# Generalized Feistel Structures Based on Tweakable Block Ciphers

Kazuki Nakaya and Tetsu Iwata

Nagoya University

FSE 2023

Beijing / Kobe

March 24, 2023

# Outline

- Introduction
- Our Contributions
- Security Proofs
- Matching Attacks
- Conclusions

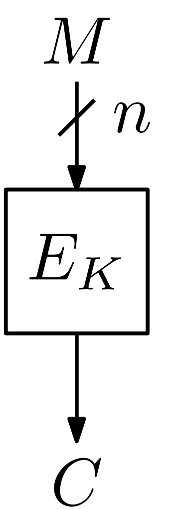
# Outline

- Introduction
- Our Contributions
- Security Proofs
- Matching Attacks
- Conclusions

# Block Ciphers

- block cipher (BC)
  - a keyed permutation $E: \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$
  - for any key $K \in \mathcal{K}$, $E_K(\cdot)$ is a permutation over $\{0,1\}^n$
  - $n$ is the block length, $n$-BC

- Construction of a secure block cipher is one of the most important problems in symmetric key cryptography.



# Secure Block Ciphers

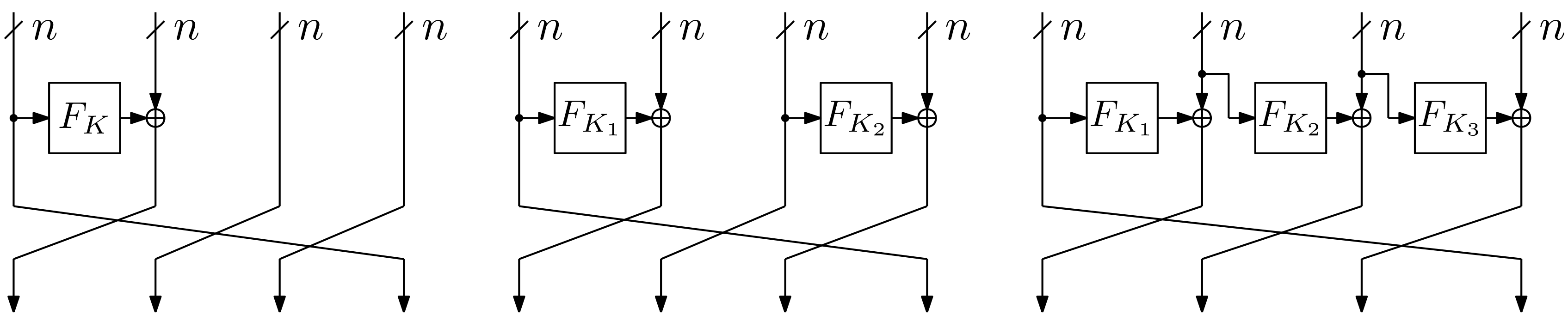
- pseudorandom permutation (PRP) [LR88]
  - real world: $E_K$, $n$-BC
  - ideal world: $\pi$, $n$-bit random permutation
  - $\mathbf{Adv}_E^{\mathrm{prp}}(\mathcal{A}) = \left|\Pr\left[\mathcal{A}^{E_K(\cdot)} = 1\right] - \Pr\left[\mathcal{A}^{\pi(\cdot)} = 1\right]\right|$
- strong pseudorandom permutation (SPRP) [LR88]
  - real world: $(E_K, E_K^{-1})$
  - ideal world: $(\pi, \pi^{-1})$
  - $\mathbf{Adv}_E^{\mathrm{sprp}}(\mathcal{A}) = \left|\Pr\left[\mathcal{A}^{E_K(\cdot), E_K^{-1}(\cdot)} = 1\right] - \Pr\left[\mathcal{A}^{\pi(\cdot), \pi^{-1}(\cdot)} = 1\right]\right|$

- Feistel structure [LR88]
  - 3-round Feistel with $n$-bit pseudorandom functions (PRFs) is a PRP
  - 4-round Feistel with $n$-bit PRFs is an SPRP

# Generalized Feistel Structures

- generalized Feistel structures (GFSs)
  - generalization of Feistel structure
  - unbalanced GFS [SK96],
    type-1, type-2, and type-3 GFSs [ZMI89], …

- type-1, type-2, type-3 GFSs [ZMI89]
  - type-1: $(2d-1)$-round is a PRP
  - type-2: $(d+1)$-round is a PRP, $(d+2)$-round is an SPRP
  - type-3: $(d+1)$-round is a PRP

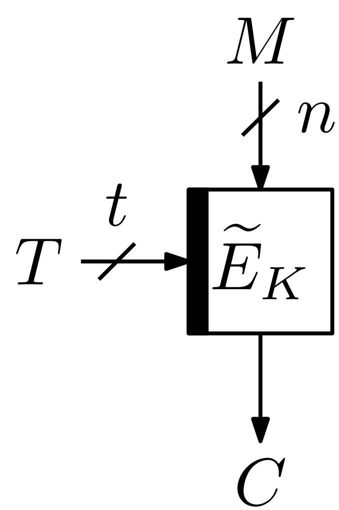



$dn$-bit type-1, type-2, type-3 GFSs $(d = 4)$

# Tweakable Block Ciphers

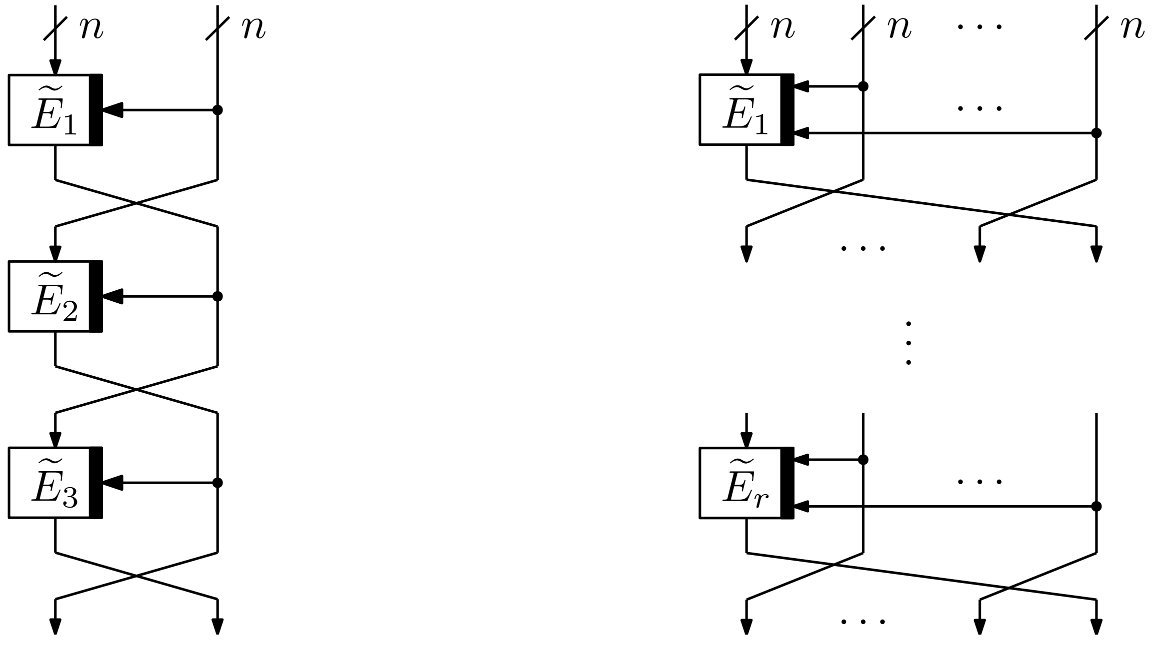
- tweakable block cipher (TBC) [LRW02, LRW11]
  - $\tilde{E}: \mathcal{K} \times \{0,1\}^t \times \{0,1\}^n \rightarrow \{0,1\}^n$
  - $T \in \{0,1\}^t$ is an additional input called a tweak
  - for any key $K \in \mathcal{K}$ and any tweak $T \in \{0,1\}^t$, $\tilde{E}_K(T,\cdot)$ is a permutation over $\{0,1\}^n$
  - $t$-bit tweak and $n$-bit block TBC, $(t,n)$-TBC

- secure TBCs from secure block ciphers [LRW02, LRW11]
- secure block ciphers from secure TBCs [Min09]



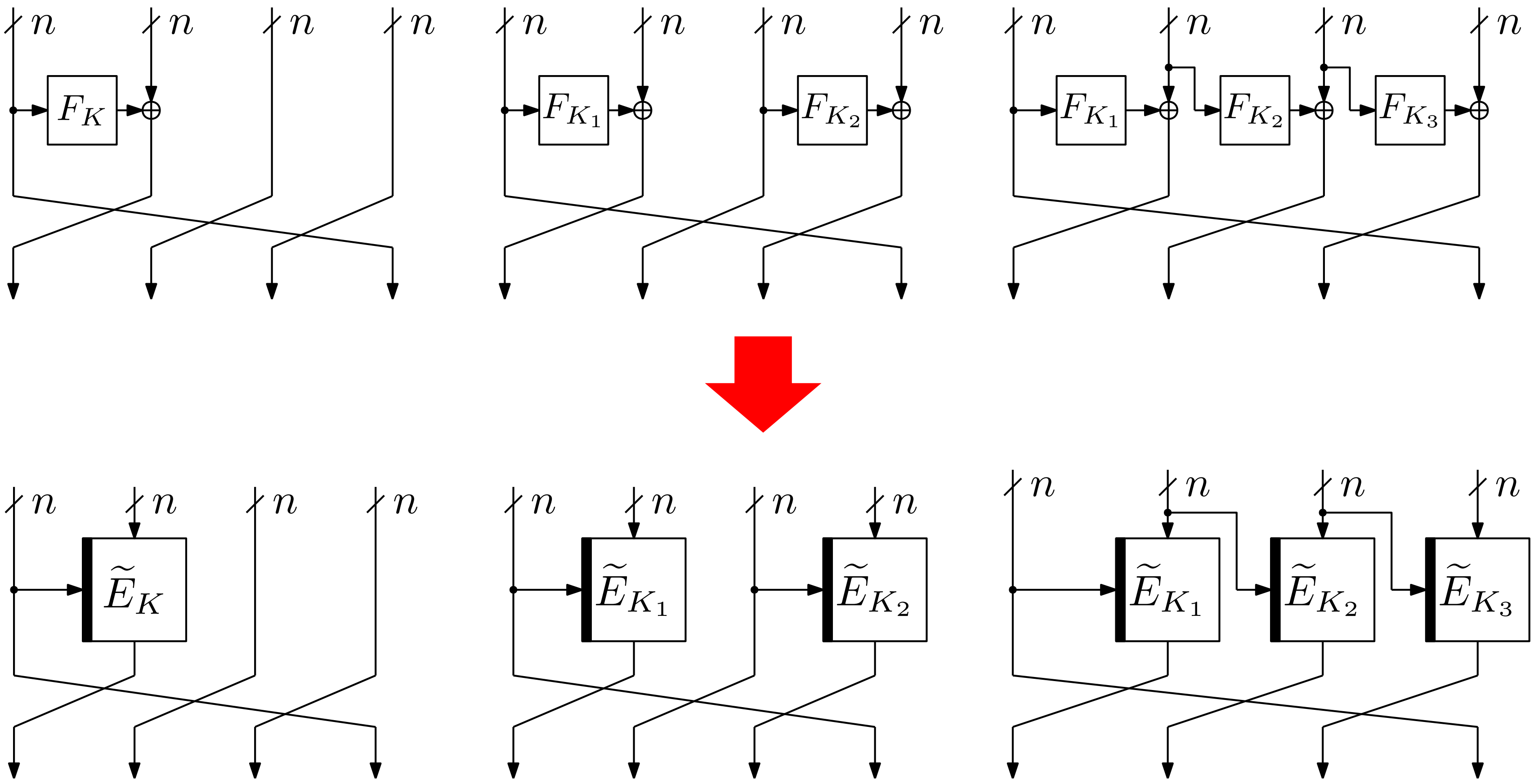
# Secure Block Ciphers from TBCs

- Coron et al. [CDMS10]
  - $2n$-BC from $(n, n)$-TBC
  - Feistel structure
- Minematsu and Nakamichi et al. [Min15,NI19]
  - $dn$-BC from $\left((d-1)n, n\right)$-TBC
  - unbalanced GFS



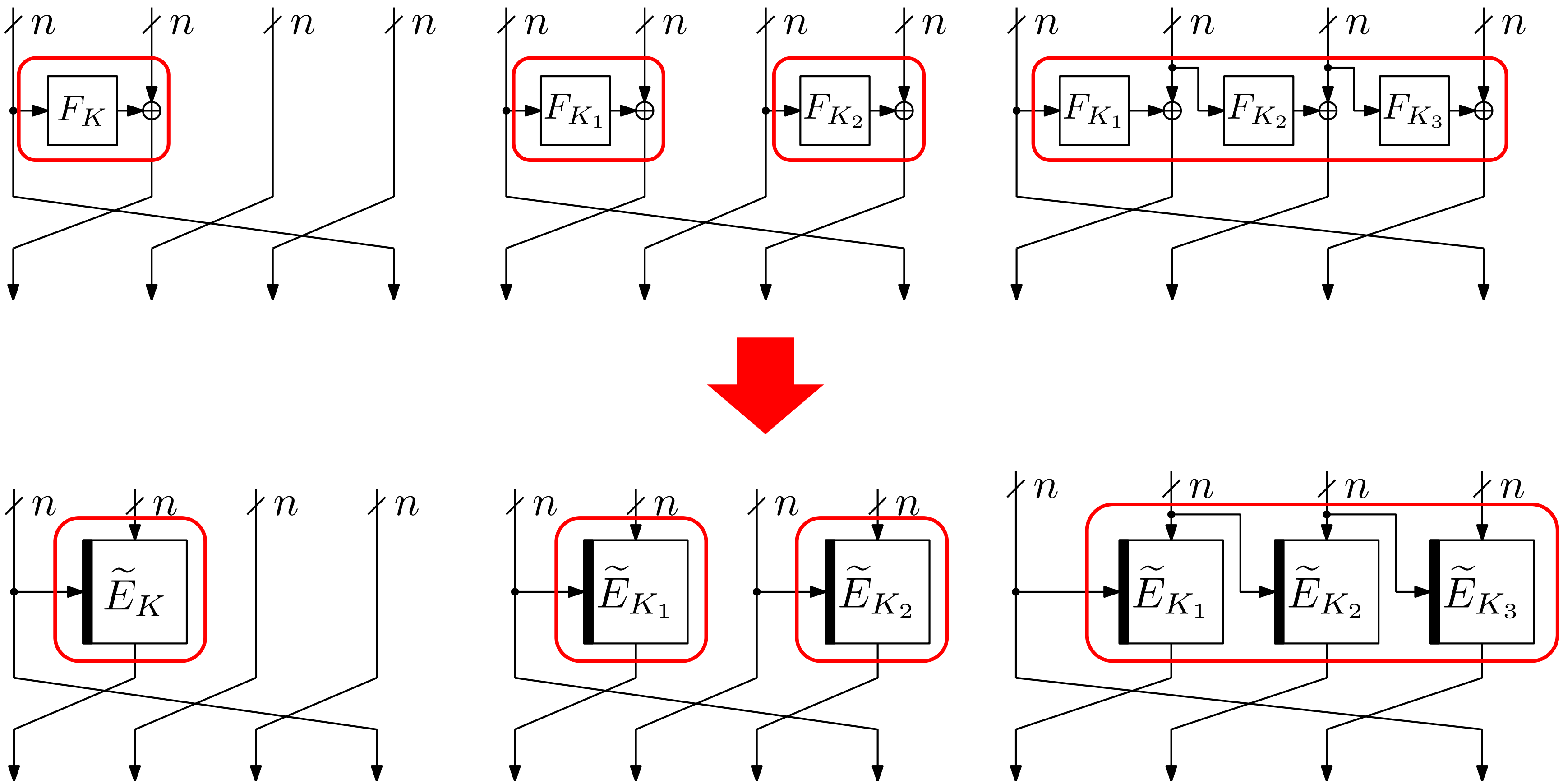
# GFSs based on TBCs

- Type-1, 2, 3 GFSs based on TBCs can naturally be defined
  - $n$-bit PRF and XOR → $(n, n)$-TBC



# GFSs based on TBCs

- Type-1, 2, 3 GFSs based on TBCs can naturally be defined
  - $n$-bit PRF and XOR → $(n, n)$-TBC



# Outline

- Introduction
- Our Contributions
- Security Proofs
- Matching Attacks
- Conclusions

# Our Contributions

| Model | Prim. | Const. | Security bound | # of rounds | Reference |
|---|---|---|---|---|---|
| PRP | TBC | Type-1 | $O(q^2/2^n)$ | $2d-2$ | This paper |
| | | | $O(q^2/2^{2n})$ | $3d-2$ | |
| SPRP | TBC | Type-1 | $O(q^2/2^n)$ | $d^2-2d+2$ | |
| | | | $O(q^2/2^{2n})$ | $d^2-d+2$ | |
| | | Type-2 | $O(q^2/2^n)$ | $d$ | |
| | | | $O(q^2/2^{2n})$ | $d+2$ | |
| | | Type-3 | $O(q^2/2^n)$ | $d$ | |
| | | | $O(q^2/2^{2n})$ | $d+1$ | |

- these primitives are $(n,n)$-TBCs, the constructions are $dn$-BCs
- $q$ is the number of queries

- We identify the number of rounds needed to achieve birthday-bound security and BBB security (with respect to $n$).
  - BBB: beyond-birthday-bound

# Our Contributions

| Model | Prim. | Const. | Security bound | # of rounds | Reference |
|---|---|---|---|---|---|
| PRP | TBC | Type-1 | $O(q^2/2^n)$ | $2d-2$ | This paper |
| | | | $O(q^2/2^{2n})$ | $3d-2$ | |
| SPRP | TBC | Type-1 | $O(q^2/2^n)$ | $d^2-2d+2$ | |
| | | | $O(q^2/2^{2n})$ | $d^2-d+2$ | |
| | | Type-2 | $O(q^2/2^n)$ | $d$ | |
| | | | $O(q^2/2^{2n})$ | $d+2$ | |
| | | Type-3 | $O(q^2/2^n)$ | $d$ | |
| | | | $O(q^2/2^{2n})$ | $d+1$ | |

- For type-1 GFS, we prove PRP and SPRP security separately
  - this construction has different security characteristics depending on the direction of the operation
- For type-2 and type-3 GFSs, we prove SPRP security

# Our Contributions

| Model | Prim. | Const. | Security bound | # of rounds | Reference |
|---|---|---|---|---|---|
| PRP | TBC | Type-1 | $O(q^2/2^n)$ | $2d-2$ | This paper |
| | | | $O(q^2/2^{2n})$ | $3d-2$ | |
| SPRP | TBC | Type-1 | $O(q^2/2^n)$ | $d^2-2d+2$ | |
| | | | $O(q^2/2^{2n})$ | $d^2-d+2$ | |
| | | Type-2 | $O(q^2/2^n)$ | $d$ | |
| | | | $O(q^2/2^{2n})$ | $d+2$ | |
| | | Type-3 | $O(q^2/2^n)$ | $d$ | |
| | | | $O(q^2/2^{2n})$ | $d+1$ | |

- We also analyse the optimality of our results with respect to the number of rounds and the attack complexity.
- We note that the constructions we consider in this paper have iterative structures

# Related Works

| Model | Prim. | Const. | Security bound | # of rounds | Reference |
|---|---|---|---|---|---|
| SPRP | PRF | Type-1 | $O\left(\frac{q^{t+1}}{2^{nt}}\right)$ | $(d^2+d-2)t+1$ | [SGW20] |
| | | Type-2 | | $2dt+1$ | |
| | | Type-3 | | $(d+2)t+1$ | |
| SPRP | PRF | Feistel | $O(q^2/2^n)$ | $4$ | [LR88] |
| | TBC | Feistel | $O(q^2/2^{2n})$ | $3$ | [CDMS10] |
| | | | $O\left(\frac{q^{(t+1)/2}}{2^{nt}}\right)$ | $4t+1$ | [SGW20] |

- in the results of [SGW20], $t \geq 1$ is a parameter that specifies the number of rounds
  - proved stronger security bounds than previous results by increasing the number of rounds

# Outline

- Introduction
- Our Contributions
- Security Proofs
- Matching Attacks
- Conclusions

# Coefficient-H Technique

- interpolation probability
  - in the real world: $\Pr[\Theta_{\mathcal{R}} = \theta]$
  - in the ideal world: $\Pr[\Theta_{\mathcal{I}} = \theta]$

- an attainable transcript:
  a transcript $\theta$ that satisfies $\Pr[\Theta_{\mathcal{I}} = \theta] > 0$

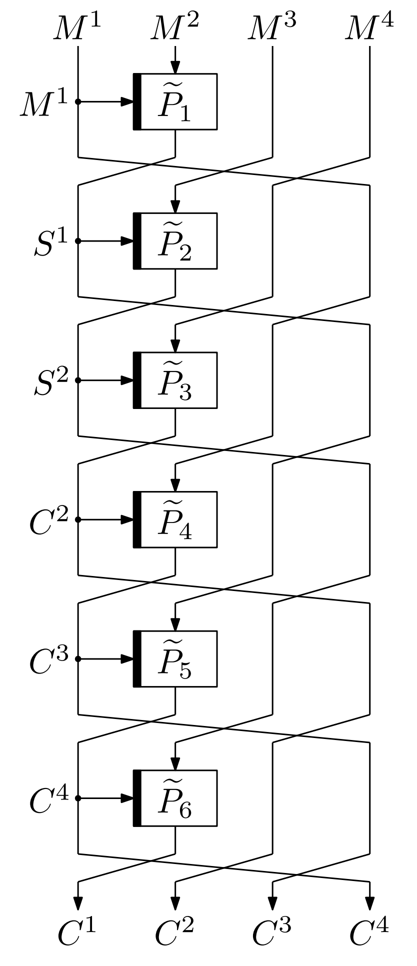
- Coefficient-H technique [Pat08, CS14]
  - partition all the attainable transcripts into $\mathrm{T}_{\mathrm{good}}$ and $\mathrm{T}_{\mathrm{bad}}$
  - assume that there exists $0 \leq \epsilon \leq 1$ such that:
    $$\forall \theta \in \mathrm{T}_{\mathrm{good}}, \qquad \frac{\Pr[\Theta_{\mathcal{R}} = \theta]}{\Pr[\Theta_{\mathcal{I}} = \theta]} \geq 1 - \epsilon$$
  - Then, $\mathbf{Adv}_{E}^{(\mathrm{model})}(\mathcal{A}) \leq \epsilon + \Pr[\Theta_{\mathcal{I}} \in \mathrm{T}_{\mathrm{bad}}]$,
    where $(\mathrm{model}) \in \{\mathrm{prp}, \mathrm{sprp}\}$ depending on the queries

- $\epsilon$ and $\Pr[\Theta_{\mathcal{I}} \in \mathrm{T}_{\mathrm{bad}}]$ depend on the definitions of the oracles and $\mathrm{T}_{\mathrm{bad}}$

# Oracle Definitions

- The real world oracle $\mathcal{R}$ : TBC-based type-1, 2, 3 GFS
  - for each query, $\mathcal{R}$ records all the internal states in $\mathcal{S}$
    $\rightarrow$ adversary $\mathcal{A}$ gets $\mathcal{S}$ after $\mathcal{A}$ makes all the queries

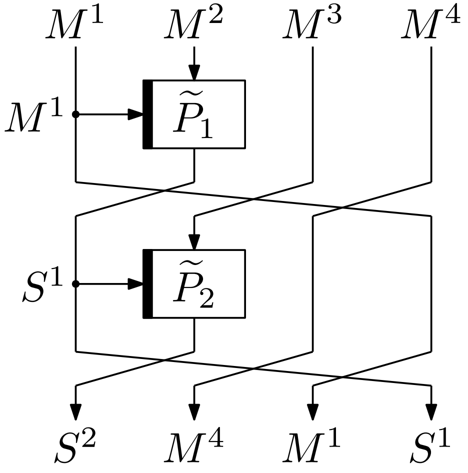
- Example: (PRP proof, birthday-bound)
  Type-1 GFS with $d = 4, r = 2d - 2 = 6$
  - computes the internal states $S^1$ and $S^2$ with $\tilde{P}_1$ and $\tilde{P}_2$
  - computes the ciphertext with $\tilde{P}_3, \ldots, \tilde{P}_6$

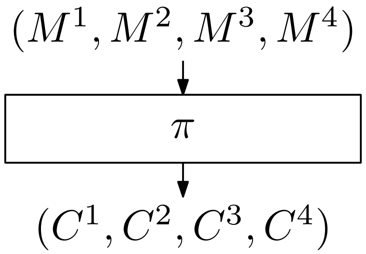


# Oracle Definitions

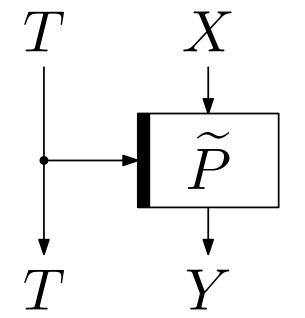
- The ideal world oracle $\mathcal{I}$ : $dn$-bit random permutation $\pi$
  - for each query, $\mathcal{I}$ uses dummy TBCs to compute dummy internal states
    (same probability distribution as in the real world)
  - adversary $\mathcal{A}$ gets $\mathcal{S}$ after $\mathcal{A}$ makes all the queries

- Example: (PRP proof, birthday-bound)
  Type-1 GFS with $d = 4, r = 2d - 2 = 6$
  - computes the internal states $S^1$ and $S^2$ with $\tilde{P}_1$ and $\tilde{P}_2$
  - computes the ciphertext with $\pi$



# Bad Transcript




◆ In the real world, for TBC $\tilde{P}$,

$$(T_i, X_i) = (T_j, X_j) \Rightarrow Y_i = Y_j$$
$$(T_i, Y_i) = (T_j, Y_j) \Rightarrow X_i = X_j$$

◆ There are conditions that can only hold in the ideal world:

$$(T_i, X_i) = (T_j, X_j) \wedge Y_i \neq Y_j$$
$$(T_i, Y_i) = (T_j, Y_j) \wedge X_i \neq X_j$$

- these conditions can hold at TBCs that are not used in the ideal world

◆ $\theta \in \mathrm{T}_{\mathrm{bad}}$ is a bad transcript if at least one of these conditions is satisfied

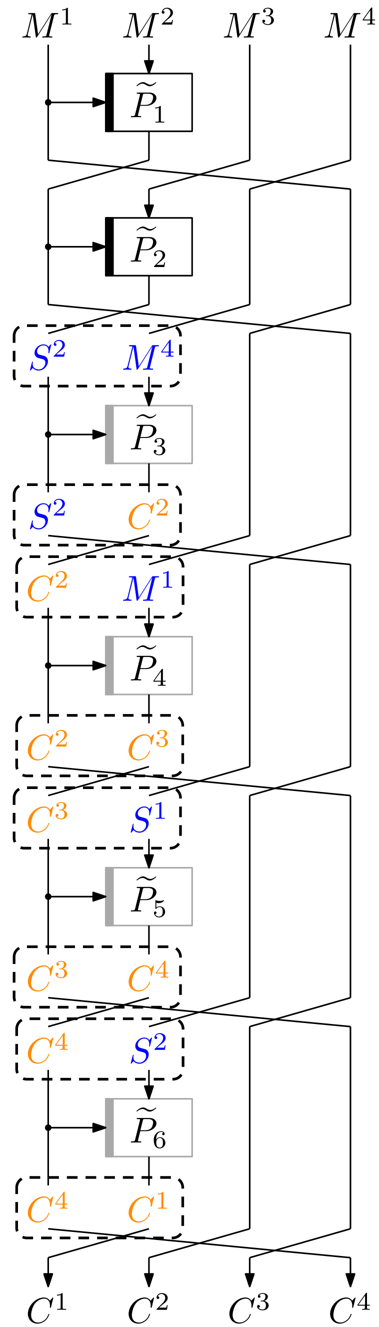
# Bad Transcript

- Example: (PRP proof, birthday-bound) Type-1 GFS with $d = 4, r = 2d - 2 = 6$

- $2n$-bit bad collisions can occur at $\tilde{P}_3, \dots, \tilde{P}_6$ that are not used in the ideal world
  - bad at $\tilde{P}_3$: $(S^2, M^4)$ and $(S^2, C^2)$
  - bad at $\tilde{P}_4$: $(C^2, M^1)$ and $(C^2, C^3)$
  - bad at $\tilde{P}_5$: $(C^3, S^1)$ and $(C^3, C^4)$
  - bad at $\tilde{P}_6$: $(C^4, S^2)$ and $(C^4, C^1)$

- We compute the probability of $\theta \in \mathrm{T}_{\mathrm{bad}}$ in the ideal world by taking summation of relevant bad probabilities.
  - For $r = 2d - 2$,

$$\Pr[\Theta_{\mathcal{J}} \in \mathrm{T}_{\mathrm{bad}}] \leq \frac{(d-1)q^2}{2^n} + \frac{0.5(d-1)q^2}{2^{2n}}$$



# Outline

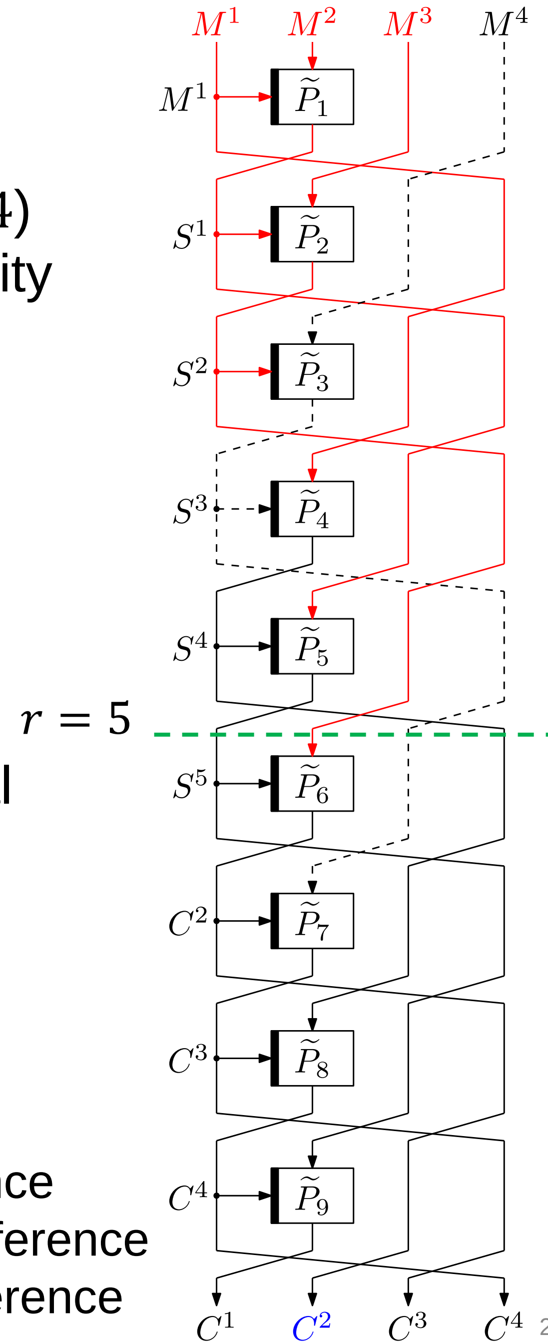
- Introduction
- Our Contributions
- Security Proofs
- Matching Attacks
- Conclusions

# Matching Attacks

- Example: CPA against Type-1 GFS ($d = 4$)
  - $r = 2d - 2 = 6$: birthday-bound security
  - $r = 3d - 2 = 10$: BBB security

- In the case $r < 6$:
  in the real world, a zero difference always exists in a ciphertext block
  $\Rightarrow$ distinguishable with 2 queries

  - implying that $r = 2d - 2$ is the optimal number of rounds for birthday-bound security



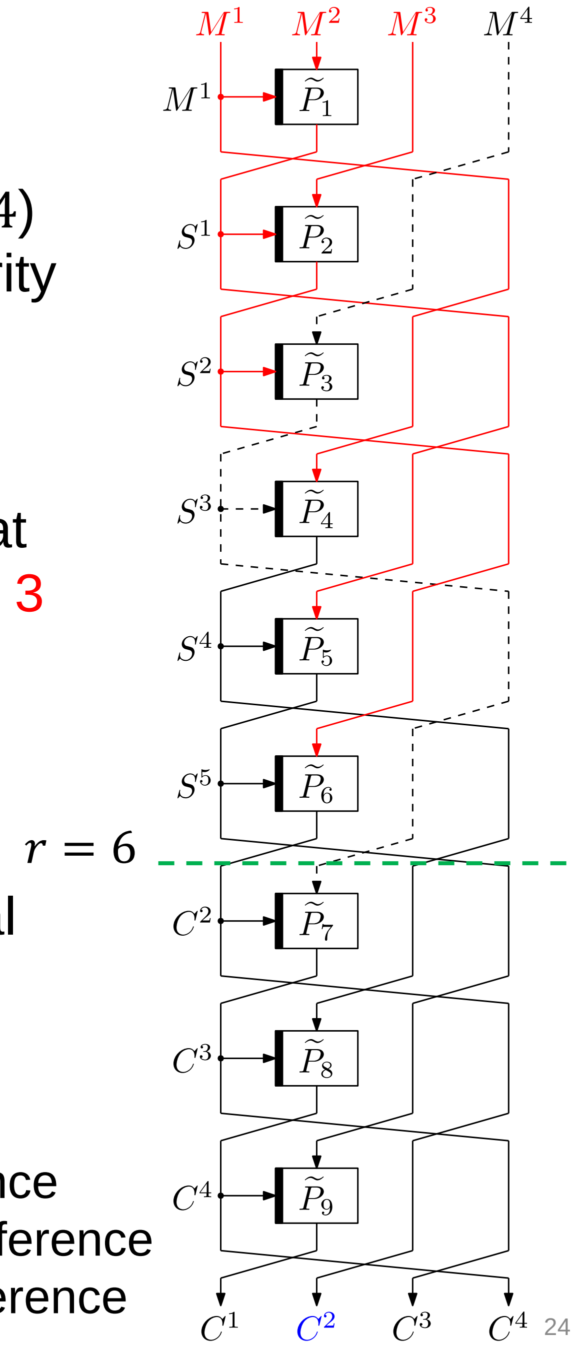

red: zero difference
dashed: non-zero difference
black: random difference

# Matching Attacks

- Example: CPA against Type-1 GFS ($d = 4$)
  - $r = 2d - 2 = 6$: birthday-bound security
  - $r = 3d - 2 = 10$: BBB security

- In the case $6 \leq r < 10$:
  in the real world, the collision probability at ciphertext block ($C^2$ in the figure) is about 3 times larger than in the ideal world (collision at $S^4$ or $S^5$ or $C^2$)
  ⇒ distinguishable with $2^{n/2}$ queries

  - implying that $r = 3d - 2$ is the optimal number of rounds for BBB security




red: zero difference
dashed: non-zero difference
black: random difference

# Outline

- Introduction
- Our Contributions
- Security Proofs
- Matching Attacks
- Conclusions

# Conclusions

- We formalized TBC-based type-1, type-2, and type-3 GFSs, and presented their provable security.
  - We identified the number of rounds to achieve birthday-bound security and BBB security.
- We also presented attacks to show the optimality of our results with respect to the number of rounds and attack complexity.
- Open questions
  - We do not know if an attack with $q = O(2^n)$ complexity exists when $r$ is larger than or equal to that for BBB security
  - stronger security bounds by increasing the number of rounds
  - indifferentiability of TBC-based GFSs

# References


- [LR88]: Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Comput., 17(2):373–386, 1988.

- [SK96]: Bruce Schneier and John Kelsey. Unbalanced feistel networks and block cipher design. In FSE ’96, volume 1039 of LNCS, pages 121–144. Springer, 1996.

- [ZMI89]: Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In CRYPTO ’89, volume 435 of LNCS, pages 461–480. Springer, 1989.

- [LRW02]: Moses D. Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable block ciphers. In CRYPTO 2002, volume 2442 of LNCS, pages 31–46. Springer, 2002.

- [LRW11]: Moses D. Liskov, Ronald L. Rivest, and David A.Wagner. Tweakable block ciphers. J. Cryptol., 24(3):588–613, 2011.

- [Min09]: Kazuhiko Minematsu. Beyond-birthdaybound security based on tweakable block cipher. In FSE 2009, volume 5665 of LNCS, pages 308–326. Springer, 2009.

# References


- [CDMS10]: Jean-Sébastien Coron, Yevgeniy Dodis, Avradip Mandal, and Yannick Seurin. A domain extender for the ideal cipher. In TCC 2010, volume 5978 of LNCS, pages 273–289. Springer, 2010.
- [Min15]: Kazuhiko Minematsu. Building blockcipher from small-block tweakable blockcipher. Des. Codes Cryptogr., 74(3):645–663, 2015.
- [NI19]: Ryota Nakamichi and Tetsu Iwata. Iterative block ciphers from tweakable block ciphers with long tweaks. IACR Trans. Symmetric Cryptol., 2019(4):54–80, 2019.
- [SGW20]: Yaobin Shen, Chun Guo, and Lei Wang. Improved security bounds for generalized feistel networks. IACR Trans. Symmetric Cryptol., 2020(1):425–457, 2020.
- [Pat08]: Jacques Patarin. The ”Coefficients H” technique. In SAC 2008, volume 5381 of LNCS, pages 328–345. Springer, 2008.
- [CS14]: Shan Chen and John P. Steinberger. Tight security bounds for key-alternating ciphers. In EUROCRYPT 2014, volume 8441 of LNCS, pages 327–350. Springer, 2014.

# Outline

- Introduction
- Our Contributions
- Security Proofs
- Matching Attacks
- Conclusions
- Appendix

# TBC calls for TBC-based GFSs

| | | The number of TBC calls | | # of parallel TBCs | |
|---|---|---|---|---|---|
| Const. | Model | for $r = r_{\mathrm{bb}}$ | for $r = r_{\mathrm{bbb}}$ | encryption | decryption |
| Type-1 | PRP | $2d - 2$ | $3d - 2$ | 1 | $d - 1$ |
| | SPRP | $d^2 - 2d + 2$ | $d^2 - d + 2$ | | |
| Type-2 | SPRP | $d^2/2$ | $d^2/2 + d$ | $d/2$ | $d/2$ |
| Type-3 | SPRP | $d^2 - d$ | $d^2 - 1$ | $d - 1$ | 1 |

- $r_{\mathrm{bb}}$ ($r_{\mathrm{bbb}}$): the number of rounds for birthday-bound security (BBB security)
- # of parallel TBCs: the number of TBCs that can be processed in parallel

- Example: when $r = r_{\mathrm{bb}}$ (SPRP),
  - if $d = 4$, # of TBC calls for Type-1 / 2 / 3 is 10 / 8 / 12
  - if $d = 8$, # of TBC calls for Type-1 / 2 / 3 is 50 / 32 / 56

    ⇒ Type-2 GFS has the smallest number of TBC calls