Toward a Rigorous Variation of Coppersmith's Algorithm on Three Variables

Aurélie Bauer[1] Antoine Joux[1,2]

[1]University of Versailles Saint-Quentin-en-Yvelines
PRISM Laboratory, France

[2]DGA

23rd May 2007

Finding roots of polynomial equations over $\mathbb{Z}$

p_1 irreducible over $\mathbb{Z}[x_1, \ldots, x_n]$

$$p_1(x_{0,1}, \ldots, x_{0,n}) = 0 \quad |x_{0,1}| < \mathbf{X_1}, \ldots, |x_{0,n}| < \mathbf{X_n} \quad \to \quad \textbf{Goal:} \text{ To recover } (x_{0,1}, \ldots, x_{0,n})$$

- **When n** $=$ **2**: Coppersmith's exact method + Variants
- **When n** $>$ **2**: Heuristic methods only

An integer lattice L (discrete subgroup of $\mathbb{Z}^n$)

$$L = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_r$$

Invariant: det L

LLL Algorithm (1982)

$$\begin{cases} (b_1, \ldots, b_r) \to (c_1, \ldots, c_r) \\ \text{GSO} : (c_1^\star, \ldots, c_r^\star) \end{cases}$$

Coppersmith's method on two variables

Example: $\boldsymbol{p_1(x,y) = a + bx + cy}$

$$|x_0| < X, |y_0| < Y$$

Goal: To construct $p_2(x,y)$ such that

$$\begin{cases} p_2(x_0, y_0) = 0 \\ p_2 \notin (p_1) \end{cases}$$

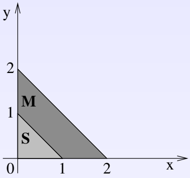


Figure: $S = \{1, x, y\}$ and $M = \{1, x, y, x^2, xy, y^2\}$

Algebraic independence between p_1 and p_2

If p_2 has monomials in M

$p_2 \in (p_1)$ $\Leftrightarrow$ p_2 linear combination of $\boldsymbol{p_1, xp_1, yp_1}$

Coppersmith's method on two variables

L_1 lattice generated by the rows of M_1

$$M_1 = \left(\begin{array}{cccccc|ccc} & & & & & & p_1 & xp_1 & yp_1 \\ \mathbf{1} & 0 & & \dots & & 0 & a & 0 & 0 \\ 0 & \frac{1}{X} & & & & & b & a & 0 \\ & & \frac{1}{Y} & & & \vdots & c & 0 & a \\ \vdots & & & \frac{1}{X^2} & & & 0 & b & 0 \\ & & & & \frac{1}{XY} & 0 & 0 & c & b \\ 0 & & \dots & & 0 & \frac{1}{Y^2} & 0 & 0 & c \end{array}\right) \begin{array}{c} \\ 1 \\ x \\ y \\ x^2 \\ xy \\ y^2 \end{array}$$

$$\mathbf{r_0} = (1, x_0, y_0, x_0^2, x_0 y_0, y_0^2) \quad \rightarrow \quad s_0 = r_0 M_1 \in L_1$$

s_0 short vector $\in L_1$

$$\begin{cases} s_0 & = & (1, \frac{x_0}{X}, \frac{y_0}{Y}, (\frac{x_0}{X})^2, \frac{x_0 y_0}{XY}, (\frac{y_0}{Y})^2, 0, 0, 0) \\ \|s_0\|_2 & \leq & \sqrt{6} \end{cases}$$

Coppersmith's method on two variables

Row operations on M_1

$$N_1 = \left(\begin{array}{c|c} A_1 & Id \\ \hline \boldsymbol{A_2} & \mathbf{0} \end{array}\right) \quad \}\boldsymbol{L_1'}$$

Every vector $u \in L_1'$ such that $\boldsymbol{u \perp \{V_{p_1}, V_{xp_1}, V_{yp_1}\}}$

- Vector $s_0 \in L_1' = (b_1, \ldots, b_r)$

If $\|s_0\|_2 < \|b_r^\star\|_2$ then $\begin{cases} (s_0|b_r^\star) = 0 \\ p_2(x_0, y_0) = 0 \end{cases}$

Algebraic independence between p_1 and p_2

Otherwise $p_2 \in (p_1)$
V_{p_2} linear combination of $V_{p_1}, V_{xp_1}, V_{yp_1}$ } **IMPOSSIBLE**

Problem with three variables

$$\begin{array}{c} p_1(x_0, y_0, z_0) = 0 \\ |x_0| < X, |y_0| < Y, |z_0| < Z \end{array}$$

Coppersmith's method
With x, y, z
and $(b^\star_{r-1}, b^\star_r)$

$\Rightarrow$

Try to create (p_2, p_3)
$p_2(x_0, y_0, z_0) = 0$
$p_3(x_0, y_0, z_0) = 0$

PROBLEM: heuristic method

p_2 independent from p_1
and
p_3 independent from p_1

BUT (p_1, p_2, p_3)
not necessarily
independent

How to ensure the independence

Notion of independence

p_1, p_2, p_3 algebraically independent if

$$P(p_1, p_2, p_3) = 0 \quad \Rightarrow \quad \mathbf{P = 0}$$

Previous construction
(p_1) is prime
$p_2 \notin (p_1)$

$\Rightarrow$

If $I = (p_1, p_2)$ prime
and $p_3 \notin I$

$\Downarrow$

INDEPENDENCE

- If I not prime $\Rightarrow$ replace it by another prime ideal I' (primary decomposition of ideals, radical)

Translate in term of linear independence

Need relation

Algebraic indep. $\Leftrightarrow$ Linear indep.

Given (p_1, p_2) want to find $\{r_1, \ldots, r_t\}$ such that

$$\{p_3 \in (p_1, p_2) \text{ and } p_3 \in M\}$$
$$\Updownarrow$$
$$\{p_3 = \textstyle\sum_{i=1}^{t} \lambda_i r_i \text{ with } \lambda_i \in \mathbb{Z}\}$$

Use Gröbner bases for the construction

If p_3 not a linear combination of the r_i's

$\Downarrow$

(p_1, p_2, p_3) independent

Generalized Coppersmith's method

Lattice L_l: Rows of M_l

$$M_l = \left(\begin{array}{ccc|c} \ddots & & & \overbrace{\downarrow \quad \downarrow \quad \downarrow}^{r_1,\ldots,r_t} \\ & \underbrace{X^{-f}Y^{-g}Z^{-h}}_{(f,g,h)\in M} & & \\ & & \ddots & \end{array} \right)$$

$$r_0 = (1, x_0, y_0, z_0, \ldots, (x_0^f y_0^g z_0^h))$$

$$t_0 = (1, \tfrac{x_0}{X}, \tfrac{y_0}{Y}, \ldots, \underbrace{0, \ldots, 0}_{t})$$

$$t_0 \in L'_l = (c_1, \ldots, c_r)$$

If $u \in L'_l$ $u \perp \{V_{r_1}, \ldots, V_{r_t}\}$

If $\|t_0\|_2 < \|c_r^\star\|_2$ then $\begin{cases} (t_0 | c_r^\star) = 0 \\ p_3(x_0, y_0, z_0) = 0 \end{cases}$

p_3 not a combination of the r_i's $\Downarrow$ **(p_1, p_2, p_3) independent**

Computing the bounds X, Y and Z

- **In general**

  Conditions **hard** to determine
  Difficulty to predict
  the determinant of a sublattice

- **However**

  For a particular shape of $\{r_1, \ldots, r_t\}$
  Known conditions on X, Y, Z
  Rigorous success

Application to a partial key exposure attack on RSA

- **Partial Key Exposure Attacks on RSA Up to Full Size Exponents.** *Eurocrypt 2005*
  M. Ernst, E. Jochemsz, A. May and B. de Weger

RSA modulus	Part of d known $\tilde{d}$
$N = pq$	$\lvert d \rvert \leq N^{\beta}$
$(e, d) : ed = 1 + k(N - (p + q - 1))$	$\lvert d_0 \rvert = \lvert d - \tilde{d} \rvert \leq N^{\delta}$

Need to find roots in a polynomial equation

- $p_1(x, y, z) = ex - yN + yz + R$ with $R = e\tilde{d} - 1$
- Root $(x_0, y_0, z_0) = (d_0, k, p + q - 1)$
- Conditions: $X = N^{\delta}$, $Y = N^{\beta}$ and $Z = 3\sqrt{N}$.

Comparison between two possible attacks

- **Heuristic attack**

  $$\begin{cases} \text{Direct construction of a lattice} \\ \text{Two short vectors} \rightarrow (p_2, p_3) \end{cases}$$

- **Our attack**

  $$\begin{cases} \text{Using } p_2 \text{ and our construction} \\ \text{Obtain a new polynomial } p_3 \end{cases}$$

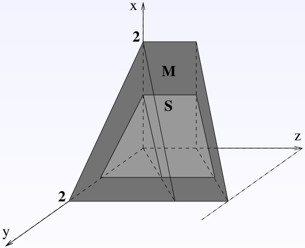
Experiments: Easy Case

$N = 256$ bits

[As in *Ernst et al.*]

$\beta = 0.35$

$d \simeq 90$ bits



Size of d_0		Heuristic A.	Our A.
δ	Bits	% Indep.	% Indep.
0.09	23	98	**100**
0.10	25	92	**100**
0.11	28	95	**100**
0.12	30	92	**100**
0.13	33	80	**100**
0.132	33	86	**100**
0.134	34	77	**100**
0.136	34	71	**100**
0.138	35	76	**100**
0.140	35	71	**100**
0.142	36	73	**100**
0.144	36	55	**100**
0.146	37	60	**100**
0.148	37	56	**100**
0.150	38	47	**100**

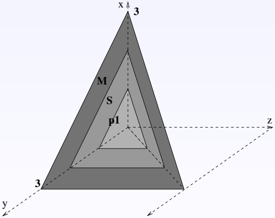
Experiments: Harder Case

$N = 256$ bits

[As in *Ernst et al.*]

$\beta = 0.3$

$d \simeq 77$ bits



Size of d_0		Heuristic A.	Our A.	
δ	Bits	% Indep.	% Indep.	Pb.
0.14	35	100	**100**	0
0.15	38	97	**100**	0
0.16	40	97	**100**	0
0.17	43	82	**100**	1
0.18	46	60	**100**	8
0.182	46	47	**100**	13
0.184	47	47	**100**	13
0.186	47	33	**100**	26
0.188	48	18	**100**	36
0.190	48	16	**100**	50
0.192	49	6	**100**	79
0.194	49	0	**100**	100
0.196	50	0	**100**	100
0.198	50	0	**100**	100
0.20	51	0	**100**	100

Analysis of a bad case

$$p_1 = 9450886190201x + ((z - 155155341747587)y + 7258280594074367 9)$$

$$(x_0 = 233, y_0 = 482, z_0 = 25517171)$$

$$(X = 496, Y = 18080, Z = 37368409)$$

Gröbner basis of $I = (p_1, p_2)$ gives:

$$\begin{cases} q_1 = xz - 39521501447/12x + 46079/6z + 6785552382017/12 \\ q_2 = y - 12/197x - 92158/197 \end{cases}$$

As $q_2(x_0, y_0, z_0) = 0$ then $x_0 \equiv 36 \mod 197$

- We can recover x_0 after 2 tests: 36,233
- Two polynomials sufficient to recover the root

Conclusion-Discussion

Toward a rigorous variation of Coppersmith's algorithm

- No more problems of independence
- Possible generalization for more variables

Future work:

- **In theory:** Conditions on X, Y, Z for the 2^{nd} phase
- More experiments on different shapes, parameters, ...