HOWNOTOLEAKASECRET
RONRIVEST,ADISHAMIR,YAELTAUMAN
MITWEIZMANNWEIZMANN
MOTIVATION:APOLITICIAN/EXECUTIVE/Employee
WANSTSTOLEAKAHOTSTORYTOAJOURNALIST
OPTIONS:MEETORSENDREGULAR/ENCRYPTEDEMAIL
-SENDADIGITALLYSIGNDEEMAIL
-USEANONYMIZER
-USEAGROUPSIGNATURESCHEME
OK:USETHENEWRINGSIGNATURESCHEME

GROUP

RING

GROUPSIGNATURESVSRINGSIGNATURES

-TRUSTEDCENTERNOTRUSTEDCENTER
-INITIALSETUPNOTSETUP
-ESPECIALIZEDKEYSSTANDARDRSAKEYS
-ANONYMITYREVOCATIONNOANONYMITYREVOCATION
-GROUPSMUSTBEPROSPECIFIEDDEFINEDBYTHECENTER
-CONTROLSAREDYNAMICDEFINEDBYANYMEMBER

EFFICIENCYOFNEWSCHEME:
ONEMODULAREXPONENTIATION+
ONEMULTIPLICATIONPERRINGMEMBER+
ONEREGULARENCRYPTIONPERRINGMEMBER
(INPREVIOUSGROUPSIGNATURES):
ATLEASTONEMODULAREXPONENTIATION/MEMBER

OTHERAPPLICATIONS:
EFFICIENTDENIABLE(DESIGNATEDVERIFIER)
SIGNATURESCHEME

SECURITYOFNEWSCHEME:
-PROBALEYQUIVALENTTOFORGERYRESISTANCE
OFTHENEWANDUNDERLYINGSIGNATURESCHEMESIMULTANEOUSLY
-UNCONDITIONALLYSIGNER-AMBIGUOUS

THENEWSCHEME:(FIRSTATTEMPT)

EACHMEMBERHASANRSAKEY:
\[ m_1, m_2, \ldots, m_k \quad (m_i = p_i \cdot q_i) \]
(SIMPLIFYINGASSUMPTION:ALLKEYSHAVESAME\(q\))
THESIGNATUREIS:
\[ x_1 \in \mathbb{Z}_{m_1}, x_2 \in \mathbb{Z}_{m_2}, \ldots, x_k \in \mathbb{Z}_{m_k} \]

DEFINE:
\[ \gamma_i = x_i^2 \pmod{m_i}, \gamma_1 = x_1^2 \pmod{m_1}, \gamma_2 = x_2^2 \pmod{m_2}, \ldots, \gamma_k = x_k^2 \pmod{m_k} \]
THEVERIFICATIONCONDITION:
\[ g(\gamma_1, \gamma_2, \ldots, \gamma_k) = m \]
WHERE\(g\)ISUNIQUELYINVERTIBLEWITH
RESPECTTOEACHONEOFITSINPUTS
A TECHNICAL PROBLEM:
- Each user has a different domain $[0,m_i]$.
- Encryptions have another domain $[0,2^b_i]$.

To unify the domains:
- Set $b = \max(m_1, m_2, \ldots, m_i, \ldots, m_k)$
- To sign a given $l$-bit $x$:
  $x = x_0 \cdot 1 + x_1 \cdot m_1 + x_2 \cdot m_2^2 + \ldots + x_j \cdot m_j^j$

Now sign separately each of $x_0 \ldots x_j-1$ 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:
- $x^2_i \equiv x_i \pmod{m_i}$
- Addition: $y_1 + y_2 + \ldots + y_k = m$ (over the integers)
- XOR: $y_1 \oplus y_2 \oplus \ldots \oplus y_k = m$ (as binary strings)
- Chaining: $P(y_{k\oplus(\oplus y_j \oplus P(y_k)))}$ (for a random permutation)

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 no 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 $3$ constants $c_1 < c_2$, s.t. $\forall$ horizontal lines, #solutions = $0 \lor c_1$
- $\forall$ vertical lines, #solutions = $0 \lor c_2$
- (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 $8$ marbles.

4 Buckets
- 0/8 marbles per bucket

3 Buckets
- 0/8 marbles per bucket
- [The proof fails if empty buckets make a single marble]
In our scheme:
\[ q(y_1, y_2, \ldots, y_k) = m, \quad y_i = x_i^e \pmod{m_i} \]

- 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 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:
   \[ m = x_1^2 + x_2^2 + x_3^2 + x_4^2 \pmod{m} \]
   If \( \forall i \, x_i^2 < m_i \), add formal moduli:
   \[ m = x_1^2 \pmod{m_1} + x_2^2 \pmod{m_2} + \ldots \]
   Countermeasures: invalidate when \( x_i \) are small, or use higher exponents.

2. Problem with XOR: prepare
   \[ x_1^2(m_1), x_2^2(m_2), \ldots, x_4^2(m_4), t \geq |m| \]
   Use linear algebra (mod 2) to find a subset of \( n \frac{|m|}{2} \) 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):

A linearized form of the ring:

\[ E_k \left[ S_k(m) \otimes \cdots \otimes E_k \left[ S_k(m) \otimes E_k \left[ S_k(m) \otimes \cdots \right] \right] \right] = v \]

The formula can be simplified for \( v = 0 \):
\[ S_k(m) \otimes \cdots \otimes E_k \left[ S_k(m) \otimes E_k \left[ S_k(m) \otimes \cdots \right] \right] = 0 \]

Each user \( i \) can solve it by fixing
\[ S_1, S_2, \ldots, S_{i-1}, S_{i+1}, \ldots, S_k \]
and solving for \( S_i \):
\[ S_i^2(m_i) \otimes E_i \left[ S_i^2(m_i) \otimes E_i \left[ \cdots \right] \right] = E_i \left[ S_i(m_i) \right] \]
which has the general form:
\[ S_i^2(m_i) = D_i \left[ \cdots \right] \otimes E_i \left[ \cdots \right] \]

We call this process GAP Bridging.
SPECIAL CASES:

A RANDOMIZED RSA SCHEME:

\[ E_k(m) \oplus S^2(m) = H(m) \]

WHEN THIS IS FORCED TO ZERO:

\[ E_k(m)[0] \oplus S^2(m) = 0 \Rightarrow S^2(m) = H(m) \]

A DESIGNATED VERIFIER SIGNATURE SCHEME:

\[ S^2(m_{\text{sender}}) \rightarrow E_k \rightarrow S^2(m_{\text{receiver}}) \]

WHEN THIS IS FORCED TO ZERO:

\[ S^2(m_2) = E_k[S^2(m_1)] \Rightarrow S^2(m_2) = D_k[H(m)] \]

- 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.

OUTLINE OF THE FORMAL PROOF OF SECURITY:

VERIFICATION CONDITION:

\[ \forall i \leq k, (x_i \oplus p(x_1 \oplus \ldots \oplus x_k) = m) \]

ASSUME THAT P IS IMPLEMENTED AS A RANDOM ORACLE

\[ R \rightarrow A \rightarrow p(x_1 \oplus \ldots \oplus x_k) \rightarrow B \]

ASSUME WLG: THE ORACLE IS ASKED EACH QUESTION ONCE

WE WANT TO TRANSFORM A TO B.

B USES A AS SUBROUTINE, AND PROVIDES ITS R AND P/P' INPUTS

\[ \text{FACTORIZATION OF ONE OF THE } m_i \]

CONSIDER THE SEQUENCE OF ORACLE CALLS:

\[ p(z_1), p'(z_2), p(z_3), p(z_4), \ldots, p'(z_k) \]

GIVEN THE FINAL SIGNATURE \( x_1, x_2, \ldots, x_k \)
WE CAN IDENTIFY THE k USEFUL CALLS.

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

\[ x_i^2 (m \cdot m_i) \oplus p(v') = p^{-1}(v'') \]

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

ASSUME THAT \( p(v') = w' \) IS THE LAST USEFUL CALL, AND \( p''(v') = w'' \) 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: \( w' \oplus w'' = x_i^2 (m \cdot m_i) \) GIVEN \( x_i, m, m_i \).
THE OVERALL STRATEGY:
- GUESS WHICH MODULUS $m_i$ WILL BE INVOLVED IN THE CRUCIAL CALL.
- PREPARE A RANDOM SQUARE $r^2 \mod m_i$.
- GUESS THE CALL WHICH WILL BE CRUCIAL.
- GUESS THE CALL WHICH WILL BE LAST BUT ONE.
- RUN THE ALGORITHM WITH RANDOM ORACLE VALUES, EXCEPT AT THE CRUCIAL STEP:
$$p(x_1), p(x_2), p'(x_3), p(x_4), p'(x_5), p(x_6)$$
- USEFUL, USELESS, LAST BUT ONE ($w^*$), USELESS, USELESS, CRUCIAL ($w'$).
- ANSWER WITH $w' = w^* \mod m_i$.

- 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 $m_i$.

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 $y_i$ SO THAT THEY LIE ON A LOW DEGREE POLYNOMIAL ($d = m - t$).
- DESIGNATED VERIFIER SIGNATURE SCHEME:
  THE SENDER SIGNS WITH GROUP {SENDER, RECEIVER}.
  [ALL CRUCIAL EMAIL SHOULD BE SIGNED THIS WAY!]
- TURNING SUCH SIGNATURES TO REAL SIGNATURES:
  REVEAL (OR ESROW) THE RECEIVER'S INNOCENCE.