On reconstructing nonlinearly encrypted signals corrupted by noise [1]

Yan V Fyodorov

Department of Mathematics

King's College London

Project supported by the EPSRC grant EP/N009436/1

Rough Landscapes: from Physics to Algorithms, KITP, January 7th 2019

[1] Based on: **YVF** *arXiv:1805.06982* [to appear in **J. Stat. Phys.**]

Background Model and Setting of the Problem:

Signals are represented by $N-$dimensional source (column) vectors $\mathbf{s} \in \mathbb{R}^N$. The associated **signal strength** R is defined via the Euclidean norm as

$$R = \sqrt{\frac{1}{N}\left(\mathbf{s}, \mathbf{s}\right)}.$$

By a (symmetric key) **encryption** of the source signal we understand a **random mapping** $\mathbf{s} \mapsto \mathbf{y} \in \mathbb{R}^M$ known both to the sender and a recipient:

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

where the collection of **random functions** $V_1(\mathbf{s}), \ldots, V_M(\mathbf{s})$ represents 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** modified by an additive random **noise**, i.e. $\mathbf{z} = \mathbf{y} + \mathbf{b}$ with the noise assumed to be normally distributed: $\mathbf{b} \sim \mathcal{N}(\mathbf{0}, \sigma^2 \mathbf{1}_M)$. A natural parameter is then the 'bare' **noise-to-signal** ratio (NSR) $\gamma = \sigma^2/R^2$.

The recipient's aim is to reconstruct the source signal $\mathbf{s}$ from the knowledge of $\mathbf{z}$.

Background Model and Setting of the Problem:

We consider the reconstruction problem under a few technical assumptions:

- The recipient is aware of the exact source signal strength $R = \sqrt{\frac{1}{N}\left(\mathbf{s},\mathbf{s}\right)}$, and therefore can restrict the signal search to the feasibility set $\mathbb{W}$ given by $(N-1)-$dimensional sphere of the radius $R\sqrt{N}$.

- The random functions $V_k(\mathbf{s})$ belong to the class of (smooth) *isotropic* mean-zero Gaussian-distributed random fields on the sphere with the covariance structure dependent only on the angle between the vectors:

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

  where the angular brackets $\langle \ldots \rangle$ denote the expected values. As our basic example we will consider the **linear-quadratic** family:

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

  where $\mathbf{a}_k \sim \mathcal{N}(\mathbf{0}, \frac{J_1^2}{N}\mathbf{1}_N)$, and the entries of $N \times N$ real symmetric GOE-like random matrices $\mathcal{J}^{(k)}, k = 1, \ldots, M$ are mean-zero i.i.d. normal with the variance $\frac{J_2^2}{N^2}$. This results in the covariance of the form $\Phi\left(u\right) = J_1^2\, u + \frac{1}{2}J_2^2 u^2$.

Background Model and Setting of the Problem:

- We consider the input signal **s** 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:

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

  where $\mathbb{W}$ is the sphere of feasible input signals. This scheme has the meaning of the Maximum–A-Posteriori (**MAP**) estimator with a uniform prior distribution over the sphere $\mathbb{W}$.

- The quality of the reconstruction will be characterized via the ratio

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

  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.
  Our goal: Evaluate p_N for $N \gg 1$ as a function of the Noise-to-Signal ratio for a given degree of **redundancy** $\mu = M/N > 1$ and **nonlinearity** $a = R^2 J_2^2 / J_1^2$.

Main Results for General Nonlinearity I:

Given the source signal strength $R > 0$, and the redundancy $\mu = M/N > 1$, the **mean value** of the parameter p_N characterising quality of the information recovery in the **Least-Square** reconstruction scheme with the noise $\mathbf{b} \sim \mathcal{N}(\mathbf{0}, \sigma^2 \mathbf{1}_M)$ is given asymptotically for $N \to \infty$ by

$$p_\infty := \lim_{N\to\infty} \langle p_N \rangle = \tfrac{t}{R}\,,$$

where the specific value of $t \in [0, R]$ should be found in the framework of the **Parisi** scheme of the **Full Replica Symmetry Breaking** (FRSB) by **minimizing** the functional

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

over t, and **maximizing** it over all the variables $v \geq 0$ and $Q \in [0, R^2]$ and over a non-decreasing function $w_s(u)$ with the argument $u \in [R^2 - Q, R^2]$.

Main Result for General Nonlinearity II:

- In a certain range of parameters (e.g. the redundancy and nonlinearity) the above variational problem is solved by the **Replica-Symmetric** Ansatz $Q = 0$. In that case for a given 'bare' Noise-to-Signal ratio $\gamma = \sigma^2/R^2$ the quality parameter $p_\infty = p \in [0,1]$ is given by the solution of a **single** algebraic equation:

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

- For the alternative range of parameters the variational problem can be solved by the **FRSB Ansatz** assuming the minimizer function $w_s(u)$ to be **continuous** and **non-decreasing** for $u \in [R^2 - Q, R^2]$. In that case the value $p_\infty = p$ is given by the solution of the system of a **pair** of algebraic equations in the variables $p \in [0,1]$ and $Q \in (0, R^2]$:

$$\mu\,\left[\Phi'(R^2 p)\right]^2\left(R^2(1-p^2) - Q\right)\right)$$

$$= p^2\Phi'(R^2 - Q)\left[R^2\gamma + \Phi(R^2) - 2\Phi(R^2 p) + \Phi(R^2 - Q)\right]$$

and

$$\left[\Phi'(R^2 - Q)\right]^3 p^2 = \mu\left[\Phi'(R^2 p)\right]^2\left[\Phi'(R^2 - Q) - \Phi''(R^2 - Q)\left(R^2(1-p^2) - Q\right)\right]$$

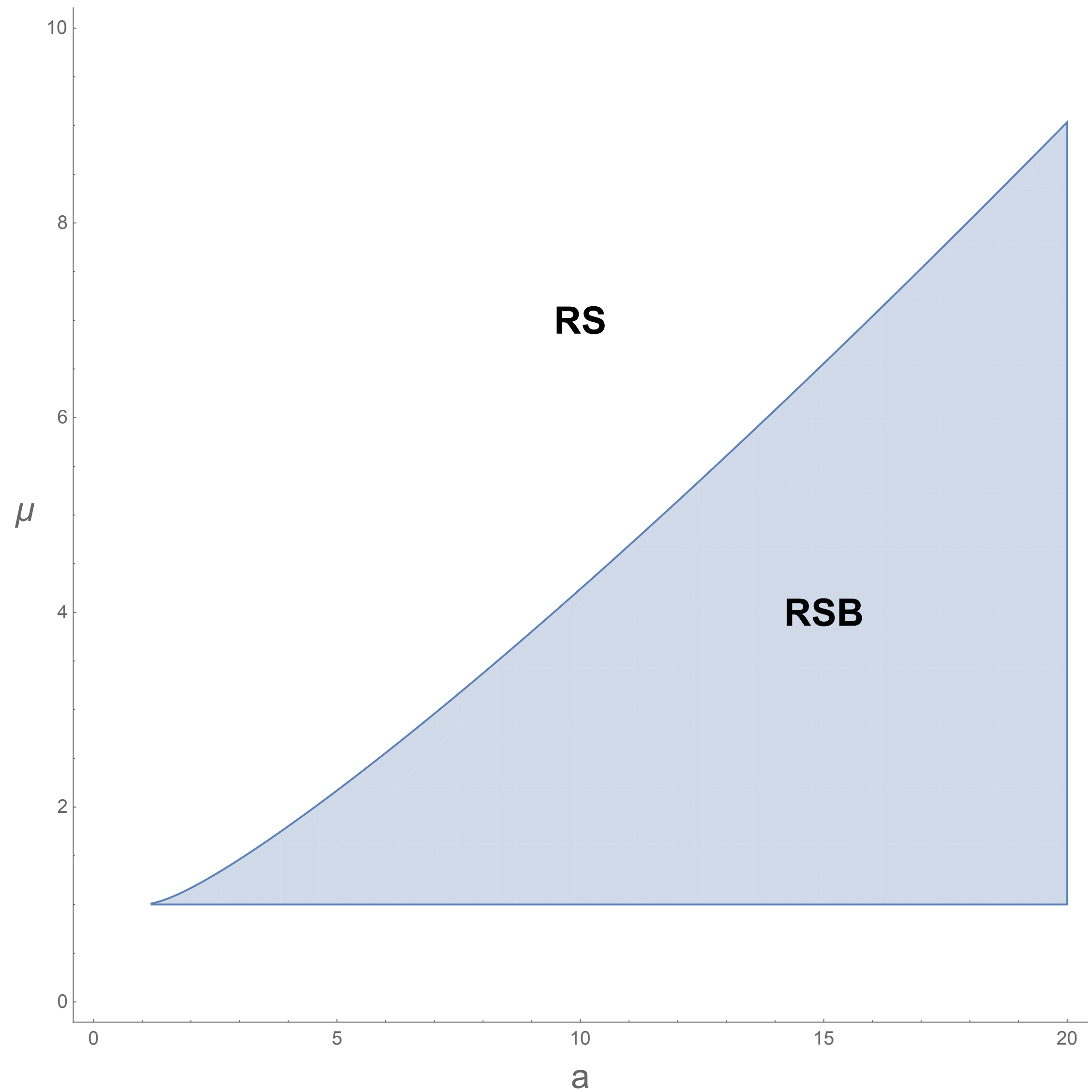

Figure 1: Schematic Phase diagram in $(a = J_2^2/J_1^2, \mu = M/N)$ plane for **Linear-Quadratic** encryptions. In the shaded region of parameters $1 < \mu < \frac{(a^{2/3} - a^{1/3} + 1)^3}{a}$ replica symmetry must be fully broken for some amplitude of the noise.

Reconstruction quality for a generic linear-quadratic encryptions:

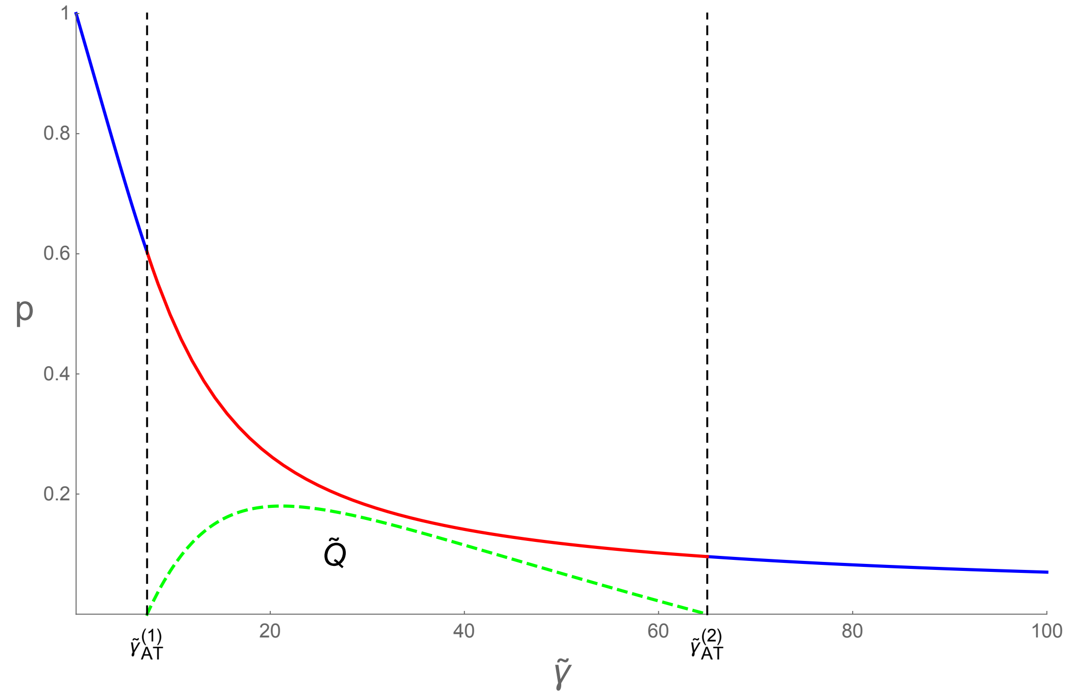

Figure 2: The **quality parameter** p as a function of the scaled **noise-to-signal** ratio $\tilde{\gamma} = \frac{\sigma^2}{R^2 J_1^2}$ for a generic representative of **Linear-Quadratic** encryptions with the nonlinearity $a = J_2^2 / J_1^2 = 8$ and the redundancy $\mu = 2$. In the interval of scaled 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 $\tilde{Q} = Q/R^2$, plotted as a green broken line. Finally, $p_\infty \sim \tilde{\gamma}^{-1/2}$ as $\tilde{\gamma} \to \infty$ as long as $a < \infty$.

Reconstruction quality for purely quadratic encryptions a $= \infty$:

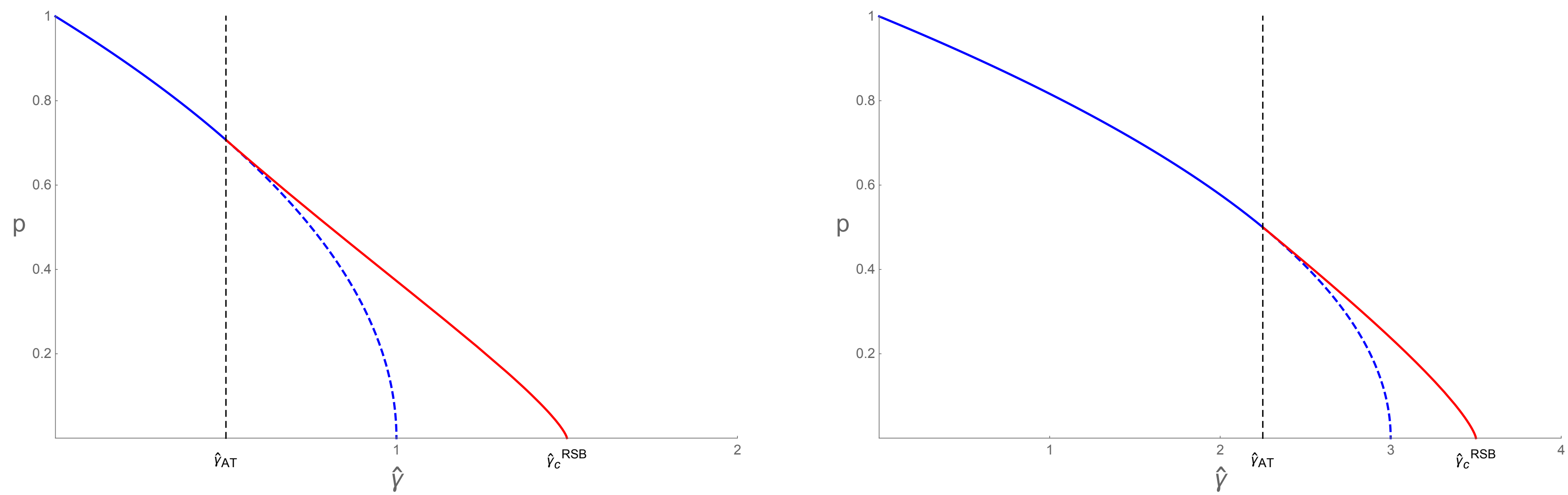

Figure 3: The **quality parameter** p as a function of the scaled **noise-to-signal** ratio $\hat{\gamma} = \frac{\sigma^2}{J_2^2 R^4}$ for **purely quadratic** encryptions and two different redundancies: $\mu = 2$ (left) and $\mu = 4$ (right).
There always exists a **threshold value** $\hat{\gamma}_c(\mu)$ such that $p_\infty = 0$ for $\hat{\gamma} > \hat{\gamma}_c(\mu)$ making the reconstruction **impossible** beyond some level of noise. The behaviour close to the threshold is given by $p_\infty \sim (\hat{\gamma}_c - \hat{\gamma})^{3/4}$ and is controlled by the **replica symmetry breaking** mechanism.
The blue broken curve is the continuation of the replica-symmetric solution in the region of Full RSB.

Remarks on the Method I:

Given the **fixed signal** **s** we interpret the **cost/loss** function

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

as an **energy** associated with a vector of N 'soft spins' $\mathrm{x}^T = (x_1, \dots, x_N)$, with the configurations constrained to the sphere $\mathbb{W}$ of radius $|\mathbf{x}| = N\sqrt{R}$. In this way we can put the **least square** minimization problem in the context of **spin glass**-like Statistical Mechanics after introducing the inverse temperature parameter $\beta > 0$, and defining the partition function of the model as

$$\mathcal{Z}_\beta = \int_{\mathbb{W}} e^{-\beta \mathcal{H}_{\mathrm{s}}(\mathbf{x})} d\mathbf{x}, \quad d\mathbf{x} = \prod_{i=1}^{N} dx_i\,.$$

We then consider the Boltzmann-Gibbs weights $\pi_\beta(\mathbf{x}) = \mathcal{Z}_\beta^{-1} e^{-\beta \mathcal{H}_{\mathbf{s}}(\mathbf{x})}$ associated with any configuration x on the sphere $\mathbb{W}$. In the **zero-temperature** limit $\beta \to \infty$ the weights $\pi_\beta(\mathbf{x})$ concentrate on the set of globally minimal values of the cost function. In particular, by considering

$$\left\langle p_N^{(\beta)} \right\rangle := \left\langle \frac{1}{\mathcal{Z}_\beta} \int_{\mathbb{W}} \frac{(\mathbf{x}, \mathbf{s})}{N R^2} e^{-\beta \mathcal{H}_{\mathbf{s}}(\mathbf{x})} d\mathbf{x} \right\rangle_{V, \mathbf{b}}$$

we aim to evaluating $p_\infty := \lim_{\beta \to \infty} \lim_{N \to \infty} \left\langle p_N^{(\beta)} \right\rangle$ providing us with a measure of the quality of the asymptotic signal reconstruction in our optimization problem.

Remarks on the Method II:

At the next step we employ the **replica trick** identity $\left\langle p_N^{(\beta)} \right\rangle = \lim_{n\to 0} \left\langle p_{N,n}^{(\beta)} \right\rangle$, where we defined

$$\left\langle p_{N,n}^{(\beta)} \right\rangle = \int_{\mathbb{W}} \cdots \int_{\mathbb{W}} \left[\frac{1}{n}\sum_{c=1}^{n} \frac{(\mathbf{x}_c, \mathbf{s})}{NR^2}\right] \left\langle e^{-\beta \sum_{a=1}^{n} \mathcal{H}_{\mathbf{s}}(\mathbf{x}_a)} \right\rangle \prod_{a=1}^{n} d\mathbf{x}_a \,.$$

Using the Gaussian nature of $V(\mathbf{x})$ entering to $\mathcal{H}_{\mathbf{s}}(\mathbf{x})$ in a squared form and exploiting its covariance structure one can show that

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

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

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

Finally, one may notice that the integrand remains **invariant** under a simultaneous change $\mathbf{x}_a \to O_{\mathbf{s}}\mathbf{x}_a$ for all $a = 1, \ldots, n$ where $O_{\mathbf{s}}$ are all possible rotations around the axis whose direction is given by the vector s. As a result, one can use the new integration variables: the $n \times n$ **matrix of scalar products** $Q_{ab} = (\mathbf{x}_a, \mathbf{x}_b) \geq 0$ and the n-component vector $\mathbf{t} = (t_1, \ldots, t_n) \in \mathbb{R}^n$ of projections $t_a = (\mathbf{x}_a, \mathbf{s})$.

Summary:

We defined an encryption of a signal $\mathrm{s} \in \mathbb{R}^{\mathbb{N}}$ as a random mapping $\mathrm{s} \mapsto \mathbf{y} \in \mathbb{R}^M$ known both to the sender and a recipient. Given the encryption redundancy (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 **s** from its corrupted image **z** $=$ **y** $+$ **b** by the **Least Square** Scheme for a certain class of random Gaussian mappings.

- We used the **Parisi replica symmetry breaking** scheme to evaluate the mean overlap $p_\infty \in [0,1]$ between the original signal and its recovered image for a given noise-to-signal ratio γ as $N \to \infty$. We explicitly analyzed the case of the **linear-quadratic** family of random mappings.

  When **nonlinearity** exceeds a certain **threshold** but redundancy is not yet too big, the **replica symmetry** is necessarily **broken** in some interval of γ.
  We show that encryptions with a nonvanishing **linear component** permit reconstructions with for any $\mu > 1$ and any $\gamma < \infty$, with $p_\infty \sim \gamma^{-1/2}$ as $\gamma \to \infty$. In contrast, for the case of **purely quadratic** nonlinearity, for any $\mu > 1$ there exists a threshold 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.

- **Open questions:**

  The problem is shown to be equivalent to finding the configuration of minimal energy in a certain version of spherical spin glass model, with **squared** Gaussian random interaction potential. It would be interesting and instructive, in particular,

  – to develop **rigorous** approach to this type of landscapes beyond replicas, in particular to study **complexity** associated with the stationary points/minima. So far we managed to do it only for the special type of **purely linear** Least Square schemes (with **R. Tublin**, in progress.)
  – to study fluctuations in the overlap and/or in the depth of global minimum, etc.
  – Analyze gradient search dynamics on the sphere.