COMPUTATIONAL SECURITY

So far: Both encryption and msg integrity are possible even against UNBOUNDED Adv but with strong limitations on usability.
(assuming Alice & Bob share UNIFORM key.)

Want: Overcome barriers for usability, while still retaining some PROVABLE SECURITY.
To do so, we will put restrictions on Adv.

For the rest of the course:

- A_{adv} will be modeled as an "EFFICIENT" machine. $\Rightarrow$ POLYNOMIAL-TIME TURING MACHINE. Moreover, A_{adv} has access to RANDOMNESS.

DEF (PPT TM) A TM A is PPT if its worst-case run time is polynomial, i.e. $\exists\ p(\lambda) \in poly(\lambda)$ s.t. $\forall\ x \in \{0,1\}^*, r \in \{0,1\}^*$ $A(x;r)$ terminates in $p(\lambda)$ steps.

($p \in poly(\lambda)$: $\exists\ c \in \mathbb{N}$ s.t. $p(\lambda) = O(\lambda^c)$.)

λ is input length

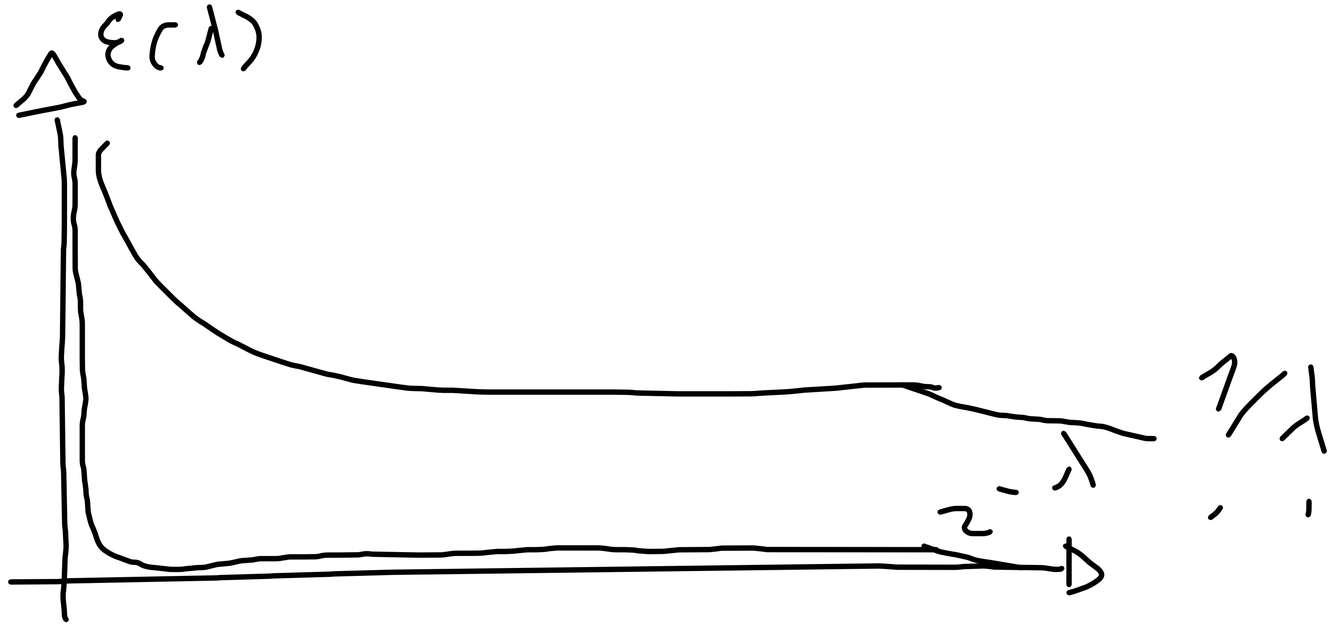
- With "small" probability Adv breaks everything. Fine if it is $\varepsilon = 2^{-80}$.

Asymptotic definition of small: NEGLIGIBLE (in λ).

↳ SECURITY PARAMETER (key length, input length.)

DEF (NEGLIGIBLE) $\varepsilon : \mathbb{N} \to [0,1]$ is negligible (denoted $\varepsilon(\lambda) = negl(\lambda)$) if $\forall\ p(\lambda) \in poly(\lambda)$

$$\varepsilon(\lambda) = O\left(1/p(\lambda)\right).$$



Ex. Show that $\varepsilon = 2^{-\lambda}$ is negl.

Ex. Let $p(\lambda), p'(\lambda) = \text{poly}(\lambda)$, $\varepsilon(\lambda), \varepsilon'(\lambda) = \text{negl}(\lambda)$.

(1) $p(\lambda) \cdot p'(\lambda) = \text{poly}(\lambda)$

(2) $p'(p(\lambda)) = \text{poly}(\lambda)$.

(3) $\varepsilon(\lambda) + \varepsilon'(\lambda) = \text{negl}(\lambda)$

(4) $p(\lambda) \cdot \varepsilon(\lambda) = \text{negl}(\lambda)$

— Base security on well-founded ASSUMPTIONS.

e.g. wt'd be great to assume $P \neq NP$

If problem hard ⇒ scheme "secure"

Examples: Integer FACTORING:

$f(p,q) = n = p \cdot q$ | p, q primes of λ-bit.

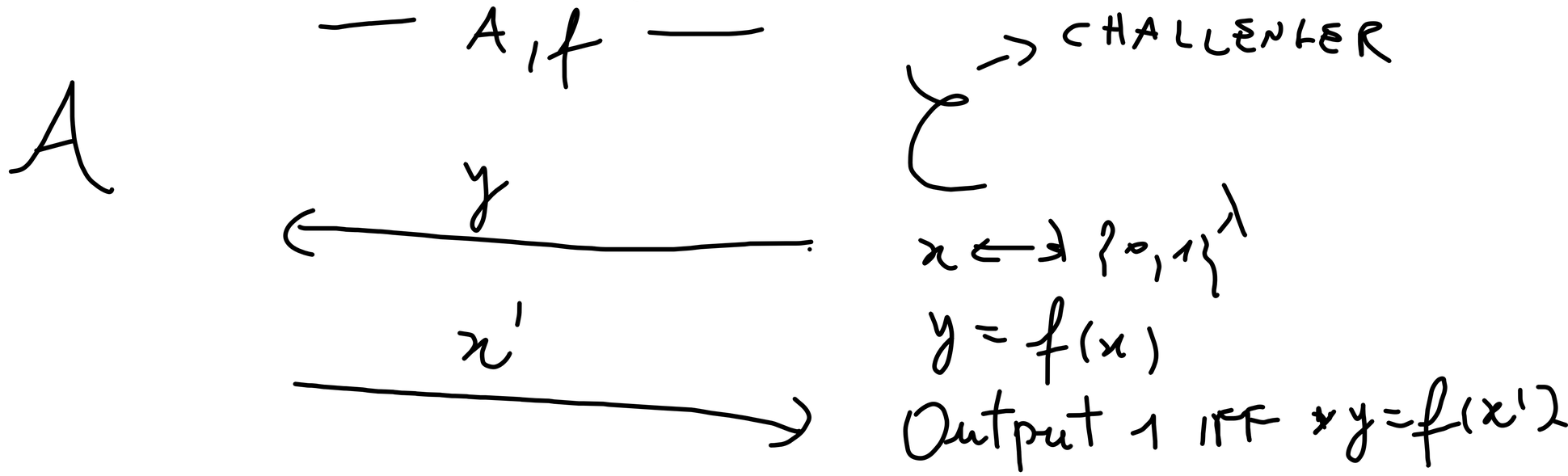
↳ $\lambda = 2048$

ONE-WAY FUNCTION

DEF (OWF) $f : \{0,1\}^* \to \{0,1\}^*$ s.t.

a OWF if: (i) $\forall x \in \{0,1\}^*$ computing $y = f(x)$ takes poly(λ) time; (ii) $\forall$ PPT A it holds $\Pr[\text{GAME}^{owf}_{A,f}(\lambda) = 1] \leq negl(\lambda)$.

$\text{GAME}^{owf}_{A,f}(\lambda)$:



Q: $OWFs \equiv (P \neq NP)$? Don't know.

$OWFs \Rightarrow (P \neq NP)$

P: Class of problems that can solve efficiently

NP: " " " whose solution can be verified efficiently

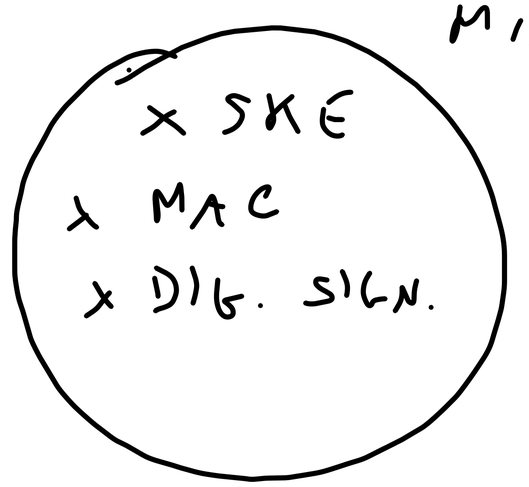
If $P = NP \Rightarrow$ No OWF because given x, I can check efficiently if $y = f(x)$.

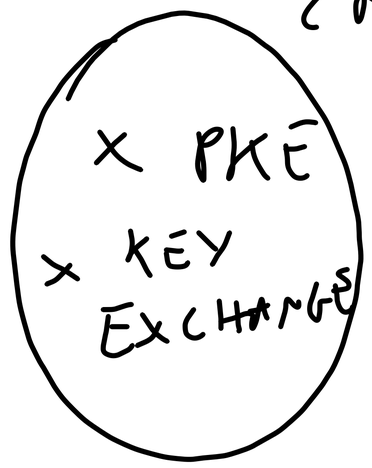
$(P \neq NP) \Rightarrow$ OWF ??!

Russel Impagliazzo:

- ALGORITMICA. $P = NP$ (NO OWFs)
- HEURISTICA. $P \neq NP$, but NO AVG-HARD PUZZLES
- PESSILAND. $P \neq NP$, but NO OWFs

- MINICRYPT. OWFs ←
- CRYPTOMANIA. ← PUBLIC-KEY CRYPTO.
- - - -
- - - - -





DEF (PRG). A function $G : \{0,1\}^\lambda \longrightarrow \{0,1\}^{\lambda + \ell}$ is a PRG with stretch $\ell = \ell(\lambda) > 0$ if: (i) G polynomial time comp.

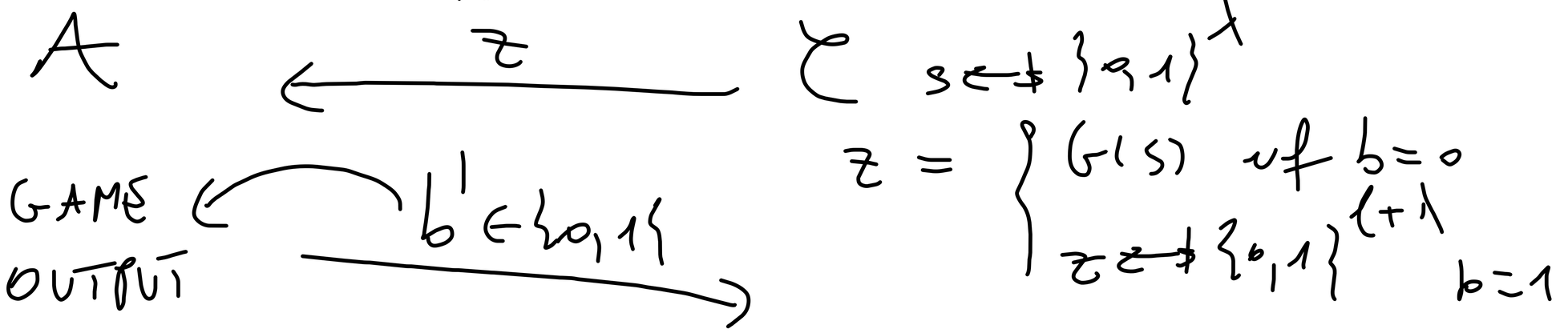
COMP.

INDIST.

(ii) $\forall$ PPT A: $\left| GAME^{PRG}_{A,G}(\lambda,0) \overset{\sim}{\approx}_c GAME^{PRG}_{A,G}(\lambda,1) \right|$

$$\left| Pr[GAME^{PRG}_{A,G}(\lambda,0) = 1] - Pr[GAME^{PRG}_{A,G}(\lambda,1) = 1] \right| \leq negl(\lambda).$$

$GAME^{PRG}_{A,G}(\lambda, b)$ $\quad b \in \{0,1\}$.



Ex. No PRG secure against UNBOUNDED A!

Plan: 1) $Enc(k, m) = G(k) \oplus m$

vs ONE-TIME "SECURE" (COMPUTATIONALLY)

2) OWF $\Rightarrow$ PRG $\leftarrow$ MINICRYPT