CR10: Cryptanalysis Autumn 2018

Lecture 7 — November, 5^{th} 2018

Lecturers ***G. Hanrot****, E. Kirshanova* *Scribe: P. Meyer*

0 Coppersmith method – univariate case: RSA with random padding

Because it is a deterministic public-key encryption scheme, the vanilla-RSA algorithm function is not a secure cryptosystem. Indeed, if the attacker can guess the original message (for instance if the plaintext space is relatively small) and check his own generated cypertext against the one he intercepted. Randomness can be introduced by using *random padding*. This is not secure however, as we describe here an efficient attack using the Coppersmith method.

0.1 The setting

Suppose we want to encrypt a message M. The cyphertext to be computed is $(M+r)^e \pmod N$ where e is the secret key, N is a public encryption parameter, and r is a 'small' random padding.

Suppose now that we encrypt and send the message twice. The attacker therefore holds two cyphertexts $c_1 = (M+r_1)^e \pmod N$ and $c_2 = (M+r_2)^e \pmod N$, and his goal is to retrieve M.

0.2 The attack

Define $Y := r_1 - r_2$ and $X := M + r_1$. The system becomes:

$$\begin{cases} c_1 = X^e \pmod N \\ c_2 = (X-Y)^e \pmod N \end{cases} \tag{1}$$

Now introduce[1] the two polynomials $P_1, P_2 \in \mathbb{K}(Y)[X]$ (say for instance $\mathbb{K} := \mathbb{Q}$), defined by:

$$\begin{cases} P_1(X,Y) = X^e - c_1 \\ P_2(X,Y) = (X-Y)^e - c_2 \end{cases} \tag{2}$$

By Bezout's theorem, there exist $Q_1, Q_2 \in \mathbb{K}(Y)[X]$ such that $Q_1P_1 + Q_2P_2 = 1$. We can assume that $\deg_X(Q_1) \leq \deg_X P_2 = e$ and $\deg_X Q_2 \leq \deg_X P_1 = e$. Indeed, since the pair (Q_1, Q_2) is such that $Q_1P_1 + Q_2P_2 = 1$, so is the pair $(Q_1', Q_2') := (Q_1 + P_2 \cdot (Q_2 \text{ quo } P_1), Q_2 - P_1 \cdot (Q_2 \text{ quo } P_1)))$. We have $\deg_X Q_2' \leq \deg_X P_1 = e$.

It then follows from '$Q_1'P_1 + Q_2'P_2 = 1$' that $\deg_X(Q_1') = \deg_X(Q_1'P_1) - \deg_X(P_1) = \deg_X(Q_2'P_2 - 1) - \deg_X(P_1) \leq \deg_X(Q_2'P_2) - \deg_X(P_1) = \deg_X(Q_2') + \deg_X(P_2) - \deg_X(P_2) = \deg_X(Q_2') \leq e$.

[1] The introduction of these polynomials is motivated by elimination theory (cf. transforming two equations with two variables into one equation with one variable).

Clearing denominators, there exist $R \in \mathbb{K}[Y]$ and $\widetilde{Q}_1, \widetilde{Q}_2 \in \mathbb{K}[X,Y]$ such that $Q_1 = \frac{\widetilde{Q}_1}{R}$ and $Q_2 = \frac{\widetilde{Q}_2}{R}$. Note that $\widetilde{Q}_1 P_1 + \widetilde{Q}_2 P_2 = R$. It follows that if (x_0, y_0) is a common root of P_1 and P_2 then $R(y_0) = 0$. .

Now, write $Q_1 P_1 + Q_2 P_2 = 1$ as a linear system of equations over $\mathbb{K}[Y]$, with unknowns $q_{1,0}, \ldots, q_{1,e-1}$ and $q_{2,0}, \ldots, q_{2,e-1}$ in $\mathbb{K}(Y)$. The matrix of the system is the Sylvester Matrix[2] $Syl(P_1, P_2)$ (P_1 and P_2 are seen as polynomials in X with polynomials in Y as coefficients):

$$Syl(P_1,P_2) = \left(\begin{array}{cccc|cccc} -c_1 & & & & (-Y)^e - c_2 & & & \\ & -c_1 & & & \binom{e}{e-1}(-Y)^{e-1} & (-Y)^e - c_2 & & \\ & & \cdots & & \cdots & & \cdots & \\ & & & -c_1 & & \cdots & & (-Y)^e - c_2 \\ 1 & & & & 1 & & & \\ & 1 & & & & 1 & & \cdots \\ & & \cdots & & & & \cdots & \\ & & & 1 & & & & 1 \end{array}\right)$$

The first $(e-1)$ columns correspond to the coefficients of P_1, appropriately translated.
The last $(e-1)$ columns correspond to the coefficients of P_2, appropriately translated.
Note that the coefficients not covered by the scope of a '...' are all nil.

By Cramer's formula, R can be taken to be the Sylvester determinant $\det(Syl(P_1, P_2))$, which is a degree e^2 polynomial. Hence $\deg(R) \leq e^2$.

Using the Coppersmith method yields either a factor of N or a solution of $R(y) = 0$ with $|y| \leq N^{1/e^2}$. In the latter case, we can try to deduce $(M + r_1)$ from this y since $(X^e - c_1)$ and $[(X - y)^e - c_2]$ have a common factor; if the latter has degree one it must be $[X - (M + r_1)]$, and we hope that Euclid's algorithm will find it (we are over a non-integral ring where we have no guarantee that Euclid's algorithm will work).

[2] We use here the convention of 'translating columns', not that of 'translating lines' - both define the same matrix up to transposition.

1 Coppersmith method – bivariate case

1.1 General description

The problem is to find a non-trivial solution to the system $\begin{cases} P(x,y) = 0 \\ |x| \leq X \\ |y| \leq Y \end{cases}$

The strategy is the same:

- look for an auxiliary polynomial Q such that $P(x,y) = 0 \pmod N \Rightarrow Q(x,y) = 0 \pmod{N^l}$ for some fixed parameter l. Natural candidates for Q include the $X^i P^k N^{l-k}$ and the $Y^j P^k N^{l-k}$;
- look for *two* linear combinations R_1 and R_2 of these candidate polynomials such that the coefficients of $R_i(xX, yY)$ are at most N^l so that $|R_i(x,y)| < N^l$ for $|x| < X$ and $|y| < Y$.

If this is the case, from $R_i(x,y) < N^l$ and $R_i(x,y) = 0 \bmod N^l$, we deduce that $R_i(x,y) = 0$ for $i = 1, 2$. Our hope is that $R_1(x,y)$ and $R_2(x,y)$ are such that the resultant $Res(R_1, R_2) := det(Syl(R_1, R_2))$ is non-zero. If this is the case we can solve the equation $Res(R_1, R_2)(y) = 0$ for y-candidates, and for each of those y recover x from $R_i(x,y) = 0$.

Note however that this strategy will not always work. Indeed if $P(x,y) = xy - N$ then finding a solution to the system $\begin{cases} P(x,y) = 0 \\ |x|, |y| \leq N^{\frac{1}{2}+\epsilon} \end{cases}$ is as hard as factoring N, which is (presumed) computationally hard in general (and indeed Coppersmith's method yields zero resultants in this case).

1.1.1 RSA with small d

A few words on Wiener's attack Suppose that $de = 1 \pmod{(p-1)(q-1)}$, ie. that $de = 1 + k * (p-1)(q-1)$ for some $k \in \mathbb{N}$.

It follows that: $\begin{array}{ccc} \frac{e}{(p-1)(q-1)} & = & \frac{1}{k(p-1)(q-1)} + \frac{k}{d} \\ \approx e/N & & \approx 1/(dN) + k/d \end{array}$

Hence, if d is small, then $\frac{k}{d}$ is a fraction with both small numerator and small denominator, and which is a good approximation of $\frac{e}{N}$. More precisely, for $d \leq \sqrt[4]{N}$, the pair (k, d) appears during the run of the extended euclidean algorithm on (e, N) as coefficients of an 'intermediate Bezout relation'[3].

Boneh-Durfee attack

Claim 1 (Boneh-Durfee attack)**.** *Heuristically, we can recover d as long as $|d| \leq N^{1-\sqrt{2}} \approx N^{0.292}$.*

[3] This is closely related to continuous fractions.

Claim 2 (Weaker version)**.** *Heuristically, we can recover d as long as $|d| \leq N^{(7-2\sqrt{7})/6} \approx N^{0.2847}$.*

For simplicity however, we will not prove [Claim 1] but [Claim 2].[4]

Suppose that $ed + k(p-1)(q-1) = 1$, ie. $ed + k(N+1-p-q) - 1 = 0$. It follows that $X[(N+1) - Y] - 1 = 0 \pmod{e}$, where $X := k \leq e^{\delta}$ (this defines $\delta \in [0,1]$) and $Y := (p+q)$ is of the order of $\sqrt{e}$.

Fix an l, which we will explicitly choose later, and consider the families of polynomials $(g_{i,k})_{i,k}$ and $(h_{j,k})_{j,k}$ defined (for some t, to be defined later) by:

$$\forall k \in [\![0; l]\!], \forall i \in [\![0; l-k]\!], g_{i,k} = e^{l-k} x^i P^k$$

and

$$\forall k \in [\![0; l]\!], \forall j \in [\![1; t]\!], h_{j,k} = e^{l-k} y^j P^k$$

The lattice L built on those polynomials has dimension:

$$dim = \frac{(l+1)(l+2)}{2} + t(l+1)$$

Let us now consider the coefficient matrix of $\begin{cases} g_{i,k}(xX, yY) \\ h_{j,k}(xX, yY) \end{cases}$ for $t = 1$ and $l = 3$ for instance.

	1	x	xy	x^2	x^2y	x^2y^2	x^3	x^3y	x^3y^2	x^3y^3	y	xy^2	x^2y^3	x^3y^4
e^3	e^3													
xe^3		Xe^3												
Pe^2			XYe^2											
x^2e^3				X^2e^3										
xPe^2					X^2Ye^2					**(don't care)**				
P^2e						X^2Y^2e								
x^3e^3							X^3e^3							
x^2Pe^2								X^3Ye^2						
xP^2e									X^3Y^2e					
P^3					**(0)**					X^3Y^3				
ye^3											Ye^3			
yPe^2												XY^2e^2		
yP^2e													X^2Y^3e	
yP^3														X^3Y^4

$$\begin{aligned} det &= e^{\left(\sum_{k=0}^{l}\sum_{l=0}^{k}(l-j)+t\sum_{j=0}^{l} j\right)} X^{\left(\sum_{k=0}^{l}\sum_{l=0}^{k}(l-j)+t\sum_{j=0}^{l} j\right)} Y^{\left(\sum_{k=0}^{l}\sum_{l=0}^{k} j+\sum_{i=1}^{t}\sum_{j=0}^{l}(i+k)\right)} \\ &= e^{l(l+1)\frac{l+2}{3}} X^{l(l+1)\left(\frac{l+2}{3}+\frac{t}{2}\right)} Y^{\left(\frac{l(l+1)(l+2)}{6}+\frac{(l+1)t(t+l+1)}{2}\right)} \end{aligned}$$

If $X = e^{\delta}$ and $Y = \sqrt{e}$ we get:

$$det = e^{\left(l(l+1)\left(\frac{l+2}{3}+\frac{t}{2}\right)(1+\delta)+\frac{l(l+1)(l+2)}{12}+t\frac{(l+1)(l+t+1)}{4}\right)}$$

[4]We derive this $\frac{7-2\sqrt{7}}{6}$ exponent bound from the determinant of a certain lattice L -defined hereafter- which is an upper bound on the length of a shortest vector of the lattice. In order to get the improved $1-\sqrt{2}$ bound, we can choose a certain sublattice L' of L whose determinant yields an improved bound on the length of its shortest vectors. However, bounding the determinant of a non-full rank lattice is not a pleasant task...

Assuming $t \approx l$ (we will have to check this condition is satisfied once we set t and l), we have:

$$\begin{aligned} det &= e^{\left(l^2(\frac{l}{3}+\frac{t}{2})(1+\delta)+\frac{l^3}{12}+\frac{tl(l+t)}{4}+\mathcal{O}(l^2)\right)} \\ &= e^{\left(\frac{4\delta+5}{16}l^3+\frac{2\delta+3}{4}l^2t+\frac{t^2l}{4}+\mathcal{O}(l^2)\right)} \end{aligned}$$

As in the univariate case, a vector of the lattice corresponds to the coefficient vector of a polynomial $R(xX, yY)$ such that $R(x, y) = 0 \bmod e^\ell$ whenever $x((N+1)-y)-1 = 0 \bmod e$. If, further, $|R(xX, yY)| < e^\ell$ for $|x|, |y| < 1$, we must have $R(x, y) = 0$. But a sufficient condition for $|R(xX, yY)| < e^\ell$ for $|x|, |y| < 1$ is that the coefficients of $R(xX, yY)$ are $< e^\ell$, up to a polynomial factor in ℓ.

For such a vector to exist in our lattice, we want $det < e^{l \cdot dim} = e^{l^3/2+tl^2+\mathcal{O}(l^2)}$.

In order to simplify the calculations, we ignore the terms of lower order in the exponent(ie. in $\mathcal{O}(l^2)$), as this does not change much.

With the simplification, the inequality becomes:

$$\frac{4\delta+5}{12}l^2 + \frac{2\delta+3}{4}tl + \frac{t^2}{4} < \frac{l^2}{2} + tl$$

$$\text{ie. } \left(\frac{4\delta-1}{12}\right)l^2 + \left(\frac{2\delta-1}{4}\right)tl + \frac{t^2}{4} < 0$$

This is true if and only if the discriminant of the left-hand side seen as a quadratic polynomial in t is non-negative, ie. $\delta^2 - \frac{7}{3}\delta + \frac{7}{12} > 0$ ie. $\delta < \frac{7-2\sqrt{7}}{6} \approx 0.2847$ (as $\delta > 1$ is non-sensical). Note that forgoing the simplification instead leads to $\delta < \frac{7}{6} - \frac{\sqrt{7+16/l+4/l^2}}{3} + \frac{5}{6l} \underset{l\to\infty}{\to} \frac{7-2\sqrt{7}}{6}$.

1.2 SiS[5] vs Lattice-based reduction

1.2.1 SiS problem

Let n, m, q, and b be positive integers such that $m >> n$.

The $SIS_{n,m,q,b}$ problem is defined as follows:

$$\begin{aligned} &\texttt{Input: } A \in (\mathbb{Z}/q\mathbb{Z})^{n\times m} \text{ chosen uniformly at random} \\ &\texttt{Output: } e \in \mathbb{Z}^m \text{ such that } \begin{cases} Ae = 0 \pmod q \\ \|e\|_\infty \leq b \\ e \neq 0 \pmod q \text{ [in order to avoid 'trivial' outputs']} \end{cases} \end{aligned}$$

We define the hash function $SWIFFT$ for a given matrix $A \in (\mathbb{Z}/q\mathbb{Z})^{n\times m}$ to be:

$$h : X \in \{0,1\}^m \mapsto AX, \text{ for some } m \text{ such that } m >> n(log\ q)$$

[5] **S**mall **I**nteger **S**olutions

Note that finding a collision for h is exactly finding $X_1, X_2 \in \{0,1\}^m$ such that $AX_1 = AX_2$, ie. $X_1 - X_2$ is a SIS solution with $b = 1$.

1.2.2 Attacking SiS with lattice-based reduction

Lemma 3. *Let $A \in (\mathbb{Z}/q\mathbb{Z})^{n\times m}$. If q is prime and A has rank n (which is true with probability exponentially close to 1 if A is sampled uniformly), then $A_q^\perp := \{x \in \mathbb{Z}^n : Ax = 0 \pmod q\}$ is a lattice of $\mathbb{R}^m$ with dimension n and determinant q^n.*

Proof.

- $\mathbb{Z}^m \supseteq A_q^\perp \supseteq q\mathbb{Z}^m$ so $dim(A_q^\perp) = m$

- Define $\phi : \begin{array}{ccc} \mathbb{Z}^m & \to & (\mathbb{Z}/q\mathbb{Z})^n \\ x & \mapsto & Ax \end{array}$. $Ker(\phi) = A_q^\perp$ so $\mathbb{Z}^m/A_q^\perp \cong (\mathbb{Z}/q\mathbb{Z})^n$. This means that $[\mathbb{Z}^m : A_q^\perp] = q^n$ which implies that $vol(A_q^\perp) = q^n vol(\mathbb{Z}^m) = q^n$.

□

By attacking with BKZ_β, we may obtain an $e \in A_q^\perp \backslash \{0\}$ such that $\|e\|_2 \leq \beta^{m/\beta} q^{n/m}$. Note that we have some degree of freedom on m: we can decrease m by setting some unknowns to 0. The optimal value of m minimises $\frac{m}{\beta}\log(\beta) + \frac{n\cdot\log(q)}{m}$, ie. $\sqrt{\frac{n\beta\log(q)}{\log(\beta)}}$ yields an e such that $\|e\|_2 < 2^{2\sqrt{\log(\beta)\cdot n\cdot\log(q)/\beta}}$. This means that for b larger than this upper bound (for a fixed value of β), the SIS problem can be solved in polynomial time by lattice basis reduction.