Complexity news:
discrete logarithms in multiplicative groups of small-characteristic finite fields—the algorithm of Barbulescu, Gaudry, Joux, Thomé

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

Also somewhat related:

I'm starting to analyze cost of NFS + CVP for class groups, unit groups, short generators of ideals, etc.; exploiting subfields (find short *norms* first), small Galois groups, etc.
Anyone else working on this?

Cryptanalytic applications: attack NTRU, Ring-LWE, FHE.
I think NTRU should switch to random prime-degree extensions with big Galois groups.

kity news:
logarithms in
cative groups of
aracteristic finite fields—
rithm of Barbulescu,
Joux, Thomé

ernstein
ty of Illinois at Chicago &
che Universiteit Eindhoven

---

ement, maybe related:
iv-mrs.fr/ati/
ot2013/
.07–11, Tahiti.
talks this month!

Also somewhat related:

I'm starting to analyze
cost of NFS + CVP
for class groups, unit groups,
short generators of ideals, etc.;
exploiting subfields
(find short *norms* first),
small Galois groups, etc.
Anyone else working on this?

Cryptanalytic applications:
attack NTRU, Ring-LWE, FHE.
I think NTRU should switch to
random prime-degree extensions
with big Galois groups.

Discrete

Goal: C
group is
$\mathbf{F}_q^* \to \mathbf{Z}$
represen

Algorith
$h_1, h_2, .$

Algorith
$\log_g h_1,$
for some

"$\log_g$" n
$g \mapsto 1$, i

s in
ups of
c finite fields—
Barbulescu,
omé

is at Chicago &
siteit Eindhoven

---

aybe related:
r/ati/

ahiti.
month!

Also somewhat related:

I'm starting to analyze
cost of NFS + CVP
for class groups, unit groups,
short generators of ideals, etc.;
exploiting subfields
(find short *norms* first),
small Galois groups, etc.
Anyone else working on this?

Cryptanalytic applications:
attack NTRU, Ring-LWE, FHE.
I think NTRU should switch to
random prime-degree extensions
with big Galois groups.

Discrete logarithm

Goal: Compute so
group isomorphism
$\mathbf{F}_q^* \to \mathbf{Z}/(q-1)$,
represented in the

Algorithm input:
$h_1, h_2, \ldots \in \mathbf{F}_q^*$.

Algorithm output:
$\log_g h_1, \log_g h_2, \ldots$
for some g.

"$\log_g$" means the
$g \mapsto 1$, if it exists.

lds—

/

ago &

hoven

ed:

Also somewhat related:

I'm starting to analyze
cost of NFS + CVP
for class groups, unit groups,
short generators of ideals, etc.;
exploiting subfields
(find short *norms* first),
small Galois groups, etc.
Anyone else working on this?

Cryptanalytic applications:
attack NTRU, Ring-LWE, FHE.
I think NTRU should switch to
random prime-degree extensions
with big Galois groups.

Discrete logarithms

Goal: Compute some
group isomorphism
$\mathbf{F}_q^* \to \mathbf{Z}/(q-1)$,
represented in the usual way

Algorithm input:
$h_1, h_2, \ldots \in \mathbf{F}_q^*$.

Algorithm output:
$\log_g h_1, \log_g h_2, \ldots \in \mathbf{Z}/(q$
for some g.

"$\log_g$" means the isomorphi
$g \mapsto 1$, if it exists.

Also somewhat related:

I'm starting to analyze cost of NFS + CVP for class groups, unit groups, short generators of ideals, etc.; exploiting subfields (find short *norms* first), small Galois groups, etc. Anyone else working on this?

Cryptanalytic applications: attack NTRU, Ring-LWE, FHE. I think NTRU should switch to random prime-degree extensions with big Galois groups.

Discrete logarithms

Goal: Compute some group isomorphism $\mathbf{F}_q^* \to \mathbf{Z}/(q-1)$, represented in the usual way.

Algorithm input: $h_1, h_2, \ldots \in \mathbf{F}_q^*$.

Algorithm output: $\log_g h_1, \log_g h_2, \ldots \in \mathbf{Z}/(q-1)$ for some g.

"$\log_g$" means the isomorphism $g \mapsto 1$, if it exists.

newhat related:

ting to analyze
NFS + CVP
groups, unit groups,
nerators of ideals, etc.;
g subfields
ort *norms* first),
alois groups, etc.
else working on this?

alytic applications:
NTRU, Ring-LWE, FHE.
NTRU should switch to
prime-degree extensions
Galois groups.

Discrete logarithms

Goal: Compute some group isomorphism $\mathbf{F}_q^* \to \mathbf{Z}/(q-1)$, represented in the usual way.

Algorithm input: $h_1, h_2, \ldots \in \mathbf{F}_q^*$.

Algorithm output: $\log_g h_1, \log_g h_2, \ldots \in \mathbf{Z}/(q-1)$ for some g.

"$\log_g$" means the isomorphism $g \mapsto 1$, if it exists.

"Generic
on avera
uniform,
Want so

ated:

alyze
/P
nit groups,
f ideals, etc.;
s
first),
s, etc.
ng on this?

ications:
g-LWE, FHE.
uld switch to
ree extensions
oups.

Discrete logarithms

Goal: Compute some group isomorphism $\mathbf{F}_q^* \to \mathbf{Z}/(q-1)$, represented in the usual way.

Algorithm input: $h_1, h_2, \ldots \in \mathbf{F}_q^*$.

Algorithm output: $\log_g h_1, \log_g h_2, \ldots \in \mathbf{Z}/(q-1)$ for some g.

"$\log_g$" means the isomorphism $g \mapsto 1$, if it exists.

"Generic" $\log_g$ alg
on average $q^{1/2+o}$
uniform, $q^{1/3+o(1)}$
Want something f

s,
tc.;

?

HE.
to
ions

Discrete logarithms

Goal: Compute some group isomorphism $\mathbf{F}_q^* \to \mathbf{Z}/(q-1)$, represented in the usual way.

Algorithm input: $h_1, h_2, \ldots \in \mathbf{F}_q^*$.

Algorithm output: $\log_g h_1, \log_g h_2, \ldots \in \mathbf{Z}/(q-1)$ for some g.

"$\log_g$" means the isomorphism $g \mapsto 1$, if it exists.

"Generic" $\log_g$ algorithms:
on average $q^{1/2+o(1)}$ operati
uniform, $q^{1/3+o(1)}$ non-unifo
Want something faster.

Discrete logarithms

Goal: Compute some group isomorphism $\mathbf{F}_q^* \to \mathbf{Z}/(q-1)$, represented in the usual way.

Algorithm input: $h_1, h_2, \ldots \in \mathbf{F}_q^*$.

Algorithm output: $\log_g h_1, \log_g h_2, \ldots \in \mathbf{Z}/(q-1)$ for some g.

"$\log_g$" means the isomorphism $g \mapsto 1$, if it exists.

"Generic" $\log_g$ algorithms: on average $q^{1/2+o(1)}$ operations uniform, $q^{1/3+o(1)}$ non-uniform. Want something faster.

Discrete logarithms

Goal: Compute some group isomorphism $\mathbf{F}_q^* \to \mathbf{Z}/(q-1)$, represented in the usual way.

Algorithm input: $h_1, h_2, \ldots \in \mathbf{F}_q^*$.

Algorithm output: $\log_g h_1, \log_g h_2, \ldots \in \mathbf{Z}/(q-1)$ for some g.

"$\log_g$" means the isomorphism $g \mapsto 1$, if it exists.

"Generic" $\log_g$ algorithms: on average $q^{1/2+o(1)}$ operations uniform, $q^{1/3+o(1)}$ non-uniform. Want something faster.

"Basic index calculus": 1968 Western–Miller, 1979 Merkle, 1979 Adleman, 1983 Hellman–Reyneri, 1984 Blake–Fuji-Hara–Mullin–Vanstone, 1985 ElGamal, 1986 Coppersmith–Odlyzko–Schroeppel, 1991 LaMacchia–Odlyzko, 1993 Adleman–DeMarrais, 1995 Semaev, 1998 Bender–Pomerance.

logarithms

ompute some
omorphism
$/(q-1)$,
ted in the usual way.

m input:
$\ldots \in \mathbf{F}_q^*$.

m output:
$\log_g h_2, \ldots \in \mathbf{Z}/(q-1)$
e g.

neans the isomorphism
f it exists.

"Generic" $\log_g$ algorithms: on average $q^{1/2+o(1)}$ operations uniform, $q^{1/3+o(1)}$ non-uniform. Want something faster.

"Basic index calculus": 1968 Western–Miller, 1979 Merkle, 1979 Adleman, 1983 Hellman–Reyneri, 1984 Blake–Fuji-Hara–Mullin–Vanstone, 1985 ElGamal, 1986 Coppersmith–Odlyzko–Schroeppel, 1991 LaMacchia–Odlyzko, 1993 Adleman–DeMarrais, 1995 Semaev, 1998 Bender–Pomerance.

"NFS":
Gordon,
Odlyzko
Weber–D
1998 We
Lercier,
Smart–V

"FFS":
Coppers
Odlyzko
Gordon–
1999 Ad
Joux–Le
2010/20
Wang–M

s

ome

n

usual way.

. $\in \mathbf{Z}/(q-1)$

isomorphism

"Generic" $\log_g$ algorithms: on average $q^{1/2+o(1)}$ operations uniform, $q^{1/3+o(1)}$ non-uniform. Want something faster.

"Basic index calculus": 1968 Western–Miller, 1979 Merkle, 1979 Adleman, 1983 Hellman–Reyneri, 1984 Blake–Fuji-Hara–Mullin–Vanstone, 1985 ElGamal, 1986 Coppersmith–Odlyzko–Schroeppel, 1991 LaMacchia–Odlyzko, 1993 Adleman–DeMarrais, 1995 Semaev, 1998 Bender–Pomerance.

"NFS": 1991 Schi
Gordon, 1993 Schi
Odlyzko, 1996 Sch
Weber–Denny, 199
1998 Weber–Denn
Lercier, 2006 Joux
Smart–Vercautere

"FFS": 1984 Copp
Coppersmith–Dave
Odlyzko, 1990 Mc
Gordon–McCurley,
1999 Adleman–Hu
Joux–Lercier, 200
2010/2012 Hayash
Wang–Matsuo–Sh

v.

$-1)$

sm

"Generic" $\log_g$ algorithms: on average $q^{1/2+o(1)}$ operations uniform, $q^{1/3+o(1)}$ non-uniform. Want something faster.

"Basic index calculus": 1968 Western–Miller, 1979 Merkle, 1979 Adleman, 1983 Hellman–Reyneri, 1984 Blake–Fuji-Hara–Mullin–Vanstone, 1985 ElGamal, 1986 Coppersmith–Odlyzko–Schroeppel, 1991 LaMacchia–Odlyzko, 1993 Adleman–DeMarrais, 1995 Semaev, 1998 Bender–Pomerance.

"NFS": 1991 Schirokauer, 1
Gordon, 1993 Schirokauer, 1
Odlyzko, 1996 Schirokauer–
Weber–Denny, 1996 Weber,
1998 Weber–Denny, 2001 Jo
Lercier, 2006 Joux–Lercier–
Smart–Vercauteren.

"FFS": 1984 Coppersmith, 1
Coppersmith–Davenport, 19
Odlyzko, 1990 McCurley, 19
Gordon–McCurley, 1994 Adl
1999 Adleman–Huang, 2001
Joux–Lercier, 2006 Joux–Le
2010/2012 Hayashi–Shinoha
Wang–Matsuo–Shirase–Taka

"Generic" $\log_g$ algorithms: on average $q^{1/2+o(1)}$ operations uniform, $q^{1/3+o(1)}$ non-uniform. Want something faster.

"Basic index calculus": 1968 Western–Miller, 1979 Merkle, 1979 Adleman, 1983 Hellman–Reyneri, 1984 Blake–Fuji-Hara–Mullin–Vanstone, 1985 ElGamal, 1986 Coppersmith–Odlyzko–Schroeppel, 1991 LaMacchia–Odlyzko, 1993 Adleman–DeMarrais, 1995 Semaev, 1998 Bender–Pomerance.

"NFS": 1991 Schirokauer, 1993 Gordon, 1993 Schirokauer, 1994 Odlyzko, 1996 Schirokauer–Weber–Denny, 1996 Weber, 1998 Weber–Denny, 2001 Joux–Lercier, 2006 Joux–Lercier–Smart–Vercauteren.

"FFS": 1984 Coppersmith, 1985 Coppersmith–Davenport, 1985 Odlyzko, 1990 McCurley, 1992 Gordon–McCurley, 1994 Adleman, 1999 Adleman–Huang, 2001 Joux–Lercier, 2006 Joux–Lercier, 2010/2012 Hayashi–Shinohara–Wang–Matsuo–Shirase–Takagi.

c" $\log_g$ algorithms:
nge $q^{1/2+o(1)}$ operations
$q^{1/3+o(1)}$ non-uniform.
omething faster.

ndex calculus": 1968
–Miller, 1979 Merkle,
lleman, 1983 Hellman–
1984 Blake–Fuji-Hara–
Vanstone, 1985 ElGamal,
ppersmith–Odlyzko–
pel, 1991 LaMacchia–
, 1993 Adleman–
ais, 1995 Semaev,
nder–Pomerance.

"NFS": 1991 Schirokauer, 1993 Gordon, 1993 Schirokauer, 1994 Odlyzko, 1996 Schirokauer–Weber–Denny, 1996 Weber, 1998 Weber–Denny, 2001 Joux–Lercier, 2006 Joux–Lercier–Smart–Vercauteren.

"FFS": 1984 Coppersmith, 1985 Coppersmith–Davenport, 1985 Odlyzko, 1990 McCurley, 1992 Gordon–McCurley, 1994 Adleman, 1999 Adleman–Huang, 2001 Joux–Lercier, 2006 Joux–Lercier, 2010/2012 Hayashi–Shinohara–Wang–Matsuo–Shirase–Takagi.

"FFS",
Shimoya
2012.10
Detrey–
Videau–
Barbules
Gaudry–
Zimmer

gorithms:
$^{(1)}$ operations
non-uniform.
aster.

ulus": 1968
979 Merkle,
83 Hellman–
ke–Fuji-Hara–
1985 ElGamal,
–Odlyzko–
LaMacchia–
leman–
Semaev,
nerance.

"NFS": 1991 Schirokauer, 1993 Gordon, 1993 Schirokauer, 1994 Odlyzko, 1996 Schirokauer–Weber–Denny, 1996 Weber, 1998 Weber–Denny, 2001 Joux–Lercier, 2006 Joux–Lercier–Smart–Vercauteren.

"FFS": 1984 Coppersmith, 1985 Coppersmith–Davenport, 1985 Odlyzko, 1990 McCurley, 1992 Gordon–McCurley, 1994 Adleman, 1999 Adleman–Huang, 2001 Joux–Lercier, 2006 Joux–Lercier, 2010/2012 Hayashi–Shinohara–Wang–Matsuo–Shirase–Takagi.

"FFS", continued:
Shimoyama–Shino
2012.10 Barbulesc
Detrey–Gaudry–Je
Videau–Zimmerma
Barbulescu–Bouvie
Gaudry–Jeljeli–Th
Zimmermann.

ions
orm.

8
e,
n–
ara–
amal,
–
a–

“NFS”: 1991 Schirokauer, 1993 Gordon, 1993 Schirokauer, 1994 Odlyzko, 1996 Schirokauer–Weber–Denny, 1996 Weber, 1998 Weber–Denny, 2001 Joux–Lercier, 2006 Joux–Lercier–Smart–Vercauteren.

“FFS”: 1984 Coppersmith, 1985 Coppersmith–Davenport, 1985 Odlyzko, 1990 McCurley, 1992 Gordon–McCurley, 1994 Adleman, 1999 Adleman–Huang, 2001 Joux–Lercier, 2006 Joux–Lercier, 2010/2012 Hayashi–Shinohara–Wang–Matsuo–Shirase–Takagi.

“FFS”, continued: 2012 Hay
Shimoyama–Shinohara–Taka
2012.10 Barbulescu–Bouvier
Detrey–Gaudry–Jeljeli–Thom
Videau–Zimmermann, 2013.
Barbulescu–Bouvier–Detrey–
Gaudry–Jeljeli–Thomé–Vide
Zimmermann.

“NFS”: 1991 Schirokauer, 1993 Gordon, 1993 Schirokauer, 1994 Odlyzko, 1996 Schirokauer–Weber–Denny, 1996 Weber, 1998 Weber–Denny, 2001 Joux–Lercier, 2006 Joux–Lercier–Smart–Vercauteren.

“FFS”: 1984 Coppersmith, 1985 Coppersmith–Davenport, 1985 Odlyzko, 1990 McCurley, 1992 Gordon–McCurley, 1994 Adleman, 1999 Adleman–Huang, 2001 Joux–Lercier, 2006 Joux–Lercier, 2010/2012 Hayashi–Shinohara–Wang–Matsuo–Shirase–Takagi.

“FFS”, continued: 2012 Hayashi–Shimoyama–Shinohara–Takagi, 2012.10 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann, 2013.04 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann.

“NFS”: 1991 Schirokauer, 1993 Gordon, 1993 Schirokauer, 1994 Odlyzko, 1996 Schirokauer–Weber–Denny, 1996 Weber, 1998 Weber–Denny, 2001 Joux–Lercier, 2006 Joux–Lercier–Smart–Vercauteren.

“FFS”: 1984 Coppersmith, 1985 Coppersmith–Davenport, 1985 Odlyzko, 1990 McCurley, 1992 Gordon–McCurley, 1994 Adleman, 1999 Adleman–Huang, 2001 Joux–Lercier, 2006 Joux–Lercier, 2010/2012 Hayashi–Shinohara–Wang–Matsuo–Shirase–Takagi.

“FFS”, continued: 2012 Hayashi–Shimoyama–Shinohara–Takagi, 2012.10 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann, 2013.04 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann.

“Not your grandpa’s FFS”: 2012.12 Joux, 2013.02 Joux, 2013.02 Göloğlu–Granger–McGuire–Zumbrägel, 2013.05 Göloğlu–Granger–McGuire–Zumbrägel, 2013.06 Barbulescu–Gaudry–Joux–Thomé.

1991 Schirokauer, 1993
1993 Schirokauer, 1994
, 1996 Schirokauer–
Denny, 1996 Weber,
eber–Denny, 2001 Joux–
2006 Joux–Lercier–
/ercauteren.

1984 Coppersmith, 1985
mith–Davenport, 1985
, 1990 McCurley, 1992
-McCurley, 1994 Adleman,
lleman–Huang, 2001
rcier, 2006 Joux–Lercier,
012 Hayashi–Shinohara–
Matsuo–Shirase–Takagi.

"FFS", continued: 2012 Hayashi–Shimoyama–Shinohara–Takagi, 2012.10 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann, 2013.04 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann.

"Not your grandpa's FFS": 2012.12 Joux, 2013.02 Joux, 2013.02 Göloğlu–Granger–McGuire–Zumbrägel, 2013.05 Göloğlu–Granger–McGuire–Zumbrägel, 2013.06 Barbulescu–Gaudry–Joux–Thomé.

Reasona
for fixed

FFS cos
$\log T \in$

rokauer, 1993
irokauer, 1994
hirokauer–
96 Weber,
ny, 2001 Joux–
x–Lercier–
n.

persmith, 1985
enport, 1985
Curley, 1992
1994 Adleman,
uang, 2001
6 Joux–Lercier,
hi–Shinohara–
irase–Takagi.

"FFS", continued: 2012 Hayashi–Shimoyama–Shinohara–Takagi, 2012.10 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann, 2013.04 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann.

"Not your grandpa's FFS": 2012.12 Joux, 2013.02 Joux, 2013.02 Göloğlu–Granger–McGuire–Zumbrägel, 2013.05 Göloğlu–Granger–McGuire–Zumbrägel, 2013.06 Barbulescu–Gaudry–Joux–Thomé.

Reasonable conjec
for fixed character

FFS costs $\le T$ whe
$\log T \in (\log q)^{1/3+}$

993
1994
oux–
1985
85
92
eman,
.
rcier,
ra–
agi.

"FFS", continued: 2012 Hayashi–Shimoyama–Shinohara–Takagi, 2012.10 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann, 2013.04 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann.

"Not your grandpa's FFS": 2012.12 Joux, 2013.02 Joux, 2013.02 Göloğlu–Granger–McGuire–Zumbrägel, 2013.05 Göloğlu–Granger–McGuire–Zumbrägel, 2013.06 Barbulescu–Gaudry–Joux–Thomé.

Reasonable conjectures for fixed characteristic:

FFS costs $\le T$ where $\log T \in (\log q)^{1/3+o(1)}$.

“FFS”, continued: 2012 Hayashi–Shimoyama–Shinohara–Takagi, 2012.10 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann, 2013.04 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann.

“Not your grandpa’s FFS”: 2012.12 Joux, 2013.02 Joux, 2013.02 Göloğlu–Granger–McGuire–Zumbrägel, 2013.05 Göloğlu–Granger–McGuire–Zumbrägel, 2013.06 Barbulescu–Gaudry–Joux–Thomé.

Reasonable conjectures for fixed characteristic:

FFS costs $\le T$ where $\log T \in (\log q)^{1/3+o(1)}$.

"FFS", continued: 2012 Hayashi–Shimoyama–Shinohara–Takagi, 2012.10 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann, 2013.04 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann.

"Not your grandpa's FFS": 2012.12 Joux, 2013.02 Joux, 2013.02 Göloğlu–Granger–McGuire–Zumbrägel, 2013.05 Göloğlu–Granger–McGuire–Zumbrägel, 2013.06 Barbulescu–Gaudry–Joux–Thomé.

Reasonable conjectures for fixed characteristic:

FFS costs $\le T$ where $\log T \in (\log q)^{1/3+o(1)}$.

2013.02 Joux algorithm: $\log T \in (\log q)^{1/4+o(1)}$.

"FFS", continued: 2012 Hayashi–Shimoyama–Shinohara–Takagi, 2012.10 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann, 2013.04 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann.

"Not your grandpa's FFS": 2012.12 Joux, 2013.02 Joux, 2013.02 Göloğlu–Granger–McGuire–Zumbrägel, 2013.05 Göloğlu–Granger–McGuire–Zumbrägel, 2013.06 Barbulescu–Gaudry–Joux–Thomé.

Reasonable conjectures for fixed characteristic:

FFS costs $\le T$ where $\log T \in (\log q)^{1/3+o(1)}$.

2013.02 Joux algorithm: $\log T \in (\log q)^{1/4+o(1)}$.

2013.06 Barbulescu–Gaudry–Joux–Thomé algorithm: $\log T \in (\log \log q)^{2+o(1)}$.

“FFS”, continued: 2012 Hayashi–Shimoyama–Shinohara–Takagi, 2012.10 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann, 2013.04 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann.

“Not your grandpa’s FFS”: 2012.12 Joux, 2013.02 Joux, 2013.02 Göloğlu–Granger–McGuire–Zumbrägel, 2013.05 Göloğlu–Granger–McGuire–Zumbrägel, 2013.06 Barbulescu–Gaudry–Joux–Thomé.

Reasonable conjectures for fixed characteristic:

FFS costs $\le T$ where $\log T \in (\log q)^{1/3+o(1)}$.

2013.02 Joux algorithm: $\log T \in (\log q)^{1/4+o(1)}$.

2013.06 Barbulescu–Gaudry–Joux–Thomé algorithm: $\log T \in (\log\log q)^{2+o(1)}$.

1994 Shor algorithm: $\log T \in (\log\log q)^{1+o(1)}$, proven; but needs a quantum computer.

continued: 2012 Hayashi–
ma–Shinohara–Takagi,
Barbulescu–Bouvier–
Gaudry–Jeljeli–Thomé–
Zimmermann, 2013.04
scu–Bouvier–Detrey–
-Jeljeli–Thomé–Videau–
mann.

ur grandpa's FFS":
Joux, 2013.02 Joux,
Göloğlu–Granger–
e–Zumbrägel, 2013.05
-Granger–McGuire–
gel, 2013.06 Barbulescu–
-Joux–Thomé.

Reasonable conjectures
for fixed characteristic:

FFS costs $\le T$ where
$\log T \in (\log q)^{1/3+o(1)}$.

2013.02 Joux algorithm:
$\log T \in (\log q)^{1/4+o(1)}$.

2013.06 Barbulescu–Gaudry–
Joux–Thomé algorithm:
$\log T \in (\log \log q)^{2+o(1)}$.

1994 Shor algorithm:
$\log T \in (\log \log q)^{1+o(1)}$, proven;
but needs a quantum computer.

Field con

I'll make
$q = p^{2n}$
p is an o
$n \in \mathbf{Z}$,

Most int

Example

(Can you
$p^{2n} - 1$

Find "ra
with an
φ of deg

Construc

2012 Hayashi–
hara–Takagi,
u–Bouvier–
eljeli–Thomé–
ann, 2013.04
er–Detrey–
omé–Videau–

a's FFS":
13.02 Joux,
Granger–
gel, 2013.05
McGuire–
06 Barbulescu–
omé.

Reasonable conjectures for fixed characteristic:

FFS costs $\le T$ where $\log T \in (\log q)^{1/3+o(1)}$.

2013.02 Joux algorithm: $\log T \in (\log q)^{1/4+o(1)}$.

2013.06 Barbulescu–Gaudry–Joux–Thomé algorithm: $\log T \in (\log \log q)^{2+o(1)}$.

1994 Shor algorithm: $\log T \in (\log \log q)^{1+o(1)}$, proven; but needs a quantum computer.

Field construction

I'll make simplifyi
$q = p^{2n}$ where
p is an odd prime
$n \in \mathbf{Z}$, $\sqrt{p} \le n \le$

Most interesting:
Example: $p = 100$
(Can you find all p
$p^{2n} - 1 = (p^n - 1$

Find "random" po
with an irreducible
φ of degree n.

Construct $\mathbf{F}_q$ as $\mathbf{F}$

yashi–
agi,
r–
né–
04
–
au–

,

05

escu–

Reasonable conjectures
for fixed characteristic:

FFS costs $\le T$ where
$\log T \in (\log q)^{1/3+o(1)}$.

2013.02 Joux algorithm:
$\log T \in (\log q)^{1/4+o(1)}$.

2013.06 Barbulescu–Gaudry–Joux–Thomé algorithm:
$\log T \in (\log\log q)^{2+o(1)}$.

1994 Shor algorithm:
$\log T \in (\log\log q)^{1+o(1)}$, proven;
but needs a quantum computer.

Field construction

I'll make simplifying assump
$q = p^{2n}$ where
p is an odd prime power,
$n \in \mathbf{Z}$, $\sqrt{p} \le n \le p$.

Most interesting: $n \approx p$.
Example: $p = 1009$, $n = 99$
(Can you find all primes divi
$p^{2n} - 1 = (p^n - 1)(p^n + 1)$

Find "random" poly in $\mathbf{F}_{p^2}[$
with an irreducible divisor
φ of degree n.

Construct $\mathbf{F}_q$ as $\mathbf{F}_{p^2}[x]/\varphi$.

Reasonable conjectures
for fixed characteristic:

FFS costs $\le T$ where
$\log T \in (\log q)^{1/3+o(1)}$.

2013.02 Joux algorithm:
$\log T \in (\log q)^{1/4+o(1)}$.

2013.06 Barbulescu–Gaudry–Joux–Thomé algorithm:
$\log T \in (\log\log q)^{2+o(1)}$.

1994 Shor algorithm:
$\log T \in (\log\log q)^{1+o(1)}$, proven;
but needs a quantum computer.

Field construction

I'll make simplifying assumption:
$q = p^{2n}$ where
p is an odd prime power,
$n \in \mathbf{Z}$, $\sqrt{p} \le n \le p$.

Most interesting: $n \approx p$.
Example: $p = 1009$, $n = 997$.
(Can you find all primes dividing
$p^{2n} - 1 = (p^n - 1)(p^n + 1)$?)

Find "random" poly in $\mathbf{F}_{p^2}[x]$
with an irreducible divisor
φ of degree n.

Construct $\mathbf{F}_q$ as $\mathbf{F}_{p^2}[x]/\varphi$.

ble conjectures
characteristic:

ts $\le T$ where
$(\log q)^{1/3+o(1)}$.

Joux algorithm:
$(\log q)^{1/4+o(1)}$.

Barbulescu–Gaudry–
homé algorithm:
$(\log\log q)^{2+o(1)}$.

or algorithm:
$(\log\log q)^{1+o(1)}$, proven;
ds a quantum computer.

Field construction

I'll make simplifying assumption:
$q = p^{2n}$ where
p is an odd prime power,
$n \in \mathbf{Z}$, $\sqrt{p} \le n \le p$.

Most interesting: $n \approx p$.
Example: $p = 1009$, $n = 997$.
(Can you find all primes dividing
$p^{2n} - 1 = (p^n - 1)(p^n + 1)$?)

Find "random" poly in $\mathbf{F}_{p^2}[x]$
with an irreducible divisor
φ of degree n.

Construct $\mathbf{F}_q$ as $\mathbf{F}_{p^2}[x]/\varphi$.

How ma
What's c
has an ir
φ of deg

For $n \le$
express e
uniquely
$\approx (p^2)^{\text{de}}$
$\approx (p^2)^n /$
$\approx (p^2)^{\text{de}}$
chance $\approx$

Similar s

Factorin
$\Rightarrow$ Quick

tures
istic:

ere
$-o(1)$.

rithm:
$-o(1)$.

u–Gaudry–
rithm:
$2+o(1)$.

m:
$1+o(1)$, proven;
um computer.

Field construction

I'll make simplifying assumption:
$q = p^{2n}$ where
p is an odd prime power,
$n \in \mathbf{Z}$, $\sqrt{p} \le n \le p$.

Most interesting: $n \approx p$.
Example: $p = 1009$, $n = 997$.
(Can you find all primes dividing
$p^{2n} - 1 = (p^n - 1)(p^n + 1)$?)

Find "random" poly in $\mathbf{F}_{p^2}[x]$
with an irreducible divisor
φ of degree n.

Construct $\mathbf{F}_q$ as $\mathbf{F}_{p^2}[x]/\varphi$.

How many polys t
What's chance tha
has an irreducible
φ of degree n?

For $n \le \deg r < 2$
express each succe
uniquely as $\varphi \cdot$ cof
$\approx (p^2)^{\deg r + 1}$ polys
$\approx (p^2)^n / n$ monic i
$\approx (p^2)^{\deg r - n + 1}$ co
chance $\approx 1/n$ that

Similar story for d

Factoring r is fast
$\Rightarrow$ Quickly find r,

–

oven;

uter.

Field construction

I'll make simplifying assumption:
$q = p^{2n}$ where
p is an odd prime power,
$n \in \mathbf{Z}$, $\sqrt{p} \le n \le p$.

Most interesting: $n \approx p$.
Example: $p = 1009$, $n = 997$.
(Can you find all primes dividing
$p^{2n} - 1 = (p^n - 1)(p^n + 1)$?)

Find "random" poly in $\mathbf{F}_{p^2}[x]$
with an irreducible divisor
φ of degree n.

Construct $\mathbf{F}_q$ as $\mathbf{F}_{p^2}[x]/\varphi$.

How many polys to try?
What's chance that $r \in \mathbf{F}_{p^2}$
has an irreducible divisor
φ of degree n?

For $n \le \deg r < 2n$:
express each successful r
uniquely as $\varphi \cdot$ cofactor.
$\approx (p^2)^{\deg r + 1}$ polys r,
$\approx (p^2)^n / n$ monic irreds φ,
$\approx (p^2)^{\deg r - n + 1}$ cofactors $\Rightarrow$
chance $\approx 1/n$ that r works.

Similar story for $\deg r \ge 2n$

Factoring r is fast.
$\Rightarrow$ Quickly find r, φ.

Field construction

I'll make simplifying assumption:
$q = p^{2n}$ where
p is an odd prime power,
$n \in \mathbf{Z}$, $\sqrt{p} \le n \le p$.

Most interesting: $n \approx p$.
Example: $p = 1009$, $n = 997$.
(Can you find all primes dividing
$p^{2n} - 1 = (p^n - 1)(p^n + 1)$?)

Find "random" poly in $\mathbf{F}_{p^2}[x]$
with an irreducible divisor
φ of degree n.

Construct $\mathbf{F}_q$ as $\mathbf{F}_{p^2}[x]/\varphi$.

How many polys to try?
What's chance that $r \in \mathbf{F}_{p^2}[x]$
has an irreducible divisor
φ of degree n?

For $n \le \deg r < 2n$:
express each successful r
uniquely as $\varphi \cdot$ cofactor.
$\approx (p^2)^{\deg r + 1}$ polys r,
$\approx (p^2)^n / n$ monic irreds φ,
$\approx (p^2)^{\deg r - n + 1}$ cofactors $\Rightarrow$
chance $\approx 1/n$ that r works.

Similar story for $\deg r \ge 2n$.

Factoring r is fast.
$\Rightarrow$ Quickly find r, φ.

nstruction

e simplifying assumption:
where
odd prime power,
$\sqrt{p} \le n \le p$.

teresting: $n \approx p$.
e: $p = 1009$, $n = 997$.
u find all primes dividing
$= (p^n - 1)(p^n + 1)$?)

ndom" poly in $\mathbf{F}_{p^2}[x]$
irreducible divisor
gree n.

ct $\mathbf{F}_q$ as $\mathbf{F}_{p^2}[x]/\varphi$.

How many polys to try?
What's chance that $r \in \mathbf{F}_{p^2}[x]$
has an irreducible divisor
φ of degree n?

For $n \le \deg r < 2n$:
express each successful r
uniquely as $\varphi \cdot$ cofactor.
$\approx (p^2)^{\deg r + 1}$ polys r,
$\approx (p^2)^n / n$ monic irreds φ,
$\approx (p^2)^{\deg r - n + 1}$ cofactors $\Rightarrow$
chance $\approx 1/n$ that r works.

Similar story for $\deg r \ge 2n$.

Factoring r is fast.
$\Rightarrow$ Quickly find r, φ.

Don't us
(Starting

Find φ c
$x^p - x^2$
Then x^p

p^2 choic
so overw
that at l
e.g. $p =$
can have

Easily ge
$x^p = x^2$
$x^p = (x$
But larg

ng assumption:

power,

p.

$n \approx p$.

9, $n = 997$.

rimes dividing

$)(p^n + 1)$?)

ly in $\mathbf{F}_{p^2}[x]$

e divisor

$_{p^2}[x]/\varphi$.

How many polys to try?

What's chance that $r \in \mathbf{F}_{p^2}[x]$

has an irreducible divisor

φ of degree n?

For $n \le \deg r < 2n$:

express each successful r

uniquely as $\varphi \cdot$ cofactor.

$\approx (p^2)^{\deg r + 1}$ polys r,

$\approx (p^2)^n / n$ monic irreds φ,

$\approx (p^2)^{\deg r - n + 1}$ cofactors $\Rightarrow$

chance $\approx 1/n$ that r works.

Similar story for $\deg r \ge 2n$.

Factoring r is fast.

$\Rightarrow$ Quickly find r, φ.

Don't use random

(Starting now: ab

Find φ dividing

$x^p - x^2 - \beta$ for so

Then $x^p = x^2 + \beta$

p^2 choices of $\beta \in$

so overwhelmingly

that at least one w

e.g. $p = 1009$, $n =$

can have $\beta^2 + 92\beta$

Easily generalize:

$x^p = x^2 + \beta x + \gamma$

$x^p = (x + \beta)/(x$ -

But larger degrees

tion:

7.

ding

?)

$x]$

How many polys to try?
What's chance that $r \in \mathbf{F}_{p^2}[x]$
has an irreducible divisor
φ of degree n?

For $n \le \deg r < 2n$:
express each successful r
uniquely as $\varphi \cdot$ cofactor.
$\approx(p^2)^{\deg r+1}$ polys r,
$\approx(p^2)^n/n$ monic irreds φ,
$\approx(p^2)^{\deg r-n+1}$ cofactors $\Rightarrow$
chance $\approx 1/n$ that r works.

Similar story for $\deg r \ge 2n$.

Factoring r is fast.
$\Rightarrow$ Quickly find r, φ.

Don't use random polys!
(Starting now: abandon pro

Find φ dividing
$x^p - x^2 - \beta$ for some $\beta \in \mathbf{F}$
Then $x^p = x^2 + \beta$ in $\mathbf{F}_q$.

p^2 choices of $\beta \in \mathbf{F}_{p^2}$,
so overwhelmingly likely
that at least one works.
e.g. $p = 1009$, $n = 997$:
can have $\beta^2 + 92\beta + 447 =$

Easily generalize: e.g., take
$x^p = x^2 + \beta x + \gamma$ or
$x^p = (x + \beta)/(x + \gamma)$.
But larger degrees are slowe

How many polys to try?
What's chance that $r \in \mathbf{F}_{p^2}[x]$
has an irreducible divisor
φ of degree n?

For $n \le \deg r < 2n$:
express each successful r
uniquely as $\varphi \cdot$ cofactor.
$\approx(p^2)^{\deg r+1}$ polys r,
$\approx(p^2)^n/n$ monic irreds φ,
$\approx(p^2)^{\deg r-n+1}$ cofactors $\Rightarrow$
chance $\approx 1/n$ that r works.

Similar story for $\deg r \ge 2n$.

Factoring r is fast.
$\Rightarrow$ Quickly find r, φ.

Don't use random polys!
(Starting now: abandon proofs.)

Find φ dividing
$x^p - x^2 - \beta$ for some $\beta \in \mathbf{F}_{p^2}$.
Then $x^p = x^2 + \beta$ in $\mathbf{F}_q$.

p^2 choices of $\beta \in \mathbf{F}_{p^2}$,
so overwhelmingly likely
that at least one works.
e.g. $p = 1009$, $n = 997$:
can have $\beta^2 + 92\beta + 447 = 0$.

Easily generalize: e.g., take
$x^p = x^2 + \beta x + \gamma$ or
$x^p = (x + \beta)/(x + \gamma)$.
But larger degrees are slower.

ny polys to try?
chance that $r \in \mathbf{F}_{p^2}[x]$
rreducible divisor
gree n?

deg $r < 2n$:
each successful r
as $\varphi \cdot$ cofactor.
$g\, r+1$ polys r,
$/n$ monic irreds φ,
$g\, r-n+1$ cofactors $\Rightarrow$
$\approx 1/n$ that r works.

story for deg $r \geq 2n$.

g r is fast.
kly find r, φ.

Don't use random polys!
(Starting now: abandon proofs.)

Find φ dividing
$x^p - x^2 - \beta$ for some $\beta \in \mathbf{F}_{p^2}$.
Then $x^p = x^2 + \beta$ in $\mathbf{F}_q$.

p^2 choices of $\beta \in \mathbf{F}_{p^2}$,
so overwhelmingly likely
that at least one works.
e.g. $p = 1009$, $n = 997$:
can have $\beta^2 + 92\beta + 447 = 0$.

Easily generalize: e.g., take
$x^p = x^2 + \beta x + \gamma$ or
$x^p = (x + \beta)/(x + \gamma)$.
But larger degrees are slower.

Low-deg

First ste
build tab
each sm
Easily ch

"Small h
$D \geq 1$;

o try?

at $r \in \mathbf{F}_{p^2}[x]$

divisor

n:

essful r

actor.

s r,

rreds φ,

ofactors $\Rightarrow$

r works.

eg $r \geq 2n$.

.

φ.

Don't use random polys!

(Starting now: abandon proofs.)

Find φ dividing
$x^p - x^2 - \beta$ for some $\beta \in \mathbf{F}_{p^2}$.
Then $x^p = x^2 + \beta$ in $\mathbf{F}_q$.

p^2 choices of $\beta \in \mathbf{F}_{p^2}$,
so overwhelmingly likely
that at least one works.
e.g. $p = 1009$, $n = 997$:
can have $\beta^2 + 92\beta + 447 = 0$.

Easily generalize: e.g., take
$x^p = x^2 + \beta x + \gamma$ or
$x^p = (x + \beta)/(x + \gamma)$.
But larger degrees are slower.

<u>Low-degree discret</u>

First step of algori
build table of $h \mapsto$
each small $h \in \mathbf{F}_p$
Easily choose g at

“Small h”: deg h
$D \geq 1$; $D \in O(\log$

$[x]$

Don't use random polys!
(Starting now: abandon proofs.)

Find φ dividing
$x^p - x^2 - \beta$ for some $\beta \in \mathbf{F}_{p^2}$.
Then $x^p = x^2 + \beta$ in $\mathbf{F}_q$.

p^2 choices of $\beta \in \mathbf{F}_{p^2}$,
so overwhelmingly likely
that at least one works.
e.g. $p = 1009$, $n = 997$:
can have $\beta^2 + 92\beta + 447 = 0$.

Easily generalize: e.g., take
$x^p = x^2 + \beta x + \gamma$ or
$x^p = (x + \beta)/(x + \gamma)$.
But larger degrees are slower.

Low-degree discrete logs

First step of algorithm:
build table of $h \mapsto \log_g h$ fo
each small $h \in \mathbf{F}_{p^2}[x] - \varphi\mathbf{F}$
Easily choose g at same tim

"Small h": $\deg h \le D$. Cho
$D \ge 1$; $D \in O(\log n / \log \log$

Don't use random polys!
(Starting now: abandon proofs.)

Find φ dividing
$x^p - x^2 - \beta$ for some $\beta \in \mathbf{F}_{p^2}$.
Then $x^p = x^2 + \beta$ in $\mathbf{F}_q$.

p^2 choices of $\beta \in \mathbf{F}_{p^2}$,
so overwhelmingly likely
that at least one works.
e.g. $p = 1009$, $n = 997$:
can have $\beta^2 + 92\beta + 447 = 0$.

Easily generalize: e.g., take
$x^p = x^2 + \beta x + \gamma$ or
$x^p = (x + \beta)/(x + \gamma)$.
But larger degrees are slower.

Low-degree discrete logs

First step of algorithm:
build table of $h \mapsto \log_g h$ for
each small $h \in \mathbf{F}_{p^2}[x] - \varphi\mathbf{F}_{p^2}[x]$.
Easily choose g at same time.

"Small h": $\deg h \leq D$. Choose
$D \geq 1$; $D \in O(\log n / \log\log n)$.

Don't use random polys!
(Starting now: abandon proofs.)

Find φ dividing
$x^p - x^2 - \beta$ for some $\beta \in \mathbf{F}_{p^2}$.
Then $x^p = x^2 + \beta$ in $\mathbf{F}_q$.

p^2 choices of $\beta \in \mathbf{F}_{p^2}$,
so overwhelmingly likely
that at least one works.
e.g. $p = 1009$, $n = 997$:
can have $\beta^2 + 92\beta + 447 = 0$.

Easily generalize: e.g., take
$x^p = x^2 + \beta x + \gamma$ or
$x^p = (x + \beta)/(x + \gamma)$.
But larger degrees are slower.

Low-degree discrete logs

First step of algorithm:
build table of $h \mapsto \log_g h$ for
each small $h \in \mathbf{F}_{p^2}[x] - \varphi\mathbf{F}_{p^2}[x]$.
Easily choose g at same time.

"Small h": $\deg h \le D$. Choose
$D \ge 1$; $D \in O(\log n / \log\log n)$.

Non-uniform approach:
algorithm A_q knows table!

Don't use random polys!

(Starting now: abandon proofs.)

Find φ dividing $x^p - x^2 - \beta$ for some $\beta \in \mathbf{F}_{p^2}$.
Then $x^p = x^2 + \beta$ in $\mathbf{F}_q$.

p^2 choices of $\beta \in \mathbf{F}_{p^2}$,
so overwhelmingly likely
that at least one works.
e.g. $p = 1009$, $n = 997$:
can have $\beta^2 + 92\beta + 447 = 0$.

Easily generalize: e.g., take
$x^p = x^2 + \beta x + \gamma$ or
$x^p = (x + \beta)/(x + \gamma)$.
But larger degrees are slower.

Low-degree discrete logs

First step of algorithm:
build table of $h \mapsto \log_g h$ for
each small $h \in \mathbf{F}_{p^2}[x] - \varphi\mathbf{F}_{p^2}[x]$.
Easily choose g at same time.

"Small h": $\deg h \le D$. Choose
$D \ge 1$; $D \in O(\log n / \log\log n)$.

Non-uniform approach:
algorithm A_q knows table!

Two reasons to be more explicit:
1. Want A with q as an input.
2. Method to build table
will be reused for larger h.

se random polys!
g now: abandon proofs.)

dividing
$-\beta$ for some $\beta \in \mathbf{F}_{p^2}$.
$= x^2 + \beta$ in $\mathbf{F}_q$.

es of $\beta \in \mathbf{F}_{p^2}$,
vhelmingly likely
east one works.
1009, $n = 997$:
e $\beta^2 + 92\beta + 447 = 0$.

eneralize: e.g., take
$+ \beta x + \gamma$ or
$+ \beta)/(x + \gamma)$.
er degrees are slower.

Low-degree discrete logs

First step of algorithm:
build table of $h \mapsto \log_g h$ for
each small $h \in \mathbf{F}_{p^2}[x] - \varphi\mathbf{F}_{p^2}[x]$.
Easily choose g at same time.

"Small h": $\deg h \le D$. Choose
$D \ge 1$; $D \in O(\log n / \log\log n)$.

Non-uniform approach:
algorithm A_q knows table!

Two reasons to be more explicit:
1. Want A with q as an input.
2. Method to build table
will be reused for larger h.

The first

$\prod_{\alpha \in \mathbf{F}_p}($
"$\equiv$" for
$x^p - x^2$

Hope th
splits in
Not an u
≈50% o

Then log
$\sum_{\alpha \in \mathbf{F}_p}$ l

This is a
among c
of monic

polys!
andon proofs.)

ome $\beta \in \mathbf{F}_{p^2}$.
β in $\mathbf{F}_q$.

$\mathbf{F}_{p^2}$,
likely
vorks.
$= 997$:
$\beta + 447 = 0$.

e.g., take
or
$+ \gamma)$.
are slower.

Low-degree discrete logs

First step of algorithm:
build table of $h \mapsto \log_g h$ for
each small $h \in \mathbf{F}_{p^2}[x] - \varphi\mathbf{F}_{p^2}[x]$.
Easily choose g at same time.

"Small h": $\deg h \le D$. Choose
$D \ge 1$; $D \in O(\log n / \log\log n)$.

Non-uniform approach:
algorithm A_q knows table!

Two reasons to be more explicit:
1. Want A with q as an input.
2. Method to build table
will be reused for larger h.

The first relation f

$\prod_{\alpha\in\mathbf{F}_p}(x - \alpha) \equiv$

"$\equiv$" for $\mathbf{F}_{p^2}[x]$: ec
$x^p - x^2 - \beta$; force

Hope that $x^2 - x$
splits in $\mathbf{F}_{p^2}[x]$, sa
Not an unreasonal
$\approx$50% of quadrati

Then $\log_g f_1 + \log$
$\sum_{\alpha\in\mathbf{F}_p} \log_g(x - \alpha$

This is a "relation
among discrete log
of monic linear po

ofs.)

$_{p^2}$.

0.

r.

Low-degree discrete logs

First step of algorithm:
build table of $h \mapsto \log_g h$ for
each small $h \in \mathbf{F}_{p^2}[x] - \varphi\mathbf{F}_{p^2}[x]$.
Easily choose g at same time.

"Small h": $\deg h \le D$. Choose
$D \ge 1$; $D \in O(\log n / \log\log n)$.

Non-uniform approach:
algorithm A_q knows table!

Two reasons to be more explicit:
1. Want A with q as an input.
2. Method to build table
will be reused for larger h.

The first relation for $D = 1$

$\prod_{\alpha \in \mathbf{F}_p} (x - \alpha) \equiv x^2 - x +$

"$\equiv$" for $\mathbf{F}_{p^2}[x]$: equal mod
$x^p - x^2 - \beta$; forces $=$ in $\mathbf{F}_q$

Hope that $x^2 - x + \beta$
splits in $\mathbf{F}_{p^2}[x]$, say as $f_1 \cdot$
Not an unreasonable hope:
≈50% of quadratics split.

Then $\log_g f_1 + \log_g f_2 =$
$\sum_{\alpha \in \mathbf{F}_p} \log_g (x - \alpha)$.

This is a "relation"
among discrete logs
of monic linear polys.

Low-degree discrete logs

First step of algorithm:
build table of $h \mapsto \log_g h$ for
each small $h \in \mathbf{F}_{p^2}[x] - \varphi\mathbf{F}_{p^2}[x]$.
Easily choose g at same time.

"Small h": $\deg h \le D$. Choose
$D \ge 1$; $D \in O(\log n / \log\log n)$.

Non-uniform approach:
algorithm A_q knows table!

Two reasons to be more explicit:

1. Want A with q as an input.
2. Method to build table will be reused for larger h.

The first relation for $D = 1$

$\prod_{\alpha \in \mathbf{F}_p} (x - \alpha) \equiv x^2 - x + \beta$.

"$\equiv$" for $\mathbf{F}_{p^2}[x]$: equal mod
$x^p - x^2 - \beta$; forces $=$ in $\mathbf{F}_q$.

Hope that $x^2 - x + \beta$
splits in $\mathbf{F}_{p^2}[x]$, say as $f_1 \cdot f_2$.
Not an unreasonable hope:
≈50% of quadratics split.

Then $\log_g f_1 + \log_g f_2 =$
$\sum_{\alpha \in \mathbf{F}_p} \log_g(x - \alpha)$.

This is a "relation"
among discrete logs
of monic linear polys.

gree discrete logs

p of algorithm:
ble of $h \mapsto \log_g h$ for
all $h \in \mathbf{F}_{p^2}[x] - \varphi \mathbf{F}_{p^2}[x]$.
hoose g at same time.

h”: $\deg h \le D$. Choose
$D \in O(\log n / \log\log n)$.

form approach:
m A_q knows table!

sons to be more explicit:
t A with q as an input.
od to build table
eused for larger h.

The first relation for $D = 1$

$\prod_{\alpha \in \mathbf{F}_p} (x - \alpha) \equiv x^2 - x + \beta$.

“$\equiv$” for $\mathbf{F}_{p^2}[x]$: equal mod
$x^p - x^2 - \beta$; forces $=$ in $\mathbf{F}_q$.

Hope that $x^2 - x + \beta$
splits in $\mathbf{F}_{p^2}[x]$, say as $f_1 \cdot f_2$.
Not an unreasonable hope:
≈50% of quadratics split.

Then $\log_g f_1 + \log_g f_2 =$
$\sum_{\alpha \in \mathbf{F}_p} \log_g(x - \alpha)$.

This is a “relation”
among discrete logs
of monic linear polys.

More rel

For $a, b,$

$(cx + d)$

$= (cx +$
$- (ax +$

$= (cx +$
$- (ax +$

$\equiv (cx +$
$- (ax +$

Left side
linear po
Often rig

te logs

ithm:

$\to \log_g h$ for

${}_2[x] - \varphi \mathbf{F}_{p^2}[x]$.

same time.

$\leq D$. Choose

$n/\log\log n)$.

oach:

vs table!

e more explicit:

as an input.

d table

larger h.

The first relation for $D = 1$

$\prod_{\alpha \in \mathbf{F}_p} (x - \alpha) \equiv x^2 - x + \beta$.

"$\equiv$" for $\mathbf{F}_{p^2}[x]$: equal mod $x^p - x^2 - \beta$; forces $=$ in $\mathbf{F}_q$.

Hope that $x^2 - x + \beta$ splits in $\mathbf{F}_{p^2}[x]$, say as $f_1 \cdot f_2$. Not an unreasonable hope: ≈50% of quadratics split.

Then $\log_g f_1 + \log_g f_2 = \sum_{\alpha \in \mathbf{F}_p} \log_g (x - \alpha)$.

This is a "relation" among discrete logs of monic linear polys.

More relations for

For $a, b, c, d \in \mathbf{F}_{p^2}$

$(cx + d) \prod_{\alpha \in \mathbf{F}_p} (ax$

$= (cx + d)(ax + b$

$- (ax + b)(cx + d$

$= (cx + d)(a^p x^p$

$- (ax + b)(c^p x^p +$

$\equiv (cx + d)(a^p (x^2$

$- (ax + b)(c^p (x^2$

Left side is produc

linear polys in $\mathbf{F}_{p^2}$

Often right side is

r

$_{p^2}[x]$.

e.

ose

$n)$.

licit:

ut.

The first relation for $D = 1$

$\prod_{\alpha \in \mathbf{F}_p} (x - \alpha) \equiv x^2 - x + \beta$.

"$\equiv$" for $\mathbf{F}_{p^2}[x]$: equal mod $x^p - x^2 - \beta$; forces $=$ in $\mathbf{F}_q$.

Hope that $x^2 - x + \beta$ splits in $\mathbf{F}_{p^2}[x]$, say as $f_1 \cdot f_2$. Not an unreasonable hope: ≈50% of quadratics split.

Then $\log_g f_1 + \log_g f_2 = \sum_{\alpha \in \mathbf{F}_p} \log_g (x - \alpha)$.

This is a "relation" among discrete logs of monic linear polys.

More relations for $D = 1$

For $a, b, c, d \in \mathbf{F}_{p^2}$:

$$(cx + d) \prod_{\alpha \in \mathbf{F}_p} (ax + b - \alpha(cx$$

$$= (cx + d)(ax + b)^p$$
$$- (ax + b)(cx + d)^p$$

$$= (cx + d)(a^p x^p + b^p)$$
$$- (ax + b)(c^p x^p + d^p)$$

$$\equiv (cx + d)(a^p(x^2 + \beta) + b^p$$
$$- (ax + b)(c^p(x^2 + \beta) + d^p$$

Left side is product of linear polys in $\mathbf{F}_{p^2}[x]$. Often right side is too.

The first relation for $D = 1$

$\prod_{\alpha \in \mathbf{F}_p} (x - \alpha) \equiv x^2 - x + \beta$.

"$\equiv$" for $\mathbf{F}_{p^2}[x]$: equal mod $x^p - x^2 - \beta$; forces $=$ in $\mathbf{F}_q$.

Hope that $x^2 - x + \beta$ splits in $\mathbf{F}_{p^2}[x]$, say as $f_1 \cdot f_2$. Not an unreasonable hope: $\approx$50% of quadratics split.

Then $\log_g f_1 + \log_g f_2 = \sum_{\alpha \in \mathbf{F}_p} \log_g (x - \alpha)$.

This is a "relation" among discrete logs of monic linear polys.

More relations for $D = 1$

For $a, b, c, d \in \mathbf{F}_{p^2}$:

$$(cx + d) \prod_{\alpha \in \mathbf{F}_p} (ax + b - \alpha(cx + d))$$
$$= (cx + d)(ax + b)^p - (ax + b)(cx + d)^p$$
$$= (cx + d)(a^p x^p + b^p) - (ax + b)(c^p x^p + d^p)$$
$$\equiv (cx + d)(a^p (x^2 + \beta) + b^p) - (ax + b)(c^p (x^2 + \beta) + d^p).$$

Left side is product of linear polys in $\mathbf{F}_{p^2}[x]$. Often right side is too.

t relation for $D = 1$

$x - \alpha) \equiv x^2 - x + \beta$.

$\mathbf{F}_{p^2}[x]$: equal mod
$-\beta$; forces $=$ in $\mathbf{F}_q$.

at $x^2 - x + \beta$
$\mathbf{F}_{p^2}[x]$, say as $f_1 \cdot f_2$.
unreasonable hope:
f quadratics split.

$\mathrm{g}_g f_1 + \log_g f_2 =$
$\mathrm{og}_g(x - \alpha)$.

n "relation"
discrete logs
c linear polys.

More relations for $D = 1$

For $a, b, c, d \in \mathbf{F}_{p^2}$:

$$(cx + d) \prod_{\alpha \in \mathbf{F}_p} (ax + b - \alpha(cx + d))$$
$$= (cx + d)(ax + b)^p$$
$$- (ax + b)(cx + d)^p$$
$$= (cx + d)(a^p x^p + b^p)$$
$$- (ax + b)(c^p x^p + d^p)$$
$$\equiv (cx + d)(a^p(x^2 + \beta) + b^p)$$
$$- (ax + b)(c^p(x^2 + \beta) + d^p).$$

Left side is product of
linear polys in $\mathbf{F}_{p^2}[x]$.
Often right side is too.

$\lambda \in \mathbf{F}^*_{p^2}$,
$\Rightarrow M, \lambda$

$m \in \mathrm{GL}$
$\Rightarrow M, m$

No othe

Is there
the set o
in PGL_2
Cremona
Bartel gi

Mindless
is not a
but want

for $D=1$

$x^2 - x + \beta$.

qual mod

es = in $\mathbf{F}_q$.

$+ \beta$

y as $f_1 \cdot f_2$.

ble hope:

cs split.

$_g f_2 =$

$)$.

„

gs

lys.

More relations for $D = 1$

For $a, b, c, d \in \mathbf{F}_{p^2}$:

$$(cx+d) \prod_{\alpha \in \mathbf{F}_p} (ax + b - \alpha(cx+d))$$
$$= (cx+d)(ax+b)^p$$
$$- (ax+b)(cx+d)^p$$
$$= (cx+d)(a^p x^p + b^p)$$
$$- (ax+b)(c^p x^p + d^p)$$
$$\equiv (cx+d)(a^p(x^2+\beta) + b^p)$$
$$- (ax+b)(c^p(x^2+\beta) + d^p).$$

Left side is product of
linear polys in $\mathbf{F}_{p^2}[x]$.
Often right side is too.

$\lambda \in \mathbf{F}_{p^2}^*$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$
$\Rightarrow M, \lambda M$ are redu

$m \in \mathrm{GL}_2(\mathbf{F}_p)$, $M \in$
$\Rightarrow M, mM$ are red

No other obvious r

Is there a nice way
the set of cosets o
in $\mathrm{PGL}_2(\mathbf{F}_{p^2})$? Be
Cremona points m
Bartel gives solutio

Mindless enumerat
is not a real bottle
but want fast mult

β.

.

$_2$.

More relations for $D = 1$

For $a, b, c, d \in \mathbf{F}_{p^2}$:

$$(cx+d) \prod_{\alpha \in \mathbf{F}_p} (ax+b-\alpha(cx+d))$$
$$= (cx+d)(ax+b)^p$$
$$- (ax+b)(cx+d)^p$$
$$= (cx+d)(a^p x^p + b^p)$$
$$- (ax+b)(c^p x^p + d^p)$$
$$\equiv (cx+d)(a^p(x^2+\beta)+b^p)$$
$$- (ax+b)(c^p(x^2+\beta)+d^p).$$

Left side is product of
linear polys in $\mathbf{F}_{p^2}[x]$.
Often right side is too.

$\lambda \in \mathbf{F}_{p^2}^*$, $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2($
$\Rightarrow M, \lambda M$ are redundant.

$m \in \mathrm{GL}_2(\mathbf{F}_p)$, $M \in \mathrm{GL}_2(\mathbf{F}_{p^2}$
$\Rightarrow M, mM$ are redundant.

No other obvious redundanc

Is there a nice way to repres
the set of cosets of $\mathrm{PGL}_2(\mathbf{F}$
in $\mathrm{PGL}_2(\mathbf{F}_{p^2})$? Best hints so
Cremona points me to $\mathbf{F}_{p^4}^*/$
Bartel gives solution for GL_2

Mindless enumeration of cos
is not a real bottleneck here
but want fast multipoint eva

More relations for $D = 1$

For $a, b, c, d \in \mathbf{F}_{p^2}$:

$$(cx+d) \prod_{\alpha \in \mathbf{F}_p} (ax + b - \alpha(cx+d))$$
$$= (cx+d)(ax+b)^p$$
$$- (ax+b)(cx+d)^p$$
$$= (cx+d)(a^p x^p + b^p)$$
$$- (ax+b)(c^p x^p + d^p)$$
$$\equiv (cx+d)(a^p(x^2+\beta)+b^p)$$
$$- (ax+b)(c^p(x^2+\beta)+d^p).$$

Left side is product of linear polys in $\mathbf{F}_{p^2}[x]$. Often right side is too.

$\lambda \in \mathbf{F}^*_{p^2}$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
$\Rightarrow$ $M, \lambda M$ are redundant.

$m \in \mathrm{GL}_2(\mathbf{F}_p)$, $M \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
$\Rightarrow$ M, mM are redundant.

No other obvious redundancies.

Is there a nice way to represent the set of cosets of $\mathrm{PGL}_2(\mathbf{F}_p)$ in $\mathrm{PGL}_2(\mathbf{F}_{p^2})$? Best hints so far: Cremona points me to $\mathbf{F}^*_{p^4}/\mathbf{F}^*_{p^2}$; Bartel gives solution for GL_2.

Mindless enumeration of cosets is not a real bottleneck here but want fast multipoint eval.

ations for $D = 1$

$c, d \in \mathbf{F}_{p^2}$:

$$\prod_{\alpha \in \mathbf{F}_p} (ax + b - \alpha(cx + d))$$

$d)(ax + b)^p$

$b)(cx + d)^p$

$d)(a^p x^p + b^p)$

$b)(c^p x^p + d^p)$

$d)(a^p(x^2 + \beta) + b^p)$

$b)(c^p(x^2 + \beta) + d^p)$.

e is product of
olys in $\mathbf{F}_{p^2}[x]$.
ght side is too.

$\lambda \in \mathbf{F}^*_{p^2}$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
$\Rightarrow M, \lambda M$ are redundant.

$m \in \mathrm{GL}_2(\mathbf{F}_p)$, $M \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
$\Rightarrow M, mM$ are redundant.

No other obvious redundancies.

Is there a nice way to represent the set of cosets of $\mathrm{PGL}_2(\mathbf{F}_p)$ in $\mathrm{PGL}_2(\mathbf{F}_{p^2})$? Best hints so far: Cremona points me to $\mathbf{F}^*_{p^4}/\mathbf{F}^*_{p^2}$; Bartel gives solution for GL_2.

Mindless enumeration of cosets is not a real bottleneck here but want fast multipoint eval.

$p^3 + p$ p
conjectu
Each suc

Only p^2
Expect e
to deterr
(or *most*
unless p

BGJT sa
but fast
gives be

(How to
Maybe c
where β

$D = 1$

:

$+ b - \alpha(cx + d))$

$)^p$

$l)^p$

$+ b^p)$

$- d^p)$

$+ \beta) + b^p)$

$+ \beta) + d^p)$.

ct of

$[x]$.

too.

$\lambda \in \mathbf{F}_{p^2}^*$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
$\Rightarrow M, \lambda M$ are redundant.

$m \in \mathrm{GL}_2(\mathbf{F}_p)$, $M \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
$\Rightarrow M, mM$ are redundant.

No other obvious redundancies.

Is there a nice way to represent the set of cosets of $\mathrm{PGL}_2(\mathbf{F}_p)$ in $\mathrm{PGL}_2(\mathbf{F}_{p^2})$? Best hints so far: Cremona points me to $\mathbf{F}_{p^4}^*/\mathbf{F}_{p^2}^*$; Bartel gives solution for GL_2.

Mindless enumeration of cosets is not a real bottleneck here but want fast multipoint eval.

$p^3 + p$ potential re
conjecturally ≈ind
Each succeeds wit

Only p^2 monic line
Expect enough rel
to determine their
(or *most* logs: ok
unless p is very sm

BGJT say sparse l
but fast matrix mu
gives better const

(How to avoid ann
Maybe cleanest: x
where β generates

$c + d))$

)

).

$\lambda \in \mathbf{F}_{p^2}^*$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
$\Rightarrow$ $M, \lambda M$ are redundant.

$m \in \mathrm{GL}_2(\mathbf{F}_p)$, $M \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
$\Rightarrow$ M, mM are redundant.

No other obvious redundancies.

Is there a nice way to represent the set of cosets of $\mathrm{PGL}_2(\mathbf{F}_p)$ in $\mathrm{PGL}_2(\mathbf{F}_{p^2})$? Best hints so far: Cremona points me to $\mathbf{F}_{p^4}^*/\mathbf{F}_{p^2}^*$; Bartel gives solution for GL_2.

Mindless enumeration of cosets is not a real bottleneck here but want fast multipoint eval.

$p^3 + p$ potential relations, conjecturally $\approx$independent.
Each succeeds with chance

Only p^2 monic linear polys.
Expect enough relations to determine their logs (or *most* logs: ok to miss a unless p is very small.

BGJT say sparse linear alge but fast matrix multiplicatio gives better const in expone

(How to avoid annihilating
Maybe cleanest: $x^p = \beta x^2$
where β generates $\mathbf{F}_{p^2}^*$.)

$\lambda \in \mathbf{F}_{p^2}^*$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
$\Rightarrow M, \lambda M$ are redundant.

$m \in \mathrm{GL}_2(\mathbf{F}_p)$, $M \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
$\Rightarrow M, mM$ are redundant.

No other obvious redundancies.

Is there a nice way to represent the set of cosets of $\mathrm{PGL}_2(\mathbf{F}_p)$ in $\mathrm{PGL}_2(\mathbf{F}_{p^2})$? Best hints so far: Cremona points me to $\mathbf{F}_{p^4}^*/\mathbf{F}_{p^2}^*$; Bartel gives solution for GL_2.

Mindless enumeration of cosets is not a real bottleneck here but want fast multipoint eval.

$p^3 + p$ potential relations, conjecturally ≈independent. Each succeeds with chance ≈1/6.

Only p^2 monic linear polys. Expect enough relations to determine their logs (or *most* logs: ok to miss a few), unless p is very small.

BGJT say sparse linear algebra; but fast matrix multiplication gives better const in exponent.

(How to avoid annihilating $\mathbf{F}_{p^2}^*$? Maybe cleanest: $x^p = \beta x^2 + 1$, where β generates $\mathbf{F}_{p^2}^*$.)

, $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
M are redundant.

$_2(\mathbf{F}_p)$, $M \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
aM are redundant.

r obvious redundancies.

a nice way to represent
of cosets of $\mathrm{PGL}_2(\mathbf{F}_p)$
$(\mathbf{F}_{p^2})$? Best hints so far:
a points me to $\mathbf{F}^*_{p^4}/\mathbf{F}^*_{p^2}$;
ives solution for GL_2.

s enumeration of cosets
real bottleneck here
t fast multipoint eval.

$p^3 + p$ potential relations,
conjecturally ≈independent.
Each succeeds with chance ≈1/6.

Only p^2 monic linear polys.
Expect enough relations
to determine their logs
(or *most* logs: ok to miss a few),
unless p is very small.

BGJT say sparse linear algebra;
but fast matrix multiplication
gives better const in exponent.

(How to avoid annihilating $\mathbf{F}^*_{p^2}$?
Maybe cleanest: $x^p = \beta x^2 + 1$,
where β generates $\mathbf{F}^*_{p^2}$.)

More rel

For each

$(ch + d)$

$= (ch +$
$- (ah +$

$= (ch +$
$- (ah +$

$\equiv (ch +$
$- (ah +$

Left side
sometim
≈5% as

$) \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
undant.

$\in \mathrm{GL}_2(\mathbf{F}_{p^2})$
dundant.

redundancies.

y to represent
of $\mathrm{PGL}_2(\mathbf{F}_p)$
est hints so far:
ne to $\mathbf{F}^*_{p^4}/\mathbf{F}^*_{p^2}$;
on for GL_2.

tion of cosets
eneck here
tipoint eval.

$p^3 + p$ potential relations,
conjecturally ≈independent.
Each succeeds with chance ≈1/6.

Only p^2 monic linear polys.
Expect enough relations
to determine their logs
(or *most* logs: ok to miss a few),
unless p is very small.

BGJT say sparse linear algebra;
but fast matrix multiplication
gives better const in exponent.

(How to avoid annihilating $\mathbf{F}^*_{p^2}$?
Maybe cleanest: $x^p = \beta x^2 + 1$,
where β generates $\mathbf{F}^*_{p^2}$.)

<u>More relations for</u>

For each small h

$(ch + d) \prod_{\alpha \in \mathbf{F}_p} (ah$

$= (ch + d)(ah +$
$- (ah + b)(ch +$

$= (ch + d)(a^p h^p$
$- (ah + b)(c^p h^p$

$\equiv (ch + d)(a^p h(x$
$- (ah + b)(c^p h(x$

Left side is produc
sometimes right si
≈5% as $D \to \infty$.

$\mathbf{F}_{p^2})$

)

ies.

ent

$p)$

o far:

$\mathbf{F}^*_{p^2}$;

2.

sets

al.

$p^3 + p$ potential relations,
conjecturally ≈independent.
Each succeeds with chance ≈1/6.

Only p^2 monic linear polys.
Expect enough relations
to determine their logs
(or *most* logs: ok to miss a few),
unless p is very small.

BGJT say sparse linear algebra;
but fast matrix multiplication
gives better const in exponent.

(How to avoid annihilating $\mathbf{F}^*_{p^2}$?
Maybe cleanest: $x^p = \beta x^2 + 1$,
where β generates $\mathbf{F}^*_{p^2}$.)

More relations for arbitrary

For each small $h \in \mathbf{F}_{p^2}[x]$:

$$(ch + d) \prod_{\alpha \in \mathbf{F}_p} (ah + b - \alpha(ch$$
$$= (ch + d)(ah + b)^p$$
$$- (ah + b)(ch + d)^p$$
$$= (ch + d)(a^p h^p + b^p)$$
$$- (ah + b)(c^p h^p + d^p)$$
$$\equiv (ch + d)(a^p h(x^2 + \beta) + b$$
$$- (ah + b)(c^p h(x^2 + \beta) + d$$

Left side is product of small
sometimes right side is too.
≈5% as $D \to \infty$. BGJT say

p^3+p potential relations, conjecturally ≈independent. Each succeeds with chance ≈1/6.

Only p^2 monic linear polys. Expect enough relations to determine their logs (or *most* logs: ok to miss a few), unless p is very small.

BGJT say sparse linear algebra; but fast matrix multiplication gives better const in exponent.

(How to avoid annihilating $\mathbf{F}_{p^2}^*$? Maybe cleanest: $x^p = \beta x^2 + 1$, where β generates $\mathbf{F}_{p^2}^*$.)

<u>More relations for arbitrary D</u>

For each small $h \in \mathbf{F}_{p^2}[x]$:

$$(ch+d) \prod_{\alpha\in\mathbf{F}_p} (ah+b-\alpha(ch+d))$$
$$= (ch+d)(ah+b)^p - (ah+b)(ch+d)^p$$
$$= (ch+d)(a^p h^p + b^p) - (ah+b)(c^p h^p + d^p)$$
$$\equiv (ch+d)(a^p h(x^2+\beta)+b^p) - (ah+b)(c^p h(x^2+\beta)+d^p).$$

Left side is product of small polys; sometimes right side is too. ≈5% as $D\to\infty$. BGJT say 1/6.

potential relations,
rally ≈independent.
cceeds with chance ≈1/6.

monic linear polys.
enough relations
mine their logs
t logs: ok to miss a few),
is very small.

ay sparse linear algebra;
matrix multiplication
tter const in exponent.

avoid annihilating $\mathbf{F}_{p^2}^*$?
cleanest: $x^p = \beta x^2 + 1$,
generates $\mathbf{F}_{p^2}^*$.)

More relations for arbitrary D

For each small $h \in \mathbf{F}_{p^2}[x]$:

$$(ch+d)\prod_{\alpha\in\mathbf{F}_p}(ah+b-\alpha(ch+d))$$
$$= (ch+d)(ah+b)^p$$
$$- (ah+b)(ch+d)^p$$
$$= (ch+d)(a^p h^p + b^p)$$
$$- (ah+b)(c^p h^p + d^p)$$
$$\equiv (ch+d)(a^p h(x^2+\beta) + b^p)$$
$$- (ah+b)(c^p h(x^2+\beta) + d^p).$$

Left side is product of small polys;
sometimes right side is too.
≈5% as $D \to \infty$. BGJT say 1/6.

Larger d

What if

Use sam
$(ch+d)$

$\equiv (ch +$
$- (ah +$

Occasio
product
We now

Left side
factor ba
Solve fo

elations,
ependent.
h chance ≈1/6.

ear polys.
ations
logs
to miss a few),
hall.

inear algebra;
ultiplication
in exponent.

nihilating $\mathbf{F}^*_{p^2}$?
$c^p = \beta x^2 + 1$,
s $\mathbf{F}^*_{p^2}$.)

<u>More relations for arbitrary *D*</u>

For each small $h \in \mathbf{F}_{p^2}[x]$:

$$(ch+d) \prod_{\alpha \in \mathbf{F}_p} (ah+b-\alpha(ch+d))$$
$$= (ch+d)(ah+b)^p$$
$$-\,(ah+b)(ch+d)^p$$
$$= (ch+d)(a^p h^p + b^p)$$
$$-\,(ah+b)(c^p h^p + d^p)$$
$$\equiv (ch+d)(a^p h(x^2+\beta) + b^p)$$
$$-\,(ah+b)(c^p h(x^2+\beta) + d^p).$$

Left side is product of small polys;
sometimes right side is too.
≈5% as $D \to \infty$. BGJT say 1/6.

<u>Larger discrete log</u>

What if $D < \deg h$

Use same equation
$(ch+d) \prod_{\alpha \in \mathbf{F}_p} (ah$
$\equiv (ch+d)(a^p h(x$
$-\,(ah+b)(c^p h(x$

Occasionally right
product of small p
We now know tho

Left side is produc
factor base: $\{h +$
Solve for each log

$\approx 1/6$.

few),

ra;

n

nt.

$F^*_{p^2}$?

$+ 1$,

More relations for arbitrary D

For each small $h \in \mathbf{F}_{p^2}[x]$:

$$(ch + d) \prod_{\alpha \in \mathbf{F}_p} (ah + b - \alpha(ch + d))$$
$$= (ch + d)(ah + b)^p$$
$$- (ah + b)(ch + d)^p$$
$$= (ch + d)(a^p h^p + b^p)$$
$$- (ah + b)(c^p h^p + d^p)$$
$$\equiv (ch + d)(a^p h(x^2 + \beta) + b^p)$$
$$- (ah + b)(c^p h(x^2 + \beta) + d^p).$$

Left side is product of small polys; sometimes right side is too. $\approx 5\%$ as $D \to \infty$. BGJT say $1/6$.

Larger discrete logs

What if $D < \deg h \leq 2D$?

Use same equation:

$$(ch + d) \prod_{\alpha \in \mathbf{F}_p} (ah + b - \alpha(ch$$
$$\equiv (ch + d)(a^p h(x^2 + \beta) + b$$
$$- (ah + b)(c^p h(x^2 + \beta) + d$$

Occasionally right side is product of small polys. We now know those discrete

Left side is product on new factor base: $\{h + \gamma : \gamma \in \mathbf{F}_p$

Solve for each $\log_g(h + \gamma)$.

More relations for arbitrary D

For each small $h \in \mathbf{F}_{p^2}[x]$:

$$(ch+d) \prod_{\alpha \in \mathbf{F}_p} (ah+b-\alpha(ch+d))$$
$$= (ch+d)(ah+b)^p$$
$$- (ah+b)(ch+d)^p$$
$$= (ch+d)(a^p h^p + b^p)$$
$$- (ah+b)(c^p h^p + d^p)$$
$$\equiv (ch+d)(a^p h(x^2+\beta) + b^p)$$
$$- (ah+b)(c^p h(x^2+\beta) + d^p).$$

Left side is product of small polys; sometimes right side is too. $\approx$5% as $D \to \infty$. BGJT say 1/6.

Larger discrete logs

What if $D < \deg h \le 2D$?

Use same equation:

$$(ch+d) \prod_{\alpha \in \mathbf{F}_p} (ah+b-\alpha(ch+d))$$
$$\equiv (ch+d)(a^p h(x^2+\beta) + b^p)$$
$$- (ah+b)(c^p h(x^2+\beta) + d^p).$$

Occasionally right side is product of small polys. We now know those discrete logs.

Left side is product on new factor base: $\{h+\gamma : \gamma \in \mathbf{F}_{p^2}\}$. Solve for each $\log_g(h+\gamma)$.

ations for arbitrary D

n small $h \in \mathbf{F}_{p^2}[x]$:

$$\prod_{\alpha \in \mathbf{F}_p} (ah + b - \alpha(ch + d))$$

$d)(ah + b)^p$

$- b)(ch + d)^p$

$d)(a^p h^p + b^p)$

$- b)(c^p h^p + d^p)$

$d)(a^p h(x^2 + \beta) + b^p)$

$- b)(c^p h(x^2 + \beta) + d^p)$.

e is product of small polys;

nes right side is too.

$D \to \infty$. BGJT say 1/6.

Larger discrete logs

What if $D < \deg h \leq 2D$?

Use same equation:

$$(ch + d) \prod_{\alpha \in \mathbf{F}_p} (ah + b - \alpha(ch + d))$$

$$\equiv (ch + d)(a^p h(x^2 + \beta) + b^p)$$

$$- (ah + b)(c^p h(x^2 + \beta) + d^p).$$

Occasionally right side is product of small polys. We now know those discrete logs.

Left side is product on new factor base: $\{h + \gamma : \gamma \in \mathbf{F}_{p^2}\}$. Solve for each $\log_g(h + \gamma)$.

For deg

D-smoo

so $\approx u^{-}$

Need $\approx p$

Note fre

Works fo

Reminisc

(1977 Sc

$(\lceil \sqrt{q} \rceil +$

$\equiv (a + b$

mod larg

Factor b

$\{\lceil \sqrt{q} \rceil -$

arbitrary D

$\in \mathbf{F}_{p^2}[x]$:

$+ b - \alpha(ch + d))$

$b)^p$

$d)^p$

$+ b^p)$

$+ d^p)$

$^2 + \beta) + b^p)$

$^2 + \beta) + d^p)$.

ct of small polys;

de is too.

BGJT say $1/6$.

Larger discrete logs

What if $D < \deg h \le 2D$?

Use same equation:

$$(ch + d) \prod_{\alpha \in \mathbf{F}_p} (ah + b - \alpha(ch + d))$$

$$\equiv (ch + d)(a^p h(x^2 + \beta) + b^p)$$

$$- (ah + b)(c^p h(x^2 + \beta) + d^p).$$

Occasionally right side is product of small polys. We now know those discrete logs.

Left side is product on new factor base: $\{h + \gamma : \gamma \in \mathbf{F}_{p^2}\}$. Solve for each $\log_g(h + \gamma)$.

For $\deg h \le (u/3)$

D-smoothness cha

so $\approx u^{-u} p^3$ relatio

Need $\approx p^2$ relation

Note free relations

Works for $u \approx$ log

Reminiscent of lin

(1977 Schroeppel)

$(\lceil\sqrt{q}\rceil + a)(\lceil\sqrt{q}\rceil$

$\equiv (a + b)\lceil\sqrt{q}\rceil +$

mod large prime q

Factor base in line

$\{\lceil\sqrt{q}\rceil + a\} \cup \{$sn

D

$h + d))$

$b^p)$

$d^p)$.

polys;

$1/6$.

Larger discrete logs

What if $D < \deg h \le 2D$?

Use same equation:

$$(ch + d) \prod_{\alpha \in \mathbf{F}_p} (ah + b - \alpha(ch + d))$$
$$\equiv (ch + d)(a^p h(x^2 + \beta) + b^p)$$
$$- (ah + b)(c^p h(x^2 + \beta) + d^p).$$

Occasionally right side is product of small polys. We now know those discrete logs.

Left side is product on new factor base: $\{h + \gamma : \gamma \in \mathbf{F}_{p^2}\}$. Solve for each $\log_g(h + \gamma)$.

For $\deg h \le (u/3)D$: D-smoothness chance $\approx u^{-u}$ so $\approx u^{-u} p^3$ relations.

Need $\approx p^2$ relations. Note free relations: smooth

Works for $u \approx \log p / \log \log$

Reminiscent of linear sieve (1977 Schroeppel):

$$(\lceil \sqrt{q} \rceil + a)(\lceil \sqrt{q} \rceil + b)$$
$$\equiv (a + b) \lceil \sqrt{q} \rceil + ab + \lceil \sqrt{q}$$

mod large prime q.

Factor base in linear sieve:

$\{\lceil \sqrt{q} \rceil + a\} \cup \{$small primes

Larger discrete logs

What if $D < \deg h \le 2D$?

Use same equation:

$$(ch+d)\prod_{\alpha\in\mathbf{F}_p}(ah+b-\alpha(ch+d))$$
$$\equiv (ch+d)(a^p h(x^2+\beta)+b^p)$$
$$-\ (ah+b)(c^p h(x^2+\beta)+d^p).$$

Occasionally right side is product of small polys.
We now know those discrete logs.

Left side is product on new factor base: $\{h+\gamma : \gamma\in\mathbf{F}_{p^2}\}$.
Solve for each $\log_g(h+\gamma)$.

For $\deg h \le (u/3)D$:
D-smoothness chance $\approx u^{-u}$
so $\approx u^{-u}p^3$ relations.

Need $\approx p^2$ relations.
Note free relations: smooth $h+\gamma$.

Works for $u \approx \log p/\log\log p$.

Reminiscent of linear sieve (1977 Schroeppel):

$$(\lceil\sqrt{q}\rceil+a)(\lceil\sqrt{q}\rceil+b)$$
$$\equiv (a+b)\lceil\sqrt{q}\rceil+ab+\lceil\sqrt{q}\rceil^2-q$$

mod large prime q.
Factor base in linear sieve:
$\{\lceil\sqrt{q}\rceil+a\}\cup\{\text{small primes}\}$.

iscrete logs

$D < \deg h \le 2D$?

e equation:

$$\prod_{\alpha \in \mathbf{F}_p} (ah + b - \alpha(ch + d))$$

$d)(a^p h(x^2 + \beta) + b^p)$

$b)(c^p h(x^2 + \beta) + d^p)$.

nally right side is

of small polys.

know those discrete logs.

e is product on new

ase: $\{h + \gamma : \gamma \in \mathbf{F}_{p^2}\}$.

r each $\log_g(h + \gamma)$.

For $\deg h \le (u/3)D$:
D-smoothness chance $\approx u^{-u}$
so $\approx u^{-u} p^3$ relations.

Need $\approx p^2$ relations.
Note free relations: smooth $h + \gamma$.

Works for $u \approx \log p / \log\log p$.

Reminiscent of linear sieve
(1977 Schroeppel):
$(\lceil\sqrt{q}\rceil + a)(\lceil\sqrt{q}\rceil + b)$
$\equiv (a + b)\lceil\sqrt{q}\rceil + ab + \lceil\sqrt{q}\rceil^2 - q$
mod large prime q.
Factor base in linear sieve:
$\{\lceil\sqrt{q}\rceil + a\} \cup \{\text{small primes}\}$.

Arbitrary

For $(u/3$

Use sam
$(ch + d)$

$\equiv (ch +$
$- (ah +$

Occasion
side; aga
Have see
$(u/3)D$-
$p^{O(1)}$ su
of which

gs

$h \leq 2D$?

n:

$+ b - \alpha(ch + d))$

${}^2 + \beta) + b^p)$

${}^2 + \beta) + d^p)$.

side is

polys.

se discrete logs.

ct on new

$\gamma : \gamma \in \mathbf{F}_{p^2}\}$.

${}_g(h + \gamma)$.

For $\deg h \leq (u/3)D$:
D-smoothness chance $\approx u^{-u}$
so $\approx u^{-u} p^3$ relations.

Need $\approx p^2$ relations.
Note free relations: smooth $h + \gamma$.

Works for $u \approx \log p / \log \log p$.

Reminiscent of linear sieve
(1977 Schroeppel):
$(\lceil \sqrt{q} \rceil + a)(\lceil \sqrt{q} \rceil + b)$
$\equiv (a + b) \lceil \sqrt{q} \rceil + ab + \lceil \sqrt{q} \rceil^2 - q$
mod large prime q.
Factor base in linear sieve:
$\{\lceil \sqrt{q} \rceil + a\} \cup \{\text{small primes}\}$.

Arbitrary discrete

For $(u/3)D < \deg$

Use same equation
$(ch + d) \prod_{\alpha \in \mathbf{F}_p} (ah$
$\equiv (ch + d)(a^p h(x$
$- (ah + b)(c^p h(x$

Occasionally $(u/3$
side; again $\{h + \gamma$
Have seen subrout
$(u/3)D$-smooth di
$p^{O(1)}$ subroutine c
of which $\Theta(p^2)$ ar

$h + d))$

$b^p)$

$d^p)$.

e logs.

$p^2\}$.

For $\deg h \le (u/3)D$:
D-smoothness chance $\approx u^{-u}$
so $\approx u^{-u} p^3$ relations.

Need $\approx p^2$ relations.
Note free relations: smooth $h + \gamma$.

Works for $u \approx \log p / \log\log p$.

Reminiscent of linear sieve
(1977 Schroeppel):
$(\lceil \sqrt{q} \rceil + a)(\lceil \sqrt{q} \rceil + b)$
$\equiv (a + b) \lceil \sqrt{q} \rceil + ab + \lceil \sqrt{q} \rceil^2 - q$
mod large prime q.
Factor base in linear sieve:
$\{\lceil \sqrt{q} \rceil + a\} \cup \{\text{small primes}\}$.

Arbitrary discrete logs

For $(u/3)D < \deg h \le (u/3$

Use same equation
$(ch + d) \prod_{\alpha \in \mathbf{F}_p} (ah + b - \alpha(ch$
$\equiv (ch + d)(a^p h(x^2 + \beta) + b$
$- (ah + b)(c^p h(x^2 + \beta) + d$

Occasionally $(u/3)D$-smooth
side; again $\{h + \gamma\}$ for left s
Have seen subroutine to con
$(u/3)D$-smooth discrete log

$p^{O(1)}$ subroutine calls,
of which $\Theta(p^2)$ are importan

For $\deg h \le (u/3)D$:
D-smoothness chance $\approx u^{-u}$
so $\approx u^{-u} p^3$ relations.

Need $\approx p^2$ relations.
Note free relations: smooth $h + \gamma$.

Works for $u \approx \log p / \log \log p$.

Reminiscent of linear sieve
(1977 Schroeppel):
$(\lceil \sqrt{q} \rceil + a)(\lceil \sqrt{q} \rceil + b)$
$\equiv (a+b)\lceil \sqrt{q} \rceil + ab + \lceil \sqrt{q} \rceil^2 - q$
mod large prime q.
Factor base in linear sieve:
$\{\lceil \sqrt{q} \rceil + a\} \cup \{\text{small primes}\}$.

Arbitrary discrete logs

For $(u/3)D < \deg h \le (u/3)^2 D$:

Use same equation
$$(ch + d) \prod_{\alpha \in \mathbf{F}_p} (ah + b - \alpha(ch + d))$$
$$\equiv (ch + d)(a^p h(x^2 + \beta) + b^p)$$
$$- (ah + b)(c^p h(x^2 + \beta) + d^p).$$

Occasionally $(u/3)D$-smooth right side; again $\{h + \gamma\}$ for left side.
Have seen subroutine to compute $(u/3)D$-smooth discrete logs.

$p^{O(1)}$ subroutine calls,
of which $\Theta(p^2)$ are important.

$h \le (u/3)D$:
thness chance $\approx u^{-u}$
$^u p^3$ relations.

p^2 relations.
e relations: smooth $h + \gamma$.

or $u \approx \log p / \log \log p$.

cent of linear sieve
chroeppel):
$- a)(\lceil \sqrt{q} \rceil + b)$
$b) \lceil \sqrt{q} \rceil + ab + \lceil \sqrt{q} \rceil^2 - q$
ge prime q.
base in linear sieve:
$+ a\} \cup \{\text{small primes}\}$.

<u>Arbitrary discrete logs</u>

For $(u/3)D < \deg h \le (u/3)^2 D$:

Use same equation
$(ch + d) \prod_{\alpha \in \mathbf{F}_p} (ah + b - \alpha(ch + d))$
$\equiv (ch + d)(a^p h(x^2 + \beta) + b^p)$
$- (ah + b)(c^p h(x^2 + \beta) + d^p)$.

Occasionally $(u/3)D$-smooth right side; again $\{h + \gamma\}$ for left side.
Have seen subroutine to compute $(u/3)D$-smooth discrete logs.

$p^{O(1)}$ subroutine calls,
of which $\Theta(p^2)$ are important.

For large

Reach d
$\log n$
$\overline{\log(u/3}$
levels of

Total co

$= \exp \Theta$

$= \exp \Theta$

What ab
Embed i
Can also

D:

ance $\approx u^{-u}$

ons.

s.

s: smooth $h + \gamma$.

$p / \log\log p$.

ear sieve

):

$+ b)$

$ab + \lceil \sqrt{q} \rceil^2 - q$

.

ear sieve:

mall primes}.

Arbitrary discrete logs

For $(u/3)D < \deg h \le (u/3)^2 D$:

Use same equation

$$(ch + d) \prod_{\alpha \in \mathbf{F}_p} (ah + b - \alpha(ch + d))$$

$$\equiv (ch + d)(a^p h(x^2 + \beta) + b^p)$$

$$- (ah + b)(c^p h(x^2 + \beta) + d^p).$$

Occasionally $(u/3)D$-smooth right side; again $\{h + \gamma\}$ for left side.

Have seen subroutine to compute $(u/3)D$-smooth discrete logs.

$p^{O(1)}$ subroutine calls, of which $\Theta(p^2)$ are important.

For larger h: recur

Reach degree $n -$

$\frac{\log n}{\log(u/3)} \in \Theta\Big(\frac{\mathrm{l}}{\mathrm{log}}$

levels of recursion.

Total cost $p^{\Theta(\log n}$

$= \exp \Theta \Big(\frac{(\log n)^2}{\log\log n}$

$= \exp \Theta \Big(\frac{(\log\log}{\log\log\mathrm{lo}}$

What about p^{2n} w

Embed into an ext

Can also use x^{char}

u

$h + \gamma$.

p.

$]^2 - q$

s}.

<u>Arbitrary discrete logs</u>

For $(u/3)D < \deg h \le (u/3)^2 D$:

Use same equation

$$(ch + d) \prod_{\alpha \in \mathbf{F}_p} (ah + b - \alpha(ch + d))$$
$$\equiv (ch + d)(a^p h(x^2 + \beta) + b^p)$$
$$- (ah + b)(c^p h(x^2 + \beta) + d^p).$$

Occasionally $(u/3)D$-smooth right side; again $\{h + \gamma\}$ for left side.
Have seen subroutine to compute $(u/3)D$-smooth discrete logs.

$p^{O(1)}$ subroutine calls,
of which $\Theta(p^2)$ are important.

For larger h: recurse.

Reach degree $n - 1$ using
$$\frac{\log n}{\log(u/3)} \in \Theta\left(\frac{\log n}{\log \log n}\right)$$
levels of recursion.

Total cost $p^{\Theta(\log n / \log \log n)}$
$$= \exp \Theta\left(\frac{(\log n)^2}{\log \log n}\right)$$
$$= \exp \Theta\left(\frac{(\log \log q)^2}{\log \log \log q}\right).$$

What about p^{2n} with $p < n$
Embed into an extension fie
Can also use x^{char} etc.

Arbitrary discrete logs

For $(u/3)D < \deg h \le (u/3)^2 D$:

Use same equation
$$(ch+d) \prod_{\alpha\in\mathbf{F}_p} (ah+b-\alpha(ch+d))$$
$$\equiv (ch+d)(a^p h(x^2+\beta)+b^p)$$
$$-(ah+b)(c^p h(x^2+\beta)+d^p).$$

Occasionally $(u/3)D$-smooth right side; again $\{h+\gamma\}$ for left side.
Have seen subroutine to compute $(u/3)D$-smooth discrete logs.

$p^{O(1)}$ subroutine calls,
of which $\Theta(p^2)$ are important.

For larger h: recurse.

Reach degree $n-1$ using
$$\frac{\log n}{\log(u/3)} \in \Theta\Big(\frac{\log n}{\log\log n}\Big)$$
levels of recursion.

Total cost $p^{\Theta(\log n/\log\log n)}$
$$= \exp\Theta\Big(\frac{(\log n)^2}{\log\log n}\Big)$$
$$= \exp\Theta\Big(\frac{(\log\log q)^2}{\log\log\log q}\Big).$$

What about p^{2n} with $p < n$?
Embed into an extension field.
Can also use x^{char} etc.