Stronger security bounds for Wegman-Carter-Shoup authenticators

D. J. Bernstein

Thanks to:
University of Illinois at Chicago
NSF CCR–9983950
Alfred P. Sloan Foundation

Standard polynomial-evaluation MAC: sender sends
$(1, m_1, m_1(r) + s_1)$;
$(2, m_2, m_2(r) + s_2)$;
$(3, m_3, m_3(r) + s_3)$.

m_1, m_2, m_3: polynomials over F; univariate; degree $\le 2^{16}$; constant coefficient 0.

r, s_1, s_2, s_3: elements of F; secret; known to sender, receiver.

F: field of size 2^{128}.

bounds

er-Shoup

is at Chicago

0

oundation

Standard polynomial-evaluation MAC: sender sends

$(1, m_1, m_1(r) + s_1)$;

$(2, m_2, m_2(r) + s_2)$;

$(3, m_3, m_3(r) + s_3)$.

m_1, m_2, m_3: polynomials over F; univariate; degree $\le 2^{16}$; constant coefficient 0.

r, s_1, s_2, s_3: elements of F; secret; known to sender, receiver.

F: field of size 2^{128}.

Wegman-Carter ve

(r, s_1, s_2, s_3) is a u

random element o

2^{512} possibilities,

each equally likely.

Wegman-Carter-Sh

$s_1 \ne s_2$; $s_1 \ne s_3$;

otherwise uniform.

$2^{256}(2^{128} - 1)(2^{12}$

possibilities, each

How secure are th

Standard polynomial-evaluation MAC: sender sends

$(1, m_1, m_1(r) + s_1)$;
$(2, m_2, m_2(r) + s_2)$;
$(3, m_3, m_3(r) + s_3)$.

m_1, m_2, m_3: polynomials over F; univariate; degree $\leq 2^{16}$; constant coefficient 0.

r, s_1, s_2, s_3: elements of F; secret; known to sender, receiver.

F: field of size 2^{128}.

Wegman-Carter version: (r, s_1, s_2, s_3) is a uniform random element of F^4. 2^{512} possibilities, each equally likely.

Wegman-Carter-Shoup version: $s_1 \neq s_2$; $s_1 \neq s_3$; $s_2 \neq s_3$; otherwise uniform. $2^{256}(2^{128} - 1)(2^{128} - 2)$ possibilities, each equally likely.

How secure are these MACs?

ial-evaluation
s
$_1$);
$_2$);
$_3$).

nomials over F;
$\le 2^{16}$;
nt 0.

ents of F;
ender, receiver.

^{28}.

Wegman-Carter version:
(r, s_1, s_2, s_3) is a uniform random element of F^4.
2^{512} possibilities, each equally likely.

Wegman-Carter-Shoup version:
$s_1 \ne s_2$; $s_1 \ne s_3$; $s_2 \ne s_3$; otherwise uniform.
$2^{256}(2^{128} - 1)(2^{128} - 2)$ possibilities, each equally likely.

How secure are these MACs?

Standard security
for Wegman-Carte

"Authenticators re
no information abo

Conditional distrib
given $(1, m_1, a_1)$,
$(3, m_3, a_3)$, is unif

There are 2^{128} pos
each consistent wi
unique choice of s
$s_2 = a_2 - m_2(r)$,

Wegman-Carter version:
(r, s_1, s_2, s_3) is a uniform random element of F^4.
2^{512} possibilities, each equally likely.

Wegman-Carter-Shoup version:
$s_1 \neq s_2$; $s_1 \neq s_3$; $s_2 \neq s_3$; otherwise uniform.
$2^{256}(2^{128} - 1)(2^{128} - 2)$ possibilities, each equally likely.

How secure are these MACs?

Standard security bounds for Wegman-Carter:

"Authenticators reveal no information about r."

Conditional distribution of r, given $(1, m_1, a_1)$, $(2, m_2, a_2)$, $(3, m_3, a_3)$, is uniform.

There are 2^{128} possible r's, each consistent with a unique choice of $s_1 = a_1 - m_1(r)$, $s_2 = a_2 - m_2(r)$, $s_3 = a_3 - m_3(r)$.

ersion:

uniform

f F^4.

houp version:

$s_2 \neq s_3$;

$^{28} - 2)$

equally likely.

ese MACs?

Standard security bounds for Wegman-Carter:

"Authenticators reveal no information about r."

Conditional distribution of r, given $(1, m_1, a_1)$, $(2, m_2, a_2)$, $(3, m_3, a_3)$, is uniform.

There are 2^{128} possible r's, each consistent with a unique choice of $s_1 = a_1 - m_1(r)$, $s_2 = a_2 - m_2(r)$, $s_3 = a_3 - m_3(r)$.

Say attacker attem

$(1, m, a)$ with $m \neq$

$m(0) = 0$; degree

Forgery is successf

$a = m(r) + s_1 \Leftarrow$

$a = m(r) + a_1 -$

r is a root of $m -$

$m - m_1 + a_1 - a$

polynomial of degr

so it has $\leq 2^{16}$ roo

Attempted forgery

$\leq 2^{16}/2^{128}$ chance

Standard security bounds for Wegman-Carter:

"Authenticators reveal no information about r."

Conditional distribution of r, given $(1, m_1, a_1)$, $(2, m_2, a_2)$, $(3, m_3, a_3)$, is uniform.

There are 2^{128} possible r's, each consistent with a unique choice of $s_1 = a_1 - m_1(r)$, $s_2 = a_2 - m_2(r)$, $s_3 = a_3 - m_3(r)$.

Say attacker attempts forgery $(1, m, a)$ with $m \neq m_1$; $m(0) = 0$; degree $\leq 2^{16}$.

Forgery is successful $\iff$
$a = m(r) + s_1 \iff$
$a = m(r) + a_1 - m_1(r) \iff$
r is a root of $m - m_1 + a_1 - a$.

$m - m_1 + a_1 - a$ is a nonzero polynomial of degree $\leq 2^{16}$ so it has $\leq 2^{16}$ roots.

Attempted forgery has $\leq 2^{16}/2^{128}$ chance of success.

bounds

er:

eveal

out r."

ution of r,

$(2, m_2, a_2)$,

form.

ssible r's,

th a

$_1 = a_1 - m_1(r)$,

$s_3 = a_3 - m_3(r)$.

Say attacker attempts forgery $(1, m, a)$ with $m \neq m_1$; $m(0) = 0$; degree $\le 2^{16}$.

Forgery is successful $\iff$ $a = m(r) + s_1 \iff$ $a = m(r) + a_1 - m_1(r) \iff$ r is a root of $m - m_1 + a_1 - a$.

$m - m_1 + a_1 - a$ is a nonzero polynomial of degree $\le 2^{16}$ so it has $\le 2^{16}$ roots.

Attempted forgery has $\le 2^{16}/2^{128}$ chance of success.

Original security b

for Wegman-Carte

"Authenticators re

very little informat

(1996 Shoup)

Stronger security b

for Wegman-Carte

"Wegman-Carter-S

identical to Wegm

(bounds, 2004.10

this proof, 2005.03

Warning: carelessn

weaker ("game-pla

Say attacker attempts forgery $(1, m, a)$ with $m \neq m_1$; $m(0) = 0$; degree $\leq 2^{16}$.

Forgery is successful $\iff$
$a = m(r) + s_1 \iff$
$a = m(r) + a_1 - m_1(r) \iff$
r is a root of $m - m_1 + a_1 - a$.

$m - m_1 + a_1 - a$ is a nonzero polynomial of degree $\leq 2^{16}$ so it has $\leq 2^{16}$ roots.

Attempted forgery has $\leq 2^{16}/2^{128}$ chance of success.

Original security bounds for Wegman-Carter-Shoup: "Authenticators reveal very little information about r." (1996 Shoup)

Stronger security bounds for Wegman-Carter-Shoup: "Wegman-Carter-Shoup is almost identical to Wegman-Carter." (bounds, 2004.10 Bernstein; this proof, 2005.03 Bernstein)

Warning: carelessness leads to weaker ("game-playing") bounds.

npts forgery

$\neq m_1$;

$\leq 2^{16}$.

ful $\iff$

$\Rightarrow$

$m_1(r) \iff$

$+ m_1 + a_1 - a$.

is a nonzero

ree $\leq 2^{16}$

ots.

has

e of success.

Original security bounds
for Wegman-Carter-Shoup:
"Authenticators reveal
very little information about r."
(1996 Shoup)

Stronger security bounds
for Wegman-Carter-Shoup:
"Wegman-Carter-Shoup is almost
identical to Wegman-Carter."
(bounds, 2004.10 Bernstein;
this proof, 2005.03 Bernstein)

Warning: carelessness leads to
weaker ("game-playing") bounds.

Fix a deterministic

generates m_1; sees

generates m_2; sees

generates m_3; sees

generates forgery a

(n, m, a) with $n \in$

$m \neq m_n$, $m(0) =$

(Generalizations: n

variable # of chos

arbitrary order of n

variable # of forge

Original security bounds for Wegman-Carter-Shoup: "Authenticators reveal very little information about r." (1996 Shoup)

Stronger security bounds for Wegman-Carter-Shoup: "Wegman-Carter-Shoup is almost identical to Wegman-Carter." (bounds, 2004.10 Bernstein; this proof, 2005.03 Bernstein)

Warning: carelessness leads to weaker ("game-playing") bounds.

Fix a deterministic attack A that generates m_1; sees $m_1(r) + s_1$; generates m_2; sees $m_2(r) + s_2$; generates m_3; sees $m_3(r) + s_3$; generates forgery attempt (n, m, a) with $n \in \{1, 2, 3\}$, $m \neq m_n$, $m(0) = 0$, deg $\leq 2^{16}$.

(Generalizations: randomized A; variable # of chosen messages; arbitrary order of nonces; variable # of forgery attempts.)

ounds
er-Shoup:
eveal
tion about r."

bounds
er-Shoup:
Shoup is almost
an-Carter."
Bernstein;
3 Bernstein)

ness leads to
aying") bounds.

Fix a deterministic attack A that generates m_1; sees $m_1(r) + s_1$; generates m_2; sees $m_2(r) + s_2$; generates m_3; sees $m_3(r) + s_3$; generates forgery attempt (n, m, a) with $n \in \{1, 2, 3\}$, $m \neq m_n$, $m(0) = 0$, deg $\leq 2^{16}$.

(Generalizations: randomized A; variable # of chosen messages; arbitrary order of nonces; variable # of forgery attempts.)

Apply A to Wegm

Pr$[a = m(r) + s_n$
Proved this earlier

For each $S \in F^3$:
conditional probab
that $a = m(r) + s$
given that $(s_1, s_2,$

Pr$[a = m(r) + s_n$
$= \sum_S$ Pr$[(s_1, s_2, s$
$= \sum_S 2^{-384} p(S)$.

Thus $\sum_S 2^{-384} p($

Fix a deterministic attack A that generates m_1; sees $m_1(r) + s_1$; generates m_2; sees $m_2(r) + s_2$; generates m_3; sees $m_3(r) + s_3$; generates forgery attempt (n, m, a) with $n \in \{1, 2, 3\}$, $m \neq m_n$, $m(0) = 0$, deg $\leq 2^{16}$.

(Generalizations: randomized A; variable # of chosen messages; arbitrary order of nonces; variable # of forgery attempts.)

Apply A to Wegman-Carter.

$\Pr[a = m(r) + s_n] \leq 1/2^{112}$. Proved this earlier.

For each $S \in F^3$: Define $p(S)$ as conditional probability that $a = m(r) + s_n$ given that $(s_1, s_2, s_3) = S$.

$\Pr[a = m(r) + s_n]$
$= \sum_S \Pr[(s_1, s_2, s_3) = S] p(S)$
$= \sum_S 2^{-384} p(S)$.

Thus $\sum_S 2^{-384} p(S) \leq 1/2^{112}$.

: attack A that
s $m_1(r) + s_1$;
s $m_2(r) + s_2$;
s $m_3(r) + s_3$;
attempt
$\in \{1, 2, 3\}$,
0, deg $\leq 2^{16}$.

randomized A;
sen messages;
nonces;
ery attempts.)

Apply A to Wegman-Carter.

$\Pr[a = m(r) + s_n] \leq 1/2^{112}$.
Proved this earlier.

For each $S \in F^3$: Define $p(S)$ as
conditional probability
that $a = m(r) + s_n$
given that $(s_1, s_2, s_3) = S$.

$\Pr[a = m(r) + s_n]$
$= \sum_S \Pr[(s_1, s_2, s_3) = S] p(S)$
$= \sum_S 2^{-384} p(S)$.

Thus $\sum_S 2^{-384} p(S) \leq 1/2^{112}$.

Apply A to Wegm

$\Pr[(s_1, s_2, s_3) = S$
$\delta = 2^{384}/2^{128}(2^{12}$

For $S \in F^3$: Cond
that $a = m(r) + s$
$(s_1, s_2, s_3) = S$, is
so $\Pr[a = m(r) +$
$\leq \sum_S 2^{-384} \delta p(S)$
This is the stronge

Could take careles
use $\Pr \leq 1$ to get
$\Pr \leq 1/2^{112} + 3/2$

Apply A to Wegman-Carter.

$\Pr[a = m(r) + s_n] \le 1/2^{112}$.
Proved this earlier.

For each $S \in F^3$: Define $p(S)$ as conditional probability that $a = m(r) + s_n$ given that $(s_1, s_2, s_3) = S$.

$\Pr[a = m(r) + s_n]$
$= \sum_S \Pr[(s_1, s_2, s_3) = S] p(S)$
$= \sum_S 2^{-384} p(S)$.

Thus $\sum_S 2^{-384} p(S) \le 1/2^{112}$.

Apply A to Wegman-Carter-Shoup.

$\Pr[(s_1, s_2, s_3) = S] \le 2^{-384}\delta$ where $\delta = 2^{384}/2^{128}(2^{128} - 1)(2^{128} - 2)$.

For $S \in F^3$: Conditional probability that $a = m(r) + s_n$, given that $(s_1, s_2, s_3) = S$, is the same $p(S)$, so $\Pr[a = m(r) + s_n]$
$\le \sum_S 2^{-384}\delta p(S) \le \delta/2^{112}$.
This is the stronger security bound.

Could take careless extra step: use $\Pr \le 1$ to get weaker bound $\Pr \le 1/2^{112} + 3/2^{128}$.

an-Carter.

$] \leq 1/2^{112}$.

.

Define $p(S)$ as

ility

s_n

$s_3) = S$.

]

$s_3) = S]p(S)$

$S) \leq 1/2^{112}$.

Apply A to Wegman-Carter-Shoup.

$\Pr[(s_1, s_2, s_3) = S] \leq 2^{-384}\delta$ where $\delta = 2^{384}/2^{128}(2^{128} - 1)(2^{128} - 2)$.

For $S \in F^3$: Conditional probability that $a = m(r) + s_n$, given that $(s_1, s_2, s_3) = S$, is the same $p(S)$, so $\Pr[a = m(r) + s_n]$ $\leq \sum_S 2^{-384}\delta p(S) \leq \delta/2^{112}$. This is the stronger security bound.

Could take careless extra step: use $\Pr \leq 1$ to get weaker bound $\Pr \leq 1/2^{112} + 3/2^{128}$.

Wegman-Carter-Sh

after 2^{40} chosen m

and D forgery atte

Stronger: $\leq\approx D/($

Careless: $\leq\approx (D/$

Original: $\leq\approx D/($

2^{60} instead of 2^{40}:

Stronger: $\leq\approx D/($

Careless: $\leq\approx (D/$

Original: $\leq\approx \infty$.

Apply A to Wegman-Carter-Shoup.

$\Pr[(s_1, s_2, s_3) = S] \le 2^{-384}\delta$ where $\delta = 2^{384}/2^{128}(2^{128}-1)(2^{128}-2)$.

For $S \in F^3$: Conditional probability that $a = m(r) + s_n$, given that $(s_1, s_2, s_3) = S$, is the same $p(S)$, so $\Pr[a = m(r) + s_n]$ $\le \sum_S 2^{-384}\delta p(S) \le \delta/2^{112}$. This is the stronger security bound.

Could take careless extra step: use $\Pr \le 1$ to get weaker bound $\Pr \le 1/2^{112} + 3/2^{128}$.

Wegman-Carter-Shoup bounds after 2^{40} chosen messages and D forgery attempts:
Stronger: $\le\approx D/(2^{112} - 2^{63})$.
Careless: $\le\approx (D/2^{112}) + (1/2^{49})$.
Original: $\le\approx D/(2^{112} - 2^{79})$.

2^{60} instead of 2^{40}:
Stronger: $\le\approx D/(2^{112} - 2^{103})$.
Careless: $\le\approx (D/2^{112}) + (1/2^{9})$.
Original: $\le\approx \infty$.

an-Carter-Shoup.

$] \le 2^{-384}\delta$ where
$^{8} - 1)(2^{128} - 2)$.

litional probability
s_n, given that
s the same $p(S)$,
$s_n]$
$) \le \delta/2^{112}$.
er security bound.

s extra step:
weaker bound
2^{128}.

Wegman-Carter-Shoup bounds after 2^{40} chosen messages and D forgery attempts:
Stronger: $\lessapprox D/(2^{112} - 2^{63})$.
Careless: $\lessapprox (D/2^{112}) + (1/2^{49})$.
Original: $\lessapprox D/(2^{112} - 2^{79})$.

2^{60} instead of 2^{40}:
Stronger: $\lessapprox D/(2^{112} - 2^{103})$.
Careless: $\lessapprox (D/2^{112}) + (1/2^{9})$.
Original: $\lessapprox \infty$.

Generalize $m_i(r)$ -
$h(m_i) + s_i$ where
small differential p
$\Pr[h(m) - h(m')$

Original bound $\approx$
for C as large as $\sqrt{}$
where C is # chos
Proof strategy is c
for larger C.

Stronger bound $\approx$
for C as large as $\sqrt{}$

Careless bound $\approx$

Wegman-Carter-Shoup bounds after 2^{40} chosen messages and D forgery attempts:
Stronger: $\le\approx D/(2^{112}-2^{63})$.
Careless: $\le\approx (D/2^{112})+(1/2^{49})$.
Original: $\le\approx D/(2^{112}-2^{79})$.

2^{60} instead of 2^{40}:
Stronger: $\le\approx D/(2^{112}-2^{103})$.
Careless: $\le\approx (D/2^{112})+(1/2^{9})$.
Original: $\le\approx \infty$.

Generalize $m_i(r)+s_i$ to any $h(m_i)+s_i$ where h has small differential probabilities: $\Pr[h(m)-h(m')=g]\le\epsilon$.

Original bound $\approx D\epsilon$ for C as large as $\sqrt{1/\epsilon}$, where C is # chosen messages. Proof strategy is doomed for larger C.

Stronger bound $\approx D\epsilon$ for C as large as $\sqrt{2^{128}}$.

Careless bound $\approx D\epsilon + C^2/2^{129}$.

houp bounds
messages
empts:
$(2^{112} - 2^{63})$.
$/2^{112}) + (1/2^{49})$.
$(2^{112} - 2^{79})$.

:
$(2^{112} - 2^{103})$.
$/2^{112}) + (1/2^{9})$.

Generalize $m_i(r) + s_i$ to any $h(m_i) + s_i$ where h has small differential probabilities: $\Pr[h(m) - h(m') = g] \le \epsilon$.

Original bound $\approx D\epsilon$ for C as large as $\sqrt{1/\epsilon}$, where C is # chosen messages. Proof strategy is doomed for larger C.

Stronger bound $\approx D\epsilon$ for C as large as $\sqrt{2^{128}}$.

Careless bound $\approx D\epsilon + C^2/2^{129}$.

Wegman-Carter-Sl
implies $h(m_i) +$ A
if AES is secure.

Explicit AES secur
$\text{AES}_k(1), \text{AES}_k(2)$
indistinguishable fr

Not true for Wegr
i.e., **not** true with
conditions $s_1 \ne s_2$
Wegman-Carter s_1
often collide for la

Generalize $m_i(r) + s_i$ to any $h(m_i) + s_i$ where h has small differential probabilities: $\Pr[h(m) - h(m') = g] \le \epsilon$.

Original bound $\approx D\epsilon$ for C as large as $\sqrt{1/\epsilon}$, where C is # chosen messages. Proof strategy is doomed for larger C.

Stronger bound $\approx D\epsilon$ for C as large as $\sqrt{2^{128}}$.

Careless bound $\approx D\epsilon + C^2/2^{129}$.

Wegman-Carter-Shoup security implies $h(m_i) + \mathrm{AES}_k(i)$ security if AES is secure.

Explicit AES security goal: $\mathrm{AES}_k(1), \mathrm{AES}_k(2), \ldots$ indistinguishable from $s_1, s_2, \ldots$.

Not true for Wegman-Carter: i.e., **not** true without conditions $s_1 \ne s_2$ etc. Wegman-Carter $s_1, s_2, \ldots, s_C$ often collide for large C.

$+ s_i$ to any
h has
probabilities:
$= g] \le \epsilon$.

$D\epsilon$
$\sqrt{1/\epsilon}$,
sen messages.
doomed

$D\epsilon$
$\sqrt{2^{128}}$.

$D\epsilon + C^2/2^{129}$.

Wegman-Carter-Shoup security implies $h(m_i) + \text{AES}_k(i)$ security if AES is secure.

Explicit AES security goal: $\text{AES}_k(1), \text{AES}_k(2), \ldots$ indistinguishable from $s_1, s_2, \ldots$.

Not true for Wegman-Carter: i.e., **not** true without conditions $s_1 \ne s_2$ etc. Wegman-Carter $s_1, s_2, \ldots, s_C$ often collide for large C.

MAC speed leader
`http://cr.yp.to`

Poly1305-AES bou
is $\lceil L/16 \rceil / 2^{103}$
for L-byte message

e.g., $\epsilon \le 2^{-92}$ for

Security gap comp
$< 1.7D/2^{92}$ if $C \le$
With old security
C was limited to a

Wegman-Carter-Shoup security implies $h(m_i) + \mathrm{AES}_k(i)$ security if AES is secure.

Explicit AES security goal: $\mathrm{AES}_k(1), \mathrm{AES}_k(2), \ldots$ indistinguishable from $s_1, s_2, \ldots$.

Not true for Wegman-Carter: i.e., **not** true without conditions $s_1 \neq s_2$ etc. Wegman-Carter $s_1, s_2, \ldots, s_C$ often collide for large C.

MAC speed leader: Poly1305-AES, `http://cr.yp.to/mac.html`.

Poly1305-AES bound on ϵ is $\lceil L/16 \rceil / 2^{103}$ for L-byte messages.

e.g., $\epsilon \le 2^{-92}$ for $L = 2048$.

Security gap compared to AES $< 1.7D/2^{92}$ if $C \le 2^{64}$. With old security bound, C was limited to about 2^{46}.

houp security
AES$_k(i)$ security

rity goal:
, . . .
rom $s_1, s_2, \ldots$.

man-Carter:
out
 etc.
$_1, s_2, \ldots, s_C$
rge C.

MAC speed leader: Poly1305-AES,
`http://cr.yp.to/mac.html`.

Poly1305-AES bound on ϵ
is $\lceil L/16 \rceil / 2^{103}$
for L-byte messages.

e.g., $\epsilon \le 2^{-92}$ for $L = 2048$.

Security gap compared to AES
$< 1.7D/2^{92}$ if $C \le 2^{64}$.
With old security bound,
C was limited to about 2^{46}.

Improved security
apply far beyond t

"Stronger security
permutations": ht
/papers.html#pe

Stronger than "ga

Another applicatio
is provably stronge
/papers.html#co
coming soon.

MAC speed leader: Poly1305-AES, `http://cr.yp.to/mac.html`.

Poly1305-AES bound on ϵ is $\lceil L/16 \rceil / 2^{103}$ for L-byte messages.

e.g., $\epsilon \le 2^{-92}$ for $L = 2048$.

Security gap compared to AES $< 1.7D/2^{92}$ if $C \le 2^{64}$. With old security bound, C was limited to about 2^{46}.

Improved security bounds apply far beyond the MAC context.

"Stronger security bounds for permutations": `http://cr.yp.to/papers.html#permutations`

Stronger than "game-playing."

Another application: Counter mode is provably stronger than CBC. `/papers.html#countermode`, coming soon.

: Poly1305-AES,
o/mac.html.

und on ϵ

es.

$L = 2048$.

pared to AES
$\leq 2^{64}$.
bound,
about 2^{46}.

Improved security bounds
apply far beyond the MAC context.

"Stronger security bounds for
permutations": `http://cr.yp.to`
`/papers.html#permutations`

Stronger than "game-playing."

Another application: Counter mode
is provably stronger than CBC.
`/papers.html#countermode`,
coming soon.

AES security probl
16-byte block inve
Partly fixed in this
but still annoying.

AES security probl
secret-index table
"Not vulnerable to
was wrong. Very h
without extreme sl
`/papers.html#ca`

Many fast stream
don't have these p
Do we want to kee

Improved security bounds apply far beyond the MAC context.

"Stronger security bounds for permutations": `http://cr.yp.to/papers.html#permutations`

Stronger than "game-playing."

Another application: Counter mode is provably stronger than CBC. `/papers.html#countermode`, coming soon.

AES security problems from 16-byte block invertibility: Partly fixed in this talk, but still annoying.

AES security problems from secret-index table lookups: "Not vulnerable to timing attacks" was wrong. Very hard to fix without extreme slowdowns. `/papers.html#cachetiming`

Many fast stream ciphers don't have these problems. Do we want to keep AES?