

# Toward a Rigorous Generalization of Coppersmith's Methods to Find Small Roots of Polynomial Equations

PhD Defense

Aurélie Bauer

University of Versailles Saint-Quentin-en-Yvelines  
PR/SM Laboratory, France

Advisor: Antoine Joux

September 15th, 2008



# Private-Key and Public-Key Cryptography

## Cryptography:



- Secure information over an insecure channel
- Ensure confidentiality, authenticity and data integrity

### Private-Key Cryptography



### Public-Key Cryptography [DH76]



**Cryptanalysis in  
public-key cryptography**

# A Well-Known Public-Key Cryptosystem

## RSA cryptosystem [RSA78]:

- Selection of two large primes  $p$  and  $q$
- Computation of  $N = pq$  and  $\phi(N) = (p - 1)(q - 1)$
- Selection of  $(e, d)$  such that

$$ed \equiv 1 \pmod{\phi(N)}$$

**Bob**

$$p_B = (e, N)$$

$$s_B = d$$

## Encryption/Decryption process

$$\overset{\text{Alice}}{C \equiv m^e \pmod{N}} \longrightarrow \overset{\text{Bob}}{C^d \equiv m \pmod{N}}$$

## Security:

Breaking RSA  $\stackrel{?}{\Leftrightarrow}$  Factoring  $N$

# Restriction to Easier Special Cases

## Most public-key cryptosystems:

- Based on hard mathematical problems
- Easier special cases  $\rightarrow$  cryptanalysis

### Factoring $N = pq$

$$p(x, y) = xy - N \quad \longrightarrow$$

**Bound  $\sqrt{N}$**

### Factoring $N = pq$ with known bits

$$p(x, y) = (\tilde{p} + x)(\tilde{q} + y) - N$$

**Bound  $\sqrt{N}/|\tilde{p}|$**

### Attacking RSA

$$p(x, y, z) = ex - 1 - yz \quad \longrightarrow$$

**Full-size roots**

### Attacking RSA with smaller keys

$$p(x, y, z) = ex - 1 - yz$$

**Smaller roots**

# Finding Small Roots of Polynomial Equations

From  $p_1(x_1, \dots, x_n)$  irreducible over  $\mathbb{Z}[x_1, \dots, x_n]$

**Recover**  $(x_{01}, \dots, x_{0n})$  of  $\mathbb{Z}^n$

• Modular case

$$\begin{cases} p_1(x_{01}, \dots, x_{0n}) \equiv 0 \pmod{N} \\ |x_{01}| < X_1, \dots, |x_{0n}| < X_n \end{cases}$$

• Integer case

$$\begin{cases} p_1(x_{01}, \dots, x_{0n}) = 0 \\ |x_{01}| < X_1, \dots, |x_{0n}| < X_n \end{cases}$$

Rigorous methods

**Modular**  $n = 1$  [Cop96b, HG97]

**Integer**  $n = 2$  [Cop96a, Cor04, Cor07]

**BUT MORE VARIABLES**

Heuristic methods only

## Coppersmith's Method in Two Variables

# Coppersmith's Method in Two Variables

**Example:**  $p_1(x, y) = a + bx + cy$   
 $|x_0| < X, |y_0| < Y$

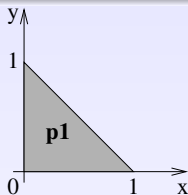


Figure: Shape of  $p_1$

**Goal:** Construct  $p_2$  such that  $p_2(x_0, y_0) = 0$

$$\begin{cases} p_1(x, y) = 0 \\ p_2(x, y) = 0 \end{cases} \Rightarrow \text{Gives } (x_0, y_0) \text{ under technical conditions}$$

**Strategy:** Construction of a polynomial  $p_2$  such that

$$p_2 \notin (p_1) \text{ and } p_2(x_0, y_0) = 0$$

# Coppersmith's Method in Two Variables

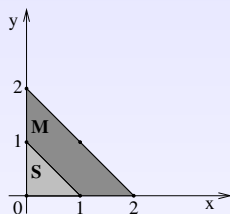


Figure:  $S = \{1, x, y\}$  and  
 $M = \{1, x, y, xy, x^2, y^2\}$

$$p_1(x, y) = a + bx + cy$$

## Geometrical considerations:

- Polynomials  $p_1, xp_1$  and  $yp_1$  in  $M$
- If  $Qp_1$  in  $M$  then  $Q$  defined over  $S$

## Algebraic independence between $p_1$ and $p_2$

If  $p_2$  has its monomials in  $M$

$$p_2 \in (p_1)$$

$\Leftrightarrow$

$p_2$  linear combination  
of  $p_1, xp_1, yp_1$

# Coppersmith's Method in Two Variables

$L_1$  lattice generated by the rows of  $M_1$

$$M_1 = \begin{pmatrix} 1 & 0 & \dots & 0 & p_1 & xp_1 & yp_1 \\ 0 & \frac{1}{X} & & & a & 0 & 0 \\ & & \frac{1}{Y} & & b & a & 0 \\ \vdots & & & \vdots & c & 0 & a \\ & & & \frac{1}{X^2} & 0 & b & 0 \\ & & & & \frac{1}{XY} & 0 & c \\ 0 & \dots & & 0 & 0 & 0 & c \\ & & & \frac{1}{Y^2} & & & \end{pmatrix} \begin{matrix} 1 \\ x \\ y \\ x^2 \\ xy \\ y^2 \end{matrix}$$

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

**$s_0$  short  
vector in  $L_1$**

$$s_0 = (1, \frac{x_0}{X}, \frac{y_0}{Y}, (\frac{x_0}{X})^2, \frac{x_0 y_0}{XY}, (\frac{y_0}{Y})^2, 0, 0, 0)$$

# Coppersmith's Method in Two Variables

$L_1$  lattice generated by the rows of  $N_1$

$$N_1 = \left( \begin{array}{ccc|ccc} \times & \dots & \times & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \vdots & \mathbf{N}_{11} & \vdots & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \times & \dots & \times & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \hline \times & \dots & \times & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \vdots & \mathbf{N}_{12} & \vdots & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \times & \dots & \times & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{array} \right) \left. \vphantom{\begin{array}{ccc|ccc} \times & \dots & \times & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \vdots & \mathbf{N}_{11} & \vdots & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \times & \dots & \times & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \hline \times & \dots & \times & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \vdots & \mathbf{N}_{12} & \vdots & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \times & \dots & \times & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{array}} \right\} L'_1$$

$s_0$  short  
vector in  $L'_1$

$$s_0 = \left( 1, \frac{x_0}{X}, \frac{y_0}{Y}, \left(\frac{x_0}{X}\right)^2, \frac{x_0 y_0}{XY}, \left(\frac{y_0}{Y}\right)^2, \mathbf{0}, \mathbf{0}, \mathbf{0} \right)$$

# Coppersmith's Method in Two Variables

- Vector  $s_0$  in  $L'_1 = (b_1, \dots, b_r)$

$$(s_0 | b_r^*) = 0 \quad \rightarrow \quad p_2(x_0, y_0) = 0$$

- Independence

Every vector  $u \in L'_1$   
such that  
 $u \perp \{V_{p_1}, V_{xp_1}, V_{yp_1}\}$

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**

## Problems when Generalizing with More Variables

# Problem with Three Variables

$$\rho_1(x_0, y_0, z_0) = 0$$
$$|x_0| < X, |y_0| < Y, |z_0| < Z$$

Coppersmith's method  
With  $x, y, z$

$\Rightarrow$

Try to create  $(\rho_2, \rho_3)$

$$\rho_2(x_0, y_0, z_0) = 0$$

$$\rho_3(x_0, y_0, z_0) = 0$$

**PROBLEM:** heuristic method

$\rho_2$  **independent** from  $\rho_1$  }  
and  
 $\rho_3$  **independent** from  $\rho_1$  }

**BUT**  $(\rho_1, \rho_2, \rho_3)$   
not necessarily  
independent

# Algebraic Independence is a Usual Assumption

## Generalizing Coppersmith's methods for more than:

- One variable (modular)
- Two variables (integer)

Enough polynomials  
but  
No **GUARANTEE** of independence

One has to assume the algebraic independence

- Classical assumption [BD00, EJMdW05, SKKO06]
- Assumption satisfied for many applications

Theoretical  
limits:

{ Artificial counter-examples [Cop01, NS01]

**More and more  
Indep. Problems**

$\Rightarrow$   $\left\{ \begin{array}{l} \text{BD's attack with X-shifts only [BM01]} \\ \text{Hinek reports [Hin04, Hin05]} \end{array} \right.$

- Attack on RSA knowing a part of secret key [EJMdW05]

Missing bits	23	25	28	30	33	34	35
Independence (%)	98	92	95	92	80	77	76

- **Unsuccessful** attack on RSA

$$ed = 1 + k \frac{\phi(N)}{2} \quad \text{with} \quad \left\{ \begin{array}{l} A = (N+1)/2 \\ s = -(p+q)/2 \end{array} \right.$$

$\downarrow$

$$ed = 1 + k(A + s)$$

# A real Case where the Heuristic Fails

Two well-known attacks when  $|d| < N^\delta$

Wiener	1990	$\delta < 0.25$	$e/A$ and $k/d$ are very near
Boneh-Durfee	2000	$\delta < 0.292$	Use of $1 + y(A + z) \pmod e$

By mixing  
the methods

$\Rightarrow$

$$d = (xd_0 + yd_1)$$
$$k = (xk_0 + yk_1)$$

Which would imply  $\delta < 0.34$

Interesting result but ...

- 1  $(p_1, p_2, p_3)$  never independent (see also [Suk02])
- 2 Max **23** polynomials (dim **50**), **all are multiples** of  $p_0$

**Heuristic Failure**

# Toward a Rigorous Variation of Coppersmith's Algorithm in Three Variables

# Working with Three Variables over the Integers

$p_1(x, y, z)$  irreducible  
 $(x_0, y_0, z_0)$  root } **Need three independent polynomials**

**First step:** Construction of  $p_2$

Coppersmith's method or variant

$p_1$  and  $p_2$  independent

$$I = (p_1, p_2)$$

**Second step:** Construction of  $p_3(x, y, z)$  such that

- $p_3(x_0, y_0, z_0) = 0$
- Polynomials  $p_1, p_2$  and  $p_3$  algebraically independent

# Notion of Independence

## Definition of independence

$p_1, p_2, p_3$  algebraically independent if

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

### Previous construction

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

$\Rightarrow$

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



**INDEPENDENCE**

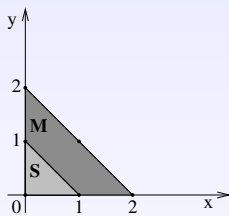
In case  $I = (p_1, p_2)$  is not prime:

- **$I$  primary:** replace it by  $\sqrt{I}$       **Primary Decomposition**
- **$I$  non primary:**  $I = I_1 \cap \dots \cap I_r$   
replace it by  $I_j$  (or  $\sqrt{I_j}$ ) such that  $(x_0, y_0, z_0) \in V(I_j)$

# Translation in Term of Linear Independence

Need relation

**Algebraic indep.  $\Leftrightarrow$  Linear indep.**

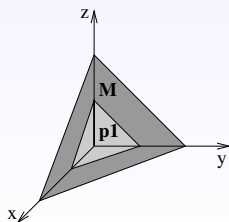


If  $p_2$  has monomials in  $M$

$$p_2 \in (p_1)$$

$\Leftrightarrow$

$p_2$  linear combination  
of  $p_1, xp_1, yp_1$



If  $p_3$  has monomials in  $M$

$$p_3 \in (p_1, p_2)$$

$\Leftrightarrow$

$p_3$  linear combination  
of  $r_1, \dots, r_t$

# Gröbner Basis Computation

Let  $(q_1, \dots, q_r)$  be a Gröbner basis of the ideal  $I$ :

$$p_3 \in (p_1, p_2)$$

$\Leftrightarrow$

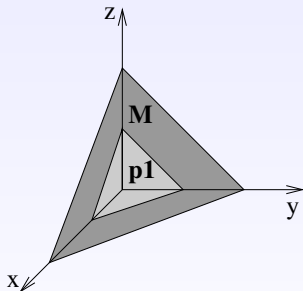
$$p_3 = P_1 q_1 + \dots + P_r q_r$$

Definition domain of the  $P_i$

Polynomials  $r_1, \dots, r_t$

**BUT**

Depend on the shape  $M$



**If  $p_3$  not a linear combination of the  $r_i$ 's**

$\Rightarrow$

**$(p_1, p_2, p_3)$  independent**

# Generalized Coppersmith's Method

$L_I$  lattice generated by the rows of  $M_I$

$$M_I = \left( \begin{array}{cccc|ccc} 1 & 0 & \dots & 0 & r_1 & \dots & r_t \\ 0 & \frac{1}{X} & & & \downarrow & \downarrow & \downarrow \\ & & \frac{1}{Y} & \vdots & & & \\ \vdots & & & \ddots & & & \\ & & & & \frac{1}{YZ} & 0 & \\ 0 & \dots & & 0 & \frac{1}{Z^2} & & \end{array} \right) \begin{array}{l} 1 \\ x \\ y \\ \vdots \\ yZ \\ z^2 \end{array}$$

$$t_0 = \left( 1, \frac{x_0}{X}, \frac{y_0}{Y}, \dots, \frac{y_0 z_0}{YZ}, \left(\frac{z_0}{Z}\right)^2, 0, \dots, 0 \right)$$

$t_0$  short  
vector in  $L'_I$

If  $u \in L'_I$   
 $u \perp \{V_{r_1}, \dots, V_{r_t}\}$

$\Rightarrow (p_1, p_2, p_3)$  independent

- **In general**

{ Conditions **hard** to determine  
Difficulty to evaluate  
the determinant of a sublattice

- **However**

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

# Cryptographic Applications

# Application to a Partial Key Exposure Attack on RSA

- Known part of the secret key [EJMdW05]

$$ed = 1 + k\phi(N)$$
$$d = (\tilde{d} + d_0)$$

$\Rightarrow$

$$p_1(x, y, z) = ex - yN + yz + R$$

with  $R = e\tilde{d} - 1$

## Finding small roots of polynomial equation

- Root  $(x_0, y_0, z_0) = (d_0, k, p + q - 1)$
- Conditions on the bounds  $X, Y$  and  $Z$

**Heuristic  
attack**

$\rightarrow$

$N = 256$  bits  
 $d \simeq 90$  bits  
**100 % Independence**

# Making Rigorous a Heuristic Attack

## Boneh-Durfee's attack on RSA with small private key [BD00]

$$\begin{aligned} ed + k(A + s) &= 1 \\ |d| &< N^\delta \end{aligned}$$

$$\Rightarrow \begin{aligned} f(x, y) &= x(A + y) - 1 \pmod e \\ &\text{Modular root } (k, s) \end{aligned}$$

### Well-chosen lattice

$$\begin{cases} p_1(x, y) \\ p_2(x, y) \end{cases}$$

$\Rightarrow$

Bound on the private key  
 $\delta < 0.292$   
Best bound ever obtained

NO GUARANTEE

Heuristic method

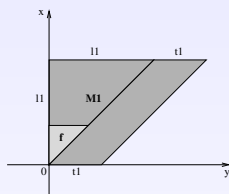
# Making Rigorous a Heuristic Attack (step 1)

Starting from  $p_1(x, y, z) = ez + x(A + y) - 1$

1 **BD's attack:**  $\delta < 0.292$

$$f(x, y) = x(A + y) - 1 \pmod{e}$$

**Bivariate polynomial**  
 $p_2(x, y)$



2 **Properties of  $I = (p_1, p_2)$**

System  $\{p_1, p_2\}$  Gröbner basis

$$\left. \begin{array}{l} \text{in}(p_1) = ez \\ \text{in}(p_2) = \lambda x^a y^b \end{array} \right\} \text{coprime}$$

The ideal  $I$  is prime

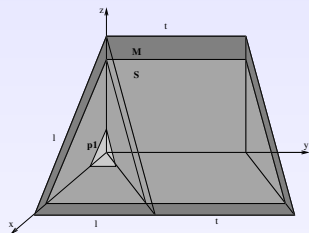
$$\mathbb{Q}[x, y, z]/I \simeq \mathbb{Q}[x, y]/(p_2)$$

$p_2$  irreducible

# Making Rigorous a Heuristic Attack (step 2)

## Construction of $p_3(x, y, z)$

Definition of  
A correct set  $M$



Want to construct  
 $p_3(x, y, z)$

such that

$$p_3 \notin I = (p_1, p_2)$$

Translate into linear independence

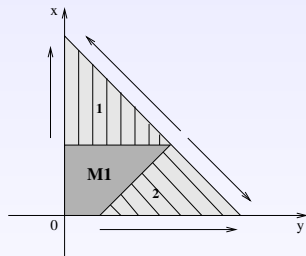
$$p_3 \in I = (p_1, p_2) \Leftrightarrow$$

Linear combination of  
 $r_1, \dots, r_t$

# Making Rigorous a Heuristic Attack (step 3)

System  $\{p_1, p_2\}$   
is a Gröbner basis

$$\Rightarrow \begin{cases} p = Q_1 p_1 + Q_2 p_2 \\ Q_1 \text{ defined over } \mathcal{S} \end{cases}$$



Polynomial  $Q_2(x, y)$   
 $Q_2 p_2 \in M_1$



**Geometrical considerations**  
 $mp_2 \in M_1$

Construction of  $p_3$  under the conditions

No additional  
constraint on  $\delta$



Rigorous method  
for  $\delta < 0.292$

## 1 Contributions of this thesis

- **Counter-example** highlighting heuristic failure
- **Rigorous construction** on three variables
- **Promising applications** of the method

## 2 Future work

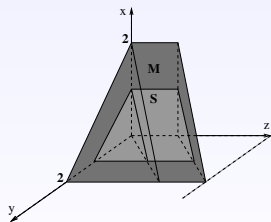
- **Determine** conditions on the bounds  $X$ ,  $Y$  and  $Z$
- **Potential adaptability** for modular equations
- **Improve** Boneh-Durfee's bound on RSA



# Experiments: Easy Case

$$N = 256 \text{ bits}$$

$$d \simeq 90 \text{ bits}$$

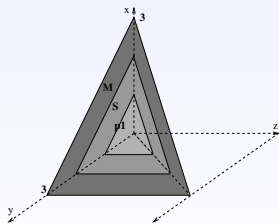


Size of $d_0$	Heuristic A.	Our A.	
Bits	% Indep.	% Indep.	% Pb
23	98	<b>100</b>	0
25	92	<b>100</b>	0
28	95	<b>100</b>	0
30	92	<b>100</b>	0
33	80	<b>100</b>	0
33	86	<b>100</b>	0
34	77	<b>100</b>	0
34	71	<b>100</b>	0
35	76	<b>100</b>	0
35	71	<b>100</b>	0
36	73	<b>100</b>	0
36	55	<b>100</b>	0
37	60	<b>100</b>	0
37	56	<b>100</b>	0
38	47	<b>100</b>	0

# Experiments: Harder Case

$N = 256$  bits

$d \simeq 77$  bits



Size of $d_0$	Heuristic A.	Our A.	
Bits	% Indep.	% Indep.	% Pb.
35	100	<b>100</b>	<b>0</b>
38	97	<b>100</b>	<b>0</b>
40	97	<b>100</b>	<b>0</b>
43	82	<b>100</b>	<b>1</b>
46	60	<b>100</b>	<b>8</b>
46	47	<b>100</b>	<b>13</b>
47	47	<b>100</b>	<b>13</b>
47	33	<b>100</b>	<b>26</b>
48	18	<b>100</b>	<b>36</b>
48	16	<b>100</b>	<b>50</b>
49	6	<b>100</b>	<b>79</b>
49	0	<b>100</b>	<b>100</b>
50	0	<b>100</b>	<b>100</b>
50	0	<b>100</b>	<b>100</b>
51	0	<b>100</b>	<b>100</b>

# Analysis of a Bad Case

$$p_1 = 9450886190201x + ((z - 155155341747587)y + 72582805940743679)$$
$$(x_0 = 233, y_0 = 482, z_0 = 25517171)$$
$$(X = 496, Y = 18080, Z = 37368409)$$

**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  $x_0 \equiv 36 \pmod{197}$

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

## When $(M, <)$ compatible

### Truncated Gröbner basis related to $M$

$G_M = \{q_{i_1}, \dots, q_{i_l}\}$  such that for all  $j \in \{1, \dots, l\}$ ,  $q_{i_j} \in M$

### Construction of $\mathcal{F} = \{r_1, \dots, r_t\}$

- Multiply each  $q_{i_j}$  by monomials: product remains in  $M$
- If  $p \in I$  and defined over  $M$ , then  $p = \sum_{i=1}^t \lambda_i r_i$ ,  $\lambda_i \in \mathbb{Z}$ .
- Complexity:  $O(rm^2)$

**Otherwise** theoretic construction more difficult

Can still be done in practice.

# A criterion that guarantees rigorous success

Shape of the set  $\mathcal{F}$


Assume  $\mathcal{F} = \{\{x^i y^j z^k p_1\}_{(i,j,k) \in S}, p_2\}$

When the pair  $(M, <)$  compatible: Link with Gröbner basis

$$G_M = \{p_1, p_2\} \\ + \\ \text{no multiples of } p_2 \in M$$

When  $G_M = \{p_1, p_2\}$ , high probability  $p_2$  on the boundary

If the first criterion is satisfied, then the second is too.

-  D. Boneh and G. Durfee.  
Cryptanalysis of RSA with Private Key Less Than  $N^{0.292}$ .  
*IEEE Transactions on Information Theory*, 46:1339–1349,  
July 2000.
-  J. Blömer and A. May.  
Low Secret Exponent RSA Revisited.  
In *CaLC '01: Revised Papers from the International  
Conference on Cryptography and Lattices*, pages 4–19,  
London, UK, 2001. Springer-Verlag.
-  D. Coppersmith.  
Finding a Small Root of a Bivariate Integer Equation;  
Factoring with high bits known.  
In *Advances in Cryptology-Eurocrypt '96, Lecture Notes in  
Computer Science*, volume 1070, pages 178–189.  
Springer-Verlag, 1996.



D. Coppersmith.

Finding a Small Root of a Univariate Modular Equation.

In *Advances in Cryptology-Eurocrypt '96, Lecture Notes in Computer Science*, volume 1070, pages 155–165. Springer Verlag, 1996.



D. Coppersmith.

Finding Small Solutions to Small Degree Polynomials.

In *Cryptography and Lattice Conference, Lecture Notes in Computer Science*, volume 2146. Springer-Verlag, 2001.



J.-S. Coron.

Finding Small Roots of Bivariate Integer Polynomial Equations Revisited.

In *Advances in Cryptology-Eurocrypt '04, Lecture Notes in Computer Science*, pages 492–505. Springer-Verlag, 2004.



J.-S. Coron.

Finding Small Roots of Bivariate Integer Polynomial Equations: A Direct Approach.

*In Advances in Cryptology-Crypto '07, Lecture Notes in Computer Science*, pages 379–394. Springer-Verlag, 2007.



W. Diffie and M. Hellman.

New Directions in Cryptography.

*IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.



M. Ernst, E. Jochemsz, A. May, and B. de Weger.

Partial Key Exposure Attacks on RSA up to Full Size Exponents.

*In Advances in Cryptology-Eurocrypt '05, Lecture Notes in Computer Science*, volume 3494, pages 371–386. Springer-Verlag, 2005.



N. Howgrave-Graham.

Finding Small Roots of Univariate Modular Equations Revisited.

*In Proceedings of the 6th IMA International Conference on Cryptography and Coding*, pages 131–142, London, UK, 1997. Springer-Verlag.



M. J. Hinek.

New partial key exposure attacks on RSA revisited.

Technical report, CACR, Centre for Applied Cryptographic Research, University of Waterloo, 2004.



M. J. Hinek.

Small Private Exponent Partial Key-Exposure Attacks on Multiprime RSA.

Technical report, CACR, Centre for Applied Cryptographic Research, University of Waterloo, 2005.



P. Nguyen and J. Stern.

The Two Faces of Lattices in Cryptology.

*In CaLC '01: Revised Papers from the International Conference on Cryptography and Lattices, 2001.*



R.L. Rivest, A. Shamir, and L.M. Adleman.

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.

*Communications of the ACM, 21(2):120–126, 1978.*



B. Santoso, N. Kunihiro, N. Kanayama, and K. Ohta.

Factorization of Square-Free Integers with High Bits Known.

*In Advances in Cryptology-Vietcrypt '06, Lecture Notes in Computer Science. Springer-Verlag, 2006.*



A.H. Suk.

Cryptanalysis of RSA with Lattice Attacks .

Master's thesis, University of Illinois at Urbana-Champaign,  
2002.