Security Analysis of HyENA Authenticated Encryption Mode

A.Chakraborti*, N.Datta, A.Jha, S.Mitragotri, M.Nandi

*NTT Secure Laboratories, Japan
Indian Statistical Institute, Kolkata, India

Nov 06, 2019

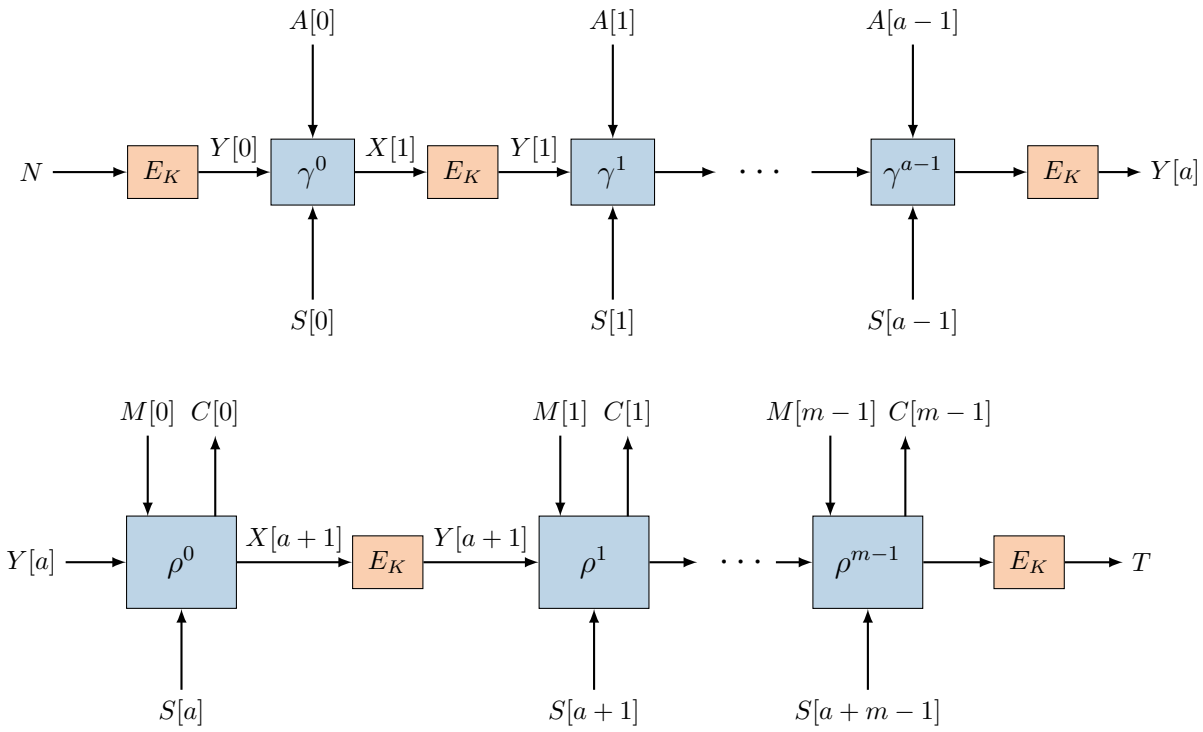
Motivation

Designing Lightweight Authenticated Encryption

- Full Rate.
- Small state size.
- Small additional operations (constant mult, xor etc).

Typical Design Choice

- Use feedback based sequential block-cipher (n-bit) mode.
- State size: block-cipher state + additional auxiliary (masking) state.



Choice of Feedback Functions

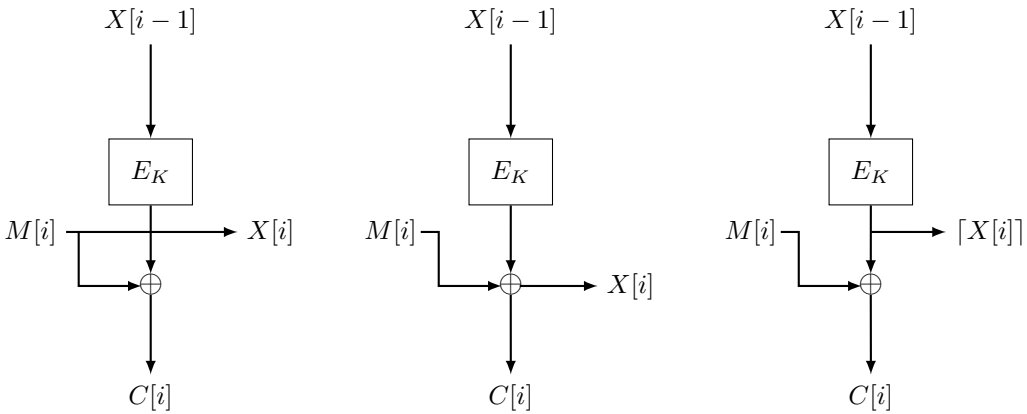


Figure: Classical Feedback Functions: PFB, OFB, CFB.

- Requires at least *n*-bit additional masking states for security of the mode.

Choice of Feedback Functions

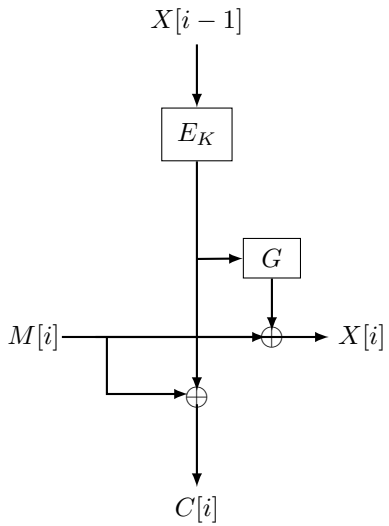


Figure: Combined Feedback Functions: CoFB [Chakraborti et al.]

- How small can we go? Requires only $n/2$-bit additional masking states.

Choice of Feedback Functions

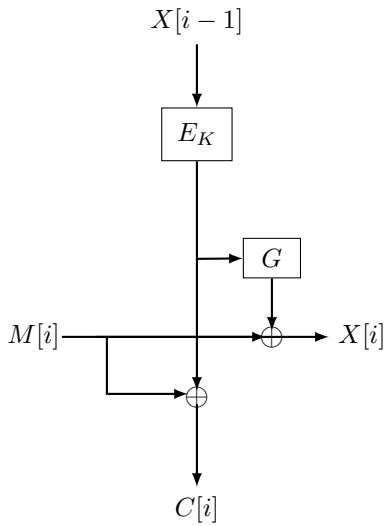


Figure: Combined Feedback Functions: CoFB [Chakraborti et al.]

- Observation: $2n$-bit XORs for the feedback function.

Choice of Feedback Functions

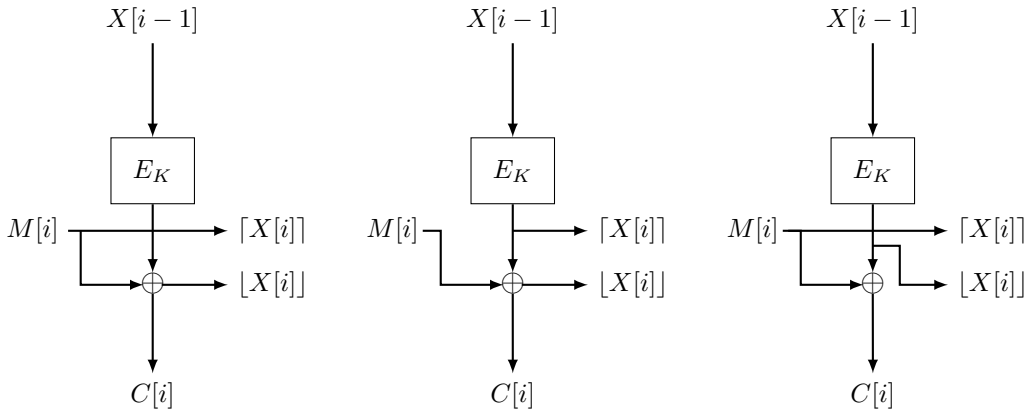


Figure: Hybrid Feedback Functions (HyFB): (PFB, CFB), (OFB, CFB), (PFB, OFB).

- Hybrid combination of classical feedbacks.
- Only *n*-bit XORs for the feedback function.

Choice of Feedback Functions

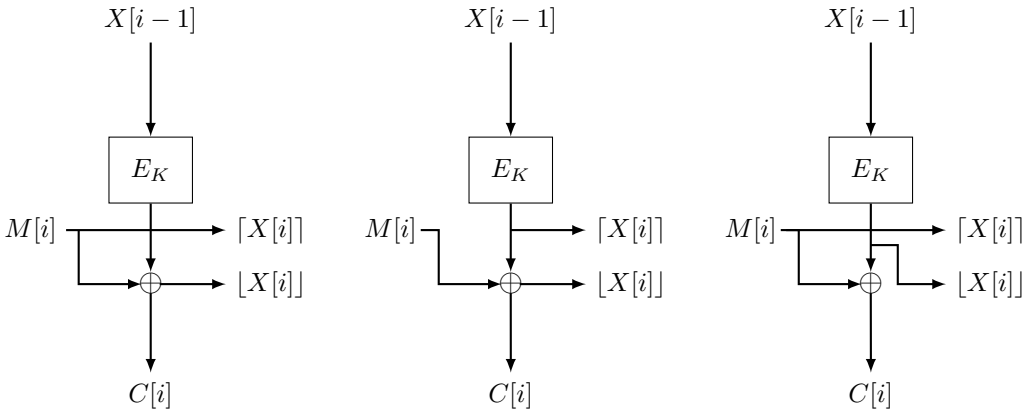


Figure: Hybrid Feedback Functions (HyFB): (PFB, CFB), (OFB, CFB), (PFB, OFB).

- Can we go even smaller? Design a feedback-baced AE with HyFB function and maximum $n/2$-bit additional masking states.

Concrete Specification of HyENA AE Mode

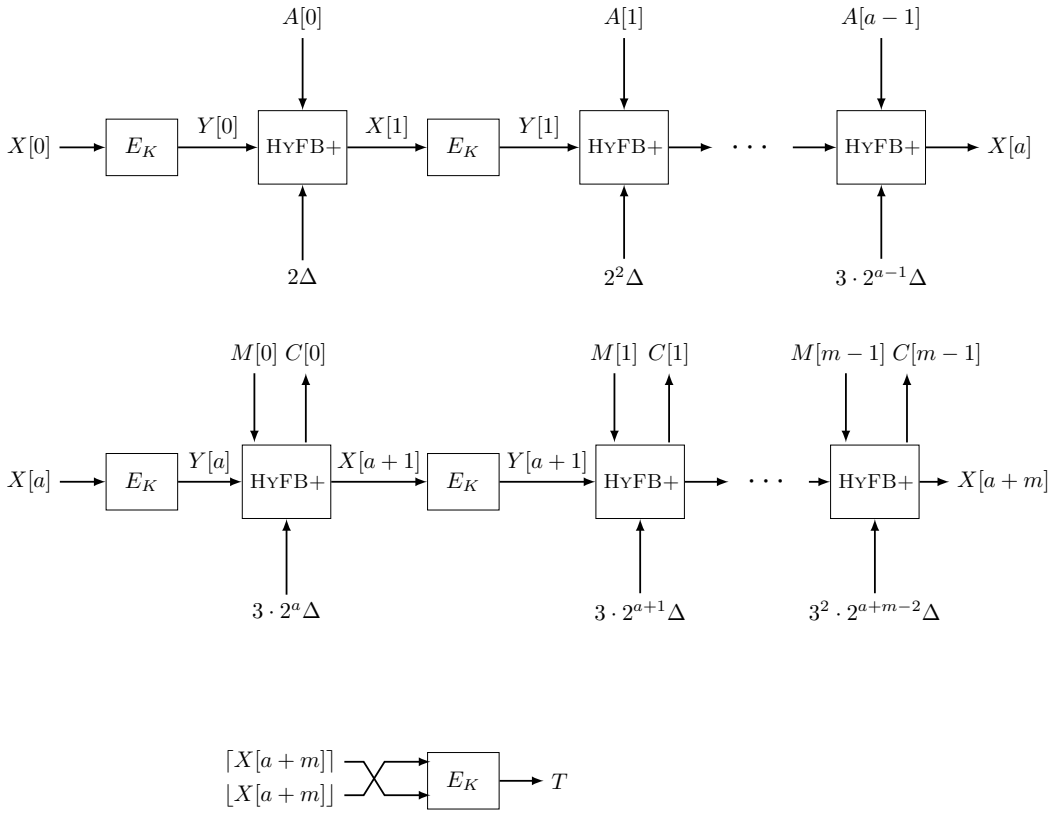
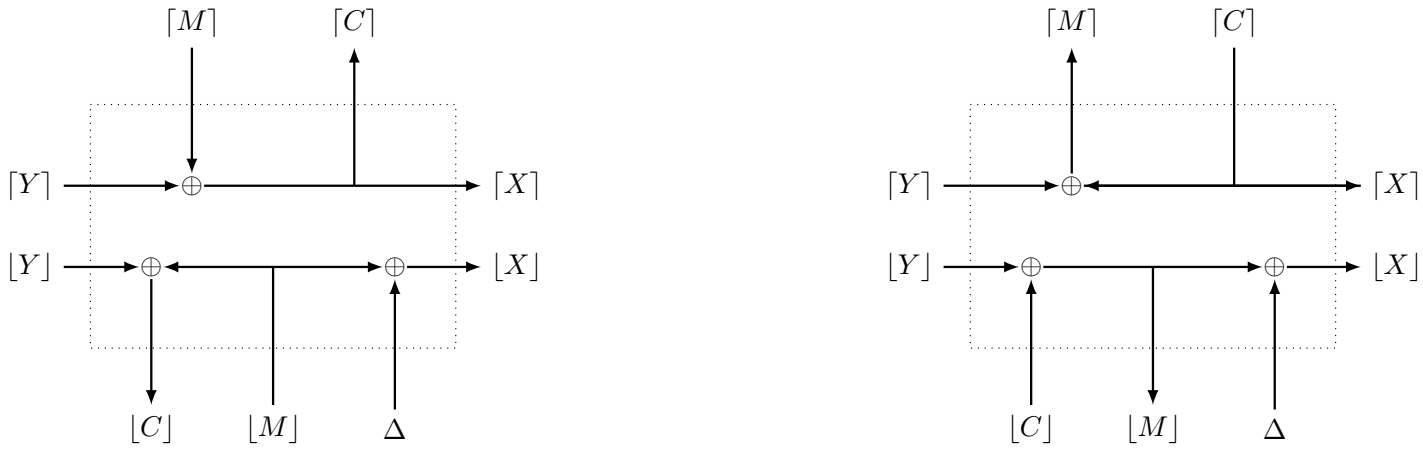


Figure: HyENA Authenticated Encryption Mode. Here $X[0] = N \| 0^{30} \| b_0 \| b_1$, $\Delta = \lceil Y[0] \rceil$.

Remark

- This version of HyENA differs from the NIST Lightweight submitted version only in the masking of the final associated data.
- This modification ensures identical AD and message processing, and achieves better hardware performance.

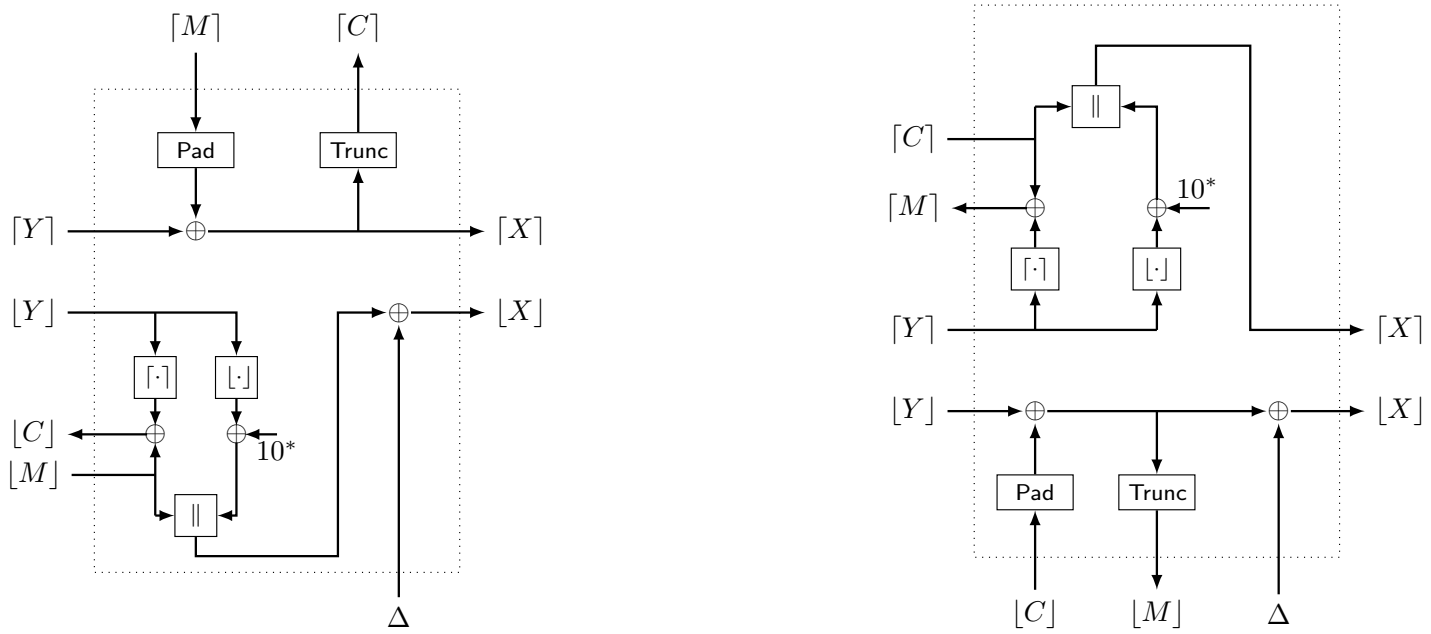
Choice of HyFB Function



(a) HyFB+ module. (b) HyFB- module.

Figure: HyFB module of HyENA for full data blocks. The number of XOR count is equals to $3n/2$.

Choice of Feedback Functions



(a) HyFB+ module. (b) HyFB- module.

Figure: HyFB module of HyENA for partial data blocks.

Security Statement for HyENA

Main Theorem

$$\mathbf{Adv}^{\mathrm{AE}}_{HyENA}(q_e, q_v, \sigma_e, \sigma_v, t) \leq \mathbf{Adv}^{\mathrm{prp}}_{E_K}(q', t') + O\left(\frac{\sigma_e}{2^{n/2}} + \frac{nq_e}{2^{n/2}} + \frac{n\sigma_v}{2^{n/2}}\right).$$

where $q' = q_e + \sigma_e + q_v + \sigma_v$ which corresponds to the total number of block cipher calls through the game and $t' = t + O(q')$.

Overall Approach

- $\mathcal{V} = \mathcal{V}_{\text{good}} \sqcup \mathcal{V}_{\text{bad}}$
- $\text{ip}_{\text{real}}(\tau)$ or $\text{ip}_{\text{ideal}}(\tau)$: Prob to realize view τ when interacting with the real or ideal resp.

Coefficients-H Technique

If the following two holds:

- In the ideal oracle, the probability of getting a view in $\mathcal{V}_{\text{bad}}$ is at most ϵ_{bad}.
- For any view $\tau \in \mathcal{V}_{\text{good}}$, we have

$$\text{ip}_{\text{real}}(\tau) \geq (1 - \epsilon_{ratio}) \cdot \text{ip}_{\text{ideal}}(\tau)$$

then $|\Pr[\mathcal{A}^{\mathcal{O}_0} = 1] - \Pr[\mathcal{A}^{\mathcal{O}_1} = 1]| \leq \epsilon_{bad} + \epsilon_{ratio}$.

Notations

- Init: Initial State
- IS: Intermediate State
- Final: Final State

- $+$: Encryption query
- -: Forging query

Bounding the BAD Views

Bounding $COLL(IS^+, IS^+)$

- $X_i^+[j] = X_{i'}^+[j']$.
- Two non-trivial linear equations:
  - One on $\lceil Y_i^+[j-1] \rceil$ and $\lceil Y_{i'}^+[j'-1] \rceil$,
  - Other on Δ_i^+ and $\Delta_{i'}^+$.
- Each probability $\frac{1}{2^n}$.
- Total number of pairs $\binom{\sigma_e}{2}$.

Bounding the BAD Views

Bounding $COLL(Init^+, IS^+)$

- $X_i^+[j] = N_{i'} \| 0^{32}$.
- Case $i \leq i'$
  - Non-trivial equations on $\lceil Y_i^+[j-1] \rceil$ (upper part),
  - Non-trivial equations on Δ_i^+ (lower part)
  - Each probability $\frac{1}{2^n}$.
  - Total number of pairs: $\binom{\sigma_e}{2}$.
- Case $i > i'$
  - Adversary can set nonce according to his choice (upper part),
  - Non-trivial equations on Δ_i^+ (lower part)
  - Each probability $\frac{1}{2^{n/2}}$.
  - Total number of pairs nq_e (Assuming $mCOLL(\lceil C \rceil) < n$).

Bounding the BAD Views

Bounding $mCOLL(\lceil C \rceil) \geq n$

- $\lceil C^+_{i_1}[j_1] \rceil = \lceil C^+_{i_1}[j_1] \rceil = \cdots = \lceil C^+_{i_n}[j_n] \rceil$.
- From the randomness of C, the probability $(\frac{1}{2^{n/2}})^{n-1}$.
- Total number of pairs $\binom{\sigma_e}{n}$.

Bounding the BAD Views

Bounding $COLL(Init^+, Final^+)$

- $\lceil X_i^+[\ell_i^+] \rceil = N_{i'} \| 0^{32}$.
- Case $i \geq i'$
  - Non-trivial equations on $\lceil Y_i^+[\ell_i^+ - 1] \rceil$ (upper part),
  - Non-trivial equations on Δ_i^+ (lower part)
  - Each probability $\frac{1}{2^n}$.
  - Total number of pairs: q_e^2.
- Case $i < i'$
  - Adversary can set nonce according to his choice (upper part),
  - Non-trivial equations on Δ_i^+ (lower part)
  - Each probability $\frac{1}{2^{n/2}}$.
  - Total number of pairs $\frac{nq_e^2}{2^{n/4}}$ (Assuming $mCOLL(X_\ell^+[32..63]) < c$, where $c = \frac{nq_e}{2^{n/4}}$).

Bounding the BAD Views

Bounding $mCOLL(\lceil X_\ell \rceil) \geq \frac{nq_e}{2^{n/4}}$

- From the randomness of Y, the probability $(\frac{1}{2^{n/4}})^{c-1}$.
- Total number of pairs $\binom{q_e}{c}$.

Bounding the BAD Views

Bounding $COLL(IS^+, IS^-)$

- $X_i^-[p_i + 1] = X_{i'}^+[j]$.
  - Adversary can fix the upper part,
  - Non-trivial equations on Δ_i^+ (lower part)
  - Each probability $\frac{1}{2^{n/2}}$.
  - Total number of pairs: $n.q_v$.

Bounding the BAD Views

Bounding $COLL(IS^{-}, INIT^{+})$

- $X_i^{-}[p_i + 1] = X_{i'}^{+}[0]$.
  - Adversary can fix the upper part,
  - Non-trivial equations on Δ_i^{+} (lower part).
  - Each probability $\frac{1}{2^{n/2}}$.
  - Total number of pairs: $q_v.2^{n/4}$.

- This doesn't provide the desired bound.
- Consider the freshness of successive block.

Bounding the BAD Views

Bounding $COLL(IS^{-}, INIT^{+})$

- $X_i^{-}[p_i + 1] = X_{i'}^{+}[0],\ X_i^{-}[p_i + 2] = X_{i''}^{+}[j]$.
  - Adversary can fix the upper part,
  - Non-trivial equations on Δ_i^{+} (lower part).
  - Each probability $\frac{1}{2^{n/2}} \cdot \frac{1}{2^{n/2}}$.
  - Total number of pairs: $2^{n/4}.n.q_v$.

Bounding the BAD Views

Bounding $COLL(IS^{-}, INIT^{+})$

- $X_i^{-}[p_i + 1] = X_{i'}^{+}[0],\ X_i^{-}[p_i + 2] = X_{i''}^{+}[j]$.
  - Adversary can fix the upper part,
  - Non-trivial equations on Δ_i^{+} (lower part).
  - Each probability $\frac{1}{2^{n/2}} \cdot \frac{1}{2^{n/2}}$.
  - Total number of pairs: $2^{n/4}.n.q_v$.

- Combining all the bad views, we have $\epsilon_{bad} \leq O\left(\frac{\sigma_e}{2^{n/2}} + \frac{nq_e}{2^{n/2}} + \frac{n\sigma_v}{2^{n/2}}\right)$.

Bounding the Interpolation Probability for GOOD Views

- $ip_{ideal}(\tau) = \frac{1}{2^{n(\sigma_e+q_e)}}$.
- $ip_{real}(\tau) \geq \frac{1}{2^{n(\sigma_e+q_e)}}\left(1 - O\left(\frac{q_v}{2^n} + \frac{2n\sigma_v}{2^{n/2}}\right)\right)$
- Combining together and using Coefficients-H Technique, the Theorem follows.

Thank you