Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2017) 25: 4901 – 4906

doi:10.3906/elk-1701-214

New Patterson–Wiedemann type functions with 15 variables in the generalized rotation-symmetric class

Selçuk KAVUT*
Department of Computer Engineering, Faculty of Engineering, Balıkesir University, Balıkesir, Turkey

Received: 22.01.2017 • **Accepted/Published Online:** 13.07.2017 • **Final Version:** 03.12.2017

Abstract: Recently, it was shown that there is no Boolean function on 15 variables with nonlinearity greater than 16276 in the class of functions that are invariant under the action of $\mathrm{GF}(2^3)^* \times GF(2^5)^*$. In this study, we consider some important subsets of this class and perform an efficient enumeration of the 15-variable Patterson–Wiedemann (PW) type functions with nonlinearity greater than the bent concatenation bound 16256 in the generalized classes of both 3-RSBFs and 5-RSBFs for which the corresponding search spaces are $2^{28.2}$ and $2^{47.85}$, respectively. For the case of 3-RSBFs, we find that there are 32 functions with nonlinearity $>$ 16256, such that 8 of them correspond to the original PW constructions, while the remaining 24 functions are new in the sense that they are not affine equivalent to the known ones. For the other case of 5-RSBFs, our results show that there are 478 functions with nonlinearity exceeding the bent concatenation bound, among which there is another set of 470 functions that are affine inequivalent to the known PW constructions.

Key words: Nonlinearity, Boolean functions, Patterson–Wiedemann type functions

1. Introduction

The design of Boolean functions on an odd number of variables n achieving very high nonlinearity, i.e. greater than the so-called bent concatenation bound $2^{n-1} - 2^{(n-1)/2}$, constitutes one of the most challenging problems encountered in the area of cryptography, coding theory, and combinatorics. Boolean functions with high nonlinearity play a crucial role in the design of a secret-key cryptosystem as they are used as building blocks to provide resistance against linear cryptanalysis [1]. In a standard correlation attack [2], where the outputs of several linear feedback shift registers (LFSRs) are combined by a nonlinear Boolean function to generate the keystream, the correlation between the keystream and one of the LFSR outputs (or a linear combination of the LFSR outputs) is used to obtain the key (i.e. the initial states of the LFSRs). In other words, a correlation attack can be mounted if there is a high correlation between the combining function and a linear function, which implies low nonlinearity. Hence, as it is well known (e.g., see [3]), high nonlinearity provides resistance against correlation and fast correlation attacks [4], as well. In coding theory, the problem is actually related to the covering radius of the first-order Reed–Muller codes of block length 2^n, which corresponds to the maximum achievable nonlinearity of n-variable Boolean functions. The existence of Boolean functions with nonlinearity exceeding the bent concatenation bound could be demonstrated for the first time for $n = 15$ by Patterson and Wiedemann [5] in 1983 using some combinatorial results together with an exhaustive search.

*Correspondence: skavut@balikesir.edu.tr

More than two decades later, 9-variable Boolean functions with nonlinearity 241 ($=2^{9-1}-2^{(9-1)/2}+1$) were identified [6] in the rotation-symmetric class and subsequently this result was improved [7] to 242 by defining the k-rotation-symmetric class.

Let $f : GF(2^n) \to GF(2^n)$ be a Patterson–Wiedemann (PW) type function as defined in [8]. Until recently, PW type functions exceeding the bent concatenation bound were known only for $n = 15 = 5 \times 3$. The next possible candidate was $n = 21 = 7 \times 3$, and such functions could be constructed [9] using a heuristic search after a long gap of more than three decades. Each function found in [9] is of nonlinearity $2^{21-1}-2^{(21-1)/2} + 61$, and the nonlinearity bound given in [10] shows that the upper bound of nonlinearity in this case could be as high as $2^{21-1}-2^{(21-1)/2}+196$ for the functions that are invariant under the action of $\mathrm{GF}(2^3)^* \times GF(2^7)^*$.

Recall that since PW type functions are idempotents for which $f(\alpha) = f(\alpha^2)\ \forall \alpha \in GF(2^n)$, they can be considered as rotation-symmetric by choosing a normal basis to represent the elements in $\mathrm{GF}(2^n)$. In [7], the (generalized) k-rotation symmetric class is defined as the class of functions that satisfy $f(\alpha) = f(\alpha^{2^k})\ \forall \alpha \in GF(2^n)$, where k is a fixed divisor of n. First, motivated by the fact that 9-variable functions with nonlinearity 242 are obtained [7] in the class of 3-rotation-symmetric Boolean functions (3-RSBFs), we consider the PW type 15-variable functions that are in the k-rotation-symmetric class (which we refer to as PW type 15-variable k-RSBFs) by relaxing the restriction of being idempotent. For $(n,\ k) = (15,\ 3)$, we perform an exhaustive search for the PW type 3-RSBFs using the system of inequalities obtained by properly modifying *Algorithm PreInequalities* in [8], which reduces the problem of finding the PW type functions to a problem of solving an integer programming problem with binary variables. In this case, there are 31 inequalities, and the size of the search space is $2^{28.2}$ (note that in [9], for $(n,\ k) = (21,\ 1)$, there are 115 inequalities and the search space is $2^{109.27}$). By fixing $f(0) = 0$, we find that there are 32 Boolean functions with nonlinearity greater than the bent concatenation bound 16256 ($=2^{15-1}-2^{(15-1)/2}$). Specifically, 8 of them correspond to the PW type 15-variable 1-RSBFs (called the PW constructions) that were given in [5], while the remaining 24 functions have different absolute indicators from those of the PW constructions and hence are not affine equivalent to any of them. One half of these 24 functions have nonlinearity 16268, and the other half have nonlinearity 16269 (as in the case of the PW constructions, one half is obtained from the other half by complementing the truth tables, except their first bits). Note that one can use these functions to obtain balanced functions with nonlinearity greater than the bent concatenation bound by suitably modifying their truth tables as in [11–13]. For $(n,\ k) = (15,\ 5)$, there are 51 inequalities, and the search space is of size $2^{48.75}$, which is huge compared to the previous case. Here, we performed an efficient enumeration algorithm on a computer with an Intel Xeon CPU E7-4890 v2 @ 2.80 GHz processor, which takes 2 weeks by exploiting all of the cores. As in $(n,\ k) = (15,\ 3)$, we fixed $f(0) = 0$ to remove the functions that are complements of each other and found that there are 478 functions with nonlinearity > 16256. Among these, 470 of them are affine inequivalent to the known PW functions. Our results confirm the nonlinearity bound in [10] for the 15-variable functions that are invariant under the action of $\mathrm{GF}(2^3)^* \times GF(2^5)^*$. In the Appendix, we present the aforementioned PW type functions in the classes of 3-RSBFs and 5-RSBFs in Tables A1 and A2, respectively. These were unknown before. The MATLAB code that we use to perform *Algorithm PrepareInequalities* [8] for both 3-RSBFs and 5-RSBFs can be found at https://drive.google.com/open?id=0B1s_TxsFtjSPSm1oZzhwaVoxa2M.

In the following section, after giving a brief background of PW type functions, we present our results in Section 3 and conclude the paper in Section 4.

2. Preliminaries

Let f: GF(2^n) $\rightarrow GF(2^n)$ be a Boolean function. We can call f balanced if the Hamming weight of its truth table is equal to 2^{n-1}.

For any $\omega \in GF(2^n)$, the Walsh–Hadamard transform $W_f(\omega)$ of f is defined as:

$$W_f(\omega) = \sum_{\alpha \epsilon GF(2^n)} (-1)^{Tr(\omega\alpha)+f(\alpha)},$$

from which the nonlinearity NL_f can be expressed as follows:

$$NL_f = 2^{n-1} - (1/2)\max_{\omega \in GF(2^n)}|W_f(\omega)|.$$

For an odd number of variables $n \geq 9$, the maximum nonlinearity is not known. The best achieved nonlinearity is known as $2^{n-1} - 2^{(n-1)/2} + 20 \times 2^{(n-15)/2}$ for $n \geq 15$ [5] and $2^{n-1} - 2^{(n-1)/2} + 2 \times 2^{(n-9)/2}$ for $n = 9$, 11, and 13 [7].

The autocorrelation function of f is given by:

$$r_f(\beta) = \sum_{\alpha \epsilon GF(2^n)} (-1)^{f(\alpha)+f(\alpha+\beta)},$$

where $\beta \in GF(2^n)$. The autocorrelation value with maximum magnitude, except the origin, is also known as the absolute indicator [14] and denoted as:

$$\Delta_f = \max_{\beta \in GF(2^n)^*}|r_f(\beta)|.$$

It was conjectured in [14] that for any balanced function f with an odd number of variables $n, \Delta_f \geq 2^{(n+1)/2}$, which has been disproved by modifying the PW type functions [8,12].

As pointed out in [8], PW construction [5] can be viewed as an interleaved sequence [15] that is defined as follows:

Definition 1 *Let $m = dr$, where d, $r > 1$ are integers. The (d, r)-interleaved sequence $A_{d,r}$, corresponding to the binary sequence $A = \{a_0, a_1, a_2, \ldots, a_{m-1}\}$, is defined as the matrix whose (i, j)th entry is equal to $a_{i,d+j}$, where $i = 0, 1, \ldots, r-1$ and $j = 0, 1, \ldots, d-1$.*

Let ξ be a primitive element in GF(2^n). Assuming that $m = 2^n - 1$, an interleaved sequence $A_{d,r}$ can be associated with the ordered sequence $\{f(1), f(\xi), f(\xi^2), \ldots, f(\xi^{2n-2})\}$ such that $a_{i,d+j} = f(\xi^{id+j})$. This interleaved sequence is called the (d, r)-interleaved sequence, corresponding to f with respect to ξ. The PW type functions are described as follows [8,16]:

Definition 2 *Let $n = tq$, where t, $q > 2$ are prime numbers such that $t > q$. Let the product $\Re = GF(2^t) \times GF(2^q)$ be the cyclic group of cardinality $r = (2^t - 1)(2^q - 1)$ in $GF(2^n)$. Let $\langle\varphi_2\rangle$ be the group of Frobenius automorphisms, where $\varphi_2 : GF(2^n) \rightarrow GF(2^n)$ is defined by $\alpha \rightarrow \alpha^2$. The function f is called PW type if it is invariant under the action of $\Re$ and $\langle\varphi_2\rangle$.*

Since the corresponding function f is invariant under the action of $\Re$, the $(d,\ r)$-interleaved sequence of a PW type function consists of either all 0 or all 1 columns by Definition 2. In addition, because of the invariance under the action of $\langle\varphi_2\rangle$, the ith column has the same value as the jth column if $i \equiv j2^s \mod d$ for some integer $s > 0$. This equivalence relation, shown by ρ_d, is given as follows:

$$i\rho_d j \Leftrightarrow \text{ there exists an integer } s > 0 \text{ such that } i \equiv j2^s mod\ d.$$

Note that the PW type functions are idempotents, i.e. $f\ (\alpha) = f(\alpha^2)\ \forall\alpha \in GF(2^n)$, and thus they can be considered [17,18] as rotation-symmetric by choosing a normal basis. The k-rotation symmetric class, which is equivalent to the rotation-symmetric class for $k = 1$, was defined in [7] as the class of functions that satisfy $f(\alpha) = f(\alpha^{2^k})\ \forall\alpha \in \mathrm{GF}(2^n)$, where k is a fixed divisor of n. Here, by imposing the condition of being k-rotation-symmetric on the PW type functions, we relax the restriction of the invariance under the action of $\langle\varphi_2\rangle$ and define the PW type k-RSBFs in the following:

Definition 3 *Let $\langle\varphi_{2^k}\rangle$ be the group of automorphisms, where k is a fixed divisor of n and $\langle\varphi_{2^k}\rangle$: $GF(2^n) \to GF(2^n)$ is defined by $\alpha \to \alpha^{2^k}$. The function f is called a PW type k-RSBF if it is invariant under the action of $\Re$ and $\langle\varphi_{2^k}\rangle$.*

The equivalence relation among the corresponding $(d,\ r)$-interleaved sequences, denoted by ρ_d^k, is then given by:

$$i\rho_d^k j \Leftrightarrow \text{ there exists an integer } s > 0 \text{ such that } i \equiv j2^{ks} modd.$$

Clearly, the PW type k-RSBFs are equivalent to the PW type functions for $k = 1$.

In the rest of this paper, we assume $f\ (0) = 0$ without loss of generality. Furthermore, we realize the function f as $f\colon \{0,\ 1\}^{\ 15} \to \{0,\ 1\}$ using the primitive polynomial $x^{15} + x\ + 1$ for $n = 15$.

3. PW type 15-variable k-RSBFs

In both of the following cases, we implement *Algorithm PrepareInequalities* [8] with our MATLAB code available at the link given in Section 1.

3.1. The case of $k = 3$

Using the mentioned code, we find that in a (151, (31)(7))-interleaved sequence there are 31 equivalence classes with respect to ρ_{151}^3. Among them, 30 are of size 5 and 1 is of size 1. Let us represent the jth equivalence class by the smallest integer among its elements as in [8]. We then have the following 31 representatives: 0, 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 14, 15, 17, 22, 23, 27, 28, 29, 30, 34, 35, 37, 46, 47, 51, 53, 68, 87, and 94. Hence, a PW type 15-variable 3-RSBF can be represented by a binary vector of length 31, i.e. $(f(1),\ f(\xi^1),\ (\xi^2), \ldots,\ f(\xi^{87}),\ f(\xi^{94}))$.

Implementing *Algorithm PreInequalities* in [8], we obtain the system of 31 inequalities in this case. Then, by carrying out an exhaustive search, we find that there are 32 solutions of the system such that each solution corresponds to an aforementioned 31-bit representative truth table (RTT). In Table A1, we give only one half of these solutions since the other half is obtained by complementing them.

The first four solutions in Table A1 give PW constructions [5] with absolute indicators 160 and 200, which correspond to PW type 1-RSBFs with respect to Definition 3. All the other RTTs yield functions with different absolute indicators and hence they are not affine equivalent to the PW constructions.

3.2. The case of $k = 5$

Here, using the equivalence relation ρ_{151}^5, it is found that there are 51 representatives: 0, 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 20, 21, 22, 23, 25, 26, 28, 30, 31, 33, 35, 37, 39, 42, 44, 46, 47, 51, 55, 56, 60, 61, 65, 66, 69, 70, 74, 75, 78, 79, 83, 84, 88, and 93. Among their equivalence classes, 50 are of size 3 and 1 is of size 1. We carried out an efficient exhaustive search algorithm to obtain all the solutions of the corresponding system of 51 inequalities that yields 478 PW type 5-RSBFs with nonlinearity exceeding the bent concatenation bound 16256. As in the case $k = 3$, half of the solutions are obtained from the other half by complementing them, and so we present only one half in Table A2, in which the first four RTTs (with $\Delta_f = 160$ and 200) are the known PW constructions in [5]. The RTTs given in Table A2 are represented in hexadecimal form, e.g., the first RTT "7DCED1A915115" should be read as $(f(1), f(\xi^1), f(\xi^2), \ldots, f(\xi^{88}), f(\xi^{93})) = (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$.

4. Conclusion

We have defined the PW type n-variable k-RSBFs and performed efficient exhaustive searches for the PW type 15-variable functions in the classes of 3-RSBFs and 5-RSBFs. The search successfully finds 24 PW type 3-RSBFs and 470 PW type 5-RSBFs, which, while having nonlinearity greater than the bent concatenation bound, are not affine equivalent to the known PW constructions in [5]. These functions were not known before, and they can be used to obtain balanced functions with nonlinearity exceeding the bent concatenation bound by modifying their truth tables as in [11–13]. Moreover, our results confirm the nonlinearity bound in [10] for the 15-variable functions that are invariant under the action of $\mathrm{GF}(2^3)^* \times \mathrm{GF}(2^5)^*$.

References

[1] Matsui M. Linear cryptanalysis method for DES cipher. In: Advances in Cryptology - EUROCRYPT'93; 23–27 May 1993; Lofthus, Norway. pp. 386-397.

[2] Siegenthaler T. Decrypting a class of stream ciphers using ciphertext only. IEEE T Comput 1985; 34: 81-85.

[3] Carlet C, Khoo K, Lim CW, Loe CW. Generalized correlation analysis of vectorial Boolean functions. In: Fast Software Encryption - FSE 2007; 26–28 March 2007; Luxembourg City, Luxembourg. pp. 382-398.

[4] Meier W, Staffelbach O. Fast correlation attacks on stream ciphers. In: Advances in Cryptology - EUROCRYPT'88; 25–27 May 1988; Davos, Switzerland. pp. 301-314.

[5] Patterson NJ, Wiedemann DH. The covering radius of the $(2^{15},16)$ Reed-Muller code is at least 16276. IEEE T Inform Theory 1983; 29: 354-356.

[6] Kavut S, Maitra S, Yücel MD. Search for Boolean functions with excellent profiles in the rotation symmetric class. IEEE T Inform Theory 2007; 53: 1743-1751.

[7] Kavut S, Yücel MD. 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class. Inform Comput 2008; 208: 341-350.

[8] Gangopadhyay S, Keskar PH, Maitra S. Patterson-Wiedemann construction revisited. Discrete Math 2006; 306: 1540-1556.

[9] Kavut S, Maitra S. Patterson-Wiedemann type functions on 21 variables with nonlinearity greater than bent concatenation bound. IEEE T Inform Theory 2016; 62: 2277-2282.

[10] Kavut S, Maitra S, Özbudak F. A super-set of Patterson-Wiedemann functions – upper bounds and possible nonlinearities. In: International Workshop on the Arithmetic of Finite Fields - WAIFI 2016; 13–15 July 2016; Ghent, Belgium. pp. 227-242.

[11] Maitra S, Kavut S, Yücel MD. Balanced Boolean function on 13-variables having nonlinearity greater than the bent concatenation bound. In: Boolean Functions: Cryptography and Applications - BFCA 2008; 19–21 May 2008; Copenhagen, Denmark. pp. 109-118.

[12] Maitra S, Sarkar P. Modifications of Patterson-Wiedemann functions for cryptographic applications. IEEE T Inform Theory 2002; 48: 278-284.

[13] Sarkar S, Maitra S. Idempotents in the neighbourhood of Patterson-Wiedemann functions having Walsh spectra zeros. Design Code Cryptogr 2008; 49: 95-103.

[14] Zhang XM, Zheng Y. GAC – The criterion for global avalanche characteristics of cryptographic functions. J Univers Comput Sci 1995; 1: 316-333.

[15] Gong G. Theory and applications of q-ary interleaved sequences. IEEE T Inform Theory 1995; 41: 400-411.

[16] Gangopadhyay S, Maitra S. Crosscorrelation spectra of Dillon and Patterson-Wiedemann type Boolean functions. IACR Cryptology ePrint Archive 2004; 2004: 14.

[17] Filiol E, Fontaine C. Highly nonlinear balanced Boolean functions with a good correlation immunity. In: Advances in Cryptology - EUROCRYPT98; 3 May–4 June 1998; Espoo, Finland. pp. 475-488.

[18] Fontaine C. On some cosets of the First-Order Reed-Muller code with high minimum weight. IEEE T Inform Theory 1999; 45: 1237-1243.

Appendix

RTTs of the PW type 15-variable 3-RSBFs and 5-RSBFs.

Table A1. The 16 RTTs of the PW type 3-RSBFs with $NL_f > 16256$ (the first two functions have $NL_f = 16276$ and the rest have $NL_f = 16268$).

#	$(f(1), f(\xi^1), f(\xi^2), \ldots, f(\xi^{87}), f(\xi^{94}))$	Δ_f
1	(1,1,1,1,1,0,1,1,0,0,0,1,1,0,1,0,0,0,1,0,0,1,1,0,0,0,1,1,1,0,0)	160
2	(1,1,1,0,1,0,0,1,0,0,1,0,1,1,1,1,0,1,1,1,1,1,0,0,0,0,0,0,1,0,0)	160
3	(1,0,0,1,0,1,1,0,1,1,0,1,0,0,0,0,1,0,0,0,0,0,1,1,1,1,1,1,0,1,1)	200
4	(1,0,0,0,0,1,0,0,1,1,1,0,0,1,0,1,1,1,0,1,1,0,0,1,1,1,0,0,0,1,1)	200
5	(1,0,1,0,0,1,1,1,1,0,1,0,1,1,1,0,1,0,0,0,0,0,0,1,1,0,0,1,1,1,0)	176
6	(1,1,0,1,0,0,0,1,1,1,0,0,0,0,0,0,1,1,1,1,0,1,1,0,1,0,0,0,1,1,1)	176
7	(1,0,0,0,1,1,0,0,0,1,0,1,1,0,1,1,1,0,1,0,1,1,0,0,1,1,1,0,0,1,0)	176
8	(1,0,0,1,0,1,0,0,0,1,1,1,1,0,1,0,0,1,1,0,0,0,1,0,1,1,0,1,0,1,1)	232
9	(1,0,0,1,0,0,1,1,1,1,0,0,0,1,0,1,1,0,1,0,0,1,0,1,0,0,1,1,0,1,1)	232
10	(1,0,0,0,0,1,1,1,1,0,0,1,1,0,0,0,1,0,0,1,1,0,1,1,1,1,1,1,0,1,0,0)	232
11	(1,1,1,0,0,0,0,1,0,1,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,1,0,0,1,1,1,0)	280
12	(1,1,0,0,1,1,1,1,0,0,1,0,0,0,0,0,1,1,1,1,0,1,1,0,1,0,0,0,1,1,0)	280
13	(1,0,1,1,1,0,0,0,1,0,0,0,1,0,1,1,1,0,1,1,1,1,0,0,1,0,1,0,0,1,0)	280
14	(1,1,1,0,0,1,0,0,0,1,1,1,1,1,0,1,1,0,0,1,0,0,1,0,1,0,1,0,0,0,1)	416
15	(1,1,0,0,1,1,1,1,1,0,1,0,0,0,0,1,1,1,0,1,0,0,0,0,0,0,1,1,1,0,1,0)	416
16	(1,0,1,1,1,0,0,0,1,1,1,0,0,0,0,1,0,0,1,1,1,0,1,1,1,0,0,1,0,1,0)	416

Table A2. The 239 RTTs of the PW type 5-RSBFs with $NL_f > 16256$ (each row of the table shows three RTTs, except the last one in which there are two RTTs. The first two functions with $\Delta_f = 160$ have $NL_f = 16276$, and the rest have $NL_f = 16268$).

#	RTTs	Δ_f	RTTs	Δ_f	RTTs	Δ_f
1	7DCED1A915115	160	427D3154DEB19	248	436D65603E63E	280
2	74D3DAE18681E	160	7074353C975A5	248	5D3617151B88F	280
3	4B2C251E797E1	200	67B3DC6F040CA	248	534CED5B8D438	280
4	42312E56EAEEA	200	5E00FD0B59D93	248	5B212EA501FF6	280
5	70E721D645CF4	208	73E15EB02D50D	248	56B29CB0AF847	288
6	50C2D31FC78E5	208	6CB8F0E0E54D9	248	472D0EE837AE8	288
7	419FCD18656DA	208	4D5862121CFFE	248	417A24683FAEE	288
8	73A7552E2D960	208	5A35D74ABF401	248	6E12C0B918DFE	288
9	5B9260949975F	208	52A5F7DE09192	248	5363CFB45C914	288
10	42949D8F6F153	208	4B43D20E5DCB9	248	4CC025B617BAF	288
11	57BBC4AA3244E	208	5A3986258CDF9	248	45AB4EBE35483	288
12	695CEB638843B	208	69B6316F42AE8	248	7873D902F3135	288
13	6C33D35323D2C	208	6D7D389204DE5	248	547DF28901DB3	288
14	646D7069C28FB	208	7D875722D1A62	248	5F3AA3BF52048	288
15	64627A99F4E1A	224	6E835E102FB27	256	495DCC6AAC34D	288
16	641552FC0DCED	224	537242EDF1E18	256	7F3E5B41C0B22	288
17	500BC2B752BCF	224	58ECCA50F764A	256	7B9D9F2AA2026	288
18	574A6BA87098F	224	50D1A6A78475F	256	653A4D721D639	288
19	6983275A9ABAC	224	4C0050BFFBD93	256	4F7D9A99064C5	288
20	662CCAFF11741	224	6E8C3D106B1E7	256	706B3AF1CA1B4	296

Table A2. Continued.

21	5AD1F2A4C0E3D	224	66AFA49746358	256	626F202C847FF	296
22	4D3CCB8F99C42	224	5794A18393DEC	256	788CED22E351E	296
23	7EB58B00C3E3C	224	6DE0062BF916D	256	617CED598CD14	296
24	73445BA9413DE	224	5B5E3B10C3387	256	44A885C6475FF	296
25	5D6BAAF2C208B	224	5694F0C3AFC46	256	61066E1C5BE4F	312
26	4D0A0F995EED2	224	43DDCE3629439	256	60B548ED717C5	312
27	5D20239FE78C6	224	6CB223637F5A0	256	5D178E09CE5E8	312
28	6D302D6972B33	224	6FB75450186D5	256	64624F3336A3E	312
29	624D2BF0195AF	224	50EB6B43FA740	256	5173C2EF94E18	312
30	6EC37A9027A0F	224	4AADF76662A11	256	43411F5DFB550	320
31	5A898335754FC	224	68A20B19F5BF4	256	794F750E80DA3	320
32	4F2D40D3ADCAC	224	6BB7C1C5A886A	256	6DACA93E9260D	320
33	416AE55F348B5	224	45DC2D67268BA	256	67590DD0E9956	320
34	405E36E8DC7B1	224	534724DFD4F10	256	4C7DD2AA8D349	320
35	7F80E8E991A63	224	6493DE5E450B6	264	67B9B56A06343	320
36	610DD97CE3332	224	421BD61D7931D	264	5B1B40C66BD2B	320
37	5254B1EFC7458	224	56EC63B2A7A60	264	513C856FD85F0	320
38	5ACD3CACF2431	224	5E82E5D21E4F8	264	45E89D6AB6A2C	320
39	53B281F278D59	224	688F0FF4D8750	264	51C8DFAB9A605	320
40	4C151C784D7EB	232	71A8FB3E00E36	264	62BF9D68F06A0	320
41	78D81FDE40C8B	232	51EA6DFD6A401	264	7E9E7627805A8	320
42	6517A73492E53	232	6A8CE0AA4A7BD	264	72AF38586F305	320
43	5B7CE95131A51	232	6EAD8522F2536	264	67B53C586909E	320
44	53EAB4C864E78	232	686A239D4B17E	264	639F448DE5CC2	320
45	599615D4E74C3	232	509081EBBA5FE	272	4FE530871F645	320
46	62FEE883E2F40	232	4CA19C61EBF15	272	7A8C136593FC2	320
47	5FF106630C4F3	232	41C016293DFEF	272	4ACF9B02CAABC	320
48	7BE6774041A63	232	60B5016FA5EE9	272	6A32511FE672A	320
49	5D3D72C68EE10	232	5B66431BF9E40	272	7B516CE113E2C	320
50	5F0C87EB491AA	240	4FA142C7EBD81	272	60477A5FCD891	336
51	7DB6440D9B827	240	725C8F532693A	272	72D24AE1DA5F0	336
52	6BE1BF87004B9	240	655DB2CA8EC62	272	420DFA967AB19	336
53	786E3A5F43930	240	64C43CE752357	272	73A583EF018CE	336
54	6FE304B26EC31	240	6B74E033A6257	272	71C73C3B1E252	336
55	4D38A5B43076F	240	57771DA3490A6	272	542661CFB3F50	336
56	7C3B73501E1AC	240	72C75A4BCF890	272	7B2B2BF02628E	336
57	6A4FF005C2B3B	240	63405B9E56EAA	272	4D7DFB1294886	336
58	5F5568E32BC11	240	4C16A4F6A3A67	272	5F5A13F55006B	336
59	49DC0694ECD5D	240	502E0FF05C3DE	272	47A6954BC4BC3	336
60	548A93D7E0D35	240	7BC26251C9C3D	272	48B88451F3FC7	392
61	5BC83A0EC3B4D	240	646F7EF044B21	272	6F7D13007F164	392
62	5B523C823BA75	240	4D596B8978C8D	272	61C2744DF3A4E	392
63	4E68FBC1FC064	240	47B87656DD08C	272	5B65E2E8F0439	392
64	7026ADB685A6E	240	6CAB3C9827669	272	5A033D5C1A3BE	392
65	6499BCE4061BF	240	501947BEF0DC9	280	48A5A94F23CDB	392
66	4C0EB4AAE6FC4	240	50027D7C9F3C5	280	6DBC0F6DB0162	392
67	498A9E94CA73D	240	772E68C26A176	280	5B1DDB0AC9613	392
68	776A123E9610F	240	6155B97D35132	280	7FF36D449084A	392
69	6CA19D13169F6	240	4E76B13614E3A	280	5CB9D3359D144	392

Table A2. Continued.

70	5F7C2BA58304E	240	695C2F30B41AF	280	6ED64489076EE	392
71	407F68237A4F3	240	535BF01871367	280	63B984E9381F9	392
72	5B95E29235DC4	240	6D56787131497	280	47A8C89FF4A29	392
73	5729DC66D680D	240	6C1ED42DE4927	280	614455974DB7A	392
74	52C5B37B0A94E	240	543BF469F5610	280	47FABE586A034	392
75	44B9BCA4163CF	248	7A263DC5CA343	280	5E2A31F1713B8	392
76	52515D793E598	248	453FC01F919EA	280	5B0B39970A9EC	392
77	7BBBA44BCC0A4	248	7E017396D44BA	280	66D4AF6B1D10C	392
78	7A889B4393795	248	54B281E1BA97E	280	4284BFFAA8A65	392
79	6E6B4D121D82F	248	4C957394EF451	280	6AC766185F8F0	392
80	6B4D7E1E45681	248	49D20D7B34ED2	280		