

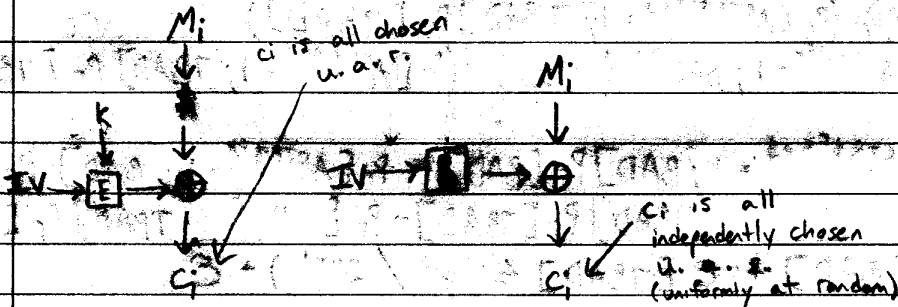
Defn Real or Random (R-or-R)

Encryption algorithm E is secure if $E_k \sim E_k \circ \$$

all information except length is thrown away

Thm IF F is a (t, q, ϵ) PRF, then CTR^F is $(t - O(q), \min(q, |Ctrs|), \epsilon)$ R-or-R secure.

Proof $CTR^{F_k} \circ \$ = CTR^R$ if the IV never repeats.



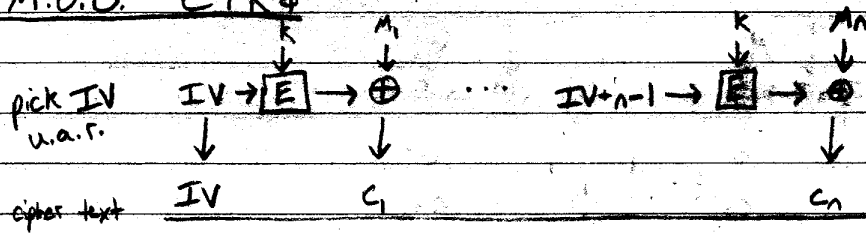
So, suppose $A(t - O(q), q, \epsilon)$ distinguishes CTR^{F_k} and $CTR^{F_k} \circ \$$, where $q \leq |Ctrs|$.

Then, A can also distinguish CTR^{F_k} and CTR^R .

Then, $B^{\circ} = A^{CTR^{\circ}}$ will distinguish F_k and R with advantage ϵ . B will make $q \leq |Ctrs|$ queries, and runs in $t - O(q) + O(q) = t$ time.

This contradicts that F is a (t, q, ϵ) PRF.

M.O.O. CTR\$



Thm If F is a (t, q, ϵ) PRF, then $CTR\F is $(t - O(q), q, \epsilon + \frac{q^2}{2^{2n+1}})$ P-or-R secure.

Proof When no counters repeat in the queries, $CTR\$^{F_k} \circ \$ = CTR\R .
And like before, $CTR\$^R \xrightarrow{+O(q)q} CTR\F_k

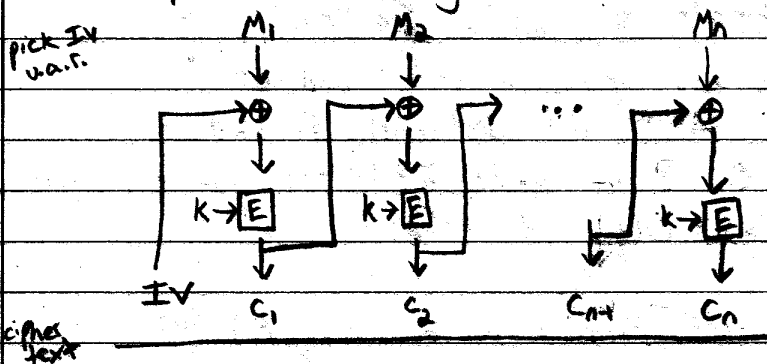
So, if IVs never repeat, then $CTR\$^{F_k} \circ \$ \xrightarrow{+O(q)q} CTR\F_k

$$\text{Adv } A = |Pr[A^{CTR\$^{F_k} \circ \$} = 1] - Pr[A^{CTR\$^{F_k}} = 1]| = |Pr[A^{CTR\$^{F_k} \circ \$} = 1; \text{BAD}] Pr[\text{BAD}] + Pr[A^{CTR\$^{F_k} \circ \$} = 1; \neg \text{BAD}] Pr[\neg \text{BAD}] - (Pr[A^{CTR\$^{F_k}} = 1; \text{BAD}] Pr[\text{BAD}] - Pr[A^{CTR\$^{F_k}} = 1; \neg \text{BAD}] Pr[\neg \text{BAD}])|$$

$$\leq |Pr[A^{CTR\$^{F_k} \circ \$} = 1; \text{BAD}] Pr[\text{BAD}] - Pr[A^{CTR\$^{F_k}} = 1; \text{BAD}] Pr[\text{BAD}]| + |Pr[A^{CTR\$^{F_k} \circ \$} = 1; \neg \text{BAD}] Pr[\neg \text{BAD}] - Pr[A^{CTR\$^{F_k}} = 1; \neg \text{BAD}] Pr[\neg \text{BAD}]|$$

$$\leq 1 \cdot Pr[\text{BAD}] + \epsilon Pr[\neg \text{BAD}] \leq (q^2 / 2^{2n+1}) + \epsilon$$

M.O.O. Cipher Block Chaining (CBC)



- parallel decryption
- single-bit error results in only two errors in output (decreases integrity)