation of the device using the clock.

V. Evaluation of MEMS-based Oscillators

In addition to common quartz crystal oscillators such as the Pierce oscillator design, there are oscillators based on Microelectromechanical Systems (MEMS) resonators. MEMS resonators are piezoelectric elements that function as mechanical resonators to generate a constant frequency needed by a clock oscillator circuit. They tend to be significantly smaller than quartz crystals. Some advantages cited for MEMS-based Oscillators include better resilience against vibration and better reliability with respect to temperature variations, compared to quartz crystals. As we find through our evaluation of the ultra freezing attacks in this section, however, our tested devices seem to be much more impacted by the LN_2 ultra freezing compared to the quartz crystals.

In our evaluation, we used 16 MHz MEMS resonators, part number `DSC6011ME2A-016.0000` from Microchip Technology, rated to −20 °C. They were used in an MEMS-based oscillator circuit shown in Figure 4. The circuit was used to generate 16 MHz clock signal. As the MEMS resonator only comes in surface-mount package, the resonator was soldered on a passive adapter board so it can be integrated with the rest of the circuit on a breadboard via jumper wires.

A. Attack Setup

As in quartz crystal experiments, the MEMS resonator was dipped in LN_2 for 30 s. The MEMS resonator were attached to long jumper wires, via the passive adapter board, to allow for dipping of the MEMS resonator, while the rest of the circuit on a breadboard could remain unaffected by the freezing. After dipping, the resonator was removed and allowed to warm up by placing it back on a lab bench at room temperature. The signal was measured between `GND` and `OUT` connections shown in Figure 4.

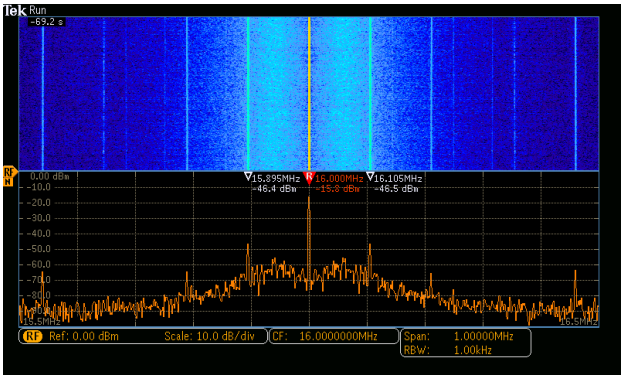

Fig. 5. Spectrogram of the MEMS resonator at room temperature before the attack.

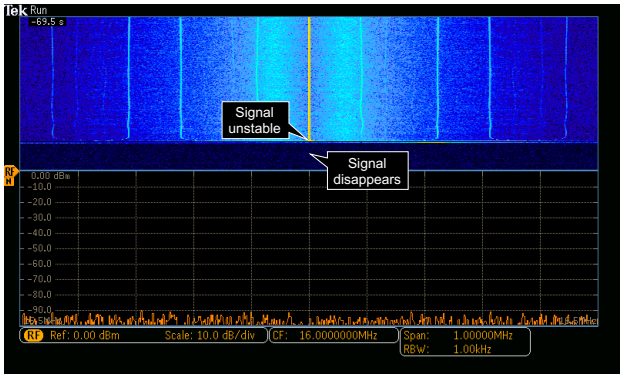

Fig. 6. Spectrogram captured during the dipping experiment when the MEMS resonator is in LN_2, after a few seconds the MEMS resonator stops to generate a signal.

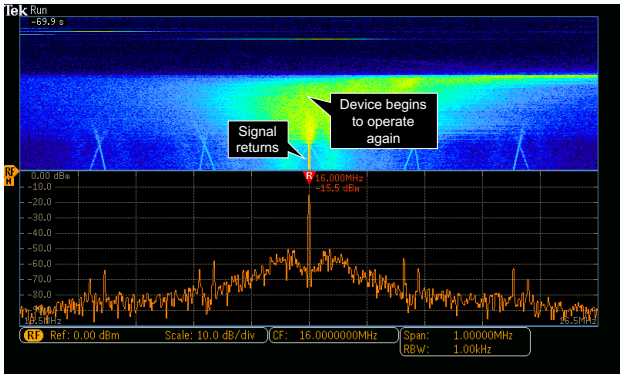

Fig. 7. Spectrogram of the MEMS resonator approximately 2.5 min after dipping, the MEMS resonator begins to generate a signal again as it warms up.

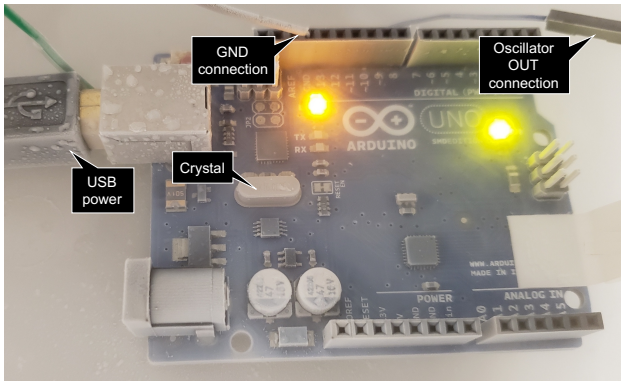

Fig. 8. Effect of pouring LN_2 on the oscillator module and the Arduino UNO board. The white haze is due to frost and fog after LN_2 pouring is stopped and before device warms up.

B. Baseline Measurements

Figure 5 shows the operation of the MEMS-based resonator at room temperature. Interestingly, in addition to the 16 MHz signal, other frequencies also show up, unlike in the quartz crystals, although they are much attenuated compared to the center 16 MHz signal. All measurements are taken using the same Tektronix MDO3104 setup as used for quarts crystals.

C. Ultra Freezing Attack Results

Figure 6 shows the spectrogram captured during the ultra freezing attack as the MEMS were dipped in LN_2. The key feature is that the MEMS actually stops to generate a signal after a few seconds, as can be seen in the spectrogram. We assume the mechanical vibration of the resonator stops as the MEMS is frozen.

Figure 7 shows the spectrogram approximately 2.5 min after dipping is finished. For multiple experiments we observed similar behavior that as the resonator warms up, it begins to oscillate again. While the frequencies were not affected much, the disappearance and reappearance of the signal indicates that the LN_2 ultra freezing attack can be used to generate clock glitches, without need for physical connection to the target device.

VI. Evaluation of Arduino UNO

To demonstrate practical effects of the ultra freezing attacks on computing devices, we first evaluated Arduino UNO SMD Edition board. Arduino UNO is an microcontroller board based on the Microchip ATmega328P chip. It can be used for variety of computing projects, including control and actuation of motors or other peripherals.

A. Crystal Oscillator

The board uses a 16 MHz quartz crystal. The crystal is connected to the `XTAL` ports on the ATmega328P chip, with a resistor and two capacitors located outside the ATmega328P chip to complete a Pierce oscillator circuit. The quartz crystal package is labeled with part number `SPK16.000G`, although specific manufacturer is unclear.

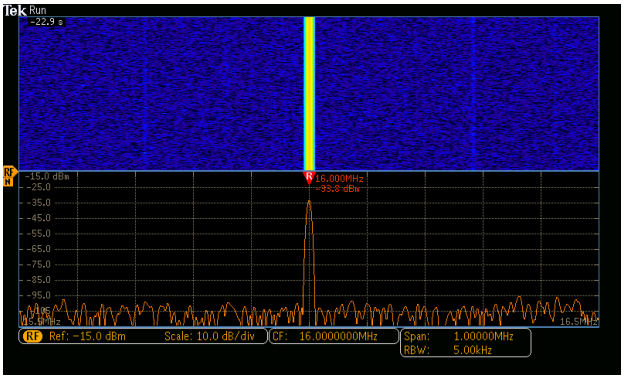

Fig. 9. Spectrogram of crystal oscillator in Arduino UNO at room temperature before attack.

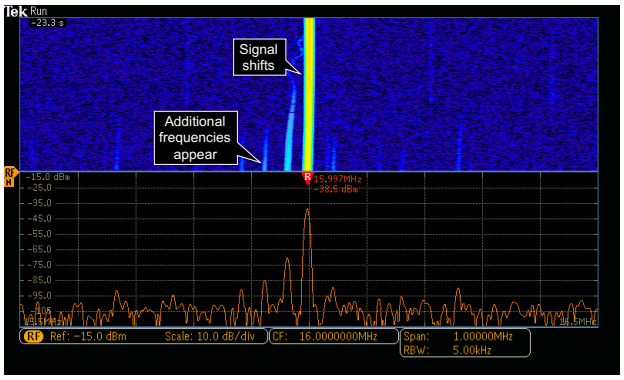

Fig. 10. Spectrogram at the start of the ultra freezing attack on the crystal in Arduino UNO.

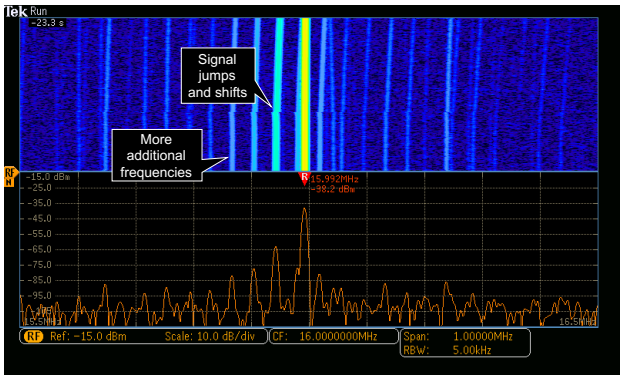

Fig. 11. Spectrogram after pouring of the LN_2 on crystal in Arduino UNO was stopped.

B. Attack Setup

The ultra freezing attacks were performed by pouring LN_2 on the quartz crystal package for approximately 5-10 s. The LN_2 was allowed to splash on other parts of the Arduino board. This was done to simulate a realistic scenario where attacker pours the LN_2 and does not modify the device, e.g., to shield the other parts of the board. Figure 8 shows the Arduino UNO board after the LN_2 pouring was stopped.

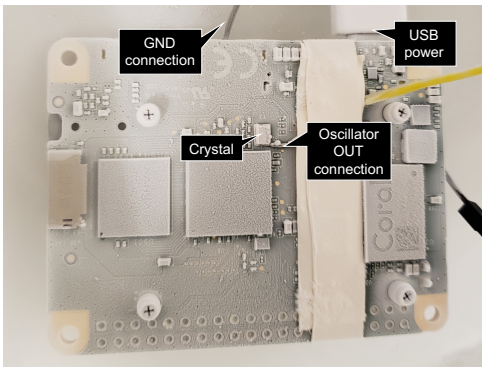

Fig. 12. Effect of pouring LN_2 on the oscillator module and the Edge TPU board. The white haze is due to frost and fog after LN_2 pouring is stopped and before device warms up.

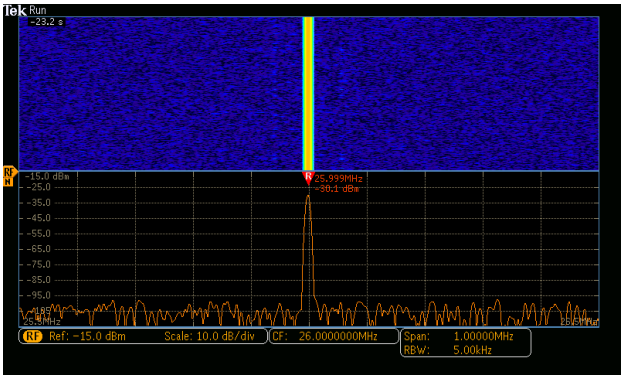

Fig. 13. Spectrogram of Edge TPU's quartz crystal's output at room temperature before attack.

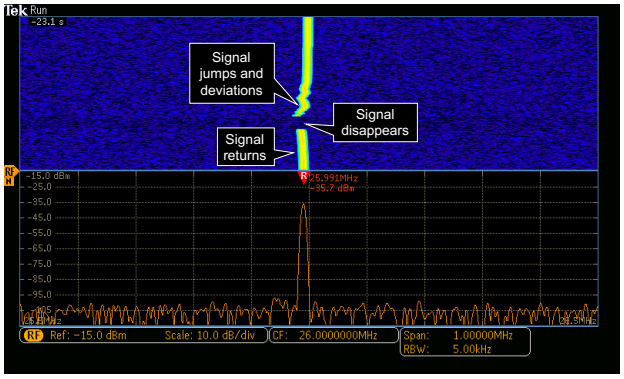

Fig. 14. Spectrogram after start of the ultra freezing attack. The LN_2 pouring was already completed, but freezing effects remain, including a glitch in the clock signal seen when the oscillating signal briefly disappears in the spectrogram.

C. Baseline Measurements

Figure 9 shows the reference measurements of the crystal's output at room temperature. The crystal generated clean signal at $16.000\,\mathrm{MHz}$, as shown by the Tektronix scope, and matching specification of the board.

D. Clock Drift

Figure 10 shows the output of the crystal as the LN_2 was poured. It can be seen that almost immediately the frequency of the crystal starts to shift. The frequency shifts by about $3\,\mathrm{kHz}$, consistent with results from testing discrete oscillators in Section IV. Longer freezing is expected to give even bigger frequency shifts, based on Section IV results.

E. Additional Frequencies

Figure 11 shows the output of the crystal after pouring of LN_2 was concluded. The frequency continued to shift as the crystal cooled even when the liquid nitrogen is no-longer poured. The frequency shifted by up to $10\,\mathrm{kHz}$. In addition, strong signals in other frequencies begun to show up, a number of them above the $-75\,\mathrm{dBm}$, which may be considered the noise floor, and these signals should not be ignored.

F. Return to Normal Operation

After approximately few minutes of heating up, the Arduino UNO returned to normal operation and the frequency of the crystal's output returned to $16\,\mathrm{MHz}$, consistent with results from testing discrete oscillators in Section IV.

VII. Evaluation of Edge TPU

As another demonstration of a practical attack, we experimented with the Google's Edge TPU. The Google's Edge TPU boards are designed for deploying Machine Learning (ML) inference at the edge, and they complement cloud-based ML solutions. By performing ML inference at the edge, communication with centralized cloud servers can be reduced, and devices can use the ML inference results directly. However, if the ML inference operation is interrupted or corrupted, wrong inference results can be generated unbeknown to the centralized cloud servers, and the edge devices can take incorrect actions. In our evaluation we aimed to analyze if clock glitching or other disruptions of the Edge TPU could be generated trough the new ultra freezing attacks.

For our tests, we evaluated the Coral Dev Board Mini, which is a single-board computer that provides ML inference in a small form factor. It includes MediaTek 8167s SoC with quad-core Arm Cortex-A35 and the Google Edge TPU coprocessor as the ML inference accelerator.

A. Crystal Oscillator

The board schematics indicate that it includes a $26\,\mathrm{MHz}$ quartz crystal that is connected to the MediaTek 8167s SoC, which is assumed to include the rest of the crystal oscillator logic. The quartz crystal is packaged in a four-terminal package, but further details are not provided by the manufacturer nor the documentation. The quartz crystal package is labeled with part number `T260`, manufacturer is unspecified, but number of manufacturers make $26\,\mathrm{MHz}$ passive quartz crystals with this label.

B. Attack Setup

Similar to evaluation of the Arduino boards, the ultra freezing attacks were performed by pouring the LN_2 over the

quartz crystal package. The LN_2 was allowed to splash on other parts of the device. After pouring was done, the device was allowed to sit and slowly return to room temperature. Figure 12 shows the Coral Dev Board Mini Edge TPU board after LN_2 pouring was stopped.

C. Baseline Measurements

Figure 13 shows the reference measurements of the crystal's output at room temperature. The Tektronix scope shows a clean signal at $25.999\,\mathrm{MHz}$.

D. Clock Glitching

Figure 14 shows the results of the ultra freezing attack. The LN_2 was poured for about 10-$20\,\mathrm{s}$. Following the pouring we can observe unstable output from the crystal, at times deviating from the specified $26\,\mathrm{MHz}$ by as much as 10-$20\,\mathrm{kHz}$.

More importantly, we also observed clock glitching where the oscillating signal briefly disappears in the spectrogram. As time progressed, further measurements showed repeated glitches which became progressively long and longer. The effect was similar to the glitches in the MEMS-based oscillators tested in Section V, but the glitches were shorter and repeated, as opposed to single, longer disappearance of the signal.

We believe this to be one of first demonstrations of short clock glitching that does not require physical connection to the target device, but can be simply achieved by pouring LN_2 over the device.

E. Board Shutdown and Return to Normal Operation

We further experienced that the crystal oscillator signal eventually disappeared with continued pouring of LN_2 and the Coral Dev Board Mini would no-longer function. However, after leaving the board at room temperature for an extended period of time, the board LEDs turned back on and board begun to function as well. The shutdown of the board can be further evaluated, and points at a possible new type of freezing-based denial-of-service attack.

VIII. Discussion and Defenses

To defend against the new ultra freezing attacks, different possible approaches are discussed below.

A. Passive Defenses

Based on our experience, quartz crystals in physically larger packages are less affected by the freezing. This may be possibly due to air or other gas inside the package acting as an insulator. Consequently, one possible mitigation, but not a full defense, is to use physically larger crystals and packages.

For a same package size, there are also crystals that are rated to different temperatures. Interestingly, given same physical size, different temperature rating does not have much impact when extreme temperatures of LN_2 are considered. We evaluate crystals with different temperature ratings in Section IV, and observed similar results for all.

B. Active Defenses

As an active defense, system temperature sensors can be deployed near critical circuits to detect the ultra freezing attacks. The system detection and response would have to happen within the short time of few seconds, so that defensive action takes place before circuit is frozen. Modern CPUs already include one or multiple thermal diodes, mostly for use with thermal management at high temperatures. These could be leveraged for defending our attacks at low temperatures. However, ultra freezing my affect the sensors themselves. Study of ultra freezing impacts on thermal sensors themselves would need to be evaluated.

In addition to, or instead of, system thermal sensors, temperature compensated crystal oscillators could be used. Temperature compensated crystal oscillators typically use a thermistor network to generate a correction voltage, which reduces the frequency variation over a range of temperatures. The have much better stability, but to best of our knowledge have not been evaluated from security perspective in context of the freezing attacks, nor are they employed in any of the devices we tested. Study of ultra freezing impacts on the thermistor network or the veractor (tuning diodes used in these circuits) and analysis of whether they are able to compensate for the extreme temperatures would need to be evaluated as well.

IX. Conclusion and Future Work

This paper introduced novel ultra freezing attacks on clock oscillator circuits, leveraging LN_2 to rapidly freeze quartz crystal oscillators and MEMS-based oscillators to temperatures approaching $-195\,^{\circ}\mathrm{C}$. In particular, we showed that when LN_2 is applied, the frequencies generated by the oscillator circuits become unstable, drift from their specification, or the oscillators even stop oscillating for a period of time. Future work can extend this first evaluation of LN_2 attacks on clock circuits by evaluating more circuits from different vendors, more complex clock circuits that incorporate phase locked loops, and analyzing how practical attacks on cryptographic circuit could be created using LN_2 freezing.

Acknowledgment

The authors would like to thank Kelly Woods and the Yale University Cleanroom for assistance in obtaining liquid nitrogen used in the experiments.

References

[1] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, "Lest we remember: cold-boot attacks on encryption keys," *Communications of the ACM*, vol. 52, no. 5, pp. 91–98, 2009.

[2] O. N. Jr., J. Morris, I. Giechaskiel, and J. Szefer, "Chill out: Freezing attacks on capacitors and dc/dc converters," in *European Test Symposium (ETS)*, 2021.

[3] T. Müller and M. Spreitzenbarth, "FROST: Forensic recovery of scrambled telephones," in *International Conference on Applied Cryptography and Network Security (ACNS)*, 2013.

[4] S. F. Yitbarek, M. T. Aga, R. Das, and T. Austin, "Cold boot attacks are still hot: Security analysis of memory scramblers in modern processors," in *International Symposium on High Performance Computer Architecture (HPCA)*, 2017.