Recovery-Key Attacks against TMN-family Framework for Mobile Wireless Networks

Tran Song Dat Phuc, Yong-Hyeon Shin*, and Changhoon Lee
Department of Computer Science and Engineering, Seoul National University of Science and Technology, Gongneung-ro, Nowon-gu, Seoul, 139-743, South Korea
[e-mail: datphuc_89@yahoo.com**,** yshin@seoultech.ac.kr, chlee@seoultech.ac.kr**]**
*Corresponding author: Yong-Hyeon Shin

Received Decebmer 15, 2020; revised February 25, 2021; accepted March 31, 2021; published June 30, 2021

Abstract

The proliferation of the Internet of Things (IoT) technologies and applications, especially the rapid rise in the use of mobile devices, from individuals to organizations, has led to the fundamental role of secure wireless networks in all aspects of services that presented with many opportunities and challenges. To ensure the CIA (confidentiality, integrity and accessibility) security model of the networks security and high efficiency of performance results in various resource-constrained applications and environments of the IoT platform, DDO-(data-driven operation) based constructions have been introduced as a primitive design that meet the demand of high speed encryption systems. Among of them, the TMN-family ciphers which were proposed by Tuan P.M., Do Thi B., etc., in 2016, are entirely suitable approaches for various communication applications of wireless mobile networks (WMNs) and advanced wireless sensor networks (WSNs) with high flexibility, applicability and mobility shown in two different algorithm selections, TMN64 and TMN128. The two ciphers provide strong security against known cryptanalysis, such as linear attacks and differential attacks. In this study, we demonstrate new probability results on the security of the two TMN construction versions – TMN64 and TMN128, by proposing efficient related-key recovery attacks. The high probability characteristics (DCs) are constructed under the related-key differential properties on a full number of function rounds of TMN64 and TMN128, as 10-rounds and 12-rounds, respectively. Hence, the amplified boomerang attacks can be applied to break these two ciphers with appropriate complexity of data and time consumptions. The work is expected to be extended and improved with the latest BCT technique for better cryptanalytic results in further research.

Keywords: Industrial IoT, TMN64, TMN128, Related-key Recovery Attack, Controlled Substitution-Permutation Network (CSPN), Data-dependent Operations (DDOs).

http://doi.org/10.3837/tiis.2021.06.012 **ISSN : 1976-7277**

1. Introduction

The explosion of mobile devices and services, as smart phones and tablets becoming an essential part of modern society, along with the rapid development and spread of the IoT technologies, is leading to the significant challenges of secure and trustworthy service composition that requires the balance the inherent tension between security and accessibility of wireless technologies and networks employed in the constrained IoT environments. In the context of unreliable constrained wireless networks for IoT networks, the specific secure requirements and needs of these networks are needed as not only dealing with the unauthorized access to systems and data, but also ensuring the suitability, mobility and applicability on both software and hardware performances when operating and integrating in such environments.

With the limitations about the processing capacity and resources, the deployment results seem not suitable for the constrained IoT environments in handling with both secure high-speed encryption and high efficiency in hardware integration. To address those issues, the prominent solution focuses on improving the protection of cipher designs by distinct switch operations and functions, like the Data-Dependent Permutation-based constructions (such as CIKS-1 [18], SCO-family [7] and Cobra-family [19] [20]), the Data-Dependent Operation-based constructions (such as CIKS-128 [8], CIKS-128H [13], MD-64 [5] and DDO-64 [14]) and the Switchable Data-Dependent Operation-based constructions (such as BMD-128 [4], XO-64 [6], BM123-64 [2]). However, the fact is, for as long as there have been wireless communication networks, there have been fatal weaknesses that were still vulnerable to well-known related attacks. One of them, simple key scheduling generator in the cipher structures for high speed transformation and lightweight targets gives cryptanalytic possibility for attackers to exploit these mechanisms by applying common related-key differential attack methods.

TMN block cipher [1] is kind of DDO-based construction proposed by Tuan P.M., Do Thi B., etc., in 2016. It has two different versions: TMN64 with 64-bits block size, covering 128-bits key size and total 10 function rounds; and TMN128 with block size of 128-bits, having 256-bits secret key size and 12 function rounds in total. These are designed in combination of new concept in functions and attributes of the data-dependent operations (DDOs) and the Controlled Substitution-Permutation Network (CSPN) frameworks [13]. Hence, the two ciphers are regarded as an effective solution with more adjustable and desirable approach for fitting targets of application and system with particular fixed designs. In the designs, the authors showed high suitability, applicability in characteristics of various other algorithms for specific high-speed networks targets, as well as high authenticity of protecting against types of popular cryptanalysis, such as differential and linear attacks, by using the improvement of on-the-fly round key generator.

1.1 Related Study

Related-key differential amplified boomerang attack was evolved by Kelsey et al. [16], which is a pure adaptive chosen-plaintext attack and is an upgrade model of the related-key boomerang attack developed by Wagner, 1999 [17] and Biham et al., 2005 [15]. Particularly, the attack had become effective cryptanalysis technique applying for various cipher mechanisms since the target aims to exploit two distinctive related-key differential characteristics for finding right quartets with high probability. Some of the previous cryptanalysis that used this attack scenario on DDO-based ciphers had given high efficiency

and high probability in cryptanalytic results, like on BMD-128 [9], XO-64 [10], DDO-64 [11], MD-64 [12], and BM123-64 [3].

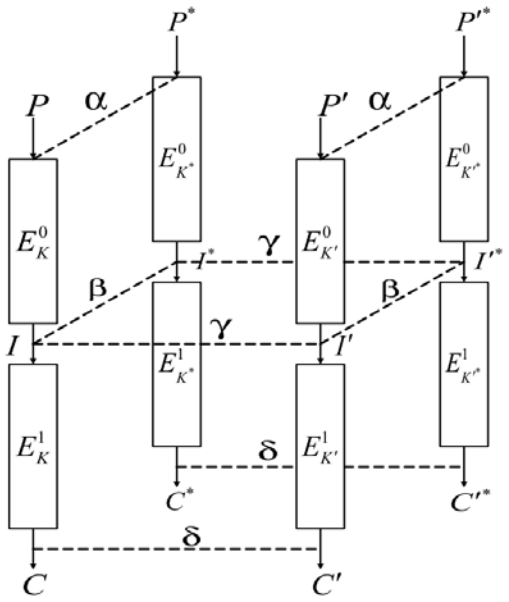


Fig. 1. The related-key boomerang characteristics.

In the model of related-key boomerang attack, the cipher E is divided into two sub-ciphers, depicted as $E = E^1 \circ E^0$. In addition, for E^0 and E^1, the related-key differentials are integrated into an adaptive chosen-plaintext and chosen-ciphertext characteristics of the cipher E, as the characteristics based on the encryption/ decryption process covering the related keys.

We suppose that $\alpha \rightarrow \beta$ is a related-key differential for E^0 with probability p using key difference ΔK, and $\delta \rightarrow \gamma$ is another related-key differential for E^1 with probability q using key difference $\Delta K'$. With the related keys K, K^*, K', K'^* where $\Delta K = K \oplus K^*$ and $\Delta K' = K' \oplus K'^*$, we can execute the attack as follows.

(1) Pick up two random plaintexts P and P', and then assign $P^* = P \oplus \alpha$, $P'^* = P' \oplus \alpha$ to get the quartet of plaintext (P, P^*, P', P'^*).

(2) Gain the matching quartet of ciphertext (C, C^*, C', C'^*), as $C = E_K(P)$, $C^* = E_{K^*}(P^*)$, $C' = E_{K'}(P')$ and $C'^* = E_{K'^*}(P'^*)$, using the secret key differences, as $\Delta K = K \oplus K^* = K' \oplus K'^*$ and $\Delta K' = K \oplus K' = K^* \oplus K'^*$.

(3) Examine whether $C \oplus C' = C^* \oplus C'^* = \delta$ or not.

If the quartet of plaintext (P, P^*, P', P'^*) progresses through **Stage 3**, we output it as a correct quartet in the model of related-key amplified boomerang attack.

The correct plaintext quartets must satisfy the following conditions:

(a) $P \oplus P^* = P' \oplus P'^* = \alpha$

(b) $I \oplus I^* = I' \oplus I'^* = \beta$

(c) $I \oplus I' = \gamma$

(d) $C \oplus C' = C^* \oplus C'^* = \delta$.

while I and I' is the intermediate encryption values after E^0.

We choose m_1 and m_2 are number of pairs of (P, P^*) and number of pairs of (P', P'^*), respectively, with difference α. As we also suppose that $\alpha \rightarrow \beta$ is the first related-key differential for E^0 under the probability of p using the key difference ΔK, and $\delta \rightarrow \gamma$ is the second related-key differential for E^1 under the probability of q using the key difference $\Delta K'$, there exists the number of pairs ($m_1 \cdot p$) and ($m_2 \cdot p$) fulfill the first related-key differential $\alpha \rightarrow \beta$ for E^0 using the key difference ΔK. Then, the quartets meet the conditions **(a)** and **(b)** are about $m_1 \cdot m_2 \cdot p^2$. Similarly, if we obtain $I \oplus I' = \gamma$ under the probability of 2^{-n} in all possible values, we get $m_1 \cdot m_2 \cdot 2^{-n} \cdot p^2$ quartets meet the requirements of **(a)**, **(b)** and **(c)**. And the related-key differential boomerang characteristic can differentiate a cipher E from a perfect cipher if the probability $p \cdot q > 2^{-n/2}$, when the supposed number of correct quartets is approximately $m_1 \cdot m_2 \cdot 2^{-n} \cdot p^2 \cdot q^2$.

1.2 Research Contributions

In this paper, we demonstrate the related-key recovery attacks on the two variants of TMN constructions, TMN64 and TMN128. The attack, by obtaining the two related-key boomerang distinguishers with high probabilities in distinct designs, can exploit a full 10-rounds and 12-rounds of TMN64 and TMN128, respectively with highly favorable cryptanalytic results. The proposed amplified boomerang attacks require about 2^{47} in complexity of data, memory bytes of 2^{50} and complexity of time using 2^{65} encryptions for the TMN64 design; and about 2^{69} complexity of data, memory bytes of 2^{72} and complexity of time using 2^{129} encryptions for TMN128 model of TMN schemes. These cryptanalytic results are the first security results on the two variants of the TMN-family so far. In this way, we prove that the TMN-family constructions, like other previous research of DDP-based or DDO-based schemes, are still vulnerable and being insecure against related-key differential cryptanalysis. The assurance of the security on these types of cipher constructions remains unclear and should be designed with a better security primitive approach.

Block cipher	Number of Rounds	Complexity of Data/ Time
TMN-64	10 / 10	2^{47} RK-CP/ 2^{65}
TMN-128	12 / 12	2^{69} RK-CP/ 2^{129}

* RK-CP: Related-Key Chosen-Plaintext

The remainder of this paper is structured as follows; the two TMN-family constructions, TMN64 and TMN128, are described in Section 2. In Section 3, we define the related-key boomerang differential properties in each round function of these two designs based on the controlled element CE $F_{2/2}$ that allows us to build the high probability of differential characteristics (DCs) presented in Section 4. Then, the recovery attacks on the TMN64 and TMN128 ciphers are proposed with the analysis methods and complexity assessments shown in Section 5. Lastly, in Section 6, we give the conclusion of all our study.

2. TMN64, TMN128 Block Ciphers Description

2.1 Preliminaries

Some notations are concisely described in this section that they are used throughout the paper. As c_1 denotes the MSB (the most significant bit) and c_n denotes the LSB (the least significant bit), a cipher C can be defined as $C = (c_1, c_2, \ldots, c_n)$.

The related-key differential characteristics applied to the amplified boomerang attack methods are combining with related differential components of block ciphers, like the input, the output, and the key of a round function.

- r : round function of a block cipher.
- $\Delta \boldsymbol{Q}_r$, $\Delta \boldsymbol{Q}_r$: round key difference values for each round r.
- $\Delta \boldsymbol{X}_r$ / $\Delta \boldsymbol{Y}_r$: input / output difference values for each round r.
- $e_{i,j}$: binary data bit adjusting for a round r, as the active bit values i and j; at the i^{th} and j^{th} positions, the bit value are '1', and the others are '0s' for each block data.

(e.g., $e_{3,5}$ = (0, 0, 1, 0, 1,…, 0)).

- $\oplus$: bitwise XOR operation.
- $\lll$, $\ggg$: bitwise left, right rotation.

2.2 TMN64, TMN128 Constructions

TMN64, TMN128 [1] are designed as DDO-based block cipher mechanisms with different data block sizes, 64-bits and 128-bits under 128-bits and 256-bits secret keys, respectively. Totally, it covers 10 rounds function for TMN64 and 12 rounds function for TMN128. A round function $\mathbf{Crypt}^{(e)}$ for each construction will do same switchable data operations from the 1st round to the last round (the FT function) for yielding the appropriate ciphertext as output.

The round function $\mathbf{Crypt}^{(e)}$ of TMN64, TMN128 is based on the controlled substitution permutation networks (**CSPN**s), an extension function **E**, two specified permutations (I_1 and I_2) and DDO-based functions $F_{n/m}^{V/e}$ ($F_{32/384}$, $F^{-1}{}_{32/384}$, $F_{64/768}$, $F^{-1}{}_{64/768}$) including basic controlled element function $F_{2/2}$.

The encryption algorithm of TMN128 can be define as:

1. Input with 128-bit block size as plaintext is divided into two sub-blocks A and B, with 64-bits for each block.

2. From the 1st round to the 11th round (as r = 1 to 11), for each round r, execute identical operations:

$(A, B) = \mathbf{Crypt}^{(0)} (A, B, Q_r , Q_r)$

$(A, B) = (B, A)$

3. Generate the 12th round (last round) integrating with the FT (final transformation):

$(A, B) = \mathbf{Crypt}^{(0)} (A, B, Q_{12}, Q_{12})$

$(A, B) = (L \oplus Q_{FT}, R \oplus Q_{FT})$

$(A, B) = (A, B)$.

Fig. 2 and **Fig. 3** illustrates the round function $\mathbf{Crypt}^{(0)}$ of TMN64 and TMN128 in details.

Refer to [1] for more description of the TMN64 and TMN128 constructions.

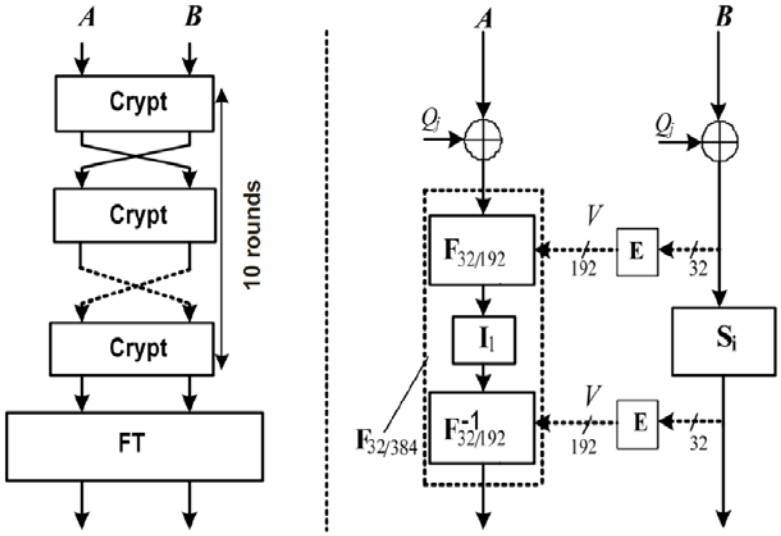


Fig. 2. The overall construction and the **Crypt**$^{(0)}$ of TMN64.

The DDO functions $F_{n/m}^{V/e}$: $F_{32/384}$, $F^{-1}{}_{32/384}$, $F_{64/768}$, and $F^{-1}{}_{64/768}$ are built based on CE $F_{2/2}$, as $F_{2/2}$ is defined by $((x_1, x_2), [v, z] / (y_1, y_2))$ (see **Fig. 4**). As the authors of TMN ciphers did not mention clearly about the way of executing $F_{2/2}$, we can refer it as same previous DDO-based schemes using for the high-speed wireless communication networks.

$$y_1 = vz \oplus vzx_1 \oplus zx_1 \oplus zx_2 \oplus x_1 \oplus v \oplus 1$$
$$y_2 = zx_1 \oplus vzx_2 \oplus z \oplus vx_1 \oplus zx_2 \oplus vz \oplus v \oplus x_2 \oplus 1$$
$$y_3 = x_1 \oplus vzx_2 \oplus vx_1 \oplus x_2 \oplus vzx_1 \oplus z.$$

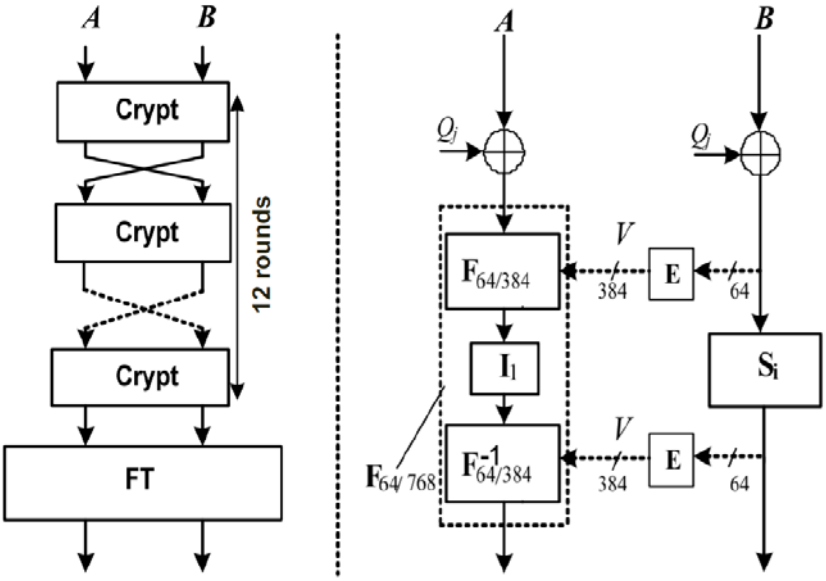
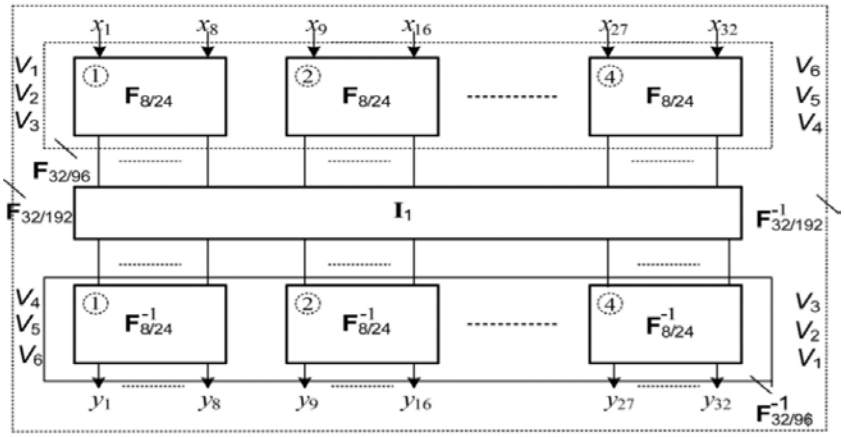


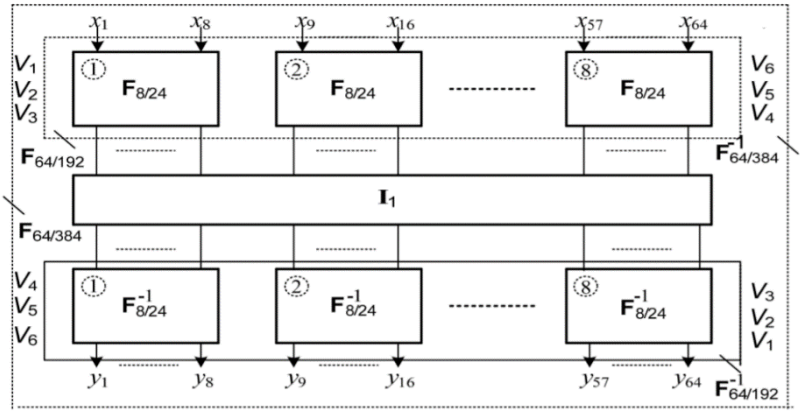
Fig. 3. The overall construction and Round function **Crypt**$^{(0)}$ of TMN128.

The extension function **E** does output controlling vector as $(V, Z) = (V_1, V_2, V_3, V_4, V_5, V_6, Z_1, Z_2, Z_3, Z_4, Z_5, Z_6)$, taking a 32-bits input X then produce 192-bits output Y for TMN64, and 64-bits input X then produce 384-bits output Y for TMN128.

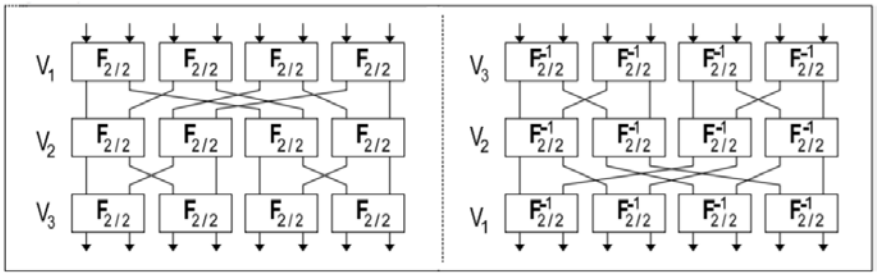
The fixed permutations are used at the right branch between two DDO operations $F_{n/m}^{V/e}$ and at the left branch of the hybrid CSPNs S_i (see **Fig. 5** and **Fig. 6**) within the two structures.



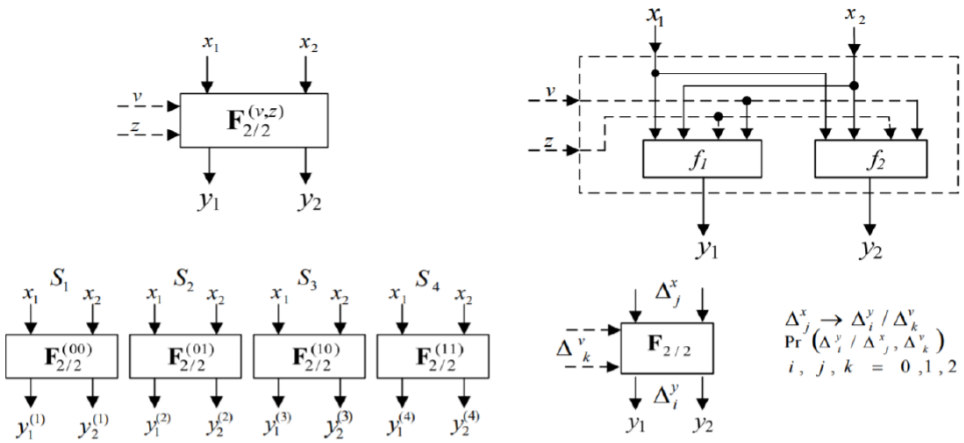
(a)



(b)



(c)



(d)

Fig. 4. DDO-based functions **(a)** $F_{32/192}$, $F^{-1}{}_{32/192}$; (**b**) $F_{64/384}$, $F^{-1}{}_{64/384}$; (**c**) $F_{8/24}$, $F^{-1}{}_{8/24}$ and (**d**) CE $F_{2/2}$.

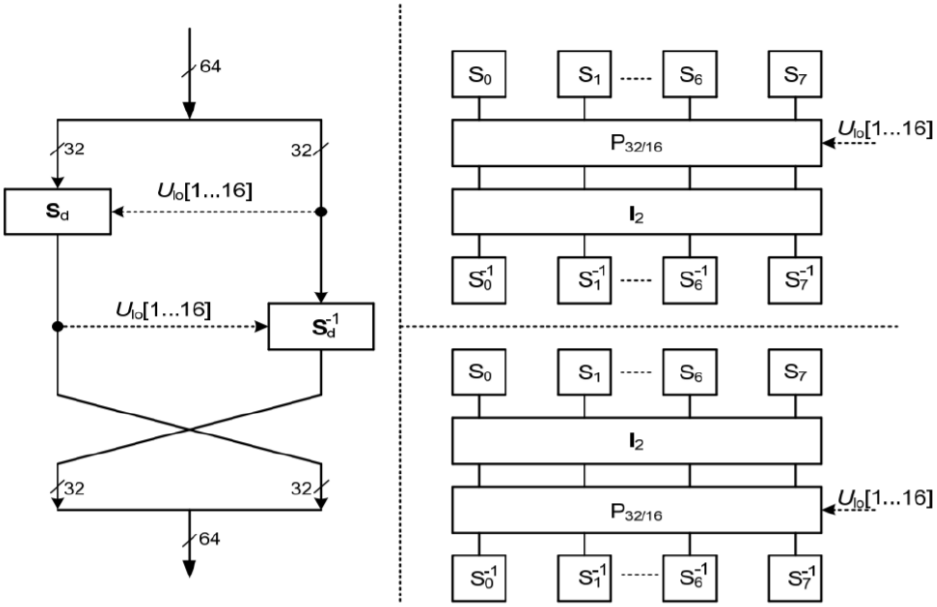


Fig. 5. CSPNs S_i, S_d and $S^{-1}{}_d$.

S-box	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
S_1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
S_2	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
S_3	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
S_4	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
S_5	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
S_7	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
S_0^{-1}	14	3	4	8	1	12	10	15	7	13	9	6	11	2	0	5
S_1^{-1}	9	10	5	0	2	15	12	3	6	13	11	14	8	1	7	4
S_2^{-1}	1	8	14	5	13	7	4	11	15	2	0	12	10	9	3	6
S_3^{-1}	12	0	15	5	1	13	10	6	11	14	8	2	4	3	7	9
S_4^{-1}	3	9	13	10	15	12	1	6	14	2	0	15	4	7	11	8
S_5^{-1}	10	4	6	15	13	14	8	3	1	11	12	0	2	7	5	9
S_6^{-1}	12	9	3	14	2	7	8	4	15	6	0	13	5	10	11	1
S_7^{-1}	12	0	15	5	7	9	10	6	3	14	4	11	8	2	13	1

Fig. 6. Different 4×4 bit S-boxes.

The extension boxes **E(X)** of TMN-64 and TMN-128.

TMN-64	
I_1	(1)(2,9)(3,17)(4,25)(5)(6,13)(7,21)(8,29)(10)(11,18)(12,26)(14)(15,22)(16,30)(19)(20,27)(23)(24,31)(28)(32)
I_2	(1)(2,5)(3,9)(4,13)(6)(7,10)(8,14)(11)(12,15)(16)
E(X)	$(X, X^{<<<6}, X^{<<<12}, X^{<<<18}, X^{<<<24}, X^{<<<30})$

TMN-128	
I_1	(1)(2,9)(3,17)(4,25)(5,33)(6,41)(7,49)(8,57)(10)(11,18)(12,26)(13,34)(14,42)(15,50)(16,58)(19)(20,27)(21,35)(22,43)(23,51)(24,59)(28)(29,36)(30,44)(31,52)(32,60)(37)(38,45)(39,53)(40,61)(46)(47,54)(48,62)(55)(56,63)(64)
I_2	(1)(2,9)(3,17)(4,25)(5)(6,13)(7,21)(8,29)(10)(11,18)(12,26)(14)(15,22)(16,30)(19)(20,27)(23)(24,31)(28)(32)
E(X)	$(X, X^{<<<12}, X^{<<<24}, X^{<<<36}, X^{<<<48}, X^{<<<60})$

The secret key scheduling is improved to deal with the weaknesses of simple weak key genegator in most DDP-based constructions, by using a on-the-fly expansion round key. The target of this function is creating the key for the next round while implementing encryption (or decryption) at same time.

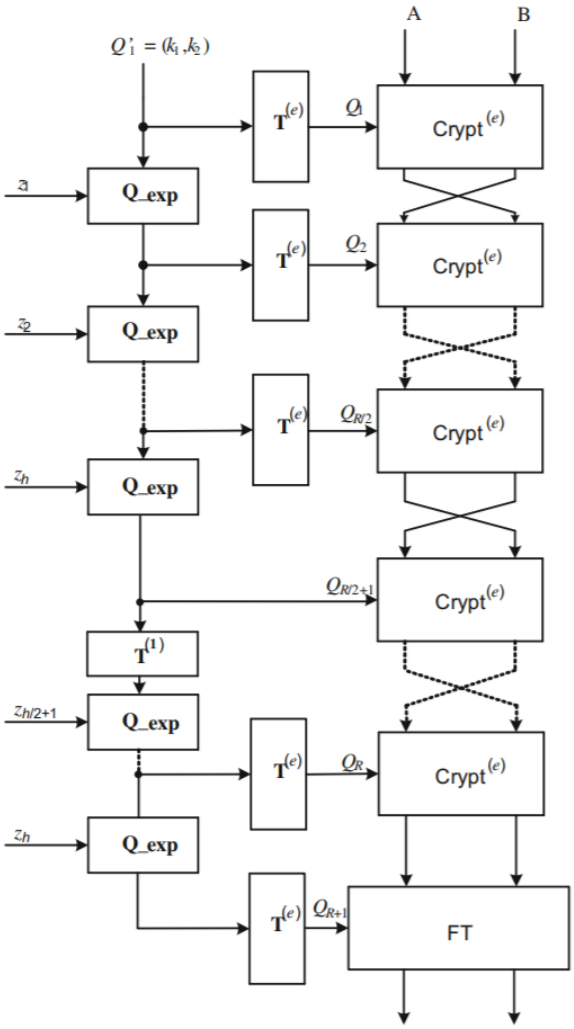


Fig. 7. On-the-fly secret round key expansion procedure.

3. Differential Properties of TMN64, TMN128

This section presents the differential properties of DDO operations in **Crypt**$^{(0)}$ round function of the two ciphers TMN64 and TMN128, based on the differential properties of CE $F_{2/2}$. These properties enable us to construct effective differential boomerang characteristics later.

3.1 Differential Properties of CE $F_{2/2}$

We assume that x_1 and x_2 are two input values and a (v, z) pair is a controlling vector of controlled element $F_{2/2}$. So, the CE $F_{2/2}$ can be depicted as $F_{2/2}(x_1, x_2, v, z)$. According to the differential distribution put in to definitions of CE $F_{2/2}$ in TMN structures, we can obtain differential properties as:

$$y_1 = vz \oplus vzx_1 \oplus zx_1 \oplus zx_2 \oplus x_1 \oplus v \oplus 1$$

$$y_2 = zx_1 \oplus vzx_2 \oplus z \oplus vx_1 \oplus zx_2 \oplus vz \oplus v \oplus x_2 \oplus 1$$

$$\Pr\left[F_{2/2}(x_1, x_2, v, z) \oplus F_{2/2}(x_1 \oplus 1, x_2, v, z) = (1, 0)\right] = 2^{-2}.$$

It means, for the difference $(x_1 \oplus 1, 0)$ of the input and the (0, 0) difference of the controlling vector, we can gain the probability of 2^{-2} with the output difference of (1, 0). This differential property can be found as same distribution with other DDO-based cipher mechanisms.

3.2 Differential Properties of TMN64 and TMN128

Applying the same method, we can distribute differential properties of DDO operations: $F_{32/192}$, $F^{-1}_{32/192}$, $F_{64/384}$ and $F^{-1}_{64/384}$. We mark X as input value and (V, Z) pair as controlling vector, and since for each TMN64 and TMN128 structure has same 3 active layers $F_{2/2}$ (within $F_{8/24}$ and $F^{-1}_{8/24}$ functions), then we have the differential properties as following:

$$\Pr\left[F_{32/192}(X, V, Z) \oplus F_{32/192}(X \oplus e_{32}, V, Z) = e_{32}\right] = 2^{-6}$$

$$\Pr\left[F^{-1}_{32/192}(X, V, Z) \oplus F^{-1}_{32/192}(X \oplus e_{32}, V, Z) = e_{32}\right] = 2^{-6}$$

$$\Pr\left[F_{64/384}(X, V, Z) \oplus F_{64/384}(X \oplus e_{64}, V, Z) = e_{64}\right] = 2^{-6}$$

$$\Pr\left[F^{-1}_{64/384}(X, V, Z) \oplus F^{-1}_{64/384}(X \oplus e_{64}, V, Z) = e_{64}\right] = 2^{-6}.$$

4. Related-key Amplified Boomerang Characteristics of TMN64, TMN128

In this section, we indicate the way of establishing the related-key differential boomerang characteristics with high probability based on the differential properties we explored before on full 10-rounds and 12-rounds of TMN64 and TMN128 block ciphers, respectively.

4.1 Related-key Amplified Boomerang Characteristic of TMN64

We suppose that the (P, P^*, P', P'^*) plaintexts with difference $\alpha = P \oplus P^* = P' \oplus P'^* = (e_{32}, e_{32})$ are encrypted to get appropriate ciphertext (C, C^*, C', C'^*) using the master keys (K, K^*, K', K'^*) satisfying the key difference $\Delta K = K \oplus K^* = K' \oplus K'^* = (e_{32}, 0, 0, 0)$.

By this way, we can generate the 1st related-key propagation of differential distinguisher $(\alpha \rightarrow \beta)$ from the 1st round to the 5th round of TMN64 to get the corresponding output difference $\beta = (0, 0)$, with probability of 1.

Then, we mark the transitional values as (I, I^*, I', I'^*) with the difference $\gamma = I \oplus I^* = I' \oplus I'^* = (0, 0)$. These values are encoded using the master key (K, K^*, K', K'^*) satisfying the key difference $\Delta K' = K \oplus K' = K^* \oplus K'^* = (0, e_{32}, 0, 0)$. Overall, we can yield the 2nd related-key propagation of differential distinguisher $(\gamma \rightarrow \delta)$ from the round 6th to the last round 10th with a probability of 2^{-12}, to get the final corresponding output difference $\delta = (e_{32}, 0)$.

Table 1. Related-key propagation of differential distinguisher on full-round of TMN64.

Round r	ΔX_r	$(\Delta Q_r, \Delta Q_r)$	Probability
1	$\alpha = (e_{32}, e_{32})$	(e_{32}, e_{32})	1
2	(0, 0)	(0, 0)	1
3	(0, 0)	(0, 0)	1

4	(0, 0)	(0, 0)	1
5	(0, 0)	(0, 0)	1
Output	$\beta = (0, 0)$		
6	$\gamma = (0, 0)$	(0, 0)	1
7	(0, 0)	(0, 0)	1
8	(0, 0)	(0, 0)	1
9	(0, 0)	(0, 0)	1
10	(0, 0)	$(e_{32}, 0)$	2^{-12}
FT	$(e_{32}, 0)$	(0, 0)	1
Output (ΔY)	$\delta = (e_{32}, 0)$		
Total			2^{-12}

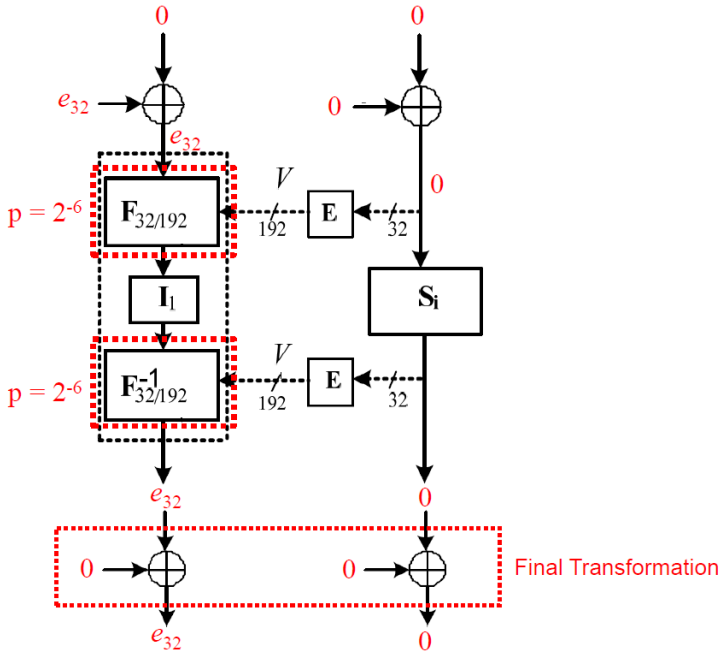


Fig. 8. Differential propagation at the 10th round and the FT on the TMN64.

For further definitions of related-key DCs on the TMN64 cipher, refer to **[Appendix A]**.

4.2 Related-key Amplified Boomerang Characteristic of TMN128

We similarly do as the same methods applied to TMN64, by assuming the plaintexts (P, P^*, P', P'^*) with difference value $\alpha = P \oplus P^* = P' \oplus P'^* = (e_{64}, e_{64})$ are encrypted to get appropriate ciphertext (C, C^*, C', C'^*) using the master keys (K, K^*, K', K'^*), as the key difference is $\Delta K = K \oplus K^* = K' \oplus K'^* = (e_{64}, 0, 0, 0)$.

In this manner, we can obtain the 1st related-key propagation of differential distinguisher ($\alpha \rightarrow \beta$) from the 1st round to the 5th round of TMN128 for obtaining the output difference $\beta = (0, 0)$, with probability of 1.

Then, we assign the transitional values as (I, I^*, I', I'^*) with the difference $\gamma = I \oplus I^* = I' \oplus I'^* = (e_{64}, e_{64})$. These values are encoded using the master key (K, K^*, K', K'^*), as the key

difference is $\Delta K' = K \oplus K' = K^* \oplus K'^* = (e_{64}, e_{64}, 0, 0)$. Finally, we can yield the 2nd related-key propagation of differential distinguisher ($\gamma \rightarrow \delta$) from round 6th to the last round 12th with a probability of 2^{-24}, to get the final corresponding output difference $\delta = (e_{64}, e_{64})$.

Table 2. Related-key propagation of differential distinguisher on full-round of TMN128.

Round r	ΔX_r	$(\Delta Q_r, \Delta Q_r)$	**Probability**
1	$\alpha = (e_{64}, e_{64})$	(e_{64}, e_{64})	1
2	(0, 0)	(0, 0)	1
3	(0, 0)	(0, 0)	1
4	(0, 0)	(0, 0)	1
5	(0, 0)	(0, 0)	1
Output	$\beta = (0, 0)$		
6	$\gamma = (e_{64}, e_{64})$	(e_{64}, e_{64})	1
7	(0, 0)	(0, 0)	1
8	(0, 0)	(0, 0)	1
9	(0, 0)	(0, 0)	1
10	(0, 0)	$(e_{64}, 0)$	2^{-12}
11	$(0, e_{64})$	(e_{64}, e_{64})	2^{-12}
12	$(0, e_{64})$	$(0, e_{64})$	1
FT	(0, 0)	(e_{64}, e_{64})	1
Output (ΔY)	$\delta = (e_{64}, e_{64})$		
Total			2^{-24}

For further definitions of related-key DCs on the TMN128 cipher, refer to **[Appendix A]**.

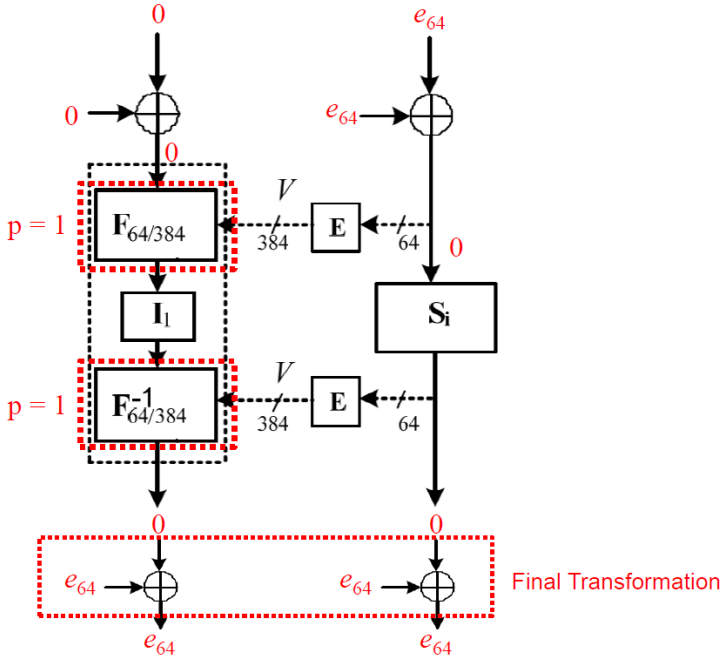


Fig. 9. Differential propagation at the 12th round and the FT on the TMN128.

5. Proposed Key Recovery Attacks on TMN64, TMN128

This section illustrates the methods we apply to employ the recovery attacks on the TMN-64 and TMN-128 constructions.

5.1 Amplified Boomerang Attack Method on TMN64

According to the obtained related-key DCs in **Section 4** for TMN64, we expect $m^2 \cdot 2^{-88}$ correct quartets when executing with m RK-CP (related-key chosen-plaintext) pairs, depicted as (P, P^*) and (P', P'^*), and the related-key amplified boomerang distribution constructed reach to the 10^{th} round of TMN64 with probability of 2^{-88} (that is $2^{-n} \cdot p^2 \cdot q^2$). And then, we select a set of 2^{46} plaintext pairs (that is $m^2 \cdot 2^{-88} = 2^3$) for the attack while we look for 8 (2^3) correct amplified boomerang quartets.

The proposed related-key recovery attack based on the amplified boomerang cryptanalytic method on full 10-rounds TMN64 as follows.

1) We firstly select a group of 2^{46} pairs of plaintext (P_j, $P_j{}^*$), (where j = 1, …, 2^{66}), and construct 2^{91} quartets of plaintext (P_i, $P_i{}^*$, $P_i{}'$, $P_i{}'^*$), (where i = 1, …, 2^{91}) under the input difference $\alpha = (e_{32}, e_{32})$. Then, the quartets of plaintext (P_i, $P_i{}^*$, $P_i{}'$, $P_i{}'^*$) are encrypted using the master key (K, K^*, K', K'^*) satisfying the differences of keys, those are $\Delta K = K \oplus K^* = K' \oplus K'^* = (e_{32}, 0, 0, 0)$ and $\Delta K' = K \oplus K' = K^* \oplus K'^* = (0, e_{32}, 0, 0)$, to obtain the appropriate quartets of ciphertext (C_i, $C_i{}^*$, $C_i{}'$, $C_i{}'^*$).

2) We examine with each i, that $C_i \oplus C_i{}' = C_i{}^* \oplus C_i{}'^* = (e_{32}, 0)$ for each route.

3) At this step, we predict a sub-key (K_1) with 32-bit key size of the FT, and gain the subkeys ($K_1{}^*$, $K_1{}'$ and $K_1{}'^*$) using the guessed key K_1.

(a.) We do decrypt for all the quartets of ciphertext (C_i, $C_i{}^*$, $C_i{}'$, $C_i{}'^*$) progressing through **Stage 2**, with the predicted quartets of sub-key to obtain 32-bit left inputs (X_i, $X_i{}^*$, $X_i{}'$, $X_i{}'^*$) on the 10^{th} round prior the additional layer of key ($\oplus$ XOR operation) at the final transformation.

(b.) Then, we check that $X_i \oplus X_i{}' = X_i{}^* \oplus X_i{}'^* = (0, 0)$ for each i value.

4) Finally, for the recovery attacks, we generate a brute-force search for catching the remaining 96-bit (K_2, K_3, K_4) with all the predicted sub-keys progressing through **Stage 3**. When any predicted 128-bits key is satisfying the pairs of two plaintext/ ciphertext, we can then do output the key as the correct 128-bits master key of the TMN64. In other ways, we return to the method at **Stage 3**.

The proposed attack on TMN64 requires 2^{46} pairs of plaintext and 2^{47} RK-CPs (related-key chosen plaintexts) as the complexity of data, under the total related-key DC of 2^{-12} probability. The requirement of memory is approximately 2^{50} ($= 2^{47} \cdot 8$) bytes during the attack. The complexity of time at **Stage 1** is around 2^{47} full 10-rounds encryptions of TMN64. We expect that each ciphertext progressing through **Stage 2** with 2^{-64} probability. Therefore, we expect

around 2^{28} (that is $2^{92} \cdot 2^{-64}$) correct quartets of ciphertext go by this stage. We look forward the complexity of time at **Stage 3** and **Stage 4** is around 2^{62} (that is $2^{64} \cdot 4 \cdot 1/8 \cdot 1/2$) and 2^{65} (that is $2^{64} \cdot 1 \cdot 2$) data encryptions, respectively. Overall, the complexity of time executing all the attack is approximately 2^{65} (that is $2^{47} + 2^{62} + 2^{65}$) TMN64 computational encryptions on average.

5.2 Amplified Boomerang Attack Method on TMN128

Following the obtained related-key DCs in **Section 4** for TMN128, we look for $m^2 \cdot 2^{-176}$ correct quartets when executing with m RK-CP (related-key chosen-plaintext) pairs, depicted as (P, P*) and (P', P'*), as the related-key amplified boomerang distribution constructed reach to the 12^{th} round of TMN128 with probability of 2^{-176} (that is $2^{-n} \cdot p^2 \cdot q^2$). And then, we select a set of 2^{90} plaintext pairs ($m^2 \cdot 2^{-176} = 2^3$) for the attack while we suppose 8 (2^3) correct amplified boomerang quartets.

The proposed related-key recovery attack based on the amplified boomerang cryptanalytic method on full 12-rounds TMN128 as follows.

1) To begin with, we prepare a group of 2^{90} pairs of plaintext (P_j, P_j *), (j = 1, …, 2^{90}), and construct corresponding 2^{179} quartets of plaintext (P_i, P_i *, P_i ', P_i '*), (i = 1, …, 2^{179}) under the input difference $\alpha = (e_{64}, e_{64})$. Then, we encode the quartets of plaintext (P_i, P_i *, P_i ', P_i '*) using the unknown sub-keys (K, K*, K', K'*) having $\Delta K = K \oplus K^* = K' \oplus K'^* = (e_{64}, 0, 0, 0)$ and $\Delta K' = K \oplus K' = K^* \oplus K'^* = (e_{64}, e_{64}, 0, 0)$ key difference, for catching the matching quartets of ciphertext (C_i, C_i *, C_i ', C_i '*).

2) We examine with each i, that $C_i \oplus C_i' = C_i^* \oplus C_i'^* = (e_{64}, e_{64})$ for each route.

3) At this step, we predict a sub-key (K_1) with 64-bit key size of the FT, and gain the subkeys (K_1*, K_1' and K_1'*) using the guessed key K_1.

(a.) We do decrypt for all the quartets of ciphertext (C_i, C_i *, C_i ', C_i '*) progressing through **Stage 2**, with the predicted quartets of sub-key to obtain 64-bit left inputs (X_i, X_i *, X_i ', X_i '*) on the 12^{th} round prior the additional layer of key ($\oplus$ XOR operation) at the final transformation.

(b.) Then, we check that $X_i \oplus X_i' = X_i^* \oplus X_i'^* = (0, 0)$ for each i value.

4) Lastly, we generate a brute-force search for catching the remaining 192-bit (K_2, K_3, K_4) with all the predicted sub-keys progressing through **Stage 3**. When any predicted 256-bits key is satisfying the pairs of two plaintext/ ciphertext, we can then do output the key as the correct 256-bits master key of the TMN64. In other ways, we return to the method at **Stage 3**.

The proposed attack on TMN128 requires 2^{90} pairs of plaintext and and 2^{91} RK-CPs (related-key chosen plaintexts) as the complexity of data, under the total related-key DC of 2^{-24} probability. The requirement of memory is approximately 2^{94} (= $2^{91} \cdot 8$) bytes during the attack. The complexity of time at **Stage 1** is around 2^{91} full 10-rounds encryptions of TMN128. Similarly, we also expect that each ciphertext progressing through **Stage 2** with 2^{-128}

probability. Therefore, we expect around 2^{52} (that is $2^{180} \cdot 2^{-128}$) correct quartets of ciphertext go by this stage. We look forward the complexity of time at **Stage 3** and **Stage 4** is around 2^{126} (that is $2^{128} \cdot 4 \cdot 1/8 \cdot 1/2$) and 2^{129} (that is $2^{128} \cdot 1 \cdot 2$) data encryptions, respectively. Overall, the complexity of time executing all the attack is approximately 2^{129} ($\approx 2^{91} + 2^{126} + 2^{129}$) TMN128 computational encryptions on average.

6. Conclusion

In this paper, we discussed the security of the TMN-family framework: TMN64 and TMN128, resisting against the related-key recovery attack based on the differential boomerang cryptanalytic method. Depending on high probability of differential characteristics we constructed, we suggested a kind of related-key recovery attacks as the amplified boomerang cryptanalysis in different two versions: on a full 10-rounds of TMN64 and 12-rounds of TMN128. The attack requires about 2^{47} RK-CP (related-key chosen plaintexts), 2^{50} memory bytes and 2^{65} complexity of time for all encryptions unit of the TMN64; and 2^{91} RK-CP (related-key chosen plaintexts), 2^{94} memory bytes and 2^{129} complexity of time for all encryptions unit of the TMN128. According to our cryptanalytic results, although the TMN constructions had enhanced the way of generating round keys to handle with the weak key scheduling problems, the full-round of TMN64 and TMN128 were distinguished from an ideal cipher properly, that proved the TMN constructions are still vulnerable to related-key differential attacks. We suggest a better primitive approach in designing the block ciphers, especially the structures based on DDP or DDO functions in the further research.

Appendix

Appendix A.

We illustrate some differential distribution of the round function at various TMN64 rounds. The differential characteristics are constructed as follows:

The first differential trail $\boldsymbol{E^0}$ with unknown input difference α and unknown output difference β is defined as $(\alpha \rightarrow \beta) = (e_{32}, e_{32}) \rightarrow (0, 0)$ from the 1st round to the 5th round with the probability $p = 1$ based on the CE $F_{2/2}$ description. And, since the difference of input at the 2nd round is vanished by the difference of round key, we have at the 3rd round, the difference of input will be '(0, 0)' that remains as the difference of output until the 5th round.

Similarly, we build the second differential trail $\boldsymbol{E^1}$ with γ difference of input and δ difference of output, $(\gamma \rightarrow \delta) = (0, 0) \rightarrow (e_{32}, 0)$, for the round $6^{th} \sim 10^{th}$ with $q = 2^{-12}$ probability. By the same way, the difference of input at the 6th round is vanished by the difference of round key, therefore it yields the difference of output (0, 0) until the 9th round.

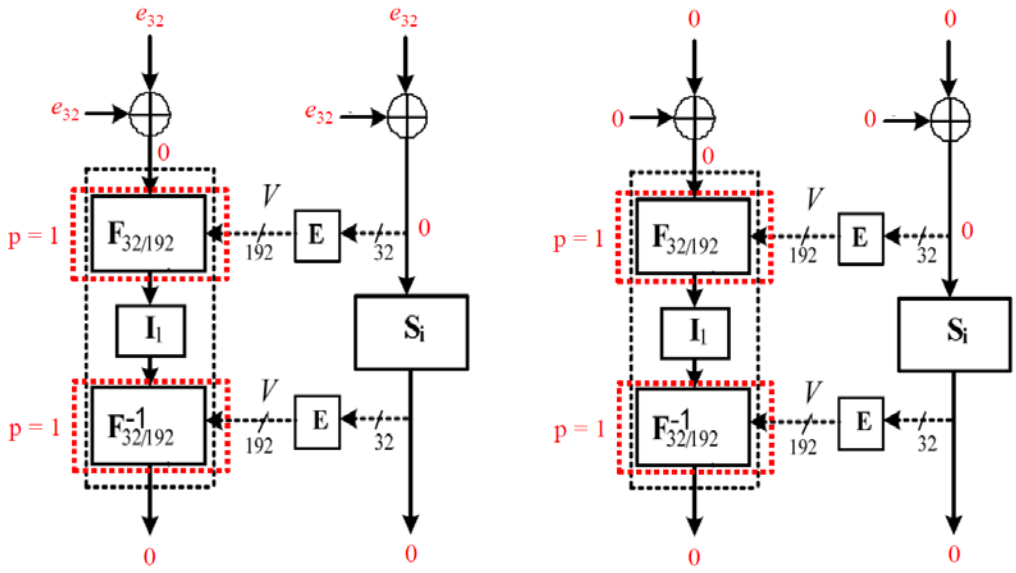


Fig. 10. Propagation in the TMN64 round function at the first round and for the $2^{nd} \rightarrow 9^{th}$ round.

Appendix B.

We illustrate some differential distribution of the round function at various TMN128 rounds. The differential characteristics are constructed as follows:

We construct the first differential trail $\boldsymbol{E}^{\mathbf{0}}$ with input difference α and output difference β by $(\alpha \rightarrow \beta) = (e_{64}, e_{64}) \rightarrow (0, 0)$ from the 1^{st} round to the 5^{th} round with $p = 1$ probability. In this manner, because the difference of input at the 2^{nd} round is vanished by the difference of round key, at the 3^{rd} round, the difference of input will be '(0, 0)' that remains as the difference of output until the 5^{th} round.

Similarly, we build the second differential trail E^1 with γ difference of input and δ difference of output, $(\gamma \rightarrow \delta) = (e_{64}, e_{64}) \rightarrow (e_{64}, e_{64})$, for the round $6^{th} \sim 12^{th}$ with $q = 2^{-24}$ probability. Following this property, the difference of input at the 6^{th} round is vanished by the difference of round key, therefore it yields the difference of output (0, 0) until the 9^{th} round. Then, we obtain the resultant probability of 2^{-12} for each round with the input difference $(0, e_{64})$ for both round under the round key difference (e_{64}, e_{64}) and $(0, e_{64})$, respectively.

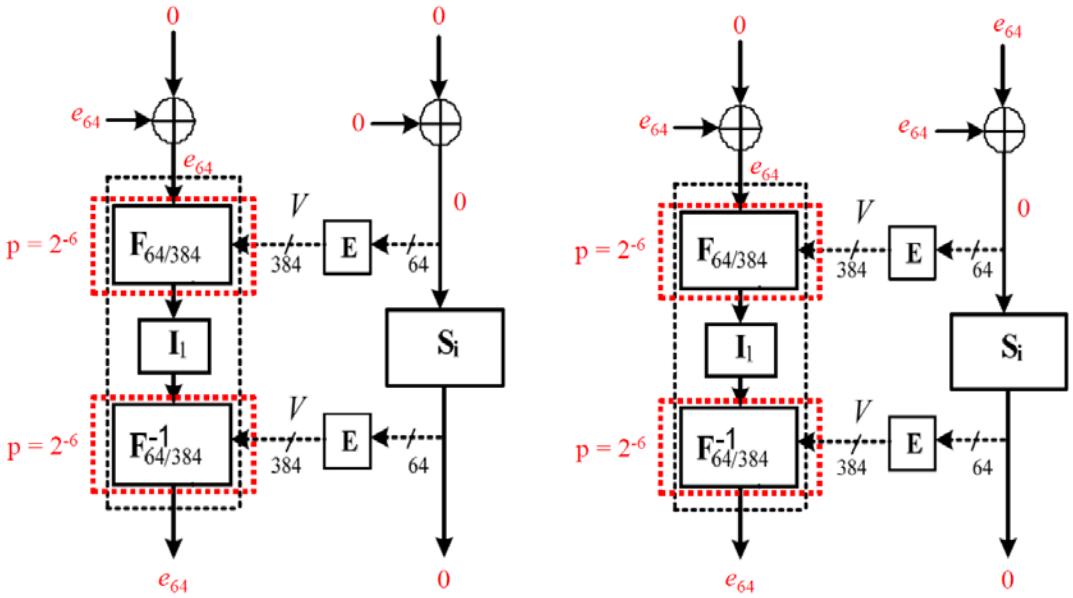


Fig. 11. Propagation in the TMN64 round function at the 10th round and 11th round.

Conflicts of Interest: The authors declare no conflict of interest.

Acknowledgement

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2020-0-01797) supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation).

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] P. M. Tuan, B. Do Thi, M. N. Hieu, and N. Do Thanh, "New Block Ciphers for Wireless Moblile Netwoks," *Advances in Information and Communication Technology*, ICTA 2016, *Intelligent Systems and Computing*, vol. 538, pp. 393-402, Dec. 2016. Article (CrossRef Link)

[2] D. Bac, N. Minh, "High-Speed Block Cipher Algorithm Based on Hybrid Method," *Ubiquitous Information Technologies and Applications. Lecture Notes in Electrical Engineering*, vol. 280, pp. 285-291, 2014. Article (CrossRef Link)

[3] T.SD. Phuc, C. Lee, "Cryptanalysis on SDDO-Based BM123-64 Designs Suitable for Various IoT Application Targets," *Symmetry*, vol. 10, no. 8, p.353, Aug 2018. Article (CrossRef Link)

[4] D. Bac, N. Minh, H. Duy, "An Effective and Secure Cipher Based on SDDO," *International Journal of Computer Network and Information Security*, vol. 4, no. 11, pp. 1-10, Oct 2012. Article (CrossRef Link)

[5] D. Bac, N. Ming, H. Duy, "New SDDO-Based Block Cipher for Wireless Sensor Network Security," *International Journal of Computer Science and Network Security*, vol. 10, no. 3, pp. 54-60, 2010.

[6] N.H. Minh, H.N. Duy, L.H. Dung, "Design and Estimate of a New Fast Block Cipher for Wireless Communication Devices," in *Proc. of 2008 International Conference Advanced Technologies for Communications*, pp. 409-412, Jan 2008. Article (CrossRef Link).

[7] N.A. Moldovyan, "On Cipher Design Based on Switchable Controlled Operations," *Computer Network Security, MMM-ACNS, Lecture Notes in Computer Science*, vol. 2776, pp. 316-327, 2003. Article (CrossRef Link)
[8] N.D. Goots, B.V. Izotov, A.A. Moldovyan, N.A. Moldovyan, *Modern cryptography: Protect Your Data with Fast Block Ciphers*, Wayne, A-LIST Publish, 2003
[9] J. Kang, K. Jeong, C. Lee, S. Hong. "Distinguishing attack on SDDO-based block cipher BMD-128," *Ubiquitous Information Technologies and Applications. Lecture Notes in Electrical Engineering*, vol. 280, pp. 595-602, 2014. Article (CrossRef Link)
[10] T.SD. Phuc, C. Lee, N. Xiong, "Cryptanalysis of the XO-64 Suitable for Wireless Systems," *Wireless Personal Communications*, vol. 93, no. 2, pp. 589-600, 2017. Article (CrossRef Link)
[11] C. Lee, J. Kim, J. Sung, S. Hong, S. Lee, "Security analysis of the full-round DDO-64 block cipher," *The Journal of Systems and Software*, vol. 81, no. 12, pp. 2328-2335, Dec 2008. Article (CrossRef Link)
[12] J. Kang, K. Jeong, S. Yeo, C. Lee, "Related-key Attack on the MD-64 Block Cipher Suitable For Pervasive Computing Environment," in *Proc. of 2012 26th International Conference on Advance Information Networking and Application Workshops*, pp. 726-731, Mar 2012. Article (CrossRef Link)
[13] N. Sklavos, N.A. Moldovyan, O. Koufopavlou, "A New DDP-based Cipher CIKS-128H: Architecture, Design & VLSI Implementation Optimization of CBC-Encryption & Hashing over 1 GBPS," in *Proc. of 2003 46th IEEE Midwest Symposium on Circuits and Systems*, vol. 1, pp. 463-466, Dec 2003. Article (CrossRef Link)
[14] N. Moldovyan, A. Moldovyan, *Data-driven Ciphers for Fast Telecommunication Systems*, United Kingdom: Auerbach Publication. Talor & Francis Group, 2008, pp. 77-185.
[15] E. Biham, O. Dunkelman, N. Keller, "Related-key boomerang and rectangle attacks," *Advances in Cryptology – EUROCRYPT'05. Lecture Notes in Computer Science*, vol. 3494, pp. 507-525, 2005. Article (CrossRef Link)
[16] J. Kelsey, T. Kohno, B. Schneier, "Amplified Boomerang Attacks against Reduced-Round MARS and Serpent," in *Proc. of International Workshop on Fast Software Encryption. Lecture Notes in Computer Science*, vol. 1978, pp. 75-93, 2000. Article (CrossRef Link)
[17] D. Wagner, "The Boomerang Attack," in *Proc. of International Workshop on Fast Software Encryption. Lecture Notes in Computer Science*, vol. 1636, pp. 156-170, 1999. Article (CrossRef Link)
[18] A. Moldovyan, N. Moldovyan, "A cipher Based on Data-Dependent Permutations," *Journal of Cryptology*, vol. 15, pp. 61-72, 2002. Article (CrossRef Link)
[19] N. Goots, N. Moldovyan, P. Moldovyanu, D. Summerville, "Fast DDP-based Ciphers: from Hardware to Software," in *Proc. of 2003 46th IEEE Midwest International Symposium on Circuits and Systems*, vol. 2, pp.770-773, Dec 2003. Article (CrossRef Link)
[20] N. Sklavos, N. Moldovyan, O. Koufopavlou, "High Speed Networking Security: Design and Implementation of Two New DDP-based Ciphers," *Mobile Networks and Applications-MONET*, vol. 10, no. 1, pp. 219-231, 2005. Article (CrossRef Link)

Tran Song Dat Phuc received the B.Sc. degree in Information Technology from HCMC University of Technology, Ho Chi Minh, Vietnam in 2011. He received the M.S., and Ph.D. degrees in Computer Science and Engineering from Seoul National University of Science and Technology, in 2015 and 2020, respectively. His research interests are cryptography, information security, network security, and digital forensics.

Yong-Hyeon Shin received the B.Sc., M.Sc., and Ph.D. degrees in Computer Science and Engineering from Seoul National University, in 1988, 1991, and 2003, respectively. He is currently a professor of Computer Science and Engineering at Seoul National University of Science and Technology, Seoul, Republic of Korea. His research interests are operating systems, web systems, computing security and embedded systems.

Changhoon Lee received the B.Sc. degree in Mathematics from Hanyang University. He received the M.Sc., and Ph.D. degrees in Information Security from Korea University in 2003 and 2008, respectively. He is currently a professor of Computer Science and Engineering at Seoul National University of Science and Technology, Seoul, Republic of Korea. His research interests are cryptography, information security, digital forensics, IoT security, cyber threat intelligence.