Simula UiB

Palma Persson†, Maiara F. Bollauf*, Hsuan-Yin Lin*, Øyvind Ytrehus*

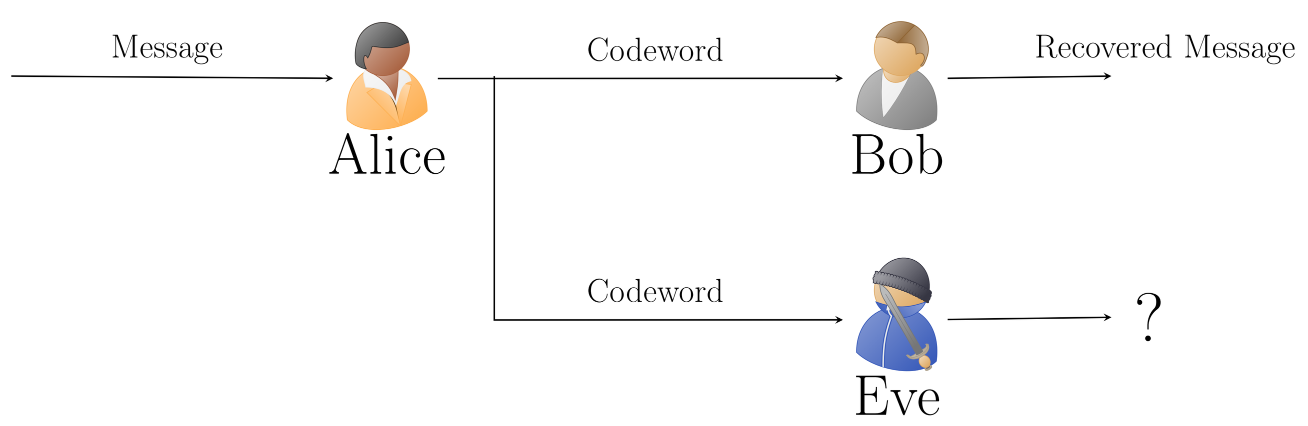
† Knowit, Oslo, Norway

* Simula UiB, Bergen, Norway

On the Secrecy Gain of Isodual Lattices from Tail-Biting Convolutional Codes

Motivation

- Wiretap channel: secure and reliable communication.



- **Challenge:** Design lattices for the Gaussian wiretap channel.

Codes and Lattices

- **Pure double circulant codes (PDCCs)** generated by $\mathsf{G} = (\mathsf{I}_k\ \mathsf{B}_k)$, where B_k is a circulant matrix

$$\mathsf{B}_k = \begin{pmatrix} b_1 & b_2 & \dots & b_k \\ b_k & b_1 & \dots & b_{k-1} \\ \vdots & \vdots & \dots & \vdots \\ b_2 & b_3 & \dots & b_1 \end{pmatrix}.$$

- Let $\mathcal{C}_s$ be the set of sequences obtained by traversing the trellis from state s at time 0 to state s at time ℓ of a convolutional code $\mathcal{C}$ with a given memory m. The set $\cup_{s=0}^{2^m}\mathcal{C}_s$ is a $[2\ell, \ell]$ linear block code known as **tail-biting (TB) convolutional code**.
- Codes such that their weight enumerator satisfy the MacWilliams identity are called formally self-dual codes.
- Let $\mathscr{C}$ be a binary $[n,k]$ code, then $\Lambda_{\mathrm{A}}(\mathscr{C}) = \frac{1}{\sqrt{2}}(\phi(\mathscr{C}) + 2\mathbb{Z}^n)$ is called a **Construction A** lattice, where ϕ denotes the natural embedding. Lattices obtained via Construction A from tail-biting convolutional codes are denoted as tail-biting (TB) lattices.

Secrecy gain of Construction A lattices

- Let Λ be a lattice with volume $\mathrm{vol}(\Lambda) = \nu^n$. The secrecy function of Λ is defined by

$$\Xi_\Lambda(\tau) = \frac{\Theta_{\nu\mathbb{Z}^n}(i\tau)}{\Theta_\Lambda(i\tau)},$$

for $\tau = -iz > 0$. The **secrecy gain** of a lattice is given by $\xi_\Lambda = \sup_{\tau>0}\Xi_\Lambda(\tau)$.
- **Objective:** Design good lattices to achieve high secrecy gain.

Theorem 1: [1, Th. 2] Let $\mathscr{C}$ be a formally self-dual code. Then

$$\left[\Xi_{\Lambda_{\mathrm{A}}(\mathscr{C})}(\tau)\right]^{-1} = \frac{W_{\mathscr{C}}\left(\sqrt{1+t(\tau)}, \sqrt{1-t(\tau)}\right)}{2^{\frac{n}{2}}},$$

where $0 < t(\tau) = \vartheta_4^2(i\tau)/\vartheta_3^2(i\tau) < 1$.

Theorem 2: [2, Th. 46] Consider $n \geq 2$. If $\mathscr{C}^\diamond$ is secrecy-optimal, i.e., $\Xi_{\Lambda_{\mathrm{A}}(\mathscr{C}^\diamond)}(\tau) \geq \Xi_{\Lambda_{\mathrm{A}}(\mathscr{C})}(\tau)$ for any formally self-dual code $\mathscr{C}$ of length n, then

$$\mathscr{C}^\diamond = \underset{\mathscr{C}\text{: formally self-dual}}{\operatorname{argmin}} \left\{\sum_{w=0}^{n} \frac{A_w(\mathscr{C})}{w+1}\right\}.$$

Contributions

- Search for rate 1/2 TB convolutional codes (resp. TB lattices) that improve on the secrecy gain.
- Best TB isodual codes are comparable with PDCC codes in terms of performance, indicating an advantage for using TB codes.
- Optimality test (Theorem 2) was performed for all TB convolutional codes.

Numerical results

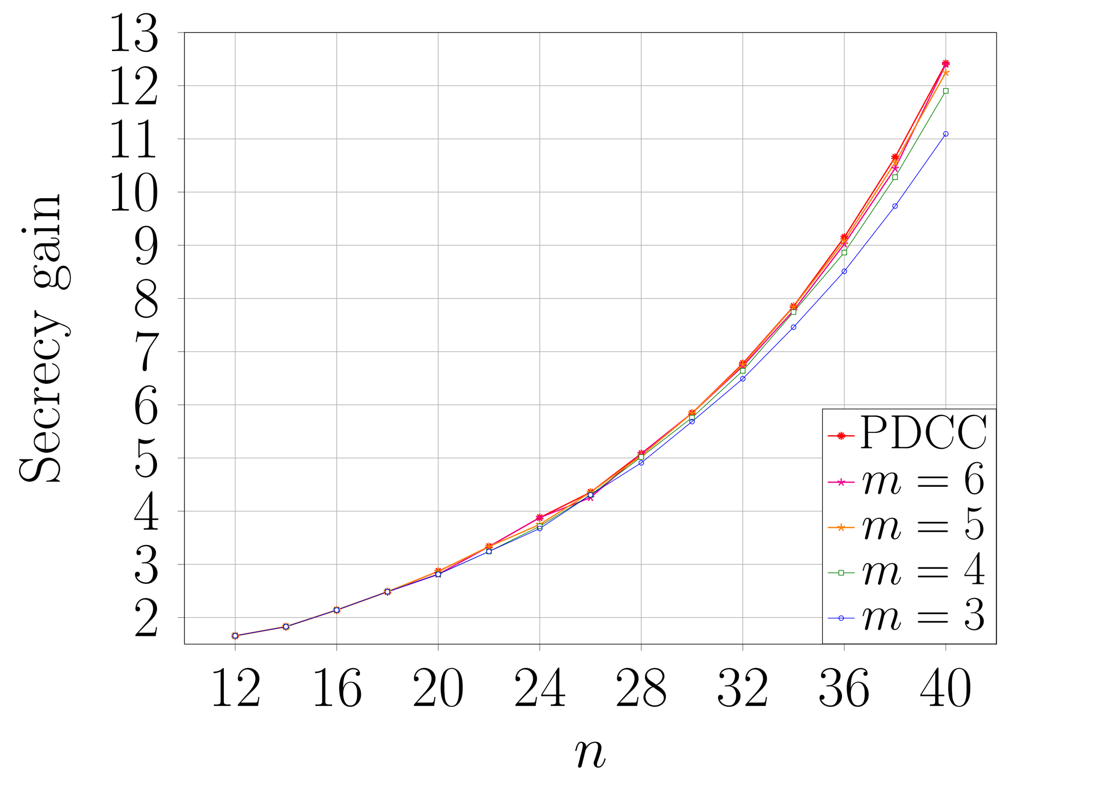


Figure: Comparison of the best-found secrecy gains of Construction A lattices obtained from TB isodual codes with memory $m = 3, 4, 5, 6$, and *the best* PDCCs, for even lengths $12 \leq n \leq 40$.

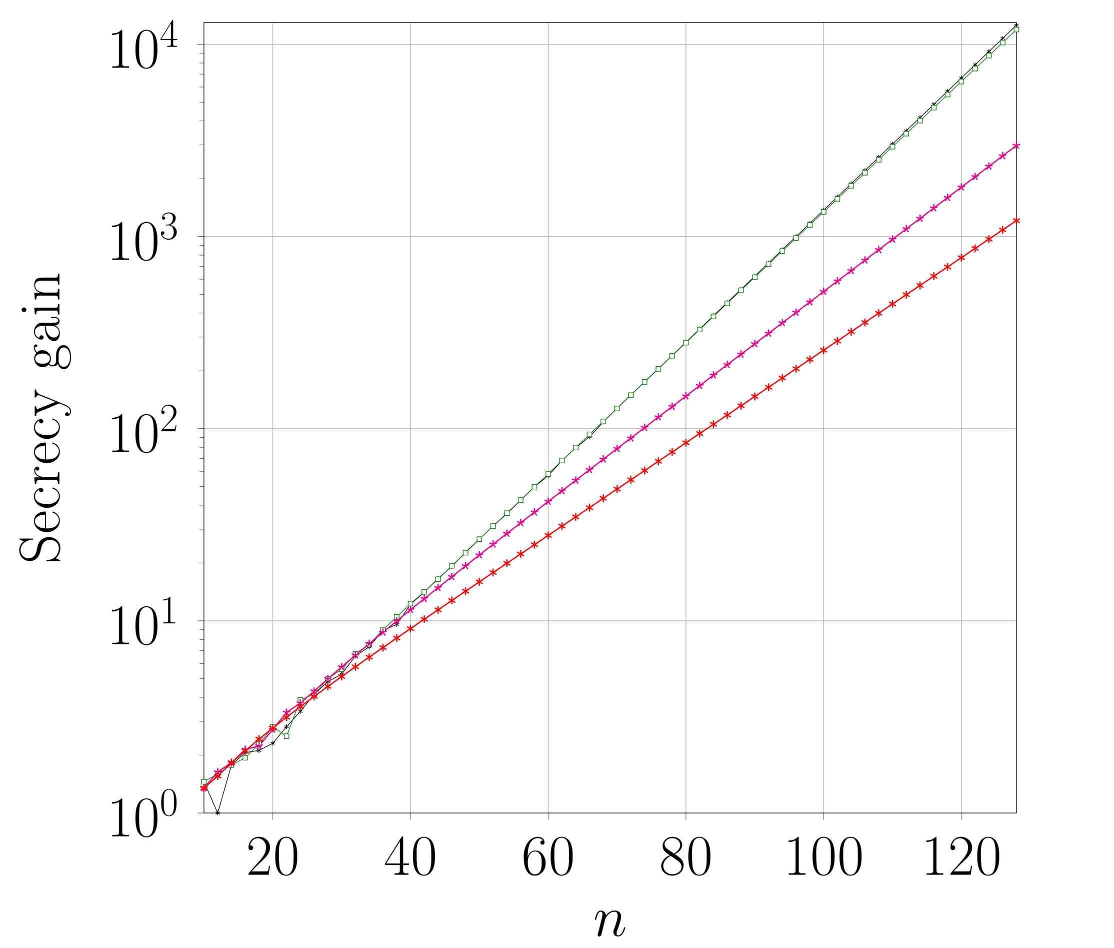


Figure: Secrecy gain evolution for fixed codes. Convolutional codes, with generator matrices in octal notion, are selected from [3], [4]: $\mathsf{G} = (5\ 7)$ (red), $\mathsf{G} = (7\ 53)$ (pink), $\mathsf{G} = (561\ 753)$ (green), $\mathsf{G} = (56235\ 63337)$ (black).

Analysis and Conclusions

- Other remarkable results that outperform unimodular lattices:
  - $n = 60$, $\xi_{\Lambda_{\mathrm{A}}(\mathscr{C})} \approx 54.721$,
  - $n = 80$, $\xi_{\Lambda_{\mathrm{A}}(\mathscr{C})} \approx 236.191$,
  - $n = 100$, $\xi_{\Lambda_{\mathrm{A}}(\mathscr{C})} \approx 991.887$.
- Exhaustive code searches of TB convolutional codes allow us to investigate the secrecy gain of higher dimensional lattices (up to $n = 108$ in this paper, but in principle, easily extendable).
- TB convolutional codes allow efficient decoding due to their trellis structure.
- Study the flatness factor in future work in order to estimate the information leakage instead of error probability.

References

[1] M. F. Bollauf, H.-Y. Lin, and Ø. Ytrehus, "The secrecy gain of formally unimodular lattices on the Gaussian wiretap channel," in *Proc. Int. Zurich Sem. Inf. Commun. (IZS)*, Zurich, Switzerland, Mar. 2–4, 2022, pp. 69–73.

[2] ——, "Formally unimodular packings for the Gaussian wiretap channel," Jun. 2022, arXiv:2206.14171v1 [cs.IT].

[3] S. Lin and D. J. Costello, Jr., *Error Control Coding*, 2nd ed. Upper Saddle River, NJ, USA: Pearson Prentice Hall, 2004.

[4] I. E. Bocharova, R. Johannesson, B. D. Kudryashov, and P. Stahl, "Tailbiting codes: Bounds and search results," *IEEE Trans. Inf. Theory*, vol. 48, no. 1, pp. 137–148, Jan. 2002.