Optimal Compromise among Security, Availability and Resources in the Design of Sequences for GNSS Spreading Code Authentication

Nicola Laurenti and Anna Poltronieri
Department of Information Engineering
University of Padova
Padova, Italy
email:nil@dei.unipd.it, anna.poltronieri92@gmail.com
ORCID 0000-0001-7592-1929

***Abstract*—Spreading code authentication has been proposed as a promising countermeasure against signal layer spoofing attacks to GNSS. It consists in replacing part of the spreading code with a secret, cryptographically generated sequence, that is also provided to legitimate receivers, allowing them to verify the signal authenticity and integrity. Different techniques and formats have been proposed, yet their formulation is typically given as a particular solution, lacking proper generality.**

This paper aims at providing a unified general model for the design, description, evaluation and comparison of such techniques, introducing simple performance and security metrics, abstracting from the particular cryptographic mechanisms required to generate the sequences. We derive a way to optimize the trade-offs between security level and signal availability to receivers that do not know the modified code, and between security level and required cryptographic resources.

We also propose a simpler mechanism that closely approaches the optimal trade-off, and show that it significantly outperforms existing and proposed techniques, especially in the typically considered performance range. Finally, we evaluate the robustness of the proposed schemes to a partial observation of the transmitted modified code by the attacker.

***Index Terms*—authentication, integrity protection, spreading codes, information entropy, satellite navigation systems global navigation satellite systems, Global Positioning System**

I. Introduction

Given the ever increasing number of applications that make use of open service (civil) GNSS signals for position, navigation or timing purposes, and hence the growing financial or terrorist incentives for attacking them, the authenticity and integrity protection of such signals has become of paramount importance. A solution that has recently been adopted in the European Galileo system, to ensure that transmitted information is received authentic and integral, is to provide navigation message authentication (NMA) via cryptographic mechanisms; however, this is not sufficient by itself, as other spoofing attacks, such as meaconing or selective delay attacks, can be carried out at the signal layer without attempting to forge or modify the navigation message. Even introducing unpredictable symbols into the navigation message, to make it more difficult for an attacker to produce a spoofed signal bearing the same message in real time, is not a definitive solution, since secret code estimation and replay (SCER) attacks have been shown to be quite effective at reproducing a valid message under favorable conditions for the attacker [1], [2].

A possible solution to offer signal authentication was proposed in several distinct fashions in [3], [4], [5], [6], [7], [8] called *spreading code authentication* (SCA) and consists in partially encrypting the PRN spreading code of each SV. That is, in replacing the publicly known open code with a new code which coincides with it for a large part, whereas it is unpredictably modified for a small number of the chips. The limitation on the amount of modified chips stems from the need to maintain a significant correlation peak value between the received authenticated signal and the original code, either to ensure PNT service availability for legacy receivers that will not perform signal verification [5], [6], or because the cryptographic seeds needed to generate the encrypted code for verification are derived from the demodulated navigation message data, in a delayed authentication fashion [7], [8]. In fact, those receivers will correlate the received signal with the open code and if the peak does not exhibit a significant loss with respect to that in the autocorrelation of the open code, the receiver can still acquire and track the signal, although a slightly higher C/N_0 will be necessary for lock-in.

Clearly there is a trade-off to be chosen, in the design of such schemes, as reducing the correlation loss and increasing the encrypted code unpredictability are conflicting objectives, depending in opposite ways on the number of chips that remain equal between the two codes. Moreover, the amount of secure information that needs to be cryptographically generated and shared among the receivers to reconstruct the encrypted code is itself a cost that increases with the encrypted code unpredictability, so that the designer also faces a security vs efficiency trade-off.

In the literature, the performances of SCA mechanisms have been evaluated in terms of correlation loss and resilience to an attack that plainly replicates the open code. In this paper, we approach the problem from a general point of view and aim to derive the optimal trade-off among correlation,

unpredictability and amount of information to be disclosed.

The paper is organized as follows. In Section II we formulate the general model of SCA and introduce the performance and security metrics that will be employed in the design trade-off. In Section III we derive the optimal design in terms of the defined trade-offs, and also propose a suboptimal design that calls for a simpler implementation, yet is asymptotically optimal in the infinite block length limit. In Section IV we provide analytical expressions for the security and performance metrics of the proposed schemes and the available literature solutions and compare them with numerical results. Then, we evaluate the robustness of the presented schemes with respect to partial observations by the attacker in Section V, and finally we draw conclusions in Section VI.

II. System model

A. General model and examples

We consider that a block $\boldsymbol{c} = [c_1, \ldots, c_L]$ of L contiguous chips $c_i \in \{0, 1\}$ from the publicly known open PRN code for SV_n is overwritten by a new block $\boldsymbol{c}' = [c'_1, \ldots, c'_L]$, randomly generated, according to some probability distribution $p_{\boldsymbol{c}'|\boldsymbol{c}}$.

For instance, in the *time division* scheme [3], [4], a subset of the chips, corresponding to a predetermined set of indices $\mathcal{I} = \{i_1, \ldots, i_k\} \subset \{1, \ldots, L\}$ are replaced by k secret, cryptographically generated bits $[d_1, \ldots, d_k]$, that is

$$c'_i = \begin{cases} c_i & , \ i \notin \mathcal{I} \\ d_j & , \ i = i_j \in \mathcal{I} \end{cases} \tag{1}$$

Ideally, in the random oracle security model, the bits $[d_1, \ldots, d_k]$ would be independent and uniformly distributed, so the conditional probability distribution $p_{\boldsymbol{c}'|\boldsymbol{c}}$ would be $p_{\boldsymbol{c}'|\boldsymbol{c}}(\boldsymbol{a}|\boldsymbol{b}) = 1/2^k$ for the 2^k pairs $(\boldsymbol{a}, \boldsymbol{b})$ with $a_i = b_i, \forall i \notin \mathcal{I}$.

On the other hand, in the *time hopping* scheme as introduced in [4], [5] the index set $\mathcal{I}$ is itself cryptographically generated, to make $\boldsymbol{c}'$ even less predictable and offer an increased robustness against denial of service attacks [9], [10]. Ideally, the index set $\mathcal{I}$ is uniformly chosen among all the combinations of k distinct indices from $\{1, \ldots, L\}$, whereas the k bits $[d_1, \ldots, d_k]$ are chosen independently of each other and of $\mathcal{I}$, so that we can write

$$p_{\boldsymbol{c}'|\boldsymbol{c}}(\boldsymbol{a}|\boldsymbol{b}) = \frac{1}{2^k} \frac{\binom{L-d_{\mathrm{H}}(\boldsymbol{a},\boldsymbol{b})}{k-d_{\mathrm{H}}(\boldsymbol{a},\boldsymbol{b})}}{\binom{L}{k}} \tag{2}$$

where $d_{\mathrm{H}}(\boldsymbol{a}, \boldsymbol{b})$ is the number of different chip values (Hamming distance) between $\boldsymbol{a}$ and $\boldsymbol{b}$. Typically, the index set $\mathcal{I}$ is represented through a separate bit sequence from the chip values $[d_1, \ldots, d_k]$.

An approach similar to time hopping, yet with a limited variability of the index set $\mathcal{I}$, is adopted in the Chimera scheme for authentication of the GPS L1C signal. In the initial proposal [7], analyzed in [11], for each block of $L = 33$ chips ("marker frame") the set $\mathcal{I}$ (of "marker locations") is randomly chosen from a list of $M = 512$ predetermined k-ples patterns with either $k = 3$ or $k = 4$, whereas $[d_1, \ldots, d_k]$ (the "marker values") are separately generated. In the more recent version [8], each "sector" of $L = 1023$ chips is divided into 31 "segments" of 33 consecutive chips and the set $\mathcal{I}$ of "marker locations" is made of n segments, with $n \in \{1, \ldots, 7\}$ governing the unpredictability vs correlation trade-off, except that chip locations $\{0, 4, 6, 29\}$ in each segment are not included in $\mathcal{I}$. Therefore, $k = 29n$ and $\mathcal{I}$ is uniquely determined by identifying the n segments out of 31 that make it, while the marker values $[d_1, \ldots, d_k]$ are separately determined.

B. Security and performance metrics

The unpredictability of the signed code from the point of view of a spoofing adversary should be evaluated taking into account that the public code is known, and is thus measured by the conditional guessing probability

$$P_{\mathrm{g}}(\boldsymbol{c}'|\boldsymbol{c}) = \sum_{\boldsymbol{b}} \max_{\boldsymbol{a}} p_{\boldsymbol{c}'|\boldsymbol{c}}(\boldsymbol{a}|\boldsymbol{b}) p_{\boldsymbol{c}}(\boldsymbol{b}) \tag{3}$$

or equivalently by the *guessing* (or *min-*) *entropy* [12]

$$H_{\min}(\boldsymbol{c}'|\boldsymbol{c}) = \log_{1/2} P_{\mathrm{g}}(\boldsymbol{c}'|\boldsymbol{c}) \quad \text{[bit]} \tag{4}$$

representing the security level (in bits) against a guessing attack. Note that using either (3) or (4) as a security measure means assuming that the verifying receiver can perfectly distinguish between the correct signed code block $\boldsymbol{c}'$ and any other L-bit sequence, and that the attacker has no other means to succeed than guessing the exact signed code sequence, with no prior information except knowledge of the public code. This represents an ideal situation, but it makes for a significant upper bound to the achievable security level by these solutions in the real world, and hence a useful design guideline. Also, it has the benefit of abstracting the analysis from the specific cryptographic mechanism used to generate the secret bits.

For those receivers that do not know the actual realization of $\boldsymbol{c}'$ prior to acquire the transmitted signal and will use the public open code $\boldsymbol{c}$ in generating the local replica, the correlation peak in the signal acquisition block will be proportional to the cross correlation between the blocks $\boldsymbol{c}$ and $\boldsymbol{c}'$

$$r_{\boldsymbol{c}\boldsymbol{c}'} = \sum_{i=1}^{L} (-1)^{c_i + c'_i} = L - 2d_{\mathrm{H}}(\boldsymbol{c}, \boldsymbol{c}') \tag{5}$$

which is itself a random variable. Thus we will evaluate the expected multiplicative loss in the correlation peak by the average correlation coefficient

$$\rho_{\boldsymbol{c}\boldsymbol{c}'} = \frac{\mathrm{E}\left[r_{\boldsymbol{c}\boldsymbol{c}'}\right]}{L} = 1 - 2\frac{\mathrm{E}\left[d_{\mathrm{H}}(\boldsymbol{c}, \boldsymbol{c}')\right]}{L} \tag{6}$$

and will use this metric as a measure of the availability offered by the authentication system to this class of receivers.

Finally, the amount of cryptographic resources (number of secure bits) that are needed to represent the actual choice of $\boldsymbol{c}'$, it is given by the $\log_2$ of the number of probable sequences, also called the conditional *Hartley* (or *max-*) *entropy* [12]

$$H_0(\boldsymbol{c}'|\boldsymbol{c}) = \log_2 \max_{\boldsymbol{b}} \left|\left\{\boldsymbol{a} \,:\, p_{\boldsymbol{c}'|\boldsymbol{c}}(\boldsymbol{a}|\boldsymbol{b}) > 0\right\}\right| \tag{7}$$

Knowing that maximizing $H_{\min}(\boldsymbol{c}'|\boldsymbol{c})$ and $r_{\boldsymbol{c}\boldsymbol{c}'}$ for a given block length L are conflicting objectives, we seek a trade-off

between them, ideally achieving the maximum possible value of one while constraining the other, and *vice versa*.

Similarly, we seek a trade-off between maximizing $H_{\min}(\boldsymbol{c}'|\boldsymbol{c})$ and minimizing $H_0(\boldsymbol{c}'|\boldsymbol{c})$, as both entropies represent a measure of unpredictability, are maximized for $\boldsymbol{c}'$ uniform among all L-bit sequences independently of $\boldsymbol{c}$, and vanish for $\boldsymbol{c}'$ uniquely determined by $\boldsymbol{c}$.

III. Optimal trade-offs

In this section we derive the optimization of both trade-offs by following a general approach, then provide an explicit constructive procedure for applying it.

A. General necessary conditions for the optimal trade-offs

Lemma 1: The optimal trade-off between $H_{\min}(\boldsymbol{c}'|\boldsymbol{c})$ and $\rho_{\boldsymbol{c}'\boldsymbol{c}}$ can be sought among the strategies of the type[1]

$$\boldsymbol{c}' = \boldsymbol{c} \oplus \boldsymbol{x} \tag{8}$$

where:

1) $\boldsymbol{x}$ is a random L-bit string independent of $\boldsymbol{c}$;
2) in the distribution of $\boldsymbol{x}$, strings $\boldsymbol{\xi}$ with the same number of 1's (Hamming weight, $w_{\mathrm{H}}(\boldsymbol{\xi})$) are equally probable.

Proof: We prove that for any possible choice of $p_{\boldsymbol{c}'|\boldsymbol{c}}$ there is a distribution $p^{\star}_{\boldsymbol{c}'|\boldsymbol{c}}$ satisfying equation (8), points 1) and 2) in the statement, that yields the same average correlation and improves on the unpredictability (or at least maintains the same), thus achieving a better (or at least equal) trade-off.

In fact, since the average signal correlation depends only on the average Hamming distance, under $p_{\boldsymbol{c}'|\boldsymbol{c}}$ we have

$$\mathrm{E}\left[d_{\mathrm{H}}(\boldsymbol{c},\boldsymbol{c}')\right] = \sum_{\delta=0}^{L} \delta q_{\delta} \quad , \quad \text{with } q_{\delta} = \sum_{d_{\mathrm{H}}(\boldsymbol{a},\boldsymbol{b})=\delta} p_{\boldsymbol{c}\boldsymbol{c}'}(\boldsymbol{a},\boldsymbol{b}) \tag{9}$$

If we let $\boldsymbol{x}$ be as in points 1) and 2) with

$$p_{\boldsymbol{x}}(\boldsymbol{\xi}) = q_{\delta} / \tbinom{L}{\delta} \quad , \quad \forall \boldsymbol{\xi} \,:\, w_{\mathrm{H}}(\boldsymbol{\xi}) = \delta \tag{10}$$

and $p^{\star}_{\boldsymbol{c}'|\boldsymbol{c}}(\boldsymbol{a}|\boldsymbol{b}) = p_{\boldsymbol{x}}(\boldsymbol{a} \oplus \boldsymbol{b})$ according to (8), with $p^{\star}_{\boldsymbol{c}'|\boldsymbol{c}}$ we obtain

$$\mathrm{E}\left[d_{\mathrm{H}}(\boldsymbol{c},\boldsymbol{c}')\right] = \mathrm{E}\left[w_{\mathrm{H}}(\boldsymbol{x})\right] = \sum_{\boldsymbol{\xi}} w_{\mathrm{H}}(\boldsymbol{\xi}) p_{\boldsymbol{x}}(\boldsymbol{\xi}) = \sum_{\delta=0}^{L} \delta q_{\delta}$$

obtaining the same average Hamming distance as with $p_{\boldsymbol{c}'|\boldsymbol{c}}$. Moreover, since the distribution $p^{\star}_{\boldsymbol{c}'|\boldsymbol{c}}(\boldsymbol{a}|\boldsymbol{b})$ is obtained as the convex combination of the $p_{\boldsymbol{c}'|\boldsymbol{c}}(\boldsymbol{a}|\boldsymbol{b})$ corresponding to different $\boldsymbol{b}$, it increases its min-entropy. ∎

Observe that both the time division and time hopping schemes satisfy (8) and 1), and time hopping also satisfies 2).

Lemma 2: The optimal trade-off between $H_{\min}(\boldsymbol{c}'|\boldsymbol{c})$ and $H_0(\boldsymbol{c}'|\boldsymbol{c})$ is achieved with any distribution $p_{\boldsymbol{c}'|\boldsymbol{c}}$ that is uniform over its support.

Proof: Since the conditional guessing and Hartley entropy represent the conditional Rényi entropy of order 0 and ∞, respectively, by [12, Prop. 3] we have

$$H_0(\boldsymbol{c}'|\boldsymbol{c}) \geq H_{\min}(\boldsymbol{c}'|\boldsymbol{c}) \tag{11}$$

with equality if and only if $p_{\boldsymbol{c}'|\boldsymbol{c}}(\boldsymbol{a}|\boldsymbol{b})$ is uniform over its support. Hence, this condition represents the best trade-off between maximizing $H_{\min}$ and minimizing H_0. ∎

Observe that time division satisfies uniformity of the distribution $p_{\boldsymbol{c}'|\boldsymbol{c}}(\boldsymbol{a}|\boldsymbol{b})$ over its support.

Theorem 1: For a fixed block length L, the optimal trade-offs

- between $H_{\min}(\boldsymbol{c}'|\boldsymbol{c})$ and $\rho_{\boldsymbol{c}'\boldsymbol{c}}$, and
- between $H_{\min}(\boldsymbol{c}'|\boldsymbol{c})$ and $H_0(\boldsymbol{c}'|\boldsymbol{c})$

are jointly achieved by the strategy (8), where $\boldsymbol{x}$ is uniformly distributed among the N binary strings with lowest Hamming weight, and N is the parameter governing the trade-off.

Proof: Follows from the lemmas above, and the fact that among all the uniform distributions over N distinct strings (yielding $P_{\mathrm{g}}(\boldsymbol{x}) = 1/N$), the expected Hamming weight is minimized by choosing the N lowest weight strings. ∎

B. Explicit procedures for the optimal trade-off

We outline two explicit procedures to achieve the optimal distribution, starting from a given block length L and a constraint either on the guessing probability or the correlation.

Procedure 1: given the length L and the constraint on the guessing probability $P_{\mathrm{g}} \leq P_{\max}$, the generation of the signed code block $\boldsymbol{c}'$ that minimizes the average Hamming distance (9) can be performed as follows:

1) let $N = \lceil 1/P_{\max} \rceil$;
2) build the set $\mathcal{N}$ of the N binary strings with lowest Hamming weight;
3) for every open code block $\boldsymbol{c}$ that needs to be authenticated, draw an independent and uniform $\boldsymbol{x}$ from $\mathcal{N}$;
4) let $\boldsymbol{c}' = \boldsymbol{c} \oplus \boldsymbol{x}$.

Procedure 2: given the length L and the constraint over the correlation loss $\rho_{\boldsymbol{c}\boldsymbol{c}'} \geq \rho_{\min}$, the generation of the signed code block $\boldsymbol{c}'$ that maximizes the guessing entropy can be performed as follows:

1) start with $k = \lfloor L(1-\rho_{\min})/2 \rfloor$;
2) compute $\rho_{\boldsymbol{c}\boldsymbol{c}'}$: if $\rho > \rho_{\min}$, increase k and repeat until a k is found such that $\rho_{\boldsymbol{c}\boldsymbol{c}'} \leq \rho_{\min}$;
3) let $N = \sum_{\delta=0}^{k} \binom{L}{\delta}$;
4) compute $\rho_{\boldsymbol{c}\boldsymbol{c}'}$; if $\rho_{\boldsymbol{c}\boldsymbol{c}'} < \rho_{\min}$, decrease N and repeat this step until the largest N such that $\rho \geq \rho_{\min}$ is found;
5) proceed as in steps 2)–4) of Procedure 1.

C. A suboptimal alternative

A suboptimal solution, which calls for a simpler implementation, is to still use (8) but choose $\boldsymbol{x}$ uniformly only among all the $\binom{L}{k}$ L-bit strings with Hamming weight k, where:

- $k = \lfloor L(1-\rho_{\min})/2 \rfloor$, if the constraint is set on the correlation coefficient $\rho_{\boldsymbol{c}\boldsymbol{c}'} \geq \rho_{\min}$
- k is the smallest integer for which $\binom{L}{k} \geq 1/P_{\max}$, if the constraint is set on the guessing probability $P_{\mathrm{g}}(\boldsymbol{c}'|\boldsymbol{c}) \leq P_{\max}$

Such solution is still optimal in the security vs resources trade-off, due to its uniformity, and is suboptimal in the security

[1] As customary, $\oplus$ denotes bitwise XOR between two binary strings

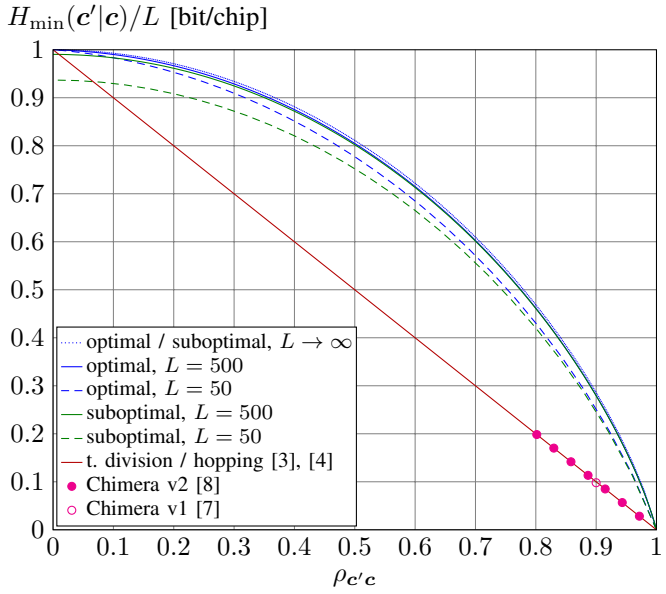

Fig. 1. Security vs availability trade-off: guessing entropy rate $H_{\min}(\boldsymbol{c}'|\boldsymbol{c})/L$ vs mean correlation coefficient $\rho_{\boldsymbol{c}\boldsymbol{c}'}$ for the existing and proposed solutions.

vs correlation trade-off, due to removing the lower weight sequences. However, it calls for a simple implementation, where independent uniform integers in $\{1, \dots, L\}$ are iteratively drawn until k different values are obtained. Also, it offers constant Hamming distance $d_{\mathrm{H}}(\boldsymbol{c}, \boldsymbol{c}') = k$ between public and secret code, which provides some margin for distinguishability even in a noisy channel scenario.

IV. Explicit expressions and numerical results

Let us derive expressions for the metrics and schemes described in Section II and Section III, and plot the results for the sake of comparison. In order to show general results applicable to any choice of the block length L, we plot entropies normalized by L, thus bounded in $[0, 1]$ and the correlation coefficient $\rho_{\boldsymbol{c}\boldsymbol{c}'}$.

For the optimal scheme with L chips and maximum Hamming distance k, let $N(L, k) = \sum_{i=0}^{k} \binom{L}{i}$; we get

$$P_{\mathrm{g}}(\boldsymbol{x}) = \frac{1}{N(L,k)} \quad , \quad H_{\min}(\boldsymbol{x}) = \log_2 N(L,k) \tag{12}$$

and

$$\mathrm{E}\left[w_{\mathrm{H}}(\boldsymbol{x})\right] = \sum_{i=0}^{k} i \binom{L}{i} = L \frac{N(L-1,k-1)}{N(L,k)} \tag{13}$$

which are represented by the blue lines in Fig. 1, for different values of L and by varying the parameter k which governs the trade-off along each curve. It is interesting to also derive the asymptotic curve as $L \to \infty$, obtained by letting $k = [\alpha L]$ be a fixed fraction of L: by the asymptotic values [13]

$$N(L, \alpha L) \to 2^{L h_2(\alpha) - \frac{1}{2}\log_2 L + O(1)}$$
$$\mathrm{E}\left[w_{\mathrm{H}}(\boldsymbol{x})\right] \to \alpha L + o(L)$$

where $h_2(\alpha) = -\alpha \log_2 \alpha - (1-\alpha)\log_2(1-\alpha)$ is the binary Shannon entropy function, we get the asymptotic curve

$$\tfrac{1}{L} H_{\min}(\boldsymbol{x}) \to h_2((1-\rho)/2) \ . \tag{14}$$

Observe that the curves for a low $L = 50$, and even more for $L = 500$ tightly approach the asymptotic curve, which can thus be taken as representative for any practical length.

For the suboptimal scheme with L chips and Hamming distance k, we get

$$P_{\mathrm{g}}(\boldsymbol{x}) = \frac{1}{\binom{L}{k}} \quad , \quad H_{\min}(\boldsymbol{x}) = \log_2 \binom{L}{k} \quad , \quad w_{\mathrm{H}}(\boldsymbol{x}) = k \tag{15}$$

as represented by the green lines in Fig. 1. Observe that while the loss from the optimal scheme is significant for lower values such as $L = 50$, the asymptotic curve for $L \to \infty$ coincides with that for the optimal scheme, since [13]

$$\log_2 \binom{L}{[\alpha L]} \sim L h_2(\alpha) \ . \tag{16}$$

This shows that the suboptimal scheme is asymptotically optimal, i.e. it achieves optimality in the infinite block length limit, and is very close to optimal for $L = 500$ already.

In the time division scheme, we trivially have

$$P_{\mathrm{g}}(\boldsymbol{x}) = 1/2^k \quad , \quad H_{\min}(\boldsymbol{x}) = k \quad , \quad \mathrm{E}\left[w_{\mathrm{H}}(\boldsymbol{x})\right] = k/2 \tag{17}$$

and the same identical values hold for the time hopping, due to the fact that $P_{\mathrm{g}}(\boldsymbol{x}) = \max_{\boldsymbol{\xi}} p_{\boldsymbol{x}}(\boldsymbol{\xi}) = p_{\boldsymbol{x}}(\mathbf{0}) = 1/2^k$, so that both the time division and time hopping schemes exhibit the same poor trade-off between security and correlation, as shown in Fig. 1. While for time division this is obviously due to fixing the indices of possibly flipped chips to a small subset, for the time hopping scheme the poor guessing entropy is due to the statistics of $\boldsymbol{x}$ being distinctly nonuniform, with $\mathbf{0}$ (that is no chips flipped) being the most likely choice.

As an example case for comparison, consider a block length $L = 500$ chips, and a customary cross correlation $\rho_{\boldsymbol{c}\boldsymbol{c}'} = 0.9$. Then, all the existing schemes yield $H_{\min} = 50$ bit of security and a guessing probability $P_{\mathrm{g}} = 9 \cdot 10^{-16}$, while the optimal and suboptimal schemes we propose would both yield $H_{\min} = 140$ security bits with $P_{\mathrm{g}} = 9 \cdot 10^{-43}$.

As for the Chimera scheme in its first version [7], where $L = 33$ and the average Hamming weight is $\mathrm{E}\left[w_{\mathrm{H}}(\boldsymbol{x})\right] = L/20$ obtaining a correlation loss $\rho_{\boldsymbol{c}\boldsymbol{c}'} = 0.9$, the authors showed in [11] that $P_{\mathrm{g}}(\boldsymbol{x}) = 0.1062$ and $H_{\min}(\boldsymbol{x}) = 3.23$ bit, which gives the single point identified by the purple circle in Fig. 1. For the more recent version of Chimera [8], where $L = 1023$ and $k = 29n$, for $n = 1, \dots, 7$ as discussed in Section II, the expressions for $\rho_{\boldsymbol{c}\boldsymbol{c}'}$ and $P_{\mathrm{g}}(\boldsymbol{c}'|\boldsymbol{c})$ in terms of k are the same as for the general time hopping scheme, and the same poor performance in the trade-off is represented by the purple bullets (one for each value of n) in Fig. 1.

As regards the trade-off between security and cryptographic resources, that is between guessing and Hartley entropies, this is optimized (with the equality $H_{\min}(\boldsymbol{c}'|\boldsymbol{c}) = H_0(\boldsymbol{c}'|\boldsymbol{c})$) by the proposed schemes and time division, owing to their uniform distribution of $\boldsymbol{x}$, as shown by the blue line in Fig. 2.

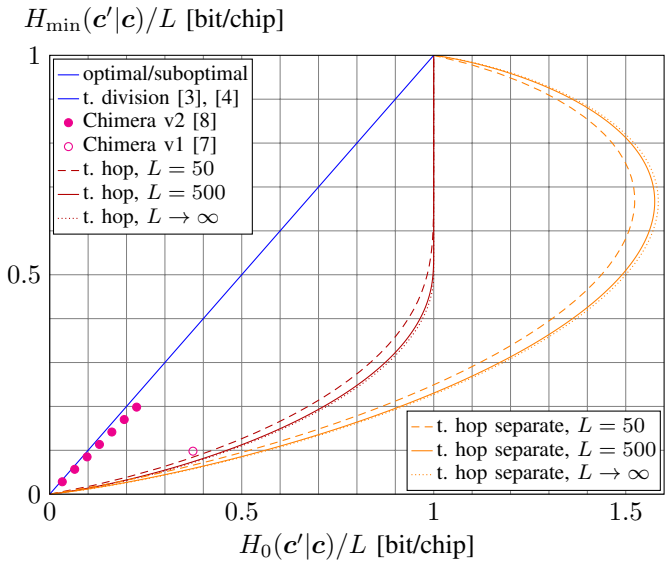

Fig. 2. Security vs resources trade-off: guessing entropy rate $H_{\min}(\boldsymbol{c}'|\boldsymbol{c})/L$ vs required secure bit rate $H_0(\boldsymbol{c}'|\boldsymbol{c})/L$ for the existing and proposed solutions.

On the contrary, the large non uniformity of the time hopping solution causes a mismatch

$$H_0(\boldsymbol{x}) = \log_2 N(L,k) > k = H_{\min}(\boldsymbol{x}) \tag{18}$$

representing a rather poor trade-off, as shown by the red curves in Fig. 2. Moreover, considering that in many implementations the bits for identifying the index set $\mathcal{I}$ and the chip values d_i are separately chosen, the number of required secure bits per chip (which is not an actual entropy) becomes

$$H_0'(\boldsymbol{x}) = \log_2 \binom{L}{k} + k > H_0(\boldsymbol{x}) \tag{19}$$

an even worse trade-off, shown by the orange curves.

As an example, in order to provide $H_{\min} = 100$ bits of security for a block of $L = 500$ chips, the proposed optimal schemes require to generate exactly $H_0 = 100$ secure random bits, while the time hopping scheme requires $H_0 = 357$ secure bits, and $H_0' = 457$ secure bits if positions and values are separately encoded.

For the first version of Chimera [7], since it employs on average $H_0'(\boldsymbol{x}) = \log_2 M + L/10 = 12.3$ secure bits per frame, the representation cost is also much larger than the guessing entropy, as shown by the purple circle in Fig. 2. On the contrary, the more recent version [8], owing to the rigid segment structure, only requires $H_0'(\boldsymbol{x}) = 5 + 4n + k$ secure bits per frame to specify the chosen sequence, and hence it is close to efficient in terms of cryptographic resources, as shown by the purple bullets in Fig. 2.

V. Robustness to Partial Observations by the Spoofer

In this section we consider the possibility that the attacker has observed part of the SCA authenticated signal before attempting to guess the secret code, thanks to a time advantage over the victim receiver. We assume that, due to a high C/N_0 condition, such observation allows him to exactly learn the value of the initial $\ell < L$ chips in block $\boldsymbol{c}'$, so that he only needs to guess the values of the remaining $L - \ell$ chips, and we evaluate the robustness of SCA schemes against this rather conservative hypothesis. A potential drawback in the schemes proposed in Section III is that since the distribution of $d_{\mathrm{H}}(\boldsymbol{c}', \boldsymbol{c})$ is more concentrated than in the time hopping scheme, the observation of i flips in the first ℓ chips may give the attacker enough information to significantly increase his probability of correctly guessing the remaining $L - \ell$ chips (e.g., if $i = k$, then there are no other flips in the remaining $L - \ell$ chips, or if $i = \ell + k - L$ then all the remaining chips must be flipped).

We denote by $\boldsymbol{c}_1'^{\ell} = [c_1', \ldots, c_\ell']$ the portion of signed code block that has been observed by the attacker, and by $\boldsymbol{c}_{\ell+1}'^{L} = [c_{\ell+1}', \ldots, c_L']$ the remaining chips he needs to guess. The residual unpredictability of $\boldsymbol{c}'$ can thus be measured by the conditional guessing probability of the unobserved chips given the knowledge of public code and observed signed chips

$$P_{\mathrm{g}}(\boldsymbol{c}_{\ell+1}'^{L}|\boldsymbol{c}, \boldsymbol{c}_1'^{\ell}) = \sum_{\boldsymbol{b},\boldsymbol{a}'} \max_{\boldsymbol{a}} p_{\boldsymbol{c}_{\ell+1}'^{L}|\boldsymbol{c},\boldsymbol{c}_1'^{\ell}}(\boldsymbol{a}|\boldsymbol{b},\boldsymbol{a}') p_{\boldsymbol{c},\boldsymbol{c}_1'^{\ell}}(\boldsymbol{b},\boldsymbol{a}') \tag{20}$$

or the corresponding guessing entropy $H_{\min}(\boldsymbol{c}_{\ell+1}'^{L}|\boldsymbol{c}, \boldsymbol{c}_1'^{\ell})$. In the assumption (8), the probability can be computed as

$$\begin{aligned} P_{\mathrm{g}}(\boldsymbol{x}_{\ell+1}^{L}|\boldsymbol{x}_1^{\ell}) &= \sum_{\boldsymbol{a}'} \max_{\boldsymbol{a}} p_{\boldsymbol{x}_{\ell+1}^{L}|\boldsymbol{x}_1^{\ell}}(\boldsymbol{a}|\boldsymbol{a}') p_{\boldsymbol{x}_1^{\ell}}(\boldsymbol{a}') \\ &= \sum_{\boldsymbol{a}'} \max_{\boldsymbol{a}} p_{\boldsymbol{x}}([\boldsymbol{a}', \boldsymbol{a}]) \\ &= \sum_{i} \max_{h} n(i,h,\ell) g(i+h) \end{aligned}$$

where $n(i,h,\ell)$ is the number of sequences $\boldsymbol{\xi}$ in the alphabet of $\boldsymbol{x}$ such that $w_{\mathrm{H}}(\boldsymbol{\xi}_1^{\ell}) = i$ and $w_{\mathrm{H}}(\boldsymbol{\xi}_{\ell+1}^{L}) = h$, while $g(\delta)$ is the value of $p_{\boldsymbol{x}}(\boldsymbol{\xi})$ when $w_{\mathrm{H}}(\boldsymbol{\xi}) = \delta$.

For the optimal trade-off scheme with maximum Hamming weight k , we have $g(\delta) = 1/N(L,k), \forall \delta \le k$ and $n(i,h,\ell) = \binom{\ell}{i}\binom{L-\ell}{h}$ for $i + h \le k$ so we obtain

$$P_{\mathrm{g}}(\boldsymbol{c}_{\ell+1}'^{L}|\boldsymbol{c}, \boldsymbol{c}_1'^{\ell}) = \frac{1}{N(L,k)} \sum_{i=0}^{\min\{\ell,k\}} \binom{\ell}{i} \tag{21}$$

whereas for the suboptimal scheme, with fixed Hamming weight $w_{\mathrm{H}}(\boldsymbol{\xi}) = k$, we have $g(k) = 1/\binom{L}{k}$, and $g(\delta) = 0$, $\forall \delta \neq k$ and $n(i,h,\ell) = \binom{\ell}{i}\binom{L-\ell}{h}$ for $i + h = k$ and $n(i,h,\ell) = 0$ otherwise, so we obtain

$$P_{\mathrm{g}}(\boldsymbol{c}_{\ell+1}'^{L}|\boldsymbol{c}, \boldsymbol{c}_1'^{\ell}) = \frac{1}{\binom{L}{k}} \sum_{i=\max\{0,\ell+k-L\}}^{\min\{\ell,k\}} \binom{\ell}{i} . \tag{22}$$

Finally, for the time hopping scheme, $g(\delta) = \binom{L-\delta}{k-\delta}/2^k$ and $n(i,h,\ell) = \binom{\ell}{i}\binom{L-\ell}{h}$ for $i + h \le k$, so we obtain

$$P_{\mathrm{g}}(\boldsymbol{c}_{\ell+1}'^{L}|\boldsymbol{c}, \boldsymbol{c}_1'^{\ell}) = \frac{1}{2^k \binom{L}{k}} \sum_{i=0}^{\min\{\ell,k\}} \binom{\ell}{i}\binom{\ell-i}{k-i} \tag{23}$$

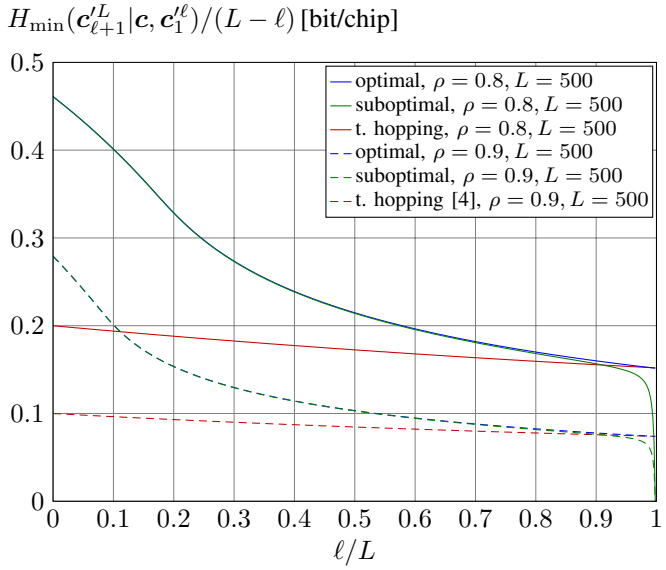

Fig. 3. Robustness to partial observation: residual guessing entropy rate $H_{\min}(c'_{\ell+1},\ldots,c'_{L}|\boldsymbol{c},c'_{1},\ldots,c'_{\ell})/(L-\ell)$ vs fraction ℓ/L of chips observed by the attacker. The curves for the optimal (blue) and suboptimal (green) scheme nearly overlap for the most part.

In Fig. 3 we plot the residual guessing entropy rate $H_{\min}(\boldsymbol{c}'^{L}_{\ell+1}|\boldsymbol{c},\boldsymbol{c}'^{\ell}_{1})/(L-\ell)$ vs the fraction ℓ/L of the signed block that has been observed by the attacker, for the three schemes considered, block length $L=500$, and two different values of the mean correlation coefficient $\rho_{\boldsymbol{c}\boldsymbol{c}'}=0.8, 0.9$. Observe that, as expected, while in the time hopping scheme the residual guessing entropy rate decreases linearly and very slowly with ℓ, such decrease is much sharper for the optimal and suboptimal schemes. However, the optimal scheme maintains a better security rate than time hopping for all ℓ, whereas the suboptimal scheme plunges to a negligible rate only when the signed block has been almost entirely observed. Hence, both schemes prove their robustness to this attack.

VI. Conclusions

In this work, we have introduced a general model of GNSS signal integrity protection through spreading code authentication (SCA), a technique also known as partial spreading code encryption. The model allows to evaluate and compare different schemes in terms of their offered security level (expressed by the guessing probability or entropy), availability to non authenticating receivers (in terms of cross correlation with the public open code) and representation efficiency (in terms of the Hartley entropy), while abstracting from specific implementation details.

A second main result of our paper is the derivation of a mechanism that achieves the best possible trade-off between security and availability, and between security and efficiency, by choosing the secret code uniformly among the N blocks that are closest to the open code. We have shown that such an optimal scheme improves significantly, in either trade-off or both, over existing proposals from the literature such as SSSC [3], Time Division and Time Hopping SAS [4], [6] or Chimera [7], [8], as those lack uniformity in choosing the secret code. We have also proposed a suboptimal solution that, while being amenable to a simpler implementation than the optimal, closely approaches the optimum performance, and asymptotically achieves it in the limit of infinitely long blocks.

Finally, we have explored the robustness of the existing and proposed schemes to partial error-free observation of the transmitted spreading code by an attacker that can exploit a time advantage with respect to the victim receiver. We observe that the superiority of our proposed schemes over the existing ones is preserved even in this conservative hypothesis.

In a critical view of our contribution, it should be noted that the security metric we employ is representative of an ideal model, with error free chip detection by the receiver and complete ignorance on the secret code by the attacker. However, our results provide significant bounds with respect to the performances that are actually achievable by each scheme in realistic scenarios, and thus represent relevant guidelines for a practical design. Introducing proper security metrics for the noisy channel and evaluating the achievable trade-offs in that context is our aim for upcoming work along this line of research.

References

[1] G. Caparra, N. Laurenti, R. T. Ioannides, and M. Crisci, "Improving Secure Code Estimation and Replay Attack and Detection on GNSS Signals," in *ESA NAVITEC*, Noordwijk, The Netherlands, Dec. 2014.

[2] G. Caparra, S. Ceccato, N. Laurenti, and J. Cramer, "Feasibility and Limitations of Self-Spoofing Attacks on GNSS Signals with Message Authentication," in *ION GNSS+*, pp. 3968–3984, 2017.

[3] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," in *ION GPS/GNSS*, pp. 1543–1552, 2003.

[4] O. Pozzobon, "Keeping the Spoofs Out. Signal Authentication Services for Future GNSS," *InsideGNSS*, vol. 6, no. 3, pp. 48-55, 2011.

[5] L. Scott, "Proving location using GPS location signatures: Why it is needed and a way to do it," in *ION GNSS*, vol. 4, pp. 2880–2892, 2013.

[6] B. Motella, D. Margaria, and M. Paonni, "SNAP: An authentication concept for the Galileo open service," in *IEEE/ION PLANS*, pp. 967–977, 2018.

[7] J. M. Anderson, *et al.*, "Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals," in *ION GNSS+*, pp. 2388–2416, 2017.

[8] Air Force Research Laboratory, Space Vehicles Directorate, Advanced GPS Technology Interface, *Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User Segment Interface*, Interface specification IS-AGT-100, 17 Apr. 2019

[9] G. Caparra, and J. T. Curran "On the Achievable Equivalent Security of GNSS Ranging Code Encryption," in *IEEE/ION PLANS*, pp. 956–966, 2018.

[10] D. Margaria, *et al.*, "Signal Structure-Based Authentication for Civil GNSSs: Recent Solutions and Perspectives," *IEEE Signal Processing Mag.*, vol. 34, no. 5, pp. 27–37, Sep. 2017.

[11] A. Poltronieri, G. Caparra, and N. Laurenti, "Analysis of the Chimera Time-Binding Scheme for Authenticating GPS L1C," in *ESA NAVITEC*, Dec. 2018.

[12] S. Fehr, and S. Berens, "On the Conditional Rényi Entropy," in *IEEE Trans. on Information Theory*, vol. 60, n. 11, pp. 6801–6810, Nov. 2014.

[13] D. Knuth, O. Patashnik, and R. Graham, *Concrete Mathematics*, Addison-Wesley, 1988.