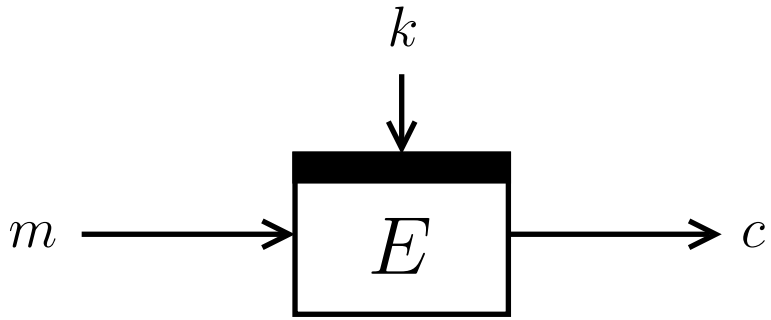
Triple and Quadruple Encryption: Bridging the Gaps

Bart Mennink and Bart Preneel
KU Leuven (Belgium)

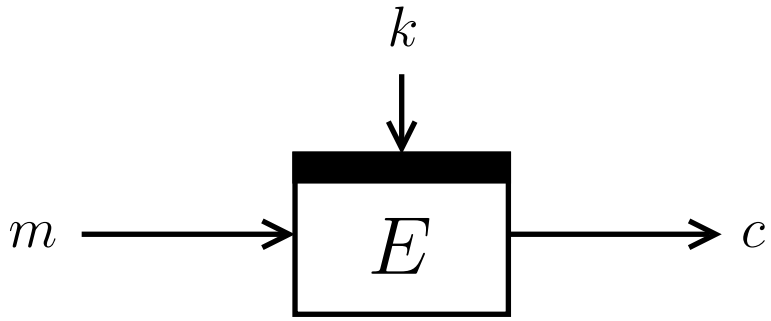
Dagstuhl — January 6, 2014

Introduction



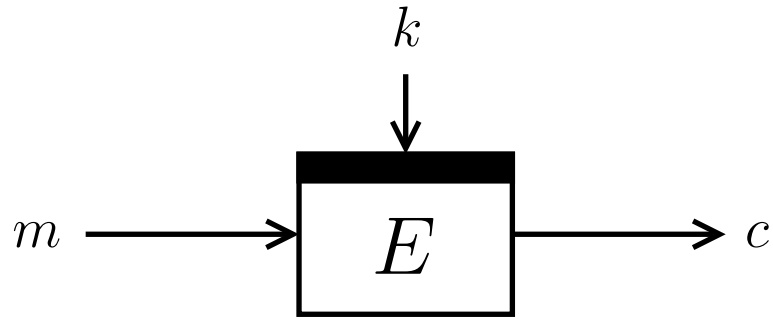
1977 DES $\kappa = 56$ $n = 64$

Introduction



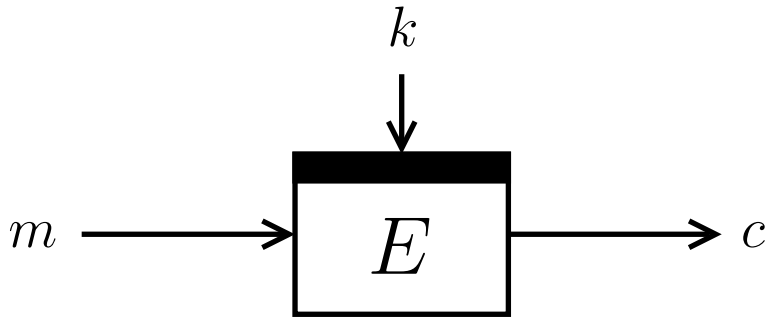
1977	DES	$\kappa = 56$	$n = 64$
1978	Triple-DES	$\kappa = 168$	$n = 64$

Introduction



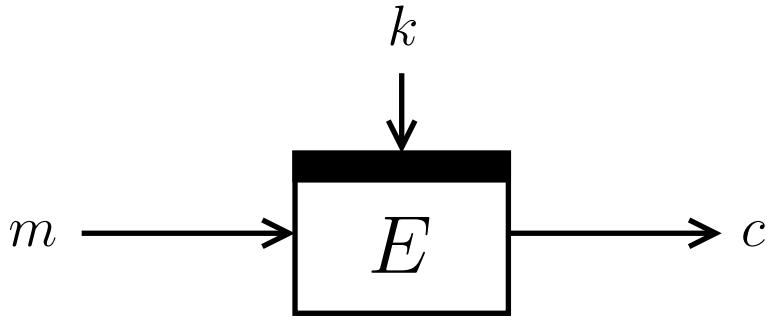
1977	DES	$\kappa = 56$	$n = 64$
1978	Triple-DES	$\kappa = 168$	$n = 64$
1984	DESX	$\kappa = 184$	$n = 64$

Introduction



1977	DES	$\kappa = 56$	$n = 64$
1978	Triple-DES	$\kappa = 168$	$n = 64$
1984	DESX	$\kappa = 184$	$n = 64$
1991	IDEA	$\kappa = 128$	$n = 64$
2001	AES	$\kappa \geq 128$	$n = 128$

Introduction



1977 DES $\kappa = 56$ $n = 64$

19

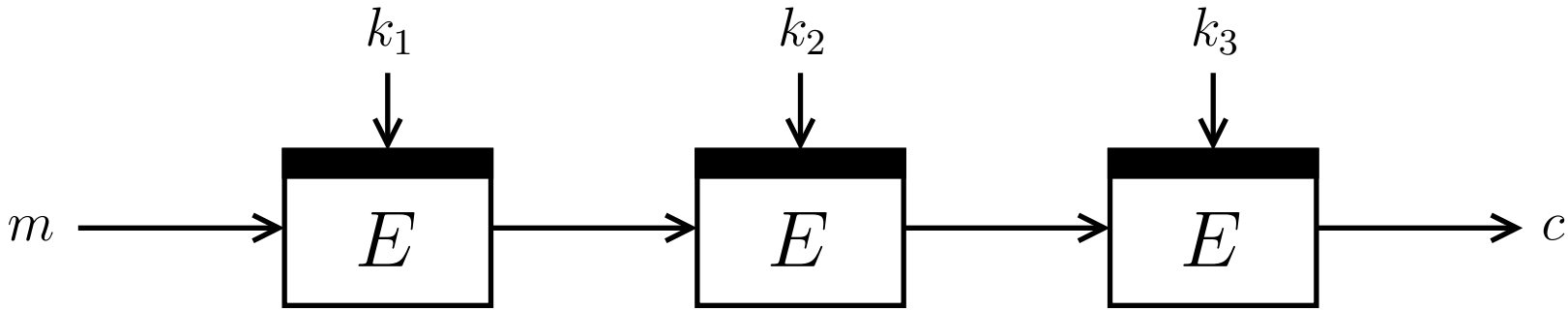
19

19

20

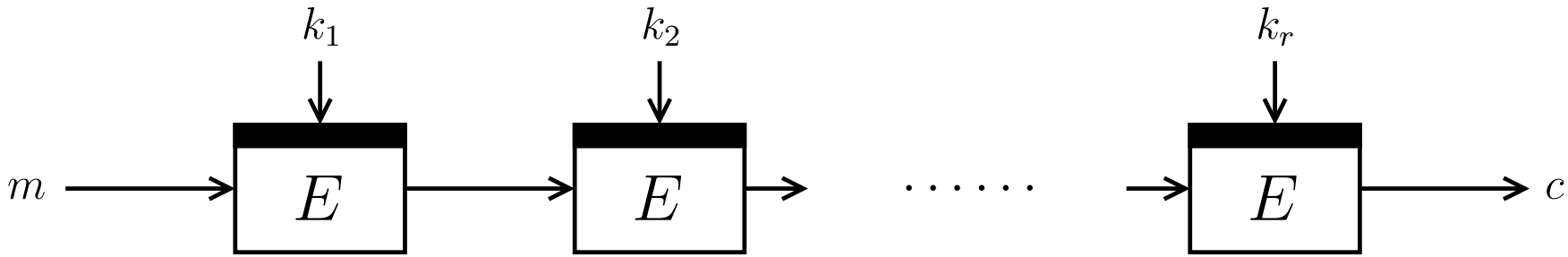
- Triple-DES still broadly used
- >1600 by NIST validated implementations
- ATMs, EMV, TLS, Microsoft, ...

Introduction: Triple-DES



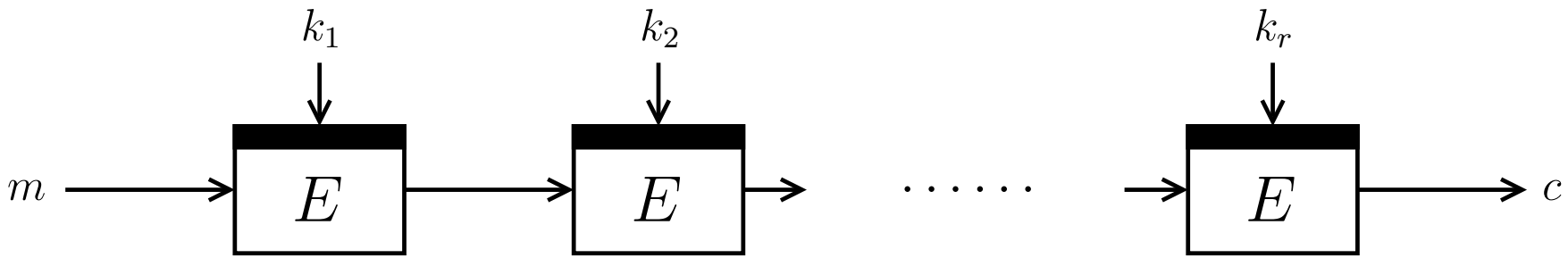
- Double-DES: only marginal security increase
- Triple-DES
  - $E \circ D \circ E$ versus $E \circ E \circ E$
  - $k_1 = k_3$ versus $k_1 \neq k_3$

Introduction: Cascade Encryption



- κ, n arbitrary
- $r' := \lceil r/2 \rceil$

Introduction: Cascade Encryption



- κ, n arbitrary
- $r' := \lceil r/2 \rceil$

- Ideal cipher model
- Information-theoretic distinguisher has access to E

State of the Art

rounds	security	attack	tight
$r = 1, 2$	κ	κ [DH77]	✓
$r = 3, 4$	$\kappa + \min\{\kappa/2, n/2\}$ [BR06,GM09]	$\kappa + n/2$ [Luc98,Gaž13]	✗
$r \geq 5$	$\kappa + \min\left\{\frac{(r'-1)}{r'}\kappa, n/2\right\}$ [GM09]	$\kappa + \frac{r'-1}{r'}n$ [Gaž13]	✗

- [Lee13]: $\kappa + \min\{\kappa, n\} - \frac{16}{r}(\frac{n}{2} + 2)$ security if $r \geq 16$

State of the Art

rounds	security	attack	tight
$r = 1, 2$	κ	κ [DH77]	✓
$r = 3, 4$	$\kappa + \min\{\kappa/2, n/2\}$ [BR06,GM09]	$\kappa + n/2$ [Luc98,Gaž13]	✗
$r \geq 5$	$\kappa + \min\left\{\frac{(r'-1)}{r'}\kappa, n/2\right\}$ [GM09]	$\kappa + \frac{r'-1}{r'}n$ [Gaž13]	✗

- [Lee13]: $\kappa + \min\{\kappa, n\} - \frac{16}{r}(\frac{n}{2} + 2)$ security if $r \geq 16$
- For $r = 3, 4$: bounds non-tight for $\kappa \leq n$

State of the Art

rounds	security	attack	tight
$r = 1, 2$	κ	κ [DH77]	✓
$r = 3, 4$	$\kappa + \min\{\kappa/2, n/2\}$ [BR06,GM09]	$\kappa + n/2$ [Luc98,Gaž13]	✗
$r \geq 5$	$\kappa + \min\left\{\frac{(r'-1)}{r'}\kappa, n/2\right\}$ [GM09]	$\kappa + \frac{r'-1}{r'}n$ [Gaž13]	✗

- [Lee13]: $\kappa + \min\{\kappa, n\} - \frac{16}{r}(\frac{n}{2} + 2)$ security if $r \geq 16$
- For $r = 3, 4$: bounds non-tight for $\kappa \leq n$

Triple-DES: $2^{84} \leq 2^{88}$

State of the Art

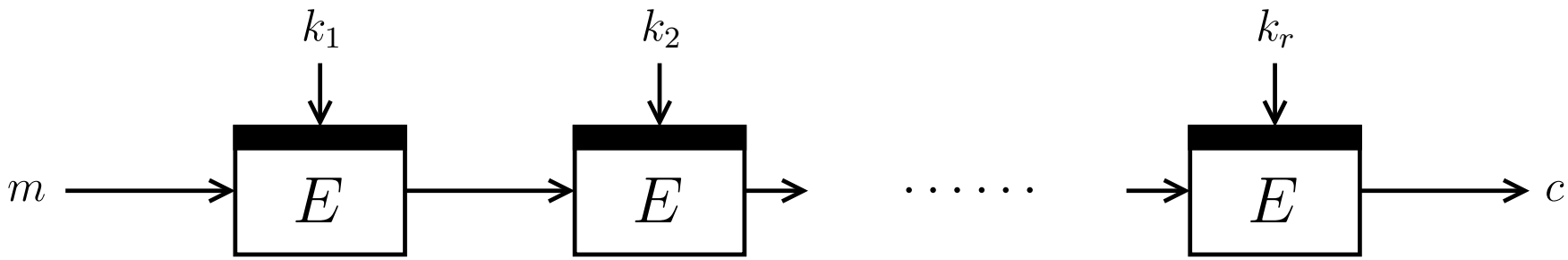
rounds	security	attack	tight
$r = 1, 2$	κ	κ [DH77]	✓
$r = 3, 4$	$\kappa + \min\{\kappa/2, n/2\}$ [BR06,GM09]	$\kappa + n/2$ [Luc98,Gaž13]	✗
$r \geq 5$	$\kappa + \min\left\{\frac{(r'-1)}{r'}\kappa, n/2\right\}$ [GM09]	$\kappa + \frac{r'-1}{r'}n$ [Gaž13]	✗

- [Lee13]: $\kappa + \min\{\kappa, n\} - \frac{16}{r}(\frac{n}{2} + 2)$ security if $r \geq 16$
- For $r = 3, 4$: bounds non-tight for $\kappa \leq n$

Triple-DES: $2^{84} \leq 2^{88}$

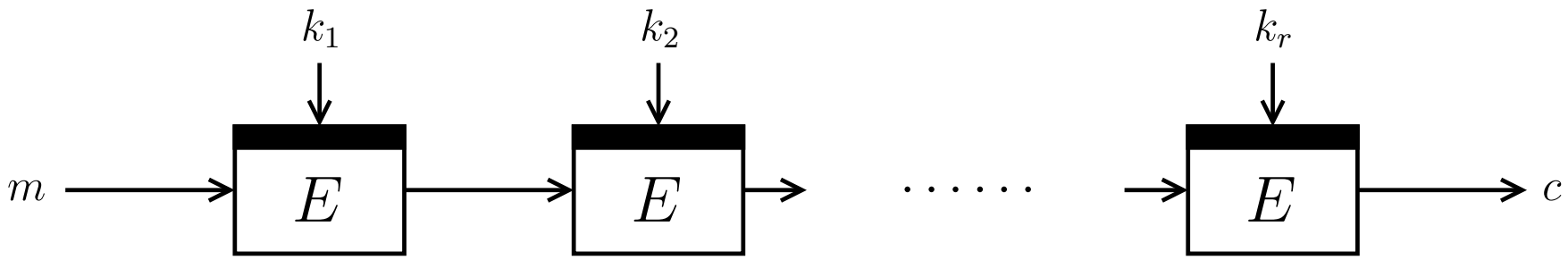
Main goal: tight security for triple encryption

Improving Attacks



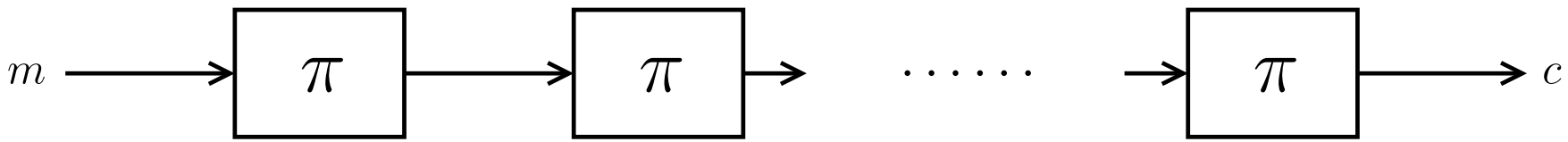
- [Gaž13]: attack in $2^{\kappa+\frac{r'-1}{r'}n}$ queries

Improving Attacks



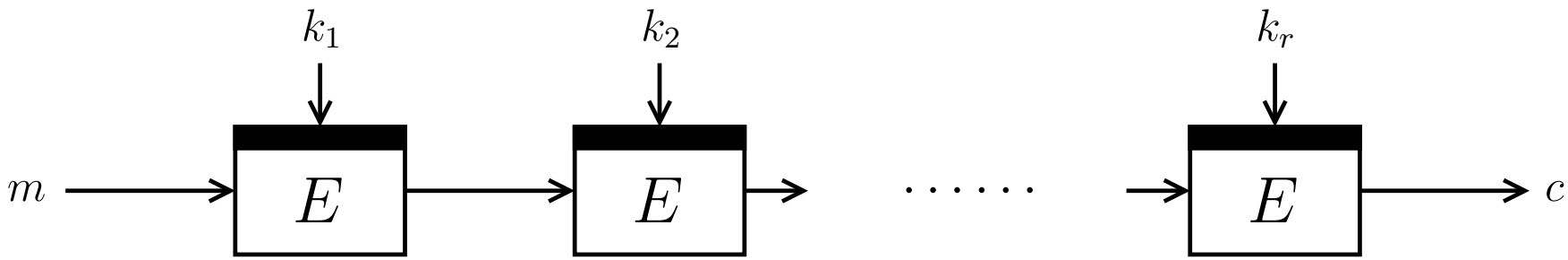
- [Gaž13]: attack in $2^{\kappa+\frac{r'-1}{r'}n}$ queries

- $\kappa = 0$:



- Distinguishable from random in constant #queries

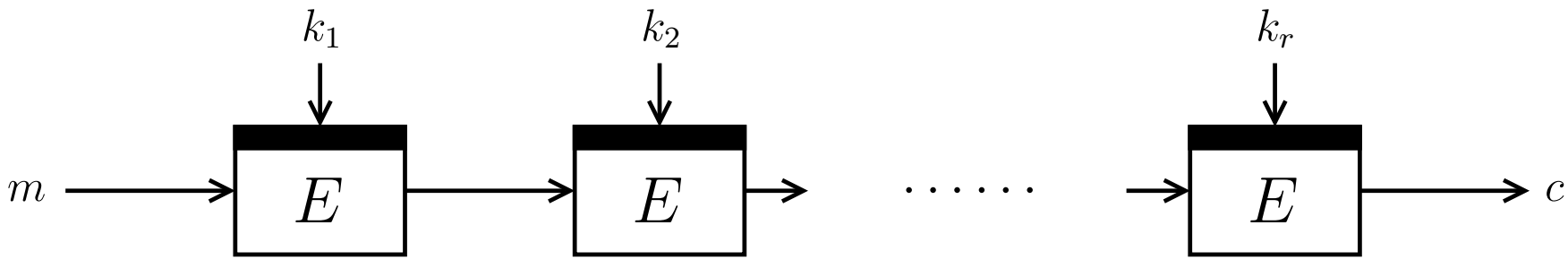
Improving Attacks



- [Gaž13]: attack in $2^{\kappa+\frac{r'-1}{r'}n}$ queries

Result 1: attack in $2^{r'\kappa}$ queries

Improving Attacks

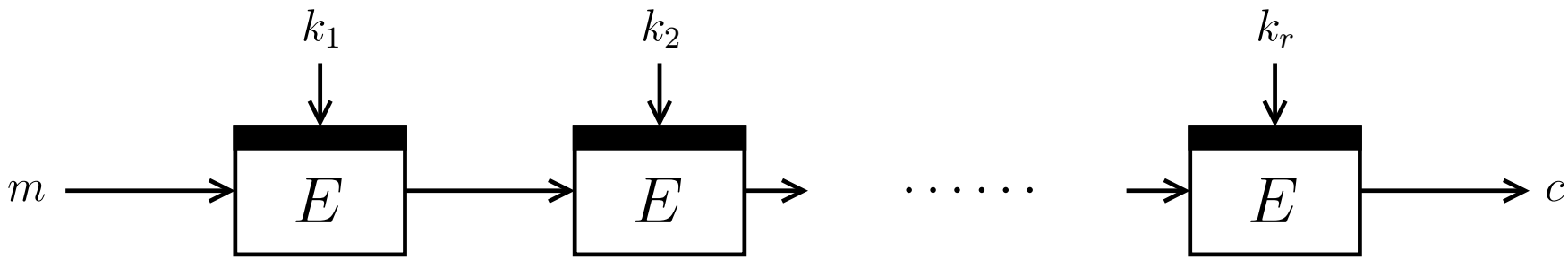


- [Gaž13]: attack in $2^{\kappa+\frac{r'-1}{r'}n}$ queries

Result 1: attack in $2^{r'\kappa}$ queries

- Attack idea:
  - Formalization of meet-in-the-middle attack
  - [DDKS12]: attack in $2^{(r-\sqrt{2r})\kappa}$ in incomparable model

Improving Attacks



- [Gaž13]: attack in $2^{\kappa+\frac{r'-1}{r'}n}$ queries

Result 1: attack in $2^{r'\kappa}$ queries

- Attack idea:
  - Formalization of meet-in-the-middle attack
  - [DDKS12]: attack in $2^{(r-\sqrt{2r})\kappa}$ in incomparable model

Corollary: attack in $2^{\kappa+\frac{r'-1}{r'}\min\{r'\kappa,n\}}$ queries

New State of the Art

rounds	security	attack	tight
$r = 1, 2$	κ	κ [DH77]	✓
$r = 3, 4$	$\kappa + \min\{\kappa/2, n/2\}$ [BR06,GM09]	$\kappa + n/2$ [Luc98,Gaž13]	✗
		$\boldsymbol{\kappa + \min\{\kappa, n/2\}}$	✗
$r \geq 5$	$\kappa + \min\left\{\frac{(r'-1)}{r'}\kappa, n/2\right\}$ [GM09]	$\kappa + \frac{r'-1}{r'}n$ [Gaž13]	✗
		$\boldsymbol{\kappa + \frac{r'-1}{r'}\min\{r'\kappa, n\}}$	✗

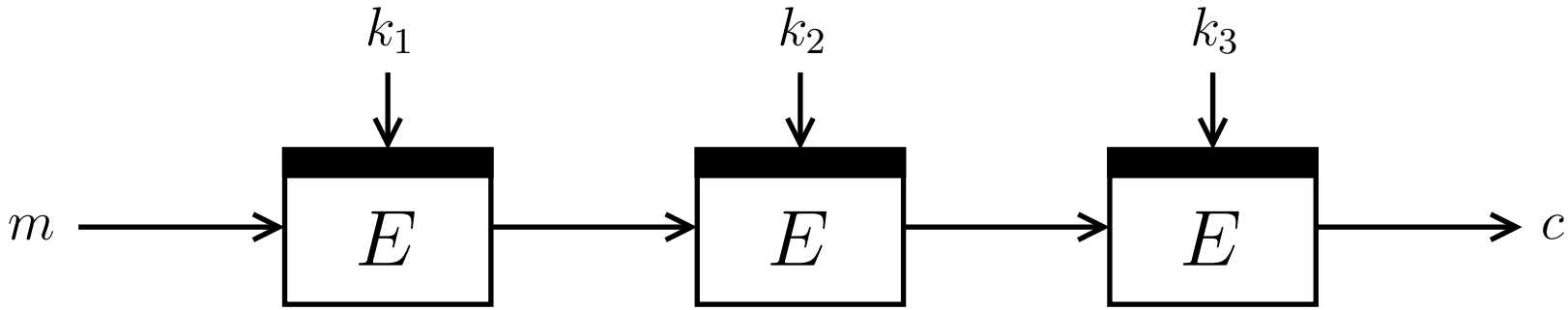
New State of the Art

rounds	security	attack	tight
$r = 1, 2$	κ	κ [DH77]	✓
$r = 3, 4$	$\kappa + \min\{\kappa/2, n/2\}$ [BR06,GM09]	$\kappa + n/2$ [Luc98,Gaž13]	✗
		$\boldsymbol{\kappa + \min\{\kappa, n/2\}}$	✗
$r \geq 5$	$\kappa + \min\left\{\frac{(r'-1)}{r'}\kappa, n/2\right\}$ [GM09]	$\kappa + \frac{r'-1}{r'}n$ [Gaž13]	✗
		$\boldsymbol{\kappa + \frac{r'-1}{r'}\min\{r'\kappa, n\}}$	✗

Triple-DES: $2^{84} \leq 2^{88}$

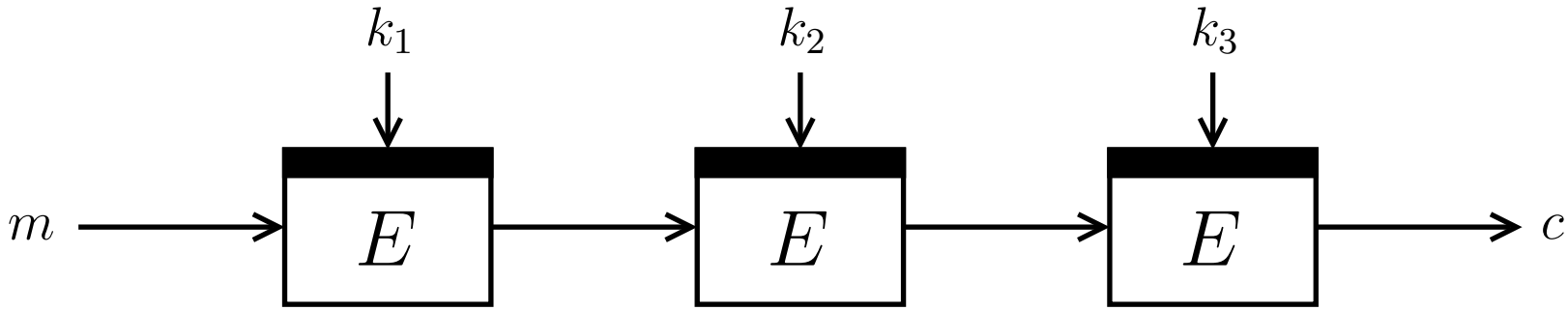
Main goal: tight security for triple encryption

Tightening Security Bounds



- [BR06,GM09]: security up to $2^{\kappa+\min\{\kappa/2,n/2\}}$ queries
- Attack in $2^{\kappa+\min\{\kappa,n/2\}}$ queries (previous slide)

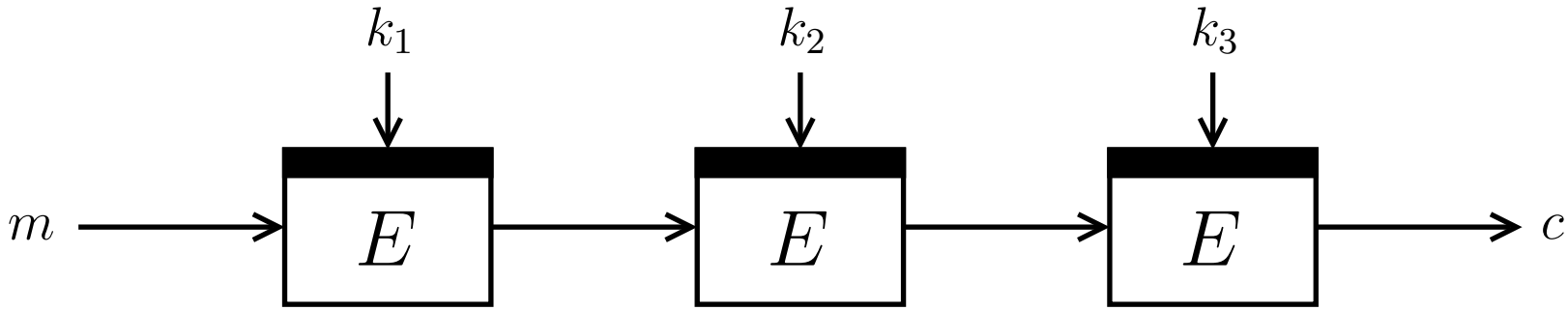
Tightening Security Bounds



- [BR06,GM09]: security up to $2^{\kappa+\min\{\kappa/2,n/2\}}$ queries
- Attack in $2^{\kappa+\min\{\kappa,n/2\}}$ queries (previous slide)

Result 2: tight security up to $2^{\kappa+\min\{\kappa,n/2\}}$ queries

Tightening Security Bounds

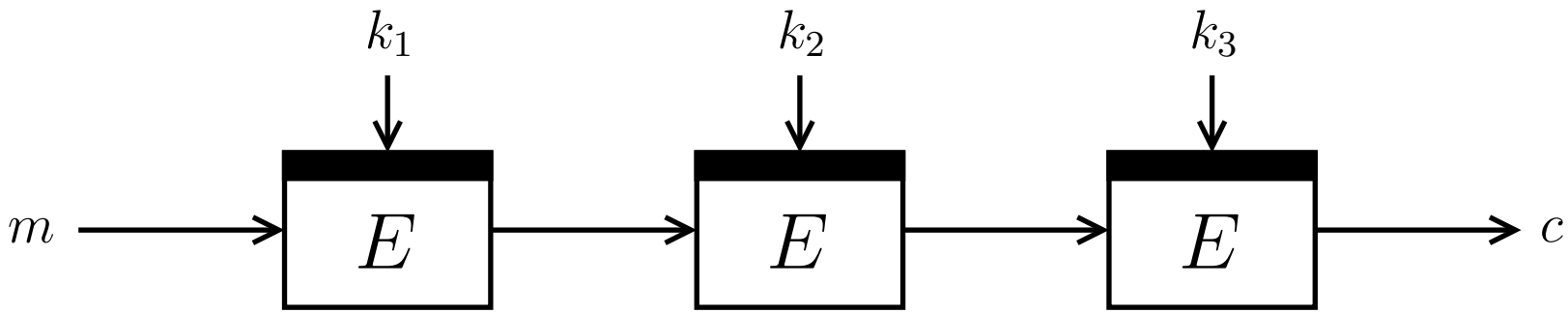


- [BR06,GM09]: security up to $2^{\kappa+\min\{\kappa/2,n/2\}}$ queries
- Attack in $2^{\kappa+\min\{\kappa,n/2\}}$ queries (previous slide)

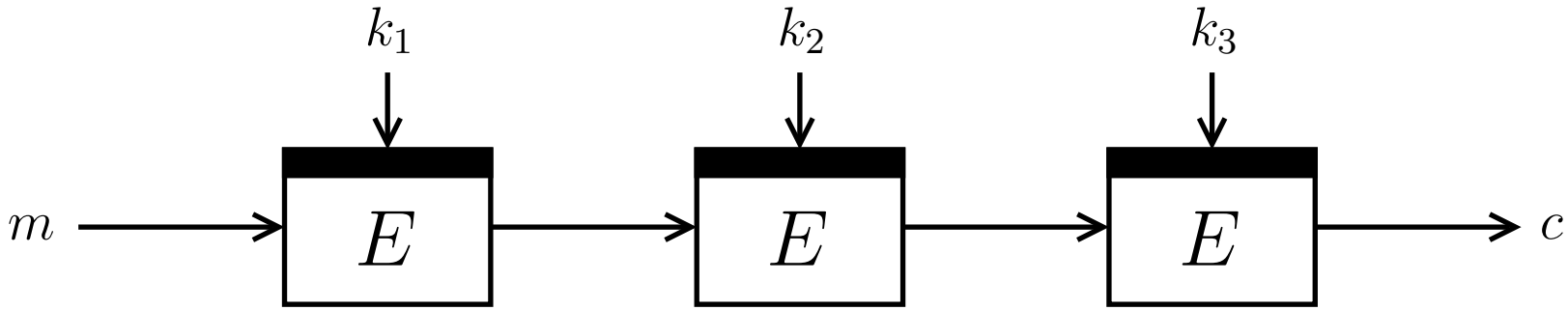
Result 2: tight security up to $2^{\kappa+\min\{\kappa,n/2\}}$ queries

- Proof idea:
  - Gap due to rather isolated lemma of [BR06,GM09]
  - Improvement of lemma leads to tight security

Tightening Security Bounds: Proof Idea

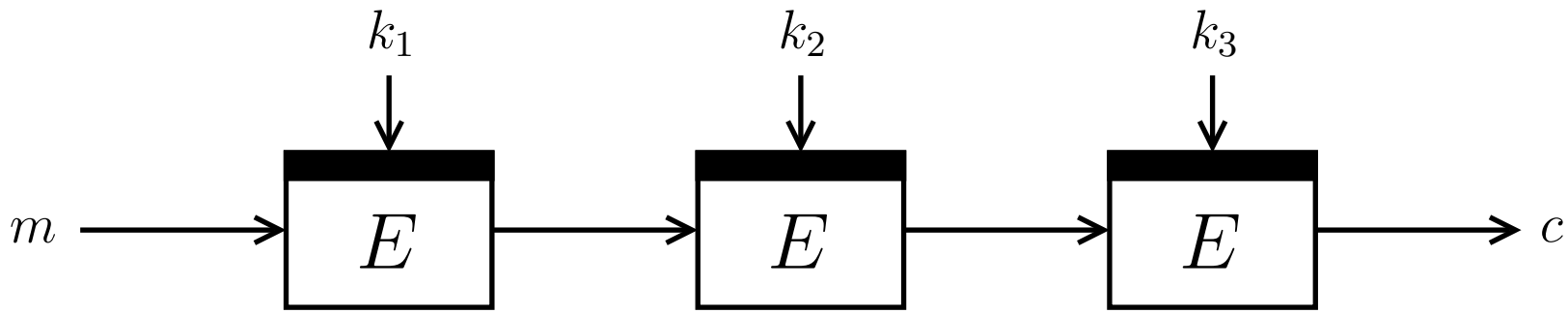


Tightening Security Bounds: Proof Idea



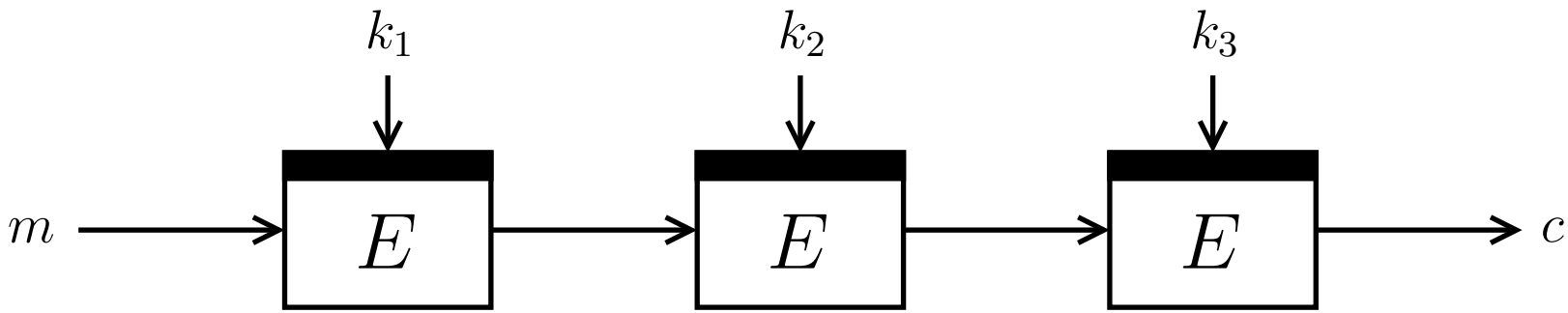
[BR06, GM09]

Tightening Security Bounds: Proof Idea



[BR06, GM09]

Tightening Security Bounds: Proof Idea



[BR06, GM09]

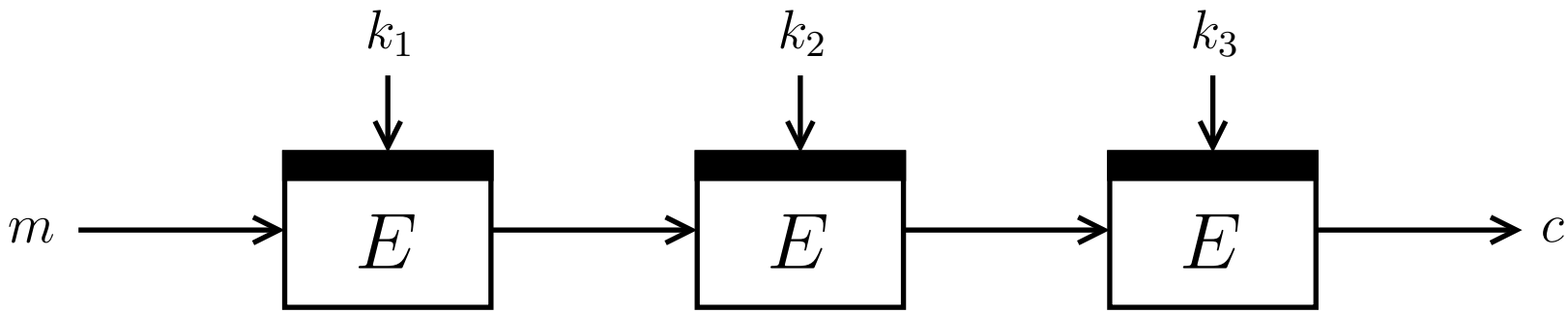
q options

$2\alpha_1$ options

q options

$(\alpha_1 = \max\{2e2^{\kappa-n}, 2n+\kappa\})$

Tightening Security Bounds: Proof Idea



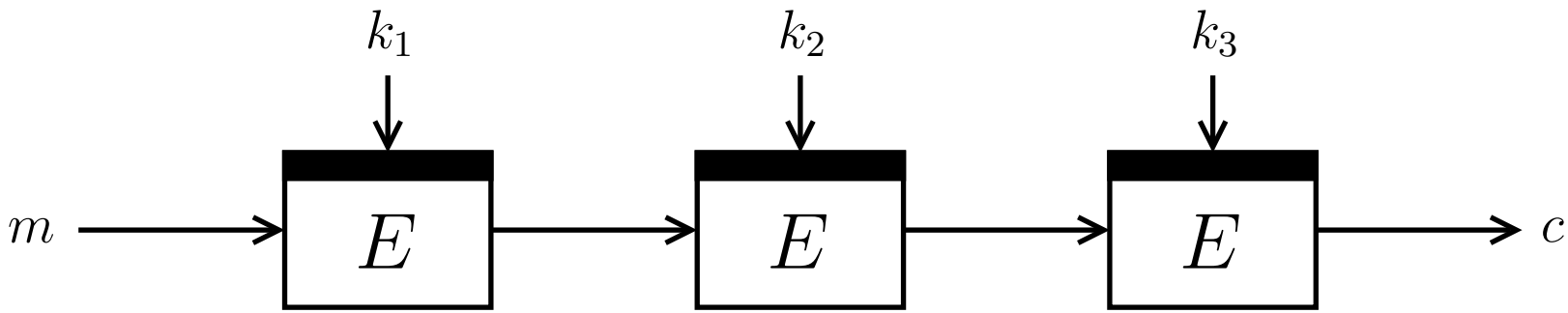
[BR06, GM09]

q options — $2\alpha_1$ options — q options

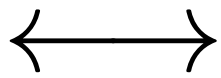
$\mathbf{E} = 2\alpha_1 q^2$

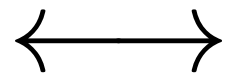
$(\alpha_1 = \max\{2e2^{\kappa-n}, 2n+\kappa\})$

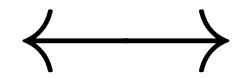
Tightening Security Bounds: Proof Idea



[BR06, GM09]



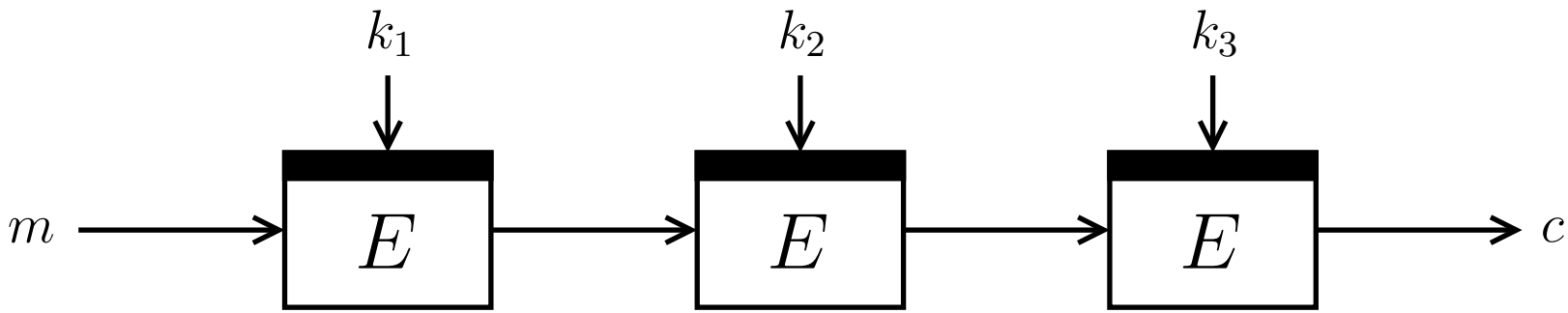




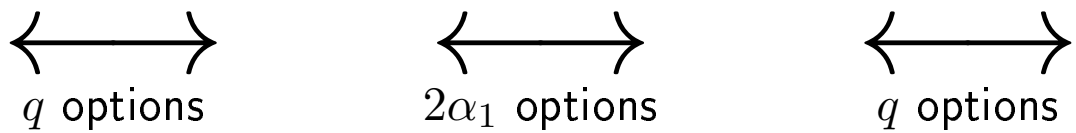
$\mathbf{E} = 2\alpha_1 q^2$ $(\alpha_1 = \max\{2e2^{\kappa-n}, 2n+\kappa\})$

now

Tightening Security Bounds: Proof Idea

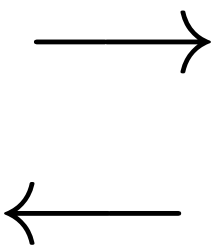


[BR06, GM09]

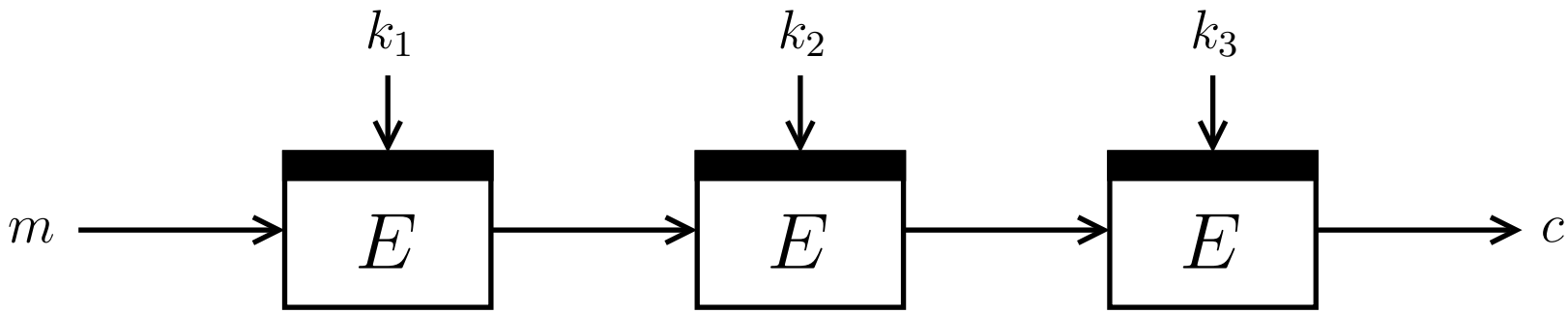


$\mathbf{E} = 2\alpha_1 q^2$ $(\alpha_1 = \max\{2e2^{\kappa-n}, 2n+\kappa\})$

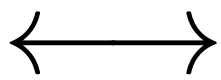
now

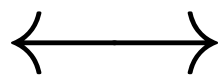


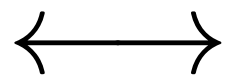
Tightening Security Bounds: Proof Idea



[BR06, GM09]

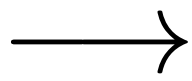


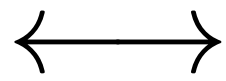


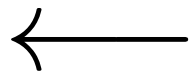


$\mathbf{E} = 2\alpha_1 q^2$ $(\alpha_1 = \max\{2e2^{\kappa-n}, 2n+\kappa\})$

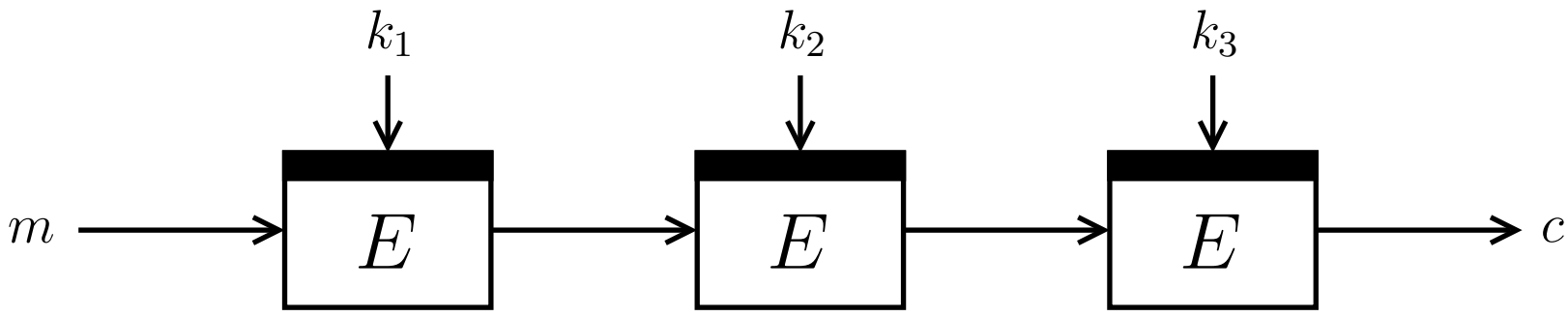
now



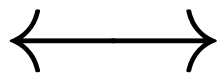


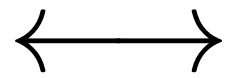


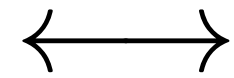
Tightening Security Bounds: Proof Idea



[BR06, GM09]



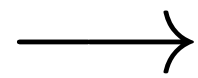


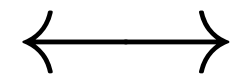


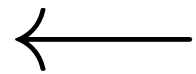
$\mathbf{E} = 2\alpha_1 q^2$

$(\alpha_1 = \max\{2e2^{\kappa-n}, 2n+\kappa\})$

now

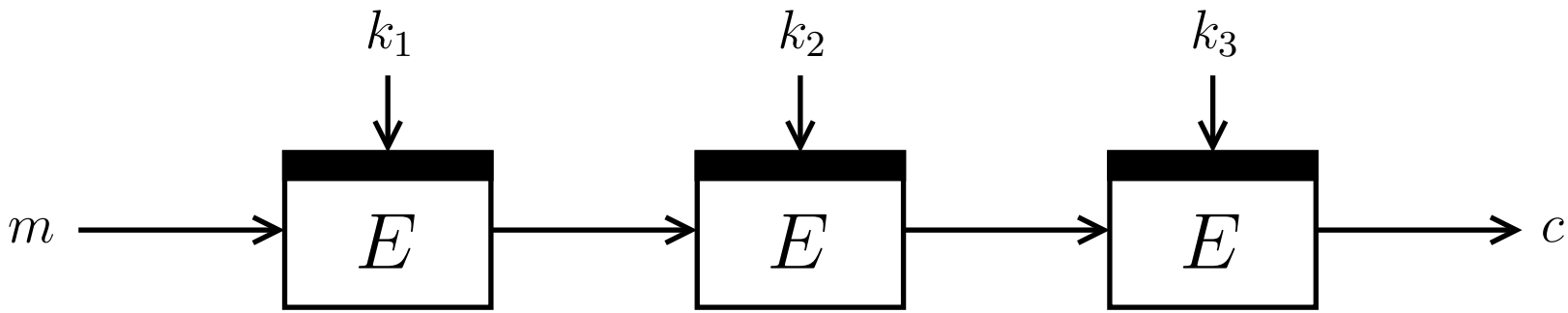




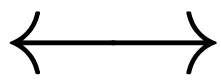


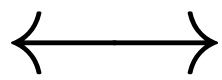
$(\alpha_2 = \max\{2eq/2^n, n+\kappa\})$

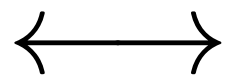
Tightening Security Bounds: Proof Idea



[BR06, GM09]



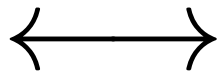


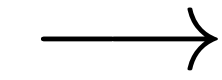


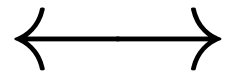
$\mathbf{E} = 2\alpha_1 q^2$

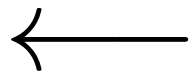
$(\alpha_1 = \max\{2e2^{\kappa-n}, 2n+\kappa\})$

now



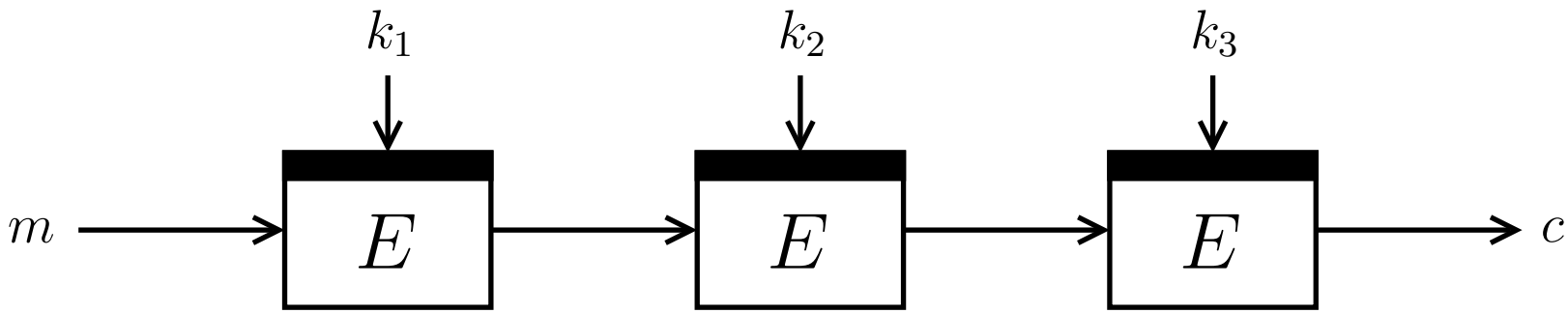




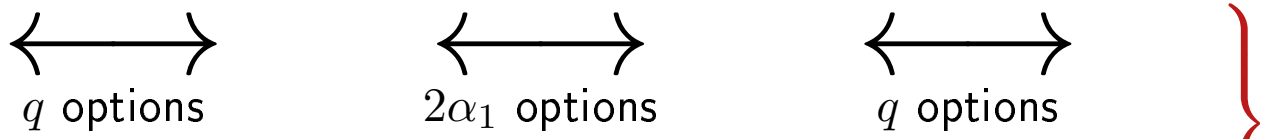


$(\alpha_2 = \max\{2eq/2^n, n+\kappa\})$

Tightening Security Bounds: Proof Idea

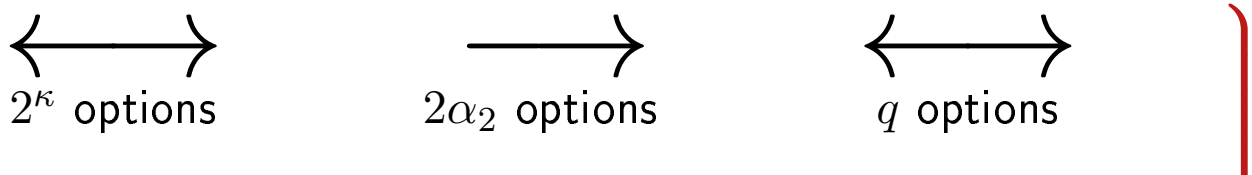


[BR06, GM09]



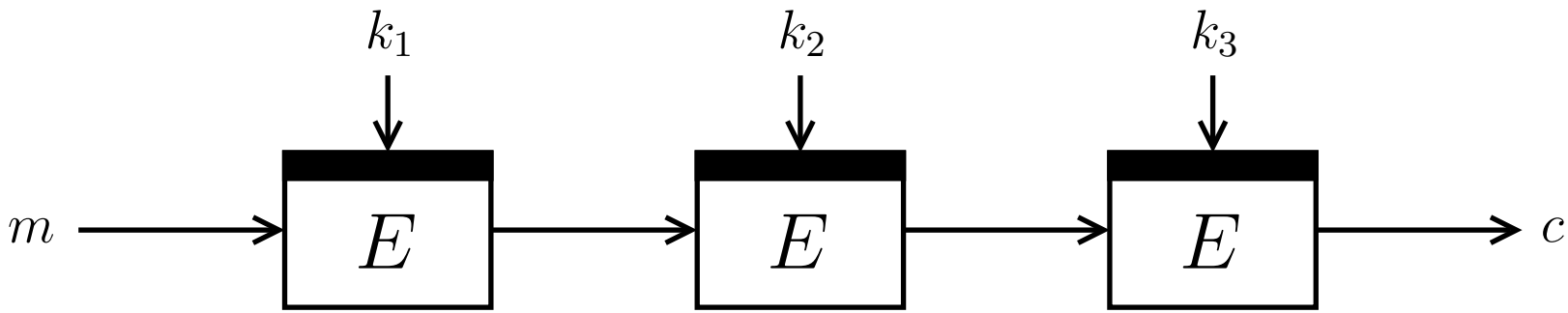
$\mathbf{E} = 2\alpha_1 q^2$ $\quad (\alpha_1 = \max\{2e2^{\kappa-n}, 2n+\kappa\})$

now

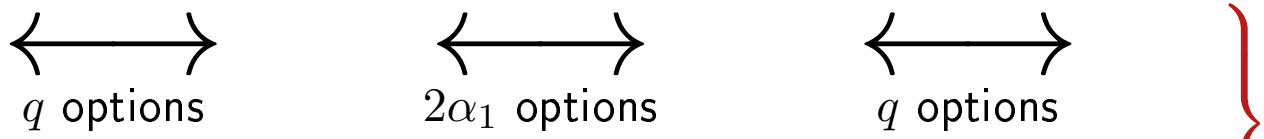


$(\alpha_2 = \max\{2eq/2^n, n+\kappa\})$

Tightening Security Bounds: Proof Idea

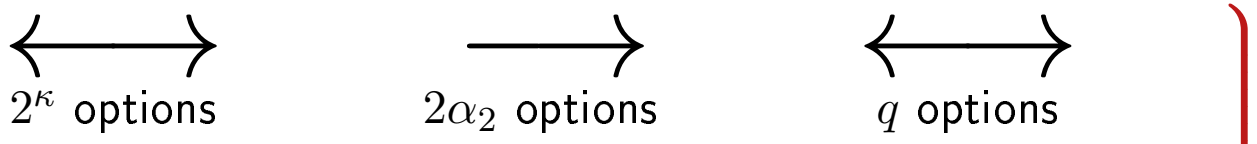


[BR06, GM09]



$\mathbf{E} = 2\alpha_1 q^2$ $\quad (\alpha_1 = \max\{2e2^{\kappa-n}, 2n+\kappa\})$

now



$\mathbf{E} = 4\alpha_2 2^\kappa q$ $\quad (\alpha_2 = \max\{2eq/2^n, n+\kappa\})$

Conclusions

rounds	security	attack	tight
$r = 1, 2$	κ	κ [DH77]	✓
$r = 3, 4$	$\kappa + \min\{\kappa/2, n/2\}$ [BR06,GM09]	$\kappa + n/2$ [Luc98,Gaž13]	✗
	$\boldsymbol{\kappa + \min\{\kappa, n/2\}}$	$\boldsymbol{\kappa + \min\{\kappa, n/2\}}$	✓
$r \geq 5$	$\kappa + \min\left\{\frac{(r'-1)}{r'}\kappa, n/2\right\}$ [GM09]	$\kappa + \frac{r'-1}{r'}n$ [Gaž13]	✗
	$\boldsymbol{\kappa + \min\{\kappa, n/2\}}$	$\boldsymbol{\kappa + \frac{r'-1}{r'}\min\{r'\kappa, n\}}$	✗

Conclusions

rounds	security	attack	tight
$r = 1, 2$	κ	κ [DH77]	✓
$r = 3, 4$	$\kappa + \min\{\kappa/2, n/2\}$ [BR06,GM09]	$\kappa + n/2$ [Luc98,Gaž13]	✗
	$\boldsymbol{\kappa + \min\{\kappa, n/2\}}$	$\boldsymbol{\kappa + \min\{\kappa, n/2\}}$	✓
$r \geq 5$	$\kappa + \min\left\{\frac{(r'-1)}{r'}\kappa, n/2\right\}$ [GM09]	$\kappa + \frac{r'-1}{r'}n$ [Gaž13]	✗
	$\boldsymbol{\kappa + \min\{\kappa, n/2\}}$	$\boldsymbol{\kappa + \frac{r'-1}{r'}\min\{r'\kappa, n\}}$	✗

- Tight security for $r \geq 5$ (non-trivial)?
- [Lee13]: asymptotic $\kappa + \min\{\kappa, n\}$ security

Conclusions

- Comparison with different model
- Consider cascaded DES

Conclusions

- Comparison with different model
- Consider cascaded DES

rounds	security	attack	attack	
			time	memory
$r = 2$	2^{56}	2^{56}		
$r = 3$	2^{88}	2^{88}		
$r = 4$	2^{88}	2^{88}		

Conclusions

- Comparison with different model
- Consider cascaded DES

rounds	security	attack	attack	
			time	memory
$r = 2$	2^{56}	2^{56}	2^{57}	2^{56}
$r = 3$	2^{88}	2^{88}	2^{112}	2^{56}
$r = 4$	2^{88}	2^{88}	2^{121}	2^{56}

Conclusions

- Comparison with different model
- Consider cascaded DES

rounds	security	attack	attack	
			time	memory
$r = 2$	2^{56}	2^{56}	2^{57}	2^{56}
$r = 3$	2^{88}	2^{88}	2^{112}	2^{56}
$r = 4$	2^{88}	2^{88}	2^{121}	2^{56}

Thank you for your attention!