Compute-and-Forward Can Buy Secrecy Cheap

Parisa Babaeiadian*, Somayeh Salimi**
*Boston University,**KTH Royal Institute of Technology

Abstract—We consider a Gaussian multiple access channel with \( K \) transmitters, a (intended) receiver and an external eavesdropper. The transmitters wish to reliably communicate with the receiver while concealing their messages from the eavesdropper. This scenario has been investigated in prior works using two different coding techniques; the random i.i.d. Gaussian coding and the signal alignment coding. Although, the latter offers promising results in a very high SNR regime, extending these results to the finite SNR regime is a challenging task. In this paper, we propose a new lattice alignment scheme based on the compute-and-forward framework which works at any finite SNR. We show that our achievable secure sum rate scales with \( \log(\text{SNR}) \) and hence, in most SNR regimes, our scheme outperforms the random coding scheme in which the secure sum rate does not grow with power. Furthermore, we show that our result matches the prior work in the high SNR regime.

The paper is organized as follows. In Section II, our setup preliminaries are described. Our main result is given in Section III along with the comparison to the prior works. In Section IV, the proof of the main result is presented. We conclude the paper in Section V. The proof of Lemma 1 used in Section IV is given in Appendix.

II. PROBLEM STATEMENT

A \( K \)-user (real) Gaussian wiretap multiple access channel (MAC) consists of \( K \) transmitters, a receiver and an external eavesdropper. The relations between the channel inputs and outputs are given as

\[
\begin{align*}
\mathbf{y} &= \sum_{\ell=1}^{K} h_{\ell} \mathbf{x}_{\ell} + \mathbf{z}, \quad \mathbf{y}_E = \sum_{\ell=1}^{K} g_{\ell} \mathbf{x}_{\ell} + \mathbf{z}_E
\end{align*}
\]

where \( \mathbf{x}_{\ell} \) is an \( N \)-length channel input vector of user \( \ell \) which satisfies the following power constraint.

\[
||\mathbf{x}_{\ell}||^2 \leq N P, \quad \forall \ell \in \{1, \ldots, K\}
\]

The vectors \( \mathbf{y} \) and \( \mathbf{y}_E \) in (1) are the receiver and the eavesdropper channel outputs, respectively. Also, \( \mathbf{z} \) and \( \mathbf{z}_E \) are the independent channel noises, each distributed i.i.d. according to \( \mathcal{N}(0, 1) \). Finally, vectors \( \mathbf{h} \triangleq [h_1, \ldots, h_K]^T \) and \( \mathbf{g} \triangleq [g_1, \ldots, g_K]^T \) are real-valued vectors representing the channel gains to the receiver and the eavesdropper, respectively. The channel model is illustrated in Fig. 1.

User \( \ell \) encodes its confidential message \( W_\ell \), which is uniformly distributed over the set \( \{1, \ldots, 2^{NR_\ell}\} \) and is independent of other users’ messages, through some stochastic mapping \( E_\ell, \) i.e., \( \mathbf{x}_{\ell} = E_\ell(W_\ell) \), for \( \ell \in \{1, \ldots, K\} \). There is also a decoder \( D \) at the receiver side which estimates the messages, i.e., \( D(\mathbf{y}) = \{W_\ell\}_{\ell=1}^K \).

Definition 1 (Achievable secure sum rate): For the described channel model, a secure sum rate \( \sum_{\ell=1}^{K} R_\ell \) is achievable, if for any \( \epsilon > 0 \) and large enough \( N \), there exist a sequence of encoders \( \{E_\ell\}_{\ell=1}^K \) and a decoder \( D \) such that

\[
\Pr\left( \bigcup_{\ell=1}^{K} \{W_\ell \neq W_E\} \right) < \epsilon
\]

\[
\sum_{\ell=1}^{K} R_\ell \leq \frac{1}{N} H(W_1, W_2, \ldots, W_K | \mathbf{y}_E) + \epsilon
\]

In light of lattice alignment technique, the compute-and-forward framework was proposed in [4] which can operate at any finite SNR. Recently, the \( K \)-user Gaussian MAC without security constraint has been investigated in [5] based on lattice coding and the compute-and-forward framework. The proposed scheme in [5] achieves the MAC sum capacity within a constant gap and for any finite SNR.

Motivated by the above arguments, we propose a new achievability scheme for the \( K \)-user Gaussian wiretap MAC in which lattice alignment is used along with the asymmetric compute-and-forward framework. We evaluate the performance of our proposed scheme both analytically and numerically for any finite SNR. We prove that our proposed scheme achieves a secure sum rate that scales with \( \log(\text{SNR}) \), in contrast to the Gaussian random coding result which does not grow with SNR and therefore, it somehow fails at moderate and high SNR regimes. Finally, we show that the asymptotic behavior of our proposed scheme agrees with the prior work result in [2] in the high SNR regime.
cancellation order in the compute-and-forward framework. Also, assume that the set of linearly independent integer-valued \( K \)-length vectors \( \{a_1, \ldots, a_K\} \) be the equations coefficients. Then, for the channel model in Section II the receiver can decode the message \( W_\ell \in \{1, \ldots, 2^{N R_\ell}\} \) with a vanishing error probability if
\[
R_\ell \leq R_{\text{comb}, \pi(\ell)} \triangleq \max_{I, h} \left\{ \frac{1}{2} \log \left( \frac{\text{SNR}_\ell}{\|F_{a_{\pi(\ell)}}\|^2} \right), 0 \right\}
\]
where the matrix \( F \) is given as
\[
F \triangleq \left( \frac{1}{P} I_{K \times K} + h h^T \right)^{-\frac{1}{2}} \times \text{diag} \left( \sqrt{\frac{\text{SNR}_1}{P}}, \ldots, \sqrt{\frac{\text{SNR}_K}{P}} \right).
\]

The direct diag(v) stands for the diagonal matrix built from the vector v and SNR \( > 0 \) is the power used at encoder \( \ell \) to generate its codewords. Notice that as long as the generated codewords are scaled properly before transmission, they would satisfy the channel input power constraint. Proposition 1 is immediately deduced from applying Theorem 2 along with Theorem 5 in [5] with an exception that, here, users operate at different powers. All other conditions stated in Theorem 5 in [5] still apply in Proposition 1.

In the following, we present a lower bound on the secure sum capacity achieved by the proposed scheme.

**Theorem 1:** A rate tuple \((R_1, \ldots, R_K)\) offers an achievable secure sum rate for the channel model described in Section II if they satisfy the following constraints:
\[
\sum_{\ell=1}^{K} R_\ell \leq \max_{\pi} R_{\text{sum}}
\]
where
\[
R_{\text{sum}} = \left( \sum_{k=2}^{K} R_{\text{comb}, k} - \frac{1}{2} \log \left( \frac{\sum_{k=1}^{K} g_k^2}{g_k^2 - 1} \right) \right)
\]

The maximum in (7) is taken over all the possible successive cancellation orders \( \pi \) and the notation \( \pi^{-1}(\cdot) \) simply denotes the inverse permutation operator.

Proof of Theorem 1 is given in Section IV.

**Comparison to the prior works**

The \( K \)-user Gaussian wiretap MAC has been investigated in [1] by means of i.i.d. Gaussian random coding. According to [1], for the considered channel model, the following secure sum rate is achievable
\[
\sum_{\ell=1}^{K} R_\ell \leq \max \left( \frac{1}{2} \log \left( \frac{1 + \|h\|^2 P}{1 + \|g\|^2 P} \right), 0 \right)
\]

Note that the right hand side of expression (9) does not scale with power \( P \) or in other words, the asymptotic behavior of (9) tends to a constant rate for a fixed number of users and a given set of channel gains. In contrast, our achievable secure sum rate in (8) scales logarithmic with \( P \). To prove this, we only need to show that the first term in (8) grows with \( \log(P) \) as the second term is constant with respect to

1Note that in Definition 1 we are interested in weak secrecy.

2The rates are determined by how closely the equations integer coefficients match the channel gains \( h_\ell \).

3The scaling factors can be absorbed into the the channel gains.
the secure sum rate in (8) grows with secure DoF of expression (8). We show that our scheme achieves a total achieves a strictly positive secure sum rate as long as the ratios fails to achieve a positive secure sum rate, while our scheme this case, according to the expression in (9), random coding exploit Theorem 12 in [5] in which it is shown that we exploit Theorem 12 in [5] in which it is shown that The numerical results are given in Fig. 2 which are evaluated in (10), we have R_{comb,k} ∝ \frac{1}{K} \log(P). As a result, the secure sum rate in (8) grows with \log(P).

The asymptotic behavior of the proposed scheme agrees with the result in [2]. In fact, we can further improve the presented scheme so that its asymptotic behavior reaches the optimal secure degrees of freedom given in [3]. The latter is aimed to be presented in the extended version.

IV. PROOF OF THEOREM 1

In this section, we use notions and properties related to the lattice coding and nested lattice structure which are discussed in detail in the seminal work by Erez and Zamir in [7]. Due to the space limitation, we avoid discussing the previously known results in this paper and we focus on the new results. Our proposed scheme provides security by confusing the eavesdropper through aligning the codewords at the eavesdropper side such that it can only decode the subsets of the codewords which have the same sum values in \mathbb{R}^N. To this end, each encoded codeword \hat{x} at transmitter \ell is scaled before the transmission by a factor of \frac{1}{\sqrt{\gamma}}, i.e., x_\ell = \frac{\hat{x}}{\sqrt{\gamma}}, so that the eavesdropper receives the sum of the codewords \hat{x} as its channel output, i.e., y_E = \sum_{\ell=1}^K \hat{x} + z_E. Consequently, user \ell generates its codewords \hat{x} using power of SNR_\ell \triangleq g_\ell^2 P so that the transmitted codewords x_\ell satisfy the power constraint in (2).

As it was mentioned earlier, to address the problem of users with different powers, we utilize the asymmetric compute-and-forward framework along with a nested lattice structure. In our asymmetric compute-and-forward framework, user \ell generates a sequence of n-length lattice codewords t_\ell using a pair of fine and coarse lattice sets as (\Lambda_f, \Lambda_c). The coarse lattice \Lambda_c is scaled such that its second moment equals to the available power at user \ell, i.e., SNR_\ell = g_\ell^2 P. Also, we impose a nested structure on the users’ lattice pairs as

\Lambda_K \subseteq \Lambda_{K-1} \subseteq \cdots \subseteq \Lambda_1 \subseteq \Lambda_{f,K} \subseteq \cdots \subseteq \Lambda_{f,1} \tag{13}

In the rest of the proof, we shall assume \pi(\ell) = \ell, \forall \ell in (8). If that is not the case, we can simply re-index the users indices
and define a nested structure as in (13) for the re-indexed users. User \( \ell \) constructs its codebook in three steps. The first step for user \( \ell \) is to construct its inner codebook \( \mathcal{L}_\ell \triangleq \Lambda_f,\ell \cap \mathcal{V}_\ell \), where \( \mathcal{V}_\ell \) is the fundamental Voronoi region of the coarse lattice \( \Lambda_c \). The ratio between the coarse and the fine lattices is such that \( \mathcal{L}_\ell \) consists of \( 2^nR_{\text{comb,}\ell} \) inner codewords \( \mathbf{t}_\ell \), i.e., \( R_{\text{comb,}\ell} = \frac{1}{n} \log |\Lambda_f,\ell \cap \mathcal{V}_\ell| \). The inner codewords \( \mathbf{t}_\ell \) have a uniform distribution over \( \mathcal{L}_\ell \).

In the second step, user \( \ell \) builds its outer codebook by generating \( B \) i.i.d. copies of the inner codewords \( \mathbf{t}_\ell \), for some large enough \( B \). Let us denote the outer codewords as \( \mathbf{\bar{t}}_\ell \). Then we have \( \mathbf{\bar{t}}_\ell \triangleq \{ \mathbf{t}^{[1]}_\ell, \ldots, \mathbf{t}^{[B]}_\ell \} \). Note that each \( \mathbf{t}^{[i]}_\ell \) is independently and uniformly distributed over \( \mathcal{L}_\ell \). It is worth to mention that the outer code is added only for technical reasons in the proof of Lemma 2 in [8] and it does not increase secrecy. Also, adding the outer layer to the codebook changes the block length of the overall codewords from \( n \) to \( N \triangleq B \times n \).

Finally, in the third step, the wiretap codebook is built. To this end, user \( \ell \) partitions the outer codewords \( \mathbf{\bar{t}}_\ell \) into \( 2^nR_c \) equal-size bins and randomly assigns each index \( w_{\ell} \in \{1, \ldots, 2^nR_c\} \) to exactly one bin. Rates \( R_c \) are chosen such that they satisfy (6) and \( \sum_{\ell=1}^{K_n} R_c = \sum_{\ell=2}^{K} R_{\text{comb,}\ell} - \frac{1}{n} \log (\sum g_i^2) + \epsilon_1 \), for some small \( \epsilon_1 > 0 \). Also, user \( \ell \) has a random dither \( \mathbf{d}^{[i]}_\ell \) for each block \( i \), which is independently generated according to a uniform distribution over \( \mathcal{V}_\ell \). Dithers are public and do not increase secrecy.

To send a message \( W_\ell = w_\ell \), user \( \ell \) randomly picks a codeword \( \mathbf{\bar{t}}_\ell \) from the corresponding bin and dithers it. Then, it scales the resulting codeword by the factor of \( \frac{1}{g_\ell} \). The signal transmitted by user \( \ell \) is

\[
\mathbf{x}_\ell \triangleq \frac{1}{g_\ell} \left( \left( \mathbf{\bar{t}}_\ell + \mathbf{d}_\ell \right) \bmod \Lambda_\ell \right)
\]

Note that in (14) the modular operation is done block-wise, meaning that for \( i \in \{1, \ldots, B\} \) the signal transmitted at block \( i \) is \( \frac{1}{g_\ell} (\mathbf{t}^{[i]}_\ell + \mathbf{d}^{[i]}_\ell) \bmod \Lambda_\ell \).

**Proof of secrecy**

In this subsection, we bound the eavesdropper’s equivocation rate. Without loss of generality, let us assume \( R_{\text{comb,}\ell} > 0 \), \( \forall \ell \). We have

\[
\frac{1}{N} H(W_1, \ldots, W_K | y_E, \bar{d}_1, \ldots, \bar{d}_K) \\
\geq \frac{1}{N} H(\mathbf{\bar{t}}_1, \ldots, \mathbf{\bar{t}}_K | y_E, \bar{d}_1, \ldots, \bar{d}_K) \\
- \frac{1}{N} H(\mathbf{\bar{t}}_1, \ldots, \mathbf{\bar{t}}_K | W_1, \ldots, W_K, y_E, d_1, \ldots, d_K) \\
\overset{(a)}{\geq} \frac{1}{N} H(\mathbf{\bar{t}}_1, \ldots, \mathbf{\bar{t}}_K | y_E, d_1, \ldots, d_K) - 2\epsilon_2 \\
\overset{(b)}{\geq} \frac{1}{N} H(\mathbf{\bar{t}}_1, \ldots, \mathbf{\bar{t}}_K | \sum_{\ell=1}^{K_n} g_\ell x_\ell, d_1, \ldots, d_K) - 2\epsilon_2 \\
\overset{(c)}{=} \frac{1}{N} \left( \frac{1}{N} H(\mathbf{\bar{t}}_1, \ldots, \mathbf{\bar{t}}_K | \sum_{\ell=1}^{K_n} g_\ell x_\ell, d_1, \ldots, d_K) \right) - 2\epsilon_2
\]

5As the average leakage rate (w.r.t. dithers) goes to zero, there must exist a sequence of deterministic dithers for which the leakage rate goes to zero.

In the above inequalities, (a) is deduced from applying the packing lemma to the outer codewords (detailed proof of this step is provided in Appendix of [8]). (b) is true since after subtracting the noise from \( y_E \), the remaining random vectors become independent of the noise. (c) is true since \( \Lambda_1 \) is the densest lattice among the lattices \( (\Lambda_1, \Lambda_2, \ldots, \Lambda_K) \), according to the nested structure in (13). Therefore,

\[
\sum_{\ell=1}^{K_n} g_\ell x_\ell \quad \bmod \quad \Lambda_1 = \sum_{\ell=1}^{K_n} \mathbf{t}_\ell \quad \bmod \quad \Lambda_1.
\]

Also, notice that

\[
H(\sum_{\ell=1}^{K} g_\ell x_\ell) = H(\sum_{\ell=1}^{K} g_\ell x_\ell + \mathbf{t}_1)\bigg|_{\mathbf{u}_1 = \sum_{\ell=1}^{K} g_\ell x_\ell + \sum_{\ell=2}^{K} \mathbf{t}_\ell} \\
\]

In this paper, we proposed a security scheme built on the asymmetric compute-and-forward framework, which works at
any finite SNR. The achievable secure sum rate presented in
our scheme scales with log(SNR) and therefore, it signifi-
cantly outperforms the existing random coding result for the
most SNR regimes. Our presented scheme also achieves a total
secure DoF of $K - 1$. This result can be furthered improved to
achieve the optimal secure DoF which is aimed to be presented
in our future work.

ACKNOWLEDGMENT

The authors would like to thank Bobak Nazer and Prakash
Ishwar for their valuable comments and helpful discussions.

REFERENCES

[1] E. Tekin and A. Yener, “The general gaussian multiple-access and two-
way wiretap channels: Achievable rates and cooperative jamming,” IEEE
Transactions on Information Theory, vol. 54, no. 6, pp. 2735–2751, 2008.
[2] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, “On the se-
cure degrees-of-freedom of the multiple-access-channel,” available online
http://arxiv.org/abs/1003.0729.
[3] J. Xie and S. Ulukus, “Secure degrees of freedom of one-hop wireless
networks,” Submitted September 2012, available online http://arxiv.org/abs/1209.5370.
[4] B. Nazer and M. Gastpar, “Compute-and-forward: Harnessing inter-
ference through structured codes,” IEEE Transactions on Information
Theory, vol. 57, no. 10, pp. 6463–6486, 2011.
[5] O. Endrelish, U. Erez, and B. Nazer, “The approximate sum ca-
pacity of the symmetric gaussian k-user interference channel,” IEEE
Transactions on Information Theory, To appear 2014, available online
http://arxiv.org/abs/1206.0197.
[6] V. Ntranos, V. R. Cadambe, B. Nazer, and G. Caire, “Asymmetric compute-and-forward,” in 51st Allerton Annual Conference on Commu-
nications, Control, and Computing, Monticello, IL, September 2013.
[7] U. Erez and R. Zamir, “Achieving $\frac{1}{2} \log(1 + \text{SNR})$ on the AWGN
channel with lattice encoding and decoding,” IEEE Transactions on
Information Theory, vol. 50, no. 10, pp. 2293–2314, 2004.
[8] P. Babaeiheidian and S. Salimi, “Compute-and-forward can buy secrecy cheap (extended version),” preprint available at
http://blogs.bu.edu/parsa/bh/files/2015/01/Extendedversion.pdf, 2015.
[9] G. D. Forney, “On the role of mmse estimation in approaching the
information-theoretic limits of linear gaussian channels: Shannon meets
wigner,” in 41st Annual Allerton Conference on Communications, Con-
trol, and Computing, Monticello, IL, September 2003.

APPENDIX

Lemma 1: Consider a set of $n$-dimensional lattices
$\Lambda_1, \ldots, \Lambda_K$ with their fundamental Voronoi regions as
$\mathcal{V}_1, \ldots, \mathcal{V}_K$. Assume that all the lattices are
scaled such that their second moments equal to $\text{SNR}_\ell =
g_{2}^{2} P, \forall \ell \in \{1, \ldots, K\}$, where $P > 0$. Now construct random
vectors $u_j$, for $j \in \{1, \ldots, K\}$, as $u_j \triangleq Q_{\Lambda_j} \left( \sum_{\ell=1}^{K} s_{\ell} \right)$,
where $s_{1}, \ldots, s_{K}$ are independent $n$-dimensional random vec-
tors uniformly distributed over $\mathcal{V}_1, \ldots, \mathcal{V}_K$, respectively, and the operation $Q_{\Lambda_j}()$ is the nearest neighbor quantizer
with respect to the lattice $\Lambda_j$. Then, for all $\epsilon > 0$ and sufficiently
large $n$, the entropy of $u_j$ is bounded as
\begin{equation}
\frac{1}{n} H(u_j) \leq (1 - \epsilon) \frac{1}{2} \log \left( \sum_{\ell=1}^{K} g_{2}^{2} \right) + \delta(\epsilon) \qquad \forall j
\end{equation}
where $\delta(\epsilon)$ tends to zero as $\epsilon \to 0$.

Proof: According to Lemma 1, $u_j$ is the output of the lattice
quantizer $Q_{\Lambda_j}$, so it can only take discrete values. To bound
the entropy of $u_j$, first we bound the range of $\sum_{\ell=1}^{K} s_{\ell}$ as
follows. Let $r_{\text{cov},\ell}$ denote the covering radius of $\Lambda_\ell$, i.e., the
radius of the smallest ball containing the Voronoi region $\mathcal{V}_\ell$.

Also, let $r_{\text{eff},\ell}$ denote the radius of the sphere which has
the same volume as the volume of $\mathcal{V}_\ell$, i.e., $\text{Vol}(B(r_{\text{eff},\ell})) =\text{Vol}(\mathcal{V}_\ell)$. Now, consider $K$ $(n$-dimensional) balls whose sec-
ond moments per dimension equal to $\sigma_1^2, \sigma_2^2, \ldots, \sigma_K^2$ and their
radii are given as $r_{\text{cov},1}, r_{\text{cov},2}, \ldots, r_{\text{cov},K}$, respectively. Next, for each $\ell \in \{1, \ldots, K\}$, consider a random vector $b_\ell$
with the uniform distribution over an $n$-dimensional ball $B(r_{\text{eff},\ell})$.
Recall that a ball has the smallest normalized second moment
for a given volume $[7]$. Therefore, we have
\begin{equation}
g_{2}^{2} P \geq \sum_{\ell=1}^{K} \frac{1}{n} E\left[\left(\frac{r_{\text{eff},\ell}}{r_{\text{cov},\ell}}\right)^{2} b_\ell^{2}\right] \geq \sum_{\ell=1}^{K} \left(\frac{r_{\text{eff},\ell}}{r_{\text{cov},\ell}}\right)^{2} \sigma_\ell^{2}, \forall \ell
\end{equation}
Now, consider a random vector $z_{eq} \triangleq \sum_{\ell=1}^{K} z_\ell$, in which
random vectors $z_\ell$ are i.i.d. according to the distribution
$\mathcal{N}(0, \sigma_\ell^{2} I)$ and therefore, $z_{eq} \sim \mathcal{N}(0, \sigma_{eq}^{2} I)$. Then, from
[17] we have $\sigma_{eq}^{2} = \sum_{\ell=1}^{K} \sigma_\ell^{2} \leq \sum_{\ell=1}^{K} \left(\frac{r_{\text{cov},\ell}}{r_{\text{eff},\ell}}\right)^{2} g_{2}^{2} P$.
Now, using Lemma 11 in [7], we conclude that
\begin{equation}
e^{K,n,c(n)} f_{s_{eq}}(z_{eq}) = e^{K,n,c(n)} (f_{s_{1}}(z_{eq})) * ... * f_{s_{K}}(z_{eq})
\end{equation}
where $n,c(n)$ goes to zero as $n$ goes to infinity. Notice that in deriving [18] we also used the fact that vectors $s_{\ell}$ are independent vectors, and hence, pdf of their sum is the convolution of their individual pdfs. Now we can bound the range of $\sum_{\ell=1}^{K} s_{\ell}$ as follows. For any $\epsilon > 0$,
\begin{equation}
\left(\frac{\sum_{\ell=1}^{K} s_{\ell}}{\sqrt{n} \sigma_{eq}^{2} + n \epsilon}\right)
\end{equation}
where inequality (a) follows from [18] and non-negativity of the $\ell_2$-
norm. Also, the last inequality is deduced from the Weak Law of
Large numbers (WLL) for sufficiently large $n$. Since we showed that $\|\sum_{\ell=1}^{K} s_{\ell}\|$ belongs to the ball $B(\sqrt{n} \sigma_{eq}^{2} + n \epsilon)$ with probability $1 - \epsilon$, it only remains to find an upper bound
on the number of non-intersecting Voronoi regions $\mathcal{V}_j$ which
fit in this ball, i.e.,
\begin{equation}
\frac{\text{Vol}(B(\sqrt{n} \sigma_{eq}^{2} + n \epsilon))}{\text{Vol}(\mathcal{V}_j)} = \frac{\text{Vol}(B(r_{\text{eff},j}))}{\text{Vol}(B(r_{\text{eff},j}))}\n\end{equation}
where inequality (a) is concluded from Lemma 6 in [7] and
inequality (b) follows from [17]. Finally, recall that for a high
dimensional good lattices, we have $\log \left(\frac{r_{\text{eff},n}}{r_{\text{eff},1}}\right) \to 0$ [7].
Therefore,
\begin{equation}
\frac{1}{n} H(u_j) \leq (1 - \epsilon) \frac{1}{2} \log \left( \sum_{\ell=1}^{K} g_{2}^{2} \right) + \delta(\epsilon).
\end{equation}
Note that using WLL, the term $\delta(\epsilon)$ tends zero as $n$ goes to
infinity. This completes the proof.

\}