Security dangers of the NIST curves

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

Joint work with:

Tanja Lange
Technische Universiteit Eindhoven

The NIST curves were designed to make DLP difficult.

Or were they?

"ECC Brainpool Standard Curves and Curve Generation version 1.0", 2005.10.19: "The choice of the seeds from which the curve parameters have been derived is not motivated leaving an essential part of the security analysis open."

Security dangers of the NIST curves

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

Joint work with:

Tanja Lange
Technische Universiteit Eindhoven

The NIST curves were designed to make DLP difficult.

Or were they?

"ECC Brainpool Standard Curves and Curve Generation version 1.0", 2005.10.19: "The choice of the seeds from which the curve parameters have been derived is not motivated leaving an essential part of the security analysis open."

Bruce Schneier, "NSA surveillance: A guide to staying secure", The Guardian, 2013.09.06: "Prefer conventional discrete-log-based systems over elliptic-curve systems; the latter have constants that the NSA influences when they can."

dangers
IST curves

ernstein
ty of Illinois at Chicago &
che Universiteit Eindhoven

ork with:

ange
che Universiteit Eindhoven

T curves were designed
DLP difficult.

they?

"ECC Brainpool Standard Curves and Curve Generation version 1.0", 2005.10.19: "The choice of the seeds from which the curve parameters have been derived is not motivated leaving an essential part of the security analysis open."

Bruce Schneier, "NSA surveillance: A guide to staying secure", The Guardian, 2013.09.06: "Prefer conventional discrete-log-based systems over elliptic-curve systems; the latter have constants that the NSA influences when they can."

But that
As far as
NIST-cu

s

is at Chicago &
siteit Eindhoven

siteit Eindhoven

---

were designed
cult.

"ECC Brainpool Standard Curves and Curve Generation version 1.0", 2005.10.19: "The choice of the seeds from which the curve parameters have been derived is not motivated leaving an essential part of the security analysis open."

Bruce Schneier, "NSA surveillance: A guide to staying secure", The Guardian, 2013.09.06: "Prefer conventional discrete-log-based systems over elliptic-curve systems; the latter have constants that the NSA influences when they can."

But that's not our
As far as we know
NIST-curve DLP i

ago &
hoven

hoven

ned

"ECC Brainpool Standard Curves and Curve Generation version 1.0", 2005.10.19: "The choice of the seeds from which the curve parameters have been derived is not motivated leaving an essential part of the security analysis open."

Bruce Schneier, "NSA surveillance: A guide to staying secure", The Guardian, 2013.09.06: "Prefer conventional discrete-log-based systems over elliptic-curve systems; the latter have constants that the NSA influences when they can."

But that's not our main poi
As far as we know today,
NIST-curve DLP is secure.

"ECC Brainpool Standard Curves and Curve Generation version 1.0", 2005.10.19: "The choice of the seeds from which the curve parameters have been derived is not motivated leaving an essential part of the security analysis open."

Bruce Schneier, "NSA surveillance: A guide to staying secure", The Guardian, 2013.09.06: "Prefer conventional discrete-log-based systems over elliptic-curve systems; the latter have constants that the NSA influences when they can."

But that's not our main point. As far as we know today, NIST-curve DLP is secure.

"ECC Brainpool Standard Curves and Curve Generation version 1.0", 2005.10.19: "The choice of the seeds from which the curve parameters have been derived is not motivated leaving an essential part of the security analysis open."

Bruce Schneier, "NSA surveillance: A guide to staying secure", The Guardian, 2013.09.06: "Prefer conventional discrete-log-based systems over elliptic-curve systems; the latter have constants that the NSA influences when they can."

But that's not our main point. As far as we know today, NIST-curve DLP is secure.

Here's our main point:
NIST-curve ECC is much less secure than NIST-curve DLP.

"ECC Brainpool Standard Curves and Curve Generation version 1.0", 2005.10.19: "The choice of the seeds from which the curve parameters have been derived is not motivated leaving an essential part of the security analysis open."

Bruce Schneier, "NSA surveillance: A guide to staying secure", The Guardian, 2013.09.06: "Prefer conventional discrete-log-based systems over elliptic-curve systems; the latter have constants that the NSA influences when they can."

But that's not our main point. As far as we know today, NIST-curve DLP is secure.

Here's our main point: **NIST-curve ECC is much less secure than NIST-curve DLP.**

If you use the NIST curves, you're probably doing it wrong.

Your code produces incorrect results for some rare curve points; leaks secret data when the input isn't a curve point; leaks secret data through cache timing; etc.

rainpool Standard Curves
ve Generation version
05.10.19: "The choice
eeds from which the curve
ers have been derived is
ivated leaving an essential
he security analysis open."

chneier, "NSA
nce: A guide to
secure", The Guardian,
06: "Prefer conventional
-log-based systems over
curve systems; the latter
nstants that the NSA
es when they can."

But that's not our main point.
As far as we know today,
NIST-curve DLP is secure.

Here's our main point:
NIST-curve ECC is much less secure than NIST-curve DLP.

If you use the NIST curves,
you're probably doing it wrong.

Your code produces incorrect results for some rare curve points; leaks secret data when the input isn't a curve point; leaks secret data through cache timing; etc.

These pr
exploitab

These at
real prot

DLP is r
compute
reveals c

Real pro
handle a
have fail
reveal ti

Attacker

tandard Curves
tion version
"The choice
which the curve
een derived is
ving an essential
y analysis open."

NSA
ide to
he Guardian,
er conventional
systems over
ms; the latter
at the NSA
ney can."

But that's not our main point.
As far as we know today,
NIST-curve DLP is secure.

Here's our main point:
NIST-curve ECC is much less secure than NIST-curve DLP.

If you use the NIST curves,
you're probably doing it wrong.

Your code produces incorrect results for some rare curve points; leaks secret data when the input isn't a curve point; leaks secret data through cache timing; etc.

These problems ar
exploitable by atta

These attacks are
real protocols, not

DLP is non-interac
computes nP corr
reveals only nP.

Real protocols
handle attacker-co
have failure cases;
reveal timing.

Attacker exploits t

urves
on
ice
curve
ed is
sential
open."

an,
tional
over
tter
A

But that's not our main point.
As far as we know today,
NIST-curve DLP is secure.

Here's our main point:
NIST-curve ECC is much less secure than NIST-curve DLP.

If you use the NIST curves,
you're probably doing it wrong.

Your code produces incorrect results for some rare curve points; leaks secret data when the input isn't a curve point; leaks secret data through cache timing; etc.

These problems are exploitable by attackers.

These attacks are against real protocols, not against D

DLP is non-interactive; computes nP correctly; reveals only nP.

Real protocols
handle attacker-controlled in
have failure cases;
reveal timing.

Attacker exploits these gaps

But that's not our main point.
As far as we know today,
NIST-curve DLP is secure.

Here's our main point:
NIST-curve ECC is much less secure than NIST-curve DLP.

If you use the NIST curves,
you're probably doing it wrong.

Your code produces incorrect
results for some rare curve points;
leaks secret data when the input
isn't a curve point; leaks secret
data through cache timing; etc.

These problems are
exploitable by attackers.

These attacks are against
real protocols, not against DLP.

DLP is non-interactive;
computes nP correctly;
reveals only nP.

Real protocols
handle attacker-controlled input;
have failure cases;
reveal timing.

Attacker exploits these gaps.

t's not our main point.
s we know today,
urve DLP is secure.

ur main point:
urve ECC is much less
than NIST-curve DLP.

se the NIST curves,
robably doing it wrong.

de produces incorrect
or some rare curve points;
cret data when the input
urve point; leaks secret
ough cache timing; etc.

These problems are
exploitable by attackers.

These attacks are against
real protocols, not against DLP.

DLP is non-interactive;
computes nP correctly;
reveals only nP.

Real protocols
handle attacker-controlled input;
have failure cases;
reveal timing.

Attacker exploits these gaps.

Can NIS
Theoreti
highly fr
of limite

r main point.
today,
s secure.

oint:
is much less
T-curve DLP.

T curves,
oing it wrong.

es incorrect
are curve points;
when the input
; leaks secret
e timing; etc.

These problems are
exploitable by attackers.

These attacks are against
real protocols, not against DLP.

DLP is non-interactive;
computes nP correctly;
reveals only nP.

Real protocols
handle attacker-controlled input;
have failure cases;
reveal timing.

Attacker exploits these gaps.

Can NIST-curve E
Theoretically, but
highly fragile; unin
of limited security

nt.

less
DLP.

ng.

t
oints;
nput
cret
etc.

These problems are
exploitable by attackers.

These attacks are against
real protocols, not against DLP.

DLP is non-interactive;
computes nP correctly;
reveals only nP.

Real protocols
handle attacker-controlled input;
have failure cases;
reveal timing.

Attacker exploits these gaps.

Can NIST-curve ECC be saf
Theoretically, but hard to do
highly fragile; unintelligent u
of limited security resources.

These problems are
exploitable by attackers.

These attacks are against
real protocols, not against DLP.

DLP is non-interactive;
computes nP correctly;
reveals only nP.

Real protocols
handle attacker-controlled input;
have failure cases;
reveal timing.

Attacker exploits these gaps.

Can NIST-curve ECC be safe?
Theoretically, but hard to do;
highly fragile; unintelligent use
of limited security resources.

These problems are
exploitable by attackers.

These attacks are against
real protocols, not against DLP.

DLP is non-interactive;
computes nP correctly;
reveals only nP.

Real protocols
handle attacker-controlled input;
have failure cases;
reveal timing.

Attacker exploits these gaps.

Can NIST-curve ECC be safe?
Theoretically, but hard to do;
highly fragile; unintelligent use
of limited security resources.

Sensible security engineering:
**Design curves for ECC security,
not just for DLP security.**

These problems are
exploitable by attackers.

These attacks are against
real protocols, not against DLP.

DLP is non-interactive;
computes nP correctly;
reveals only nP.

Real protocols
handle attacker-controlled input;
have failure cases;
reveal timing.

Attacker exploits these gaps.

Can NIST-curve ECC be safe?
Theoretically, but hard to do;
highly fragile; unintelligent use
of limited security resources.

Sensible security engineering:
**Design curves for ECC security,
not just for DLP security.**

Detailed analysis online now
(+ white paper coming soon):
cr.yp.to/talks/2013.05.31
/slides-dan+tanja
-20130531-4x3.pdf

These problems are
exploitable by attackers.

These attacks are against
real protocols, not against DLP.

DLP is non-interactive;
computes nP correctly;
reveals only nP.

Real protocols
handle attacker-controlled input;
have failure cases;
reveal timing.

Attacker exploits these gaps.

Can NIST-curve ECC be safe?
Theoretically, but hard to do;
highly fragile; unintelligent use
of limited security resources.

Sensible security engineering:
**Design curves for ECC security,
not just for DLP security.**

Detailed analysis online now
(+ white paper coming soon):
cr.yp.to/talks/2013.05.31
/slides-dan+tanja
-20130531-4x3.pdf

⇒ Use Curve25519.

These problems are
exploitable by attackers.

These attacks are against
real protocols, not against DLP.

DLP is non-interactive;
computes nP correctly;
reveals only nP.

Real protocols
handle attacker-controlled input;
have failure cases;
reveal timing.

Attacker exploits these gaps.

Can NIST-curve ECC be safe?
Theoretically, but hard to do;
highly fragile; unintelligent use
of limited security resources.

Sensible security engineering:
**Design curves for ECC security,
not just for DLP security.**

Detailed analysis online now
(+ white paper coming soon):
cr.yp.to/talks/2013.05.31
/slides-dan+tanja
-20130531-4x3.pdf

$\Rightarrow$ Use Curve25519. Or $x^2+y^2 = 1+3617x^2y^2 \bmod 2^{414}-17$.