Bent Sequences over Hadamard Codes for Physically Unclonable Functions

Patrick Solé, Wei Cheng, Sylvain Guilley, Olivier Rioul

Bent Sequences over Hadamard Codes for Physically Unclonable Functions

Patrick Solé*, Wei Cheng†, Sylvain Guilley‡†, and Olivier Rioul†
*I2M (Aix-Marseille Univ., Centrale Marseille, CNRS), Marseille, France, patrick.sole@telecom-paris.fr
†LTCI, Télécom Paris, Institut Polytechnique de Paris, Palaiseau, France, firstname.lastname@telecom-paris.fr
‡Secure-IC S.A.S., Tour Montparnasse, 33 avenue du Maine, 75015, Paris, France, sylvain.guilley@secure-ic.com

***Abstract*—We study challenge codes for physically unclonable functions (PUFs). Starting from the classical Hadamard challenge code, we augment it by one vector. Numerical values suggest that the optimal choice of this vector for maximizing the entropy is to pick a vector the farthest away from the code formed by the challenges and their binary complements.**

This leads us to study the covering radius of Hadamard codes. A notion of bent sequence that generalizes the classical notion from Hadamard matrices of Sylvester type to general Hadamard matrices is given. Lower bounds for Paley-type Hadamard matrices are given.

I. Introduction

Relying on the inherent imperfection of the fabrication process, physically unclonable functions (PUFs) [1] provide a practical solution to identify and authenticate integrated circuits. As a security primitive, PUFs provide more security compared to stored keys. As an example, since the static random values output of a PUF are re-generated at every boot, tampering attacks are avoided.

There are many constructions of PUFs and among them, the delay PUF formalizes several instances including Arbiter PUF [8], Ring-oscillator PUF [21] and Loop-PUF [5], etc. As in [17], [18], the delay PUF can be characterized by a stochastic model, in which all delays follow an i.i.d. Gaussian distribution. This model is validated experimentally, by Pelgrom coefficients [16]. Therefore, we can focus on the unified multivariate Gaussian model to characterize the properties of delay PUFs.

A given PUF outputs statically random values as responses to different challenges. The quality of randomness of the responses, measured by entropy, is important to assess the security of a PUF [3], [17]. The entropy depends on the choice of the challenges and relates to the entropy of the generated cryptographic key. Obviously, a large amount of entropy can be extracted from the PUF with many challenges [20]. However, it is still an open question how to maximize the entropy given a fixed number of challenges.

Previous works: An initial work [17] studied the sequence of challenges which make the entropy increase in a greedy fashion (where every new challenge added is the one that maximizes the overall entropy compared to the previous challenge code). For completeness, Fig. 1 reproduces Figure 4(b) of [17], which has been obtained by Monte-Carlo estimation using $100,000$ draws. This shows how entropy increases with the code size, featuring different regimes.

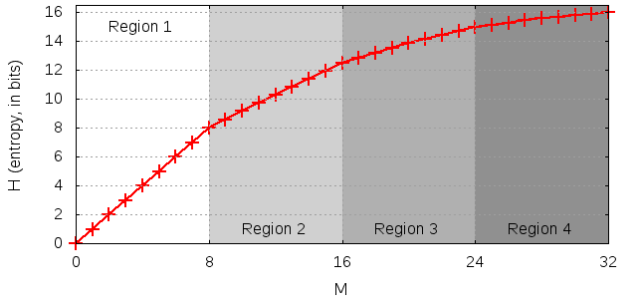

Fig. 1: Evolution of entropy when the number of challenges increases shown in Figure 4(b) of [17]. The entropy for $M > 8$ challenges is in fact slightly underestimated: For $M = 32$ challenges, the entropy reached in [17] is about 16 bits, whereas for 10 million draws, we found it closer to 18.2 bits. However, the identified challenges are the same in both cases.

Particularly interesting is the structure of the growing challenge codes: It is such that each region in Fig. 1 contains only orthogonal added challenges (codewords). As a result, it was conjectured in [17] that the greedy algorithm gives a challenge code consisting in the union of several Hadamard codes.

Contributions: The present work shows that the challenge codes which optimizes the entropy are governed by general properties of the codes rather than by a greedy construction (which is known to be suboptimal). In this paper, we propose a new method to choose one optimal challenge vector on top of a Hadamard code in order to maximize the entropy of the PUF responses.

First of all, we present several invariant properties of entropy under permutations on the challenge code. Next, we postulate that the new vector added to a Hadamard code maximizes the entropy when it minimizes the *total deviation* (maximum absolute value of the inner products against challenge codewords). Equivalently, this vector should reach the covering radius of the complemented challenge code ($\mathcal{C} \cup (-\mathcal{C})$ where $\mathcal{C}$ is the challenge code). Numerical simulation by Monte-Carlo estimation validates this theoretical postulate.

We find both lower and upper bounds on the covering radius of complemented Hadamard codes. We derive optimal vectors corresponding to the exact value of covering radius when the length n of the challenge code is at most 32. We then introduce the notion of bent sequence w.r.t. a general Hadamard matrix, which generalizes the classical notion of bent sequences for Sylvester-type Hadamard matrices. When n is a perfect square, optimal vectors added to the challenge

code are such bent sequences. Exact calculations in length 16 confirm their existence. Estimates of the total deviation are derived for the class of Paley Hadamard matrices.

Outline: The remainder of this paper is organized as follows. Section II introduces the delay PUF and challenge codes. Section III shows that the entropy is invariant to some permutations on challenge codes. Then Section IV is devoted to extend one more challenge upon the Hadamard code and Section V provides connections and numerics on bent sequences. The experimental results are in Section VI. Section VII concludes.

II. Preliminaries

We first introduce several definitions:

Definition 1 (Delay PUF [17]): *A* challenge c *is a vector of* n *control bits* $c = (c_1, c_2, \ldots, c_n) \in \{\pm 1\}^n$. *Let* Δ_1, Δ_2, $\ldots$, Δ_n *be i.i.d. zero-mean Gaussian variables characterizing the technological dispersion in a PUF. The* bit response *to challenge* c *is*

$$B_c = sign(c_1\Delta_1 + c_2\Delta_2 + \cdots + c_n\Delta_n) \in \{\pm 1\}, \quad (1)$$

Definition 2 (Challenge Code [17]): *A challenge* code $\mathcal{C}$ *is a set of* M n*-bit challenges that form a* (n, M) *binary code. We shall identify* $\mathcal{C}$ *with the* $M \times n$ *matrix of* ± 1*'s whose rows are the challenges.*

Definition 3 (Entropy of a PUF [17]): *The* M *codewords* c *and their complements* $-c$ *are used to challenge the PUF elements. The corresponding identifier is the* M*-bit vector*

$$B = (B_c)_{c\in\mathcal{C}} \quad (2)$$

and the entropy *of the PUF responses is* $H = H(B)$.

Definition 4 (Hadamard Matrix): *A* Hadamard matrix *of order* n *is any real matrix* H *of order* n *with entries* ± 1 *such that* $HH^T = nI$.

For $n > 2$, the integer n must be a multiple of 4. Hadamard conjectured in 1893 that Hadamard matrices exist for all such n's. There are many known constructions of Hadamard matrices [22]. In this paper, we will need the Hadamard matrix of Sylvester type defined for $n = 2^m$, $m > 0$, by $H_{uv} = (-1)^{<u.v>}$, for $u, v \in \mathbb{F}_2^m$ and related to the first order Reed-Muller code [13]. The construction of Paley type depends on quadratic residues over finite fields and is recalled in Section V-B.

Definition 5 (Hadamard Code): *Let* $\mathcal{C}$ *be a binary code of length* n *over the alphabet* $A = \{\pm 1\} \subset \mathbb{Q}$. *A* Hadamard code $\mathcal{H}$ *is a code of length* n *over* A *with* $|\mathcal{H}| = n$ *codewords that are pairwise orthogonal. Thus we can think of its codewords as the rows of a Hadamard matrix* $\mathbf{H}$ *of order* n. *The set of Hadamard codes of length* n *is denoted by* $\mathcal{H}_n$.

Definition 6 (Deviation): *The* deviation *of an arbitrary vector* $x \in A^n$ *from code* $\mathcal{C}$ *is defined as*

$$\theta(\mathcal{C}, x) = \max_{y\in\mathcal{C}} |\langle x, y\rangle| \quad (3)$$

where $\langle x, y\rangle$ *denote the standard inner product of* x *and* y. *It can be easily seen that* $\langle x, y\rangle = n - 2d(x, y)$ *where* $d(,)$ *denotes Hamming distance. The* total deviation *of the code* $\mathcal{C}$ *is then*

$$\theta(\mathcal{C}) = \min_{x\in A^n} \theta(\mathcal{C}, x). \quad (4)$$

We recall [17, Theorem 1] that the optimal choices for the first $M = n$ challenge codewords are given by a Hadamard matrix $\mathcal{C} = \mathcal{H}$ with entropy $H = n$ bits.

III. Impact of Equivalent Codes on Entropy

The entropy H depends on the joint distribution of Gaussian variables Δ_i or more precisely, on the joint probabilities of signs of the Gaussian variables $c_1\Delta_1 + c_2\Delta_2 + \cdots + c_n\Delta_n$ for all codewords c. As a result, we have the following

Lemma 1: *The entropy* H *of a PUF with challenge code* $\mathcal{C}$ *is fully determined by the Gram matrix* $\mathrm{cov}(\mathcal{C}) = \mathcal{C}\mathcal{C}^t$ *of inner products* $\{\langle x, y\rangle\}_{x,y\in\mathcal{C}}$.

Proof: The zero-mean Gaussian vector $\mathcal{C}\Delta$ where $\Delta = (\Delta_1, \Delta_2, \ldots, \Delta_n)^t \sim \mathcal{N}(0, \mathbf{I})$ is fully determined by its correlation matrix $\mathcal{C}\mathcal{C}^t$. Since B is vector of the signs of all components of $\mathcal{C}\Delta$, its distribution and, therefore, its entropy $H = H(B)$, is also fully determined by $\mathcal{C}\mathcal{C}^t$. ∎

Recall that an *equivalent code* is obtained from $\mathcal{C}$ by a serial of operations consisting of:

- an arbitrary permutation of the coordinate positions,
- in any coordinate position, multiplication by any non-zero scalars.

Here the code is defined over $A = \{\pm 1\}$, and we have the following

Lemma 2: *Equivalent challenge codes give the same entropy* H.

Proof: First consider a permutation P on coordinates. Each element $cov(\mathcal{C})_{ij}$ is obtained by scalar product of ith and jth codewords x and y. Assume $\mathsf{P}(x)$, $\mathsf{P}(y)$ be the permuted codewords, then $cov(\mathcal{C})'_{ij} = \langle \mathsf{P}(x), \mathsf{P}(y)\rangle = \langle x, y\rangle = cov(\mathcal{C})_{ij}$ for any i and j. Hence $cov(\mathcal{C})$ and entropy are invariant.

Second consider multiplication by a non-zero scalar, which can only be ± 1, in any coordinate position. Then trivially inner products are unchanged, so that $cov(\mathcal{C})$ and entropy are again invariant. ∎

Lemma 3: *Permuting the order of codewords gives the same entropy* H.

Notice that this amounts to applying any permutation on rows and columns of $cov(\mathcal{C})$, which leaves entropy invariant.

Proof: Permuting the order of codewords of $\mathcal{C}$ corresponds to a permutation of the components of B, which does not change $H = H(B)$. ∎

Lemma 4: *Replacing any codewords with their binary complements gives the same entropy* H.

Proof: Replacing one codeword $c \in \mathcal{C}$ by $-c$ corresponds to replacing B_c by $-B_c$ in the binary vector B, which does not change its entropy $H = H(B)$. ∎

IV. Extending One More Challenge and Bounds

As proven in [17, Theorem 1], the optimal choices for the first $M = n$ challenge codewords are given by a Hadamard matrix. At the next $(n + 1)$th step, instead of the greedy

(exhaustive) search, we propose a constructive approach for choosing the $M = n + 1$ codewords based on the smallest total deviation $\theta(\mathcal{C})$.

Basically, we postulate that the Hamming distance between $(n+1)$th codeword and $\mathcal{C}$ plays a role in entropy H, which connects to the deviation. The main conjecture is as follows.

Conjecture 1: *For $(n+1)$th codeword, minimizing the deviation gives the maximal entropy H.*

A. Deviation Bounds and Bent Sequences

Proposition 1 (Upper Bound): *If $\mathcal{C}$ is a code of length n over A, then its total deviation is bounded above as $\theta(\mathcal{C}) \leq n$.*

Proof: By the Cauchy-Schwarz inequality, $|\langle x, y\rangle|^2 \leq \|x\|^2\|y\|^2 = n^2$. ∎

An improved upper bound for Hadamard codes will be given in Corollary 1.

Theorem 1 (Lower Bound and Bent Sequence): *If $\mathcal{H}$ is a Hadamard code of length n, its total deviation is bounded below as $\theta(\mathcal{H}) \geq \sqrt{n}$. Equality occurs if and only if $|\langle x, h\rangle| = \sqrt{n}$ for all $h \in \mathcal{H}$. In that case, n is a perfect square, and the vector x achieving $\theta(\mathcal{H}) = \sqrt{n}$ is called a* bent sequence *w.r.t. the code $\mathcal{H}$.*

Proof: The codewords $h \in \mathcal{H}$ form an orthogonal basis of $\mathbb{R}^n$ and the decomposition of any $x \in A^n$ onto this orthogonal basis writes

$$x = \sum_{h\in\mathcal{H}} \frac{\langle x, h\rangle}{\|h\|^2} h \tag{5}$$

where $\|x\|^2 = \|h\|^2 = n$. Therefore,

$$n = \|x\|^2 = \sum_{h\in\mathcal{H}} \frac{|\langle x, h\rangle|^2}{n} \leq \theta(\mathcal{H})^2 \tag{6}$$

with equality if and only if $|\langle x, h\rangle| = \sqrt{n}$ for all $h \in \mathcal{H}$, which can occur only if $n = |\langle x, h\rangle|^2$ is a perfect square. ∎

If $n = 2^m$, and $\mathbf{H}$ is a Hadamard matrix of Sylvester type [13] then an x that is a bent sequence w.r.t. $\mathbf{H}$ induces a bent Boolean function X by $X(u) = x_u$ for all $u \in \mathbb{F}_2^m$.

B. Properties of Bent Sequences

In general, bent sequences are not balanced, in the sense that their Hamming weight is not equal to half their length.

Proposition 2: *If $\mathcal{H}$ is a Hadamard code of length n that contains the all-one vector, then its attached bent sequences have Hamming weight $\frac{n\pm\sqrt{n}}{2}$.*

Proof: Assume h is the all-one vector, and x is a bent sequence. Then $\langle x, h\rangle = \pm\sqrt{n} = \sum_{i=1}^n x_i = n - 2w_H(x)$. ∎

Definition 7 (Dual sequence): *If x is a bent sequence w.r.t. a Hadamard matrix $\mathbf{H}$ of order n, then $\langle x, h\rangle = \pm\sqrt{n}$ for all $h \in \mathcal{H}$ so that the sequence*

$$y = \frac{x\mathbf{H}^T}{\sqrt{n}} \in A^n. \tag{7}$$

We call y the dual sequence *of x. If $y = x$, we say that x is a* self-dual *bent sequence.*

Proposition 3: *If x is a bent sequence w.r.t. to a Hadamard matrix $\mathbf{H}$ of order n, then its dual sequence y is bent w.r.t. $\mathbf{H}^T$, and the dual sequence of y is x.*

Proof: By assumption $\mathbf{H}\mathbf{H}^T = \mathbf{H}^T\mathbf{H} = n\mathbf{I}$, implying $y\mathbf{H} = \sqrt{n}\cdot x \in A^n$, which shows both assertions. ∎

When $\mathbf{H}$ is the Sylvester matrix, we recover the standard notion and properties of the dual bent function introduced by Dillon under the name "Fourier transform" [7].

We now generalize the notion of direct product of bent functions. Recall that the *Kronecker product* of two vectors u and v of length n and m is the vector $u \otimes v$ of length nm defined by $(u \otimes v)_{(i,j)} = u_i v_j$. Similarly, the Kronecker product of two matrices U and V of respective orders n and m is the matrix $U \otimes V$ of order nm defined by

$$(U \otimes V)_{(i,j)(k,l)} = U_{ij}V_{kl}. \tag{8}$$

It is well-known and easy to check that the Kronecker product of Hadamard matrices is a Hadamard matrix [12].

Proposition 4: *If u and v are bent sequences w.r.t. the Hadamard matrices U and V then $u \otimes v$ is a bent sequence w.r.t. the Hadamard matrix $U \otimes V$.*

Proof: Let n and m be the respective orders of U and V. The result follows then because $\sqrt{n}\sqrt{m} = \sqrt{nm}$. ∎

V. Connections

A. Covering Radius

Recall that the *covering radius* of a code $\mathcal{C}$ is

$$r(\mathcal{C}) = \max_{x\in A^n} \min_{y\in\mathcal{C}} d_H(x, y). \tag{9}$$

Theorem 2: *Let $\mathcal{H}$ be a Hadamard code of length n. If $\mathcal{C} = \mathcal{H} \cup (-\mathcal{H})$, then $\theta(H) = n - 2r(\mathcal{C})$.*

Proof: Note first that for $x \in A^n$ and $y \in \mathcal{H}$ we have $|\langle x, y\rangle| = \pm\langle x, y\rangle = \langle x, \pm y\rangle$. Hence for fixed $x \in A^n$, we have: $\max\{|\langle x, y\rangle| \mid y \in \mathcal{H}\} = \max\{\langle x, y\rangle \mid y \in \mathcal{H} \cup -\mathcal{H}\}$. Since $\langle x, y\rangle = n - 2d_H(x, y)$, the result follows by definition of the covering radius. ∎

Corollary 1: *For $n \geq 8$ we have $r(\mathcal{C}) \geq n/4$ so $\theta(\mathcal{H}) \leq \frac{n}{2}$.*

Proof: The covering radius of any code is bounded below by its packing radius (a.k.a. error-correction capacity). If the code is not perfect then this bound can be augmented by one. Hence for the Hadamard code $\mathcal{C}$, of minimum distance $\frac{n}{2}$, the packing radius is

$$r(\mathcal{C}) \geq \left\lfloor \frac{n/2 - 1}{2} \right\rfloor = \left\lfloor \frac{n}{4} - \frac{1}{2} \right\rfloor = \frac{n}{4} - 1. \tag{10}$$

The result follows since the parameters of perfect binary codes (linear or not) are those of the Hamming codes and of the Golay code [13]. ∎

B. Hadamard Matrices of Paley Type

Let q be an odd prime power. Let χ be the quadratic character (Legendre symbol), defined on $\mathbb{F}_q$ by the relation

$$\chi(x) = \begin{cases} 0, & \text{for } x = 0, \\ 1, & \text{for } x = \square, \\ -1 & \text{for } x \neq \square \end{cases} \tag{11}$$

where $\square$ denotes an arbitrary quadratic residue of $\mathbb{F}_q$.

The Jacobsthal matrix Q is then defined as $Q_{xy} = \chi(y-x)$, where $x, y \in \mathbb{F}_q$. Next, we define a conference matrix as

$$\mathbf{C} = \begin{pmatrix} 0 & j \\ \pm j^T & Q \end{pmatrix}, \tag{12}$$

where j is the all-one row vector of length q.

If $q \equiv 3 \pmod 4$ (resp. $q \equiv 1 \pmod 4$) we choose the sign so that $\mathbf{C}$ is antisymmetric (resp. symmetric). With these notations $I_{q+1} + \mathbf{C}$ (resp. $\begin{pmatrix} I_{q+1} + \mathbf{C} & -I_{q+1} + \mathbf{C} \\ -I_{q+1} + \mathbf{C} & -I_{q+1} - \mathbf{C} \end{pmatrix}$), is a Hadamard matrix of order $q+1$ (resp. $2(q+1)$) [12, Chap. 18].

We need the Weil estimate for character sums

$$|\sum_{t \in \mathbb{F}_q} \chi(f(t))| \leq 2\sqrt{q} \tag{13}$$

for f any cubic polynomial with three distinct roots [10, Th. 11.23]. Assume first that $q \equiv 3 \pmod 4$. Label the rows and columns of C by $\infty \cup \mathbb{F}_q$. Consider the vector defined by $X_\infty = X_0 = 1$, and $X_t = \chi(f(t))$, where f is an arbitrary quadratic such that $(t-1)f(t)$ has three distinct roots. By definition

$$\theta(P, X) = \max_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} |\chi((y-x)f(y))|. \tag{14}$$

If x equals either one of the zeros of f, then the character sum reduces to $\sum_{t \in \mathbb{F}_q} \chi(h(t))$ with h of degree one, which is $= 0$ by [4, p. 9]. If not, by the Weil inequality, we see that the deviation of the code P attached to the rows of the Paley matrix and to the vector X is $\theta(P, X) \leq 2\sqrt{q}$ entailing a total deviation $\theta(P) \leq 2\sqrt{q}$. Hence,

$$r(P) \geq \frac{n - 2\sqrt{q}}{2}. \tag{15}$$

If $q \equiv 1 \pmod 4$, similarly, we obtain $r(P) \geq \frac{n-4\sqrt{q}}{2}$.

We summarize this discussion in the following theorem.

Theorem 3: *Let P be the code formed by the rows of a Paley matrix of order n, and $\mathcal{P} = P \cup -P$. Then*

- *if $q \equiv 3 \pmod 4$ then $r(\mathcal{P}) \geq \frac{n-2\sqrt{q}}{2}$;*
- *if $q \equiv 1 \pmod 4$ then $r(\mathcal{P}) \geq \frac{n-4\sqrt{q}}{2}$.*

C. Numerics

The following examples were computed in `Magma` [23]. The codes for n a power of 2 are linear, which allows us to use `Magma`'s `CoveringRadius` command. The upper bounds are $\lfloor \frac{n-\sqrt{n}}{2} \rfloor$, coming from $\theta(\mathcal{C}) \geq \sqrt{n}$.

- for $n = 8$ we have $r(\mathcal{C}) = 2$, $\theta(\mathcal{C}) = 4$.
- for $n = 12$, we have $3 \leq r(\mathcal{C}) \leq 4$. The lower bound is by Corollary 1. In fact the upper bound must be met by the arguments in [11, P. 120–121]. There are exactly 440 vectors at distance 4 from the code.
- for $n = 16$, we have in the Sylvester case $r(\mathcal{C}) = 6$, $\theta(\mathcal{C}) = 4$. Thus any x at distance 6 is a classical bent function. For the Hadamard matrix of index i in `Magma` database we get
  - for $i = 2$ the parameters $r(\mathcal{C}) = 5$, $\theta(\mathcal{C}) = 6$. Thus no bent sequence can exist.
  - for $i = 3$ the parameters $r(\mathcal{C}) = 5$, $\theta(\mathcal{C}) = 6$. Thus no bent sequence can exist.
  - for $i = 4$ the parameters $r(\mathcal{C}) = 6$, $\theta(\mathcal{C}) = 4$. Thus any of the 384 x's at distance 6 is a bent sequence in the sense of the preceding section.
  - for $i = 5$ the parameters $r(\mathcal{C}) = 6$, $\theta(\mathcal{C}) = 4$. Thus any of the 128 x's at distance 6 is a bent sequence in the sense of the preceding section.
- for $n = 20$, we have $5 \leq r(\mathcal{C}) \leq 7$. The lower bound is by Corollary 1. The upper bound is met with equality for all three possible Hadamard matrices of size 20. There are exactly 40128 vectors at distance 7 from the code.
- for $n = 24$, we have $8 \leq r(\mathcal{C}) \leq 9$. The lower bound is by the supercode lemma [6], upon observing that the linear span of $\mathcal{C}$ is the extended Golay code of minimum distance 8. The upper bound is met with equality. There are exactly 7040 vectors at distance 9 from the code.
- for $n = 28$, we have $7 \leq r(\mathcal{C}) \leq 11$. In fact, the upper bound is met with equality for the first 20 (out of 487 in total) Hadamard matrices of size 28. In addition, there are 2808 vectors at distance 11 from the code.
- for $n = 32$, we have $8 \leq r(\mathcal{C}) \leq 13$. The true value is $r(\mathcal{C}) = 12$ [2].
- for $n = 36$, we have $9 \leq r(\mathcal{C}) \leq 15$. If a bent sequence exists it will not be a bent function in the classical sense.

VI. Experimental Results

As shown in Lemma 1, the entropy of a delay PUF is determined by the Gram matrix of its challenge code $\mathcal{C}$. Let v be an added challenge codeword to the Hadamard code, then $\mathcal{C}$ has $M = n + 1$ codewords and

$$cov(\mathcal{C}) = \mathcal{C}\mathcal{C}^t = \begin{pmatrix} n\mathbf{I} & \mathbf{v} \\ \mathbf{v}^t & n \end{pmatrix} \tag{16}$$

where $\mathbf{I}$ is the identity matrix of size n and $\mathbf{v} = \mathcal{C}v^t$ is the vector of the scalar products between all codewords in the corresponding Hadamard code and v. With Lemma 4, we deduce that by changing sign of one vector in the Hadamard code does not change the entropy, and happens to only flip the sign of corresponding coordinate of $\mathbf{v}$ in $cov(\mathcal{C})$. Therefore, relying on Lemma 2, 3 and 4, both the signs and orders of values in $\mathbf{v}$ have no impact on entropy. Therefore, we take $\mathbf{v}$ with its sorted absolute values to classify all possible candidates for $(n+1)$th codeword.

In order to estimate the entropy, we utilize Monte-Carlo simulation with 10,000,000 draws. The results are as follows for $n \in \{8, 12, 16\}$.

A. Cases $n = 8$ and $n = 12$

Taking $n = 8$, there is only one Hadamard code $\mathcal{C}$ and excluding these codewords in $\mathcal{C} \cup -\mathcal{C}$ gives 240 candidates for the extended one. As expected, all 240 candidates[1] are classified into two classes according to two possibilities of $\mathbf{v}$ as shown in Fig. 2. In particular, 112 candidates correspond to $\theta(\mathcal{C}) = 4$.

[1]All candidates are indexed in lexicographical order in the sequel.

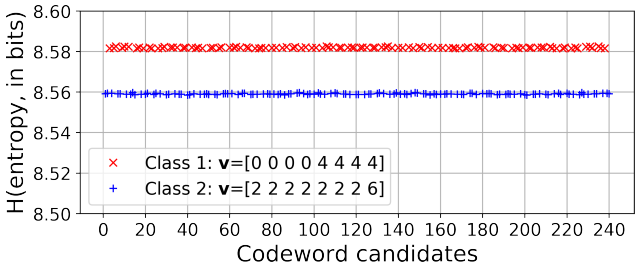

Fig. 2: Expanding one codeword when $n = 8$.

When $n = 12$, there is also only one Hadamard code [17]. All other 4072 candidates for 13th codeword are classified into four cases with different $\mathbf{v}$. The evaluation results are shown in Fig. 3. Particularly, 440 candidates are with $\theta(\mathcal{C}) = 4$.

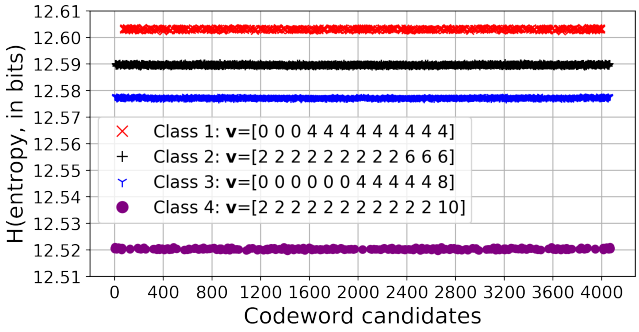

Fig. 3: Four classes of candidates when $n = 12$.

B. Case $n = 16$

We take the fifth Hadamard code in `Magma` database for $n = 16$, which is of our interest for bent sequences. As shown in Fig. 4, all 65504 candidates are classified into nine classes and the corresponding values of $\mathbf{v}$ is shown as in Tab. I.

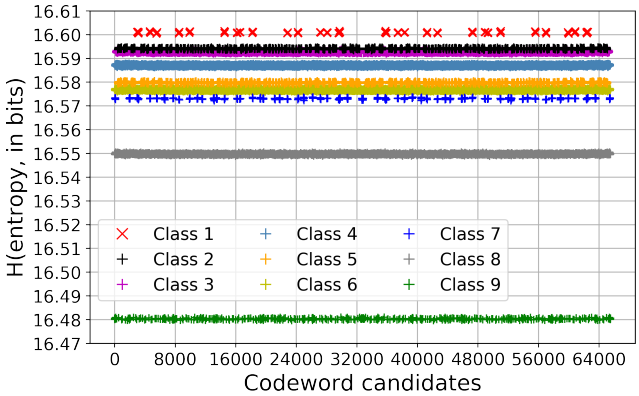

Fig. 4: Nine classes of candidates when $n = 16$.

As highlighted in Fig. 4, all 128 bent sequences with deviations equal to 4 give the maximal entropy. Similarly, there are 384 bent sequences giving the maximal entropy if the fourth Hadamard code is used (see Section V-C).

C. Marginal entropy

We show in Fig. 2, 3 and 4 that the next codeword v which maximizes the entropy is the one with $\theta(\mathcal{C}, v) = \theta(\mathcal{C})$. Moreover, we show in Fig. 5 the marginal entropy, which is

TABLE I: Classifying codeword candidates with $n = 16$.

	$\mathbf{v}$ (up to coordinate sign & sorting)	$\theta(\mathcal{C}, v)$	#Candidates
Class 1	[4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4]	**4**	**128**
Class 2	[0 0 0 4 4 4 4 4 4 4 4 4 4 4 4 8]	8	3072
Class 3	[2 2 2 2 2 2 2 2 2 2 6 6 6 6 6 6]	6	14336
Class 4	[0 0 0 0 0 0 4 4 4 4 4 4 4 4 8 8]	8	22272
Class 5	[0 0 0 0 0 0 0 0 0 4 4 4 4 8 8 8]	8	3072
Class 6	[2 2 2 2 2 2 2 2 2 2 2 6 6 6 10]	10	17920
Class 7	[0 0 0 0 0 0 0 0 0 0 0 8 8 8 8]	8	352
Class 8	[0 0 0 0 0 0 0 0 4 4 4 4 4 4 4 12]	12	3840
Class 9	[2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 14]	14	512

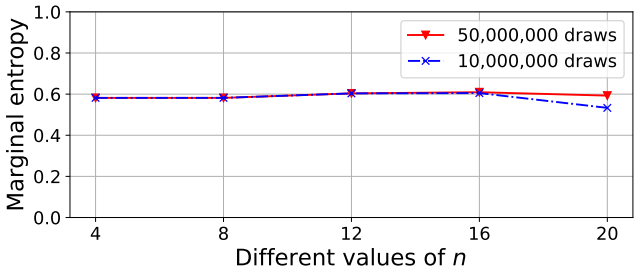

Fig. 5: Marginal entropy as n varies.

the increased entropy after extending challenge code with one more codeword. Interestingly, the optimal sequences give the similar marginal entropy when taking different n. Note that taking 10,000,000 draws underestimates the entropy, which results in the decrease in marginal entropy when $n = 20$.

VII. Conclusions

In this paper, we present the optimal choice of $M = n + 1$ challenges to a delay PUF, which gives the maximal entropy of responses. We highlight that the entropy of a delay PUF is determined by the Gram matrix of its challenge code. Relying on the Gram matrix, we show that the entropy is invariant to several code properties. Therefore, we present a method to classify all candidates for $(n + 1)$th challenge codeword into a very limited number of classes, although the total number of candidates is $2^n - 2n$, which is exponential in n.

Furthermore, we propose to use the (total) deviations as a selection metric. Specifically, we show that these optimal choices minimize the deviations to the total deviation on a Hadamard code and form bent sequences when n is a perfect square. The experimental results validate our findings that these optimal choices all lead to the maximal entropy.

In this work, we have used the same well-established PUF model as in [17], [18] where there is no dependency between challenge-response pairs. Furthermore, we considered a noiseless case where the response is not affected by internal or external noise. The model is arguably ideal and taking both noise and dependence of challenge-response pairs [19] into account is a topic for future investigation.

References

[1] S. Guilley, S. Hamaguchi, and Y. Kang, "ISO/IEC NP 20897. Information technology – Security techniques – Security requirements, test and evaluation methods for physically unclonable functions for

generating nonstored security parameters," https://www.iso.org/standard/76353.html.

[2] E. Berlekamp and L. Welch, "Weight distributions of the cosets of the (32,6) Reed-Muller code," *IEEE Transactions on Information Theory*, Vol. 18, No. 1, pp. 203–207, 1972.

[3] P. Tuyls, B. Skoric, T. Ignatenko, F. Willems, and G.-J. Schrijen, "Entropy estimation for optical pufs based on context-tree weighting methods," in *Security with Noisy Data*. Springer, 2007, pp. 217–233.

[4] B.C. Berndt, R.J. Evans, and K.S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society 21, Wiley (1998).

[5] Z. Cherif, J. Danger, S. Guilley, and L. Bossuet, "An easy-to-design PUF based on a single oscillator: The loop PUF," in *15th Euromicro Conference on Digital System Design, DSD 2012, Çeşme, Izmir, Turkey, September 5-8, 2012*. IEEE Computer Society, 2012, pp. 156–162. [Online]. Available: http://dx.doi.org/10.1109/DSD.2012.22

[6] G. D. Cohen, M. G. Karpovsky, H. F. Mattson Jr., and J. R. Schatz, "Covering radius—Survey and recent results," *IEEE Transactions on Information Theory*, Vol. 31, No. 3, pp. 328–343, 1985.

[7] J. F. Dillon, *Elementary Hadamard Difference Sets*, Ph.D. Thesis, University of Maryland, 1974.

[8] B. Gassend, D. E. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, Washington, DC, USA, November 18-22, 2002*, V. Atluri, Ed. ACM, 2002, pp. 148–160. [Online]. Available: http://doi.acm.org/10.1145/586110.586132

[9] D. Holcomb, W. Burleson, and K. Fu. "Power-Up SRAM state as an identifying fingerprint and source of true random numbers," *IEEE Trans. Computers*, Vol. 58, No. 9, pp. 1198–1210, Sept. 2009.

[10] H. Iwaniec, E. Kowalski, *Analytic number theory*, American Mathematical Society, 2004.

[11] J. H. van Lint, *Introduction to Coding Theory*, 3rd edition, Springer: Berlin, New-York, 1999.

[12] J. H. van Lint and R. Wilson, *A course in Combinatorics*, 2nd edition, Cambridge University Press, 2001.

[13] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Elsevier, Amsterdam, North Holland, 1977.

[14] S. Mesnager, *Bent functions, fundamentals and results*, Springer, Switzerland, 2016.

[15] K-U. Schmidt, "Asymptotically optimal Boolean functions," *J. Combin. Theory* Ser. A 164, pp. 50–59, 2019.

[16] M. J. Pelgrom, A. C. Duinmaijer, and A. P. Welbers, "Matching properties of MOS transistors," *IEEE Journal of Solid State Circuits*, Vol. 24, No. 5, pp. 1433–1439, 1989.

[17] O. Rioul, P. Solé, S. Guilley, and J. Danger, "On the entropy of physically unclonable functions," in *IEEE International Symposium on Information Theory, ISIT 2016, Barcelona, Spain, July 10-15, 2016*. IEEE, 2016, pp. 2928–2932. [Online]. Available: http://dx.doi.org/10.1109/ISIT.2016.7541835

[18] A. Schaub, O. Rioul, J.-L. Danger, S. Guilley, and J. Boutros, "Challenge Codes for Physically Unclonable Functions with Gaussian Delays: A Maximum Entropy Problem," *Adv. in Math. of Comm.*, 2019.

[19] A. Schaub, J.-L. Danger, O. Rioul, and S. Guilley, "The Big Picture of Delay-PUF Dependability," in *24th European Conference on Circuit Theory and Design*, September 7-10 2020, Sofia, Bulgaria.

[20] A. Schaub, O. Rioul, and J. J. Boutros, "Entropy estimation of physically unclonable functions via Chow parameters," in *57th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2019, Monticello, IL, USA, September 24-27, 2019*. IEEE, 2019, pp. 698–704. [Online]. Available: https://doi.org/10.1109/ALLERTON.2019.8919927

[21] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of the 44th Design Automation Conference, DAC 2007, San Diego, CA, USA, June 4-8, 2007*. IEEE, 2007, pp. 9–14. [Online]. Available: http://doi.acm.org/10.1145/1278480.1278484

[22] Horadam, K. J. *Hadamard matrices and their applications*. Princeton University Press, Princeton, NJ, 2007.

[23] University of Sydney (Australia). *Magma Computational Algebra System*. http://magma.maths.usyd.edu.au/magma/, Accessed on 2021-01-08.