



A Spin Glass Model for Reconstructing Nonlinearly Encrypted Signals Corrupted by Noise

Yan V. Fyodorov¹ 

Received: 12 August 2018 / Accepted: 11 December 2018 / Published online: 12 January 2019
© The Author(s) 2019

Abstract

We define a (symmetric key) encryption of a signal $\mathbf{s} \in \mathbb{R}^N$ as a random mapping $\mathbf{s} \mapsto \mathbf{y} = (y_1, \dots, y_M)^T \in \mathbb{R}^M$ known both to the sender and a recipient. In general the recipients may have access only to images \mathbf{y} corrupted by an additive noise of unknown strength. Given the encryption redundancy parameter (ERP) $\mu = M/N \geq 1$ and the signal strength parameter $R = \sqrt{\sum_i s_i^2}/N$, we consider the problem of reconstructing \mathbf{s} from its corrupted image by a Least Square Scheme for a certain class of random Gaussian mappings. The problem is equivalent to finding the configuration of minimal energy in a certain version of spherical spin glass model, with *squared* Gaussian random interaction potential. We use the Parisi replica symmetry breaking scheme to evaluate the mean overlap $p_\infty \in [0, 1]$ between the original signal and its recovered image (known as 'estimate') as $N \rightarrow \infty$, for a given ('bare') noise-to-signal ratio (NSR) $\gamma \geq 0$. Such an overlap is a measure of the quality of the signal reconstruction. We explicitly analyze the general case of *linear-quadratic* family of random mappings and discuss the full $p_\infty(\gamma)$ curve. When nonlinearity exceeds a certain threshold but redundancy is not yet too big, the replica symmetric solution is necessarily broken in some interval of NSR. We show that encryptions with a nonvanishing linear component permit reconstructions with $p_\infty > 0$ for any $\mu > 1$ and any $\gamma < \infty$, with $p_\infty \sim \gamma^{-1/2}$ as $\gamma \rightarrow \infty$. In contrast, for the case of *purely quadratic* nonlinearity, for any ERP $\mu > 1$ there exists a threshold NSR value $\gamma_c(\mu)$ such that $p_\infty = 0$ for $\gamma > \gamma_c(\mu)$ making the reconstruction impossible. The behaviour close to the threshold is given by $p_\infty \sim (\gamma_c - \gamma)^{3/4}$ and is controlled by the replica symmetry breaking mechanism.

Keywords Spin glass · Signal reconstruction · Inference

1 Introduction

1.1 Description of the Problem

In this paper we consider a schematic model of a reconstruction of a source signal from its encrypted form corrupted by an additive noise when passed from a sender to a recipient.

✉ Yan V. Fyodorov
yan.fyodorov@kcl.ac.uk

¹ Department of Mathematics, King's College London, London WC2R 2LS, UK

Signals are represented by N -dimensional source (column) vectors $\mathbf{s} = \begin{pmatrix} s_1 \\ \vdots \\ s_N \end{pmatrix} \in \mathbb{R}^N$,

and we define the associated signal strength R via the Euclidean norm as $R = \sqrt{\frac{1}{N} (\mathbf{s}, \mathbf{s})}$, where (\cdot, \cdot) stands for the Euclidean inner product in \mathbb{R}^N . By a (symmetric key) *encryption*

of the source signal we understand a *random mapping* $\mathbf{s} \mapsto \mathbf{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_M \end{pmatrix} \in \mathbb{R}^M$ known both to the sender and a recipient. For further reference we find it useful to write the mapping component-wise explicitly as

$$y_k = V_k(\mathbf{s}), \quad k = 1, \dots, M, \quad (1)$$

with the collection of random functions $V_1(\mathbf{s}), \dots, V_M(\mathbf{s})$ representing an encryption algorithm shared between the parties participating in the signal exchange. Due to imperfect communication channels the recipients however get access to the encrypted signals only in a corrupted form \mathbf{z} . We consider only the simplest corruption mechanism when the encrypted images \mathbf{y} are modified by an additive random noise, i.e. $\mathbf{z} = \mathbf{y} + \mathbf{b}$. The noise vectors \mathbf{b} are further assumed to be normally distributed: $\mathbf{b} \sim \mathcal{N}(\mathbf{0}, \sigma^2 \mathbf{1}_M)$, i.e. components b_k , $k = 1, \dots, M$ are i.i.d. mean zero real Gaussian variables with the covariance $\langle b_k b_l \rangle = \delta_{kl} \sigma^2$, where the notation $\langle \dots \rangle$ here and henceforth stands for the expected value $\mathbb{E}[\dots]$ with respect to all types of random variables. A natural parameter is then the 'bare' noise-to-signal ratio (NSR) $\gamma = \sigma^2/R^2$, which will be eventually converted to true NSR dependent on the parameters of encryption algorithm (we will later on refer to such conversion in the text as an appropriate 'scaling') characterizing the level of signal corruption in the chosen type of encryption.

The recipient's aim is to reconstruct the source signal \mathbf{s} from the knowledge of \mathbf{z} . In the presence of noise such reconstruction can be only approximate, and reconstructed signals are known in the signal processing literature as 'estimates' of the source signals. Their properties depend on the reconstruction scheme (or the 'estimator') used. Our assumption is that the strength of the noise, i.e. the parameter σ^2 , is not used by the recipient when reconstructing the source signal. We consider the input signal through the reconstruction procedure as a *fixed* vector, and then employ the Least-Square reconstruction scheme, which for a given set of observations $z_k = V_k(\mathbf{s}) + b_k$ returns an estimate of the input signal as

$$\mathbf{x} := \text{Argmin}_{\mathbf{w}} \left[\sum_{k=1}^M \frac{(z_k - V_k(\mathbf{w}))^2}{2} \right], \quad \mathbf{w} \in \mathbb{W} \subseteq \mathbb{R}^N, \quad (2)$$

where \mathbb{W} is a set of feasible input signals.

To avoid misunderstanding, we briefly contrast our approach with the Bayesian inference philosophy. In the latter framework one assumes that the probability density $\rho(\mathbf{w})$ over the set \mathbb{W} of feasible input signals (the 'prior' distribution) is either known or one can make an Ansatz on its form. The Bayes theorem provides the *a posteriori* probability density $p(\mathbf{w}|\mathbf{z})$ of the input signal \mathbf{w} for a given observation \mathbf{z} in the form $p(\mathbf{w}|\mathbf{z}) = p(\mathbf{z}|\mathbf{w})\rho(\mathbf{w})/\int_{\mathbb{W}} p(\mathbf{z}|\mathbf{w})\rho(\mathbf{w})d\mathbf{w}$, where $p(\mathbf{z}|\mathbf{w})$ is the probability to observe \mathbf{z} for a given input \mathbf{w} . In Bayesian inference one then seeks to minimize some *expected* (with respect to $p(\mathbf{w}|\mathbf{z})$) error/loss function. For example, if one seeks to minimize the *mean square error* loss function (MMSE), the optimal estimate is given by the mean $\mathbf{x}_{MMSE} := \int_{\mathbb{W}} \mathbf{w} p(\mathbf{w}|\mathbf{z}) d\mathbf{w}$. In our model with the Gaussian noise $\mathbf{b} \sim \mathcal{N}(\mathbf{0}, \sigma^2 \mathbf{1}_M)$ the probability $p(\mathbf{z}|\mathbf{w})$ to observe \mathbf{z} is given by $p(\mathbf{z}|\mathbf{w}) \sim$

$\exp \left\{ - \sum_{k=1}^M \frac{(z_k - V_k(\mathbf{w}))^2}{2\sigma^2} \right\}$. Therefore evaluation of \mathbf{x}_{MMSE} requires that the noise strength σ^2 is explicitly known to the recipient. Such a knowledge is formally not required in the estimate Eq. (2) used in the present paper. Instead we note that our approach can be given a formal Bayesian meaning as a Maximum-A-Posteriori (MAP) estimator (optimal under 'hit-or-miss' or 0–1 loss function) with a uniform prior distribution $\rho(\mathbf{w}) = \text{const}$ over the feasibility set \mathbb{W} . In such a case it also incidentally coincides with the maximal likelihood (ML) estimator which seeks to maximize the probability $p(\mathbf{z}|\mathbf{w})$ over \mathbf{w} for the observation \mathbf{z} corresponding to the actual input signal \mathbf{s} .

Quality of the signal reconstruction under our scheme is then characterized by the value of a distortion parameter measuring the difference between the fixed source signal \mathbf{s} and the estimate \mathbf{x} . For this one may use any suitable distance function $d(\mathbf{x}; \mathbf{s})$, e.g the Euclidean distance normalized to the signal strength:

$$d(\mathbf{x}; \mathbf{s}) = \frac{(\mathbf{x} - \mathbf{s}, \mathbf{x} - \mathbf{s})}{NR^2}. \quad (3)$$

One is interested in getting the expression for the distortion in the asymptotic limit of large signal dimensions $(M, N) \rightarrow \infty$. As long as M remains smaller than N , any solution $\mathbf{x} \in \mathbb{W} \subseteq \mathbb{R}^N$ of the set of M equations $b_k + V_k(\mathbf{s}) - V_k(\mathbf{x}) = 0$, $k = 1, \dots, M$ will be corresponding to the exactly zero value of the cost function, and could be used as a legitimate estimate. The set of estimates then form continuously parametrized manifolds in \mathbb{R}^N . It is therefore clear that even in the absence of any noise full reconstruction of the signal for $M < N$ under this scheme is impossible. Although such a case is not at all devoid of interest, we do not treat it in the present paper leaving it for a separate study. In contrast, for 'redundantly' encrypted signals with $M \geq N$ the set of possible estimates generically consists of isolated points in \mathbb{R}^N . To this end we introduce the Encryption Redundancy Parameter (ERP) $\mu = M/N \in (1, \infty)$. We will see that under such conditions signals can be in general faithfully reconstructed in some range of the noise-to-signal ratios $\gamma > 0$.

In this paper we are going to apply tools of Statistical Mechanics for calculating the average asymptotic distortion for a certain class of the least square reconstruction of a randomly encrypted noisy signal. As this is essentially a large-scale random optimization problem, methods of statistical mechanics of disordered systems like the replica trick developed in theory of spin glasses are known to be efficient in providing important analytical insights in the statistical properties of the solution, see e.g. [31,34]. It is also worth noting that distinctly different aspects of the problem of information reconstruction (the so-called *error-correcting* procedures) were discussed in the framework of spin glass ideas already in the seminal work by Sourlas [39].

We consider the reconstruction problem under two technical assumptions. The first assumption is that the recipient is aware of the exact source signal strength R , and therefore can restrict the least square minimization search in Eq. (2) to the feasibility set \mathbb{W} given by $(N - 1)$ -dimensional sphere of the radius $R\sqrt{N}$. We will refer to such a condition as the 'spherical constraint'. From the point of view of the Bayesian analysis our reconstruction scheme can be considered as a MAP estimator with postulated prior distribution being the uniform measure on the above-mentioned $(N - 1)$ -dimensional sphere. As the lengths of both the input signal \mathbf{s} and an estimator \mathbf{x} are fixed to $R\sqrt{N}$, the distance Eq. (3) depends only on the scalar product (\mathbf{x}, \mathbf{s}) . We therefore can conveniently characterize the quality of the reconstruction via the *quality parameter* defined as

$$p_N = \frac{(\mathbf{x}, \mathbf{s})}{NR^2} \in [0, 1], \quad (4)$$

where $p_N = 1$ corresponds to a reconstruction without any macroscopic distortion, whereas $p_N = 0$ manifests impossibility to recover any information from the originally encrypted signal. Note that the assumption of the fixed input signal strength R is technically convenient but can be further relaxed; the analysis can be extended, without much difficulty, to the search in a spherical shell $R_1\sqrt{N} \leq |\mathbf{w}| \leq R_2\sqrt{N}$, and allows to include additive penalty terms which do not violate the rotational symmetry, e.g. squared Euclidean norm of the signal, and hopefully to some other situations.

Our second assumption is that the random functions $V_k(\mathbf{s})$ belong to the class of (smooth) *isotropic* gaussian-distributed random fields on the sphere, independent for different values of k (and independent of the noise \mathbf{b}), with mean-zero and the covariance structure dependent only on the angle between the vectors. Using the scaling appropriate for our problem in the limit of large N we represent such covariances as

$$\langle V_k(\mathbf{x}) V_l(\mathbf{s}) \rangle = \delta_{lk} \Phi \left(\frac{(\mathbf{x}, \mathbf{s})}{N} \right), \quad (5)$$

where the angular brackets $\langle \dots \rangle$ denote the expectation with respect to the corresponding probability measures. We will further assume for simplicity that $\Phi(u)$ in Eq. (5) is infinitely differentiable.

The simplest case of random fields of this type corresponds to a *linear* encryption algorithm, with the functions $V_k(\mathbf{x})$, $k = 1, \dots, M$ chosen in the form of random linear combinations:

$$V_k(\mathbf{x}) = \sum_{i=1}^N a_{ki} x_i := (\mathbf{a}_k, \mathbf{x}), \quad (6)$$

where the vectors \mathbf{a}_k are assumed to be random, mean-zero mutually independent Gaussian, each with N i.i.d. components characterized by the variances $\langle a_{ki} a_{lj} \rangle = \frac{J_1^2}{N} \delta_{lk} \delta_{ij}$. Such choice implies the covariance Eq. (5) with $\Phi(u) = J_1^2 u$.

The linear encryption is very special, yet not completely trivial, instance of the reconstruction problem, as in that case one can formally solve the minimization problem by the method of Lagrange multipliers explicitly. To this end we introduce the cost function (cf. Eq. (2))

$$\mathcal{H}_s(\mathbf{x}) = \sum_{k=1}^M \mathcal{H}_s^{(k)}(\mathbf{x}), \quad \mathcal{H}_s^{(k)}(\mathbf{x}) = \frac{(b_k + V_k(\mathbf{s}) - V_k(\mathbf{x}))^2}{2}, \quad (7)$$

which depends on the source signal \mathbf{s} as a parameter. Then following the standard idea of a constrained minimization we need to consider the stationarity conditions $\nabla \mathcal{L}_{\lambda, \mathbf{s}}(\mathbf{x}) = 0$ for the Lagrangian $\mathcal{L}_{\lambda, \mathbf{s}}(\mathbf{x}) = \mathcal{H}_s(\mathbf{x}) - \frac{\lambda}{2}(\mathbf{x}, \mathbf{x})$, with real λ being the Lagrange multiplier taking care of the spherical constraint. In the general case of a non-linear encryption algorithm this procedure does not seem to help much to our analysis, as the stationarity equations look hard to study. In the linear case one can however introduce a $N \times M$ matrix A whose M rows are represented by (transposed) vectors \mathbf{a}_k^T featuring in Eq. (6). We then can easily see that the stationarity conditions in that case amount to the following matrix equation:

$$A^T [A(\mathbf{x} - \mathbf{s}) - \mathbf{b}] = \lambda \mathbf{x}, \quad (8)$$

which can be then immediately solved and provides the signal estimate in the form

$$\mathbf{x} = \left[\mathbf{1}_N + \lambda (A^T A - \lambda \mathbf{1}_N)^{-1} \right] \mathbf{s} + (A^T A - \lambda \mathbf{1}_N)^{-1} A^T \mathbf{b}. \quad (9)$$

The possible set of Lagrange multipliers is obtained by solving the equation implied by the spherical constraint: $(\mathbf{x}, \mathbf{x}) = NR^2$, which is in general equivalent to a polynomial equation of degree $2N$ in λ . The number of real solutions of that equation depends on the noise vector \mathbf{b} . One of the real solutions corresponds to the minimum of the cost function, others to saddle-points or maxima. In particular, in the (trivial) limiting case of no noise $\mathbf{b} = 0$ the global minimum corresponds to $\lambda = 0$ implying reconstruction with no distortion: $\mathbf{x} = \mathbf{s}$, hence $p_N = 1$ as is natural to expect. At the same time, for any $\mathbf{b} \neq 0$ the analysis of Eq. (9) becomes a non-trivial problem. One possible way is to account for the presence of a weak noise with small variance σ^2 by developing a perturbation theory in the small scaled NSR parameter $\tilde{\gamma} = \frac{\sigma^2}{J_1^2 R^2} \ll 1$. Such a theory is outlined in the Appendix A, where we find that for a given value of ERP $\mu > 1$ and in the leading order in $\tilde{\gamma}$ the asymptotic disorder-averaged quality reconstruction parameter defined in Eq. (4) is given by:

$$p_\infty := \lim_{N \rightarrow \infty} \langle p_N \rangle = 1 - \tilde{\gamma} \frac{1}{\mu - 1} + o(\tilde{\gamma}). \quad (10)$$

This result is based on the asymptotic mean density of eigenvalues of random Wishart matrices $A^T A$ due to Marchenko and Pastur [30]. Similarly, one can develop a perturbation theory for very big NSR $\tilde{\gamma} \gg 1$, see Appendix A. In this way one finds that the Lagrange multiplier $|\lambda| \sim (\mu\tilde{\gamma})^{1/2}$ and $p_\infty \sim \sqrt{\frac{\mu}{\tilde{\gamma}}}$.

Although the perturbation theories are conceptually straightforward, and can be with due effort extended to higher orders, the calculations quickly become too cumbersome. At the moment we are not aware of any direct approach to our minimization problem in the linear encryption case which may provide non-perturbative results, as $N \rightarrow \infty$, for asymptotic distortion p_∞ at values of scaled NSR parameter $\tilde{\gamma}$ of the order of unity. At the same time we will see that methods of statistical mechanics provide a very explicit expression for any $\tilde{\gamma}$.

It is necessary to mention that various instances of not dissimilar *linear* reconstruction problems in related forms received recently a considerable attention. The emphasis in those studies seems however to be mainly restricted to the case of source signals being subject to a compressed sensing, i.e. represented by a sparse vector with a finite fraction of zero entries, see e.g. [28,32,42] and references therein. To this end especially deserve mentioning the works [7–9] which studied the mean value of distortions for MAP estimator for a linear problem (though with prior distribution different from the spherical constraint). More recently, a very general signal reconstruction problem for nonlinear encryption functions of a linear random mapping was considered in the framework of statistical-mechanics based Bayesian approach in [6]. One may also mention a particular case of *bi-linear* reconstruction considered in a similar framework in [38]. Although having a moderate overlap with methods used in this work, the actual calculations and the main message of those papers seem rather different.

In particular, our main emphasis will be on ability to analyse the case of a quite general *nonlinear* random Gaussian encryptions¹. The corresponding class of functions $V_k(\mathbf{x})$ extends the above-mentioned case of random linear forms to higher-order random forms, the first nontrivial example being the form of degree 2:

$$V_k(\mathbf{x}) = (\mathbf{a}_k, \mathbf{x}) + \frac{1}{2}(\mathbf{x}, \mathcal{J}^{(k)}\mathbf{x}), \quad (11)$$

¹ In the context of compressed sensing some reconstruction aspects of nonlinear models were considered, e.g. in [10,37], but our approach seems distinctly different.

where entries of $N \times N$ real symmetric random matrices $\mathcal{J}^{(k)}$, $k = 1, \dots, M$ are mean-zero Gaussian variables (independent of the vectors \mathbf{a}_k) with the covariance structure

$$\left\langle \mathcal{J}_{ij}^{(k)} \mathcal{J}_{mn}^{(l)} \right\rangle = \frac{J_2^2}{N^2} \delta_{lk} (\delta_{im} \delta_{jn} + \delta_{in} \delta_{jm}), \quad (12)$$

which eventually results in the covariance Eq. (5) of the form $\Phi(u) = J_1^2 u + \frac{1}{2} J_2^2 u^2$. We will refer to the above class of random encryptions as the *linear-quadratic family*.

In fact, the general covariance structure of isotropic Gaussian random fields on a sphere of radius $R\sqrt{N}$ is also well-known from the theory of spherical spin glasses: these are functions which can be represented by a (possibly, terminating) series with non-negative coefficients:

$$\Phi(u) = \sum_{l=1}^{\infty} c_l u^l, \quad c_l \geq 0 \quad \forall l \quad (13)$$

such that $\Phi(R^2)$ has a finite value, see e.g. [1]. Although our theory of encrypted signal reconstruction will be developed at $N \gg 1$ for the general Gaussian case, all the explicit analysis of the ensuing equations will be restricted to the case of the linear-quadratic family, Eq. (11).

As our main results reported below are asymptotic in nature and employ N as a big parameter, it is natural to ask how robust are our findings against relaxing the Gaussianity assumption. For the linear case Eq. (6) such generalization is possible, see e.g. [7], by considering rotationally-invariant ensemble of the associated matrices A and employing the large- N asymptotics of the so-called spherical integrals found in [24,25]. Whether similar methods may help to settle the question for the linear-quadratic family by replacing the GOE matrices $\mathcal{J}^{(k)}$ with their counterparts from more general class of rotationally-invariant random matrix ensembles remains an interesting topic for a future research.

1.2 Main Results

Our first main result is the following

Proposition 1 *Given a value of $R > 0$ characterizing the source signal strength, and the value of the ERP $\mu > 1$, consider the functional*

$$\begin{aligned} \mathcal{E}[w_s(u); Q, v, t] = & - \left[\frac{R^2 - t^2 - Q}{v + \int_{R^2-Q}^{R^2} w_s(u) du} + \int_{R^2-Q}^{R^2} \frac{dq}{v + \int_q^{R^2} w_s(u) du} \right] \\ & + \mu \left[\frac{\sigma^2 + \Phi(R^2) - 2\Phi(Rt) + \Phi(R^2 - Q)}{1 + v\Phi'(R^2) + \int_{R^2-Q}^{R^2} w_s(u)\Phi'(u) du} \right. \\ & \left. + \int_{R^2-Q}^{R^2} \frac{\Phi'(q) dq}{1 + v\Phi'(R^2) + \int_q^{R^2} w_s(u)\Phi'(u) du} \right], \quad (14) \end{aligned}$$

where the variable $v \geq 0$, the variables t and Q take values in intervals $[-R, R]$ and $[0, R^2]$, correspondingly, and $w_s(u)$ is a non-decreasing function in $u \in [R^2 - Q, R^2]$. Then in the framework of the Parisi scheme of the Full Replica Symmetry Breaking (FRSB) the mean value of the parameter p_N characterising quality of the information recovery in the signal

reconstruction scheme, Eqs. (2)–(5), with normally distributed noise $\mathbf{b} \sim \mathcal{N}(\mathbf{0}, \sigma^2 \mathbf{1}_M)$ is given for $N \rightarrow \infty$ by

$$p_\infty := \lim_{N \rightarrow \infty} \langle p_N \rangle = \frac{t}{R}, \quad (15)$$

where the specific value of the parameter t to be substituted to Eq. (15) should be found by simultaneously minimizing the functional $\mathcal{E}[w_s(u); Q, v, t]$ over t and maximizing it over all other parameters and the function $w_s(u)$.

Our next result provides an explicit solution to this variational problem in a certain range of parameters.

Proposition 2

In the range of parameters such that the solution t to the equation

$$\mu R^2 [\Phi'(Rt)]^2 (R^2 - t^2) = t^2 \Phi'(R^2) [R^2 \gamma + \Phi(R^2) - 2\Phi(Rt) + \Phi(R^2)] \quad (16)$$

satisfies the inequality

$$[\Phi'(R^2)]^3 \frac{t^2}{R^2} \leq \mu [\Phi'(Rt)]^2 [\Phi'(R^2) - \Phi''(R^2)(R^2 - t^2)] \quad (17)$$

the variational problem Eq. (14) is solved by the Replica-Symmetric Ansatz $Q = 0$. In particular, for a given 'bare' Noise-to-Signal ratio $\gamma = \sigma^2/R^2$ the quality parameter p_∞ defined in Eq. (15) is given by the solution of the following equation:

$$p^2 \left(\gamma + 2 \frac{\Phi(R^2) - \Phi(R^2 p)}{R^2} \right) = \mu (1 - p^2) \frac{[\Phi'(R^2 p)]^2}{\Phi'(R^2)}. \quad (18)$$

In addition, for the range of parameters such that the solution t of Eq. (68) violates the inequality Eq. (69) the variational problem Eq. (14) can be solved by the FRSB Ansatz amounting to assuming the minimizer function $w_s(u)$ to be continuous and non-decreasing. In this case the value p of the quality parameter p_∞ defined in Eq. (15) is given by the solution of the following system of two equations in the variables $p \in [0, 1]$ and $Q \in [0, R^2]$:

$$\begin{aligned} \mu [\Phi'(R^2 p)]^2 (R^2(1 - p^2) - Q) &= p^2 \Phi'(R^2 - Q) [R^2 \gamma + \Phi(R^2) \\ &\quad - 2\Phi(R^2 p) + \Phi(R^2 - Q)] \end{aligned} \quad (19)$$

and

$$[\Phi'(R^2 - Q)]^3 p^2 = \mu [\Phi'(R^2 p)]^2 [\Phi'(R^2 - Q) - \Phi''(R^2 - Q)(R^2(1 - p^2) - Q)]. \quad (20)$$

We finally note in passing that the FRSB scheme as we use it automatically includes the case of the so-called 1-Step Replica Symmetry Breaking (1-RSB) which corresponds to looking for a solution of the variational problem being a constant function $w_s(u) = \text{const}$, $\forall u \in [R^2 - Q, Q]$. Closer inspection, which we however omit, shows that such a solution respecting the required constraints on the parameters v , t and Q simply does not exist, and any nontrivial solution $w_s(u)$ is continuous and increasing in the interval $[R^2 - Q, Q]$. The question whether the variational problem may have a valid solution with higher discrete level of the replica-symmetry breaking (the so-called r -step, which in our language will correspond to $w_s(u)$ being nondecreasing in $[R^2 - Q, Q]$, but with $r - 1$ discontinuities) has been however not investigated. Note, that in general in the spin-glass literature such a possibility is considered to be relatively exotic, though can not be excluded on general grounds, see [3].

1.2.1 Results for the Linear-Quadratic Family of Encryptions

Both Propositions providing the solution of our reconstruction problem in full generality, for every specific choice of the covariance structure $\Phi(u)$ the equations need to be further analyzed. In this work we performed a detailed analysis of the case of encryptions belonging to the linear-quadratic family Eq. (11) with the covariance structure of the form $\Phi(u) = J_1^2 u + \frac{1}{2} J_2^2 u^2$. The most essential qualitative features of the analysis are summarized below.

For such a family, apart from our main control parameters, scaled NSR $\tilde{\gamma} = \gamma/J_1^2$ and ERP μ , the reconstruction is very essentially controlled by an important parameter $a = R^2 J_2^2 / J_1^2$ which reflects the degree of *nonlinearity* in the encryption mapping. Our first result is that there exists a threshold value of this parameter, $a = 1$, such that for all encryptions in the family with $a < 1$ the variational problem is always solved with the Replica-Symmetric Ansatz Eq. (18). In contrast, for linear-quadratic encryptions with higher nonlinearity $a > 1$ there exists a threshold value of the ERP $\mu = \frac{(a^{2/3} - a^{1/3} + 1)^3}{a} := \mu_{AT}(a) > 1$ such that for any $\mu \in (1, \mu_{AT}(a))$ the replica symmetric solution is broken in some interval of NSR and is replaced by one with FRSB. This implies that increasing redundancy for a fixed non-linearity one eventually always ends up in the replica-symmetric phase, see the phase diagram in Fig. 1.

In contrast, at a fixed nonlinearity $a > 1$ and not too big redundancy values $\mu \in (1, \mu_{AT}(a))$ there exists generically an interval of scaled NSR's $\tilde{\gamma}_{AT}^{(1)} < \tilde{\gamma} < \tilde{\gamma}_{AT}^{(2)}$ such that the replica-symmetry is broken inside and preserved for $\tilde{\gamma}$ outside that interval. The exact values $\tilde{\gamma}_{AT}^{(1,2)}$ can be in general found only by numerically solving the 4th-order poly-

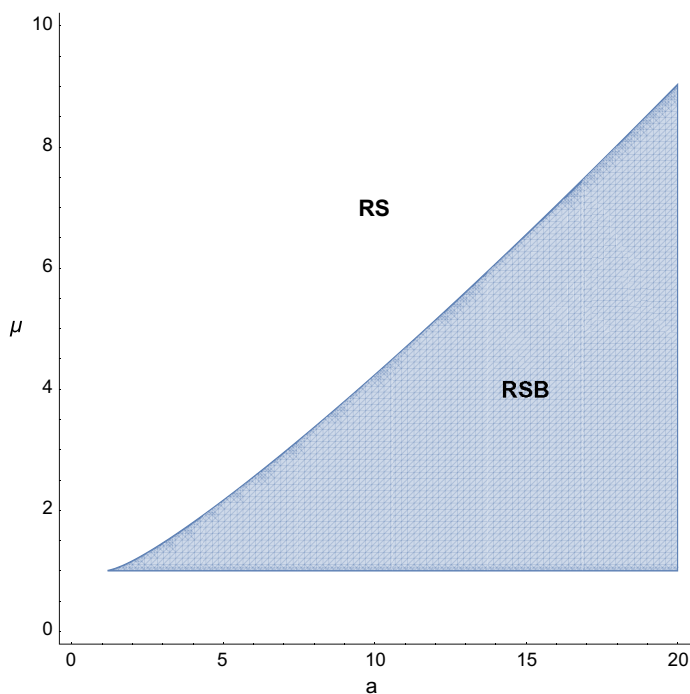


Fig. 1 Schematic Phase diagram in (a, μ) plane. In the shaded region of parameters $1 < \mu < \frac{(a^{2/3} - a^{1/3} + 1)^3}{a}$ replica symmetry can be fully broken for some amplitude of the noise

nomial equation, see Eq. (57). At the same time, using that for large enough scaled NSR $\tilde{\gamma} > \tilde{\gamma}_{AT}^{(2)}$ the replica symmetry is restored, one can employ the RS equation Eq. (57) to determine the behaviour of the quality parameter $p_\infty(\tilde{\gamma})$ as $\tilde{\gamma} \rightarrow \infty$. One finds that in all cases but one this quantity vanishes for asymptotically large values of NSR as $p_\infty \sim \tilde{\gamma}^{-1/2}$, see Eq. (58), i.e. in qualitatively the same way as for purely linear system with $a = 0$.

The only exceptional case, showing qualitatively different behaviour to the above picture, is that of *purely quadratic* encryption with vanishing linear component,² when $J_1 \rightarrow 0$ at a fixed value of $J_2 > 0$. The appropriately rescaled NSR in this case is $\hat{\gamma} = \frac{\gamma}{J_2^2 R^2}$. In this

limit the second threshold $\tilde{\gamma}_{AT}^{(2)}$ escapes to infinity and the replica symmetry is broken for *all* $\hat{\gamma} > \hat{\gamma}_{AT} = (\mu - 1)^2/\mu$. Moreover, most importantly there exists a threshold NSR value $\hat{\gamma}_c = \mu - \frac{1}{2} > \hat{\gamma}_{AT}$ such that $p_\infty = 0$ for $\hat{\gamma} > \hat{\gamma}_c$ making the reconstruction impossible. The full curve $p_\infty(\hat{\gamma})$ can be explicitly described in this case analytically. In particular, the behaviour close to the threshold NSR is given by $p_\infty \sim (\hat{\gamma}_c - \hat{\gamma})^{3/4}$ and the non-trivial exponent 3/4 is completely controlled by the FRSB mechanism.

The existence of a sharp NSR threshold $\hat{\gamma}_c$ in the pure quadratic encryption case may have useful consequences for security of transmitting the encrypted signal. Indeed, it is a quite common assumption that an eavesdropper may get access to the transmitted signal by a channel with inferior quality, characterized by higher level of noise. This may then result in impossibility for eavesdroppers to reconstruct the quadratically encoded signal even if the encoding algorithm is perfectly known to them.

1.2.2 General Remarks on the Method

The task of optimizing various random 'cost functions', not unlike $\mathcal{H}_s(\mathbf{x})$ in Eq. (7), is long known to be facilitated by a recourse to the methods of statistical mechanics, see e.g. [34] and [31] for early references and introduction to the method. In that framework one encounters the task of evaluating expected values over distributions of random variables coming through the cost function in both numerator and denominator of the equations describing the quantities of interest, see the right-hand side of Eq. (22) below. Performing such averaging is known to be one of the central technical problems in the theory of disordered systems. One of the most powerful, though non-rigorous, methods of dealing with this problem at the level of theoretical physics is the (in)famous replica trick, see [31] and references therein. A considerable progress achieved in the last decades in developing rigorous aspects of that theory [4,33] makes this task, in principle, feasible for the cases when the random energy function $\mathcal{H}_s(\mathbf{x})$ is *Gaussian*-distributed. The model where configurations are restricted to the surface of a sphere are known in the spin-glass literature as 'spherical models', but their successful treatment, originally nonrigorous [13,14,27] and in recent years rigorous [1,5, 11,12,40,41], seems again be restricted to the normally-distributed case. In the present [2] case however the cost function is *per se* not Gaussian, but represented as a sum of *squared* Gaussian-distributed terms. We are not aware of any systematic treatment of spherical spin glass models with such type of spin interaction. Some results obtained by extending replica trick treatment to this type of random functions were given by the present author in [18], but details were never published. To present the corresponding method on a meaningful example is one of the goals of the present paper. Indeed, we shall see that, with due modifications,

² It is worth noting that in the absence of linear component the encryption mapping $V(\mathbf{s})$ in Eq. (11) becomes invariant with respect to the reflections $\mathbf{s} \rightarrow -\mathbf{s}$. As a result, the least-square reconstruction may formally return solutions with negative values of the parameter p_N in Eq. (4). To avoid this we consider the pure quadratic case as the limit $J_1 \rightarrow 0$ taken *after* $N \rightarrow \infty$, which is enough to break the mentioned invariance.

the method is very efficient, and, when combined with the Parisi replica symmetry breaking Ansatz allows to get a reasonably detailed insight into the reconstruction problem. As squared gaussian-distributed terms are common to many optimization problems based on the Least Square method, one may hope that the approach proposed in the present paper may prove to be of wider utility. In particular, an interesting direction of future research may be study of the minima, saddles and other structures of this type in the arising 'optimization landscape' following an impressive recent progress in this direction for Gaussian spherical model, see [35] and references therein. This may help to devise better search algorithms for solutions of the optimization problems of this type.

Another technical aspect of our treatment which is worth mentioning is as follows. In problems of this sort replica treatment is much facilitated by noticing that after performing the disorder averaging the replicated partition function possesses a high degree of invariance: an arbitrary simultaneous $O(N)$ rotation of all n replica vectors \mathbf{x}_a , $a = 1, \dots, n$ leaves the integrand invariant. To exploit such an invariance in the most efficient way one may use a method suggested in the framework of Random Matrix Theory in the works [17,23]³ That method allowed one to convert the integrals over N -component vectors \mathbf{x}_a , $a = 1, \dots, n$ to a single positive-definite $n \times n$ matrix $Q_{ab} \geq 0$. Such transformation then allows to represent the integrand in a form ideally suited for extracting the large- N asymptotic of the integral. In the context of spin glasses and related statistical mechanics systems this method was first successfully used in [22] and then [20,21], and most recently in [29], and proved to be a very efficient framework for implementing the Parisi FRSB scheme. In the present problem however the integrand has lesser invariance due to presence of a fixed direction exemplified by the original message \mathbf{s} . Namely, it is invariant only with respect to rotations forming a subgroup of $O(N)$ consisting of all $N \times N$ orthogonal transformations O_s satisfying $O_s^T O_s = \mathbf{1}_N$ and $O_s \mathbf{s} = \mathbf{s}$. In the Appendix C we prove a Theorem which is instrumental in adjusting our approach to the present case of a fixed direction. One may hope that this generalization may have other applications beyond the present problem.

2 Statistical Mechanics Approach to Reconstruction Problem

2.1 General Setting of the Problem

To put the least square minimization problem Eq. (2) in the context of Statistical Mechanics, one follows the standard route and interprets the cost function in Eq. (7) as an energy associated with a configuration \mathbf{x}^T of N spin variables (x_1, \dots, x_N) , constrained to the sphere of radius $|\mathbf{x}| = N\sqrt{R}$. This allows one to treat our minimization problem as a problem of Statistical Mechanics, by introducing the temperature parameter $T > 0$, and considering the Boltzmann-Gibbs weights $\pi_\beta(\mathbf{x}) = \mathcal{Z}_\beta^{-1} e^{-\beta \mathcal{H}_s(\mathbf{x})}$ associated with any configuration \mathbf{x} on the sphere, with \mathcal{Z}_β being the partition function of the model for the inverse temperature $\beta = T^{-1}$:

$$\mathcal{Z}_\beta = \int_{|\mathbf{x}|=R\sqrt{N}} e^{-\beta \mathcal{H}_s(\mathbf{x})} d\mathbf{x}, \quad d\mathbf{x} = \prod_{i=1}^N dx_i. \quad (21)$$

The power of the method is that in the zero-temperature limit $\beta \rightarrow \infty$ the Boltzmann-Gibbs weights concentrate on the set of globally minimal values of the cost function, so that for any well-behaving function $g(\mathbf{x})$ the thermal average value $g_\beta(\mathbf{x}) := \int g(\mathbf{x}) \pi_\beta(\mathbf{x}) d\mathbf{x}$ should

³ Equivalent transformations were also suggested earlier in [36], see also [15].

tend to the value of that function evaluated at the argument corresponding to solutions of the minimization problem Eq. (2). To this end we introduce the thermal average $p_N^{(\beta)}$ of the distance function defined in Eq. (3) and consider its expected value with respect to both the set of random functions $V_k(\mathbf{x})$ and the noise \mathbf{b} :

$$\left\langle p_N^{(\beta)} \right\rangle := \left\langle \frac{1}{\mathcal{Z}_\beta} \int_{|\mathbf{x}|=R\sqrt{N}} \frac{(\mathbf{x}, \mathbf{s})}{NR^2} e^{-\beta \mathcal{H}_s(\mathbf{x})} d\mathbf{x} \right\rangle_{V, \mathbf{b}}. \quad (22)$$

Our goal is to evaluate the above quantity for finite $\beta = 1/T$ in the limit of large $N \gg 1$, and eventually perform the zero temperature limit $T \rightarrow 0$ thus extracting $p_\infty := \lim_{\beta \rightarrow \infty} \lim_{N \rightarrow \infty} \left\langle p_N^{(\beta)} \right\rangle$ providing us with a measure of the quality of the asymptotic signal reconstruction in the original optimization problem.

2.2 Replica Trick

The main challenge in evaluating the right-hand side in Eq. (22) is related to presence of random Gaussian variables entering $\mathcal{H}_s(\mathbf{x})$ both in the integrand and through the normalization factor $1/\mathcal{Z}_\beta$ in the Boltzmann–Gibbs weights. To bypass this difficulty we follow the framework of the replica trick by representing the normalization factor formally as $1/\mathcal{Z}_\beta = \lim_{n \rightarrow 0} \mathcal{Z}_\beta^{n-1}$ and treating the parameter n before the limit as a positive integer. Employing Eq. (21) for each factor in \mathcal{Z}_β^{n-1} one than can represent Eq. (22) formally as

$$\left\langle p_N^{(\beta)} \right\rangle = \lim_{n \rightarrow 0} \left\langle p_{N,n}^{(\beta)} \right\rangle, \quad (23)$$

where we defined

$$\left\langle p_{N,n}^{(\beta)} \right\rangle = \int_{|\mathbf{x}_1|=R\sqrt{N}} \cdots \int_{|\mathbf{x}_n|=R\sqrt{N}} \left[\frac{1}{n} \sum_{c=1}^n \frac{(\mathbf{x}_c, \mathbf{s})}{NR^2} \right] \left\langle e^{-\beta \sum_{a=1}^n \mathcal{H}_s(\mathbf{x}_a)} \right\rangle \prod_{a=1}^n d\mathbf{x}_a. \quad (24)$$

The disorder average can be now performed in the following steps. First, using the additive form of the cost function in Eq. (7) and independence of $\mathcal{H}_s^{(k)}(\mathbf{x}_a)$ for different $k = 1, \dots, M$ we obviously have

$$\left\langle e^{-\beta \sum_{a=1}^n \mathcal{H}_s(\mathbf{x}_a)} \right\rangle = \left\langle e^{-\beta \sum_{a=1}^n \mathcal{H}_s^{(k)}(\mathbf{x}_a)} \right\rangle^M. \quad (25)$$

Using the Gaussian nature of $V(\mathbf{x})$ entering to $\mathcal{H}_s^{(k)}(\mathbf{x})$ in a squared form, see Eq. (7), and exploiting the covariance structure Eq. (5) one can show that

$$\left\langle e^{-\beta \sum_{a=1}^n \mathcal{H}_s^{(k)}(\mathbf{x}_a)} \right\rangle = [\det \mathcal{G}(\mathbf{x}_1, \dots, \mathbf{x}_n; \mathbf{s})]^{-1/2}, \quad (26)$$

where we have introduced the (positive definite) $n \times n$ matrix $\mathcal{G}(\mathbf{x}_1, \dots, \mathbf{x}_n; \mathbf{s})$ with entries

$$\begin{aligned} \mathcal{G}_{ab}(\mathbf{x}_1, \dots, \mathbf{x}_n; \mathbf{s}) &= \delta_{ab} \\ &+ \beta \left[\sigma^2 + \Phi(R^2) + \Phi\left(\frac{(\mathbf{x}_a, \mathbf{x}_b)}{N}\right) - \Phi\left(\frac{(\mathbf{x}_a, \mathbf{s})}{N}\right) - \Phi\left(\frac{(\mathbf{x}_b, \mathbf{s})}{N}\right) \right]. \end{aligned} \quad (27)$$

For convenience of the reader we provide a derivation of the formula Eq. (26) in the Appendix B. Note that this result is well-known in the probability literature, see e.g. [26]. We see that

$$\left\langle p_{N,n}^{(\beta)} \right\rangle = \int_{|\mathbf{x}_a|=R\sqrt{N}} \left[\frac{1}{n} \sum_{c=1}^n \frac{(\mathbf{x}_c, \mathbf{s})}{NR^2} \right] [\det \mathcal{G}(\mathbf{x}_1, \dots, \mathbf{x}_n; \mathbf{s})]^{-M/2} \prod_{a=1}^n d\mathbf{x}_a. \quad (28)$$

At this step it is very helpful to notice that the integrand in Eq. (28) possesses a high degree of invariance. Namely, consider all possible rotations around the axis whose direction is given by the vector \mathbf{s} . Such rotations form a subgroup of $O(N)$ consisting of all $N \times N$ orthogonal transformations $O_{\mathbf{s}}$ satisfying $O_{\mathbf{s}}^T O_{\mathbf{s}} = \mathbf{1}_N$ and $O_{\mathbf{s}} \mathbf{s} = \mathbf{s}$. Then the integrand in Eq. (28) remains invariant under a simultaneous change $\mathbf{x}_a \rightarrow O_{\mathbf{s}} \mathbf{x}_a$ for all $a = 1, \dots, n$. In the Appendix C we prove a Theorem which is instrumental for implementing our previous approach to similar problems [22] to the present case of somewhat lesser invariance. Not surprisingly, in such a case the integration needs to go not only over $n \times n$ matrix of scalar products $Q_{ab} = (\mathbf{x}_a, \mathbf{x}_b) \geq 0$, but also over an n -component vector $\mathbf{t} = (t_1, \dots, t_n) \in \mathbb{R}^n$ of projections $t_a = (\mathbf{x}_a, \mathbf{s})$. Applying the Theorem and rescaling for convenience the integration variables $Q_{ab} \rightarrow N Q_{ab}$ and $\mathbf{t} \rightarrow \sqrt{N} \mathbf{t}$ we bring Eq. (29) to the form

$$\left\langle p_{N,n}^{(\beta)} \right\rangle = N^{\frac{n(N-n-1)}{2}} C_{N-1,n}^{(o)} \int_{D_n} \left[\frac{1}{n} \sum_{c=1}^n \frac{t_c}{R} \right] [\det Q]^{-\frac{(n+2)}{2}} e^{-\frac{N}{2} F(Q, \mathbf{t})} dQ d\mathbf{t}, \quad (29)$$

where $C_{N,n}^{(o)}$ is defined in Eq. (110), the integration goes over the domain

$$D_n : (Q > 0, \quad \mathbf{t} \in \mathbb{R}^n, \quad Q_{aa} + t_a^2 = R^2, \quad \forall a = 1, \dots, n) \quad (30)$$

and we defined

$$F(Q, \mathbf{t}) = \mu \text{Tr} \ln [\mathbf{1}_n + \beta g(Q, \mathbf{t})] - \text{Tr} \ln Q, \quad (31)$$

with $n \times n$ matrix $g(Q, \mathbf{t})$ characterized by its entries (cf. Eq. (27))

$$g_{ab}(Q, \mathbf{t}) = \sigma^2 + \Phi(R^2) + \Phi(Q_{ab} + t_a t_b) - \Phi(R t_a) - \Phi(R t_b). \quad (32)$$

So far our treatment of $\left\langle p_{N,n}^{(\beta)} \right\rangle$ was exact for any positive integer values N and n satisfying $N > n + 1$ and involved no approximations. Our goal is however to extract the leading behaviour of that object as $N \gg 1$ and allowing formally n to take non-integer values to be able to perform the replica limit $n \rightarrow 0$.

2.3 Variational Problem in the Framework of the Parisi Ansatz

Clearly, the form of the integrand in Eq. (29) being proportional to the factor $e^{-\frac{N}{2} F(Q, \mathbf{t})}$ is suggestive of using the Laplace (a.k.a saddle-point or steepest descent) method. In following this route we resort to a non-rigorous and heuristic, but computationally efficient scheme of Parisi replica symmetry breaking [31]. We implement this scheme in a particular variant most natural for models with rotational invariance, going back to Crisanti and Sommers paper [13], and somewhat better explained in the Appendix A of [22], and in even more detail in the Appendix C of [19]. We therefore won't discuss the method itself in the present paper, only giving a brief account of necessary steps.

The scheme starts with a standard assumption that in the replica limit $n \rightarrow 0$ the integral is dominated by configurations of matrices Q which for finite integer n have a special hierarchically built structure characterized by the sequence of integers

$$n = m_0 \geq m_1 \geq m_2 \geq \dots \geq m_k \geq m_{k+1} = 1 \quad (33)$$

and the values placed in the off-diagonal entries of the Q matrix block-wise, and satisfying:

$$0 < q_0 \leq q_1 \leq q_2 \leq \dots \leq q_k. \quad (34)$$

Finally, we complete the procedure by filling in the n diagonal entries Q_{aa} of the matrix Q with one and the same value $Q_{aa} = q_d := q_{k+1} \geq q_k$. Note that in our particular case the diagonal entries q_d must in fact be chosen in the form $q_d = R^2 - t_a^2$, in order to respect the constraints imposed by the integration domain Eq. (30). As to the vector \mathbf{t} of variables t_a , we are making an additional assumption that with respect to those variables the integral is in fact dominated by equal values: $t_a = t, \forall a = 1, \dots, n$.

Obviously, the matrix $g(Q, \mathbf{t})$ defined in Eq. (32) inherits the hierarchical structure from Q , with parameters $m_l, l = 0, \dots, k+1$ shared by both matrices, but parameters q_l replaced by parameters g_l given by

$$g_l = \sigma^2 + \Phi(R^2) - 2\Phi(Rt) + \Phi(q_l + t^2), \quad l = 0, 1, \dots, k \quad (35)$$

and

$$g_{k+1} = \sigma^2 + 2\Phi(R^2) - 2\Phi(Rt) := g_d.$$

The next task of the scheme is to express both $\text{Tr} \ln g(Q, \mathbf{t})$ and $\text{Tr} \ln Q$ in terms of the parameters entering Eqs. (33) and (34). This is most easily achieved by writing down all distinct eigenvalues $\lambda_1, \dots, \lambda_{k+2}$ of the involved matrices, and their degeneracies $d_{i+2} = n(m_{i+1}^{-1} - m_i^{-1}) \forall i = 0, \dots, k$, and $d_1 = 1$. For the matrix Q those eigenvalues are listed, e.g., in the appendix C of [19], and for the matrix $g(Q, \mathbf{t})$ the corresponding expressions can be obtained from those for Q by replacing q_l by parameters g_l from Eq. (35). The subsequent treatment is much facilitated by introducing the following (generalized) function of the variable q :

$$x(q) = n + \sum_{l=0}^k (m_{l+1} - m_l) \theta(q - q_l), \quad (36)$$

where we use the notation $\theta(z)$ for the Heaviside step function: $\theta(z) = 1$ for $z > 0$ and zero otherwise. In view of the inequalities Eqs. (33, 34) the function $x(q)$ is piecewise-constant non-increasing, and changes between $x(0 < q < q_0) = m_0 \equiv n$ through $x(q_{i-1} < q < q_i) = m_i$ for $i = 1, \dots, k$ to finally $x(q_k < q < q_d) = m_{k+1} \equiv 1$. A clever observation by Crisanti and Sommers allows one to express eigenvalues of any function of the hierarchical matrix Q in terms of simple integrals involving $x(q)$. In particular, for eigenvalues $\lambda_i^{(g)}$ of the matrix $g(Q, \mathbf{t})$ we have:

$$\lambda_1^{(g)} = \int_0^{q_d} x(q) \frac{dg_t}{dq} dq, \quad \text{and} \quad \lambda_{i+2}^{(g)} = \int_{q_i}^{q_d} x(q) \frac{dg_t}{dq} dq, \quad i = 0, \dots, k, \quad (37)$$

where we introduced a piecewise-continuous function $g_t(q), q \in [0, q_d]$ such that in the interval $q \in [q_0, q_k]$ it is given by

$$g_t(q_0 \leq q \leq q_k) = \sigma^2 + \Phi(R^2) - 2\Phi(Rt) + \Phi(q + t^2), \quad (38)$$

whereas outside that interval it has two constant values:

$$g_t(0 \leq q < q_0) = 0 \quad \text{and} \quad g_t(q_k < q \leq q_d := q_{k+1}) = \sigma^2 + 2\Phi(R^2) - 2\Phi(Rt). \quad (39)$$

In particular, $\lambda_1^{(g)}$ can be further rewritten as

$$\lambda_1^{(g)} = \int_0^{q_0} x(q) \frac{dg_t}{dq} dq + \int_{q_0}^{q_d} x(q) \frac{dg_t}{dq} dq = n g_t(q_0) + \int_{q_0}^{q_d} x(q) \frac{dg_t}{dq} dq. \quad (40)$$

Such a representation, together with the definition Eq. (36) of the function $x(q)$ facilitates calculating quantities interesting to us in the replica limit as:

$$\begin{aligned} \lim_{n \rightarrow 0} \frac{1}{n} \text{Tr} \ln (\mathbf{1}_n + \beta g(Q, \mathbf{t})) &= \lim_{n \rightarrow 0} \frac{1}{n} \left[\ln \left(1 + \beta \lambda_1^{(g)} \right) + \sum_{i=0}^k d_{i+2} \ln \left(1 + \beta \lambda_{i+2}^{(g)} \right) \right] \\ &= \lim_{n \rightarrow 0} \frac{1}{n} \ln \left(1 + \beta n g_t(q_0) + \beta \int_{q_0}^{q_d} x(q) \frac{dg_t}{dq} dq \right) \\ &\quad + \lim_{n \rightarrow 0} \int_{q_0-0}^{q_k+0} \ln \left(1 + \beta \int_q^{q_d} x(q) \frac{dg_t}{dq} dq \right) \frac{d}{dq} \left[\frac{1}{x(q)} \right] dq. \end{aligned} \quad (41)$$

In the last term it is convenient to integrate by parts, and use $x(q_k+0) = 1$ and $x(q_0-0) = n$, which after obvious regrouping of terms reduces the right-hand side of Eq. (41) as

$$\begin{aligned} \lim_{n \rightarrow 0} \frac{1}{n} \left[\ln \left(1 + \beta n g_t(q_0) + \beta \int_{q_0}^{q_d} x(q) g'_t(q) dq \right) - \ln \left(1 + \beta \int_{q_0}^{q_d} x(q) g'_t(q) dq \right) \right] \\ + \lim_{n \rightarrow 0} \left\{ \ln [1 + \beta (g_t(q_d) - g_t(q_k))] + \beta \int_{q_0}^{q_k} \frac{g'_t(q) dq}{1 + \beta \int_q^{q_d} x(\tilde{q}) g'_t(\tilde{q}) d\tilde{q}} \right\}, \end{aligned} \quad (42)$$

where we denoted $g'_t(q) := \frac{dg_t}{dq}$. The limit $n \rightarrow 0$ is now easy to perform following the general prescription of the Parisi method: in such a limit the inequality Eq. (33) should be reversed:

$$n = 0 \leq m_1 \leq m_2 \leq \dots \leq m_k \leq m_{k+1} = 1, \quad (43)$$

and the function $x(q)$ is now transformed to a non-decreasing function of the variable q in the interval $q_0 \leq q \leq q_k$, and satisfying outside that interval the following properties

$$x(q < q_0) = 0, \quad \text{and} \quad x(q > q_k) = 1. \quad (44)$$

In general, such a function also depends on the increasing sequence of k real parameters m_l described in Eq. (43). Performing the corresponding limit and taking into account that in view of $x(q < q_0) = 0$ we have

$$\int_0^{q_0} \frac{g'_t(q) dq}{1 + \beta \int_q^{q_d} x(\tilde{q}) g'_t(\tilde{q}) d\tilde{q}} = \frac{g_t(q_0)}{1 + \beta \int_{q_0}^{q_d} x(q) g'_t(q) dq},$$

we eventually see that

$$\begin{aligned} \lim_{n \rightarrow 0} \frac{1}{n} \text{Tr} \ln (\mathbf{1}_n + \beta g(Q, \mathbf{t})) &= \ln [1 + \beta (g_t(q_d) - g_t(q_k))] \\ &\quad + \beta \int_0^{q_k} \frac{g'_t(q) dq}{1 + \beta \int_q^{q_d} x(\tilde{q}) g'_t(\tilde{q}) d\tilde{q}}, \end{aligned} \quad (45)$$

and by a similar calculation also find:

$$\lim_{n \rightarrow 0} \frac{1}{n} \text{Tr} \ln Q = \ln (q_d - q_k) + \int_0^{q_k} \frac{dq}{\int_q^{q_d} x(\tilde{q}) d\tilde{q}}. \quad (46)$$

The two formulas Eqs. (45)–(46) provide us therefore with a full formal control of the main exponential factor $e^{-\frac{N}{2} F(Q, \mathbf{t})}$ in Eq. (29) for $N \rightarrow \infty$ in the replica limit $n \rightarrow 0$. Note that the fact that the limit in the left hand-side of Eq. (46) is finite implies also that $\det Q|_{n \rightarrow 0} \rightarrow 1$ further implying $[\det Q]^{-\frac{(n+2)}{2}}|_{n \rightarrow 0} = 1$ in Eq. (29). Collecting finally all factors in Eq. (29)

when performing the replica limit $n \rightarrow 0$, using explicit forms Eqs. (38)–(39), remembering $q_d = R^2 - t^2$ and finally understanding by $x(q)$ only its non-trivial part in the interval q_0, q_k we arrive to the following

Proposition 2.1 *Given the values of real parameters $R > 0$ and $\mu > 1$, consider the functional*

$$\begin{aligned} \phi[x(q); q_0, q_k, t] = & \mu \ln(1 + \beta [\Phi(R^2) - \Phi(q_k + t^2)]) - \ln(R^2 - t^2 - q_k) \\ & + \mu \frac{\beta [\sigma^2 + \Phi(R^2) - 2\Phi(Rt) + \Phi(q_0 + t^2)]}{1 + \beta [\Phi(R^2) - \Phi(q_k + t^2)] + \beta \int_{q_0}^{q_k} x(u) \Phi'(u + t^2) du} \\ & - \frac{q_0}{R^2 - t^2 - q_k + \int_{q_0}^{q_k} x(u) du} \\ & + \mu \beta \int_{q_0}^{q_k} \frac{\Phi'(q + t^2) dq}{1 + \beta [\Phi(R^2) - \Phi(q_k + t^2)] + \beta \int_q^{q_k} x(u) \Phi'(u + t^2) du} \\ & - \int_{q_0}^{q_k} \frac{dq}{R^2 - t^2 - q_k + \int_q^{q_k} x(u) du} \quad , \end{aligned} \quad (47)$$

which depends on the parameters $-R \leq t \leq R$, and $0 \leq q_0 \leq q_k < q_d = R^2 - t^2$ and a non-decreasing function $x(q)$ of the variable q in the interval $q_0 \leq q \leq q_k$. Then in the framework of the replica trick the asymptotic mean value of the quality parameter $\langle p_N^{(\beta)} \rangle$ as $N \rightarrow \infty$ is given by

$$\lim_{N \rightarrow \infty} \langle p_N^{(\beta)} \rangle = \frac{t}{R} \quad , \quad (48)$$

where the specific value of the parameter t is found by simultaneously minimizing the functional $\phi[x(q); q_0, q_k, t]$ over t and maximizing it over all other parameters and the function $x(q)$.

Recall, however, that for the purposes of our main goal the quantity $\langle p_N^{(\beta)} \rangle$ is only of auxiliary interest, and is used to provide an access to its 'zero-temperature' limit $\beta = \frac{1}{T} \rightarrow \infty$ which is expected to coincide with the quality parameter characterizing the performance of our signal reconstruction scheme. A simple inspection shows that in such a limit the combination $T\phi[x(q); q_0, q_k, t]$ does have a well-defined finite value if we make the following *low temperature Ansatz* valid for $T \rightarrow 0$

$$q_k = R^2 - t^2 - vT, \quad q_0 = R^2 - t^2 - Q, \quad \beta x(u) \rightarrow w(u) := w_s(u + t^2) \quad , \quad (49)$$

with v, Q and $w_s(u)$ tending to a well-defined finite limit as $T \rightarrow 0$. Performing the corresponding limit in Eq. (47) and changing $u \rightarrow u - t^2$ one arrives at the statement of the **Proposition 1** in the Main Results section.

3 Analysis of the Variational Problem

To solve the arising problem of extremizing the functional $\mathcal{E}[w_s(u); Q, v, t]$ from Eq. (14) we first consider the stationarity equations with respect to three parameters: t, Q and v . The

conditions $\frac{\partial \mathcal{E}}{\partial t} = 0$ and $\frac{\partial \mathcal{E}}{\partial Q} = 0$ yield the two equations, the first being

$$\frac{t}{v + \int_{R^2-Q}^{R^2} w_s(u) du} = \mu \frac{R\Phi'(Rt)}{1 + v\Phi'(R^2) + \int_{R^2-Q}^{R^2} w_s(u)\Phi'(u) du}, \quad (50)$$

and, assuming that $w_s(R^2 - Q) \neq 0$, the second one:

$$\frac{R^2 - t^2 - Q}{\left(v + \int_{R^2-Q}^{R^2} w_s(u) du\right)^2} = \mu \Phi'(R^2 - Q) \frac{\sigma^2 + \Phi(R^2) - 2\Phi(Rt) + \Phi(R^2 - Q)}{\left(1 + v\Phi'(R^2) + \int_{R^2-Q}^{R^2} w_s(u)\Phi'(u) du\right)^2}. \quad (51)$$

The Eq. (51) can be used to simplify the third equation arising from the stationarity condition $\frac{\partial \mathcal{E}}{\partial v} = 0$ bringing it eventually to the following form:

$$\begin{aligned} & \frac{R^2 - t^2 - Q}{\left(v + \int_{R^2-Q}^{R^2} w_s(u) du\right)^2} \left[1 - \frac{\Phi'(R^2)}{\Phi'(R^2 - Q)}\right] + \int_{R^2-Q}^{R^2} \frac{dq}{\left(v + \int_q^{R^2} w_s(u) du\right)^2} \\ & = \mu \Phi'(R^2) \int_{R^2-Q}^{R^2} \frac{\Phi'(q) dq}{\left(1 + v\Phi'(R^2) + \int_q^{R^2} w_s(u)\Phi'(u) du\right)^2}. \end{aligned} \quad (52)$$

3.1 Replica Symmetric Solution

Notice that the last equation Eq. (52) is identically satisfied with the choice $Q = 0$, defining the so-called Replica Symmetric (RS) solution. For such a choice the interval $[R^2 - Q, R^2]$ of the support of the function $w_s(u)$ shrinks to a point, making that function immaterial for the variational procedure. Moreover, the equations Eqs. (50)–(51) drastically simplify yielding the pair:

$$\frac{t}{v} = \mu \frac{R\Phi'(Rt)}{1 + v\Phi'(R^2)}, \quad \frac{R^2 - t^2}{v^2} = \mu \Phi'(R^2) \frac{\sigma^2 + 2\Phi(R^2) - 2\Phi(Rt)}{(1 + v\Phi'(R^2))^2}. \quad (53)$$

Remarkably, this pair can be further reduced to a single equation in the variable $p = t/R$, precisely one given in the list of Main Results, see Eq. (18), thus providing the asymptotic value of the quality reconstruction parameter $p_\infty = p$.

As expected, in the case of no noise $\gamma = 0$ the solution of Eq. (18) is provided by $p = 1$ corresponding to the perfect reconstruction of the source signal. It is also easy to treat the equation perturbatively in the case of weak noise $\gamma \rightarrow 0$ and obtain to the leading order:

$$p = 1 - \frac{\gamma}{2(\mu - 1)\Phi'(R^2)} + o(\gamma). \quad (54)$$

In particular, this result agrees with the first-order perturbation theory analysis for the linear case $\Phi(u) = u$, see Eq. (10) and Appendix A, and generalizes it to a generic nonlinearity. It also emphasizes the natural fact that the signal recovery becomes very sensitive to the noise for the values of ERP $\mu \rightarrow 1$.

For the linear-quadratic family Eq. (11) with the covariance structure of the form $\Phi(u) = J_1^2 u + \frac{1}{2} J_2^2 u^2$ the equation Eq. (18) can be readily studied non-perturbatively for any value of NSR. We start with two limiting cases in the family: that of 'purely linear' and 'purely

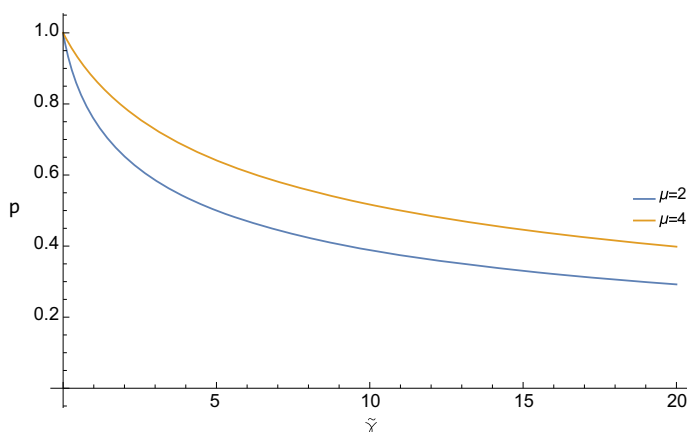


Fig. 2 The quality parameter p as a function of the scaled noise-to-signal ratio $\tilde{\gamma}$ for purely linear encryptions and two different values of the ERP, $\mu = 2$ and $\mu = 4$

quadratic' encryptions. In the former case $J_2 = 0$, but $J_1 \neq 0$ and after introducing the scaled NSR $\tilde{\gamma} := \gamma/J_1^2$ we arrive at a cubic equation

$$p^2 (\tilde{\gamma} + 2(1 - p)) = \mu(1 - p^2) . \quad (55)$$

In particular, p is nonvanishing for any value of the scaled NSR $0 \leq \tilde{\gamma} < \infty$, and tends to zero as $p \sim \sqrt{\mu/\tilde{\gamma}}$ for $\tilde{\gamma} \gg 1$, in full agreement with the direct perturbation theory approach, see appendix A. For intermediate NSR values the solution can be easily plotted numerically, see Fig. 2.

In the opposite case of purely quadratic encryption when $J_1 = 0$ but $J_2 \neq 0$ the equation Eq. (18) is biquadratic, so that one can find the RS solution explicitly. Introducing the rescaled NSR pertinent to this limit as $\hat{\gamma} := \frac{\gamma}{J_2^2 R^2}$ we have

$$p = \begin{cases} \sqrt{1 - \frac{\hat{\gamma}}{\mu-1}} & \text{if } \hat{\gamma} \leq \hat{\gamma}_c^{(RS)} := \mu - 1 \\ 0 & \hat{\gamma} > \hat{\gamma}_c^{(RS)} \end{cases} . \quad (56)$$

Thus, in this case the replica-symmetric solution predicts the existence of a NSR threshold $\hat{\gamma}_c^{(RS)} = \mu - 1$ beyond which meaningful reconstruction of the encrypted signal is impossible. We will see later on that although this conclusion is qualitatively correct, the actual value for the threshold and the critical exponent controlling the behaviour close to the threshold is different and is obtained when the phenomenon of the replica symmetry breaking is taken into account.

Finally, in the case of a generic linear-quadratic encryption with both $J_1 \neq 0$ and $J_2 \neq 0$ the resulting equation Eq. (18) is a general polynomial of the fourth degree. Introducing again the scaled NSR $\tilde{\gamma} := \gamma/J_1^2$ and a parameter characterizing effective non-linearity of the mapping $a := (R J_2/J_1)^2$ we can rewrite the equation as:

$$(1 + a)p^2 (\tilde{\gamma} + 2(1 - p) + a(1 - p^2)) = \mu(1 - p^2)(1 + ap^2) . \quad (57)$$

In particular, we see that p tends to zero as NSR $\tilde{\gamma} \rightarrow \infty$ as in the purely linear case:

$$p = \sqrt{\frac{\mu}{1+a} \frac{1}{\tilde{\gamma}}} + o(\tilde{\gamma}^{-1/2}) . \quad (58)$$

We will see in the next section that generically for linear-quadratic encryptions with big enough, but finite nonlinear component $1 < a < \infty$ the replica-symmetric solution of the variational problem is not correct in some interval of the scaled NSR $\tilde{\gamma}_{AT}^{(1)} < \tilde{\gamma} < \tilde{\gamma}_{AT}^{(2)}$, and should be replaced with one involving $Q \neq 0$. Nevertheless, asymptotic decay of the quality parameter p for $\gamma \rightarrow \infty$ is always given by Eq. (58), apart from the only limiting case of purely quadratic encryption, when $a \rightarrow \infty$.

3.2 Solution with Fully Broken Replica Symmetry

The goal of the present section is to seek for a solution of the variational problem for the functional Eq. (14) which breaks the replica symmetry, so that $Q > 0$. Doing this necessarily implies taking the function $w_s(u)$ into account, and deriving the equation involving such a function. The corresponding equation is obtained by requiring stationarity of the functional \mathcal{E} with respect to a variation of $w_s(u)$, assuming that function to be continuous in the interval $u \in [R^2 - Q, R^2]$. Let us reiterate that this potentially includes the case of 1RSB solutions corresponding to $w_s(u) = w = \text{const}$, $\forall u \in [R^2 - Q, R^2]$. For every value of q in that interval it yields the equation

$$\begin{aligned} & \frac{R^2 - t^2 - Q}{\left(v + \int_{R^2-Q}^{R^2} w_s(u) du\right)^2} + \int_{R^2-Q}^q \frac{d\tilde{q}}{\left(v + \int_{\tilde{q}}^{R^2} w_s(u) du\right)^2} \\ &= \mu \Phi'(q) \left[\frac{\sigma^2 + \Phi(R^2) - 2\Phi(Rt) + \Phi(R^2 - Q)}{\left(1 + v\Phi'(R^2) + \int_{R^2-Q}^{R^2} w_s(u)\Phi'(u) du\right)^2} \right. \\ & \quad \left. + \int_{R^2-Q}^q \frac{\Phi'(\tilde{q})d\tilde{q}}{\left(1 + v\Phi'(R^2) + \int_{\tilde{q}}^{R^2} w_s(u)\Phi'(u) du\right)^2} \right], \end{aligned} \quad (59)$$

which using again Eq.(51) can be simplified into

$$\begin{aligned} & \frac{R^2 - t^2 - Q}{\left(v + \int_{R^2-Q}^{R^2} w_s(u) du\right)^2} \left[1 - \frac{\Phi'(q)}{\Phi'(R^2 - Q)} \right] + \int_{R^2-Q}^q \frac{d\tilde{q}}{\left(v + \int_{\tilde{q}}^{R^2} w_s(u) du\right)^2} \\ &= \mu \Phi'(q) \int_{R^2-Q}^q \frac{\Phi'(\tilde{q})d\tilde{q}}{\left(1 + v\Phi'(R^2) + \int_{\tilde{q}}^{R^2} w_s(u)\Phi'(u) du\right)^2}. \end{aligned} \quad (60)$$

Our first observation is that setting $q = R^2$ in Eq. (60) in fact reproduces Eq. (52), so the fundamental system comprises three rather than four independent stationarity conditions: Eqs. (50), (51) and either Eq. (59) or (60). Next we observe that Eq. (50) can be rewritten as

$$\frac{1 + v\Phi'(R^2) + \int_{R^2-Q}^{R^2} w_s(u)\Phi'(u) du}{v + \int_{R^2-Q}^{R^2} w_s(u) du} = \mu \frac{R\Phi'(Rt)}{t}, \quad (61)$$

which when substituted to Eq. (51) yields the following equation

$$\mu R^2 [\Phi'(Rt)]^2 (R^2 - t^2 - Q) = t^2 \Phi'(R^2 - Q) [\sigma^2 + \Phi(R^2) - 2\Phi(Rt) + \Phi(R^2 - Q)]. \quad (62)$$

After introducing the variable $p = t/R$, and the NSR $\gamma = \sigma^2/R^2$ the above equation is presented in the Main Results section, see Eq. (19).

At the next step we differentiate Eq. (59) over the variable q , and find that for any $q \in [R^2 - Q, R^2]$ holds:

$$\begin{aligned} \frac{1}{\left(v + \int_q^{R^2} w_s(u) du\right)^2} &= \mu \frac{[\Phi'(q)]^2}{\left(1 + v\Phi'(R^2) + \int_q^{R^2} w_s(u)\Phi'(u) du\right)^2} \\ &+ \mu \Phi''(q) \left[\frac{\sigma^2 + \Phi(R^2) - 2\Phi(Rt) + \Phi(R^2 - Q)}{\left(1 + v\Phi'(R^2) + \int_{R^2-Q}^{R^2} w_s(u)\Phi'(u) du\right)^2} \right. \\ &\left. + \int_{R^2-Q}^q \frac{\Phi'(\tilde{q})d\tilde{q}}{\left(1 + v\Phi'(R^2) + \int_{\tilde{q}}^{R^2} w_s(u)\Phi'(u) du\right)^2} \right]. \end{aligned} \quad (63)$$

Now, by comparing Eq. (63) with Eq. (59) and assuming that $\Phi''(q) \neq 0$ one arrives to the following relation:

$$\begin{aligned} \frac{R^2 - t^2 - Q}{\left(v + \int_{R^2-Q}^{R^2} w_s(u) du\right)^2} &+ \int_{R^2-Q}^q \frac{d\tilde{q}}{\left(v + \int_{\tilde{q}}^{R^2} w_s(u) du\right)^2} \\ &= \frac{\Phi'(q)}{\Phi''(q)} \left[\frac{1}{\left(v + \int_q^{R^2} w_s(u) du\right)^2} - \mu \frac{[\Phi'(q)]^2}{\left(1 + v\Phi'(R^2) + \int_q^{R^2} w_s(u)\Phi'(u) du\right)^2} \right]. \end{aligned} \quad (64)$$

We further substitute the value $q = R^2 - Q$ in the above getting

$$\begin{aligned} \frac{R^2 - t^2 - Q}{\left(v + \int_{R^2-Q}^{R^2} w_s(u) du\right)^2} &= \frac{\Phi'(R^2 - Q)}{\Phi''(R^2 - Q)} \left[\frac{1}{\left(v + \int_{R^2-Q}^{R^2} w_s(u) du\right)^2} \right. \\ &\left. - \mu \frac{[\Phi'(R^2 - Q)]^2}{\left(1 + v\Phi'(R^2) + \int_{R^2-Q}^{R^2} w_s(u)\Phi'(u) du\right)^2} \right], \end{aligned} \quad (65)$$

which we further rearrange into

$$\begin{aligned} \frac{\left(1 + v\Phi'(R^2) + \int_{R^2-Q}^{R^2} w_s(u)\Phi'(u) du\right)^2}{\left(v + \int_{R^2-Q}^{R^2} w_s(u) du\right)^2} &\left[\frac{\Phi'(R^2 - Q)}{\Phi''(R^2 - Q)} - (R^2 - t^2 - Q) \right] \\ &= \mu \frac{[\Phi'(R^2 - Q)]^3}{\Phi''(R^2 - Q)}. \end{aligned} \quad (66)$$

Finally, upon using Eq. (61) the above relation is transformed into the following equation:

$$[\Phi'(R^2 - Q)]^3 \frac{t^2}{R^2} = \mu [\Phi'(Rt)]^2 [\Phi'(R^2 - Q) - \Phi''(R^2 - Q)(R^2 - t^2 - Q)], \quad (67)$$

which is yet another equation presented in the Main Results section, see Eq. (20).

We therefore conclude that the pair of equations Eqs. (62) and (67) is sufficient for finding the values of the parameters t and Q , and hence for determining the value of p giving the quality of the reconstruction procedure.

Using the above pair, the first task is to determine the range of NSR parameter $\gamma = \sigma^2/R^2$ where the solution with $Q > 0$ is at all possible. The boundary of this region which we denote as γ_{AT} (in the general spin-glass context such boundaries are known as the de-Almeida-Thouless lines [16]) can be found by setting $Q = 0$ in Eqs. (62) and (67), yielding the system of two equations:

$$\mu R^2 [\Phi'(Rt)]^2 (R^2 - t^2) = t^2 \Phi'(R^2) [R^2 \gamma_{AT} + \Phi(R^2) - 2\Phi(Rt) + \Phi(R^2)] \quad (68)$$

and

$$[\Phi'(R^2)]^3 p^2 = \mu [\Phi'(Rt)]^2 [\Phi'(R^2) - \Phi''(R^2)(R^2 - t^2)]. \quad (69)$$

Moreover, it is not difficult to understand that by replacing in Eq. (69) the equality sign $=$ with the inequality sign \leq defines the NSR domain $\gamma \leq \gamma_{AT}$ corresponding to solutions with stable unbroken replica symmetry, $Q = 0$.

3.3 Analysis of Replica Symmetry Breaking for the Linear-Quadratic Family of Encryptions

In this section we use the following scaling variables naturally arising when performing the analysis of the general case of linear-quadratic family: the scaled NSR $\tilde{\gamma} = \sigma^2/J_1^2 R^2$, the variables $p = t/R$ and $\tilde{Q} = Q/R^2$ and the non-linearity parameter $a = (R J_2/J_1)^2$.

3.3.1 Position of the de-Almeida Thouless Boundary

Not surprisingly, the equation Eq. (68) in scaled variables simply coincides with Eq. (57), which we repeat below for convenience of the exposition:

$$(1 + a)p^2 (\tilde{\gamma}_{AT} + 2(1 - p) + a(1 - p^2)) = \mu(1 - p^2)(1 + ap)^2, \quad (70)$$

whereas Eq. (69) takes after simple rearrangements the form

$$p^2 = \frac{\mu}{(1 + a)^3} (1 + ap^2)(1 + ap)^2. \quad (71)$$

One can further use Eq. (71) to bring Eq. (70) to a more convenient form explicitly defining $\tilde{\gamma}_{AT}$ as:

$$\tilde{\gamma}_{AT} = (1 - p)^2 \frac{(a^2 + a - 1) + 2a(a + 1)p + a^2 p^2}{1 + ap^2}. \quad (72)$$

To find $\tilde{\gamma}_{AT}$ for given values of the parameters $\mu \geq 1$ and $a \geq 0$ one has to find a value $p \in [0, 1]$ by solving Eq. (71), and substitute it to Eq. (72). A simple consideration shows that both sides of Eq. (71), $f_L(p) = p^2$ and $f_R(p) = \frac{\mu}{(1 + a)^3} (1 + ap^2)(1 + ap)^2$ are monotonically increasing and convex for $p \in [0, 1]$, with the value of the right-hand side being larger than the left-hand side at both ends of the interval, see Fig. 3. This implies that generically there must

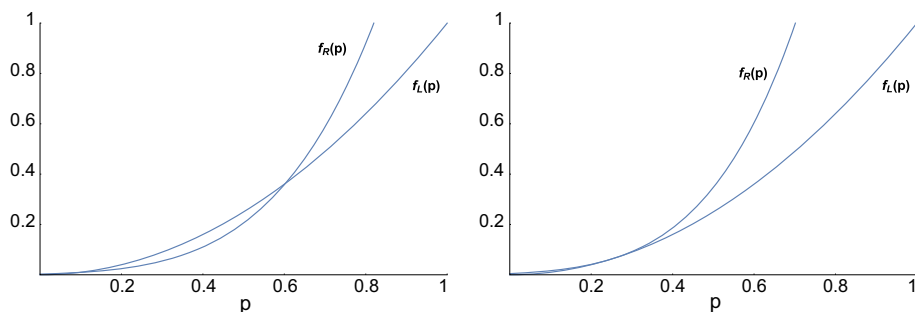


Fig. 3 Plots of $f_L(p)$ and $f_R(p)$ for $a = 8$ and $\mu = 2$ (left) and $\mu = (3/2)^3$ (right). In the former case the two curves intersect in two points $p_2 < p_1$, in the latter case the two curves touch each other at $p = a^{-2/3} = 0.25$. For $\mu > (3/2)^3$ the two curves do not intersect (not shown)

be either no solutions if $\mu > \mu_{AT}(a)$, or two solutions: $0 \leq p_2 < p_1 < 1$ if $\mu < \mu_{AT}(a)$. The parameter $\mu_{AT}(a)$ is precisely one when only a single solution is possible, and corresponds geometrically to the situation when the curves $f_L(p)$ and $f_R(p)$ touch each other at some $p = p_{AT} \in [0, 1]$, see the Fig. 3 below. The latter can be then found as a solution to the system of two equations: $f_L(p) = f_R(p)$ and $f'_L(p) = f'_R(p)$ for p_{AT} and μ_{AT} for a given $a > 1$. Surprisingly, the system can be solved explicitly:

$$p_{AT} = a^{-2/3}, \quad \mu_{AT}(a) = \frac{(a^{2/3} - a^{1/3} + 1)^3}{a}. \quad (73)$$

A detailed mathematical analysis of the discriminant of the 4th-order polynomial equation Eq. (71)⁴ fully confirms the picture outlined above, giving the explicit criterion for existence of solutions in the (μ, a) parameter plane, cf. Fig. 1:

- (i) For a given $\mu > 1$ no solutions with $p \in [0, 1]$ are possible for $a < 1$, whereas for a fixed $a > 1$ no solutions exist for $\mu > \mu_{AT}(a)$.
- (ii) For $\mu = \mu_{AT}(a)$ there exists a single solution: $p = p_{AT}$.
- (iii) For a given $a > 1$ and $1 < \mu < \mu_{AT}(a)$ there exist exactly two solutions $0 \leq p_2 < p_1 < 1$.

Correspondingly, in the case (i) the RS solution is valid for all values of the scaled Noise-to-Signal ratio $\tilde{\gamma}$, with the parameter p given by solving the RS equation Eq. (57). In contrast, in the last case (iii) the two solutions give rise to two different AT thresholds in the scaled NRS values: $\tilde{\gamma}_{AT}^{(2)} > \tilde{\gamma}_{AT}^{(1)}$. In other words, for fixed values of parameters μ and a there is generically an interval of NSR's $\tilde{\gamma}_{AT}^{(1)} < \tilde{\gamma} < \tilde{\gamma}_{AT}^{(2)}$ such that the replica-symmetry is broken inside and preserved for $\tilde{\gamma}$ outside that interval.

As is easy to see, for the minimal value ERP $\mu = 1$ and any $a > 1$ one must have only one solution at the edge of the interval: $p = 1$, with $\tilde{\gamma}_{AT} = 0$. Let us increase μ slightly so that $\mu - 1 \ll 1$. A simple perturbation analysis then shows that a solution to Eq. (71) close to the interval edge exists, and is given by:

$$p_1 = 1 - \frac{a+1}{2(a-1)}(\mu-1) + o(\mu-1). \quad (74)$$

⁴ I am grateful to Dr. Mihail Poplavskiy for his help with the corresponding analysis.

We conclude that for a fixed $a > 1$ and small ERP values $\mu - 1 \ll 1$ the replica symmetry is broken for NRS satisfying

$$\tilde{\gamma} > \tilde{\gamma}_{AT}^{(1)} = \left(a - \frac{1}{4}\right) \left(\frac{a+1}{a-1}\right)^2 (\mu - 1)^2 + o((\mu - 1)^2). \quad (75)$$

Finally, one may also consider the AT equations in the limiting case of large nonlinearity $a \gg 1$ when the quadratic term in the covariance is dominant over the linear term. In this limit one easily finds two solutions of Eq. (71), given to the leading orders by $p_1^2 \approx 1/\mu$ and $p_2 \approx \frac{\sqrt{\mu}}{a^{3/2}}$ yielding the AT thresholds

$$\tilde{\gamma}_{AT}^{(1)} \approx a \frac{(\mu - 1)^2}{\mu}, \quad \tilde{\gamma}_{AT}^{(2)} \approx a^2 + 2\sqrt{\mu a}. \quad (76)$$

We see that the ratio $\tilde{\gamma}_{AT}^{(1)}/a$ remains finite in the limit $a \rightarrow 0$, whereas $\tilde{\gamma}_{AT}^{(2)}/a \rightarrow \infty$. To interpret this fact we recall that $a \rightarrow \infty$ is equivalent to $J_1^2 \rightarrow 0$ at a fixed value of $J_2^2 > 0$. Then the value $\tilde{\gamma}_a \equiv \frac{\gamma}{J_2^2} := \hat{\gamma}$. We conclude that the value $\tilde{\gamma}_{AT}^{(1)}/a = \frac{(\mu-1)^2}{\mu} := \hat{\gamma}_{AT}$ must give the value of AT boundary in NRS for a given ERP $\mu > 1$ for the purely quadratic encryption, with the second threshold in this limiting case escaping to infinity and leaving the system in the RSB phase for all $\hat{\gamma} > \frac{(\mu-1)^2}{\mu}$. This conclusion will be fully confirmed by a detailed analysis of the purely quadratic case given in the next section.

3.3.2 Analysis of Solutions with the Broken Replica Symmetry for the Linear-Quadratic Family of Encryptions

After getting some understanding of the domain of parameters where replica symmetry is expected to be broken, let us analyse the pair of equations Eqs. (62) and (67), looking for a solution with $0 < Q \leq 1$. As before introduce $p = t/R$ and $\tilde{Q} = Q/R^2$ as our main variables of interest.

We start with considering the two limiting cases in the family: that of purely linear scheme with $\Phi(u) = J_1^2 u$ and the opposite limiting case of purely quadratic encryption scheme with $\Phi(u) = J_2^2 \frac{u^2}{2}$. In the former case the previous analysis indicates that only RS solution must be possible. Indeed, we immediately notice that for purely linear scheme Eq. (67) takes the form $p^2 = \mu$ which can not have any solution as $\mu > 1$ but $p \in [0, 1]$.⁵ We conclude that a solution with broken replica symmetry $Q > 0$ does not exist, so in this case the correct value of p is always given by solving the RS equation Eq. (55), as anticipated.

In the opposite limiting case of purely quadratic encryption we first need to introduce a different scaling for NRS as $\hat{\gamma} = \frac{\gamma}{J_2^2 R^2}$. Then one may notice that unless $p = 0$ (which is always a solution) the pair Eqs. (62) and (67) reduces to the form

$$\mu(1 - p^2 - \tilde{Q}) = (1 - \tilde{Q}) \left[\hat{\gamma} + 1 - p^2 - \tilde{Q} + \frac{1}{2} \tilde{Q}^2 \right], \quad \mu p^2 = (1 - \tilde{Q})^3. \quad (77)$$

Since $p \neq 0$ implies $\tilde{Q} \neq 1$, we can further simplify this system and bring it to the form

$$\tilde{Q}^3 + 3 \left(\frac{\mu}{2} - 1 \right) \tilde{Q}^2 + 3\tilde{Q}(1 - \mu) + \delta\mu = 0, \quad \mu p^2 = (1 - \tilde{Q})^3, \quad (78)$$

⁵ One can in fact easily demonstrate that the pair Eqs. (62) and (67) can not have a real solution for any $\mu > 0$.

where we introduced, in accordance with the Eq. (76),

$$\delta = \hat{\gamma} - \hat{\gamma}_{AT}, \quad \hat{\gamma}_{AT} := \frac{(\mu - 1)^2}{\mu}. \quad (79)$$

At this point we need to recall that the broken replica symmetry corresponds to $Q \in (0, R^2]$, hence $\tilde{Q} \in (0, 1]$. It is easy to show that the cubic equation in Eq. (78) may have a positive solution in that interval only for $\delta > 0$. We conclude that the replica symmetry is broken for $\hat{\gamma} > \hat{\gamma}_{AT}$ whereas for $\hat{\gamma} < \hat{\gamma}_{AT}$ the RS solution with $Q \equiv 0$ and p given by Eq. (57) remains valid. For small $0 < \delta \ll 1$ one easily finds $\tilde{Q} = \frac{\mu}{3(\mu-1)}\delta + O(\delta^2)$ ⁶. On the other hand one can see that the solution $\tilde{Q}(\delta) \rightarrow 1$ as $\delta \rightarrow \delta_c = \frac{3}{2} - \frac{1}{\mu}$, so that a meaningful solution only exists in the interval $\delta \in [0, \delta_c]$. Moreover, it is easy to show that for $\delta \rightarrow \delta_c$ we have $\tilde{Q} = 1 - \sqrt{\frac{2}{3}(\delta_c - \delta)}$. We see that the second of Eq. (78) then implies that when approaching the true threshold value $\tilde{\gamma}_c^{(RSB)} = \mu - \frac{1}{2}$ dictated by broken replica symmetry the quality parameter vanishes as $p \sim (\hat{\gamma}_c^{(RSB)} - \hat{\gamma})^{3/4}$ rather than as a square root, as in the replica-symmetric solution Eq. (56).

To study the behaviour of the solution $\tilde{Q}(\delta)$ for δ of the order of one it is instructive to consider a particular (but generic) case of $\mu = 2$, when $\delta_c = 1$. The cubic equation for \tilde{Q} takes then a particular simple form:

$$\tilde{Q}^3 - 3\tilde{Q} + 2\delta = 0, \quad (80)$$

which represents one of the rare instances when the Cardano formula for solving cubic equations is really helpful for the analysis. Indeed, according to the Cardano formula in this case the solution is given by

$$\tilde{Q} = \left[-\delta + \sqrt{\delta^2 - 1} \right]^{1/3} + \left[-\delta - \sqrt{\delta^2 - 1} \right]^{1/3}. \quad (81)$$

As $\delta \in [0, 1]$ we can further parametrize $\delta = \sin \phi$, $\phi \in [0, \pi/2]$, and obtain the three different solutions to Eq. (80) in the following form

$$\tilde{Q}_n = 2 \cos \left(\frac{1}{3} \left[\phi + \pi \left(2n + \frac{1}{2} \right) \right] \right), \quad n = 0, 1, 2. \quad (82)$$

We see then that $\tilde{Q}_{0,1}$ are outside the interval $[0, 1]$, as $\tilde{Q}_0 = 2 \cos \left(\frac{1}{3}\phi + \frac{\pi}{6} \right) \in [1, \sqrt{3}]$ and $\tilde{Q}_1 = 2 \cos \left(\frac{1}{3}\phi + \frac{\pi}{6} \right) \in [-\sqrt{3}, -1]$, whereas $\tilde{Q}_2 = 2 \sin \frac{\phi}{3}$ is exactly the valid solution.

The nature of the solution for purely quadratic scheme for a general $\mu > 1$ is exactly of the same type. After finding \tilde{Q} from the cubic equation for $\tilde{\gamma}_{AT} < \tilde{\gamma} \leq \tilde{\gamma}_c^{(RSB)} = \mu - 1/2$ we find the quality parameter p from the second of Eq. (78), and combining it with RS expression Eq. (56) obtain the full corresponding curve for $p(\hat{\gamma})$ for a given μ . In particular, for the above special value $\mu = 2$ the full curve can be described by an explicit expression:

$$p = \begin{cases} \sqrt{1 - \hat{\gamma}} & \text{if } \hat{\gamma} \leq \hat{\gamma}_{AT} = \frac{1}{2} \\ \frac{1}{\sqrt{2}} \left[1 - 2 \sin \frac{1}{3} \left(\arcsin \left(\hat{\gamma} - \frac{1}{2} \right) \right) \right]^{3/2} & \text{if } \frac{1}{2} \leq \hat{\gamma} \leq \hat{\gamma}_c^{(RSB)} = \frac{3}{2} \\ 0 & \text{if } \hat{\gamma} > \hat{\gamma}_c^{(RSB)} = \frac{3}{2} \end{cases}, \quad (83)$$

which is depicted in the left figure below. For $\mu \neq 2$ the analytic solution of the cubic equation is less instructive, and it is easier to solve the equation numerically (Fig. 4).

⁶ The two other solutions of the cubic equation can be shown to be out of the interval $(0, 1]$, see the explicit example below.

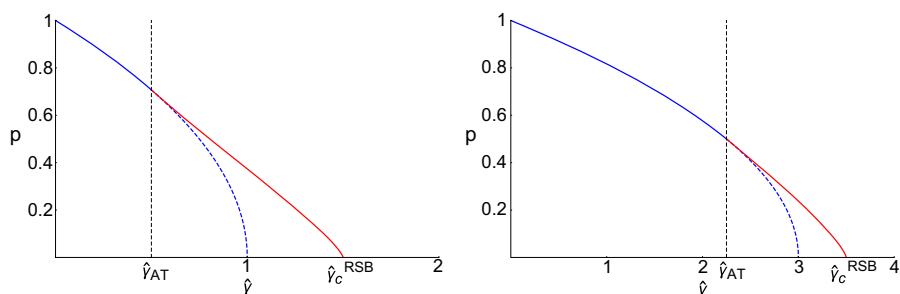


Fig. 4 The quality parameter p as a function of the scaled noise-to-signal ratio $\hat{\gamma}$ for purely quadratic encryptions and two different values of the ERP, $\mu = 2$ (left) and $\mu = 4$ (right). The blue broken curve is the continuation of the replica-symmetric solution in the region of Full RSB

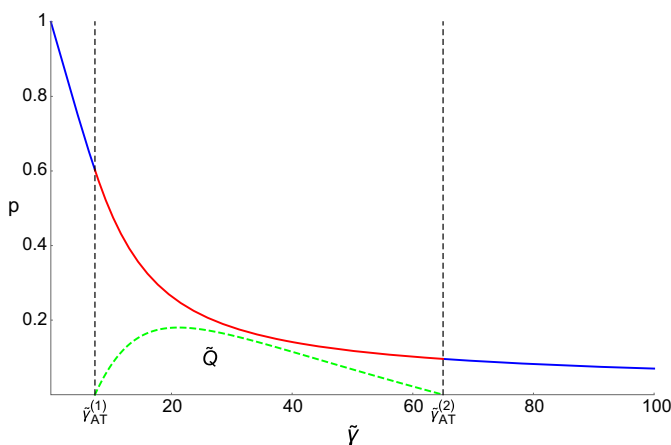


Fig. 5 The quality parameter p as a function of the scaled noise-to-signal ratio $\tilde{\gamma}$ for a generic representative of linear-quadratic encryptions for the nonlinearity $a = 8$ and ERP $\mu = 2$. In the interval of scaled noise-to-signal ratio $\tilde{\gamma}_2^{(AT)} < \tilde{\gamma} < \tilde{\gamma}_2^{(AT)}$ the replica symmetry is broken as signified by a non-zero values of the parameter \tilde{Q} , plotted as a green broken line

After full understanding of the limiting cases we briefly discuss the solution for a generic linear-quadratic encryption algorithm with some finite value $1 < a < \infty$ of the nonlinearity parameter. In this case the NRS scaling is still given by the NRS variable $\tilde{\gamma} = \gamma/J_1^2$. One recalls that for a given a as long as $\mu < \mu_{AT}(a) = \frac{(a^{2/3} - a^{1/3} + 1)^3}{a}$ there exists two NSR thresholds $\tilde{\gamma}_{AT}^{(1)}$ and $\tilde{\gamma}_{AT}^{(2)}$ such that for $\tilde{\gamma} \notin [\tilde{\gamma}_{AT}^{(1)}, \tilde{\gamma}_{AT}^{(2)}]$ the curve $p(\tilde{\gamma})$ is given by RS solution Eq. (57), whereas for $\tilde{\gamma} \in [\tilde{\gamma}_{AT}^{(1)}, \tilde{\gamma}_{AT}^{(2)}]$ the curve $p(\tilde{\gamma})$ is given by the Full RSB solution from the system of two equations:

$$p^2 = \frac{\mu}{[1 + a(1 - \tilde{Q})]^3} (1 + ap^2)(1 + ap)^2 \quad (84)$$

and

$$\begin{aligned} & \left[1 + a(1 - \tilde{Q})\right] p^2 \left(\tilde{\gamma} + 2(1 - p) + a(1 - p^2) - a\tilde{Q} + a\frac{1}{2}\tilde{Q}^2 \right) \\ &= \mu(1 - p^2 - \tilde{Q})(1 + ap)^2. \end{aligned} \quad (85)$$

In Fig. 5 we plot the full resulting curve for a generic choice of parameters.

Acknowledgements The author is grateful to Ali Bereyhi, Jean-Philippe Bouchaud, Ralf Mueller, Hermann Schulz-Baldes, Guilhem Semerjian, Nicolas Sourlas, Francesco Zamponi, and Lenka Zdeborova for enlightening discussions and encouraging interest in this work, to Christian Schmidt for careful reading of the manuscript and many advices, and to Dr. Mihail Poplavskyi for his help with analysis of Eq. (71) and preparing figures for this article. The financial support by EPSRC Grant EP/N009436/1 “The many faces of random characteristic polynomials” is acknowledged with thanks.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

Appendix A: Perturbation Theory in the Lagrange Multipliers Framework

We set the parameter $J_1^2 = 1$ in this Appendix.

Substituting the solution Eq. (9) into the spherical constraint $(\mathbf{x}, \mathbf{x}) = NR^2$ and using the notations $W := A^T A$ and $G = (W - \lambda \mathbf{1}_N)^{-1}$ one gets an equation for the Lagrange multiplier λ :

$$2\lambda (\mathbf{s}, G\mathbf{s}) + 2 \left(\mathbf{s}, G A^T \mathbf{b} \right) + \lambda^2 (\mathbf{s}, G^2 \mathbf{s}) + 2\lambda \left(\mathbf{s}, G^2 A^T \mathbf{b} \right) + \left(\mathbf{b}, A G^2 A^T \mathbf{b} \right) = 0. \quad (86)$$

Recall that for $\sigma = 0$ the global minimum corresponds to $\lambda = 0$, so we will look for a weak-noise expansion $\lambda = \lambda_1 \sigma + \lambda_2 \sigma^2 + \dots \ll 1$, writing $\mathbf{b} = \sigma \boldsymbol{\xi}$, with components of the vector $\boldsymbol{\xi}$ having variance unity and remembering that for $M > N$ the matrix $W > 0$ with probability tending to one is invertable, one can safely expand $G \approx W^{-1} + \lambda W^{-2} + \dots$ and substituting this to Eq. (86) find the first and then second order coefficient in the Lagrange multiplier as:

$$\lambda_1 = -\frac{(\mathbf{s}, W^{-1} A^T \boldsymbol{\xi})}{p_1}, \quad \lambda_2 = -\frac{1}{2p_1} \left[3\lambda_1^2 p_2 + 4\lambda_1 (\mathbf{s}, W^{-2} A^T \boldsymbol{\xi}) + (\boldsymbol{\xi}, A W^{-2} A^T \boldsymbol{\xi}) \right], \quad (87)$$

where we introduced the following notations:

$$p_1 = (\mathbf{s}, W^{-1} \mathbf{s}), \quad p_2 = (\mathbf{s}, W^{-2} \mathbf{s}). \quad (88)$$

Using this one can get the following expansion for the quality parameter Eq. (4):

$$\begin{aligned} 1 - p_N &= \frac{1}{NR^2} \left\{ \sigma \left[\lambda_1 p_1 + (\mathbf{s}, W^{-1} A^T \boldsymbol{\xi}) \right] \right. \\ &\quad \left. + \sigma^2 \left[\lambda_1^2 p_2 + \lambda_2 p_1 + \lambda_1 (\mathbf{s}, W^{-2} A^T \boldsymbol{\xi}) \right] + \dots \right\} \end{aligned} \quad (89)$$

valid at every realization of both the noise and the random matrix A . Substituting here Eq. (87) and taking the expected value first only over the Gaussian noise $\boldsymbol{\xi}$ gives after straightforward,

but somewhat lengthy manipulations, to the leading order:

$$1 - p_N = \frac{\sigma^2}{NR^2} p_1 \langle \lambda_2 \rangle_\xi = \frac{\sigma^2}{2NR^2} \left[\text{Tr} [W^{-1}] - \frac{p_2}{p_1} \right]. \quad (90)$$

It remains to perform the average over the ensemble of Wishart matrices W with $M > N$. One finds that as long as $N \gg 1$ the fraction p_2/p_1 remains of the order of unity, whereas the first term $\text{Tr} [W^{-1}] = O(N)$ and is dominant. Using the well-known Marchenko-Pastur limiting law for the spectral density of eigenvalues of W

$$\rho_{MP}(\lambda) = \frac{2}{\pi} \frac{1}{(\sqrt{\lambda_+} - \sqrt{\lambda_-})^2} \frac{\sqrt{(\lambda - \lambda_-)(\lambda_+ - \lambda)}}{\lambda}, \quad \lambda_- \leq \lambda \leq \lambda_+, \quad (91)$$

where $\lambda_{\pm} = (\sqrt{\mu} \pm 1)^2$ are positions of the spectral edges, one can find for the mean trace of the resolvent:

$$\lim_{N \rightarrow \infty} \frac{1}{N} \langle [(W - \lambda \mathbf{1}_N)^{-1}] \rangle = \frac{2}{\sqrt{\lambda_- \lambda_+} - \lambda + \sqrt{(\lambda - \lambda_-)(\lambda - \lambda_+)}} , \quad \lambda < \lambda_- . \quad (92)$$

In particular, for $\lambda = 0$ we have

$$\lim_{N \rightarrow \infty} \frac{1}{N} \langle \text{Tr} [W^{-1}] \rangle = \frac{1}{\sqrt{\lambda_- \lambda_+}} = \frac{1}{\mu - 1} . \quad (93)$$

resulting in Eq. (10) valid in the first-order in small-noise value.

One can also straightforwardly extract the behaviour for asymptotically large noise variance values $(\mathbf{b}, \mathbf{b}) \propto \sigma^2 \rightarrow \infty$ when Eq. (9) implies that

$$\mathbf{x} \approx (W - \lambda \mathbf{1}_N)^{-1} A^T \mathbf{b} . \quad (94)$$

Substituting Eq. (94) to the spherical constraint gives

$$(\mathbf{x}, \mathbf{x}) = \mathbf{b}^T A (W - \lambda \mathbf{1}_N)^{-2} A^T \mathbf{b} = NR^2 , \quad (95)$$

and further averaging over the Gaussian noise \mathbf{b} the above relation yields:

$$1 = \frac{\sigma^2}{NR^2} \text{Tr} [A (W - \lambda \mathbf{1}_N)^{-2} A^T] = \frac{\sigma^2}{NR^2} \text{Tr} [(W - \lambda \mathbf{1}_N)^{-2} W] . \quad (96)$$

It is clear that for $\tilde{\gamma} = \frac{\sigma^2}{R^2} \gg 1$ the relevant value of the Lagrange multiplier λ has to be large in modulus, $|\lambda| \gg 1$, which immediately implies in the large- N limit:

$$\lambda^2 \approx \tilde{\gamma} \frac{1}{N} \text{Tr} W |_{N \rightarrow \infty} = \tilde{\gamma} \int_{\lambda_-}^{\lambda_+} \rho_{MP}(\lambda) \lambda d\lambda = \tilde{\gamma} \frac{(\sqrt{\lambda_+} + \sqrt{\lambda_-})^2}{4} = \tilde{\gamma} \mu , \quad (97)$$

so that $|\lambda| \approx \sqrt{\tilde{\gamma} \mu} \gg 1$. Now, the Eq. (9) implies for the quality parameter

$$p_N = \frac{(\mathbf{x}, \mathbf{s})}{NR^2} = 1 - \frac{\lambda}{NR^2} \mathbf{s}^T (W - \lambda \mathbf{1}_N)^{-1} \mathbf{s} + \frac{1}{NR^2} \mathbf{s}^T (W - \lambda \mathbf{1}_N)^{-1} A^T \mathbf{b} . \quad (98)$$

Expanding for large $|\lambda| \sim \sqrt{\tilde{\gamma}} \gg 1$ as

$$\mathbf{s}^T (W - \lambda \mathbf{1}_N)^{-1} \mathbf{s} \approx -\frac{NR^2}{\lambda} + \frac{1}{\lambda^2} (\mathbf{s}, W \mathbf{s}) + \dots, \quad \mathbf{s}^T (W - \lambda \mathbf{1}_N)^{-1} A^T \mathbf{b} \approx -\frac{1}{\lambda} \mathbf{s}^T A^T \mathbf{b} + \dots$$

shows that to the leading order

$$p_N = -\frac{1}{\lambda} \frac{1}{NR^2} \left[(\mathbf{s}, W\mathbf{s}) + (\mathbf{s}, A^T \mathbf{b}) \right], \quad (99)$$

which upon averaging over the Wishart matrices W and the noise \mathbf{b} , taking the limit $N \rightarrow \infty$, and taking into account that actually $\lambda \rightarrow -\infty$, yields

$$p_\infty = \frac{1}{|\lambda|} \frac{1}{N} \langle \text{Tr } W \rangle |_{N \rightarrow \infty} = \frac{\mu}{\sqrt{\mu \tilde{\gamma}}} = \sqrt{\frac{\mu}{\tilde{\gamma}}}. \quad (100)$$

Appendix B

In this Appendix we give a proof of the following

Lemma

Let $\mathbf{x} \in \mathbb{R}^N$, and $V(\mathbf{x})$ be a Gaussian random field with mean zero and the covariance

$$\langle V(\mathbf{x}_1) V(\mathbf{x}_2) \rangle = \phi(\mathbf{x}_1; \mathbf{x}_2), \quad (101)$$

where $\phi(\mathbf{x}; \mathbf{y}) = \phi(\mathbf{y}; \mathbf{x})$ is any suitable covariance structure function. Then for any $\beta > 0$ holds

$$\left\langle e^{-\frac{\beta}{2} \sum_{a=1}^n V^2(\mathbf{x}_a)} \right\rangle = [\det \mathcal{G}(\mathbf{x}_1, \dots, \mathbf{x}_n)]^{-1/2}, \quad (102)$$

where the (positive definite) $n \times n$ matrix $\mathcal{G}(\mathbf{x}_1, \dots, \mathbf{x}_n)$ has the entries

$$\mathcal{G}_{ab}(\mathbf{x}_1, \dots, \mathbf{x}_n) = \delta_{ab} + \beta \phi(\mathbf{x}_a; \mathbf{x}_b). \quad (103)$$

Proof it is convenient to linearize the squared terms in the exponential by exploiting the Gaussian integration of an auxiliary real variable u_a for every $a = 1, \dots, n$ (the trick known in the physical literature as the Hubbard-Stratonovich transformation):

$$e^{-\frac{\beta}{2} V^2(\mathbf{x}_a)} = \int_{\mathbb{R}} e^{-i\sqrt{\beta} u_a V(\mathbf{x}_a)} \frac{e^{-\frac{1}{2} u_a^2} du_a}{\sqrt{2\pi}}, \quad (104)$$

which implies

$$\left\langle e^{-\frac{\beta}{2} \sum_{a=1}^n V^2(\mathbf{x}_a)} \right\rangle = \int_{\mathbb{R}^n} \left\langle e^{-i\sqrt{\beta} \sum_{a=1}^n u_a V(\mathbf{x}_a)} \right\rangle e^{-\frac{1}{2} \sum_a u_a^2} \prod_a \frac{du_a}{\sqrt{2\pi}}. \quad (105)$$

Now the average is immediate to perform due to the Gaussian nature of the random field $V(\mathbf{x})$. Using Eq. (101) we get:

$$\left\langle e^{-i\sqrt{\beta} \sum_{a=1}^n u_a V(\mathbf{x}_a)} \right\rangle = e^{-\frac{\beta}{2} \sum_{a,b} u_a u_b \phi(\mathbf{x}_a; \mathbf{x}_b)}. \quad (106)$$

Substituting now Eq. (106) back to Eq. (105) we see that the integrals over the variables u_a remain multivariate Gaussian, and hence can be easily performed, resulting in Eq. (102). \square

Appendix C

In this Appendix we give a proof of the following

Theorem

Consider a function $F(\mathbf{x}_1, \dots, \mathbf{x}_n; \mathbf{s})$ of N -component real vectors \mathbf{x}_l $1 \leq l \leq n$ and a N -component real vector \mathbf{s} (considered as a parameter) such that

$$\int_{\mathbb{R}^N} d\mathbf{x}_1 \dots \int_{\mathbb{R}^N} d\mathbf{x}_n |F(\mathbf{x}_1, \dots, \mathbf{x}_n; \mathbf{s})| < \infty. \quad (107)$$

Suppose further that the function F depends on its arguments only via $n(n+1)/2$ scalar products $\tilde{Q}_{ab} = (\mathbf{x}_a, \mathbf{x}_b)$, $1 \leq a, b \leq n$ and on n projections $\tilde{t}_a = (\mathbf{x}_a, \mathbf{s})$ for $a = 1, \dots, n$. Rewrite then such a function as $\mathcal{F}(\tilde{Q}, \tilde{\mathbf{t}})$ of $n \times n$ real symmetric matrix \tilde{Q} with entries \tilde{Q}_{ab} and a vector $\tilde{\mathbf{t}} = (t_1, \dots, t_n)$. Then for $N \geq n+1$ the integral defined as

$$I_{N,n}^{(F)}(\mathbf{s}) = \int_{\mathbb{R}^N} d\mathbf{x}_1 \dots \int_{\mathbb{R}^N} d\mathbf{x}_n F(\mathbf{x}_1, \dots, \mathbf{x}_n; \mathbf{s}) \quad (108)$$

is equal to

$$I_{N,n}^{(\mathcal{F})}(\mathbf{s}) = C_{N-1,n}^{(o)} \int_{Q>0} \mathcal{F}(Q + \mathbf{t} \otimes \mathbf{t}^T, |\mathbf{s}|\mathbf{t}) [\det Q]^{(N-n-2)/2} dQ d\mathbf{t}. \quad (109)$$

where the proportionality constant is given by

$$C_{N,n}^{(o)} = \frac{\pi^{\frac{n}{2} \left(N - \frac{n-1}{2} \right)}}{\prod_{k=0}^{n-1} \Gamma \left(\frac{N-k}{2} \right)}, \quad (110)$$

the integration in the Eq. (109) goes over the manifold of real symmetric non-negative definite $n \times n$ matrices Q and the vector $\mathbf{t} \in \mathbb{R}^n$, whereas the diadic product $T = \mathbf{t} \otimes \mathbf{t}^T$ is used to denote a (rank one) $n \times n$ matrix T with entries $T_{ab} = t_a t_b$.

Proof Denote $\mathbf{e}_N = (0, \dots, 0, 1)$ the last of the standard basis vectors in \mathbb{R}^N . Then there exists an orthogonal transformation $O(\mathbf{s}) \in O(N)$ such that we can represent the vector \mathbf{s} as $\mathbf{s} = |\mathbf{s}|O(\mathbf{s})\mathbf{e}_N$. Perform the transformation of variables $\mathbf{x}_a \rightarrow \mathbf{y}_a = O(\mathbf{s})\mathbf{x}_a$, $\forall a = 1, \dots, n$ in the integrand of Eq. (108). Such transformation leaves invariant the volume element: $\prod_a d\mathbf{x}_a = \prod_a d\mathbf{y}_a$ and the scalar products $\tilde{Q}_{ab} = (\mathbf{x}_a, \mathbf{x}_b) = (\mathbf{y}_a, \mathbf{y}_b)$, $1 \leq a, b \leq n$ but transforms the n projections $\tilde{t}_a = (\mathbf{x}_a, \mathbf{s})$ for all $a = 1, \dots, n$ into $\tilde{t}_a = |\mathbf{s}|y_{aN}$, where y_{aN} is the N -th component of the vector \mathbf{y}_a . Now decompose each vector \mathbf{y}_a as $\mathbf{y}_a = (\mathbf{v}_a, y_{aN})$, where \mathbf{v}_a are $(N-1)$ -dimensional vectors. Such a decomposition implies:

$$\tilde{Q}_{ab} = (\mathbf{y}_a, \mathbf{y}_b) = (\mathbf{v}_a, \mathbf{v}_b) + y_{aN} y_{bN}, \quad \prod_a d\mathbf{y}_a = \prod_a d\mathbf{v}_a \prod_a dy_{aN},$$

so that using the notations of the Theorem, renaming $y_{Na} \rightarrow t_a$ and introducing $Q_{ab}^{(\mathbf{v})} = (\mathbf{v}_a, \mathbf{v}_b)$ and $\mathbf{t} = (t_1, \dots, t_n)$ we can rewrite Eq.(108) as

$$I_{N,n}^{(F)}(\mathbf{s}) = \int_{\mathbb{R}^n} \mathcal{I}_{N,n}^{(F)}(\mathbf{t}; \mathbf{s}) d\mathbf{t}, \quad \mathcal{I}_{N,n}^{(F)}(\mathbf{t}; \mathbf{s}) := \int_{\mathbb{R}^{N-1}} d\mathbf{v}_1 \dots \int_{\mathbb{R}^{N-1}} d\mathbf{v}_n \mathcal{F}(Q^{(\mathbf{v})} + \mathbf{t} \otimes \mathbf{t}^T, |\mathbf{s}|\mathbf{t}). \quad (111)$$

Note that the last integral with respect to vectors \mathbf{v}_a , $a = 1, \dots, n$ has the full $O(N-1)$ invariance of the integrand. The statement of the Theorem then immediately follows by applying to this situation the 'dimensional reduction' formula suggested for the first time in [36] and essentially rediscovered in [17]; see the Appendix D of [23] and the appendix B of [19] for alternative proofs. \square

References

1. Auffinger, A., Ben Arous, G.: Complexity of random smooth functions on the high-dimensional sphere. *Ann. Prob.* **41**(6), 4214–4247 (2013)
2. Auffinger, A.: Chen, Wei-Kuo: On the energy landscape of spherical spin glasses. *Adv. Math.* **330**, 553–588 (2018)
3. Auffinger, A., Zeng, Q.: Existence of two-step replica symmetry breaking for the spherical mixed p-spin glass at zero temperature. *Commun. Math. Phys.* (to appear)
4. Bovier, A.: *Statistical Mechanics of Disordered systems: a Mathematical Perspective* (Cambridge Series in Statistical and Probabilistic Mathematics. Cambridge University Press, Cambridge (2016)
5. Baik, J., Lee, J.O.: Fluctuations of the free energy of the spherical Sherrington-Kirkpatrick model. *J. Stat. Phys.* **165**(2), 185–224 (2016)
6. Barbier, J., Krzakala, F., Macris, N., Miolane, L., Zdeborova, L.: Phase Transitions, Optimal Errors and Optimality of Message-Passing in Generalized Linear Models. [arXiv:1708.03395](https://arxiv.org/abs/1708.03395)
7. Boreyhi, A., Mueller, R., Schulz-Baldes, H.: Statistical Mechanics of MAP estimation: General replica Ansatz. [arXiv:1612.01980](https://arxiv.org/abs/1612.01980)
8. Boreyhi, A., Mueller, R., Schulz-Baldes, H.: Replica Symmetry Breaking in Compressive Sensing. *IEEE Information Theory and Applications Workshop, (ITA)* (2017), pp. 1–7 [e-preprint [arXiv:1704.08013](https://arxiv.org/abs/1704.08013)]
9. Boreyhi, A., Mueller, R.: Maximum-A-Posteriori signal recovery with prior information: applications to compressed sensing. [arXiv:1802.05776](https://arxiv.org/abs/1802.05776)
10. Blumensath, T.: Compressed sensing with nonlinear observations and related nonlinear optimization problems. *IEEE Trans. Inf. Theory* **59**(6), 3466–3474 (2013)
11. Chen, W.-K., Sen, A.: Parisi formula, disorder chaos and fluctuation for the ground state energy in the spherical mixed p-spin models. *Commun. Math. Phys.* **350**, 129–173 (2017)
12. Chen, W.-K., Panchenko, D.: Temperature chaos in some spherical mixed p-spin models. *J. Stat. Phys.* **166**(5), 1151–1162 (2017)
13. Crisanti, A., Sommers, H.-J.: The spherical p-spin interaction spin glass model: the statics. *Zeitsch. f. Phys. B* **87**(3), 341–354 (1992)
14. Cugliandolo, L.F., Dean, D.S.: On the dynamics of a spherical spin-glass in a magnetic field. *J. Phys. A* **28**, L453–459 (1995)
15. David, F., Duplantier, B., Guitter, E.: Renormalization theory for interacting crumpled manifolds. *Nucl. Phys. B* **394**, 555–664 (1993)
16. de Almeida, J.R.L., Thouless, D.J.: Stability of the Sherrington-Kirkpatrick solution of a spin glass model. *J. Phys. A* **11**(5), 983–990 (1978)
17. Fyodorov, Y.V.: Negative moments of characteristic polynomials of random matrices: Ingham-Siegel integral as an alternative to Hubbard-Stratonovich transformation. *Nucl. Phys. B* **621**, 643–674 (2002)
18. Fyodorov, Y.V.: On statistical mechanics of a single particle in high-dimensional random landscapes. *Acta Phys. Pol. B* **38**(13), 4055–4066 (2007)
19. Fyodorov, Y.V.: Multifractality and freezing phenomena in random energy landscapes: an introduction. *Physica A* **389**, 4229–4254 (2010)
20. Fyodorov, Y.V., Bouchaud, J.-P.: Statistical mechanics of a single particle in a multiscale random potential: Parisi landscapes in finite-dimensional Euclidean spaces. *J. Phys. A* **41**, 324009 (2008)
21. Fyodorov, Y.V., Le Doussal, P.: Topology trivialization and large deviations for the minimum in the simplest random optimization. *J. Stat. Phys.* **154**(1–2), 466–490 (2014)
22. Fyodorov, Y.V., Sommers, H.-J.: Classical particle in a box with random potential: exploiting rotational symmetry of replicated Hamiltonian. *Nucl. Phys. B* **764**(3), 128–167 (2007)
23. Fyodorov, Y.V., Strahov, E.: Characteristic polynomials of random Hermitian matrices and Duistermaat-Heckman localisation on non-compact Kähler manifolds. *Nucl. Phys. B* **630**, 453–491 (2002)
24. Guionnet, A., Zeitouni, O.: Large deviations asymptotics for spherical integrals. *J. Funct. Anal.* **188**(2), 461–515 (2002)
25. Guionnet, A., Maida, M.: A Fourier view on the R -transform and related asymptotics of spherical integrals. *J. Funct. Anal.* **222**(2), 435–490 (2005)
26. Kogan, H., Marcus, M.B., Rosen, J.: Permanent processes. *Commun. Stoch. Anal.* **5**(1), 6 (2011) [arXiv:1008.3522](https://arxiv.org/abs/1008.3522)
27. Kosterlitz, J.M., Thouless, D.J., Jones, R.C.: Spherical model of a spin glass. *Phys. Rev. Lett.* **36**, 1217–1220 (1976)
28. Krzakala, F., Mezard, M., Sausset, F., Sun, Y.F., Zdeborova, L.: Statistical-physics-based reconstruction in compressed sensing. *Phys. Rev. X* **2**, 021005 (2012)
29. Kurchan, J., Maimbourg, T., Zamponi, F.: Statics and dynamics of infinite-dimensional liquids and glasses: a parallel and compact derivation. *J. Stat. Mech.* **2016**(3), 033210 (2016)

30. Marchenko, V.A., Pastur, L.A.: Distribution of eigenvalues for some sets of random matrices. *Mat. Sb. (N.S.)* **72**(114), 507–536 (1967)
31. Mezard, M., Parisi, G., Virasoro, M.: *Spin glass theory and beyond: An Introduction to the Replica Method and Its Applications*. (World Scientific Lecture Notes In Physics). World Scientific Publishing Company, Singapore (1986)
32. Montanari, A.: Statistical Estimation: from denoising to sparse regression and hidden cliques. In: Krzakala, F., et al. (eds.) *Statistical Physics, Optimization, Inference, and Message-Passing Algorithms: Lecture Notes of the Les Houches School of Physics: Special Issue, October 2013*. Oxford University Press, Oxford (2016)
33. Panchenko, D.: *The Sherrington-Kirkpatrick Model*. Springer Monographs in Mathematics. Springer, New York (2013)
34. Parisi, G.: Constraint optimization and statistical mechanics. In: book series: *Proc. Int. Sch. Physics ENRICO FERMI* **155**, 205–228 (2004) [e-preprint [arXiv:cs/0312011](https://arxiv.org/abs/cs/0312011)]
35. Ros, V., Ben Arous, G., Biroli, G., Cammarota, C.: Complex energy landscapes in spiked-tensor and simple glassy models: ruggedness, arrangements of local minima and phase transitions. [arXiv:1804.02686](https://arxiv.org/abs/1804.02686)
36. Percus, J.K.: Dimensional reduction of integrals of orthogonal invariants. *Commun. Pure Appl. Math.* **40**(4), 449–453 (1957)
37. Plan, Y., Vershynin, R.: The generalized lasso with nonlinear observations. *IEEE Trans. Inf. Theory* **62**(3), 1528–1537 (2016)
38. Schülke, C., Schniter, P., Zdeborova, L.: Phase diagram of matrix compressed sensing. *Phys. Rev. E* **94**(6), 062136 (2016)
39. Sourlas, N.: Spin-glass models as error-correcting codes. *Nature* **339**, 693–695 (1989)
40. Subag, E.: The complexity of spherical p-spin models—a second moment approach. *Ann. Probab.* **45**(5), 3385–3450 (2017)
41. Talagrand, M.: Free energy of the spherical mean-field model. *Probab. Theory Relat. Fields* **134**, 339–382 (2006)
42. Zdeborova, L., Krzakala, F.: Statistical physics of inference: Thresholds and algorithms. *Adv. Phys.* **65**(5), 453–552 (2016) [arXiv:1511.02476](https://arxiv.org/abs/1511.02476)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.