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.
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.

2014 Wikipedia: "GCM mode is used in the IEEE 802.1AE (MACsec) Ethernet security, IEEE 802.11ad, ANSI (INCITS) Fibre Channel Security Protocols (FC-SP), IEEE P1619.1 tape storage, IETF IPsec standards, 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.

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, IEEE P1619.1 tape storage standards, SSH and 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.

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), 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.

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.

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.

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.
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.

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.
The impact of security proofs: two troublesome case studies

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

2004: GCM is published
2004: XCBv1 is published.
2007: NIST standardizes GCM.
2007: XCBv2 is published with security proof.

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.
2004: GCM is published with security proof.
2004: XCBv1 is published.
2007: NIST standardizes GCM.
2007: XCBv2 is published with security proof.

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.
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.
GCM mode is used in the IEEE 802.1AE (MACsec) Ethernet security, IEEE 802.11ad (also known as WiGig), ANSI (INCITS) Fibre Channel Protocols (FC-SP), IEEE 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.

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.

Modern “provable security” is fragile and untrustworthy. Do we have a strategy to eliminate these failures?
“GCM mode is used in the IEEE 802.1AE (MACsec) Ethernet security, IEEE 802.11ad (also known as WiGig), Fibre Channel (FC-SP), and TLS 1.2. AES-GCM is included into the NSA Suite B Cryptography.

GCM has been proven secure in the concrete security model.

Modern “provable security” is fragile and untrustworthy. Do we have a strategy to eliminate these failures?

What does this mean?
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?