Proving tight security for Rabin–Williams signatures

D. J. Bernstein
University of Illinois at Chicago

Thanks to:
NSF CCR–9983950
NSF DMS–0140542
NSF ITR–0716498
Alfred P. Sloan Foundation

Warning: Springer mangled the bibliography, labels, et al. Please use non-mangled paper:
`cr.yp.to/papers.html#rwtight`

Part 1: simulators

1993 Bellare–Rogaway
prove loose reduction:
hash-generic attack on RSA
$\Rightarrow$ computing eth roots.

1996 Bellare–Rogaway
prove *tight* reduction:
hash-generic attack on RSA
with large hash randomization
$\Rightarrow$ computing eth roots.

Signature of m under key pq is
(r, s) where $s^e - H(r, m) \in pq\mathbf{Z}$.
Signer chooses long random r.

Rabin signature system:
more complicated than RSA
but provides faster verification.

1996 Bellare–Rogaway
outline tight reduction:
hash-generic attack on Rabin
with large hash randomization
and *unstructured* square roots
$\Rightarrow$ factorization.

"SignPRab . . .
returns a random square root . . .
We stress that a random root is
chosen; a fixed root won't do."

But most papers and software specify *principal* square roots: square roots that are squares. Or sometimes |principal|; marginally more complicated but saves a bit of space.

Given distinct primes $p, q \in 3 + 4\mathbf{Z}$ and a square h modulo pq: compute $h^{(p+1)/4} \bmod p$; compute $h^{(q+1)/4} \bmod q$; combine $\rightarrow$ principal $\sqrt{h} \bmod pq$.

Are implementors willing to randomize the $\sqrt{h}$? Unclear.

Furthermore, Rabin is obsolete.

Rabin–Williams signature system:
more complicated than Rabin
but provides faster signing.

Rabin verifier checks that
s is a square root of $h = H(r, m)$.
Signer has to find square h.

Rabin–Williams verifier
checks that (e, f, s) is a
tweaked square root of h:
$e \in \{-1, 1\}$, $f \in \{1, 2\}$,
and $efs^2 - h \in pq\mathbf{Z}$.
Require $p \in 3 + 8\mathbf{Z}$, $q \in 7 + 8\mathbf{Z}$.
Now every h works.

2000 Bernstein posting
(incorporated into this paper)
proves tight reduction:
hash-generic attack on RW
with large hash randomization
and |principal| tweaked $\sqrt{h}$
$\Rightarrow$ factorization.

Main work in proof:
simulate RW signer.
Given public key,
generate uniform random h
and |principal| tweaked $\sqrt{h}$.

Part 2: 1-bit randomization

Are implementors willing
to randomize hashes? Unclear.
Space; time; complication.

1997 Barwood, 1997 Wigley:
"Why not [secretly]
derive the random number
from the message to be signed?"
Still some costs
but somewhat more palatable.

Now have a **fixed** signer:
signer generates same signature
if message is signed again.

2003 Katz–Wang
prove tight reduction:
hash-generic attack on RSA with
fixed 1-bit hash randomization
$\Rightarrow$ computing eth roots.

Signer secretly derives
unpredictable bit r from m;
$h = H(r, m)$; $s = h^{1/e} \bmod pq$.

Clever new idea in proof:
simulate $H(r, m)$ honestly;
choose $H(1 - r, m)$ as a target.

Katz–Wang theorem is for all
"claw-free permutation pairs,"
not just RSA.

Can apply theorem to exponent-2
claw-free permutation pair from
1988 Goldwasser–Micali–Rivest.
Oops, very slow verification:
receiver checks Jacobi symbols.

Drop Jacobi symbol?
Then receiver's squaring is fast
but isn't a permutation!
Can't apply theorem.

2003 Bernstein posting
(incorporated into this paper)
proves tight reduction:
hash-generic attack on RW with
fixed 1-bit hash randomization
and $|\text{principal}|$ tweaked $\sqrt{h}$
$\Rightarrow$ factorization.

Generalizes Katz–Wang idea
beyond “permutation pairs”;
combines with RW simulator.

Part 3: 0-bit randomization

2004 Koblitz–Menezes conjecture: hash-generic attack on RSA-FDH (i.e., 0-bit hash randomization) is no easier than eth roots, and no easier than factoring.

2002 Coron:
"FDH cannot be proven as secure as inverting RSA."

2004 Koblitz–Menezes: "It is not reasonable to hope for a tight reduction" given Coron's theorem; but still hope for equal security.

2006.11 Bernstein posting (incorporated into this paper) proves tight reduction: hash-generic attack on RW with 0-bit hash randomization and fixed unstructured tweaked $\sqrt{h}$ $\Rightarrow$ factorization.

2007.11 posting by Gentry–Peikert–Vaikuntanathan (part of a STOC 2008 paper) proves tight reduction for more general FDH systems.

Are implementors willing
to use this system? Unclear!
Still some $\sqrt{h}$ complication.

Conjecture:
hash-generic attack on RW
with 0-bit hash randomization
and $|$principal$|$ tweaked $\sqrt{h}$
is no easier than factorization.

Coron's theorem seems to prohibit
tight black-box reduction;
but still hope for equal security.

Appendix

See companion paper
"RSA signatures and
Rabin-Williams signatures:
the state of the art"
for further discussion of
implementation options:
verification faster than squaring,
compressing keys to 1/3 size,
avoiding Euclid, et al.

`cr.yp.to/papers.html#rwsota`

Why don't these new theorems contradict 2002 Coron? How can FDH have tight security?

Answer: Coron's theorem assumes "unique" signatures. This is not a technicality!

Coron uses reduction
to simulate many signatures;
then rewinds reduction,
feeds it one signature.
Applied to my RW reduction,
this signature doesn't
accurately simulate forgery,
and doesn't find p and q.

I submitted this paper
to Crypto 2007.

Rejected because of prior art.
Comment from the reviewer:
"I was really flabbergasted by the
idea that this simple observation
had escaped the community
for so long. So I just spent
a few minutes on google . . .
K.Kurosawa, W.Ogata 'Efficient
Rabin-type Digital Signature
Schemes' Designs, Codes and
Cryptography, 16(1) 1999 . . .
They don't make a big deal
about it, but they do prove it."

Crypto 2007 program committee later retracted all of these claims of prior art.

Me: “Does everyone agree that the Kurosawa-Ogata ‘proof’ is wrong?”

Official PC response: “Yes.”

Me: “Does anyone see a way to prove the ‘theorem’ claimed by Kurosawa and Ogata?”

Official PC response: “No.”

1999 Kurosawa–Ogata "theorem"
is my 2006.11 theorem? No!

They claim tight reduction:
hash-generic attack on RW
with 0-bit hash randomization
and principal tweaked $\sqrt{h}$
$\Rightarrow$ factorization.

Proof is fatally flawed.
Simulator doesn't work.

2007.02 Ogata–Matsumoto
(independently of my 2006 work)
point out flaw in 1999 "proof."
Still no erratum in the journal
that published the 1999 paper.