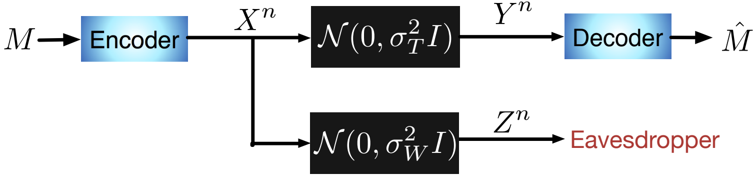
Explicit Capacity-Achieving Coding Scheme for the Gaussian Wiretap Channel

Himanshu Tyagi and Alexander Vardy

UC San Diego

The Gaussian wiretap channel



Power constraint

$$\|e(m)\|_2^2 \leq nP \text{ for all messages m}$$

Probability of error

$$\epsilon(e, d) \triangleq \max_{m \in \{0,1\}^k} \mathrm{P}\left(d(Y^n) \neq m \mid m \text{ is sent}\right)$$

Security parameter

$$\sigma(e, d) \triangleq I(M \wedge Z^n)$$

Wiretap channel capacity

Capacity C_s = Maximum possible rate of a wiretap codes such that

$$\epsilon(e_n, d_n) \to 0 \text{ and } I(M \wedge Z^n) \to 0 \quad \text{(strong secrecy)}$$

Characterization of C_s

Wyner 1975: Degraded wiretap channel

Csiszár and Körner 1978: General wiretap channel

L.-Y.-Cheong and Hellman 1978: Gaussian wiretap channel

$$C_s = \frac{1}{2}\log\left(\frac{1 + P/\sigma_T^2}{1 + P/\sigma_W^2}\right) = C(T) - C(W)$$

Codes for wiretap channels

Algebraic codes: Wei 1991

Schemes based on LDPC codes: Thangaraj et. al. 2007

Scheme based on Polar codes: Mahdavifar and Vardy 2010

Lattice codes for the GWC: Oggier, Solé, and Belfiore 2010

Codes for wiretap channels

Algebraic codes: Wei 1991

Schemes based on LDPC codes: Thangaraj et. al. 2007

Scheme based on Polar codes: Mahdavifar and Vardy 2010

Lattice codes for the GWC: Oggier, Solé, and Belfiore 2010

Story before 2010: No explicit capacity achieving schemes available

Codes for wiretap channels

Algebraic codes: Wei 1991

Schemes based on LDPC codes: Thangaraj et. al. 2007

Scheme based on Polar codes: Mahdavifar and Vardy 2010

Lattice codes for the GWC: Oggier, Solé, and Belfiore 2010

Story before 2010: No explicit capacity achieving schemes available

Hayashi and Matsumoto 2010, Bellare, Tessaro and Vardy 2012:

Constructions using invertible extractors

Decouple error correction and secrecy

What are extractors?

Question. Given correlated random variables U and Z, can you *extract* bits from U that are almost independent of Z?

What are extractors?

Question. Given correlated random variables U and Z, can you *extract* bits from U that are almost independent of Z?

(Impagliazzo et. al. '89, Bennett et. al. '95) Can construct an efficient random mapping F such that $I(F(U) \wedge Z) \approx 0$

What are extractors?

Question. Given correlated random variables U and Z, can you *extract* bits from U that are almost independent of Z?

(Impagliazzo et. al. '89, Bennett et. al. '95) Can construct an efficient random mapping F such that $I(F(U) \wedge Z) \approx 0$

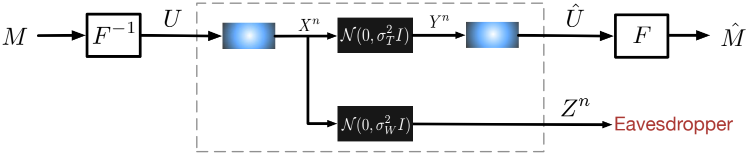


Figure: Wiretap codes from channel codes, via extractors

What are extractors?

Question. Given correlated random variables U and Z, can you *extract* bits from U that are almost independent of Z?

(Impagliazzo et. al. '89, Bennett et. al. '95) Can construct an efficient random mapping F such that $I(F(U) \wedge Z) \approx 0$

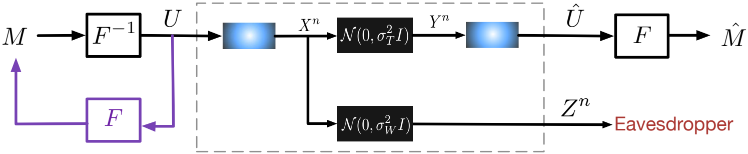


Figure: Wiretap codes from channel codes, via extractors

Efficient extractors using a 2-universal hash family

Consider mappings $f : \{0,1\}^l \times \{0,1\}^l \to \{0,1\}^k$ defined by

$$f : (s, v) \mapsto (s * v)_k$$

$*$ is multiplication in $GF(2^l)$

$(\cdot)_k$ selects the k most significant bits

$\{f_s(v) = f(s, v),\ s \in \mathcal{S}\}$ constitutes a 2-universal hash family

Efficient extractors using a 2-universal hash family

Consider mappings $f : \{0,1\}^l \times \{0,1\}^l \to \{0,1\}^k$ defined by

$$f : (s, v) \mapsto (s * v)_k$$

$*$ is multiplication in $GF(2^l)$

$(\cdot)_k$ selects the k most significant bits

$\{f_s(v) = f(s, v),\ s \in \mathcal{S}\}$ constitutes a 2-universal hash family

Can be implemented efficiently

Efficient extractors using a 2-universal hash family

Consider mappings $f : \{0,1\}^l \times \{0,1\}^l \to \{0,1\}^k$ defined by

$$f : (s, v) \mapsto (s * v)_k$$

$*$ is multiplication in $GF(2^l)$

$(\cdot)_k$ selects the k most significant bits

$\{f_s(v) = f(s, v),\ s \in \mathcal{S}\}$ constitutes a 2-universal hash family

Can be implemented efficiently

But is it invertible?

Efficient extractors using a 2-universal hash family

Consider mappings $f : \{0,1\}^l \times \{0,1\}^l \to \{0,1\}^k$ defined by

$$f : (s, v) \mapsto (s * v)_k$$

$*$ is multiplication in $GF(2^l)$

$(\cdot)_k$ selects the k most significant bits

$\{f_s(v) = f(s, v),\ s \in \mathcal{S}\}$ constitutes a 2-universal hash family

Can be implemented efficiently

But is it invertible?

Almost! The map $\phi : (s, m, b) \mapsto s^{-1} * (m|b)$ satisfies

$$f(s, \phi(s, m, b)) = m, \quad \text{for all } s, b$$

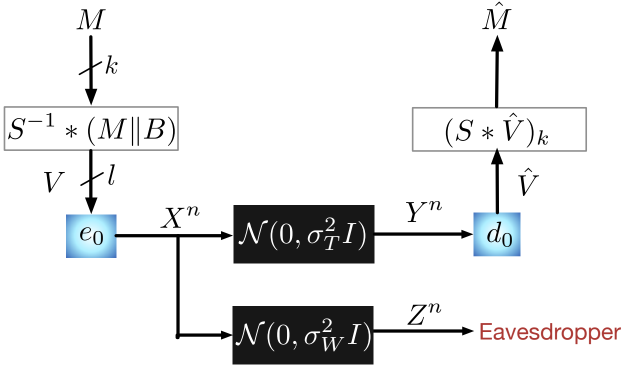
$(\cdot|\cdot)$ denotes concatenation

Explicit codes for wiretap channels

(e_0, d_0) be an (n, l) transmission code satisfying the power constraint

Shared public randomness: $S \sim \texttt{unif}\{0,1\}^l$

Local Randomness: $B \sim \texttt{unif}\{0,1\}^{l-k}$



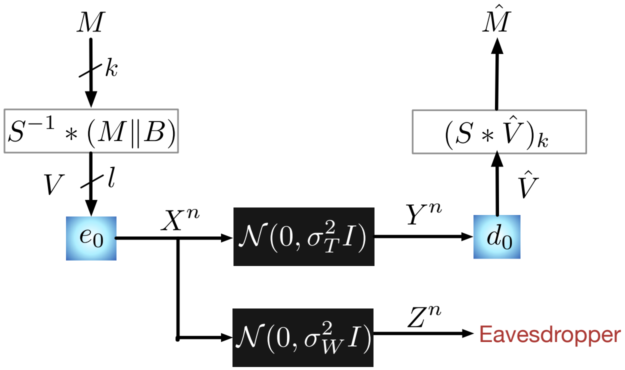
S can be dropped with negligible rate loss

Explicit codes for wiretap channels

(e_0, d_0) be an (n, l) transmission code satisfying the power constraint

Shared public randomness: $S \sim \texttt{unif}\{0,1\}^l$

Local Randomness: $B \sim \texttt{unif}\{0,1\}^{l-k}$



S can be dropped with negligible rate loss

A new simple proof applicable to GWC

Hayashi and Matsumoto assume that uniform distribution achieves C_s

Bellare and Tessaro assume discrete symmetric wiretap channel

How do you handle continuous alphabet and power constraints?

A new simple proof applicable to GWC

Hayashi and Matsumoto assume that uniform distribution achieves C_s

- *not applicable to Gaussian channels*

Bellare and Tessaro assume discrete symmetric wiretap channel

- *not applicable to Gaussian channels*

How do you handle continuous alphabet and power constraints?

A new simple proof applicable to GWC

Hayashi and Matsumoto assume that uniform distribution achieves C_s

- *not applicable to Gaussian channels*

Bellare and Tessaro assume discrete symmetric wiretap channel

- *not applicable to Gaussian channels*

How do you handle continuous alphabet and power constraints?

It suffices to show:

$$\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\texttt{unif}}\mathrm{P}_{Z^nS}\|_1 \approx e^{-n\delta}$$

since

$$\begin{aligned} I(M \wedge Z^n, S) &\leq k - H(M \mid Z^n, S) \\ &= D(\mathrm{P}_{MZ^nS} \| \mathrm{P}_{\texttt{unif}}\mathrm{P}_{Z^nS}) \end{aligned}$$

A key tool: Leftover Hash Lemma

The conditional min-entropy is defined as

$$H_{min}(\mathrm{P}_{UZ} \mid \mathrm{P}_Z) = -\log \int_{\mathbb{R}^n} \max_u \mathrm{P}_U(u)\, p(z|u)dz$$

and the smooth conditional min-entropy is defined as

$$H^{\epsilon}_{min}(\mathrm{P}_{UZ} \mid \mathrm{P}_Z) = \sup_{\substack{\mathrm{Q}_{UZ}: \\ \|\mathrm{Q}_{UZ} - \mathrm{P}_{UZ}\|_1 \le \epsilon}} H_{min}(\mathrm{Q}_{UZ} \mid \mathrm{Q}_Z)$$

Lemma

For a 2-universal hash family $\left\{f_s : \mathcal{U} \to \{1, ..., 2^k\} | s \in \mathcal{S}\right\}$ *and* $S \sim \mathtt{unif}(\mathcal{S})$, *we have*

$$\|\mathrm{P}_{f_S(U)ZS} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_Z\mathrm{P}_S\|_1 \le 2\epsilon + \frac{1}{2}\sqrt{2^{k - H^{\epsilon}_{min}(\mathrm{P}_{UZ}|\mathrm{P}_Z)}}.$$

Proof of security: Step 1

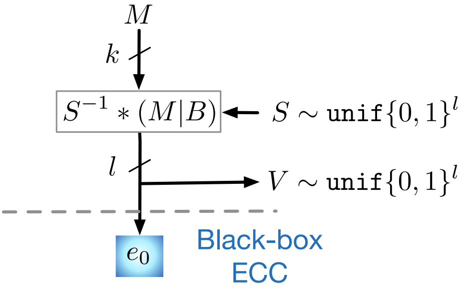
To show: $\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_{Z^nS}\|_1 \approx e^{-n\delta}$

Can we apply the leftover hash lemma?

Proof of security: Step 1

To show: $\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_{Z^nS}\|_1 \approx e^{-n\delta}$

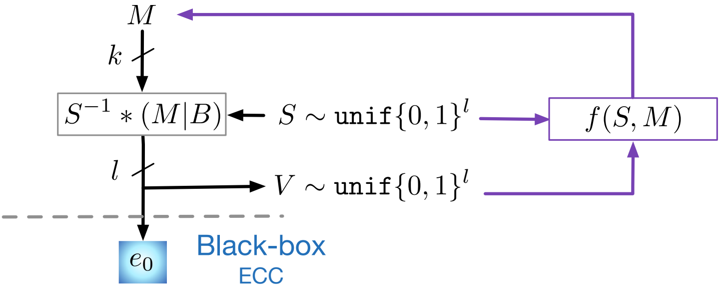
Can we apply the leftover hash lemma?



Proof of security: Step 1

To show: $\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\texttt{unif}}\mathrm{P}_{Z^nS}\|_1 \approx e^{-n\delta}$

Can we apply the leftover hash lemma?



Proof of security: Step 1

To show: $\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_{Z^nS}\|_1 \approx e^{-n\delta}$

Can we apply the leftover hash lemma?

Lemma (Transformation of random variables)

For RVs S, M, V, Z^n as above, we have

$$\mathrm{P}_{MVZ^nS} \equiv \mathrm{P}_{\tilde{M}\tilde{V}\tilde{Z}^n\tilde{S}},$$

where $\tilde{S}$ and $\tilde{V}$ are independent, $(\tilde{S}, \tilde{M})$—$\tilde{V}$—$\tilde{Z}^n$ form a Markov chain, and

$$\tilde{S} \sim \mathtt{unif}\{0,1\}^l, \quad \tilde{V} \sim \mathtt{unif}\{0,1\}^l,$$

$\tilde{M} = f(\tilde{S}, \tilde{V})$ *and* $\mathrm{P}_{\tilde{Z}^n|\tilde{V}} \equiv \mathrm{P}_{Z^n|V}$.

Proof of security: Step 2

We apply leftover hash lemma with $U = \tilde{V}$ and $Z = \tilde{Z}^n$

Lemma

For RVs $M, Z^n, S, \tilde{V}, \tilde{Z}^n$ as above, we have

$$\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_{Z^nS}\|_1 \le 2\epsilon + \frac{1}{2}\sqrt{2^{k - H_{\min}^{\epsilon}(\mathrm{P}_{\tilde{V}\tilde{Z}^n}|\mathrm{P}_{\tilde{Z}^n})}}.$$

Proof of security: Step 2

We apply leftover hash lemma with $U = \tilde{V}$ and $Z = \tilde{Z}^n$

Lemma

For RVs $M, Z^n, S, \tilde{V}, \tilde{Z}^n$ as above, we have

$$\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_{Z^nS}\|_1 \le 2\epsilon + \frac{1}{2}\sqrt{2^{k - H_{\min}^{\epsilon}(\mathrm{P}_{\tilde{V}\tilde{Z}^n}|\mathrm{P}_{\tilde{Z}^n})}}.$$

For sets $\mathcal{Z}_v \subseteq \mathbb{R}^n$ such that $\int_{\mathcal{Z}_v} p(z|v) \ge 1 - 2\epsilon$,

$$H_{min}^{\epsilon}(\mathrm{P}_{\tilde{V}\tilde{Z}^n}|\mathrm{P}_{\tilde{Z}^n}) \ge l - \log \int_{\mathbb{R}^n} \max_v \mathbf{1}(z \in \mathcal{Z}_v)p(z|v)dz,$$

where

$$p(z|v) = g\left(\sigma_W^{-1}(z - e_0(v))\right).$$

Proof of security: Step 2

We apply leftover hash lemma with $U = \tilde{V}$ and $Z = \tilde{Z}^n$

Lemma

For RVs $M, Z^n, S, \tilde{V}, \tilde{Z}^n$ as above, we have

$$\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_{Z^nS}\|_1 \leq 2\epsilon + \frac{1}{2}\sqrt{2^{k-H_{\min}^{\epsilon}(\mathrm{P}_{\tilde{V}\tilde{Z}^n}|\mathrm{P}_{\tilde{Z}^n})}}.$$

For sets $\mathcal{Z}_v \subseteq \mathbb{R}^n$ such that $\int_{\mathcal{Z}_v} p(z|v) \geq 1 - 2\epsilon$,

$$H_{min}^{\epsilon}(\mathrm{P}_{\tilde{V}\tilde{Z}^n}|\mathrm{P}_{\tilde{Z}^n}) \geq l - \log \int_{\mathbb{R}^n} \max_v \mathbf{1}(z \in \mathcal{Z}_v)p(z|v)dz,$$

where

$$p(z|v) = g\left(\sigma_W^{-1}(z - e_0(v))\right).$$

Bounding $H_{\min}^{\epsilon}\left(\mathrm{P}_{\tilde{V}\tilde{Z}^n} \mid \mathrm{P}_{\tilde{Z}^n}\right)$ is a concentration problem at its heart

Proof of security: Step 2

We apply leftover hash lemma with $U = \tilde{V}$ and $Z = \tilde{Z}^n$

Lemma

For RVs $M, Z^n, S, \tilde{V}, \tilde{Z}^n$ as above, we have

$$\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_{Z^nS}\|_1 \leq 2\epsilon + \frac{1}{2}\sqrt{2^{k - H_{\mathrm{min}}^{\epsilon}(\mathrm{P}_{\tilde{V}\tilde{Z}^n}|\mathrm{P}_{\tilde{Z}^n})}}.$$

Lemma

Fix $0 < \delta < 1/2$ and let $\epsilon = e^{-n\delta^2/8}$. Then,

$$H_{min}^{\epsilon}(\mathrm{P}_{\tilde{V}\tilde{Z}^n}|\mathrm{P}_{\tilde{Z}^n}) \geq l - \frac{n}{2}\log\left(1 + \delta + \frac{P}{\sigma_W^2}\right) - \frac{n\delta}{2} + o(n).$$

Main result

Theorem (Security bound for the scheme)

For a message $M \sim \texttt{unif}\{0,1\}^k$*, the proposed coding scheme satisfies*

$$\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\texttt{unif}}\mathrm{P}_{Z^nS}\|_1 \lesssim \frac{1}{2}\sqrt{2^{k-l+\frac{n}{2}\log\left(1+\delta+\frac{P}{\sigma_W^2}\right)+\frac{n\delta}{2}+o(n)}}$$

for all $\delta > 0$.

For a code (e_0, d_0) of rate R, the rate of the resulting code is

$$\frac{k}{n} \approx R - \frac{1}{2}\log\left(1+\delta+\frac{P}{\sigma_W^2}\right) - \frac{\delta}{2}$$

Main result

Theorem (Security bound for the scheme)

For a message $M \sim \texttt{unif}\{0,1\}^k$, *the proposed coding scheme satisfies*

$$\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\texttt{unif}}\mathrm{P}_{Z^nS}\|_1 \lesssim \frac{1}{2}\sqrt{2^{k-l+\frac{n}{2}\log\left(1+\delta+\frac{P}{\sigma_W^2}\right)+\frac{n\delta}{2}+o(n)}}$$

for all $\delta > 0$.

For a code (e_0, d_0) of rate R, the rate of the resulting code is

$$\frac{k}{n} \approx R - \frac{1}{2}\log\left(1+\delta+\frac{P}{\sigma_W^2}\right) - \frac{\delta}{2}$$

In particular, if (e_0, d_0) achieves transmission capacity, the proposed codes achieve the capacity of the wiretap channel

Closing remarks

Our analysis relies only on eavesdropper's channel being Gaussian, no assumptions needed on the transmission channel

Extensions to eavesdropper's noise being logconcave?

Security when $M \not\sim \texttt{unif}\{0,1\}^k$?