Examples of hard problems:

ONE-WAY FUNCTIONS

FACTORING

$n = p \cdot q$

p, q primes (RANDOM)
of size λ bits

DISCRETE LOG

$y = g^x \bmod p$

p is λ-bit prime (PUBLIC)

g is public mod p.

$x \in \{0, 1, \ldots, p-1\}$
RANDOM

POST-QUANTUM PROBLEMS

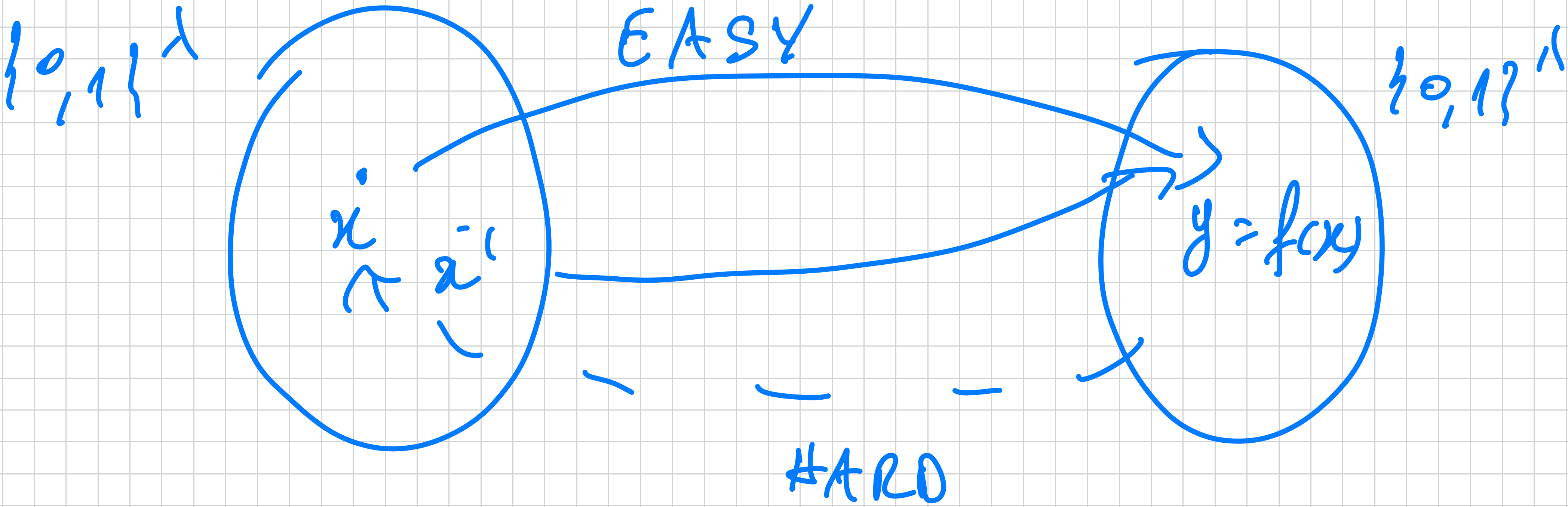
LWE

$P \neq NP$

DEF (OWF). A deterministic function $f : \{0,1\}^\lambda \to \{0,1\}^\lambda$ is a one-way function if: $\forall$ PPT A, $\exists$ negl. function $\varepsilon(\lambda)$ s.t.

$$\Pr\left[f(x') = y : x \leftarrow \{0,1\}^\lambda ; y = f(x) ; x' \leftarrow A(y) \right] \leq \varepsilon(\lambda)$$

(We also assume $f(x)$ is poly-time computable.)



FACTORING : $x = (p, q)$ and $y = n = p \cdot q$.

$$\mathrm{GAME}^{\mathrm{owf}}_{f,\mathcal{A}}(\lambda)$$

$\mathcal{A}$		$\mathcal{C}_{\mathrm{OWF}}$
		$x \leftarrow \{0,1\}^\lambda$
		$y = f(x)$
	$\xleftarrow{\quad y \quad}$	
	$\xrightarrow{\quad x' \quad}$	
		OUTPUT 1 iff $y = f(x')$

EQUIVALENT DEF: f is a OWF if

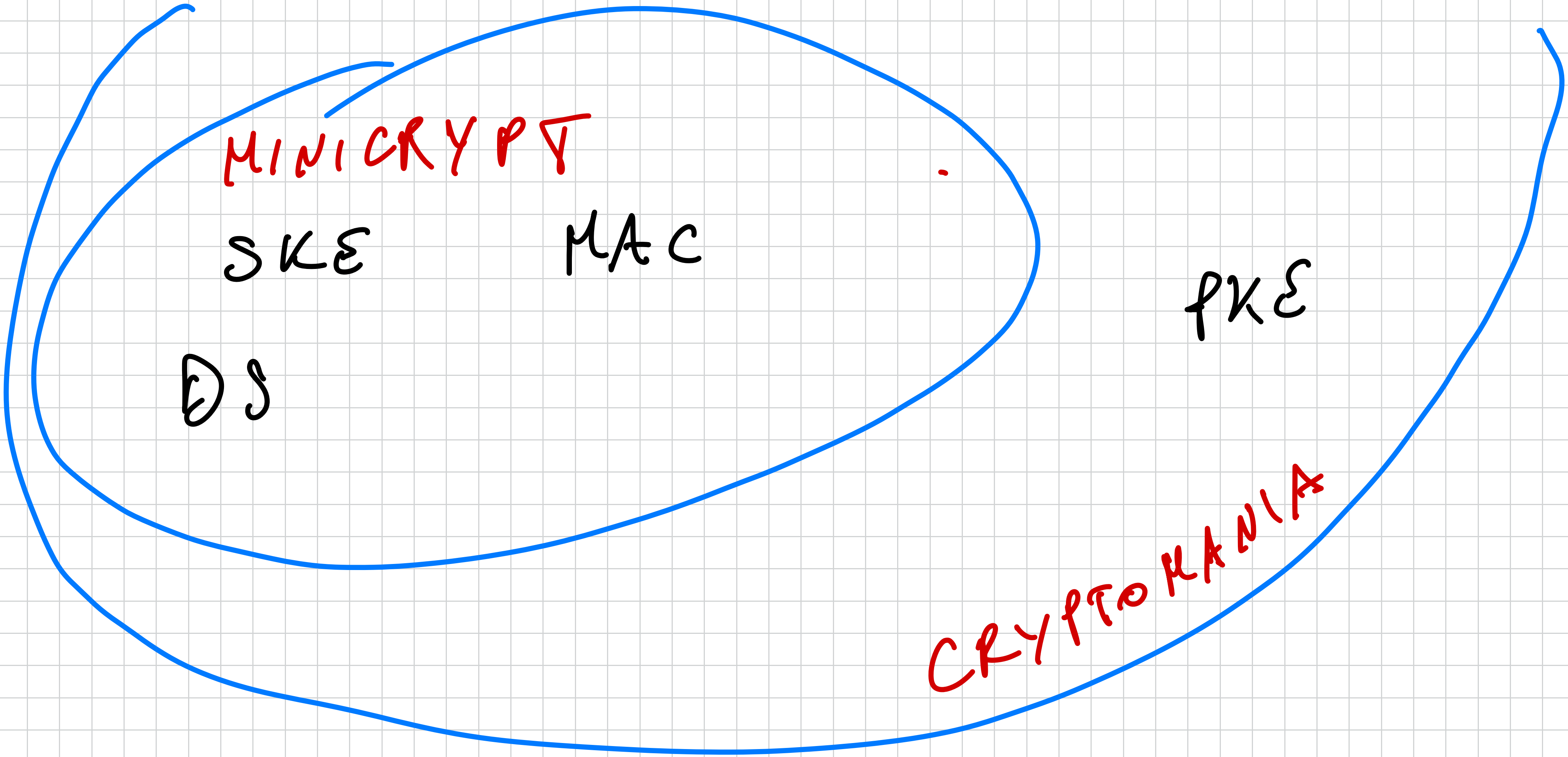
$\forall$ PPT $\mathcal{A}$:

$$\Pr\left[\mathrm{GAME}_{f}^{\mathrm{owf}}(\lambda) = 1 \right] \leq \mathrm{negl}(\lambda)$$

Q: Is the existence of owfs the same as $P \neq NP$? We don't know.

$$\mathrm{OWF} \Rightarrow (P \neq NP).$$

But we don't know $(P \neq NP) \Rightarrow \mathrm{OWF}$



MINICRYPT: OWFs EXIST.

CRYPTOMANIA: PUBLIC-KEY CRYPTO EXIST.

Theory versus Practice.

Symmetric crypto:

- Theory: OWFs or FACTORING, DL, ...
- Practice: Advanced Encryption Standard (AES).

Asymmetric crypto:

- Theory = Practice using concrete problems (FACTORING, DL, ..)

PSEUDORANDOMNESS

In the information-theoretic setting we can't do better than extracting $\approx k$ RANDOM BITS from a source X with min-entropy $\geq k$.

Pseudorandomness: Weaken security in order to produce unlimited randomness.

DEF (PRG). A function $G : \{0,1\}^{\lambda} \to \{0,1\}^{\lambda + \ell(\lambda)}$ is a PRG with stretch $\ell(\lambda)$ if: $\forall$ PPT A

$$\Pr\left[\mathrm{GAME}^{prg}_{G,A}(\lambda) = 1\right] \le \frac{1}{2} + negl(\lambda)$$

(G is deterministic; efficiently computable. $\ell(\lambda) \ge 1$.).

$$\mathrm{GAME}^{prg}_{G,A}(\lambda)$$

A $\qquad\qquad$ $\mathcal{C}_{prg}$

$$A \xleftarrow{\quad z \quad} \mathcal{C}_{prg}$$

$$A \xrightarrow{\quad b' \quad} \mathcal{C}_{prg}$$

$s \leftarrow \{0,1\}^{\lambda}$; $b \leftarrow \{0,1\}$

$$z = \begin{cases} G(s) & \text{if } b = 0 \\ u \leftarrow \{0,1\}^{\lambda+\ell} & \text{if } b = 1 \end{cases}$$

Made with Goodnotes

OUTPUT 1

IFF $b' = b$.

EXERCISE: No PRG can be secure against UNBOUNDED ADVERSARIES.

In the real world: E.g. /dev/rand in LINUX they extract s from min-entropy source X and then use a concrete G.

$$\underline{\mathrm{GAME}}^{prg}_{G,A}\underline{(\lambda, b)}$$

$$\underline{\mathrm{GAME}}^{prg}_{G,A}\underline{(\lambda, 0)} \quad b = 0$$

$$A \xleftarrow{\ z\ } C$$

$s \leftarrow \{0,1\}^\lambda$

$z = G(s)$

$$A \xrightarrow{\ b' \in \{0,1\}\ } C$$

$$\underline{\mathrm{GAME}}^{prg}_{G,A}\underline{(\lambda, b=1)}$$

$$A \xleftarrow{\ z\ } C$$

$$A \xrightarrow{\ b\ } C$$

$z \leftarrow \{0,1\}^{\lambda+\ell}$

\underline{DEF} (PRG) $G : \{0,1\}^\lambda \to \{0,1\}^{\ell+\lambda}$ is a PRG if $\forall A$: $\mathrm{GAME}^{prg}_{G,A}(\lambda, 0) \approx_c \mathrm{GAME}^{prg}_{G,A}(\lambda, 1)$

$\Rightarrow$ It means: $\forall$ PPT $\mathcal{A}$

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

where the game output is $b' \in \{0,1\}$.

Intuitively: If $\mathcal{A}(z)$ can predict s there is no security.

Because $\mathcal{A}$ can check if $z = G(s)$ and if so output $b' = 1$. Otherwise $b' = 0$.

EXERCISE. Every PRG G is also a OWF.

Next times:

- Theory: OWF $\Rightarrow$ PRG with $\ell(\lambda) = poly(\lambda)$

- Practice: Given some amount of stretch (say $\lambda \to 2\lambda$) then we get $\ell(\lambda) = poly(\lambda)$