AES and Mixed AES/Gold Spreading Sequences for Satellite Uplink Code Division Multiplexing

AES and Mixed AES/Gold Spreading Sequences for Satellite Uplink Code Division Multiplexing

Roberto Garello, *Senior Member, IEEE,* Monica Visintin, Riccardo Schiavone, Alessandro Compagnoni, and Carla Fabiana Chiasserini, *Fellow, IEEE*

***Abstract*—In this paper we study spreading sequences for Code Division Multiplexing (CDM) generated from the AES algorithm in counter mode. These sequences are robust against jamming because they cannot be reconstructed from one of their segments. Additionally, they are flexible, have a large cardinality, and can be obtained from a small key. We show how their linear complexity profile, error probability, and acquisition performance are aligned with those of random sequences. To further enhance them, we introduce a new family of mixed AES/Gold sequences. First, we demonstrate how we can generate cosets of extended Gold sequences which are perfectly orthogonal for CDM. Then, we combine AES sequences and Gold cosets: the new sequences have better performance in terms of error probability and acquisition, while maintaining protection against jamming. All results are derived analytically and validated through simulation. As a case study, we consider an uplink scenario from a ground station to a constellation of Low Earth Orbit satellites. The proposed mixed sequences allow for a significant increase in the number of satellites that can be served in parallel, while maintaining the same level of performance and protection against jamming.**

***Index Terms*—Code Division Multiplexing, Spreading Sequences, AES sequences, Gold sequences, Satellite Communications.**

I. Introduction

DIRECT sequence spread spectrum (DSSS) modulation ([1], [2], [3]) is an effective solution for a myriad of applications. where it offers numerous advantages, including innate ability to serve multiple users in parallel and resistance to interference and jamming. Many spreading sequences have been introduced for DSSS and CDM (Code Division Multiplexing)/CDMA (Code Division Multiple Access) applications. (In this paper we use the term CDM to denote the communication link from a single transmitter to many users, while the term CDMA is used for the transmission on the other direction.) Among these sequences there are algebraic sequences like m-sequences [4] and their truncated versions [5], Gold sequences [6], Kasami sequences [7] and many others, such as [8], [9], [10], [11], [12], [13]. Some examples from recent works include [14], [15], [16], [17]. Typically, these sequences have very good properties in terms of correlation, which makes their performance closely approach theoretical limits such as Welch bound [18] and Sidelnikov bound [19].

For many applications, robustness to jamming is of key importance ([20], [21], [22], [23], [24]). Even if CDM and CDMA offer a natural protection against jamming, they are vulnerable to attacks that exploit the user's spreading code. If an attacker manages to recover it, it can start transmitting a dummy signal encoded with this code and disrupt the normal operation of the system by a denial of service attack. As in several systems it is feasible to recover segments of the spreading sequence from intercepted portions of the transmitted signal, it is crucial to ensure that reconstructing the entire sequence from a segment is nearly impossible. Unfortunately, this is typically not the case for many algebraic sequences, where an attacker can reconstruct the entire sequence by retrieving only a small signal portion, using algorithms such as Berlekamp/Massey ([25], [26]). From that point onwards, it is able to perform a disruptive jamming attack.

In this paper, we address the above issue by focusing on spreading sequences generated from the AES algorithm [27] operating in counter mode, where both the secret key and an increasing counter are used as input to generate blocks of spreading chips ([28], [29]). [1] These sequences are robust against jamming and have a number of properties that are very useful for several relevant applications, like the LEO use case discussed below.

A. The LEO Use Case and its Requirements

Although the sequences studied in this paper can be applied to any terrestrial or space system, we focus on the case study

[1]We remark here that in this paper the AES algorithm is not considered for encrypting the information messages, but for generating spreading codes which are applied to CDM at the physical layer, against jamming.

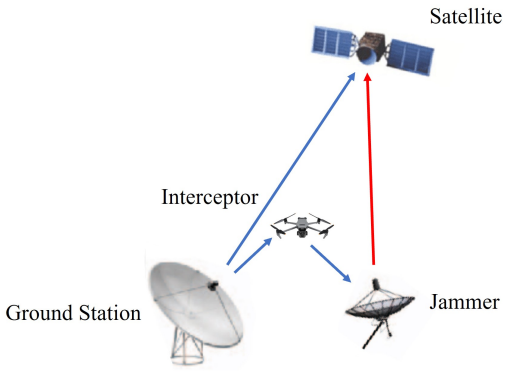

Fig. 1. Jamming attack: a flying object intercepts a portion of the sequence, the attacker rebuilds the entire one and carries out a denial of service attack.

R. Garello, M. Visintin, R. Schiavone, A. Compagnoni, and C. F. Chiasserini are with the Department of Electronic and Communications, Politecnico di Torino, Torino, 10129 Italy, e-mail: (name.surname@polito.it).

of a satellite telecommand uplink, from a ground station to a constellation of LEO satellites.

Currently, there is considerable interest in LEO satellite constellations, driven by a diverse range of applications. These include, for example, non-terrestrial networks [30], mega-constellations for broadband internet [31] and direct-to-satellite Internet of Things (IoT) services [32]. This growing interest is also coupled with a focus on innovative techniques to meet the evolving demands of these advanced communication systems [33], [34], [35]. For LEO constellations, Telecommand uplink operations managed by ground stations are crucial for the effective operation and maintenance of the satellite network [36]. The ability to remotely control and monitor the satellites from Earth is essential to ensure the constellation's performance and stability. Ground stations must constantly communicate with the satellites to manage their orbits, monitor their health, make real-time adjustments, avoid collisions, update sensor operations, and correct any drift.

CDM is one of the most widely used techniques for LEO satellite uplink. Its popularity stems from the ability to serve multiple satellites simultaneously within the same frequency band by using spreading sequences with good cross-correlation properties. These properties help minimize interference among signals directed to different satellites, ensuring reliable communication and control.

Modern LEO constellations have typically a large size, as several hundreds or even thousands of satellites are needed to provide global or country coverage. Moreover, the visibility window is very limited (as an example, for very low orbits it can be of few minutes). It follows that the ground station must serve many satellites, visible for a limited time, and continuously changing. This imposes the following requirements, which have a relevant impact on the spreading sequences.

Robustness against jamming: as shown in Fig. 1 it is relatevely easy (from another spacecraft or a flying vehicle) to intercept portions of the transmitted signal. Then, it must be very difficult to recover the entire sequence from one of its segments, otherwise the Jammer can perform its attack. First of all, the sequence must be very long, much longer than the spreading factor (if its length is equal to the spreading factor, we observe a bit and we have the sequence or its inverse). Second, it must have a Linear Complexity Profile (LCP) similar to that of a random sequence. The LCP is the length of the shortest Linear Feedback Shift Register (LFSR) that can generate the sequence [37]. The LCP of an ideal random sequence of length n is $n/2$: it increases linearly with the length. As we will show in this paper, AES sequences have both these two properties, differently from algebraic sequences.

Flexible Bit-rate: the system must be able to change the bit rate in real time, hence to modify the spreading factor accordingly. Algebraic sequences are typically forced to have a length equal to the spreading factor (which is often of type 2^m-1), otherwise they lose most of their correlation properties [5]. Instead, AES sequences can realize any spreading factor and sequence length.

Uncoordinate multiple access: The association satellites/sequences is of key importance for this uplink system. The ideal solution would be to assign to each satellite a set of sequences that remain unchanged for its entire operational life. However, if the number of sequences is limited (as for many algebraic sequences), this is not possible. In this case, it is necessary to reassign the sequence each time the satellite becomes visible. Conversely, if the number of sequences is large, it is possible to assign them permanently to the satellite without having to renegotiate each time it becomes visible. Then it is important to have a class of sequences with a huge cardinality. As we will see in the next section, AES sequences possess this property. This eliminates the necessity of continuous registration and coordination of the sequences and allows for uncoordinated multiple access operation, a big advantage for satellite operations, especially for modern age LEO constellations of thousands of satellites.

Algorithmic construction: In space, memories are subject to interference from cosmic rays, so it is preferable that sequences do not need to be stored entirely but can be reconstructed from a short vector. Both AES and most algebraic sequences have this property.

To summarize, the additional requirements imposed on the sequences by the LEO use case are:

1) sequence length much longer than the spreading factor,
2) difficulty of reconstructing the sequence from one of its segments,
3) flexible spreading factor and length,
4) large cardinality,
5) construction from a short vector of bits.

B. Paper contribution

Our main contributions are as follows:

- *AES spreading sequences*: We study the performance of AES sequences generated in counter mode in terms of: *(i)* cross-correlation, *(ii)* linear complexity profile, *(iii)* error probability, *(iv)* acquisition. First, we provide an analytical characterization of the properties of random sequences, and then we show that AES sequences exhibit behavior that closely aligns with those properties. Thus, they are able to guarantee the same performance as binary random sequences in terms of error probability and acquisition, while being robust against jamming.
- *Orthogonal cosets of extended Gold codes*: We introduce such codes and demonstrate their perfect orthogonality for CDM.
- *Mixed AES/Gold sequences:* We show how we can mix AES and cosets of extended Gold sequences to obtain a new family of spreading sequences. Then, we present a complete analytic and simulation study of the newly proposed mixed sequences. Remarkably, they retain all the good anti-jamming properties of AES sequences, but with better error probability and acquisition performance.
- *LEO Use Case:* The new mixed codes are very good candidates for the LEO uplink scenario due to their numerous advantages: they are long, flexible, numerous, can be generated from a small key, support any spreading factor, outperform random sequences, and offer strong robustness against jamming. Through both analytical and

simulation-based evaluations, we demonstrate their substantial gains in terms of Signal-to-Noise Ratio (SNR) and the number of satellites that can be served simultaneously. In some cases, these codes can even double the number of supported satellites.

C. Paper organization

The paper is organized as follows. Section II describes the generation of AES sequences in counter mode, their randomness properties, and their linear complexity profile. Therein, we also provide an analytical characterization of the performance of random sequences in terms of error probability and acquisition. We then compare these results to those of AES sequences, demonstrating an excellent match between the two. The orthogonality properties of extended Gold sequences for CDM are demonstrated in Section III. In Section IV, we propose the novel family of mixed AES/Gold sequences and their coset-based construction. The performance of mixed sequences in terms of error probability and acquisition is studied in Section V, where we derive analytical expressions, validate them through simulations, and highlight the gain achieved compared to random sequences. We examine both AWGN and LMS channels, considering transmission scenarios with and without coding. Finally, Section VI summarizes the presented results and draws our conclusions.

II. AES SPREADING SEQUENCES

In this section, we first describe how to generate spreading sequences by using the AES algorithm in counter mode, then we discuss their randomness properties and their performance.

The Advanced Encryption Standard (AES) has been designated by the National Institute of Standards and Technology (NIST) as the standard for private key encryption [27]. It is a block cipher admitting a block length of 128 bits, and three possible key lengths: 128, 192, and 256 bits. In our studies, we have verified that the properties of AES sequences for CDM applications are independent of the key length. Therefore, in the following, we will focus on keys of length 128 bits. AES operates on blocks of data, transforming them through a series of substitution, permutation, and mixing operations. A detailed description of AES and its different modes can be found, for example, in [38].

The idea of using the AES algorithm in counter mode as a pseudo-random sequence generator ([28], [29]) is described in Fig. 2. There is no plaintext to encrypt. The secret key is fixed. The counter is set to an initial value and, together with the key, is input to the AES algorithm to generate a first block of 128 pseudo-random bits. The counter is increased (by one, or according to a chosen rule) and the AES algorithm is used to generate another 128-bit block, which is appended to the previous one. The procedure is repeated until a multiple of 128 greater than the expected sequence length is reached. The excess bits are discarded, and the AES spreading sequence is obtained. This way, the sequences are very flexible: we can realize any sequence length L and implement any spreading factor $M < L$. Moreover, 2^{128} different blocks can be generated, so the cardinality is huge.

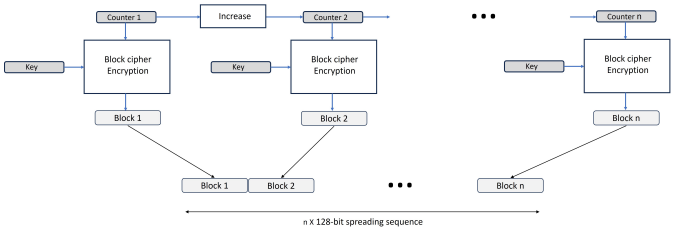

Fig. 2. Generation of AES spreading sequences in counter mode.

A. Parameter setting

In this section, we discuss the selection of the numerical values used in our examples, which are applied in the analysis of the LEO use case presented in the following. The LEO constellations that we consider in this paper have a size ranging from a few tens to a few hundreds to a few thousand satellites (we do not consider mega-constellations of several thousands of satellites, like Starlink.) From a study we conducted for the European Space Agency (ESA), given a LEO constellation of about 6000 satellites, we quantified a maximum number of 55 satellites that were visible at the same time from a given ground station location. Instead, the mean value is quite small, a few units. This is the reason why we considered values between 3 and 50 for N_U, the number of satellites served simultaneously at a given moment, in our examples. The telecommand bit rate for LEO satellites is usually between 1 kbps and 128 kbps, depending on the number of satellites to be served. If we adopt a CDM approach, we can use the entire available band, and we have some tens of MHz to share among the satellites. Corresponding values of the spreading factor M may vary from some tens to some thousands. In our examples we focused on the two values equal to $M = 127$ and $M = 1000$, but the results have general validity and can be extended to any other value. For the sequence length, for jamming protection, we typically assume it is at least two orders of magnitude bigger than the spreading factor (this makes unfeasible the reconstruction of the sequence even if the attacker is able to intercept the whole sequence length, because it is modulated by at least 100 bits).

B. Randomness

In this section, we analyze the randomness of AES sequences. First of all, the cross-correlation between two randomly-extracted AES sequences is close to the binomial distribution of a true random sequence, as shown by the comparison of the two cumulative distribution functions in Fig. 3.

Second, we consider the Linear Complexity Profile (LCP), which provides a measure of how "random" the sequence appears. For a given binary sequence $s_1, s_2, s_3, ...$, the linear complexity $\gamma(n)$ is the length of the shortest Linear Feedback Shift Register (LFSR) that can generate the sequence from s_1 to s_n. The linear complexity can be calculated using algorithms such as the Berlekamp-Massey algorithm. A random binary sequence has an LCP that grows linearly as $n/2$ [37].

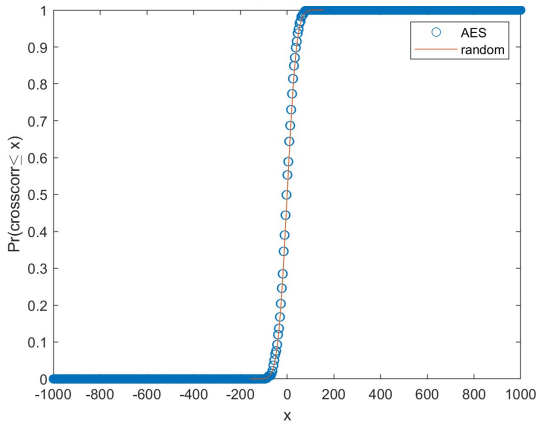

Fig. 3. Cumulative distribution function of the cross-correlation between two randomly extracted AES sequences of length $L = 1000$, comparison with ideal random behaviour.

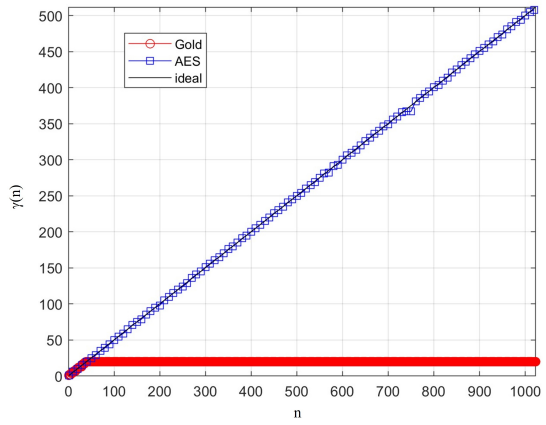

Fig. 4. Linear Complexity Profile: AES spreading sequence, Gold sequence and ideal random behaviour.

It is important that this complexity is maintained consistently as the sequence progresses. Sharp drops in the complexity profile indicate weaknesses and potential vulnerabilities. In fact, an attacker who intercepts a segment of the sequence can apply the linear recurrence to reconstruct the entire sequence. The LCP of an AES sequence and a Gold sequence of length $L = 1023$ are shown in Fig. 4. It is clearly evident that, while the linear complexity of the Gold sequence caps at 20, which is twice the length of the shift registers generating it, the linear complexity of the AES sequence continues to increase linearly. This serves as a measure of the randomness of these sequences and their robustness against jamming.

C. Error Probability Performance

In this section, we compare the error probability of AES sequences over an additive white Gaussian channel against that of random sequences for the considered uplink scenario. We have a transmitter that serves N_U users with a CDM system, with the spreading sequences aligned at the transmitter and received with the same alignment at each user (the term synchronous CDMA is also used to denote this system). We focus on a base-band 2-PAM constellation with rectangular waveform. The transmitted signal is equal to:

$$s_T(t) = \sum_{i=0}^{N_U-1} \sum_n \alpha_i b_i'(n) P_{T_b}(t-nT_b) \sum_m c_i'(m) P_{T_c}(t-mT_c) \tag{1}$$

where:

- α_i is the signal level that determines the power transmitted to user i, equal to $P_i = \alpha_i^2$. (Hereafter, we will assume $\alpha_i = \alpha$, equal for all the users.)
- $b_i'(n)$ is the n-th bipolar (+1/-1)[2] information symbol transmitted to user i,
- $P_T(t)$ is the rectangular pulse with unit amplitude for $0 \le t < T$ and zero elsewhere,
- T_b is the bit time,
- $c_i'(m)$ is the m-th bipolar symbol corresponding to the binary spreading sequence chip $c_i(m)$ assigned to user i,
- T_c is the chip time, with $T_c = T_b/M$ (M the spreading factor),

The following lemma provides the analytic expression of the error probability of random sequences.

Corollary 1. *[Error probability of random sequences] Given a CDM system with a transmitter serving N_U users with the same power, to each user is assigned a random binary sequence with spreading factor M. The bit error probability for a generic user indexed by i is given by:*

$$P(e) = \frac{1}{2}\mathrm{erfc}\sqrt{\frac{\left(\frac{E_b}{N_o}\right)_i}{1 + 2\frac{(N_U-1)}{M}\left(\frac{E_b}{N_o}\right)_i}} \tag{2}$$

where E_b/N_0 is the signal to noise ratio for the i-th receiver.

This corollary follows as a particular case from Theorem 2 in Section V.

Now that we have established the ideal performance of random spreading sequences, it is interesting to compare it to that of some spreading sequences. In Fig. 5 and Fig. 6, we present the performance for spreading factors $M = 127$ and $M = 1000$; notably, the plots show:

- The 2-PAM ideal curve, which is the error rate lower bound because it corresponds to perfectly orthogonal sequences assigned to all users.
- The analytical curve of Eq. (2) for random sequences.
- The simulated curve for random sequences.
- The simulated curve for AES sequences.
- The simulated curves for two Gold sequences, one with a spreading factor M equal or almost equal to the sequence length L and the other with $M \ll L$.

Note that, in the paper, we refer to baseband signals and therefore use 2-PAM as a reference; however, all results are equivalent for 2-PSK and 4-PSK constellations, which are used to transmit CDM signals to satellites.

Looking at the results, we can observe a perfect match between AES simulations and random analytical curves. This

[2]We use the following notation: if $a \in \{0,1\}$ is a chip/bit, then $a' \in \{-1,1\}$ is the corresponding bipolar symbol.

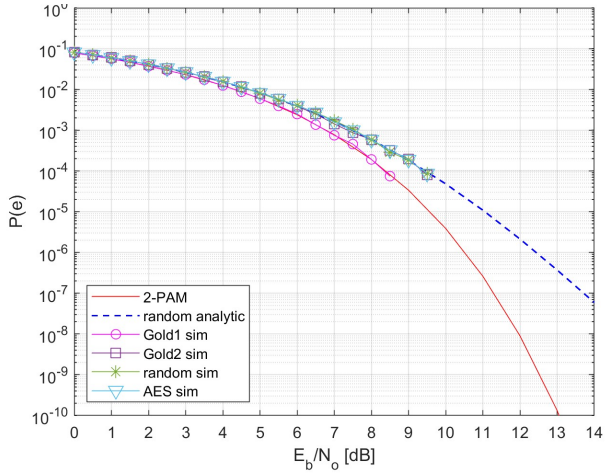

Fig. 5. CDM bit error probability for $M = 127$ and $N_U = 3$ users. Comparison among 2PAM lower bound, ideal random sequence analytic curve, ideal random sequence simulation, AES sequence simulation, Gold sequence 1 with $L = M = 127$, Gold sequence 2 with $L = 1023$.

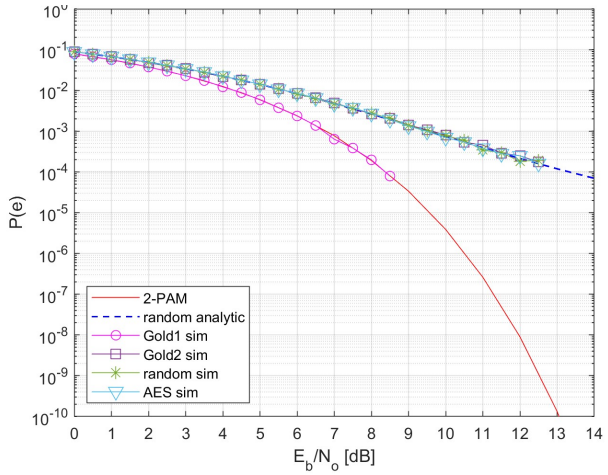

Fig. 6. CDM bit error probability for $M = 1000$ and $N_U = 50$. Comparison among 2PAM lower bound, ideal random sequence analytic curve, ideal random sequence simulation, AES sequence simulation, Gold sequence 1 with $L = 1023$, Gold sequence 2 with $L = 2047$.

alignment of the error probability curves is a strong indicator of randomness, as it demonstrates that AES sequences exhibit statistical properties identical to those of truly random sequences, ensuring performance that is consistent with that expected from the random behavior under theoretical conditions. This further confirms the randomness of AES sequences, along with the cross-correlation behavior in Fig. 3 and the linear complexity profile in Fig. 4.

As for Gold sequences, the results show that their performance is excellent when the spreading factor is close to the entire code length. When instead the spreading factor is much less than the sequence length (anti-jamming requirement 1 of the previous section), the Gold sequences perform as the random and AES sequences.

D. Acquisition

In this section, we analyze the acquisition phase, that involves aligning the spreading sequence between the transmitter and the receiver at the beginning of the visibility window. As explained in Section I, in LEO scenarios where jamming protection is fundamental, the spreading sequences are much longer than the spreading factor. Moreover, the ground station transmitter and the LEO receivers are connected only sporadically. When they are not connected they maintain a rough alignment, but it must be precisely acquired at the beginning of the visibility window. For this purpose, at the start of the window, the transmitter sends a sequence segment without modulating data (i.e. $b'_i(n) = 1$ in Eq. 1), to which the user synchronizes.

On board, a vector $\underline{r}$ of N received samples $r(m)$ is correlated to N chips of the local replica. The result is checked against a threshold τ, which, when exceeded, triggers the declaration of a successful lock. To speed up the process, we can compare the vector $\underline{r}$ against S blocks of N symbols at the same time. Given the received signal $r(t)$ we consider a block of N received samples

$$\underline{r} = (r(0), ..., r(m), ..., r(N-1)), \tag{3}$$

obtained by projecting $r(t)$ over the normalized rectangular pulse of duration T_c:

$$r(m) = \frac{1}{\alpha T_c}\int_{mT_c}^{(m+1)T_c} r(t)dt = \frac{1}{\sqrt{E_c}}\frac{1}{\sqrt{T_c}}\int_{mT_c}^{(m+1)T_c} r(t)dt. \tag{4}$$

Note that samples are generated at rate $R_c = 1/T_c$.

The user compares $\underline{r}$ against $S = P+1$ blocks of N symbols of the local replica of the bipolar spreading sequence $\underline{c}'_i$. If the local code is

$$\underline{c}'_i = (c'_i(0), c'_i(1), \ldots, c'_i(i), \ldots)$$

we consider S consecutive segments position k of the local code and is made of N chips:

$$\underline{s}'_i(k) = (c'_i(k), \ldots, c'_i(k+N-1)). \tag{5}$$

For each segment we compute the inner product with the received samples

$$\Gamma(k) = (\underline{r}, \underline{s}'_i(k)) = \sum_{m=0}^{N-1} r(m)c'_i(k+m). \tag{6}$$

The synchronizer

- computes the S inner products $\Gamma(k)$, with $0 \le k \le S-1$
- identifies the index $k_{\max}$ where $\Gamma(k)$ is maximum
- compares $\Gamma(k_{\max})$ against a threshold value τ.

If $\Gamma(k_{\max}) \ge \tau$, the value $k_{\max}$ is declared as the correct local code phase, otherwise it continues with the next S segments of the local code.

To compare the received signal against $S = P + 1$ blocks of the local replica in parallel, a commonly used approach is the $K = N + P$-symbol FFT-based scheme described in Fig. 7. Note that, since the FFT is the correct tool for periodic signals, it is necessary to use zero padding: N input samples are padded with P zeros, so that the FFT correctly measures $(P + 1)$ values of the inner product between the incoming signal and the local replica.

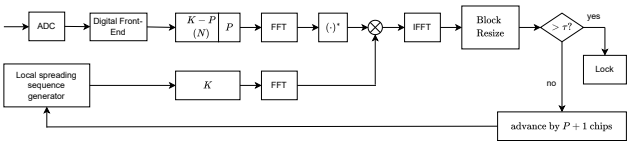

Fig. 7. Spreading code acquisition subsystem based on FFT, assuming one sample per chip.

Now, we calculate the probability of missed detection and wrong lock for random sequences and we compare them against those of AES sequences.

1) Missed detection: First we compute the missed detection probability. Suppose that $\underline{r}$ is aligned with the segment $\underline{s}'_i(0)$ starting from $c'_i(0)$ and N is an integer multiple of the spreading factor $N = kM$. We compute the inner product with $\underline{s}'_i(0)$. The missed detection $P_{md}(\tau) = Pr\left(\Gamma(0) < \tau\right)$ is established by the following result.

Corollary 2 (Missed-detection probability for a random sequence)**.** *Given a CDM system with N_U users and spreading factor M using random sequences, we perform acquisition on $N = kM$ symbols. The missed detection probability is given by*

$$P_{md}(\tau) = \frac{1}{2}\text{erfc}\frac{N-\tau}{\sqrt{2N\left(\sigma^2 + N_U - 1\right)}} \tag{7}$$

where E_c is the chip energy and

$$\sigma^2 = \frac{1}{2\frac{E_c}{N_o}} = \frac{1}{\frac{2}{M}\frac{E_b}{N_o}} \tag{8}$$

This result follows as a particular case from Theorem 3 in Section V.

2) Wrong lock: Now we compute the wrong lock probability, i.e., the probability that the inner product is above threshold for a segment different from the correct one. Suppose as before that $\underline{r}$ is aligned with the segment $\underline{s}'_i(0)$ starting from $c'_i(0)$. We want to compute the probability that the inner product between $\underline{r}$ and a segment $\underline{s}'_i(\ell)$ different from $\underline{s}'_i(0)$ is above the threshold. Then we must compute the wrong lock probability as $P_{wl}(\tau) = Pr\left(\Gamma(\ell) > \tau\right)$. We have the following result.

Corollary 3 (Wrong lock probability for a random sequence)**.** *Given a CDM system with N_U users and spreading factor M, using random sequences, we perform acquisition on $N = kM$ symbols. The wrong lock probability is given by*

$$P_{wl}\left(\tau\right) = \frac{1}{2}\text{erfc}\frac{\tau}{\sqrt{2N\left(N_U + \sigma^2\right)}}, \tag{9}$$

where E_c is the chip energy and

$$\sigma^2 = \frac{1}{2\frac{E_c}{N_o}} = \frac{1}{\frac{2}{M}\frac{E_b}{N_o}} \tag{10}$$

This result follows from a particular case of Theorem 4 in Section V.

As an example, the missed detection and wrong lock probabilities for random sequences are reported in Fig. 8 for N=128 received symbols. The corresponding Receiver Operating Characteristics (ROC) is reported in Fig. 9. In both these two figures we add the simulated performance of AES sequences. From these results we can see a perfect match between the simulated mixed curves and the analytic random curves, thus confirming our AES randomness hypothesis.

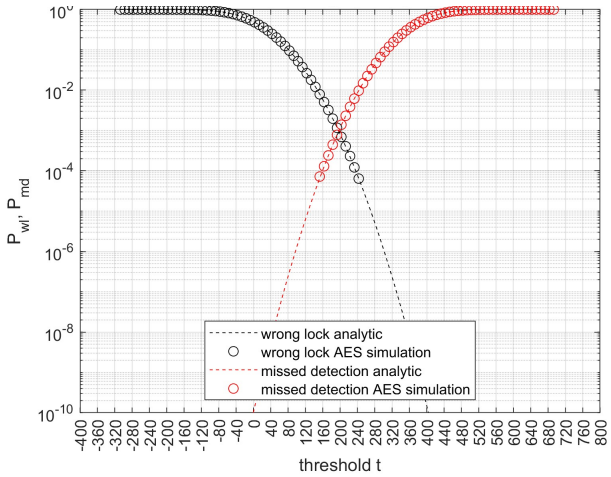

Fig. 8. Missed detection and wrong lock probabilities, analytic and simulation results, AES sequence with $N = M = 128$, $N_U = 5$, $E_c/N_o = 0$ dB.

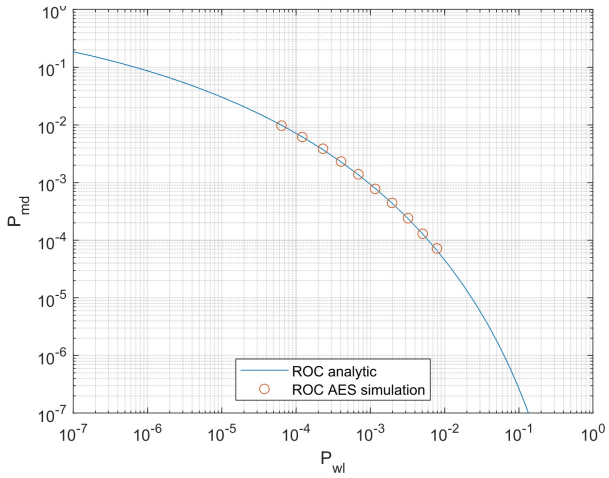

Fig. 9. ROC analytic and simulated results, for AES sequences, with $N = M = 128$, $N_U = 5$, $E_c/N_o = 0$ dB.

E. Discussion

We have shown that the AES sequences possess all the five properties introduced in section I. Then, they are very good candidates for our LEO scenario or others with similar requirements. Now that we have established that AES sequences perform like random ones, in the next section will show how we can further improve their performance, while maintaining jamming protection, by mixing AES and Gold sequences.

III. The Construction of Orthogonal Cosets of Extended Gold Codes

In this section we prove that, by acting properly, we can take a set of Gold codes, correctly align them, extend them by one chip, add the same vector to all of them to obtain

a coset, and we get a set of spreading sequences which are perfectly orthogonal for CDM.

Gold codes [6] are widely used in telecommunications and signal processing thanks to to their remarkable properties in terms of low cross-correlation. They are generated by combining two m-sequences [4] obtained from two n-cell linear feedback shift registers (LFSRs) characterized by paired polynomials.

We start from a binary m-sequence $\underline{c}_1$ generated by an LFSR with primitive polynomial $p_1(D)$ of degree n ($n \geq 2$, n not divisible by 4), and another m-sequence $\underline{c}_2$ generated by an LFSR with primitive polynomial $p_2(D)$ of degree n which is paired to $p_1(D)$. (Let α be a primitive element of the Galois field GF(2^m), the paired polynomial $p_2(D)$ is the minimal polynomial of α^t with $t = 2^{\frac{n+1}{2}}$ for n odd or $t = 2^{\frac{n+2}{2}}$ for n even. Equivalently, $\underline{c}_2$ is obtained as the (2^t+1)-st decimation of $\underline{c}_1$).

The set of Gold codes is made by the $(2^n + 1)$ sequences obtained as:

$$\left\{\underline{c}_1, \underline{c}_2, \underline{c}_1 \oplus T^i\left(\underline{c}_2\right)\right\}, \quad 0 \leq i < 2^n - 1 \tag{11}$$

where T^i is the cyclic shift by i positions and $\oplus$ is the binary sum in GF(2) (ex-or).

The basic properties of Gold sequences are then

- Sequence length (period): $L_G = 2^n - 1$
- Number of Gold sequences: $L_G + 2$
- cross-correlation property: for any pair of sequences the cyclic cross-correlation has only three possibile values: $-t, -1, t-2$.

Let us first consider the reduced set

$$\hat{C} = \left\{\underline{c}_1, \underline{c}_1 \oplus T^i\left(\underline{c}_2\right)\right\}, \quad 0 \leq i < 2^n - 1 \tag{12}$$

of cardinality $L_G+1 = 2^n$. In [39] it was proved that the inner product between two bipolar vectors $\underline{v}'_1, \underline{v}'_2$ corresponding to two binary $\underline{v}_1, \underline{v}_2 \in \hat{C}$ is

$$(\underline{v}'_1, \underline{v}'_2) = \sum_{m=0}^{L_G-1} v'_1(m)v'_2(m) = -1. \tag{13}$$

We now extend this results by showing that bipolar vectors of *cosets* of extended Gold codes are orthogonal. Let us first consider the set $\hat{C}_{eG}$ obtained by adding a final symbol equal to zero to all the vectors of $\hat{C}$. This set is made by 2^n vectors of length $L_{eG} = 2^n$. Given a binary vector $\underline{v}$ of length L_{eG}, let us consider the binary set $\overline{C}_{eG} = \underline{v} \oplus \hat{C}_{eG}$ and the corresponding bipolar set $\overline{C}'_{eG}$.

Theorem 1 (Orthogonality of cosets of extended Gold codes)**.** *The inner product between any pair of coset vectors $\underline{a}', \underline{b}' \in \overline{C}'_{eG}$ is equal to zero:*

$$(\underline{a}', \underline{b}') = \sum_{m=0}^{L_{eG}} a'(m)b'(m) = 0. \tag{14}$$

Proof: Given the m-sequence $\underline{c}_2$ of length $L_G = 2^n - 1$, the set $C = \{\underline{0}, \underline{c}, T(\underline{c}), \ldots, T^{L-1}(\underline{c})\}$, where $\underline{0}$ represents the all-zero vector, is a binary linear code [39]. In fact, it is closed with respect to the binary sum, because the sum of two shifted m-sequences is still in C:

$$\forall i, j, \exists h : T^i(\underline{c}) \oplus T^j(\underline{c}) = T^h(\underline{c}). \tag{15}$$

It follows that the set $\hat{C}_{eG}$ is a binary linear code made by L_{eG} vectors of L_{eG} bits. The set $\overline{C} = \underline{v} \oplus \hat{C}_{eG}$ is then a coset of a binary linear code.

We remember that all m-sequences have Hamming weight $w_H(\underline{c}) = \frac{L_G+1}{2} = \frac{L_{eG}}{2}$. Then, all non-zero vectors of $\hat{C}_{eG}$ have the same weight. Given two bipolar vectors $\underline{a}', \underline{b}'$ of length L_{eG}, their inner product is linked to the Hamming distance of the corresponding binary vectors $\underline{a}, \underline{b}$ by

$$(\underline{a}', \underline{b}') = L_{eG} - 2d_H(\underline{a}, \underline{b}). \tag{16}$$

Given the bipolar version $\overline{C}'_{eG}$ of the coset $\overline{C}_{eG}$, if $\underline{a}', \underline{b}' \in \overline{C}'_{eG}$, we have:

$$\begin{aligned}(\underline{a}', \underline{b}') &= L_{eG} - 2d_H(\underline{a}, \underline{b}) \\ &= L_{eG} - 2d_H(\underline{v} \oplus T^i(\underline{c}), \underline{v} \oplus T^j(\underline{c}) \\ &= L_{eG} - 2w_H(\underline{v} \oplus T^i(\underline{c}) \oplus \underline{v} \oplus T^j(\underline{c}) \\ &= L_{eG} - 2w_H(T^h(\underline{c})) = 0.\end{aligned} \tag{17}$$

■

Note that the performance of even and odd-degree Gold codes can be very different (see [40], [41]), but the property demonstrated in Theorem 1 is based on the constituent m-sequences and then is valid in both cases.

The coset $\overline{C}_{eG}$ is made by 2^n vectors of $L_{eG} = 2^n$ binary symbols. In the following, we will refer to $\overline{C}$ as a *Gold coset* and we will use it to build the new mixed sequences.

IV. Mixed AES/Gold sequences

In this section, we present the idea of mixing AES and Gold coset sequences. We will refer to the information bits to be transmitted as 'bits' and to the symbols of the spreading sequences as 'chips'. Suppose we want to generate a sequence of L chips, where the spreading factor (number of chips per bit) is $M < L$. As explained before in our applications, to guarantee jamming resistance, the sequence length is always much longer than the spreading factor.

To each user we assign:

- A different AES sequence $\underline{c}_1 = (c_1(m))$ of length L, generated in counter mode as explained in Section II.
- A different extended Gold code $\underline{c}_2 = (c_2(m)) \in \hat{C}$ of length $L_{eG} = 2^n < M$.
- The same AES sequence $\underline{v}$.

We build the mixed sequence as follows.

- We partition the AES sequence of L chips into segments of M chips (each segment corresponds to one bit).
- We randomly select $L_{eG} \leq M$ positions which are the same for each bit and for each user.
- For each bit, for each user, the L_{eG} chips of the AES sequence are replaced by the L_{eG} chips of a coset of the Gold sequence, using a vector $\underline{v}$, common to all the satellites, that changes at every bit

Mathematically, given the chip index m, let us write it as $m = jM + m_1$, where j is the bit number and $m_1 \in Z_M =$

$\{0, 1, ..., M-1\}$. We denote by $X \subseteq Z_M$ the set of L_{eG} coordinates where we want to replace the AES chips. Let us consider the one-to-one map

$$f : X \to Z_{L_{eG}} = \{0, 1, ..., L_{eG} - 1\} \tag{18}$$

and a sequence of vectors $\underline{v}_j$ of L_{eG} binary symbols.

For any chip index $m = jM + m_1$, for any bit j, we build the mixed sequence $\underline{c}_3 = (c_3(m))$ as:

$$c_3(m) = \begin{cases} c_1(m), & \text{if } m_1 \notin X \\ c_2(f(m_1)) \oplus v_j(f(m_1)), & \text{if } m_1 \in X \end{cases} \tag{19}$$

A very simple toy example is shown in Fig. 11 for a sequence length $L = 16$, a spreading factor $M = 8$, a Gold sequence length $L_{eG} = 4$. The shown sequence corresponds to two bits, each of 8 chips. The set used for Gold substitution is $X = \{1, 3, 4, 7\}$. The AES sequence is $c_1(m)$ in the first row, the Gold sequence is $c_2(m)$ in the second row, the mixed sequence is in the third row. Chips $v_j(m)$ are the same for all the satellites.

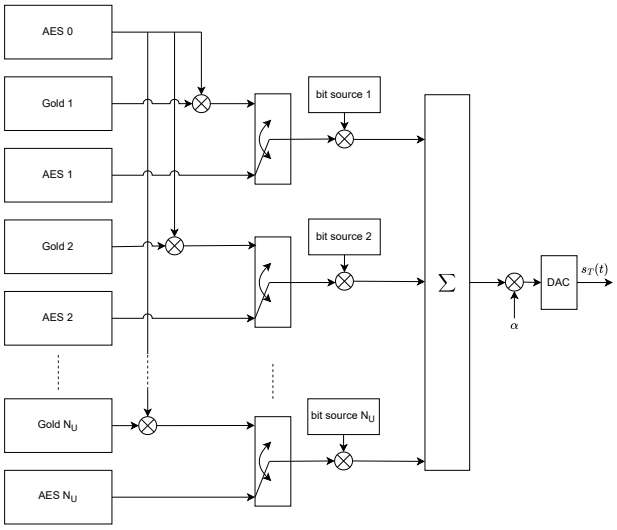

Fig. 10. Transmitted signal generation (all signals have values ± 1 apart from $s_T(t)$).

A. Random Vector Masking

In principle, we could simply duplicate the extended Gold sequence identical for each bit without using vector $\underline{v}$. However, when we perform acquisition, we would encounter peaks with periodicity M in the cross-correlation function, corresponding to the duplicated Gold sequence, resulting in an increased probability of false lock. That's why we introduce masking through the application of the random vectors $\underline{v}$, that generate Gold cosets. In practice, the simplest way to implement this masking is by generating an additional AES sequence alongside those assigned to the N_U satellites. For each bit, we can add the chips from this sequence to the Gold code at the $N_{L_{eG}}$ positions. (As an alternative, we could also add the additional sequence to the entire mixed sequence, without altering the properties of the mixed sequences in terms of performance or jamming resistance.) The overall structure of the transmitter is shown in Fig. 10.

V. Performance of Mixed AES/Gold Sequences

In this section, we compute the error probability of mixed sequences and the achieved gain with respect to AES/PRN sequences.

A. Bit Error Probability

The following theorem provides the analytic expression of the bit error probability of mixed sequences.

Theorem 2. *[Error probability of Mixed sequences] Given an uplink CDM system serving N_U users with the same power, to each user is assigned a mixed sequence with spreading factor M and number of Gold symbols per bit $L_{eG} < M$. The bit error probability for a generic user #i is given by:*

$$P(e) = \frac{1}{2}\text{erfc}\sqrt{\frac{\left(\frac{E_b}{N_o}\right)_i}{1 + 2\frac{(N_U-1)(M-L_{eG})}{M^2}\left(\frac{E_b}{N_o}\right)_i}} \tag{20}$$

Proof:

The structure of the transmitted signal is described in Eq. (1). Let us focus on the first bit interval $0 \le t < T_b$. In this interval the transmitted signal is

$$s_T(t) = \alpha \sum_{j=0}^{N_U-1} b'_j(0)\bar{c}_j(t) = \alpha b'_i(0)\bar{c}'_i(t) + \alpha \sum_{j=0, j\neq i}^{N_U-1} b'_j(0)\bar{c}'_j(t) \tag{21}$$

where $\bar{c}'_j(t) = \sum_{m=0}^{M-1} c'_j(m) P_{T_c}(t - mT_c)$ is the spreading signal corresponding to the first bit, i.e., the first M chips.

Suppose to transmit the information symbol $b'_i(0) = -1$ to user number i. This user receives

$$r(t) = s_T(t) + n(t)$$

where $n(t)$ is the noise waveform added by the AWGN channel, characterized by a power spectral density equal to $N_o/2$. User i projects $r(t)$ over the unit energy basis signal $\frac{1}{\sqrt{T_b}} c'_i(t)$ and obtains the random variable

$$r = a + x + n.$$

The first term is the useful component corresponding to the first term of (21):

$$a = \alpha\sqrt{T_b} b'_i(0) = -\alpha\sqrt{T_b} = -\sqrt{E_b}.$$

The second term x, corresponding to the second term of (21), measures the impact of the $N_I = N_U - 1$ interferers. Their contribution is equal to

$$x = \gamma \frac{\alpha}{\sqrt{T_b}} T_c \tag{22}$$

where γ is the sum of H equiprobable terms ± 1, being $H = (N_U - 1)(M - L_{eG})$. This term is computed over the $(M - L_{eG})$ AES coordinates only, which are equivalent to random

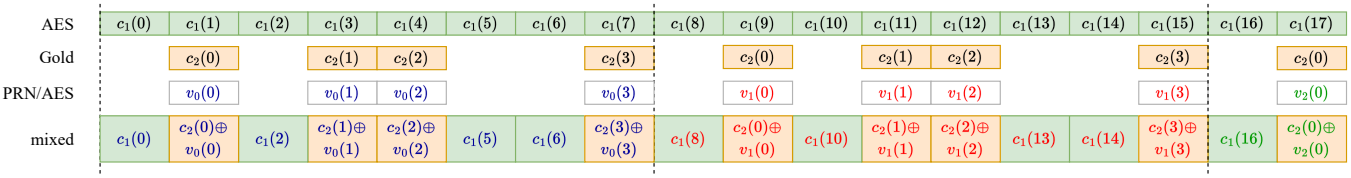

Fig. 11. Example of mixed sequence for $L = 16, M = 8, L_{eG} = 4$. Green cells = AES, Pink cells = Gold, blue symbols= first bit, red symbols = second bit, green symbols = third bit.

bits. Thanks to Theorem 1, since the Gold coset vectors are orthogonal, the contribution of the other L_{eG} Gold coordinates is zero. Given a binomial random variable h with mean value $H/2$ and variance $H/4$, we have $\gamma = H - 2h$ that, for H large enough, can be modeled as $\mathcal{N}(0, H)$.[3] Then x can be modeled as

$$\mathcal{N}\left(0, H\alpha^2 \frac{T_c^2}{T_b}\right) = \mathcal{N}\left(0, H\frac{E_b}{M^2}\right), \tag{23}$$

being E_b the energy per bit. The third term n has a Gaussian pdf $\mathcal{N}\left(0, \frac{N_o}{2}\right)$. It follows that the error probability is

$$P(e) = Pr(x + n > -a) = \frac{1}{2}\text{erfc}\sqrt{\frac{a^2}{2\left(\frac{N_o}{2} + \frac{H}{M^2}E_b\right)}}$$
$$= \frac{1}{2}\text{erfc}\sqrt{\frac{E_b}{N_o + 2\frac{N_I(M-L_{eG})}{M^2}E_b}} \tag{24}$$

and Equation (20) follows, having set, more correctly, the signal to noise ratio for user i equal to $(E_b/N_o)_i$ (visible users typically have different slant ranges and path losses).

(Note: When $L_{eG} = 0$ we have plain AES sequences and Corollary 1 follows.) ■

Some examples of error rate performance for mixed sequences are shown in Fig. 12 and 13 for $M = 128$ and in Fig. 14 for $M = 1000$. There is a perfect match between the simulation results and the analytic curves. We can also appreciate the gain with respect to the pure AES/PRN sequences that, in some cases, can be very large. Regarding the comparison with Gold sequences, it is worth noting that, as shown in Figures 5 and 6, the error probability of complete Gold sequences overlaps with the ideal 2-PAM curve, while that of truncated sequences aligns with random sequences.

B. Gain and Floor

The advantage in terms of performance offered by mixed sequences compared to AES sequences is twofold: the gain at the same BER and the error floor reduction. Firstly, they ensure a gain at the same probability of error, out of the floor region. Given the value $\left(\frac{E_b}{N_o}\right)^*$ necessary to achieve an error rate $P(e)^*$ for mixed sequences, we denote by value $\left(\frac{E_b}{N_o}\right)' = G\left(\frac{E_b}{N_o}\right)^*$ the ratio necessary to achieve the same error rate in case of AES/PRN sequences. This corollary quantifies the gain G.

[3]Equivalently, γ is the sum of H i.i.d. random variables with equally likely values ± 1; the central limit theorem states that $\gamma/\sqrt{H}$ has approximately a Gaussian distribution with zero mean and variance 1, for $H \to \infty$.

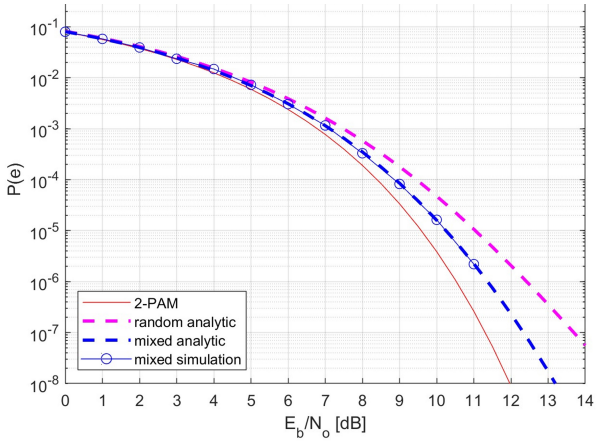

Fig. 12. Bit error probability results for mixed sequences with $M = 128$, $L_{eG} = 64$, $N_I = 2$, $N_U = 3$.

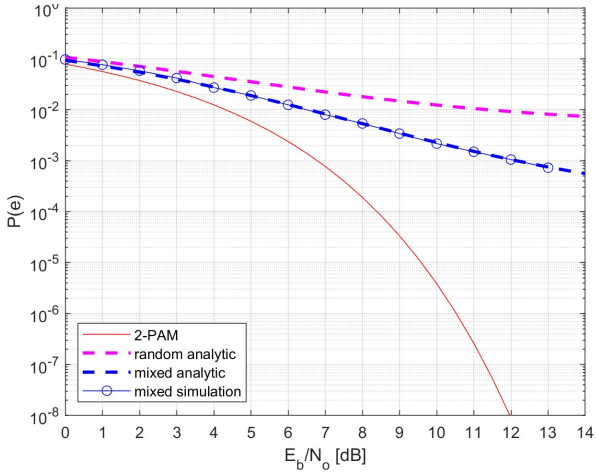

Fig. 13. Bit error probability results for mixed sequences with $M = 128$, $L_{eG} = 64$, $N_I = 19$, $N_U = 20$.

Corollary 4. *Under the conditions of Theorem 2, fixed the error probability value $P(e)^*$, the gain in terms of E_b/N_o achieved by the mixed sequences with respect to a random sequence is given by*

$$G = \frac{1}{1 - \frac{2(N_U-1)L_{eG}}{M^2}\left(\frac{E_b}{N_o}\right)^*} \tag{25}$$

Proof: The error probability of random sequences is given in Corollary 1, that of mixed sequences in Theorem 2.

To compute the gain G, since the two systems achieve the same error probability $P(e)^*$, we can write

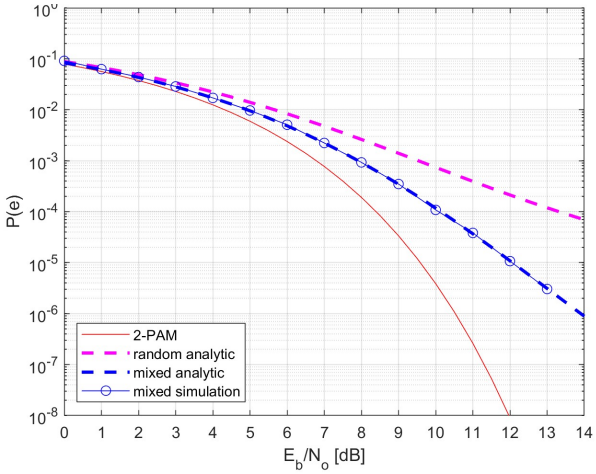

Fig. 14. Bit error probability results for mixed sequences with $M = 1000$, $L_{eG} = 512$, $N_I = 59$, $N_U = 60$

$$\frac{1}{2}\text{erfc}\sqrt{\frac{\left(\frac{E_b}{N_o}\right)^*}{1+2\frac{N_I(M-L_{eG})}{M^2}\left(\frac{E_b}{N_o}\right)^*}} = \frac{1}{2}\text{erfc}\sqrt{\frac{\left(\frac{E_b}{N_o}\right)^* G}{1+2\frac{N_I}{M}\left(\frac{E_b}{N_o}\right)^* G}} \tag{26}$$

and Equation (25) follows. ■

An example of the behaviours of the gain achieved by mixed sequences for different error rates and number of users is shown in Fig. 15 for $M = 128$.

A second important aspect for applications is the reduction of the error floor. As the number of interferers increases, performance curves exhibit a floor, since the errors are due not to thermal noise but to the interfering signals. Looking at the example in Fig. 13, we can observe that the error floor is around $8 \cdot 10^{-3}$ for the random sequences and around $7 \cdot 10^{-4}$ for the mixed sequence. This phenomenon is also reflected in Fig. 15, where we see that the curves for a certain error probability are interrupted above a threshold value of N_U. That threshold value represents the number of interferers that induce an error floor equal or slightly larger than the selected error rate in the case of random sequences. Consequently, the gain diverges. Therefore, it is interesting to compare, at the same error floor $P_{floor}(e)$ and the same spreading factor M, what is the number of interferers in the two cases.

Corollary 5. *Under the conditions of Theorem 2, being $N_{I,AES}$ the interferers for the AES/PRN sequences and $N_{I,mixed}$ those for the mixed sequence, the two systems have the same error floor, for the same spreading factor M, if*

$$\left\lfloor \frac{M}{M-L_{eG}} N_{I,AES} \right\rfloor - 1 \leq N_{I,mixed} \leq \left\lfloor \frac{M}{M-L_{eG}} N_{I,AES} \right\rfloor \tag{27}$$

Proof: The error floor is given by

$$P_{floor}(e) = \frac{1}{2}\text{erfc}\sqrt{\frac{M^2}{2N_{I,mixed}(M-L_{eG})}}$$

for the mixed sequence, while it is

$$P_{floor}(e) = \frac{1}{2}\text{erfc}\sqrt{\frac{M}{2N_{I,AES}}}$$

for the AES/PRN sequences; these two results are obtained by setting $N_o = 0$ in Eq. (2) and in Eq. (20), respectively. Eq. (27) is derived by equating the two formulas of $P_{floor}(e)$ and taking into account the integer constraint. ■

Therefore, the performance curves of mixed sequences have the same error floor as AES/PRN spreading sequences for a much higher number of interferers. Fig. 16 shows an example: for $L_{eG}/M \simeq 1/2$, the number of users that causes a certain floor for mixed sequences is approximately double compared to that for AES sequences, increasing for example from 14 to 27 for a floor at 10^{-3}. This result is evidently significant for practical applications with many users.

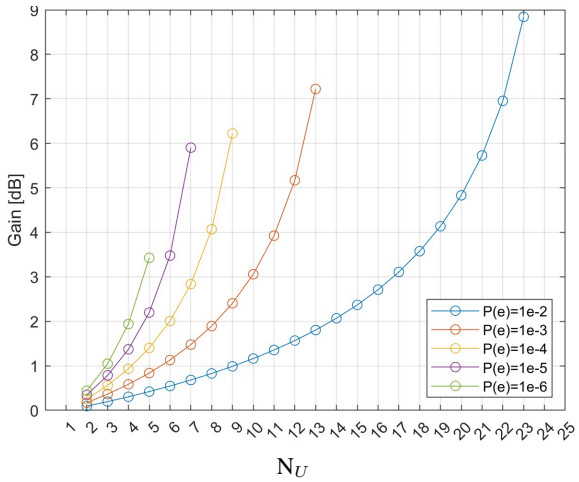

Fig. 15. Gain achieved by mixed sequences with respect to AES sequences (out of the floor region) vs. the number of users, for $M = 128$ and $L_{eG} = 64$.

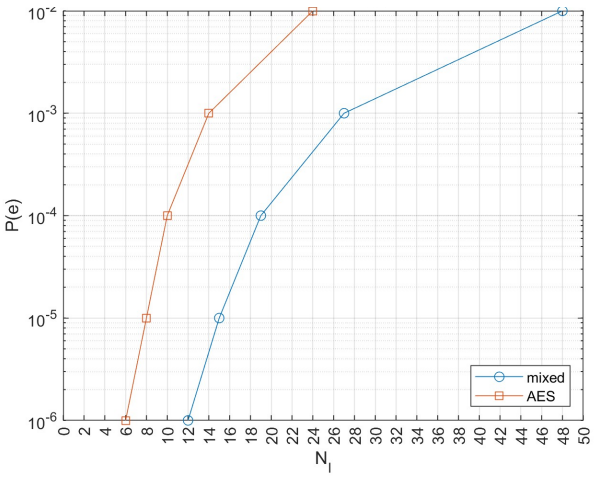

Fig. 16. Number of users corresponding to a floor at the given $P(e)$, for $M = 128$ and $L_{eG} = 64$.

C. Performance over the Land Mobile-Satellite Channel

We also conducted an experiment using the two-state Land Mobile-Satellite (LMS) channel model of the ITU-R P.681-11 [42] in an urban scenario with a station transmitting in the uplink Ku band at 10 Mbps. The elevation angle was set to 45 degrees and the azimuth observation to 0 degrees. The results for a number of satellites $N_S = 1, 3, 20$ are shown in Fig. 17, where we compare the LMS performance of:

- mixed sequences (spreading factor $M = 128$, $L_{eG} = 64$, length $L = 10,000$),
- AES sequences ($M = 128$, $L = 10,000$),
- extended Gold codes ($M = L = 128$),
- truncated Gold codes ($M = 128, L = 1023$)
- entire Golay [15] sequences ($M = L = 128$) taken from [15]
- truncated Golay [15] sequences ($M = 128, L = 2048$).

Looking at the plot, the following key observations can be made:

- As expected, for a single user all sequences achieve similar performance over the LMS channel, inferior to that observed over the AWGN channel.
- As noted previously in Fig. 5 and Fig. 6, entire Gold sequences are orthogonal and align with single-user performance (their curves for $N_S = 1$, 3, and 20 coincide), while truncated Gold sequences for $N_S > 1$ align with AES performance.
- A similar behavior is observed with Golay sequences: when used in their entirety, they are perfectly orthogonal (their curves for $N_S = 1$, 3, and 20 coincide), but when truncated[4], they lose this property and for $N_S > 1$ align with the performance of AES and truncated Gold sequences.
- When several satellites are used, and the sequence length is greater than the spreading factor, mixed sequences outperform AES, truncated Gold, and truncated Golay sequences, even on the LMS channel.

These results confirm that, even on LMS channels, mixed sequences provide a performance gain in the presence of interfering satellites (N_S>1), when the sequence length significantly exceeds the spreading factor, as required for jamming protection.

D. Impact on Error Correction Coding

When considering the impact of a channel code, the gain provided by the mixed sequences is further amplified. For the telecommand link, the most recent code introduced by the Consultative Committee for Space Data Systems (CCSDS) (which unites all the space agencies worldwide), is the $(128, 64)$ Low Density Parity Check (LDPC) code ([43], [44]).

Fig. 18 compares the bit error probability of LDPC-coded mixed sequences (blue lines) to that of LDPC-coded AES/PRN sequences (magenta lines) over the AWGN channel. The comparison is performed for $M = 128$, $L_{eG} = 64$, and two scenarios for $N_I = 20$ (dashed lines) and $N_I = 50$ (solid lines). The results clearly highlight that (i) the LDPC code allows to substantially decrease the error rate, thus avoiding the error floor, and (ii) the coded mixed sequences can provide a significant gain that increases with the number of users.

[4]Note that in reality Golay sequences, when truncated, result in poor correlation properties, similar to what happens to Walsh-Hadamard sequences. For this reason, we have selected subsets that do not contain poorly correlated sub-sequences. The resulting subsets do perform really close to random sequences.

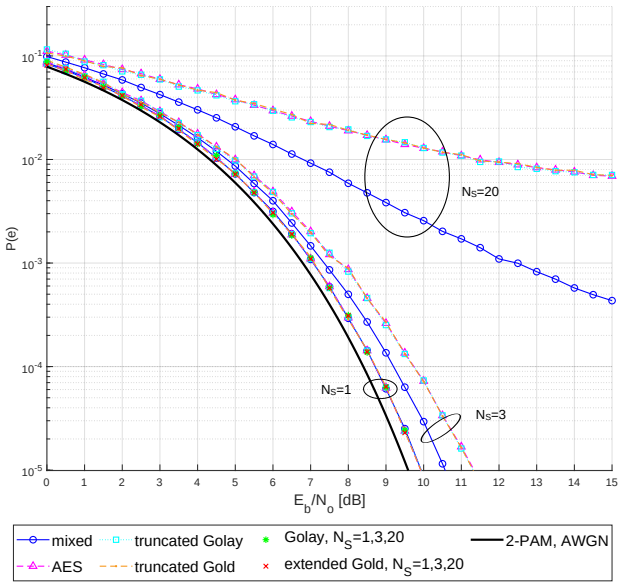

Fig. 17. Bit error probability results for different spreading sequences over the LMS channel (and AWGN 2-PAM curve).

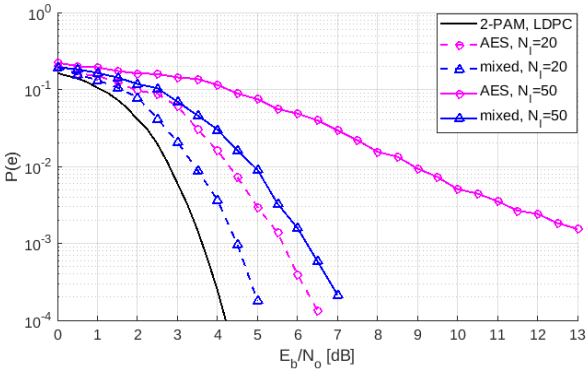

Fig. 18. Error probability results for LDPC coded mixed and AES sequences, $M = 128$, $L_{eG} = 64$, $N_I = 20$ and 50.

E. Acquisition

Given the acquisition scenario described in Section II-D, we analyze the acquisition performance of mixed sequences.

1) Missed detection for mixed sequences:

Theorem 3. *[Missed-detection probability for a mixed sequence] Given a CDM system with N_U users and spreading factor M, using mixed sequences with $L_{eG} < M$ Gold symbols. We perform acquisition on $N = kM$ chips. The missed detection probability is given by*

$$P_{md}(\tau) = \frac{1}{2}\text{erfc}\frac{N-\tau}{\sqrt{2\left(N\sigma^2 + (N_U - 1)(N - kL_{eG})\right)}} \quad (28)$$

where E_c is the chip energy and

$$\sigma^2 = \frac{1}{2\frac{E_c}{N_o}} = \frac{1}{\frac{2}{M}\frac{E_b}{N_o}} \tag{29}$$

Proof: When we project over the normalized pulse as in Eq. (4), assuming an AWGN channel (noise power spectral density $N_o/2$), $r(m)$ is

$$\begin{aligned} r(m) &= \sum_{i=0}^{N_U-1} b'_i\left(\left\lfloor \frac{m}{M} \right\rfloor\right) c'_i(m) + w(m) \\ &= \sum_{i=0}^{N_U-1} b'_i(\overline{m}) c'_i(m) + w(m) \end{aligned} \tag{30}$$

where $w(m)$ is a zero mean Gaussian random variable with variance $N_o/(2E_c)$: $w(m) \sim \mathcal{N}(0, N_o/(2E_c))$.

Considering that the transmitted signal for user i has $b'_i(n) = 1$, we obtain

$$r(m) = c'_i(m) + \sum_{j\neq i} b'_j(\overline{m}) c'_j(m) + w(m) \tag{31}$$

The receiver spreading sequence is aligned to the incoming sequence and the inner product in Eq. (6) is equal to

$$\begin{aligned} \Gamma(0) = (\underline{r}, \underline{s}'_i(0)) &= \sum_{m=0}^{N-1} r(m) c'_i(m) \\ &= \sum_{m=0}^{N-1} c'_i(m) c'_i(m) + \sum_{j=1, j\neq i}^{N_U} \sum_{m=0}^{N-1} b'_j(\overline{m}) c'_j(m) c'_i(m) \\ &+ \sum_{m=0}^{N-1} w(m) c'_i(m) = N + \gamma_2 + \gamma_3. \end{aligned}$$

The second term γ_2 is the sum of H terms equal to ± 1 with the same probability, where $H = (N_U - 1)(N - kL_{eG})$. This term is computed over the $(N - kL_{eG})$ AES coordinates, which are equivalent to random bits. The second part is computed on the $k \times L_{eG}$ Gold coordinates: thanks to Theorem 1, since the Gold coset vectors are orthogonal, the contribution of the other $k \times L_{eG}$ Gold coordinates is zero. Then $\gamma_2 \sim \mathcal{N}(0, H)$.

The third term γ_3 can be modeled as $\mathcal{N}\left(0, N\sigma^2\right)$. Then Γ can be modeled as $\mathcal{N}\left(N, N\sigma^2 + H\right)$. It follows

$$P_{md}(\tau) = Pr(\Gamma(0)) < \tau) = \frac{1}{2}\mathrm{erfc}\frac{N - \tau}{\sqrt{2(N\sigma^2 + H)}}$$

and Eq. (28) is derived.

(Note: when $L_{eG} = 0$, we obtain plain AES sequences and Corollary 2 follows). ∎

2) Wrong lock for mixed sequences:

Theorem 4. *[Wrong lock for mixed sequences] Given a CDM system with N_U users and spreading factor M, using mixed sequences with L_{eG} Gold symbols. We perform acquisition on $N = kM$ chips. The false alarm probability is given by*

$$P_{wl}(\tau) = Pr(\Gamma' > \tau) = \frac{1}{2}\mathrm{erfc}\frac{\tau}{\sqrt{2N(1 + N_I + \sigma^2)}}, \tag{32}$$

where E_c is the chip energy and

$$\sigma^2 = \frac{1}{2\frac{E_c}{N_o}} = \frac{1}{\frac{2}{M}\frac{E_b}{N_o}}$$

Proof: Sample $r(m)$ is that in Eq. (31), but now the receiver projects over

$$\underline{s}'_i(\ell) = (c'_i(\ell), c'_i(\ell+1), \ldots, c'_i(\ell+N-1))$$

and the inner product is

$$\begin{aligned} \Gamma(\ell) = (\underline{r}, \underline{s}'_i(\ell)) &= \sum_{m=0}^{L-1} r(m) c'_i(m+\ell) \\ &= \sum_{n=0}^{N-1} c'_i(m) c'_i(m+\ell) \\ &+ \sum_{j=1, j\neq i}^{N_U} b'_j(\overline{m}) \sum_{m=0}^{N-1} c'_j(m) c'_i(m+\ell) \\ &+ \sum_{m=0}^{L-1} w(m) c'_i(m+\ell) = \gamma_1 + \gamma_2 + \gamma_3 \end{aligned}$$

The first term γ_1 is the sum of N terms equal to ± 1 with the same probability and it can be modeled as $\mathcal{N}(0, N)$.

Since we are using the vector masking of the Gold code, the autocorrelation properties are equivalent to those of a random sequence. Then, the second term γ_2 is the sum of $H = NN_I$ terms equal to ± 1 with the same probability, and it can be modeled as $\mathcal{N}(0, NN_I)$.

The third term γ_3 can be modeled as $\mathcal{N}\left(0, N\sigma^2\right)$. Then Γ can be modeled as $\mathcal{N}\left(0, N + NN_I + N\sigma^2\right)$ and the wrong lock probability is

$$P_{wl}(\tau) = Pr(\Gamma_\ell > \tau) = \frac{1}{2}\mathrm{erfc}\frac{\tau}{\sqrt{2N(1 + N_I + \sigma^2)}}$$

and Eq. (32) follows.

(Note: this result does not depend on L_{eG}, then it holds also for Corollary 3 on random sequences). ∎

We can compare the simulated missed detection and wrong lock performance of the mixed sequences against the analytic results of Theorems 3 and 4. The Receiver Operating Characteristics (ROC) for the AES and the mixed sequences are compared in Fig. 19, where simulation results for the mixed sequence are also shown.

We can observe that the ROC curves of the mixed sequences are superior to those of the random sequences. To better quantify the gain achieved by the mixed sequences, we can set, e.g., the P_{wl} value to 10^{-3} and calculate the corresponding P_{md} as a function of the SNR E_c/N_0. The result is shown in Fig. 20. We can see that, at the same P_{wl} and P_{md} levels, the mixed sequences achieve a significant advantage of several dBs in terms of E_c/N_0.

Finally, in Fig. 21 we investigate the acquisition time of the mixed sequences, by comparing their performance to that of AES/random sequences. The results show that mixed sequences can be acquired even at very low SNR and offer a complexity advantage (requiring shorter segment lengths N) compared to AES/random sequences, while maintaining the same acquisition time and probability.

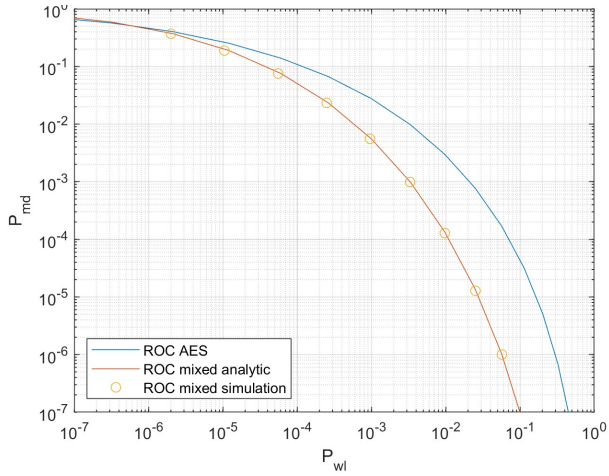

Fig. 19. ROC for mixed and AES sequences, analytic and simulated results, mixed sequence with $N = M = 128, L_{eG} = 64, N_U = 5$

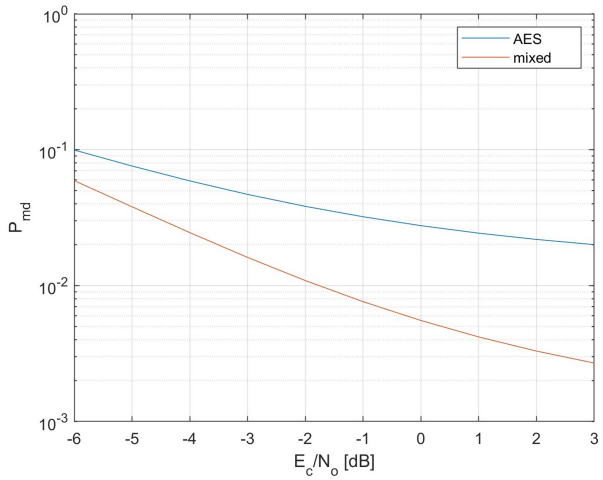

Fig. 20. Probability of missed detection vs. Signal-to-Noise ratio for $P_{wl} = 10^{-3}$ for mixed and AES sequences, mixed sequence with $N = M = 128, L_{eG} = 64, N_U = 5$.

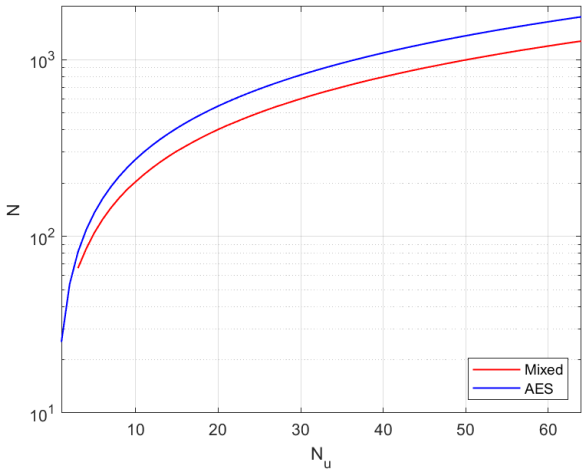

Fig. 21. Number of correlation chips N required to achieve the same acquisition time for mixed and AES/PRN sequences: $L_{eG} = 64$, $E_c/N_0 = 0$ dB, $L = 1000$, and acquisition time of 505 chips.

F. Discussion

The mixed sequences inherit from the AES component all the five properties introduced in section I. They are still very long, they can realize any length L and spreading factor $M > L_{eG}$, they work with $M \ll L$. They still ensure a high level of protection against jamming derived from the impossibility of reconstructing the sequence from a segment. They still ensure a high level of protection against jamming derived from the impossibility of reconstructing the sequence from a segment. In fact, we still have $M - L_{eG}$ chips per bit of the AES sequence and this makes the reconstruction of the whole sequence impossible if $M - L_{eG}$ is not too small (in our examples, we typically use a ratio $L_{eG}/M \simeq 1/2$ and $L_{eG} \geq 64$). Actually, also the L_{eG} Gold chips are unpredictable by an external attacker thanks to the masking by the common AES sequence (but not if the attacker is one of the legitimate satellites served by the same ground station).

While maintaining the same anti-jamming protection, the mixed sequences achieve lower error performance and better acquisition performance thanks to the insertion of the aligned Gold coset segments which decrease their inner products. This allows to increase the number of users served in parallel.

A drawback of the mixed constructions is a modest increase in complexity because it is necessary to alternate the chips of AES and Gold sequences and sum the masking sequence. A more significant issue is related to cardinality, which is constrained by the number of Gold coset elements L_{eG} and, therefore, is lower than the spreading factor M. However, except for mega-constellations of tens of thousands of satellites where it could be problematic, for most applications the spreading factor is enough to serve usual LEO constellations (from several tens to hundreds of satellites or more depending on M). If the constellation is bigger, we can still use mixed sequences for a subset of the satellites obtaining a gain.

The five anti-jamming properties introduced in Section I, that AES and mixed sequences possess, are difficult to satisfy all at once by classical or recently introduced sequences ([14], [15], [16], [17]). We have shown how algebraically generated sequences have a low linear complexity, thus they can be reconstructed from a segment. Furthermore, these sequences lose their correlation properties if used with a spreading factor much less than the length of the sequence.

Finally, Wash-Hadamard sequences, having inner product equal to zero, might be used instead of the extended Gold code. In the context of satellite systems, however, Gold sequences are usually preferred since they can be generated simply from two LFSRs instead of being stored (see the small vector generation requirement in Section I).

VI. Conclusions

In this paper, we have studied AES spreading sequences generated by applying the AES algorithm in counter mode. We have evaluated their linear complexity profile, error probability and acquisition performance and verified that they are aligned to those of random sequences. Then, AES sequences are a very good candidate for jamming-resistant applications: their length can be much longer than the spreading factor, they

cannot be reconstructed from a segment, their cardinality is huge, they can be built from a small key. Algebraic sequences, both classical ([6], [7]) and reecnt ([14], [15], [16], [17]) have very good correlation properties when used in full, but when the length is much greater than the spreading factor, their performance also aligns with that of random sequences. Moreover, they do not possess all the other properties together.

To further enhance the performance of AES sequences, we have introduced cosets of extended Gold codes, demonstrating their orthogonality properties for CDM. Then we have used them to build a new family of mixed sequences, obtained by combining AES sequences and Gold cosets. We calculated the error probability of these sequences, both analytically and through simulation, and demonstrated that they yield a significant performance gain. We analyzed both AWGN and LMS channels, considering uncoded and coded transmission. The mixed sequences may allow doubling the number of users that cause a certain level of error floor. We also analyzed acquisition performance, showing that a relevant SNR gain is achieved in this case, too. The mixed sequences inherit the anti-jamming properties of AES sequences and increase their performance thanks to the insertion of the aligned Gold coset segments, which improves the cross-correlation.

As a case study, we have considered a ground station using CDM to serve LEO satellites: the mixed sequences allow to significantly increase the number of satellites that can be served in parallel, while maintaining the same level of performance and protection against jamming.

ACKNOWLEDGMENT

The authors are grateful to the European Space Agency for their support of this study, and to the Editor and the Reviewers for their valuable comments that have significantly improved the article.

This work was partially supported by the European Union—Next Generation EU under the Italian National Recovery and Resilience Plan (NRRP), Mission 4, Component 2, Investment 1.3, CUP E13C22001870001, partnership on "Telecommunications of the Future" (PE00000001—program "RESTART").

REFERENCES

[1] A. J. Viterbi, *CDMA: Principles of Spread Spectrum Communication*. Prentice Hall, 1995.

[2] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[3] D. Torrieri, *Principles of Spread-Spectrum Communication Systems*. Springer Nature, 2022.

[4] S. W. Golomb, *Shift Register Sequences*. San Francisco, CA: Holden-Day, 1967.

[5] M. Baldi, F. Chiaraluce, N. Boujnah, and R. Garello, "On the Autocorrelation Properties of Truncated Maximum-Length Sequences and Their Effect on the Power Spectrum," *IEEE Transactions on Signal Processing*, vol. 58, no. 12, pp. 6284–6297, 2010.

[6] R. Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing," *IEEE Transactions on Information Theory*, vol. 13, no. 4, pp. 619–621, 1967.

[7] T. Kasami, "Weight Distribution Formula for some Class of Cyclic Codes," Coordinated Science Lab., University of Illinois, Report R-285, 1966.

[8] J. Olsen, R. Scholtz, and L. Welch, "Bent-function Sequences," *IEEE Transactions on Information Theory*, vol. 28, no. 6, pp. 858–864, 1982.

[9] B. Z. Kamaletdinov, "Optimal Sets of Binary Sequences," *Problems of Information Transmission*, vol. 32, no. 2, pp. 39–44, 1996.

[10] J. J. Rushanan, "Weil Sequences: A Family of Binary Sequences with Good Correlation Properties," in *2006 IEEE International Symposium on Information Theory*, 2006, pp. 1648–1652.

[11] O. Moreno and A. Tirkel, "New Optimal Low Correlation Sequences for Wireless Communications," in *Sequences and Their Applications – SETA 2012*, T. Helleseth and J. Jedwab, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 212–223.

[12] K. Gurumurty, D. TirumalaRao, and G. ManmadhaRao, "Performance of Modified Jacobi Sequences with Good Merit Factor," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 3, no. 5, pp. 17–24, 2014.

[13] H. Zhang, R. Li, J. Wang, Y. Chen, and Z. Zhang, "Reed-Muller Sequences for 5G Grant-Free Massive Access," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, 2017, pp. 1–7.

[14] M. K. Song, G. Kim, H.-Y. Song, and K. W. Song, "Punctured Bent Function Sequences for Watermarked DS-CDMA," *IEEE Communications Letters*, vol. 23, no. 7, pp. 1194–1197, 2019.

[15] N. Y. Yu, "Binary Golay Spreading Sequences and Reed-Muller Codes for Uplink Grant-Free NOMA," *IEEE Transactions on Communications*, vol. 69, no. 1, pp. 276–290, 2021.

[16] D. Zhang and T. Helleseth, "Sequences With Good Correlations Based on Circular Florentine Arrays," *IEEE Transactions on Information Theory*, vol. 68, no. 5, pp. 3381–3388, 2022.

[17] P. V. Kumar, D. Dharmappa, and S. Mishra, "Interleaved Z4-Linear Sequences With Low Correlation for Global Navigation Satellite Systems," *IEEE Transactions on Information Theory*, vol. 70, no. 3, pp. 2224–2253, 2024.

[18] L. Welch, "Lower Bounds on the Maximum Cross Correlation of Signals," *IEEE Transactions on Information Theory*, vol. 20, no. 3, pp. 397–399, 1974.

[19] V. M. Sidelnikov, "On Mutual Correlation of Sequences," *Soviet Mathematics-Doklady*, vol. 12, pp. 197–201, 1971.

[20] P. Yue, J. An, J. Zhang, J. Ye, G. Pan, S. Wang, P. Xiao, and L. Hanzo, "Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1604–1652, 2023.

[21] R. Han, M. Liu, J. Wang, L. Bai, and J. Liu, "Anti-Jamming Strategy for Satellite Internet of Things: Beam Switching and Optimization," *IEEE Internet of Things Journal*, vol. 10, no. 23, pp. 20 254–20 263, 2023.

[22] H. Otay, K. Humadi, and G. K. Kurt, "Dark Side of HAPS Systems: Jamming Threats towards Satellites," in *2023 IEEE Future Networks World Forum (FNWF)*, 2023, pp. 1–6.

[23] V. S. R. Kantheti, C.-H. Lin, S.-C. Lin, and L. C. Chu, "Anti-Jamming Resilient LEO Satellite Swarms," in *MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM)*, 2023, pp. 77–82.

[24] B. Ren, H. Ge, G. Xu, and Y. Zhang, "Anti-Jamming Analysis and Application of Starlink System," in *2023 International Conference on Networking, Informatics and Computing (ICNETIC)*, 2023, pp. 149–151.

[25] E. R. Berlekamp, *Algebraic Coding Theory* . McGraw-Hill Inc.,USA, 1968.

[26] J. L. Massey, "Shift-Register Synthesis and BCH Decoding," *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, 1969.

[27] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," *Federal Information Processing Standards Publication 197*, 2001.

[28] E. Barker and J. Kelsey, "Recommendation for Random Number Generation Using Deterministic Random Bit Generators," *SP 800-90A Rev. 1, National Institute of Information Technology*, 2015.

[29] L. Kamrath, M. Baginski, and S. Martin, "Reduction of Doppler and Range Ambiguity Using AES-192 Encryption-Based Pulse Coding," *Sensors*, vol. 23, no. 5, 2023.

[30] M. Giordani and M. Zorzi, "Non-Terrestrial Networks in the 6G Era: Challenges and Opportunities," *IEEE network*, vol. 35, no. 2, pp. 244–251, 2020.

[31] H. Xie, Y. Zhan, G. Zeng, and X. Pan, "LEO Mega-Constellations for 6G Global Coverage: Challenges and Opportunities," *IEEE Access*, vol. 9, pp. 164 223–164 244, 2021.

[32] Z. Qu, G. Zhang, H. Cao, and J. Xie, "LEO Satellite Constellation for Internet of Things," *IEEE Access*, vol. 5, pp. 18 391–18 401, 2017.

[33] M. R. Dakkak, D. G. Riviello, A. Guidotti, and A. Vanelli-Coralli, "Evaluation of Multi-User Multiple-Input Multiple-Output Digital Beamforming Algorithms in B5G/6G Low Earth Orbit Satellite Systems," *International Journal of Satellite Communications and Networking*, 2023.

[34] A. Guidotti, A. Vanelli-Coralli, M. Conti, S. Andrenacci, S. Chatzinotas, N. Maturo, B. Evans, A. Awoseyila, A. Ugolini, T. Foggi, L. Gaudio, N. Alagha, and S. Cioni, "Architectures and Key Technical Challenges for 5G Systems Incorporating Satellites," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2624–2639, 2019.

[35] X. Zhai, L. Xiao, T. Ding, J. Zhou, P. Xiao, and T. Jiang, "Golden Angle Modulation Aided Differential OFDM-IM for LEO Satellite Communications," *IEEE Communications Letters*, vol. 28, no. 7, pp. 1604–1608, 2024.

[36] A. Modenini and B. Ripani, "A tutorial on the tracking, telemetry, and command (TT&C) for space missions," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1510–1542, 2023.

[37] M. Elia, G. Morgari, and M. Spicciola, "On Binary Sequences Generated by Self-clock Controlled LFSR," in *19th International Symposium on Mathematical Theory of Networks and Systems – MTNS 2010*, 2010, pp. 1275–1281.

[38] J. Daemen and V. Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard," *Springer*, 2002.

[39] J. L. Massey and T. Mittelholzer, "Welch's Bound and Sequence Sets for Code-Division Multiple-Access Systems," in *Sequences II: Methods in Communication, Security and Computer Sciences*. Springer, 1993, pp. 63–78.

[40] O. B. Wojuola and S. H. Mneney, "Performance of Even- and Odd-Degree Gold codes in a Multi-User Spread-Spectrum System," in *4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems (VITAE)*, 2014.

[41] ——, "Multiple-Access Interference of Gold Codes in a DS-CDMA System," *SAIEE African Research Journal*, vol. 106, no. 1, pp. 4–10, 2015.

[42] ITU, "Propagation Data Required for the Design Systems in the Land Mobile-Satellite Service." *ITU-R Recommendation P.681-11*, 2019.

[43] CCSDS, "TC Synchronization and Channel Coding," *Blue Book 231.0-B-4*, 2021.

[44] M. Baldi, M. Bertinelli, F. Chiaraluce, P. Closas, P. Dhakal, R. Garello, N. Maturo, M. Navarro, J. M. Palomo, E. Paolini, S. Pfletschinger, P. F. Silva, L. Simone, and J. Vilà-Valls, "State-of-the-art Space Mission Telecommand Receivers," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 6, pp. 4–15, 2017.