Post-Quantum Cryptography

Based on Lattices and on Multivariate Polynomial Equations

Daniel Cabarcas Jaramillo

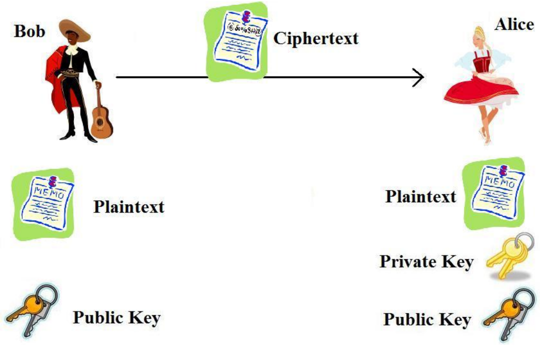
Escuela de Matemáticas
Universidad Nacional de Colombia, Sede Medellín

Eafit, Medellín, August 2016

Overview

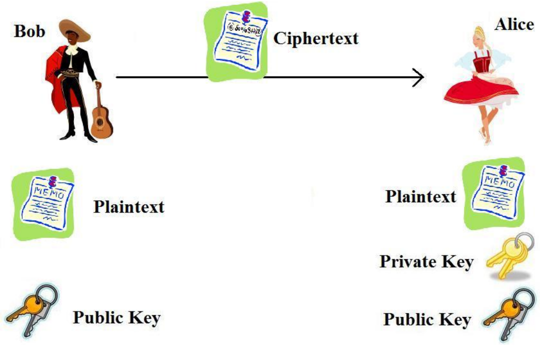
Post-Quantum Cryptography

- Public key crypto – 60's – DH (Discrete log), RSA (Factoring)



Post-Quantum Cryptography

- Public key crypto – 60's – DH (Discrete log), RSA (Factoring)



- Shor's discrete log and factoring quantum algorithms 1996
- First post-quantum workshop 2006
- NSA anouncement 2015, NIST competition open 2016

Post-Quantum Cryptography – Flavors

Based on:

- Lattice theory
- Multivariate Polynomials
- Coding Theory
- Hash functions

Content

Lattice-Based Crypto

Pros:

- Robust security guarantee: Worst-to-average-case reduction
- Flexibility: Homomorphic encryption, obfuscation

Cons:

- Inefficient
- Hard to determine secure parameters

Cryptographic Hash Function

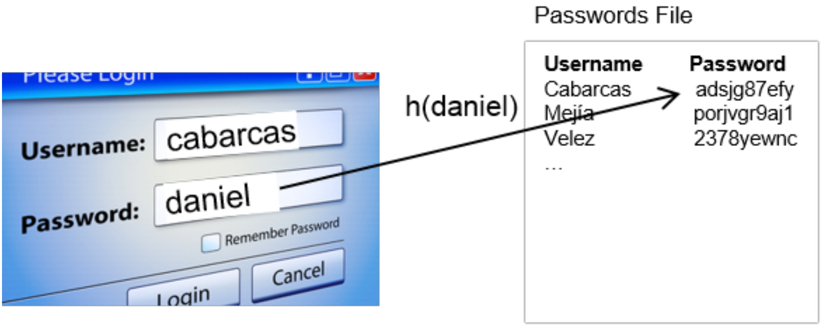
A cryptographic hash function $h(x)$ provides:

- **Compression:** the range of h is smaller than its domain
- **Efficiency:** It is efficient to compute h
- **Collision resistance:** It is unfeasible to find $x \neq y$ such that $h(x) = h(y)$

Cryptographic Hash Function

A cryptographic hash function $h(x)$ provides:

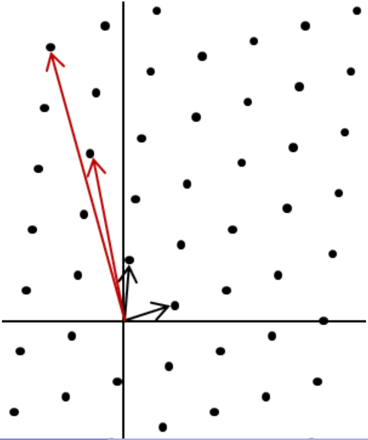
- **Compression:** the range of h is smaller than its domain
- **Efficiency:** It is efficient to compute h
- **Collision resistance:** It is unfeasible to find $x \neq y$ such that $h(x) = h(y)$
- **Application:** Store passwords



Lattice Theory

- A **lattice** is a discrete subgroup of $\mathbb{R}^n$
- A **basis** B for a lattice L is a set of LI vectors $b_1, \ldots, b_m$ such that $L = \mathcal{L}(B) = \{\sum x_i b_i : x_i \in \mathbb{Z}\}$

- Given an arbitrary basis, in general, it is hard to find **the shortest vector**
- The best algorithms are:
  - LLL, finds an exp. approx. in poly time
  - Ennumeration, finds the shortest vector in exp. time
  - BKZ, can be tuned



Lattice-based Hash [Ajt96]

- For a security parameter n
- Let $m, q \in \mathbb{N}$ be such that $n \log q < m < \frac{q}{2n^4}$ y $q = \mathcal{O}(n^c)$ for some constant c (e.g. $m = n^2, q = n^7$)
- Choose $M \leftarrow \mathbb{Z}_q^{n \times m}$

$$\begin{aligned} h_M \colon \{0,1\}^m &\to \mathbb{Z}_q^n \\ s &\mapsto Ms \mod q \end{aligned}$$

Lattice-based Hash [Ajt96]

- For a security parameter n
- Let $m, q \in \mathbb{N}$ be such that $n \log q < m < \frac{q}{2n^4}$ y $q = \mathcal{O}(n^c)$ for some constant c (e.g. $m = n^2, q = n^7$)
- Choose $M \leftarrow \mathbb{Z}_q^{n \times m}$

$$\begin{aligned} h_M \colon \{0,1\}^m &\to \mathbb{Z}_q^n \\ s &\mapsto Ms \mod q \end{aligned}$$

- Compression and efficiency are easy to verify

Lattice-based Hash [Ajt96]

- For a security parameter n
- Let $m, q \in \mathbb{N}$ be such that $n \log q < m < \frac{q}{2n^4}$ y $q = \mathcal{O}(n^c)$ for some constant c (e.g. $m = n^2, q = n^7$)
- Choose $M \leftarrow \mathbb{Z}_q^{n \times m}$

$$\begin{aligned} h_M \colon \{0,1\}^m &\to \mathbb{Z}_q^n \\ s &\mapsto Ms \mod q \end{aligned}$$

- Compression and efficiency are easy to verify
- Security: consider the lattice

$$\Lambda_q^*(M) = \{v \in \mathbb{R}^m : Mv = 0 \mod q\}$$

Worst-to-Average-Case Reduction

Theorem ([Ajt96])

If it is possible for an adversary, that executes in poli(n) *time, to find a collision of* **one** *randomly chosen instance of* h_M *with non-negligible probability, then it is possible to solve* **any** *instance of* n^c*-SIVP in dimension* n *in* poli(n) *time.*

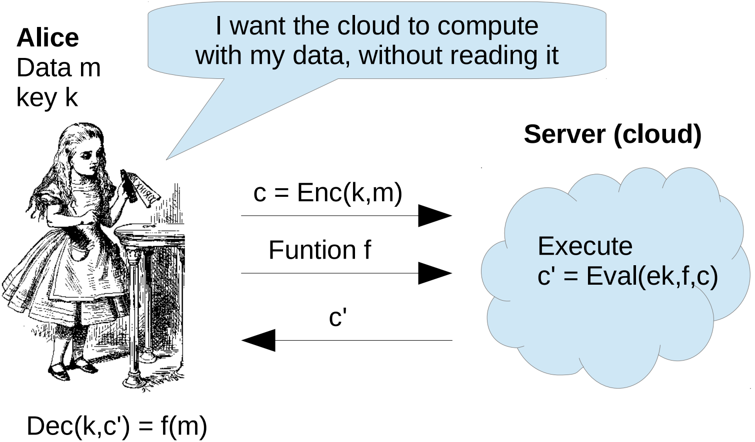
Developments Since Ajtai's work

- Efficiency improvements to Ajtai's hash [Mic01, MR07]
- LWE problem and public key encryption based on LWE [Reg05]
- Ring-LWE [LPR10]
- Fully homomorphic encryption (FHE) [Gen09]

My Work

- Discrete Ziggurat Gaussian Sampling [BCG+14]
- Uniform noise lattice-based encryption [CGW14]
- Ring Isomorphism encoding for FHE [GC14]

Homomorphic Encryption



Integer Encoding in HE

- The potential of HE is huge
- To compute over encrypted data is **ineficient**
- We should take the most out of each homomorphic operation
- The space of messages in HE has an **algebraic structure** e.g $R_p = \mathbb{Z}[x]/\langle x^n + 1, p\rangle$, with p an integer

Integer Encoding in HE

- The potential of HE is huge
- To compute over encrypted data is **ineficient**
- We should take the most out of each homomorphic operation
- The space of messages in HE has an **algebraic structure** e.g $R_p = \mathbb{Z}[x]/\langle x^n + 1, p\rangle$, with p an integer

¿How to encode as much information as possible in this message space, in a way that the operations are meaningful?

RIE Integer Encoding [GC14]

- Message space: $R_p = \mathbb{Z}[x]/\left\langle x^n + 1, p \right\rangle$

Key observation: R_p is isomorphic as a ring to $\mathbb{Z}_t$ for certain polynomials p

RIE Integer Encoding [GC14]

- Message space: $R_p = \mathbb{Z}[x] / \langle x^n + 1, p \rangle$

Key observation: R_p is isomorphic as a ring to $\mathbb{Z}_t$ for certain polynomials p

- Then we can encode integers directly

RIE Integer Encoding [GC14]

- Message space: $R_p = \mathbb{Z}[x]/\langle x^n + 1, p \rangle$

> **Key observation:** R_p is isomorphic as a ring to $\mathbb{Z}_t$ for certain polynomials p

- Then we can encode integers directly
- This does not affect the security of the scheme

RIE Integer Encoding [GC14]

- Message space: $R_p = \mathbb{Z}[x]/\langle x^n + 1, p\rangle$

Key observation: R_p is isomorphic as a ring to $\mathbb{Z}_t$ for certain polynomials p

- Then we can encode integers directly
- This does not affect the security of the scheme
- And improves the efficency compared to previously used encodings

Content

Crypto Based on Multivariate Polynomials

Pros:

- Efficient constructions
- Practical security well understood

Cons:

- Attacks on Ad hoc constructions have deslegitimize the area

MPKC – General Idea

- k finite field of q elements (e.g., $k = \{0, 1\}$).

MPKC – General Idea

- k finite field of q elements (e.g., $k = \{0, 1\}$).
- **Public key**: a trapdoor function $P : k^n \to k^m$ defined by

$$P(x_1, \ldots, x_n) = (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n)).$$

MPKC – General Idea

- k finite field of q elements (e.g., $k = \{0, 1\}$).
- **Public key**: a trapdoor function $P : k^n \to k^m$ defined by

$$P(x_1, \ldots, x_n) = (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n)).$$

- **Private key**: a way (the trapdoor information) to “invert” P.

MPKC – General Idea

- k finite field of q elements (e.g., $k = \{0, 1\}$).
- **Public key**: a trapdoor function $P : k^n \rightarrow k^m$ defined by

$$P(x_1, \ldots, x_n) = (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n)).$$

- **Private key**: a way (the trapdoor information) to "invert" P.
- **Plaintext:** $(x_1, \ldots, x_n)$.

MPKC – General Idea

- k finite field of q elements (e.g., $k = \{0, 1\}$).
- **Public key**: a trapdoor function $P : k^n \to k^m$ defined by

$$P(x_1, \ldots, x_n) = (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n)).$$

- **Private key**: a way (the trapdoor information) to "invert" P.
- **Plaintext:** $(x_1, \ldots, x_n)$.
- **Ciphertext:** $(y_1, \ldots, y_m) = P(x_1, \ldots, x_n)$.

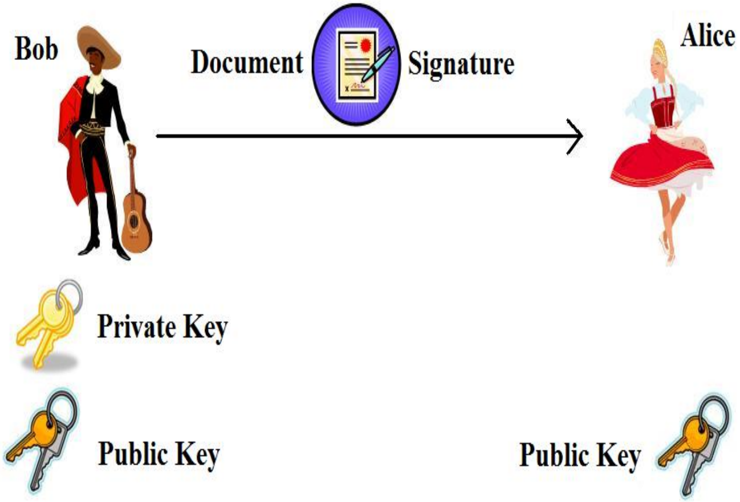
MPKC – General Idea

- k finite field of q elements (e.g., $k = \{0, 1\}$).
- **Public key**: a trapdoor function $P : k^n \to k^m$ defined by

$$P(x_1, \ldots, x_n) = (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n)).$$

- **Private key**: a way (the trapdoor information) to "invert" P.
- **Plaintext:** $(x_1, \ldots, x_n)$.
- **Ciphertext:** $(y_1, \ldots, y_m) = P(x_1, \ldots, x_n)$.
- **Underlying problem:**
  - MQ: Solving a system of multivariate quadratic equations
  - NP-complete

Signature Scheme



MPKC Signature Scheme – Oil-Vinegar [Pat97]

- Oil-Vinegar polynomial:

$$f = \sum_{i=1}^{o}\sum_{j=1}^{v} a_{ij}x_i t_j + \sum_{i=1}^{v}\sum_{j=1}^{v} b_{ij}t_i t_j + \sum_{i=1}^{o} c_i x_i + \sum_{j=1}^{v} d_j t_j + e,$$

with $a_{ij}, b_{ij}, c_i, d_j, e \in k$.

MPKC Signature Scheme – Oil-Vinegar [Pat97]

- Oil-Vinegar polynomial:

$$f = \sum_{i=1}^{o}\sum_{j=1}^{v} a_{ij}x_i t_j + \sum_{i=1}^{v}\sum_{j=1}^{v} b_{ij}t_i t_j + \sum_{i=1}^{o} c_i x_i + \sum_{j=1}^{v} d_j t_j + e,$$

  with $a_{ij}, b_{ij}, c_i, d_j, e \in k$.

- **Private key:**
  - $F = (f_1, \ldots, f_o) : k^{o+v} \to k^o$, with f_i randomly chosen O-V polynomials.
  - $L : k^{o+v} \to k^{o+v}$ invertible affine transformation chosen uniformly at random.

- **Public key:** $P = (p_1, \cdots, p_o) : k^{o+v} \to k^o$ defined by

$$P(x_1, \ldots, x_o, t_1, \ldots, t_v) = F \circ L(x_1, \ldots, x_o, t_1, \ldots, t_v).$$

Oil-Vinegar Signature Generation

- Randomly choose $t_1 = w_1, \ldots, t_v = w_v$, with $w_1, \ldots, w_v \in k$.

Oil-Vinegar Signature Generation

- Randomly choose $t_1 = w_1, \dots, t_v = w_v$, with $w_1, \dots, w_v \in k$.
- Plug those into $F \Rightarrow$ linear system in variables $x_1, \dots, x_o$:

$$\begin{aligned} f_1(x_1, \dots, x_o, w_1, \dots, w_v) &= \tilde{y}_1 \\ f_2(x_1, \dots, x_o, w_1, \dots, w_v) &= \tilde{y}_2 \\ &\vdots \\ f_o(x_1, \dots, x_o, w_1, \dots, w_v) &= \tilde{y}_o, \end{aligned} \tag{1}$$

Oil-Vinegar Signature Generation

- Randomly choose $t_1 = w_1, \dots, t_v = w_v$, with $w_1, \dots, w_v \in k$.
- Plug those into $F \Rightarrow$ linear system in variables $x_1, \dots, x_o$:

$$\begin{aligned} f_1(x_1, \dots, x_o, w_1, \dots, w_v) &= \tilde{y}_1 \\ f_2(x_1, \dots, x_o, w_1, \dots, w_v) &= \tilde{y}_2 \\ &\vdots \\ f_o(x_1, \dots, x_o, w_1, \dots, w_v) &= \tilde{y}_o, \end{aligned} \tag{1}$$

- We solve this system using Gaussian elimination.

Oil-Vinegar Signature Generation

- Randomly choose $t_1 = w_1, \dots, t_v = w_v$, with $w_1, \dots, w_v \in k$.
- Plug those into $F \Rightarrow$ linear system in variables $x_1, \dots, x_o$:

$$\begin{aligned} f_1(x_1, \dots, x_o, w_1, \dots, w_v) &= \tilde{y}_1 \\ f_2(x_1, \dots, x_o, w_1, \dots, w_v) &= \tilde{y}_2 \\ &\vdots \\ f_o(x_1, \dots, x_o, w_1, \dots, w_v) &= \tilde{y}_o, \end{aligned} \tag{1}$$

- We solve this system using Gaussian elimination.
- If (1) has no solutions, repeat the process.

Developments in MPKC

- Signature schemes: U-OV [KPG99], HFEv- [PGC98]
- Identification scheme: Sakumoto [SSH11]
- Stream cipher: QUAD [BGP06]
- Attacks: Groebner bases [FJ03], min-rank [KS99], differential [DFSS07]

My Work

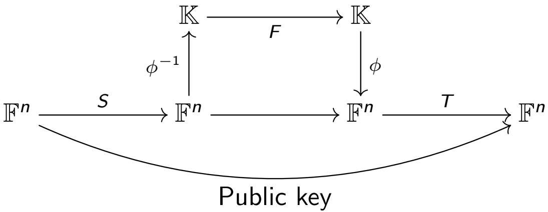
- Improvements in Groebner basis computation [MCD+10, BCDM10, CD11]
- Improvements to ZHFE [BCE+16]

Hidden Field Equations (HFE)

- $\mathbb{F} = \mathbb{F}_q$, $\mathbb{K}$ a degree n extension field of $\mathbb{F}$.
- $\phi\colon \mathbb{K} \to \mathbb{F}^n$ the standard $\mathbb{F}$-linear isomorphism.
- Choose a polynomial $F : \mathbb{K} \to \mathbb{K}$ of Hamming weight two, i.e,

$$F(X) = \sum_{q^i+q^j \leq D} a_{ij} X^{q^i+q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c,$$

- Choose uniformly at random two invertible affine transformations S and T over $\mathbb{F}^n$.

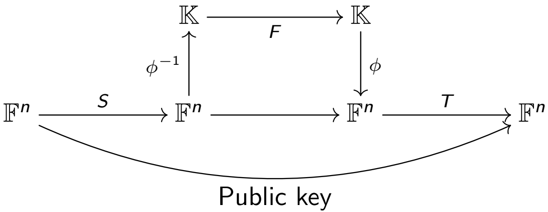


Hidden Field Equations (HFE)

- $\mathbb{F} = \mathbb{F}_q$, $\mathbb{K}$ a degree n extension field of $\mathbb{F}$.
- $\phi \colon \mathbb{K} \to \mathbb{F}^n$ the standard $\mathbb{F}$-linear isomorphism.
- Choose a polynomial $F : \mathbb{K} \to \mathbb{K}$ of Hamming weight two, i.e,

$$F(X) = \sum_{q^i+q^j \leq D} a_{ij} X^{q^i+q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c,$$

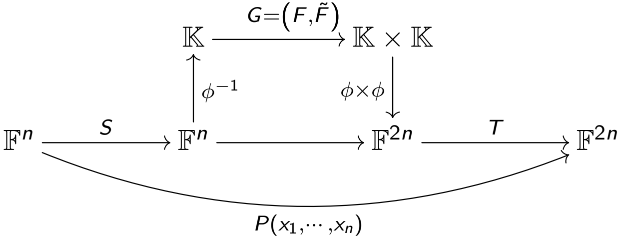
- Choose uniformly at random two invertible affine transformations S and T over $\mathbb{F}^n$.



- Broken by Groebner bases [FJ03], and min-rank [KS99]

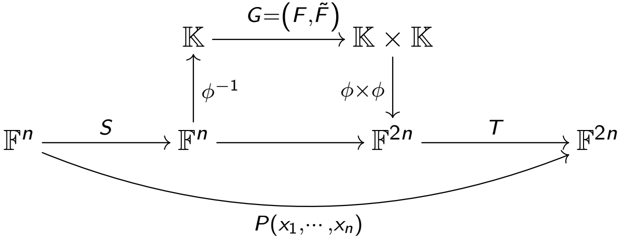
ZHFE trapdoor function [PBD15]

- $G = \left(F, \tilde{F}\right) : \mathbb{K} \to \mathbb{K} \times \mathbb{K}$ with $F, \tilde{F}$ of high degree and hegh rank.
- The new trapdoor function is $P = T \circ (\phi \times \phi) \circ G \circ \phi^{-1} \circ S$.



ZHFE trapdoor function [PBD15]

- $G = \left(F, \tilde{F}\right) : \mathbb{K} \to \mathbb{K} \times \mathbb{K}$ with $F, \tilde{F}$ of high degree and hegh rank.
- The new trapdoor function is $P = T \circ (\phi \times \phi) \circ G \circ \phi^{-1} \circ S$.



- G is chosen so that there exist Ψ of the form

$$\begin{aligned}\Psi =& X\left(\alpha_1 F_0 + \cdots + \alpha_n F_{n-1} + \beta_1 \tilde{F}_0 + \cdots + \beta_n \tilde{F}_{n-1}\right) + \\ & X^q\left(\alpha_{n+1} F_0 + \cdots + \alpha_{2n} F_{n-1} + \beta_{n+1} \tilde{F}_0 + \cdots + \beta_{2n} \tilde{F}_{n-1}\right),\end{aligned}$$

  such that $\deg(\Psi) \leq D_0$.

Thanks

Daniel Cabarcas – dcabarc@unal.edu.co

Facultad de Ciencias
Escuela de Matemáticas
Sede Medellín

UNIVERSIDAD NACIONAL DE COLOMBIA

Bibliography I

Miklós Ajtai.
Generating hard instances of lattice problems (extended abstract).
In *28th Annual ACM Symposium on Theory of Computing*, pages 99–108. ACM Press, May 1996.

Johannes Buchmann, Daniel Cabarcas, Jintai Ding, and MohamedSaiedEmam Mohamed.
Flexible partial enlargement to accelerate gröbner basis computation over GF2.
In DanielJ. Bernstein and Tanja Lange, editors, *Progress in Cryptology – AFRICACRYPT 2010*, volume 6055 of *Lecture Notes in Computer Science*, pages 69–81. Springer Berlin Heidelberg, 2010.

John B. Baena, Daniel Cabarcas, Daniel E. Escudero, Jaiberth Porras-Barrera, and Javier A. Verbel.
Efficient zhfe key generation.
In Tsuyoshi Takagi, editor, *Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings*, volume 9606 of *Lecture Notes in Computer Science*, pages 213–232. Springer International Publishing, Cham, 2016.

Johannes Buchmann, Daniel Cabarcas, Florian Göpfert, Andreas Hülsing, and Patrick Weiden.
Discrete ziggurat: A time-memory trade-off for sampling from a gaussian distribution over the integers.
In Tanja Lange, Kristin Lauter, and Petr Lisonak, editors, *Selected Areas in Cryptography – SAC 2013*, Lecture Notes in Computer Science, pages 402–417. Springer Berlin Heidelberg, 2014.

Côme Berbain, Henri Gilbert, and Jacques Patarin.
Quad: A practical stream cipher with provable security.
In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 109–128. Springer Berlin / Heidelberg, 2006.

Daniel Cabarcas and Jintai Ding.
Linear algebra to compute syzygies and gröbner bases.
In *Proceedings of the 36th international symposium on Symbolic and algebraic computation*, ISSAC '11, pages 67–74, New York, NY, USA, 2011. ACM.

Bibliography II

Daniel Cabarcas, Florian Göpfert, and Patrick Weiden.
Provably secure lwe encryption with smallish uniform noise and secret.
In *Proceedings of the 2Nd ACM Workshop on ASIA Public-key Cryptography*, ASIAPKC '14, pages 33–42, New York, NY, USA, 2014. ACM.

Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern.
Practical cryptanalysis of Sflash.
In Alfred Menezes, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2007.

Jean-Charles Faugère and Antoine Joux.
Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases.
In *Advances in cryptology—CRYPTO 2003*, volume 2729 of *Lecture Notes in Comput. Sci.*, pages 44–60. Springer, Berlin, 2003.

Matthias Geihs and Daniel Cabarcas.
Efficient integer encoding for homomorphic encryption via ring isomorphisms, 2014.
Sometido para publicación.

Craig Gentry.
A fully homomorphic encryption scheme.
PhD thesis, Stanford University, 2009.
crypto.stanford.edu/craig.

Aviad Kipnis, Jacques Patarin, and Louis Goubin.
Unbalanced oil and vinegar signature schemes.
In *Advances in cryptology—EUROCRYPT '99 (Prague)*, volume 1592 of *Lecture Notes in Comput. Sci.*, pages 206–222. Springer, Berlin, 1999.

Bibliography III

Aviad Kipnis and Adi Shamir.
Cryptanalysis of the HFE public key cryptosystem by relinearization.
In *Advances in cryptology—CRYPTO '99 (Santa Barbara, CA)*, volume 1666 of *Lecture Notes in Comput. Sci.*, pages 19–30. Springer, Berlin, 1999.

Vadim Lyubashevsky, Chris Peikert, and Oded Regev.
On ideal lattices and learning with errors over rings.
In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23. Springer, May 2010.

Mohamed Saied Emam Mohamed, Daniel Cabarcas, Jintai Ding, Johannes Buchmann, and Stanislav Bulygin.
MXL3: An efficient algorithm for computing gröbner bases of zero-dimensional ideals.
In Donghoon Lee and Seokhie Hong, editors, *Information, Security and Cryptology – ICISC 2009*, volume 5984 of *Lecture Notes in Computer Science*, pages 87–100. Springer Berlin Heidelberg, 2010.

Daniele Micciancio.
Improving lattice based cryptosystems using the Hermite Normal Form.
In *CaLC*, volume 2146 of *LNCS*, pages 126–145. Springer, 2001.

Daniele Micciancio and Oded Regev.
Worst-case to average-case reductions based on Gaussian measures.
SIAM Journal on Computing, 37(1):267–302, 2007.

Jacques Patarin.
Oil and vinegar signature scheme.
Dagstuhl Workshop on Cryptography, 1997.

Jaiberth Porras, John B. Baena, and Jintai Ding.
New Candidates for Multivariate Trapdoor Functions.
Revista Colombiana de MatemÃ¡ticas, 49(1):57–76, 2015.

Bibliography IV

Jacques Patarin, Louis Goubin, and Nicolas Courtois.
C*-+ and HM: Variations around two schemes of T. Matsumoto and H. Imai.
In *ASIACRYPT '98: Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security*, pages 35–49, London, UK, 1998. Springer-Verlag.

Oded Regev.
On lattices, learning with errors, random linear codes, and cryptography.
In Harold N. Gabow and Ronald Fagin, editors, *37th Annual ACM Symposium on Theory of Computing*, pages 84–93. ACM Press, May 2005.

Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari.
Public-key identification schemes based on multivariate quadratic polynomials.
In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 706–723. Springer Berlin / Heidelberg, 2011.

Appendix 1: SIVP

n^c-SIVP. Approximate Shortest Independent Vectors Problem

Appendix 1: SIVP

n^c-SIVP. Approximate Shortest Independent Vectors Problem
Given a basis B for an n dimension lattice L in $\mathbb{R}^n$, find a set of n LI vectors $v_1, \ldots, v_n$ such that

$$\max\{\|v_i\|\} \leq n^c \cdot \min\{\|S\| : S \text{ Set of } n \text{ LI vectors in } L\}$$