Iterative Block Ciphers from Tweakable Block Ciphers with Long Tweaks

Ryota Nakamichi and Tetsu Iwata

Nagoya University, Japan

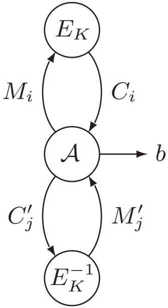
FSE 2020
November 9–13, 2020, Virtual

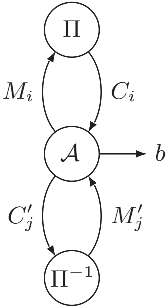
Block Ciphers

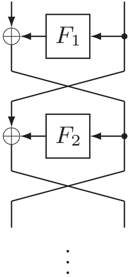
- block cipher (BC)
  - $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$
  - n is the block length, n-BC
  - for each $K \in \mathcal{K}$, $E_K(\cdot) \in \mathrm{Perm}(n)$
- Construction of a secure and efficient block cipher is one of the most important problems in symmetric key cryptography

Provably Secure BCs

- strong pseudorandom permutation (SPRP) [LR88]
  - real world: $(E_K, E_K^{-1}), E_K \in \mathrm{Perm}(n)$, n-BC
  - ideal world: $(\Pi, \Pi^{-1}), \Pi \in \mathrm{Perm}(n)$, a random permutation
  - $\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{A}) = \Pr[\mathcal{A}^{E_K, E_K^{-1}} \Rightarrow 1] - \Pr[\mathcal{A}^{\Pi, \Pi^{-1}} \Rightarrow 1]$
- 4-round Feistel cipher with n-bit PRFs is an SPRP [LR88]
  - For any $\mathcal{A}$ that makes q queries, $\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{A})$ is $O(q^2/2^n)$
  - a birthday bound with respect to the input/output length of the underlying primitive







[LR88] Michael Luby and Charles Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. SIAM J. Comput., 1988

Beyond-Birthday-Bound Secure BCs

- LR result is $O(q^2/2^n)$, requires $q \ll 2^{n/2}$
- BBB (beyond-birthday-bound) secure constructions?
  - BCs that remain secure even if $q \geq 2^{n/2}$
  - 5-round or 6-round Feistel cipher [Pat04]
  - many-round Feistel cipher [MP03]
- The use of a tweakable block cipher (TBC) as a building block [Min09]

[Pat04] Jacques Patarin. Security of Random Feistel Schemes with 5 or More Rounds. CRYPTO 2004

[MP03] Ueli M. Maurer and Krzysztof Pietrzak. The Security of Many-Round Luby- Rackoff Pseudo-Random Permutations. EUROCRYPT 2003

[Min09] Kazuhiko Minematsu. Beyond-Birthday-Bound Security Based on Tweakable Block Cipher. FSE 2009

Tweakable Block Ciphers (TBCs)

- Generalization of BCs, and they take an additional input called a tweak [LRW02]
  - $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$
  - $\mathcal{T}$ is the tweak space, if $\mathcal{T} = \{0,1\}^t$, then t is the tweak length, (n,t)-TBC
  - for each $K \in \mathcal{K}$ and $T \in \mathcal{T}$, $E_K(\cdot, T) \in \mathrm{Perm}(n)$
- TBCs are useful
  - encryption scheme schemes, MACs, authenticated encryption schemes
- There are many constructions of a TBC based on BCs
  - LRW1, LRW2 [LRW02], XEX [Rog04]
- constructions of BCs from TBCs
- There are a number of recent proposals as a primitive
  - TWEAKEY framework [JNP14]
  - CAESAR submissions (KIASU-BC, Deoxys-BC, Joltik-BC, Scream), SKINNY [BJK+16], QARMA [Ava17], CRAFT [BLMR19]

[LRW02] Moses Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable Block Ciphers. CRYPTO 2002

[Rog04] Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. ASIACRYPT 2004

BCs from TBCs

- $2n$-BC from (n, n)-TBCs and universal hash functions [Min09]
- $2n$-BC from (n, n)-TBCs only [CDMS10]
- dn-BC from $(n, \tau n)$-TBCs with $d = \tau + 1$ and $\tau \geq 1$ [Min15]

- We focus on iterative constructions of BCs
  - a fixed input length keyed permutation
  - the block length is a multiple of n

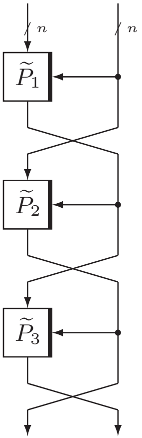
[CDMS10] Jean-Sébastien Coron, Yevgeniy Dodis, Avradip Mandal, and Yannick Seurin. A Domain Extender for the Ideal Cipher. TCC 2010

[Min15] Kazuhiko Minematsu. Building blockcipher from small-block tweakable blockcipher. Des. Codes Cryptography, 2015

BCs from TBCs [CDMS10]

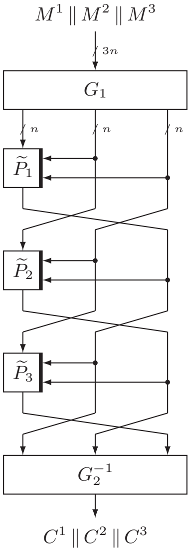
- $2n$-BC from (n, n)-TBCs [CDMS10]
  - $\widetilde{P}_i$ is $\widetilde{E}_{K_i}$
- $O(q^2/2^n)$ security with 2 rounds (birthday bound)
- $O(q^2/2^{2n})$ security with 3 rounds (BBB)

- domain extender for the ideal cipher, indifferentiability setting, ideal cipher model
- tweakable block ciphers



BCs from TBCs [Min15]

- dn-BC from $(n, \tau n)$-TBCs with $d = \tau + 1$ and $\tau \geq 1$ [Min15]
  - a TBC with "long tweaks"
  - $\tau = 2$ and $d = 3$ in the figure
- The middle part has d rounds
- G_1 and G_2 are keyed permutations that satisfy certain combinatorial requirements
  - can be non-cryptographic permutations
    - pairwise independent permutations
  - can also be cryptographic permutations
    - d rounds, $3d$ rounds in total
- $O(q^2/2^{dn})$ security with good G_1 and G_2



BCs from TBCs

Construction	Block (bits)	TBC	TBC calls	Bound (Limit on q)
Coron et al. [CDMS10]	$2n$	(n, n)	3	$q^2/2^{2n}$
Minematsu [Min15]	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$3d$	$q^2/2^{dn}$
Theorem 1	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$3d - 2$	$q^2/2^{dn}$
Theorem 2	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$d + \ell$	$q^2/2^{(1+\ell)n}$ $(q \leq 2^n)$
Theorem 3	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	d	$q^2/2^n$

- $d = \tau + 1$, and the security bounds neglect constants
- In Theorem 2, $\ell = 1, \ldots, d - 1$

- Theorem 1: The security remains the same even if we reduce the number of rounds by two
- Theorem 2: If $q \leq 2^n$, BBB security is achieved as low as $d + 1$ rounds ($\ell = 1$), and the security exponentially improves by adding rounds, up to $2d - 1$ rounds
- Theorem 3: birthday bound with d rounds, and there is a matching attack

BCs from TBCs

Construction	Block (bits)	TBC	TBC calls	Bound (Limit on q)
Coron et al. [CDMS10]	$2n$	(n, n)	3	$q^2/2^{2n}$
Minematsu [Min15]	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$3d$	$q^2/2^{dn}$
Theorem 1	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$3d - 2$	$q^2/2^{dn}$
Theorem 2	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$d + \ell$	$q^2/2^{(1+\ell)n}$ $(q \leq 2^n)$
Theorem 3	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	d	$q^2/2^n$

- $d = \tau + 1$, and the security bounds neglect constants
- In Theorem 2, $\ell = 1, \ldots, d - 1$

- Theorem 1: The security remains the same even if we reduce the number of rounds by two
- Theorem 2: If $q \leq 2^n$, BBB security is achieved as low as $d + 1$ rounds $(\ell = 1)$, and the security exponentially improves by adding rounds, up to $2d - 1$ rounds
- Theorem 3: birthday bound with d rounds, and there is a matching attack

BCs from TBCs

Construction	Block (bits)	TBC	TBC calls	Bound (Limit on q)
Coron et al. [CDMS10]	$2n$	(n, n)	3	$q^2/2^{2n}$
Minematsu [Min15]	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$3d$	$q^2/2^{dn}$
Theorem 1	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$3d - 2$	$q^2/2^{dn}$
Theorem 2	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$d + \ell$	$q^2/2^{(1+\ell)n}$ $(q \leq 2^n)$
Theorem 3	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	d	$q^2/2^n$

- $d = \tau + 1$, and the security bounds neglect constants
- In Theorem 2, $\ell = 1, \ldots, d - 1$

- Theorem 1: The security remains the same even if we reduce the number of rounds by two
- Theorem 2: If $q \leq 2^n$, BBB security is achieved as low as $d + 1$ rounds ($\ell = 1$), and the security exponentially improves by adding rounds, up to $2d - 1$ rounds
- Theorem 3: birthday bound with d rounds, and there is a matching attack

BCs from TBCs

Construction	Block (bits)	TBC	TBC calls	Bound (Limit on q)
Coron et al. [CDMS10]	$2n$	(n, n)	3	$q^2/2^{2n}$
Minematsu [Min15]	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$3d$	$q^2/2^{dn}$
Theorem 1	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$3d - 2$	$q^2/2^{dn}$
Theorem 2	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	$d + \ell$	$q^2/2^{(1+\ell)n}$ $(q \leq 2^n)$
Theorem 3	dn, $d = 2, 3, \ldots$	$(n, \tau n)$	d	$q^2/2^n$

- $d = \tau + 1$, and the security bounds neglect constants
- In Theorem 2, $\ell = 1, \ldots, d - 1$

- Theorem 1: The security remains the same even if we reduce the number of rounds by two
- Theorem 2: If $q \leq 2^n$, BBB security is achieved as low as $d + 1$ rounds ($\ell = 1$), and the security exponentially improves by adding rounds, up to $2d - 1$ rounds
- Theorem 3: birthday bound with d rounds, and there is a matching attack

Implication

- Assume that we use SKINNY with 128-bit blocks, 256-bit tweaks, and 128-bit keys (384-bit tweakey) with r rounds, and assume that it is perfectly secure
- 384-BC with $128r$-bit keys

r	key length (bits)	Bound (Limit on q)	Ref.
9	128×9	$q^2/2^{384}$	[Min15]
7	128×7	$q^2/2^{384}$	Theorem 1
5	128×5	$q^2/2^{384}$ $(q \leq 2^{128})$	Theorem 2, $\ell = 2$
4	128×4	$q^2/2^{256}$ $(q \leq 2^{128})$	Theorem 2, $\ell = 1$
3	128×3	$q^2/2^{128}$	Theorem 3

Coefficient-H Technique

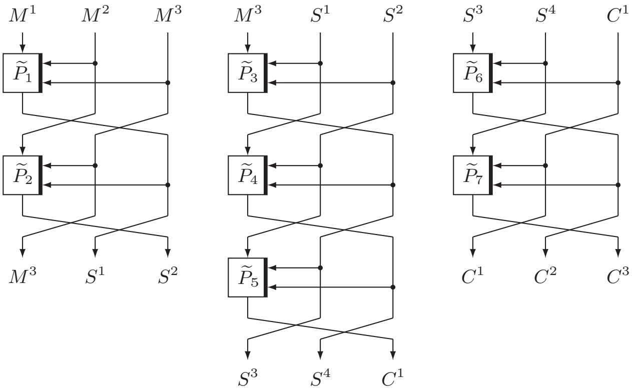
- Patarin's coefficient-H technique [Pat08, CS14]
- partition all the transcripts such that $\Pr[\Theta_{\text{ideal}} = \theta] > 0$ into good ones T_{good} and bad ones T_{bad}
- Suppose that there exist ϵ_1 and ϵ_2 that satisfy:
  - $\forall \theta \in \mathsf{T}_{\text{good}}, \dfrac{\Pr[\Theta_{\text{real}} = \theta]}{\Pr[\Theta_{\text{ideal}} = \theta]} \geq 1 - \epsilon_1$, and
  - $\Pr[\Theta_{\text{ideal}} \in \mathsf{T}_{\text{bad}}] \leq \epsilon_2$

  Then, $\mathbf{Adv}_E^{\text{sprp}}(\mathcal{A}) \leq \epsilon_1 + \epsilon_2$

[Pat08] Jacques Patarin. The "Coefficients H" Technique. SAC 2008

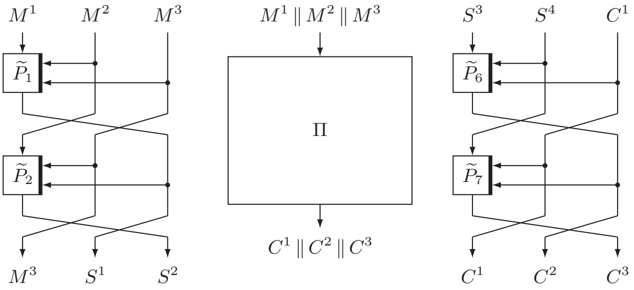
[CS14] Shan Chen and John P. Steinberger. Tight Security Bounds for Key-Alternating Ciphers. EUROCRYPT 2014

Theorem 1, $(3d-2)$-Round Construction



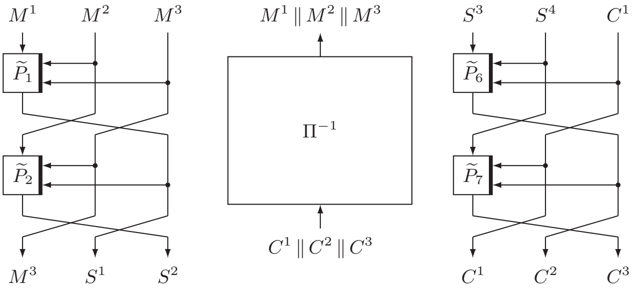
- 7 rounds when $d = 3$, $S^1, \ldots, S^4$ are internal variables
- Real world: Following [CS14], we release $S^1, \ldots, S^4$ to $\mathcal{A}$ after making all the queries

Theorem 1, $(3d-2)$-Round Construction



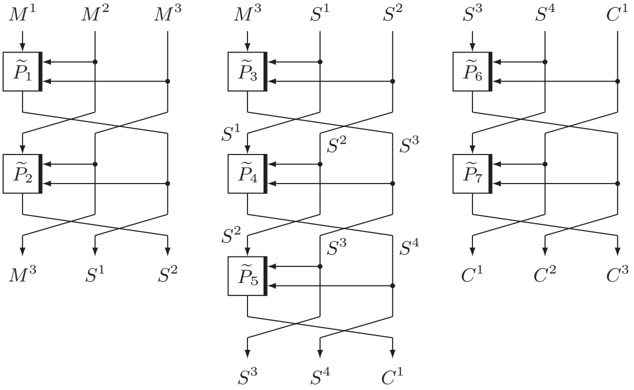
- Ideal world: use Π and Π^{-1}, and also dummy $\widetilde{P}_1, \widetilde{P}_2, \widetilde{P}_6, \widetilde{P}_7$ to compute $S^1, \ldots, S^4$

Theorem 1, $(3d-2)$-Round Construction



- Ideal world: use Π and Π^{-1}, and also dummy $\widetilde{P}_1, \widetilde{P}_2, \widetilde{P}_6, \widetilde{P}_7$ to compute $S^1, \ldots, S^4$

Theorem 1, $(3d-2)$-Round Construction



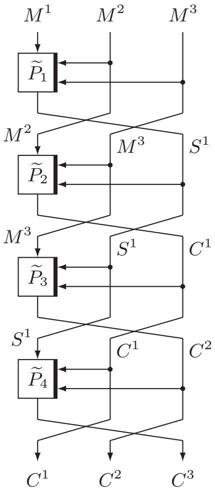
- In the ideal world, a transcript is bad if
  - (S_i^1, S_i^2, S_i^3) collides
  - (S_i^2, S_i^3, S_i^4) collides
- the bad event involves randomness of $3n$ bits

Theorem 1, $(3d-2)$-Round Construction

- In general, we have $S^1, \ldots, S^{2d-2}$ as internal variables
- In the ideal world, a transcript is bad if
  - $(S_i^1, \ldots, S_i^d)$ collides
  - $(S_i^2, \ldots, S_i^{d+1})$ collides
  - $\ldots$
  - $(S_i^{d-1}, \ldots, S_i^{2d-2})$ collides
- $d-1$ cases, and the bad event involves randomness of dn bits
- $\Pr[\Theta_{\text{ideal}} \in \mathsf{T}_{\text{bad}}] \leq \dfrac{0.5(d-1)q^2}{2^{dn}}$
- $\forall \theta \in \mathsf{T}_{\text{good}}, \dfrac{\Pr[\Theta_{\text{real}} = \theta]}{\Pr[\Theta_{\text{ideal}} = \theta]} \geq 1 - \dfrac{0.5q^2}{2^{dn}}$
- $\mathbf{Adv}_E^{\text{sprp}}(\mathcal{A}) \leq \dfrac{0.5dq^2}{2^{dn}}$ from the coefficient-H technique

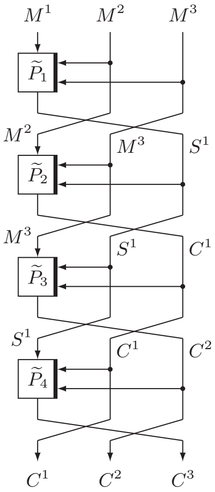
Theorem 2, $(d+\ell)$-Round Construction

- 4 rounds when $d = 3$ and $\ell = 1$
- S^1 is the only internal variable
- In the ideal world, S^1 is generated with dummy $\widetilde{P}_1$ if the i-th query is an encryption query, and with dummy $\widetilde{P}_4$ if the i-th query is a decryption query
- In the ideal world, a transcript is bad if
  - (M_i^2, M_i^3, S_i^1) collides (impossible for an encryption query)
  - (M_i^3, S_i^1, C_i^1) collides
  - (S_i^1, C_i^1, C_i^2) collides (impossible for a decryption query)
- The bad event involves randomness of $2n$ bits



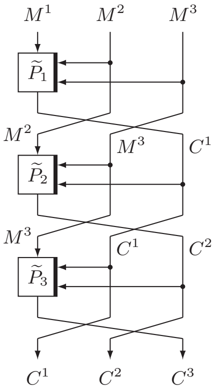
Theorem 2, $(d+\ell)$-Round Construction

- In general, the bad event involves randomness of $(\ell+1)n$ bits
- $\Pr[\Theta_{\text{ideal}} \in \mathsf{T}_{\text{bad}}] \leq \dfrac{(d-1)q^2}{2^{(\ell+1)n}}$
  - rely on $q \leq 2^n$ to derive the upper bound
- $\forall \theta \in \mathsf{T}_{\text{good}}, \dfrac{\Pr[\Theta_{\text{real}} = \theta]}{\Pr[\Theta_{\text{ideal}} = \theta]} \geq 1 - \dfrac{0.5q^2}{2^{dn}}$
- $\mathbf{Adv}_E^{\text{sprp}}(\mathcal{A}) \leq \dfrac{dq^2}{2^{(\ell+1)n}}$ from the coefficient-H technique



Theorem 3, d-Round Construction

- 3 rounds when $d = 3$
- birthday bound security, no internal variable
- matching attack
  - make encryption queries
    - with distinct M^1
    - with fixed M^2 and M^3
  - C^1 is always distinct in the real world, but can collide in the ideal world



Conclusions

Construction	Block (bits)	TBC	TBC calls	Bound (Limit on q)
Coron et al. [CDMS10]	$2n$	(n, n)	3	$q^2/2^{2n}$
Minematsu [Min15]	$dn,\ d = 2, 3, \ldots$	$(n, \tau n)$	$3d$	$q^2/2^{dn}$
Theorem 1	$dn,\ d = 2, 3, \ldots$	$(n, \tau n)$	$3d - 2$	$q^2/2^{dn}$
Theorem 2	$dn,\ d = 2, 3, \ldots$	$(n, \tau n)$	$d + \ell$	$q^2/2^{(1+\ell)n}$ $(q \leq 2^n)$
Theorem 3	$dn,\ d = 2, 3, \ldots$	$(n, \tau n)$	d	$q^2/2^n$

- Open questions
  - We do not know if the condition of $q \leq 2^n$ can be removed from Theorem 2
  - The tightness of Theorems 1 and 2 is open
  - Generalization to enciphering schemes
  - The analysis in the indifferentiability framework (please check [NI20b])

Thank you!

[NI20b] Ryota Nakamichi and Tetsu Iwata. Beyond-Birthday-Bound Secure Cryptographic Permutations from Ideal Ciphers with Long Keys. FSE 2020

Conclusions

Construction	Block (bits)	TBC	TBC calls	Bound (Limit on q)
Coron et al. [CDMS10]	$2n$	(n, n)	3	$q^2/2^{2n}$
Minematsu [Min15]	$dn,\ d = 2, 3, \ldots$	$(n, \tau n)$	$3d$	$q^2/2^{dn}$
Theorem 1	$dn,\ d = 2, 3, \ldots$	$(n, \tau n)$	$3d - 2$	$q^2/2^{dn}$
Theorem 2	$dn,\ d = 2, 3, \ldots$	$(n, \tau n)$	$d + \ell$	$q^2/2^{(1+\ell)n}$ $(q \leq 2^n)$
Theorem 3	$dn,\ d = 2, 3, \ldots$	$(n, \tau n)$	d	$q^2/2^n$

- Open questions
  - We do not know if the condition of $q \leq 2^n$ can be removed from Theorem 2
  - The tightness of Theorems 1 and 2 is open
  - Generalization to enciphering schemes
  - The analysis in the indifferentiability framework (please check [NI20b])

Thank you!

[NI20b] Ryota Nakamichi and Tetsu Iwata. Beyond-Birthday-Bound Secure Cryptographic Permutations from Ideal Ciphers with Long Keys. FSE 2020