

TPMとの戯れ

縁川 志穂 (@elliptic_shiho)

2023/08/10 @ Security Camp 全国大会 '23

Who

- L-1(暗号化通信ゼミ) 講師
- GMO Cybersecurity by Ierae, Inc.
- 全国大会('15), 全国大会講師('18 -)
- 暗号理論 / 数学

TPM

- Trusted Platform Module
 - 特に2.0を仮定
- Trusted Computing Groupが制定
 - 國際規格(ISO/IEC 11889:2015)
- Windows 11ではTPM 2.0は必須コンポーネント

TPM

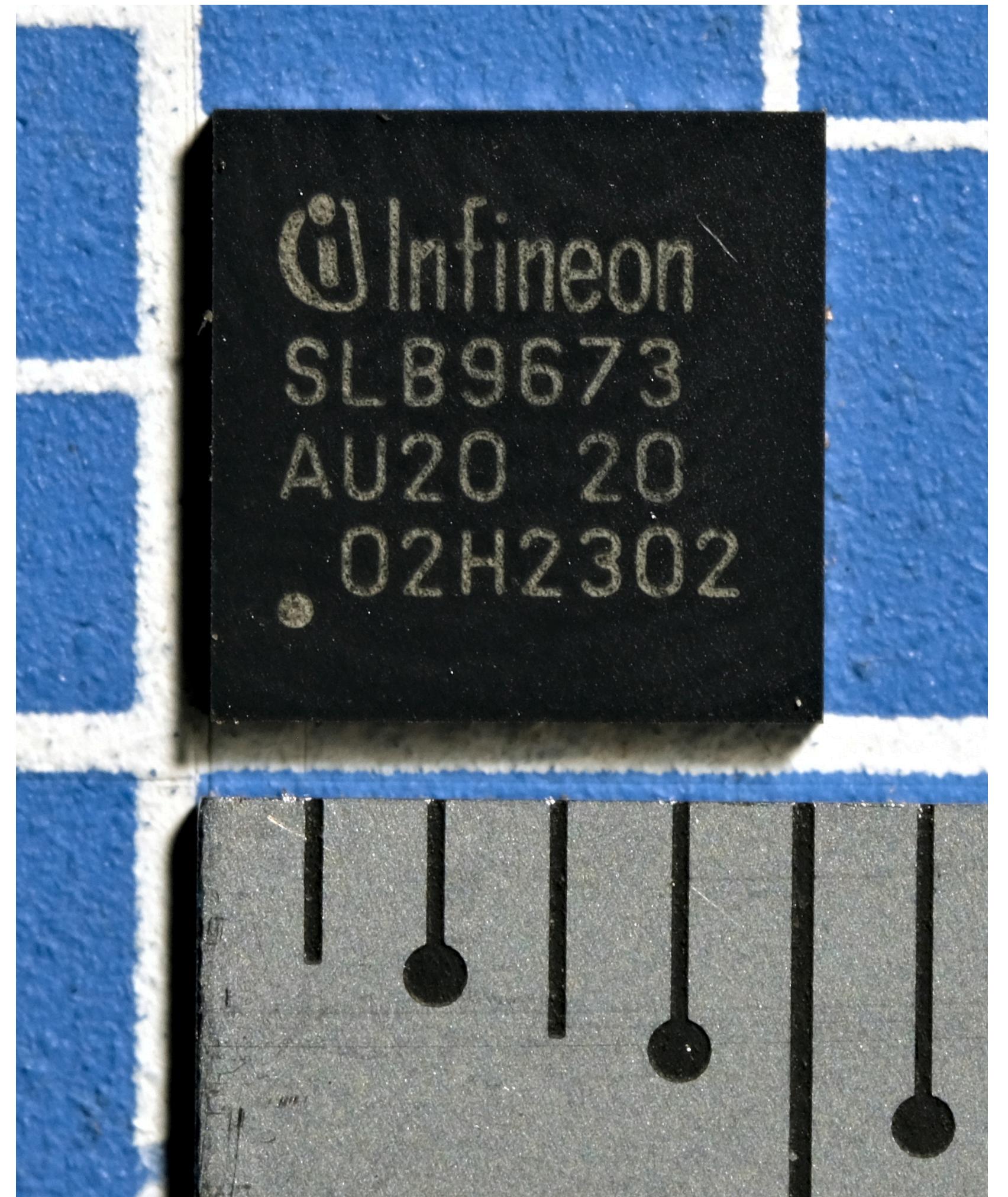
- ・何ができるのか
 - ・暗号化・復号
 - ・鍵生成
 - ・安全性の高い乱数生成
- ・アテストーションによる内容の保証も可
- ・耐タンパ性の保証 → TPM内で生成 && 取り出し不可指定をした秘密鍵は誰も知り得ない
- ・面白そう

TPM / Hardware

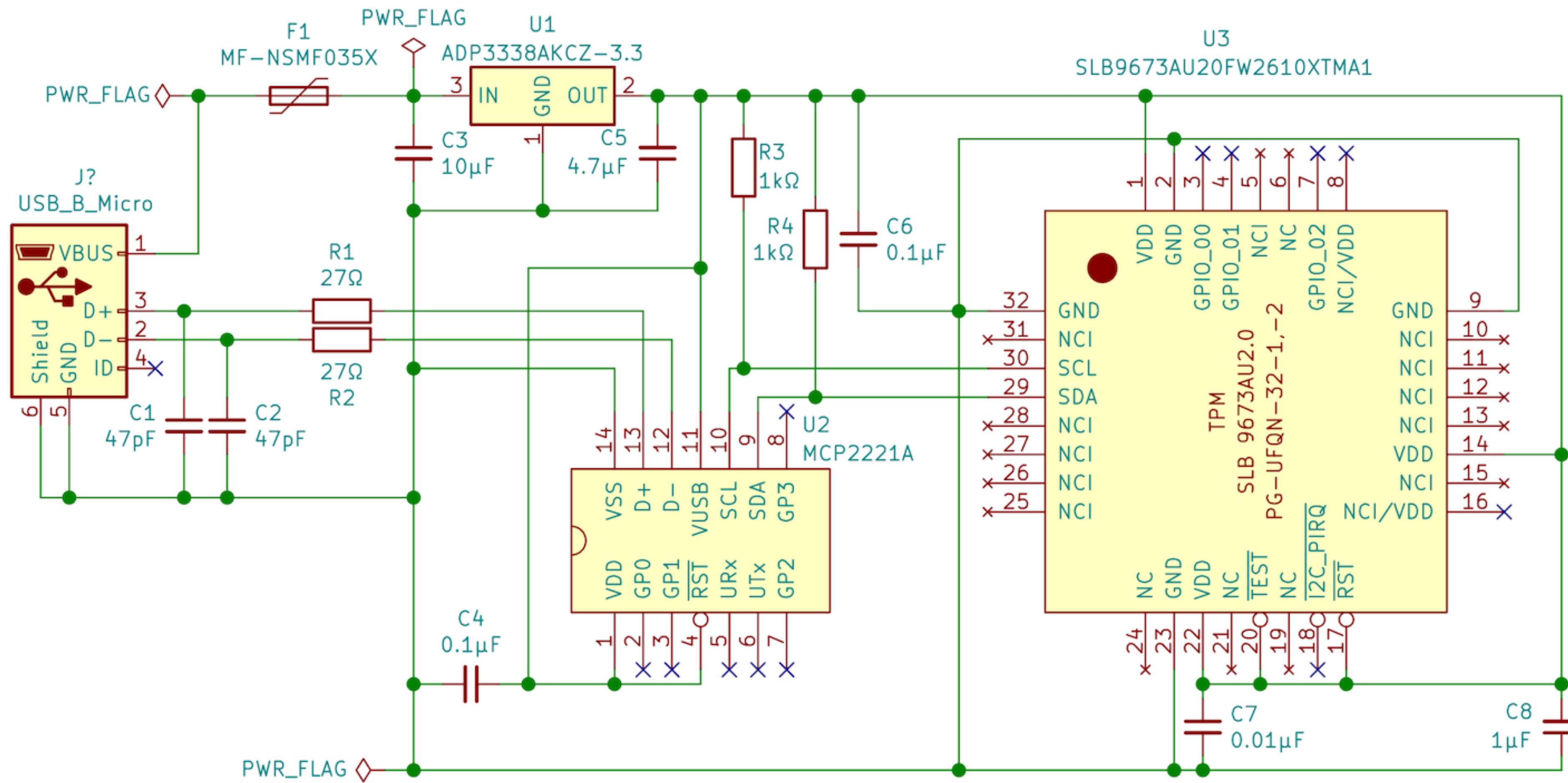
- そうと決まればチップ選定
 - Yubikey, YubiHSMライクにしたい → USB経由
 - Microchip MCP2221A (USB-HID ⇄ I²Cブリッジ)なら手元にある
 - Digi-keyにある手頃なチップは?

TPM / Hardware

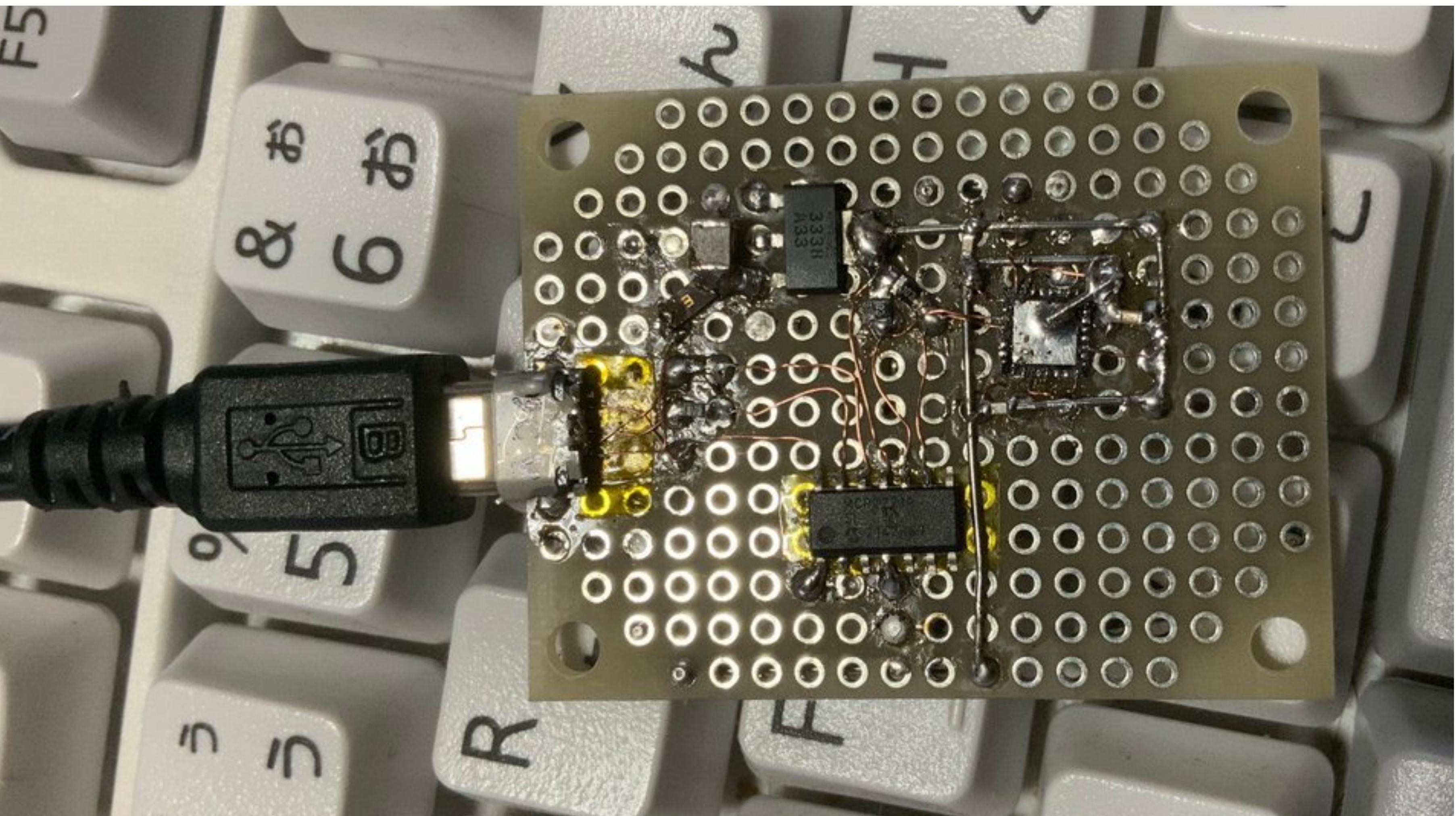
- Infineon OPTIGA TPM SLB9673シリーズ
 - SLB9673AU20FW2610XTMA1
 - 1枚@881JPY, 100枚@647.86JPY
- Atmel / Microchipも出しているが, そちらはNDA必須



TPM / Hardware



TPM / Hardware



TPM / Software

- ・ 目標: TPMをSSH Agentとして使う
- ・ 開発言語はRust
- ・ <https://github.com/ssh-slb9673-playground/tpm-ssh-agent>



TPM / Software

- ・ 目標: TPMをSSH Agentとして使う
- ・ 開発言語はRust
- ・ <https://github.com/ssh-slb9673-playground/tpm-ssh-agent>



TPM / Software / MCP2221A

- MCP2221Aのドライバは一応ある
- google/mcp2221-rs
 - 新しいMacで動かない
 - <https://github.com/libusb/libusb/issues/1014>
- Linux Kernelのhid_mcp2221 (を経由したi2cdev)
 - Linux専用かつ不安定
- ZakKemble/libmcp2221
 - Rust → Cのunsafe wrapperを書きたくない
- 結局hidapi経由でドライバを書いた



TPM / Software / TCTI

- TPMはコマンドで操作する
 - コマンドを送る・受け取る部分はまた別のレイヤ
 - TCTI (TPM Command Transmission Interface)
- 情報が全くない
 - 仕様書自体は丁寧にかかれているので、じっくり読めばわかる
- Device Driver Design Principlesという神ドキュメント



TPM / Software / TPM API

- TCTIがあるおかげで仕様書は独立
 - ⇔ 全く違う仕様書を並行して読むのと同じ労力
- 丁寧だし量もそこまでではない(4分冊で合計2000p程度), しかし各所に散らばった定義を探すのに時間がかかる
 - [1] Chap. 5 "Navigating the Specification"に大変助けられた



TPM / Software / SSH Agent

- 既にRustでSSH Agentのプロトコルを喋るcrateは存在する
 - wiktor-k/ssh-agent-lib
- これまで開発したAPIを活用し、TPM内で生成したRSA鍵に対して「公開鍵リストを提示」「与えられたデータに署名する」をそれぞれやればよい



TPM / Result

```
Wed Aug  9 17:09:15 JST 2023 ~/prog/repo/slb9673_driver
> SSH_AUTH_SOCK=`pwd`/connect.sock ssh shiho@172.16.104.124
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-155-generic x86_6
4)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

0のアップデートはすぐに適用されます。

62 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Aug  9 17:09:11 2023 from 172.16.104.107
Wed Aug  9 17:09:24 JST 2023 ~ 100%
> cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQCI4hYPZn2gtfsgx9LYeKUToW6M
fA31ZiKK0t02yR0LYW7LYAyAGYMfHLf512WTlrgc0hPWZEnlerU84SXGdUUwK9c0
52V6nH8ay5alYmyVNEb280aQV1iW4jQsbY1G0Czf1l0aDEc/v9PvPBpSK+3346CJ
JPT94Da3oRsrVyv7r69F4lqsqpb3NDu+CaQI9YAJpi+qp0pI6ehw+M51Y2XxcA7g
aguwMeM+/7bSNZz0YvBvHIREX7qGQ2fZI+k/0dxfty2khk6wuk6kr7UjgRqMplZ+
Lle3qMWbDmu65Jp/BXWa6g6MRJsR90GBA0luAbjmHye6MWEEnTAp+EJ68FSkl tpm
_key
Wed Aug  9 17:09:31 JST 2023 ~ 100%
> █

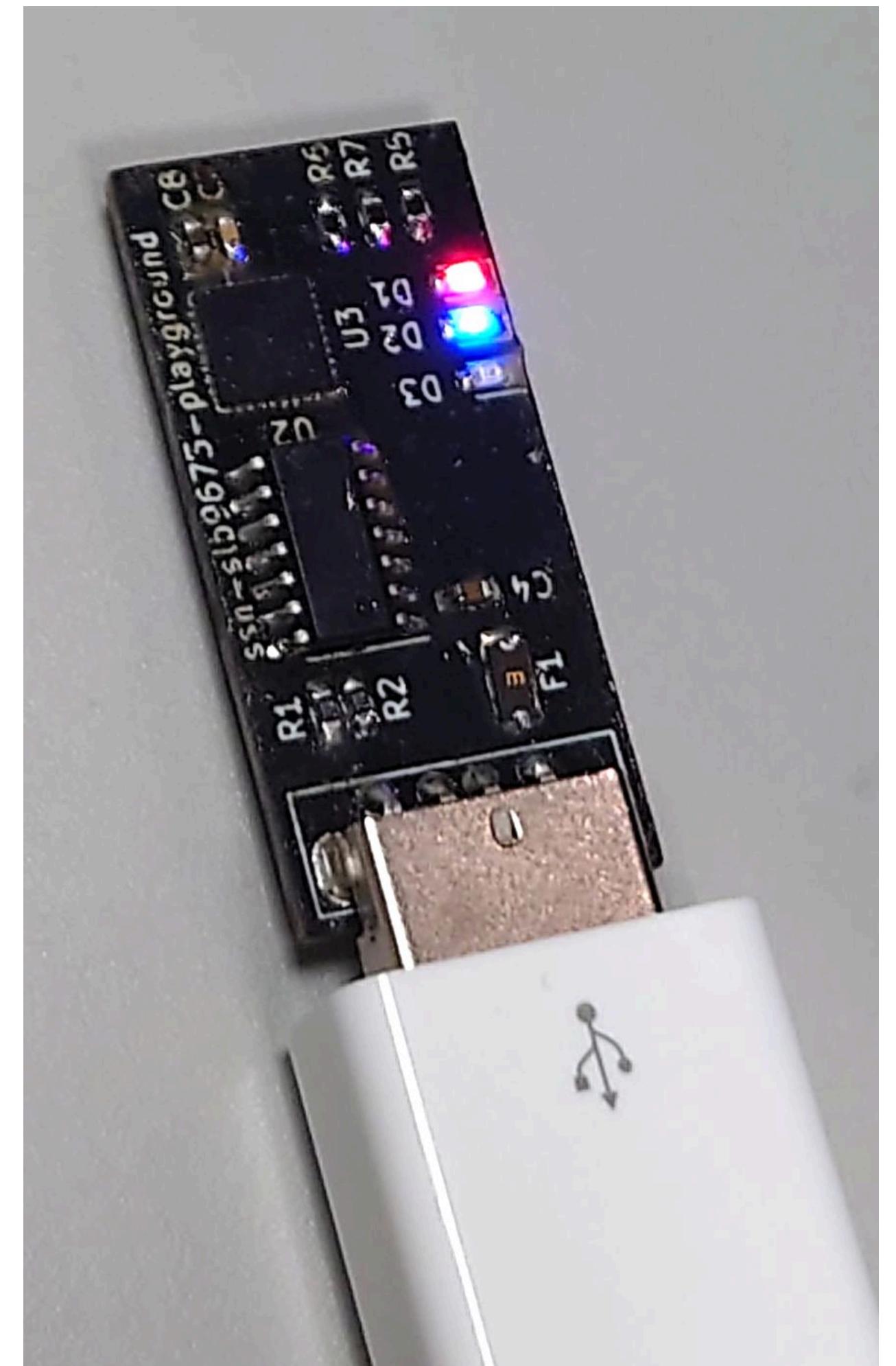
### TPM Information #####
* Vendor ID: 15d1
* Device ID: 001c
* Revision ID: 0016
* Interface Type: FIFO over I2C
* Interface Version: TCG I2C Interface 1.0
* TPM Family: TPM 2.0
* Guard time: 0 usec
* Need Guard time?
  - Write after Write: false
  - Write after Read: false
  - Read after Write: false
  - Read after Read: false
  - ACK/NACK to repeated START: false
* I2C Bus Speed Capabilities
  - Standard Mode: Supported
  - Fast Mode: Supported
  - Fast Mode Plus: Supported
  - High-Speed Mode: Unsupported
* Supported locality: [0, 1, 2, 3, 4]
* Changing I2C Address: Supported (by TCG-defined mechanism)
* Burst count: Dynamic
[+] SSH Public Key: ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQCI4hYP
Zn2gtfsgx9LYeKUToW6MfA31ZiKK0t02yR0LYW7LYAyAGYMfHLf512WTlrgc0hPW
ZEnlerU84SXGdUUwK9c052V6nH8ay5alYmyVNEb280aQV1iW4jQsbY1G0Czf1l0a
DEc/v9PvPBpSK+3346CJPT94Da3oRsrVyv7r69F4lqsqpb3NDu+CaQI9YAJpi+q
p0pI6ehw+M51Y2XxcA7gaguwMeM+/7bSNZz0YvBvHIREX7qGQ2fZI+k/0dxfty2k
hk6wuk6kr7UjgRqMplZ+Lle3qMWbDmu65Jp/BXWa6g6MRJsR90GBA0luAbjmHye6
MWEEnTAp+EJ68FSkl tpm_key
Run agent at connect.sock
refresh nonce
set tpm nonce
rotate nonce
rotate nonce
█
```

Afterwords

- ・仕様書が丁寧な反面解説情報が少ない
 - ・十分に扱いやすいソフトウェアスタックがある ⇔ 自作するメリットが薄
 - ・アーキテクチャの複雑を考えるともう少し情報はほしい
- ・SSH Agentはソケット経由なので、並行プログラミングまで一通り必須
 - ・ちょうどいいプログラミングの教材では？
 - ・今回のプロジェクトは4700行程度

Addendum

- 昨年のL1ゼミ受講生であるsaitenさん(@sort_reverse)にプリント基板を起こしてもらった
 - かっこいい
 - この場を借りて感謝



References

- [1]: Will Arthur, David Challener, and Kenneth Goldman. 2015. *A Practical Guide to TPM 2.0: Using the Trusted Platform Module in the New Age of Security*. Apress Berkeley, CA.
 - オープンアクセス
 - その他仕様書
 - ssh-slb9673-playground/tpm-ssh-agentのREADME.mdに列挙

