CSCI 1510

- One-Way Function
- Hard-Core Predicate / Bit
- PRG from OWP

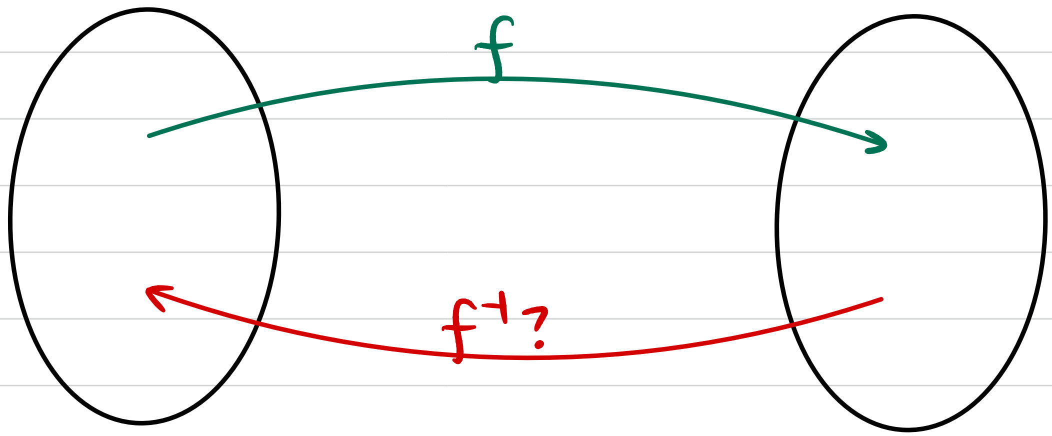
$$
\begin{tikzcd}
 & \text{CPA-Enc} \arrow[dr] & & \text{CCA (Secrecy)} \\
\text{PRF} \arrow[ur] \arrow[dr] & & \text{Authenticated Encryption} \arrow[ur, dash] \arrow[dr, dash] & \\
\text{How to construct?} \arrow[u, bend left] & \text{MAC} \arrow[ur] & & \text{Unforgeable (Integrity)}
\end{tikzcd}
$$

Practical Constructions: Block Cipher

Theoretical Constructions: from One-Way Function (OWF)

One-Way Function

$f: \{0,1\}^* \to \{0,1\}^*$ that is easy to compute & hard to invert.



One-Way Function

<u>Def</u> A function $f: \{0,1\}^* \to \{0,1\}^*$ is a **one-way function (OWF)** if

- easy to compute: $\exists$ poly-time algorithm M_f computing f. $\forall x$. $M_f(x) = f(x)$.
- hard to invert: $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x))] \le \varepsilon(n)$$

One-way permutation (OWP): $\{0,1\}^n \to \{0,1\}^n$, bijective.

$C(1^n)$		$\mathcal{A}(1^n)$
$x \xleftarrow{\$} \{0,1\}^n$		
$y := f(x)$		
	$\xrightarrow{\quad y \quad}$	
		output x'

$\Pr[f(x') = y] \le \varepsilon(n)$.

What if $\mathcal{A}$ is computationally unbounded?

Candidate One-Way Functions

- **Factoring:** $f(x, y) = x \cdot y$

  x, y are n-bit primes

- **Subset Sum:** $f(x_1, x_2, \cdots, x_n, J) = (x_1, x_2, \cdots, x_n, \sum_{j \in J} x_j \bmod 2^n)$

  $x_i \in \{0,1\}^n$ interpreted as an integer
  $J \in \{0,1\}^n$ interpreted as a subset of $[n]$

- **Discrete Log:** $f_{p,g}(x) = g^x \bmod p$

  p is an n-bit prime.
  g is a "generator" for $\mathbb{Z}_p^*$.

- **SHA-2 / AES**

Exercises: Is g necessarily a OWF?

Let $f: \{0,1\}^n \to \{0,1\}^n$ be a OWF.

① $g(x) = \begin{cases} f(x) & \text{if } x \neq 0^n \\ x & \text{otherwise} \end{cases}$.

② $g(x) = f(x)[1 \ldots n-1]$ (least significant bit truncated)

③ $g(x, y) = (f(x), y)$

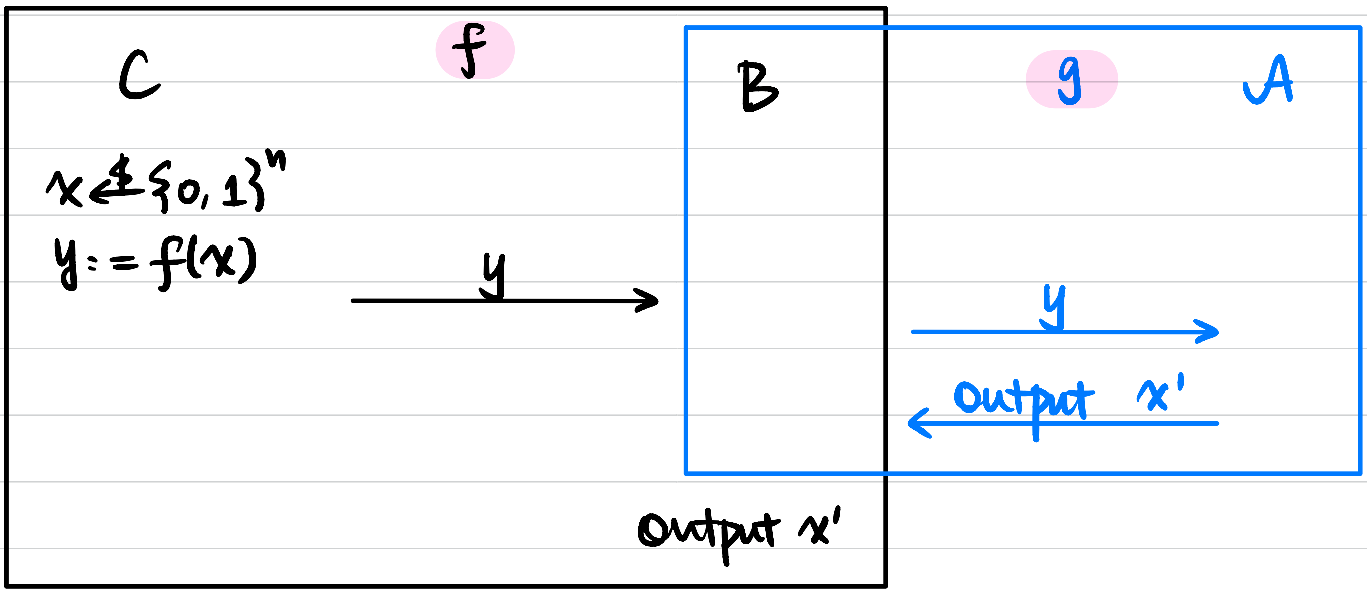
① Let $f: \{0,1\}^n \to \{0,1\}^n$ be a OWF.

$$g(x) = \begin{cases} f(x) & \text{if } x \neq 0^n \\ x & \text{otherwise} \end{cases}$$

g is still a OWF.

<u>Proof</u> Assume not, then $\exists$ PPT $\mathcal{A}$ that breaks the one-wayness of g.

We construct a PPT B to break the one-wayness of f.



$$\Pr[f(x')=y] = \Pr[x=0^n]\cdot\Pr[f(x')=y \mid x=0^n] + \Pr[x\neq 0^n]\cdot\Pr[f(x')=y \mid x\neq 0^n]$$

$$\geq 0 + (1-2^n)\cdot\Pr[g(x')=y \mid x\neq 0^n] \geq \text{non-negl}(n) - 2^{-n}$$

$$\text{non-negl}(n) \leq \Pr[\mathcal{A} \text{ breaks } g] = \Pr[x=0^n]\cdot\Pr[\mathcal{A} \text{ breaks } g \mid x=0^n] + \Pr[x\neq 0^n]\cdot\Pr[\mathcal{A} \text{ breaks } g \mid x\neq 0^n]$$

$$\leq 2^{-n} + (1-2^n)\cdot\Pr[g(x')=y \mid x\neq 0^n]$$

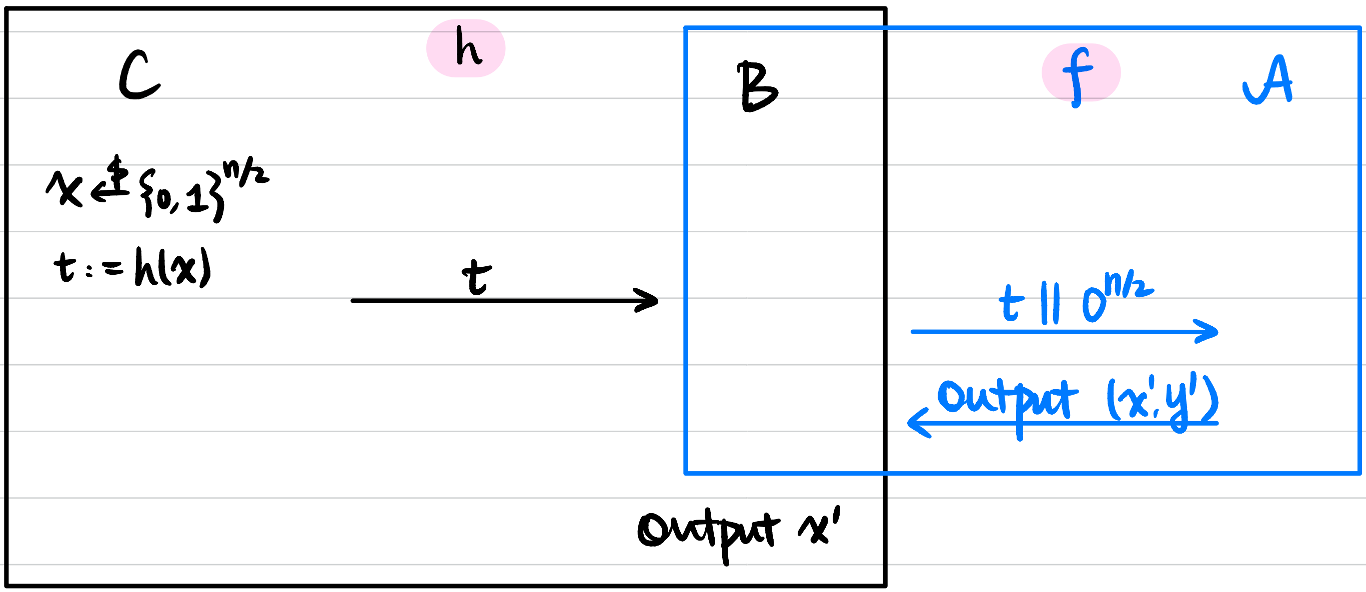
② Let $h: \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ be a OWF.

$$f(x,y) = \begin{cases} h(x) \,\|\, 0^{n/2} & \text{if } y \neq 0^{n/2} \\ x \,\|\, 0^{n/2-1} \,\|\, 1 & \text{otherwise} \end{cases}$$

Step 1: f is a OWF.

<u>Proof</u> Assume not, then $\exists$ PPT $\mathcal{A}$ that breaks the one-wayness of f.

We construct a PPT B to break the one-wayness of h.



$$\Pr[h(x') = t] = \Pr[f(x', y') = t \| 0^{n/2} \mid y \neq 0^{n/2}] \geq \frac{\text{non-negl}(n) - 2^{-n/2}}{1 - 2^{-n/2}}$$

$$\text{non-negl}(n) \leq \Pr[\mathcal{A} \text{ breaks } f] = \Pr[y = 0^{n/2}] \cdot \Pr[\mathcal{A} \text{ breaks } f \mid y = 0^{n/2}] + \Pr[y \neq 0^{n/2}] \cdot \Pr[\mathcal{A} \text{ breaks } f \mid y \neq 0^{n/2}]$$

$$\leq 2^{-n/2} + (1 - 2^{-n/2}) \cdot \Pr[f(x', y') = t \| 0^{n/2} \mid y \neq 0^{n/2}]$$

Let $h: \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ be a OWF.

$$f(x,y) = \begin{cases} h(x) \,\|\, 0^{n/2} & \text{if } y \neq 0^{n/2} \\ x \,\|\, 0^{n/2-1} \,\|\, 1 & \text{otherwise} \end{cases}$$

$$g(x,y) = \begin{cases} h(x) \,\|\, 0^{n/2-1} & \text{if } y \neq 0^{n/2} \\ x \,\|\, 0^{n/2-1} & \text{otherwise} \end{cases}$$

Step 2: g is not a OWF.

We can construct a PPT $\mathcal{A}$ to break the one-wayness of g:

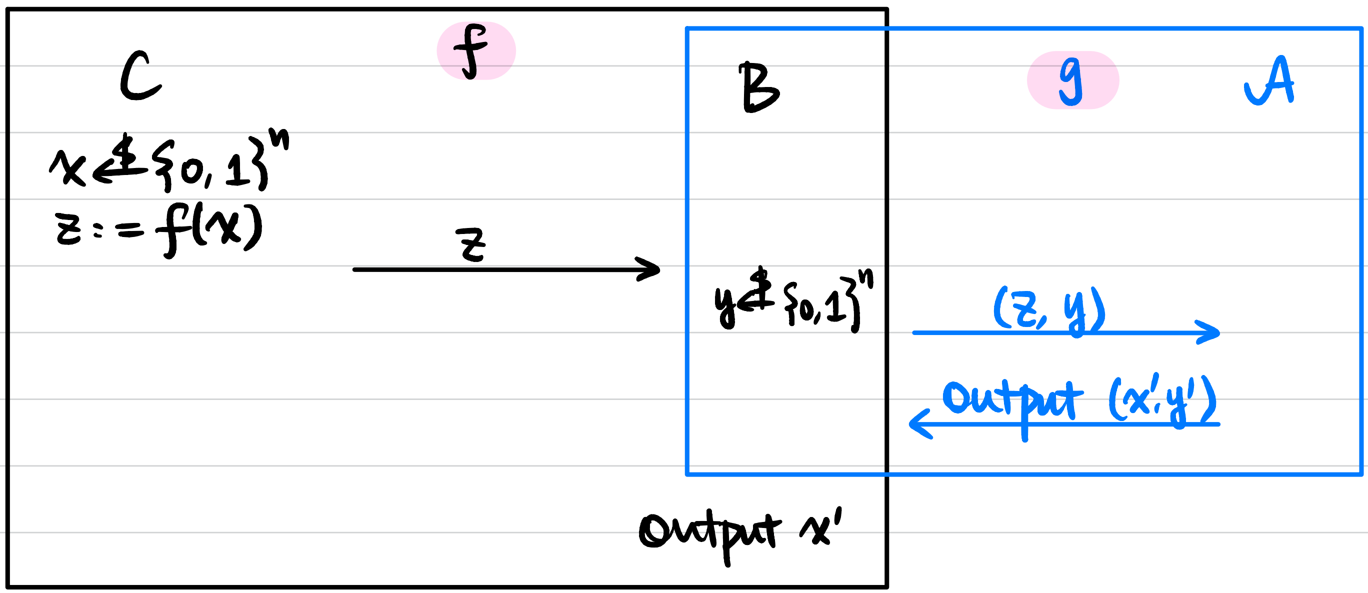
On input $z = t \| 0^{n/2-1}$, output $(x,y) = (t, 0^{n/2})$

③ Let $f: \{0,1\}^n \to \{0,1\}^n$ be a OWF.

$g(x, y) = (f(x), y)$. g is still a OWF.

<u>Proof</u> Assume not, then $\exists$ PPT $\mathcal{A}$ that breaks the one-wayness of g.

We construct a PPT $\mathcal{B}$ to break the one-wayness of f.



$$\Pr[f(x') = z] \geq \Pr[g(x', y') = (z, y)] \geq \text{non-negl}(n).$$

Hard-Core Predicate / Bit

Def A function $hc: \{0,1\}^* \to \{0,1\}$ is a hard-core predicate / bit of a function f if

- hc can be computed in poly time
- $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\mathcal{A}(1^n, f(x)) = hc(x)] \le \frac{1}{2} + \varepsilon(n)$$

$C(1^n)$		$\mathcal{A}(1^n)$
$x \xleftarrow{\$} \{0,1\}^n$		
$y := f(x)$	$\xrightarrow{\ y\ }$	
		output b'

$\Pr[hc(x) = b'] \le \frac{1}{2} + \varepsilon(n)$.

Does every OWF have a hard-core predicate? Open Problem!

Constructing Hard-Core Predicate

Thm (Goldreich-Levin) Assume OWFs (resp. OWPs) exist.

Then there exists a OWF (resp. OWP) g and a hard-core predicate hc of g.

OWP

Given a OWF f,

OWP

Construct another OWF $g(x, r) := (f(x), r)$, $|x| = |r|$.

with a hard-core predicate $hc(x, r) := \bigoplus_{i=1}^{n} x_i \cdot r_i$

Let $f: \{0,1\}^n \to \{0,1\}^n$ be a OWF.

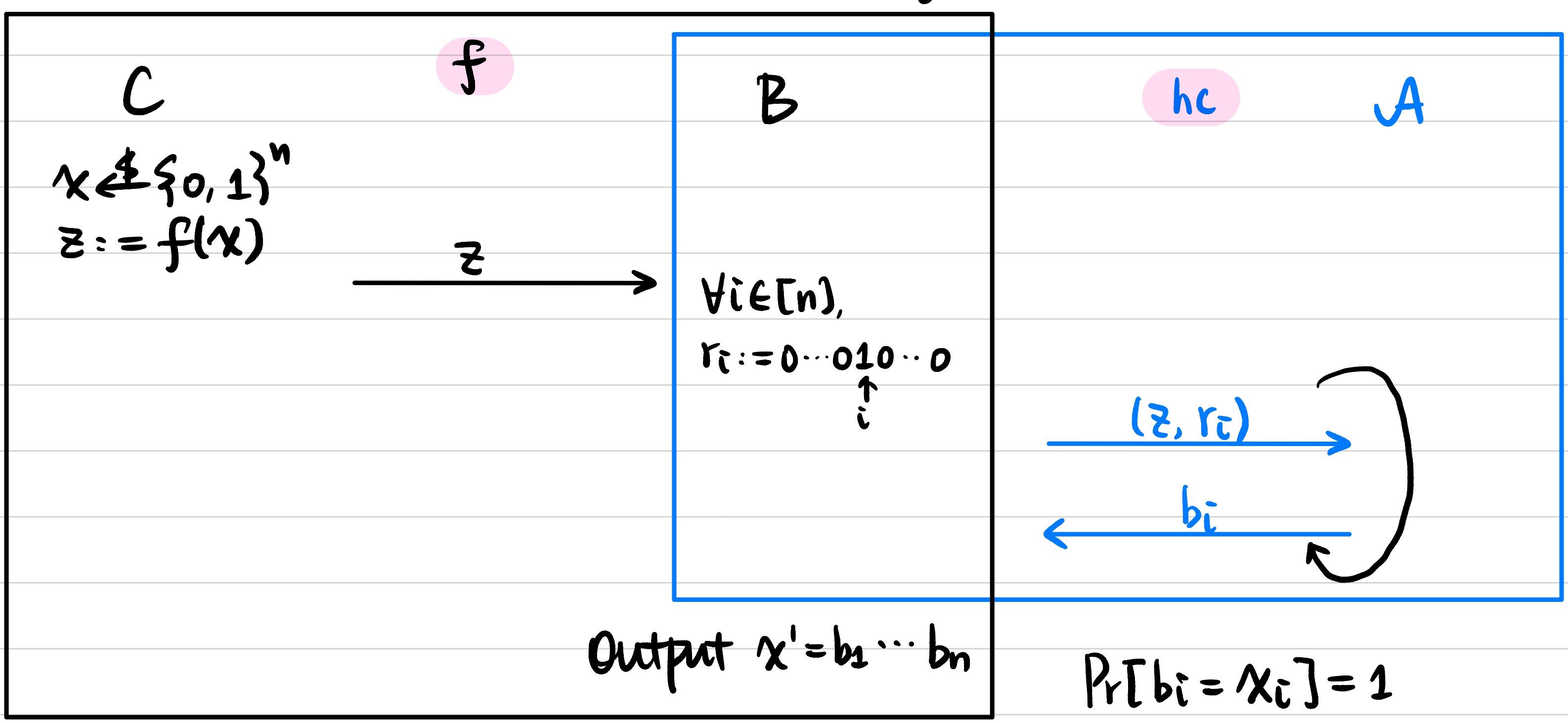
$g(x, r) := (f(x), r)$, $|x| = |r| = n$. g is still a OWF.

$hc(x, r) := \bigoplus_{i=1}^{n} x_i \cdot r_i$

Thm hc is a hard-core predicate of g.

Proof Assume not, then $\exists$ PPT $\mathcal{A}$ that breaks the hard-core predicate hc. ← with probability 1.

We construct a PPT B to break the one-wayness of f.



$\Pr[b_i = x_i] = 1$

$\Pr[x' = x] = 1$.

Constructing PRG from OWP

Let $g : \{0,1\}^n \to \{0,1\}^n$ be a OWP with hard-core predicate hc.

Construct $G : \{0,1\}^n \to \{0,1\}^{n+1}$

$$G(s) = g(s) \,\|\, hc(s).$$

Thm G is a PRG.

$\mathcal{H}_0$: $s \xleftarrow{\$} \{0,1\}^n$, output $g(s) \,\|\, hc(s)$.

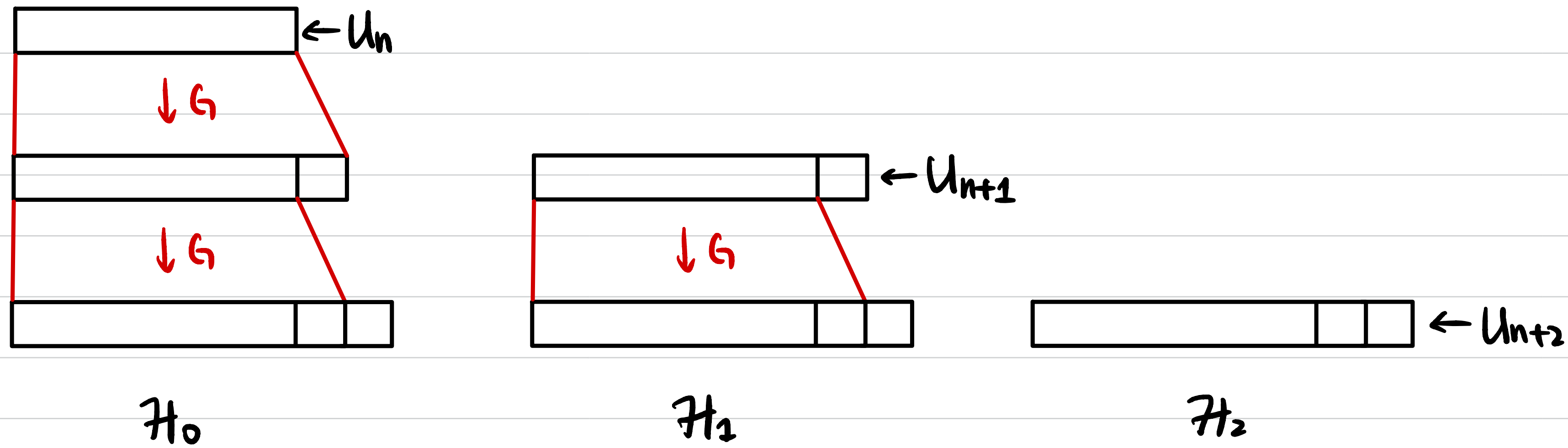
hc security

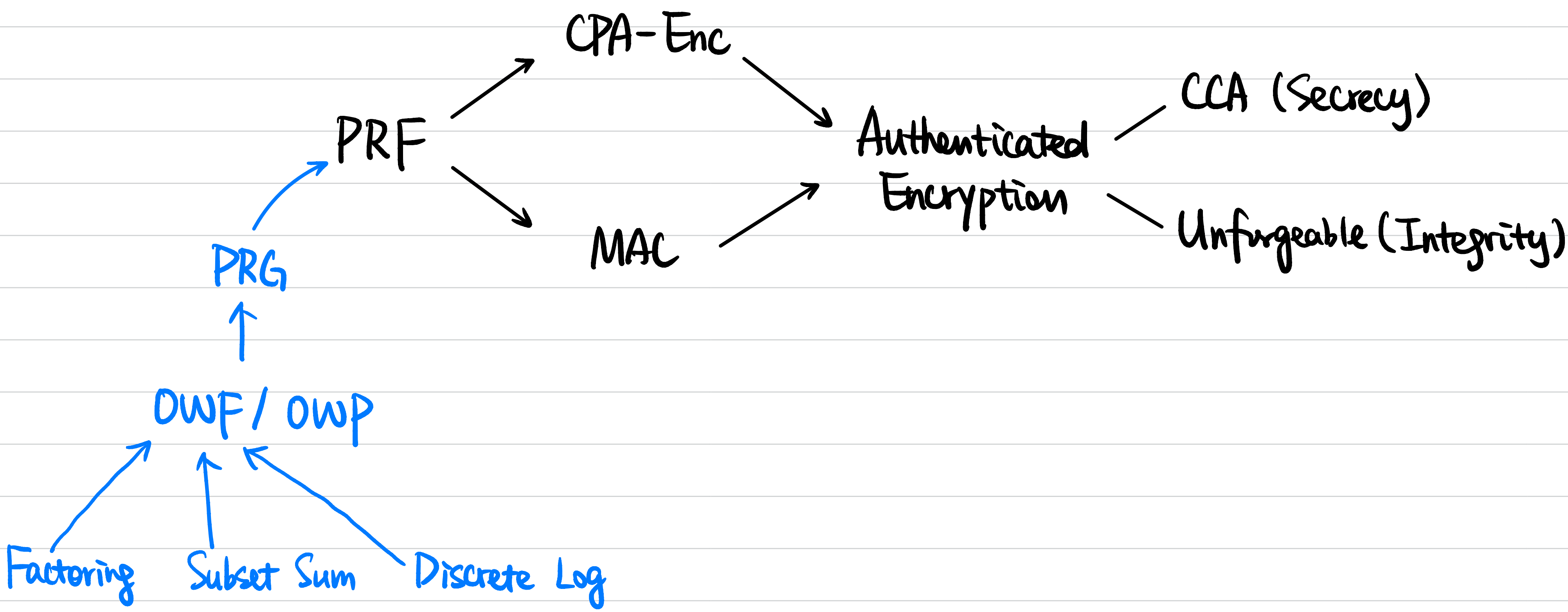
$\mathcal{H}_1$: $s \xleftarrow{\$} \{0,1\}^n$, $b \xleftarrow{\$} \{0,1\}$, output $g(s) \,\|\, b$

identical distribution since g is permutation

$\mathcal{H}_2$: $r \xleftarrow{\$} \{0,1\}^n$, $b \xleftarrow{\$} \{0,1\}$, output $r \,\|\, b$

Increasing the Expansion





CPA-Enc
PRF
MAC
Authenticated Encryption
CCA (Secrecy)
Unforgeable (Integrity)
PRG
OWF / OWP
Factoring
Subset Sum
Discrete Log