ALGEBRAIC EQUATIONS AND CRYPTOGRAPHY– SOME RECENT RESULTS

ADI SHAMIR
APPLIED MATHEMATICS
THE WEIZMANN INSTITUTE
REHOVOT, ISRAEL

PARADIGMS OF MODERN CRYPTOGRAPHY:

- USE TRAPDOOR ONE-WAY FUNCTIONS: f IS EASY TO EVALUATE, APPARENTLY HARD TO INVERT, BUT ACTUALLY EASY TO INVERT WHEN SOME TRAPDOOR INFORMATION IS KNOWN.
- USE f TO ENCRYPT CLEARTEXTS AND TO VERIFY SIGNATURES; USE f^{-1} TO DECRYPT CIPHERTEXTS AND TO GENERATE SIGNATURES.
- USE NUMBER-THEORETIC MAPPINGS MODULO A COMPOSITE $n = p \cdot q$: THE APPLICATION OF f CONSISTS OF EVALUATING ALGEBRAIC EQUATIONS MODULO n, AND THE INVERSION OF f CONSISTS OF SOLVING ALGEBRAIC EQUATIONS MODULO n.

THE SECURITY OF CRYPTOSYSTEMS

SUCH A CRYPTOSYSTEM IS CALLED "PROVABLY SECURE" IF THE COMPUTATION OF f^{-1} IS AT LEAST AS HARD AS THE FACTORIZATION OF THE MODULUS n, IN THE FOLLOWING SENSE:

ALGORITHM FOR SOLVING A NON-NEGLIGIBLE FRACTION OF THE ALGEBRAIC EQUATIONS $\Rightarrow$ ALGORITHM FOR FACTORING n WHICH RUNS IN EXPECTED POLYNOMIAL TIME IN SIZE OF n

EXAMPLES:

- RABIN: $x^2 = v \pmod n$. PROVABLY SECURE.
- CUBIC RSA: $x^3 = v \pmod n$. AN OPEN PROBLEM.
- ONG-SCHNORR-SHAMIR: $x^2 + ky^2 = v \pmod n$. PROVEN INSECURE BY POLLARD.

THE GENERAL PROBLEM: GIVEN i ALGEBRAIC EQUATIONS OF DEGREE d IN j VARIABLES MODULO $n = p \cdot q$, IS THEIR SOLUTION AS HARD AS FACTORING THE MODULUS n?

1

CRYPTOSYSTEMS BASED ON ALGEBRAIC EQUATIONS MODULO $n=pq$:

RABIN: $x^2 = v \pmod n$

AS SECURE AS THE FACTORIZATION OF n

CUBIC RSA: $x^3 = v \pmod n$

AN OPEN PROBLEM

OSS: $x^2 - cy^2 = v \pmod n$

BROKEN BY POLLARD

A MAJOR OPEN PROBLEM:

GIVEN A SYSTEM OF ALGEBRAIC EQUATIONS MOD n, IS ITS SOLUTION AT LEAST AS HARD AS FACTORING n?

2

INTEGER VS. POLYNOMIAL FACTORIZATION

- FACTORING $n=pq$ IS BELIEVED TO BE HARD FOR RANDOM p, q
- FACTORING $F=P \cdot Q$ DEPENDS ON THE DOMAIN, WITH MANY RESULTS
- CONSIDER THE COMBINED FACTORIZATION PROBLEM

$$F = PQ \pmod{n=pq}$$

IS THE FACTORIZATION OF F AS HARD AS THE FACTORIZATION OF n?

IN WORST CASE, YES:

3

PROOF:

1. SOME POLYNOMIAL FACTORIZATION PROBLEMS ARE EQUIVALENT TO SQUARE ROOT EXTRACTION $\pmod n$:

$$x^2 - a^2 y^2 = (x + ay)(x - ay) \pmod n$$

F $\quad$ P $\quad$ Q

2. SQUARE ROOT EXTRACTION $\pmod n$ IS EQUIVALENT TO THE FACTORIZATION OF n:

$a^2 \pmod n$ HAS 4 SQUARE ROOTS, OBTAINED BY CHINESE REMAINDERING

$$\pm a \pmod p, \quad \pm a \pmod q.$$

KNOWLEDGE OF SOME PAIRS OF ROOTS LEADS TO FACTORING BY GCD.

4

HOWEVER, THIS SHEDS NO LIGHT ON:

- THE DIFFICULTY OF FACTORING RANDOMLY CHOSEN PRODUCTS
- THE DIFFICULTY OF FACTORING F OF PARTICULAR FORMS
- THE DIFFICULTY OF FACTORING WHEN PARTIAL INFORMATION ON P AND Q IS KNOWN.

IN MOST CASES, WE CANNOT REDUCE THE PROBLEM OF FACTORING F INTO SQUARE ROOT EXTRACTION.

EXAMPLES:

1. $P=(x+ay)$, $Q=(x-ay)$ $(\text{mod } n)$

   $F=x^2-a^2y^2$ $(\text{mod } n)$

   THE FACTORIZATION IS HARD

2. $P=(x+ay)$ $Q=(x+ay)$ $(\text{mod } n)$

   $F=x^2+2axy+a^2y^2$ $(\text{mod } n)$

   THE FACTORIZATION IS EASY

3. $P=(x^3+ax+b)$ $Q=(x^3+cx+d)$ $(\text{mod } n)$

   $F=x^6+(a+c)x^4+(b+d)x^3+acx^2+(ad+bc)x+bd$

   THE FACTORIZATION IS HARD

4. $P=(x^4+ax+b)$ $Q=(x^3+cx+d)$ $(\text{mod } n)$

   $F=x^7+cx^5+(a+d)x^4+bx^3+acx^2+(ad+bc)x+bd$

   THE FACTORIZATION IS EASY

5. $P=(ax+by+cz+\cdots)$ $Q=(dx+ey+fz+\cdots)$ $(\text{mod } n)$

   THE FACTORIZATION IS HARD

6. SAME AS (5), BUT KNOWING THAT $a=0$

   THE FACTORIZATION IS EASY

7. SAME AS (5), BUT KNOWING THAT $a=1$

   THE FACTORIZATION IS HARD

8. $P=(ax+a)$ $Q=(bx+b)$ $(\text{mod } n)$

   THE FACTORIZATION IS EASY

9. $P=(ax+a+1)$ $Q=(bx+b+1)$ $(\text{mod } n)$

   THE FACTORIZATION IS HARD

10. $P=(a^2x^3y+b^3xz+(a+b^2)yz)(ax+by+8z)+1$

    $Q=(c^2x^3y+d^3xz+(c+d^2)yz)(cx+dy+8z)+1$

    THE FACTORIZATION IS HARD

DEFINITION OF THE PROBLEM:

- AN ALGEBRAIC FORM $\mathcal{F}$: A MULTIVARIATE POLYNOMIAL IN $x, y, \cdots$ WHOSE COEFFICIENTS ARE RATIONAL FUNCTIONS IN $a, b, \cdots$
- AN ALGEBRAIC COLLECTION $\mathbb{C}(\mathcal{F})$: ALL THE POLYNOMIALS GENERATED BY SUBSTITUTING $a, b, \cdots$ WITH VALUES FROM $\mathbb{Z}_n$. WLG, ASSUME THAT THEY ARE MONIC.
- THE FACTORIZATION PROBLEM: GIVEN $\mathcal{F}_1, \mathcal{F}_2$ AND $F=P\cdot Q$ $(\text{mod } n)$, WHERE $P \in_R \mathbb{C}(\mathcal{F}_1)$ AND $Q \in_R \mathbb{C}(\mathcal{F}_2)$, CAN YOU FACTOR F INTO $P'\cdot Q'$ OF THE GIVEN FORMS?

REMARK: EVERYTHING EXCEPT n IS ASSUMED TO HAVE A FIXED SIZE.

WHY WE DO NOT CONSIDER COMPLETE FACTORIZATIONS INTO IRREDUCIBLE FACTORS?

EXAMPLE: IS x IRREDUCIBLE $\text{mod } n$?

NO: $$x=\frac{1}{p^2+q^2}\underbrace{(px+q)(qx+p)}_{pqx^2+(p^2+q^2)x+pq} \quad (\text{mod } n)$$

- DEGREES ARE NOT ADDITIVE MOD n!
- THERE ARE NO MONIC IRREDUCIBLE POLYNOMIALS $\text{mod } n$
- KNOWING ANY IRREDUCIBLE POLYNOMIAL $\text{mod } n$ IS EQUIVALENT TO FACTORING n.

WE NEED THE RESULT: A MONIC MULTIVARIATE POLYNOMIAL F OF DEGREE d CAN HAVE AT MOST 2^{2d} POSSIBLE FACTORIZATIONS INTO MONIC POLYNOMIALS P, Q MODULO $n=pq$

THE MAIN RESULT: ANY ALGEBRAIC FACTORIZATION PROBLEM WITH NON-TRIVIAL $\mathcal{F}_1 = \mathcal{F}_2$ IS AT LEAST AS HARD AS THE FACTORIZATION OF n.

REMARKS:

- $\mathcal{F}$ IS TRIVIAL IF $\mathbb{C}(\mathcal{F})$ CONSISTS OF A SINGLE POLYNOMIAL. IF EITHER $\mathcal{F}_1$ OR $\mathcal{F}_2$ IS TRIVIAL, THE POLYNOMIAL FACTORIZATION PROBLEM IS EASY.
- THIS IS THE PROPER EXTENSION FROM NUMBERS TO POLYNOMIALS OF THE STATEMENT "SQUARE ROOT EXTRACTION IS DIFFICULT".

THE EASY PROOF:

$$F = P \cdot Q \pmod{n}$$

$$F = Q \cdot P \pmod{n}$$

SINCE $\mathcal{F}_1 = \mathcal{F}_2$, THESE TWO FACTORIZATIONS ARE INDISTINGUISHABLE.

CONSIDER NOW THE HALF SYMMETRY IMPLIED BY SWITCHING P AND Q $(\bmod p)$ AND KEEPING THEM $(\bmod q)$. CALL THE CHINESE REMAINDERED RESULTS R AND S:

$$\begin{cases} R = P \pmod{p} \\ R = Q \pmod{q} \end{cases} \qquad \begin{cases} S = Q \pmod{p} \\ S = P \pmod{q} \end{cases}$$

LEMMA: IF $\mathcal{F}_1 = \mathcal{F}_2$, THEN $F = R \cdot S \pmod{n}$ AND R, S ALSO BELONG TO $\mathbb{C}(\mathcal{F}_i)$.

PROOF: CHINESE REMAINDER THE RANDOM

ASSUME THAT SOMEONE CHOOSES $F = P \cdot Q \pmod{n}$ AND GETS $F = R \cdot S \pmod{n}$ FROM A FACTORING BLACK BOX:

$P - R = 0 \pmod{p}$ BY DEFINITION

$P - R = P - Q \neq 0 \pmod{q}$ WITH OVERWHELMING PROBABILITY FOR NON-TRIVIAL FORMS $\mathcal{F}$ BY THE PROPERTIES OF LOW DEGREE POLYNOMIALS

TO FACTOR n, COMPUTE ITS GCD WITH EACH COEFFICIENT OF $P - R \pmod{n}$.

NOTE THAT:

- THE FACTORIZATIONS $F = PQ \pmod{n}$, $F = RS \pmod{n}$ ARE (INFORMATION THEORETICALLY) INDISTINGUISHABLE
- THE PROBABILITY OF GETTING $R \cdot S$ FROM THE BLACK BOX IS AT LEAST 2^{-2d}.

CAN WE EXTEND THE RESULT FROM FACTORIZATION BASED EQUATIONS TO GENERAL ALGEBRAIC EQUATIONS?

OUR PROOF TECHNIQUE RELIED ON FIVE BASIC INGREDIENTS:

INVARIANCE: SQUARING IS INVARIANT UNDER $\mathcal{I}$. MULTIPLICATION IS INVARIANT UNDER LEFT/RIGHT ORDER.

MODULARITY: THE INVARIANT OPERATION SHOULD HAVE THE CHINESE REMAINDER PROPERTY.

INVERTIBILITY: THE INPUT AND OUTPUT OF THE OPERATION SHOULD HAVE THE SAME PROBABILITY.

NON-TRIVIALITY: THE INPUT AND OUTPUT SHOULD BE DIFFERENT W.H.P.

BOUNDEDNESS: THE EQUIVALENCE CLASSES SHOULD HAVE POLYNOMIALLY BOUNDED SIZES.

A SYSTEM OF MULTIVARIATE POLYNOMIAL EQUATIONS OF FIXED DEGREE d:

$$E_1(a,b,\cdots) = v_1 \pmod m$$
$$\vdots$$
$$E_k(a,b,\cdots) = v_k \pmod m$$

IS CALLED **RANDOMLY SOLVABLE** IF THE E_i ARE FIXED, AND THE v_i ARE GENERATED BY A RANDOM SUBSTITUTION OF VALUES INTO $a,b,\cdots$

MAIN RESULT: IF A RANDOMLY SOLVABLE SYSTEM OF EQUATIONS IS INVARIANT UNDER SOME INVERTIBLE RATIONAL TRANSFORMATION OF THE VARIABLES WHICH IS NOT THE IDENTITY, AND THE SYSTEM HAS POLYNOMIAL # OF SOLUTIONS, THEN FINDING ANY ONE OF THEM IS AT LEAST AS DIFFICULT AS THE FACTORIZATION OF m.

EXAMPLES:

- IN THE FACTORING APPLICATION, ALL THE EQUATIONS $E_i(a',b',\cdots,a'',b'',\cdots)=v_i$ WERE INVARIANT UNDER $a' \leftrightarrow a''$, $b' \leftrightarrow b''$
- THE EXCHANGE CAN BE PARTIAL, AS IN:
  $a^2+b^2+abc+ad+bd=v$ UNDER $a \leftrightarrow b$.
- THE TRANSFORMATION CAN BE LINEAR:
  $a^2+(a+b)^2=v$ UNDER $a \leftarrow a+b$, $b \leftarrow b$.
- THE TRANSFORMATION CAN BE RATIONAL:
  $a^2+b^{-2}=v$ UNDER $a \leftarrow 1/b$, $b \leftarrow 1/a$.

APPLICATION: THE SECURITY OF CUBIC RSA

- SOLVING $a^3 = v \pmod m$ IS NOT KNOWN TO BE EQUIVALENT TO FACTORING.
- SOLVING $a^3+b^3=v \pmod m$, $(a+b)^3=u \pmod m$ IS PROVABLY EQUIVALENT TO FACTORING.