Reduction in Lossiness of RSA Trapdoor Permutation

Santanu Sarkar

Chennai, India 3 November, 2012

Presented by: Subhadeep Banik

Φ-Hiding Assumption

- Φ-Hiding Assumption: For an RSA modulus $N = pq$ and a prime e,

  "it is hard to decide whether e divides
  $$\Phi(N) = (p-1)(q-1),"$$

- Φ-Hiding problem can be solved efficiently using the idea of Coppersmith if $e \geq N^{0.25}$

Multi-Prime Φ-Hiding Assumption

- Multi-Prime RSA: $N = p_1 \cdots p_m$, with p_i (for $1 \leq i \leq m$) primes of same bitsize.
- Multi-Prime Φ-Hiding Assumption has been proposed by Kiltz et al in Crypto 2010
- Considered Multi-Prime RSA with modulus $N = p_1 \cdots p_m$. The prime e is chosen such that e divides $p_1 - 1, \ldots, p_{m-1} - 1$.
- Multi-Prime Φ-Hiding Assumption, which states that

  "it is hard to decide whether e divides $p_i - 1$ for all but one prime factor of N".

Cryptanalysis of Multi-Prime Φ-Hiding Assumption

- Kiltz et al. present a cryptanalysis of the Multi-Prime Φ-Hiding Assumption using the idea of Herrmann et al. (Asiacrypt 2008)
- Note that if e divides all $p_i - 1$ for $1 \leq i \leq m$, $N \equiv 1 \bmod e$.
- It gives a polynomial time distinguisher.
- To decide if e is Multi-Prime Φ-Hidden in N, consider the system of equations $ex_1 + 1 \equiv 0 \bmod p_1, ex_2 + 1 \equiv 0 \bmod p_2, \ldots, ex_{m-1} + 1 \equiv 0 \bmod p_{m-1}$.

Idea of Kiltz et al

- Kiltz et al. construct a polynomial equation

$$e^{m-1}\left(\prod_{i=1}^{m-1} x_i\right) + \cdots + e\left(\sum_{i=1}^{m-1} x_i\right) + 1 \equiv 0 \bmod \prod_{i=1}^{m-1} p_i$$

  by multiplying all given equations.

- Then they linearize the polynomial and solve it using a result due to Herrmann and May.

- However, the work of Herrmann and May provides an algorithm with runtime exponential in the number of unknown variables.

- So for large m, the idea will not be efficient.

Idea of Herrmann

- In Africacrypt 2011, Herrmann improved the attack of Kiltz et al.
- Suppose we have $(ex_1+1)(ex_2+1)(ex_3+1) \equiv 0 \bmod p_1p_2p_3$.
- Instead of considering the polynomial equation

  $e^3x_1x_2x_3+e^2(x_1x_2+x_1x_3+x_2x_3)+e(x_1+x_2+x_3)+1 \equiv 0 \bmod p_1p_2p_3$,

  Herrmann considered the polynomial equation

  $$e^2x + ey + 1 \equiv 0 \bmod p_1p_2p_3,$$

  where $x = ex_1x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3$ and $y = x_1 + x_2 + x_3$ are the unknowns.
- One positive side is that it has only two variables x, y instead of the original three x_1, x_2, x_3.
- On the negative side, the size of the variable x is increased by a factor of e compared to the original unknown variables x_1, x_2, x_3.

Idea of Herrmann

In the general case, instead of considering the polynomial $e^{m-1}y_{m-1} + e^{m-2}y_{m-2} + \cdots + ey_1 + 1$ over the variables $y_1, \ldots, y_{m-1}$ with root

$$(y_1, \ldots, y_{m-1}) = \left(\prod_{i=1}^{m-1} x_i, \ldots, \sum_{i=1}^{m-1} x_i \right),$$

Herrmann considered the polynomial $e^2x + ey + 1$ over the variables x, y with root

$$(x_0, y_0) = \left(e^{m-3} \prod_{i=1}^{m-1} x_i + \cdots + \sum_{j>i} x_i x_j, \sum_{i=1}^{m-1} x_i \right)$$

to obtain the improvement over the work of Kiltz et al.

Our Idea

- The variable y_0 is much smaller than x_0.
- Herrmann already mentioned that one may get better bound for these unbalanced variables.
- However this option has not been analyzed systematically in the literature till date.
- In this work we analyzed this issue carefully.

Reduction of Lossiness

In the following Table, we present the impact of our result on the work of Kiltz et al.

Value of m	Lossiness in the work of Kiltz et al.		
	Before the work of Herrmann	After the work of Herrmann	After our work
4	806	778	768
5	872	822	778

Table: Impact of our results on the lossiness of Kiltz et al. for different values of m, with 2048 bit N and for 80 bit security.

Howgrave-Graham: 1997

Lemma

Let $h(x_1, x_2) \in \mathbb{Z}[x_1, x_2]$ *be the sum of at most* ω *monomials. Suppose that* $h(x_1^{(0)}, x_2^{(0)}) \equiv 0 \pmod{N^m}$ *where* $|x_1^{(0)}| \leq X_1, |x_2^{(0)}| \leq X_2$ *and*

$$||h(x_1 X_1, x_2 X_2)|| < \frac{N^m}{\sqrt{\omega}}.$$

Then $h(x_1^{(0)}, x_2^{(0)}) = 0$ *over the integers.*

Lenstra, Lenstra and L. Lovász: 1982

Lemma

Let L be an integer lattice of dimension ω. The LLL algorithm applied to L outputs a reduced basis of L spanned by $\{v_1, \ldots, v_\omega\}$ with

$$||v_1|| \leq ||v_2|| \leq 2^{\omega/4} \det(L)^{1/(\omega-1)}$$

in polynomial time of dimension ω and the bit size of the entries of L.

Our Result

Our approach is exactly the same as Herrmann except that we use extra shifts over the variable y.

Theorem

Let $N = p_1 \cdots p_m$ be a Multi-Prime RSA modulus where p_i are of same bit size for $1 \leq i \leq m$. Let e be a prime such that $e > N^{\frac{1}{m}-\delta}$. Then one can solve Multi-Prime hidden Φ problem in polynomial time if there exist two non-negative real numbers τ_1, τ_2 such that

$$\begin{aligned}\Psi(\tau_1, \tau_2, \delta, m) =& 3\tau_1\tau_2^2 m - \tau_2^3 m + 3\tau_1^2\delta m - 6\tau_1\tau_2 m + 3\tau_2^2 m + 9\tau_1\delta m + \\ & 6\tau_1\tau_2 + 3\tau_1 m - 3\tau_2 m + 3\delta m - 9\tau_1 + 3\tau_2 + m - 3 < 0.\end{aligned}$$

Idea of the proof

- To decide if e is Multi-Prime Φ-hidden in N, consider the system of equations

$$ex_1 + 1 \equiv 0 \bmod p_1, \dots, ex_{m-1} + 1 \equiv 0 \bmod p_{m-1}$$

- Now consider the polynomial $g(x, y) = e^2x + ey + 1$.
- It is clear that $g(x_0, y_0) \equiv 0 \bmod P$ where

$$(x_0, y_0) = \left(e^{m-3} \prod_{i=1}^{m-1} x_i + \cdots + \sum_{j>i} x_i x_j, \sum_{i=1}^{m-1} x_i \right).$$

- From $g(x, y)$, one can obtain a polynomial $f(x, y)$ of the form $x + a_1 y + a_2$ such that $f(x_0, y_0) \equiv 0 \bmod P$.
- Take two integers $X = N^{\frac{m-3}{m}+2\delta}$ and $Y = N^{\delta}$.
- It can be shown that X, Y is an upper bound on x_0, y_0 respectively.

Idea of the proof

- Now consider the set of polynomials

$$g_{k,i}(x, y) = y^i f^k(x, y) N^{\max\{s-k,0\}},$$

for $k = 0, \ldots, u$, $i = 0, \ldots, u - k + t$ where u is a positive integer and s, t are non-negative integers.

- Note that $g_{k,i}(x_0, y_0) \equiv 0 \bmod P^s$, where $P = \prod_{i=1}^{m-1} p_i$
- Now we construct the lattice L spanned by the coefficient vectors of the polynomials $g_{k,i}(xX, yY)$.

Idea of the proof

- One can check that the dimension of the lattice L is
$$\omega = \sum_{k=0}^{u} \sum_{i=0}^{u-k+t} 1 \approx \frac{u^2}{2} + tu.$$

- The determinant of L is
$$det(L) = \prod_{k=0}^{u} \prod_{i=0}^{u-k+t} X^k \cdot Y^i \cdot N^{\max\{s-k,0\}} = X^{s_X} Y^{s_Y} N^{s_N}, \quad (1)$$

$$\begin{aligned} \text{where} \quad s_X &= \sum_{k=0}^{u} \sum_{i=0}^{u-k+t} k \approx t\frac{u^2}{2} + \frac{u^3}{6}, \\ s_Y &= \sum_{k=0}^{u} \sum_{i=0}^{u-k+t} i \approx \frac{t^2 u}{2} + \frac{tu^2}{2} + \frac{u^3}{6}, \\ s_N &= \sum_{k=0}^{u} \sum_{i=0}^{u-k+t} \max\{s-k,0\} \approx \frac{us^2}{2} + \frac{ts^2}{2} - \frac{s^3}{6} \end{aligned}$$

Idea of the proof

- Using Lattice reduction on L by LLL algorithm, one can find two non-zero vectors b_1, b_2 such that $||b_1|| \leq ||b_2|| \leq 2^{\frac{\omega}{4}}(det(L))^{\frac{1}{\omega-1}}$.
- The vectors b_1, b_2 are the coefficient vector of the polynomials $h_1(xX, yY), h_2(xX, yY)$ with

$$||h_1(xX, yY)|| = ||b_1|| \qquad \text{and} \qquad ||h_2(xX, yY)|| = ||b_2||,$$

  where $h_1(x, y), h_2(x, y)$ are the integer linear combinations of the polynomials $g_{k,i}(x, y)$.
- Hence $h_1(x_0, y_0) \equiv h_2(x_0, y_0) \equiv 0 \bmod P^s$.

Idea of the proof

- To find two polynomials $h_1(x, y), h_2(x, y)$ which share the root (x_0, y_0) over integers, using previous Lemmas we get the condition
$$2^{\frac{\omega}{4}}(det(L))^{\frac{1}{\omega-1}} < \frac{P^s}{\sqrt{\omega}}.$$
- Note that ω is the dimension of the lattice which we may consider as small constant with respect to the size of P and the elements of L.
- Thus, neglecting $2^{\frac{\omega}{4}}$ and $\sqrt{\omega}$, we get $det(L) < (P^s)^{\omega-1}$.

Idea of the proof

- In general, it is considered that the condition $det(L) < (P^s)^\omega$ is sufficient to find two polynomials $h_1(x, y), h_2(x, y)$ such that $h_1(x_0, y_0) = h_2(x_0, y_0) = 0$.
- Under the assumption that $\gcd(h_1, h_2) = 1$, we can collect the root (x_0, y_0) using resultant method.
- Let $t = \tau_1 u$ and $s = \tau_2 u$ where τ_1, τ_2 are non-negative reals.
- Now putting the value of t, s in the condition $det(L) < P^{s\omega}$, we get the required condition.

Comparison of our upper bounds of δ with Kiltz et al. and Herrmann

Value of m	Upper bound on δ		
	Our result	Herrmann	Kiltz et al.
3	0.1283	0.1283	0.1283
4	0.0835	0.0833	0.0787
5	0.0608	0.0596	0.0535
6	0.0475	0.0454	0.0388
7	0.0387	0.0360	0.0295
8	0.0327	0.0295	0.0232
9	0.0283	0.0247	0.0188
10	0.0248	0.0211	0.0154

Table: Comparison of upper bound on δ between our result and those of Herrmann and Kiltz et al.

Comparison with Tosu and Kunihiro

- Tosu and Kunihiro (ACISP 2012) have studied Multi-Prime Φ-Hiding Problem.
- They have mentioned that their bound is same as Herrmann Method for $m = 3, 4, 5$.
- Hence for $m = 4, 5$, our method is better.
- Also for larger m, our method is better.
- For an example take $m = 10$ with 4096 bit modulus.
- Attack of Tosu and Kunihiro works when size of e is more than 314.
- However, in our case lower bound on size of e is $(0.1 - 0.0248) \times 4096 = 308$.

Acknowledgments

Heartiest thanks to Subhadeep Banik for delivering this talk.
Thanks a lot to the PC-Chairs for allowing this presentation.

THANK YOU

FOR YOUR KIND ATTENTION

Questions/comments
are most welcome at
sarkar.santanu.bir@gmail.com