Explicit Capacity-Achieving Coding Scheme for the Gaussian Wiretap Channel

Himanshu Tyagi and Alexander Vardy

UC San Diego
The Gaussian wiretap channel

\[ M \rightarrow \text{Encoder} \rightarrow X^n \rightarrow \mathcal{N}(0, \sigma^2_T I) \rightarrow Y^n \rightarrow \text{Decoder} \rightarrow \hat{M} \]

\[ \mathcal{N}(0, \sigma^2_W I) \rightarrow Z^n \rightarrow \text{Eavesdropper} \]

**Power constraint**

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

**Probability of error**

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

**Security parameter**

\[ \sigma(e, d) \triangleq I(M \wedge Z^n) \]
Wiretap channel capacity

Capacity $C_s = \text{Maximum possible rate of a wiretap codes such that}$

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

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
**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 $I(F(U) \land Z) \approx 0$
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 $I(F(U) \land Z) \approx 0$

---

**Figure:** Wiretap codes from channel codes, via 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 $I(F(U) \land Z) \approx 0$

**Figure:** Wiretap codes from channel codes, via extractors
Consider mappings \( f : \{0, 1\}^l \times \{0, 1\}^l \rightarrow \{0, 1\}^k \) defined by

\[
f : (s, v) \mapsto (s * v)_k
\]

\(*\) is multiplication in \( GF(2^l) \)
\((\cdot)_k\) selects the \( k \) most significant bits

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

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

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

$\ast$ is multiplication in $GF(2^l)$

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

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

*Can be implemented efficiently*
Efficient extractors using a 2-universal hash family

Consider mappings \( f : \{0, 1\}^l \times \{0, 1\}^l \rightarrow \{0, 1\}^k \) defined by

\[
f : (s, v) \mapsto (s \ast v)_k
\]

\( \ast \) is multiplication in \( GF(2^l) \)

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

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

*Can be implemented efficiently*

But is it invertible?
Consider mappings \( f : \{0, 1\}^l \times \{0, 1\}^l \rightarrow \{0, 1\}^k \) defined by

\[
f : (s, v) \mapsto (s \ast v)_k
\]

\( \ast \) is multiplication in \( GF(2^l) \)

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

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

*Can be implemented efficiently*

**But is it invertible?**

Almost! The map \( \phi : (s, m, b) \mapsto s^{-1} \ast (m|b) \) 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: \(S \sim \text{unif}\{0, 1\}^l\)
Local Randomness: \(B \sim \text{unif}\{0, 1\}^{l-k}\)

\(S\) 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: \(S \sim \text{unif}\{0,1\}^l\)

Local Randomness: \(B \sim \text{unif}\{0,1\}^{l-k}\)

\(S\) 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:

$$\left\| P_{MZ^nS} - P_{\text{unif}P_{Z^nS}} \right\|_1 \approx e^{-n\delta}$$

since

$$I(M \wedge Z^n, S) \leq k - H(M \mid Z^n, S)$$
$$= D(P_{MZ^nS} \parallel P_{\text{unif}P_{Z^nS}})$$
A key tool: Leftover Hash Lemma

The conditional min-entropy is defined as

\[ H_{\text{min}}(P_{UZ} \mid P_Z) = -\log \int_{\mathbb{R}^n} \max_u P_U(u) p(z \mid u) dz \]

and the smooth conditional min-entropy is defined as

\[ H_{\text{min}}^\epsilon(P_{UZ} \mid P_Z) = \sup_{Q_{UZ} : \|Q_{UZ} - P_{UZ}\|_1 \leq \epsilon} H_{\text{min}}(Q_{UZ} \mid Q_Z) \]

Lemma

For a 2-universal hash family \( \{f_s : \mathcal{U} \to \{1, \ldots, 2^k\} \mid s \in S\} \) and \( S \sim \text{unif}(S) \), we have

\[ \|P_{f_s(U)ZS} - P_{\text{unif}}P_ZP_S\|_1 \leq 2\epsilon + \frac{1}{2} \sqrt{2^k - H_{\text{min}}^\epsilon(P_{UZ} \mid P_Z)}. \]
Proof of security: Step 1

To show: $\|P_{MZ^nS} - P_{unif}P_{Z^nS}\|_1 \approx e^{-n\delta}$

Can we apply the leftover hash lemma?
Proof of security: Step 1

To show: \( \|P_{MZ^nS} - P_{unif}P_{Z^nS}\|_1 \approx e^{-n\delta} \)

Can we apply the leftover hash lemma?

\[ M \]
\[ k \]
\[ S^{-1} \star (M|B) \]
\[ S \sim \text{unif}\{0,1\}^l \]
\[ l \]
\[ V \sim \text{unif}\{0,1\}^l \]

\[ e_0 \]

Black-box ECC
Proof of security: Step 1

To show: \( \| P_{MZ^nS} - P_{unif} P_{Z^nS} \|_1 \approx e^{-n\delta} \)

Can we apply the leftover hash lemma?

\[ M \]
\[ k \]
\[ S^{-1} \ast (M|B) \]
\[ S \sim \text{unif}\{0,1\}^l \]
\[ f(S, M) \]
\[ V \sim \text{unif}\{0,1\}^l \]

Black-box ECC
Proof of security: Step 1

To show: \( \|P_{MZ^nS} - P_{\text{unif}P_{Z^nS}}\|_1 \approx e^{-n\delta} \)

Can we apply the leftover hash lemma?

**Lemma (Transformation of random variables)**

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

\[ P_{MVZ^nS} \equiv P_{\tilde{M}\tilde{V}\tilde{Z}^n\tilde{S}}, \]

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

\[ \tilde{S} \sim \text{unif}\{0,1\}^l, \quad \tilde{V} \sim \text{unif}\{0,1\}^l, \]

\[ \tilde{M} = f(\tilde{S}, \tilde{V}) \text{ and } P_{\tilde{Z}^n|\tilde{V}} \equiv P_{Z^n|V}. \]
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

$$\|P_{MZ^nS} - P_{\text{unif}}P_{Z^nS}\|_1 \leq 2\epsilon + \frac{1}{2}\sqrt{2^{k-H^e_{\min}(P_{\tilde{V}\tilde{Z}^n}|P_{\tilde{Z}^n})}}.$$
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

$$\|P_M Z^n S - P_{\text{unif}} P Z^n S\|_1 \leq 2\epsilon + \frac{1}{2} \sqrt{2^{k-H_{\min}^e(P_{\tilde{V}} \tilde{Z}^n | P \tilde{Z}^n)}}.$$  

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

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

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

$$\|P_{MZ^nS} - P_{\text{unif}}P_{Z^nS}\|_1 \leq 2\epsilon + \frac{1}{2}\sqrt{2^{k-H^e_{\min}(P_{\tilde{V}\tilde{Z}^n}|P_{\tilde{Z}^n})}}.$$ 

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

$$H^e_{\min}(P_{\tilde{V}\tilde{Z}^n}|P_{\tilde{Z}^n}) \geq l - \log \int_{\mathbb{R}^n} \max_v 1(z \in \mathcal{Z}_v)p(z|v)dz,$$

where

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

Bounding $H^e_{\min}(P_{\tilde{V}\tilde{Z}^n}|P_{\tilde{Z}^n})$ 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*

\[
\| P M Z^n S - P_{\text{unif}} P Z^n S \|_1 \leq 2\epsilon + \frac{1}{2} \sqrt{2^{k-H_{\min}^e(P \tilde{V} \tilde{Z}^n|P \tilde{Z}^n)}}.
\]

**Lemma**

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

\[
H_{\min}^e(P \tilde{V} \tilde{Z}^n|P \tilde{Z}^n) \geq l - \frac{n}{2} \log \left( 1 + \delta + \frac{P}{\sigma_W^2} \right) - \frac{n\delta}{2} + o(n).
\]
Main result

Theorem (Security bound for the scheme)

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

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

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 $M \sim \text{unif}\{0,1\}^k$, the proposed coding scheme satisfies

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

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 $M \sim \text{unif}\{0, 1\}^k$?