# Linear Programming Bounds on the Kissing Number of q-ary Codes

Patrick Solé, Yi Liu, Wei Cheng, Sylvain Guilley, Olivier Riou

# Linear Programming Bounds on the Kissing Number of $q$-ary Codes

Patrick Solé*, Yi Liu†, 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 use linear programming (LP) to derive upper and lower bounds on the "kissing number" $A_d$ of any $q$-ary linear code C with distance distribution frequencies $A_i$, in terms of the given parameters $[n, k, d]$. In particular, a polynomial method gives explicit analytic bounds in a certain range of parameters, which are sharp for some low-rate codes like the first-order Reed-Muller codes. The general LP bounds are more suited to numerical estimates. Besides the classical estimation of the probability of decoding error and of undetected error, we outline recent applications in hardware protection against side-channel attacks using code-based masking countermeasures, where the protection is all the more efficient as the kissing number is low.**

## I. Introduction

The *kissing number* $A_d$ of a linear code is the number of nonzero codewords of minimum weight $d$. This fundamental invariant is the leading term in the well-known Bhattacharyya upper bound on the probability of decoding error on a binary symmetric channel BSC($p$) [1, § 6.8]

$$P_{de} \leq \sum_{i=d}^{n} A_i \gamma^i \sim A_d \gamma^d$$

as $p \to 0$, where $\gamma = 2\sqrt{p(1-p)}$. It is also the leading term in the probability of undetected error [2, Chap. 1]

$$P_{ue} = \sum_{i=d}^{n} A_i p^i (1-p)^{n-i} \sim A_d p^d (1-p)^{n-d}$$

as $p \to 0$. We are also motivated by a recent application to code-based masking as explained in the next section.

For a given minimum distance $d$, the kissing number can vary significantly as shown in Fig. 2. Therefore, the problem we consider is given the length, size, and minimum distance of a code, how to bound the kissing number above and below.

Building on MacWilliams formula of $q$-ary codes for Hamming weight enumerators [2, Chap. 5, Eq. (47)], we solve this problem by linear programming. This approach can be exploited numerically, using the linear programming solver of [4], or analytically via the polynomial method of [2, Chap. 17, Th. 20]. As shown in Tables I and II, for binary codes, the numerical method is more precise, while the polynomial method is useful to create insightful bounds with an explicit analytical expression.

The more general problem of bounding arbitrary weight frequencies is studied using similar techniques in [5]. However, the results in [5] are mostly asymptotic: it gives non-explicit asymptotic bounds on all weight frequencies. In Ashikhmin's work [11], he investigated the existence of codes whose kissing number satisfying an asymptotic lower bound. In the present paper we have strived to derive explicitly possibility bounds for any $q$-ary linear codes with given parameters $[n, k, d]$.

The material is arranged as follows. Section II motivates our study in terms of code-based masking. Section III collects the notions and notations needed for the rest of the paper. Section IV is devoted to the linear programming bounds and Section V to the polynomial method. Section VI applies the results to code-based masking. Section VII concludes the article and presents some open problems.

## II. Motivation

In the field of embedded cryptography, one attack strategy consists in the measurement and subsequent analysis of so-called side-channel emanations. In this kind of attack, the attacker aims at correlating measurements with internal sensitive values which depend on the secret key.

In order to mitigate this threat, the designer can implement countermeasures, such as random masking of sensitive values. One formalization of this is referred to as "code-based masking": the sensitive variable is encoded and added to a random mask which lives in a complementary set.

Several papers study cases where the sensitive data and the random mask encodings are linear. It can then be proved that the impact of the countermeasure depends on two properties of the dual of the masking code: its minimum distance $d$ and its kissing number $A_d$ [6].

Fig. 1 shows the impact of the kissing number on the security level in four cases of code-based masking, as measured by mutual information between side-channel leakage and the sensitive variables. It can be shown [6, Theorem 4] that the mutual information is asymptotically proportional to the code kissing number for large noise variance $\sigma^2$. From the defender's viewpoint, for a given minimum distance, the random masking is all the more secure as the kissing number is small. By contrast, from the attacker's viewpoint, the countermeasure is all the more breakable as the kissing number is large.

## III. Background

Let $C$ be a linear code over finite field $GF(q)$, with length $n$, size $M = q^k$ for some integer $k$, and minimal distance $d$. $q$ can be any prime power.

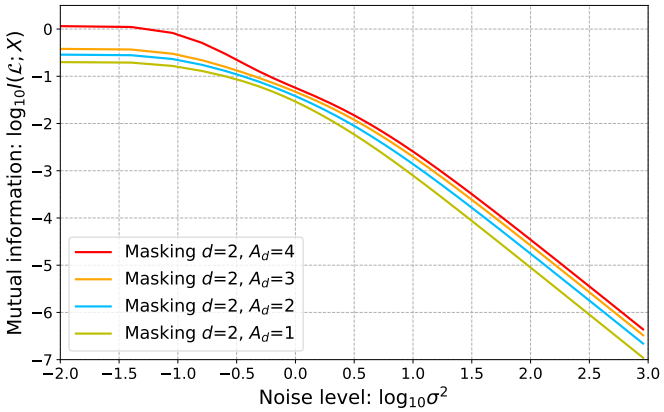


Fig. 1. The impact of the kissing number on information leakage [6].

We recall several known definitions on linear codes.

***Definition 1 (Hamming Weight [2, Chap 1, §3]):*** *The* Hamming weight*, or simply the weight, of a vector $x = (x_1, \cdots, x_n)$ is the number of nonzero $x_i$. It is denoted as $w_H(x)$.*

***Definition 2 (Weight Distribution [2, Chap 2, §1]):*** *If $C$ is an $(n, M, d)$ code, let $A_i$ be the number of codewords of Hamming weight $i$: $A_i = |\{x \in C \mid w_H(x) = i\}|$. The sequence $A_0, A_1, \ldots A_n$ is called the* weight distribution *of $C$.*

***Definition 3 (Dual Weight Distribution [2, Chap 5, §2]):*** *If $C$ is an $[n, k, d]$ linear code, let $A'_i$ be the number of codewords of its dual code of Hamming weight $i$: $A'_i = |\{y \mid w_H(y) = i \text{ and } x \cdot y = 0 \quad \forall x \in C\}|$. The sequence $A'_0, A'_1, \ldots A'_n$ is called the* dual weight distribution *of $C$.*

By definition, $A_0 = 1$, and

$$q^k = 1 + A_d + \sum_{j=d+1}^{n} A_j. \tag{1}$$

***Definition 4 (Krawtchouk Polynomial [2, Chap 5, §7]):*** *For any prime power $q$ and positive integer $n$, define the Krawtchouk polynomial*

$$P_k(x; n) = P_k(x) = \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{x}{j} \binom{n-x}{k-j} \tag{2}$$

*where $k = 0, 1, \ldots, n$.*

See [2, Chap 5, §7] for background on these polynomials, and [2, Chap 17, §4] for their use in the context of LP bounds.

For linear codes over $GF(q)$, by MacWilliams formula for q-ary codes [2, Chap. 5, Eq. (47)] we have $q^k \sum_{i=0}^{n} A'_i x^{n-i} y^i = \sum_{i=0}^{n} A_i (x + (q-1)y)^{n-i} (x-y)^i$, which means

$$q^k A'_i = \sum_{j=0}^{n} A_j P_i(j). \tag{3}$$

for all $i = 0, 1, \ldots, n$.

## IV. Linear Programming Bounds

To implement linear programming, we need the following theorem:

***Theorem 1 (Lower Bound on the Kissing Number):*** *If $C$ is an $[n, k, d]$ $q$-ary code then $A_d \geq q^k - 1 - \lfloor L \rfloor$, where $L$ denotes the maximum of $\sum_{j=d+1}^{n} A_j$ subject to the $2n - d$ constraints*

$$-P_i(0) - (q^k - 1)P_i(d) \leq \sum_{j=d+1}^{n} A_j (P_i(j) - P_i(d)) \tag{4}$$

*for $i = 1, 2, \ldots, n$, and $A_j \geq 0$ for $j = d+1, d+2, \cdots, n$.*

*Proof:* By definition of $A'_i$, we have $A'_i \geq 0$ for $i = 1, 2, \ldots, n$ which, from (3), reads $P_i(0) + A_d P_i(d) + \sum_{j=d+1}^{n} A_j P_i(j) \geq 0$. Substituting $A_d = q^k - 1 - \sum_{j=d+1}^{n} A_j$ gives (4). The Theorem is proved by using (1) again. ∎

We have a similar result for upper bounds.

***Theorem 2 (Upper Bound on the Kissing Number):*** *If $C$ is an $[n, k, d]$ $q$-ary code then $A_d \leq q^k - 1 - \lceil S \rceil$ where $S$ denotes the minimum of $\sum_{j=d+1}^{n} A_j$ under the same constraints as above.*

*Proof:* The proof is similar as Theorem 1, so it is omitted. ∎

Consider the $n$ inequality constraints (Eq.(4))

$$-P_i(0) - (q^k - 1)P_i(d) \leq \sum_{j=d+1}^{n} A_j (P_i(j) - P_i(d)).$$

for $i = 1, 2, \ldots, n$, along with the $n-d$ constraints $A_j \geq 0$ for $j = d+1, d+2, \cdots, n$. In this mathematical program, the $A_j$'s are considered as rational variables if linear programming is used, or integral variables if integer programming is intended. Both approaches can be tried in `Magma` [4].

The calculation result of the linear programming method is presented in Fig. 2 (on the next page). Here we focus on binary codes, and take different rates $R = \frac{k}{n}$ as different examples ($R \approx \frac{1}{2}$ and $R \approx \frac{1}{3}$), with $d$ being the best known for given parameters $[n, k]$. The LP bounds are represented for $n$ ranging from 3 to 16. We omit the cases when $k = 1$ because they are trivial situations with only two codewords. For some choices $[3, 2, 2]$, $[6, 3, 3]$, $[7, 4, 3]$, $[8, 4, 4]$, $[5, 2, 3]$, $[6, 2, 4]$, $[15, 5, 7]$ and $[16, 5, 8]$, the lower and upper bounds agree and the kissing number is necessarily unique.

However, in general, the lower and upper bounds do not agree, and it is possible to find actual codes with different kissing numbers between those bounds, as represented in light blue color in Fig. 2. The research has been carried out by randomly selecting linear codes of parameters $[n, k, d]$ and the range displayed in blue correspond to actually discovered codes amongst the ones we explored. Our search could not be exhaustive so that there might exist codes with lower or higher kissing numbers. Some exceptions are when:

- $[n, k, d] = [8, 4, 4]$ and $[16, 8, 5]$, as those are unique codes (extended Hamming code [2] and shortened QR code [2]). The uniqueness of the latter is proven in [9].

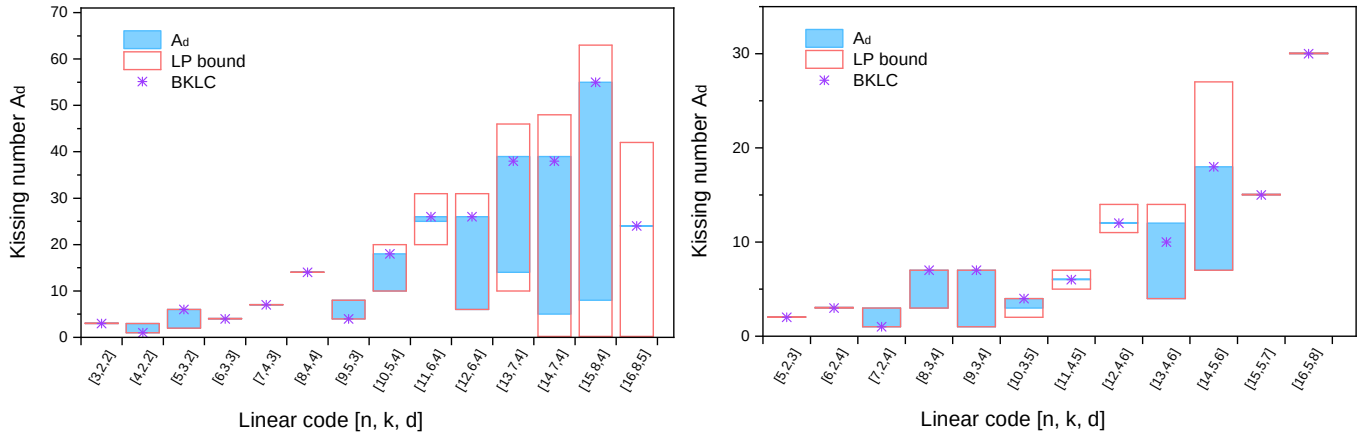


Fig. 2. Linear programming bounds on the kissing number for $R \approx 1/2$ (left) and $R \approx 1/3$ (right). Bounds are tight for $n = 3, 4, 5, 6, 7, 8, 9$ (left) and $n = 5, 6, 7, 8, 9, 15, 16$ (right).

- $[n, k, d] \in \{[3, 2, 2], [6, 3, 3], [7, 4, 3], [5, 2, 3], [6, 2, 4], [11, 4, 5], [12, 4, 6], [15, 5, 7], [16, 5, 8]\}$, as the room between lower and upper bounds is limited.

We also superimposed in Fig. 2 the special case of `Magma` Best Known Linear Code (BKLC). The function BKLC(n,d) returns a code with the largest known dimension, for a given length and minimum distance, consistently with Grassl database [8], which favors codes obtained by some algebraic construction. On several occasions, especially for rate $1/2$ codes, the kissing number of BKLC is relatively high, hence `Magma` is not adapted to applications requiring a small kissing number.

## V. Polynomial Method

The following identity is a polynomial way of expressing the duality of LP.

***Lemma 1 (Polynomial Method [7, Eq.(18)]):*** *Let $\beta(x) \in \mathbb{Q}[x]$ denote a polynomial with Krawtchouk expansion*

$$\beta(x) = \sum_{j=0}^{n} \beta_j P_j(x).$$

*The following identity holds*

$$\sum_{i=0}^{n} \beta(i) A_i = q^k \sum_{j=0}^{n} \beta_j A'_j. \tag{5}$$

*Proof:* Immediate by (3), upon swapping the order of summation. ∎

### A. Lower Bounds

Using Lemma 1 we have the following theorem. This theorem can also be obtained by setting appropriate parameters in [5, Thm 1].

***Theorem 3 (Lower Bound [5]):*** *Let $\beta(x) \in \mathbb{Q}[x]$ satisfying*

$$\begin{aligned} \beta_j &\geq 0, \forall j = 0, 1, \ldots, n, && (6)\\ \beta(x) &\leq 0, \forall x \in (d, n], && (7)\\ \beta(d) &> 0, && (8)\\ q^k \beta_0 &> \beta(0). && (9) \end{aligned}$$

*Then we have the lower bound*

$$A_d \geq \frac{q^k \beta_0 - \beta(0)}{\beta(d)}.$$

*Proof:* By Lemma 1 we have

$$\beta(0) + A_d \beta(d) + \sum_{i=d+1}^{n} \beta(i) A_i \geq q^k \beta_0 A'_0 = q^k \beta_0,$$

implying

$$\beta(0) + A_d \beta(d) \geq q^k \beta_0.$$

The last two inequalities come from the assumptions on $\beta(x)$. ∎

The main result of this paragraph are the following corollaries. First, we consider the case of $\beta$ linear.

***Corollary 1:*** *If $d = [(n-1)(q-1)/q]$, then*

$$A_d \geq \frac{q^k - nq + n - 1}{(n-d)q - n + 1}.$$

*Proof:* Take $\beta(x) = nq - n + 1 - qx$, where $P_1(x) = (q-1)n - qx$. By construction $\beta_0 = \beta_1 = 1$. Note that $\beta(0) = nq - n + 1$, and $\beta(d) = nq - n + 1 - qd$. We see that $\beta(x) \leq 0$, for $x$ an integer $\geq \frac{nq-n+1}{q}$. So in order to satisfied $\beta(x) \leq 0$, $\forall x \in (d, n]$, we must have $d + 1 \geq \frac{nq-n+1}{q}$. Combine with $\beta(d) > 0$ we have $(q-1)(n-1) \leq qd < (q-1)(n-1) + q$. Plugging this data into Theorem 3, the result follows. ∎

Next, we consider the case of $\beta$ a quadric.

***Corollary 2:*** *If $qd > nq - n - 2q + 1$ then*

$$A_d \geq \frac{q^{k-2} n(n - qn + qd + 2q - 1) - nd - n}{n - d}.$$

*Proof:* Assume $\beta = 1 + \beta_1 P_1(x) + \beta_2 P_2(x)$. Here $P_2(x) = \frac{q^2}{2} x^2 + \frac{q(q-2nq+2n-2)}{2} x + (q-1)^2 \binom{n}{2}$. To ensure the negativity of $\beta$ for $x \in (d, n]$ the simplest is to assume $\beta(d+1) = \beta(n) = 0$. This gives a system of two equations in $\beta_1, \beta_2$. The solution according to Wolfram alpha is

$$\beta_1 = \frac{nq - 2n - dq - 2q + 2}{n(n - qn + qd + 2q - 1)}, \beta_2 = \frac{-2}{n(n - qn + qd + 2q - 1)}.$$

This yields $\beta(d) = \frac{q^2(n-d)}{n(n-qn+qd+2q-1)}$, and $\beta(0) = \frac{q^2(d+1)}{(n-nq+qd+2q-1)}$. The result follows by Theorem 3. ∎

*Example:* Consider the binary code $C = RM(1,m)$, when $k = m+1$, and $d = 2^{m-1}$. It is well-known that $C$ is a two-weight code with $A_0 = A_{2^m} = 1$, and $A_{2^{m-1}} = 2^{m+1}-2$. Since $2d-n+3 > 0$, using Corollary 2 we have $A_d \geq 2^{m+1}-2$. So $RM(1,m)$ meets the lower bound.

*Remark:* For binary codes, if $n = 2d$, Corollary 2 always works better than Corollary 1. And if $n = 2d+1$, Corollary 2 works better if and only if $2^{k-1} \geq (n-d)$.

This result can be improved in some cases.

***Corollary 3:*** *If $C$ is a binary code and all weights of $C$ lie in the range [d, n-d], with distance $d < \frac{n}{2}$ and $(n-2d-1)^2 < n+1$, then*

$$A_d \geq \frac{2^{k-2}(n^2-4nd-3n)+(2^k+1)d(d+1)}{(2d-n)} - d - 1.$$

*Proof:* Because all weights of $C$ lie in the range [d, n-d], for a quadratic $\beta$, to ensure its negativity on the weights it is enough to assume $\beta(d+1) = \beta(n-d) = 0$. This gives a system of two equations in $\beta_1, \beta_2$, if we write $\beta = 1 + \beta_1 P_1(x) + \beta_2 P_2(x)$. The solution according to Wolfram alpha is

$$\beta_1 = \beta_2 = \frac{2}{n+1-(n-2d-1)^2}$$

This yields $\beta(d) = \frac{-4n+8d}{n^2-4nd-3n+4d^2+4d}$, and $\beta(0) = \frac{4(d^2+d-nd-n)}{n^2-4nd-3n+4d^2+4d}$. The result follows by Theorem 3. ∎

### B. Upper Bounds

Like Theorem 3, the following theorem can also be obtained by setting appropriate parameters in [5, Thm 1].

***Theorem 4 (Upper Bound [5]):*** *Let $\beta(x) \in \mathbb{Q}[x]$ satisfying*

$$\begin{aligned} \beta_j &\leq 0, \forall j = 1, \ldots, n, && (10)\\ \beta(x) &\geq 0, \forall x \in (d, n], && (11)\\ \beta(d) &> 0, && (12)\\ q^k \beta_0 &> \beta(0). && (13) \end{aligned}$$

*Then we have the upper bound*

$$A_d \leq \frac{q^k \beta_0 - \beta(0)}{\beta(d)}.$$

The proof is analogous to that of Theorem 3 and is omitted.

The main result of this paragraph are the following corollaries. First, we consider the case of $\beta$ linear.

***Corollary 4:*** *If $n - nq + 1 + qd > 0$, then*

$$A_d \leq \frac{q^k + nq - n - 1}{n - nq + 1 + qd}.$$

*Proof:* Take $\beta(x) = n - nq + 1 + qx$, where $P_1(x) = (q-1)n - qx$. By construction $\beta_0 = 1$, and $\beta_1 = -1$. Note that $\beta(0) = n - nq + 1$, and $\beta(d) = n - nq + 1 + qd$. We see that $\beta(x) > 0$, for $x$ an integer $> \frac{n-nq+1}{q}$. Plugging this data into Theorem 4, the result follows. ∎

Next, we consider the case of $\beta$ a quadric.

***Corollary 5:*** *If $d < \frac{(q-1)n+1}{q}$, then*

$$A_d \leq \frac{q^{k-2}n(qn-n-qd+1)+n(d-1)}{n-d}.$$

*Proof:* Assume $\beta = 1 - \beta_1 P_1(x) - \beta_2 P_2(x)$, with $\beta_1, \beta_2 > 0$. To ensure the positivity of $\beta$ for $x \in (d, n]$ the simplest is to assume $\beta(d-1) = \beta(n) = 0$. This gives a system of two equations in $\beta_1, \beta_2$. The solution according to `Magma` [4] is

$$\beta_1 = \frac{2n+dq-2-nq}{qn^2-n^2-qdn+n},\ \beta_2 = \frac{2}{qn^2-n^2-qdn+n}.$$

This yields $\beta(d) = \frac{q^2(n-d)}{qn^2-n^2-qdn+n}$, and $\beta(0) = \frac{q^2(1-d)}{qn-n-qd+1}$. The result follows by Theorem 4. ∎

*Example:* Still consider the binary code $C = RM(1,m)$, where $n = 2^m$, $k = m+1$, and $d = 2^{m-1}$. Using Corollary 5, we have $A_d \leq 2^{m+1}-2$. From Corollary 2 we know $A_d \geq 2^{m+1}-2$. So $A_d = 2^{m+1}-2$. Because $A_0 = 1$, it proved that $RM(1,m)$ is a two-weight codes. $RM(1,m)$ is the only code we know that satisfies the upper bound and the lower bound at the same time.

This result can be improved in some cases.

***Corollary 6:*** *If $C$ is a binary code and all weights of $C$ lie in the range [d, n-d], with $n-2d > 0$ and $(n-2d+2)^2 > n$, then*

$$A_d \leq \frac{2^{k-2}\big((n-2d+2)^2-n\big)+(d-1)(n+1-d)}{n+1-2d}$$

*Proof:* For a quadratic $\beta$, of concavity $\cap$, to ensure its positivity on the weights it is enough to assume $\beta(d-1) = \beta(n-d+1) = 0$.

This gives a system of two equations in $\beta_1, \beta_2$, if we write $\beta = 1 - \beta_1 P_1(x) - \beta_2 P_2(x)$. The solution according to `Magma` [4] is

$$\beta_1 = 0, \beta_2 = \frac{2}{(n-2d+2)^2-n}$$

This yields $\beta(0) = \frac{4(d-1)(d-n-1)}{(n-2d+2)^2-n}$ and $\beta(d) = \frac{4(1-2d+n)}{(n-2d+2)^2-n}$. The result follows then by Theorem 4. ∎

Table I,II contain the results of binary codes.

Table I shows that the LP bound is more precise in general than the polynomial method. The interest of the latter resides in producing intuitive bounds with a closed formula.

Table II shows the LP bounds for $n$ ranging from 17 to 32. It is a supplement to the results in Fig. 2. Because it is difficult to calculate all possible values of $A_d$, we did not compare the bounds with the range of $A_d$ as Fig. 2. As we can see from Tab. II, for some values $[22, 11, 7]$, $[23, 12, 7]$ and $[24, 12, 8]$, the lower and upper bounds agree, which means the LP bounds must be tight at these values. It also shows that when $n$ is large, the lower bounds for some values may be trivial (smaller than 1), while the upper bounds are much smaller than the trivial bounds ($A_d \leq 2^k - 1$).

TABLE I
UPPER/LOWER BOUNDS FOR SOME LINEAR CODES

| Binary code | Lower bound of $A_d$ | | Upper bound of $A_d$ | |
|---|---|---|---|---|
| $[n,k,d]$ | Poly. method | LP bound | LP bound | Poly. method |
| $[8,3,4]$ | 2 | 3 | 7 | 10 |
| $[8,4,4]$ | 14 | 14 | 14 | 14 |
| $[9,3,4]$ | $-2$ | 1 | 7 | 12 |
| $[9,4,4]$ | 6 | 6 | 14 | 19 |
| $[10,3,5]$ | 0 | 2 | 4 | 12 |
| $[10,4,4]$ | $-2$ | 12 | 15 | 25 |
| $[11,4,5]$ | 4 | 5 | 7 | 22 |
| $[12,4,6]$ | 10 | 11 | 14 | 18 |
| $[13,4,6]$ | 2 | 4 | 14 | 24 |
| $[14,4,7]$ | 8 | 8 | 8 | 20 |
| $[14,5,6]$ | 2 | 7 | 27 | 50 |
| $[15,4,8]$ | 15 | 15 | 15 | 15 |
| $[15,5,7]$ | 15 | 15 | 15 | 41 |
| $[16,4,8]$ | 6 | 7 | 15 | 22 |
| $[16,5,8]$ | 30 | 30 | 30 | 30 |

TABLE II
LP BOUNDS FOR SOME LINEAR CODES

| Binary codes (R $\approx \frac{1}{2}$) | | | Binary codes (R $\approx \frac{1}{3}$) | | |
|---|---|---|---|---|---|
| $[n,k,d]$ | lower bound | upper bound | $[n,k,d]$ | lower bound | upper bound |
| $[17,9,5]$ | 17 | 50 | $[17,6,7]$ | 12 | 23 |
| $[18,9,6]$ | 69 | 142 | $[18,6,8]$ | 32 | 50 |
| $[19,10,5]$ | $-14$ | 72 | $[19,6,8]$ | 12 | 51 |
| $[20,10,6]$ | 40 | 209 | $[20,7,8]$ | 29 | 83 |
| $[21,11,6]$ | 56 | 282 | $[21,7,8]$ | 9 | 83 |
| $[22,11,7]$ | 176 | 176 | $[22,7,8]$ | -3 | 88 |
| $[23,12,7]$ | 253 | 253 | $[23,8,8]$ | -2 | 143 |
| $[24,12,8]$ | 759 | 759 | $[24,8,8]$ | -12 | 163 |
| $[25,13,6]$ | $-23$ | 526 | $[25,8,9]$ | $-29$ | 64 |
| $[26,13,7]$ | $-67$ | 295 | $[26,9,9]$ | $-43$ | 100 |
| $[27,14,7]$ | $-33$ | 353 | $[27,9,10]$ | 31 | 247 |
| $[28,14,8]$ | 295 | 1138 | $[28,9,10]$ | $-4$ | 259 |
| $[29,15,7]$ | $-182$ | 509 | $[29,10,10]$ | $-5$ | 396 |
| $[30,15,8]$ | 105 | 1724 | $[30,10,11]$ | $-14$ | 178 |
| $[31,16,8]$ | 168 | 1985 | $[31,10,12]$ | 149 | 442 |
| $[32,16,8]$ | $-36$ | 2274 | $[32,11,12]$ | 298 | 639 |

## VI. APPLICATIONS IN CODE-BASED MASKING

Recall from Section II that the kissing number is one of the two factors that determines the concrete side-channel security level in the code-based masking [6] because the mutual information that measures the informativeness of leakage is proportional to the kissing number. In this respect, Theorem 3 and 4 enable us to bound the security gains induced by the corresponding code-based masking. In particular, given the code parameters $[n,k,d]$, these two theorems indicate the best and the worst cases of codes that can be achieved in practice.

Taking the code $[8,4,4]$ in Tab. I as an example, it is unique and has been proven to be the best case in the code-based masking with two shares over $\mathbb{F}_{2^4}$, given the variance of Gaussian noise is greater than $1.0$ [10]. In this case, both lower bounds and upper bounds coincide in $14$. Another example is the code $[12,4,6]$, which is the optimal choice in three share cases over $\mathbb{F}_{2^4}$ [6]. In the latter case, the lower and upper LP bounds are 11 and 14, respectively, where the BKLC code in `Magma` gives $A_d = 12$. It is worth mentioning that $A_d = 12$ is unique for all codes $[12,4,6]$ which is verified by exhaustive code search, although there are several non-equivalent classes.

In general, algebraic codes owing to their large automorphism group have a large kissing number. At the opposite, the application of code-based masking favors codes with low kissing number, which are less studied and certainly deserve more attention.

## VII. CONCLUSION AND OPEN PROBLEMS

In this article, we have derived novel lower and upper bounds on the kissing number of linear codes (Corollaries 1 to 6). It would be interesting to extend its applicability to wider classes of codes by considering polynomials of higher degrees. In another direction, restricting our attention to some special classes of codes like the BCH codes for instance could lead to sharper bounds by addition of new linear constraints. Besides, the derivation of asymptotic lower bounds on the kissing number (when $n \to \infty$) is interesting to lower bound the information leakage of code-based masking for very high-order masking orders.

## REFERENCES


[1] John G. Proakis and Masoud Salehi, *Digital Communications*, 5th Ed., McGraw-Hill, 2008.

[2] Florence Jessie MacWilliams, Neil James Alexander Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1981.

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

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

[5] Alexei Ashikmin, Alexander Barg, Simon Litsyn, "Estimates on the distance distribution of Codes and Designs," *IEEE Trans. on Information Theory*, Vol. IT-47, 2001. 1056–1061.

[6] Wei Cheng, Sylvain Guilley, Claude Carlet, Sihem Mesnager, and Jean-Luc Danger, "Optimizing inner product masking scheme by a coding theory approach," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 220–235, 2021. [Online]. Available: https://doi.org/10.1109/TIFS.2020.3009609

[7] Philips Delsarte, "Bounds on unrestricted codes, by linear programming," *Philips Res. Repts*, vol. 27, 1972

[8] Markus Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Online available at http://www.codetables.de/, 2007, accessed on 2012-07-23.

[9] Koichi Betsumiya and Masaaki Harada, "Binary optimal odd formally self-dual codes," *Des. Codes Cryptography*, Vol. 23, No. 1, pp. 11–22, 2001. http://www.math.nagoya-u.ac.jp/~koichi/paper/fsd-odd.pdf.

[10] Claude Carlet and Sylvain Guilley, "Statistical properties of side-channel and fault injection attacks using coding theory," *Cryptography and Communications*, Vol. 10, No. 5, pp. 909–933, 2018.

[11] Alexei Ashikhmin, Alexander Barg and Serge Vladut, "Linear codes with exponentially many light vectors," *J. Comb. Th. A*, No. 2, pp. 396–399, 2001.