A Life's Work on Hadamard Matrices, Statistical Designs, Bent Functions and their Application to Computer and Information Security in Networks and Telecommunications

Jennifer Seberry

1 Hadamard matrices in Space Communications

One hundred years ago, in 1893, Jacques Hadamard [21] found square matrices of orders 12 and 20, with entries ± 1, which had all their rows (and columns) orthogonal. These matrices, $X = (x_{ij})$, satisfied the equality of the following inequality

$$|det\ X|^2 \leq \Pi_{i=1}^{n} \sum_{j=1}^{n} |x_{ij}|^2$$

and had maximal determinant. Hadamard actually asked the question of matrices with entries on the unit disc but his name has become associated with the real matrices.

Hadamard was not the first to study these matrices for J.J. Sylvester in 1857 in his seminal paper "Thoughts on inverse orthogonal matrices, simultaneous sign-successions and tessellated pavements in two or more colours with application to Newton's rule, ornamental tile work and the theory of numbers" [55] had found such matrices for all orders which are powers of two. Nevertheless, Hadamard showed matrices with elements ± 1 and maximal determinant could exist for all orders 1, 2, and $4t$ and so the Hadamard conjecture "that there exists an *Hadamard matrix*, or square matrix with every element ± 1 and all row (column) vectors orthogonal" came from here. The survey by J. Seberry and M. Yamada [51] indicates the progress that has been made in the past 100 years.

Hadamard's inequality applies to matrices from the unit circle and matrices with entries ± 1, $\pm i$ and pairwise orthogonal rows (and columns) are called *complex Hadamard matrices* (note the scalar product is $a.b = \sum a_i b_i^*$ for complex numbers). These matrices were first studied by R.J. Turyn [58]. We believe complex Hadamard matrices exist for every order $n \equiv 0 \pmod 2$. The truth of this conjecture implies the truth of the Hadamard conjecture.

In the 1960's the U.S. Jet Propulsion Laboratories (JPL) was working toward building the Mariner and Voyager space probes to visit Mars and the other planets of the solar system. Those of us who saw early black and white pictures of the back of the moon remember that whole lines were missing. The first black and white television pictures from the first landing on the moon were extremely poor quality. How many of us remember that the recent fly-by of Neptune was from a space probe launched in the seventies? We take the high quality colour pictures of Jupiter, Saturn, Uranus, Neptune and their moons for granted.

In brief, these high quality colour pictures are taken by using three black and white pictures taken in turn through red, green and blue filters. Each picture is then considered as a thousand by a thousand matrix of black and white pixels. Each picture is graded on a scale of, say, one to sixteen, according to its greyness. So white is one and black is sixteen. These grades are then used to choose a codeword in, say, an eight error correction code based on, say, the Hadamard matrix of order 32. The codeword is transmitted to Earth, error corrected, the three black and white pictures reconstructed and then a computer used to reconstruct the coloured pictures.

Hadamard matrices were used for these codewords for two reasons, first, error correction codes based on Hadamard matrices have maximal error correction capability for a given length of codeword and, second, the Hadamard matrices of powers of two are analogous to the Walsh functions, thus all the computer processing can be accomplished using additions (which are very fast and easy to implement in computer hardware) rather than multiplications (which are far slower).

It was S. W. Golomb, L Baumert and Marshall Hall Jr [5] working with JPL who sparked the interest in Hadamard matrices in the past thirty years. They pioneered the use of computing in the construction of Hadamard matrices, the existence of which is an NPC problem (or a problem which has computational resources exponential in the input to find the answer but easy to check the answer once it has been given).

Sylvester's original construction for Hadamard matrices is equivalent to finding Walsh functions [24] which are the discrete analogue of Fourier Series.

Just as any curve can be written as an infinite Fourier series

$$\sum_n a_n \sin nt + b_n \cos nt$$

the curve can be written in terms of Walsh functions

$$\sum_n a_n \; sal(i,t) + b_n \; cal(i,t) = \sum_n c_n \; wal(i,t).$$

The hardest curve to model with Fourier series is the step function $wal_2(0,t)$ and errors lead to the Gibbes phenomenon. Similarly, the hardest curve to model with Walsh functions is the basic $\sin 2\pi t$ or $\cos 2\pi t$ curve. Still, we see that we can transform from one to another.

Many problems require Fourier transforms to be taken, but Fourier transforms require many multiplications which are slow and expensive to execute. On the other hand, the fast Walsh-Hadamard transform uses only additions and subtractions (addition of the complement) and so is extensively used, as

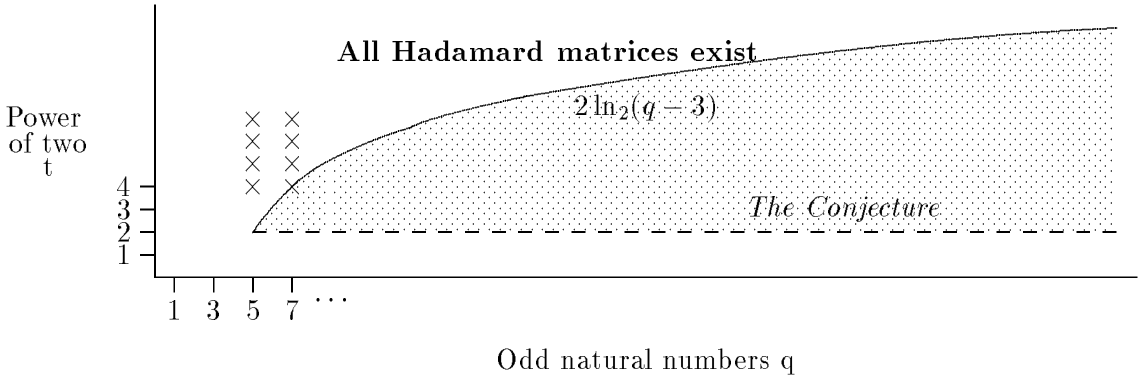

Figure 1: Hadamard matrix of order $2^t q$

the foundation of the Fast Fourier Transform, to transform power sequence spectrum density, band compression of television signals or facsimile signals or image processing.

Walsh functions are easy to extend to higher dimensions (and higher dimensional Hadamard matrices) to model surfaces in three and higher dimensions – Fourier series are more difficult to extend. Walsh-Hadamard transforms in higher dimensions are also effected using only additions (and subtractions). Some of the of the first significant papers describing Walsh-Hadamard transforms in higher dimensions is J Hammer and J Seberry [23, 22].

In 1976 Jennifer Seberry Wallis in her classic paper "On the existence of Hadamard matrices" [59] showed that "given any odd natural number q there exists a $t \approx 2\ ln_2(q-3)$ so that there is an Hadamard matrix of order $2^t q$ (and hence for all orders $2^s q,\ s \geq t$)". This was the first time a general bound had been given for all orders of Hadamard matrices. Previous results had been more ad hoc. To achieve this result she had to invent a whole new area of Discrete Mathematics known as "Orthogonal Designs". Her theorem is represented graphically in Figure 1.

This result has been improved by R. W. Craigen and H. Kharaghani [11, 26]. In fact, as was shown in Seberry and Yamada [51], Hadamard matrices are known to exist, of order $2^2 q$, for most $q < 3,000$ (we have results up to 40,000 which are similar). In many other cases Hadamard matrices of order $2^3 q$ or $2^4 q$ exist. A quick look shows most of the very difficult cases are for q (prime) $\equiv 3 \pmod 4$.

Hadamard's original construction for Hadamard matrices is a "multiplication theorem" as it uses the fact that the Kronecker product of Hadamard matrices of orders $2^a m$ and $2^b n$ is an Hadamard matrix of order $2^{a+b} mn$. Our graph shows we would like to reduce this power of two. In his book, *Hadamard Matrices and their Applications*, Agayan [4] shows how to multiply these Hadamard matrices to get an Hadamard matrix of order $2^{a+b-1} mn$ (a result which lowers the curve in our graph except for q, a prime). This result has been extended by R. Craigen, Jennifer Seberry and Xian-Mo Zhang showed this astonishing ability to reduce the powers of two on multiplication could also be extended to the multiplication of four matrices at a time [10].

Paley's 1933 "direct" construction [41] which gives Hadamard matrices of order $\Pi_{i,j}(p_i + 1).[2.(q_j + 1)]$, p_i (prime power) $\equiv 3 \pmod 4$, q_j (prime power) $\equiv 1 \pmod 4$ is extremely productive of Hadamard matrices but we note again the proliferation of powers of two as more products are taken. Paley also introduced matrices which, later when it became known that they gave the most efficient scheme for connecting a network for conference telephony, became known as conference matrices. To this day there are only four infinite classes of conference matrices known, Seberry pointed the way to the second of these classes and in [60], later Seberry and Whiteman [50] gave fourth and last discovered method.

Many people do not realize that in the same issue of the *Journal of Mathematics and Physics* as Paley's paper appears, J.A. Todd showed the equivalence of Hadamard matrices of order $4t$ and SBIBD$(4t-1, 2t-1, t-1)$. This family of SBIBD, its complementary family SBIBD$(4t-1, 2t, t)$ and the family SBIBD$(4s^2, 2s^2 \pm s, s^2 \pm s)$ are called *Hadamard designs*. The latter family satisfies the constraint $v = 4(k - \lambda)$ for $v = 4s^2$, $k = 2s^s \pm s$ and $\lambda = s^2 \pm s$ which appears in some constructions (e.g. Shrikhande [54]). Hadamard designs have the maximum number of one's in their incidence matrices of all incidence matrices of SBIBD(v, k, λ) (see Tsuzuku [57]). That Seberry [46] noted a special property of these matrices in "SBIBD$(4k^2$, $2k^2 + k$, $k^2 + k)$ and Hadamard matrices of order $4k^2$ with maximal excess are equivalent", led to a number of authors finding many families of new designs in this special class [30, 47, 33].

In 1944 J. Williamson [62], who coined the name *Hadamard determinants*, first constructed what have come to be called *Williamson matrices*, or with a small set of conditions, *Williamson type matrices*. These matrices are used to replace the variables of a formally orthogonal matrix. We say Williamson type matrices are "plugged in" to the second matrix. Other matrices which can be "plugged in" to arrays of variables are called *suitable matrices*. Generally the arrays into which suitable matrices are plugged are *orthogonal designs* which have formally orthogonal rows (and columns) but may have variations such as Goethals-Seidel arrays, Wallis-Whiteman arrays, Spence arrays, generalized quaternion arrays, Agayan families, Kharaghani's methods, regular s-sets of regular matrices which give new matrices. This is an extremely prolific method of construction. Seberry and her students have made extensive use of computers to amass data for relevant searches.

Another area which Seberry has popularized is the study of weighing matrices, which are square matrices, ($W(n, k) = W$ with elements 0, ± 1, which satisfy $WW^T = kI$. These matrices are interesting because they tell us hold to design the most efficient experiments to weigh very small objects and design masks for diffraction gratings for spectroscopic analysis.

Seberry conjectured that "if $n \equiv 0(mod 4)$ there exists a $W(n, k)$ for all k, $0 \leq k \leq n$". This has led to an explosion of interest around the world with email collaboration between Greece, Israel, Japan, Australia, Canada, Taiwan, USA and Mexico.

	Matrices	OD's
Strongest	Skew-weighing	$\mathrm{OD}(n; 1, k)$
	Weighing $W(n; k)$ n odd	
	Weighing $W(2n, k)$ n odd	$\mathrm{OD}(2n; a, b)$ n odd
	Weighing $W(4n, k)$ n odd	$\mathrm{OD}(4n; a, b, c, d)$ n odd
Weakest	$W(2^s n, k)$, n odd, $s \geq 3$	$\mathrm{OD}(2^s n; u_1, u_2, ..., u_s)$ n odd

Table 1: Weighing matrix and OD conjectures

Seberry and her co-authors have made many conjectures relating to weighing matrices, Hadamard matrices and orthogonal designs. The hierarchy of conjectures for weighing matrices and OD's is more straightforward. Settling the OD conjecture in Table 1 would settle the weighing matrix conjecture to its left.

2 Sequences in Telecommunications

Engineers concerned with finding the exact distance from their Earth base to the Moon, Venus and the other planets, or even to a moving aircraft, use radar signals which consist of sequences of binary entries, effectively 1 and -1. Unfortunately they have found that the type of single sequences they prefer to use, known as Barker sequences, apparently do not exist for lengths greater than 13.

A desire for longer usable sequences has prompted research engineers to consider sets of two or more binary and ternary sequences for these problems and others concerned with range, depth or information compression. Depending on the number of sequences and the alphabet of their description we have various sequences known as Golay, ternary pairs, Turyn, T-, base, normal, base, Yang and near-Yang sequences.

There has been an extensive search for Golay sequences but except for Turyn's result that these sequences exist for all lengths of the form $2^a 10^b 26^c$, where a, b and c are non-negative integers, all other results have proved negative. Recent theoretical work by Koukouvinos and Kounias [29], Koukouvinos, Kounias and Sotirakoglou [27] and Eliahou, Kervaire and Saffari [16, 17] show that Golay sequences do not exist for $n = 2p$ where p has any prime factor $\equiv 3 \pmod 4$. This means the unresolved cases < 200 are $n = 74, 82, 106, 116, 122, 130, 136, 146, 148, 164, 170, 178, 194$.

Seberry and her student and colleague Genet Edmonson and M Anderson [15], were able to establish that all Turyn sequences of length ≤ 43 were known, the longest length being 15. Given these disappointing results the search shifted to other kinds of 4 complementary sequences Seberry and her student Joan Cooper [9] were able to find sequences of commuting variable which led to the entire new field of *Orthogonal Designs*.

Recently Seberry and her student Marc Gysin [19, 20] have applied the powerful theory of cyclotomy to search for 2-complementary and 4-complementary sequences, supplementary differences, Hadamard matrices, weighing matrices, statistical designs such as D-optimal and SBIBD [28, 31, 33, 47, 48, 34, 42]. Cyclotomy has been used since the fundamental paper of Bose in 1939 to find balanced incomplete block designs for medical and agricultural experiments. D. Dokovic has used a similar approach to search for specials kinds of Hadamard matrices and D-optimal designs with considerable success. optimal designs [31].

Using another method Seberry and her colleague C Koukouvinos were able to find the first infinite family of the statistical designs known as D-optimal designs [32].

Seberry has also pioneered the whole field of *Bhaskar Rao Designs*, which are now coming to the fore in relation to perfect hashing functions and cryptographic functions.

3 Hadamard Matrices and Bent Functions for Network Security

There are two types of cryptographic algorithms: private key and public key. Public key algorithms are thought to be very secure in practice but too slow for high rates of data flow desired. Public key methods can be used in a hybrid system to transmit keys for use in private key encryption schemes which are needed to encrypt data at rates of megabytes per second.

Hadamard matrices and bent functions are used in the study of the design of S-boxes which are fundamental to the construction of cryptographically strong SPN algorithms (substitution-permutation-network)for private key cryptography.

Differential cryptanalysis and linear cryptanalysis, discovered by Biham and Shamir[6] and Matsui [36] respectively, are currently the most powerful cryptanalytic attacks against (secret-key) encryption ciphers (algorithms), especially against DES-like substitution-permutation ciphers. The attacks also apply to other cryptographic primitives such as one-way functions. Since the introduction of differential cryptanalysis, researchers have devoted considerable effort to the design of S-boxes (substitution boxes) which are the core of many modern private key data encryption and hashing algorithms such as DES, LOKI, CASE, MD4, MD5 and HAVAL.

Seberry, as leader of the team which designed the LOKI family of encryption algorithms [7] and the HAVAL family [64] of hashing algorithms, encouraged the use of discrete mathematics and number theory in the design of these families. This is crucial as all hashing algorithms, except HAVAL which is based on Hadamard matrices and bent functions, have been compromised by mathematical insights into their structures. Cryptanalysts have shown LOKI is stronger than DES. Seberry introduced the study of *bent function* to the academic researchers in Australia.

The strength of a cryptographic algorithm is primarily determined by that of the S-boxes employed by the algorithm and its key schedule which determines how to incorporate the secret key. In the recent past, a number of criteria for designing strong S-boxes have been identified by researchers in the field, including Gordon and Retkin [18], Webster and Tavares [61], Adams and Tavares [1, 2, 3], O'Connor [40], and Seberry, Zhang and Zheng [52]. Some of the criteria include high nonlinearity, the strict avalanche criterion (SAC), high order propagation, high nonlinear order and correlation immunity. While it is relatively easy to design S-boxes that satisfy some of these criteria, it has not been possible to have them satisfy all the criteria, since a few of the criteria seem to contradict each other. It is even more difficult to design S-boxes that balance the various criteria and resist the two most powerful known cryptanalytic attacks, differential cryptanalysis [6] and linear cryptanalysis [36].

Important "cryptographic criteria" that have to be taken into consideration include those for individual functions [3, 12, 37] and those for a set of functions. Criteria for individual functions include:

(i) being balanced, (ii) being highly nonlinear, (iii) satisfying the strict avalanche criterion (SAC), (iv) satisfying the propagation criterion, (v) having high nonlinear order (i.e. algebraic degree), (vi) satisfying the correlation immunity criterion, (vii) having no or small number of linear structures.

The above criteria are largely motivated by the two principles for security: "confusion" and "diffusion". The confusion means that the dependence of the key on the plaintext and ciphertext should be very complex, while the diffusion requires that each bit of plaintext and each bit of key influence each bit of ciphertext. For example, the nonlinearity is for confusion, while the SAC is for diffusion.

Only a few researchers have attempted to make a detailed study of the complex inter-relationships between the various cryptographic criteria.

In many cryptographic designs we not only require the individual component functions of the S-box to have good cryptographic properties but also consider correlations among these individual functions [2, 12, 14, 39, 56]. This is best shown by linear cryptanalysis which exploits low nonlinearity of linear combinations of the component functions of an S-box. Consequently, each nonzero linear combination of the components should satisfy a number of strict conditions.

Seberry and her colleagues X-M Zhang and Y Zheng [53] used group Hadamard matrices, which are closely related to Bhaskar Rao designs [45], and generalized Hadamard matrices [44] to obtain extremely secure cryptographic boolean functions.

To counter the differential attack, it has been realized that S-boxes should have good difference distribution tables. Based on early work in [2, 12, 14, 39, 56], Seberry and X-M Zhang identified the three principles for strong difference distribution tables of S-boxes which is captured by a measurement called *robustness*. So far no efficient method has been found to generate S-boxes having good difference distributions and also satisfying other criteria.

4 Privacy, Computer and Network Security

Seberry has made other significant contributions to privacy and security.

With her student and colleague M Miller [38] she introduced the concept of *relative compromise* of statistical databases. This gave a new and unforeseen method to compromise the confidentiality and privacy of information and is based on combinatorial designs.

She led the team which proposed beaconising networks [25] to provide authentication services. The advantage of this method is that it avoids previous protocol problems associated with replay attacks and provides an alternative to timestamping. She has studied a number of other scenarios (see for example [13]) involving the real problem of all networks, authentication, are you sure you are communicating with the party with whom you think you are communicating.

The Zheng-Seberry [65] public key system is one of the very few extant public key cryptosystems.

References

[1] C. M. Adams. On immunity against Biham and Shamir's differential cryptanalysis. *Information Processing Letters*, 41:77–80, 1992.

[2] C. M. Adams and S. E. Tavares. Generating and counting binary bent sequences. *IEEE Transactions on Information Theory*, 36(5):1170–1173, 1990.

[3] C. M. Adams and S. E. Tavares. The use of bent sequences to achieve higher-order strict avalanche criterion. Technical Report TR 90-013, Department of Electrical Engineering, Queen's University, 1990.

[4] S. S. Agaian. In *Hadamard Matrices and their Applications*, volume 1168 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-Heidelberg-New York, 1985.

[5] L. D. Baumert, S. W. Golomb, and M. Hall Jr. *Bull. Amer. Math. Soc.*, 68:237–238, 1962.

[6] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

[7] L. P. Brown, M. Kwan, J. Pieprzyk and J. Seberry, Improving resistance to differential cryptanalysis and the redesign of LOKI, *Advances in Cryptology -ASIACRYPT'91*, eds. H. Imai, R. L. Rivest and T. Matsumoto, 739, Lecture Notes in Computer Science, Springer-Verlag, (1993), p36-50.

[8] Claude Carlet, Jennifer Seberry and Xian-Mo Zhang, Comments on "generating and counting binary bent sequences," *IEEE Trans Inf Theory*, 40, (1994), 600-600.

[9] Joan Cooper and Jennifer Wallis. A construction for hadamard arrays. *Bull. Austral. Math. Soc.*, 7:269–278, 1972.

[10] R. Craigen, Jennifer Seberry, and Xian-Mo Zhang. Product of four hadamard matrices. *J. Combinatorial Th. (Ser A)*, 59:318–320, 1992.

[11] R. C. Craigen, W. Holtzmann, and H. Kharaghani. On the asymptotic existence of complex hadamard matrices. *Journal of Combinatorial Designs*. To appear.

[12] M. H. Dawson and S. E. Tavares. An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks. In *Advances in Cryptology - EUROCRYPT'91*, volume 547 of *Lecture Notes in Computer Science*, pages 352–367. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[13] Yvo Desmedt and Jennifer Seberry, Practical proven secure authentication with arbitration, (Jennifer Seberry and Yuliang Zheng, (Eds.)) *Advances in Cryptography - Auscrypt'92,* Conference held at the Gold Coast, Australia, December 1992, 718, Lecture Notes in Computer Science, Springer-Verlag, Berlin–Heidelberg–New York, (1993), 27-32.

[14] J. Detombe and S. Tavares. Constructing large cryptographically strong S-boxes. In *Advances in Cryptology - AUSCRYPT'92*, volume 718 of *Lecture Notes in Computer Science*, pages 165–181. Springer-Verlag, Berlin-Heidelberg-New York, 1993.

[15] Genet M'gan Edmonson, Jennifer Seberry, and Malcolm Anderson. On the existence of Turyn sequences of length less than 43. *Mathematics of Computation*, 62:351–362, 1994.

[16] S. Eliahou, M. Kervaire, and B. Saffari. A new restriction on the lengths of Golay complementary sequences. *J. Combin. Th. (Ser A)*, 55:49–59, 1990.

[17] S. Eliahou, M. Kervaire, and B. Saffari. On Golay polynomial pairs. *Adv in Appl. Math.*, 12:235–292, 1991.

[18] J. Gordon and H. Retkin. Are big S-boxes best? In *Proc of the Workshop on Cryptography*, Lecture Notes in Computer Science, pages 257–262. Springer-Verlag, Berlin-Heidelberg-New York, 1982.

[19] Marc Gysin and Jennifer Seberry. Construction methods for weighing matrices of order $4n$ and weight $4n-2$, $2n-1$ and n using elementary properties of cyclotomy. In *Conference on Combinatorial Mathematics and Combinatorial Computing*, Auckland, 1994.

[20] Marc Gysin and Jennifer Seberry. New weighing matrices through linear combinations of generalized cosets. In *Conference on Combinatorial Mathematics and Combinatorial Computing*, University of Technology, Sydney, jul 1996.

[21] J. Hadamard. Résolution d'une question rélative aux determinants. *Bull. des Sciences Mathematiques*, 17:240–246, 1893.

[22] J. Hammer and Jennifer Seberry. Higher dimensional orthogonal designs and hadamard matrices ii. *Congressus Numerantium*, 27:23–29, 1979. Proceedings of the Nineth Manitoba Conference on Numerical Mathematics.

[23] J. Hammer and Jennifer Seberry. Higher dimensional orthogonal designs and applications. *IEEE Transactions on Information Theory*, 27(6):772–779, 1981.

[24] Henning F Harmuth. *Transmission of Information by Orthogonal Functions*. Springer-Verlag, Berlin-Heidelberg-New York, 1972.

[25] Azad Jiwa, Thomas Hardjono and Jennifer Seberry, Beacons for authentication in distributed systems, *J Computer Security*, 4, (1996) 81-96.

[26] H. Kharaghani. A construction for block circulant orthogonal designs. *Journal of Combinatorial Designs*, 1996.

[27] C. Koukouvinos, C. Kounias, and K. Sotirakoglou. On Golay sequences. *Disc. Math.*, 92:177–185, 1991.

[28] C. Koukouvinos, M. Mitrouli, and Jennifer Seberry. On the smith normal form of d-optimal designs. *J. Linear and Multilinear Algebra*, 247:277–295, 1996.

[29] Christos Koukouvinos and Stratis Kounias. There are no Golay sequences of length 2.7^t. *Discrete Math.* To appear.

[30] Christos Koukouvinos, Stratis Kounias, and Jennifer Seberry. Further hadamard matrices with maximal excess and new SBIBD($4k^2$, $2k^2 + k$, $k^2 + k$). *Utilitas Math.*, 36:135–150, 1989.

[31] Christos Koukouvinos, Stratis Kounias, and Jennifer Seberry. Supplementary difference sets and optimal designs. *Discrete Math.*, 87:49–58, 1991.

[32] Christos Koukouvinos, Stratis Kounias, and Jennifer Seberry. Supplementary difference sets and optimal designs. *Discrete Math.*, 87:49–58, 1991.

[33] Christos Koukouvinos and Jennifer Seberry. Construction of new hadamard matrices with maximal excess and infinitely many new

SBIBD($4k^2$, $2k^2 + k$, $k^2 + k$). In Rolf Rees, editor, *Graphs, Matrices and Designs: A Festschrift for Norman J. Pullman*, Lecture Notes in Pure and Applied Mathematics. Marcel Dekker, 1992.

[34] Thomas Kunkle and Jennifer Seberry. A few more small defining sets for SBIBD($4t-1, 2t-1, t-1$). *Bull. Inst. Comb. and Appl.*, 12:61–64, 1994.

[35] John Loxton, David S.P. Khoo, Gregory J. Bird and Jennifer Seberry, A cubic RSA code equivalent to factorisation, *J. Cryptology,* 5,(1992), 139-150.

[36] M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, Berlin-Heidelberg-New York, 1994.

[37] W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology - EUROCRYPT'89*, volume 434 of *Lecture Notes in Computer Science*, pages 549–562. Springer-Verlag, Berlin, Heidelberg, New York, 1990.

[38] Mirka Miller and Jennifer Seberry, Relative compromise of statistical databases, *Australian Computer Society*, 21, (1989) 56-62.

[39] K. Nyberg. Differentially uniform mappings for cryptography. In *Advances in Cryptology - EUROCRYPT'93*, volume 756 of *Lecture Notes in Computer Science*, pages 55–65. Springer-Verlag, Berlin-Heidelberg-New York, 1994.

[40] L. O'Connor. *Affinity and Degeneracy in Boolean Functions with Applications to Cryptography.* Phd thesis, Queen's University, Ontario, Department of Electrical Engineering, 1992.

[41] R. E. A. C. Paley. On orthogonal matrices. *J. Math. Phys.*, 12:311–320, 1933.

[42] Dinesh Sarvate and Jennifer Seberry. A note on small defining sets for some SBIBD($4t-1,\ 2t-1,\ t-1$). *Bull. Inst. Comb. and Appl.*, 10:26–32, 1994.

[43] Jennifer Seberry, Some remarks on generalized Hadamard matrices and theorems of Rajkundlia on SBIBDs, *Combinatorial Mathematics VI.* Lecture Notes in Mathematics, Vol. 748, Springer-Verlag, Berlin-Heidelberg-New York, (1979), 154-164.

[44] Jennifer Seberry, A construction for generalized Hadamard matrices, *J. Statistical Inference and Planning*, 4, (1980), 365-368.

[45] Jennifer Seberry, Generalized Bhaskar Rao designs with block size three, *J.Statistical Planning and Inference*, 11, (1985), 373-380.

[46] Jennifer Seberry. SBIBD($4k^2$, $2k^2 + k$, $k^2 + k$) and hadamard matrices of order $4k^2$ with maximal excess are equivalent. *Graphs and Combinatorics*, 5:373–383, 1989.

[47] Jennifer Seberry. Existence of SBIBD($4k^2$, $2k^2 + k$, $k^2 + k$) and hadamard matrices with maximal excess. *Austral. J. Combinatorics*, 4:87–92, 1991.

[48] Jennifer Seberry. On small defining sets for some SBIBD($4t - 1$, $2t - 1$, $t - 1$). *Bull. Inst. Comb. and Appl.*, 4:58–62, 1992.

[49] Jennifer Seberry and David Skillicorn, All directed BIBDs with k = 3 exist, *J. Combinatorial Theory (Ser. A)*, 29, (1980), 244-248.

[50] Jennifer Seberry and A.L. Whiteman. A new construction for conference matrices. *Ars. Combinatoria*, 16:119–127, 1983.

[51] Jennifer Seberry and Mieko Yamada. Hadamard matrices, sequences, and block designs. In D. J. Stinson and J. Dinitz, editors, *Contemporary Design Theory - A Collection of Surveys*, pages 431–560. John Wiley and Sons, 1992.

[52] Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. Systematic generation of cryptographically robust s-boxes. In *Proceedings of the First ACM Conference on Computer and Communications Security*, pages 171–182, Fairfax, VA, 1993. The Association for Computing Machinery.

[53] Jennifer Seberry, Xian-Mo Zhang and Yuliang Zheng, Cryptographic boolean functions via group Hadamard matrices, *Australas. J. Combin.*, 10, (1994), 131-145.

[54] S. S. Shrikhande. On a two parameter family of balanced incomplete block designs. *Sankhya (Ser. A)*, 24:33–40, 1962.

[55] J. J. Sylvester. Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. *Phil. Mag.*, 34:461–475, 1867.

[56] S. E. Tavares, M. Sivabalan, and L. E. Peppard. On the designs of SP networks from an information theoretic point of view. In *Advances in Cryptology - CRYPTO'92*, volume 740 of *Lecture Notes in Computer Science*, pages 260–279. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[57] T. Tsuzuku. *Finite Groups and Finite Geometries.* Cambridge University Press, Cambridge, 1982.

[58] R. J. Turyn. *Complex Hadamard matrices, Structures and their Applications.* Gordon and Breach, New York, 1970.

[59] J. Seberry Wallis. On the existence of hadamard matrices. *J. Combin. Th. (Ser. A)*, 21:188–195, 1976.

[60] Jennifer Wallis. Some (1, -1) matrices. *J. Combinatorial Theory, Ser. B.*, 10:1–11, 1971.

[61] A. F. Webster and S. E. Tavares. On the design of S-boxes. In *Advances in Cryptology - CRYPTO'85*, volume 219 of *Lecture Notes in Computer Science*, pages 523–534. Springer-Verlag, Berlin-Heidelberg-New York, 1986.

[62] J. Williamson. Hadamard's determinant theorem and the sum of four squares. *Duke Math. J.*, 11:65–81, 1944.

[63] A. M. Youssef and S. E. Tavares. Resistance of balanced S-boxes to linear and differential cryptanalysis. *Information Processing Letters*, 56:249–252, 1995.

[64] Yuliang Zheng, Josef Pieprzyk and Jennifer Seberry, HAVAL - A one-way hashing algorithm with variable length output, ed. Jennifer Seberry and Yuliang Zheng, *Advances in Cryptography - Auscrypt'92*, Conference held at the Gold Coast, Australia, December 1992, Vol 718, Lecture Notes in Computer Science, Springer-Verlag, Berlin-Heidelberg-New York, 1993, 83-104.

[65] Yuliang Zheng and Jennifer Seberry, Immunizing public key cryptosystems against chosen ciphertext attacks, *IEEE J on Selected Areas in Communications*, 11, (1993), 715-724.

*Final Remark: Drs Eliahou, Kervaire and Saffari have asked me to clarify this statement; Koukouvinos, Kounias and Sotirakoglou excluded Golay sequences of lengths $2 \cdot 7^t$, lengths $2 \cdot p$, $p \equiv 3 \pmod 4$ which were excluded by Shalom Eliahou, Michel Kervaire and Bahman Saffari.