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 \(\leq 2^{16}\); constant coefficient 0.

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

\(F\): field of size \(2^{128}\).
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 \cdot m_1, m_1(r) + s_1);
(2 \cdot m_2, m_2(r) + s_2);
(3 \cdot 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:
\( r \neq s_1; \ s_1 \neq s_3; \ r \neq s_2; \ s_2 \neq s_3; \)
otherwise uniform.
\( 2^{256}(2^{128} – 1)(2^{128} – 2) \) possibilities, each equally likely.

How secure are these MACs?
Standard 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?
Standard polynomial-evaluation MAC:

The sender sends

\[
(1 + 1) + 1; \\
(2 + 2) + 2; \\
(3 + 3).
\]

which are polynomials over \( F \);

with degree \( \leq 2^{16} \);

constant coefficient 0.

\( 1, 2, 3: \) 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?

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 \( s_1, s_2, s_3 \), each consistent with a unique choice of \( s_1, s_2, s_3 \).

\( s_2 = a_2 - m_2(r), \)
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
\(s_1 = a_1 - m_1(r), s_2 = a_2 - m_2(r), s_3 = a_3 - m_3(r)\).
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 $m = m(0) = 0$; degree $2^{16}$.

 Forgery is successful if $a = m(r) + s_1 \iff a = m(r) + a_1 - s_1 - m_1(r)$, so $r$ is a root of $m - m_1 + a_1 - a$. This is a nonzero polynomial of degree $2^{16}$, so it has $\leq 2^{16}$ roots.

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

\((1, m, a)\) with \(m \neq m_1\); 

\(m(0) = 0; \text{ degree } \leq 2^{16}\).

Forgery is successful \(\iff\)

\[a = m(r) + s_1 \iff a = m(r) + a_1 - m_1(r) \iff r \text{ is a root of } m - m_1 + a_1 - a.\]

\(m - m_1 + a_1 - a\) 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.
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.
Attempts forgery
\[ \neq m_1; \]
\[ \leq 2^{16}. \]
Successful \iff
\[ m_1(r) \iff \]
\[ m_1 + a_1 - a. \]
Is a nonzero
degree \leq 2^{16}
root.

Has

one 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 attack
that
generates \( m_1 \); sees
\[ m_1 + \frac{a_1 - a}{}, \]
generates \( m_2 \); sees
\[ m_2 + a_2 - a, \]
generates forgery attempt
\[ (n, m, a) \text{ with } n \neq \]
m \( \neq \) m_n, m(0) = \( \).

(Generalizations: randomized;
variable \# of chosen messages;
arbitrary order of nonces;
variable \# of forgery attempts.)
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 $n \in \{1, 2, 3\}$,
$m \neq m_n$, $m(0) = 0$, $\text{deg} \leq 2^{16}$.

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

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

Thus $\sum_S 2^{-384} p(S) = 2^{-384}$. 

Apply to Wegman-Carter.
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 $\sum_S 2^{-384}p(S) \leq 1/2^{112}$. 
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 Wegman-Carter-Shoup.

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

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 $\Pr[a = m(r) + s_n] \leq \sum_S 2^{-384}\delta p(S)$.

This is the stronger security bound.

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

Apply $A$ to Wegman-Carter-Shoup.

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

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
$$\Pr \leq 1/2^{112} + 3/2^{128}.$$
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-Shoup bounds after $2^{40}$ chosen messages and $D$ forgery attempts:

Stronger: $\leq \approx D/(2^{112} - 2^{63}).$
Careless: $\leq \approx (D/2^{112}) + (1/2^{49}).$
Original: $\leq \approx D/(2^{112} - 2^{79}).$

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

Stronger: $\leq \approx D/(2^{112} - 2^{103}).$
Careless: $\leq \approx (D/2^{112}) + (1/2^{9}).$
Original: $\leq \approx \infty.$
Wegman-Carter-Shoup bounds after $2^{40}$ chosen messages and $D$ forgery attempts:

Stronger: $\leq \approx D/(2^{112} - 2^{63})$.

Careless: $\leq \approx (D/2^{112}) + (1/2^{49})$.

Original: $\leq \approx D/(2^{112} - 2^{79})$.

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

Stronger: $\leq \approx D/(2^{112} - 2^{103})$.

Careless: $\leq \approx (D/2^{112}) + (1/2^9)$.

Original: $\leq \approx \infty$.

Generalize $m_i(r) = h(m_i) + s_i$ where $s_i$ is chosen randomly and have small differential probability.

Original bound $\approx C$ for $C$ as large as $\sqrt{\#}$ messages.

Proof strategy is doomed for larger $C$.

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

Careless bound $\approx C$ for $C$ as large as $\sqrt{\#}$ messages.
Wegman-Carter-Shoup bounds after $2^{40}$ chosen messages and $D$ forgery attempts:

**Stronger:** $\leq \approx D/(2^{112} - 2^{63})$.

**Careless:** $\leq \approx (D/2^{112}) + (1/2^{49})$.

**Original:** $\leq \approx D/(2^{112} - 2^{79})$.

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

**Stronger:** $\leq \approx D/(2^{112} - 2^{103})$.

**Careless:** $\leq \approx (D/2^{112}) + (1/2^{9})$.

**Original:** $\leq \approx \infty$.

---

Generalize $m_i(r) + s_i$ to any $h(m_i) + s_i$ where $h$ has small differential probabilities:

$$\Pr[h(m) - h(m') = g] \leq \epsilon.$$ 

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 bounds after 2^{40} chosen messages and forgery attempts:
- Stronger: \( \left( 2^{112} - 2^{63} \right) \).
- Careless: \( \left( 2^{112} \right) + \left( 1 / 2^{49} \right) \).
- Original: \( \left( 2^{112} - 2^{79} \right) \).

2^{60} instead of 2^{40}:
- Stronger: \( \left( 2^{112} - 2^{103} \right) \).
- Careless: \( \left( 2^{112} \right) + \left( 1 / 2^9 \right) \).
- Original: (as large as 1).

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

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 \( h(m_i) + AES(m_i) \) if AES is secure.
Explicit AES security goal:
\( \text{AES}_k(1), \text{AES}_k(2) \) indistinguishable from
\( \text{AES}_k(1), \text{AES}_k(2) \) not true for Wegman-Carter:
i.e., not true without conditions \( s_1 \neq s_2 \). Wegman-Carter \( s_1 = s_2 \) often collide for large.
Generalize $m_i(r) + s_i$ to any $h(m_i) + s_i$ where $h$ has small differential probabilities: $\Pr[h(m) - h(m') = g] \leq \epsilon$.

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 $h(m_i) + \text{AES}_k(i)$ 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 $s_1 \neq s_2$ etc.

Wegman-Carter $s_1, s_2, \ldots, s_C$ often collide for large $C$. 
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 \( s_1 \neq s_2 \) etc.

Security gap compared to AES \( 1 \leq 7 \leq 2^{92} \) if \( C \leq 64 \).

With old security bound, was limited to about \( 2^{46} \).


Poly1305-AES bound on \( C \geq 16 \) is \( \lceil L/16 \rceil / 2^{103} \) for \( L \)-byte messages.

e.g., \( \varepsilon \leq 2^{-92} \) for \( C = 2048 \).

\[ D \varepsilon + C^2 / 2^{129}. \]
Wegman-Carter-Shoup security implies $h(m_i) + AES_k(i)$ security if AES is secure.

Explicit AES security goal: $AES_k(1)$, $AES_k(2)$, ... indistinguishable from $s_1$, $s_2$, ...

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


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

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

Security gap compared to AES $< 1.7D/2^{92}$ if $C \leq 2^{64}$.

With old security bound, $C$ was limited to about $2^{46}$.
Wegman-Carter-Shoup security implies $\text{AES}_k(i)$ security if $\text{AES}$ is secure.

Explicit $\text{AES}$ security goal:

\[ \text{AES}(1) \] \[ \text{AES}(2) \] \[ \text{indistinguishable from} \] \[ 1 \] \[ 2 \] .

Not true for Wegman-Carter: i.e., not true without conditions $1 = 2$ etc.

Wegman-Carter $1$ $2$ often collide for large $L$.


Poly1305-AES bound on $\epsilon$ is $\frac{[L/16]}{2^{103}}$ for $L$-byte messages.

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

Security gap compared to $\text{AES}$ is $< 1.7D/2^{92}$ if $C \leq 2^{64}$.

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. http://cr.yp.to/papers.html#countermode, coming soon.
MAC speed leader: Poly1305-AES, 
http://cr.yp.to/mac.html.

Poly1305-AES bound on $\epsilon$ is $\lfloor L/16 \rfloor / 2^{103}$ for $L$-byte messages.

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

Security gap compared to AES is $< 1.7D/2^{92}$ if $C \leq 2^{64}$.
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.
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.
http://cr.yp.to/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.
http://cr.yp.to/papers.html#cachetiming

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