LPN Codes for PCG and PCF

Shen Dong

SJTU

January 3, 2024

Outline

Contents

Primal LPN

Definition

(Primal LPN). Let $\mathcal{D}(\mathcal{R}) = \left\{\mathcal{D}_{k,n}(\mathcal{R})\right\}_{k,n\in\mathbb{N}}$ *denote a family of efficiently sampleable distributions over a ring* $\mathcal{R}$*, such that for any* $k, n \in \mathbb{N}, \mathrm{Im}\left(\mathcal{D}_{k,n}(\mathcal{R})\right) \subseteq \mathcal{R}^n$*. Let* $\mathbf{C}$ *be a probabilistic code generation algorithm such that* $\mathbf{C}(k, n, \mathcal{R})$ *outputs a matrix* $A \in \mathcal{R}^{n\times k}$*. For dimension* $k = k(\lambda)$*, number of samples (or block length)* $n = n(\lambda)$*, and ring* $\mathcal{R} = \mathcal{R}(\lambda)$*, the (primal)* $(\mathcal{D}, \mathbf{C}, \mathcal{R})$-$\mathrm{LPN}(k, n)$ *assumption states that*

$$\left\{(A, \mathbf{b}) \mid A \overset{\$}{\leftarrow} \mathbf{C}(k, n, \mathcal{R}), \mathbf{e} \overset{\mathbb{F}}{\leftarrow} \mathcal{D}_{k,n}(\mathcal{R}), \mathbf{s} \overset{\mathbb{F}}{\leftarrow} \mathbb{F}^k, \mathbf{b} \leftarrow A \cdot \mathbf{s} + \mathbf{e}\right\}$$
$$\overset{c}{\approx} \left\{(A, \mathbf{b}) \mid A \overset{\$}{\leftarrow} \mathbf{C}(k, n, \mathcal{R}), \mathbf{b} \overset{\$}{\leftarrow} \mathcal{R}^n\right\}.$$

Dual LPN

Definition

(Dual LPN) Let $\mathcal{D}(\mathcal{R}) = \left\{\mathcal{D}_{k,n}(\mathcal{R})\right\}_{k,n\in\mathbb{N}}$ *denote a family of efficiently sampleable distributions over a ring* $\mathcal{R}$*, such that for any* $k, n \in \mathbb{N}, \operatorname{Im}\left(\mathcal{D}_{k,n}(\mathcal{R})\right) \subseteq \mathcal{R}^n$*. Let* $\mathbf{C}'$ *be a probabilistic code generation algorithm such that* $\mathbf{C}'(n-k, n, \mathcal{R})$ *outputs a matrix* $H \in \mathcal{R}^{(n-k)\times n}$*. For dimension* $(n-k)$ *and number of samples (or block length)*n*,* $n = n(\lambda)$*,* $k = k(\lambda)$*, and ring* $\mathcal{R} = \mathcal{R}(\lambda)$*, the (dual)* $(\mathcal{D}, \mathbf{C}', \mathcal{R})$-LPN$(n-k, n)$ *assumption states that*

$$\left\{(H, \mathbf{b}) \mid H \stackrel{\$}{\leftarrow} \mathbf{C}'(n-k, n, \mathcal{R}), \mathbf{e} \stackrel{\mathbb{F}}{\leftarrow} \mathcal{D}_{k,n}(\mathcal{R}), \mathbf{b} \leftarrow H \cdot \mathbf{e}\right\}$$

$$\stackrel{c}{\approx} \left\{(H, \mathbf{b}) \mid H \stackrel{\$}{\leftarrow} \mathbf{C}'(n-k, n, \mathcal{R}), \mathbf{b} \stackrel{\$}{\leftarrow} \mathcal{R}^{n-k}\right\}.$$

Noise Distributions

- Bernoulli noise: $\mathbf{e} \leftarrow \mathrm{Ber}^n_{w/n}(\mathbb{F}_2)$
- Exact hamming weight noise: $\mathbf{e} \leftarrow \mathrm{HW}^n_w(\mathbb{F}_2)$
- Regular noise: $\mathbf{e} \leftarrow \mathrm{Reg}^n_w(\mathbb{F}_2)$

LPN-friendly Codes

What codes are secure in LPN assumption?

- Standard LPN
- Variable-Density LPN (2020,2023)
- Silver LDPC Codes (2021)
- Expander-Accumulator Codes (2022)
- Expander-Convolute Codes (2023)

Contents

Linear Attacks

Current Attacks:

- Gaussian Elimination
- BKW Algorithm and Covering Codes
- Information Set Decoding Attacks
- Generalized Birthday Attacks
- Statistical Decoding Attacks
- ...

Linear attacks! A common framework in which an adversary is trying to detect a bias in the LPN samples **by computing a linear combination of the samples**.
from [BCG+20] VDLPN

Bias of Distributions

Definition

(Bias of a Distribution). Given a distribution $\mathcal{D}$ over $\mathbb{F}^n$ and a vector $\mathbf{u} \in \mathbb{F}^n$, the bias of $\mathcal{D}$ with respect to $\mathbf{u}$, denoted $\mathrm{bias}_{\mathbf{u}}(\mathcal{D})$, is equal to

$$\mathrm{bias}_{\mathbf{u}}(\mathcal{D}) = \left| \mathbb{E}_{\mathbf{x}\sim\mathcal{D}}\left[\mathbf{u}^\top \cdot \mathbf{x}\right] - \mathbb{E}_{\mathbf{x}\sim\mathcal{U}_n}\left[\mathbf{u}^\top \cdot \mathbf{x}\right] \right| = \left| \mathbb{E}_{\mathbf{x}\sim\mathcal{D}}\left[\mathbf{u}^\top \cdot \mathbf{x}\right] - \frac{1}{|\mathbb{F}|} \right|,$$

where $\mathcal{U}_n$ denotes the uniform distribution over $\mathbb{F}^n$. The bias of $\mathcal{D}$, denoted $\mathrm{bias}(\mathcal{D})$, is the maximum bias of $\mathcal{D}$ with respect to any nonzero vector $\mathbf{u}$.

Linear Test Framework

Definition

(Security against Linear Tests).
Let $\mathcal{R}$ be a ring, and let $\mathcal{D} = \left\{\mathcal{D}_{k,n}\right\}_{k,n\in\mathbb{N}}$ denote a family of noise distributions over $\mathcal{R}^n$. Let $\mathbf{C}$ be a probabilistic code generation algorithm such that $\mathbf{C}(k,n)$ outputs a matrix $H \in \mathcal{R}^{k\times n}$. Let $\varepsilon, \eta : \mathbb{N} \mapsto [0,1]$ be two functions. We say that the $(\mathcal{D}, \mathbf{C}, \mathcal{R})$-LPN$(k,n)$ is (ε, η)-secure against linear tests if for any (possibly inefficient) adversary $\mathcal{A}$ which, on input H outputs a nonzero $\mathbf{v} \in \mathcal{R}^n$, it holds that

$$\Pr\left[H \stackrel{\$}{\leftarrow} \mathbf{C}(k,n), \mathbf{v} \stackrel{\$}{\leftarrow} \mathcal{A}(H) : \mathrm{bias}_{\mathbf{v}}\left(\mathcal{D}_H\right) \geq \varepsilon(\lambda)\right] \leq \eta(\lambda),$$

where $\mathcal{D}_H$ denotes the distribution induced by sampling $\mathbf{e} \leftarrow \mathcal{D}_{n,N}$, and outputting the LPN samples $H \cdot \mathbf{e}$.

Minimum Distance and Dual Distance

Definition

(Minimum Distance). the smallest Hamming distance between any two different codewords, and is equal to the minimum Hamming weight of the non-zero codewords in the code.
If A is a generator matrix of a linear code $\mathcal{C}$, then its minimum distance write $d(A)$

$$d(A) = \sharp \textit{the minimum weight of a vector in } A\textit{'s rowspan.}$$

Definition

(Dual Distance). If H is the parity check matrix of $\mathcal{C}$, the largest integer d such that every subset of d rows of H is linearly independent is called the dual distance of $\mathcal{C}$.

$$dd(H) = d(A)$$

Linear Test based on Minimum Distance

Lemma

For any $d \in \mathbb{N}$, the $(\mathcal{D}, \mathbf{C}, \mathcal{R})$-LPN$(k, n)$ is (ε_d, η_d)-secure against linear tests, where

$$\varepsilon_d = \max_{HW(\mathbf{v}) > d} \mathrm{bias}_{\mathbf{v}}\left(\mathcal{D}_{k,n}\right), \qquad \eta_d = \Pr_{H \xleftarrow{\$} \mathbf{C}(k,n)}[\mathrm{d}(H) \le d].$$

$$\Pr\left[H \xleftarrow{\$} \mathbf{C}(k,n), \mathbf{v} \xleftarrow{\$} \mathcal{A}(H) : \mathrm{bias}_{\mathbf{v}}\left(\mathcal{D}_H\right) \ge \varepsilon_d\right] \le \eta_d$$

$$\Pr\left[H \xleftarrow{\$} \mathbf{C}(k,n), \mathbf{v} \xleftarrow{\$} \mathcal{A}(H) : \mathrm{bias}_{\mathbf{v}}\left(\mathcal{D}_H\right) \ge \max_{HW(\mathbf{v}) > d} \mathrm{bias}_{\mathbf{v}}\left(\mathcal{D}_{k,n}\right)\right] \le$$

$$\Pr_{H \xleftarrow{\$} \mathbf{C}(k,n)}[\mathrm{d}(H) \le d]$$

Pseudorandom Minimum Distance

Definition

(Pseudodistance) Let $\mathbf{C}$ *be a probabilistic code generation algorithm such that* $\mathbf{C}(k,n)$ *outputs a matrix* $H \in \mathbb{F}_2^{k\times n}$*. For a weight parameter* $\delta(\lambda)$*, we say that* $\mathbf{C}(k(\lambda), n(\lambda))$ *has pseudodistance* $\delta(\lambda)$ *if for every PPT algorithm* $\mathcal{A}$ *there is a negligible function* **negl** *such that*

$$\Pr\left[\mathcal{A}(H) = \vec{x} \text{ s.t. } \vec{x} \neq \overrightarrow{0} \textit{ and } \mathcal{HW}\left(\vec{x}^\top H\right) \leq \delta n \mid H \xleftarrow{\$} \mathbf{C}(k,n)\right] \leq \mathbf{negl}(\lambda)$$

Computing minimum distance is NP hard. Silver, EA-Code: estimate the minimum distance in a **heuristic/empirical** way.(making silver fail...)

Minimum Distance and Noise Rate

If $|v| = d$, and noise rate is r, then

$$\Pr\left[\mathbf{e} \leftarrow \mathrm{Ber}_r^n(\mathbb{F}_2) : \mathbf{v}^\top \cdot \mathbf{e} = 1\right] = \frac{1 - (1-2r)^d}{2}$$

$$\mathrm{bias}_{\mathbf{v}}\left(\mathrm{Ber}_r^n(\mathbb{F}_2)\right) = (1-2r)^d \leq e^{-2rd}$$

Leverage between minimum distance and noise rate:
$A\mathbf{s} + \mathbf{e}$, $\mathbf{s}$ is uniformly random, $d(A) = d$.

- If the adversary choose $\vec{v}$ s.t. $wt(\vec{v}) \leq d$, then $\vec{v}^T A \neq \vec{0}$, and $\vec{v}^T A \vec{s}$ is uniformly random.
- If the adversary choose $\vec{v}$ s.t. $wt(\vec{v}) > d$, then by adding noise rate make $\vec{v}^T \mathbf{e}$ looks random.

Contents

Expander-Accumulator Code

Definition

$H \xleftarrow{\$} EAGen(k, n, p, \mathcal{R})$

- $\vec{r_1}^T, \ldots, \vec{r_k}^T \xleftarrow{\$} Ber_p^n(\mathcal{R})$ *independently, and put* $B = [\vec{r_1} \| \vec{r_2} \ldots \| \vec{r_k}]^T$
- $A \in \mathcal{R}^{n \times n}$ *is the Accumulator matrix, with 1's on and below the main diagonal, and 0's elsewhere.*
- *from EAGen outputs* $H = BA, B \in \mathcal{R}^{k \times n}, A \in \mathcal{R}^{n \times n}, H \in \mathcal{R}^{k \times n}$

It's assumed that $\mathcal{R} = \mathbb{F}_2$.

EA-LPN Assumption

Definition

(EA-LPN Assumption).

$$\left\{(H,\vec{b}) \mid H \xleftarrow{\$} \mathrm{EAGen}(k,n,p,\mathcal{R}), \vec{e} \xleftarrow{\$} \mathcal{D}_N(\mathcal{R}), \vec{b} \leftarrow H\cdot\vec{e}\right\}$$
$$\overset{c}{\approx} \left\{(H,\vec{b}) \mid H \xleftarrow{\$} \mathrm{EAGen}(k,n,p,\mathcal{R}), \vec{b} \xleftarrow{\$} \mathcal{R}^N\right\}.$$

According to the Linear Test Framework, we should prove that $d(H)$ is unlikely to be small.

$$\mathcal{HW}(\vec{y}^T) = \mathcal{HW}(\vec{x}^T H) = \mathcal{HW}(\vec{x}^T BA)$$

Bound $\mathcal{HW}(\vec{x}^T H)$

Lemma

Denote code rate $R = \dfrac{k}{n}$. *Fix* $p \in (0, \frac{1}{2})$ *and* $\delta > 0$. *Let* $r \in \mathbb{N}$ *and let* $\vec{x} \in \mathbb{F}_2^k$ *be a vector of weight* r. *define* $\xi_r = (1-2p)^r$, *Then*

$$\Pr\left[\mathcal{HW}(\vec{x}^T H) \leq \delta n\right] \leq 2\exp\left(-2n\frac{1-\xi_r}{1+\xi_r}(\frac{1}{2}-\delta)^2\right)$$

Markov Chain and Random Walk

- state space V
- transition matrix $P \in \mathbb{R}^{V\times V}$, $P_{u,v} = \Pr[\vec{u} \to \vec{v}]$.
- a distribution over the state space $\vec{\nu} \in \mathbb{R}^V$.
- random walk by P on V: $x_0 \leftarrow \vec{\nu}$. For $i \in [n]$, sample $x_i \leftarrow P_{x_{i-1}}$.
- stationary distribution: $\vec{\pi} \in \mathbb{R}^V$ s.t. $\vec{\pi}P = \vec{\pi}$
- irreducible: strongly connected
- reversible: $\forall u, v \in V, \quad \vec{\pi}_u P_{u,v} = \vec{\pi}_v P_{v,u}$
- spectral gap of P

Irreducible chain has a unique stationary distribution, therefore has unique max eigenvalue 1.

Expander Hoeffding Bound

Theorem

(Expander Hoeffding Bound). Let $(\mathcal{V}, P)$ denote a finite, irreducible and reversible Markov chain with stationary distribution $\vec{\pi}$ and second largest eigenvalue λ. Let $f \colon \mathcal{V} \to [0,1]$ with $\mu = \mathbb{E}_{V\sim\vec{\pi}}[f(V)]$. For any integer $N \geq 1$, consider the random variable $S_N = \sum_{i=1}^{N} f(V_i)$, where V_0 is sampled uniformly at random from V and then $V_1, \ldots, V_N$ is a random walk starting at V_0. Then, for $\lambda_0 = \max(0, \lambda)$ and any $\varepsilon > 0$ with $\mu + \varepsilon < 1$, the following bound holds:

$$\Pr\left[S_N \geq N(\mu+\varepsilon)\right] \leq \exp\left(-2\frac{1-\lambda_0}{1+\lambda_0}N\varepsilon^2\right)$$

.

Piling-up Lemma

Lemma

(Piling-up Lemma). For any $r \in (0, \frac{1}{2})$ *and any integer* n*, given* n *random variables* $X_1, \ldots, X_n$ *i.i.d. to* $Ber_r(\mathbb{F}_2)$*, we have*

$$\Pr\left[\oplus_{i=1}^{n} X_i = 0\right] \leq \frac{1}{2} + \frac{(1-2r)^n}{2}$$

EA Code Viewed as Random Walk

$$
\begin{aligned}
B =& \left[\vec{c_1}, \dots, \vec{c_n}\right], \vec{c_i} \in \mathbb{F}_2^k \\
H =& BA = \left[\left(\vec{c_1} + \cdots + \vec{c_n}\right), \left(\vec{c_2} + \cdots + \vec{c_n}\right), \dots, \vec{c_n}\right] \\
\left(y_1, \dots, y_n\right) =& \left(\vec{x}^T\left(\vec{c_1} + \cdots + \vec{c_n}\right), \vec{x}^T\left(\vec{c_2} + \cdots + \vec{c_n}\right), \dots, \vec{x}^T\vec{c_n}\right) \\
y_n =& \vec{x}^T\vec{c_n}, y_i = y_{i+1} + \vec{x}^T\vec{c_i}, \forall 1 \le i \le n-1
\end{aligned}
$$

See $y_n, \dots, y_1$ as a random walk on state space $\mathcal{V} = \{0, 1\}$, and each step is a random variable $\vec{x}^T\vec{c_i}$.

$wt(\vec{x}^T) = r, \vec{c_i} \xleftarrow{\$} Ber_p^k(\mathbb{F}_2)$, then by piling-up lemma:

$$
\Pr\left[\vec{x}^T\vec{c_i} = 0\right] = \frac{1}{2} + \frac{(1-2p)^r}{2} = \frac{1-\xi_r}{2}
$$

EA Code Viewed as Random Walk

$$\Pr\left[\vec{x}^T\vec{c}_i = 0\right] = \frac{1}{2} + \frac{(1-2p)^r}{2} = \frac{1-\xi_r}{2}$$

$$\text{transition } P = \begin{bmatrix} 0 \to 0 & 0 \to 1 \\ 1 \to 0 & 1 \to 1 \end{bmatrix} = \begin{bmatrix} \frac{1+\xi_r}{2} & \frac{1-\xi_r}{2} \\ \frac{1-\xi_r}{2} & \frac{1+\xi_r}{2} \end{bmatrix}$$

P is irreducible and reversible, and ξ_r is the second largest eigenvalue of P, and $\left(\frac{1}{2}, \frac{1}{2}\right)$ is the stationary distribution of P.
Define a function $f : \mathcal{V} \to [0,1]$: $f(0) = 1, f(1) = 0$, then by Expander Hoeffding Bound we have:

$$\begin{aligned} \Pr\left[\mathcal{HW}(\vec{x}^T H) \le \delta n\right] &= \Pr\left[\Sigma_{i=0}^n V_i \le \delta n\right] \\ &= \Pr\left[S_n = \Sigma_{i=0}^n f(V_i) \ge (1-\beta)n\right] \\ &\le \exp\left(-2\frac{1-\xi_r}{1+\xi_r} n\beta^2\right) \end{aligned}$$

Bound on $d(H)$

Use union bound for all $\vec{x} \in \mathbb{F}_2^k$ of weight r:

Theorem

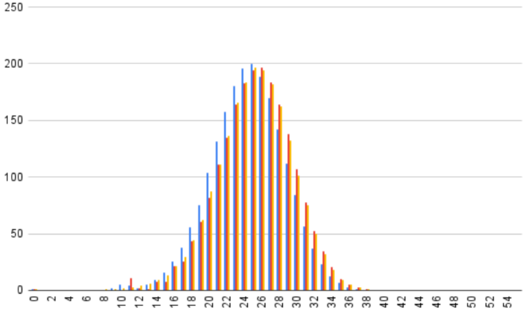
Theorem 3.10 Let $k, n \in \mathbb{N}$ with $k \leq n$ and put $R = \frac{k}{n}$, which we assume to be a constant. Let $C > 0$ and set $p = \frac{C \ln n}{n} \in (0, 1/2)$. Fix $\delta \in (0, 1/2)$ and put $\beta = 1/2 - \delta$. Then, assuming n is sufficiently large and assume $R < \min\left\{\frac{2}{\ln 2} \cdot \frac{1-e^{-1}}{1+e^{-1}} \cdot \beta^2, \frac{2}{e}\right\}$ and $C > \frac{1}{\beta^2}$, we have

$$\Pr[\mathrm{d}(H) \geq \delta n \mid H \xleftarrow{\$} \mathrm{EAGen}(k, n, p)] \geq 1 - 2Rn^{-2\beta^2 C + 2}.$$

$p = \Theta(\frac{\log n}{n})$, constant rate, $\Pr\left[d(H) = \Omega(n)\right] = 1 - 1/\operatorname{poly}(n)$
$p = \Theta\left(\frac{\log^2 n}{n}\right)$, constant rate, $\Pr\left[d(H) = \Omega(n)\right] = 1 - 1/n^{-O(\log n)}$, which is negligible in n.

Variants

- B's rows from exact weight distribution
- B's rows from regular distribution



heuristically using $\mathcal{HW}(\vec{x}^T H)$ as $d(H)$. Blue corresponds to exact; red corresponds to regular; and orange corresponds to Bernoulli.

Contents

Expander-Convolute Codes

Definition

$H \xleftarrow{\$} ECGen(k, n, p, \mathcal{R})$

For a ring $\mathcal{R}$ *and parameters* $w, k, n \in \mathbb{N}$ *with* $w \ll k \leq n$*, which is* B*'s row weight.* $m \in \mathbb{N}, m \leq n$ *is the size of convolutional internal state.*

- $B \in \mathcal{R}^{k \times n}$, $B_{i,j} \leftarrow \mathrm{Ber}_{p_\mathrm{w}}(\mathcal{R})$, $p_\mathrm{w} = \frac{w}{n}$
- *convolutional code generator matrix* $C \in \mathcal{R}^{n \times n}$ *upper-triangular matrix with state size* m*, below the diagonal being some linear combination of the following* m *columns.*
- *from* $ECGen$ *outputs* $H = BC, B \in \mathcal{R}^{k \times n}, C \in \mathcal{R}^{n \times n}, H \in \mathcal{R}^{k \times n}$

Better than EA-Code, more generalized.

EC-LPN Assumption

Definition

(EC-LPN). Let $\mathcal{D}(\mathcal{R}) = \{\mathcal{D}_n(\mathcal{R})\}_{n\in\mathbb{N}}$ *denote a family of efficiently sampleable distributions over a ring* $\mathcal{R}$*, such that for any* $n \in \mathbb{N}$*,* $\mathrm{Im}\left(\mathcal{D}_n(\mathcal{R})\right) \subseteq \mathcal{R}^n$*. For a dimension* $k = k(\kappa)$*, number of samples* $n = n(\kappa)$*, expansion weight* $w = w(\kappa) \in [n]$*, state size* $m = m(\kappa) \in [n]$*, convolving density* $p_c = p_c(\kappa) \in [0, 1]$ *and ring* $\mathcal{R} = \mathcal{R}(\kappa)$*, the* $(\mathcal{D}, \mathcal{R})$*-EC-LPN*$(w, m, k, n, p_c)$ *assumption states that*

$$\begin{aligned}&\{(H, \mathbf{b}) \ s.t. \ H \leftarrow ECGen\,(w, m, k, n, p_c, \mathcal{R})\,, \mathbf{e} \leftarrow \mathcal{D}_n(\mathcal{R}, \mathbf{b} \leftarrow H\mathbf{e})\}\\ &\qquad \overset{c}{\approx} \left\{(H, \mathbf{b}) \ s.t. \ H \leftarrow ECGen\,(w, m, k, n, p_c, \mathcal{R})\,, \mathbf{b} \leftarrow \mathcal{R}^k\right\}.\end{aligned}$$

Roadmap: also random walking on Markov chains, and bound the visits to the state 1. But irreversible???

EC Code Viewed as Random Walk

$$B = [\vec{c_1}, \ldots, \vec{c_n}], \vec{c_i} \in \mathbb{F}_2^k, \vec{c_i} \leftarrow \mathrm{Ber}_{p_w}^k$$
$$y_i = \Sigma_{j\in[m]}\alpha_{i,j}y_{i,j} + \vec{x}^T\vec{c_i}, \forall 2 \leq i \leq n$$

Denote the internal state by $\vec{\sigma_i} = (y_{i-1}, \ldots, y_{i-m})$, so $y_i = \vec{x}^T\vec{c_i} + \vec{\sigma_i}^T\vec{\alpha_i}$.

$$\begin{aligned}
&\Pr[y_i = 1 \mid \vec{\sigma_i}] \\
&= \Pr\left[\vec{x}^T\vec{c_i} = 0\right]\Pr\left[\vec{\sigma_i}^T\vec{\alpha_i} = 1\right] + \Pr\left[\vec{x}^T\vec{c_i} = 1\right]\Pr\left[\vec{\sigma_i}^T\vec{\alpha_i} = 0\right] \\
&= \frac{1+(1-2p_w)^r}{2}\Pr\left[\vec{\sigma_i}^T\vec{\alpha_i} = 1\right] + \frac{1-(1-2p_w)^r}{2}\Pr\left[\vec{\sigma_i}^T\vec{\alpha_i} = 0\right]
\end{aligned}$$

$\alpha_{i,j}$ is random(if $p_c = \frac{1}{2}$), but the internal state has impact on the probability.

EC Code Viewed As Random Walk

$$\Pr\left[y_i = 1 \mid \vec{\sigma}_{i-1} \neq \vec{0}\right] = \frac{1}{2}$$
$$\Pr\left[y_i = 1 \mid \vec{\sigma}_{i-1} = \vec{0}\right] = \frac{1-(1-2p_w)^r}{2}$$
$$\Pr\left[y_i = 0 \mid \vec{\sigma}_{i-1} \neq \vec{0}\right] = \frac{1}{2}$$
$$\Pr\left[y_i = 0 \mid \vec{\sigma}_{i-1} = \vec{0}\right] = \frac{1+(1-2p_w)^r}{2}$$

Situation is only bad when $\vec{\sigma}_{i-1} = \vec{0}$, intuitively better than EA-Code. Then we can view the **changes of internal state** as a random walk on $\mathcal{V} = \{0,1\}^m$, and each step is y_i. Imagine the transition matrix being $2^m \times 2^m$, but with many 0's.
But this scale is too large to analyze, so we shrink the Markov chain.

EC Code Viewed As Random Walk, Shrunk

Intuition: only all-0 state matter, so we only care how far is the internal state from all-0 state.
We can group states based on the **suffix of the m bits representing the state**, shrinking all the 2^m states to $m-1$ states: $1, 0_1, 0_2, \ldots, 0_{m-1}, 0_m$. Define $p_r := \frac{1-(1-2p_w)^r}{2}$

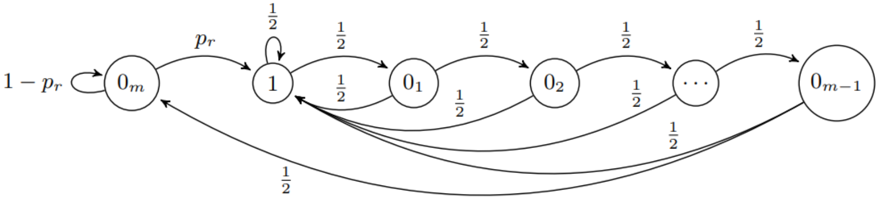


Figure: 1, Shrunk Markov Chain, irreversible

EC Code Viewed As Random Walk, Reversible

for some $\theta_m > 0$, $\Pr[0 \to 0] = 1 - p_r$, $\Pr[0 \to ?] = p_r$, $\Pr[? \to 0] = 2^{-(m+\theta_m)}$, $\Pr[? \to ?] = 1 - 2^{-(m+\theta_m)}$ 0 is the same as 0_m, and ? emulates all other states, containing all different paths to 0_m.

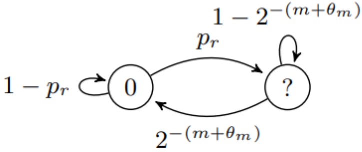


Figure: 2, Coupling Markov Chain, reversible

Reversible. Claim walking on these two Markov Chains, ♯(steps on ?) bounds ♯(steps on 1) because of the coupling of the two chains.

Theorem

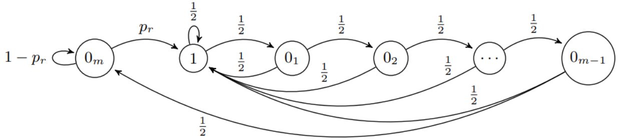
Let n denote the length of the random walks performed on the chains in Figures 1 and 2, where $m \geq \log n + 2$. Starting from state 0_m of the irreversible chain (Figure 1), let X_i be the indicator of being in state 1 at step i. Starting from state 0 of the reversible chain (Figure 2), let Y_i be the indicator of being in state? at step i and then ***uniformly mapping ? to*** $\{0,1\}$ $\left(\textbf{\textit{with probability}}\ \frac{1}{2}\right)$*. Fix $\delta \in [0,1]$ and $\hat{k} > 0$. Then, there exists $\theta_m \in [0,1)$ such that*

$$\Pr\left[\sum_{i\in[n]} X_i \leq \delta n - \hat{k}(m-1)\right] \leq \frac{1}{1-\exp\left(-\frac{\tilde{\delta}_r \hat{k}}{2+\tilde{\delta}_r}\right)} \Pr\left[\sum_{i\in[n]} Y_i \leq \delta n\right]$$

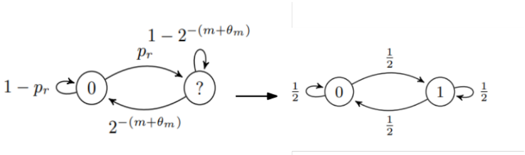
where $\tilde{\delta}_r = \frac{\hat{k}}{n \cdot 2^{-(m+\theta_m)} \cdot p_r}$.

Conjecture: Theorem holds for all $m \geq 2$.

Flip a Coin, But Heavier



In i steps, $S_0 : 0_m \to \dots 0_m \to 1 \quad S_1 : 1 \to \cdots \to 0_{m-1} \to 0_m$



In i steps, $S_0' : 0 \to \dots 0 \to ? \quad S_1' : ? \to \cdots \to ? \to 0$
$S_0 = S_0'$, $S_1(p) - (m-1) \geq S_1'(p)$.

Lemma

Fix $\hat{k} > 0$. *Define* $\tilde{\delta}_r = \frac{\hat{k}}{n \cdot 2^{-m} \cdot p_r}$. *Then, we have with probability at least* $1 - \exp\left(-\frac{\tilde{\delta}_r \hat{k}}{2+\tilde{\delta}_r}\right)$ *:*

$$HW\left(Z_{\tilde{X}}\right) \geq HW\left(Z_{\tilde{Y}}\right) - \hat{k}(m-1)$$

Theorem

$$\Pr\left[\sum_{i \in [n]} X_i \leq \delta n - \hat{k}(m-1)\right] \leq \frac{1}{1 - \exp\left(-\frac{\tilde{\delta}_r \hat{k}}{2+\tilde{\delta}_r}\right)} \Pr\left[\sum_{i \in [n]} Y_i \leq \delta n\right]$$

where $\tilde{\delta}_r = \frac{\hat{k}}{n \cdot 2^{-(m+\theta m)} \cdot p_r}$.

Bound $\Sigma_{i\in[n]} Y_i$ on Reversible Chain

$$\vec{\pi}_r = \left(\frac{2^{-(m+\theta_m)}}{p_r + 2^{-(m+\theta_m)}}, \frac{p_r}{p_r + 2^{-(m+\theta_m)}}\right)$$

$$\lambda_r = 1 - p_r - 2^{-(m+\theta_m)}$$

Walk on the reversible chain for n steps, the time we visit ? is bounded by Expander Hoeffding Inequality:

$$\Pr\left[N_? < n\vec{\pi}_{r,?} - \epsilon\right] \leq \left(1 + 2^{m+\theta_m} p_r\right) \exp\left(-2\frac{\epsilon^2}{n} \cdot \frac{1-\lambda_r}{1+\lambda_r}\right)$$

And in the ? state, suppose we walk T steps on the flipping-coin chain, bound the time we visit 1, $\epsilon = (\frac{1}{2} - \beta)T$

$$\Pr\left[N_1 \leq \frac{1}{2}T - \epsilon\right] \leq \exp\left(\frac{-2\epsilon^2}{T}\right) = \chi_{\beta,T}$$

.

$N_?, N_1 \rightarrow \Pr\left[\sum_{i\in[n]} Y_i \leq \delta n\right] \rightarrow \Pr\left[\sum_{i\in[n]} X_i \leq \delta n - \hat{k}(m-1)\right] \rightarrow$
$\mathcal{HW}(\vec{(x)}^T H) \rightarrow \Pr\left[d(H) \leq \delta n - \hat{k}(m-1)\right]$

Theorem

Let $w, m, k, n \in \mathbb{N}$ with $w, m, k \leq n$. Define $R = \frac{k}{n}$. Fix $\delta \in [0,1]$ and $\hat{k} > 0$. We assume that the following hold: $w = C \ln n$ for some $C > 2$; $m = C_m \log n$ for some $C_m > 1$; $R \leq \frac{2}{e}$, $C\left(\frac{20}{41} - \delta\right)^2 > 2$ and $R < \frac{1}{\ln 2} \cdot \frac{e-1}{e+1}\left(\frac{20}{41} - \delta\right)^2$; $\hat{k} \geq n^{1-C_m}$ and $\hat{k} \geq 2\ln 2$. Then, for all sufficiently large n,

$$\Pr\left[\mathrm{d}(G) < \delta n - \hat{k}(m-1) : G \leftarrow \mathrm{ECGen}\left(w, m, k, n, \frac{1}{2}, \mathbb{F}_2\right)\right]$$
$$\leq 2Rn^{-C\left(\frac{20}{41}-\delta\right)^2 + C_m + 3}$$

When $\mathcal{R} = \mathbb{F}_2$, $w, m = \Theta(\log n)$, $p_c = \frac{1}{2}$, secure against Linear Test.

Contents

Empirical Method Guided

fastest(linear encoding time, cache-friendly), linear minimum time.

Warning: The conjectured linear minimum distance of this work has been shown to be false. Silver codes should not be used. See [RRT23].

The Construction of Silver:

- Empirical estimation of minimum distance
  - Brouwer-Zimmerman algorithm: solving exact minimum distance (exponential, $n \leq 180$)
  - Noise impulse method: by solving a flipped vector close to zero vector to approximate $d(H)$
- Try to fit into an efficient decoder: g-ALT (better efficiency)
- Try to get better memory locality (better efficiency)

g-Approximate Lower Triangle Matrix

Definition

(g-ALT). If H can be transformed into the form below with ***only column and row swaps****, then it can be encode in $O(n+g^2)$ time*

1. null space of H doesn't change with only column and row swaps
2. Silver want to keep $g = O(\sqrt{n})$ to achieve linear encoding time.

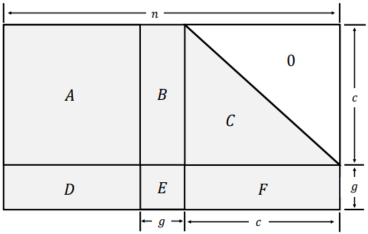


Fig. 9: The structure of an g approximate lower triangular matrix. The diagonal of C should all be ones.

LDPC Code and Tanner Graph

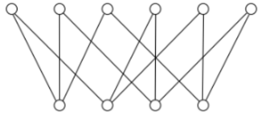
Definition

(regular LDPC Code). An LDPC code with constant number of 0*'s per row and per column.*

Definition

(Tanner Graph). A Tanner graph of an LDPC code with parity check matrix $\boldsymbol{H}$ *is a bipartite graph* $\{V_1, V_2\}$*, having one vertex in* V_1 *for each row of* $\mathbf{H}$*(called check nodes) and one vertex in* V_2 *for each column of* $\mathbf{H}$*(called variable nodes), and there is an edge between two vertice* c_i *and* v_j *exactly when* $h_{ij} \neq 0$*.*

$$\boldsymbol{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

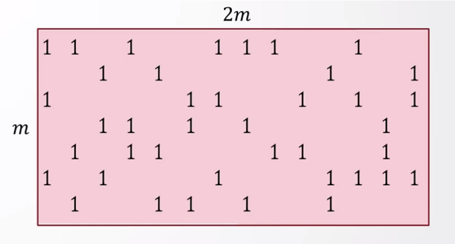


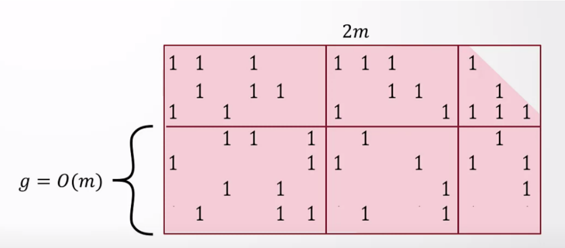
Tanner Graph and Minimum Distance

- We don't want short circle, which means small $d(H)$
- We don't want too many variable nodes with degree 2, if $H \in \mathbb{F}_2^{k \times n}$, if $n_2/m < 1,\ d(H) = O(\log n);\ n_2/m > 1,\ \Pr[d(H) = O(n)] > 0$
- It is well-known that odd column weight t LDPC codes achieve better minimum distance performance

Standard LDPC

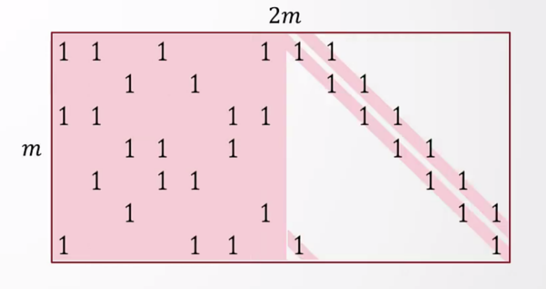
- well-studied security, under Alekhnovich Assumption
- $g = O(n)$, which cannot be efficiently encoded.





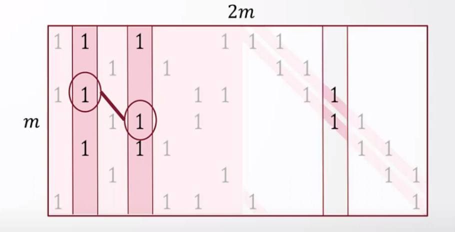
Tillich-Zémor Code

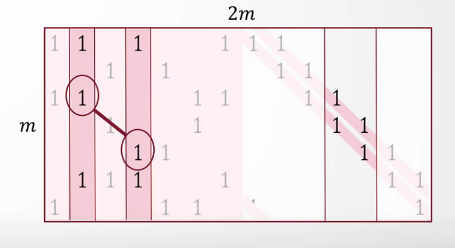
- with structure $H = [L \| R]$, $k = m = n/2$. L is a $m \times m$ matrix standard sparse, R is a $m \times m$ matrix with a diagonal bind, its n_2/m is 1.
- sublinear minimum distance due to the diagonal bind.
- fast encoding, $O(n)$



Tillich-Zémor Code

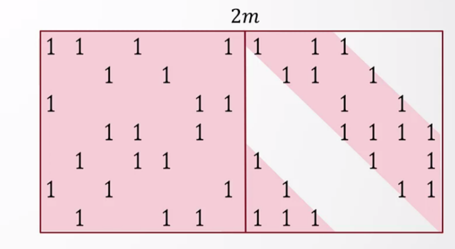
The diagonal bind is concentrated, R cancelling L.





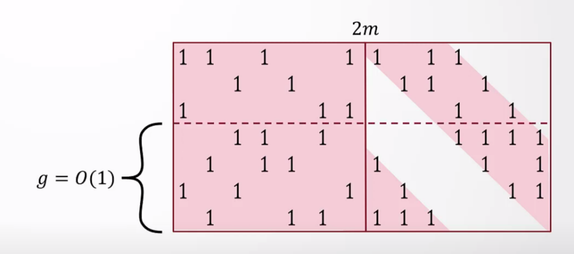
Silver #1

- start with TZ Codes, removing weight-2 columns(i.e. degree-2 variable nodes in Tanner Graph)
- efficient encoding, $g = O(1)$ which depends on the fixed column weight(the hight of the left bottom).
- much better minimum distance than TZ Codes.

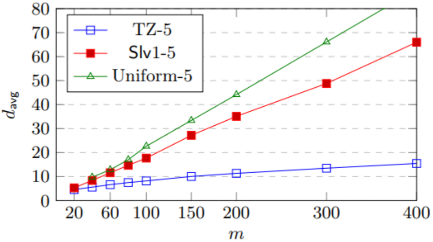


Silver #1

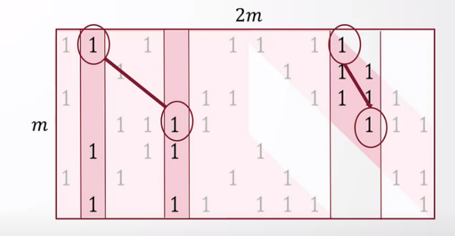
- start with TZ Codes, removing weight-2 columns(i.e. degree-2 variable nodes in Tanner Graph)
- efficient encoding, $g = O(1)$ which depends on the fixed column weight(the hight of the left bottom).
- much better minimum distance than TZ Codes. But still sublinear due to clumping.



Silver #1

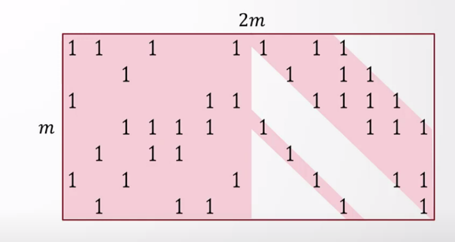


(b) Average minimum distance of weight $t = 5$

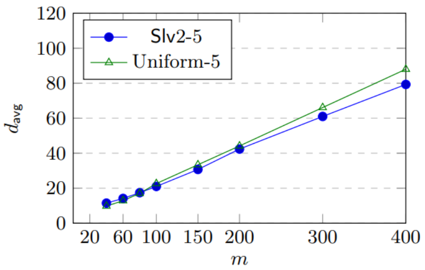


Silver #2

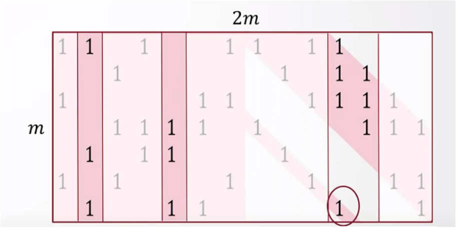
- adding additional weight one diagonals below the main diagonal prevents clumping, because there may be some 1 at bottom.
- achieve almost linear minimum distance, close to uniform LDPC.
- keep efficient encoding, $g = O(1)$



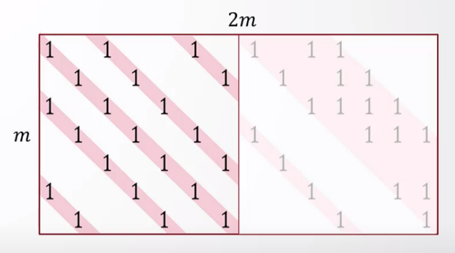
Silver #2

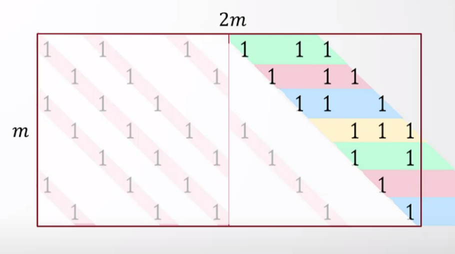


(b) d_{avg} of column weight 5 codes.

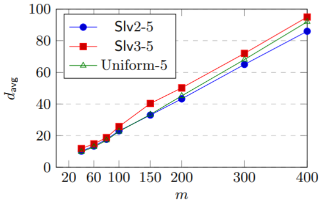


Silver #3, #5

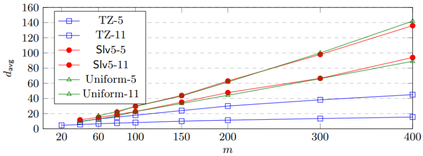




Silver #3, #5



(a) Average minimum distance of Slv2, Slv3 vs uniform with $t = 5$.



Failed Security

- A kind of convolutional code which has been studied (trubo-like codes), but with weak internal state.
- Failed linear minimum distance at large scale: Silver was only able to evaluate the codes of size up to n = 800 and observed minimum distance up to 140. our attacks show that the minimum distance of these codes stop growing at approximately8 705 or 4, 158 depending on the variant.
- Stronger turbo-like variant with permutation matrix rather than shifts in silver, only achieve linear minimum distance when w is relatively small, i.e. w 5, 11 as Silver specifies.

Possible Future Analysis

- silver-turbo-RA-EA-EC
- regular ISD

References

PCF from VDLPN https://eprint.iacr.org/2020/1417 revisited
https://eprint.iacr.org/2023/650.pdf
silver LDPC https://eprint.iacr.org/2021/1150
https://www.youtube.com/watch?v=FCNcrxcFLtU
Expand-Accumulate Codes https://eprint.iacr.org/2022/1014
Expand-Convolute Codes https://eprint.iacr.org/2023/882