1

THE DISCRETE LOG IS VERY DISCREET

AVITAL SCHRIFT, ADI SHAMIR
APPLIED MATH DEPT
THE WEIZMANN INSTITUTE OF SCIENCE
ISRAEL

2

THE GENERAL PROBLEM:

LET f BE A ONE WAY FUNCTION:

$$x \xrightarrow[\text{EASY}]{} f(x) \qquad f(x) \xrightarrow[\text{DIFFICULT}]{} x$$

HOWEVER, PARTIAL INFORMATION ABOUT x MAY LEAK OUT. LET B BE A PREDICATE:

$$f(x) \xrightarrow[?]{} B(x)$$

TYPICAL CLASSES OF BOOLEAN PREDICATES:

- PARTICULAR BITS
- RELATIONSHIP BETWEEN BITS
- ARBITRARY PREDICATES ON A SUBSET OF BITS.

5

THE PROBLEM CONSIDERED IN THIS TALK:

$$f_{g,n}(x) = g^x \pmod{n}$$

WHERE:

- n IS A BLUM INTEGER (WITH UNKNOWN FACTORIZATION):
  $n = p \cdot q$, p, q PRIMES, $|p| = |q|$,
  $p \equiv q \equiv 3 \pmod{4}$.
- g IS A QUADRATIC RESIDUE MODULO n, WHICH IS EITHER RANDOMLY CHOSEN OR GUARANTEED TO HAVE A HIGH ORDER

6

WE WANT TO PROVE:

FOR <u>ANY</u> BOOLEAN PREDICATE B OF THE RIGHT HALF OF THE BINARY REPRESENTATION OF x,

$B(x)$ CANNOT BE APPROXIMATED WITH A NON-NEGLIGIBLE ADVANTAGE FOR RANDOMLY CHOSEN INPUTS $g, n, g^x \pmod{n}$

UNDER THE SOLE ASSUMPTION THAT POLYSIZE CIRCUITS CANNOT FACTOR A NON-NEGLIGIBLE FRACTION OF BLUM INTEGERS.

8

THE NEW IDEA:

FOR A PRIME MODULUS n:

$$g^n = g^1 \pmod{n}$$

FOR A COMPOSITE MODULUS n:

$$g^n = g^{n-\varphi(n)} = g^{n-(p-1)(q-1)}$$
$$= g^{n-pq+p+q-1} = g^{p+q-1} \pmod{n}$$

(UNLESS THE ORDER OF g IS EXTREMELY SMALL)

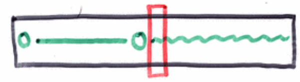
LET $S = p+q-1$. THEN:

- S IS SMALL (HALF SIZE NUMBER).
- $g^S \pmod{n}$ IS EASY TO COMPUTE.
- KNOWLEDGE OF S IMPLIES FACTORING.

9

THE MIDDLE BIT OF THE DISCRETE LOG CANNOT BE COMPUTED.

$S=$



THE BINARY REPRESENTATION OF THE DISCRETE LOG OF $g^n \pmod{n}$.

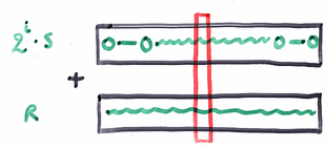
THIS REPRESENTATION CAN BE MOVED LEFT i BITS BY CONSIDERING THE DISCRETE LOG OF $g^{2^i \cdot n} \pmod{n}$, PROVIDED THAT $i < \frac{|n|}{2}$.

BY VIEWING THE MIDDLE BIT THROUGHOUT THE LEFT-SHIFT PROCESS, WE CAN GET ALL OF S AND THUS FACTOR n

10

THE MIDDLE BIT OF THE DISCRETE LOG CANNOT BE APPROXIMATED:

CONSIDER $g^R \cdot g^{2^i n} = g^{R+2^i \cdot S} \pmod{n}$



AS LONG AS $i < \frac{n}{2}$ THE ADDITION IS UNLIKELY TO CAUSE AN OVERFLOW OR TO SKEW THE DISTRIBUTION OF THE RESULT.

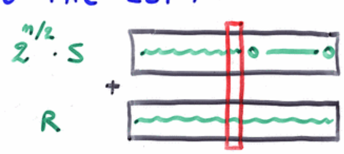
WE CAN REPEATEDLY APPROXIMATE THE MIDDLE BIT IN THE SUM

BUT WE HAVE TO CONTROL THE CARRY INTO

11

THE SOLUTION:

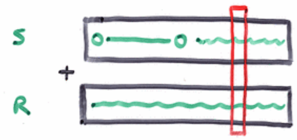
- FIRST MOVE S ALL THE WAY TO THE LEFT:



- RANDOMIZE SUFFICIENTLY MANY TIMES TO FIND THE LSB OF S WITH OVERWHELMING PROBABILITY
- ZERO THIS BIT IN S, AND REPEAT WITH FEWER LEFT SHIFTS

12

THE RIGHT HAND SIDE BITS CANNOT BE APPROXIMATED:



- WE CAN FIND ALL THE BITS OF S TO THE RIGHT OF THE WINDOW
- TO SHIFT S TO THE RIGHT OF ITS ORIGINAL POSITION, WE HAVE TO EXTRACT SQUARE ROOTS
- BUT THIS IS DIFFICULT WHEN THE FACTORIZATION OF m IS UNKNOWN

13

THE SOLUTION:

WE RANDOMIZE THE CHOICE OF g:

g_0 IS RANDOM

$g_{i+1} = g_i^2 \pmod{m}$

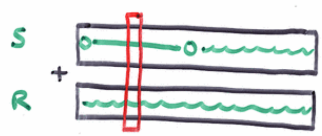
$g = g_k$ FOR $k \approx \frac{n}{2}$

SQUARING MODULO BLUM INTEGERS IS A PERMUTATION OVER QUADRATIC RESIDUES, SO g IS RANDOM.

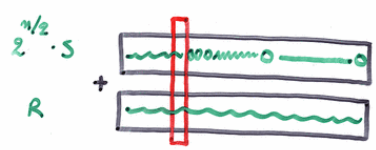
NOW $\sqrt{g^s} \pmod{m}$ CAN BE COMPUTED AS g_{k-1}^s, ITS SQUARE ROOT IS g_i^s ETC.

14

THE LEFT HAND SIDE BITS CANNOT BE APPROXIMATED:



WE CANNOT PREVENT THE (EFFECTS OF THE) ADDITION CARRIES ON THE WINDOW VALUES:



WE GUESS AND ZERO THE $O(\log\log n)$ BITS IN THE SHIFTED S WHICH ARE TO THE RIGHT OF THE WINDOW

IF WE ARE RIGHT ...

15

FOR EACH BIT POSITION AND EACH GUESSED VALUE OF THE $O(\log\log n)$ BITS WE GET SOME PREDICTION OF ONE BIT IN S.

WE CAN CHAIN THESE PREDICTIONS FROM RIGHT TO LEFT IN A UNIQUE WAY:

ASSUMPTION

$0 \leftarrow 11010$

$1 \leftarrow 01101$

$1 \leftarrow 10110$

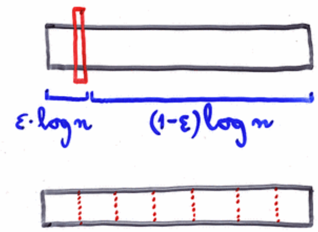
$0 \leftarrow 11011$

CONCLUSION: 011011010

WE GET $O(\log n)$ POSSIBLE BIT STRINGS

16

OVERALL METHOD FOR LEFT HAND SIDE WINDOWS:



DIVIDE S INTO $1/\varepsilon$ PIECES. GET $O(\log n)$ POSSIBLE VALUES FOR EACH PIECE. COMBINE INTO $O(\log^{1/\varepsilon} n)$ POSSIBLE VALUES. USE EXPONENTIATION TO PICK THE CORRECT VALUE.

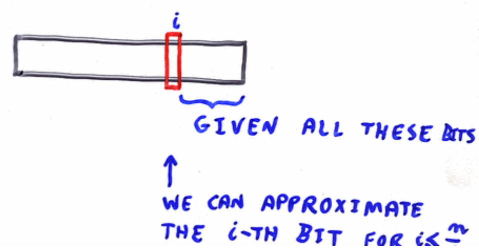
OPEN PROBLEM: HOW SECURE ARE THE BITS BETWEEN $\log\log n$ AND $\varepsilon \log n$?

17

SIMULTANEOUS BIT SECURITY:

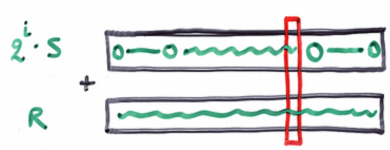
TO PROVE THAT THE RIGHT HALF OF THE BITS ARE SIMULTANEOUSLY SECURE, IT SUFFICES TO SHOW THAT NONE OF THEM CAN BE APPROXIMATED EVEN WHEN GIVEN ALL THE BITS TO THEIR RIGHT.

ASSUME THIS IS NOT THE CASE:



18

BUT IN OUR PROOF TECHNIQUE THE RIGHT HAND BITS ARE ACTUALLY KNOWN:



SO WE COULD USE THE ADVANTAGE TO COMPUTE S AND THUS FACTOR n WITH HIGH PROBABILITY.