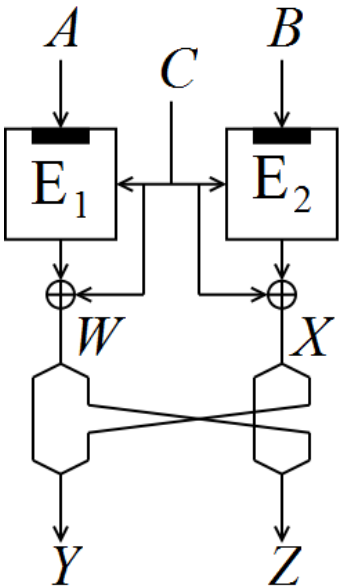
# On the Collision and Preimage Security of MDC-4 in the Ideal Cipher Model

Bart Mennink, KU Leuven

FSE 2012 Rump Session, Washington, DC

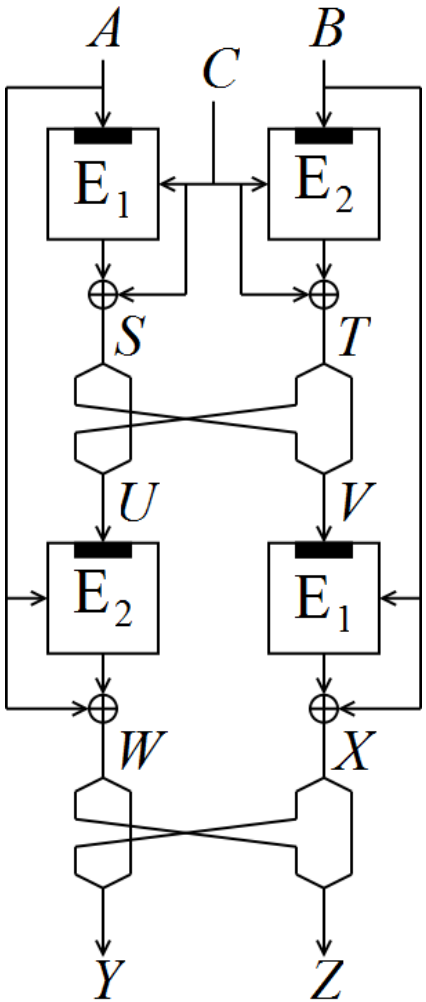
March 20, 2012

# MDC-4




$(E_1, E_2)$ vs. $E$

$f_{\text{MDC-2}}$ vs. $f_{\text{MDC-4}}$



# MDC-4 Based on Two Block Ciphers $E_1, E_2$

| | collision | | preimage | | ideal primitives |
|---|---|---|---|---|---|
| | security | attack | security | attack | |
| MDC-2 | $2^{3n/5}$ [Ste07] | $2^n/n$ [KMRT09] | $2^n$ | $2^n$ [KMRT09] | $(E_1, E_2)$ |
| MDC-4 | $2^{n/2}$ | $2^n$ | $2^n$ | $2^{7n/4}$ [KP97] | $(E_1, E_2)$ |

# MDC-4 Based on Two Block Ciphers $E_1, E_2$

| | collision | | preimage | | ideal primitives |
|---|---|---|---|---|---|
| | security | attack | security | attack | |
| MDC-2 | $2^{3n/5}$ [Ste07] | $2^n/n$ [KMRT09] | $2^n$ | $2^n$ [KMRT09] | $(E_1, E_2)$ |
| MDC-4 | $2^{5n/8}$ | $2^n$ | $2^n$ | $2^{7n/4}$ [KP97] | $(E_1, E_2)$ |

## Collision Resistance

- We achieve a (better) $2^{5n/8}$ security bound
- Steinberger's proof inapplicable, proof from scratch

independent analysis by Fleischmann et al.: $2^{3n/5}$ bound

# MDC-4 Based on Two Block Ciphers $E_1, E_2$

| | collision | | preimage | | ideal primitives |
|---|---|---|---|---|---|
| | security | attack | security | attack | |
| MDC-2 | $2^{3n/5}$ [Ste07] | $2^n/n$ [KMRT09] | $2^n$ | $2^n$ [KMRT09] | $(E_1, E_2)$ |
| MDC-4 | $2^{5n/8}$ | $2^n$ | $2^{5n/4}$ | $2^{7n/4}$ [KP97] | $(E_1, E_2)$ |

## Collision Resistance

- We achieve a (better) $2^{5n/8}$ security bound
- Steinberger's proof inapplicable, proof from scratch

independent analysis by Fleischmann et al.: $2^{3n/5}$ bound

## Preimage Resistance

- $2^{5n/4}$ security bound (beyond birthday bound!)

# MDC-4 Based on One Block Cipher $E$

| | collision | | preimage | | ideal primitives |
|---|---|---|---|---|---|
| | security | attack | security | attack | |
| MDC-2 | $2^{3n/5}$ [Ste07] | $2^n/n$ [KMRT09] | $2^n$ | $2^n$ [KMRT09] | $E$ or $(E_1, E_2)$ |
| MDC-4 | $2^{5n/8}$ | $2^n$ | $2^{5n/4}$ | $2^{7n/4}$ [KP97] | $(E_1, E_2)$ |
| MDC-4 | $2^{n/2}$ | $2^n$ | $2^n$ | $2^{7n/4}$ [KP97] | $E$ |

# MDC-4 Based on One Block Cipher $E$

| | collision | | preimage | | ideal primitives |
|---|---|---|---|---|---|
| | security | attack | security | attack | |
| MDC-2 | $2^{3n/5}$ [Ste07] | $2^n/n$ [KMRT09] | $2^n$ | $2^n$ [KMRT09] | $E$ or $(E_1, E_2)$ |
| MDC-4 | $2^{5n/8}$ | $2^n$ | $2^{5n/4}$ | $2^{7n/4}$ [KP97] | $(E_1, E_2)$ |
| MDC-4 | $2^{5n/8}$ | $2^n$ | $2^n$ | $2^{7n/4}$ [KP97] | $E$ |

## Collision Resistance

- $2^{5n/8}$ security bound still applies

  independent analysis by Fleischmann et al.: $2^{3n/5}$ bound

# MDC-4 Based on One Block Cipher $E$

| | collision | | preimage | | ideal primitives |
|---|---|---|---|---|---|
| | security | attack | security | attack | |
| MDC-2 | $2^{3n/5}$ [Ste07] | $2^n/n$ [KMRT09] | $2^n$ | $2^n$ [KMRT09] | $E$ or $(E_1, E_2)$ |
| MDC-4 | $2^{5n/8}$ | $2^n$ | $2^{5n/4}$ | $2^{7n/4}$ [KP97] | $(E_1, E_2)$ |
| MDC-4 | $2^{5n/8}$ | $2^n$ | $2^n$ | $2^n$ | $E$ |

## Collision Resistance

- $2^{5n/8}$ security bound still applies

  independent analysis by Fleischmann et al.: $2^{3n/5}$ bound

## Preimage Resistance

- If $Y = Z$: preimage attack in $2^n$ queries!!
- Restricted to $Y \neq Z$: bound of $2^{5n/4}$ carries over

# Conclusions

| | collision | | preimage | | ideal primitives |
|---|---|---|---|---|---|
| | security | attack | security | attack | |
| MDC-2 | $2^{3n/5}$ [Ste07] | $2^n/n$ [KMRT09] | $2^n$ | $2^n$ [KMRT09] | $E$ or $(E_1, E_2)$ |
| MDC-4 | $2^{5n/8}$ | $2^n$ | $2^{5n/4}$ | $2^{7n/4}$ [KP97] | $(E_1, E_2)$ |
| MDC-4 | $2^{5n/8}$ | $2^n$ | $2^n$ | $2^n$ | $E$ |

*Thanks for your attention!*