point of access comes equipped with G_{pub}. Whenever someone requires an asset, the corresponding Fuzzy Sketch with trapdoor is computed. Depending on context, the access point sends the sketch at once or sends regularly a list containing several sketches to the authority. Hence, using the original personal data in the central database, the authority can apply the correction function with the trapdoor and so comparing with its reference, the authority can take the appropriate decision. This application is intended to protect the processing and the transmission to the database of personal data.

Now, suppose we want to avoid an attacker to have access to personal data in the database or to learn the membership of a given person directly from the database. We then construct the central database, not with personal data, but with the corresponding fuzzy sketches. Hence without the trapdoor, an attacker would not succeed in using the correction function Cor_{trap} (or an equivalent one), and so would not be able to link a personal data to a fuzzy sketch stored in the database. However, the authority, which possesses the knowledge of the trapdoor, can compute Cor_{trap} when an access point sends it data.

V. Conclusion

We show how to include a trapdoor into the Fuzzy Sketches of Juels and Wattenberg.

This renewal in the utilization of the cryptosystem of McEliece can also be viewed as a way of encrypting fuzzy data. And we hope that this will incite to retain more attention on public-key cryptosystem based on error-correcting codes. In particular, the correction capacity of—what we call—McEliece channel (errors that can be added to a hard instance of the cryptosystem of McEliece and corrected) has to be improved.

We give two examples of use of our ideas in Section IV and hope that our work might serve as inspiration for future work in this area, leading to new applications.

Acknowledgment

The authors wish to thank the anonymous referees for their useful suggestions which improved the presentation of this paper.

References

[1] C. M. Adams and H. Meijer, "Security-related comments regarding McEliece's public-key cryptosystem," in *Proc. Adv. Crypt.—CRYPTO*, 1987, pp. 224–228.

[2] ——, "Security-related comments regarding McEliece's public-key cryptosystem," *IEEE Trans. Inf. Theory*, vol. 35, pp. 454–455, 1989.

[3] X. Boyen, "Reusable cryptographic fuzzy extractors," in *Proc. ACM Conf. Comput. Commun. Sec.*, 2004, pp. 82–91.

[4] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith, "Secure remote authentication using biometric data," in *Proc. Adv. Crypt.—EUROCRYPT*, 2005, pp. 147–163.

[5] A. Canteaut and F. Chabaud, "A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511," *IEEE Trans. Inf. Theory*, vol. 44, pp. 367–378, 1998.

[6] G. Cohen and G. Zémor, "The wire-tap channel applied to biometrics," in *Proc. ISITA2004*, Parma, Italy, Oct. 10–13, 2004.

[7] ——, "Generalized coset schemes for the wire-tap channel: Application to biometric," in *Proc. IEEE Int. Symp. Inf. Theory*, Chicago, IL, Jun. 27–Jul. 2 2004.

[8] G. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through offline biometric identification," in *Proc. IEEE Symp. Sec. Priv.*, 1998, pp. 148–157.

[9] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Adv. Crypt.—EUROCRYPT 2004*, pp. 523–540.

[10] I. Dumer, D. Micciancio, and M. Sudan, "Hardness of approximating the minimum distance of a linear code," *IEEE Trans. Inf. Theory*, vol. 49, pp. 22–37, 2003.

[11] N. Frykholm and A. Juels, "Error-tolerant password recovery," in *Proc. ACM Conf. Comput. Commun. Sec.*, Philadelphia, PA, Nov. 6–8, 2001, pp. 1–9.

[12] T. Johansson and F. Jönsson, "On the complexity of some cryptographic problems based on the general decoding problem," *IEEE Trans. Inf. Theory*, vol. 48, pp. 2669–2678, 2002.

[13] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int. Symp. Inf. Theory*, 2002.

[14] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. ACM Conf. Comput. Commun. Sec.*, 1999, pp. 28–36.

[15] P. J. Lee and E. F. Brickell, "An observation on the security of McEliece's public-key cryptosystem," in *Proc. Adv. Crypt.—EUROCRYPT*, Davos, Switzerland, May 25–27, 1988, pp. 275–280.

[16] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *JPL DSN Progr. Rep.*, pp. 114–116, 1978.

[17] J. van Tilburg, "On the McEliece public-key cryptosystem," in *Proc. Adv. Crypt.—CRYPTO*, Santa Barbara, CA, Aug. 21–25, 1988, pp. 119–131.

On the Existence of $(9, 3, 5, 240)$ Resilient Functions

Ziad Saber, Mohammad Faisal Uddin, *Student Member, IEEE*, and Amr Youssef, *Senior Member, IEEE*

***Abstract*—Using a heuristic search technique, several examples for 9-variable Boolean functions with nonlinearity 240, algebraic degree 5, and resiliency degree 3 were constructed. This construction affirmatively answers the open problem about the existence of such functions.**

***Index Terms*—Boolean functions, cryptography, resilient functions.**

I. Introduction

Resilient functions are an important class of Boolean functions. These functions play a central role in several cryptographic applications [1], especially stream cipher design [2].

For basic definitions, a review of some recent results, and open problems related to resilient functions construction, the reader is referred to [3]–[5].

Let (n, m, d, NL) denote an n-variable, m-resilient Boolean function with algebraic normal form degree d and nonlinearity NL. Similarly, let $[n, m, d, NL]$ denote an unbalanced correlation immune function with the same notation as above.

Previous results have yielded $[9, 3, 5, 240]$ functions. However, the existence of $(9, 3, 5, 240)$ has been an open problem [5].

In this short correspondence, we answer this question affirmatively by providing some examples, obtained using a heuristic search technique, for these functions.

Throughout the rest of this section, we present some definitions and preliminaries used by our search procedure.

Manuscript received January 21, 2006; revised January 31, 2006. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada under Grant N00930.

Z. Saber and M. F. Uddin are with the Department of Electrical and Computer Engineering, Concordia University, Montreal, OC H3G 1M8, Canada (e-mail: z_saber@encs.concordia.ca; mf_uddinr@encs.concordia.ca).

A. Youssef is with Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC H3G 1MB, Canada (e-mail: youssef@ciise.concordia.ca).

Communicated by E. Okamoto, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2006.872862

The Hadamard–Walsh transform of $f : Z_2^n \to Z_2$ is defined by

$$F(w) = \sum_{x \in Z_2^n} (-1)^{f(x)} (-1)^{w \cdot x}$$

where $w \cdot x$ denotes the dot product between w and x, i.e.,

$$w \cdot x = \bigoplus_{i=1}^{n} w_i x_i .$$

If f is a resilient function of degree m, then $F(w) = 0$ for all w with Hamming weight less than or equal to m [6].

Lemma 1: The spectrum of any $(n, m, -, 2^{n-1} - 2^{m+1})$ function is necessarily a three-valued function $(0, \pm 2^{m+2})$, noting that $m > \lfloor n/2 - 2 \rfloor$ [3].

These functions with three-valued spectrum are known as plateaued functions [8].

Lemma 2: The algebraic degree of the function $(n, m, -, 2^{n-1} - 2^{m+1})$ is always maximum and equal to $n - m - 1$ [9].

Definition 1: $f_1 : Z_2^n \to Z_2$ and $f_2 : Z_2^n \to Z_2$ are said to have nonoverlapping Walsh transform coefficients iff $F_1(w) \neq 0 \Rightarrow F_2(w) = 0$ and $F_2(w) \neq 0 \Rightarrow F_1(w) = 0$ for all $w \in Z_2^n$.

II. Resilient Functions Construction by Spectral Inversion

Clark *et al.* [7] introduced the idea of Boolean functions construction by spectral inversion and applied it for the construction of several cryptographic functions of interest. The basic idea is to start with a set of Walsh coefficients that satisfy the required constraint. However, since it is not guaranteed that such a spectrum will be the Walsh spectrum for some Boolean function, our problem is reduced to finding a permutation such that when it is applied to this set, the resulting function obtained by applying the inverse Walsh transform to the permuted spectrum is Boolean. While a few permutations, after inverse Walsh transform, will correspond to Boolean functions, most will not. With each permutation, we associate a cost that indicates how far the permuted spectrum is from the spectrum of a valid Boolean function. The objective function, to be minimized, by our search[1] is given by [7]

$$\sum_{s \in Z_n 2^n} | \sum_{w \in Z_2^n} F(w) F(w \oplus s)) |.$$

Direct application of spectral inversion technique to construct a $(9, 3, 5, 240)$ function proved to be not successful [7] because of the huge permutation search space.

The following lemma follows directly from the basic definition of the Walsh transform.

Lemma 3: Let $f : Z_2^{n+2} \to Z_2$ be the function obtained from the concatenation of f_1, f_2, f_3, and f_4, $f_i : Z_2^n \to Z_2$, i.e., $f = [f_1 | f_2 | f_3, f_4]$. Then the Walsh transform F of f is given by

$$F = [\ F_1 + F_2 + F_3 + F_4 | F_1 - F_2 + F_3 - F_4 |\ F_1 + F_2 - F_3 - F_4 | F_1 - F_2 - F_3 + F_4\ ].$$

Lemmas 1–3 indicate that it is possible to construct an $(n, m, n - m - 1, 2^{n-1} - 2^{m+1})$ function where $m > \lfloor \frac{n}{2} - 2 \rfloor$ from the concatenation of four $(n - 2, m, n - m - 3, 2^{n-3} - 2^{m+1})$ functions with nonoverlapping Walsh coefficients, if such four functions exist.

[1]Our heuristic permutation search is based on a modified version of particle swarm optimization (PSO) [10], [11]. Details of PSO are outside the scope of this correspondence.

TABLE I
Two Examples for $(9, 3, 5, 240)$ Functions

5666A9A5969A69599A695996A595666A
39C659A6C9366A952ED1E41BD12E27D8
3C87C3D2B45A1EA56978692D87C3D23C
38CDD6236792897CC73229DC986D7683
0FD8E235F0271DCA74A3994E8B5C66B1
7A8525DAC43BA75819E6EC139B6452AD
3C966996696969C3C33C96C3C3963C3C
5666A9A5969A69599A695996A595666A

Thus, the search for $(9, 3, 5, 240)$ functions is reduced to finding four $(7, 3, 3, 48)$ functions with nonoverlapping spectrum coefficients. This helps us in reducing the search space dramatically compared to the direct search for a $(9, 3, 5, 240)$ function. The search algorithm starts by finding one $(7, 3, 3, 48)$ function, f_1 using spectral inversion, then proceeding to find the next function f_i, $i = 2, 3, 4$ with the following additional conditions on its Walsh transform:

$$F_{i-j}(w) \neq 0 \Rightarrow F_i(w) = 0 \text{ and } F_i(w) \neq 0 \Rightarrow F_{i-j}(w) = 0$$

where $1 \leq j \leq i - 1$.

Table I shows, in hexadecimal notation, two examples for $(9, 3, 5, 240)$ functions obtained, in few minutes, by our search.

References

[1] A. Menezes, P. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1996.

[2] T. Siegenthaler, "Correlation immunity of nonlinear combining functions for cryptographic applications," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 5, pp. 776–780, Sep. 1984.

[3] P. Sarkar and S. Maitra, "Nonlinearity bounds and constructions of resilient Boolean functions," in *Proc. Cypto 2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Speinger-Verlag, 2000, vol. 1880, pp. 515–532.

[4] S. Maitra and E. Pasalic, "Further construction of resilient Boolean function with very high nonlinearity," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1825–1834, Jul. 2002.

[5] P. Sarkar and S. Maitra, "Construction of nonlinear resilient Boolean functions using "small" affine functions," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2185–2193, Sep. 2004.

[6] X. Guo-Zhen and J. Massey, "A spectral characterization of correlation-immune combining functions," *IEEE Trans. Inf. Theory*, vol. 34, no. 3, pp. 569–571, May 1988.

[7] J. Clark, J. Jacob, S. Maitra, and P. Stanica, "Almost Boolean functions: The design of Boolean functions by spectral inversion," in *Proc. 2003 Congr. Evolutionary Computation*, vol. 3, Canberra, Australia, Dec. 2003, pp. 2173–2180.

[8] X. Zhang and Y. Zheng, "Plateaued functions," in *Proc. Int. Conf. Information and Communications Security (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, Nov. 1999, vol. 1726, pp. 284–300.

[9] C. Carlet, "On the coset of weight divisibility and nonlinearity of resilient and correlation immune functions," in *Advances in Cryptography CRYPTO 1991*. Berlin, Germany: Springer-Verlag, 1992, pp. 86–100.

[10] "Special issue on particle swarm optimization," *IEEE Trans. Evol. Comput.*, vol. 8, no. 3, Jun. 2004.

[11] X. Hu, R. C. Eberhart, and Y. Shi, "Swarm intelligence for permutation optimization: A case study of n-queens problem," in *Proc. 2003 IEEE Swarm Intelligence Symp.*, Indianapolis, IN, Apr. 2003, pp. 243–246.