VARIABLE INPUT LENGTH (SAE)

Recall: $Enc(k, m) = (F_k(r) \oplus m, r)$

CPA-secure.

Q: What if $m = (m_1, m_2, \ldots, m_t)$

$t \in \mathbb{N}$; $|m_i| = \lambda$ or $m(\lambda) = n$

Options:

1) Use some F with range n.

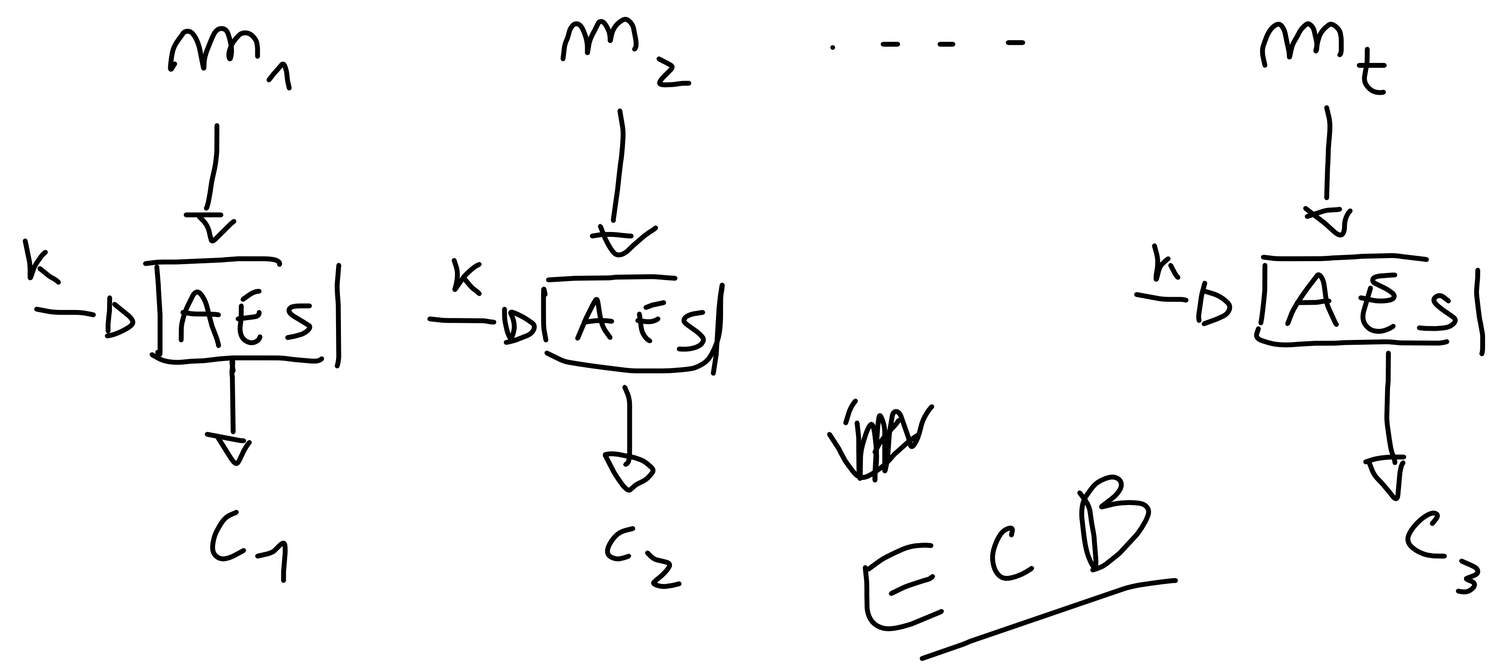
AES: $n = 256$

2) Mode of operation (ANSI/ISO STD).

Given $F_k : \{0,1\}^n \to \{0,1\}^n$ (AES) / (PRF)

use it to get VIL CPA-secure SKE.

Standards: CBC, ~~OFB~~ CFB, OFB, CTR.



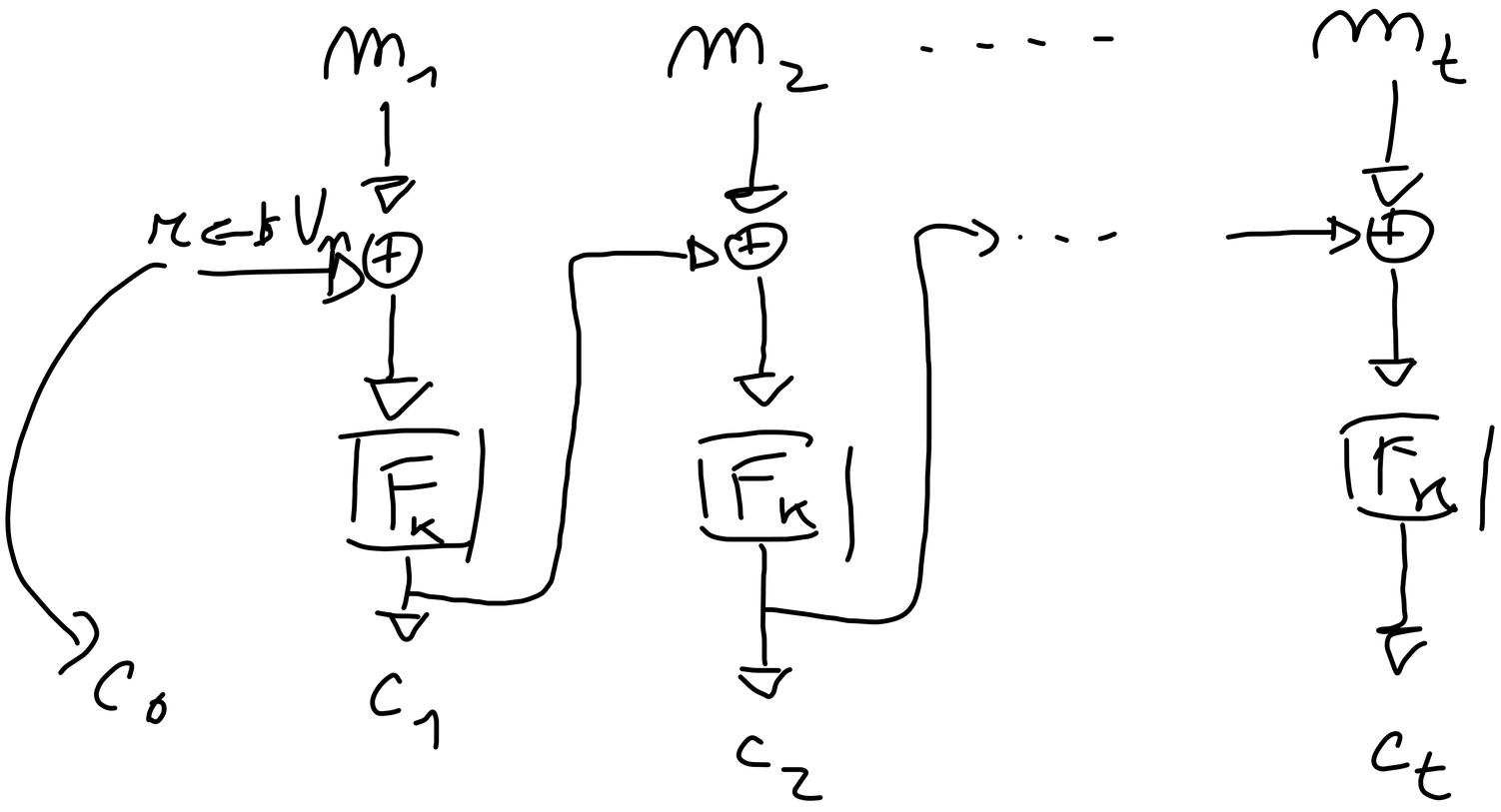
ECB

Deterministic

NOT

CPA-secure

CBC



$C = (c_1, \dots, c_t)$.

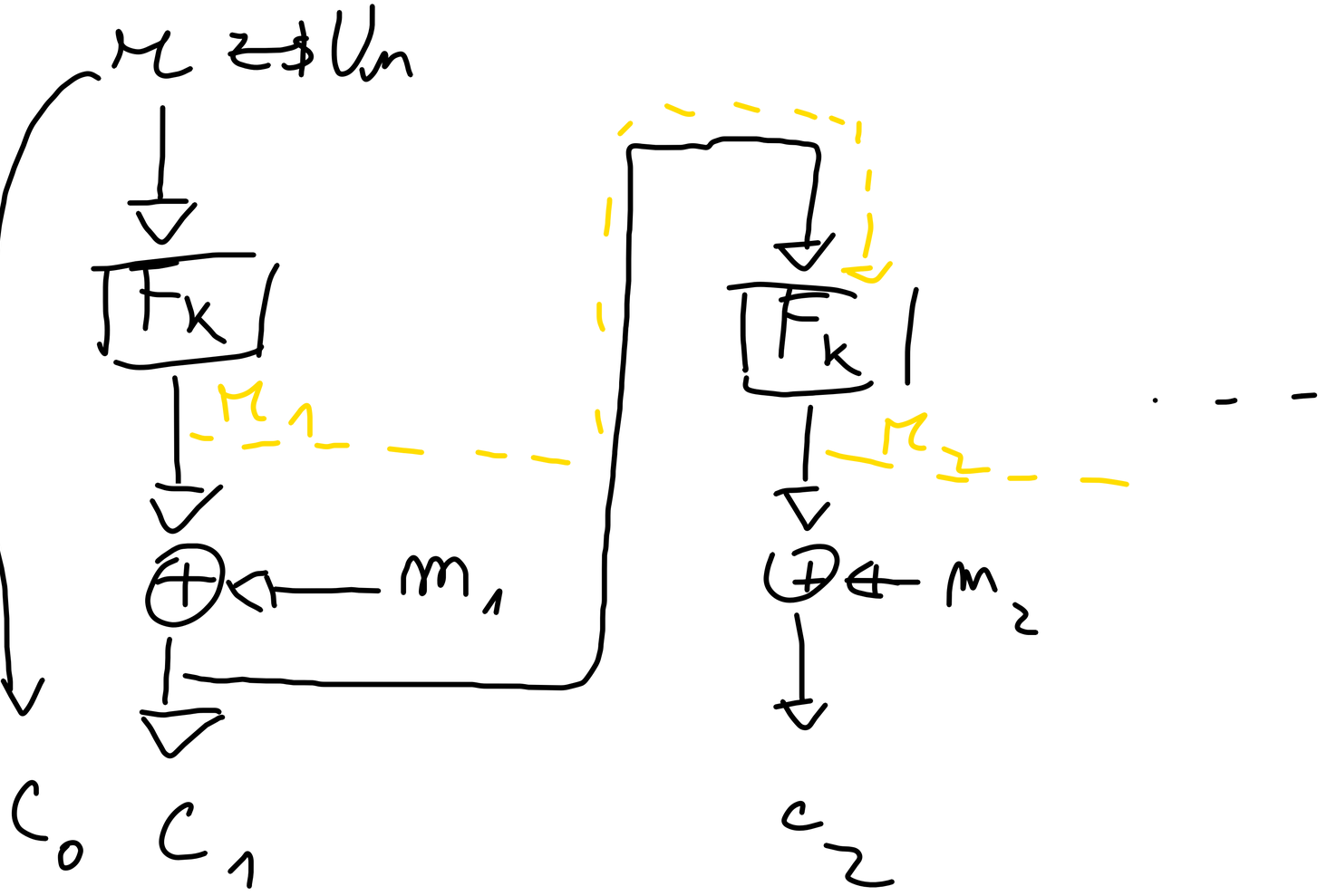
$c_i = F_k(c_{i-1} \oplus m_i)$

$c_0 = r$.

Issue: How to invert F_k ??? See later lecture!

- AES is invertible!
- Need a PRP (Pseudorandom Permutation)

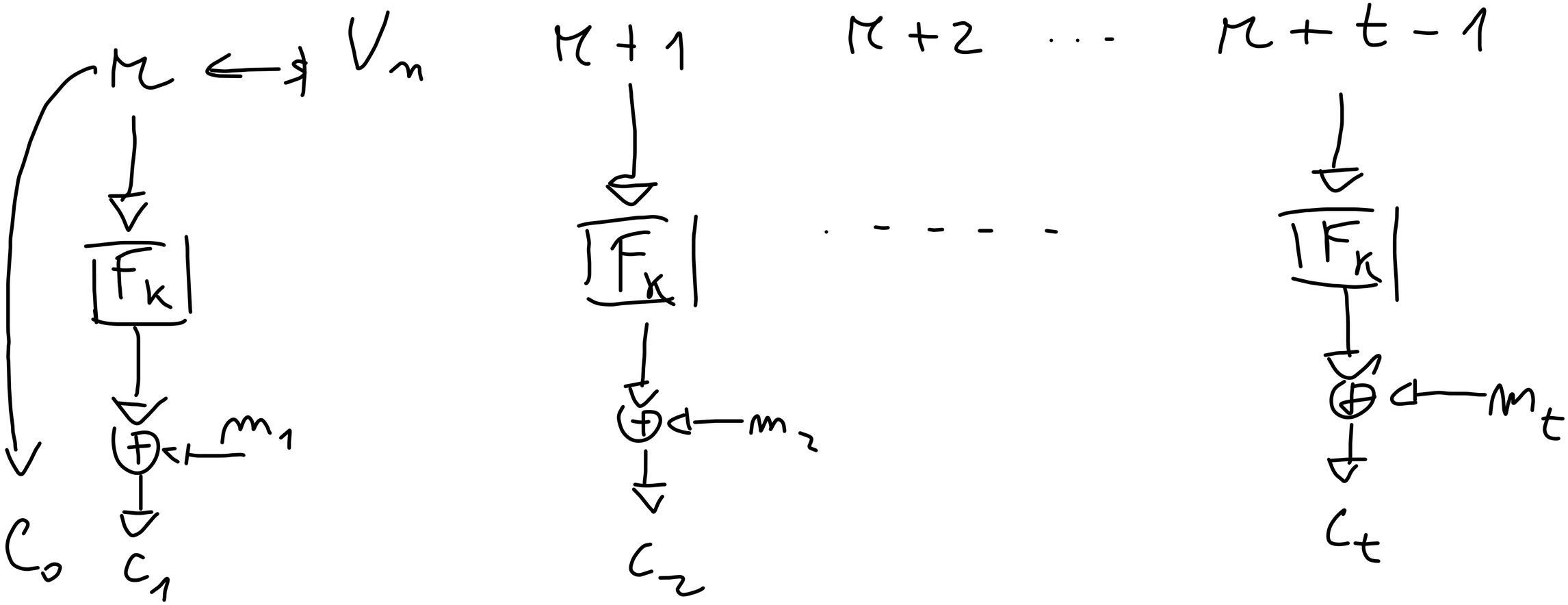
CFB / OFB



No need to invert F_k (PRF vs func)

CTR

Think of n as $n \in \mathbb{N}$ with $n \leq 2^m - 1$.



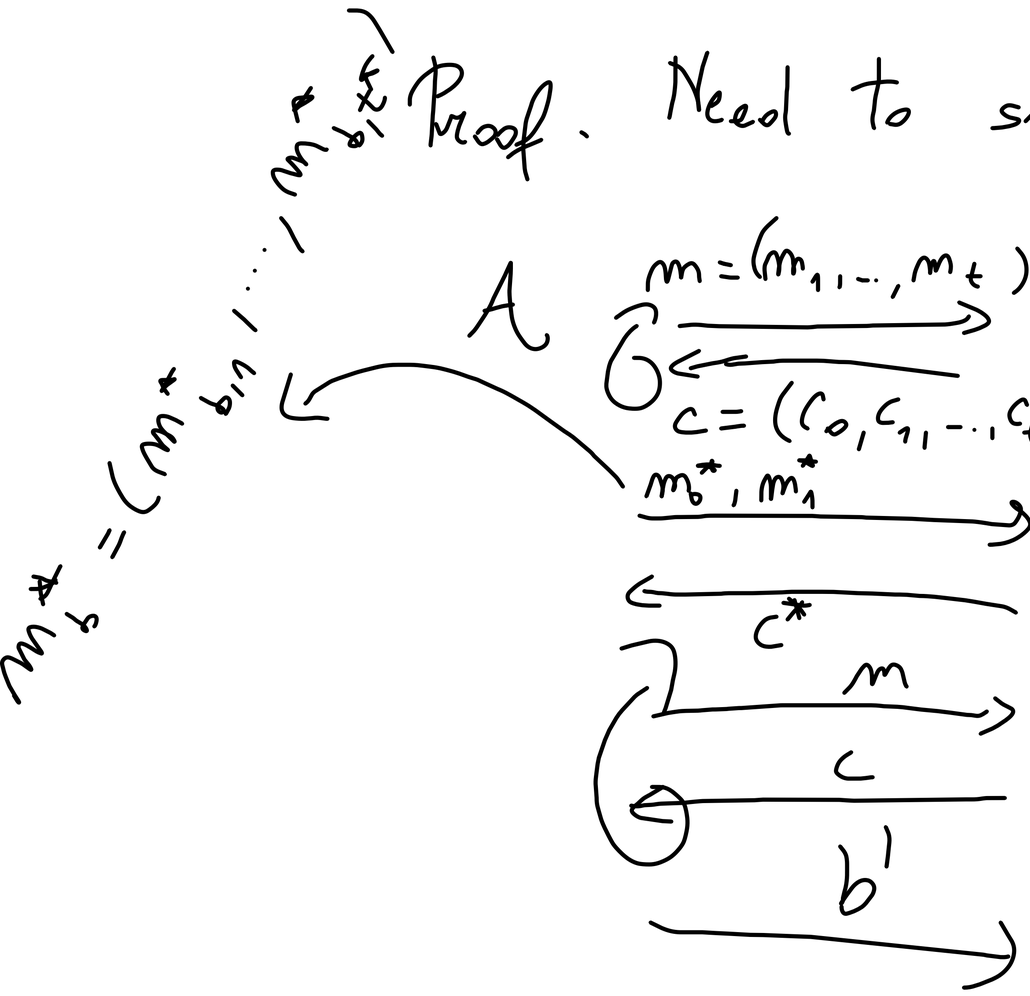
Addition mod 2^m

THM. Assuming $\mathcal{F} = \{F_k\}$ is a PRF, the above SKE is CPA-secure for VIL.

Proof. Need to show $\text{GAME}^{cpa}(\lambda, 0) \approx_c \text{GAME}^{cpa}(\lambda, 1)$

$\left(m_b^* = (m_b[1], \dots, m_b[t])\right)$

↪ If you like it



$k \leftarrow\$ V_\lambda$

$\begin{cases} r \leftarrow\$ V_n \\ c_0 = r \\ c_i = F_k(r+i-1) \oplus m_i \end{cases}$

$r^* \leftarrow\$ V_n$

$c_0^* = r^* + 1 \quad c^* = (c_0^*, \dots, c_t^*)$

$c_i^* = F_k(r^*+i-1) \oplus m_{b,i}^*$

Define $HYB(\lambda, b)$ to be the same except that

$$c_i = R(r_i + i - 1) \oplus m_i; \quad c_i^* = R(r^* + i - 1) \oplus m_{b,i}^*$$

$$R \leftarrow\$ \mathcal{R}(\lambda, n, n).$$

$$n = n(\lambda).$$

LEMMA $HYB(\lambda, 0) \overset{\sim}{\approx}_c HYB(\lambda, 1)$ $\rightarrow$ $\overset{\sim}{\approx}_s$ STATISTICAL!

LEMMA $GAME(\lambda, b) \overset{\sim}{\approx}_c HYB(\lambda, b)$, $\forall\, b \in \{0,1\}$.

Proof. Reduction to PRF security. Standard. ▨

→ Proof. We use $R(\cdot)$ on $r^*, r^*+1, \ldots, r^*+t^*-1$.

And for each $i \in [q]$ also on $r_i, r_i+1, \ldots, r_i+t_i-1$

Let BAD be the event that the sequence

$r^*, r^*+1, \ldots, r^*+t^*-1$ OVERLAPS at some

point with $r_i, r_i+1, \ldots, r_i+t_i-1$ $\forall i$.

BAD: $\exists i, j, j'$ s.t. $i \in [q]$

$r_i + j = r^* + j'$ $0 \le j \le t_i - 1$

$0 \le j' \le t^* - 1$

If $\overline{\text{BAD}}$, then m_b^* is encrypted via OTP and

thus perfectly hidden ($HYB(\lambda,0) \equiv HYB(\lambda,1)$ conditioned on $\overline{\text{BAD}}$).

By the LEMMA of GAME PLAYING, we just prove

$\Pr[\text{BAD}] \le \text{negl}(\lambda)$.

Let $t^*, t_i = q = poly(\lambda)$.

For $i \in [q]$, let BAD_i the event that

$r_i, r_i + 1, \ldots, r_i + 6q - 1$ overlaps.

$$\Pr[BAD] = \Pr[\exists i : BAD_i]$$

$$\leq \sum_{i=1}^{q} \Pr[BAD_i] \leq \frac{2q^2}{2^m} = negl(\lambda)$$

Fix r^*. There is OVERLAP if $r^* - q + 1 \leq r_i \leq r^* + q - 1$

So $\Pr[BAD_i] \leq \frac{2q-1}{2^m}$