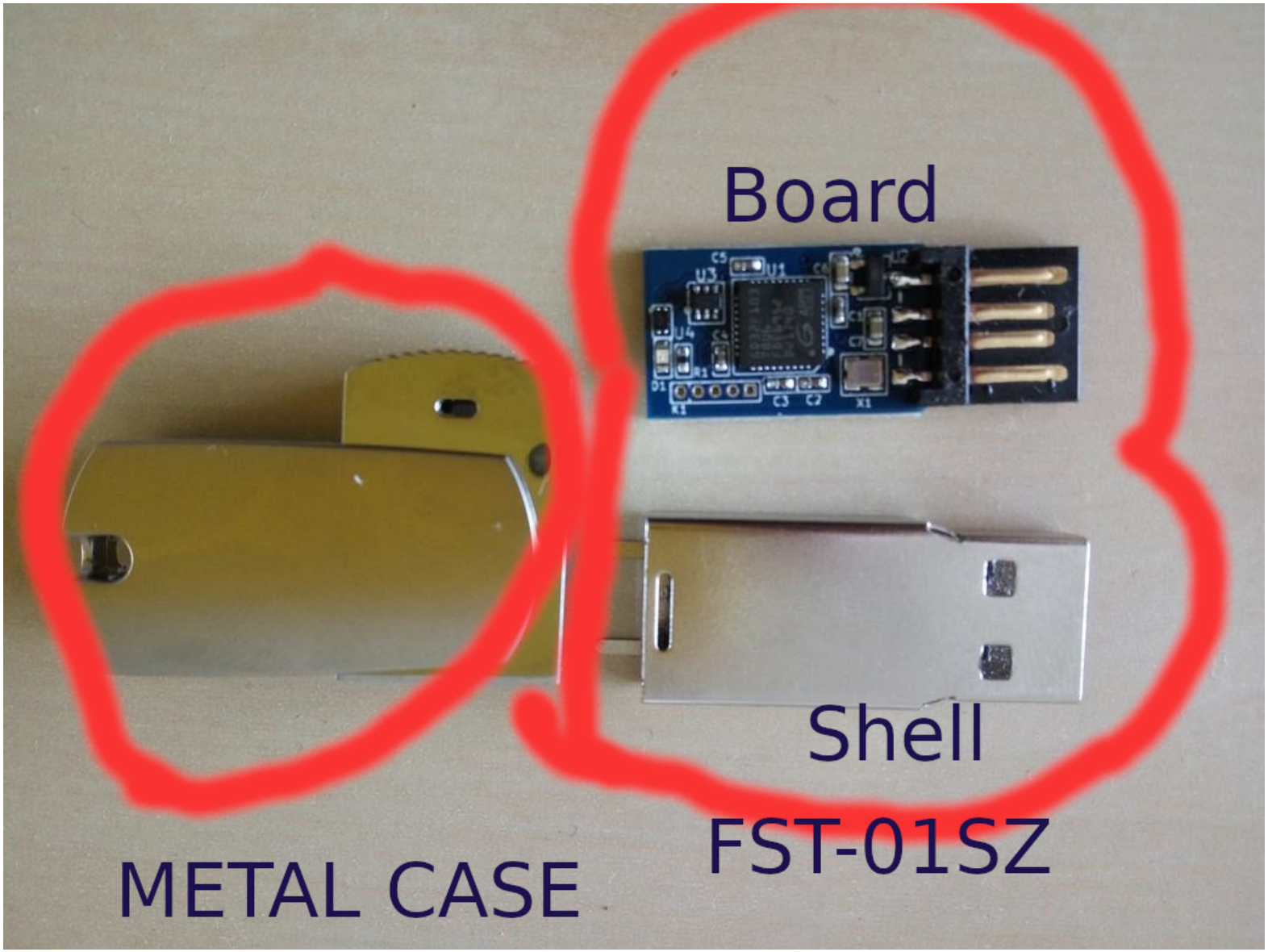
FST-01SZ
(FIying Stone Tiny 01 revision ShenZhen)
free hardware design for Gnuk Token

Niibe Yutaka
gniibe@fsij.org

2019-02-03

FST-01SZ (board+shell) is ready now!

FST-01SZ (board+shell) and case

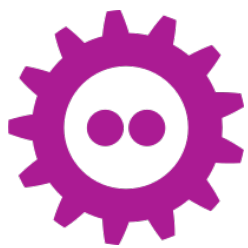


Acknowledgment

Special Thanks	Luis Felipe R. Murillo
SZDIY	Rafael, Fonzie, Terry and Nala
Seeed Technology	Vivian, XuanYu, Simon and Nana
FOSDEM and "CAD and Open Hardware" devroom	
Free Software Foundation	johns and johnh
Debconf18	PaulLiu, YaoWei
Debian	noodles, zigo, glaubitz and dkg
GnuPG	wk and aheinecke
RiseUP	micah and guido
GnuPG friends	Justus, Kai, and Neal
FSIJ	hironobu, kaz and knok
Bro. in Hong Kong:	Satoshi

About Me - Niibe with 'g'

- GNU Project
  - 90s: GNU Emacs, Guile, glibc, GCC
  - 00s: GPLv3
  - 10s: www.gnu.org (Japanese), GnuPG
- GNU/Linux on SuperH around 2000
- FSIJ since 2002
- Debian developer since 2005
- GnuPG developer since 2011

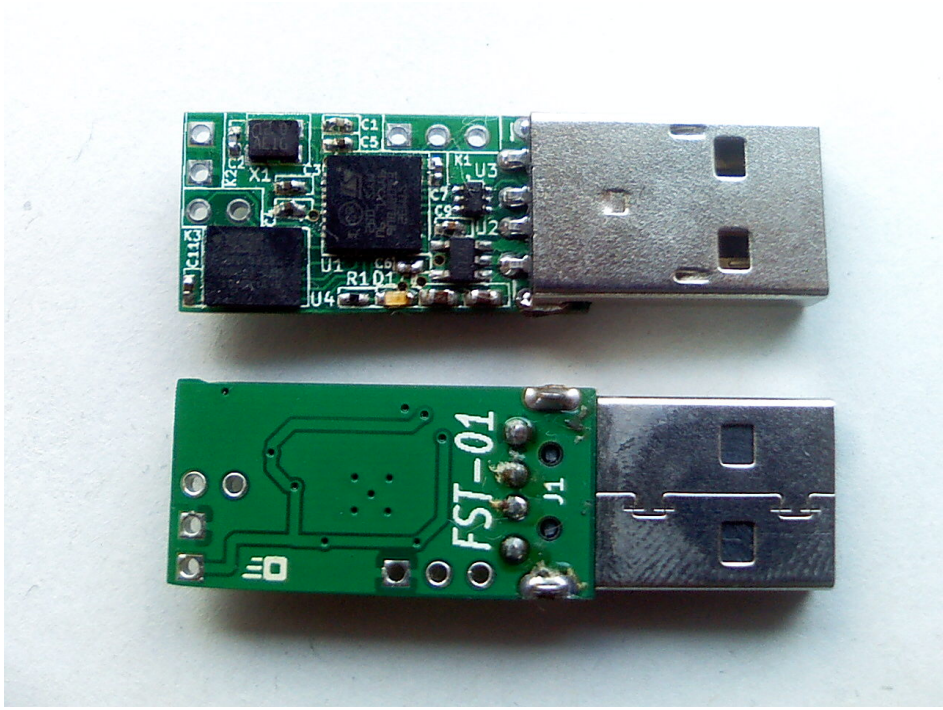


0, 1, and *

0: NeuG	Nobody should control on random number generation
1: Gnuk	Privacy is important It's only you who controls your private keys
*: GNU	Everyone deserves computing freedom

Gnuk Token - for user freedom

- Firmware: “Gnuk” is free software
- **FST-01**: Reference free hardware design
  - Original version: 2011
  - Manufactured in 2012



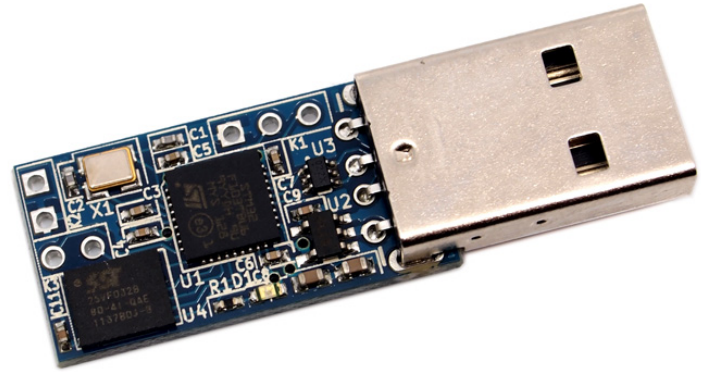
Why Gnuk Token?

- To control our crypto computation
  - Minimize the attack surface
- Goal: can be **reproduced** by others
  - All technical docs available
  - **Free (as in freedom)** tool
    - KiCAD
    - GNU Toochains
    - OpenOCD...
  - No NDA, **never**!
  - Avoiding possible backdoors

My use case of Gnuk Token

At work

At home



On the go

2012

FST-01G

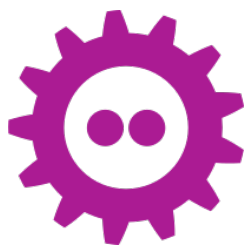
- Design updated in 2016, because...
  - KiCAD: **format change**
  - LDO: discon
  - SPI flash in original version: **not used**
- Manufactured in 2017

FST-01SZ

- Design updated in 2018, because...
  - KiCAD: **format change**
  - MCU protection: reverse engineered???
  - USB-A connector: **too large**

FST-01SZ's challenge

- Use of **Chinese** parts
  - **GD32F103TB** (replaces STM32F103TB)
    - Newer
    - Faster
    - Cheaper
  - **Chinese** USB form factor: **"Wrist-Board"**
    手腕板
- Use of unique tools
  - Test clip with pogo pin needles
  - BeagleBone Green as JTAG/SWD debugger



GD32F103TB

- GD stands for “Giga Device” (not Godot Engine :-)
- ARM Cortex-M3 core
- Can run @ 96MHz with USB
- no wait cycle, no cache accessing flash
  - static RAM loaded by flash content at boot
  - less side channel info: power analysis, timing analysis
- Peripherals like USB and ADC are independent implementation

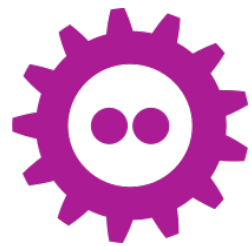
USB form factor

手腕板

- Chinese De-facto standard
- Smaller form factor
  - metal shell
  - plastic connector
- Used for USB Memory

USB form factor: The parts

- ZL-271 (left, metal shell, `CJ-AM-C5B0C010`)
- ZL-272 (right, plastic connector)



The name: wrist-board (1)

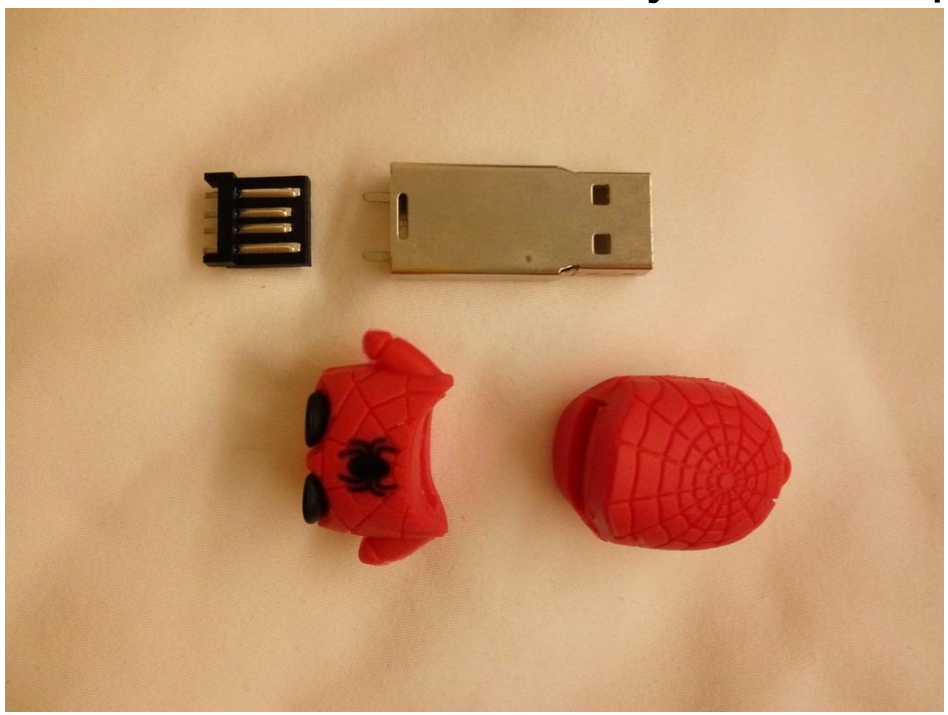
手腕板

- Originally one for wrist band USB memory

The name: wrist-board (2)

手腕板

- But now, there are many kinds of plastic covers, like:



The name: wrist-board (2)

手腕板

- Or, there is a metal case

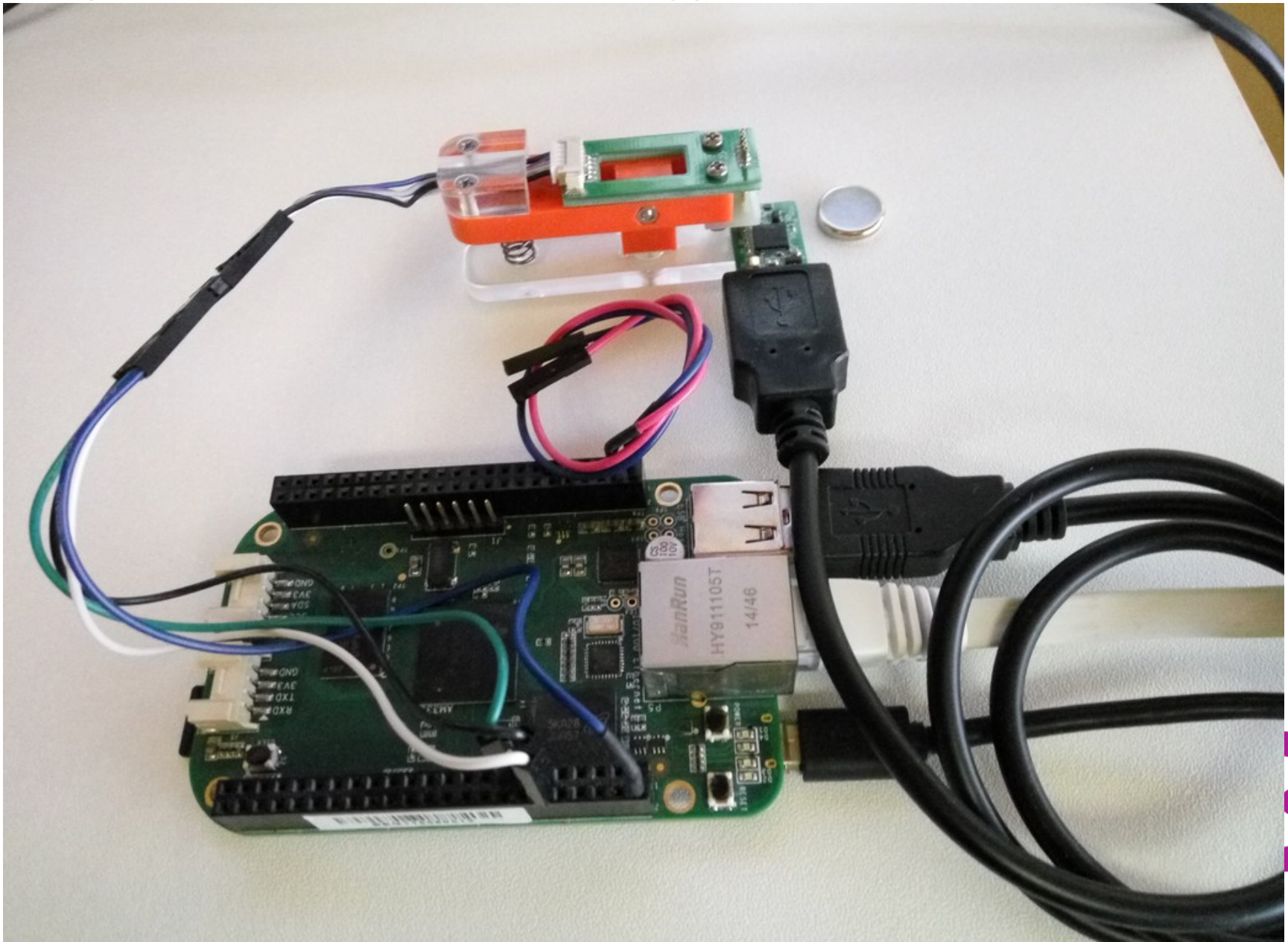
FST-01SZ with metal case

- Putting the board+shell into the case
- It's an one-way procedure
- Offering a feature of tamper resistance

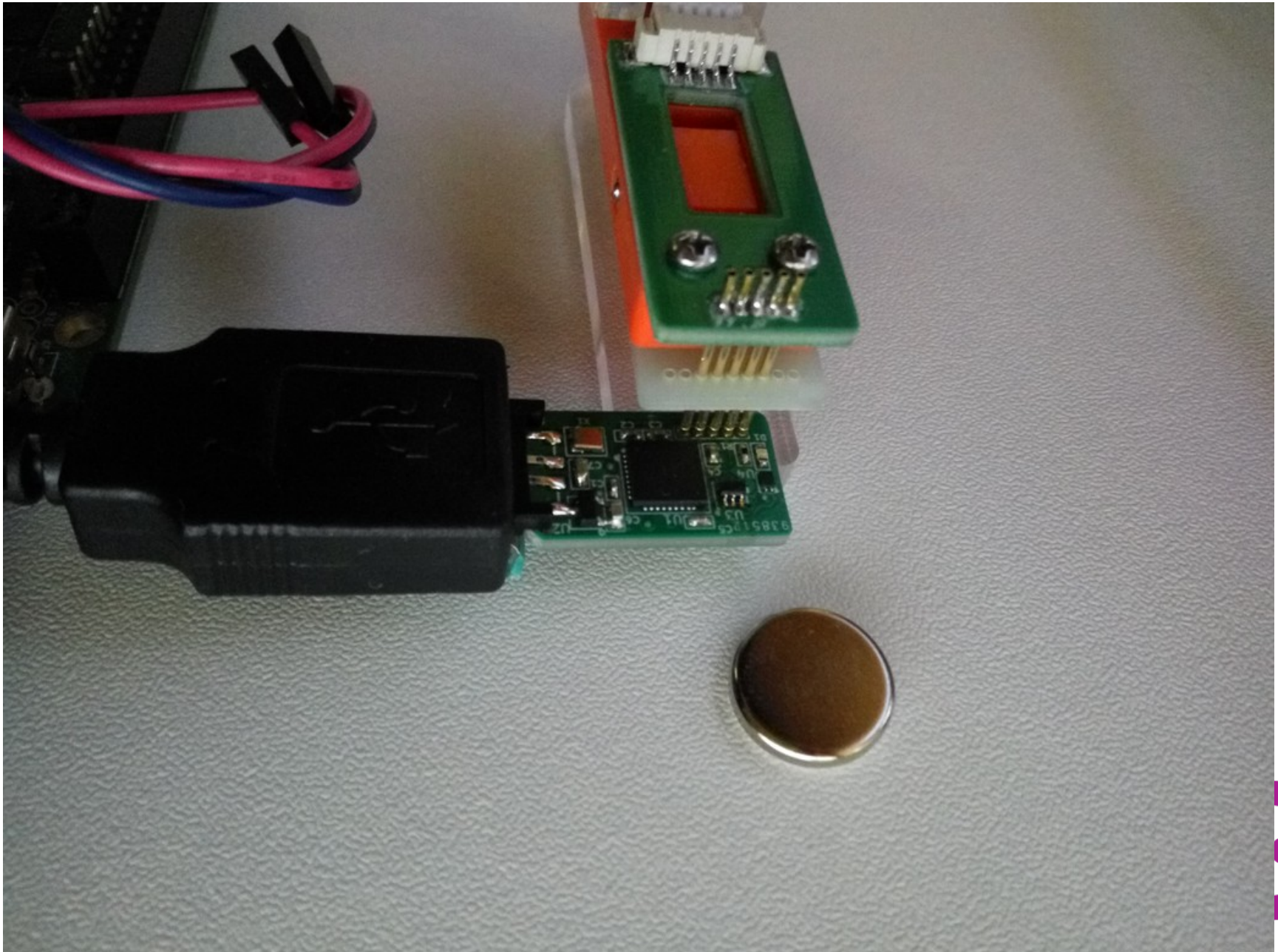
FST-01SZ prototype in action

FST-01SZ prototype to be flashed and tested

BeagleBone Green as SWD debugger



Chinese test clip with pogo pin needles



Experiences (1) - Reproducibility

Our purpose is reproducibility for computing freedom

- Component availability matters
- Tools' data format matters, too
- As well as tools themselves

Experiences (2) - Test plan

For reproducibility, if it is intended for (mass) production,

- Test plan should be a part of "Open Hardware Design"
- I'd like to propose a practice publishing a test plan for hardware design

Experiences (3) - China

It's good to learn Chinese culture for better communication

- The holiday seasons (Chinese New Year, National Day)
- How Taobao and Alibaba work (for unique parts)
- Relationship between person is so important
  - It's good you meet in person occasionally
- Better to confirm: exact part, exact material, date...

Experiences (4) - China

- Specifying manufacturer and MPN (Manufacturer Product Number) is not enough
  - it's OK, when it's available in Digikey, Mouser, etc.
  - when it's a Chinese unique part not available there...
  - better to confirm with your own eyes
- For them, it's a kind of reference number
- **Remember**: the copycat culture
- **I like it!**: Re-implementation is good for improvement and innovation!

Experiences (5) - ShenZhen

Another big city in China

- Computer and electronics
- Many young engineers
- QR-code payment
- Surveillance system and “SECURITY” persons

To summarize

- In 2011, I started using PCB service in ShenZhen
  - Mainly because it's cheap
- Things have been **evolved** a lot in China
- Now, good PCBA service is also available
- And many unique **advantage**s, like:
  - **GD32F103TB**
  - "Wrist-Board"
  - BeagleBone Green
  - Test clip with pogo pin needles
- I take **advantage** of those things in **ShenZhen**
- ... to achieve good product

Discussion

Here are my questions (and my children's one)...

- How do you maintain your hardware design in a repo?
  - Do you also put the output (gerber) to a repo?
- How do you ensure the output is same as yours?
  - Do you use some automation (with CI/CD)?
- How do you care about reproducibility?

Discussion

Here are my questions (and my children's one)...

- How do you maintain your hardware design in a repo?
  - Do you also put the output (gerber) to a repo?
- How do you ensure the output is same as yours?
  - Do you use some automation (with CI/CD)?
- How do you care about reproducibility?
- If it is so reproducible, why people buy from you, papa?

Discussion

Here are my questions (and my children's one)...

- How do you maintain your hardware design in a repo?
  - Do you also put the output (gerber) to a repo?
- How do you ensure the output is same as yours?
  - Do you use some automation (with CI/CD)?
- How do you care about reproducibility?
- If it is so reproducible, why people buy from you, papa?
  - Well, I don't know... but...

Discussion

Here are my questions (and my children's one)...

- How do you maintain your hardware design in a repo?
  - Do you also put the output (gerber) to a repo?
- How do you ensure the output is same as yours?
  - Do you use some automation (with CI/CD)?
- How do you care about reproducibility?
- If it is so reproducible, why people buy from you, papa?
  - Well, I don't know... but...
  - There is a tribe called hackers...

Questions?

Questions?

Happy Hacking!