Signature sizes:
a call to action

D. J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

RSA signatures are big.

Signature sizes: a call to action

D. J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

RSA signatures are big.

1990 Schnorr signatures are much smaller: $3n$ bits for security 2^n.

Often misquoted as $4n$ bits; e.g., 2009 Neven–Smart–Warinschi claims to improve Schnorr from $4n$ to $3n$ ("saving twenty-five percent in signature size").

Signature sizes: a call to action

D. J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

RSA signatures are big.

1990 Schnorr signatures are much smaller: $3n$ bits for security 2^n.

Often misquoted as $4n$ bits; e.g., 2009 Neven–Smart–Warinschi claims to improve Schnorr from $4n$ to $3n$ ("saving twenty-five percent in signature size").

2001 Boneh–Lynn–Shacham pairing-based "short signatures": $2n$ bits.

re sizes:

action

ernstein

ty of Illinois at Chicago &

che Universiteit Eindhoven

RSA signatures are big.

1990 Schnorr signatures
are much smaller:
$3n$ bits for security 2^n.

Often misquoted as $4n$ bits;
e.g., 2009 Neven–Smart–
Warinschi claims to improve
Schnorr from $4n$ to $3n$
("saving twenty-five percent
in signature size").

2001 Boneh–Lynn–Shacham
pairing-based "short signatures":
$2n$ bits.

1996 Pa

2001 Pa
"Quartz"

"Very sh
asymmet

Also ach
MQ sign
often wi
but HFE
and insp

Further
at exper
verificati

is at Chicago &
siteit Eindhoven

RSA signatures are big.

1990 Schnorr signatures
are much smaller:
$3n$ bits for security 2^n.

Often misquoted as $4n$ bits;
e.g., 2009 Neven–Smart–
Warinschi claims to improve
Schnorr from $4n$ to $3n$
("saving twenty-five percent
in signature size").

2001 Boneh–Lynn–Shacham
pairing-based "short signatures":
$2n$ bits.

1996 Patarin "HF
2001 Patarin–Cou
"Quartz": n bits.

"Very short
asymmetric signat

Also achieved by
MQ signature sch
often with smaller
but HFEv- has a l
and inspires confi

Further save, e.g.,
at expense of mul
verification cost b

ago &
hoven

RSA signatures are big.

1990 Schnorr signatures
are much smaller:
$3n$ bits for security 2^n.

Often misquoted as $4n$ bits;
e.g., 2009 Neven–Smart–
Warinschi claims to improve
Schnorr from $4n$ to $3n$
("saving twenty-five percent
in signature size").

2001 Boneh–Lynn–Shacham
pairing-based "short signatures":
$2n$ bits.

1996 Patarin "HFEv-",
2001 Patarin–Courtois–Goub
"Quartz": n bits.

"Very short
asymmetric signatures".

Also achieved by many othe
MQ signature schemes,
often with smaller keys;
but HFEv- has a long histor
and inspires confidence.

Further save, e.g., 10 bits
at expense of multiplying
verification cost by $\leq 2^{10}$.

RSA signatures are big.

1990 Schnorr signatures
are much smaller:
$3n$ bits for security 2^n.

Often misquoted as $4n$ bits;
e.g., 2009 Neven–Smart–
Warinschi claims to improve
Schnorr from $4n$ to $3n$
("saving twenty-five percent
in signature size").

2001 Boneh–Lynn–Shacham
pairing-based "short signatures":
$2n$ bits.

1996 Patarin "HFEv-",
2001 Patarin–Courtois–Goubin
"Quartz": n bits.

"Very short
asymmetric signatures".

Also achieved by many other
MQ signature schemes,
often with smaller keys;
but HFEv- has a long history
and inspires confidence.

Further save, e.g., 10 bits
at expense of multiplying
verification cost by $\leq 2^{10}$.

natures are big.

hnorr signatures
h smaller:
for security 2^n.

isquoted as $4n$ bits;
09 Neven–Smart–
hi claims to improve
from $4n$ to $3n$
twenty-five percent
ture size").

oneh–Lynn–Shacham
based "short signatures":

1996 Patarin "HFEv-",
2001 Patarin–Courtois–Goubin
"Quartz": n bits.

"Very short
asymmetric signatures".

Also achieved by many other
MQ signature schemes,
often with smaller keys;
but HFEv- has a long history
and inspires confidence.

Further save, e.g., 10 bits
at expense of multiplying
verification cost by $\leq 2^{10}$.

"Messag
signatur
Measure
signatur
Often $4n$

Many pa
message

1993 Ny
2000 Pi
2001 Na
message
Deploym

e big.

atures

y 2^n.

as $4n$ bits;
Smart–
o improve
o $3n$
ve percent
.

–Shacham
ort signatures”:

1996 Patarin “HFEv-”,
2001 Patarin–Courtois–Goubin
“Quartz”: n bits.

“Very short
asymmetric signatures”.

Also achieved by many other
MQ signature schemes,
often with smaller keys;
but HFEv- has a long history
and inspires confidence.

Further save, e.g., 10 bits
at expense of multiplying
verification cost by $\leq 2^{10}$.

“Message recovery
signature conveys
Measure “signatur
signature size – m
Often $4n$ or $3n$, s

Many papers/stan
message recovery

1993 Nyberg–Ruep
2000 Pintsov–Van
2001 Naccache–St
message recovery
Deployment stopp

res”:

1996 Patarin “HFEv-”,
2001 Patarin–Courtois–Goubin
“Quartz”: n bits.

“Very short
asymmetric signatures”.

Also achieved by many other
MQ signature schemes,
often with smaller keys;
but HFEv- has a long history
and inspires confidence.

Further save, e.g., 10 bits
at expense of multiplying
verification cost by $\leq 2^{10}$.

“Message recovery”:
signature conveys message.
Measure “signature overhea
signature size − message siz
Often $4n$ or $3n$, sometimes

Many papers/standards:
message recovery for RSA.

1993 Nyberg–Rueppel,
2000 Pintsov–Vanstone,
2001 Naccache–Stern:
message recovery for ECDS
Deployment stopped by pat

1996 Patarin "HFEv-",
2001 Patarin–Courtois–Goubin
"Quartz": n bits.

"Very short
asymmetric signatures".

Also achieved by many other
MQ signature schemes,
often with smaller keys;
but HFEv- has a long history
and inspires confidence.

Further save, e.g., 10 bits
at expense of multiplying
verification cost by $\leq 2^{10}$.

"Message recovery":
signature conveys message.
Measure "signature overhead":
signature size − message size.
Often $4n$ or $3n$, sometimes $2n$.

Many papers/standards:
message recovery for RSA.

1993 Nyberg–Rueppel,
2000 Pintsov–Vanstone,
2001 Naccache–Stern:
message recovery for ECDSA.
Deployment stopped by patents.

tarin "HFEv-",
tarin–Courtois–Goubin
": n bits.

hort
tric signatures".

hieved by many other
nature schemes,
th smaller keys;
Ev- has a long history
ires confidence.

save, e.g., 10 bits
se of multiplying
ion cost by $\leq 2^{10}$.

"Message recovery":
signature conveys message.
Measure "signature overhead":
signature size − message size.
Often $4n$ or $3n$, sometimes $2n$.

Many papers/standards:
message recovery for RSA.

1993 Nyberg–Rueppel,
2000 Pintsov–Vanstone,
2001 Naccache–Stern:
message recovery for ECDSA.
Deployment stopped by patents.

Latest m
2012 Ki
"Digital
minimal
will appe

"Our ma
revisit th
exists a
scheme
that has
overhead
previous
required

Ev-”,
rtois–Goubin

ures”.

many other
emes,
keys;
ong history
dence.

10 bits
tiplying
$y \leq 2^{10}$.

“Message recovery”:
signature conveys message.
Measure “signature overhead”:
signature size − message size.
Often $4n$ or $3n$, sometimes $2n$.

Many papers/standards:
message recovery for RSA.

1993 Nyberg–Rueppel,
2000 Pintsov–Vanstone,
2001 Naccache–Stern:
message recovery for ECDSA.
Deployment stopped by patents.

Latest message-re
2012 Kiltz–Pietrza
“Digital signature
minimal overhead”
will appear at Cry

“Our main contrib
revisit the questio
exists a digital sig
scheme with mess
that has minimal
overhead. . . . The
previous construct
required an overhe

bin

r

y

"Message recovery":
signature conveys message.
Measure "signature overhead":
signature size − message size.
Often $4n$ or $3n$, sometimes $2n$.

Many papers/standards:
message recovery for RSA.

1993 Nyberg–Rueppel,
2000 Pintsov–Vanstone,
2001 Naccache–Stern:
message recovery for ECDSA.
Deployment stopped by patents.

Latest message-recovery pap
2012 Kiltz–Pietrzak–Szegedy
"Digital signatures with
minimal overhead". Rumor:
will appear at Crypto 2013.

"Our main contribution is to
revisit the question if there
exists a digital signature
scheme with message recove
that has minimal ($\approx n$ bits)
overhead. ... The best
previous constructions
required an overhead of $2n$."

"Message recovery":
signature conveys message.
Measure "signature overhead":
signature size − message size.
Often $4n$ or $3n$, sometimes $2n$.

Many papers/standards:
message recovery for RSA.

1993 Nyberg–Rueppel,
2000 Pintsov–Vanstone,
2001 Naccache–Stern:
message recovery for ECDSA.
Deployment stopped by patents.

Latest message-recovery paper:
2012 Kiltz–Pietrzak–Szegedy
"Digital signatures with
minimal overhead". Rumor:
will appear at Crypto 2013.

"Our main contribution is to
revisit the question if there
exists a digital signature
scheme with message recovery
that has minimal ($\approx n$ bits)
overhead. ... The best
previous constructions
required an overhead of $2n$."

ge recovery":
e conveys message.
e "signature overhead":
e size − message size.
n or $3n$, sometimes $2n$.

apers/standards:
recovery for RSA.

yberg–Rueppel,
ntsov–Vanstone,
ccache–Stern:
recovery for ECDSA.
nent stopped by patents.

Latest message-recovery paper:
2012 Kiltz–Pietrzak–Szegedy
"Digital signatures with
minimal overhead". Rumor:
will appear at Crypto 2013.

"Our main contribution is to
revisit the question if there
exists a digital signature
scheme with message recovery
that has minimal ($\approx n$ bits)
overhead. ... The best
previous constructions
required an overhead of $2n$."

Conclusi

1. Many
signatur

y":
message.
re overhead":
nessage size.
ometimes $2n$.

dards:
for RSA.

ppel,
stone,
tern:
for ECDSA.
ed by patents.

Latest message-recovery paper: 2012 Kiltz–Pietrzak–Szegedy "Digital signatures with minimal overhead". Rumor: will appear at Crypto 2013.

"Our main contribution is to revisit the question if there exists a digital signature scheme with message recovery that has minimal ($\approx n$ bits) overhead. ... The best previous constructions required an overhead of $2n$."

Conclusions:

1. Many people ca
signature size.

d":
ze.
$2n$.

A.
ents.

Latest message-recovery paper: 2012 Kiltz–Pietrzak–Szegedy "Digital signatures with minimal overhead". Rumor: will appear at Crypto 2013.

"Our main contribution is to revisit the question if there exists a digital signature scheme with message recovery that has minimal ($\approx n$ bits) overhead. ... The best previous constructions required an overhead of $2n$."

Conclusions:

1. Many people care about signature size.

Latest message-recovery paper: 2012 Kiltz–Pietrzak–Szegedy "Digital signatures with minimal overhead". Rumor: will appear at Crypto 2013.

"Our main contribution is to revisit the question if there exists a digital signature scheme with message recovery that has minimal ($\approx n$ bits) overhead. ... The best previous constructions required an overhead of $2n$."

Conclusions:

1. Many people care about signature size.

Latest message-recovery paper: 2012 Kiltz–Pietrzak–Szegedy "Digital signatures with minimal overhead". Rumor: will appear at Crypto 2013.

"Our main contribution is to revisit the question if there exists a digital signature scheme with message recovery that has minimal ($\approx n$ bits) overhead. ... The best previous constructions required an overhead of $2n$."

Conclusions:

1. Many people care about signature size.

2. Many people are shockingly ignorant of short MQ signatures.

Latest message-recovery paper:
2012 Kiltz–Pietrzak–Szegedy
"Digital signatures with
minimal overhead". Rumor:
will appear at Crypto 2013.

"Our main contribution is to
revisit the question if there
exists a digital signature
scheme with message recovery
that has minimal ($\approx n$ bits)
overhead. ... The best
previous constructions
required an overhead of $2n$."

Conclusions:

1. Many people care about
signature size.

2. Many people are shockingly
ignorant of short MQ signatures.

3. Need to raise awareness
of MQ capabilities.
e.g. add Quartz to eBATS.
http://bench.cr.yp.to