Post-quantum cryptography

D. J. Bernstein
University of Illinois at Chicago

"If a quantum computer is created . . . then the levels of security that we now have to protect our information on computers will be worthless. It is absolutely essential that quantum cryptography be developed out before quantum computers become a reality."

Calgary press release, 2004.
Author not clearly identified.
Barry Sanders named as contact.

Post-quantum cryptography

D. J. Bernstein
University of Illinois at Chicago

"If a quantum computer is created . . . then the levels of security that we now have to protect our information on computers will be worthless. It is absolutely essential that quantum cryptography be developed out before quantum computers become a reality."

Calgary press release, 2004.
Author not clearly identified.
Barry Sanders named as contact.

2009 Sanders: "I am not responsible for this press release."

uantum cryptography

Bernstein

sity of Illinois at Chicago

"If a quantum computer is created . . . then the levels of security that we now have to protect our information on computers will be worthless. It is absolutely essential that quantum cryptography be developed out before quantum computers become a reality."

Calgary press release, 2004.
Author not clearly identified.
Barry Sanders named as contact.

2009 Sanders: "I am not responsible for this press release."

2005 ic
"Futur
with Q

"Finall
quantu
break p

"[5] Quant
that exp
to proce
the realn
will even

yptography

ois at Chicago

"If a quantum computer is created . . . then the levels of security that we now have to protect our information on computers will be worthless. It is absolutely essential that quantum cryptography be developed out before quantum computers become a reality."

Calgary press release, 2004.
Author not clearly identified.
Barry Sanders named as contact.

2009 Sanders: "I am not responsible for this press release."

2005 id Quantiqu
"Future-proof Da
with Quantum C

"Finally, it is alre
quantum comput
break public key

"[5]Quantum compute
that exploit the laws
to process informatio
the realm of experim
will eventually be bu

y

cago

"If a quantum computer is created . . . then the levels of security that we now have to protect our information on computers will be worthless. It is absolutely essential that quantum cryptography be developed out before quantum computers become a reality."

Calgary press release, 2004.
Author not clearly identified.
Barry Sanders named as contact.

2009 Sanders: "I am not responsible for this press release."

2005 id Quantique white p
"Future-proof Data Confid
with Quantum Cryptograp

"Finally, it is already prove
quantum computers[5] will a
break public key cryptogra

"[5]Quantum computers are comp
that exploit the laws of quantum
to process information. They are
the realm of experimental researc
will eventually be built."

"If a quantum computer is created . . . then the levels of security that we now have to protect our information on computers will be worthless. It is absolutely essential that quantum cryptography be developed out before quantum computers become a reality."

Calgary press release, 2004.
Author not clearly identified.
Barry Sanders named as contact.

2009 Sanders: "I am not responsible for this press release."

2005 id Quantique white paper "Future-proof Data Confidentiality with Quantum Cryptography":

"Finally, it is already proven that quantum computers[5] will allow to break public key cryptography."

"[5]Quantum computers are computers that exploit the laws of quantum physics to process information. They are still in the realm of experimental research, but will eventually be built."

"If a quantum computer is created . . . then the levels of security that we now have to protect our information on computers will be worthless. It is absolutely essential that quantum cryptography be developed out before quantum computers become a reality."

Calgary press release, 2004.
Author not clearly identified.
Barry Sanders named as contact.

2009 Sanders: "I am not responsible for this press release."

2005 id Quantique white paper "Future-proof Data Confidentiality with Quantum Cryptography":

"Finally, it is already proven that quantum computers[5] will allow to break public key cryptography."

"[5]Quantum computers are computers that exploit the laws of quantum physics to process information. They are still in the realm of experimental research, but will eventually be built."

2009 id Quantique erratum: "MOST CURRENTLY USED public key algorithms."

uantum computer is
d . . . then the levels of
y that we now have to
t our information on
ters will be worthless. It is
tely essential that quantum
graphy be developed out
quantum computers
e a reality."

y press release, 2004.
not clearly identified.
Sanders named as contact.

anders: "I am not
sible for this press release."

2005 id Quantique white paper "Future-proof Data Confidentiality with Quantum Cryptography":

"Finally, it is already proven that quantum computers[5] will allow to break public key cryptography."

"[5]Quantum computers are computers that exploit the laws of quantum physics to process information. They are still in the realm of experimental research, but will eventually be built."

2009 id Quantique erratum: "MOST CURRENTLY USED public key algorithms."

"Once
energy
comput
to prov
most e
standar
other s
comput
will fal

(Magiq
the "ex

omputer is
the levels of
now have to
mation on
e worthless. It is
ial that quantum
developed out
computers
"

ease, 2004.
y identified.
med as contact.

I am not
his press release."

2005 id Quantique white paper "Future-proof Data Confidentiality with Quantum Cryptography":

"Finally, it is already proven that quantum computers[5] will allow to break public key cryptography."

"[5]Quantum computers are computers that exploit the laws of quantum physics to process information. They are still in the realm of experimental research, but will eventually be built."

2009 id Quantique erratum: "MOST CURRENTLY USED public key algorithms."

"Once the enorm
energy boost tha
computers are ex
to provide hits th
most encryption
standards—and a
other standard ba
computational di
will fall, experts

(Magiq's web site
the "experts" are

of
to

s. It is
uantum
out
s

.
d.
ontact.

elease."

2005 id Quantique white paper "Future-proof Data Confidentiality with Quantum Cryptography":

"Finally, it is already proven that quantum computers[5] will allow to break public key cryptography."

"[5]Quantum computers are computers that exploit the laws of quantum physics to process information. They are still in the realm of experimental research, but will eventually be built."

2009 id Quantique erratum: "MOST CURRENTLY USED public key algorithms."

"Once the enormous energy boost that quantum computers are expected to provide hits the street, most encryption security standards—and any other standard based on computational difficulty—will fall, experts believe."

(Magiq's web site, 2008; the "experts" aren't named

2005 id Quantique white paper "Future-proof Data Confidentiality with Quantum Cryptography":

"Finally, it is already proven that quantum computers[5] will allow to break public key cryptography."

"[5]Quantum computers are computers that exploit the laws of quantum physics to process information. They are still in the realm of experimental research, but will eventually be built."

2009 id Quantique erratum:
"MOST CURRENTLY USED public key algorithms."

"Once the enormous energy boost that quantum computers are expected to provide hits the street, most encryption security standards—and any other standard based on computational difficulty—will fall, experts believe."

(Magiq's web site, 2008; the "experts" aren't named)

d Quantique white paper
e-proof Data Confidentiality
uantum Cryptography":

y, it is already proven that
m computers[5] will allow to
ublic key cryptography."

tum computers are computers
loit the laws of quantum physics
ss information. They are still in
m of experimental research, but
tually be built."

d Quantique erratum:
T CURRENTLY USED
key algorithms."

"Once the enormous
energy boost that quantum
computers are expected
to provide hits the street,
most encryption security
standards—and any
other standard based on
computational difficulty—
will fall, experts believe."

(Magiq's web site, 2008;
the "experts" aren't named)

Is cryp

Imagin
15 year
someon
success
of a lar

New Y
"INTE
KILLE

Users p

What h

ue white paper
ata Confidentiality
ryptography":

eady proven that
ters[5] will allow to
cryptography."

ers are computers
s of quantum physics
on. They are still in
nental research, but
ilt."

ue erratum:
NTLY USED
thms."

"Once the enormous
energy boost that quantum
computers are expected
to provide hits the street,
most encryption security
standards—and any
other standard based on
computational difficulty—
will fall, experts believe."

(Magiq's web site, 2008;
the "experts" aren't named)

Is cryptography d

Imagine:
15 years from no
someone announ
successful constr
of a large quantu

New York Times
"INTERNET CR
KILLED BY PH

Users panic.

What happens to

aper
entiality
hy":

n that
allow to
phy."

outers

n physics

e still in
ch, but

n:
ED

"Once the enormous
energy boost that quantum
computers are expected
to provide hits the street,
most encryption security
standards—and any
other standard based on
computational difficulty—
will fall, experts believe."

(Magiq's web site, 2008;
the "experts" aren't named)

<u>Is cryptography dead?</u>

Imagine:
15 years from now
someone announces
successful construction
of a large quantum comput

New York Times headline:
"INTERNET CRYPTOGRA
KILLED BY PHYSICISTS

Users panic.

What happens to cryptogra

"Once the enormous
energy boost that quantum
computers are expected
to provide hits the street,
most encryption security
standards—and any
other standard based on
computational difficulty—
will fall, experts believe."

(Magiq's web site, 2008;
the "experts" aren't named)

Is cryptography dead?

Imagine:
15 years from now
someone announces
successful construction
of a large quantum computer.

New York Times headline:
"INTERNET CRYPTOGRAPHY
KILLED BY PHYSICISTS."

Users panic.

What happens to cryptography?

the enormous
boost that quantum
ters are expected
vide hits the street,
ncryption security
rds—and any
tandard based on
tational difficulty—
l, experts believe."

q's web site, 2008;
xperts" aren't named)

Is cryptography dead?

Imagine:
15 years from now
someone announces
successful construction
of a large quantum computer.

New York Times headline:
"INTERNET CRYPTOGRAPHY
KILLED BY PHYSICISTS."

Users panic.

What happens to cryptography?

RSA: D

nous
t quantum
xpected
ne street,
security
any
ased on
fficulty—
believe."

e, 2008;
en't named)

Is cryptography dead?

Imagine:
15 years from now
someone announces
successful construction
of a large quantum computer.

New York Times headline:
"INTERNET CRYPTOGRAPHY
KILLED BY PHYSICISTS."

Users panic.

What happens to cryptography?

RSA: Dead.

n

d)

Is cryptography dead?

Imagine:
15 years from now
someone announces
successful construction
of a large quantum computer.

New York Times headline:
"INTERNET CRYPTOGRAPHY
KILLED BY PHYSICISTS."

Users panic.

What happens to cryptography?

RSA: Dead.

Is cryptography dead?

Imagine:
15 years from now
someone announces
successful construction
of a large quantum computer.

New York Times headline:
"INTERNET CRYPTOGRAPHY
KILLED BY PHYSICISTS."

Users panic.

What happens to cryptography?

RSA: Dead.

Is cryptography dead?

Imagine:
15 years from now
someone announces
successful construction
of a large quantum computer.

New York Times headline:
"INTERNET CRYPTOGRAPHY
KILLED BY PHYSICISTS."

Users panic.

What happens to cryptography?

RSA: Dead.

DSA: Dead.

ECDSA: Dead.

Is cryptography dead?

Imagine:
15 years from now
someone announces
successful construction
of a large quantum computer.

New York Times headline:
"INTERNET CRYPTOGRAPHY
KILLED BY PHYSICISTS."

Users panic.

What happens to cryptography?

RSA: Dead.

DSA: Dead.

ECDSA: Dead.

ECC in general: Dead.

HECC in general: Dead.

Is cryptography dead?

Imagine:
15 years from now
someone announces
successful construction
of a large quantum computer.

New York Times headline:
"INTERNET CRYPTOGRAPHY
KILLED BY PHYSICISTS."

Users panic.

What happens to cryptography?

RSA: Dead.

DSA: Dead.

ECDSA: Dead.

ECC in general: Dead.

HECC in general: Dead.

Buchmann–Williams: Dead.

Class groups in general: Dead.

Is cryptography dead?

Imagine:
15 years from now
someone announces
successful construction
of a large quantum computer.

New York Times headline:
"INTERNET CRYPTOGRAPHY
KILLED BY PHYSICISTS."

Users panic.

What happens to cryptography?

RSA: Dead.
DSA: Dead.
ECDSA: Dead.
ECC in general: Dead.
HECC in general: Dead.
Buchmann–Williams: Dead.
Class groups in general: Dead.

"They're all dead, Dave."

Is cryptography dead?

Imagine:
15 years from now
someone announces
successful construction
of a large quantum computer.

New York Times headline:
"INTERNET CRYPTOGRAPHY
KILLED BY PHYSICISTS."

Users panic.

What happens to cryptography?

RSA: Dead.
DSA: Dead.
ECDSA: Dead.
ECC in general: Dead.
HECC in general: Dead.
Buchmann–Williams: Dead.
Class groups in general: Dead.

"They're all dead, Dave."

But we have other types of
cryptographic systems!

Hash-based cryptography.
Example: 1979 Merkle hash-tree
public-key signature system.

tography dead?

e:

rs from now

ne announces

sful construction

rge quantum computer.

ork Times headline:

RNET CRYPTOGRAPHY

D BY PHYSICISTS."

panic.

happens to cryptography?

RSA: Dead.

DSA: Dead.

ECDSA: Dead.

ECC in general: Dead.

HECC in general: Dead.

Buchmann–Williams: Dead.

Class groups in general: Dead.

"They're all dead, Dave."

But we have other types of cryptographic systems!

Hash-based cryptography.
Example: 1979 Merkle hash-tree public-key signature system.

Code-
Examp
hidden-
public-

Lattice
Examp

Multiv
equati
Examp
1996 P
public-

Secret
Examp
"Rijnda

dead?

w
ces
uction
um computer.

headline:
RYPTOGRAPHY
YSICISTS."

o cryptography?

RSA: Dead.
DSA: Dead.
ECDSA: Dead.
ECC in general: Dead.
HECC in general: Dead.
Buchmann–Williams: Dead.
Class groups in general: Dead.

"They're all dead, Dave."

But we have other types of cryptographic systems!

Hash-based cryptography.
Example: 1979 Merkle hash-tree public-key signature system.

Code-based cry
Example: 1978 M
hidden-Goppa-co
public-key encryp

Lattice-based c
Example: 1998 "

Multivariate-qu
equations crypt
Example:
1996 Patarin "H
public-key signat

Secret-key cryp
Example: 1998 D
"Rijndael" ciphe

ter.

APHY

."

aphy?

RSA: Dead.
DSA: Dead.
ECDSA: Dead.
ECC in general: Dead.
HECC in general: Dead.
Buchmann–Williams: Dead.
Class groups in general: Dead.

"They're all dead, Dave."

But we have other types of cryptographic systems!

Hash-based cryptography.
Example: 1979 Merkle hash-tree public-key signature system.

Code-based cryptograph
Example: 1978 McEliece hidden-Goppa-code public-key encryption syste

Lattice-based cryptograp
Example: 1998 "NTRU."

Multivariate-quadratic-equations cryptography.
Example:
1996 Patarin "HFE^{v-}" public-key signature system

Secret-key cryptography.
Example: 1998 Daemen–R
"Rijndael" cipher, aka "AE

RSA: Dead.

DSA: Dead.

ECDSA: Dead.

ECC in general: Dead.

HECC in general: Dead.

Buchmann–Williams: Dead.

Class groups in general: Dead.

"They're all dead, Dave."

But we have other types of cryptographic systems!

Hash-based cryptography.
Example: 1979 Merkle hash-tree public-key signature system.

Code-based cryptography.
Example: 1978 McEliece hidden-Goppa-code public-key encryption system.

Lattice-based cryptography.
Example: 1998 "NTRU."

Multivariate-quadratic-equations cryptography.
Example:
1996 Patarin "HFE^{v-}" public-key signature system.

Secret-key cryptography.
Example: 1998 Daemen–Rijmen "Rijndael" cipher, aka "AES."

Dead.

Dead.

A: Dead.

general: Dead.

in general: Dead.

ann–Williams: Dead.

groups in general: Dead.

re all dead, Dave."

e have other types of

graphic systems!

based cryptography.

le: 1979 Merkle hash-tree

key signature system.

Code-based cryptography.

Example: 1978 McEliece

hidden-Goppa-code

public-key encryption system.

Lattice-based cryptography.

Example: 1998 "NTRU."

Multivariate-quadratic-equations cryptography.

Example:

1996 Patarin "HFE^{v-}"

public-key signature system.

Secret-key cryptography.

Example: 1998 Daemen–Rijmen

"Rijndael" cipher, aka "AES."

Dead.

: Dead.

ams: Dead.

general: Dead.

d, Dave."

er types of

stems!

ptography.

Merkle hash-tree

ure system.

Code-based cryptography.
Example: 1978 McEliece
hidden-Goppa-code
public-key encryption system.

Lattice-based cryptography.
Example: 1998 "NTRU."

Multivariate-quadratic-equations cryptography.
Example:
1996 Patarin "HFE^{v-}"
public-key signature system.

Secret-key cryptography.
Example: 1998 Daemen–Rijmen
"Rijndael" cipher, aka "AES."

d.
ead.

f

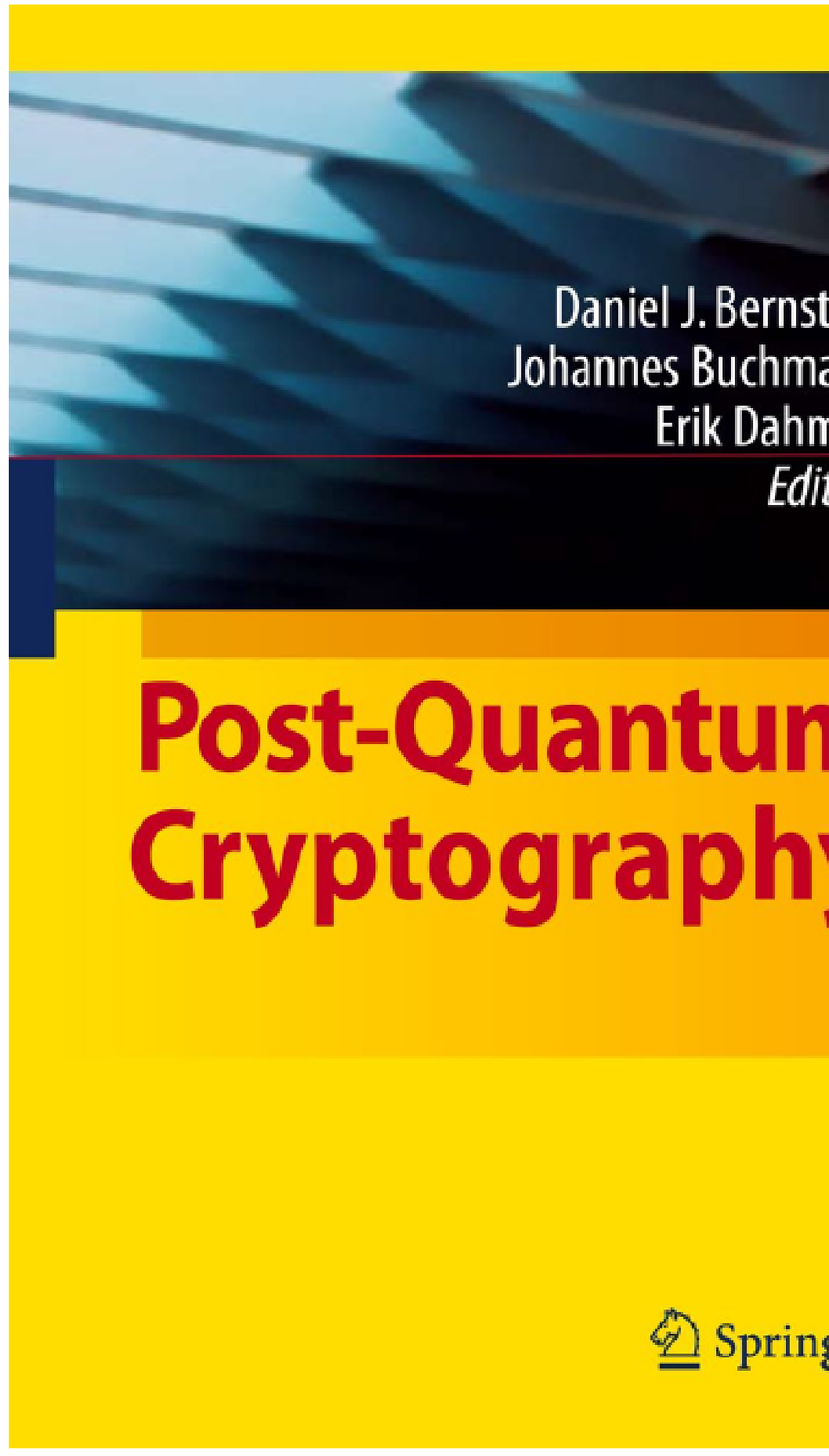
y.
h-tree
n.

Code-based cryptography.
Example: 1978 McEliece
hidden-Goppa-code
public-key encryption system.

Lattice-based cryptography.
Example: 1998 “NTRU.”

Multivariate-quadratic-equations cryptography.
Example:
1996 Patarin “HFE^{v-}”
public-key signature system.

Secret-key cryptography.
Example: 1998 Daemen–Rijmen
“Rijndael” cipher, aka “AES.”

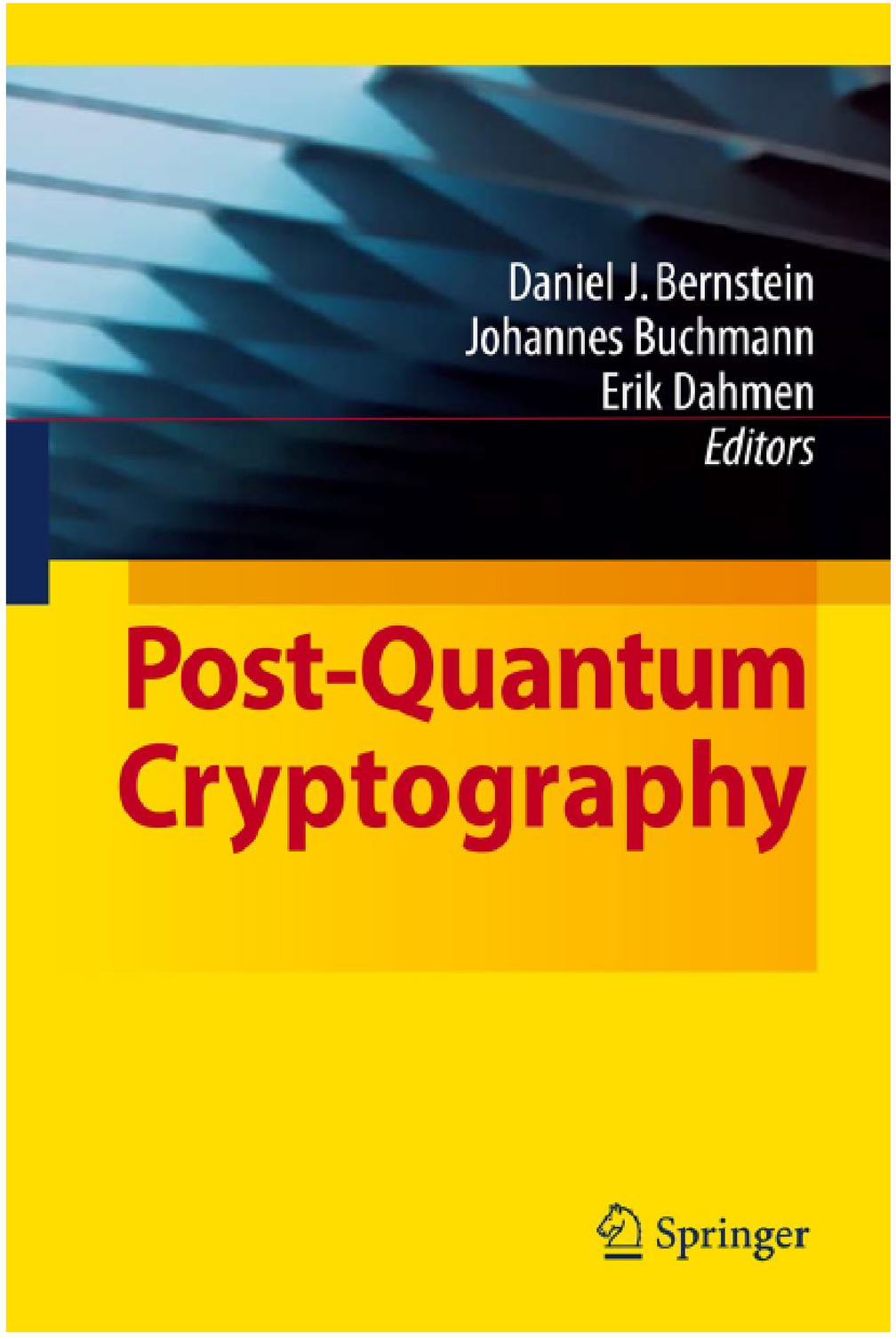


Code-based cryptography.
Example: 1978 McEliece
hidden-Goppa-code
public-key encryption system.

Lattice-based cryptography.
Example: 1998 "NTRU."

Multivariate-quadratic-equations cryptography.
Example:
1996 Patarin "HFE^{v-}"
public-key signature system.

Secret-key cryptography.
Example: 1998 Daemen–Rijmen
"Rijndael" cipher, aka "AES."

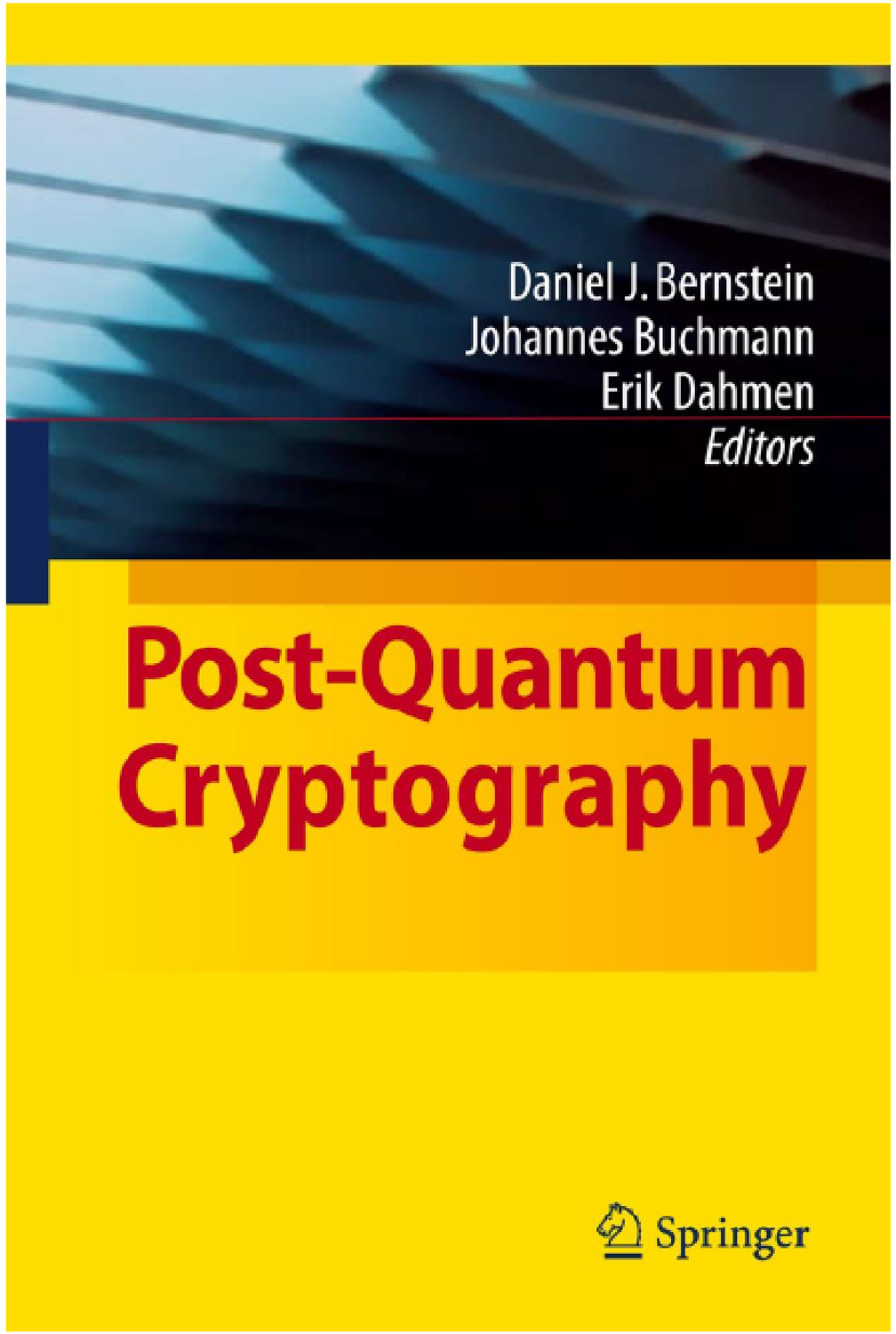


based cryptography.
le: 1978 McEliece
-Goppa-code
key encryption system.

e-based cryptography.
le: 1998 "NTRU."

variate-quadratic-
ons cryptography.
le:
Patarin "HFE^{v-}"
key signature system.

-key cryptography.
le: 1998 Daemen–Rijmen
ael" cipher, aka "AES."



Bernste
post-qu

Hallgre
"Quant

Buchm
"Hash-
scheme

Overbe
"Code-

Miccia
"Lattic

Ding, Y
public

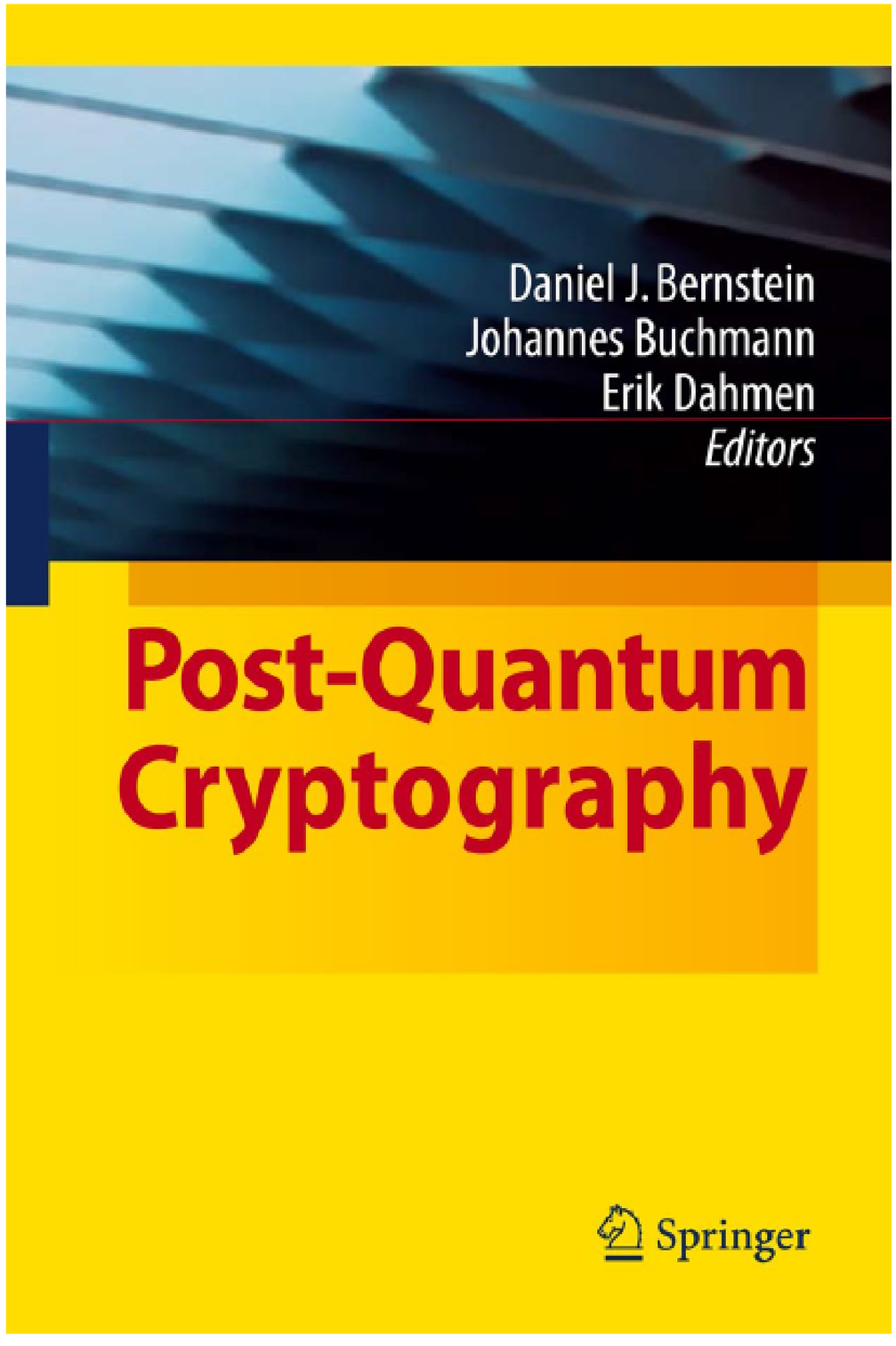
ptography.
McEliece
de
ption system.

ryptography.
"NTRU."

adratic-
ography.

FE^{v-}"
ure system.

tography.
Daemen–Rijmen
r, aka "AES."



Bernstein: "Intro
post-quantum cr

Hallgren, Vollme
"Quantum comp

Buchmann, Dahr
"Hash-based digi
schemes."

Overbeck, Sendri
"Code-based cryp

Micciancio, Rege
"Lattice-based cr

Ding, Yang: "Mu
public key crypto

y.

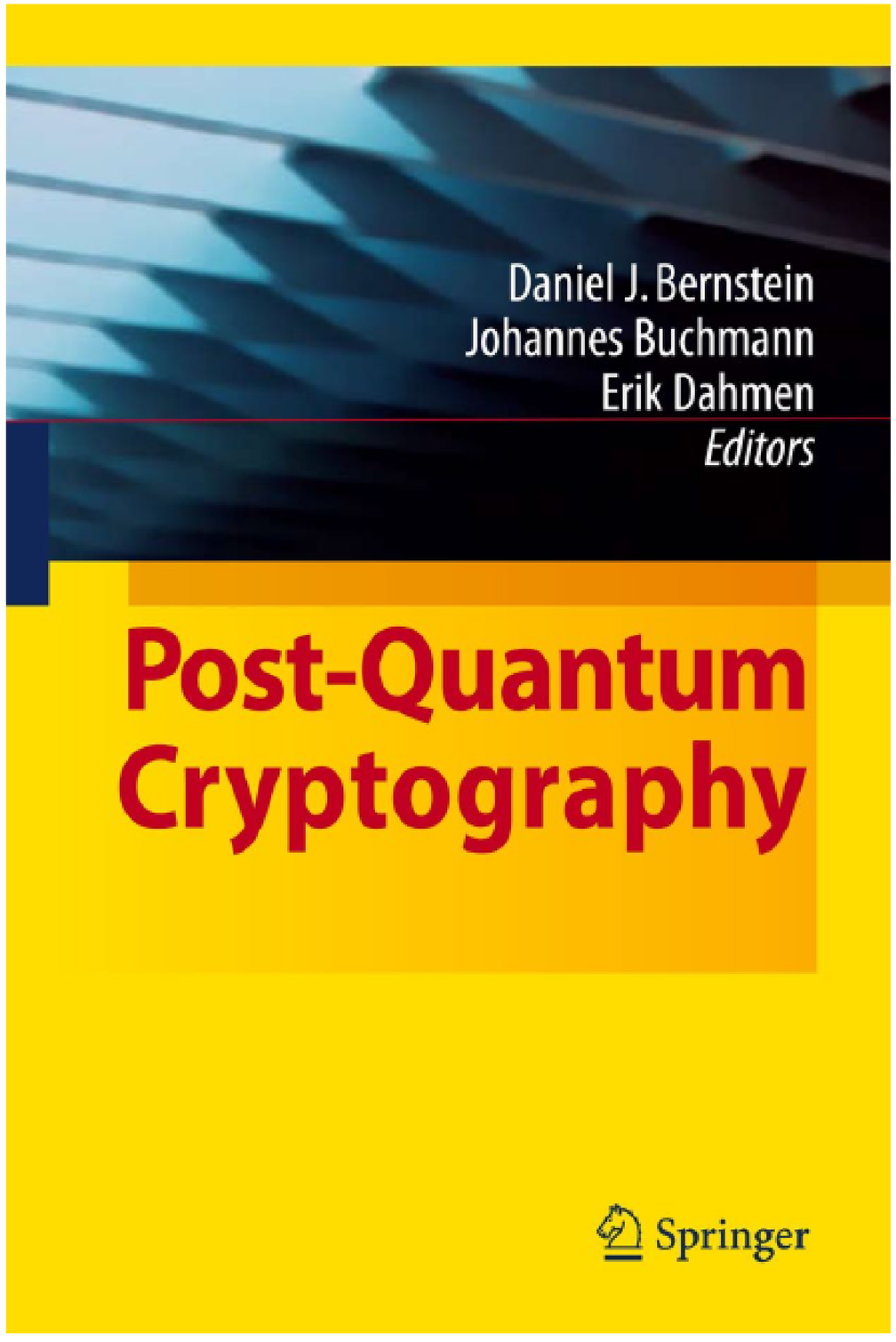
em.

phy.

n.

ijmen

ES."



Bernstein: "Introduction to post-quantum cryptograph

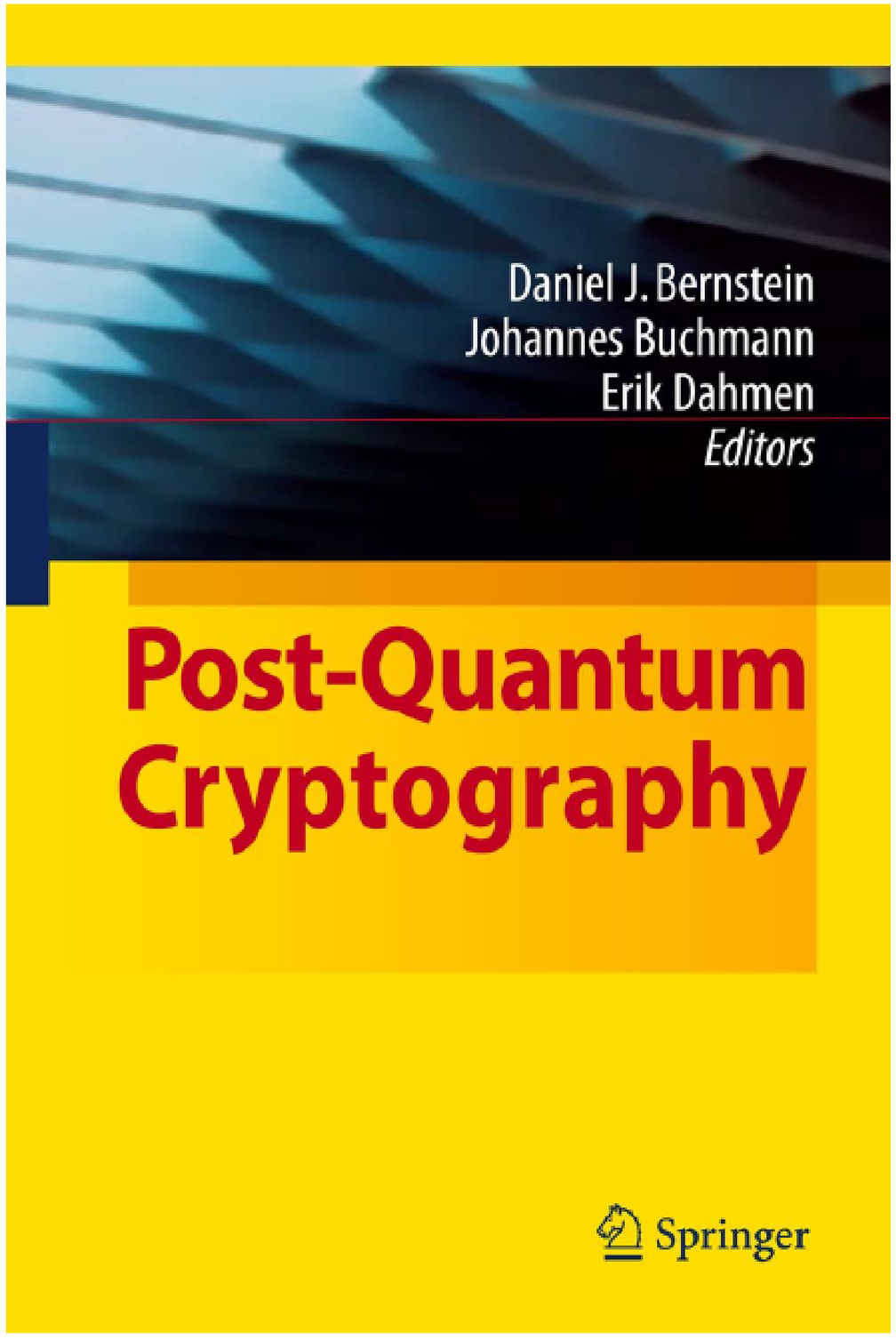
Hallgren, Vollmer: "Quantum computing."

Buchmann, Dahmen, Szyd "Hash-based digital signatu schemes."

Overbeck, Sendrier: "Code-based cryptography.

Micciancio, Regev: "Lattice-based cryptograph

Ding, Yang: "Multivariate public key cryptography."



Bernstein: "Introduction to post-quantum cryptography."

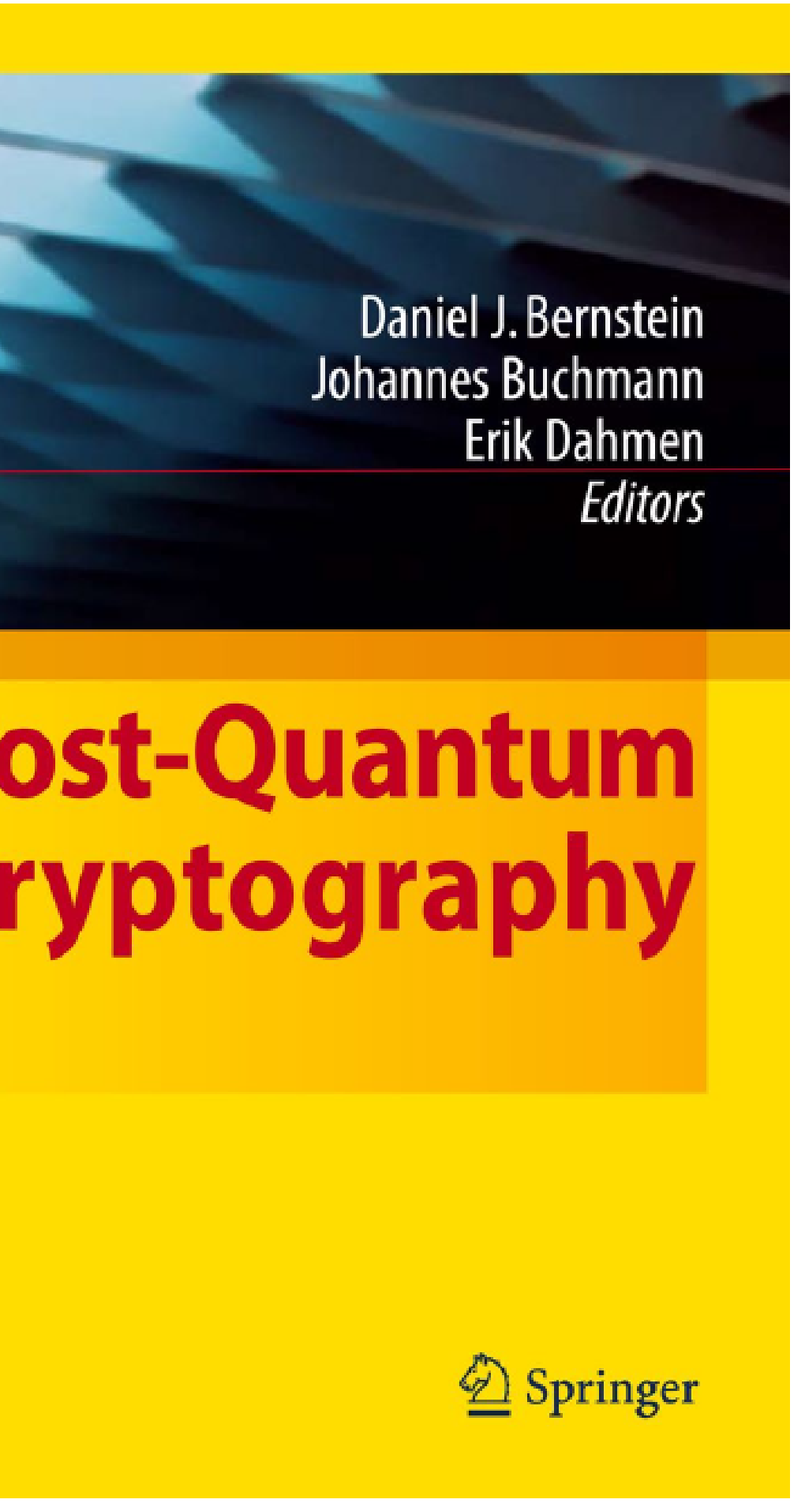
Hallgren, Vollmer: "Quantum computing."

Buchmann, Dahmen, Szydlo: "Hash-based digital signature schemes."

Overbeck, Sendrier: "Code-based cryptography."

Micciancio, Regev: "Lattice-based cryptography."

Ding, Yang: "Multivariate public key cryptography."



Bernstein: "Introduction to post-quantum cryptography."

Hallgren, Vollmer: "Quantum computing."

Buchmann, Dahmen, Szydlo: "Hash-based digital signature schemes."

Overbeck, Sendrier: "Code-based cryptography."

Micciancio, Regev: "Lattice-based cryptography."

Ding, Yang: "Multivariate public key cryptography."

The M

Receive

$500 \times$

Specifi

Messag

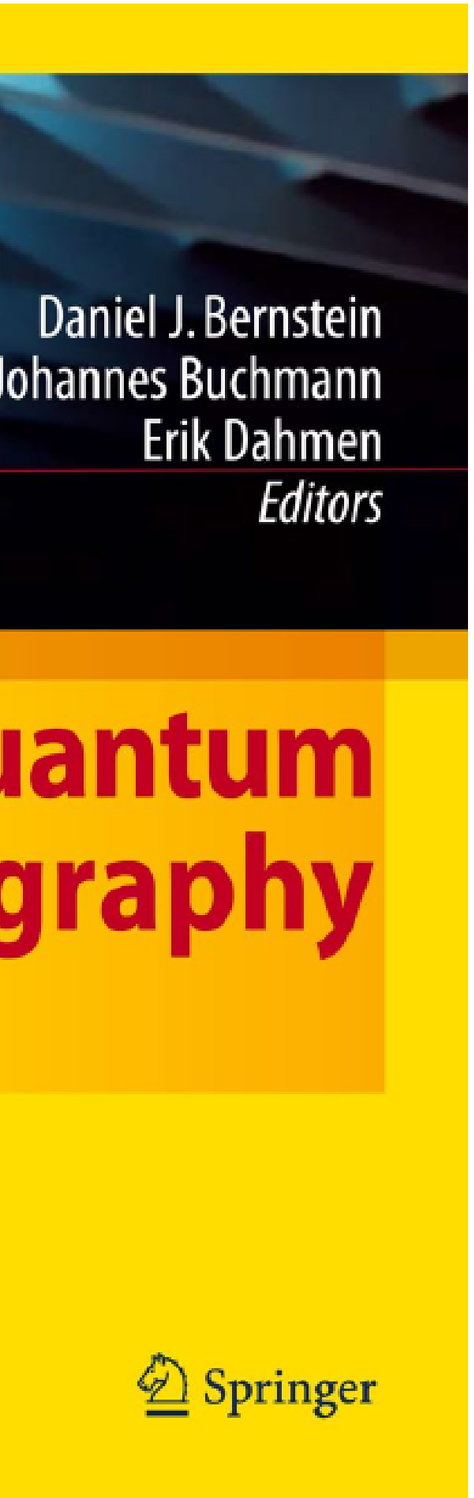
1024-b

i.e., $\{m$

Encryp

Can us

to encr



Bernstein: "Introduction to post-quantum cryptography."

Hallgren, Vollmer: "Quantum computing."

Buchmann, Dahmen, Szydlo: "Hash-based digital signature schemes."

Overbeck, Sendrier: "Code-based cryptography."

Micciancio, Regev: "Lattice-based cryptography."

Ding, Yang: "Multivariate public key cryptography."

The McEliece cry

Receiver's public
500×1024 matr
Specifies linear **F**

Messages suitabl
1024-bit strings
i.e., $\{m \in \mathbf{F}_2^{1024}$
$\#\{i : m_i$

Encryption of m

Can use m as se
to encrypt much

Bernstein: "Introduction to post-quantum cryptography."

Hallgren, Vollmer: "Quantum computing."

Buchmann, Dahmen, Szydlo: "Hash-based digital signature schemes."

Overbeck, Sendrier: "Code-based cryptography."

Micciancio, Regev: "Lattice-based cryptography."

Ding, Yang: "Multivariate public key cryptography."

The McEliece cryptosystem

Receiver's public key: "ran

500×1024 matrix K over

Specifies linear $\mathbf{F}_2^{1024} \to \mathbf{F}_2^5$

Messages suitable for encry

1024-bit strings of weight 5

i.e., $\{m \in \mathbf{F}_2^{1024} :$

$\#\{i : m_i = 1\} = 50$

Encryption of m is $Km \in$

Can use m as secret AES k

to encrypt much more data

Bernstein: "Introduction to post-quantum cryptography."

Hallgren, Vollmer: "Quantum computing."

Buchmann, Dahmen, Szydlo: "Hash-based digital signature schemes."

Overbeck, Sendrier: "Code-based cryptography."

Micciancio, Regev: "Lattice-based cryptography."

Ding, Yang: "Multivariate public key cryptography."

The McEliece cryptosystem

Receiver's public key: "random" 500×1024 matrix K over $\mathbf{F}_2$. Specifies linear $\mathbf{F}_2^{1024} \to \mathbf{F}_2^{500}$.

Messages suitable for encryption: 1024-bit strings of weight 50; i.e., $\{m \in \mathbf{F}_2^{1024} :$

$$\#\{i : m_i = 1\} = 50\}.$$

Encryption of m is $Km \in \mathbf{F}_2^{500}$.

Can use m as secret AES key to encrypt much more data.

ein: "Introduction to
uantum cryptography."

en, Vollmer:
tum computing."

ann, Dahmen, Szydlo:
-based digital signature
es."

eck, Sendrier:
-based cryptography."

ncio, Regev:
ce-based cryptography."

Yang: "Multivariate
key cryptography."

The McEliece cryptosystem

Receiver's public key: "random"
500×1024 matrix K over $\mathbf{F}_2$.
Specifies linear $\mathbf{F}_2^{1024} \to \mathbf{F}_2^{500}$.

Messages suitable for encryption:
1024-bit strings of weight 50;
i.e., $\{m \in \mathbf{F}_2^{1024} :$
$\#\{i : m_i = 1\} = 50\}$.

Encryption of m is $Km \in \mathbf{F}_2^{500}$.

Can use m as secret AES key
to encrypt much more data.

Attacke
can eas
from K
such th

i.e. Att
elemen
Note th

Attacke
to find
at dista
Presum

But de

oduction to
yptography."

r:
uting."

men, Szydlo:
ital signature

ier:
ptography."

ev:
ryptography."

ultivariate
ography."

The McEliece cryptosystem

Receiver's public key: "random"
500×1024 matrix K over $\mathbf{F}_2$.
Specifies linear $\mathbf{F}_2^{1024} \to \mathbf{F}_2^{500}$.

Messages suitable for encryption:
1024-bit strings of weight 50;
i.e., $\{m \in \mathbf{F}_2^{1024} :$
$\#\{i : m_i = 1\} = 50\}$.

Encryption of m is $Km \in \mathbf{F}_2^{500}$.

Can use m as secret AES key
to encrypt much more data.

Attacker, by linea
can easily work b
from Km to *som*
such that $Kv =$

i.e. Attacker finc
element $v \in m +$
Note that $\#\mathrm{Ker}K$

Attacker wants t
to find element c
at distance only
Presumably uniq

But decoding isn

o
y."
lo:
ure
."
ny."

The McEliece cryptosystem

Receiver's public key: "random"
500×1024 matrix K over $\mathbf{F}_2$.
Specifies linear $\mathbf{F}_2^{1024} \to \mathbf{F}_2^{500}$.

Messages suitable for encryption:
1024-bit strings of weight 50;
i.e., $\{m \in \mathbf{F}_2^{1024} :$
$\#\{i : m_i = 1\} = 50\}$.

Encryption of m is $Km \in \mathbf{F}_2^{500}$.

Can use m as secret AES key
to encrypt much more data.

Attacker, by linear algebra,
can easily work backwards
from Km to *some* $v \in \mathbf{F}_2^{10}$
such that $Kv = Km$.

i.e. Attacker finds *some*
element $v \in m + \mathrm{Ker}K$.
Note that $\#\mathrm{Ker}K \geq 2^{524}$.

Attacker wants to decode
to find element of $\mathrm{Ker}K$
at distance only 50 from v
Presumably unique, reveali

But decoding isn't easy!

The McEliece cryptosystem

Receiver's public key: "random"
500×1024 matrix K over $\mathbf{F}_2$.
Specifies linear $\mathbf{F}_2^{1024} \to \mathbf{F}_2^{500}$.

Messages suitable for encryption:
1024-bit strings of weight 50;
i.e., $\{m \in \mathbf{F}_2^{1024} :$

$$\#\{i : m_i = 1\} = 50\}.$$

Encryption of m is $Km \in \mathbf{F}_2^{500}$.

Can use m as secret AES key
to encrypt much more data.

Attacker, by linear algebra,
can easily work backwards
from Km to *some* $v \in \mathbf{F}_2^{1024}$
such that $Kv = Km$.

i.e. Attacker finds *some*
element $v \in m + \mathrm{Ker}K$.
Note that $\#\mathrm{Ker}K \geq 2^{524}$.

Attacker wants to decode v:
to find element of $\mathrm{Ker}K$
at distance only 50 from v.
Presumably unique, revealing m.

But decoding isn't easy!

cEliece cryptosystem

er's public key: "random"
1024 matrix K over $\mathbf{F}_2$.
es linear $\mathbf{F}_2^{1024} \to \mathbf{F}_2^{500}$.

ges suitable for encryption:
it strings of weight 50;
$n \in \mathbf{F}_2^{1024}$:
$\#\{i : m_i = 1\} = 50\}$.

tion of m is $Km \in \mathbf{F}_2^{500}$.

e m as secret AES key
rypt much more data.

Attacker, by linear algebra,
can easily work backwards
from Km to *some* $v \in \mathbf{F}_2^{1024}$
such that $Kv = Km$.

i.e. Attacker finds *some*
element $v \in m + \mathrm{Ker}K$.
Note that $\#\mathrm{Ker}K \geq 2^{524}$.

Attacker wants to decode v:
to find element of $\mathrm{Ker}K$
at distance only 50 from v.
Presumably unique, revealing m.

But decoding isn't easy!

Informa

Choose
$S \subseteq \{1$

For typ
that $\mathbf{F}_2^{\$}$
is inver

Hope m
Apply i
revealin

If $m \notin$
$\approx 2^{80}$ c

yptosystem

key: "random"
ix K over $\mathbf{F}_2$.
$\mathbf{F}_2^{1024} \to \mathbf{F}_2^{500}$.

e for encryption:
of weight 50;
:
$= 1\} = 50\}$.

is $Km \in \mathbf{F}_2^{500}$.

cret AES key
more data.

Attacker, by linear algebra,
can easily work backwards
from Km to *some* $v \in \mathbf{F}_2^{1024}$
such that $Kv = Km$.

i.e. Attacker finds *some*
element $v \in m + \mathrm{Ker}K$.
Note that $\#\mathrm{Ker}K \geq 2^{524}$.

Attacker wants to decode v:
to find element of $\mathrm{Ker}K$
at distance only 50 from v.
Presumably unique, revealing m.

But decoding isn't easy!

Information-set d

Choose random s
$S \subseteq \{1, 2, 3, \ldots,$

For typical K: G
that $\mathbf{F}_2^S \hookrightarrow \mathbf{F}_2^{1024}$
is invertible.

Hope $m \in \mathbf{F}_2^S$; c
Apply inverse ma
revealing m if m

If $m \notin \mathbf{F}_2^S$, try ag
$\approx 2^{80}$ operations

n

ndom"
$\mathbf{F}_2$.
$^{500}_2$.

yption:
50;

0}.
$\mathbf{F}_2^{500}$.

key
a.

Attacker, by linear algebra,
can easily work backwards
from Km to *some* $v \in \mathbf{F}_2^{1024}$
such that $Kv = Km$.

i.e. Attacker finds *some*
element $v \in m + \mathrm{Ker}K$.
Note that $\#\mathrm{Ker}K \geq 2^{524}$.

Attacker wants to decode v:
to find element of $\mathrm{Ker}K$
at distance only 50 from v.
Presumably unique, revealing m.

But decoding isn't easy!

Information-set decoding

Choose random size-500 su
$S \subseteq \{1, 2, 3, \ldots, 1024\}$.

For typical K: Good chanc
that $\mathbf{F}_2^S \hookrightarrow \mathbf{F}_2^{1024} \xrightarrow{K} \mathbf{F}_2^{50}$
is invertible.

Hope $m \in \mathbf{F}_2^S$; chance ≈ 2
Apply inverse map to Km,
revealing m if $m \in \mathbf{F}_2^S$.

If $m \notin \mathbf{F}_2^S$, try again.
$\approx 2^{80}$ operations overall.

Attacker, by linear algebra,
can easily work backwards
from Km to *some* $v \in \mathbf{F}_2^{1024}$
such that $Kv = Km$.

i.e. Attacker finds *some*
element $v \in m + \mathsf{Ker}K$.
Note that $\#\mathsf{Ker}K \geq 2^{524}$.

Attacker wants to decode v:
to find element of $\mathsf{Ker}K$
at distance only 50 from v.
Presumably unique, revealing m.

But decoding isn't easy!

Information-set decoding

Choose random size-500 subset
$S \subseteq \{1, 2, 3, \ldots, 1024\}$.

For typical K: Good chance
that $\mathbf{F}_2^S \hookrightarrow \mathbf{F}_2^{1024} \xrightarrow{K} \mathbf{F}_2^{500}$
is invertible.

Hope $m \in \mathbf{F}_2^S$; chance $\approx 2^{-53}$.
Apply inverse map to Km,
revealing m if $m \in \mathbf{F}_2^S$.

If $m \notin \mathbf{F}_2^S$, try again.
$\approx 2^{80}$ operations overall.

er, by linear algebra,
sily work backwards
Km to *some* $v \in \mathbf{F}_2^{1024}$
hat $Kv = Km$.

tacker finds *some*
t $v \in m + \mathsf{Ker}K$.
hat $\#\mathsf{Ker}K \geq 2^{524}$.

er wants to decode v:
element of $\mathsf{Ker}K$
ance only 50 from v.
nably unique, revealing m.

coding isn't easy!

Information-set decoding

Choose random size-500 subset
$S \subseteq \{1, 2, 3, \ldots, 1024\}$.

For typical K: Good chance
that $\mathbf{F}_2^S \hookrightarrow \mathbf{F}_2^{1024} \xrightarrow{K} \mathbf{F}_2^{500}$
is invertible.

Hope $m \in \mathbf{F}_2^S$; chance $\approx 2^{-53}$.
Apply inverse map to Km,
revealing m if $m \in \mathbf{F}_2^S$.

If $m \notin \mathbf{F}_2^S$, try again.
$\approx 2^{80}$ operations overall.

Various

1988 L

1988 L

1989 S

1990 v

1994 C

1998 C

1998 C

2^{68} Alp

2008 B
further
2^{58} Co
carried

ar algebra,
backwards
ne $v \in \mathbf{F}_2^{1024}$
Km.

ls *some*
– Ker$K$.
$K \geq 2^{524}$.

o decode v:
of Ker$K$
50 from v.
ue, revealing m.

't easy!

Information-set decoding

Choose random size-500 subset
$S \subseteq \{1, 2, 3, \ldots, 1024\}$.

For typical K: Good chance
that $\mathbf{F}_2^S \hookrightarrow \mathbf{F}_2^{1024} \xrightarrow{K} \mathbf{F}_2^{500}$
is invertible.

Hope $m \in \mathbf{F}_2^S$; chance $\approx 2^{-53}$.
Apply inverse map to Km,
revealing m if $m \in \mathbf{F}_2^S$.

If $m \notin \mathbf{F}_2^S$, try again.
$\approx 2^{80}$ operations overall.

Various improven
1988 Lee–Brickel
1988 Leon;
1989 Stern;
1990 van Tilburg
1994 Canteaut–C
1998 Canteaut–C
1998 Canteaut–S
2^{68} Alpha cycles.

2008 Bernstein–L
further improvem
2^{58} Core 2 Quad
carried out succe

024

v:

.

ng m.

Information-set decoding

Choose random size-500 subset $S \subseteq \{1, 2, 3, \ldots, 1024\}$.

For typical K: Good chance that $\mathbf{F}_2^S \hookrightarrow \mathbf{F}_2^{1024} \xrightarrow{K} \mathbf{F}_2^{500}$ is invertible.

Hope $m \in \mathbf{F}_2^S$; chance $\approx 2^{-53}$.
Apply inverse map to Km, revealing m if $m \in \mathbf{F}_2^S$.

If $m \notin \mathbf{F}_2^S$, try again.
$\approx 2^{80}$ operations overall.

Various improvements:

1988 Lee–Brickell;

1988 Leon;

1989 Stern;

1990 van Tilburg;

1994 Canteaut–Chabanne;

1998 Canteaut–Chabaud;

1998 Canteaut–Sendrier.

2^{68} Alpha cycles.

2008 Bernstein–Lange–Pet
further improvements;
2^{58} Core 2 Quad cycles;
carried out successfully!

Information-set decoding

Choose random size-500 subset $S \subseteq \{1, 2, 3, \ldots, 1024\}$.

For typical K: Good chance that $\mathbf{F}_2^S \hookrightarrow \mathbf{F}_2^{1024} \xrightarrow{K} \mathbf{F}_2^{500}$ is invertible.

Hope $m \in \mathbf{F}_2^S$; chance $\approx 2^{-53}$.
Apply inverse map to Km, revealing m if $m \in \mathbf{F}_2^S$.

If $m \notin \mathbf{F}_2^S$, try again.
$\approx 2^{80}$ operations overall.

Various improvements:

1988 Lee–Brickell;

1988 Leon;

1989 Stern;

1990 van Tilburg;

1994 Canteaut–Chabanne;

1998 Canteaut–Chabaud;

1998 Canteaut–Sendrier.

2^{68} Alpha cycles.

2008 Bernstein–Lange–Peters:
further improvements;
2^{58} Core 2 Quad cycles;
carried out successfully!

ation-set decoding

e random size-500 subset
$1, 2, 3, \ldots, 1024\}$.

pical K: Good chance
$\mathbf{F}_2^S \hookrightarrow \mathbf{F}_2^{1024} \xrightarrow{K} \mathbf{F}_2^{500}$
rtible.

$m \in \mathbf{F}_2^S$; chance $\approx 2^{-53}$.
inverse map to Km,
ng m if $m \in \mathbf{F}_2^S$.

$\mathbf{F}_2^S$, try again.
operations overall.

Various improvements:
1988 Lee–Brickell;
1988 Leon;
1989 Stern;
1990 van Tilburg;
1994 Canteaut–Chabanne;
1998 Canteaut–Chabaud;
1998 Canteaut–Sendrier.
2^{68} Alpha cycles.

2008 Bernstein–Lange–Peters:
further improvements;
2^{58} Core 2 Quad cycles;
carried out successfully!

1988 L
Hope t
for som
Reuse
for all

1989 S
Hope t
for low
Search
functio

2008 B
more re

decoding

size-500 subset
1024}.

ood chance
$\xrightarrow{K}$ $\mathbf{F}_2^{500}$

hance $\approx 2^{-53}$.
ap to Km,
$\in \mathbf{F}_2^S$.

gain.
overall.

Various improvements:
1988 Lee–Brickell;
1988 Leon;
1989 Stern;
1990 van Tilburg;
1994 Canteaut–Chabanne;
1998 Canteaut–Chabaud;
1998 Canteaut–Sendrier.
2^{68} Alpha cycles.

2008 Bernstein–Lange–Peters:
further improvements;
2^{58} Core 2 Quad cycles;
carried out successfully!

1988 Lee–Brickell
Hope that $m + e$
for some weight-
Reuse one matrix
for all choices of

1989 Stern idea:
Hope that $m + e$
for low-weight ve
Search for collisio
function of e, fu

2008 Bernstein–L
more reuse, optim

ubset

ce
00

$^{-53}$.

Various improvements:
1988 Lee–Brickell;
1988 Leon;
1989 Stern;
1990 van Tilburg;
1994 Canteaut–Chabanne;
1998 Canteaut–Chabaud;
1998 Canteaut–Sendrier.
2^{68} Alpha cycles.

2008 Bernstein–Lange–Peters:
further improvements;
2^{58} Core 2 Quad cycles;
carried out successfully!

1988 Lee–Brickell idea:
Hope that $m + e \in \mathbf{F}_2^S$
for some weight-2 vector e
Reuse one matrix inversion
for all choices of e.

1989 Stern idea:
Hope that $m + e + e' \in \mathbf{F}$
for low-weight vectors e, e'
Search for collision betwee
function of e, function of e

2008 Bernstein–Lange–Pet
more reuse, optimization, e

Various improvements:
1988 Lee–Brickell;
1988 Leon;
1989 Stern;
1990 van Tilburg;
1994 Canteaut–Chabanne;
1998 Canteaut–Chabaud;
1998 Canteaut–Sendrier.
2^{68} Alpha cycles.

2008 Bernstein–Lange–Peters:
further improvements;
2^{58} Core 2 Quad cycles;
carried out successfully!

1988 Lee–Brickell idea:
Hope that $m + e \in \mathbf{F}_2^S$
for some weight-2 vector e.
Reuse one matrix inversion
for all choices of e.

1989 Stern idea:
Hope that $m + e + e' \in \mathbf{F}_2^S$
for low-weight vectors e, e'.
Search for collision between
function of e, function of e'.

2008 Bernstein–Lange–Peters:
more reuse, optimization, etc.

s improvements:
ee–Brickell;
eon;
tern;
an Tilburg;
anteaut–Chabanne;
anteaut–Chabaud;
anteaut–Sendrier.
pha cycles.

Bernstein–Lange–Peters:
improvements;
re 2 Quad cycles;
out successfully!

1988 Lee–Brickell idea:
Hope that $m + e \in \mathbf{F}_2^S$
for some weight-2 vector e.
Reuse one matrix inversion
for all choices of e.

1989 Stern idea:
Hope that $m + e + e' \in \mathbf{F}_2^S$
for low-weight vectors e, e'.
Search for collision between
function of e, function of e'.

2008 Bernstein–Lange–Peters:
more reuse, optimization, etc.

Modern

Easily
a large
$(n/2)$
e.g., 18

Larger
e.g. m

All kno
roughly
For mu
see 200
Peters–

ments:
ll;

g;
Chabanne;
Chabaud;
Sendrier.

Lange–Peters:
nents;
cycles;
ssfully!

1988 Lee–Brickell idea:
Hope that $m + e \in \mathbf{F}_2^S$
for some weight-2 vector e.
Reuse one matrix inversion
for all choices of e.

1989 Stern idea:
Hope that $m + e + e' \in \mathbf{F}_2^S$
for low-weight vectors e, e'.
Search for collision between
function of e, function of e'.

2008 Bernstein–Lange–Peters:
more reuse, optimization, etc.

Modern McEliece

Easily rescue syst
a larger public ke
$(n/2) \times n$ matrix
e.g., 1800×3600

Larger weight: $\approx$
e.g. $m \in \mathbf{F}_2^{3600}$ o

All known attack
roughly $2^{n/(2 \lg n)}$
For much more p
see 2009 Bernste
Peters–van Tilbo

ers:

1988 Lee–Brickell idea:
Hope that $m + e \in \mathbf{F}_2^S$
for some weight-2 vector e.
Reuse one matrix inversion
for all choices of e.

1989 Stern idea:
Hope that $m + e + e' \in \mathbf{F}_2^S$
for low-weight vectors e, e'.
Search for collision between
function of e, function of e'.

2008 Bernstein–Lange–Peters:
more reuse, optimization, etc.

Modern McEliece

Easily rescue system by usi
a larger public key: "rando
$(n/2) \times n$ matrix K over **F**
e.g., 1800×3600.

Larger weight: $\approx n/(2 \lg n$
e.g. $m \in \mathbf{F}_2^{3600}$ of weight 1

All known attacks scale ba
roughly $2^{n/(2 \lg n)}$ operatio
For much more precise ana
see 2009 Bernstein–Lange–
Peters–van Tilborg.

1988 Lee–Brickell idea:
Hope that $m + e \in \mathbf{F}_2^S$
for some weight-2 vector e.
Reuse one matrix inversion
for all choices of e.

1989 Stern idea:
Hope that $m + e + e' \in \mathbf{F}_2^S$
for low-weight vectors e, e'.
Search for collision between
function of e, function of e'.

2008 Bernstein–Lange–Peters:
more reuse, optimization, etc.

Modern McEliece

Easily rescue system by using
a larger public key: "random"
$(n/2) \times n$ matrix K over $\mathbf{F}_2$.
e.g., 1800×3600.

Larger weight: $\approx n/(2 \lg n)$.
e.g. $m \in \mathbf{F}_2^{3600}$ of weight 150.

All known attacks scale badly:
roughly $2^{n/(2 \lg n)}$ operations.
For much more precise analysis
see 2009 Bernstein–Lange–
Peters–van Tilborg.

ee–Brickell idea:
hat $m + e \in \mathbf{F}_2^S$
ne weight-2 vector e.
one matrix inversion
choices of e.

tern idea:
hat $m + e + e' \in \mathbf{F}_2^S$
-weight vectors e, e'.
for collision between
n of e, function of e'.

Bernstein–Lange–Peters:
euse, optimization, etc.

Modern McEliece

Easily rescue system by using a larger public key: "random" $(n/2) \times n$ matrix K over $\mathbf{F}_2$. e.g., 1800×3600.

Larger weight: $\approx n/(2 \lg n)$. e.g. $m \in \mathbf{F}_2^{3600}$ of weight 150.

All known attacks scale badly: roughly $2^{n/(2 \lg n)}$ operations. For much more precise analysis see 2009 Bernstein–Lange–Peters–van Tilborg.

Receive
public
hidden
that al

Namely
$(n/2) \times$
$(n/2) \times$
$n \times n$

Detecti
seems
than at

ll idea:
$e \in \mathbf{F}_2^S$
2 vector e.
k inversion
e.

$e + e' \in \mathbf{F}_2^S$
ectors e, e'.
on between
nction of e'.

Lange–Peters:
mization, etc.

Modern McEliece

Easily rescue system by using a larger public key: "random" $(n/2) \times n$ matrix K over $\mathbf{F}_2$. e.g., 1800×3600.

Larger weight: $\approx n/(2 \lg n)$. e.g. $m \in \mathbf{F}_2^{3600}$ of weight 150.

All known attacks scale badly: roughly $2^{n/(2 \lg n)}$ operations. For much more precise analysis see 2009 Bernstein–Lange–Peters–van Tilborg.

Receiver secretly
public key K wit
hidden Goppa-co
that allows fast d

Namely: $K = SI$
$(n/2) \times (n/2)$ in
$(n/2) \times n$ Goppa
$n \times n$ permutati

Detecting this st
seems even more
than attacking ra

.

S
$_2$
.

n
e'.

ers:

etc.

Modern McEliece

Easily rescue system by using a larger public key: "random" $(n/2) \times n$ matrix K over $\mathbf{F}_2$. e.g., 1800×3600.

Larger weight: $\approx n/(2 \lg n)$. e.g. $m \in \mathbf{F}_2^{3600}$ of weight 150.

All known attacks scale badly: roughly $2^{n/(2 \lg n)}$ operations. For much more precise analysis see 2009 Bernstein–Lange–Peters–van Tilborg.

Receiver secretly generates public key K with a hidden Goppa-code structu that allows fast decoding.

Namely: $K = SHP$ for sec $(n/2) \times (n/2)$ invertible m $(n/2) \times n$ Goppa matrix H $n \times n$ permutation matrix

Detecting this structure seems even more difficult than attacking random K.

Modern McEliece

Easily rescue system by using a larger public key: "random" $(n/2) \times n$ matrix K over $\mathbf{F}_2$. e.g., 1800×3600.

Larger weight: $\approx n/(2 \lg n)$. e.g. $m \in \mathbf{F}_2^{3600}$ of weight 150.

All known attacks scale badly: roughly $2^{n/(2 \lg n)}$ operations. For much more precise analysis see 2009 Bernstein–Lange–Peters–van Tilborg.

Receiver secretly generates public key K with a hidden Goppa-code structure that allows fast decoding.

Namely: $K = SHP$ for secret $(n/2) \times (n/2)$ invertible matrix S, $(n/2) \times n$ Goppa matrix H, $n \times n$ permutation matrix P.

Detecting this structure seems even more difficult than attacking random K.

n McEliece

rescue system by using
r public key: "random"
$\times n$ matrix K over $\mathbf{F}_2$.
300×3600.

weight: $\approx n/(2 \lg n)$.
$\in \mathbf{F}_2^{3600}$ of weight 150.

own attacks scale badly:
$2^{n/(2 \lg n)}$ operations.
uch more precise analysis
09 Bernstein–Lange–
-van Tilborg.

Receiver secretly generates public key K with a hidden Goppa-code structure that allows fast decoding.

Namely: $K = SHP$ for secret $(n/2) \times (n/2)$ invertible matrix S, $(n/2) \times n$ Goppa matrix H, $n \times n$ permutation matrix P.

Detecting this structure seems even more difficult than attacking random K.

Goppa

Fix $q \in$
$t \in \{2,$
$n \in \{t$
e.g. $q =$
or $q =$

Receive
the par
for the
irreduc
binary
a moni
polyno
distinct

e

tem by using
ey: "random"
× K over $\mathbf{F}_2$.
0.

$\approx n/(2 \lg n)$.
of weight 150.

ks scale badly:
$)$ operations.
precise analysis
ein–Lange–
org.

Receiver secretly generates
public key K with a
hidden Goppa-code structure
that allows fast decoding.

Namely: $K = SHP$ for secret
$(n/2) \times (n/2)$ invertible matrix S,
$(n/2) \times n$ Goppa matrix H,
$n \times n$ permutation matrix P.

Detecting this structure
seems even more difficult
than attacking random K.

Goppa codes

Fix $q \in \{8, 16, 32$
$t \in \{2, 3, \ldots, \lfloor (q$
$n \in \{t \lg q + 1, t$
e.g. $q = 1024$, t
or $q = 4096$, $t =$

Receiver's matrix
the parity-check
for the classical (
irreducible length
binary Goppa co
a monic degree-t
polynomial $g \in \mathbf{F}$
distinct $a_1, a_2, \ldots$

ng
om"
$\mathbf{F}_2$.

).
150.

dly:
ns.
lysis
-

Receiver secretly generates public key K with a hidden Goppa-code structure that allows fast decoding.

Namely: $K = SHP$ for secret $(n/2) \times (n/2)$ invertible matrix S, $(n/2) \times n$ Goppa matrix H, $n \times n$ permutation matrix P.

Detecting this structure seems even more difficult than attacking random K.

Goppa codes

Fix $q \in \{8, 16, 32, \ldots\}$;
$t \in \{2, 3, \ldots, \lfloor (q-1)/\lg q$
$n \in \{t \lg q + 1, t \lg q + 2, \ldots$
e.g. $q = 1024$, $t = 50$, $n =$
or $q = 4096$, $t = 150$, $n =$

Receiver's matrix H is the parity-check matrix for the classical (genus-0) irreducible length-n degree binary Goppa code defined a monic degree-t irreducibl polynomial $g \in \mathbf{F}_q[x]$ and distinct $a_1, a_2, \ldots, a_n \in \mathbf{F}_q$

Receiver secretly generates
public key K with a
hidden Goppa-code structure
that allows fast decoding.

Namely: $K = SHP$ for secret
$(n/2) \times (n/2)$ invertible matrix S,
$(n/2) \times n$ Goppa matrix H,
$n \times n$ permutation matrix P.

Detecting this structure
seems even more difficult
than attacking random K.

Goppa codes

Fix $q \in \{8, 16, 32, \ldots\}$;
$t \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$;
$n \in \{t \lg q + 1, t \lg q + 2, \ldots, q\}$.
e.g. $q = 1024$, $t = 50$, $n = 1024$.
or $q = 4096$, $t = 150$, $n = 3600$.

Receiver's matrix H is
the parity-check matrix
for the classical (genus-0)
irreducible length-n degree-t
binary Goppa code defined by
a monic degree-t irreducible
polynomial $g \in \mathbf{F}_q[x]$ and
distinct $a_1, a_2, \ldots, a_n \in \mathbf{F}_q$.

er secretly generates
key K with a
Goppa-code structure
lows fast decoding.

y: $K = SHP$ for secret
$\times (n/2)$ invertible matrix S,
$\times n$ Goppa matrix H,
permutation matrix P.

ing this structure
even more difficult
ttacking random K.

Goppa codes

Fix $q \in \{8, 16, 32, \ldots\}$;
$t \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$;
$n \in \{t \lg q + 1, t \lg q + 2, \ldots, q\}$.
e.g. $q = 1024$, $t = 50$, $n = 1024$.
or $q = 4096$, $t = 150$, $n = 3600$.

Receiver's matrix H is
the parity-check matrix
for the classical (genus-0)
irreducible length-n degree-t
binary Goppa code defined by
a monic degree-t irreducible
polynomial $g \in \mathbf{F}_q[x]$ and
distinct $a_1, a_2, \ldots, a_n \in \mathbf{F}_q$.

. . . whi

View e
as a co
Then H

generates
h a
de structure
decoding.

HP for secret
vertible matrix S,
a matrix H,
on matrix P.

ructure
difficult
andom K.

Goppa codes

Fix $q \in \{8, 16, 32, \ldots\}$;
$t \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$;
$n \in \{t \lg q + 1, t \lg q + 2, \ldots, q\}$.
e.g. $q = 1024$, $t = 50$, $n = 1024$.
or $q = 4096$, $t = 150$, $n = 3600$.

Receiver's matrix H is
the parity-check matrix
for the classical (genus-0)
irreducible length-n degree-t
binary Goppa code defined by
a monic degree-t irreducible
polynomial $g \in \mathbf{F}_q[x]$ and
distinct $a_1, a_2, \ldots, a_n \in \mathbf{F}_q$.

. . . which means:

$$\begin{pmatrix} \frac{1}{g(a_1)} & \cdots \\ \frac{a_1}{g(a_1)} & \cdots \\ \vdots & \ddots \\ \frac{a_1^{t-1}}{g(a_1)} & \cdots \end{pmatrix}$$

View each eleme
as a column in $\mathbf{F}$
Then $H : \mathbf{F}_2^n \to$

ıre

cret

natrix S,

H,

P.

Goppa codes

Fix $q \in \{8, 16, 32, \ldots\}$;
$t \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$;
$n \in \{t \lg q + 1, t \lg q + 2, \ldots, q\}$.
e.g. $q = 1024$, $t = 50$, $n = 1024$.
or $q = 4096$, $t = 150$, $n = 3600$.

Receiver's matrix H is
the parity-check matrix
for the classical (genus-0)
irreducible length-n degree-t
binary Goppa code defined by
a monic degree-t irreducible
polynomial $g \in \mathbf{F}_q[x]$ and
distinct $a_1, a_2, \ldots, a_n \in \mathbf{F}_q$.

. . . which means: $H =$

$$\begin{pmatrix} \frac{1}{g(a_1)} & \cdots & \frac{1}{g(a_n)} \\ \frac{a_1}{g(a_1)} & \cdots & \frac{a_n}{g(a_n)} \\ \vdots & \ddots & \vdots \\ \frac{a_1^{t-1}}{g(a_1)} & \cdots & \frac{a_n^{t-1}}{g(a_n)} \end{pmatrix}$$

View each element of $\mathbf{F}_q$ h
as a column in $\mathbf{F}_2^{\lg q}$.
Then $H : \mathbf{F}_2^n \to \mathbf{F}_2^{t \lg q}$.

Goppa codes

Fix $q \in \{8, 16, 32, \ldots\}$;
$t \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$;
$n \in \{t \lg q + 1, t \lg q + 2, \ldots, q\}$.
e.g. $q = 1024$, $t = 50$, $n = 1024$.
or $q = 4096$, $t = 150$, $n = 3600$.

Receiver's matrix H is
the parity-check matrix
for the classical (genus-0)
irreducible length-n degree-t
binary Goppa code defined by
a monic degree-t irreducible
polynomial $g \in \mathbf{F}_q[x]$ and
distinct $a_1, a_2, \ldots, a_n \in \mathbf{F}_q$.

. . . which means: $H =$

$$\begin{pmatrix} \frac{1}{g(a_1)} & \cdots & \frac{1}{g(a_n)} \\ \frac{a_1}{g(a_1)} & \cdots & \frac{a_n}{g(a_n)} \\ \vdots & \ddots & \vdots \\ \frac{a_1^{t-1}}{g(a_1)} & \cdots & \frac{a_n^{t-1}}{g(a_n)} \end{pmatrix}.$$

View each element of $\mathbf{F}_q$ here
as a column in $\mathbf{F}_2^{\lg q}$.
Then $H : \mathbf{F}_2^n \to \mathbf{F}_2^{t \lg q}$.

codes

$\in \{8, 16, 32, \ldots\}$;

$3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$;

$\lg q + 1, t \lg q + 2, \ldots, q\}$.

$= 1024$, $t = 50$, $n = 1024$.

4096, $t = 150$, $n = 3600$.

er's matrix H is

rity-check matrix

classical (genus-0)

ible length-n degree-t

Goppa code defined by

c degree-t irreducible

mial $g \in \mathbf{F}_q[x]$ and

t $a_1, a_2, \ldots, a_n \in \mathbf{F}_q$.

. . . which means: $H =$

$$\begin{pmatrix} \frac{1}{g(a_1)} & \cdots & \frac{1}{g(a_n)} \\ \frac{a_1}{g(a_1)} & \cdots & \frac{a_n}{g(a_n)} \\ \vdots & \ddots & \vdots \\ \frac{a_1^{t-1}}{g(a_1)} & \cdots & \frac{a_n^{t-1}}{g(a_n)} \end{pmatrix}.$$

View each element of $\mathbf{F}_q$ here as a column in $\mathbf{F}_2^{\lg q}$.
Then $H : \mathbf{F}_2^n \to \mathbf{F}_2^{t \lg q}$.

More u
the ma
from **F**

H is th
where
and $\mathbf{F}_q$
$\lfloor g/x \rfloor$,

One-lin
$\frac{g - g(}{x -}$

$2, \ldots\};$

$q - 1)/\lg q\rfloor\};$

$\lg q + 2, \ldots, q\}.$

$= 50,\ n = 1024.$

$150,\ n = 3600.$

x H is

matrix

(genus-0)

n-n degree-t

de defined by

irreducible

$\mathbf{F}_q[x]$ and

$\ldots, a_n \in \mathbf{F}_q.$

. . . which means: $H =$

$$\begin{pmatrix} \frac{1}{g(a_1)} & \cdots & \frac{1}{g(a_n)} \\ \frac{a_1}{g(a_1)} & \cdots & \frac{a_n}{g(a_n)} \\ \vdots & \ddots & \vdots \\ \frac{a_1^{t-1}}{g(a_1)} & \cdots & \frac{a_n^{t-1}}{g(a_n)} \end{pmatrix}.$$

View each element of $\mathbf{F}_q$ here as a column in $\mathbf{F}_2^{\lg q}$.
Then $H : \mathbf{F}_2^n \to \mathbf{F}_2^{t \lg q}$.

More useful view

the map $m \mapsto \sum$

from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]$

H is the matrix f

where $\mathbf{F}_2^n$ has sta

and $\mathbf{F}_q[x]/g$ has

$\lfloor g/x \rfloor,\ \lfloor g/x^2 \rfloor,$.

One-line proof: I

$$\frac{g - g(a_i)}{x - a_i} = \sum_{j \geq 0}$$

$\rfloor\}$;
$\ldots, q\}$.
$= 1024$.
3600.

$-t$
by
e

q.

. . . which means: $H =$

$$\begin{pmatrix} \frac{1}{g(a_1)} & \cdots & \frac{1}{g(a_n)} \\ \frac{a_1}{g(a_1)} & \cdots & \frac{a_n}{g(a_n)} \\ \vdots & \ddots & \vdots \\ \frac{a_1^{t-1}}{g(a_1)} & \cdots & \frac{a_n^{t-1}}{g(a_n)} \end{pmatrix}.$$

View each element of $\mathbf{F}_q$ here as a column in $\mathbf{F}_2^{\lg q}$.
Then $H : \mathbf{F}_2^n \to \mathbf{F}_2^{t \lg q}$.

More useful view: Consider
the map $m \mapsto \sum_i m_i/(x -$
from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$.

H is the matrix for this ma
where $\mathbf{F}_2^n$ has standard bas
and $\mathbf{F}_q[x]/g$ has basis
$\lfloor g/x \rfloor$, $\lfloor g/x^2 \rfloor$, . . . , $\lfloor g/x^t$

One-line proof: In $\mathbf{F}_q[x]$ ha

$$\frac{g - g(a_i)}{x - a_i} = \sum_{j \geq 0} a_i^j \left\lfloor g/x^{j+} \right.$$

. . . which means: $H =$

$$\begin{pmatrix} \frac{1}{g(a_1)} & \cdots & \frac{1}{g(a_n)} \\ \frac{a_1}{g(a_1)} & \cdots & \frac{a_n}{g(a_n)} \\ \vdots & \ddots & \vdots \\ \frac{a_1^{t-1}}{g(a_1)} & \cdots & \frac{a_n^{t-1}}{g(a_n)} \end{pmatrix}.$$

View each element of $\mathbf{F}_q$ here as a column in $\mathbf{F}_2^{\lg q}$.
Then $H : \mathbf{F}_2^n \to \mathbf{F}_2^{t \lg q}$.

More useful view: Consider the map $m \mapsto \sum_i m_i/(x - a_i)$ from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$.

H is the matrix for this map where $\mathbf{F}_2^n$ has standard basis and $\mathbf{F}_q[x]/g$ has basis $\lfloor g/x \rfloor$, $\left\lfloor g/x^2 \right\rfloor$, . . . , $\left\lfloor g/x^t \right\rfloor$.

One-line proof: In $\mathbf{F}_q[x]$ have

$$\frac{g - g(a_i)}{x - a_i} = \sum_{j \geq 0} a_i^j \left\lfloor g/x^{j+1} \right\rfloor.$$

ch means: $H =$

$$\begin{pmatrix} \frac{1}{g(a_1)} & \cdots & \frac{1}{g(a_n)} \\ \frac{a_1}{g(a_1)} & \cdots & \frac{a_n}{g(a_n)} \\ \vdots & \ddots & \vdots \\ \frac{a_1^{t-1}}{g(a_1)} & \cdots & \frac{a_n^{t-1}}{g(a_n)} \end{pmatrix}.$$

ach element of $\mathbf{F}_q$ here
olumn in $\mathbf{F}_2^{\lg q}$.
$H : \mathbf{F}_2^n \to \mathbf{F}_2^{t \lg q}$.

More useful view: Consider the map $m \mapsto \sum_i m_i/(x - a_i)$ from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$.

H is the matrix for this map where $\mathbf{F}_2^n$ has standard basis and $\mathbf{F}_q[x]/g$ has basis $\lfloor g/x \rfloor$, $\lfloor g/x^2 \rfloor$, ..., $\lfloor g/x^t \rfloor$.

One-line proof: In $\mathbf{F}_q[x]$ have

$$\frac{g - g(a_i)}{x - a_i} = \sum_{j \geq 0} a_i^j \left\lfloor g/x^{j+1} \right\rfloor.$$

Decodi

1975 P
can qu
if weig

Given c
receive
by app
decode
by Patt
comput
by app

$$H = \begin{pmatrix} \cdot & \frac{1}{g(a_n)} & \cdot \\ \cdot & \frac{a_n}{g(a_n)} & \cdot \\ \cdot & \vdots & \cdot \\ \cdot & \frac{a_n^{t-1}}{g(a_n)} & \cdot \end{pmatrix}.$$

nt of $\mathbf{F}_q$ here
$\lg q$
$_2$.
$\mathbf{F}_2^{t \lg q}$.

More useful view: Consider the map $m \mapsto \sum_i m_i/(x - a_i)$ from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$.

H is the matrix for this map where $\mathbf{F}_2^n$ has standard basis and $\mathbf{F}_q[x]/g$ has basis $\lfloor g/x \rfloor$, $\lfloor g/x^2 \rfloor$, ..., $\lfloor g/x^t \rfloor$.

One-line proof: In $\mathbf{F}_q[x]$ have

$$\frac{g - g(a_i)}{x - a_i} = \sum_{j \geq 0} a_i^j \left\lfloor g/x^{j+1} \right\rfloor.$$

Decoding Goppa

1975 Patterson:
can quickly find
if weight of m is

Given ciphertext
receiver compute
by applying secre
decodes H to ob
by Patterson's al
computes messag
by applying secre

)

.

ere

More useful view: Consider the map $m \mapsto \sum_i m_i/(x-a_i)$ from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$.

H is the matrix for this map where $\mathbf{F}_2^n$ has standard basis and $\mathbf{F}_q[x]/g$ has basis $\lfloor g/x \rfloor$, $\left\lfloor g/x^2 \right\rfloor$, ..., $\left\lfloor g/x^t \right\rfloor$.

One-line proof: In $\mathbf{F}_q[x]$ have

$$\frac{g-g(a_i)}{x-a_i} = \sum_{j \geq 0} a_i^j \left\lfloor g/x^{j+1} \right\rfloor.$$

Decoding Goppa codes

1975 Patterson: Given Hm can quickly find m if weight of m is $\leq t$.

Given ciphertext $Km = SH$ receiver computes HPm by applying secret S^{-1}; decodes H to obtain Pm by Patterson's algorithm; computes message m by applying secret P^{-1}.

More useful view: Consider the map $m \mapsto \sum_i m_i/(x-a_i)$ from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$.

H is the matrix for this map where $\mathbf{F}_2^n$ has standard basis and $\mathbf{F}_q[x]/g$ has basis $\lfloor g/x \rfloor$, $\left\lfloor g/x^2 \right\rfloor$, ..., $\left\lfloor g/x^t \right\rfloor$.

One-line proof: In $\mathbf{F}_q[x]$ have

$$\frac{g-g(a_i)}{x-a_i} = \sum_{j \geq 0} a_i^j \left\lfloor g/x^{j+1} \right\rfloor.$$

Decoding Goppa codes

1975 Patterson: Given Hm, can quickly find m if weight of m is $\leq t$.

Given ciphertext $Km = SHPm$: receiver computes HPm by applying secret S^{-1}; decodes H to obtain Pm by Patterson's algorithm; computes message m by applying secret P^{-1}.

useful view: Consider
p $m \mapsto \sum_i m_i/(x-a_i)$
$\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$.

he matrix for this map
$\mathbf{F}_2^n$ has standard basis
$[x]/g$ has basis
$\left\lfloor g/x^2 \right\rfloor, \ldots, \left\lfloor g/x^t \right\rfloor$.

he proof: In $\mathbf{F}_q[x]$ have

$$\frac{1}{x-a_i} = \sum_{j \geq 0} a_i^j \left\lfloor g/x^{j+1} \right\rfloor.$$

Decoding Goppa codes

1975 Patterson: Given Hm,
can quickly find m
if weight of m is $\leq t$.

Given ciphertext $Km = SHPm$:
receiver computes HPm
by applying secret S^{-1};
decodes H to obtain Pm
by Patterson's algorithm;
computes message m
by applying secret P^{-1}.

Patters
having
where
Output

If $r =$

If $r \neq$
Lift $\sqrt{r}$
to $s \in$

Consid
generat

Define
as norm

Find a
nonzero

: Consider
$\sum_i m_i/(x-a_i)$
$\rfloor/g$.

for this map
andard basis
basis
$\ldots, \lfloor g/x^t \rfloor$.

n $\mathbf{F}_q[x]$ have
$a_i^j \lfloor g/x^{j+1} \rfloor$.

Decoding Goppa codes

1975 Patterson: Given Hm,
can quickly find m
if weight of m is $\leq t$.

Given ciphertext $Km = SHPm$:
receiver computes HPm
by applying secret S^{-1};
decodes H to obtain Pm
by Patterson's algorithm;
computes message m
by applying secret P^{-1}.

Patterson input i
having form $\sum_i$
where $m \in \mathbf{F}_2^n$ h
Output will be m

If $r = 0$, output

If $r \neq 0$:
Lift $\sqrt{r^{-1} - x}$ fr
to $s \in \mathbf{F}_q[x]$ of d

Consider lattice
generated by $(s,$

Define length of
as norm of $\alpha^2 +$

Find a minimum-
nonzero vector (

r

$- a_i)$

ap

sis

$\Big]$.

ave

$^{-1}\Big]$.

Decoding Goppa codes

1975 Patterson: Given Hm,
can quickly find m
if weight of m is $\leq t$.

Given ciphertext $Km = SHPm$:
receiver computes HPm
by applying secret S^{-1};
decodes H to obtain Pm
by Patterson's algorithm;
computes message m
by applying secret P^{-1}.

Patterson input is $r \in \mathbf{F}_q[x$
having form $\sum_i m_i/(x - a$
where $m \in \mathbf{F}_2^n$ has weight
Output will be m.

If $r = 0$, output 0 and stop

If $r \neq 0$:
Lift $\sqrt{r^{-1} - x}$ from $\mathbf{F}_q[x]/$
to $s \in \mathbf{F}_q[x]$ of degree $< t$.

Consider lattice $L \subseteq \mathbf{F}_q[x]^2$
generated by $(s, 1)$ and $(g,$

Define length of (α, β)
as norm of $\alpha^2 + x\beta^2$.

Find a minimum-length
nonzero vector $(\alpha_0, \beta_0) \in$

Decoding Goppa codes

1975 Patterson: Given Hm,
can quickly find m
if weight of m is $\leq t$.

Given ciphertext $Km = SHPm$:
receiver computes HPm
by applying secret S^{-1};
decodes H to obtain Pm
by Patterson's algorithm;
computes message m
by applying secret P^{-1}.

Patterson input is $r \in \mathbf{F}_q[x]/g$
having form $\sum_i m_i/(x - a_i)$
where $m \in \mathbf{F}_2^n$ has weight $\leq t$.
Output will be m.

If $r = 0$, output 0 and stop.

If $r \neq 0$:
Lift $\sqrt{r^{-1} - x}$ from $\mathbf{F}_q[x]/g$
to $s \in \mathbf{F}_q[x]$ of degree $< t$.

Consider lattice $L \subseteq \mathbf{F}_q[x]^2$
generated by $(s, 1)$ and $(g, 0)$.

Define length of (α, β)
as norm of $\alpha^2 + x\beta^2$.

Find a minimum-length
nonzero vector $(\alpha_0, \beta_0) \in L$.

ng Goppa codes

atterson: Given Hm,
ickly find m
ht of m is $\leq t$.

ciphertext $Km = SHPm$:
r computes HPm
lying secret S^{-1};
s H to obtain Pm
terson's algorithm;
tes message m
lying secret P^{-1}.

Patterson input is $r \in \mathbf{F}_q[x]/g$
having form $\sum_i m_i/(x - a_i)$
where $m \in \mathbf{F}_2^n$ has weight $\leq t$.
Output will be m.

If $r = 0$, output 0 and stop.

If $r \neq 0$:
Lift $\sqrt{r^{-1} - x}$ from $\mathbf{F}_q[x]/g$
to $s \in \mathbf{F}_q[x]$ of degree $< t$.

Consider lattice $L \subseteq \mathbf{F}_q[x]^2$
generated by $(s, 1)$ and $(g, 0)$.

Define length of (α, β)
as norm of $\alpha^2 + x\beta^2$.

Find a minimum-length
nonzero vector $(\alpha_0, \beta_0) \in L$.

Monic
is exac
Factor

Why th
Define
Write ϵ
Have ϵ
so $\beta^2/$
so $s =$
i.e., $(\alpha$
Volume
(α, β)
so $\epsilon =$
ϵ is squ

codes

Given Hm,

m

$\leq t$.

$Km = SHPm$:

es HPm

et S^{-1};

tain Pm

gorithm;

ge m

et P^{-1}.

Patterson input is $r \in \mathbf{F}_q[x]/g$
having form $\sum_i m_i/(x - a_i)$
where $m \in \mathbf{F}_2^n$ has weight $\leq t$.
Output will be m.

If $r = 0$, output 0 and stop.

If $r \neq 0$:
Lift $\sqrt{r^{-1} - x}$ from $\mathbf{F}_q[x]/g$
to $s \in \mathbf{F}_q[x]$ of degree $< t$.

Consider lattice $L \subseteq \mathbf{F}_q[x]^2$
generated by $(s, 1)$ and $(g, 0)$.

Define length of (α, β)
as norm of $\alpha^2 + x\beta^2$.

Find a minimum-length
nonzero vector $(\alpha_0, \beta_0) \in L$.

Monic part of ϵ_0
is exactly $\prod_{i:m_i=$
Factor ϵ_0 and pri

Why this works:

Define $\epsilon = \prod_{i:m$
Write ϵ as $\alpha^2 +$
Have $\epsilon'/\epsilon = r$ in
so $\beta^2/(\alpha^2 + x\beta^2$
so $s = \alpha/\beta$ in $\mathbf{F}_q$
i.e., $(\alpha, \beta) \in L$.
Volume of L forc
$(\alpha, \beta) \in (\alpha_0, \beta_0)$
so $\epsilon =$ square $\cdot \epsilon_0$
ϵ is squarefree so

n,

HPm:

Patterson input is $r \in \mathbf{F}_q[x]/g$
having form $\sum_i m_i/(x-a_i)$
where $m \in \mathbf{F}_2^n$ has weight $\leq t$.
Output will be m.

If $r = 0$, output 0 and stop.

If $r \neq 0$:
Lift $\sqrt{r^{-1}-x}$ from $\mathbf{F}_q[x]/g$
to $s \in \mathbf{F}_q[x]$ of degree $< t$.

Consider lattice $L \subseteq \mathbf{F}_q[x]^2$
generated by $(s,1)$ and $(g,0)$.

Define length of (α,β)
as norm of $\alpha^2 + x\beta^2$.

Find a minimum-length
nonzero vector $(\alpha_0,\beta_0) \in L$.

Monic part of $\epsilon_0 = \alpha_0^2 + x$
is exactly $\prod_{i:m_i=1}(x-a_i)$
Factor ϵ_0 and print m.

Why this works:
Define $\epsilon = \prod_{i:m_i=1}(x-a$
Write ϵ as $\alpha^2 + x\beta^2$ in $\mathbf{F}_q$
Have $\epsilon'/\epsilon = r$ in $\mathbf{F}_q[x]/g$
so $\beta^2/(\alpha^2+x\beta^2) = 1/(s^2$
so $s = \alpha/\beta$ in $\mathbf{F}_q[x]/g$;
i.e., $(\alpha,\beta) \in L$.
Volume of L forces
$(\alpha,\beta) \in (\alpha_0,\beta_0)\mathbf{F}_q[x]$
so $\epsilon = \text{square} \cdot \epsilon_0$;
ϵ is squarefree so square $\in$

Patterson input is $r \in \mathbf{F}_q[x]/g$
having form $\sum_i m_i/(x-a_i)$
where $m \in \mathbf{F}_2^n$ has weight $\leq t$.
Output will be m.

If $r = 0$, output 0 and stop.

If $r \neq 0$:
Lift $\sqrt{r^{-1}-x}$ from $\mathbf{F}_q[x]/g$
to $s \in \mathbf{F}_q[x]$ of degree $< t$.

Consider lattice $L \subseteq \mathbf{F}_q[x]^2$
generated by $(s,1)$ and $(g,0)$.

Define length of (α,β)
as norm of $\alpha^2 + x\beta^2$.

Find a minimum-length
nonzero vector $(\alpha_0,\beta_0) \in L$.

Monic part of $\epsilon_0 = \alpha_0^2 + x\beta_0^2$
is exactly $\prod_{i:m_i=1}(x-a_i)$.
Factor ϵ_0 and print m.

Why this works:
Define $\epsilon = \prod_{i:m_i=1}(x-a_i)$.
Write ϵ as $\alpha^2 + x\beta^2$ in $\mathbf{F}_q[x]$.
Have $\epsilon'/\epsilon = r$ in $\mathbf{F}_q[x]/g$
so $\beta^2/(\alpha^2+x\beta^2) = 1/(s^2+x)$
so $s = \alpha/\beta$ in $\mathbf{F}_q[x]/g$;
i.e., $(\alpha,\beta) \in L$.
Volume of L forces
$(\alpha,\beta) \in (\alpha_0,\beta_0)\mathbf{F}_q[x]$
so $\epsilon = \text{square} \cdot \epsilon_0$;
ϵ is squarefree so square $\in \mathbf{F}_q$. ■

son input is $r \in \mathbf{F}_q[x]/g$
form $\sum_i m_i/(x-a_i)$
$m \in \mathbf{F}_2^n$ has weight $\leq t$.
t will be m.

0, output 0 and stop.

0:
$\overline{r^{-1}-x}$ from $\mathbf{F}_q[x]/g$
$\mathbf{F}_q[x]$ of degree $< t$.

er lattice $L \subseteq \mathbf{F}_q[x]^2$
ted by $(s,1)$ and $(g,0)$.

length of (α,β)
m of $\alpha^2 + x\beta^2$.

minimum-length
o vector $(\alpha_0,\beta_0) \in L$.

Monic part of $\epsilon_0 = \alpha_0^2 + x\beta_0^2$
is exactly $\prod_{i:m_i=1}(x-a_i)$.
Factor ϵ_0 and print m.

Why this works:
Define $\epsilon = \prod_{i:m_i=1}(x-a_i)$.
Write ϵ as $\alpha^2 + x\beta^2$ in $\mathbf{F}_q[x]$.
Have $\epsilon'/\epsilon = r$ in $\mathbf{F}_q[x]/g$
so $\beta^2/(\alpha^2+x\beta^2) = 1/(s^2+x)$
so $s = \alpha/\beta$ in $\mathbf{F}_q[x]/g$;
i.e., $(\alpha,\beta) \in L$.
Volume of L forces
$(\alpha,\beta) \in (\alpha_0,\beta_0)\mathbf{F}_q[x]$
so $\epsilon = \text{square} \cdot \epsilon_0$;
ϵ is squarefree so square $\in \mathbf{F}_q$. ■

What i
m havi

Volume
(α,β)

But ca
$(\alpha_0,\beta_0$

Then ϵ
of $\epsilon_0 =$
and ϵ_1
Coeffic
"small"

s $r \in \mathbf{F}_q[x]/g$
$m_i/(x - a_i)$
as weight $\leq t$.
n.

0 and stop.

om $\mathbf{F}_q[x]/g$
egree $< t$.

$L \subseteq \mathbf{F}_q[x]^2$
1) and $(g, 0)$.

(α, β)
$x\beta^2$.

-length
$\alpha_0, \beta_0) \in L$.

Monic part of $\epsilon_0 = \alpha_0^2 + x\beta_0^2$
is exactly $\prod_{i:m_i=1}(x - a_i)$.
Factor ϵ_0 and print m.

Why this works:
Define $\epsilon = \prod_{i:m_i=1}(x - a_i)$.
Write ϵ as $\alpha^2 + x\beta^2$ in $\mathbf{F}_q[x]$.
Have $\epsilon'/\epsilon = r$ in $\mathbf{F}_q[x]/g$
so $\beta^2/(\alpha^2 + x\beta^2) = 1/(s^2 + x)$
so $s = \alpha/\beta$ in $\mathbf{F}_q[x]/g$;
i.e., $(\alpha, \beta) \in L$.
Volume of L forces
$(\alpha, \beta) \in (\alpha_0, \beta_0)\mathbf{F}_q[x]$
so $\epsilon = \text{square} \cdot \epsilon_0$;
ϵ is squarefree so square $\in \mathbf{F}_q$. ■

What if Patterso
m having weight

Volume argumen
$(\alpha, \beta) \notin (\alpha_0, \beta_0)$

But can compute
$(\alpha_0, \beta_0), (\alpha_1, \beta_1)$

Then ϵ is a linea
of $\epsilon_0 = \alpha_0^2 + x\beta_0^2$
and $\epsilon_1 = \alpha_1^2 + x\beta_1^2$
Coefficients are s
"small" depends

$x]/g$
$a_i)$
$\leq t$.

o.

$/g$

2

0).

L.

Monic part of $\epsilon_0 = \alpha_0^2 + x\beta_0^2$
is exactly $\prod_{i:m_i=1}(x - a_i)$.
Factor ϵ_0 and print m.

Why this works:
Define $\epsilon = \prod_{i:m_i=1}(x - a_i)$.
Write ϵ as $\alpha^2 + x\beta^2$ in $\mathbf{F}_q[x]$.
Have $\epsilon'/\epsilon = r$ in $\mathbf{F}_q[x]/g$
so $\beta^2/(\alpha^2 + x\beta^2) = 1/(s^2 + x)$
so $s = \alpha/\beta$ in $\mathbf{F}_q[x]/g$;
i.e., $(\alpha, \beta) \in L$.
Volume of L forces
$(\alpha, \beta) \in (\alpha_0, \beta_0)\mathbf{F}_q[x]$
so $\epsilon = \text{square} \cdot \epsilon_0$;
ϵ is squarefree so square $\in \mathbf{F}_q$. ■

What if Patterson is used f
m having weight $> t$?

Volume argument fails.
$(\alpha, \beta) \notin (\alpha_0, \beta_0)\mathbf{F}_q[x]$.

But can compute short bas
$(\alpha_0, \beta_0), (\alpha_1, \beta_1)$ of L.

Then ϵ is a linear combinat
of $\epsilon_0 = \alpha_0^2 + x\beta_0^2$
and $\epsilon_1 = \alpha_1^2 + x\beta_1^2$.
Coefficients are small squar
"small" depends on weight

Monic part of $\epsilon_0 = \alpha_0^2 + x\beta_0^2$
is exactly $\prod_{i:m_i=1}(x - a_i)$.
Factor ϵ_0 and print m.

Why this works:
Define $\epsilon = \prod_{i:m_i=1}(x - a_i)$.
Write ϵ as $\alpha^2 + x\beta^2$ in $\mathbf{F}_q[x]$.
Have $\epsilon'/\epsilon = r$ in $\mathbf{F}_q[x]/g$
so $\beta^2/(\alpha^2 + x\beta^2) = 1/(s^2 + x)$
so $s = \alpha/\beta$ in $\mathbf{F}_q[x]/g$;
i.e., $(\alpha, \beta) \in L$.
Volume of L forces
$(\alpha, \beta) \in (\alpha_0, \beta_0)\mathbf{F}_q[x]$
so $\epsilon = \text{square} \cdot \epsilon_0$;
ϵ is squarefree so square $\in \mathbf{F}_q$. ■

What if Patterson is used for
m having weight $> t$?

Volume argument fails.
$(\alpha, \beta) \notin (\alpha_0, \beta_0)\mathbf{F}_q[x]$.

But can compute short basis
$(\alpha_0, \beta_0), (\alpha_1, \beta_1)$ of L.

Then ϵ is a linear combination
of $\epsilon_0 = \alpha_0^2 + x\beta_0^2$
and $\epsilon_1 = \alpha_1^2 + x\beta_1^2$.
Coefficients are small squares;
"small" depends on weight of m.

part of $\epsilon_0 = \alpha_0^2 + x\beta_0^2$
tly $\prod_{i:m_i=1}(x - a_i)$.
ϵ_0 and print m.

his works:
$\epsilon = \prod_{i:m_i=1}(x - a_i)$.
ϵ as $\alpha^2 + x\beta^2$ in $\mathbf{F}_q[x]$.
$r'/\epsilon = r$ in $\mathbf{F}_q[x]/g$
$(\alpha^2 + x\beta^2) = 1/(s^2 + x)$
α/β in $\mathbf{F}_q[x]/g$;
$,\beta) \in L$.
e of L forces
$\in (\alpha_0, \beta_0)\mathbf{F}_q[x]$
square $\cdot\, \epsilon_0$;
uarefree so square $\in \mathbf{F}_q$. ■

What if Patterson is used for m having weight $> t$?

Volume argument fails.
$(\alpha, \beta) \notin (\alpha_0, \beta_0)\mathbf{F}_q[x]$.

But can compute short basis $(\alpha_0, \beta_0), (\alpha_1, \beta_1)$ of L.

Then ϵ is a linear combination of $\epsilon_0 = \alpha_0^2 + x\beta_0^2$ and $\epsilon_1 = \alpha_1^2 + x\beta_1^2$.
Coefficients are small squares;
"small" depends on weight of m.

Divisor

Want a
given p
with go

Easy if

1984 L
algorith

1997 K
polyno
$v \geq n^3$

1998 C
Graham
time al

$= \alpha_0^2 + x\beta_0^2$
$=1(x - a_i)$.
int m.

$_{i=1}(x - a_i)$.
$x\beta^2$ in $\mathbf{F}_q[x]$.
$\mathbf{F}_q[x]/g$
$^2) = 1/(s^2 + x)$
$_q[x]/g$;

ces
$)\mathbf{F}_q[x]$
$_0$;
square $\in \mathbf{F}_q$. ■

What if Patterson is used for m having weight $> t$?

Volume argument fails.
$(\alpha, \beta) \notin (\alpha_0, \beta_0)\mathbf{F}_q[x]$.

But can compute short basis $(\alpha_0, \beta_0), (\alpha_1, \beta_1)$ of L.

Then ϵ is a linear combination of $\epsilon_0 = \alpha_0^2 + x\beta_0^2$ and $\epsilon_1 = \alpha_1^2 + x\beta_1^2$.
Coefficients are small squares;
"small" depends on weight of m.

Divisors in residu

Want all divisors
given positive int
with $\gcd\{v, n\} =$

Easy if $v \geq n^{1/2}$

1984 Lenstra: po
algorithm for $v \geq$

1997 Konyagin–P
polynomial-time
$v \geq n^{3/10}$.

1998 Coppersmit
Graham–Nagaraj
time algorithm fo

β_0^2
.

i).
$[x]$.

$+ x$)

$\mathbf{F}_q$. ■

What if Patterson is used for m having weight $> t$?

Volume argument fails.
$(\alpha, \beta) \notin (\alpha_0, \beta_0)\mathbf{F}_q[x]$.

But can compute short basis
$(\alpha_0, \beta_0), (\alpha_1, \beta_1)$ of L.

Then ϵ is a linear combination
of $\epsilon_0 = \alpha_0^2 + x\beta_0^2$
and $\epsilon_1 = \alpha_1^2 + x\beta_1^2$.
Coefficients are small squares;
"small" depends on weight of m.

Divisors in residue classes

Want all divisors of n in u
given positive integers u, v
with $\gcd\{v, n\} = 1$.

Easy if $v \geq n^{1/2}$.

1984 Lenstra: polynomial-t
algorithm for $v \geq n^{1/3}$.

1997 Konyagin–Pomerance
polynomial-time algorithm
$v \geq n^{3/10}$.

1998 Coppersmith–Howgra
Graham–Nagaraj: polynom
time algorithm for $v \geq n^{1/}$

What if Patterson is used for m having weight $> t$?

Volume argument fails.
$(\alpha, \beta) \notin (\alpha_0, \beta_0)\mathbf{F}_q[x]$.

But can compute short basis
$(\alpha_0, \beta_0), (\alpha_1, \beta_1)$ of L.

Then ϵ is a linear combination
of $\epsilon_0 = \alpha_0^2 + x\beta_0^2$
and $\epsilon_1 = \alpha_1^2 + x\beta_1^2$.
Coefficients are small squares;
"small" depends on weight of m.

Divisors in residue classes

Want all divisors of n in $u + v\mathbf{Z}$, given positive integers u, v, n with $\gcd\{v, n\} = 1$.

Easy if $v \geq n^{1/2}$.

1984 Lenstra: polynomial-time algorithm for $v \geq n^{1/3}$.

1997 Konyagin–Pomerance: polynomial-time algorithm for $v \geq n^{3/10}$.

1998 Coppersmith–Howgrave-Graham–Nagaraj: polynomial-time algorithm for $v \geq n^{1/4+\epsilon}$.

f Patterson is used for
ing weight $> t$?

e argument fails.
$\notin (\alpha_0, \beta_0)\mathbf{F}_q[x]$.

n compute short basis
$)$, (α_1, β_1) of L.

is a linear combination
$= \alpha_0^2 + x\beta_0^2$
$= \alpha_1^2 + x\beta_1^2$.
ients are small squares;
' depends on weight of m.

Divisors in residue classes

Want all divisors of n in $u + v\mathbf{Z}$, given positive integers u, v, n with $\gcd\{v, n\} = 1$.

Easy if $v \geq n^{1/2}$.

1984 Lenstra: polynomial-time algorithm for $v \geq n^{1/3}$.

1997 Konyagin–Pomerance: polynomial-time algorithm for $v \geq n^{3/10}$.

1998 Coppersmith–Howgrave-Graham–Nagaraj: polynomial-time algorithm for $v \geq n^{1/4+\epsilon}$.

2000 B
algorith
algorith

Functio
famous
algorith
of Reed

Can bu
of "Co
and "S
See, e.g
"Reduc
to find
of univ

n is used for
$> t$?

t fails.
$)\mathbf{F}_q[x]$.

e short basis
) of L.

r combination
$^2_0$
β_1^2.
small squares;
on weight of m.

Divisors in residue classes

Want all divisors of n in $u + v\mathbf{Z}$, given positive integers u, v, n with $\gcd\{v, n\} = 1$.

Easy if $v \geq n^{1/2}$.

1984 Lenstra: polynomial-time algorithm for $v \geq n^{1/3}$.

1997 Konyagin–Pomerance: polynomial-time algorithm for $v \geq n^{3/10}$.

1998 Coppersmith–Howgrave-Graham–Nagaraj: polynomial-time algorithm for $v \geq n^{1/4+\epsilon}$.

2000 Boneh: can
algorithm as a lis
algorithm for CR

Function-field an
famous 1999 Gur
algorithm for list
of Reed–Solomon

Can build grand
of "Coppersmith-
and "Sudan-type
See, e.g., my sur
"Reducing lattice
to find small-heig
of univariate poly

for

sis

tion

res;
t of m.

Divisors in residue classes

Want all divisors of n in $u + v\mathbf{Z}$, given positive integers u, v, n with $\gcd\{v, n\} = 1$.

Easy if $v \geq n^{1/2}$.

1984 Lenstra: polynomial-time algorithm for $v \geq n^{1/3}$.

1997 Konyagin–Pomerance: polynomial-time algorithm for $v \geq n^{3/10}$.

1998 Coppersmith–Howgrave-Graham–Nagaraj: polynomial-time algorithm for $v \geq n^{1/4+\epsilon}$.

2000 Boneh: can view sam
algorithm as a list-decodin
algorithm for CRT codes.

Function-field analogue is
famous 1999 Guruswami–S
algorithm for list decoding
of Reed–Solomon codes.

Can build grand unified pic
of "Coppersmith-type" alg
and "Sudan-type" algorith
See, e.g., my survey paper
"Reducing lattice bases
to find small-height values
of univariate polynomials."

Divisors in residue classes

Want all divisors of n in $u + v\mathbf{Z}$, given positive integers u, v, n with $\gcd\{v, n\} = 1$.

Easy if $v \geq n^{1/2}$.

1984 Lenstra: polynomial-time algorithm for $v \geq n^{1/3}$.

1997 Konyagin–Pomerance: polynomial-time algorithm for $v \geq n^{3/10}$.

1998 Coppersmith–Howgrave-Graham–Nagaraj: polynomial-time algorithm for $v \geq n^{1/4+\epsilon}$.

2000 Boneh: can view same algorithm as a list-decoding algorithm for CRT codes.

Function-field analogue is famous 1999 Guruswami–Sudan algorithm for list decoding of Reed–Solomon codes.

Can build grand unified picture of "Coppersmith-type" algorithms and "Sudan-type" algorithms. See, e.g., my survey paper "Reducing lattice bases to find small-height values of univariate polynomials."

s in residue classes

all divisors of n in $u + v\mathbf{Z}$,
positive integers u, v, n
$\gcd\{v, n\} = 1$.

$v \geq n^{1/2}$.

enstra: polynomial-time
hm for $v \geq n^{1/3}$.

Konyagin–Pomerance:
mial-time algorithm for
$^{3/10}$.

Coppersmith–Howgrave-
n–Nagaraj: polynomial-
gorithm for $v \geq n^{1/4+\epsilon}$.

2000 Boneh: can view same algorithm as a list-decoding algorithm for CRT codes.

Function-field analogue is famous 1999 Guruswami–Sudan algorithm for list decoding of Reed–Solomon codes.

Can build grand unified picture of "Coppersmith-type" algorithms and "Sudan-type" algorithms. See, e.g., my survey paper "Reducing lattice bases to find small-height values of univariate polynomials."

2008 B

Tweak
in the
to find
linear
with s

ue classes

of n in $u + v\mathbf{Z}$,
tegers u, v, n
= 1.

olynomial-time
$\geq n^{1/3}$.

Pomerance:
algorithm for

th–Howgrave-
: polynomial-
or $v \geq n^{1/4+\epsilon}$.

2000 Boneh: can view same algorithm as a list-decoding algorithm for CRT codes.

Function-field analogue is famous 1999 Guruswami–Sudan algorithm for list decoding of Reed–Solomon codes.

Can build grand unified picture of "Coppersmith-type" algorithms and "Sudan-type" algorithms. See, e.g., my survey paper "Reducing lattice bases to find small-height values of univariate polynomials."

2008 Bernstein:

Tweak parameter
in the same algor
to find all divisor
linear combinatio
with small coprim

$+ v\mathbf{Z}$,
$, n$

time

e:
for

ave-
nial-
$4+\epsilon}$.

2000 Boneh: can view same
algorithm as a list-decoding
algorithm for CRT codes.

Function-field analogue is
famous 1999 Guruswami–Sudan
algorithm for list decoding
of Reed–Solomon codes.

Can build grand unified picture
of "Coppersmith-type" algorithms
and "Sudan-type" algorithms.
See, e.g., my survey paper
"Reducing lattice bases
to find small-height values
of univariate polynomials."

2008 Bernstein:

Tweak parameters
in the same algorithm
to find all divisors of n tha
linear combinations of u, v
with small coprime coeffici

2000 Boneh: can view same algorithm as a list-decoding algorithm for CRT codes.

Function-field analogue is famous 1999 Guruswami–Sudan algorithm for list decoding of Reed–Solomon codes.

Can build grand unified picture of "Coppersmith-type" algorithms and "Sudan-type" algorithms. See, e.g., my survey paper "Reducing lattice bases to find small-height values of univariate polynomials."

2008 Bernstein:

Tweak parameters
in the same algorithm
to find all divisors of n that are
linear combinations of u, v
with small coprime coefficients.

2000 Boneh: can view same algorithm as a list-decoding algorithm for CRT codes.

Function-field analogue is famous 1999 Guruswami–Sudan algorithm for list decoding of Reed–Solomon codes.

Can build grand unified picture of "Coppersmith-type" algorithms and "Sudan-type" algorithms. See, e.g., my survey paper "Reducing lattice bases to find small-height values of univariate polynomials."

2008 Bernstein:

Tweak parameters in the same algorithm to find all divisors of n that are linear combinations of u, v with small coprime coefficients.

Apply to the Goppa situation: analogous algorithm finds all divisors of $\prod_i (x - a_i)$ that are linear combinations of ϵ_0, ϵ_1 with small coprime coefficients.

Compared to Patterson, pushes allowable weight of m up to $\approx t + t^2/n$.

Boneh: can view same
hm as a list-decoding
hm for CRT codes.

on-field analogue is
s 1999 Guruswami–Sudan
hm for list decoding
d–Solomon codes.

uild grand unified picture
ppersmith-type" algorithms
udan-type" algorithms.
g., my survey paper
cing lattice bases
small-height values
ariate polynomials."

2008 Bernstein:

Tweak parameters
in the same algorithm
to find all divisors of n that are
linear combinations of u, v
with small coprime coefficients.

Apply to the Goppa situation:
analogous algorithm finds all
divisors of $\prod_i (x - a_i)$ that are
linear combinations of ϵ_0, ϵ_1
with small coprime coefficients.

Compared to Patterson,
pushes allowable weight of m
up to $\approx t + t^2/n$.

New al
is copri

Easy to
a small

... unl
ϵ_1/ϵ_0 i
Can th

I don't
Weil fo
can sho
$\epsilon_0(x)\epsilon$

has no

n view same
st-decoding
T codes.

alogue is
ruswami–Sudan
decoding
n codes.

unified picture
-type" algorithms
" algorithms.
vey paper
e bases
ght values
ynomials."

2008 Bernstein:

Tweak parameters
in the same algorithm
to find all divisors of n that are
linear combinations of u, v
with small coprime coefficients.

Apply to the Goppa situation:
analogous algorithm finds all
divisors of $\prod_i (x - a_i)$ that are
linear combinations of ϵ_0, ϵ_1
with small coprime coefficients.

Compared to Patterson,
pushes allowable weight of m
up to $\approx t + t^2/n$.

New algorithm as
is coprime to $\prod_i$

Easy to achieve b
a small multiple

... unless $n = q$
ϵ_1/ϵ_0 is a permu
Can this happen

I don't know any
Weil forces rathe
can show that th

$$\frac{\epsilon_0(x)\epsilon_1(y) - \epsilon_1(}{x - y}$$

has no points ov

ne
g

Sudan

cture
orithms
ms.

2008 Bernstein:

Tweak parameters
in the same algorithm
to find all divisors of n that are
linear combinations of u, v
with small coprime coefficients.

Apply to the Goppa situation:
analogous algorithm finds all
divisors of $\prod_i (x - a_i)$ that are
linear combinations of ϵ_0, ϵ_1
with small coprime coefficients.

Compared to Patterson,
pushes allowable weight of m
up to $\approx t + t^2/n$.

New algorithm assumes tha
is coprime to $\prod_i (x - a_i)$.

Easy to achieve by adding
a small multiple of ϵ_0 to ϵ_1

... unless $n = q$ and
ϵ_1/ϵ_0 is a permutation fun
Can this happen to Patters

I don't know any examples
Weil forces rather large deg
can show that the curve

$$\frac{\epsilon_0(x)\epsilon_1(y) - \epsilon_1(x)\epsilon_0(y)}{x - y} =$$

has no points over $\mathbf{F}_q$.

2008 Bernstein:

Tweak parameters
in the same algorithm
to find all divisors of n that are
linear combinations of u, v
with small coprime coefficients.

Apply to the Goppa situation:
analogous algorithm finds all
divisors of $\prod_i (x - a_i)$ that are
linear combinations of ϵ_0, ϵ_1
with small coprime coefficients.

Compared to Patterson,
pushes allowable weight of m
up to $\approx t + t^2/n$.

New algorithm assumes that ϵ_1
is coprime to $\prod_i (x - a_i)$.

Easy to achieve by adding
a small multiple of ϵ_0 to ϵ_1.

... unless $n = q$ and
ϵ_1/ϵ_0 is a permutation function.
Can this happen to Patterson?

I don't know any examples.
Weil forces rather large degree:
can show that the curve

$$\frac{\epsilon_0(x)\epsilon_1(y) - \epsilon_1(x)\epsilon_0(y)}{x - y} = 0$$

has no points over $\mathbf{F}_q$.

Bernstein:

parameters
same algorithm
all divisors of n that are
combinations of u, v
mall coprime coefficients.

to the Goppa situation:
ous algorithm finds all
s of $\prod_i (x - a_i)$ that are
combinations of ϵ_0, ϵ_1
mall coprime coefficients.

red to Patterson,
allowable weight of m
$\approx t + t^2/n$.

New algorithm assumes that ϵ_1
is coprime to $\prod_i (x - a_i)$.

Easy to achieve by adding
a small multiple of ϵ_0 to ϵ_1.

... unless $n = q$ and
ϵ_1/ϵ_0 is a permutation function.
Can this happen to Patterson?

I don't know any examples.
Weil forces rather large degree:
can show that the curve

$$\frac{\epsilon_0(x)\epsilon_1(y) - \epsilon_1(x)\epsilon_0(y)}{x - y} = 0$$

has no points over $\mathbf{F}_q$.

Many
in code

e.g. 20
Hide q
as quas
Key le
Encryp
Decryp

2009 B
to Misc
reducin

rs
rithm
s of n that are
ons of u, v
me coefficients.

ppa situation:
thm finds all
$- a_i)$ that are
ons of ϵ_0, ϵ_1
me coefficients.

tterson,
weight of m
.

New algorithm assumes that ϵ_1 is coprime to $\prod_i (x - a_i)$.

Easy to achieve by adding a small multiple of ϵ_0 to ϵ_1.

. . . unless $n = q$ and ϵ_1/ϵ_0 is a permutation function.
Can this happen to Patterson?

I don't know any examples.
Weil forces rather large degree:
can show that the curve

$$\frac{\epsilon_0(x)\epsilon_1(y) - \epsilon_1(x)\epsilon_0(y)}{x - y} = 0$$

has no points over $\mathbf{F}_q$.

Many other curre
in code-based cry

e.g. 2009 Misocz
Hide quasi-dyadi
as quasi-dyadic p
Key length only
Encryption time
Decryption time

2009 Bernstein:
to Misoczki–Barr
reducing time to

t are

ents.

on:

all

t are

ϵ_1

ents.

m

New algorithm assumes that ϵ_1 is coprime to $\prod_i (x - a_i)$.

Easy to achieve by adding a small multiple of ϵ_0 to ϵ_1.

... unless $n = q$ and ϵ_1/ϵ_0 is a permutation function. Can this happen to Patterson?

I don't know any examples. Weil forces rather large degree: can show that the curve

$$\frac{\epsilon_0(x)\epsilon_1(y) - \epsilon_1(x)\epsilon_0(y)}{x - y} = 0$$

has no points over $\mathbf{F}_q$.

Many other current topics in code-based cryptography

e.g. 2009 Misoczki–Barreto Hide quasi-dyadic Goppa c as quasi-dyadic public key. Key length only $b^{1+o(1)}$. Encryption time $b^{\lg 3+o(1)}$. Decryption time $b^{\lg 3+o(1)}$.

2009 Bernstein: easy tweak to Misoczki–Barreto algorit reducing time to $b^{1+o(1)}$.

New algorithm assumes that ϵ_1 is coprime to $\prod_i (x - a_i)$.

Easy to achieve by adding a small multiple of ϵ_0 to ϵ_1.

... unless $n = q$ and ϵ_1/ϵ_0 is a permutation function. Can this happen to Patterson?

I don't know any examples.

Weil forces rather large degree: can show that the curve

$$\frac{\epsilon_0(x)\epsilon_1(y) - \epsilon_1(x)\epsilon_0(y)}{x - y} = 0$$

has no points over $\mathbf{F}_q$.

Many other current topics in code-based cryptography.

e.g. 2009 Misoczki–Barreto: Hide quasi-dyadic Goppa code as quasi-dyadic public key. Key length only $b^{1+o(1)}$. Encryption time $b^{\lg 3+o(1)}$. Decryption time $b^{\lg 3+o(1)}$.

2009 Bernstein: easy tweak to Misoczki–Barreto algorithms, reducing time to $b^{1+o(1)}$.

gorithm assumes that ϵ_1
ime to $\prod_i (x - a_i)$.

o achieve by adding
l multiple of ϵ_0 to ϵ_1.

ess $n = q$ and
s a permutation function.
is happen to Patterson?

know any examples.
orces rather large degree:
ow that the curve

$$\frac{\epsilon_1(y) - \epsilon_1(x)\epsilon_0(y)}{x - y} = 0$$

points over $\mathbf{F}_q$.

Many other current topics
in code-based cryptography.

e.g. 2009 Misoczki–Barreto:
Hide quasi-dyadic Goppa code
as quasi-dyadic public key.
Key length only $b^{1+o(1)}$.
Encryption time $b^{\lg 3+o(1)}$.
Decryption time $b^{\lg 3+o(1)}$.

2009 Bernstein: easy tweak
to Misoczki–Barreto algorithms,
reducing time to $b^{1+o(1)}$.

Last sli

2009.0
Special
Attacki

2009.1
Perform
Encryp
and Cr
Submis

2010.0
Third I
on Pos
Submis

ssumes that ϵ_1
$(x - a_i)$.

by adding
of ϵ_0 to ϵ_1.

and
tation function.
to Patterson?

examples.
r large degree:
e curve
$\frac{x)\epsilon_0(y)}{} = 0$

er $\mathbf{F}_q$.

Many other current topics
in code-based cryptography.

e.g. 2009 Misoczki–Barreto:
Hide quasi-dyadic Goppa code
as quasi-dyadic public key.
Key length only $b^{1+o(1)}$.
Encryption time $b^{\lg 3+o(1)}$.
Decryption time $b^{\lg 3+o(1)}$.

2009 Bernstein: easy tweak
to Misoczki–Barreto algorithms,
reducing time to $b^{1+o(1)}$.

Last slide: adver

2009.09.09–10, L
Special-purpose
Attacking Crypto

2009.10.12–13, E
Performance Enh
Encryption and D
and Cryptograph
Submission dead

2010.05.25–28, D
Third Internation
on Post-Quantum
Submission dead

at ϵ_1

$_1$.

ction.

son?

.

gree:

= 0

Many other current topics
in code-based cryptography.

e.g. 2009 Misoczki–Barreto:
Hide quasi-dyadic Goppa code
as quasi-dyadic public key.
Key length only $b^{1+o(1)}$.
Encryption time $b^{\lg 3+o(1)}$.
Decryption time $b^{\lg 3+o(1)}$.

2009 Bernstein: easy tweak
to Misoczki–Barreto algorithms,
reducing time to $b^{1+o(1)}$.

Last slide: advertisements

2009.09.09–10, Lausanne:
Special-purpose Hardware
Attacking Cryptographic S

2009.10.12–13, Berlin: Sof
Performance Enhancement
Encryption and Decryption
and Cryptographic Compile
Submission deadline 2009.

2010.05.25–28, Darmstadt
Third International Worksh
on Post-Quantum Cryptog
Submission deadline 2009.

Many other current topics
in code-based cryptography.

e.g. 2009 Misoczki–Barreto:
Hide quasi-dyadic Goppa code
as quasi-dyadic public key.
Key length only $b^{1+o(1)}$.
Encryption time $b^{\lg 3+o(1)}$.
Decryption time $b^{\lg 3+o(1)}$.

2009 Bernstein: easy tweak
to Misoczki–Barreto algorithms,
reducing time to $b^{1+o(1)}$.

Last slide: advertisements

2009.09.09–10, Lausanne:
Special-purpose Hardware for
Attacking Cryptographic Systems.

2009.10.12–13, Berlin: Software
Performance Enhancement for
Encryption and Decryption
and Cryptographic Compilers.
Submission deadline 2009.08.30.

2010.05.25–28, Darmstadt: The
Third International Workshop
on Post-Quantum Cryptography.
Submission deadline 2009.11.15.