

An improved near-capacity lower bound for Reed–Solomon lists on multiplicative subgroups

Al Kindi
Miden
al.kindi@miden.team

September 2026

Abstract

We give an elementary construction of large Reed–Solomon lists on multiplicative subgroups. For every fixed rational rate $\rho \in (0, 1)$, suitable sequences of lengths give lists of size at least $2^{(2-o(1))H(\rho)/\eta}$ at agreement fraction $\rho + \eta$ as $\eta \rightarrow 0$, where H is binary entropy. This doubles the leading entropy exponent of the antipodal lower bound stated by Arnon, Boneh, and Fenzl, building on the construction of Krachun, Kazanin, and Haböck. If the reduced denominator of ρ is a power of two, the lengths can also be chosen as powers of two. The construction lifts subsets with a prescribed product from a quotient subgroup of size s . This fixes a coefficient while losing at most a factor s in the number of subsets. More precisely, for $n = hs$, $h \geq 2$, and $1 \leq m \leq s - 2$, a code of dimension $\kappa = mh$ on a subgroup of order n has a word with at least $\binom{s-1}{m+1}/s$ codewords at agreement $\kappa + 2h - 1$. This holds over every field containing the required roots of unity. Consequently, the exponent constant c_2 in the universal list-size conjecture of the S-two whitepaper must satisfy $c_2 \geq 2$.

1 Introduction and main result

We study the size of Reed–Solomon lists when the required agreement fraction is only η above the code rate ρ . The Johnson bound gives polynomial list sizes above agreement $\sqrt{\rho}$ [8, 6], whereas multiplicative subgroup domains admit lists exponential in $1/\eta$ near capacity [2, 9, 1]. Our construction doubles the leading entropy exponent of the antipodal lower bound stated in [1, Corollary C.7], which builds on the subgroup construction of [9].

Let K be a field containing a primitive n -th root of unity ζ , and write $\mu_n = \{\zeta^j : 0 \leq j < n\} \subset K^*$. For $1 \leq \kappa < n$, let C_κ be the Reed–Solomon code obtained by evaluating polynomials of degree below κ on μ_n . Its rate is $\rho = \kappa/n$. Identifying codewords with their defining polynomials, we write the list at agreement A with a received word $w : \mu_n \rightarrow K$ as

$$\mathcal{L}_A(w) = \{P \in K[X] : \deg P < \kappa, \quad |\{x \in \mu_n : P(x) = w(x)\}| \geq A\}.$$

Theorem 1.1. *Let h, s, m be positive integers with $h \geq 2$ and $1 \leq m \leq s - 2$, and put $n = hs$. Over every field containing a primitive n -th root of unity, the code C_κ with $\kappa = mh$ has a word w such that*

$$|\mathcal{L}_A(w)| \geq \frac{1}{s} \binom{s-1}{m+1}, \quad A = \kappa + 2h - 1. \tag{1}$$

Every exhibited codeword agrees with w on exactly A points, and no codeword agrees with w on more than A points.

Agreement A corresponds to relative Hamming distance $1 - A/n$; its slack above the rate is $\eta = (A - \kappa)/n$.

We use base-two logarithms and binary entropy $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$, with $0 \log_2 0 = 0$. A rational rate is dyadic if its reduced denominator is a power of two.

For a fixed rational rate ρ , we take $m = \rho s$ and let s grow through multiples of the denominator of ρ . The theorem then gives the following asymptotic bound at rate exactly ρ .

Corollary 1.2. *Fix a rational $\rho \in (0, 1)$. Let s, h be positive integers with $\rho s \in \mathbb{Z}$, $\rho s \leq s - 2$, and $h \geq 2$, and set*

$$n = hs, \quad \kappa = \rho n, \quad \eta = \frac{2h-1}{n} = \frac{2-1/h}{s}.$$

Over every field containing a primitive n -th root of unity, some word has a list at relative agreement $\rho + \eta$ satisfying

$$\log_2 |\mathcal{L}_{(\rho+\eta)n}(w)| \geq \left(2 - \frac{1}{h}\right) \frac{H(\rho)}{\eta} - O_\rho(\log s). \quad (2)$$

Along sequences with $s, h \rightarrow \infty$, the right-hand side is $(2 - o(1)) H(\rho)/\eta$. If ρ is dyadic, both s and h may be powers of two, and hence so may n .

The gain comes from the choice of coefficient to prescribe. Each u -subset $U \subseteq \mu_s$ lifts under $x \mapsto x^h$ to an agreement set whose vanishing polynomial is $\prod_{y \in U} (X^h - y)$. Its nonzero terms have degrees divisible by h . For even s , the antipodal construction uses unions of pairs $\{y, -y\}$. When u is odd, it adds one fixed point to unions of pairs avoiding that point and its negative. These subsets have a common sum. We instead group the u -subsets by their product. There are only s possible products, so one is shared by at least $\binom{s}{u}/s$ subsets. The lifted vanishing polynomials have the same leading and constant terms. Subtracting each vanishing polynomial from the sum of these common terms and dividing by X^h gives low-degree candidates for a common received word. Taking $u = m + 1$ and multiplying by a common vanishing polynomial then adds $h - 1$ fixed agreement points at dimension exactly mh . We reserve one fibre for these points, which accounts for the excluded quotient point in the count $\binom{s-1}{m+1}/s$ of Theorem 1.1.

Relation to earlier work. Lifting subsets from a quotient group appears in the proximity-gap constructions of [2, Section 7] and is used for large Reed–Solomon lists in [9, Remark 5]. The presentation in [1, Appendix C] restates and slightly generalizes the latter construction. The other ingredient is Cheng–Wan’s residue-class method [4, Section 3]: group subsets according to their vanishing polynomials modulo a fixed polynomial. With modulus X , this is exactly the condition of having a prescribed product.

Recent work also gives capacity-radius decoding results over prime fields [3, 7, 5]. In particular, [7, Theorem 1.1] bounds lists by $n^{O_\eta(1)}$ at each fixed positive slack η , for sufficiently large n and prime field size at least n . Such bounds retain a dependence on the length. Our result constrains the dependence on $1/\eta$ of proposed bounds that are uniform in the length and the field.

Section 2 proves Theorem 1.1. Section 3 proves Corollary 1.2 and compares the constructions at the same domain, dimension, and agreement. Section 4 derives the constraint on universal list bounds and gives a numerical consequence for correlated agreement.

2 The construction

Write $n = hs$ and let $v_T(X) = \prod_{x \in T} (X - x)$ be the vanishing polynomial of a finite set $T \subset K$. Under the map $\pi : \mu_n \rightarrow \mu_s$, $x \mapsto x^h$, the fibre above $y \in \mu_s$ is $\{x \in \mu_n : x^h = y\}$. It consists of the h distinct roots of $X^h - y$. Thus

$$v_{\pi^{-1}(U)}(X) = \prod_{y \in U} (X^h - y) = v_U(X^h) \quad (U \subseteq \mu_s). \quad (3)$$

2.1 A two-term word

We first construct a word whose candidates agree with it on u complete fibres. Since every point of μ_n is nonzero, the reciprocal term X^{-h} defines a function on this domain. For $h \geq 2$, $2 \leq u < s$, and $\beta \in \mu_s$, define the received word and code dimension by

$$W_\beta(X) = X^{(u-1)h} + (-1)^u \beta X^{-h}, \quad \kappa_0 = (u-2)h + 1. \quad (4)$$

Proposition 2.1. *For each u -subset $U \subseteq \mu_s$ with $\prod_{y \in U} y = \beta$, the polynomial*

$$Q_U(X) = X^{-h}(X^{uh} + (-1)^u \beta - v_U(X^h)) \quad (5)$$

has degree below κ_0 and agrees with W_β exactly on $\pi^{-1}(U)$, a set of uh points. Distinct subsets give distinct codewords of C_{κ_0} . For this code, some β gives

$$|\mathcal{L}_{uh}(W_\beta)| \geq \frac{1}{s} \binom{s}{u}.$$

Proof. We first check that division by X^h in (5) produces a polynomial of the required degree. Since $v_U(Y)$ is monic of degree u with constant coefficient $(-1)^u \beta$, the polynomial

$$G_U(Y) = Y^u + (-1)^u \beta - v_U(Y)$$

has degree at most $u-1$ and is divisible by Y . Substituting $Y = X^h$ shows that $Q_U = X^{-h}G_U(X^h)$ is a polynomial, with

$$\deg Q_U \leq (u-1)h - h = (u-2)h < \kappa_0.$$

Its agreement with the received word follows from

$$W_\beta - Q_U = X^{-h}v_U(X^h) = X^{-h}v_{\pi^{-1}(U)}(X), \quad (6)$$

where the second equality is (3). The roots on μ_n are therefore exactly the uh points of $\pi^{-1}(U)$. Distinct U give distinct vanishing polynomials and hence distinct Q_U . Since $\deg Q_U < \kappa_0 = (u-2)h + 1 < hs = n$, their evaluations on the n distinct points of μ_n are also distinct.

There are $\binom{s}{u}$ subsets and at most s possible products in μ_s , proving the lower bound by the pigeonhole principle. $\square$

2.2 Adding fixed agreement points

Set $u = m + 1$. Proposition 2.1 gives candidates of degree at most $(m-1)h$, whereas the target code C_{mh} permits degree up to $mh - 1$. The difference is

$$(mh - 1) - (m - 1)h = h - 1.$$

We use this remaining degree allowance to add agreement points. Multiplying the word and every candidate by a common factor B preserves their existing agreements and adds agreement wherever B vanishes. We can take B to have $h - 1$ distinct roots while keeping every candidate in C_{mh} . To ensure that these roots add new agreements, we choose them in the fibre above 1 and restrict the quotient subsets to avoid 1. The agreement then rises from $(m+1)h$ to $mh + 2h - 1$ at dimension mh . Figure 1 shows the fixed roots and the varying fibres.

Exact product-class counts. The pigeonhole estimates can be sharpened by counting the constructed families exactly. Fix a generator ζ_s of μ_s , and let $N_{s,u}(b)$ count the u -subsets with product ζ_s^b . Their exponent sums are b modulo s , so the cyclic subset-sum formula stated in [10, Corollary 1.2] gives

$$N_{s,u}(b) = \frac{1}{s} \sum_{d|\gcd(s,u)} (-1)^{u+u/d} c_d(b) \binom{s/d}{u/d}, \quad c_d(b) = \sum_{\substack{a \bmod d \\ \gcd(a,d)=1}} e^{2\pi i ab/d}. \quad (10)$$

Here c_d is the Ramanujan sum. Proposition 2.1 therefore gives a list of size at least $\max_{b \in \mathbb{Z}/s} N_{s,u}(b)$.

For the fixed-root construction, let $M_{s,u}(b)$ count the same subsets with 1 excluded. Separating subsets according to whether they contain 1 gives $N_{s,u}(b) = M_{s,u}(b) + M_{s,u-1}(b)$, hence

$$M_{s,u}(b) = \sum_{j=0}^u (-1)^{u-j} N_{s,j}(b), \quad (11)$$

where $N_{s,0}(b)$ is 1 for $b = 0$ in $\mathbb{Z}/s$ and 0 otherwise. Choosing a largest such class in the proof of Theorem 1.1 strengthens its lower bound to $\max_{b \in \mathbb{Z}/s} M_{s,m+1}(b)$. These are counts of the exhibited candidates; all depend only on the cyclic group of exponents.

3 List sizes and comparison with the antipodal construction

3.1 The entropy exponent

Proof of Corollary 1.2. Set $m = \rho s$. The assumptions give an integer $1 \leq m \leq s-2$, so Theorem 1.1 applies with $\kappa = mh = \rho n$. The exact ratio

$$\frac{\binom{s-1}{m+1}}{\binom{s}{m}} = \frac{(s-m)(s-m-1)}{s(m+1)} \longrightarrow \frac{(1-\rho)^2}{\rho} > 0$$

shows that these binomial coefficients differ by a factor bounded above and below by positive constants depending only on ρ . Stirling's formula gives $\binom{s}{m} = \Theta_\rho(s^{-1/2} 2^{sH(\rho)})$. Thus (1) implies

$$\log_2 |\mathcal{L}_A(w)| \geq \log_2 \left(\frac{1}{s} \binom{s-1}{m+1} \right) = sH(\rho) - \frac{3}{2} \log_2 s + O_\rho(1).$$

The estimate is uniform in h and the field. Substituting $s = (2 - 1/h)/\eta$ proves (2). As $s, h \rightarrow \infty$, the logarithmic loss is $o(s)$ and $2 - 1/h \rightarrow 2$, giving coefficient two.

Finally, if $\rho = a/2^d$ is dyadic, take $s = 2^t$ with $t \geq d$, so $m = \rho s = a2^{t-d}$ is an integer. For sufficiently large t , we also have $m \leq s-2$. Letting h grow through powers of two makes $n = hs$ a power of two throughout, proving the final assertion. $\square$

3.2 A comparison at the same parameters

To isolate the effect of prescribing the product, we compare Proposition 2.1 with the antipodal construction, using u complete fibres in both cases. Suppose s is even and set

$$n = hs, \quad \kappa_0 = (u-2)h + 1, \quad A = uh.$$

The antipodal construction underlying [1, Corollary C.7] uses parameters $(m, r, k) = (h, u, \kappa_0)$. That corollary is stated for power-of-two evaluation domains; the argument below extends the construction to the present setting with even s . Its exhibited family has size

$$L_{\text{ant}} = \begin{cases} \begin{pmatrix} s/2 \\ u/2 \end{pmatrix}, & u \text{ even}, \\ \begin{pmatrix} s/2 - 1 \\ (u-1)/2 \end{pmatrix}, & u \text{ odd}. \end{cases} \quad (12)$$

For even u , the subsets are unions of antipodal pairs and have sum zero. The identity $(X^h - y)(X^h + y) = X^{2h} - y^2$ identifies this case with the all-subsets construction of [9, Remark 5 and Appendix A]: choose $u/2$ elements of $\mu_{s/2}$ and lift with fibre size $2h$. For odd u , one fixed point is added to unions of pairs avoiding that point and its negative. In both cases the sum σ is common to the family, so $X^{uh} - \sigma X^{(u-1)h} - v_U(X^h)$ has degree at most $(u-2)h < \kappa_0$. Proposition 2.1 instead fixes the constant coefficient and divides by X^h , retaining at least $\binom{s}{u}/s$ subsets.

To compare exponents, take $u/s \rightarrow \rho \in (0, 1)$. Stirling's formula applied to (12) and to the bound $\binom{s}{u}/s$ gives

$$\log_2 L_{\text{ant}} = \frac{s}{2} H(\rho) + o(s), \quad \log_2 \left(\frac{1}{s} \binom{s}{u} \right) = s H(\rho) + o(s).$$

The actual rate is $\kappa_0/n = (u-2)/s + 1/(hs) \rightarrow \rho$, and both constructions have slack $\eta = (2-1/h)/s$. Thus their leading coefficients are respectively $1 - 1/(2h)$ and $2 - 1/h$ when written in units of $H(\rho)/\eta$. The comparison doubles the exponent at each fixed h ; allowing $h \rightarrow \infty$ gives coefficients one and two. Corollary 1.2 additionally keeps the rate exactly fixed.

A finite example. The improvement is already visible at length 64. Take $h = 4$, $s = 16$, and $u = 6$, so both constructions use dimension 17 and agreement 24. The antipodal count in (12) is $\binom{8}{3} = 56$. The pigeonhole estimate in Proposition 2.1 guarantees $\lceil \binom{16}{6}/16 \rceil = 501$ candidates; the exact count (10) improves this to 504. Indeed, $\gcd(16, 6) = 2$, so only the terms $d = 1, 2$ occur. Since $c_1(b) = 1$ and $c_2(b) = (-1)^b$, we obtain

$$N_{16,6}(b) = \frac{\binom{16}{6} - (-1)^b \binom{8}{3}}{16} = \begin{cases} 497, & b \text{ even}, \\ 504, & b \text{ odd}. \end{cases}$$

Choose the class with exponent sum 1, hence product ζ_{16} . Proposition 2.1 gives the received word

$$W(X) = X^{20} + \zeta_{16} X^{-4}$$

with at least 504 distinct codewords of degree below 17, each agreeing on 24 points. Thus the exhibited family is nine times the antipodal family of 56 at the same domain, dimension, and agreement. The calculation holds over every field containing μ_{64} .

4 Consequences for list bounds and correlated agreement

Universal list bounds. Conjecture 1 of the S-two whitepaper [11, Appendix A.5] asks, for each rate ρ , for constants $c_1, c_2 \geq 1$ depending only on ρ such that every Reed–Solomon code over a prime field has list size at most

$$c_1 2^{c_2 H(\rho)/\eta} \quad \text{at distance } \theta = 1 - \rho - \eta \quad (13)$$

up to the base-field Elias radius. The whitepaper uses $c_1 = c_2 = 1$ in its parameter estimates. To compare our construction with this bound, we must ensure that its distance lies inside that radius.

For a field of size q , let $r_E(q, \rho) \in (0, 1 - 1/q)$ be the unique solution of

$$H_q(r_E) = 1 - \rho, \quad H_q(x) = \frac{H(x) + x \log_2(q-1)}{\log_2 q}.$$

This is the radius in [11, equations (123)–(124)]. Since $H(x) \leq 1$ and $\log_2(q-1) \leq \log_2 q$, its defining equation gives

$$r_E(q, \rho) \geq 1 - \rho - \frac{1}{\log_2 q}. \quad (14)$$

Corollary 4.1. *Fix a rational $\rho \in (0, 1)$. Suppose that constants $c_1 > 0$ and $c_2 \in \mathbb{R}$, depending only on ρ , make (13) an upper bound for all received words of every rate- ρ Reed–Solomon code over every prime field, whenever $0 \leq \theta < r_E(p, \rho)$. Then $c_2 \geq 2$. For dyadic ρ , the same conclusion follows if the assumed bound is restricted to evaluation domains that are power-of-two subgroups.*

Proof. Let $s \rightarrow \infty$ through multiples of the denominator of ρ , with $\rho s \leq s - 2$, and choose $h = s$, $n = s^2$. For each s , Dirichlet’s theorem gives a prime $p \equiv 1 \pmod{s^2}$ with $p > 2^s$. The congruence ensures that $\mathbb{F}_p$ contains μ_n . Corollary 1.2 therefore gives a word for a code of rate exactly ρ with

$$\log_2 |\mathcal{L}_A(w)| \geq s H(\rho) - O_\rho(\log s), \quad \eta = \frac{2 - 1/s}{s}.$$

The distance $\theta = 1 - \rho - \eta$ is nonnegative because $A \leq n - 1$ in Theorem 1.1. Moreover, $1/\log_2 p < 1/s < \eta$, so (14) gives

$$\theta < 1 - \rho - \frac{1}{\log_2 p} \leq r_E(p, \rho).$$

The assumed bound (13) thus applies to this word, and comparison yields

$$s H(\rho) - O_\rho(\log s) \leq \log_2 c_1 + \frac{c_2 s H(\rho)}{2 - 1/s}.$$

Divide by $s H(\rho) > 0$ and let $s \rightarrow \infty$. The constants are independent of s and p , so the limit gives $1 \leq c_2/2$. If ρ is dyadic, choosing s to be a power of two throughout also makes $n = s^2$ a power of two. $\square$

Correlated agreement. The lists-to-lines reduction of [2, Sections 6.1–6.2] transfers the larger lists to lower bounds on bad mixing challenges. For $u \geq 3$, the source dimension in Section 3.2 is $\kappa_0 = (u - 2)h + 1$. The reduction gives target dimension $\kappa = \kappa_0 - 1 = (u - 2)h$, preserving agreement $A = uh$.

Let $K = \mathbb{F}_Q$ contain μ_n . Start with a received word $W : \mu_n \rightarrow K$ and L distinct source polynomials $P_1, \dots, P_L$ of degree at most κ , each agreeing with W on at least A points, where $A > \kappa$. Assume

$$\kappa \binom{L}{2} < Q - n. \quad (15)$$

We construct fixed words $u_0, u_1 : \mu_n \rightarrow K$ such that no pair of target codewords agrees with them on a common set of at least A points, yet at least L challenges $\lambda \in K$ make $u_0 + \lambda u_1$ agree with a

target codeword on at least A points. These are bad challenges for correlated agreement. For a uniformly sampled challenge $\lambda \in K$, this gives

$$\Pr_{\lambda \leftarrow K}[\lambda \text{ is bad}] \geq \frac{L}{Q}.$$

To construct these words, first use (15) to choose $a \in K \setminus \mu_n$ where $P_1(a), \dots, P_L(a)$ are pairwise distinct: each difference $P_i - P_j$ with $i \neq j$ has at most κ roots, so all pairwise collisions exclude at most $\kappa \binom{L}{2}$ points. Define

$$u_0(x) := \frac{W(x)}{x-a}, \quad u_1(x) := \frac{1}{x-a}, \quad x \in \mu_n.$$

These words are fixed before the mixing challenge λ is sampled uniformly from K . The resulting mixed word is

$$w_\lambda(x) := u_0(x) + \lambda u_1(x) = \frac{W(x) + \lambda}{x-a}.$$

For each source polynomial P_i , define

$$\lambda_i := -P_i(a), \quad f_i(X) := \frac{P_i(X) - P_i(a)}{X-a}.$$

The factor theorem shows that f_i is a polynomial of degree below κ . Wherever $W(x) = P_i(x)$, we have $w_{\lambda_i}(x) = f_i(x)$. Thus the L distinct challenges $\lambda_1, \dots, \lambda_L$ each give a mixed word agreeing with a target codeword on at least A points.

To see why these challenges are bad for correlated agreement, suppose there were polynomials F_0, F_1 of degree below κ and a set $S \subseteq \mu_n$, $|S| \geq A$, with $u_0 = F_0$ and $u_1 = F_1$ on S . In particular, F_1 would agree with $u_1(x) = 1/(x-a)$ on S , so

$$F_1(x) = \frac{1}{x-a} \implies (x-a)F_1(x) - 1 = 0 \quad (x \in S).$$

Thus $G(X) := (X-a)F_1(X) - 1$ would have at least A distinct roots. But $\deg F_1 < \kappa$ gives $\deg G \leq \kappa$, and $G(a) = -1$ shows that G is nonzero. A nonzero polynomial of degree at most κ has at most κ roots, contradicting $A > \kappa$. Hence no such common agreement set exists. Each λ_i nevertheless gives at least A agreements for the mixture, and is therefore a bad challenge. Since the λ_i are distinct, this proves the stated count and probability bounds.

For example, take $p = 2^{64} - 2^{32} + 1$, $n = 2^{23}$, and $\kappa = 2^{20}$, with $h = n/s$ and $u = \kappa/h + 2 = s/8 + 2$. Here $n \mid p-1$, so $\mu_n \subset \mathbb{F}_p$, and the target rate is exactly $1/8$. For the even values of u used in Table 1, the source counts

$$L_{\text{ant}} = \binom{s/2}{u/2}, \quad L_{\text{prod}} = \left\lceil \frac{1}{s} \binom{s}{u} \right\rceil$$

come from (12) and Proposition 2.1. Both satisfy (15) in each row of Table 1. The product bounds exceed 2^{-100} over $\mathbb{F}_{p^2}$ and 2^{-128} over $\mathbb{F}_{p^3}$ at the respective distances shown.

The fixed-root step of Section 2.2 also applies after the fibre quotient of [9, Appendix A], using the degree saved by quotienting in X^h to add fixed agreement points. This raises the agreement threshold at the same target dimension, at the cost of excluding one quotient point from the source subsets.

Field	s	Distance $1 - A/n$	Antipodal	Product
$\mathbb{F}_{p^2}$	64	27/32	$2^{-110.38}$	$2^{-96.86}$
$\mathbb{F}_{p^3}$	128	55/64	$2^{-157.32}$	$2^{-127.32}$

Table 1: Bad-challenge probability lower bounds at $n = 2^{23}$ and $\kappa = 2^{20}$. Here $p = 2^{64} - 2^{32} + 1$; entries are the rounded values of L/Q for the respective source counts.

Acknowledgements. We thank Ulrich Haböck for discussions that motivated this investigation.

AI assistance. AI tools assisted with editing the exposition, reviewing arguments, and checking numerical examples.

References

- [1] G. Arnon, D. Boneh, G. Fenzi, *Open problems in list decoding and correlated agreement*, IACR Cryptology ePrint Archive, Report 2026/680, revision of July 6, 2026.
- [2] E. Ben-Sasson, D. Carmon, U. Haböck, S. Kopparty, S. Saraf, *On proximity gaps for Reed–Solomon codes*, ECCC TR25-169; IACR Cryptology ePrint Archive, Report 2025/2055.
- [3] J. Brakensiek, Y. Chen, A. Putterman, Z. Zhang, K. Z. Zheng, *Algorithmic list decoding of Reed–Solomon codes up to capacity*, ECCC TR26-164, revision 1, September 5, 2026.
- [4] Q. Cheng, D. Wan, On the list and bounded distance decodability of Reed–Solomon codes, *SIAM J. Comput.* **37** (2007), no. 1, 195–209. Preprint: arXiv:math/0405082 (2004).
- [5] Q. Dao, S. D. Kominers, J. Thaler, *Reed–Solomon codes beyond Johnson: Efficient decoding and smaller cryptographic proofs*, IACR Cryptology ePrint Archive, Report 2026/2056.
- [6] V. Guruswami, M. Sudan, Improved decoding of Reed–Solomon and algebraic-geometry codes, *IEEE Trans. Inform. Theory* **45** (1999), 1757–1767.
- [7] F. G. Jeronimo, *Algorithmic list decoding at capacity and optimal proximity gaps for Reed–Solomon codes*, ECCC TR26-169, 2026.
- [8] S. M. Johnson, A new upper bound for error-correcting codes, *IRE Trans. Inform. Theory* **8** (1962), 203–207.
- [9] D. Krachun, S. Kazanin, U. Haböck, *Failure of proximity gaps close to capacity*, IACR Cryptology ePrint Archive, Report 2026/782.
- [10] J. Li, D. Wan, Counting subset sums of finite abelian groups, *J. Combin. Theory Ser. A* **119** (2012), no. 1, 170–182.
- [11] D. Carmon, L. Goldberg, U. Haböck, L. Lerer, I. Lesokhin, S. Papini, S. Samocha, *S-two whitepaper*, IACR Cryptology ePrint Archive, Report 2026/532, revision of March 24, 2026.