Cryptography and Electrostatics

Ted Chinburg, Brett Hemenway, Nadia Heninger, and Zachary Scherr

March 29, 2017
Motivation: RSA encryption

**Goal:** Tell your friend how to send you a message that everyone can hear, but that only you can readily decode.

**The RSA method:**
1. You choose an integer $d > 2$ and large random primes $p \neq q$ such that $\gcd(d, (p - 1)(q - 1)) = 1$.
2. You calculate $N = pq$. You then broadcast $N$ and $d$, but not $p$ and $q$.

**Encryption:**
1. Your friend wishes to send you the message $m \mod N$, with $m$ relatively prime to $N$.
2. They calculate $c = m^d \mod N$ and broadcast an integer $c$ in $[0, N - 1]$ in this residue class.
Decryption:

1. You need to find \( m \) mod \( N \) from \( N, d \) and \( c \), where \( c \) is an integer such that

\[
    c \equiv m^d \mod N.
\]

2. From \( p, q \) and \( d \) you find \( d' \) so

\[
    dd' \equiv 1 \mod (p - 1)(q - 1).
\]

3. The order of the multiplicative group \((\mathbb{Z}/N)^*\) of invertible residue classes mod \( N \) is \((p - 1)(q - 1)\). So

\[
    m^{dd'} = m^{1+(p-1)(q-1)h} = a \mod N
\]

for \( m \in (\mathbb{Z}/N)^* \) when we write \( dd' = 1 + (p - 1)(q - 1)h \)
for some integer \( h \).

4. Step (3) gives

\[
    m = m^{dd'} = c^{d'} \mod N
\]

so we can recover \( m \) from \( c \) after finding \( d' \).
What could go wrong?

1. Certainly, if one had a quick way to find the prime factorization of big integers $N$, an eavesdropper could find $p$ and $q$ from $N = pq$ and then find $m$ from $c$.

   **My advice:** If you find a way to do this, pack a suitcase and hit the road. A lot of people will be looking for you.

2. But there might be some other way to find $m$ from $c$.
   
   a. If the congruence class $m \mod N$ giving the message is represented by too small an integer $m$, we have a chance to find $m$ from $c = m^d \mod N$.
   
   b. For instance, if $0 < m^d < N$, then we can just take the $d^{th}$ root of $c = m^d$ in the integers to find $m$. Finding roots in the integers can be done quickly.
3. One way out of the potential problem posed by (2) is to add some publicly known padding \( a \) to the message \( m \).

   a. You pick \( a > N \), and you broadcast \( N, d \) and \( a \).
   b. Your friend now encrypts his message \( m \) mod \( N \) by sending \( c' = (a + m)^d \) mod \( N \).
   c. Decryption works as before to find \( a + m \) mod \( N \) from \( c' \), since you know the factors \( p \) and \( q \) of \( N \). Then

   \[
   m \text{ mod } N = (a + m \text{ mod } N) - (a \text{ mod } N).
   \]

   d. For \( m > 0 \), the representative for \( c' = (a + m)^d \) mod \( N \) in the range between 0 and \( N \) is not just \( (a + m)^d \). So we can’t decrypt by just taking roots of integers.
Coppersmith’s discovery
Coppersmith developed a method for defeating the padding strategy if $|m| < N^{1/d}$, based on this result:

**Theorem (Coppersmith)**

*Given a monic polynomial $f \in \mathbb{Z}[x]$ of degree $d$ and modulus $N \in \mathbb{Z}$, there is a polynomial time algorithm in $\log N$ and $d$ for finding all $m \in \mathbb{Z}$ satisfying*

$$f(m) \equiv 0 \mod N \quad \text{and} \quad |m| < N^{1/d}.$$ 

For the padded message problem, let

$$f(x) = (a + x)^d - c$$

for known $a, c$. We can quickly find solutions $m$ with $|m| < N^{1/d}$ and

$$(a + m)^d - c \equiv f(m) \equiv 0 \mod N.$$
Why is this an interesting theorem?

1. Can compute roots of polynomials in polynomial time.

2. Can compute roots of polynomials modulo primes in polynomial time.

3. To compute roots of polynomials modulo composite integers, best algorithm in general is to factor $N$, solve mod each prime, and use Chinese remainder theorem/Hensel lifting to generate solutions mod $N$.

4. By accepting a bound on solution size, Coppersmith’s method lets us find small roots without factoring $N$. 
Coppersmith’s Algorithm Outline

Input: $f = x^d + f_{d-1}x^{d-1} + \cdots + f_0 \in \mathbb{Z}[x]$, modulus $N \in \mathbb{Z}$

Desired output: All $r \in \mathbb{Z}, |r| < N^{1/d}$ with $f(r) \equiv 0 \mod N$.

Algorithm idea:

1. Construct auxiliary polynomial $h(x) \in \mathbb{Q}[x]$ satisfying:
   • For any $f(r) \equiv 0 \mod N$, $h(r) \in \mathbb{Z}$.
     • A construction with this property is
       $$h(x) = \sum_{i,j} a_{i,j}x^i(f(x)/N)^j \quad a_{i,j} \in \mathbb{Z}$$
   • We want an $h(x)$ so that $|h(r)| < 1$ for all $r \in \mathbb{C}$ such that $|r| < N^{1/d}$.
2. The two properties together imply $h(r) = 0$ if $r$ is desired output.
   • $h(r) \in \mathbb{Z}$ and $|h(r)| < 1 \implies h(r) = 0$.

3. Compute roots of $h$ and check conditions.
Coppersmith’s Algorithm Outline

Input: \( f = x^d + f_{d-1}x^{d-1} + \cdots + f_0 \in \mathbb{Z}[x] \), modulus \( N \in \mathbb{Z} \)

Desired output: All \( r \in \mathbb{Z}, |r| < N^{1/d} \) with \( f(r) \equiv 0 \) mod \( N \).

1. Fix a parameter \( \ell > 0 \). Consider the lattice \( A_\ell \) of all polynomials of degree \( \leq \ell d - 1 \) that are integral combinations of polynomials of the form

\[
h_{i,j}(x) = x^i(f(x)/N)^j
\]

with

\[
0 \leq i < d = \deg(f(x)) \quad \text{and} \quad i + jd < \ell d.
\]

Any polynomial \( h(x) \) in \( A_\ell \) has the property that if \( r \in \mathbb{Z} \) and \( f(r) \equiv 0 \) mod \( N \) then \( h(r) \in \mathbb{Z} \).
2. Suppose $T > 0$ is a real parameter. By the discussion of auxiliary polynomials, it will be enough to find a non-zero element $h(x)$ of $A_\ell$ such that $|h(r)| < 1$ for all $r \in \mathbb{C}$ with $|r| \leq T$ when we let $T = N^{1/d}$.

3. Write each generator $h_{i,j}(x)$ of $A_\ell$ in the form

$$h_{i,j}(x) = a_0 + a_1(x/T) + \cdots a_{\ell d-1}(x/T)^{\ell d-1}$$

for some vector

$$a(i,j) = (a_0, a_1, \ldots, a_{\ell d-1}) \quad \text{in} \quad \mathbb{R}^{\ell d}.$$
4. The vectors \(a(i,j)\) generate a lattice \(\mathcal{L}\) in \(\mathbb{R}^{\ell d}\). The LLL algorithm quickly finds a non-zero "short" vector \(\tilde{a} = (\tilde{a}_0, \ldots, \tilde{a}_{\ell d-1})\) in this lattice with respect to the usual Euclidean \(L^2\) norm on \(\mathbb{R}^{\ell d}\) given by

\[ |\tilde{a}|_2 = \sqrt{\tilde{a}_0^2 + \ldots \tilde{a}_{\ell d-1}^2}. \]

This \(\tilde{a}\) corresponds to an element \(h(x) \neq 0\) of \(A_\ell\). "Short" means

\[ |\tilde{a}|_2 \leq 2^{(\ell d-1)/4} |\text{det} \mathcal{L}|^{1/(\ell d)} \]

when \(|\text{det}(\mathcal{L})|\) is the volume of \(\mathbb{R}^n / \mathcal{L}\).

5. For \(|r| \leq T\) we get

\[ |h(r)| = |\tilde{a}_0 + \tilde{a}_1(r/T) + \ldots + \tilde{a}_{\ell d-1}(r/T)^{\ell d-1}| \leq |\tilde{a}|_1. \]

where

\[ |\tilde{a}|_1 = |\tilde{a}_0| + |\tilde{a}_1| + \ldots + |\tilde{a}_{\ell d-1}| \]

is the \(L^1\) norm.
6. By Cauchy-Schwarz, the $L^1$ and $L^2$ norms of $\tilde{a}$ satisfy an inequality

$$|\tilde{a}|_1 \leq \sqrt{\ell d}|\tilde{a}|_2 \leq \sqrt{\ell d} \ 2^{(\ell d - 1)/4} \ |\det \mathcal{L}|^{1/(\ell d)}$$

7. Show that for a judicious choice of $\ell$ and $T = N^{1/d}$ this leads to a quick way to find an $0 \neq h(x) \in A_\ell$ with

$$|h(r)| \leq |\tilde{a}|_1 < 1 \quad \text{for} \quad |r| < N^{1/d}.$$ 

Doing this depends on a careful calculation of $|\det \mathcal{L}|.$
Lattice Bounds

**Theorem (Minkowski-Hermite)**

There is a universal minimal constant $\gamma_n$ (the Hermite constant) such that if $\mathcal{L}$ = lattice in $\mathbb{R}^n$, then there is a non-zero $v \in \mathcal{L}$ with

$$|v|_2 \leq \gamma_n \cdot |\det \mathcal{L}|^{1/n}$$

One has $\sqrt{\frac{n}{2\pi e}} \leq \gamma_n \leq \sqrt{\frac{n}{\pi e}}$.

**Theorem (LLL)**

We can find a vector $v \neq 0$ of length

$$|v|_2 < 2^{(n-1)/4} |\det \mathcal{L}|^{1/n}$$

in polynomial time.
Is Coppersmith’s bound $|r| < N^{1/d}$ optimal?

- Yes, in general. Consider $f(x) = x^d$, $N = p^d$.
  
  Attempting to improve bound to $|r| < N^{1/d+\epsilon}$ yields $2N^\epsilon$ multiples of $p$ that are roots.
  
  Exponentially many solutions cannot be enumerated in polynomial time.

- Counterexample does not rule out most applications of cryptographic interest, where e.g. $N = pq$ or solution is known to be unique by construction.
An upper bound on Coppersmith’s method

You can’t improve on Coppersmith’s bounds for univariate polynomials using auxiliary polynomials the way he does.

**Theorem (Hemenway, Heninger, Scherr, C.)**

Let \( f \in \mathbb{Z}[x] \) be monic, degree \( d \), modulus \( N \in \mathbb{Z} \), \( \epsilon > 0 \). There is no auxiliary polynomial of the form

\[
h(x) = \sum_{i,j} a_{i,j} x^i (f / N)^j
\]

so that \( |h(z)| < 1 \) for all \( z \) satisfying \( |z| \leq N^{1/d+\epsilon} \).
Capacity of a set: Definition 1

Transfinite Diameter

Let $E$ be a compact subset of $\mathbb{C}$ closed under complex conjugation.

**Definition (nth transfinite diameter)**

$$d_n(E) = \sup_{z_1,\ldots,z_n \in E} \prod_{i<j} |z_i - z_j|^{1/(\binom{n}{2})}$$

**Example (Unit circle)**

$$d_2(E) = 2$$
Capacity of a set: Definition 1

Transfinite Diameter

Let $E$ be a compact subset of $\mathbb{C}$ closed under complex conjugation.

Definition ($n$th transfinite diameter)

$$d_n(E) = \sup_{z_1, \ldots, z_n \in E} \prod_{i < j} |z_i - z_j|^{1/(n)}$$

Definition (Capacity)

$$\gamma(E) = \lim_{n \to \infty} d_n(E)$$
Capacity of a set: Definition 1

Transfinite Diameter

Let $E$ be a compact subset of $\mathbb{C}$ closed under complex conjugation.

Definition (Capacity)

$$\gamma(E) = \lim_{n \to \infty} d_n(E)$$

Example (Unit circle)

$$\gamma(E) = 1$$
Transfinite diameters and conjugates of algebraic integers

Suppose $z_1, \ldots, z_n$ in $E$ are the conjugates of a degree-$n$ algebraic integer.

\[
\prod_{i=1}^{n}(x - z_i) = f(x) \in \mathbb{Z}[x] \quad \text{monic, irreducible}
\]

discriminant: \quad \Delta f(x) = \prod_{i<j}(z_i - z_j)^2 \in \mathbb{Z}, \neq 0

\[
d_n(E) \geq \prod_{i<j}|z_i - z_j|^\frac{2}{n(n-1)} = |\Delta f(x)|^\frac{1}{n(n-1)} \geq 1
\]

- $d_n(E) \geq 1$ if $E$ contains all conjugates of a degree-$n$ algebraic integer.

Corollary

*If there are infinitely many algebraic integers with all conjugates in $E$ then $\gamma(E) \geq 1$*
Capacity of a set: Definition 2

Electrostatics

Consider unit charge distribution consisting of $n$ repelling point charges at $z_1, \ldots, z_n$ in $E$, each with charge $1/n$.

Potential energy between $z_i, z_j = -\frac{\log |z_i - z_j|}{n^2}$

Potential energy of charged state $= -\sum_{i<j} \frac{\log |z_i - z_j|}{n^2}$

Example (Unit circle)
Minimum potential energy of $n$ charges in $E$: $\approx -\log d_n(E)$

**Definition (Capacity)**

$$-\log \gamma(E) = \lim_{n \to \infty} -\log d_n(E)$$

This is the minimal potential energy of a unit charge distribution on $E$. 
Consider the set of degree-\( n \) polynomials bounded on \( E \):

\[
b_n = \sup \left\{ |r| \mid \exists p(x) = r x^n + \cdots + p_0 \in \mathbb{R}[x] \text{ s.t. } \sup_{z \in E} |p(z)| \leq 1 \right\}
\]

**Definition (Capacity)**

\[
\gamma(E) = \lim_{n \to \infty} b_n^{1/n}
\]
Capacity of a set: Definition 4
Sectional capacity

\[ F_n = \{ p(x) \in \mathbb{R}[x], \deg p(x) \leq n, \sup_{z \in E} |p(z)| < 1 \} \]

\[ F_n \subseteq \mathbb{R} \oplus \cdots \oplus \mathbb{R} \quad \text{convex symmetric subset} \]

Definition (Sectional capacity)

\[ \log \gamma(E) = \lim_{n \to \infty} \frac{-2 \log \text{Vol}(F_n)}{n^2} \]
Applying sectional capacity to polynomials

Theorem (Minkowski)
If $\text{Vol}(F_n) > 2^{n+1}$ then there is a $p(x) \in F_n \cap \mathbb{Z}[x]$, $p(x) \neq 0$

**Consequences** Recall that

$$\log \text{Vol}(F_n) \approx (-n^2/2) \log \gamma(E)$$

If $\gamma(E) < 1$ then $-\log \gamma(E) > 0$ so for large $n$:

$$\log \text{Vol}(F_n) \approx (n^2/2)(- \log \gamma(E)) > (n + 1) \log 2$$

($\implies$ There will be such a $p(x)$.)
Applying sectional capacity to polynomials

Lemma
\( \gamma(E) < 1 \implies \text{there is a nonzero } p(x) \in \mathbb{Z}[x] \text{ with } |p(z)| < 1 \text{ for } z \in E. \)

Consider \( z_1, \ldots, z_n \) conjugates of some algebraic integer in \( E \).

- \( |p(z_1)|, \ldots, |p(z_n)| < 1 \), so \( |N(p(z_1))| = \prod_i |p(z_i)| < 1 \) and is an integer, so \( N(p(z_1)) = 0 \).
  (Here \( N \) is the norm from \( \mathbb{Q}(z_1) \) to \( \mathbb{Q} \).)

- So zeros of \( p(x) \) include all algebraic integers with conjugates in this set, so \( p \) vanishes at all such elements in \( E \).
Theorem

Let $E$ be a compact subset of $\mathbb{C}$ closed under complex conjugation.

- If $\gamma(E) < 1$, then there are finitely many irreducible monic polynomials with integer coefficients with all roots in $E$.

- If $\gamma(E) > 1$, then for every open neighborhood $U$ of $E$, there are infinitely many irreducible monic polynomials with integer coefficients with all roots lying in $U$. 
Linking capacity theory and Coppersmith’s method

• We have already discussed:
  Let $E \subseteq \mathbb{C}$ compact, stable under complex conjugation.
  When does there exist a $h(x) \in \mathbb{Z}[x]$ so that $|h(z)| < 1$ if $z \in E$?

• For Coppersmith’s theorem, we are looking for an auxiliary polynomial in $\mathbb{Q}[x]$ of the form

$$h(x) = \sum_{i,j} c_{i,j} x^i (f(x)/N)^j, \quad a_{i,j} \in \mathbb{Z} \quad (1)$$

satisfying $|h(z)| < 1$ for $z \in \mathbb{C}$ with $|z| < T$.

This looks a lot like the capacity theory we were talking about, except $h(x)$ might not be in $\mathbb{Z}[x]$.

But we know (1) implies that if $z$ and $f(z)/N$ are algebraic integers then $h(z)$ is an algebraic integer.
New problem: When is there an $h(x) \in \mathbb{Q}[x]$ so that

1. $|h(z)| < 1$ if $z \in E \subseteq \mathbb{C}$

2. $h(z)$ is an algebraic integer for all algebraic integers $z$ satisfying $f(z) \equiv 0 \mod N$ in the ring of all algebraic integers.
Cantor and Rumely's enhanced capacity theory

Suppose $E_p$ is a subset of $\mathbb{Q}_p$ for each prime $p$, and that $E_\infty$ is a subset of $\mathbb{C}$. If these satisfy the appropriate hypotheses, one can define a capacity

$$\gamma(E) = \gamma_\infty(E_\infty) \cdot \prod_p \gamma_p(E_p)$$

associated to $E = \prod_p E_p \times E_\infty$ for which the following is true:

Theorem (Cantor)

- If $\gamma(E) < 1$ then there exists a nonzero polynomial $h(x) \in \mathbb{Q}[x]$ satisfying
  $$|h(z)|_p \leq 1 \quad \forall p \text{ and } z \in E_p \quad \text{and} \quad |h(z)|_\infty < 1 \quad \text{for } z \in E_\infty.$$

- If $\gamma(E) > 1$ then no such polynomial exists.
Now we let:

\[ E_p = f^{-1}\left(\{z \mid |z|_p \leq |N|_p\}\right) \quad \text{and} \quad E_\infty = \{z \in \mathbb{C} \mid |z| \leq T\} \]

With these choices, a polynomial \( h(x) \in \mathbb{Q}[x] \) has the above properties if and only if:

1. For all algebraic integers \( z \) for which \( f(z) \equiv 0 \mod N \) in the ring of algebraic integers, \( h(z) \) is an algebraic integer.
2. For all complex \( z \) with \( |z| \leq T \) one has \( |h(z)| < 1 \).

One now computes, using Rumely and Cantor’s formulas, that

\[ \gamma(E) = TN^{-1/d}. \]

Then \( \gamma(E) < 1 \) is equivalent to

\[ T < N^{1/d} \]

and this is why Coppersmith’s method cannot be improved!
Lattices of binomial polynomials

Definition (Binomial polynomial)

\[ b_i(x) = \binom{x}{i} = x \cdot (x - 1) \ldots (x - i + 1)/i! \]

\[ b_i(z) \in \mathbb{Z} \text{ for any } z \in \mathbb{Z}. \]

Theorem (Polya)

If \( h(x) \in \mathbb{Q}[x] \) then \( h(z) \in \mathbb{Z} \) for all \( z \in \mathbb{Z} \) \iff \( h(x) \) is a integer combination of binomial polynomials \( b_i(x) \).

Coppersmith asked if one could improve the theorem using binomial polynomials:

\[ h(x) = \sum_{i,j \geq 0} a_{i,j} b_i(x) b_j(f(x)/N) \]

These no longer have the property that \( h(z) \) is an algebraic integer whenever both \( z \) and \( f(z)/N \) are.
Binomial polynomials don’t help

**Theorem**

Let $\epsilon > 0$ and $M$ a positive integer, $319 \leq M \leq 1.48774N^\epsilon$. If there is a nonzero polynomial

$$h(x) = \sum_{0 \leq i,j \leq M} a_{i,j}b_i(x)b_j(f(x)/N)$$

with $a_{i,j} \in \mathbb{Z}$ such that

$$|h(z)| < 1 \text{ for } z \in \{z \in \mathbb{C} \mid |z| \leq N^{1/d+\epsilon}\}$$

then $N$ must have a prime factor less than $M$.

**Moral:** If $N$ does not already have a very small prime factor, any auxiliary polynomial $h(x)$ constructed from binomial polynomials would have to be of too large a degree to be useful for an algorithm that runs in polynomial time in $\ln(N)$. 
Another application: Factoring RSA moduli with partial information

**Given:** An integer $N$ which is a product $pq$ of two unknown odd prime numbers $p \neq q$.

**Problem:** Suppose one is also given some fraction of the digits of the factor $p$ of $N$. When is this information sufficient to find $p$ (and hence also $q$) in polynomial time in $\log_2(N)$?

**Theorem (Coppersmith)**

Suppose $N = pq$ has $m = \lfloor \log_2(N) \rfloor + 1$ binary digits. One can find $p$ and $q$ in polynomial time if one knows either of the following:

1. The highest order $m/4$ binary digits of either $p$ or $q$, or
2. The lowest order $m/4$ binary digits of either $p$ or $q$. 
This is another application of the auxiliary polynomial method using LLL.

**Theorem (Hemenway, Heninger, Scherr, C.)**

One can’t use Coppersmith’s method in general to find \( p \) even when one knows the leading digit of \( p \) together with one block of 99.99999...% of the remaining ones, with the unknown digits being two blocks of equal size, one of which includes the lowest order digits.

\[
p = X????????????????????????????????????????????????????????????????????????????????????????????
\]

**Why:** Capacity theory says the required one variable auxiliary polynomials don’t exist.

**But:** There might be useful multivariable polynomials!
Summary

*Cryptographic applications of capacity theory: On the optimality of Coppersmith’s method for univariate polynomials*
Ted Chinburg, Brett Hemenway, Nadia Heninger, and Zachary Scherr

- If you want to improve univariate Coppersmith theorem, you will need to use a new method.
- New links between capacity theory and cryptography.

Future Work

- Bivariate polynomials.
- Solving equations modulo divisors.
- Multivariate polynomials.