Hardware Wallets

What makes them secure?

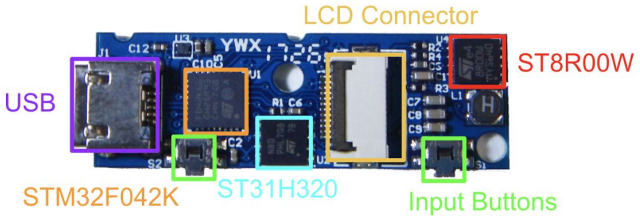

Ledger

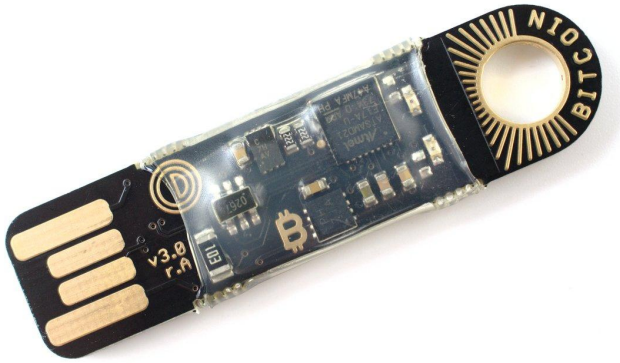

OPENDIME


TREZOR

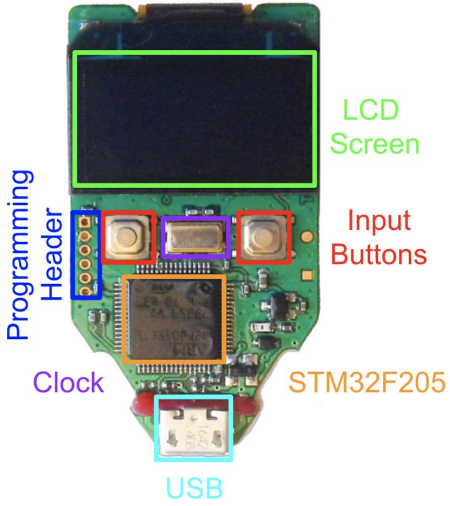

tangem


To begin configuration,
press both buttons.
Ledger


LCD Connector
ST8R00W
USB
STM32F042K
ST31H320
Input Buttons


BITCOIN


TREZOR
Welcome!
Please visit
trezor.io/start


LCD
Screen
Input
Buttons
Programming
Header
Clock
STM32F205
USB


SMART BANKING
BITCOIN HK
BITCOIN • ASSOCIATION • HONG KONG
POWERED BY
tangem

Security

Accidental Loss	Purposeful Attack
discarded flash	online scam
broken hard drive	malware
forgotten passphrase	offline con
lost paper phrase	hardware attacks

Security

Accidental Loss **Purposeful Attack**

Hardware Wallets

Dedicated Hardware	Secure Hardware
reduce key exposure	supply chain
reduce efficiency of	evil maid
simple malware	physical theft
physical risk	interface malware

Hardware Wallets

Ledger

partially secure electronics*

ST31 EAL5+ x STM32

Opendime

partially secure electronics*

ATECC508A x SAMD21

Trezor

insecure electronics*

STM32

Tangem

fully secure electronics*

S3D350A EAL6+

Hardware Wallets

Ledger

Simple Theft,

Private Use Only

Opendime

One–TX

Public Circulation

Trezor

Windows Malware,

Private Use Only

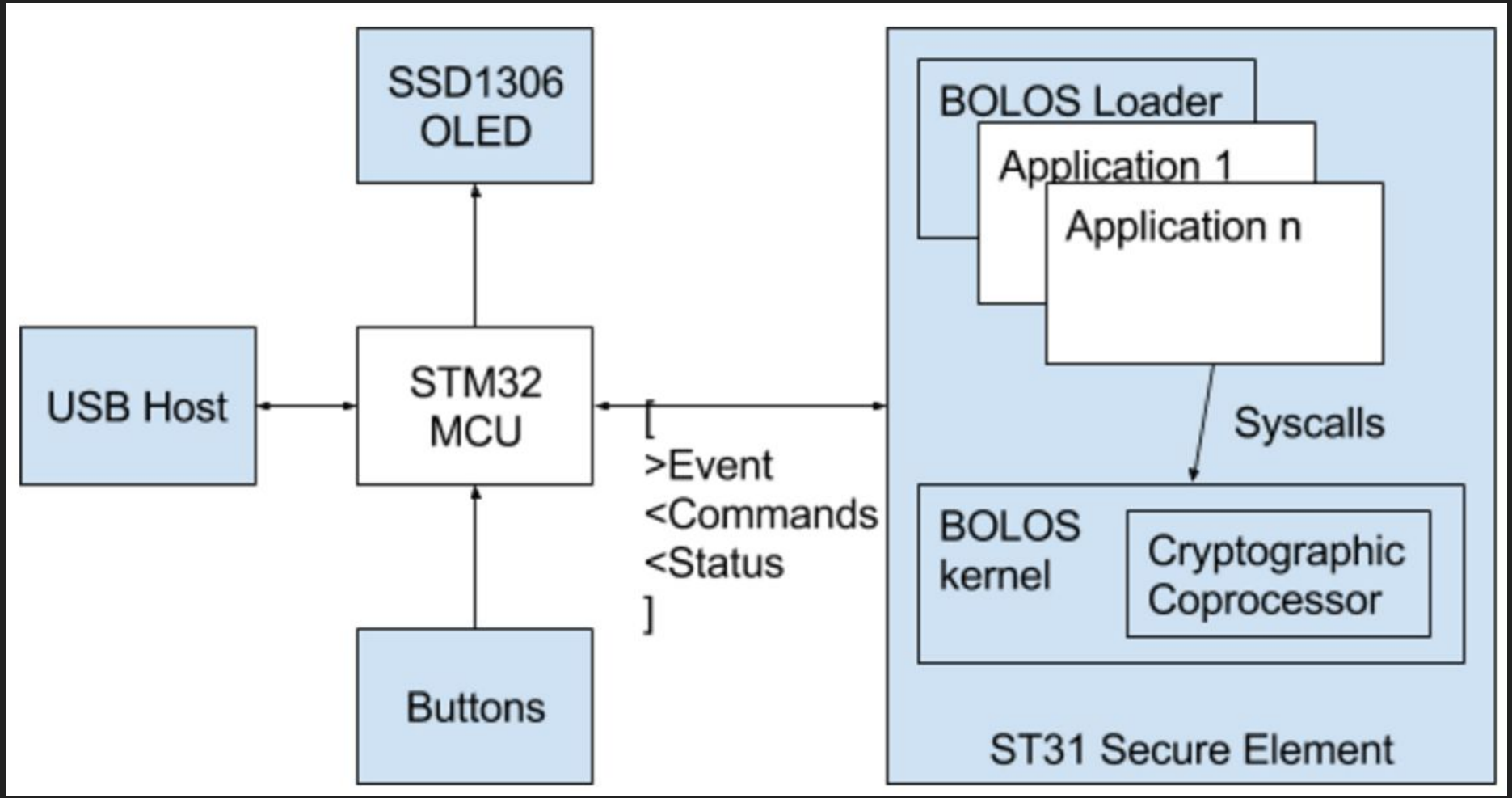
Tangem

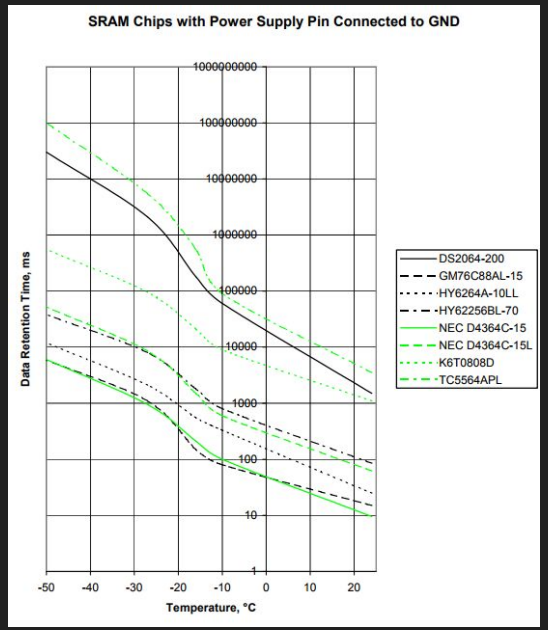
Infinite-TX

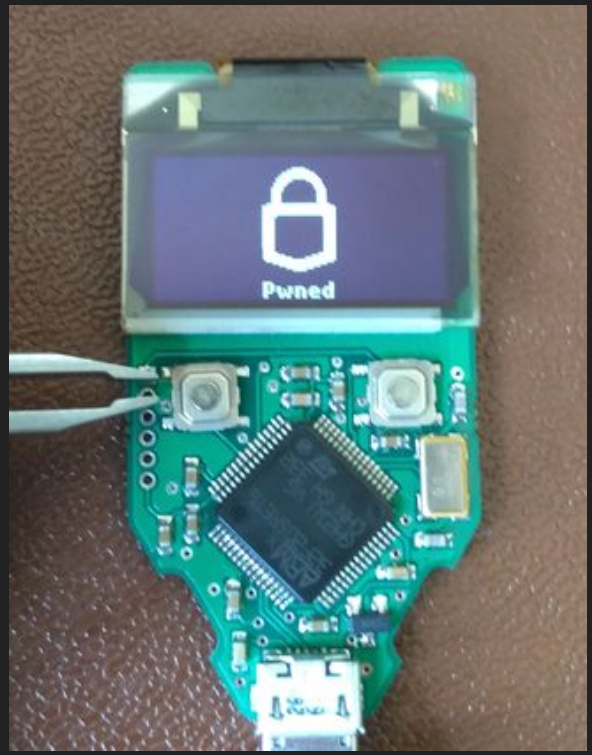
Public Circulation

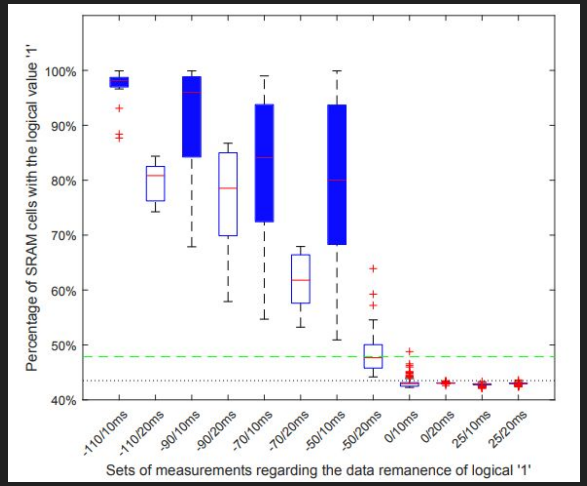
Wallet Vulnerabilities

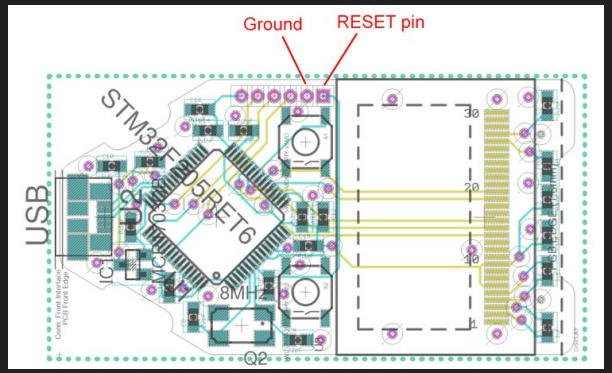
	Ledger	**Trezor**	**Opendime**	**Tangem**
Supply Chain	straightforward	trivial	hard	EAL6+
Evil Maid	straightforward	straightforward	hard	EAL6+
Physical Theft	hard	trivial	hard	EAL6+
Terminal Virus	hard	hard	trivial	targeted
Interface Attack	EAL5+	possible	SE	EAL6+
Forgotten Key	possible	possible	N/A	N/A (default)

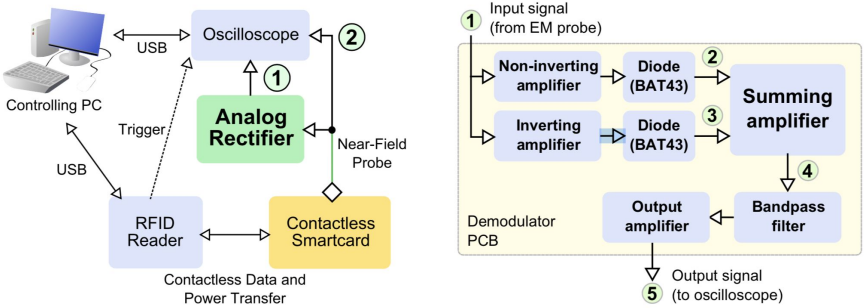

SSD1306
OLED
USB Host
STM32
MCU
Buttons
[
>Event
<Commands
<Status
]
BOLOS Loader
Application 1
Application n
Syscalls
BOLOS
kernel
Cryptographic
Coprocessor
ST31 Secure Element


SRAM Chips with Power Supply Pin Connected to GND
Data Retention Time, ms
1000000000
100000000
10000000
1000000
100000
10000
1000
100
10
1
-50
-40
-30
-20
-10
0
10
20
Temperature, °C
DS2064-200
GM76C88AL-15
HY6264A-10LL
HY62256BL-70
NEC D4364C-15
NEC D4364C-15L
K6T0808D
TC5564APL


Pwned

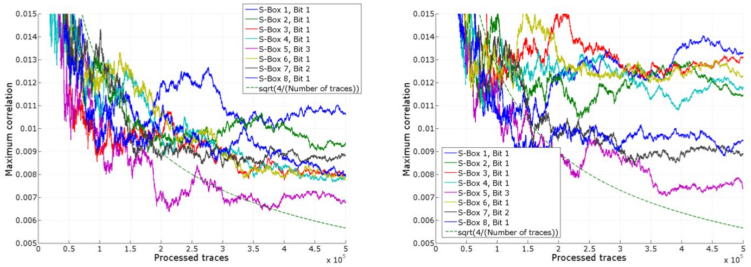

Percentage of SRAM cells with the logical value '1'
100%
90%
80%
70%
60%
50%
40%
-110/10ms
-110/20ms
-90/10ms
-90/20ms
-70/10ms
-70/20ms
-50/10ms
-50/20ms
0/10ms
0/20ms
25/10ms
25/20ms
Sets of measurements regarding the data remanence of logical '1'


Ground
RESET pin
USB
STM32F205RET6
8MHz
Q2



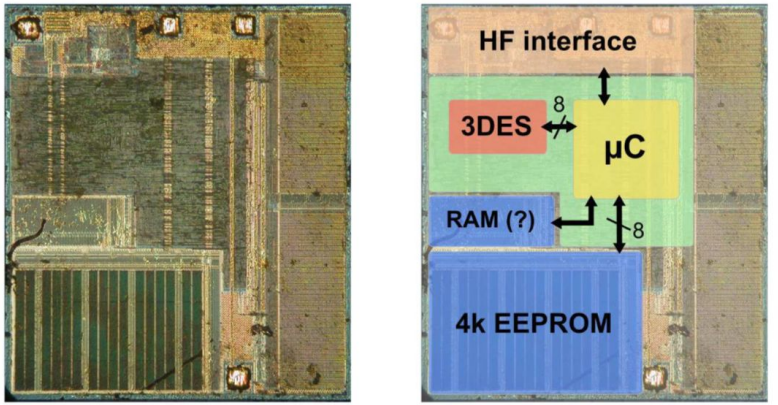
(a) Overall structure (b) Analog demodulation circuitry

Fig. 1: Measurement setup



(a) Time domain (b) Frequency domain

Fig. 9: Maximum correlation coefficient for the correct key, 1-bit model, Hamming distance $R_0 \rightarrow R_1$ for all S-Boxes



(a) IC photo (b) Hypothetical structure

Fig. 4: The DESFire MF3ICD40 IC