Polynomials with Error (PWE)

M. R. Albrecht⋆, J.-C. Faugère⋆, D. Lin†, and L. Perret⋆

INRIA⋆, Paris-Rocquencourt Center, SALSA Project
UPMC Univ Paris 06, UMR 7606, LIP6, F-75005, Paris, France
CNRS, UMR 7606, LIP6, F-75005, Paris, France
SKLOIS†, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China

Abstract

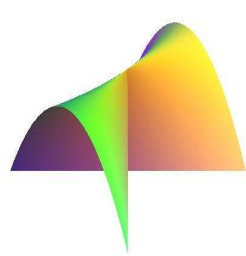
We investigate the hardness of solving non-linear equations modulo a prime $q = \text{poly}(n)$ with noise (typically a Gaussian), i.e., some equations of the algebraic system are erroneous. This problem, that we have called *Polynomial With Errors* (PWE), is a non-linear (and rather natural) generalization of the *Learning With Errors* (LWE) problem [Reg10]. Cryptographic schemes based on LWE [Reg10] enjoy usually of very strong security guarantee thanks to properties such as decision/search equivalence, average/worst case equivalence and a reduction to the worst-case of some classical lattice problems. On the other hand, such strong guarantees lead so far to rather impractical schemes as pointed in [RS10]. The hardness of PWE is supported by the hardness of solving algebraic equations without errors; the PoSSo problem. Solving non-linear system being significantly harder than solving a linear system, it is reasonable to expect that solving PWE will be harder than LWE. However, it can be shown that if the number of equations is $\text{poly}(n)$ (n being the number of variables) then PWE is essentially equivalent to a LWE instance with bigger parameters. Therefore, the most interesting case to consider is PWE for a fixed and small number ($\text{i.e.} < \text{poly}(n)$) of equations. We denote by bPWE this problem, i.e. PWE with a bounded ($< \text{poly}(n)$) number of samples. We prove that bPWE has also a decision/search equivalence and average-case/worst-case reduction. As a by-product, we show that such results also hold for bPWE without noise, i.e. PoSSo. Finally, It is possible to design a public-key encryption scheme based on bPWE we similar to the one using LWE [Reg10]. However, it has been shown that there s an equivalence between solving and sampling in the noise free setting. The result mentionned before is an obstacle to adapt the proof of security.

Polynomial System Solving (PoSSo) problem

Let $\mathbb{K}$ be a finite field.

- **Input:** non-linear polynomials $f_1(x_1,\ldots,x_n),\ldots,f_m(x_1,\ldots,x_n) \in \mathbb{K}[x_1,\ldots,x_n]$ of degree $d > 1$.
- **Secret:** a vector $\mathbf{z} = (\mathbf{z_1},\ldots,\mathbf{z_n}) \in \mathbb{K}^n$ chosen uniformly such that:

$$\begin{cases} f_1(z_1,\ldots,z_n) = 0 \\ f_2(z_1,\ldots,z_n) = 0 \\ \vdots \\ \vdots \\ f_m(z_1,\ldots,z_n) = 0 \end{cases}$$



Set of solutions of a surface.

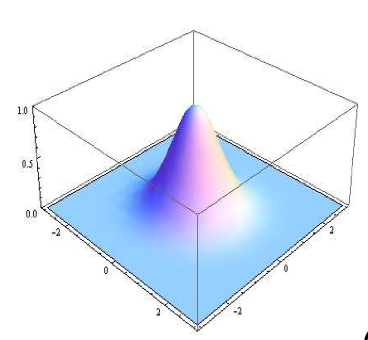
Question: find a common zero of $f_1,\ldots,f_m$.

Polynomial With Errors (PWE) problem

Let $q = \text{char}(\mathbb{K})$ be a prime, and $\chi_{\alpha,q}$ be the **(discretized) Gaussian distribution** of standard deviation $\alpha \cdot q$.

- **Input:** non-linear polynomials $f_1(x_1,\ldots,x_n),\ldots,f_m(x_1,\ldots,x_n) \in \mathbb{K}[x_1,\ldots,x_n]$ of degree $d > 1$.
- **Secret:** a vector $\mathbf{z} = (\mathbf{z_1},\ldots,\mathbf{z_n}) \in \mathbb{K}^n$ chosen uniformly such that:

$$\begin{cases} f_1(z_1,\ldots,z_n) = e_1 \\ f_2(z_1,\ldots,z_n) = e_2 \\ \vdots \\ \vdots \\ f_m(z_1,\ldots,z_n) = e_m \end{cases} \quad \text{with } (e_1,\ldots,e_m) \in (\chi_{\alpha,q})^m.$$



Gaussian in 2D.

Question: find the secret.

Remark. PWE is at least as hard as PoSSo.

- ☞ Let d be the degree of the equations. If $m = \mathcal{O}(n^d)$, then PWE ≈ LWE and PoSSo is easy (i.e. can be solved in poly-time).
- ☞ We consider PWE with $m \approx Cn$ (with $C > 1$ being a constant), i.e. **fixed and bounded number of samples (unlike LWE)**.
- ☞ For random instances with such parameters, PoSSo is algorithmically hard (i.e. the best algorithm is exponential).
- ☞ The secret is unique w.h.p.

Property [Work in Progress]
Let $q = \text{char}(\mathbb{K}) = \text{poly}(n)$ be a prime. We denote by dPoSSo *(resp.* dPWE*) the decisional variant of* PoSSo *(resp.* PWE*). It holds that:*

- ☞ **(search-to-decision)** PoSSo *(resp.* PWE*) and* dPoSSo *(resp.* dPWE*) are equivalent.*
  - *Proof adapted from [BGP09, MM11].*
- ☞ **(amplification)** *An algorithm allowing to solve* PoSSo *(resp.* PWE*) for a small fraction (poly-size) of the secrets allows to solve* PoSSo *(resp.* PWE*) for all secrets.*
  - *Proof adapted from [Reg09].*

Cryptosystem based on PWE

Motivation.

- ☞ Design a cryptosystem using the hardness of **random instances** of PoSSo (and not based on lattices problems)
  - Can lead to smaller public-key than "basic" PKC based on LWE.

Description of the Scheme.

- **Private key.** The private key is a vector $\mathbf{s}$ chosen uniformly at ransom in $\mathbb{Z}_q^n$.
- **Public key.** The public key is $\big(\mathbf{p} = (p_1,\ldots,p_m), \mathbf{b}\big) \in \mathbb{Z}_q[x_1,\ldots,x_n]^m \times \mathbb{Z}_q^m$ such that $\mathbf{b} = \mathbf{p}(\mathbf{s}) + \mathbf{e}$, with $\mathbf{e} \in (\chi_{\alpha,q})^m$.
- **Encryption.** For each bit of the message, we generate $(r_1,\ldots,r_m) \in \mathbb{Z}_2^m$. To encrypt $m \in \mathbb{Z}_2$, we send $\big(\sum_{i=1}^m p_i \cdot r_i, \sum_{i=1}^m b_i \cdot r_i + m \cdot \lfloor \frac{q}{2} \rfloor\big)$.
- **Decryption.** The decryption of a pair $(p,b) \in \mathbb{Z}_q[x_1,\ldots,x_n] \times \mathbb{Z}_q$ is 0 if $b - p(\mathbf{s}) \mod q$ is closer to 0 than to $\lfloor \frac{q}{2} \rfloor$, and 1 otherwise.

Remark. As described, the security proof from [Reg09] can not be directly adapted. Indeed, $\sum_{i=1}^m p_i \cdot r_i$ is **not uniform** in $\mathbb{Z}_q[x_1,\ldots,x_n]$.

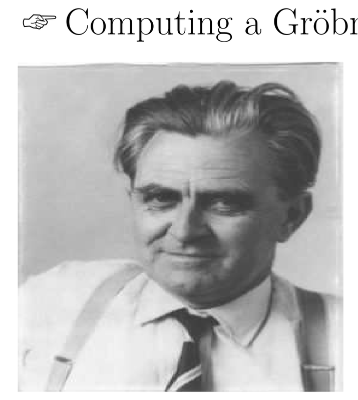
- ☞ More generally, let $\mathcal{I} =< p_1,\ldots,p_m >$ be an ideal of $\mathbb{K}[x_1,\ldots,x_n]$. Then, sampling uniformly elements of $\mathcal{I}$ is **as difficult as** computing a Gröbner basis of $\mathcal{I}$ [MRAP11].

Underlying Tool: Gröbner Bases

Definition [Buchberger 1965/1976 [Buc65]]
We fix an admissible ordering on the **monomials** *(i.e. a power product $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$) of $\mathbb{K}[x_1,\ldots,x_n]$. Let $\mathcal{I} =< f_1,\ldots,f_m >$ be an ideal of $\mathbb{K}[x_1,\ldots,x_n]$. A subset $G \subset \mathcal{I}$ is a* **Gröbner basis** *if:*

$$\forall f \in \mathcal{I},\ \exists g \in G \text{ such that LeadingMononomial}(g) \text{ divides LeadingMononomial}(f).$$

- ☞ Computing a Gröbner basis allows to solve PoSSo (and much more …)



W. Gröbner.

B. Buchberger.

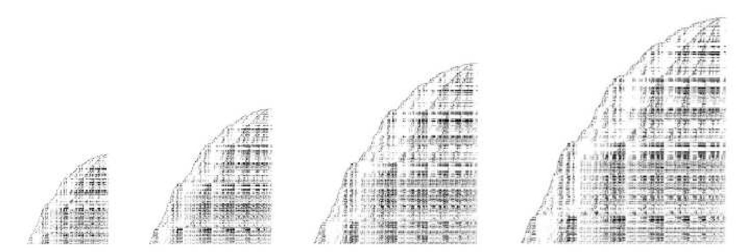
Algorithms & Complexity

- Buchberger's algorithm [Buc65] (1965)
- F_4/F_5 (J.-C. Faugère [Fau99, Fau02], 1999/2002)

⇒ For a **zero-dimensional** (i.e. **finite number of solutions**) system of n variables with m equations, the complexity of F_5 is :

$$\mathcal{O}\left(n^{3 \cdot d_{reg}(m,n)}\right),$$

$d_{reg}(m,n)$ being the **maximum degree** reached during the computation (a.k.a. degree of regularity).



Matrices occuring during the computation of a Gröbner basis with matrix-F_5. The last matrix considered is of size $\mathcal{O}\big(n^{d_{reg}(m,n)}\big)$.

Theorem [Bar04, BFSY05]
For a semi-regular system (i.e. **algebraic formalization of a random system of equations***) of quadratic equations, the complexity of computing a Gröbner basis is:*

- ☞ exponential *when $m = C \cdot n$ or $m = n + (C - 1)$ ($C \geq 1$ being a constant),*
- ☞ sub-exponential *when $m = C \cdot n \cdot \log(n)$,*
- ☞ polynomial *when $m = C \cdot n^2$.*

References

[Bar04] Magali Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie.* PhD thesis, Université de Paris VI, 2004.

[BFSY05] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Bo-Yin Yang. Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In *Proc. of MEGA 2005, Eighth International Symposium on Effective Methods in Algebraic Geometry*, 2005.

[BGP09] Côme Berbain, Henri Gilbert, and Jacques Patarin. Quad: A multivariate stream cipher with provable security. *J. Symb. Comput.*, 44(12):1703–1723, 2009.

[Buc65] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, University of Innsbruck, 1965.

[Fau99] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139:61–88, June 1999.

[Fau02] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In T. Mora, editor, *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation ISSAC*, pages 75–83. ACM Press, July 2002. isbn: 1-58113-484-3.

[MM11] Daniele Micciancio and Petros Mol. Pseudorandom knapsacks and the sample complexity of lwe search-to-decision reductions, 2011.

[MRAP11] Jean-Charles Faugère Martin R. Albrecht, Pooya Farshim and Ludovic Perret. Polly cracker, revisited, 2011.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), 2009.

[Reg10] Oded Regev. The learning with errors problem (invited survey). In *IEEE Conference on Computational Complexity*, pages 191–204. IEEE Computer Society, 2010.

[RS10] Markus Rückert and Michael Schneider. Estimating the security of lattice-based cryptosystems. *Cryptology ePrint Archive*, (2010/137), 2010.