The HMAC brawl

Daniel J. Bernstein
University of Illinois at Chicago

2012.02.19 Koblitz–Menezes "Another look at HMAC":

"... Third, we describe a fundamental flaw in Bellare's 2006 security proof for HMAC, and show that with the flaw removed the proof gives a security guarantee that is of little value in practice."

2012.03.02: "Bellare contacted us and told us that he strongly objected to our language—especially the word 'flaw'—..."

IAC brawl

. Bernstein
ty of Illinois at Chicago

2012.02.19 Koblitz–Menezes
"Another look at HMAC":

"... Third, we describe a
fundamental flaw in Bellare's
2006 security proof for HMAC,
and show that with the
flaw removed the proof gives
a security guarantee that is of
little value in practice."

2012.03.02: "Bellare contacted
us and told us that he strongly
objected to our language—
especially the word 'flaw'—..."

Yehuda
really ou
there is
the proo
uniform
to not b
is NO F

Jonatha
researche
concerne
Alfred M
an invite
2012 rel
criticizin
I share t

n

is at Chicago

2012.02.19 Koblitz–Menezes "Another look at HMAC":

"... Third, we describe a fundamental flaw in Bellare's 2006 security proof for HMAC, and show that with the flaw removed the proof gives a security guarantee that is of little value in practice."

2012.03.02: "Bellare contacted us and told us that he strongly objected to our language—especially the word 'flaw'—..."

Yehuda Lindell: "T
really outdid them
there is actually n
the proof of securi
uniform model, wh
to not be familiar
is NO FLAW here

Jonathan Katz: "I
researchers are jus
concerned about t
Alfred Menezes wi
an invited talk at
2012 related to his
criticizing provable
I share this concer

ago

2012.02.19 Koblitz–Menezes
"Another look at HMAC":

"... Third, we describe a
fundamental flaw in Bellare's
2006 security proof for HMAC,
and show that with the
flaw removed the proof gives
a security guarantee that is of
little value in practice."

2012.03.02: "Bellare contacted
us and told us that he strongly
objected to our language—
especially the word 'flaw'—..."

Yehuda Lindell: "This time
really outdid themselves sinc
there is actually no error. Ra
the proof of security is in th
uniform model, which they a
to not be familiar with. ...
is NO FLAW here whatsoeve

Jonathan Katz: "Many
researchers are justifiably
concerned about the fact th
Alfred Menezes will be givin
an invited talk at Eurocrypt
2012 related to his line of pa
criticizing provable security.
I share this concern."

2012.02.19 Koblitz–Menezes "Another look at HMAC":

"... Third, we describe a fundamental flaw in Bellare's 2006 security proof for HMAC, and show that with the flaw removed the proof gives a security guarantee that is of little value in practice."

2012.03.02: "Bellare contacted us and told us that he strongly objected to our language—especially the word 'flaw'—..."

Yehuda Lindell: "This time they really outdid themselves since there is actually no error. Rather the proof of security is in the non-uniform model, which they appear to not be familiar with. ... There is NO FLAW here whatsoever."

Jonathan Katz: "Many researchers are justifiably concerned about the fact that Alfred Menezes will be giving an invited talk at Eurocrypt 2012 related to his line of papers criticizing provable security. I share this concern."

.19 Koblitz–Menezes
er look at HMAC":

rd, we describe a
ental flaw in Bellare's
curity proof for HMAC,
w that with the
noved the proof gives
ty guarantee that is of
ue in practice."

.02: "Bellare contacted
old us that he strongly
to our language—
y the word 'flaw'—. . ."

Yehuda Lindell: "This time they really outdid themselves since there is actually no error. Rather the proof of security is in the non-uniform model, which they appear to not be familiar with. . . . There is NO FLAW here whatsoever."

Jonathan Katz: "Many researchers are justifiably concerned about the fact that Alfred Menezes will be giving an invited talk at Eurocrypt 2012 related to his line of papers criticizing provable security. I share this concern."

2012.03.
". . . Thi
fundame
practice-
Bellare's
HMAC,
defect re
a securit
little val

z–Menezes
HMAC":

cribe a
in Bellare's
of for HMAC,
h the
proof gives
ee that is of
tice."

are contacted
t he strongly
nguage—
d 'flaw'—..."

Yehuda Lindell: "This time they really outdid themselves since there is actually no error. Rather the proof of security is in the non-uniform model, which they appear to not be familiar with. ... There is NO FLAW here whatsoever."

Jonathan Katz: "Many researchers are justifiably concerned about the fact that Alfred Menezes will be giving an invited talk at Eurocrypt 2012 related to his line of papers criticizing provable security. I share this concern."

2012.03.17 Koblitz
"... Third, we des
fundamental defec
practice-oriented s
Bellare's 2006 secu
HMAC, and show
defect removed his
a security guarante
little value in prac

s

s
AC,

s
of

ted
gly

. . ”

Yehuda Lindell: “This time they really outdid themselves since there is actually no error. Rather the proof of security is in the non-uniform model, which they appear to not be familiar with. . . . There is NO FLAW here whatsoever.”

Jonathan Katz: “Many researchers are justifiably concerned about the fact that Alfred Menezes will be giving an invited talk at Eurocrypt 2012 related to his line of papers criticizing provable security. I share this concern.”

2012.03.17 Koblitz–Meneze
“. . . Third, we describe a fundamental defect from a practice-oriented standpoint Bellare’s 2006 security result HMAC, and show that with defect removed his proof giv a security guarantee that is little value in practice.”

Yehuda Lindell: "This time they really outdid themselves since there is actually no error. Rather the proof of security is in the non-uniform model, which they appear to not be familiar with. ... There is NO FLAW here whatsoever."

Jonathan Katz: "Many researchers are justifiably concerned about the fact that Alfred Menezes will be giving an invited talk at Eurocrypt 2012 related to his line of papers criticizing provable security. I share this concern."

2012.03.17 Koblitz–Menezes: "... Third, we describe a fundamental defect from a practice-oriented standpoint in Bellare's 2006 security result for HMAC, and show that with this defect removed his proof gives a security guarantee that is of little value in practice."

Yehuda Lindell: "This time they really outdid themselves since there is actually no error. Rather the proof of security is in the non-uniform model, which they appear to not be familiar with. ... There is NO FLAW here whatsoever."

Jonathan Katz: "Many researchers are justifiably concerned about the fact that Alfred Menezes will be giving an invited talk at Eurocrypt 2012 related to his line of papers criticizing provable security. I share this concern."

2012.03.17 Koblitz–Menezes: "... Third, we describe a fundamental defect from a practice-oriented standpoint in Bellare's 2006 security result for HMAC, and show that with this defect removed his proof gives a security guarantee that is of little value in practice."

What's going on here?

Lindell: "This time they
utdid themselves since
actually no error. Rather
of of security is in the non-
model, which they appear
e familiar with. . . . There
LAW here whatsoever."

n Katz: "Many
ers are justifiably
ed about the fact that
Menezes will be giving
ed talk at Eurocrypt
ated to his line of papers
g provable security.
his concern."

2012.03.17 Koblitz–Menezes:
"... Third, we describe a
fundamental defect from a
practice-oriented standpoint in
Bellare's 2006 security result for
HMAC, and show that with this
defect removed his proof gives
a security guarantee that is of
little value in practice."

What's going on here?

Classic B
metric fo

"The ma
over all
restricte
example
of the 'a
that the
in the ga
[the ciph
from a r

This time they
selves since
o error. Rather
ty is in the non-
hich they appear
with. . . . There
whatsoever."

Many
tifiably
he fact that
ll be giving
Eurocrypt
s line of papers
e security.
n."

2012.03.17 Koblitz–Menezes:
"... Third, we describe a fundamental defect from a practice-oriented standpoint in Bellare's 2006 security result for HMAC, and show that with this defect removed his proof gives a security guarantee that is of little value in practice."

What's going on here?

Classic Bellare–Kil
metric for cipher i

"The maximum,
over all adversaries
restricted to q' inp
examples and exec
of the 'advantage'
that the adversary
in the game of dis
[the cipher for a se
from a random pe

they
ce
ather
e non-
appear
There
er."

at
g

apers

2012.03.17 Koblitz–Menezes:
"... Third, we describe a fundamental defect from a practice-oriented standpoint in Bellare's 2006 security result for HMAC, and show that with this defect removed his proof gives a security guarantee that is of little value in practice."

What's going on here?

Classic Bellare–Kilian–Rogaw
metric for cipher insecurity:

"The maximum,
over all adversaries
restricted to q' input-output
examples and execution time
of the 'advantage'
that the adversary has
in the game of distinguishing
[the cipher for a secret key]
from a random permutation

2012.03.17 Koblitz–Menezes:
"... Third, we describe a fundamental defect from a practice-oriented standpoint in Bellare's 2006 security result for HMAC, and show that with this defect removed his proof gives a security guarantee that is of little value in practice."

What's going on here?

Classic Bellare–Kilian–Rogaway metric for cipher insecurity:

"The maximum,
over all adversaries
restricted to q' input-output
examples and execution time t',
of the 'advantage'
that the adversary has
in the game of distinguishing
[the cipher for a secret key]
from a random permutation."

.17 Koblitz–Menezes:
rd, we describe a
ental defect from a
-oriented standpoint in
s 2006 security result for
and show that with this
emoved his proof gives
ty guarantee that is of
ue in practice."

---

going on here?

Classic Bellare–Kilian–Rogaway
metric for cipher insecurity:

"The maximum,
over all adversaries
restricted to q' input-output
examples and execution time t',
of the 'advantage'
that the adversary has
in the game of distinguishing
[the cipher for a secret key]
from a random permutation."

2005 Be

"For exa
somethi

$$\leq c_1 \cdot \frac{t/}{}$$

... In ot
we are c
attacks
search o
We migh
to AES
like [AE

$$\leq c_1 \cdot \frac{t/}{}$$

z–Menezes:
cribe a
ct from a
standpoint in
urity result for
that with this
s proof gives
ee that is of
tice."

---

here?

Classic Bellare–Kilian–Rogaway
metric for cipher insecurity:

"The maximum,
over all adversaries
restricted to q' input-output
examples and execution time t',
of the 'advantage'
that the adversary has
in the game of distinguishing
[the cipher for a secret key]
from a random permutation."

2005 Bellare–Roga

"For example we n
something like [DE
$\leq c_1 \cdot \frac{t/T_{\mathrm{DES}}}{2^{55}} + c$
... In other words
we are conjecturin
attacks are either
search or linear cry
We might be bold
to AES and conjec
like [AES insecurit
$\leq c_1 \cdot \frac{t/T_{\mathrm{AES}}}{2^{128}} + c_2$

s:

in
t for
this
ves
of

Classic Bellare–Kilian–Rogaway metric for cipher insecurity:

"The maximum,
over all adversaries
restricted to q' input-output
examples and execution time t',
of the 'advantage'
that the adversary has
in the game of distinguishing
[the cipher for a secret key]
from a random permutation."

2005 Bellare–Rogaway:

"For example we might conj
something like [DES insecur

$$\leq c_1 \cdot \frac{t/T_{\mathsf{DES}}}{2^{55}} + c_2 \cdot \frac{q}{2^{40}}$$

... In other words,
we are conjecturing that the
attacks are either exhaustive
search or linear cryptanalysis
We might be bolder with re
to AES and conjecture some
like [AES insecurity]

$$\leq c_1 \cdot \frac{t/T_{\mathsf{AES}}}{2^{128}} + c_2 \cdot \frac{q}{2^{128}}."$$

Classic Bellare–Kilian–Rogaway metric for cipher insecurity:

"The maximum,
over all adversaries
restricted to q' input-output
examples and execution time t',
of the 'advantage'
that the adversary has
in the game of distinguishing
[the cipher for a secret key]
from a random permutation."

2005 Bellare–Rogaway:

"For example we might conjecture something like [DES insecurity]

$$\leq c_1 \cdot \frac{t/T_{\mathsf{DES}}}{2^{55}} + c_2 \cdot \frac{q}{2^{40}}$$

... In other words,
we are conjecturing that the best attacks are either exhaustive key search or linear cryptanalysis.
We might be bolder with regard to AES and conjecture something like [AES insecurity]

$$\leq c_1 \cdot \frac{t/T_{\mathsf{AES}}}{2^{128}} + c_2 \cdot \frac{q}{2^{128}}."$$

Bellare–Kilian–Rogaway
or cipher insecurity:

aximum,
adversaries
d to q' input-output
s and execution time t',
dvantage'
adversary has
ame of distinguishing
her for a secret key]
andom permutation."

2005 Bellare–Rogaway:

"For example we might conjecture something like [DES insecurity]

$$\leq c_1 \cdot \frac{t/T_{\mathsf{DES}}}{2^{55}} + c_2 \cdot \frac{q}{2^{40}}$$

... In other words,
we are conjecturing that the best attacks are either exhaustive key search or linear cryptanalysis.
We might be bolder with regard to AES and conjecture something like [AES insecurity]

$$\leq c_1 \cdot \frac{t/T_{\mathsf{AES}}}{2^{128}} + c_2 \cdot \frac{q}{2^{128}}."$$

2006 Be
(q, t) ins
$\leq$ partic
(q', t') i
compres

Quantita
"Assume
against
is exhaus
The bou
up to ro

HMAC:
key-deriv

ian–Rogaway
nsecurity:

s
but-output
cution time t',

has
tinguishing
ecret key]
rmutation."

2005 Bellare–Rogaway:

"For example we might conjecture something like [DES insecurity]

$$\leq c_1 \cdot \frac{t/T_{\mathsf{DES}}}{2^{55}} + c_2 \cdot \frac{q}{2^{40}}$$

... In other words, we are conjecturing that the best attacks are either exhaustive key search or linear cryptanalysis. We might be bolder with regard to AES and conjecture something like [AES insecurity]

$$\leq c_1 \cdot \frac{t/T_{\mathsf{AES}}}{2^{128}} + c_2 \cdot \frac{q}{2^{128}}."$$

2006 Bellare NMA
(q, t) insecurity of
$\leq$ particular functi
(q', t') insecurity o
compression funct

Quantitative summ
"Assume that the
against h as a PR
is exhaustive key s
The bound justifie
up to roughly $2^{c/2}$

HMAC: similar sto
key-derivation com

way

e t',

g

."

2005 Bellare–Rogaway:

"For example we might conjecture something like [DES insecurity]

$$\leq c_1 \cdot \frac{t/T_{\mathsf{DES}}}{2^{55}} + c_2 \cdot \frac{q}{2^{40}}$$

... In other words,
we are conjecturing that the best attacks are either exhaustive key search or linear cryptanalysis.
We might be bolder with regard to AES and conjecture something like [AES insecurity]

$$\leq c_1 \cdot \frac{t/T_{\mathsf{AES}}}{2^{128}} + c_2 \cdot \frac{q}{2^{128}}."$$

2006 Bellare NMAC theorem

(q, t) insecurity of NMAC-H
$\leq$ particular function of
(q', t') insecurity of the
compression function inside

Quantitative summary:
"Assume that the best attac
against h as a PRF
is exhaustive key search. ...
The bound justifies NMAC
up to roughly $2^{c/2}/m$ queri

HMAC: similar story, with
key-derivation complications

2005 Bellare–Rogaway:

"For example we might conjecture something like [DES insecurity]

$$\leq c_1 \cdot \frac{t/T_{\mathsf{DES}}}{2^{55}} + c_2 \cdot \frac{q}{2^{40}}$$

... In other words,
we are conjecturing that the best attacks are either exhaustive key search or linear cryptanalysis.
We might be bolder with regard to AES and conjecture something like [AES insecurity]

$$\leq c_1 \cdot \frac{t/T_{\mathsf{AES}}}{2^{128}} + c_2 \cdot \frac{q}{2^{128}}."$$

2006 Bellare NMAC theorem:
(q, t) insecurity of NMAC-H
$\leq$ particular function of
(q', t') insecurity of the
compression function inside H.

Quantitative summary:
"Assume that the best attack against h as a PRF
is exhaustive key search. ...
The bound justifies NMAC
up to roughly $2^{c/2}/m$ queries."

HMAC: similar story, with
key-derivation complications.

llare–Rogaway:

mple we might conjecture
ng like [DES insecurity]
$/T_{\mathsf{DES}}$
$\frac{}{2^{55}} + c_2 \cdot \frac{q}{2^{40}}$
ther words,
onjecturing that the best
are either exhaustive key
r linear cryptanalysis.
nt be bolder with regard
and conjecture something
S insecurity]
$/T_{\mathsf{AES}}$
$\frac{}{2^{128}} + c_2 \cdot \frac{q}{2^{128}}$."

2006 Bellare NMAC theorem:
(q, t) insecurity of NMAC-H
$\leq$ particular function of
(q', t') insecurity of the
compression function inside H.

Quantitative summary:
"Assume that the best attack
against h as a PRF
is exhaustive key search. ...
The bound justifies NMAC
up to roughly $2^{c/2}/m$ queries."

HMAC: similar story, with
key-derivation complications.

Problem
over *all*
not just

Can spe
precomp
t counts
not prec

away:

might conjecture
ES insecurity]

$$\cdot \frac{q}{2^{40}}$$

,

g that the best
exhaustive key
yptanalysis.
er with regard
cture something
y]

$$\cdot \frac{q}{2^{128}} \cdot$$

"

2006 Bellare NMAC theorem:
(q, t) insecurity of NMAC-H
$\leq$ particular function of
(q', t') insecurity of the
compression function inside H.

Quantitative summary:
"Assume that the best attack
against h as a PRF
is exhaustive key search. . . .
The bound justifies NMAC
up to roughly $2^{c/2}/m$ queries."

HMAC: similar story, with
key-derivation complications.

Problem: The met
over *all* time-t alg
not just the algorit

Can spend a very
precomputing the
t counts algorithm
not precomputatio

ecture
ity]

e best
e key
s.
gard
ething

2006 Bellare NMAC theorem:
(q, t) insecurity of NMAC-H
$\leq$ particular function of
(q', t') insecurity of the
compression function inside H.

Quantitative summary:
"Assume that the best attack
against h as a PRF
is exhaustive key search. ...
The bound justifies NMAC
up to roughly $2^{c/2}/m$ queries."

HMAC: similar story, with
key-derivation complications.

Problem: The metric maxim
over *all* time-t algorithms,
not just the algorithms we k

Can spend a very long time
precomputing the algorithm.
t counts algorithm run time,
not precomputation time.

2006 Bellare NMAC theorem:
(q, t) insecurity of NMAC-H
$\leq$ particular function of
(q', t') insecurity of the
compression function inside H.

Quantitative summary:
"Assume that the best attack
against h as a PRF
is exhaustive key search. ...
The bound justifies NMAC
up to roughly $2^{c/2}/m$ queries."

HMAC: similar story, with
key-derivation complications.

Problem: The metric maximizes
over *all* time-t algorithms,
not just the algorithms we know.

Can spend a very long time
precomputing the algorithm.
t counts algorithm run time,
not precomputation time.

2006 Bellare NMAC theorem:
(q, t) insecurity of NMAC-H
$\leq$ particular function of
(q', t') insecurity of the
compression function inside H.

Quantitative summary:
"Assume that the best attack
against h as a PRF
is exhaustive key search. ...
The bound justifies NMAC
up to roughly $2^{c/2}/m$ queries."

HMAC: similar story, with
key-derivation complications.

Problem: The metric maximizes
over *all* time-t algorithms,
not just the algorithms we know.

Can spend a very long time
precomputing the algorithm.
t counts algorithm run time,
not precomputation time.

e.g. There *exists* an algorithm
finding AES key in time $\approx 2^{85}$
given a few known plaintexts.

e.g. There exists a *fast* algorithm
breaking AES, chance $\approx 2^{-64}$.

llare NMAC theorem:
security of NMAC-H
ular function of
nsecurity of the
sion function inside H.

ative summary:
e that the best attack
h as a PRF
stive key search. . . .
nd justifies NMAC
ughly $2^{c/2}/m$ queries."

similar story, with
vation complications.

Problem: The metric maximizes
over *all* time-t algorithms,
not just the algorithms we know.

Can spend a very long time
precomputing the algorithm.
t counts algorithm run time,
not precomputation time.

e.g. There *exists* an algorithm
finding AES key in time $\approx 2^{85}$
given a few known plaintexts.

e.g. There exists a *fast* algorithm
breaking AES, chance $\approx 2^{-64}$.

Inescapa

The Bell
conjectu

AC theorem:
NMAC-H
ion of
of the
ion inside H.

mary:
best attack
F
search. ...
es NMAC
$/m$ queries."

ory, with
nplications.

Problem: The metric maximizes
over *all* time-t algorithms,
not just the algorithms we know.

Can spend a very long time
precomputing the algorithm.
t counts algorithm run time,
not precomputation time.

e.g. There *exists* an algorithm
finding AES key in time $\approx 2^{85}$
given a few known plaintexts.

e.g. There exists a *fast* algorithm
breaking AES, chance $\approx 2^{-64}$.

Inescapable conclu

The Bellare–Roga
conjectures are fal

n:

H.

ck

es."

.

Problem: The metric maximizes
over *all* time-t algorithms,
not just the algorithms we know.

Can spend a very long time
precomputing the algorithm.
t counts algorithm run time,
not precomputation time.

e.g. There *exists* an algorithm
finding AES key in time $\approx 2^{85}$
given a few known plaintexts.

e.g. There exists a *fast* algorithm
breaking AES, chance $\approx 2^{-64}$.

Inescapable conclusions:

The Bellare–Rogaway
conjectures are false.

Problem: The metric maximizes
over *all* time-t algorithms,
not just the algorithms we know.

Can spend a very long time
precomputing the algorithm.
t counts algorithm run time,
not precomputation time.

e.g. There *exists* an algorithm
finding AES key in time $\approx 2^{85}$
given a few known plaintexts.

e.g. There exists a *fast* algorithm
breaking AES, chance $\approx 2^{-64}$.

Inescapable conclusions:

The Bellare–Rogaway
conjectures are false.

Problem: The metric maximizes
over *all* time-t algorithms,
not just the algorithms we know.

Can spend a very long time
precomputing the algorithm.
t counts algorithm run time,
not precomputation time.

e.g. There *exists* an algorithm
finding AES key in time $\approx 2^{85}$
given a few known plaintexts.

e.g. There exists a *fast* algorithm
breaking AES, chance $\approx 2^{-64}$.

Inescapable conclusions:

The Bellare–Rogaway
conjectures are false.

The Bellare assumption is false.

Problem: The metric maximizes
over *all* time-t algorithms,
not just the algorithms we know.

Can spend a very long time
precomputing the algorithm.
t counts algorithm run time,
not precomputation time.

e.g. There *exists* an algorithm
finding AES key in time $\approx 2^{85}$
given a few known plaintexts.

e.g. There exists a *fast* algorithm
breaking AES, chance $\approx 2^{-64}$.

Inescapable conclusions:

The Bellare–Rogaway
conjectures are false.

The Bellare assumption is false.

Koblitz–Menezes analysis:
2006 Bellare proof says nothing
if you use HMAC-SHA-1 for
2^{30} medium-length messages;
Bellare claim was 2^{60}.

Problem: The metric maximizes
over *all* time-t algorithms,
not just the algorithms we know.

Can spend a very long time
precomputing the algorithm.
t counts algorithm run time,
not precomputation time.

e.g. There *exists* an algorithm
finding AES key in time $\approx 2^{85}$
given a few known plaintexts.

e.g. There exists a *fast* algorithm
breaking AES, chance $\approx 2^{-64}$.

Inescapable conclusions:

The Bellare–Rogaway
conjectures are false.

The Bellare assumption is false.

Koblitz–Menezes analysis:
2006 Bellare proof says nothing
if you use HMAC-SHA-1 for
2^{30} medium-length messages;
Bellare claim was 2^{60}.

The classic metric is busted:
massively inaccurate measure
of actual cryptanalysis.

: The metric maximizes
time-t algorithms,
the algorithms we know.

nd a very long time
puting the algorithm.
algorithm run time,
omputation time.

re *exists* an algorithm
AES key in time $\approx 2^{85}$
few known plaintexts.

re exists a *fast* algorithm
AES, chance $\approx 2^{-64}$.

Inescapable conclusions:

The Bellare–Rogaway
conjectures are false.

The Bellare assumption is false.

Koblitz–Menezes analysis:
2006 Bellare proof says nothing
if you use HMAC-SHA-1 for
2^{30} medium-length messages;
Bellare claim was 2^{60}.

The classic metric is busted:
massively inaccurate measure
of actual cryptanalysis.

Fix metr
algorithm
Kills nor
including
and muc

Fix metr
"time" t
Kills ma
(e.g., re
becomes
and still

Fix metr
circuit A
but kills

tric maximizes
orithms,
thms we know.

long time
algorithm.
run time,
on time.

an algorithm
n time $\approx 2^{85}$
n plaintexts.

fast algorithm
nce $\approx 2^{-64}$.

Inescapable conclusions:

The Bellare–Rogaway conjectures are false.

The Bellare assumption is false.

Koblitz–Menezes analysis: 2006 Bellare proof says nothing if you use HMAC-SHA-1 for 2^{30} medium-length messages; Bellare claim was 2^{60}.

The classic metric is busted: massively inaccurate measure of actual cryptanalysis.

Fix metric by focu
algorithms we kno
Kills non-construct
including 2006 Be
and much more of

Fix metric by swit
"time" to number
Kills many proofs
(e.g., repeated-que
becomes much mo
and still breaks all

Fix metric by swit
circuit AT? Might
but kills most proo

nizes

know.

m
85
s.

rithm
64
.

Inescapable conclusions:

The Bellare–Rogaway conjectures are false.

The Bellare assumption is false.

Koblitz–Menezes analysis: 2006 Bellare proof says nothing if you use HMAC-SHA-1 for 2^{30} medium-length messages; Bellare claim was 2^{60}.

The classic metric is busted: massively inaccurate measure of actual cryptanalysis.

Fix metric by focusing on algorithms we know? Kills non-constructive proofs including 2006 Bellare proof and much more of literature

Fix metric by switching from "time" to number of NAND Kills many proofs in literatu (e.g., repeated-query elimina becomes much more expens and still breaks all ciphers.

Fix metric by switching to circuit AT? Might save ciph but kills most proofs in litera

Inescapable conclusions:

The Bellare–Rogaway conjectures are false.

The Bellare assumption is false.

Koblitz–Menezes analysis: 2006 Bellare proof says nothing if you use HMAC-SHA-1 for 2^{30} medium-length messages; Bellare claim was 2^{60}.

The classic metric is busted: massively inaccurate measure of actual cryptanalysis.

Fix metric by focusing on algorithms we know? Kills non-constructive proofs, including 2006 Bellare proof and much more of literature.

Fix metric by switching from "time" to number of NANDs? Kills many proofs in literature (e.g., repeated-query elimination becomes much more expensive), and still breaks all ciphers.

Fix metric by switching to circuit AT? Might save ciphers, but kills most proofs in literature.