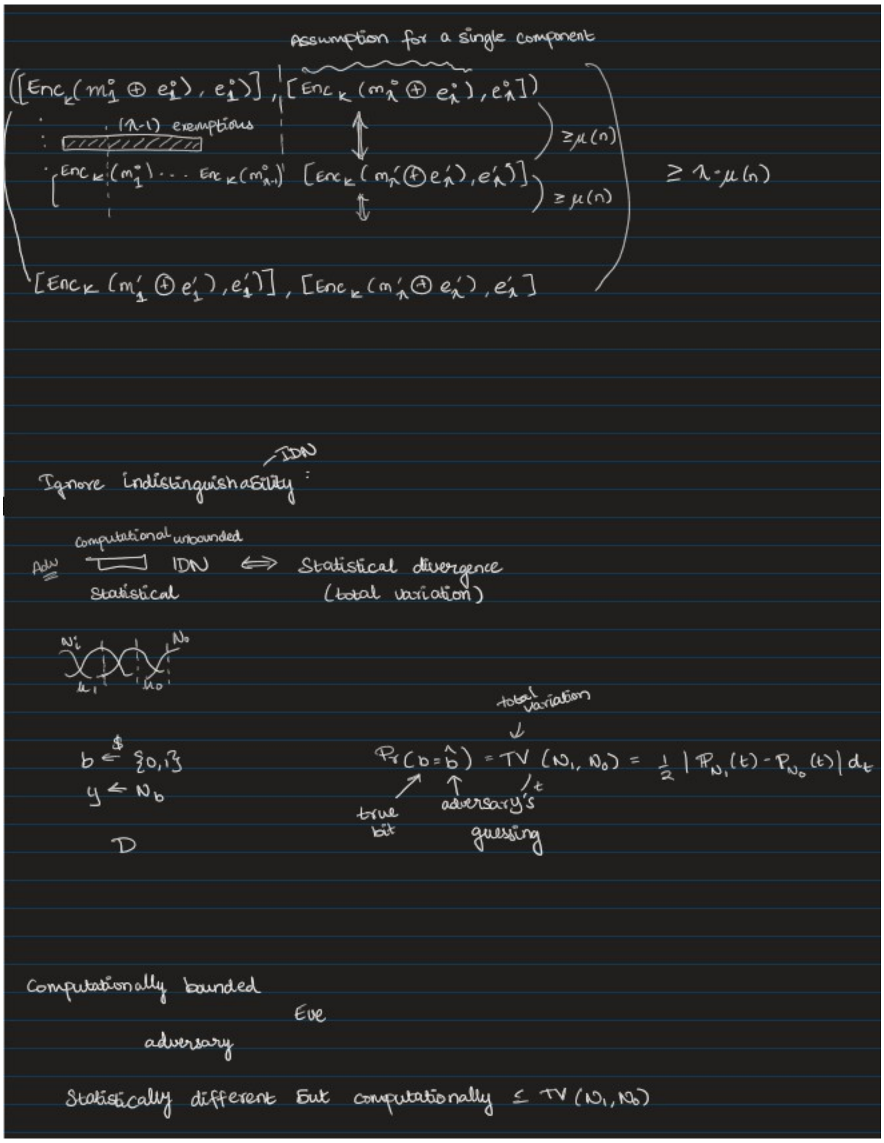
Purdue CS555 Cryptography Lecture 3

September 2, 2025

Initialization Vector and One-time Padding



Key Lemma: Hybrid Argument for Accumulated Advantage

i. User randomly selects two sequences $\{m_1^0, m_2^0, \ldots, m_\lambda^0\}$ and $\{m_1^1, m_2^1, \ldots, m_\lambda^1\}$ where each m_i^0 and m_i^1 are i.i.d. uniform, and sends them to adversary

ii. User randomly selects key k and $b \leftarrow \{0, 1\}$, and sends $\mathbf{c} = \{\text{Enc}(k, m_1^b), \ldots, \text{Enc}(k, m_\lambda^b)\}$ to adversary

iii. For any PPT algorithm Eve: $\Pr[\text{Eve}(\mathbf{c}) = b] \leq \frac{1}{2} + \lambda \cdot \mu(n)$

Pseudorandom Generators (PRG)

Definition

A pseudorandom generator (PRG) is a deterministic function $G : \{0,1\}^* \to \{0,1\}^*$ that takes as input a (short) random seed $s \leftarrow \{0,1\}^\lambda$ and stretches it into a longer string $G(s) \in \{0,1\}^n$ that "looks random."

Formal Definition: A deterministic polynomial-time computable function $G : \{0,1\}^n \to \{0,1\}^m$ is a PRG if:

- **Expansion:** $m > n$ (output longer than input)
- **Pseudorandomness:** For every PPT algorithm D (distinguisher), there exists negligible function μ such that:
$$|\Pr[D(G(U_n)) = 1] - \Pr[D(U_m) = 1]| = \mu(n)$$
where U_ℓ denotes uniform distribution over $\{0,1\}^\ell$.

Overcoming Shannon's Conundrum

Using PRG, we can encrypt $(n+1)$-bit message with n-bit key

Construction:

- $\text{Gen}(1^n)$: Generate random n-bit key k
- $\text{Enc}(k, m)$: Expand k into $(n+1)$-bit string $k' = G(k)$, output $c = k' \oplus m$
- $\text{Dec}(k, c)$: Output $G(k) \oplus c$

Correctness: $\text{Dec}(k, c) = G(k) \oplus c = G(k) \oplus (G(k) \oplus m) = m$

Security (First Reduction): Suppose for contradiction there exists PPT Eve and polynomial p such that:
$$\Pr[k \leftarrow \{0,1\}^n; b \leftarrow \{0,1\}; c = G(k) \oplus m_b : \text{Eve}(c) = b] \geq \frac{1}{2} + \frac{1}{p(n)}$$

But with truly random key: $\Pr[k' \leftarrow \{0,1\}^{n+1}; c = k' \oplus m_b : \text{Eve}(c) = b] = \frac{1}{2}$ (one-time pad security).

This gives us distinguisher Eve' for G, contradicting PRG assumption.

Next-Bit Unpredictability (NBU)

Alternative Definition

A function $G : \{0,1\}^n \to \{0,1\}^m$ is **next-bit unpredictable** if for every PPT algorithm P (predictor) and every $i \in \{1, \ldots, m\}$, there exists negligible μ such that:
$$\Pr[y \leftarrow G(U_n) : P(y_1 y_2 \ldots y_{i-1}) = y_i] = \frac{1}{2} + \mu(n)$$

Intuition: Given first $i-1$ bits of PRG output, cannot predict i-th bit better than random guessing.

Equivalence Theorem

Theorem: A PRG G is indistinguishable if and only if it is next-bit unpredictable.

Indistinguishability $\Rightarrow$ NBU: If predictor P succeeds, construct distinguisher D:

1. On input y, run P on prefix $y_1 y_2 \ldots y_{i-1}$
2. If P returns y_i, output 1 ("PRG"), else output 0 ("Random")

Then: $\Pr[D(G(U_n)) = 1] \geq \frac{1}{2} + \frac{1}{\text{poly}(n)}$ but $\Pr[D(U_m) = 1] = \frac{1}{2}$.

NBU $\Rightarrow$ Indistinguishability: Harder direction, uses hybrid argument.

Hybrid Argument

Averaging Lemma (Pigeonhole)

Let $p_0, p_1, \ldots, p_m$ be real numbers such that $p_m - p_0 \geq \varepsilon$. Then there exists index i such that $p_i - p_{i-1} \geq \varepsilon/m$.

Proof: $p_m - p_0 = \sum_{j=1}^{m}(p_j - p_{j-1}) \geq \varepsilon$. At least one term must be $\geq \varepsilon/m$.

Extension: From 1-bit to Many-bit