Design and Implementation of a Negative Voltage Fault Injection Attack Prototype

Christian Kudera[1], Markus Kammerstetter[1,2], Markus Müllner[1,2], Daniel Burian[2], and Wolfgang Kastner[3]

[1] Secure Systems Lab Vienna, Research Division of Automation Systems, Institute of Computer Engineering, TU Wien, Vienna, Austria
{ckudera}@seclab.tuwien.ac.at
[2] Trustworks KG, Vienna, Austria
{m.kammerstetter,m.muellner,d.burian}@trustworks.at
[3] Research Division of Automation Systems, Institute of Computer Engineering, TU Wien, Vienna, Austria
{k}@auto.tuwien.ac.at

***Abstract*—Fault attacks are a well known physical attack type. A common fault injection technique is a short term variation of the supply voltage causing a vulnerable processor to misinterpret or skip instructions. Conventional voltage fault injection attacks thus often pull the supply voltage either to GND or to a low positive voltage. However, with steadily increasing integration depths and device speeds, classical voltage fault injection suffers from increasing capacitive loads and short glitch duration requirements that are no longer feasible when pulling to GND or even to a positive voltage. In this paper, we present negative voltage fault injection attacks as a potential solution to this problem. In contrast to conventional voltage fault injection, negative voltage levels are used to discharge the target with significantly higher slew rates. We explored several design approaches to generate negative voltage glitches. The most promising design has been chosen for a hardware prototype implementation. Our results indicate that negative voltage fault injection enables shorter glitch pulse widths in presence of capacitive loads. We thus believe that our approach is promising for devices with high integration depths.**

I. Introduction

Gartner forecasts that 20.8 billion connected things will be in worldwide use in 2020 [1]. As data in embedded devices is often highly confidential, privacy and security expectations must be met. Furthermore, the highly distributed nature of embedded devices allows malicious attackers to physically access those systems. System implementations thus need to be hardened against physical attacks just the same. Among these attacks, fault attacks are a well known physical attack method. One of the most common fault injection techniques is a short term variation in supply voltage causing a processor to misinterpret or skip instructions [2]. Even though fault attacks have been known for over 15 years, manufacturers of embedded devices often do not consider fault attacks during system development. The first academic fault attack [3] described a number of methods for attacking public key algorithms. A more recent real-world attack was the Xbox360 reset glitch attack [4] in 2012. The focus of the attack was to execute unsigned code to circumvent Microsoft's security concept. In a nutshell, the processor of the console was attacked by sending a short reset pulse that changed the behavior of the `memcmp` function during the bootloader signature verification. In presence of the fault attack, the `memcmp` function returned the incorrect result that there was no difference between the stored and the computed signature. The attack thus circumvented the copy protection of the game console and playing pirated games became possible. The attack was implemented in the form of so called *mod chips* to be useable for everyday consumers. Mod chips are a mass market today.

Ultimately, the necessity of voltage fault injection evaluation tools is twofold: On one side, manufacturers and security evaluation labs need ways to test real-world systems against fault injection attacks. On the other side, independent security researchers can utilize fault injection tools to bypass firmware readout protections on embedded devices. Once the firmware is available to the analyst, it can be tested for security vulnerabilities. While classical voltage fault injection equipment commonly pulls the power rail to GND or to low positive voltages, it is increasingly getting harder to achieve short glitch durations on targets with higher integration depths and capacitive loads. As a result, the discharging during glitch generation takes more time and the achievable minimal glitch duration is longer. We believe that negative voltage fault injection attacks provide advantages in these scenarios. Utilizing negative voltage during the generation of a fault, higher slew rates are expected due to the faster discharging of the circuit implementations. In this paper, we explore and evaluate several design approaches to generate negative voltage glitches. We implemented the most promising design approach to obtain a negative voltage fault injection prototype. Our results indicate that negative voltage fault injection enables shorter glitch pulse widths in presence of capacitive loads. In summary, our contributions are as follows:

- Several fault injection methods are identified and analyzed with regard to their usability for negative voltage fault injection attacks.
- Different approaches and ideas for negative voltage glitch generation are explored and evaluated in simulations.
- Based on the results of these simulations, a hardware prototype for negative voltage fault injection attacks is implemented.
- Utilizing oscilloscope measurements, the prototype is evaluated against the simulation results.

II. Related Work

Recently, two commercial solutions for voltage fault injection attacks have been released: The VC Glitcher [5] including the Glitch Amplifier by Riscure[1] and the ChipWhisperer [6] with the VC Glitch add-on by NewAE Technology Inc.[2]. While the Riscure solution allows negative voltages to some extent, both approaches primarily focus on conventional voltage fault injection attacks.

In 2000, Sergei P. Skorobogatov released a summary [7] of possible attack vectors on common microcontrollers. Even though the summary was released over a decade ago, most of the microcontrollers covered are still in use today. Voltage glitching was one of the described attack vectors, but negative voltage fault attacks are not specifically covered.

In 2006, Bar-El et al. described different fault injection attacks on cryptographic implementations in their paper [2]. However, negative voltage fault attacks are not mentioned in their publication.

In 2014, Carpi et al. published a paper [8] which summarized a novel methodology for choosing multiple parameters required for effective faults on smart cards. Since their search space for the glitch voltage was between -5.0 V and -0.05 V, they handled negative voltage fault injection attacks, but only for low power smart cards and not for microcontrollers or larger controllers in general.

In the same year, Zussa et al. released a paper [9] where they analyzed positive and negative voltage fault attacks on Field Programmable Gate Arrays (FPGAs) with an on-chip voltmeter. Although they used negative voltage to inject the glitch, they didn't compare conventional voltage fault injection attacks against negative voltage fault injection attacks.

III. Notations

In the following, we describe our notations for the voltage levels and time periods:

- Glitch Signal Voltage High ($V_{GS_{High}}$): High logic level of the glitch signal.
- Glitch Signal Voltage Low ($V_{GS_{Low}}$): Low logic level of the glitch signal.
- Glitch Signal Width (GS_{Width}): The time period of the rectangular pulsed glitch signal from the moment it rises from $V_{GS_{Low}}$ until reaching $V_{GS_{Low}}$ again.
- Glitch Signal Rise Time (GS_{Rise}): The time period needed to rise from $V_{GS_{Low}}$ to $V_{GS_{High}}$.
- Glitch Signal Fall Time (GS_{Fall}): The time period needed to fall from $V_{GS_{High}}$ to $V_{GS_{Low}}$.
- Glitch Signal On Time (GS_{On}): The time period how long the rectangular pulsed glitch signal is at $V_{GS_{High}}$.
- Glitch Voltage High ($V_{G_{High}}$): Voltage level when no glitch is inserted. Normally, this voltage is the required power supply line voltage of a target according to its datasheet.
- Glitch Voltage Low ($V_{G_{Low}}$): The lowest voltage level of an inserted glitch.
- Glitch Offset (G_{Offset}): The time period between the moment the glitch signal rises from $V_{GS_{Low}}$ to the moment the voltage level of the power supply line voltage falls from $V_{G_{High}}$.
- Glitch Width (G_{Width}): The time period of the inserted glitch from the moment the voltage falls from $V_{G_{High}}$ until the moment it reaches $V_{G_{High}}$ again.
- Glitch Fall Time (G_{Fall}): The time period needed to fall from $V_{G_{High}}$ to $V_{G_{Low}}$.
- Glitch Rise Time (G_{Rise}): The time period needed to rise from $V_{G_{Low}}$ to $V_{G_{High}}$.

[1]https://www.riscure.com

[2]https://newae.com/

IV. Hardware Requirements

The most important requirement is to increase the slew rate and thus to minimize the glitch fall time (G_{Fall}) as well as the glitch rise time (G_{Rise}). Another important requirement is that the glitch width (G_{Width}) needs to be controlled via the glitch signal width (GS_{Width}). The glitch width (G_{Width}) should be variably selectable. It should be at least 31.25 ns long so that microcontrollers up to 32 MHz can be tested. Furthermore, it should be possible to insert a series of glitches in short intervals. The glitch voltage high ($V_{G_{High}}$) should be 3.3 V, which is the default power supply voltage for modern microcontrollers [10]. The glitch voltage low ($V_{G_{Low}}$) should be variably selectable between 0.0 V and -6.0 V. The incoming logical glitch trigger signal has a low level ($V_{GS_{Low}}$) of 0.0 V and a high level ($V_{GS_{High}}$) of 3.3 V. The hardware has to be able to interpret this signal correctly.

V. Design Approaches

A. Design Approach 1: NMOS-PMOS Circuit

The idea of the first approach is to switch between two voltage sources. The first one provides the operating voltage required by the target. The second one can be arbitrarily adjusted between -6.0 V and 0.0 V. To insert a glitch, the power source is switched from the first one to the second one for an arbitrary amount of time. Fig. 1 illustrates this design approach. An n-type and a p-type metal–oxide–semiconductor field-effect transistor (MOSFET), hereinafter described as NMOS and PMOS, are used to switch between the two voltage sources. As long as no glitch is injected, the NMOS isn't active and the PMOS provides the operating supply voltage. If a glitch is injected into the supply voltage, the PMOS is switched off and the NMOS is switched on to inject the glitch. MOSFET drivers are used to produce high-current drive input for the gates to ensure high slew rates [11].

For the transistors, the Infineon BSD235C [12] type is used. It provides a rise time of 5.0 ns for the PMOS and a rise time of 3.6 ns for the NMOS. The Linear Technology LTC1693-5 [13] and LTC1693-3 [14] are used as PMOS and NMOS drivers, respectively. As illustrated, both drivers have different pins. The pin IN (Pin 1) is a driver input independent from V_{CC}. The glitch signal is connected to this pin. The V_{CC} pin (Pin 8) is the power supply input. It must be between 4.5 V

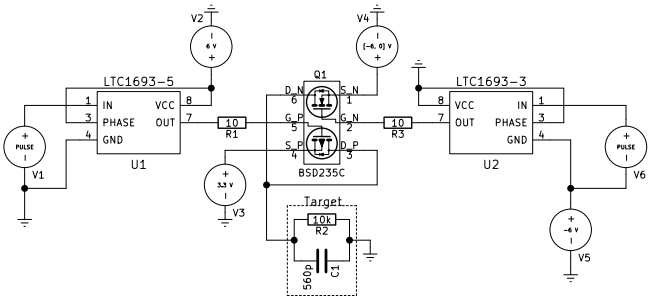

Fig. 1. NMOS-PMOS Circuit for the First Design Approach.

and 13.2 V. The output pin (Pin 7) is the driver output. When the logic signal is low, the voltage at the output is equal to the GND voltage. If the logic signal is high, the voltage at the output is equal to the V_{CC} voltage. Since the PHASE pin (Pin 3) is not used, it is connected to the V_{CC} pin as recommended in the datasheet. The current between the MOSFET drivers and the transistor gates is limited by the resistors R_1 and R_3 to protect the gates.

In n-type MOSFETs, the current between drain and source can only flow if the voltage U_{GS} between gate and source is positive and higher as the threshold U_{TH} ($U_{TH} > 0V$). In p-type MOSFETs, if the voltage U_{GS} between gate and source is negative and lower as the threshold U_{TH} ($U_{TH} < 0V$), current can flow from source to drain. According to the datasheet, the threshold U_{TH} for the NMOS is 0.95 V and for the PMOS it is -0.9 V. In the following, the boundary values for this design approach are calculated to check if the approach is technically feasible.

The terms $U_{GS_{Low}}$ and $U_{GS_{High}}$ are used below. $U_{GS_{Low}}$ is the gate source voltage of a MOSFET if no glitch is injected, and $U_{GS_{High}}$ is the gate source voltage of a MOSFET if a glitch is injected.

For the PMOS, the cases of an active and non-active glitch signal need to be considered where 3.3 V is applied at their respective source inputs. Since $U_{GS_{Low}}$ is negative ($U_{GS_{Low}} = 0 - 3.3 = -3.3$ V) and lower as the threshold U_{TH} (-3.3 V $<$ -0.9 V), the PMOS is active and the target is supplied with the voltage from power supply V_3. In comparison, $U_{GS_{High}}$ is positive ($U_{GS_{High}} = 6 - 3.3 = 2.7$ V) and therefore the PMOS is not active if a glitch is injected. The PMOS would thus work as expected.

Since the voltage of the negative voltage source can be between -6.0 V and 0.0 V, there are two scenarios that need to be analyzed individually. For both scenarios, the case of an active and non-active glitch signal needs to be considered. First, we observe the case where -6.0 V is applied at the source of the MOSFET. Since $U_{GS_{Low}} = -6.0 - -6.0 = 0.0$ V is lower as the threshold U_{TH} (0.0 V $<$ 0.95 V), the NMOS is not active. In comparison, $U_{GS_{High}}$ is positive ($U_{GS_{High}} = 0 - -6.0 = 6.0$ V) and higher as the threshold U_{TH} (6.0 V $>$ 0.95 V). As a consequence if a glitch is injected, the NMOS is active and provides the voltage of the negative voltage supply to the target.

In our second case, 0.0 V is applied at the source of the MOSFET. Since $U_{GS_{Low}}$ is negative ($U_{GS_{Low}} = -6.0 - 0.0 = -6.0$ V), the NMOS is not active if no glitch is injected. However, $U_{GS_{High}}$ is positive ($U_{GS_{High}} = 0 - 0.0 = 0.0$ V) and lower as the threshold U_{TH} (0.0 V $<$ 0.95 V). As a result, the NMOS is not active if a glitch is injected. The target would thus float since it is neither supplied with the positive nor with the negative voltage source. In order for the MOSFET to be active, in this scenario the voltage at the source would at least have to be at a lower voltage as $-U_{TH}$. However, this violates the requirement of a variable negative voltage source between -6.0 V and 0.0 V as defined in section Section IV. The design approach is thus not feasible.

B. Design Approach 2: NMOS Circuit

Similarly to the previous approach, the general idea of this approach is to switch between two voltage sources. The first supply provides the operating voltage required by the target. The second voltage can be arbitrarily adjusted between -6.0 V and 0.0 V. To insert a glitch, the power source is switched from the first one to the second one for an arbitrary amount of time. Fig. 2 illustrates the design approach.

Instead of a p-type and an n-type MOSFET, this design uses two identical n-type MOSFETs IRF7821 [15]. As long as no glitch is injected, NMOS Q_1 is active and NMOS Q_2 is inactive. As a consequence, the voltage source V_6 provides 3.3 V to the target. If a glitch is injected, NMOS Q_1 is inactive and NMOS Q_2 is active. The active NMOS thus connects the negative voltage source V_5 to the target. This MOSFET switching behavior is achieved by the LM5134 [16] MOSFET drivers U_1 and U_2. They are equipped with a noninverting and inverting signal input. If the input signal is applied to the IN pin while the INB Pin is connected to V_{SS}, the OUT pin is low if no glitch is inserted and high if a glitch is inserted. In contrast, when the input signal is applied to the INB pin while the IN pin is connected to V_{DD}, the OUT pin is high if no glitch is inserted and low if a glitch is inserted. To achieve high slew rates, the output (OUT pin) high signal of the the drivers U_1 and U_2 is equal to 12.0 V relative to the GND of the drivers. Since the applied voltage at the source of NMOS Q_2 must be arbitrary selectable and the GND of MOSFET driver U_2 is connected to the source of NMOS Q_2, the GND of the driver U_2 is shifted to the voltage level of the negative voltage source V_5. The current between the MOSFET drivers and the transistor gates is limited by the resistors R_1 and R_2 to protect the gates.

According to the IRF7821 datasheet [15], the threshold U_{TH} is 1.0 V. In the following, the boundary values for this design approach are calculated to determine if the approach is feasible in practice.

First, we consider the case where no glitch is injected. In this case, the output of the driver U_1 is 12.0 V and U_2 is 0.0 V relative to V_5. For Q_1, $U_{GS_{Low}} = 12.0 - 3.3 = 8.7$ V is always positive and higher as the threshold U_{TH}. For Q_2: If V_5 is -6.0 V $U_{GS_{Low}} = -6.0 - -6.0 = 0.0$ V. In the other case, if V_5 is 0.0 V, $U_{GS_{Low}} = 0.0 - 0.0 = 0.0$ V. $U_{GS_{Low}}$ is for

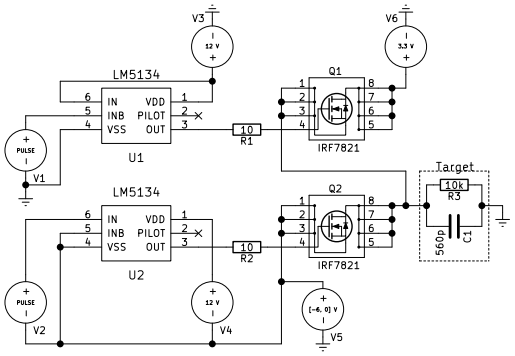

Fig. 2. NMOS Circuit for the Second Design Approach.

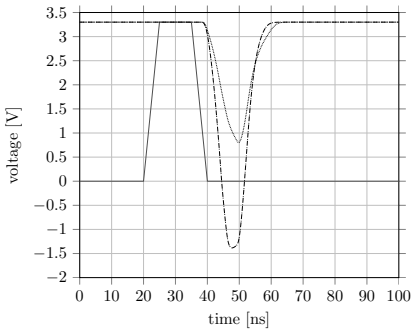

Fig. 3. NMOS Design Approach Simulation: Glitch Signal (solid), Simulation A (dotted) and Simulation B (dot-dashed)

both cases 0.0 V, since the gate driver voltage is referenced to source instead of GND. As a result, Q_2 is not active and Q_1 is active, supplying the target with 3.3 V.

Second, we consider the case where a glitch is injected. In this case, the output of the driver U_1 is 0.0 V and U_2 is 12.0 V relative to V_5. We assume the voltage on source Q_1 is 3.3 V. Since $U_{GS_{High}} = 0.0 - 3.3 = -3.3$ V is negative and lower as the treshhold U_{TH}, Q_1 is not active. For Q_2: If V_5 is -6.0 V, $U_{GS_{High}} = 6.0 - -6.0 = 12.0$ V. In the other case, if V_5 is 0.0 V $U_{GS_{High}} = 12.0 - 0.0 = 12.0$ V. $U_{GS_{High}}$ is for both cases 12.0 V since the gate driver voltage is referenced to source instead of GND. As a result, Q_2 is active, pulling the target to the negative voltage source V_5. From the theoretical view, the design approach would thus work as expected.

To test the behavior of the design approach and to measure the peak currents, we conducted SPICE (Simulation Program with Integrated Circuit Emphasis) simulations A and B. Table I provides an overview of the used components and their values. In both simulations, the same values and components are used. The only exception is that Simulation A is simulated with a negative supply voltage level (V_5) of 0.0 V, while Simulation B uses a negative supply voltage level (V_5) of -6.0 V. The results of the simulations are visible in Fig. 3. The solid waveform represents the glitch signal for both simulations, the dotted waveform shows the result of Simulation A and the dot-dashed waveform illustrates the result of Simulation B. As in previous simulations, the target is simulated with a 10 kΩ resistor R_3 and a 560 pF capacitor C_1 in parallel.

For both simulations, the measured currents are within the maximum ratings specified in the IRF7821 datasheet [15]. In the following, the results of Simulation A are described. The glitch offset (G_{Offset}) (i.e. the time period between the moment the glitch signal rises from $V_{GS_{Low}}$ and the moment the voltage level of the power supply line voltage falls from $V_{G_{High}}$) is 18.76 ns. After 11.09 ns, a $V_{GS_{Low}}$ voltage drop to 0.79 V is achieved. The short time of 10 ns GS_{On} is not sufficient to reach the negative supply voltage level V_5. Thereafter, the supply voltage is pulled to $V_{G_{High}}$ within 13.31 ns. This results in a glitch width (G_{Width}) of 24.40 ns. In contrast, the following values can be measured for Simulation B: As in Simulation A, the glitch offset(G_{Offset}) is 18.76 ns. For the glitch fall time (G_{Fall}), a value of 9.19 ns can be measured. The glitch rise time (G_{Rise}) is 13.62 ns. This results in a glitch width (G_{Width}) of 22.81 ns. The glitch voltage low ($V_{G_{Low}}$) is -1.37 V due to the glitch signal on time (GS_{On}) of 10 ns being too short to reach the negative power supply voltage level V_5 of -6.0 V.

In summary, the two simulations show that the second design approach works as expected and that the hardware requirements specified in Section IV can be fulfilled.

VI. Implementation of Prototype

Fig. 4 illustrates the prototype implementation. The glitch signal is inserted externally via an SMA connector. The ADuM1100 [17] digital isolators U_1 and U_2 are used to shift the logic level of the glitch signal to the level required by the MOSFET drivers. The isolators transfer the incoming logic signal IN with the voltage level VDD_1 to the outgoing logic signal OUT with the voltage level VDD_2. Since the incoming glitch signal is equal to 3.3 V, the voltage supply VDD_1 must also be 3.3 V. This voltage is provided by the signal +3.3V_isolated, which is generated by a linear voltage regulator. In fact, only the isolator U_2 would be necessary since the glitch signal for the MOSFET driver of the MOSFET Q_1 does not have to be transferred. However, the glitch signal must arrive at both drivers as concurrently as possible. To achieve a close to equal delay, isolator U_1 is necessary. For this reason, the voltage V_ADUM is 3.3 V. For the MOSFET driver of MOSFET Q_2, the glitch signal must be transferred to 3.3 volts relative to GNDA. This is achieved with the voltage V_ADUM_REL provided to VDD_2 of isolator U_2. GNDA

TABLE I
VALUES USED FOR THE SECOND DESIGN APPROACH SIMULATIONS

Component	Simulation A	Simulation B
Power supply voltage level V_6	3.3 V	3.3 V
Negative supply voltage level V_5	0.0 V	-6.0 V
Glitch signal voltage level high	3.3 V	3.3 V
Glitch signal voltage level low	0.0 V	0.0 V
Glitch signal turn on time	20 ns	20 ns
Glitch signal rise time	5 ns	5 ns
Glitch signal fall time	5 ns	5 ns
Glitch signal on time	10 ns	10 ns

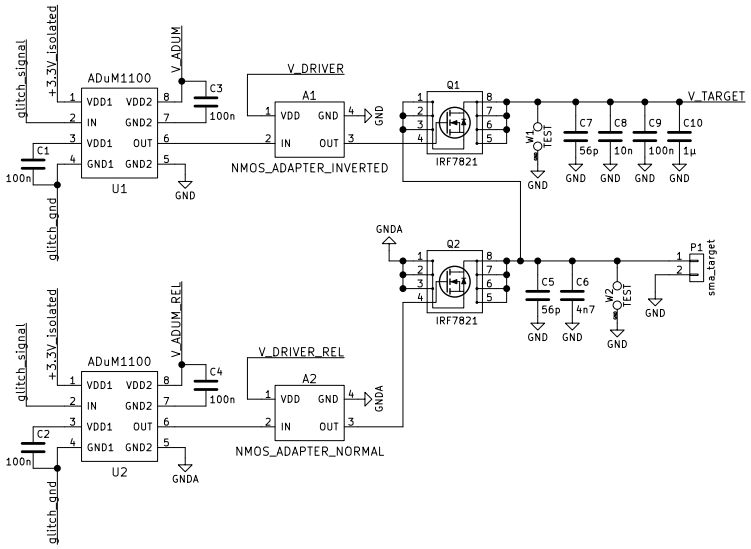

Fig. 4. Schematic of the Prototype

can be adjusted between -6.0 V and 0.0 V by means of a potentiometer. The requirement of the arbitrary negative voltage source (see Section IV) is thus achieved. The capacitors C_1, C_2, C_3 and C_4 with a capacitance of 100 nF are used as recommended by the data sheet [17]. The driver U_3 is powered by the supply voltage V_DRIVER. The decoupling capacitors C_5, C_7, C_9, and C_{11} ensure a stabilization of the voltage. The glitch signal, which is already shifted to the required logic level, is inserted at input INB. As a result, if the level of the glitch signal is low (e.g., no glitch is injected), the output (OUT) is equal to V_DRIVER. If the level of the glitch signal is high (e.g., a glitch is injected), the output (OUT) is equal to GND. The current between the driver U_3 and the MOSFET gate is limited by the resistor R_1 to protect the gate. The driver U_4 is powered by the supply voltage V_DRIVER_REL. The decoupling capacitors C_6, C_8, C_{10}, and C_{12} ensure a stabilization of the voltage. The glitch signal, which is already shifted to the required logic level, is inserted at input IN. As a result, if the level of the glitch signal is low (e.g., no glitch is injected), the output (OUT) is equal to GNDA. If the level of the glitch signal is high (e.g., a glitch is injected), the output (OUT) is equal to V_DRIVER_REL. Similarly to the inverted adapter, the current between the driver U_4 and the MOSFET gate is limited by the resistor R_2 to protect the gate. The two NMOS Q_1 and Q_2 are alternately active and supply the target through the SMA connector sma_target (P_1). The target is thus supplied either with 3.3 V (V_TARGET) or with a negative voltage between -6.0 V and 0.0 V (GNDA). In contrast to the second design approach (Section V-B), for the prototype the decoupling capacitors C_{13-18} are used to prevent ringing on the supply voltage of the target at the moment a glitch is inserted. The values for the decoupling capacitors were chosen according to best practice recommendations [18]. To test the prototype, test points W_1 and W_2 are provided with a special mount for the probes of an oscilloscope.

We designed the printed circuit boards for the prototype and the adapters with KiCad, a well known electronic computer-aided design (ECAD) suite. The final prototype can be seen in Fig. 5.

VII. Evaluation of Prototype

To verify the functionality of the prototype, we used the test setup illustrated in Fig. 6. A signal generator generates a pulsed signal with a GS_{Rise} time of 5 ns, a GS_{On} time of 10 ns and a GS_{Fall} time of 5 ns. This signal is used as reference glitch trigger signal and it is thus connected to the glitch signal input of the prototype. The output of the prototype

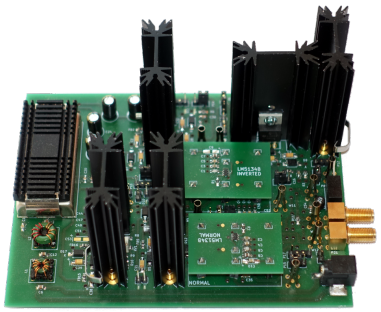

Fig. 5. Image of the Final Prototype

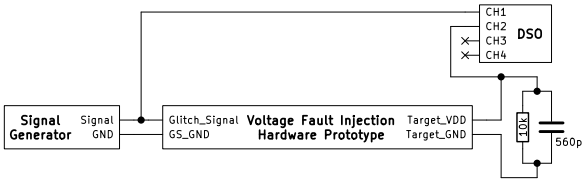

Fig. 6. Prototype Evaluation Test Setup

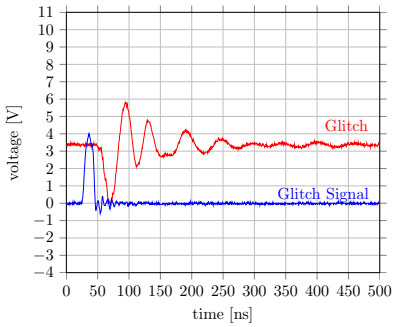

Fig. 7. Result of the Protoype Test with a GNDA of 0.0 V

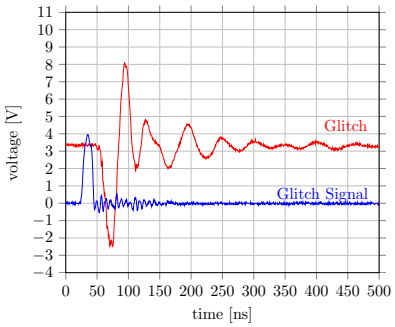

Fig. 8. Result of the Protoype Test with a GNDA of -6.0 V

is connected to a resistor and a capacitor in parallel. To check the behavior of the prototype, the glitch signal and the output of the prototype are connected to a digital storage oscilloscope. Fig. 7 illustrates the result of the prototype test with a GNDA of 0.0 V. The blue waveform shows the glitch signal generated by the signal generator. The glitch signal width (GS_{Width}) is about 20 ns. The red waveform shows the output of the prototype with the injected glitch. The glitch reaches a $V_{G_{Low}}$ of 0.0 V.

Fig. 8 illustrates the result of the prototype test with a GNDA of -6.0 V. The glitch signal width (GS_{Width}) is about 20 ns. The glitch width (G_{Width}) is about 30 ns. The glitch reaches a $V_{G_{Low}}$ of -2.5 V.

The results of the prototype test are comparable to the results of simulations A and B. Therefore, we can derive that the prototype fulfills the requirements specified in Section IV.

VIII. Conclusion and Future Work

In this paper, we formulated the hypothesis that negative voltage fault injections have advantages over their conventional counterparts. In a first step, we compared different fault injection setups and analyzed their usability for negative voltage fault injection. On the basis of our comparision, we specified hardware requirements for a negative voltage fault injection attack prototype. Overall, we explored two approaches for negative voltage glitch generation and simulated the most promising one with detailed SPICE simulations. Based on the simulation results, we implemented a hardware prototype that has been evaluated against the simulation results. Our evaluation showed that the hardware prototype adhered to the SPICE simulation results. In future work, we plan to compare negative voltage fault injection attacks against conventional voltage fault injection attacks on real world target devices such as microcontrollers.

Acknowledgment

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 646580. The hardware security tests during development were supported by the Trustworks hardware security lab (https://www.trustworks.at).

References

[1] R. van der Meulen, "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015," November 2015, accessed 2 April 2018. [Online]. Available: http://www.gartner.com/newsroom/id/3165317

[2] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, "The Sorcerer's Apprentice Guide to Fault Attacks," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 370–382, 2006.

[3] D. Boneh, R. A. DeMillo, and R. J. Lipton, *On the Importance of Checking Cryptographic Protocols for Faults*. Springer Berlin Heidelberg, 1997.

[4] E. DeBusschere and M. McCambridge, "Modern game console exploitation," University of Arizona, Tech. Rep., 2012.

[5] Riscure, "VC Glitcher Datasheet," accessed 2 April 2018. [Online]. Available: https://www.riscure.com/uploads/2017/07/datasheet_vcglitcher.pdf

[6] C. O'Flynn and Z. D. Chen, *ChipWhisperer: An Open-Source Platform for Hardware Embedded Security Research*. Springer International Publishing, 2014, pp. 243–260.

[7] S. P. Skorobogatov, "Copy Protection in Modern Microcontrollers," University of Cambridge, Tech. Rep., 2000, accessed 2 April 2018. [Online]. Available: http://www.cl.cam.ac.uk/~sps32/mcu_lock.html

[8] R. B. Carpi, S. Picek, L. Batina, F. Menarini, D. Jakobovic, and M. Golub, *Glitch It If You Can: Parameter Search Strategies for Successful Fault Injection*. Springer International Publishing, 2014.

[9] L. Zussa, J. M. Dutertre, J. Clediere, and B. Robisson, "Analysis of the fault injection mechanism related to negative and positive power supply glitches using an on-chip voltmeter," in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, May 2014, pp. 130–135.

[10] JEDEC, "Interface Standard for Nominal 3 V/3.3 V Supply Digital Integrated Circuits," *JESD8C.01*, 2007.

[11] L. Technology, "Micropower High Side MOSFET Drivers," *Application Note 53*, 1993, accessed 2 April 2018. [Online]. Available: http://cds.linear.com/docs/en/application-note/an53.pdf

[12] Infineon, "BSD235C OptiMOS2 + OptiMOS-P 2 Small Signal Transistor," accessed 2 April 2018. [Online]. Available: http://www.infineon.com/

[13] L. Technology, "LTC1693-5 High Speed SingleP-Channel MOSFET Driver Datasheet," accessed 2 April 2018. [Online]. Available: http://cds.linear.com/docs/en/datasheet/16935f.pdf

[14] ——, "LTC1693-3 High Speed Single/DualN-Channel MOSFET Driver Datasheet," accessed 2 April 2018. [Online]. Available: http://cds.linear.com/docs/en/datasheet/1693fa.pdf

[15] Infineon, "IRF7821 N-Channel HEXFET Power MOSFET Datasheet," accessed 2 April 2018. [Online]. Available: http://www.infineon.com/

[16] T. Instruments, "LM5134 Single7.6-A Peak Current Low-SideGate Driver With a PILOT Output," accessed 2 April 2018. [Online]. Available: http://www.ti.com/lit/ds/symlink/lm5134.pdf

[17] Analog Devices, "ADuM 1100 Datasheet," accessed 2 April 2018. [Online]. Available: http://www.analog.com/media/en/technical-documentation/data-sheets/ADUM1100.pdf

[18] P. Horowitz and W. Hill, *The Art of Electronics*. Cambridge University Press, 2015. [Online]. Available: https://books.google.at/books?id=LAiWPwAACAAJ