TOWARDS A CHARACTERIZATION OF THE COVERT CAPACITY OF BOSONIC CHANNELS UNDER TRACE DISTANCE

IEEE International Symposium on Information Theory ▪ June 2022

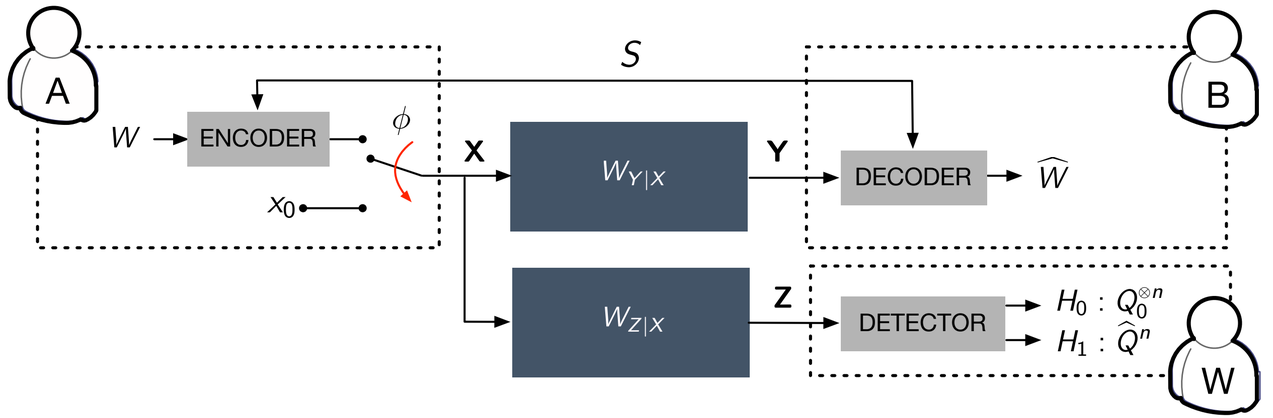
Shi-Yuan Wang, Tuna Erdoğan, and Matthieu R. Bloch

School of Electrical and Computer Engineering

- **COVERT COMMUNICATIONS**
  - Enhance privacy by **avoiding exposure of information transmission**
  - Communication with **low probability of detection**

- **FUNDAMENTAL LIMITS OF COVERT COMMUNICATIONS**
  - (*Square Root Law* **[Bash et al.'13]**) No more than $\mathcal{O}(\sqrt{n})$ bits over n uses of noisy memoryless channel
  - **Zero-rate** regime: rate of communication **vanishes** asymptotically

- **EXTENSIONS AND RELATED WORKS**
  - First- and second-order asymptotics **[Wang et al.'16, Bloch'16, Tahmasbi-Bloch'19]**
  - Multiuser channels **[Arumugam-Bloch'18'19'19, Tan-Lee'19,Cho-Li'21]**
  - Codes for covert communications **[Frèche et al.'17, Kadampot et al.'18'19, Lamarca-Matas'19, Zhang et al.'20, Wang-Bloch'21]**
  - AWGN channels **[Wang et al.'16, Zhang et al.'19, Yan et al.'19]**
  - MIMO-AWGN channels **[Abdelaziz-Koksal'17, Bendary et al.'19, Wang-Bloch'21]**
  - Variational distance constraint **[Tahmasbi-Bloch'19, Zhang et al.'19, Wang-Bloch'21]**
  - Classical-Quantum channels **[Bash et al.'15, Sheikholeslami et al.'16, Wang'16]**
  - Bosonic Channels **[Bullock et al.'20, Gagatsos et al.'20]**



- Switch $\phi \in \{0, 1\}$ controls transmission state at Alice
- **Innocent symbol** x_0 **:** *absence of communications*
  - Induces distributions $P_0 \triangleq W_{Y|X=x_0}$ and $Q_0 \triangleq W_{Z|X=x_0}$
- **Code** $\mathcal{C}$ **:** *occurrence of communications*
  - induces distribution $\widehat{Q}^n$ at Willie

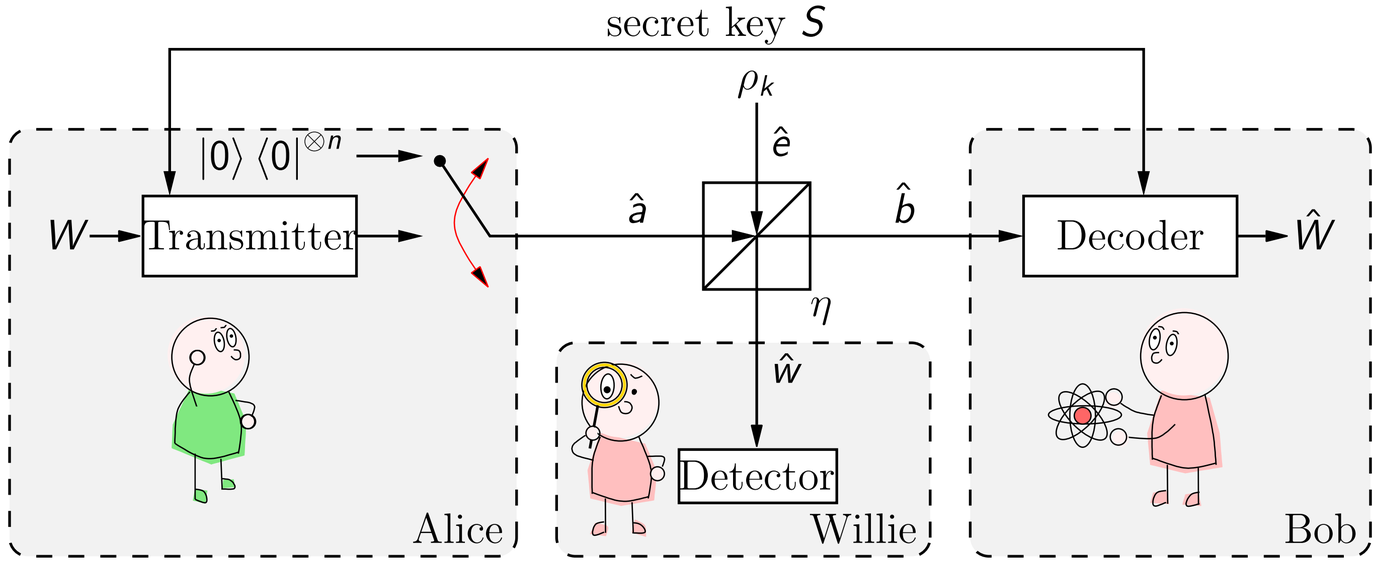
- **RELIABILITY:** Bob reliably recovers the message and guesses when the communication occurs

- **DETECTION:** Willie (passive warden) distinguishes
  - Hypothesis H_0 : $Q_0^{\otimes n}$ (*absence of communications*)
  - Hypothesis H_1 : $\widehat{Q}^n$ (*occurrence of communications*)

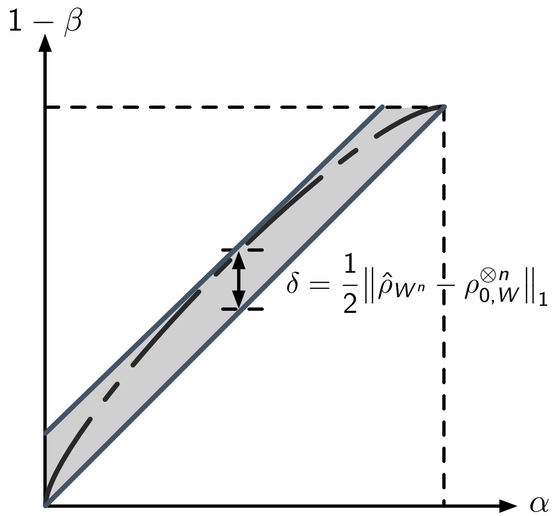
- **GOAL:** make sure Willie's test close to **blind test**

- Single-mode lossy thermal-noise bosonic channel $\mathcal{L}_{A\to BW}^{(\eta,k)}$
  - Transmissivity η
  - Described by a beamsplitter $\hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e}$, and $\hat{w} = \sqrt{1-\eta}\hat{a} + \sqrt{\eta}\hat{e}$
  - Environment in thermal bath with mean photon number k
    - Thermal state

$$\rho_k = \frac{1}{\pi k}\int \exp\left(-\frac{|\alpha|^2}{k}\right) d^2\alpha\, |\alpha\rangle\langle\alpha| = \sum_{n=0}^{\infty} \frac{k^n}{(k+1)^{n+1}} |n\rangle\langle n|$$



- **DEFINITION:** $(M, K, n, \epsilon, \delta)$ -code $\mathcal{C}$
  - Uniformly distributed message $W \in [\![1, M]\!]$
  - Uniformly distributed secret key $S \in [\![1, K]\!]$ shared with Bob
  - Encoding channel $\mathcal{E}_{SW\to A^n} : |s\rangle\langle s|_S \otimes |w\rangle\langle w|_W \mapsto \rho_{A^n}(s, w)$
  - Collection of decoding POVMs $\{\{\Pi_{B^n}^{(s,w)}\}_{w\in[\![1,M]\!]}\}_{s\in[\![1,K]\!]}$
  - Induces $\hat{\rho}_{W^n} \triangleq \frac{1}{MK}\sum_{s=1}^{K}\sum_{w=1}^{M} \mathrm{tr}_{B^n}\left(\left(\mathcal{L}_{A\to BW}^{(\eta,k)}\right)^{\otimes n} \rho_{A^n}(s, w)\right)$ at Willie



- **RELIABILITY METRIC**
  - Maximal average probability of error $P_e \triangleq \max_{s\in[\![1,K]\!]} \mathbb{P}\left(\widehat{W} \neq W | S = s\right) \leqslant \epsilon$

- **COVERTNESS METRIC**
  - For any test $\mathcal{T}_{W^n\to\{0,1\}}$ conducted by Willie, the probabilities of false alarm α and missed detection β satisfy

$$1 \geqslant \alpha + \beta \geqslant 1 - \frac{1}{2}\left\|\hat{\rho}_{W^n} - \rho_{0,W}^{\otimes n}\right\|_1 \geqslant 1 - \delta$$

  - Any test conducted by Willie is close to **blind test**

- **Trace distance** is the covertness metric that carries operational meaning

- **[Tahmasbi-Bloch'19]** investigates the impact and operational meaning of different covertness metrics for classical case
  - Relative entropy $\mathbb{D}(\widehat{Q}^n \,\|\, Q_0^{\otimes n})$
  - Variational distance $\mathbb{V}(\widehat{Q}^n, Q_0^{\otimes n})$
  - Optimal probability of missed detection $\beta_\alpha(Q_0^{\otimes n}, \widehat{Q}^n)$

- **CHOICE OF COVERTNESS METRIC MATTERS**
  - **No strong converse** for covertness in covert communication
  - Asymptotics of covert capacity depend on covertness metric

- **DRAWBACKS OF RELATIVE ENTROPY**
  - Loose proxy for variational distance, more stringent
  - Operational meaning preserved in variational distance

- Using variational distance leads to a 25% relative increase in throughput **[Wang-Bloch'21]**

- **TAKE AWAY:** variational distance is more operationally relevant, and so is trace distance

- **KNOWN RELATIONS [Hayashi'17]**

$$1-\sqrt{F(\rho,\sigma)} \leqslant \frac{1}{2}\|\rho-\sigma\|_1 \leqslant \sqrt{1-F(\rho,\sigma)} \leqslant \sqrt{\mathbb{D}(\rho\,\|\,\sigma)}$$

  - Fidelity is multiplicative for tensor-product states
  - Fidelity retains properties of distance through purified distance $P(\rho,\sigma) \triangleq \sqrt{1-F(\rho,\sigma)}$

- **[Bullock et al.'20], [Gagatsos et al.'20]** use quantum relative entropy

- We use purified distance (and therefore fidelity) as intermediate metric in achievability
  - **TECHNICAL DETAIL:** require triangle inequality and purified distance for resolvability analysis

DEFINITION: ACHIEVABLE THROUGHPUT AND COVERT CAPACITY

$(M, K, n, \epsilon, \delta)$ - code is ϵ-reliable and δ-covertness if $P_e \leqslant \epsilon$ and $\frac{1}{2}\left\|\hat{\rho}_{W^n} - \rho_{0,W}^{\otimes n}\right\|_1 \leqslant \delta$.

The maximum number of messages that can be transmitted by an $(M, K, n, \epsilon, \delta)$-code is $M^*(n, \epsilon, \delta)$.

Covert Capacity:

$$C_{\text{cov}} \triangleq \lim_{n\to\infty} \frac{\log M^*(n, \epsilon, \delta)}{\sqrt{n}}$$

For a sequence of code achieving covert capacity, **secret key throughput** is $\lim_{n\to\infty} \frac{\log K}{\sqrt{n}}$.

THEOREM: COVERT CAPACITY OF LOSSY THERMAL-NOISE BOSONIC CHANNEL

Covert capacity satisfies

$$\frac{2\sqrt{\eta k(\eta k+1)}}{1-\eta}\eta\log\left(1+\frac{1}{(1-\eta)k}\right)Q^{-1}\left(\frac{1-\delta}{2}\right) \geqslant C_{\text{cov}} \geqslant \frac{2\sqrt{\eta k(\eta k+1)}}{1-\eta}\eta\log\left(1+\frac{1}{(1-\eta)k}\right)\delta$$

Lower bound is achievable with key throughput satisfying

$$2\sqrt{\eta k(\eta k+1)}\left(\log\left(1+\frac{1}{\eta k}\right)-\frac{\eta}{1-\eta}\log\left(1+\frac{1}{(1-\eta)k}\right)\right)^+\delta$$

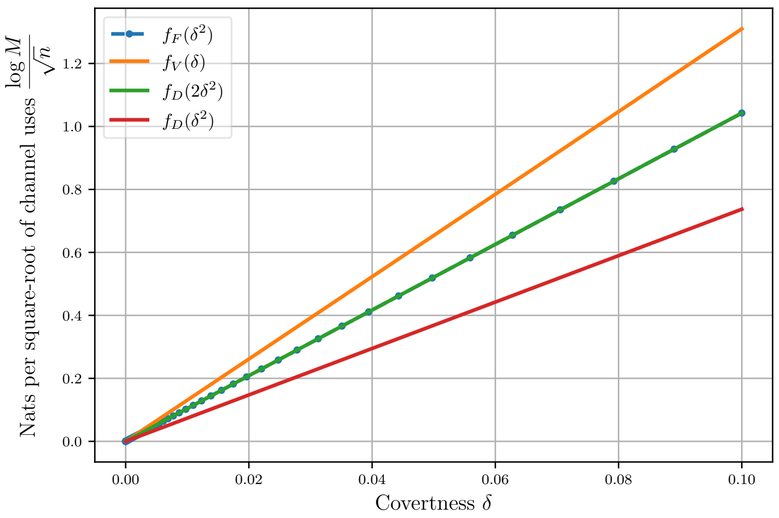
where $(x)^+ \triangleq \max(x, 0)$.

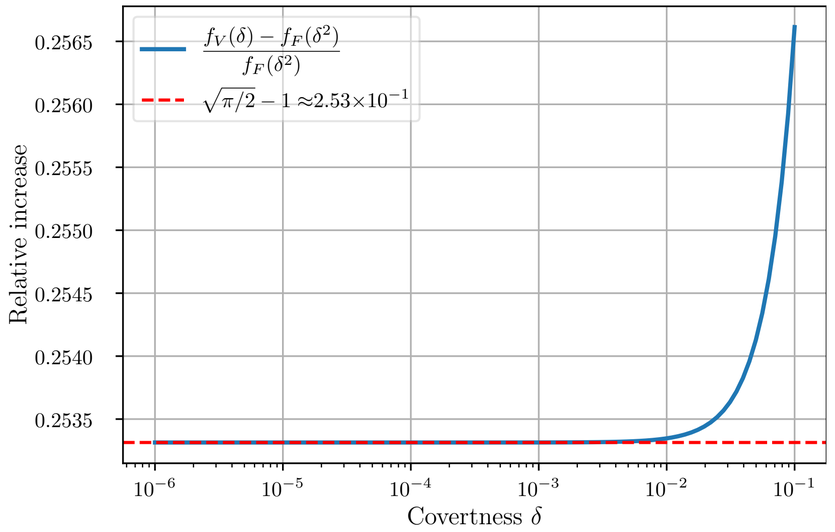
- **TAKE AWAY:** covert capacity is a function of covertness metric.

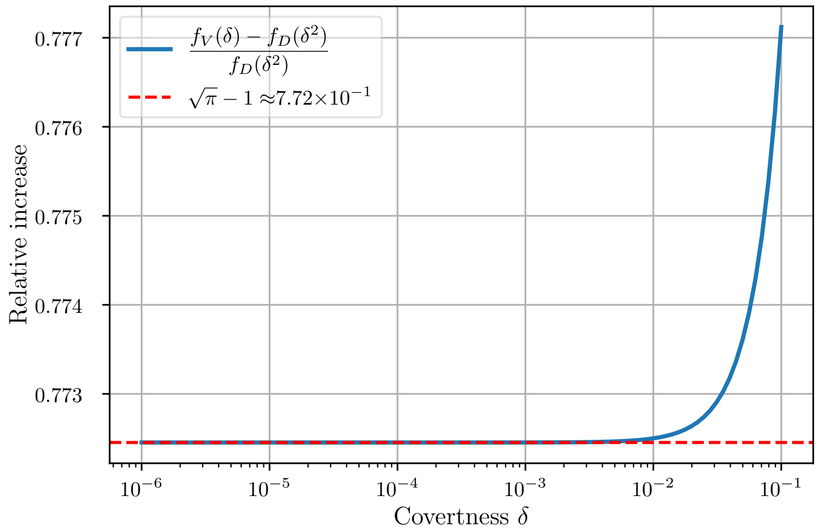
- **COMPARISON:** given $\frac{1}{2}\left\|\hat{\rho}_{W^n} - \rho_{0,W}^{\otimes n}\right\|_1 \leqslant \sqrt{1 - F(\hat{\rho}_{W^n}, \rho_{0,W}^{\otimes n})} \leqslant \sqrt{\mathbb{D}(\hat{\rho}_{W^n} \,\|\, \rho_{0,W}^{\otimes n})} \leqslant \delta$
  - Upper-bound is derived with trace distance metric, denoted by $f_V(\delta)$
  - Lower-bound is derived with fidelity metric, denoted by $f_F(\delta^2)$
  - We also compare previous result by **[Gagatsos et al.'20]** with quantum relative entropy metric, denoted by $f_D(\delta^2)$
- However, **[Bullock et al.'20]** and **[Gagatsos et al.'20]** consider **quantum Pinsker's inequality**
  - We denote this result by $f_D(2\delta^2)$

$$\frac{1}{2}\left\|\hat{\rho}_{W^n} - \rho_{0,W}^{\otimes n}\right\|_1 \leqslant \sqrt{\frac{\mathbb{D}(\hat{\rho}_{W^n} \,\|\, \rho_{0,W}^{\otimes n})}{2}} \leqslant \delta$$

- From above inequalities, $f_V(\delta) \geqslant f_F(\delta^2) = f_D(2\delta^2) \geqslant f_D(\delta^2)$







- **GOAL:** use **fidelity** to ensure $\frac{1}{2}\left\|\hat{\rho}_{W^n} - \rho_{0,W}^{\otimes n}\right\|_1 \leqslant \sqrt{1 - F(\hat{\rho}_{W^n}, \rho_{0,W}^{\otimes n})} \leqslant \delta$

- Coherent-state QPSK signaling with mean photon number decreasing in $\mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$
  - Ensure signal to be close to innocent states
  - Precise control of covertness

- One-shot channel reliability and resolvability
  - Existence of codebook that is reliable and does not change covertness much
  - Second-order asymptotic

- Coherent-state QPSK with **decreasing** mean photon number
  - Generated state at Alice's system $\rho_{n,XA} \triangleq \sum_{x\in[\![0,3]\!]} \frac{1}{4} |x\rangle\langle x|_X \otimes \left|u_n e^{j\pi x/2}\right\rangle\left\langle u_n e^{j\pi x/2}\right|_A$
  - Induced state at Willie's system $\rho_{n,XW} \triangleq \sum_{x\in[\![0,3]\!]} \frac{1}{4} |x\rangle\langle x|_X \otimes \rho_{\eta k,W}(\sqrt{1-\eta}u_n e^{j\pi x/2})$
  - **INTUITION:** perturbation in displacement around thermal state
- Perturbation theory for quantum fidelity **[Grace-Guha'21]**

LEMMA: FIDELITY ANALYSIS OF COHERENT-STATE QPSK

By setting $u_n \triangleq \frac{\left(4\eta k(\eta k+1)(\delta-2\kappa)^2\right)^{\frac{1}{4}}}{\sqrt{1-\eta}n^{\frac{1}{4}}}$, we have

$$F\left(\rho_{n,W}^{\otimes n}, \rho_{0,W}^{\otimes n}\right) \geqslant 1-(\delta-2\kappa)^2+\frac{(\delta-2\kappa)^4}{2}.$$

- Make sure existence of a codebook that is both reliable and covert

- **INGREDIENT**
  - Position-based coding and sequential decoding **[Wilde'17]**, **[Oskouei et al.'18]**
  - Convex-split lemma **[Anshu et al.'19]**, **[Khatri et al.'19]**

LEMMA: ONE-SHOT CHANNEL RELIABILITY AND RESOLVABILITY

By choosing fix $\epsilon, \kappa, \gamma_1, \gamma_2, \gamma_3 > 0$, then for a bi-partite state ρ_{XA} and a channel $\mathcal{G} : \rho_{XA} \mapsto \rho_{XBW}$, there exists a coding scheme such that

$$\log M \geqslant \mathbb{D}_{\mathrm{H}}^{\epsilon^2/10-\gamma_1}(\rho_{XB} \,\|\, \rho_X \otimes \rho_B) - \log\left(\frac{4\epsilon^2}{10\gamma_1^2}\right),$$

$$\log MK \leqslant \mathbb{D}_{\max}^{\kappa/2-\gamma_2-\gamma_3}(\rho_{XW} \,\|\, \rho_X \otimes \rho_W) + 2\log\left(\frac{1}{\gamma_2}\right) + \log\left(\frac{8}{\gamma_3^2}\right),$$

$$\mathbb{E}_{\mathcal{C},S}\left\{\mathbb{P}\left(\widehat{W} \neq W|S\right)\right\} \leqslant \frac{\epsilon^2}{10},$$

$$\mathbb{E}_{\mathcal{C}}\left\{\frac{1}{2}\|\hat{\rho}_W - \rho_W\|_1\right\} \leqslant \kappa - \gamma_2,$$

where $\mathcal{C}$ is the codebook.

- Analyze **trace distance** directly with techniques developed in **[Tahmasbi-Bloch'19, Zhang et al.'19, Wang-Bloch'21]**

- Constrained to **coherent-state** codebook
  - A **weaker** converse
  - **No entanglement** within modes
  - Possible to lift this constraint

- Establish lower bound on trace distance related to minimum received **photon number** of codewords
  - Require us to find a simple to analyze yet powerful test for Willie
  - Photon counter

- Show existence of good sub-code resulting in **low covertness metric**

- Obtain upper bound on **covert message size** of good sub-code

- Suboptimal photon counting test POVM $\{T, I - T\}$

$$T \triangleq \sum_{m_1+m_2+\cdots+m_n \geqslant \tau} |m_1\rangle\langle m_2| \otimes |m_2\rangle\langle m_2| \otimes \cdots \otimes |m_n\rangle\langle m_n|$$

  - Since modes are in tensor-product states, it reduces to a classical test $T(m^n) = \mathbb{1}\left\{\sum_{i=1}^{n} m_i \geqslant \tau\right\}$

- Carefully choose threshold and use photon number statistics of displaced thermal states with Berry-Esseen Theorem

LEMMA: LOWER BOUND ON TRACE DISTANCE

By setting $\tau = \dfrac{(1-\eta)N_*}{2} + n\eta k$, we have

$$\begin{aligned}\frac{1}{2}\left\|\hat{\rho}_{W^n} - \rho_{0,W}^{\otimes n}\right\|_1 &\geqslant 1 - \alpha - \beta \\ &\geqslant 1 - 2Q\left(\frac{(1-\eta)N_*}{2\sqrt{n\eta k(\eta k+1)}}\right) - \frac{(1-\eta)^2(1+2\eta k)N_*^2}{4\sqrt{2\pi}n^{3/2}[\eta k(\eta k+1)]^{3/2}} - \frac{B_0+B_1}{\sqrt{n}},\end{aligned}$$

where $N_* \triangleq \min_{m\in\mathcal{M}} \sum_{i=1}^{n} \left|\alpha_i^{(m)}\right|^2$ is minimum photon number of codewords, α is false-alarmed probability, β is missed-detection probability, and B_0, B_1 are some constants.

- **INTUITION:** covertness metric is higher in a set of high-photon-number codewords
- Partition code $\mathcal{C}$ into high-photon-number (bad) sub-code $\mathcal{C}^{(h)}$ and low-photon-number (good) sub-code $\mathcal{C}^{(\ell)}$

> **LEMMA:** EXISTENCE OF GOOD SUB-CODE
>
> For any covert codebook $\mathcal{C}$, let $\lim_{n\to\infty} \gamma_n = 0$. Then there exists a sub-code $\mathcal{C}^{(\ell)}$ such that $\left|\mathcal{C}^{(\ell)}\right| \geqslant \gamma_n |\mathcal{C}|$ and photon-number of codewords $N^{(c)} \leqslant A\sqrt{n}$,
>
> $$A \triangleq \frac{2\sqrt{\eta k(\eta k+1)}}{1-\eta} Q^{-1}\left(\frac{1-\delta}{2} - \frac{\nu^2(1-\eta)^2(1+2\eta k)}{4\sqrt{2\pi n}[\eta k(\eta k+1)]^{3/2}} - \gamma_n\right),$$
>
> where ν depends on channel.

- Characterize upper bound on photon-number of codewords in good sub-code

- Code $\mathcal{C}$ consists of K sub-codes $\mathcal{C}_s$ indexed by key $s \in [\![1, K]\!]$
  - Size of each sub-code is M
  - $\mathcal{C}_s^{(\ell)} \triangleq \mathcal{C}_s \cap \mathcal{C}^{(\ell)}$
  - By pigeonhole principle, $\left|\mathcal{C}_s^{(\ell)}\right| \geqslant \gamma_n M$

- We find an upper bound on $\log \left|\mathcal{C}_s^{(\ell)}\right|$ and therefore apply it to M
  - For bosonic channel, what we need is the bound on photon number we derived earlier
  - By Fano's inequality, Holevo bound, and capacity of bosonic channel

$$\log \left|\mathcal{C}_s^{(\ell)}\right| (1 - \frac{\epsilon_n}{\gamma_n}) - 1 \leqslant nC(\frac{A}{\sqrt{n}}, \eta, k) \leqslant \eta A \sqrt{n} \log \left(1 + \frac{1}{(1-\eta)k}\right)$$

$$\begin{aligned} \liminf_{n\to\infty} \frac{\log M}{\sqrt{n}} &\leqslant \liminf_{n\to\infty} \frac{\log \left|\mathcal{C}_s^{(\ell)}\right| - \log \gamma_n}{\sqrt{n}} \\ &= \frac{2\sqrt{\eta k(\eta k + 1)}}{1-\eta} \eta \log \left(1 + \frac{1}{(1-\eta)k}\right) Q^{-1}\left(\frac{1-\delta}{2}\right) \end{aligned}$$

  - $C(N, \bar{N}, \eta)$ is channel capacity of bosonic channel with photon numbers of two ports $N, \bar{N}$ and transmissivity η

- Gaussian ensemble $\left\{ \frac{1}{\pi s_n} \exp\left(-\frac{|\alpha|^2}{s_n} \right), |\alpha\rangle \langle \alpha| \right\}$ with $s_n = \frac{2\sqrt{\eta k(\eta k+1)}}{1-\eta} Q^{-1}\left(\frac{1-\delta}{2} \right)$ would achieve upper-bound
  - **TECHNICAL DIFFICULTY:** our coding theorem does not support uncountable alphabet
- Direct analysis of QPSK signaling with trace distance is challenging
- To extend converse to general *n*-mode states, consider applying an entanglement-breaking processing channel

$$\rho_W \mapsto \sum_m \mathrm{tr}\left(|m\rangle \langle m| \rho_W \right) \otimes |m\rangle \langle m|_M$$

  - Destroy entanglement between modes
  - Any single-mode Gaussian state is thermal state with displacement and symplectic transform

- **CONCLUSION**
  - Covert capacity of bosonic channel depends on choice of covertness metric
  - Trace distance is ultimate covertness metric carrying operational meaning
  - Characterize secret-key throughput of bosonic covert communications

Fundamental Limits of Quantum-Secure Covert Communication Over Bosonic Channels
M. S. Bullock, C. N. Gagatsos, S. Guha, and B. A. Bash
IEEE Journal on Selected Areas in Communications, vol. 38, no. 3, Mar. 2020

Covert Capacity of Bosonic Channels
C. N. Gagatsos, M. S. Bullock, and B. A. Bash
IEEE Journal on Selected Areas in Information Theory, vol. 1, no. 2, Feb. 2020

First- and Second-Order Asymptotics in Covert Communication
M. Tahmasbi and M. R. Bloch
IEEE Transactions on Information Theory, vol. 65, no. 4, Apr. 2019

Covert MIMO Communications under Variational Distance Constraint
S.-Y. Wang and M. R. Bloch
IEEE Transactions on Information Forensics and Security, vol. 16, 2021.

Quantum Information Theory
M. Hayashi
Springer Berlin Heidelberg, 2017

Undetectable Radios: Covert Communication under Spectral Mask Constraints
Qiaosheng Eric Zhang, Matthieu R. Bloch, Mayank Bakshi, Sidharth Jaggi
Proc. of IEEE International Symposium on Information Theory, Paris, France, Jul. 2019

Perturbation Theory for Quantum Information
M. R. Grace and S. Guha
arXiv preprint, 2106.05533, Jun. 2021

Position-based Coding and Convex Splitting for Private Communication over Quantum Channels
M. M. Wilde
Quantum Information Processing, vol. 16, no. 10, p. 264, Oct. 2017

Union Bound for Quantum Information Processing
S. K. Oskouei, S. Mancini, and M. M. Wilde
Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, vol. 475, no. 2221, Apr. 2018

Building Blocks for Communication Over Noisy Quantum Networks
A. Anshu, R. Jain, and N. A. Warsi
IEEE Transactions on Information Theory, vol. 65, no. 2, Feb. 2019

Second-order Coding Rates for Key Distillation in Quantum Key Distribution
S. Khatri, E. Kaur, S. Guha, and M. M. Wilde,
arXiv e-prints, 1910.03883, Oct. 2019