The impact of security proofs: two troublesome case studies

D. J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

2004: GCM is published
with security proof.

2004: XCBv1 is published.

The impact of security proofs: two troublesome case studies

D. J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

2004: GCM is published with security proof.

2004: XCBv1 is published.

2007: NIST standardizes GCM.

2007: XCBv2 is published with security proof.

The impact of security proofs: two troublesome case studies

D. J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

2004: GCM is published with security proof.

2004: XCBv1 is published.

2007: NIST standardizes GCM.

2007: XCBv2 is published with security proof.

2010: IEEE standardizes XCBv2.

The impact of security proofs: two troublesome case studies

D. J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

2004: GCM is published
with security proof.

2004: XCBv1 is published.

2007: NIST standardizes GCM.

2007: XCBv2 is published
with security proof.

2010: IEEE standardizes XCBv2.

2014 Wi
is used i
(MACse
802.11a
ANSI (I
Security
P1619.1
standard
AES-GC
NSA Su

The impact of security proofs: two troublesome case studies

D. J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

2004: GCM is published
with security proof.

2004: XCBv1 is published.

2007: NIST standardizes GCM.

2007: XCBv2 is published
with security proof.

2010: IEEE standardizes XCBv2.

2014 Wikipedia: “
is used in the IEEE
(MACsec) Etherne
802.11ad (also kn
ANSI (INCITS) Fi
Security Protocols
P1619.1 tape stor
standards, SSH an
AES-GCM is inclu
NSA Suite B Cryp

The impact of security proofs: two troublesome case studies

D. J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

2004: GCM is published with security proof.

2004: XCBv1 is published.

2007: NIST standardizes GCM.

2007: XCBv2 is published with security proof.

2010: IEEE standardizes XCBv2.

2014 Wikipedia: “GCM mod
is used in the IEEE 802.1AE
(MACsec) Ethernet security,
802.11ad (also known as Wi
ANSI (INCITS) Fibre Chann
Security Protocols (FC-SP),
P1619.1 tape storage, IETF
standards, SSH and TLS 1.2
AES-GCM is included into t
NSA Suite B Cryptography.

The impact of security proofs: two troublesome case studies

D. J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

2004: GCM is published with security proof.

2004: XCBv1 is published.

2007: NIST standardizes GCM.

2007: XCBv2 is published with security proof.

2010: IEEE standardizes XCBv2.

2014 Wikipedia: "GCM mode is used in the IEEE 802.1AE (MACsec) Ethernet security, IEEE 802.11ad (also known as WiGig), ANSI (INCITS) Fibre Channel Security Protocols (FC-SP), IEEE P1619.1 tape storage, IETF IPsec standards, SSH and TLS 1.2. AES-GCM is included into the NSA Suite B Cryptography. . . .

The impact of security proofs: two troublesome case studies

D. J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

2004: GCM is published with security proof.

2004: XCBv1 is published.

2007: NIST standardizes GCM.

2007: XCBv2 is published with security proof.

2010: IEEE standardizes XCBv2.

2014 Wikipedia: "GCM mode is used in the IEEE 802.1AE (MACsec) Ethernet security, IEEE 802.11ad (also known as WiGig), ANSI (INCITS) Fibre Channel Security Protocols (FC-SP), IEEE P1619.1 tape storage, IETF IPsec standards, SSH and TLS 1.2. AES-GCM is included into the NSA Suite B Cryptography. . . . GCM has been **proven secure in the concrete security model**."

The impact of security proofs: two troublesome case studies

D. J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

2004: GCM is published with security proof.

2004: XCBv1 is published.

2007: NIST standardizes GCM.

2007: XCBv2 is published with security proof.

2010: IEEE standardizes XCBv2.

2014 Wikipedia: "GCM mode is used in the IEEE 802.1AE (MACsec) Ethernet security, IEEE 802.11ad (also known as WiGig), ANSI (INCITS) Fibre Channel Security Protocols (FC-SP), IEEE P1619.1 tape storage, IETF IPsec standards, SSH and TLS 1.2. AES-GCM is included into the NSA Suite B Cryptography. . . . GCM has been **proven secure in the concrete security model**."

XCB also widely used? Maybe.

pact of security proofs:
ublesome case studies

ernstein

ty of Illinois at Chicago &
che Universiteit Eindhoven

CM is published
urity proof.

CBv1 is published.

IST standardizes GCM.

CBv2 is published
urity proof.

EEE standardizes XCBv2.

2014 Wikipedia: "GCM mode is used in the IEEE 802.1AE (MACsec) Ethernet security, IEEE 802.11ad (also known as WiGig), ANSI (INCITS) Fibre Channel Security Protocols (FC-SP), IEEE P1619.1 tape storage, IETF IPsec standards, SSH and TLS 1.2. AES-GCM is included into the NSA Suite B Cryptography. . . . GCM has been **proven secure in the concrete security model**."

XCB also widely used? Maybe.

2012 Iwa
Original
New att
main pa
New pro

urity proofs:
ase studies

is at Chicago &
siteit Eindhoven

---

blished
f.

ublished.

ardizes GCM.

ublished
f.

ardizes XCBv2.

2014 Wikipedia: “GCM mode is used in the IEEE 802.1AE (MACsec) Ethernet security, IEEE 802.11ad (also known as WiGig), ANSI (INCITS) Fibre Channel Security Protocols (FC-SP), IEEE P1619.1 tape storage, IETF IPsec standards, SSH and TLS 1.2. AES-GCM is included into the NSA Suite B Cryptography. . . . GCM has been **proven secure in the concrete security model**.”

XCB also widely used? Maybe.

2012 Iwata–Ohash
Original GCM proo
New attack “inval
main part of the p
New proof, **lower**

fs:
s

ago &
hoven

CM.

CBv2.

2014 Wikipedia: “GCM mode is used in the IEEE 802.1AE (MACsec) Ethernet security, IEEE 802.11ad (also known as WiGig), ANSI (INCITS) Fibre Channel Security Protocols (FC-SP), IEEE P1619.1 tape storage, IETF IPsec standards, SSH and TLS 1.2. AES-GCM is included into the NSA Suite B Cryptography. . . . GCM has been **proven secure in the concrete security model**.”

XCB also widely used? Maybe.

2012 Iwata–Ohashi–Minema
Original GCM proof was wro
New attack “invalidates the
main part of the privacy pro
New proof, **lower security l**

2014 Wikipedia: "GCM mode is used in the IEEE 802.1AE (MACsec) Ethernet security, IEEE 802.11ad (also known as WiGig), ANSI (INCITS) Fibre Channel Security Protocols (FC-SP), IEEE P1619.1 tape storage, IETF IPsec standards, SSH and TLS 1.2. AES-GCM is included into the NSA Suite B Cryptography. . . . GCM has been **proven secure in the concrete security model**."

XCB also widely used? Maybe.

2012 Iwata–Ohashi–Minematsu: Original GCM proof was wrong. New attack "invalidates the main part of the privacy proof". New proof, **lower security level**.

2014 Wikipedia: “GCM mode is used in the IEEE 802.1AE (MACsec) Ethernet security, IEEE 802.11ad (also known as WiGig), ANSI (INCITS) Fibre Channel Security Protocols (FC-SP), IEEE P1619.1 tape storage, IETF IPsec standards, SSH and TLS 1.2. AES-GCM is included into the NSA Suite B Cryptography. . . . GCM has been **proven secure in the concrete security model**.”

XCB also widely used? Maybe.

2012 Iwata–Ohashi–Minematsu: Original GCM proof was wrong. New attack “invalidates the main part of the privacy proof”. New proof, **lower security level**.

2013 Chakraborty–Hernandez-Jimenez–Sarkar: Original XCBv2 proof was wrong. New proof for some message lengths, but the “resulting bound that can be proved is much worse than what has been claimed by the authors.”

2014 Wikipedia: "GCM mode is used in the IEEE 802.1AE (MACsec) Ethernet security, IEEE 802.11ad (also known as WiGig), ANSI (INCITS) Fibre Channel Security Protocols (FC-SP), IEEE P1619.1 tape storage, IETF IPsec standards, SSH and TLS 1.2. AES-GCM is included into the NSA Suite B Cryptography. . . . GCM has been **proven secure in the concrete security model**."

XCB also widely used? Maybe.

2012 Iwata–Ohashi–Minematsu: Original GCM proof was wrong. New attack "invalidates the main part of the privacy proof". New proof, **lower security level**.

2013 Chakraborty–Hernandez-Jimenez–Sarkar: Original XCBv2 proof was wrong. New proof for some message lengths, but the "resulting bound that can be proved is much worse than what has been claimed by the authors." New **efficient attack** on XCBv2 for other message lengths.

ikipedia: “GCM mode
n the IEEE 802.1AE
c) Ethernet security, IEEE
d (also known as WiGig),
NCITS) Fibre Channel
Protocols (FC-SP), IEEE
tape storage, IETF IPsec
ls, SSH and TLS 1.2.
M is included into the
ite B Cryptography. . . .
s been **proven secure in
crete security model**.”

o widely used? Maybe.

2012 Iwata–Ohashi–Minematsu: Original GCM proof was wrong. New attack “invalidates the main part of the privacy proof”. New proof, **lower security level**.

2013 Chakraborty–Hernandez-Jimenez–Sarkar: Original XCBv2 proof was wrong. New proof for some message lengths, but the “resulting bound that can be proved is much worse than what has been claimed by the authors.” New **efficient attack** on XCBv2 for other message lengths.

What do

Modern
is fragile

Do we h
to elimin

“GCM mode
E 802.1AE
et security, IEEE
own as WiGig),
bre Channel
(FC-SP), IEEE
age, IETF IPsec
nd TLS 1.2.
ded into the
tography. . . .
oven secure in
urity model.”

sed? Maybe.

2012 Iwata–Ohashi–Minematsu: Original GCM proof was wrong. New attack “invalidates the main part of the privacy proof”. New proof, **lower security level**.

2013 Chakraborty–Hernandez-Jimenez–Sarkar: Original XCBv2 proof was wrong. New proof for some message lengths, but the “resulting bound that can be proved is much worse than what has been claimed by the authors.” New **efficient attack** on XCBv2 for other message lengths.

What does this mo

Modern “provable
is fragile and untru

Do we have a stra
to eliminate these

de
E
IEEE
Gig),
el
IEEE
IPsec
2.
he
. . .
re in
lel.”
be.

2012 Iwata–Ohashi–Minematsu: Original GCM proof was wrong. New attack “invalidates the main part of the privacy proof”. New proof, **lower security level**.

2013 Chakraborty–Hernandez-Jimenez–Sarkar: Original XCBv2 proof was wrong. New proof for some message lengths, but the “resulting bound that can be proved is much worse than what has been claimed by the authors.” New **efficient attack** on XCBv2 for other message lengths.

What does this mean?

Modern “provable security” is fragile and untrustworthy.

Do we have a strategy to eliminate these failures?

2012 Iwata–Ohashi–Minematsu: Original GCM proof was wrong. New attack "invalidates the main part of the privacy proof". New proof, **lower security level**.

2013 Chakraborty–Hernandez-Jimenez–Sarkar: Original XCBv2 proof was wrong. New proof for some message lengths, but the "resulting bound that can be proved is much worse than what has been claimed by the authors." New **efficient attack** on XCBv2 for other message lengths.

What does this mean?

Modern "provable security" is fragile and untrustworthy.

Do we have a strategy to eliminate these failures?

2012 Iwata–Ohashi–Minematsu: Original GCM proof was wrong. New attack “invalidates the main part of the privacy proof”. New proof, **lower security level**.

2013 Chakraborty–Hernandez-Jimenez–Sarkar: Original XCBv2 proof was wrong. New proof for some message lengths, but the “resulting bound that can be proved is much worse than what has been claimed by the authors.” New **efficient attack** on XCBv2 for other message lengths.

What does this mean?

Modern “provable security” is fragile and untrustworthy.

Do we have a strategy to eliminate these failures?

Do security proofs actually reduce risk compared to thorough cryptanalysis?

2012 Iwata–Ohashi–Minematsu: Original GCM proof was wrong. New attack "invalidates the main part of the privacy proof". New proof, **lower security level**.

2013 Chakraborty–Hernandez-Jimenez–Sarkar: Original XCBv2 proof was wrong. New proof for some message lengths, but the "resulting bound that can be proved is much worse than what has been claimed by the authors." New **efficient attack** on XCBv2 for other message lengths.

What does this mean?

Modern "provable security" is fragile and untrustworthy.

Do we have a strategy to eliminate these failures?

Do security proofs actually reduce risk compared to thorough cryptanalysis?

Did the security proofs encourage standardization *without* thorough cryptanalysis?

2012 Iwata–Ohashi–Minematsu: Original GCM proof was wrong. New attack "invalidates the main part of the privacy proof". New proof, **lower security level**.

2013 Chakraborty–Hernandez-Jimenez–Sarkar: Original XCBv2 proof was wrong. New proof for some message lengths, but the "resulting bound that can be proved is much worse than what has been claimed by the authors." New **efficient attack** on XCBv2 for other message lengths.

What does this mean?

Modern "provable security" is fragile and untrustworthy.

Do we have a strategy to eliminate these failures?

Do security proofs actually reduce risk compared to thorough cryptanalysis?

Did the security proofs encourage standardization *without* thorough cryptanalysis?

Did the security proofs *deter* cryptanalysis?