HOW TO LEAK A SECRET

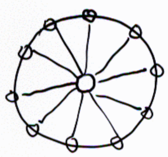
RON RIVEST, ADI SHAMIR, YAEL TAUMAN
MIT WEIZMANN WEIZMANN

MOTIVATION: A POLITICIAN/EXECUTIVE/EMPLOYEE WANTS TO LEAK A HOT STORY TO A JOURNALIST

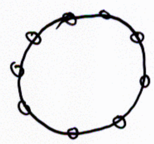
OPTIONS:
- MEET OR SEND REGULAR/ENCRYPTED EMAIL
- SEND A DIGITALLY SIGNED EMAIL
- USE AN ANONYMIZER
- USE A GROUP SIGNATURE SCHEME

OR:
- USE THE NEW RING SIGNATURE SCHEME

GROUP



RING



GROUP SIGNATURES VS RING SIGNATURES

GROUP SIGNATURES	RING SIGNATURES
∃ TRUSTED CENTER	NO CENTER
∃ INITIAL SETUP	NO SETUP
∃ SPECIALIZED KEYS	STANDARD RSA KEYS
∃ ANONYMITY REVOCATION	NO ANONIMITY REVOCATION
GROUPS MUST BE PRESPECIFIED (DEFINED BY THE CENTER)	RINGS ARE DYNAMIC (DEFINED BY ANY MEMBER)

EFFICIENCY OF NEW SCHEME:

ONE MODULAR EXPONENTIATION +
ONE MULTIPLICATION PER RING MEMBER +
ONE REGULAR ENCRYPTION PER RING MEMBER

(IN PREVIOUS GROUP SIGNATURES:
AT LEAST ONE MODULAR EXPONENTIATION/MEMBER)

OTHER APPLICATIONS:

EFFICIENT DENIABLE (DESIGNATED VERIFIER) SIGNATURE SCHEME

⋮

SECURITY OF NEW SCHEME:

- PROVABLY EQUIVALENT TO FORGERY RESISTANCE OF THE UNDERLYING SIGNATURE SCHEME IN THE RANDOM ORACLE MODEL
- UNCONDITIONALLY SIGNER-AMBIGUOUS

THE NEW SCHEME: (FIRST ATTEMPT)

EACH MEMBER HAS AN RSA KEY:

$$n_1, n_2, \dots, n_k \qquad (n_i = p_i \cdot q_i)$$

(SIMPLIFYING ASSUMPTION: ALL KEYS HAVE SAME SIZE)

THE SIGNATURE IS:

$$x_1 \in \mathbb{Z}_{n_1},\ x_2 \in \mathbb{Z}_{n_2}, \dots, x_k \in \mathbb{Z}_{n_k}$$

DEFINE:

$$y_1 = x_1^2 \pmod{n_1},\ y_2 = x_2^2 \pmod{n_2}, \dots, y_k = x_k^2 \pmod{n_k}$$

THE VERIFICATION CONDITION:

$$g(y_1, y_2, \dots, y_k) = m$$

WHERE g IS UNIQUELY INVERTIBLE WITH RESPECT TO EACH ONE OF ITS INPUTS

A TECHNICAL PROBLEM:

- EACH USER HAS A DIFFERENT DOMAIN $[0, m_i)$
- ENCRYPTIONS HAVE ANOTHER DOMAIN $[0, 2^b)$

TO UNIFY THE DOMAINS:

- SET $b > \max(m_1, m_2, \cdots, m_i, \cdots, m_k)$
- TO SIGN A GIVEN b-bit x:

$$x = x_0 \cdot 1 + x_1 \cdot m_i + x_2 \cdot m_i^2 + \cdots + x_j \cdot m_i^j$$

NOW SIGN SEPARATELY EACH OF $x_0 \cdots x_{j-1}$ LEAVING x_j UNCHANGED

IF THE ORIGINAL SIGNATURE SCHEME IS A TRAPDOOR PERMUTATION OVER $[0, m_i)$, THE EXTENDED SIGNATURE SCHEME IS A TRAPDOOR PERMUTATION OVER THE UNIFIED $[0, 2^b)$

CONCRETE EXAMPLES: $(y_i = x_i^2 \pmod{m_i})$

ADDITION: $y_1 + y_2 + \cdots + y_k = m$ (OVER THE INTEGERS)

XOR: $y_1 \oplus y_2 \oplus \cdots \oplus y_k = m$ (AS BINARY STRINGS)

CHAINING: $P(y_1 \oplus P(y_2 \oplus \cdots P(y_{k-1} \oplus P(y_k))))$ (FOR A RANDOM PERM P)

THE SECURITY REQUIREMENTS:

COMPLETENESS: ANY MESSAGE CAN BE SIGNED BY ANY MEMBER OF THE GROUP

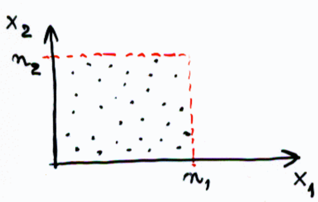
SOUNDNESS: ONLY MEMBERS OF THE GROUP CAN SIGN MESSAGES

ANONYMITY: IT IS (INFORMATION THEORETICALLY) IMPOSSIBLE TO DETERMINE WHICH MEMBER PRODUCED A GIVEN COLLECTION OF SIGNATURES

PROOF OF PERFECT ANONYMITY IN RABIN SCHEME:

THIS ARGUMENT IS MISLEADING:

CONSIDER A FIXED m AND TWO MEMBERS, AND MARK ALL THE VALID SIGNATURES:



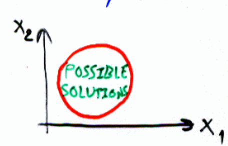
$$g[x_1^2 \pmod{m_1},\ x_2^2 \pmod{m_2}] = m$$

THE ALGORITHM:

- CHOOSE ONE OF x_1, x_2 UNIFORMLY FROM ITS RANGE
- IF $\nexists$ SOLUTION FOR OTHER VARIABLE, REPEAT
- OTHERWISE, CHOOSE UNIFORMLY ONE OF POSSIBLE VALUES OF OTHER VARIABLE, AND OUTPUT THE PAIR OF (x_1, x_2).

CAN YOU DISTINGUISH BETWEEN THE CASES?

IN GENERAL, YES:



THEOREM: ASSUME $\exists$ CONSTANTS c_1, c_2 S.T.

$\forall$ HORIZONTAL LINES, #SOLUTIONS $= 0 \vee c_1$

$\forall$ VERTICAL LINES, #SOLUTIONS $= 0 \vee c_2$

[REMARK: THE CLAIM IS INCORRECT IF 0 REPLACED BY 1]

THEN THE TWO CASES ARE PERFECTLY INDISTINGUISHABLE, AND THUS WE HAVE INFORMATION THEORETICAL ANONYMITY.

PROOF: BY THE MARBLES AND BUCKETS ARGUMENT: ASSUME THAT THERE ARE 24 MARBLES.

4 BUCKETS
0/8 MARBLES PER BUCKET

3 BUCKETS
0/12 MARBLES PER BUCKET

[THE PROOF FAILS IF EMPTY BUCKETS ~~HAVE~~ CONTAIN A SINGLE MARBLE]

IN OUR SCHEME:

$$g(y_1, y_2, \cdots y_i, \cdots, y_k) = m, \quad y_i = x_i^e \pmod{n_i}$$

- IF $e=3$ [RSA SIGNATURES] THE SOLVED y_i HAS 0 OR 1 POSSIBLE VALUES, AND THUS THE k POSSIBLE DISTRIBUTIONS ARE PERFECTLY INDISTINGUISHABLE.
- IF $e=2$ [RABIN SIGNATURES] THE SOLVED y_i HAS 0 OR 4 USUAL SOLUTIONS, AND VERY RARELY 2 SOLUTIONS, AND THUS THE k DISTRIBUTIONS ARE STATISTICALLY INDISTINGUISHABLE.
- IN BOTH CASES, THE ANONYMITY IS INFORMATION THEORETIC, EVEN AGAINST A POWERFUL ADVERSARY THAT KNOWS ALL THE FACTORIZATIONS.

PROOF OF SOUNDNESS: TRICKY:

1. PROBLEM WITH ADDITION:

   SIGNATURES FOR 4-GROUPS CAN BE FORGED:

   $$m = x_1^2 + x_2^2 + x_3^2 + x_4^2 \quad \text{[OVER THE INTEGERS]}$$

   IF $\forall i \;\; x_i^2 < n_i$, ADD FORMAL MODULI:

   $$m = x_1^2 \pmod{n_1} + x_2^2 \pmod{n_2} + \cdots$$

   COUNTERMEASURES: INVALIDATE WHEN x_i ARE SMALL, OR USE HIGHER EXPONENTS.

2. PROBLEM WITH XOR: PREPARE

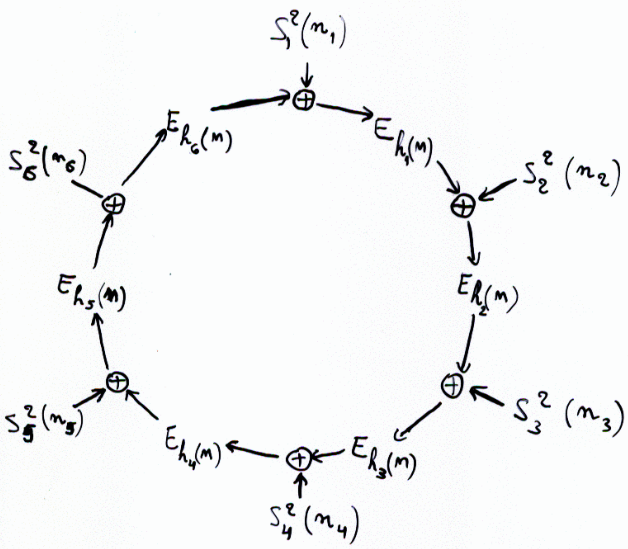
   $$x_1^2(n_1),\ x_2^2(n_2),\ \cdots\ x_t^2(n_t),\quad t \geq |m|$$

   USE LINEAR ALGEBRA (mod 2) TO FIND A SUBSET OF $\sim \frac{|m|}{2}$ VALUES THAT XOR TO m

   COUNTERMEASURES: DISALLOW LARGE GROUPS.

3. THE CHAINED CONSTRUCTION: PROVABLY SECURE IN THE RANDOM ORACLE MODEL

THE PROPOSED RING SIGNATURE SCHEME:
(USING RABIN'S SIGNATURES):



- THE RING CAN BE SUCCESSFULLY CLOSED BY ANY ONE OF ITS MEMBERS
- THE SCHEME IS SYMMETRIC ROTATIONALLY
- THE SYMMETRY CAN BE BROKEN BY FORCING ONE VALUE TO 0.

A LINEARIZED FORM OF THE RING:

$$E_k\left[S_k^2(m_k) \oplus \cdots \oplus E_2\left[S_2^2(m_2) \oplus E_1\left[S_1^2(m_1) \oplus v\right]\right]\right] = v$$

THE FORMULA CAN BE SIMPLIFIED FOR $v=0$:

$$S_k^2(m_k) \oplus \cdots \oplus E_2\left[S_2^2(m_2) \oplus E_1\left[S_1^2(m_1)\right]\right] = 0$$

EACH USER i CAN SOLVE IT BY FIXING $S_1, S_2 \cdots S_{i-1}, S_{i+1} \cdots S_k$ AND SOLVING FOR S_i:

$$S_i^2(m_i) \oplus E_{i-1}\left[S_{i-1}^2(m_{i-1}) \oplus E_{i-2}[\cdots]\right] = D_i\left[\cdots S_{k-1}^2(m_{k-1}) \oplus D_{k-1}\left[S_k^2(m_k)\right]\right]$$

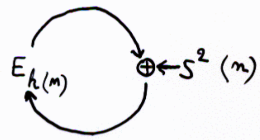
WHICH HAS THE GENERAL FORM:

$$S_i^2(m_i) = D_i[\cdots] \oplus E_{i-1}[\cdots]$$

WE CALL THIS PROCESS GAP BRIDGING

SPECIAL CASES:

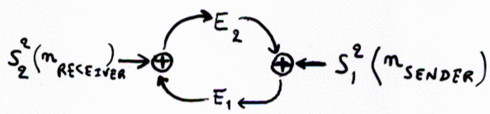
A RANDOMIZED RSA SCHEME:



WHEN THIS IS FORCED TO ZERO:

$$E_{h(m)}[0] \oplus S^2(m) = 0 \Rightarrow S^2(m) = H(m)$$

A DESIGNATED VERIFIER SIGNATURE SCHEME:

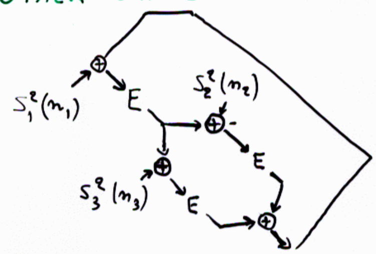


WHEN THIS IS FORCED TO ZERO:

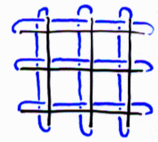
$$S_1^2(m_S) = E_{h(m)}[S_2^2(m_R)] \Leftrightarrow S_2^2(m_R) = D_{h(m)}[S_1^2(m_S)]$$

- EITHER THE SENDER OR THE RECEIVER CAN GENERATE THE SIGNATURE.
- THE RECEIVER KNOWS HE DIDN'T SIGN
- A THIRD PARTY FINDS THE TWO CASES INDISTINGUISHABLE

OTHER GAP BRIDGING STRUCTURES:



OR:



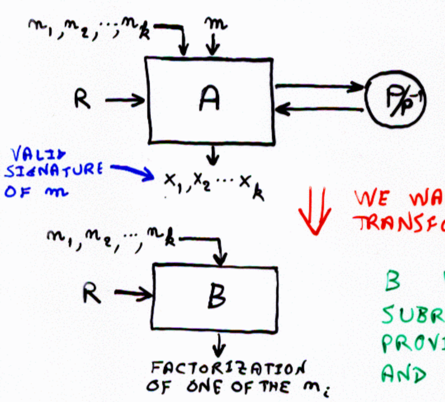
USE ALTERNATING E AND $\oplus S_i^2(m_i)$, WITH SOME IMPOSED EQUALITIES BETWEEN ROW AND COL VALUES

OUTLINE OF THE FORMAL PROOF OF SECURITY:

VERIFICATION CONDITION:

$$y_i = x_i^2 \pmod{n_i},\ P(y_1 \oplus P(y_2 \oplus \cdots (y_{k-1} \oplus P(y_k))\cdots)) = m$$

ASSUME THAT P IS IMPLEMENTED AS A RANDOM ORACLE



ASSUME WLG: THE ORACLE IS ASKED EACH QUESTION ONCE

$\Downarrow$ WE WANT TO TRANSFORM A TO B.

B USES A AS SUBROUTINE, AND PROVIDES ITS R AND P/P^{-1} INPUTS

- CONSIDER THE SEQUENCE OF ORACLE CALLS:

$$P(z_1),\ P^{-1}(z_2),\ P(z_3),\ P(z_4),\ \cdots,\ P^{-1}(z_u)$$

- GIVEN THE FINAL SIGNATURE $x_1, x_2, \cdots, x_k$ WE CAN IDENTIFY THE k USEFUL CALLS.

- DEFINE THE CRUCIAL CALL AS THE LAST USEFUL CALL. IT MAKES IT POSSIBLE TO WRITE:

$$x_i^2 \pmod{n_i} \oplus P(V') = P^{-1}(V'')$$

ONE OF THEM IS THE LAST USEFUL CALL, AND THE OTHER IS THE LAST BUT ONE USEFUL CALL (IN THE CYCLIC ORDER)

- ASSUME THAT $P(V') = W'$ IS THE LAST USEFUL CALL, AND $P^{-1}(V'') = W''$ IS THE LAST BUT ONE USEFUL CALL. WE WANT TO KEEP ALL THE FIRST $k-1$ USEFUL CALLS UNCHANGED, BUT CHANGE THE VALUE RETURNED BY THE CRUCIAL CALL INTO A RANDOMLY CHOSEN SQUARE: $W' \oplus W'' = R^2 \pmod{n_i}$. GIVEN x_i, WE FACTOR n_i

17

THE OVERALL STRATEGY:

- GUESS WHICH MODULUS m_i WILL BE INVOLVED IN THE CRUCIAL CALL.
- PREPARE A RANDOM SQUARE $R^2 \pmod{m_i}$
- GUESS THE #CALL WHICH WILL BE CRUCIAL
- GUESS THE # CALL WHICH WILL BE LAST BUT ONE
- RUN THE ALGORITHM A WITH RANDOM ORACLE VALUES, EXCEPT AT THE CRUCIAL STEP:

$P(z_1)$,	$P(z_2)$,	$P^{-1}(z_3)$,	$P(z_4)$,	$P^{-1}(z_5)$,	$P(z_6)$
USEFUL	USELESS	LAST BUT ONE (W'')	USELESS	USELESS	CRUCIAL (W')

ANSWER WITH $W' = W'' \oplus R^2 \pmod{m_i}$

- THE PROBABILITY THAT OUR GUESSES ARE CORRECT IS POLYNOMIALLY LARGE
- IF THEY ARE CORRECT, WE GET TWO SQUARE ROOTS OF THE SAME y_i, AND THUS FACTOR m_i

36

EXTENSIONS AND APPLICATIONS:

- PROVING INNOCENCE:

  USER i CHOOSES EACH x_j, $j \neq i$ PSEUDORANDOMLY FROM SEED S_j.

  TO PROVE THAT j IS NOT GUILTY, i REVEALS S_j.

- CONFESSION:

  USER i CHOOSES ALL THE x_j, $j \neq i$ PSEUDORANDOMLY FROM SEED S.

  TO PROVE THAT HE IS THE SOURCE, i REVEALS S.

- MULTISOURCED LEAKS:

  t DISTINCT SOURCES CAN CHOOSE THE y_j SO THAT THEY LIE ON A LOW DEGREE POLYNOMIAL $(d = n - t)$

- DESIGNATED ~~CONFIRMER~~ VERIFIER SIGNATURE SCHEME:

  THE SENDER SIGNS WITH GROUP {SENDER, RECEIVER}.

  [ALL CASUAL EMAIL SHOULD BE SIGNED THIS WAY!]

- TURNING SUCH SIGNATURES TO REAL SIGNATURES: REVEAL (OR ESCROW) THE RECEIVER'S INNOCENSE.