Looking Back—My Life as a Mathematician and Cryptographer[⋆]

Douglas R. Stinson

David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada

Abstract. In this paper, I look back at my career as a mathematician and mathematical cryptographer, mainly concentrating on my student days and the early parts of my career. I also discuss my research philosophy and what I mean by the term "combinatorial cryptography." Along the way, I recall some influential people, books and papers.

Overview

I would like to thank the SAC 2019 organizers for inviting me to give an invited talk at SAC 2019, which was held at the University of Waterloo. This talk was also happening in conjunction with my retirement from the University of Waterloo, which took place on September 1, 2019. I suggested that I might give a (mostly) non-technical talk of a somewhat autobiographical nature, and they agreed. Thus, I used the talk to look back at my career as a mathematician and mathematical cryptographer, mainly concentrating on my student days and the early parts of my career. This paper will serve as a summary of the material in my talk.

The following are the main topics I discussed.

- My involvement with SAC
- Transitions: math contests → mathematical research → computer science → mathematical cryptography
- Combinatorial cryptography: what is it?
- Influences: people, books, papers
- Research philosophy and mathematical exposition.

SAC and Me

I have been involved with SAC from the beginning. I attended and spoke at the first SAC Workshop, which was held at Queen's University in 1994. My talk there was entitled "Recent results on resilient functions." I was an invited speaker at SAC 1995, SAC 2013, and SAC 2019. I was Co-chair of SAC in 2000 and 2010. I was Chair of the SAC organizing board from 2000–2007 and a Member of the

[⋆] D.R. Stinson's research is supported by NSERC Discovery grant RGPIN-03882.

SAC organizing board from 2000–2014. I created the first SAC web pages in 2003.

The first six editions of SAC were held at Queen's University and Carleton University. In 2000, SAC was held at the University of Waterloo for the first time and there was discussion there about the future direction of SAC. I was an early voice calling for SAC to be held exclusively in Canada. The following quote is from the minutes of the SAC 2000 Board Meeting:

> "It was suggested by D. Stinson that SAC be officially designated as a 'Canadian workshop series in cryptography' in the Draft Guidelines."

Given my long participation with SAC, it was a pleasure and an honour to be invited to speak at SAC 2019.

Cribbage

One of my first "mathematical" memories was watching my parents and grandparents play cribbage. I do not recall my age exactly, but I was perhaps 6 or 7 years old at the time. I was very interested in scoring the hands, where points are given for pairs, combinations of cards that sum to 15, runs of three or more, etc. The details aren't important, but the scoring system is rather complex. Two facts that I found fascinating were that

- a count of 19 is impossible and
- 29 is the maximum possible count.

I suppose this was my first experience with the concept of mathematical impossibility.

One example of a 29-count hand in cribbage would consist of the five of clubs, diamonds and hearts and the jack of spades. If the five of spades is then "cut" (this is a card that is common to all the players' hands), then the result is a 29-count hand:

- $\binom{4}{2} = 6$ pairs → 12 points
- $4 + \binom{4}{3} = 8$ fifteens → 16 points
- 1 point for the "Jack of nobs" (i.e, the player's hand contains the jack of the same suit as the card that is cut)
- total: $12 + 16 + 1 = 29$ points.

Note that three of a kind $= \binom{3}{2} =$ three pairs and four of a kind $= \binom{4}{2} = 6$ pairs. This is combinatorics in action! Perhaps this inspired me to become a combinatorial mathematician.

Math Contests

I always enjoyed math classes in school, in part because I could do tests without having to memorize boring facts![1] However, my serious involvement in mathematics really started with high school math contests. I began high school in 1970 (grade 9) at John F. Ross Collegiate and Vocational Institute in Guelph, which is just a few minutes down the highway from Waterloo. The University of Waterloo ran the *Junior Math Contest*, which was a multiple choice contest for students in grades 9–11.

That year, a grade 10 student (Bob Saul) finished first in our school and I finished second. The next year, when I was in grade 10, I finished in the top 15 in Ontario and I was invited to the Junior Math Contest Seminar held at the University of Waterloo in June 1972. I attended the JMC seminar again in June 1973 after finishing in the top 10 in Ontario.

Ross Honsberger

I first heard Ross Honsberger speak at the JMC seminars. Ross (1929–2016) was a masterful mathematical expositor and an entertaining speaker who was a long-time faculty member at UW. For many years, Ross taught a popular course on problem solving, consisting of 100 problems.

Ross was the author of numerous books such as "Ingenuity in Mathematics" [9]. One particularly memorable lecture I recall from the 1973 JMC seminar was on the topic of a checker-jumping problem known as "Conway's Soldiers".

As it is explained in Wikipedia:[2]

> "*Conway's Soldiers* or the *checker-jumping problem* is a one-person mathematical game or puzzle devised and analyzed by mathematician John Horton Conway in 1961. A variant of peg solitaire, it takes place on an infinite checkerboard. The board is divided by a horizontal line that extends indefinitely. Above the line are empty cells and below the line are an arbitrary number of game pieces, or "soldiers". As in peg solitaire, a move consists of one soldier jumping over an adjacent soldier into an empty cell, vertically or horizontally (but not diagonally), and removing the soldier which was jumped over. The goal of the puzzle is to place a soldier as far above the horizontal line as possible. Conway proved that, regardless of the strategy used, there is *no finite series of moves that will allow a soldier to advance more than four rows above the horizontal line*. His argument uses a carefully chosen weighting of cells (involving the golden ratio), and he proved that the total weight can only decrease or remain constant. This argument has been reproduced in a number of popular math books."

[1] I did have to memorize the multiplication table, but this did not bother me.

[2] This quote is from the Wikipedia article "Conway's Soldiers" (`https://en.wikipedia.org/wiki/Conway's_Soldiers`), which is released under the Creative Commons Attribution-Share-Alike License 3.0

The weight of the destination cell four rows above the x-axis is $>$ the weights of all the cells (an infinite number of them) below the x-axis. Since the total weight never decreases with any move, the destination cell cannot be reached. I did not understand all the intricacies of the proof at the time, but I was convinced I had seen something remarkable!

From High School to University

Ontario used to have a fifth year of high school, which was designated as grade 13. A diploma would be awarded after grade 12, but students who intended to go to university would take grade 13. I took grade 11 and grade 12 math while I was enrolled in grade 11. While I was in grade 12 (1973–1974), I took the three grade 13 math courses and I applied for early admission to UW. My parents took me to UW to meet with the Dean of Mathematics, Ken Fryer, who indicated that Waterloo would be happy to accept me even though I would not have a grade 13 diploma. I continued to be involved in various math contests—that year I won the *UW Descartes Math Contest* with a score of 99/100 and I finished second in the *Canadian Math Olympiad*.

The 1974 "Special K" Math Contest

Murray Klamkin (1921–2004) joined UW as a visiting professor in 1974. At the time he was the principal research scientist at Ford Motor Company. Later Murray was chair of the Mathematics Department at the University of Alberta, from 1976–1981.

Murray was well-known as a "*prolific proposer and editor of professionally challenging mathematical problems*".[3] In 1974, he instituted the *Special K* and *Euler* math contests for undergraduates. I won the Special K contest (for first-year students) that year.

One of the problems in the Special K contest that year was written up by Ross Honsberger in his book "Mathematical Morsels" [10], which was published in 1978. Here is the description of the problem, which Ross termed the "Chauffeur problem":

> "Mr. Smith, a commuter, is picked up each day at the train station at exactly 5 o'clock. One day he arrived unannounced on the 4 o'clock train and began to walk home. Eventually he met the chauffeur driving to the station to get him. The chauffeur drove the rest of the way home, getting him there 20 minutes earlier than usual.
> On another day, Mr. Smith arrived unexpectedly on the 4:30 train, and again began walking home. Again he met the chauffeur and rode the

[3] This quote is from the Wikipedia article "Murray S. Klamkin" (`https://en.wikipedia.org/wiki/Murray_S._Klamkin`), which is released under the Creative Commons Attribution-Share-Alike License 3.0

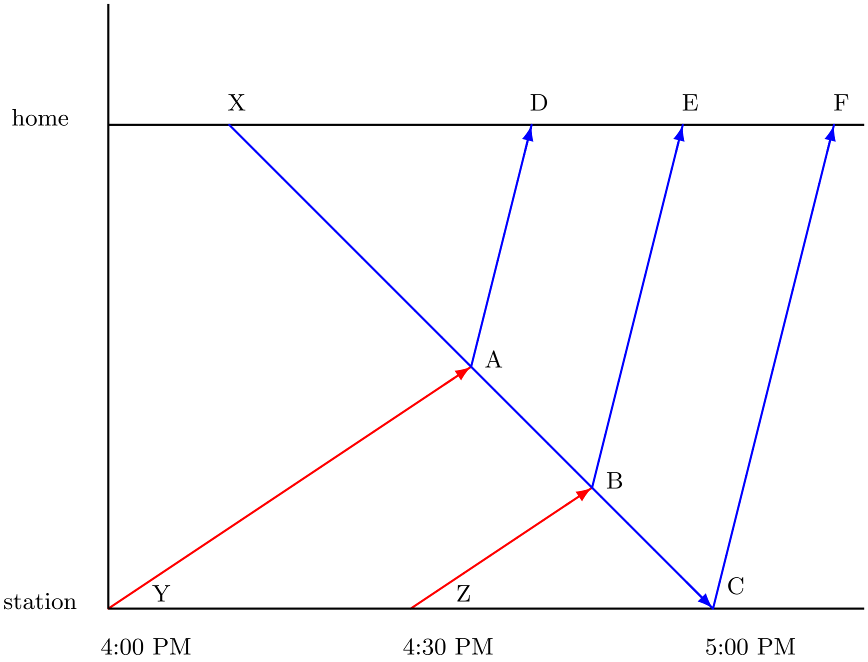

Fig. 1. Mr. Smith and the chauffeur

rest of the way with him. How much ahead of time were they this time? (Assume constant speeds of walking and driving and that no time is lost in turning the car around and picking up Mr. Smith.)

The answer to the problem (namely, 10 minutes) is intuitively obvious, but a bit of work is required to give a convincing mathematical proof. I provided an algebraic solution to this question. My solution was correct but not very illuminating. Another student who wrote the contest, Rick Cameron, provided a much more satisfying solution, which was related by Ross Honsberger in [10]. The basic idea is to plot "distance from the station" on one axis and "time" on the other axis.[4] See Figure 1.

- On a normal day, the chauffeur proceeds from X to C where he meets Mr. Smith. They then drive to F.
- When Mr. Smith arrives on the 4:00 train, the chauffeur proceeds from X to A. There he meets Mr. Smith, who has walked from Y to A. They then drive to D.
- When Mr. Smith arrives on the 4:30 train, the chauffeur proceeds from X to B. There he meets Mr. Smith, who has walked from Z to B. They then drive to E.

[4] This is sometimes called a *Minkowski diagram*.

We observe that XAD, XBE and XCF are similar triangles, as are YAC and ZBC. The length of the line segment YZ is the same as the length of the line segment ZC, so the line segments AB and BC have the same lengths. Hence, the line segments DE and EF have the same lengths. Since we are told that DF has length 20 (minutes), it follows that EF has length 10 (minutes).

I can honestly say that I do not remember the details of the solution I gave, and I cannot remember any of the other problems in this contest. What sticks in my mind 45 years later is Rick's solution.

Ron Mullin

After my second year of undergraduate studies, Ron Mullin hired me as a undergraduate research assistant in 1976. Ron of course is well-known as a leading researcher in combinatorics (especially design theory) and cryptography. Ron eventually became my PhD supervisor; he was clearly the main influence in my mathematical career. Among many other things, I credit Ron with helping me make the transition from problem solver to researcher. Ron was the first graduate of the University of Waterloo—he received the very first degree (an MA in mathematics) awarded at the very first convocation in June, 1960. Another bit of trivia is that Ron and I are both natives of Guelph, Ontario.

At Ron's suggestion, I attended the ManiWat Workshop in the summer of 1976. The ManiWat workshops took place from 1975–1985 at a former convent in St. Pierre, Manitoba that was owned by Ralph Stanton (1923–2010). These workshops were modelled after Oberwolfach. This was my first "up-close" exposure to mathematicians "in the wild" doing research, with a bottle of beer in one hand and a piece of chalk in the other hand!

That year, the workshop consisted of one week of computational number theory followed by a week of design theory. I recall hearing lectures from Dan Shanks about the SQUFOF (*SQU*are *FO*rm *F*actorization) factoring algorithm. In the design theory week, Ron Mullin gave a series of talks on the problem of packing pairs into quadruples. This problem requires the determination of the maximum number of four-subsets of a v-set such that no pair is contained in more than one four-subset; I was working at the time on some special cases of that problem for Ron.

Ron Mullin hired me as a URA for three consecutive years. I worked on various problems including packings, mutually orthogonal latin squares and skew Room squares. Mostly I was doing computational work as I found the theory very complicated.

I was especially mystified by recursive constructions for block designs, which I felt was the most complicated mathematics I had ever seen. I tried to read various papers by Hanani, Mills, Wilson, etc., but the methods and notation were daunting. In retrospect, it took a considerable amount of time for me to become comfortable with the theoretical underpinnings of recursive constructions for designs. However, finally there was an epiphany. I vividly recall in 1978 when Ron showed me a new PBD (pairwise balanced design) construction on the blackboard in his office. For the first time, I really understood how a recursive PBD construction worked. This construction, which appeared in [11], was of fundamental importance in attacking the skew Room square problem since it could provide PBDs of odd orders whose block sizes were orders of skew Room squares (i.e., odd integers ≥ 7).

Here is a brief summary of the construction. First, it requires the construction of two small designs:

1. Deleting a point from a transversal design $\mathrm{TD}(7, 9)$, we obtain a group-divisible design (GDD) with group type $8^1 6^9$ and having blocks of size 7 and 9.
2. Start with a $\mathrm{TD}(7, 8)$. Adjoint a new point to each group and then delete some other point. The result is a GDD with group type $8^1 6^8$ and having blocks of size 7 and 9.

We use these two GDDs as "building blocks" in a recursive construction. Start with a $\mathrm{TD}(10, m)$ and then delete $m-t$ points from one group (where $0 \leq t \leq m$). This produces a GDD with group type $m^9 t^1$ and having blocks of size 9 and 10.

Next, give the points in one group of size m weight 8, give all other points weight 6 and apply Wilson's Fundamental GDD Construction (see [20]). Each block B of the GDD is replaced by a copy of one of our two "building blocks," in such a way that the groups of the GDD align with the copies of the points in B: a block of size 10 is replaced by the blocks of the GDD #1, and a block of size 9 is replaced by the blocks of the GDD #2.

This yields a GDD of group type $(6m)^8(8m)^1(6t)^1$, having blocks of size 7 and 9. If we now add one new point to each of the groups, we obtain a pairwise balanced design (PBD) on $56m+6t+1$ points, having block sizes $7, 9, 6m+1, 6t+1$ and $8m + 1$.

Graduate Studies

I completed my Bachelor of Mathematics degree at the University of Waterloo in 1978, majoring in C&O (Combinatorics and Optimization) and Pure Mathematics. Then I started graduate school at Ohio State, but I already had a "head start" of two years on learning how to do research. Ohio State was a hotbed of combinatorics in the 1970s. Furthermore, a number of now well-known combinatorial researchers were grad students at OSU at the time, including Jeff Dinitz, Dan Archdeacon, KT Arasu, Jeff Kahn, and Ernie Brickell. Ohio State was where I met my long-time friend and frequent collaborator Jeff Dinitz.

I obtained a Masters Degree at Ohio State in 1980 and then I returned to Waterloo to complete my PhD. I received my PhD in Combinatorics and Optimization from UW in 1981. The title of my thesis was "Some classes of frames, and the spectra of skew Room squares and Howell designs."

Various people have asked me how I managed to complete a PhD in three years. I firmly believe that the reason I was able to do this was due to the two years of "apprenticeship" under Ron's guidance while I was still an undergrad:

the hard work of learning how to do research was already in place before I began my graduate studies.

Easing into the World of Computer Science

The academic job market in math was very challenging in 1981, but there seemed to be substantially more opportunities in computer science than there were in mathematics at that time. I applied for and was awarded an NSERC PDF (postdoctoral fellowship), which I decided to hold at the Computer Science department at the University of Manitoba. This was in spite of the fact that I had essentially no computer science training as a student. However, at that time, there were several people in the Computer Science Department at the University of Manitoba who had research interests in combinatorics, including Ralph Stanton, John van Rees, John Bate and Bill Kocay, so it was actually quite a good academic fit for me.

A year later, in 1982, I was awarded an NSERC University Research Fellowship which I held at the University of Manitoba from 1982–1989. Being in a computer science department, I expanded my research to pursue more algorithmic aspects of combinatorial designs, such as isomorphism testing, enumeration of designs and hill-climbing algorithms. Actually, I had previously worked on hill-climbing algorithms with Jeff Dinitz while we were grad students. Jeff and I devised the first successful hill-climbing algorithm to construct a nontrivial combinatorial structure, namely, strong starters in cyclic groups. However, when we published our paper [7] in 1981, we were not even aware of the term "hill-climbing algorithm."

Cryptography

After obtaining my PhD, I was interested in broadening my research expertise, but this was a slow process. In the early 1980s, I started to become aware of cryptography through the work by Blake, Fuji-Hara, Mullin and Vanstone [3] on the discrete logarithm problem in finite fields of characteristic 2. This Waterloo research group solved the discrete logarithm problem in $\mathbb{F}_{2^{127}}$ using some new extensions of index calculus methods. There was a commercial implementation of key exchange in $\mathbb{F}_{2^{127}}$ at the time, which was rendered insecure by this algorithm.

I also heard research talks by Gus Simmons on the topic of unconditionally secure authentication codes.[5] Ernie Brickell, who was working for Gus Simmons at Sandia Labs, was also investigating authentication codes, but from a more combinatorial point of view. (Ernie was a grad student at OSU at the same time I was there. We later collaborated on several cryptography papers starting in the late 1980s.)

Ernie presented a paper [5] on authentication codes entitled "A few results in message authentication" at the Southeastern Conference on Combinatorics,

[5] Gus was another important influence on my career.

Graph Theory and Computing held in Baton Rouge in 1984. This paper includes a (three-dimensional) $6 \times 6 \times 6$ Howell cube on 12 points. The Howell cube could be used to construct a certain type of "optimal" authentication code that was termed "doubly perfect" by Ernie.

The Howell cube can be described as three orthogonal one-factorizations of a certain 6-regular graph on 12 vertices. The construction of two-dimensional Howell designs was one of the main problems I addressed (and solved) in my PhD thesis. Ernie's paper was the first time I saw a cryptographic application of combinatorial designs.

Ernie's Howell cube can be presented as a list of quadruples. Each quadruple has the form (row, column, level, pair). The row, column and level specify a cell in a cube, and the cell contains an unordered pair of elements. The quadruples in Brickell's cube are as follows:

1, 1, 1, $\{1,2\}$
1, 2, 2, $\{3,4\}$
1, 3, 3, $\{5,6\}$
1, 4, 4, $\{7,8\}$
1, 5, 5, $\{9,10\}$
1, 6, 6, $\{11,12\}$
2, 1, 2, $\{9,11\}$
2, 2, 1, $\{5,7\}$
2, 3, 6, $\{1,10\}$
2, 4, 5, $\{2,12\}$
2, 5, 3, $\{3,8\}$
2, 6, 4, $\{4,6\}$
3, 1, 3, $\{7,12\}$
3, 2, 6, $\{2,8\}$
3, 3, 1, $\{4,9\}$
3, 4, 2, $\{6,10\}$
3, 5, 4, $\{1,11\}$
3, 6, 5, $\{3,5\}$
4, 1, 4, $\{5,10\}$
4, 2, 5, $\{1,6\}$
4, 3, 2, $\{8,12\}$
4, 4, 1, $\{3,11\}$
4, 5, 6, $\{4,7\}$
4, 6, 3, $\{2,9\}$
5, 1, 5, $\{4,8\}$
5, 2, 3, $\{10,11\}$
5, 3, 4, $\{2,3\}$
5, 4, 6, $\{5,9\}$
5, 5, 1, $\{6,12\}$
5, 6, 2, $\{1,7\}$
6, 1, 6, $\{3,6\}$
6, 2, 4, $\{9,12\}$
6, 3, 5, $\{7,11\}$
6, 4, 3, $\{1,4\}$
6, 5, 2, $\{2,5\}$
6, 6, 1, $\{8,10\}$

Each two dimensional projection of the Howell cube is a 6×6 array such that every symbol occurs once in each row and once in each column, and no pair of symbols occurs in more than one cell of the array.

It took me a couple more years, but by 1986 I started to work on combinatorial aspects of authentication codes and I presented my first cryptography paper ([15]) at CRYPTO '86. The CRYPTO conferences have been held annually in Santa Barbara since 1981.

At the CRYPTO '86 conference, I heard a number of fascinating talks on various aspects of cryptography. I was particularly intrigued by the notion of a threshold scheme and I published my first paper on that topic ([18], joint with Scott Vanstone) at CRYPTO '87. Our paper used combinatorial designs to construct threshold schemes.

Over the next few years, I wrote a number of papers on these two topics. Obviously this was a natural way for me to leverage my expertise in combinatorics in a new research area. Combinatorial cryptography began to establish itself as a distinct subarea of cryptography by the early 1990s as more examples of combinatorial cryptography were studied.

Here are a few topics in combinatorial cryptography, along with the year that I first studied them, over the following 17 years. (There are numerous additional topics in combinatorial cryptography that I have studied since then.)

- authentication codes (1986)
- threshold schemes (1987)
- resilient and correlation-immune functions (1992)
- visual cryptography (1996)
- broadcast encryption (1996)
- combinatorial key predistribution (1997)
- frameproof codes and traceability codes (1998)
- all-or-nothing transforms (2001)
- unconditionally secure commitment schemes (2002)
- generic algorithms for the discrete logarithm problem (2003)

What is Combinatorial Cryptography?

I like to conceptualize combinatorial cryptography as a process:

starting point: define an unconditionally secure[6] cryptographic primitive or protocol;

security definitions are phrased in terms of probability distributions;

optimal and/or "uniform" cases lead to the consideration of combinatorial objects;

cryptographic requirements motivate the mathematics that is used;

solutions might use "off-the-shelf" designs, codes, and extremal set systems, for example, but they might also motivate the study of new mathematical problems;

combinatorial characterizations, which establish the equivalence of cryptographic primitives and combinatorial structures, can sometimes be proven.

Shannon and the One-time Pad

Claude Shannon (1916–2001) was one of the giants of 20th-century science. He invented information theory and did seminal work in coding theory, cryptography, and digital circuit design. One of Shannon's many contributions in cryptography was to give the first proof of security (in 1949) of the *Vernam One-time Pad*,

[6] Unconditional security is basically the same thing as being secure against an infinitely powerful adversary.

provided the key is only used once (see [13]). I consider Shannon's security proof as being the birth of combinatorial cryptography.

An interesting historical fact is that the *One-time Pad* was invented in 1882 by Frank Miller, a Sacramento banker (see [1]). (Gilbert Vernam rediscovered the *One-time Pad* in 1917.)

The *One-time Pad* encrypts an n-bit plaintext $\mathbf{x}$ with an n-bit key $\mathbf{K}$, obtaining an n-bit ciphertext

$$\mathbf{y} = \mathbf{x} \oplus \mathbf{K}.$$

The ciphertext is decrypted by computing

$$\mathbf{x} = \mathbf{y} \oplus \mathbf{K}.$$

Shannon defined the concept of *perfect secrecy* to describe the situation where

$$\Pr[\mathbf{X} = \mathbf{x} | \mathbf{Y} = \mathbf{y}] = \Pr[\mathbf{X} = \mathbf{x}]$$

for all plaintexts $\mathbf{x}$ and all ciphertexts $\mathbf{Y}$. "Perfect secrecy" means that an observer does not gain any information about the plaintext after seeing a ciphertext.

It is not hard to prove that

$$|\mathcal{K}| \geq |\mathcal{Y}| \geq |\mathcal{X}|$$

if perfect secrecy is achieved. Furthermore, in the "boundary case" where

$$|\mathcal{K}| = |\mathcal{Y}| = |\mathcal{X}|,$$

perfect secrecy is achieved if and only if the encryption matrix is a latin square of order $|\mathcal{X}|$. That is, this optimal solution has a combinatorial characterization.

Here is an example of the *One-time Pad* with $n = 3$:

	K							
$\mathbf{x}$	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

The encryption matrix of the *One-time Pad* is a latin square of order 2^n, so it achieves perfect secrecy. The proof makes clear the underlying combinatorial structure of the optimal solution, as opposed to the algebraic description of the *One-time Pad*. Any latin square yields an encryption scheme that provides perfect secrecy. Thus, the security is based on the combinatorial structure, not the fact that encryption is done using XOR (exclusive-or) operations.

My Paper with Jim Massey

My most famous co-author was Paul Erdös, but in cryptography, I would point to my paper with Jim Massey (1934–2013). Jim is well-known for his work in decoding algorithms (e.g., the Berlekamp-Massey algorithm), block cipher design, convolutional codes, etc.

Jim and I co-authored a 1995 paper on resilient functions [17], entitled "An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions," that was published in the *Journal of Cryptology*. This paper provides a nice example of how coding theory was used to disprove a conjecture, based on an appropriate combinatorial characterization.

An (n, k, t)*-resilient function* (or *RF*) is a function $f : (\mathbb{Z}_2)^n \rightarrow (\mathbb{Z}_2)^k$ such that, if any t inputs are fixed and the remaining $n-t$ inputs are chosen uniformly and independently at random, then every output k-tuple is equally likely. Given n and k, the fundamental problem is to maximize t.

A resilient function f is *linear* if $f(\mathbf{x}) = \mathbf{x}M$ for some n by k binary matrix M. It was known that the existence of an $[n, k, d]$-binary code is equivalent to the existence of a linear $(n, k, d-1)$-RF. Thus, studying linear resilient functions is equivalent to studying linear codes. Perhaps based on this equivalence, it was conjectured in 1988 by Bennett, Brassard and Robert [2] that, if an (n, k, t)-RF exists, then a linear (n, k, t)-RF exists.

I proved the following combinatorial characterization of (n, k, t)-RF in 1993 in [16]: An (n, k, t)-RF is equivalent to a large set of orthogonal arrays $OA_\lambda(t, n, 2)$, where $\lambda = 2^{n-k-t}$. In a bit more detail, if f is an (n, k, t)-RF, then, for any binary k-tuple $\mathbf{y}$, the inverse image $f^{-1}(\mathbf{y})$ is an orthogonal array and the 2^k orthogonal arrays thus obtained comprise a large set (i.e., they partition the entire space $\{0, 1\}^n$).

The above-mentioned characterization allows coding-theoretic methods to be used to study arbitrary (linear or nonlinear) resilient functions. Using the (nonlinear) Kerdock codes, it is possible to construct a $(2^{r+1}, 2^{r+1}-2r-2, 5)$-RF. The Kerdock code has dual distance $d' = 6$ and hence it is an orthogonal array with strength $t = 5$. In the original version of the paper, which was submitted to the *Journal of Cryptology*, I provided a complicated method of extending this OA to a large set of OAs. The nonexistence of a linear RF with the same parameters followed from known results in coding theory. A referee of the paper pointed out that my construction was not needed because the Kerdock code is systematic and hence a large set of orthogonal arrays (consisting of translates of the code) exist trivially. The editor-in-chief of the *Journal of Cryptology* at the time, Gilles Brassard, suggested that I include the referee as a co-author (if the referee was willing). The referee turned out to be Jim Massey.

It is interesting to note that most of the disproof of the conjecture used "off-the-shelf" coding theory, ultimately based on Delsarte's seminal work [6]. The tricky part was extending a nonlinear orthogonal array to a large set of orthogonal arrays. However, as described above, this turned out to be not so tricky after all!

Research Philosophy

Up to the present day, I have continued my research in combinatorial mathematics, applications of combinatorics and various aspects of cryptography, including, of course, combinatorial cryptography. I have never been so interested in developing theory for its own sake—I like to see some kind of motivation for the problems I study. I also try to be cognizant of the danger of researching ever more specialized problems which may not be of interest to anyone but the author, such as “hemi-demi-flippoids that vanish under close inspection.”[7]

I choose my research topics based on various criteria:

- intrinsic interest of the problem (aesthetics)
- my ability to make a contribution based on my knowledge and skill set, and
- potential applications of the problem in any area of computer science.

I have often sought out “practically motivated” problems raised by others when I think that combinatorial techniques will prove fruitful in their solution. At the same time, I also work on any mathematical problems (usually combinatorial) that happen to appeal to me.

Some Influential Books

I thought it might be of interest to mention a few examples of extremely well-written books from which I have learned a great deal.

H. J. Ryser, *Combinatorial Mathematics*, 1963 [12]. From the preface: “But effort and ingenuity lead to mastery, and our subject holds rich rewards for those who learn its secrets.” This book is a very short but well written classic treatment of combinatorial theory up to the year 1963. It still makes excellent reading today.

M. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, 1979 [8]. Wikipedia states: “In a 2006 study, the CiteSeer search engine listed the book as the most cited reference in computer science literature.”[8] This is, in my opinion, the best example of a clearly written book on a very technical subject. It is how I (as a complete novice) learned about this theory in the early 1980s.

G. J. Simmons (Editor), *Contemporary Cryptology: The Science of Information Integrity*, 1992 [14]. This book is an edited collection of extremely useful survey articles, which is now (unavoidably) somewhat out of date. The field of cryptography needs more survey papers! These are invaluable to keep track of research trends and to summarize the most important developments in the field.

[7] I attribute this amusing term to Curt Lindner.

[8] This quote is from the Wikipedia article “Computers and Intractability” (`https://en.wikipedia.org/wiki/Computers_and_Intractability`), which is released under the Creative Commons Attribution-Share-Alike License 3.0

J. H. van Lint and R. M. Wilson, *A Course in Combinatorics, 2nd Edition*, 2001 [19]. This is my favourite combinatorics book. It is extremely well written and it contains a wealth of information on many areas of combinatorics. A reader can just pick it up and start reading any random page, and there will be interesting, beautiful mathematics to be found.

Mathematical Exposition

I would like to stress the importance of clear mathematical exposition. The following quote is sometimes attributed (perhaps erroneously[9]) to Albert Einstein:

> "If you can't explain it simply, you don't understand it well enough."

I saw this quote last winter on a poster on the door of an engineering faculty member's office door that I passed each day when I walked indoors from my car to the Davis Centre.

My goal is always to explain things clearly and precisely. Here are a few guiding principles for my mathematical writing and research talks:

- Use mathematics and English to reinforce each other. For example, give precise mathematical definitions but also explain what the definitions mean in plain language.
- Do not overburden the reader (or listener) with cumbersome notation, unnecessary jargon, etc.
- Whenever possible, provide examples to illustrate concepts, definitions, proofs, etc. An example is worth a hundred proofs!
- If something is complicated, try to simplify it! Simplification benefits the reader, of course, but it can also lead to a deeper understanding by the writer, which may suggest generalizations, extensions, etc. There have been many times when my understanding of a research paper has been accomplished by simplifying the ideas, notation, etc., and this has led to me doing additional research on the same problem.

The following definition is from a recent preprint on the IACR eprint server. It is a typical example of the kind of notation that is commonly encountered in cryptographic definitions.[10]

[9] There is apparently no source to substantiate the claim that Einstein actually said this, but it is still a good quote.

[10] I should emphasize that I am not specifically criticizing the wording and notation in this definition. I am just using it to illustrate how complicated cryptographic definitions have become in recent years.

> Intuitively, a secure secret sharing scheme must be such that all qualified subsets of players can efficiently reconstruct the secret, whereas all unqualified subset have no information (possibly in a computational sense) about the secret.
>
> **Definition 2** (Secret sharing scheme)**.** Let $n \in \mathbb{N}$, and $\mathcal{A}$ be an access structure for n parties. We say that $\Sigma = (\mathsf{Init}, \mathsf{Share}, \mathsf{Rec})$ is a secret sharing scheme realizing access structure $\mathcal{A}$ in the CRS model, with message space $\mathcal{M}$ and share space $\mathcal{S} = \mathcal{S}_1 \times \cdots \times \mathcal{S}_n$, if it is an n-party secret sharing in the CRS model with the following properties.
>
> (i) **Correctness:** For all $\lambda \in \mathbb{N}$, all $\omega \in \mathsf{Init}(1^\lambda)$, all messages $m \in \mathcal{M}$, and for all subsets $\mathcal{I} \in \mathcal{A}$, we have that $\mathsf{Rec}(\omega, (\mathsf{Share}(\omega, m))_{\mathcal{I}}) = m$, with overwhelming probability over the randomness of the sharing algorithm.
>
> (ii) **Privacy:** For all PPT adversaries $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$, we have
>
> $$\{\mathbf{Privacy}_{\Sigma,\mathsf{A}}(\lambda, 0)\}_{\lambda\in\mathbb{N}} \approx_c \{\mathbf{Privacy}_{\Sigma,\mathsf{A}}(\lambda, 1)\}_{\lambda\in\mathbb{N}},$$
>
> where the experiment $\mathbf{Privacy}_{\Sigma,\mathsf{A}}(\lambda, b)$ is defined by
>
> $$\mathbf{Privacy}_{\Sigma,\mathsf{A}}(\lambda, b) := \left\{ \begin{array}{c} \omega \leftarrow\$\ \mathsf{Init}(1^\lambda); (m_0, m_1, \mathcal{U} \notin \mathcal{A}, \alpha_1) \leftarrow\$\ \mathsf{A}_1(\omega) \\ s \leftarrow\$\ \mathsf{Share}(\omega, m_b); b' \leftarrow\$\ \mathsf{A}_2(\alpha_1, s_{\mathcal{U}}) \end{array} \right\}.$$

The above mathematical definition is very hard to decipher for anyone who is not already an expert. There is nothing unusual about this example, as cryptography papers are frequently burdened by extremely complicated notation, definitions, proofs, etc. However, it should be noted that the paragraph preceding the formal definition conveys the essential idea in a concise and understandable way, which is a definite positive.

How to Turn a Complex Mystery into a Simple Truth

The eminent combinatorial mathematician Curt Lindner gave a memorable after-dinner speech at the 1984 Southeastern Conference on Combinatorics, Graph Theory and Computing, having the above-mentioned title. I emailed Curt recently to fill in a few details about this talk. Curt said this:

> "I showed how to get an embedding for a partial idempotent quasigroup of order n into a complete idempotent quasigroup of order $4n$ with a simple picture . . . then I gave a proof that the containing quasigroup was finite using universal algebra. The universal algebra proof was 50 pages and used reduction chains to canonical forms.
>
> I conjectured that if I gave the universal algebra proof at a famous university it would be considered beautiful mathematics . . . whereas if I gave the $4n$ proof most of the people in the audience would say 'who the hell invited this idiot to give a talk.'
>
> I was illustrating the fact for many people it's the machinery that matters, not the result."

Of course the first result is much stronger than the second one. The question Curt is raising is whether complicated "deep" mathematics is really to be preferred over simple, direct arguments. Personally, I have always been most inspired by clarity, creativity, and originality.

Photo

The following photo was taken at a reception at SAC 2019 immediately following my talk. From left to right, there is Ron Mullin (my PhD supervisor), me, and Atefeh Mashatan. Atefeh introduced my talk; she is a former PhD student of mine who is now a faculty member at Ryerson University in Toronto.

Dedications

Research is much easier and enjoyable with the contributions of collaborators. I would like to dedicate this talk to all my co-authors over the years:

B. Alspach, B. Anderson, D. Archdeacon, A. Assaf, G. Ateniese, M. Atici, T. Berson, J. Bierbrauer, E. Billington, S. Blackburn, C. Blundo, E. Brickell, H. Cao, J. Carter, M. Carter, M. Chateauneuf, D. Chen, K. Chen, C. Colbourn, M. Colbourn, P. D'Arco, A. De Bonis, A. De Santis, D. Deng, J. Dinitz, P. Dukes, P. Eisen, P. Erdös, T. Etzion, H. Ferch, L. Frota-Mattos, A. Giorgio Gaggia, I. Goldberg, G. Gong, K. Gopalakrishnan, D. Gordon, M. Grainger, C. Guo, A. Hamel, A. Hartman, K. Henry, D. Hoffman, J. Horton, E. Ihrig, T. Johansson, S. Judah, B. Kacsmar, M. Kendall, K. Khoo, W. Kishimoto, W. Kocay, E. Kramer, D. Kreher, K. Kurosawa, T. Laing, K. Lauinger, J. Lee, P.-C. Li, C. Lindner, A. Ling, X. Ma, S. Magliveras, K. Martin, W. Martin, A. Mashatan, J. Massey, B. Masucci, A. Mattern, J. McSorley, E. Mendelsohn,

W. Mills, J. Muir, R. Mullin, M. Nandi, N. Nasr Esfahani, S.-L. Ng, M. Nojoumian, W. Ogata, K. Okada, P. Ostergard, K. Ouafi, A. Panoui, M. Paterson, R. Phan, K. Phelps, M. Qu, R. Rees, C. Rodger, A. Rosa, B. Roy, H. Saido, P. Sarkar, P. Schellenberg, E. Seah, V. Sós, J. Staddon, R. Stanton, R. Strobl, J. Sui, B. Sunar, C. Swanson, L. Teirlinck, T. Tillson, T.V. Tran, J. Upadhyay, U. Vaccaro, J. Van Rees, S. Vanstone, S. Veitch, D. Wagner, W. Wallis, Y. Wang, R. Wei, W. Wei, Y.-J. Wei, J. Wu, J. Yates, J. Yin, G. Zaverucha, S. Zhang, and L. Zhu.

As well, I would like to dedicate this paper to my family: my wife, Janet; my children, Michela and Aiden; and my brothers, Murray and Tom.

References

1. S. M. Bellovin. Frank Miller: inventor of the one-time pad. *Cryptologia* **35** (2011), 203–222.
2. C. H. Bennett, G. Brassard and J.-M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing* **17** (1988), 210–229.
3. I. F. Blake, R. Fuji-Hara, R. C. Mullin and S. A. Vanstone. Computing logarithms in finite fields of characteristic two. *SIAM Journal on Algebraic and Discrete Methods* **5** (1984), 276–285.
4. G. Brian, A. Faonio and D. Venturi. Continuously non-malleable secret sharing for general access structures. *Cryptology ePrint Archive: Report 2019/602.*
5. E. F. Brickell. A few results in message authentication. *Congressus Numerantium* **43** (1984), 141–154.
6. P. Delsarte. *The Association Schemes of Coding theory.* PhD Thesis, Université Catholique de Louvain, June 1973.
7. J. H. Dinitz and D. R. Stinson. A fast algorithm for finding strong starters. *SIAM Journal on Algebraic and Discrete Methods* **2** (1981), 50–56.
8. M. R. Garey and D. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness.* W. H. Freeman and Company, 1979.
9. R. Honsberger. *Ingenuity in Mathematics.* MAA, 1975.
10. R. Honsberger. *Mathematical Morsels.* MAA, 1979.
11. R. C. Mullin, D. R. Stinson and W. D. Wallis. Concerning the spectrum of skew Room squares. *Ars Combinatoria* **6** (1978), 277–291.
12. H. Ryser. *Combinatorial Mathematics.* Math. Assoc. Amer, 1963.
13. C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal* **28** (1949), 656–715.
14. G. J. Simmons, (Editor) *Contemporary Cryptology: The Science of Information Integrity*, IEEE Press, 1992.
15. D. R. Stinson. Some constructions and bounds for authentication codes. *Lecture Notes in Computer Science* **263** (1987), 418–425 (Advances in Cryptology – CRYPTO '86).
16. D. R. Stinson. Resilient functions and large sets of orthogonal arrays. *Congressus Numerantium* **92** (1993), 105–110.
17. D. R. Stinson and J. L. Massey. An infinite class of counterexamples to a conjecture concerning non-linear resilient functions. *Journal of Cryptology* **8** (1995), 167–173.

18. D. R. Stinson and S. A. Vanstone. A combinatorial approach to threshold schemes. *Lecture Notes in Computer Science* **293** (1988), 330–339 (Advances in Cryptology – CRYPTO '87).
19. J. H. van Lint and R. M. Wilson. *A Course in Combinatorics, 2nd Edition*, Cambridge University Press, 2001.
20. R. M. Wilson. Constructions and uses of pairwise balanced designs. In "Combinatorics, Proceedings of the NATO Advanced Study Institute held at Nijenrode Castle, Breukelen, The Netherlands 8–20 July 1974," NATO Advanced Study Institutes Series book series (ASIC, vol. 16), pp. 19–42.