Bringing Hardware Hacking to Life

Colin O’Flynn – Dalhousie University / NewAE Technology Inc.

HCSS 2015

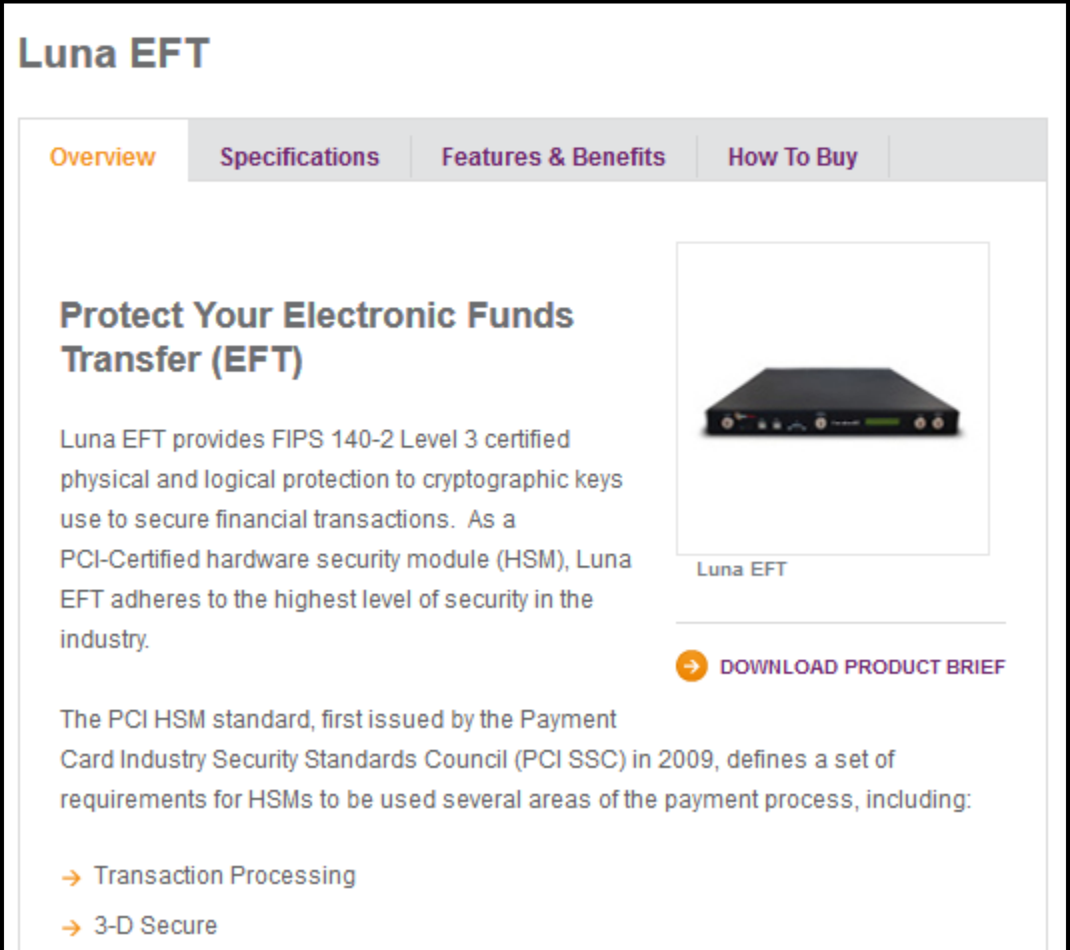
Overview

- Hardware Security?
- Side-Channel Analysis
- Examples of Side-Channel Analysis
- Glitching Attacks
- Examples of Glitching Attacks

About Me

- PhD at Dalhousie University (Ongoing)
- Designed open-source hardware security project (ChipWhisperer), 2nd-place winner of 2014 Hackaday Prize
- Commercialization through NewAE Technology Inc.
- Previously talked at Blackhat US/EU/AD, RECON, Embedded System Conference, etc.

Hardware Security?



Luna EFT

Protect Your Electronic Funds Transfer (EFT)

Luna EFT provides FIPS 140-2 Level 3 certified physical and logical protection to cryptographic keys use to secure financial transactions. As a PCI-Certified hardware security module (HSM), Luna EFT adheres to the highest level of security in the industry.

Luna EFT

The PCI HSM standard, first issued by the Payment Card Industry Security Standards Council (PCI SSC) in 2009, defines a set of requirements for HSMs to be used several areas of the payment process, including:

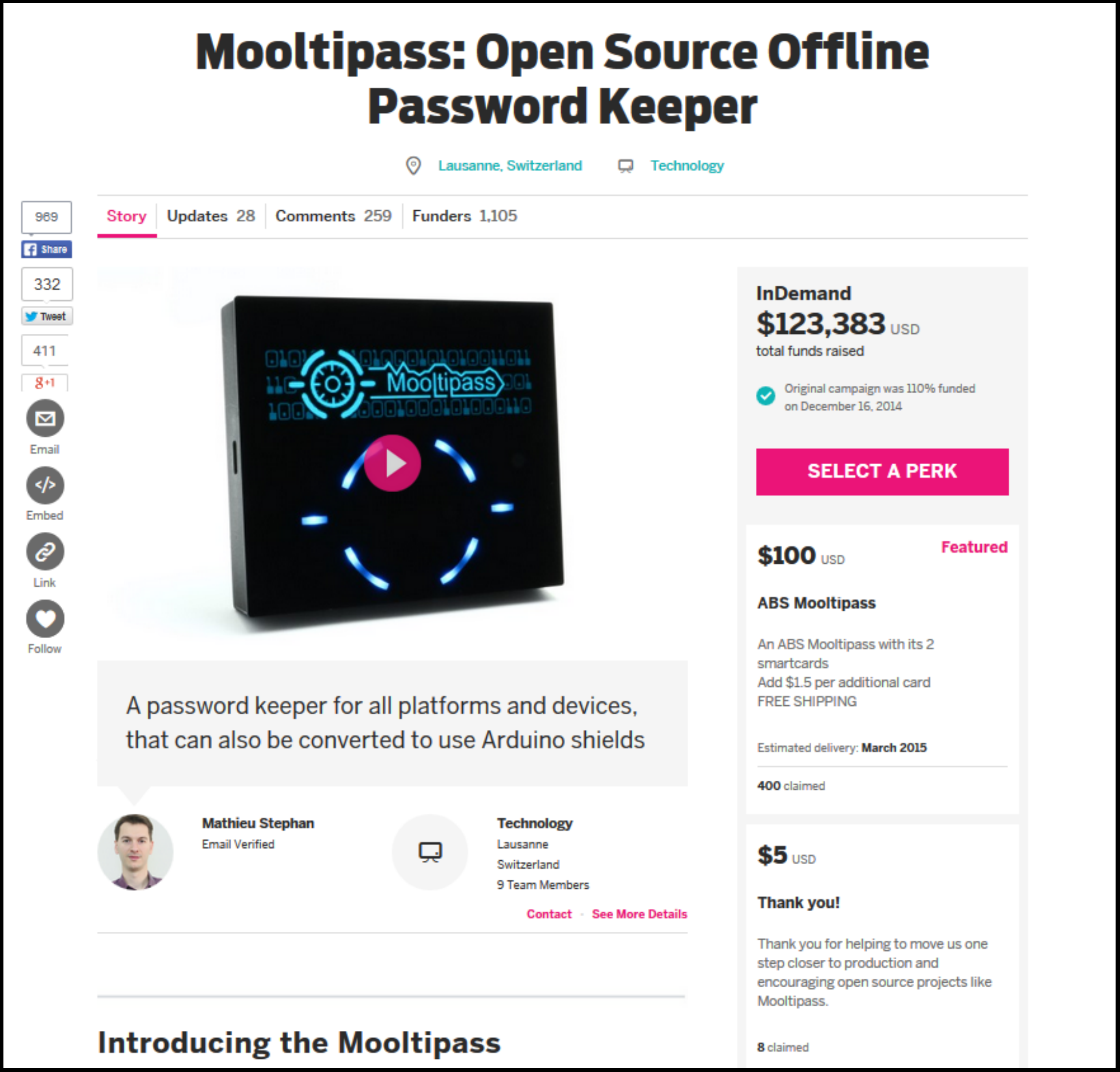
- Transaction Processing
- 3-D Secure

Hardware Security?

Hardware Security?

Hardware Security?

Hardware Security?



Mooltipass: Open Source Offline Password Keeper

Lausanne, Switzerland   Technology

Story | Updates 28 | Comments 259 | Funders 1,105

A password keeper for all platforms and devices, that can also be converted to use Arduino shields

Mathieu Stephan
Email Verified

Technology
Lausanne
Switzerland
9 Team Members

Contact · See More Details

InDemand
$123,383 USD
total funds raised

Original campaign was 110% funded on December 16, 2014

SELECT A PERK

$100 USD   Featured

ABS Mooltipass

An ABS Mooltipass with its 2 smartcards
Add $1.5 per additional card
FREE SHIPPING

Estimated delivery: March 2015

400 claimed

$5 USD

Thank you!

Thank you for helping to move us one step closer to production and encouraging open source projects like Mooltipass.

8 claimed

Introducing the Mooltipass

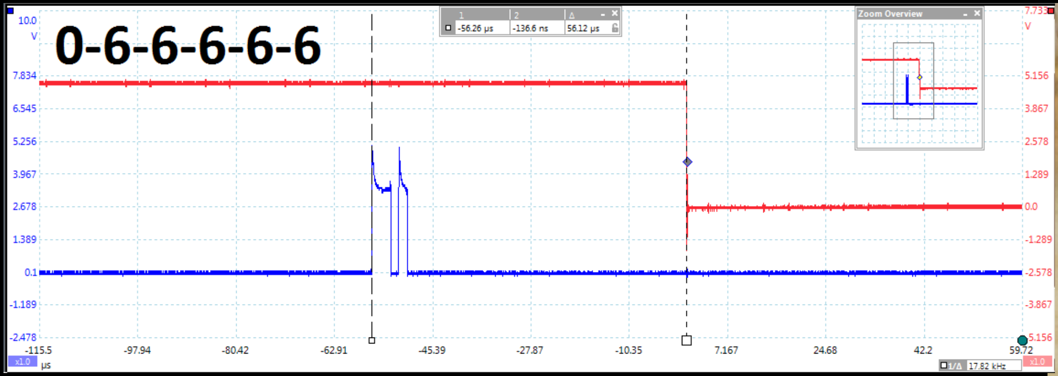
IEEE 802.15.4 Nodes

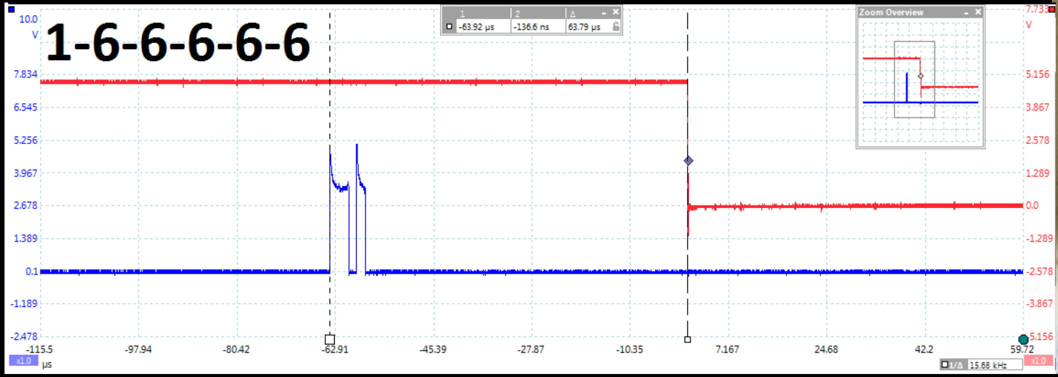
IEEE 802.15.4

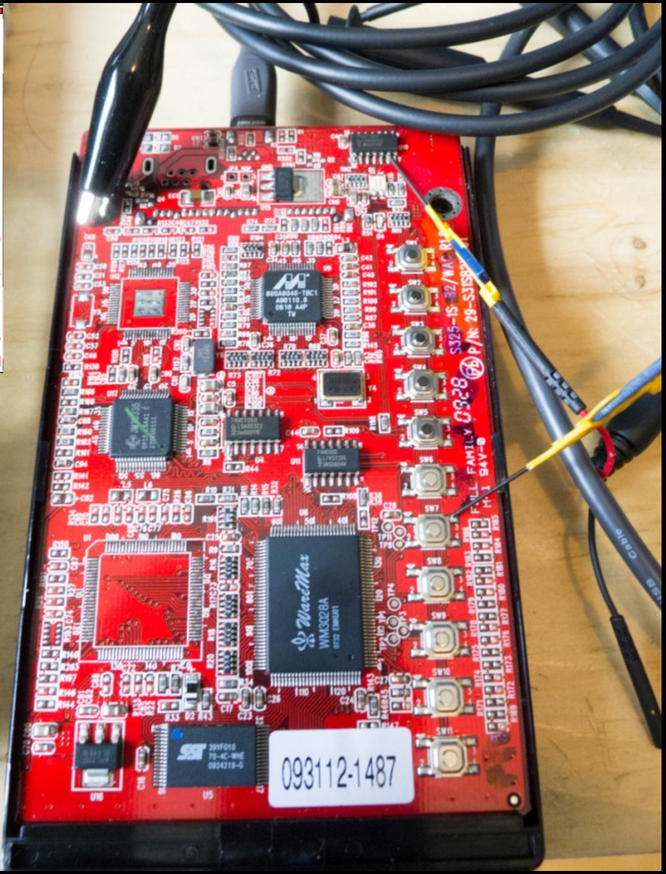
00.178
02
I-210+C
12 345 679
CL 200
240V
3W
FM2S
60HZ
TA 30
12345679

Bluetooth Low Energy

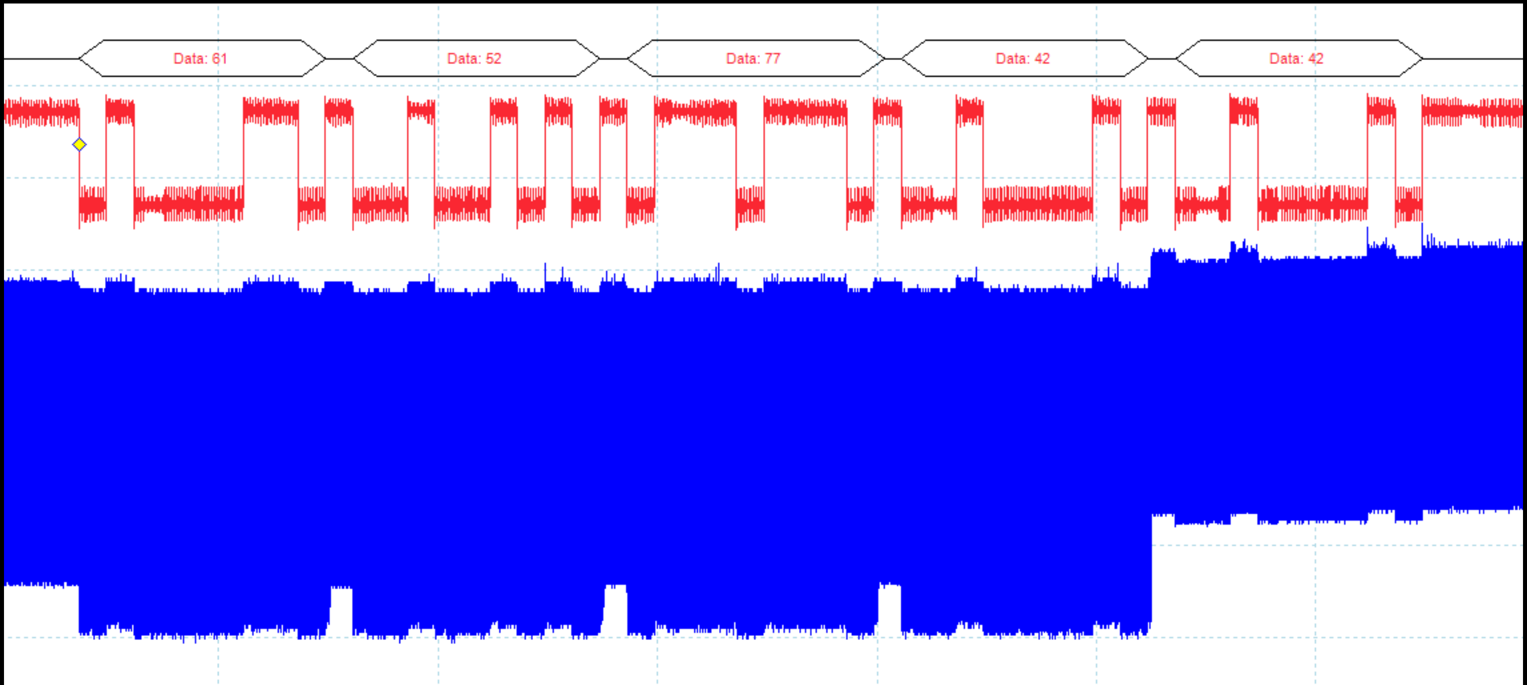
Timing Attacks



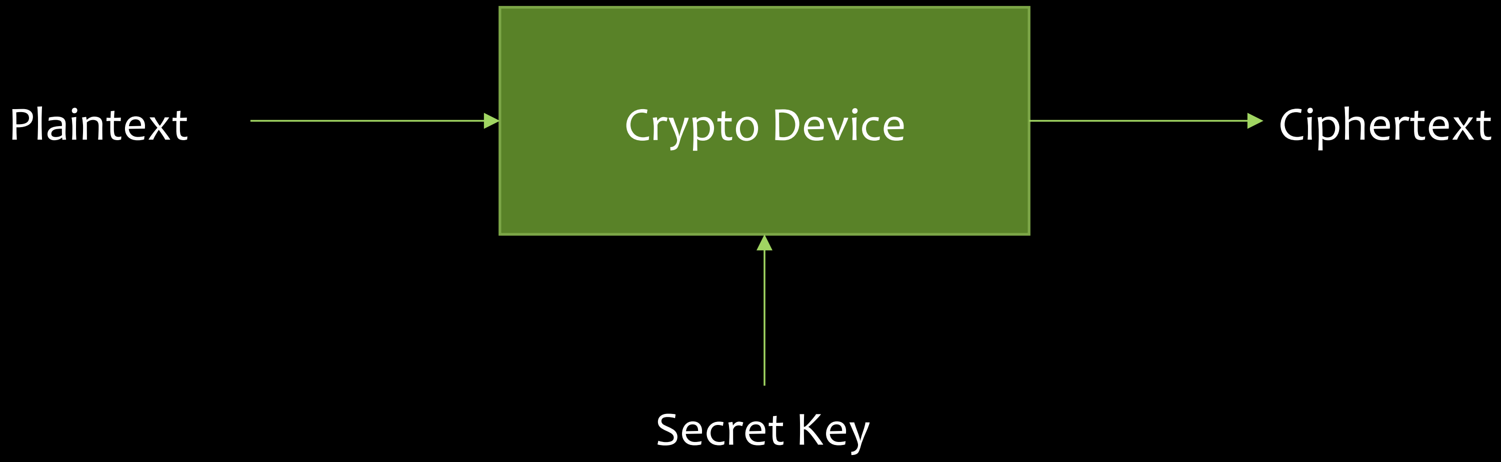




Timing Attacks with Power



Side Channel Power Analysis



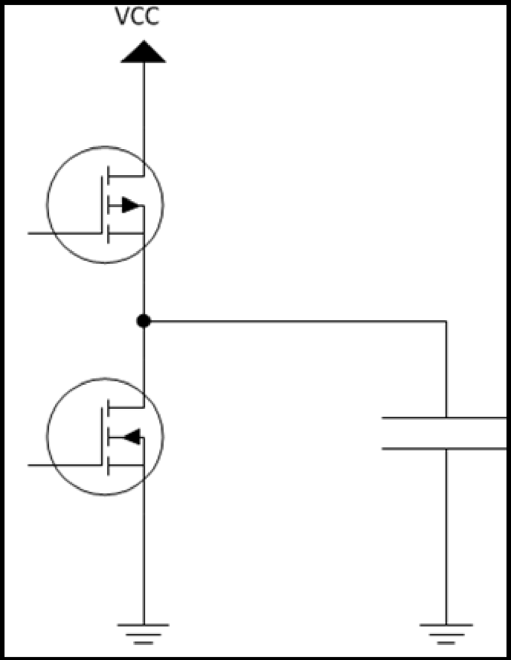
Plaintext

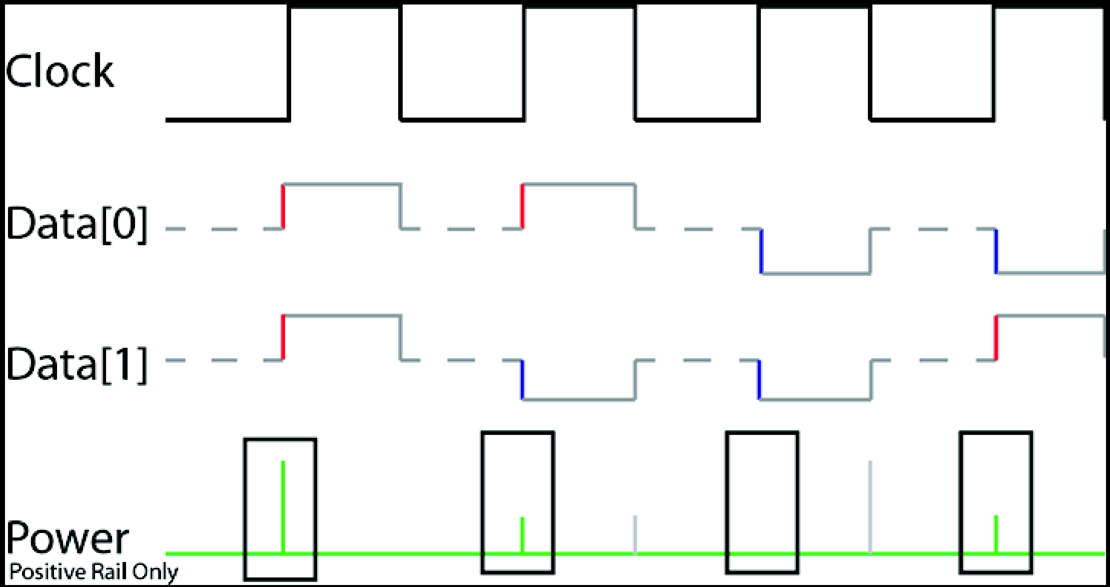
Crypto Device

Ciphertext

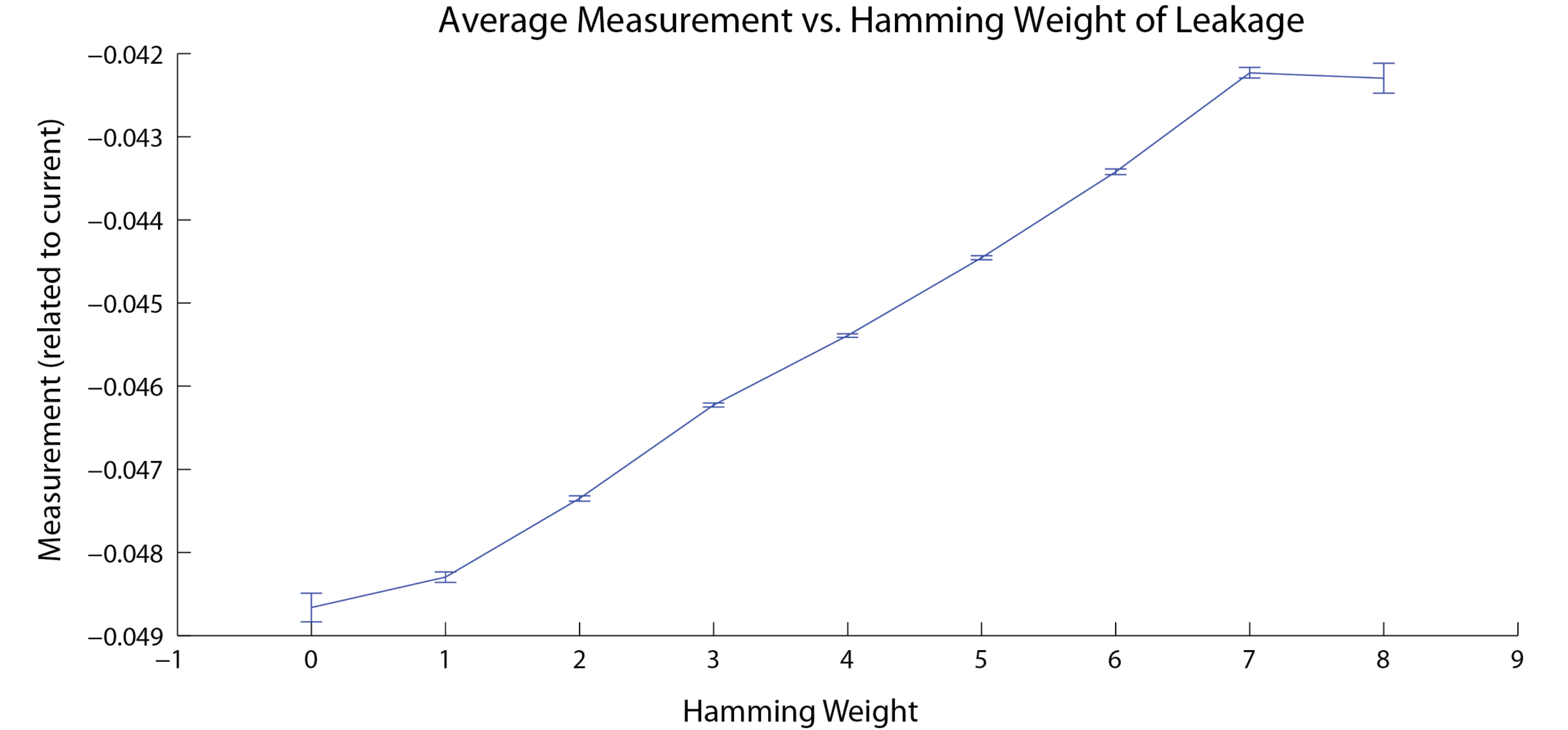
Secret Key

Side Channel Analyis

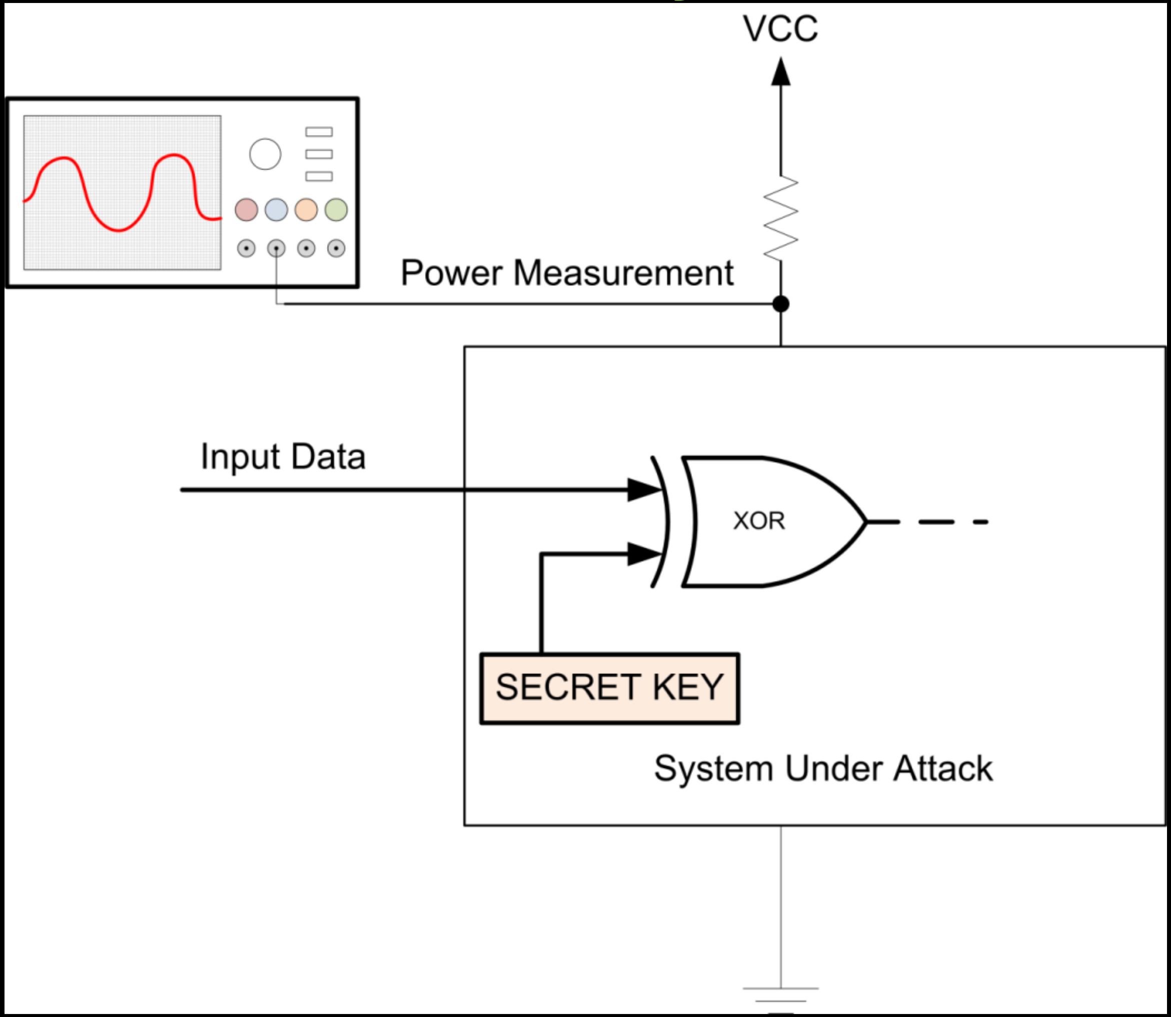




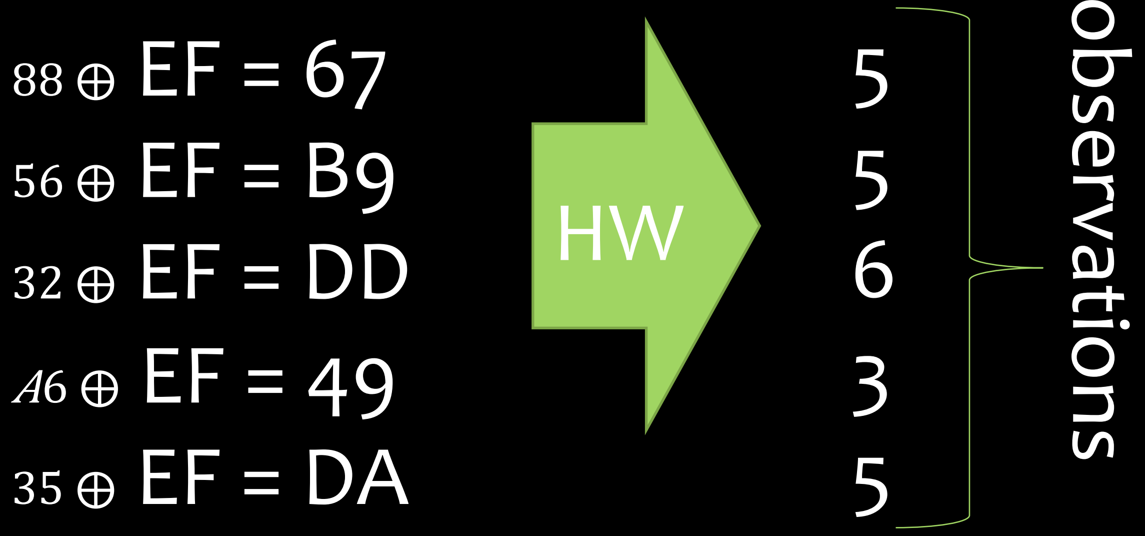
Side Channel Analysis



Measurement System



Assume user is ‘encrypting’ a 1-byte piece of data by XORing with a 1-byte secret key (EF), and we cannot observe output of XOR. This becomes:



$88 \oplus \mathrm{EF} = 67$

$56 \oplus \mathrm{EF} = \mathrm{B9}$

$32 \oplus \mathrm{EF} = \mathrm{DD}$

$A6 \oplus \mathrm{EF} = 49$

$35 \oplus \mathrm{EF} = \mathrm{DA}$

HW

5

5

6

3

5

observations

Masking unknowns…

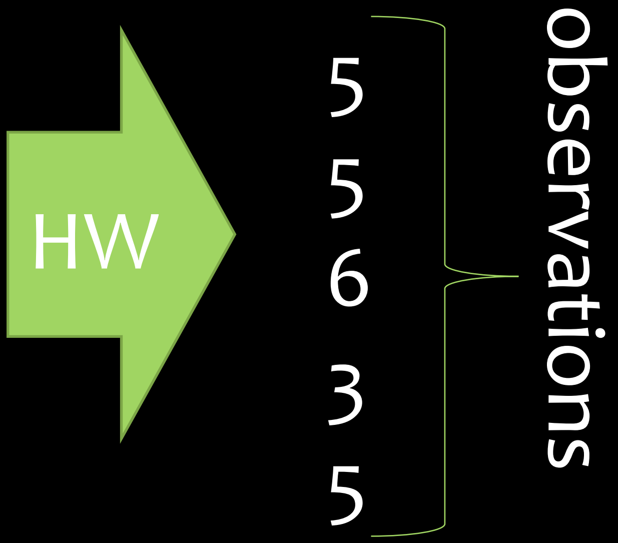
$88 \oplus \mathrm{KK} = ?$

$56 \oplus \mathrm{KK} = ?$

$32 \oplus \mathrm{KK} = ?$

$A6 \oplus \mathrm{KK} = ?$

$35 \oplus \mathrm{KK} = ?$



Guess KK = 0x00

$88 \oplus 00 = 88$

$56 \oplus 00 = 56$

$32 \oplus 00 = 32$

$A6 \oplus 00 = A6$

$35 \oplus 00 = 35$

2

4

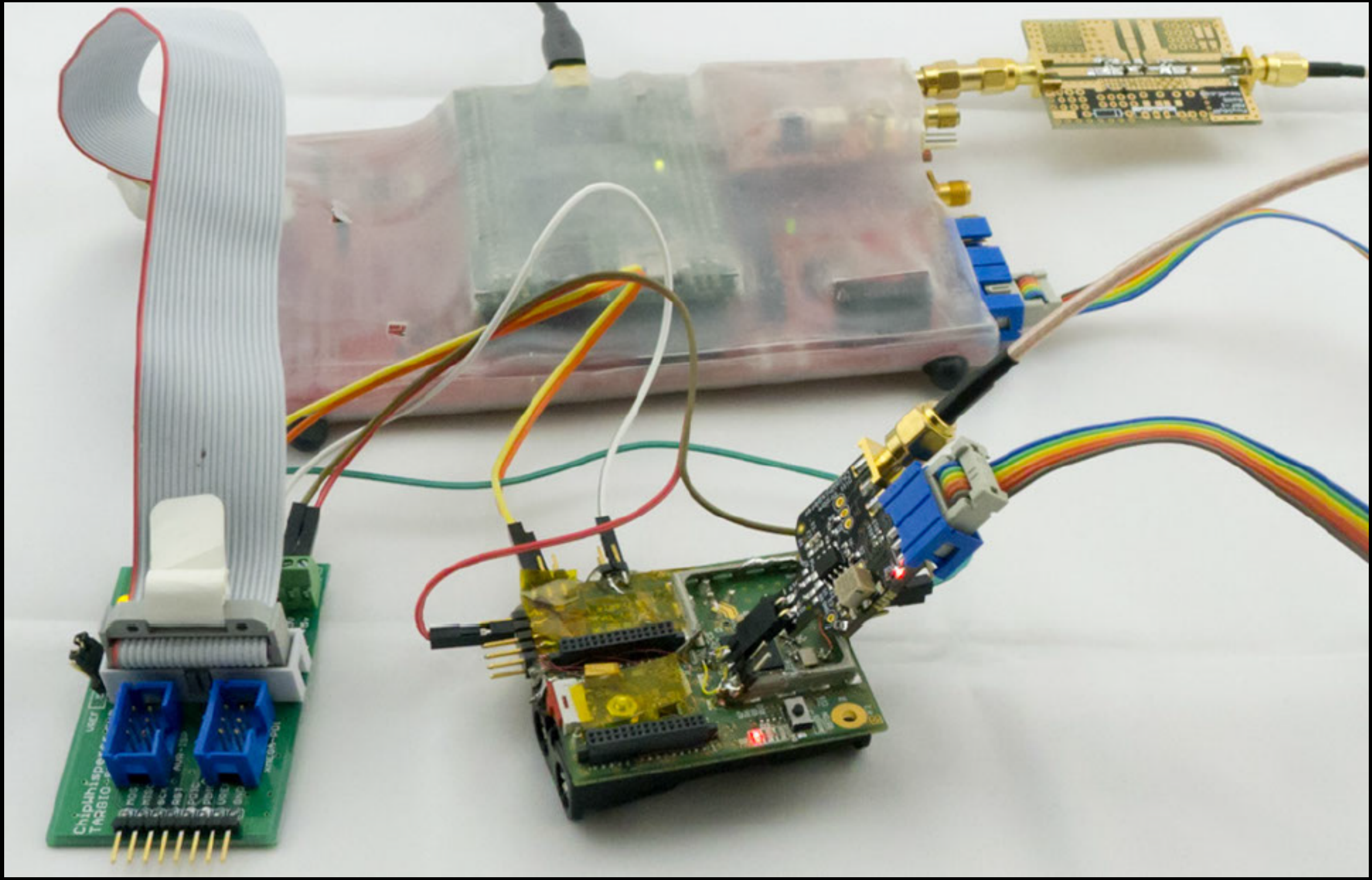
3

4

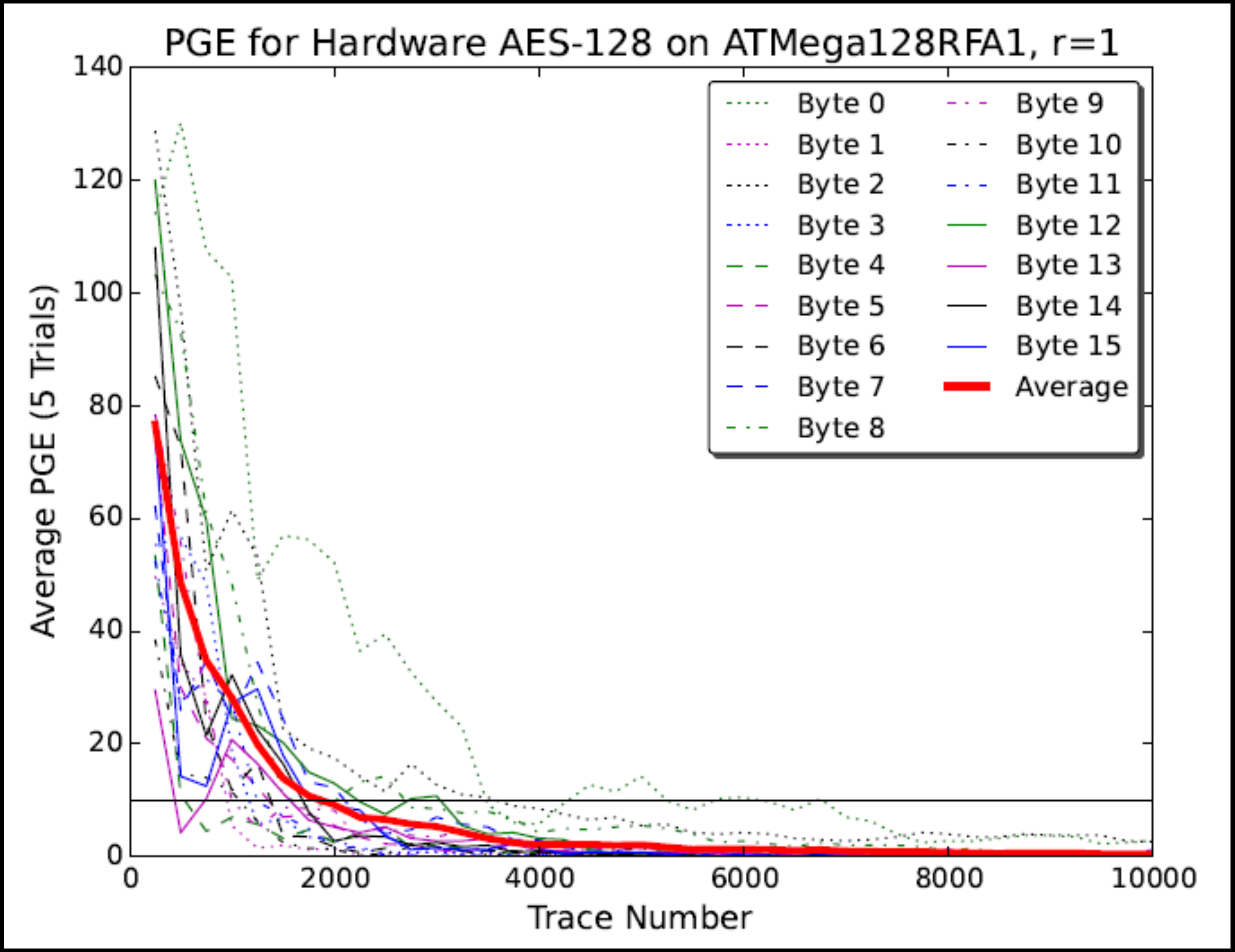
4

Hypothesis

Example: IEEE 802.15.4



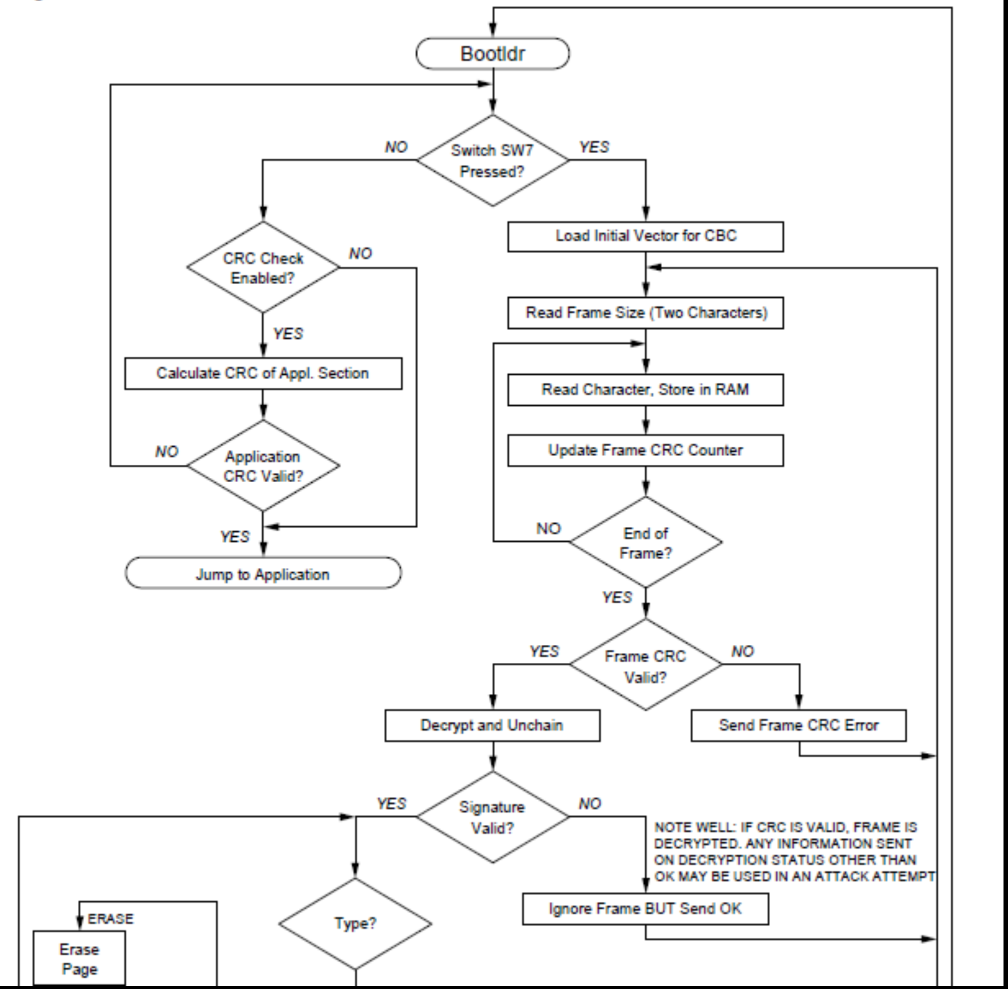
Example: IEEE 802.15.4



Example: IEEE 802.15.4

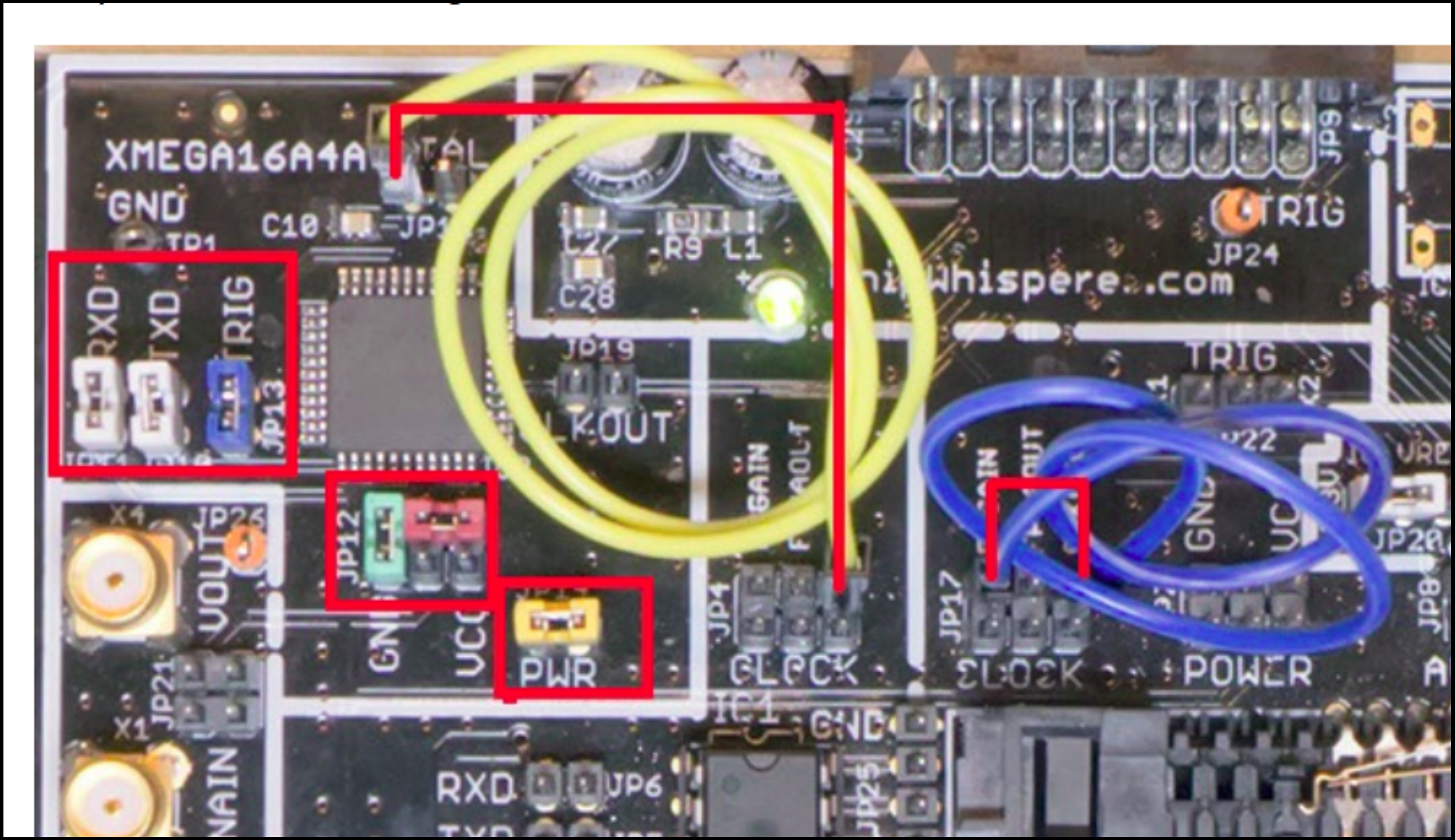
Example: AES-256 Bootloader

Figure 4-5. Flowchart for the AVR bootloader.

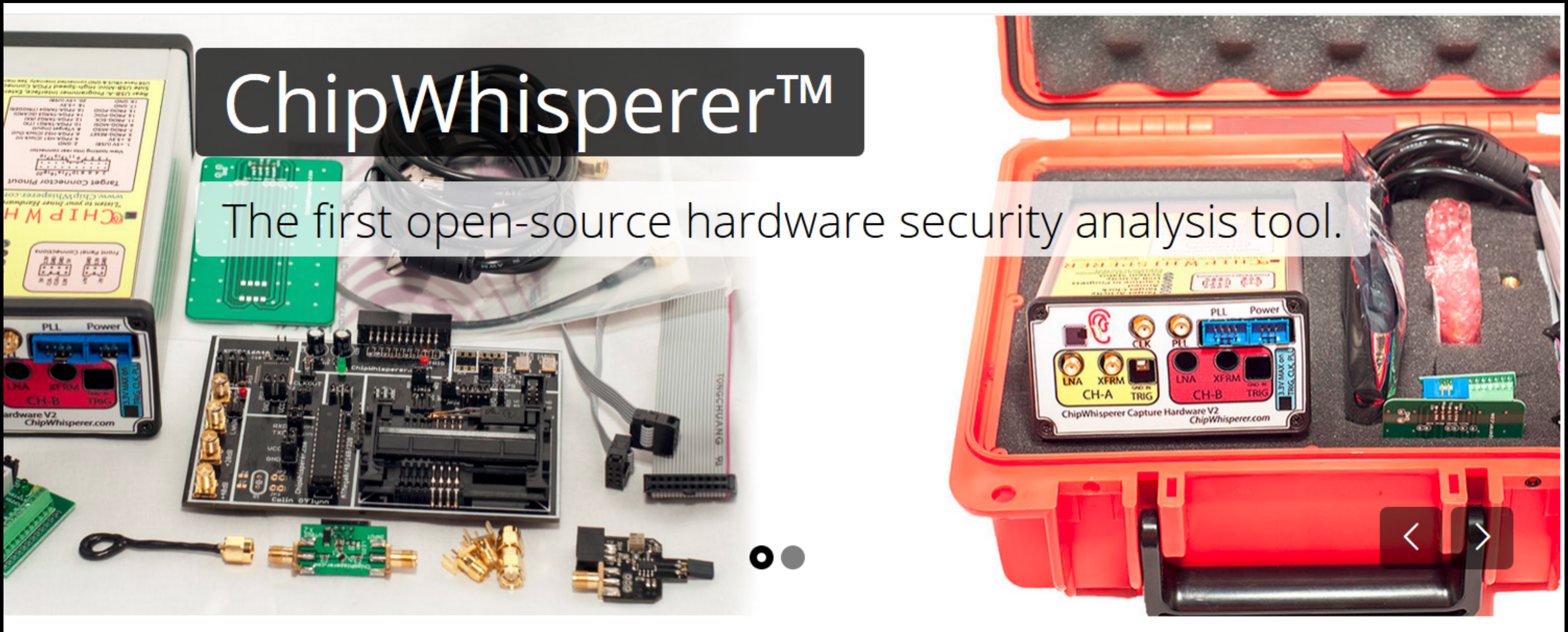


NOTE WELL: IF CRC IS VALID, FRAME IS DECRYPTED. ANY INFORMATION SENT ON DECRYPTION STATUS OTHER THAN OK MAY BE USED IN AN ATTACK ATTEMPT

XMEGA in Real Life



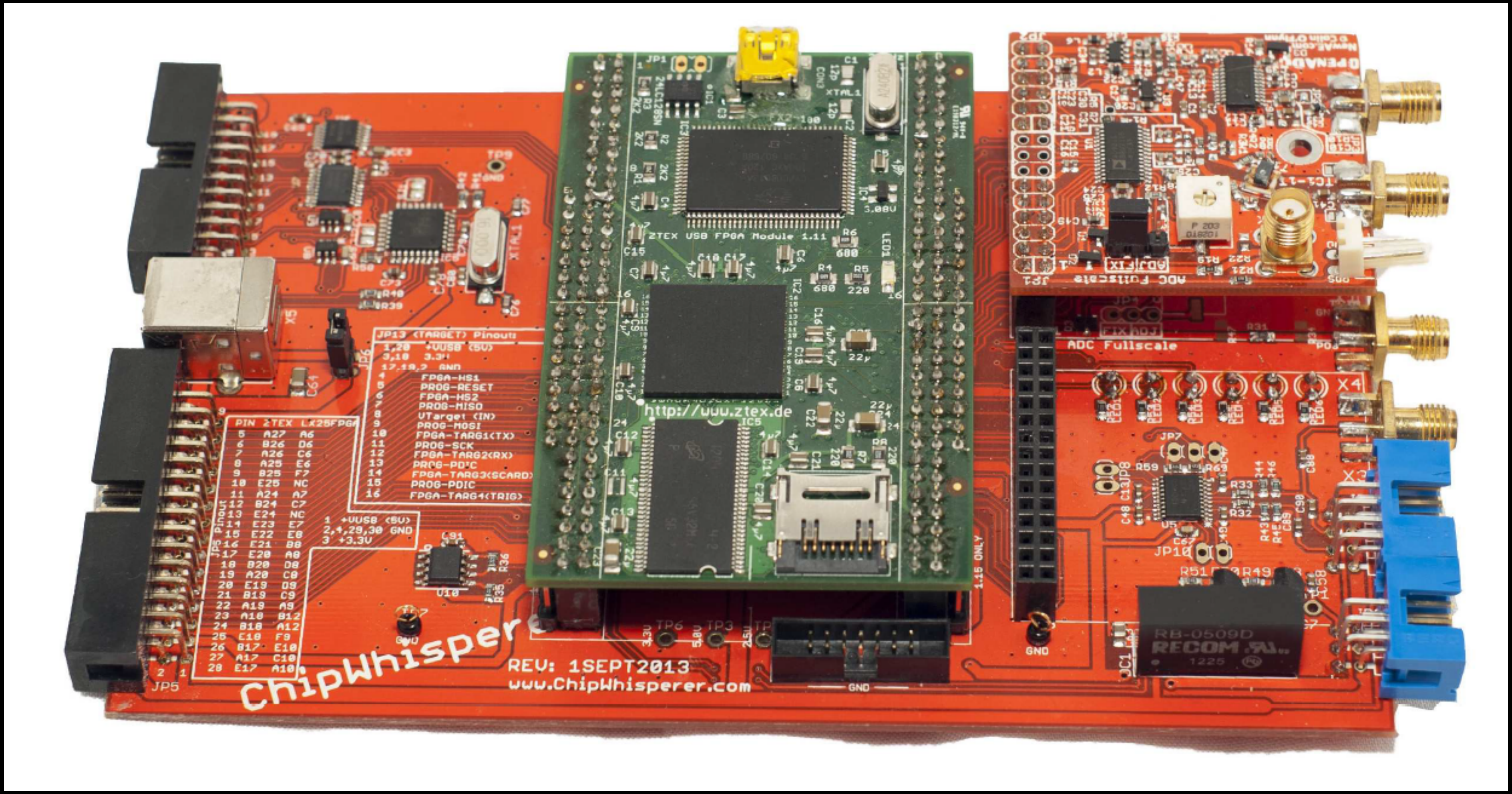
Cheap Hardware… First Ver



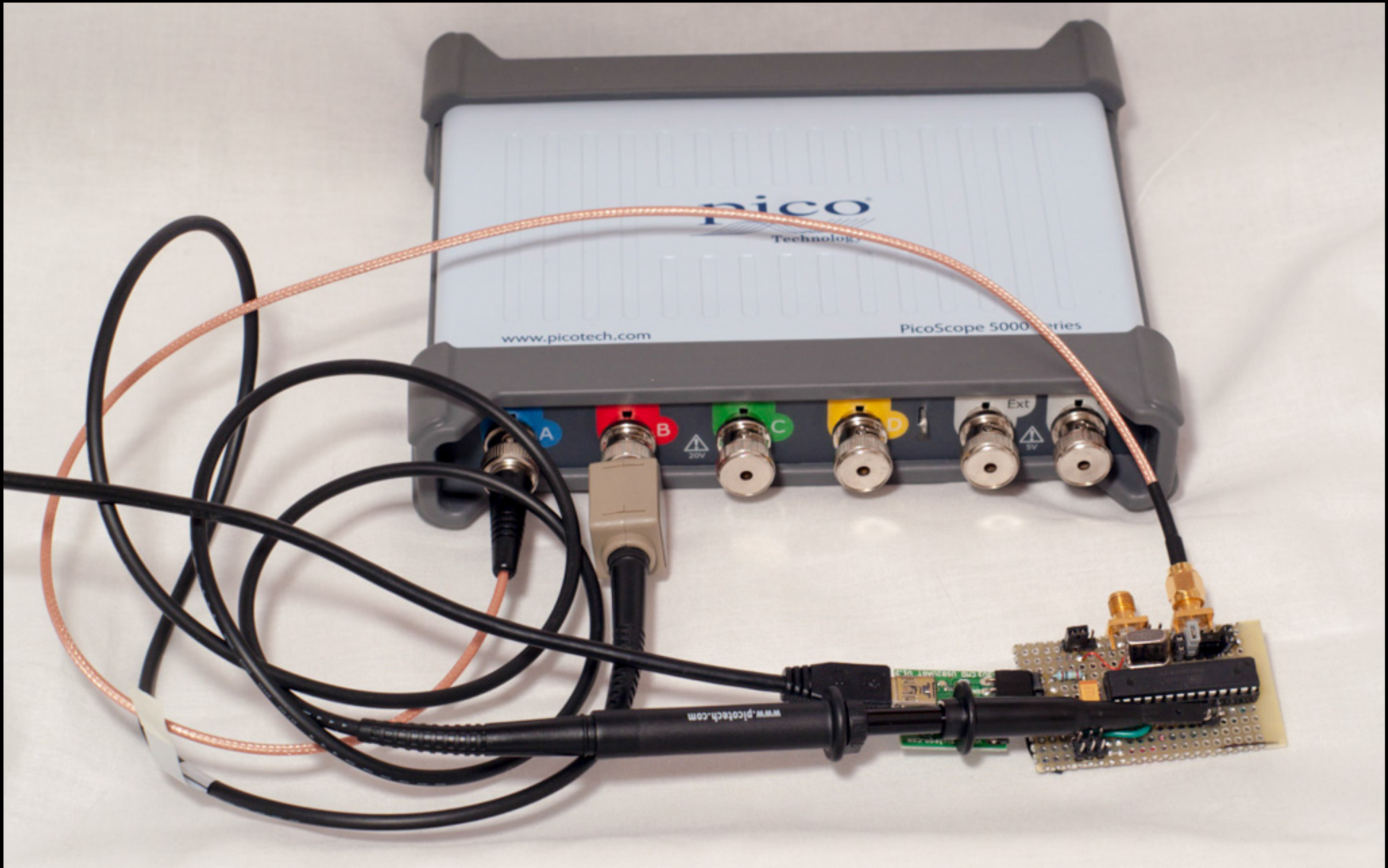
ChipWhisperer™

The first open-source hardware security analysis tool.

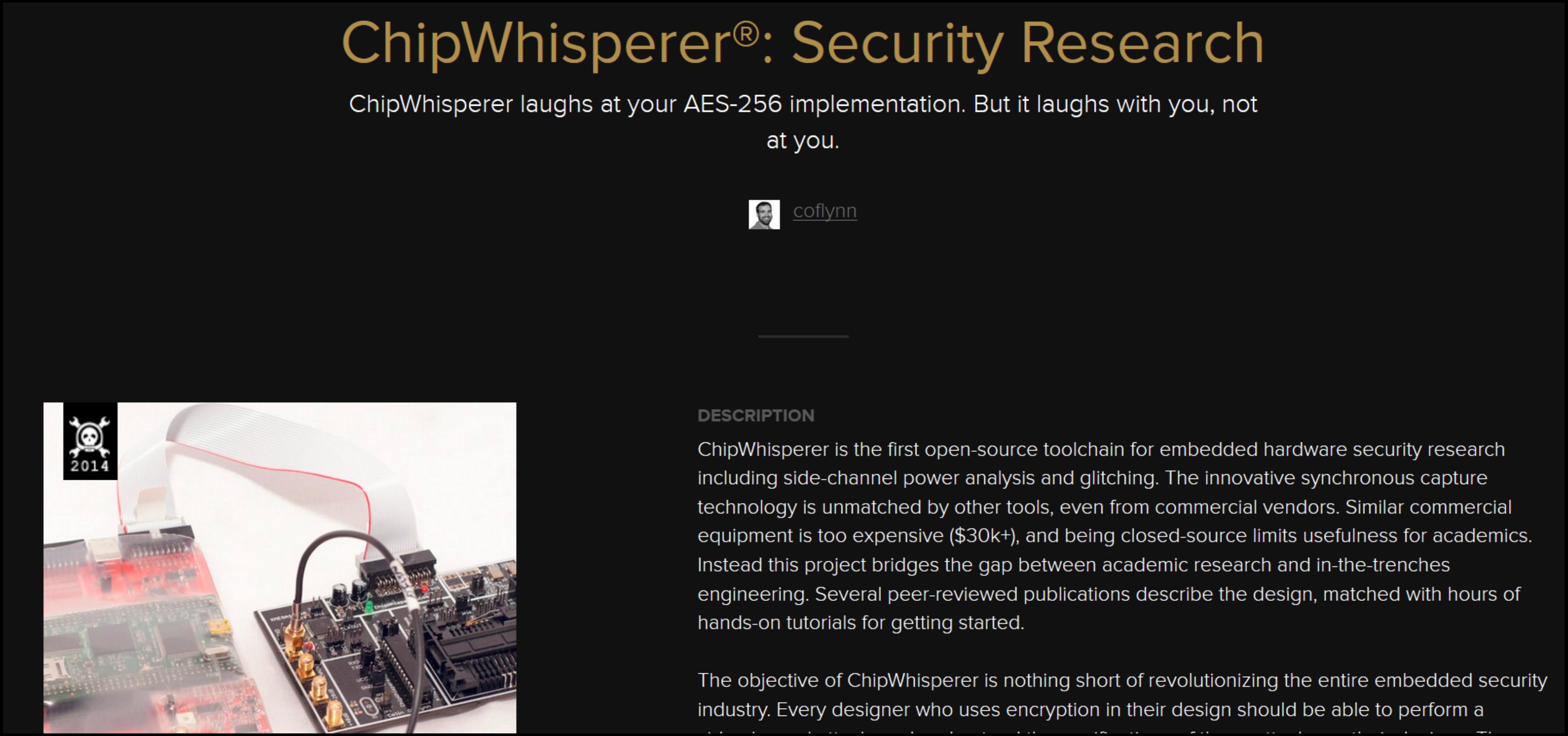
Capture Hardware



Scope-Based Capture



Hackaday Prize 2014



ChipWhisperer®: Security Research

ChipWhisperer laughs at your AES-256 implementation. But it laughs with you, not at you.

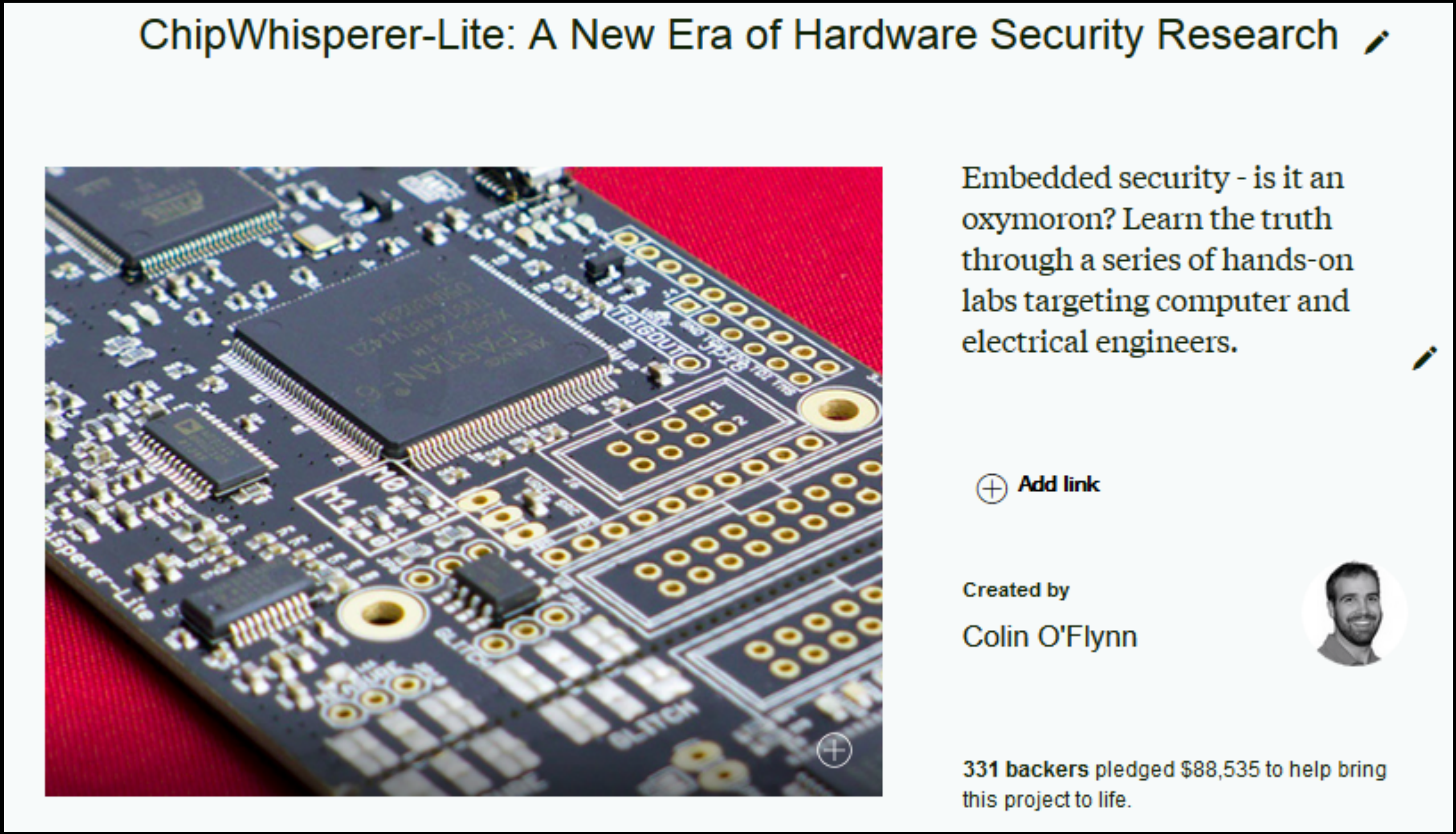
coflynn

DESCRIPTION

ChipWhisperer is the first open-source toolchain for embedded hardware security research including side-channel power analysis and glitching. The innovative synchronous capture technology is unmatched by other tools, even from commercial vendors. Similar commercial equipment is too expensive ($30k+), and being closed-source limits usefulness for academics. Instead this project bridges the gap between academic research and in-the-trenches engineering. Several peer-reviewed publications describe the design, matched with hours of hands-on tutorials for getting started.

The objective of ChipWhisperer is nothing short of revolutionizing the entire embedded security industry. Every designer who uses encryption in their design should be able to perform a

ChipWhisperer-Lite Kickstarter



ChipWhisperer-Lite: A New Era of Hardware Security Research

Embedded security - is it an oxymoron? Learn the truth through a series of hands-on labs targeting computer and electrical engineers.

Created by

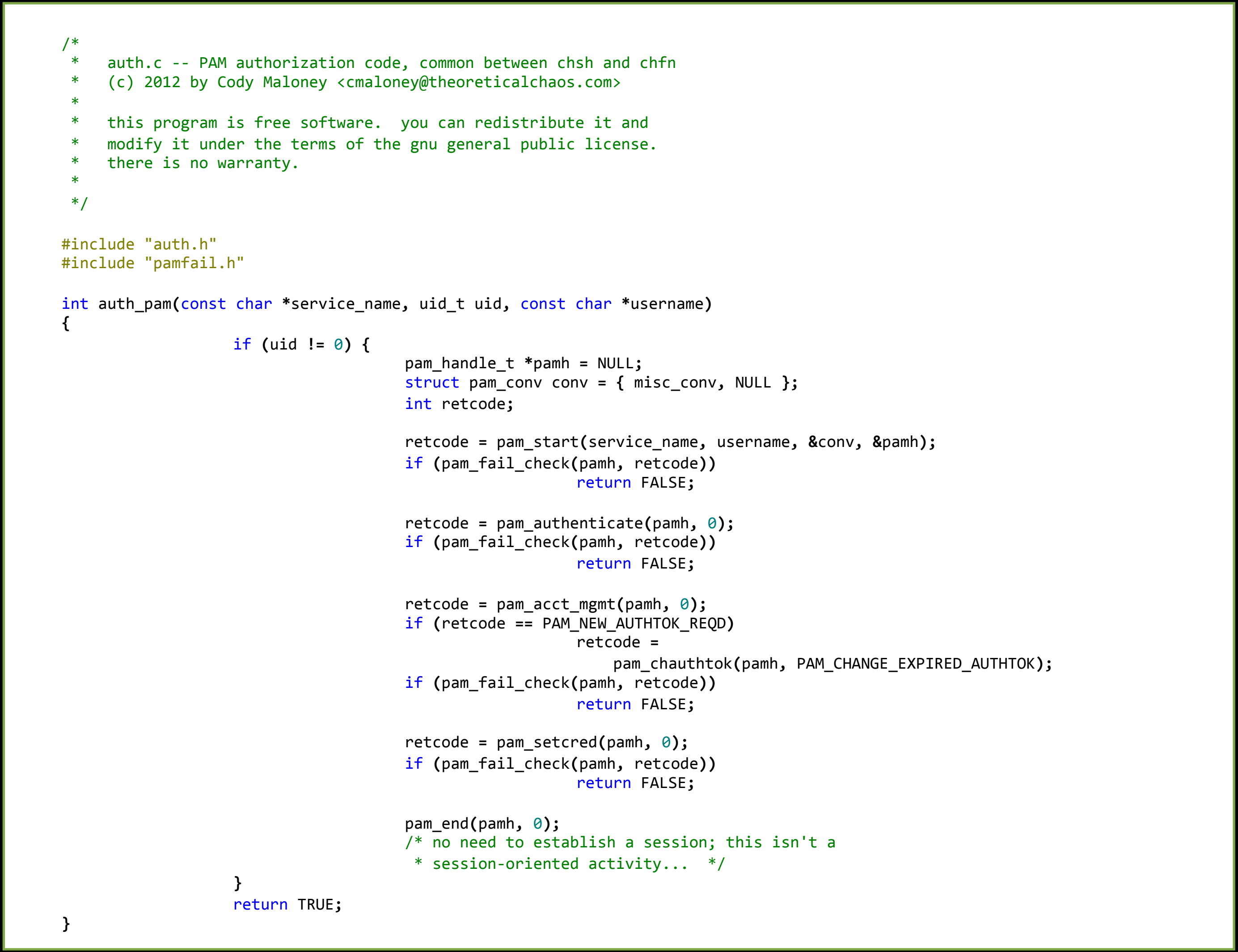
Colin O'Flynn

331 backers pledged $88,535 to help bring this project to life.

Demo of Side-Channel Analysis

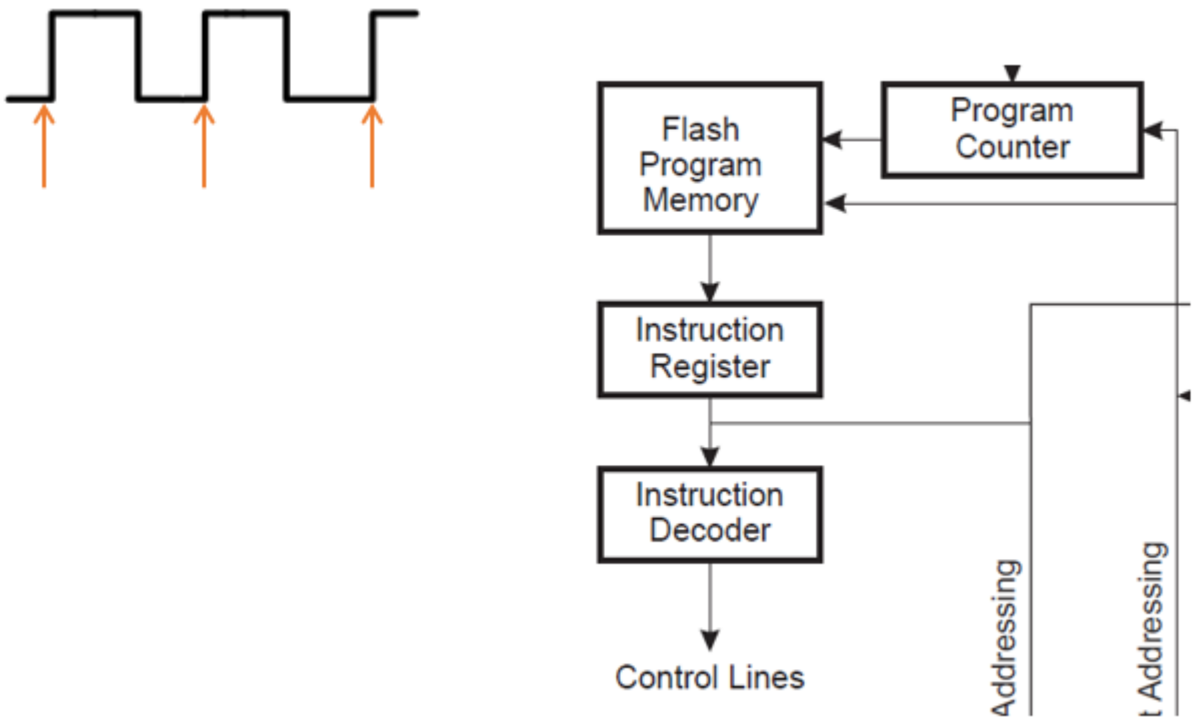
- ChipWhisperer-Lite Based Hardware

Glitching Attacks

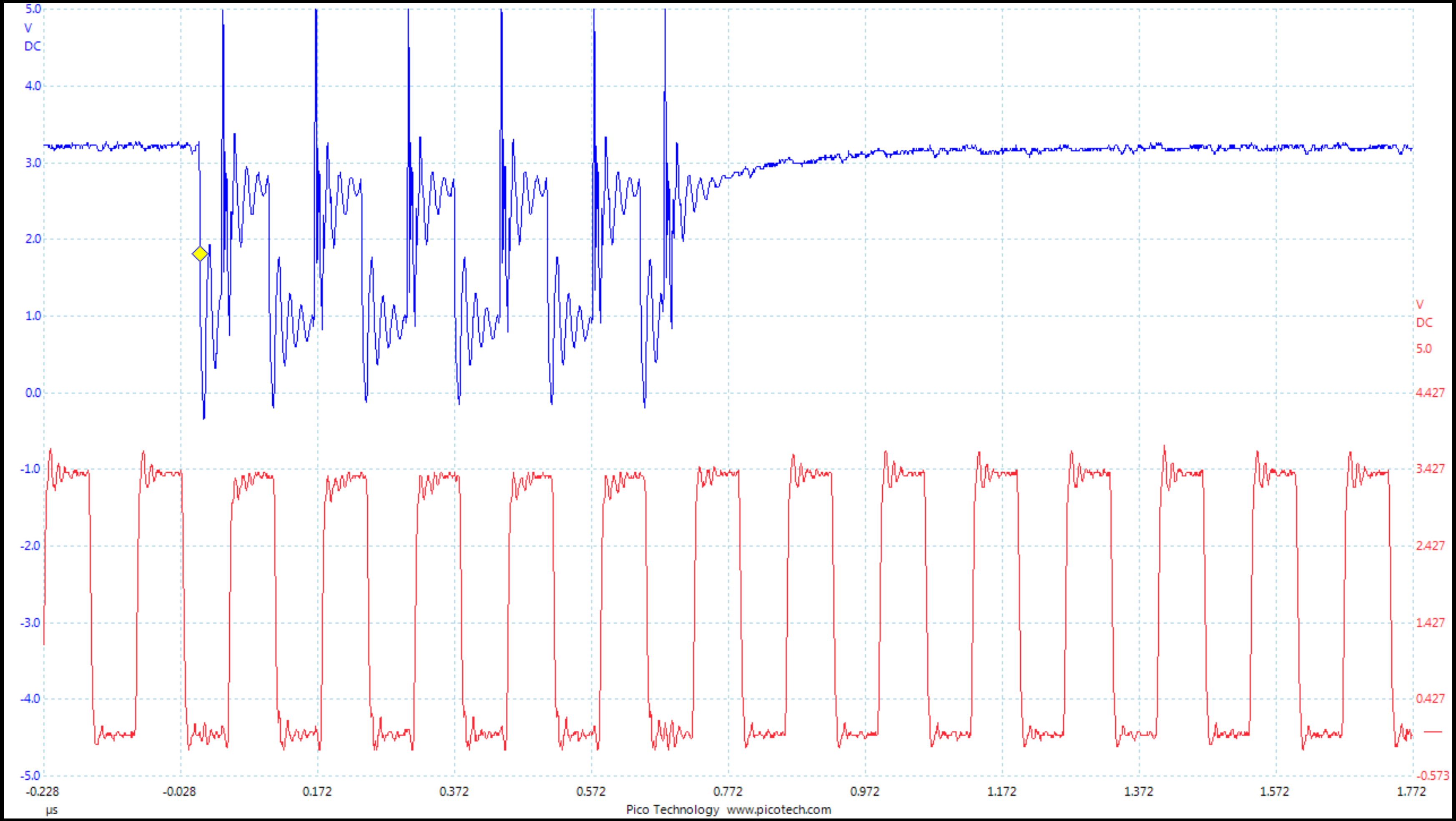


```
/*
 *   auth.c -- PAM authorization code, common between chsh and chfn
 *   (c) 2012 by Cody Maloney <cmaloney@theoreticalchaos.com>
 *
 *   this program is free software.  you can redistribute it and
 *   modify it under the terms of the gnu general public license.
 *   there is no warranty.
 *
 */

#include "auth.h"
#include "pamfail.h"

int auth_pam(const char *service_name, uid_t uid, const char *username)
{
                  if (uid != 0) {
                                    pam_handle_t *pamh = NULL;
                                    struct pam_conv conv = { misc_conv, NULL };
                                    int retcode;

                                    retcode = pam_start(service_name, username, &conv, &pamh);
                                    if (pam_fail_check(pamh, retcode))
                                                      return FALSE;

                                    retcode = pam_authenticate(pamh, 0);
                                    if (pam_fail_check(pamh, retcode))
                                                      return FALSE;

                                    retcode = pam_acct_mgmt(pamh, 0);
                                    if (retcode == PAM_NEW_AUTHTOK_REQD)
                                                      retcode =
                                                          pam_chauthtok(pamh, PAM_CHANGE_EXPIRED_AUTHTOK);
                                    if (pam_fail_check(pamh, retcode))
                                                      return FALSE;

                                    retcode = pam_setcred(pamh, 0);
                                    if (pam_fail_check(pamh, retcode))
                                                      return FALSE;

                                    pam_end(pamh, 0);
                                    /* no need to establish a session; this isn't a
                                     * session-oriented activity...  */
                  }
                  return TRUE;
}
```

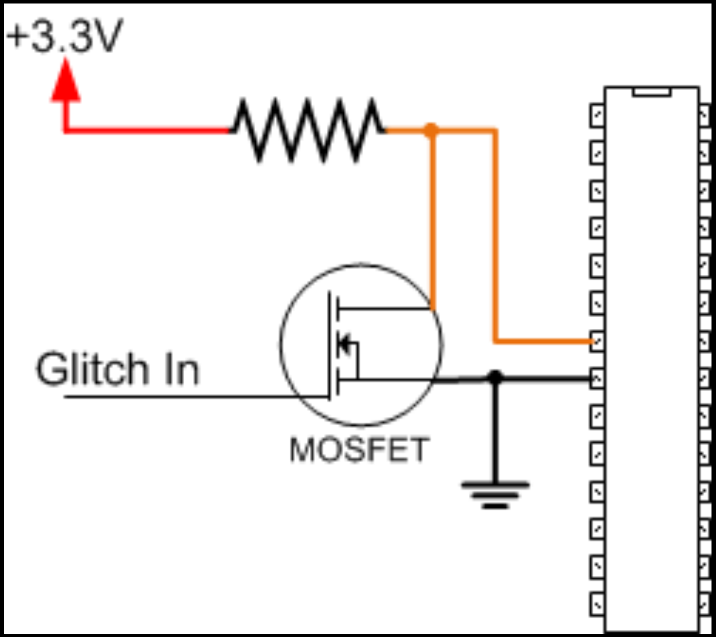
Glitching Attacks - Clock



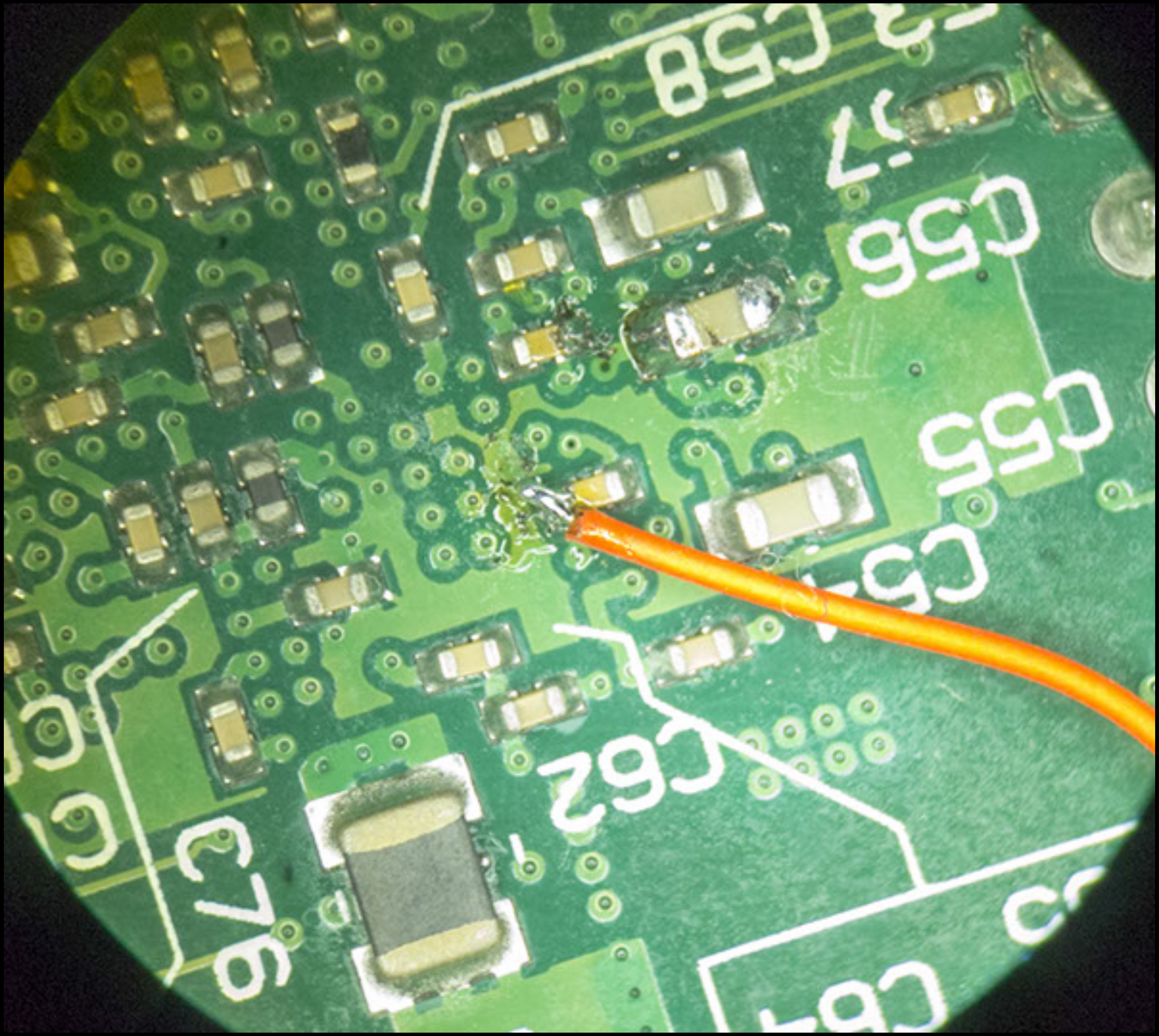
Glitching Attacks - VCC



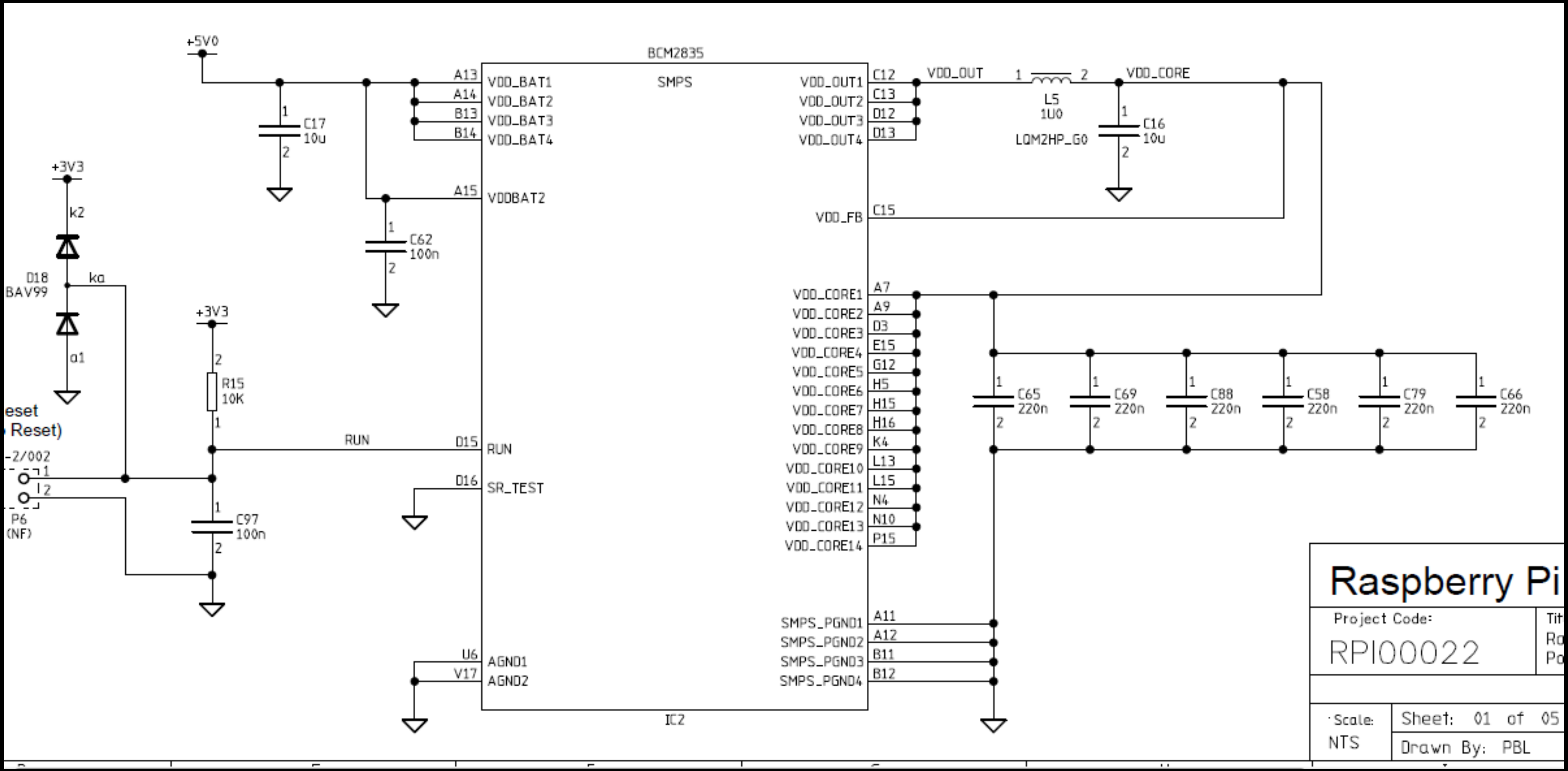
Glitching Attacks - VCC



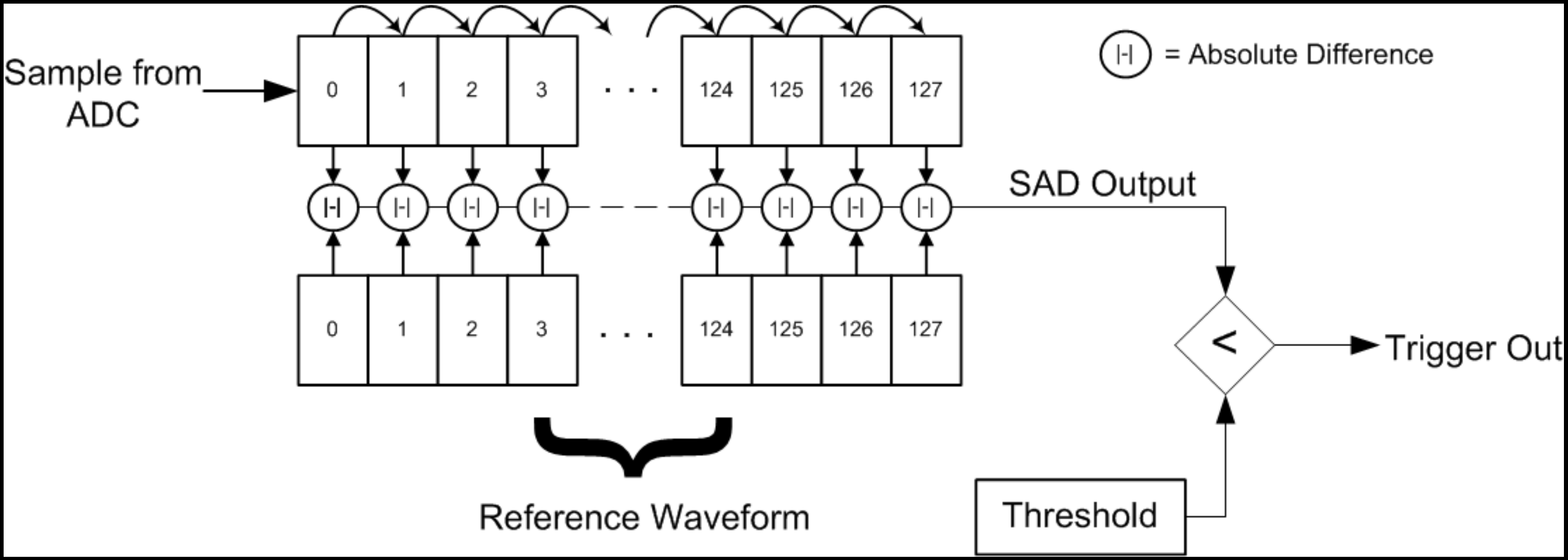
Raspberry Pi



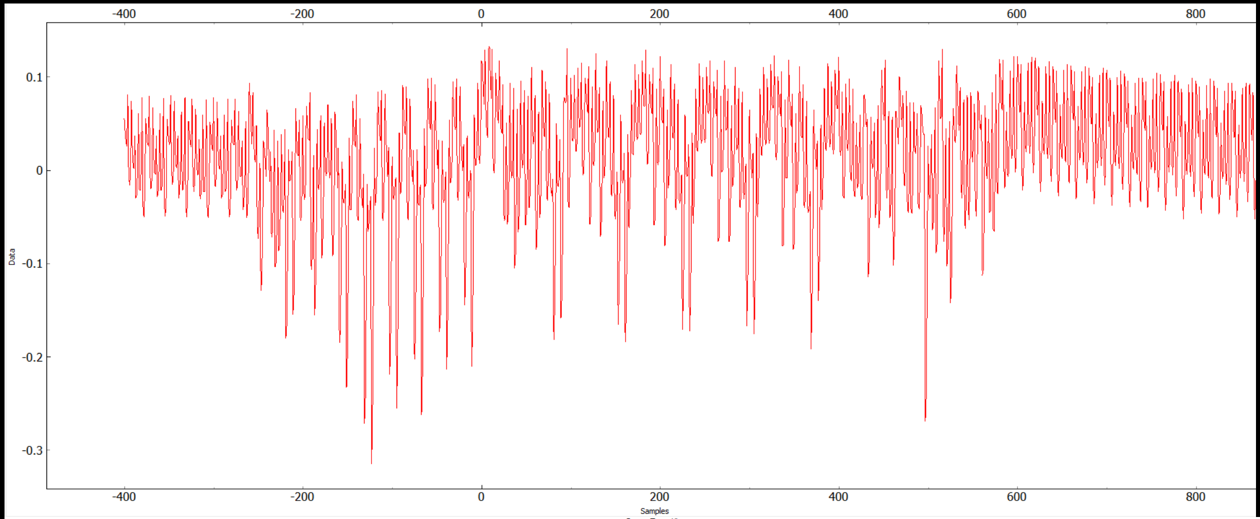
Raspberry Pi

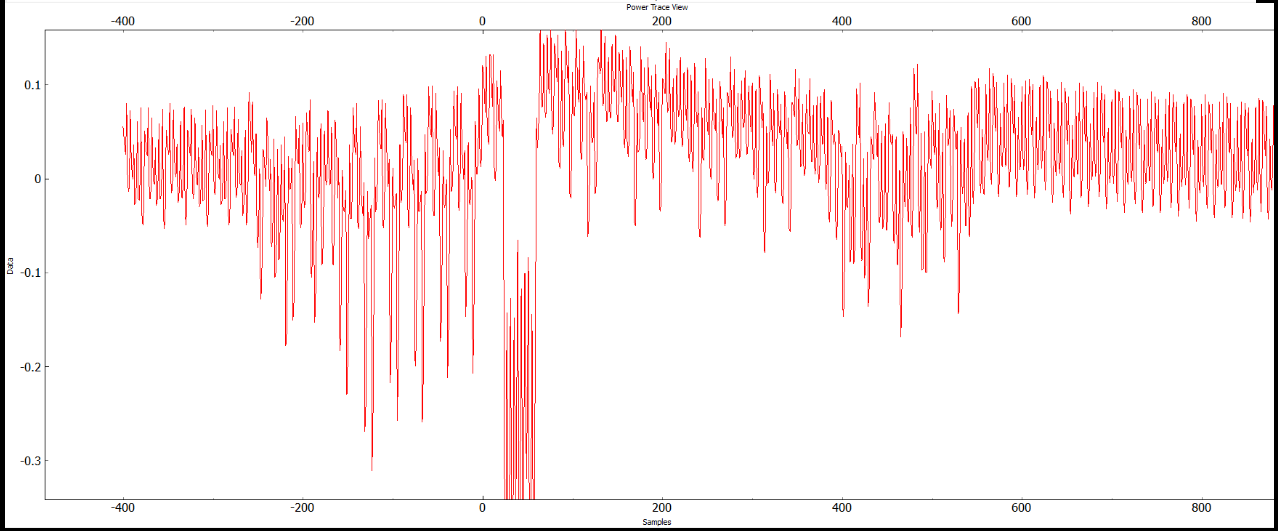


Triggering Attacks



Examples of Triggering





Conclusions

Contact Details / More Info

www.ChipWhisperer.com

www.NewAE.com

Email: coflynn@newae.com

Twitter: @colinoflynn