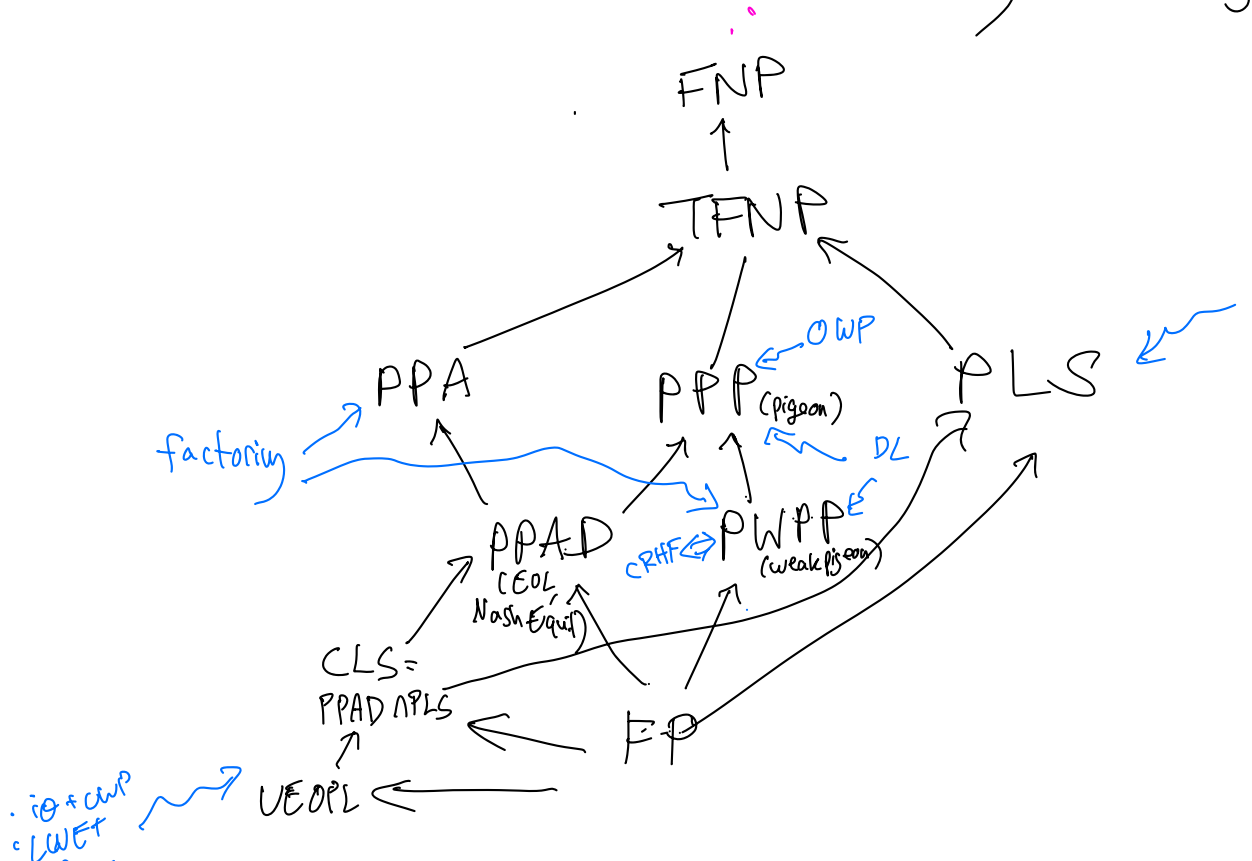
Overview of Crypto ∩ TFNP: some known things, what we'll see later, project ideas

(disclaimer: some inaccuracies, things missing)



$A \to B$: means $A \subseteq B$ (if solving all problems in B easy $\Rightarrow$ " " " " in A")

$A \rightsquigarrow B$ means: if "A is hard" then B is hard.

We saw:

- Factoring $\leq^{\#}$ PPA ∩ PWPP

Next time:

- DL variations in PPP/PWPP, ...

"topic 1 on webpage"

Recall def of OWP: $f: \{0,1\}^n \to \{0,1\}^n$ is a permutation

f is poly computable, and f is a OWF, namely

$\forall$ ppt A $\quad \underset{x \leftarrow \{0,1\}^n}{\text{Prob}}\left[A(f(x)) = x\right] \leq$ negligible

claim: if OWP exist then PIGEON is hard (on average)

pf: Assume f is a OWP.

given $C: \{0,1\}^n \to \{0,1\}^n$

computing f, and $y \in \{0,1\}^n$

↘ given $C: \{0,1\}^n \to \{0,1\}^n$ output preimage of 0^n or a collision $x_1 \neq x_2$ $C(x_1) = C(x_2)$

define $C_y: \{0,1\}^n \to \{0,1\}^n$ as follows:

$$C_y(x) = \begin{cases} C(x) & \text{if } C(x) \neq 0^n \\ y & \text{if } C(x) = 0^n \end{cases}$$

case 1: $y \neq 0^n$: 0^n is not in the co-domain of C_y

PIGEON solver for C_y

gives - ~~preimage of 0^n~~
- collision

C_y has exactly one collision: $C_y(x_1) = C_y(x_2) = y$ the preimage of 0^n + the preimage of y ✓

case 2: $y = 0^n$: $C_y = C$ doesn't have any collision

so PIGEON solver returns

→ found preimage of y

~~preimage of 0^n~~
- ~~collision~~

in any case, PIGEON(c_y) gives $f^{-1}(y)$, i.e. inverts f.

This shows sampling uniformly from $\{c_y\}$ gives a hard distribution for PIGEON $\not\Rightarrow$ efficient solver that succeeds with non-negl prob. ☒

claim: CRHF exist $\Leftrightarrow$ WEAK-PIGEON is hard on average.

pf sketch: follows almost directly from defs.

fixed-length CRHF: efficient (Gen, H) s.t. $Gen(1^n) \to s$

$H^s : \{0,1\}^{L(n)} \to \{0,1\}^n$

$L(n) > n$

(Topic 3+4 on webpage): cryptographic hardness of PPAD (actually CLS)


"unambiguous, incremental, succinct, non-interactive argument"
⇒ PPAD is hard on average.

 = ???

can construct in different ways:

(1) iO + OWP (or from iO + functional-encryption)
↑ can be constructed from a combo of assumptions...

(2) LWE + hardness of IS (iterated squaring) in RSA group.

Note: ⇒ other cool applications (eg VDF)

Viewing this in terms of "Impagliazzo worlds"

- Algorithmica → TFNP = FP (TFNP easy even in worst case)
- Heuristica → TFNP is easy on average
- Pessiland → TFNP is hard on average (Topic 2 on the webpage)
- Minicrypt - OWF ⇒ hardness in TFNP??
  - Minicrypt + OWP → PPP hard on avg
  - CRHF: PWPP hard on avg
- Cryptomania (~factoring/DL) - PPA, PWPP, ... hard on average
  PKE ⇒ hardness in TFNP?

- obfustopia → PPAD (CLS, etc) hard on average

Open problems (and project topics?)

- crypto ⇒ hardness in TFNP?
- hardness in TFNP ⇒ crypto?
- higher/lower classes → eg UEOPL
- other connections → higher in TFPH? Avoid, ...

proof complexity?

In particular:

- in minicrypt:

  Can you show OWF ⇒ hard problem in TFNP?

  → topic 5 on webpage:
  a partial negative answer
  (b.b. separation in some cases)

more generally: better crypto assumption ⇒ PPAD hardness

- in cryptomania: any P.K primitive ⇒ hardness anywhere in TFNP??
- Can you construct a OWF by assuming TFNP avg-case hardness? (other than PPP ⇒ CRHF)

- some b.b. separation PPAD hard $\not\Rightarrow$ OWF

- Factoring in TFNP: Dan has some open problems

eg: OWF + hardness of your favorite TFNP problem

- weak crypto + TFNP hard $\Rightarrow$ strong crypto (PKE)

or crypto + TFNP hard $\Rightarrow$ TFNP harder