Des. Codes Cryptogr. (2015) 77:287–299
DOI 10.1007/s10623-015-0106-2

Guest Editorial: Special Issue in Honor of Scott A. Vanstone

Ian Blake[1] · **Alfred Menezes**[2] · **Doug Stinson**[2]

Published online: 8 July 2015

On March 2, 2014, Scott Vanstone passed away at his home in Campbellville, Canada, after a short battle with cancer.

Scott completed his Ph.D. in 1974 under the supervision of Ron Mullin at the University of Waterloo. His Ph.D. thesis and much of his early work was in combinatorial design theory. In the 1980s he started working in cryptography. During his career, he made many contributions to the fields of design theory and cryptography. He was very influential in the development, standardization, deployment and commercialization of elliptic curve cryptography. He authored several widely-used books including *An Introduction to Error Correction Codes with Applications* (with Paul van Oorschot), *Applications of Finite Fields* (with Ian Blake, Shuhong Gao, Alfred Menezes, Ron Mullin and Tomik Yaghoobian), *Handbook of Applied Cryptography* (with Alfred Menezes and Paul van Oorschot), *Guide to Elliptic Curve Cryptography* (with Darrel Hankerson and Alfred Menezes), and *Introduction to Mathematical Thinking: Algebra and Number Systems* (with Will Gilbert). In 1990, he co-founded the journal *Designs, Codes and Cryptography* with Dieter Jungnickel and Ron Mullin, and served as its Editor-in-Chief until 1999.

This volume of *Designs, Codes and Cryptography* is a recognition of Scott's contributions and influence in the areas of cryptography, coding theory, combinatorial design theory, and finite fields. It begins with tributes written by Dieter Jungnickel, Neal Koblitz, Esther Lamken, Peter Landrock and Ron Mullin, and complete lists of his Ph.D. students and publications. This is followed by the contributed papers, written by some of Scott's close collaborators, colleagues and friends.

✉ Alfred Menezes
ajmeneze@uwaterloo.ca

Ian Blake
ifblake@ece.ubc.ca

Doug Stinson
dstinson@uwaterloo.ca

[1] University of British Columbia, Vancouver, BC V6T 1Z4, Canada

[2] University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

Scott had an impressive ability to determine interesting and important problems. His enthusiasm and imagination for research together with a tireless energy in pursuing it were hallmarks of his career. He was among the first to recognize the significance and potential of the discrete logarithm problem on elliptic curves, an area that generated enormous interest over the past few decades. His generosity in sharing his ideas and working with friends, colleagues and new researchers to the field was unparalleled. His wonderful sense of humour, outgoing personality and constant friendship will be missed by those of us fortunate enough to have known and worked with him.

1 Scott A. Vanstone (1947–2014)

1.1 Dieter Jungnickel

The first time Scott and I met was in May 1978, during an Oberwolfach meeting on *Finite Geometries*. We kept meeting at conferences, and in 1984 (when I was visiting the University of Toronto) Scott invited me for my first talk in Waterloo. We made plans for collaborating then, and during the years from 1986 to 1999 we published 17 joint papers. From 1985 to 1999, I visited Waterloo regularly, since 1994 as an Adjunct Professor. I am very grateful for this long and fruitful research collaboration. During one of my visits, we conceived the idea of starting a new high-level journal, which led to the foundation of *Designs, Codes and Cryptography* in 1990, jointly with Ron Mullin.

Of course I cannot describe everything we worked on, the areas ranging from designs and finite geometries via finite fields to graphs and codes. So I'll just mention one topic in more detail, namely graphical codes. It had been known for some time that the cycle space of a connected graph G yields an interesting binary code, which goes back to pioneering papers by Bredeson and Hakimi in the late 1960s: if G has m edges, n vertices, and girth g, one obtains a binary $[m, m - n + 1, g]$-code. We decided to study this topic in more depth, which resulted in seven papers [167,170,171,174,175,179,180]. In particular, we analyzed two construction methods which can be used to augment the cycle space codes and which tend to produce graphical codes of large dimensions. We then used techniques from combinatorial optimization to devise decoding procedures which turned out to have basically linear complexity (in the length of the code) and were thus considerably more efficient than previous approaches to decoding graphical codes. These results were then also extended to ternary and even general q-ary codes.

Moreover, we found interesting connections between extensions of codes based on complete graphs, (shortened) Hamming codes, and codes with minimum distance 5. Finally, we also managed to apply graphical codes to graphical enumeration, where we gave an elegant proof of Read's theorem on the generating function for the number of Eulerian graphs with p vertices and also obtained a new analogous result for bipartite Eulerian graphs.

It was a real privilege to know Scott, not only for our research but also very much on a personal level: over the years, a close friendship developed. I can recall a multitude of pleasant non-mathematical encounters, like going to the theatre or concerts or simply meeting for drinks or dinner, mostly in Canada but also several times when Scott came to Germany. I am sure that his legacy will remain alive for a long time, and that he will always be fondly remembered by his many friends and associates. Personally, I deeply miss him.

1.2 Neal Koblitz

I first met Scott at Crypto '88. He had a few questions and observations about elliptic curve cryptography (ECC) and told me about the work he was doing on implementation. At that time he was the only person I knew who believed that ECC could be commercialized in the immediate future as a practical alternative to RSA.

Soon after, he invited me to visit Waterloo, where he was leading an interdisciplinary team that had developed improved algorithms and chips for finite field arithmetic and was starting to do the same for elliptic curve computations. Scott's team of mathematicians, computer scientists, and engineers, which included faculty, graduate students, and even undergraduates, was ahead of its time. This was well before "transdisciplinarity," "vertical integration," and "undergraduate research" became buzzwords in academia.

Many researchers work on problems in math and computer science that are peripherally related to cryptography and obtain results that have little or no significance for real-world data security. Not Scott. He consistently focused on mathematical problems that are of central importance in practice. For example, in 1993, in joint work with Menezes and Okamoto [159], he found the first successful attack on the Elliptic Curve Discrete Log Problem (whose assumed intractability forms the basis of ECC) that applies to an important class of curves (those with "low embedding degree"). In the 1990s Scott designed the Elliptic Curve Digital Signature Algorithm (ECDSA) and worked hard to get it standardized and deployed. The ECDSA has stood the test of time and today is widely used in applications ranging from smartphones to Bitcoin.

Scott had a delightful sense of humor and sense of fun. After the movie "Sneakers" came out in 1992, he and I were discussing whether it might stimulate more public interest in cryptography. Scott thought it would be cool for the IACR to give Robert Redford, the star of the film, a special award at the next Crypto meeting. Scott was on the IACR Board, but when he proposed it, other Board members thought it would be undignified for a high-brow academic conference to give such an award, and they rejected the idea.

Scott was also generous—to students, colleagues, and philanthropic causes. He and his wife Sherry Shannon-Vanstone have made large annual donations to support the Kovalevskaia Grants for Mexican women mathematicians, a joint project of the Kovalevskaia Fund and the Mexican Mathematical Society.

Scott was an inspiration to those who knew him.

1.3 Esther Lamken

Scott's first love in mathematics was combinatorial design theory. He wrote his thesis in 1974 on the structure of (r, λ)-designs. This was an exciting time to be in design theory; the Kirkman Schoolgirl Problem and the Room square problem (both from the 1850s) had recently been solved. It was the beginning of a period of tremendous growth in design theory and Scott contributed greatly to this growth with over 130 papers in design theory and related areas of coding theory. He made fundamental contributions to several areas of design theory, and his early results included work on mutually orthogonal Latin squares, (r, λ)-designs, balanced tournament designs, and Howell designs. He was a master of combinatorial constructions and recursions and one of the first to use computers and combinatorial searches for designs. Direct constructions (often rooted in algebraic constructions and geometry) combined with combinatorial recursions allowed him to completely settle several existence problems.

One of Scott's most important contributions in design theory was his work on designs with orthogonal resolutions. Scott's interest in coding theory had led him to investigate equidistant permutation arrays which can be thought of as error correcting codes. In [10], Scott (with Deza and Mullin) showed that doubly resolvable balanced incomplete block designs could be used to construct EPAs. This began a fruitful investigation on designs with orthogonal resolutions; a few early noteworthy papers are [11,16,27,31,41,42,45,46,51]. With the smallest case (Room squares) settled, Scott turned his attention to larger block sizes. Scott had an amazing talent for discovering and seeing structure in finite geometries and he discovered new connections between finite projective and affine geometries and designs with orthogonal resolutions. With Ryoh Fuji-Hara (his first PhD student), he did a considerable amount of work on orthogonal resolutions of lines in geometries. They constructed the first infinite classes of doubly resolvable BIBDs for prime power block sizes. Scott spent a great deal of time and effort on the existence of DR$(v, 3, 1)$-BIBDs which he called Kirkman squares. He encouraged many of us to work on this difficult problem, a generalization of both the Room square and Kirkman Schoolgirl problems. His ideas played an important role when we (Colbourn, Lamken, Ling, Mills) finally settled the problem in 2002. His work on designs with orthogonal resolutions was unique and demonstrated his ability to find new connections between designs, finite geometries, and coding theory. I was Scott's second PhD student, and Scott and I did a lot of work together on designs with orthogonal resolutions and on special types of balanced tournament designs. We determined the spectrum for both factored BTDs and partitioned BTDs and discovered new connections to other designs; see [121] for an early survey. As I work on existence questions for designs with orthogonal resolutions and generalized BTDs and Kirkman squares, I am often reminded of Scott's ideas and creativity in design theory.

I was fortunate to be Scott's student; he was a wonderful advisor, mentor, collaborator, and friend. He was always enthusiastic and generous with his ideas and time. We met quite frequently to discuss research. I still remember a phone call I got from him as a grad student. It was Saturday and he called to tell me how much he liked the material I'd just given him and to tell me the ideas it had given him for new research. It was characteristic of Scott—thoughtful, generous, and inspiring! When I remember Scott these days, I think back to all those afternoons spent happily discussing research over coffee and I treasure those times.

1.4 Peter Landrock

The first time I really became aware of Scott's contributions in cryptography was in 1992, when we both ran for presidency of the IACR. I won by a few votes—not because I was a better cryptographer, on the contrary, I was relatively new to the field—but because I had the good fortune of serving as the general chair of Eurocrypt '90 in Aarhus, Denmark, which had gone very well, and I simply won because of that.

With a strong mathematical background, I had been somewhat disappointed with the lack of quality of mathematics in some of the articles that had been accepted in some of the Eurocrypt conferences back then. But this soon changed as a number of excellent mathematicians, as Scott, were drawn to the field, and I was particularly delighted to learn that the person I had been running against was a first-rate mathematician.

But what impressed me most at the time with Scott—and continued to impress me—was that he was one of the few persons who had managed to build an impressive company in the areas of applied cryptography, Certicom—and yet to continue serious research in pure mathematics in parallel. It was exactly the commercial potential that had fascinated me when I started teaching that subject around the time Certicom was founded. Scott immediately grasped the potential of elliptic curves in secure communication, and went for it. His work on elliptic curves over characteristic 2 finite fields with Gord Agnew and Ron Mullin quickly made Certicom a highly respected company, which more than anything was based on Scott's insight into elliptic curves, his evangelism on the subject, and his active participation in the company.

I started Cryptomathic the year after Certicom was founded with my students Ivan Damgård and Jørgen Brandt, and during the 1990s a common interest and respect for each other's commercial efforts developed between Scott and me, to the extent that at Eurocrypt 2000 in Belgium we were very close to announcing that Certicom had acquired Cryptomathic. But in spite of this not happening, our friendship continued right until the sad day where Scott passed away much too early. Even though we would always begin our conversations on commercial aspects of our companies when we met, we would most of the time switch to mathematical problems instead after a short while.

1.5 Ron Mullin

Early one afternoon in 1972, a young man whom I had not met, walked into my office and said "Sir, I want to be your graduate student." I talked to him for a while and said to myself "I definitely want this young man to be my graduate student", and so began my lifelong friendship and many years of collaboration with Scott Vanstone.

Scott wrote an outstanding dissertation and graduated with his Ph.D. in 1974, and soon became well-known for his work in design theory. One strong indicator of this fact is the story of his second graduate student, Esther Lamken. Although Scott was at Waterloo, Esther's degree is from the University of Michigan! Esther began as a strong doctoral student at Michigan who was interested in design theory. The faculty there knew of Scott by reputation and decided that it was in Esther's best interest to work under Scott while writing her dissertation. Esther's thesis bordered on being encyclopedic, and their collaboration continued for many decades.

Working with Scott was always fun. In particular I enjoyed working with him (and others) on optimal normal bases. A normal basis in $\mathbb{F} = \mathbb{F}_{q^n}$ is a basis of the form $B = (\alpha, \alpha^q, \dots, \alpha^{q^{n-1}})$, that is, a set of algebraic conjugates of some element in $\mathbb{F}$. It has long been noted that raising a field element represented by coordinates with respect to this basis to the qth power is equivalent to a cyclic shift. This is particularly interesting when the ground field is $\mathbb{F}_2$ because of the square-and-multiply algorithm used for exponentiation. Squaring becomes straightforward, but the multiplication has to be dealt with. The bilinear form representing the product of two elements in such a representation tends to have a large number of nonzero terms as n grows. We called this number the complexity of the basis since it is a good indicator of the difficulty of implementing the calculation in either hardware or software. Tables of the minimum complexity of all normal bases in $\mathbb{F}_{2^n}$ for the first few values of n showed that the complexity could be as small as $2n - 1$ (which is easily shown to be minimal, and which we called optimal), but these were relatively rare. Our task was to determine the pattern for optimal bases and prove that it held for finite fields of all characteristics [116]. We found sufficient conditions by providing constructions. The results provided algorithms for efficient exponentiation in $\mathbb{F}_{2^n}$ for relatively large values of n. That the sufficient conditions we found were also necessary was subsequently shown by S. Gao in his doctoral thesis. For an example of their proposed use in current cryptography see, for example, "Whirlwind, a new cryptographic hash function" by P. Baretto, V. Nikov, S. Nikova, V. Rijmen and E. Tischhauser, *Designs, Codes and Cryptography* 56, (2010) 141–162.

Scott was an outstandingly brilliant mathematician who had great insight and foresight and nowhere is this shown better than by his work in elliptic curve cryptography (ECC). He took the idea of using elliptic curve groups for cryptographic purposes when many were extremely skeptical, and made ECC into what it is today, the most efficient and secure of all public-key algorithms.

He was a great mentor to his graduate students, easy to work with, and generous with his ideas. This was also the case when he worked with colleagues. But the same can be said about his relations with people in general. He made long-standing friends easily with his warmth, his sense of humour, his great generosity, and his ability to relate to others. His friends numbered in the hundreds, and he delighted in them. He was truly an exceptional human being. Words are inadequate to express the contributions that he made.

He was a great friend and a great man who is very sorely missed by so many.

1.6 Scott Vanstone's Ph.D. students

(1) Ryoh Fuji-Hara
(2) Esther Lamken (co-supervised with Andreas Blass)
(3) Donald Curran
(4) Paul van Oorschot
(5) Steve Furino
(6) Alfred Menezes
(7) Minghua Qu
(8) Robert Zuccherato
(9) Robert Lambert (co-supervised with Ian Blake)
(10) Charles Lam (co-supervised with Guang Gong)
(11) John Proos
(12) Ken Giuliani (co-supervised with Guang Gong)
(13) Berkant Ustaoğlu (co-supervised with Alfred Menezes)

List of Publications

1. Mullin R., Vanstone S.: An approximation of BIBDs by regular pairwise balanced designs; Case $\lambda \geq 2$. In: Proceedings of the Third Conference on Numerical Mathematics. University of Manitoba, Winnipeg, pp. 61–72 (1973).
2. Mullin R., Vanstone S.: On the size of $(r, 2)$-designs. In: Proceedings of the Fourth Southeastern Conference on Combinatorics, Graph Theory and Computing, Boca Raton, pp. 445–457 (1973).

3. Vanstone S.: The extendability of $(r, 1)-$designs. In: Proceedings of the Third Conference on Numerical Mathematics. University of Manitoba, Winnipeg, pp. 409–418 (1973).
4. Mullin R., Vanstone S.: A bound for $v_0(r, \lambda)$. In: Proceedings of the Fifth Southeastern Conference on Combinatorics, Graph Theory and Computing, Boca Raton, pp. 661–673 (1974).
5. Vanstone S.: Geometries and designs. Utilitas Math. **6**, 337–341 (1974).
6. McCarthy D., Mullin R., Schellenberg P., Stanton R., Vanstone S.: On the non-existence of (7,1)-designs with $v = 31, b \leq 43$. In: Proceedings of the Fifth Conference on Numerical Mathematics. University of Manitoba, Winnipeg, pp. 479–495 (1975).
7. Mullin R., Vanstone S.: On regular pairwise balanced designs of order 6 and index 1. Utilitas Math. **8**, 349–369 (1975).
8. Vanstone S.: A note on a construction of BIBDs. Utilitas Math. **7**, 321–322 (1975).
9. Vanstone S.: The non-existence of (7,1)-designs with $v = 31, b \geq 50$. In: Proceedings of the Fifth Conference on Numerical Mathematics. University of Manitoba, Winnipeg, pp. 497–532 (1975).
10. Deza M., Mullin R., Vanstone S.: Room squares and equidistant permutation arrays. Ars Comb. **2**, 235–244 (1976).
11. Hoffman F., Schellenberg P., Vanstone S.: A starter-adder approach to equidistant permutation arrays and generalized Room squares. Ars Comb. **1**, 307–319 (1976).
12. McCarthy D., Mullin R., Schellenberg P., Stanton R., Vanstone S.: On approximations to a finite projective plane of order 6. Ars Comb. **2**, 111–168 (1976).
13. McCarthy D., Stanton R., Vanstone S.: On an extremal class of (r, λ)-designs related to a problem of Doehlert and Klee. Ars Comb. **2**, 305–317 (1976).
14. Mullin R., Vanstone S.: A generalization of a theorem of Totten. J. Aust. Math. Soc. Ser. A **22**, 494–500 (1976).
15. Mullin R., Vanstone S.: On the non-existence of a certain design. Utilitas Math. **9**, 193–207 (1976).
16. Schellenberg P., Vanstone S.: Some results on equidistant permutation arrays of index 1. In: Proceedings of the Sixth Conference on Numerical Mathematics, University of Manitoba, Winnipeg, pp. 389–410 (1976).
17. Vanstone S.: Towards the uniqueness of a (7,1)-design on 31 varieties. In: Proceedings of the Sixth Conference on Numerical Mathematics, University of Manitoba, Winnipeg, pp. 265–285 (1976).
18. McCarthy D., Vanstone S.: Embedding $(r, 1)$-designs in finite projective planes. Discret. Math. **19**, 67–76 (1977).
19. McCarthy D., Vanstone S.: On (r, λ)-designs and finite projective planes. Utilitas Math. **11**, 57–74 (1977).
20. Mullin R., Singhi N., Vanstone S.: Embedding the affine complement of three intersecting lines in a finite projective plane. J. Aust. Math. Soc. Ser. A **24**, 458–464 (1977).
21. Schellenberg P., van Rees G., Vanstone S.: The existence of balanced tournament designs. Ars Comb. **3**, 303–318 (1977).
22. Schellenberg P., Vanstone S.: Recursive constructions for equidistant permutation arrays. J. Aust. Math. Soc. Ser. A **24**, 216–223 (1977).
23. Schellenberg P., Vanstone S.: A construction for BIBDs based on an intersection property. Utilitas Math. **11**, 313–324 (1977).
24. Stanton R., Vanstone S.: Some lower bounds on the size of Doehlert–Klee designs. Ars Comb. **4**, 123–132 (1977).
25. Stanton R., Vanstone S.: Further results on a problem of Doehlert and Klee. Utilitas Math. **12**, 263–271 (1977).
26. Vanstone S., Schellenberg P.: A construction for equidistant permutation arrays of index one. J. Comb. Theory Ser. A **23**, 180–186 (1977).
27. Deza M., Mullin R., Vanstone S.: Orthogonal systems. Aequationes Math. **17**, 322–330 (1978).
28. Deza M., Vanstone S.: Bounds for permutation arrays. J. Stat. Plann. Inference **2**, 197–209 (1978).
29. Schellenberg P., van Rees G., Vanstone S.: Four pairwise orthogonal Latin squares of side 15. Ars Comb. **6**, 141–150 (1978).
30. Vanstone S.: Extremal (r, λ)-designs. Discret. Math. **23**, 57–66 (1978).
31. Vanstone S.: Pairwise Orthogonal generalized room squares and equidistant permutation arrays. J. Comb. Theory Ser. A **25**, 84–89 (1978).
32. McCarthy D., Singhi N., Vanstone S.: A graph theoretical approach to embedding $(r, 1)$-designs. In: Topics in Graph Theory, pp. 289–304. Academic Press, London (1979).
33. McCarthy D., Vanstone S.: On the structure of regular pairwise balanced designs. Discret. Math. **25**, 237–244 (1979).
34. Mullin R., Vanstone S.: Embedding the pseudocomplement of a quadrilateral in a finite projective plans. Ann. N. Y. Acad. Sci. **319**, 405–413 (1979).

35. Stanton R., Vanstone S.: Some theorems on DK-designs. Ars Comb. **8**, 117–130 (1979).
36. Vanstone S.: A note on a class of maximal equidistant permutation arrays. Utilitas Math. **16**, 217–221 (1979).
37. Vanstone S.: Resolvable (r, λ)-designs and the Fisher inequality. J. Aust. Math. Soc. Ser. A **28**, 471–478 (1979).
38. Vanstone S.: The asymptotic behaviour of equidistant permutation arrays. Can. J. Math. **31**, 45–48 (1979).
39. Vanstone S.: Irreducible regular pairwise balanced designs. Utilitas Math. **15**, 249–259 (1979).
40. Deza M., Vanstone S.: Some maximal equidistant permutation arrays. J. Korean Math. Soc. **17**, 45–51 (1980).
41. Fuji-Hara R., Vanstone S.: Transversal designs and doubly-resolvable designs. Eur. J. Comb. **1**, 219–223 (1980).
42. Fuji-Hara R., Vanstone S.: On the spectrum of doubly resolvable Kirkman systems. Congr. Numer. **28**, 399–407 (1980).
43. Fuji-Hara R., Vanstone, S.: On automorphisms of doubly resolvable designs. Lecture Notes in Mathematics, vol. 829, pp. 29–36 (1980).
44. Gardner B., Vanstone S.: Some results on irreducible (r, λ)-designs. Utilitas Math. **18**, 291–300 (1980).
45. Mathon R., Vanstone S.: On the existence of doubly resolvable Kirkman systems and equidistant permutation arrays. Discret. Math. **30**, 157–172 (1980).
46. Mathon R., Vanstone S.: Doubly resolvable Kirkman systems. Congr. Numer. **29**, 611–625 (1980).
47. Mullin R., Schellenberg P., van Rees G., Vanstone S.: On the construction of perpendicular arrays. Utilitas Math. **18**, 141–160 (1980).
48. Mullin R., Schellenberg P., Stinson D., Vanstone S.: Some results on the existence of squares. Ann. Discret. Math. **6**, 257–274 (1980).
49. Mullin R., Vanstone S.: Steiner systems and Room squares. Ann. Discret. Math. **7**, 95–104 (1980).
50. Schellenberg P., Vanstone S.: The existence of Howell designs of side $2n$ and order $2n + 2$. Congr. Numer. **29**, 879–887 (1980).
51. Vanstone S.: Doubly resolvable designs. Discret. Math. **29**, 77–86 (1980).
52. Colbourn C., Vanstone S.: Doubly resolvable twofold triple systems. In: Proceedings of the Eleventh Conference on Numerical Mathematics, University of Manitoba, Winnipeg, pp. 219–223 (1981).
53. Deza M., Mullin R., Vanstone S.: Recent results on (r, λ)-designs and some related areas. Int. J. Math. Stat. **4**, 140–158 (1981).
54. Fuji-Hara R., Vanstone S.: Recursive constructions for skew resolutions in affine geometries. Aequationes Math. **23**, 242–251 (1981).
55. Fuji-Hara R., Vanstone S.: Equidistant permutation arrays from finite geometries. Congr. Numer. **32**, 333–345 (1981).
56. Fuji-Hara R., Vanstone S.: Mutually orthogonal resolutions from finite geometries. Ars Comb. **12**, 189–207 (1981).
57. Mullin R., Schellenberg P., Vanstone S., Wallis W.: On the existence of frames. Discret. Math. **37**, 79–104 (1981).
58. Schellenberg P., Stinson D., Vanstone S., Yates J.: The existence of Howell designs of side $n + 1$ and order $2n$. Combinatorica **1**, 289–301 (1981).
59. Deza M., Vanstone S.: On maximal equidistant permutation arrays. Ann. Discret. Math. **12**, 87–94 (1982).
60. Fuji-Hara R., Vanstone S.: Orthogonal resolutions of lines in $AG(n, q)$. Discret. Math. **41**, 17–28 (1982).
61. Mullin R., Stinson D., Vanstone S.: Kirkman triple systems containing maximum subdesigns. Utilitas Math. **21C**, 283–300 (1982).
62. van Rees G., Vanstone S.: Equidistant permutation arrays: a bound. J. Aust. Math. Soc. Ser. A **33**, 262–274 (1982).
63. Vanstone S.: On mutually orthogonal resolutions and near-resolutions. Ann. Discret. Math. **15**, 357–369 (1982).
64. Vanstone S., Rosa A.: Starter-adder techniques for Kirkman squares and Kirkman cubes of small sides. Ars Comb. **14**, 199–212 (1982).
65. Fuji-Hara R., Vanstone S.: Affine geometries obtained from projective geometries and skew resolutions. Ann. Discret. Math. **18**, 355–376 (1983).
66. Goulden I., Vanstone S.: The number of solutions to an equation arising from a problem on Latin squares. J. Aust. Math. Soc. Ser. A **34**, 138–142 (1983).
67. Rosa A., Vanstone S.: Kirkman cubes. Ann. Discret. Math. **18**, 699–712 (1983).
68. Vanstone S.: A note on the existence of strong Kirkman cubes. Ann. Discret. Math. **17**, 629–632 (1983).
69. Vanstone S.: Some results on strong skew resolutions. Matematiche (Catania) **38**, 173–180 (1983).

70. Blake I., Fuji-Hara R., Mullin R., Vanstone S.: Computing logarithms in finite fields of characteristic two. SIAM J. Algebraic Discret. Methods **5**, 276–285 (1984).
71. Fuji-Hara R., Vanstone S.: On a line partitioning problem for $PG(2k, q)$. Rendiconti del Seminario Matemàtico di Brescia **7**, 337–341 (1984).
72. Jackson D., Vanstone S. (eds.): Enumeration and Design. Academic Press, London (1984).
73. Jimbo M., Vanstone S.: Recursive constructions for resolvable and doubly resolvable 1-rotational Steiner 2-designs. Utilitas Math. **26**, 45–61 (1984).
74. Lamken E., Vanstone S.: Complementary Howell designs of side $2n$ and order $2n + 2$. Congr. Numer. **41**, 83–113 (1984).
75. Mullin R., Vanstone S.: Asymptotic properties of locally extensible designs. Geom. Dedicata **15**, 269–277 (1984).
76. Stinson D., Vanstone S.: A note on non-isomorphic Kirkman triple systems. J. Comb. Inf. Syst. Sci. **9**, 113–116 (1984).
77. Blake I., Mullin R., Vanstone S.: Computing logarithms in $GF(2^n)$. In: Advances in Cryptology—CRYPTO ’85. Lecture Notes in Computer Science, vol. 196, pp. 73–82 (1985).
78. Gionfriddo M., Vanstone S.: On L_2-colourings of a graph. J. Inf. Optim. Sci. **6**, 243–246 (1985).
79. Kocay W., Stinson D., Vanstone S.: On strong starters in cyclic groups. Discret. Math. **56**, 45–60 (1985).
80. Lamken E., Mullin R., Vanstone S.: Some non-existence results on twisted planes related to minimum covers. Congr. Numer. **48**, 265–275 (1985).
81. Lamken E., Vanstone S.: The existence of factored balanced tournament designs. Ars Comb. **19**, 157–160 (1985).
82. Lamken E., Vanstone S.: The existence of $KS_k(v; \mu, \lambda)$: I. The main constructions. Utilitas Math. **27**, 111–130 (1985).
83. Lamken E., Vanstone S.: The existence of $KS_k(v; \mu, \lambda)$: II. Special constructions. Utilitas Math. **27**, 131–155 (1985).
84. Lamken E., Vanstone S.: The existence of partitioned balanced tournament designs of side $4n + 1$. Ars Comb. **20**, 29–44 (1985).
85. Rosa A., Vanstone S.: On the existence of strong Kirkman cubes of order 39 and block size 3. Ann. Discret. Math. **26**, 309–319 (1985).
86. Stinson D., Vanstone S.: A Kirkman square of order 51 and block size 3. Discret. Math. **55**, 107–111 (1985).
87. Stinson D., Vanstone S.: A few more balanced Room squares. J. Aust. Math. Soc. Ser. A **39**, 344–352 (1985).
88. Stinson D., Vanstone S.: Some non-isomorphic Kirkman triple systems of order 39 and 51. Utilitas Math. **27**, 199–205 (1985).
89. Jungnickel D., Vanstone S.: On resolvable designs $S_3(3; 4, v)$. J. Comb. Theory Ser. A **43**, 334–337 (1986).
90. Lamken E., Vanstone S.: Designs with mutually orthogonal resolutions. Eur. J. Comb. **7**, 249–257 (1986).
91. Lamken E., Vanstone S.: Elliptic semiplanes and group divisible designs with orthogonal resolutions. Aequationes Math. **30**, 80–92 (1986).
92. Lamken E., Vanstone S.: Existence results for $KS_3(v; 2, 4)$s. Discret. Math. **62**, 197–210 (1986).
93. Lamken E., Vanstone S.: A generalization of the Room square problem. Congr. Numer. **51**, 265–276 (1986).
94. Stinson D., Vanstone S.: Orthogonal packings in $PG(5, 2)$. Aequationes Math. **31**, 159–168 (1986).
95. Colbourn C., Curran D., Vanstone S.: Recursive constructions for Kirkman squares with block size 3. Utilitas Math. **32**, 169–174 (1987).
96. Fuji-Hara R., Vanstone S.: The existence of orthogonal resolutions of lines in $AG(n, q)$. J. Comb. Theory Ser. A **45**, 139–147 (1987).
97. Fuji-Hara R., Vanstone S.: Balanced Room squares from finite geometries and their generalizations. Ann. Discret. Math. **34**, 179–188 (1987).
98. Furino S., Vanstone S.: Hyperplane skew resolutions in spaces of even dimension. Ars Comb. **24**, 63–69 (1987).
99. Jungnickel D., Vanstone S.: Hyperfactorizations of graphs and 5-designs. Kuwait J. Math. **14**, 213–223 (1987).
100. Jungnickel D., Vanstone S.: Conical embeddings of Steiner systems. Rendiconti del Circolo Matematico di Palermo, Series **II**(36), 90–94 (1987).
101. Koyama K., Vanstone S.: How to demonstrate the breaking of public key cryptosystems. In: Proceedings of the 1987 Workshop on Cryptography and Information Security, pp. 161–170 (1987).
102. Lamken E., Mills W., Mullin R., Vanstone S.: Coverings of pairs by quintuples. J. Comb. Theory Ser. A **44**, 49–68 (1987).

103. Lamken E., Vanstone S.: The existence of partitioned balanced tournament designs of side $4n + 3$. Ann. Discret. Math. **34**, 319–338 (1987).
104. Lamken E., Vanstone S.: The existence of partitioned balanced tournament designs. Ann. Discret. Math. **34**, 339–352 (1987).
105. Lamken E., Vanstone S.: Skew transversals in frames. J. Combin. Math. Comb. Comput. **2**, 37–50 (1987).
106. Agnew G., Mullin R., Vanstone S.: An interactive data exchange protocol based on discrete exponentiation. In: Advances in Cryptology—EUROCRYPT '88. Lecture Notes in Computer Science, vol. 453, pp. 159–166 (1988).
107. Agnew G., Mullin R., Vanstone S.: Fast exponentiation in $GF(2^n)$. In: Advances in Cryptology—EUROCRYPT '88. Lecture Notes in Computer Science, vol. 453, pp. 251–255 (1988).
108. Blake I., van Oorschot P., Vanstone S.: Complexity issues for public key cryptography. Perform. Limits Commun. Theory Pract. **142**, 75–97 (1988).
109. Curran D., Vanstone S.: Doubly resolvable designs from generalized Bhaskar Rao designs. Discret. Math. **73**, 49–63 (1988–1989).
110. Fuji-Hara R., Vanstone S.: Hyperplane skew resolutions and their applications. J. Comb. Theory Ser. A **47**, 134–144 (1988).
111. Hall Jr M., Roth R., van Rees G., Vanstone S.: On designs $(22, 33, 12, 8, 4)$. J. Comb. Theory Ser. A **47**, 157–175 (1988).
112. Lamken E., Vanstone S.: The existence of a class of Kirkman squares of index 2. J. Aust. Math. Soc. Ser. A **44**, 33–41 (1988).
113. Lamken E., Vanstone S.: Orthogonal resolutions in odd balanced tournament designs. Gr. Comb. **4**, 241–255 (1988).
114. Lamken E., Vanstone S.: A note on group divisible designs with mutually orthogonal resolutions. J. Aust. Math. Soc. Ser. A **44**, 397–401 (1988).
115. Lamken E., Vanstone S.: On the existence of $(2, 4; 3, m, h)$-frames for $h = 1, 3$ and 6. J. Comb. Math. Combin. Comput. **3**, 135–151 (1988).
116. Mullin R., Onyszchuk I., Vanstone S., Wilson, R.: Optimal normal bases in $GF(p^n)$, Discret. Appl. Math. **22** 149–161 (1988–1989).
117. Stinson D., Vanstone S.: A combinatorial approach to threshold schemes. SIAM J. Discret. Math. **2**, 230–236 (1988).
118. Ash D., Blake I., Vanstone S.: Low complexity normal bases. Discret. Appl. Math. **25**, 191–210 (1989).
119. Beutelspacher A., Jungnickel D., Vanstone S.: On the chromatic index of a finite projective space. Geom. Dedicata **32**, 313–318 (1989).
120. Jungnickel D., Vanstone S.: On primitive polynomials over finite fields. J. Algebra **124**, 337–353 (1989).
121. Lamken E., Vanstone S.: Balanced tournament designs and related topics. Discret. Math. **77**, 159–176 (1989).
122. Menezes A., van Oorschot P., Vanstone S.: Some computational aspects of root finding in $GF(q^m)$. In: Symbolic and Algebraic Computation. Lecture Notes in Computer Science, vol. 358, pp. 259–270 (1989).
123. Phelps K., Stinson D., Vanstone S.: The existence of simple $S_3(3, 4, v)$. Discret. Math. **77**, 255–258 (1989).
124. Vanstone S., van Oorschot P.: An Introduction to Error Correcting Codes with Applications. Kluwer Academic Publishers, Dordrecht (1989).
125. van Oorschot P., Vanstone S.: A geometric approach to root finding in $GF(q^m)$. IEEE Trans. Inf. Theory **35**, 444–453 (1989).
126. Agnew G., Mullin R., Vanstone S.: Improved digital signature scheme based on discrete exponentiation. Electron. Lett. **26**, 1024–1025 (1990).
127. Agnew G., Mullin R., Vanstone, S.: A fast elliptic curve cryptosystem. In: Advances in Cryptology—EUROCRYPT '89. Lecture Notes in Computer Science, vol. 434, pp. 706–708 (1990).
128. Beth T., Vanstone S., Agnew G.: What one should know about public key algorithms—today! Securicom **90**, 47–63 (1990).
129. Jungnickel D., Menezes A., Vanstone S.: On the number of self-dual bases of $GF(q^m)$ over $GF(q)$. Proc. AMS **109**, 23–29 (1990).
130. Lamken E., Vanstone S.: The existence of skew Howell designs of side $2n$ and order $2n + 2$. J. Comb. Theory Ser. A **54**, 20–40 (1990).
131. Lamken E., Vanstone S.: Balanced tournament designs and resolvable $(v, 3, 2)$-BIBDs. Discret. Math. **83**, 37–47 (1990).
132. Lamken E., Vanstone S.: Balanced tournament designs with almost orthogonal resolutions. J. Aust. Math. Soc. Ser. A **49**, 175–195 (1990).

133. Menezes A., Vanstone S.: The implementation of elliptic curve cryptosystems. In: Advances in Cryptology—AUSCRYPT '90. Lecture Notes in Computer Science, vol. 453, pp. 2–13 (1990).
134. Menezes A., Vanstone S.: Isomorphism classes of elliptic curves over finite fields of characteristic 2. Utilitas Math. **38**, 135–154 (1990).
135. Vanstone S., van Oorschot P.: On splitting sets in block designs and finding roots of polynomials. Discret. Math. **84**, 71–85 (1990).
136. van Oorschot P., Vanstone S.: Some geometric aspects of root finding in $GF(q^m)$. Contemp. Math. **111**, 303–307 (1990).
137. Agnew G., Mullin R., Onyszchuk I., Vanstone S.: An implementation for a fast public-key cryptosystem. J. Cryptol. **3**, 63–79 (1991).
138. Boros E., Jungnickel D., Vanstone S.: The existence of non-trivial hyperfactorizations of K_{2n}. Combinatorica **11**, 9–15 (1991).
139. Jungnickel D., Vanstone S.: Triple systems in $PG(2, q)$. Discret. Math. **92**, 131–135 (1991).
140. Jungnickel D., Mullin R., Vanstone S.: The spectrum of α-resolvable block designs with block size 3. Discret. Math. **97**, 269–277 (1991).
141. Lamken E., Rees R., Vanstone S.: Class-uniformly resolvable pairwise balances designs with block sizes 2 and 3. Discret. Math. **92**, 197–209 (1991).
142. Menezes A., Vanstone S. (eds.): Advances in Cryptology—CRYPTO '90, Lecture Notes in Computer Science, vol. 537 (1991).
143. Phelps K., Vanstone S.: Isomorphism of strong starters in cyclic groups. J. Comb. Theory Ser. A **57**, 287–293 (1991).
144. Beutelspacher A., Jungnickel D., van Oorschot P., Vanstone S.: Pair-splitting sets in $AG(m, q)$. SIAM J. Discret. Math. **5**, 451–459 (1992).
145. Koyama K., Maurer U., Okamoto T., Vanstone S.: New public-key schemes based on elliptic curves over the ring Z_n. In: Advances in Cryptology—CRYPTO '91. Lecture Notes in Computer Science, vol. 576, pp. 252–266 (1992).
146. Menezes A., van Oorschot P., Vanstone S.: Subgroup refinement algorithms for root finding in $GF(q)$. SIAM J. Comput. **21**, 228–239 (1992).
147. Menezes A., Vanstone S.: A note on cyclic groups, finite fields, and the discrete logarithm problem. Appl. Algebra Eng. Commun. Comput. **3**, 67–74 (1992).
148. Seberry J., McKay B., Vanstone S. (eds.): Selected papers in combinatorics—a volume dedicated to R.G. Stanton. In: Discrete Mathematics, vol. 92 (1991).
149. Tonchev V., Vanstone S.: On Kirkman triple systems of order 33. Discret. Math. **106–107**, 493–496 (1992).
150. Agnew G., Mullin R., Vanstone S.: An implementation of elliptic curve cryptosystems over $F_{2^{155}}$. IEEE J. Sel. Areas Commun. **11**, 804–813 (1993).
151. Agnew G., Mullin R., Vanstone S.: Arithmetic operations in $GF(2^m)$. J. Cryptol. **6**, 3–13 (1993).
152. Agnew G., Mullin R., Vanstone S.: On the development of a fast elliptic curve cryptosystem. In: Advances in Cryptology—EUROCRYPT '92. Lecture Notes in Computer Science, vol. 658, pp. 482–487 (1993).
153. Blake I., Gao S., Menezes A., Mullin R., Vanstone S., Yaghoobian T.: Applications of Finite Fields. Kluwer Academic Publishers, Dordrecht (1993).
154. Furino S., Vanstone S.: Pairwise balanced designs with block sizes $5t + 1$. In: Graphs, Matrices, and Designs. Lecture Notes in Pure and Applied Mathematics, vol. 139, pp. 147–170 (1993).
155. Gilbert W., Vanstone S.: Classical Algebra. Waterloo Mathematics Foundation, Waterloo (1993).
156. Harper G., Menezes A., Vanstone S.: Public-key cryptosystems with very small key lengths. In: Advances in Cryptology—EUROCRYPT '92. Lecture Notes in Computer Science, vol. 658, pp. 163–173 (1993).
157. Jungnickel D., Vanstone S. (eds.): Coding Theory, Design Theory, Group Theory. Wiley, New York (1993).
158. Lamken E., Vanstone S.: Existence results for doubly near resolvable $(v, 3, 2)$-BIBDs. Discret. Math. **120**, 135–148 (1993).
159. Menezes A., Okamoto T., Vanstone S.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inf. Theory **39**, 1639–1646 (1993).
160. Menezes A., Vanstone S.: Elliptic curve cryptosystems and their implementation. J. Cryptol. **6**, 209–224 (1993).
161. Menezes A., Vanstone S., Zuccherato R.: Counting points on elliptic curves over F_{2^m}. Math. Comput. **60**, 407–420 (1993).
162. Vanstone S., Stinson D., Schellenberg P., Rosa A., Rees R., Colbourn C., Carter M., Carter J.: Hanani triple systems. Israel J. Math. **83**, 305–319 (1993).
163. Qu M., Vanstone S.: Factorizations in the elementary abelian p-group and their cryptographic significance. J. Cryptol. **7**, 201–2012 (1994).

164. Qu M., Vanstone S.: The knapsack problem in cryptography. Contemp. Math. **168**, 291–308 (1994).
165. Vanstone S., Zuccherato R.: Using four-prime RSA in which some of the bits are specified. Electron. Lett. **30**, 2118–2119 (1994).
166. Gao S., Vanstone S.: On orders of optimal normal basis generators. Math. Comput. **64**, 1227–1233 (1995).
167. Jungnickel D., Vanstone S.: An application of coding theory to a problem in graphical enumeration. Arch. Math. **65**, 461–464 (1995).
168. Lee T., Vanstone S.: Subspaces and polynomial factorization over finite fields. Appl. Algebra Eng. Commun. Comput. **6**, 147–157 (1995).
169. Vanstone S., Zuccherato R.: Short RSA keys and their generation. J. Cryptol. **8**, 101–114 (1995).
170. Jungnickel D., De Resmini M., Vanstone S.: Codes based on complete graphs. Des. Codes Cryptogr. **8**, 159–165 (1996).
171. Jungnickel D., Vanstone S.: Graphical codes—a tutorial. Bull. ICA **18**, 45–64 (1996).
172. Menezes A., van Oorschot P., Vanstone S.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1996).
173. Wevrick D., Vanstone S.: Class-uniformly resolvable designs with block sizes 2 and 3. J. Comb. Des. **4**, 177–202 (1996).
174. Jungnickel D., Vanstone S.: Graphical codes revisited. IEEE Trans. Inf. Theory **43**, 136–146 (1997).
175. Jungnickel D., Vanstone S.: An application of difference sets to a problem concerning graphical codes. J. Stat. Plan. Inference **62**, 43–46 (1997).
176. Vanstone S.: Elliptic curve cryptosystem—The answer to strong, fast public-key cryptography for securing constrained environments. Inf. Secur. Tech. Rep. **2**, 78–87 (1997).
177. Vanstone S., Zuccherato R.: Elliptic curve cryptosystems using curves of smooth order over the ring $\mathbb{Z}_n$. IEEE Trans. Inf. Theory **43**, 1231–1237 (1997).
178. Müller V., Vanstone S., Zuccherato R.: Discrete logarithm based cryptosystems in quadratic function fields of characteristic 2. Des. Codes Cryptogr. **14**, 159–178 (1998).
179. Jungnickel D., Vanstone S.: q-ary graphical codes. Discret. Math. **208–209**, 375–386 (1999).
180. Jungnickel D., Vanstone S.: Ternary graphical codes. J. Comb. Math. Comb. Comput. **29**, 17–31 (1999).
181. Gallant R., Lambert R., Vanstone S.: Improving the parallelized Pollard lambda search on anomalous binary curves. Math. Comput. **69**, 1699–1705 (2000).
182. Koblitz N., Menezes A., Vanstone S.: The state of elliptic curve cryptography. Des. Codes Cryptogr. **19**, 173–193 (2000).
183. Lam C., Shallit J., Vanstone S.: Worst-case analysis of an algorithm for computing the greatest common divisor of *n* inputs. In: Coding Theory, Cryptography and Related Areas, pp. 156–166. Springer, Berlin (2000).
184. Gallant R., Lambert R., Vanstone S.: Faster point multiplication on elliptic curves with efficient endomorphisms. In: Advances in Cryptology—CRYPTO 2001. Lecture Notes in Computer Science, vol. 2139, pp. 190–200 (2001).
185. Johnson D., Menezes A., Vanstone S.: The elliptic curve digital signature algorithm (ECDSA). Int. J. Inf. Secur. **1**, 36–63 (2001).
186. Pintsov L., Vanstone S.: Postal revenue collection in the digital age. In: Financial Cryptography 2000. Lecture Notes in Computer Science, vol. 2001, pp. 105–120 (1962).
187. Brown D., Gallant R., Vanstone S.: Provably secure implicit certificate schemes. In: Financial Cryptography 2001. Lecture Notes in Computer Science, vol. 2339, pp. 156–165 (2002).
188. Lam C., Gong G., Vanstone S.: Message authentication codes with error correcting capabilities. In: Information and Communications Security—ICICS 2002. Lecture Notes in Computer Science, vol. 2513, pp. 354–366 (2002).
189. Qu M., Stinson D., Vanstone S.: Cryptanalysis of the Sakazaki-Okamoto-Mambo ID-based key distribution system over elliptic curves. In: Finite Fields with Applications in Coding Theory. Cryptography and Related Areas, pp. 263–269. Springer, Berlin (2002).
190. Antipa A., Brown D., Menezes A., Struik R., Vanstone S.: Validation of elliptic curve public keys. In: Proceedings of PKC 2003. Lecture Notes in Computer Science, vol. 2567, pp. 211–223 (2003).
191. Law L., Menezes A., Qu M., Solinas J., Vanstone S.: An efficient protocol for authenticated key agreement. Des. Codes Cryptogr. **28**, 119–134 (2003).
192. Vanstone S.: Next generation security for wireless: elliptic curve cryptography. Comput. Secur. **22**, 412–415 (2003).
193. Gilbert W., Vanstone S.: Introduction to Mathematical Thinking: Algebra and Number Systems. Pearson, London (2004).
194. Hankerson D., Menezes A., Vanstone S.: Guide to Elliptic Curve Cryptography. Springer, Berlin (2004).

195. Antipa A., Brown D., Gallant R., Lambert R., Struik R., Vanstone S.: Accelerated verification of ECDSA signatures. In: Selected Areas in Cryptography—SAC 2005. Lecture Notes in Computer Science, vol. 3897, pp. 307–318 (2006).