MEMORIAL TRIBUTE

In Memoriam: Peter L. Montgomery (1947–2020)

Joppe W. Bos and Kristin E. Lauter

Peter Lawrence Montgomery passed away on February 18, 2020. Peter was a brilliant mathematician whose inventions found their way into the everyday life of billions of people on a daily basis. If you have visited a webpage, made an electronic payment, or used a messaging app, then chances are high that one of the mathematical techniques proposed by and named after Peter Montgomery was used to ensure your security in a time and memory efficient way. Peter's main contributions are in the field of *computational number theory*. Peter was largely motivated by the desire to improve *integer factorization algorithms* although he also wrote papers about many other techniques ranging from extremely clever low-level computer algorithms to cryptosystems built on top of algebraic number theory. His contributions end up being useful to speed up the arithmetic in virtually all public-key cryptographic systems used around the globe to protect our information today.

1. His Life

Peter was born in San Francisco, California, on September 25, 1947. He attended UC Berkeley and received a BA with Honors in Mathematics in 1969 and an MA in 1971. Peter's undergraduate advisor was Derrick H. Lehmer, an excellent match given Peter's research interest since high school: integer factorization.

In 1967, Peter was among the five highest-ranking participants in the William Lowell Putnam Mathematical competition, and was named a Putnam Fellow. In 1972, Peter started working as a junior programmer for System Development Corporation (later called Unisys Corporation) in Huntsville, Alabama, and became the expert on the Cray CDC 7600 supercomputer.

During this time Peter remained active in the mathematical community. This is illustrated by a series of papers with Erdős, Graham, Rothschild, Spencer, and Strauss (see [EGM+73] and related work) in the mid-1970s on Euclidean Ramsey theorems. When implementing textbook multiprecision multiplication in assembler on a PDP series computer, he noticed there were unused registers and wanted to find a way to exploit them [BL17]. He managed to do so by interleaving the multiplication with the modular reduction. This led to arguably one of his most widely-used results: Montgomery multiplication.

About twenty years after his time in Berkeley, David G. Cantor supervised Peter's PhD dissertation on his favorite topic in computational number theory. He received his PhD in mathematics from UCLA in 1992. Peter held a position in the mathematics department at Oregon State University in 1993. He was active in his factoring research while at OSU, but he found teaching in the classroom challenging.

In 1998 Peter accepted a position with the Cryptography and Anti-Piracy group at Microsoft Research in Redmond, WA. Peter's contributions to Microsoft products were focused around public-key cryptography. Bignum

Joppe W. Bos is a senior principal cryptographer at NXP Semiconductors. His email address is joppe.bos@nxp.com.

Kristin E. Lauter is a principal researcher and partner research manager at Microsoft Research, and affiliate professor at the University of Washington. Her email address is klauter@microsoft.com.

Communicated by Notices *Associate Editor William McCallum.*

DOI: https://doi.org/10.1090/noti2258

Figure 1. Peter L. Montgomery at age 15 (left), in 1980 (middle), and in 2009 (right).

was the library he wrote for modular arithmetic which was used as the foundation for his internal implementation of the RSA cryptosystem. The second author worked closely with Peter from 1999–2010 on optimizing and deploying Microsoft's Elliptic Curve Cryptography library across all platforms; it was exposed through CNG, the Crypto Next Generation API, which started shipping in Windows Vista in 2005.

Peter retired from Microsoft in 2014.

2. Kristin E. Lauter

Peter was one of only a few PhD mathematicians at Microsoft Research in 1999 when I arrived, and he was my closest colleague and only collaborator for my first few years there. We published four papers and numerous patents on elliptic curve and hyperelliptic curve cryptography together, optimizing for efficiency of operations for different machine instruction sets, introducing algorithmic improvements, and alternative approaches to point compression.

Peter did not like to go anywhere in a car because he said "it is good for the individual, but not for society." This is also highlighted in the letter Peter wrote for his 1995 high school reunion.

> The environmental movement blossomed while I was at Berkeley, and I vowed in 1972 never to drive again. But Huntsville lacked sidewalks between home and work. For one year, I walked with large placards "WE NEED SIDEWALKS" and "WHERE'S MY LANE," until the City Council voted to install sidewalks near schools and to fund bike lanes and paths.

When Peter was interviewed for a job at AT&T/Bell Labs in the 1990s, he was distressed because there were no sidewalks on campus when he went for the interview, so he turned down the job. He said he had also taken part in campus demonstrations during his time as a student at UC Berkeley in the 60s, for various progressive causes.

At Microsoft Research (MSR), Peter took the city bus to team dinners and events (and knew the schedules by heart). He always walked or took the shuttle around Microsoft campus, and I did not like to drive either, so we often walked or took the shuttle together to the other side of campus for meetings with Windows developers. I learned many number-theoretic algorithms from him while riding the shuttle and walking around together. He explained the algorithms using small numerical examples. For example, he always wanted to factor the room number for the meeting we were going to. With the building number, it was a 6- or 7-digit number, which gave him a chance to figure out or explain many factoring tricks to me.

Peter also loved children, and he often bought presents for my twin daughters, such as blinking tennis shoes for their third birthday (see Figure 2 (left)). He was in Europe when my daughters were born and so he collected and brought back to me the newspapers from three or four major European cities from the day of their birth. On several occasions he brought presents for them to work, wrapped in store packaging, which he carried around campus to meetings until he had a chance to give them to me. He was happy to help me watch them at the number theory conference in Banff in 2003 when they were 3 (see Figure 2 (right)). On an outing up the Banff gondola, he thought that all their requests were perfectly reasonable and that we


Figure 2. Peter Montgomery with Kristin Lauter's daughters at the Conference in Number Theory in Honour of Professor H.C. Williams, Banff, Alberta, Canada, 2003.

should accommodate all of them, which was not always possible due to safety concerns!

Peter insisted on taking the Greyhound bus back and forth from Seattle to Banff for the conference, which was an overnight trip with some delays on the road and so he arrived a little late (and with some funny stories to tell). He took the bus or train to many other conferences as well, such as the biannual West Coast Number Theory conferences in Asilomar outside of Monterrey, California. He loved the problem session at the biannual West Coast Number Theory conference, interacting with people and submitting and solving problems. He also loved the problems in the MAA *American Mathematical Monthly* publication, and often wrote up solutions to those problems.

Peter was very generous, and he always wanted to contribute something so he often bought watermelons and made brownies for Crypto group meetings and parties. He didn't shy away from taking part in activities and one year we almost lost him when he attempted to go out on a canoe on Lake Sammamish during a team picnic.

He also knew that I liked to play bridge, so for many years he would cut out the bridge column from the newspaper on a daily or weekly basis and leave it on my desk in the morning so we could discuss it at lunchtime. He always liked to have two cans of grape juice and a chocolate milk in the Microsoft cafeteria with his lunch, and he did not like spicy food so he often got fried chicken.

Before he moved up to Redmond he telecommuted from Marin County. He lived there with his mother and her caregiver until his mother passed away. When he needed to come to Redmond for a visit he would wake up early so he could take public transportation to the San Francisco airport in time for his flight. When he moved to Redmond he lived in various apartments by himself. I became concerned about the access and the uneven sidewalks he could trip on in the darkness. When I talked to him about moving into an assisted care facility close to campus, he told me that would not work while he was working, because they served lunch at the facility and he would not be there for lunch if he was at the office.

Peter had a true passion for mathematics and loved Techfest (the annual Microsoft internal research 2.5-day fair) even though most people could not understand his explanations of our Elliptic Curve Cryptography software. See Figure 3 for "Evening Destinations," a puzzle Peter created for Techfest to explain the Number Field Sieve. He gave the names of 40 US States in a list, and the puzzle was to find the subset of them such that each letter (with capitalization) appeared an even number of times, in the amalgamated set of letters. If you work on this puzzle, you will get a good idea of what it was like to learn number-theoretic algorithms from Peter.

Peter was a funny and fun-loving person, a gentle and generous soul.

3. Joppe W. Bos

During his time at MSR, Peter continued collaborations with researchers world-wide and was a regular long-term guest at various universities and research institutes in Europe. I have fond memories of Peter's visit during my PhD at the laboratory for cryptologic algorithms at the École Polytechnique Fédérale de Lausanne (EPFL) in Switzerland. When bringing Peter to his hotel it was always a challenge to bring his considerable suitcase on the Lausanne metro since regular cabs were simply not up to the task.

During this time we worked on computational approaches to compute a 112-bit elliptic curve discrete logarithm (at the time a computational new record) using a

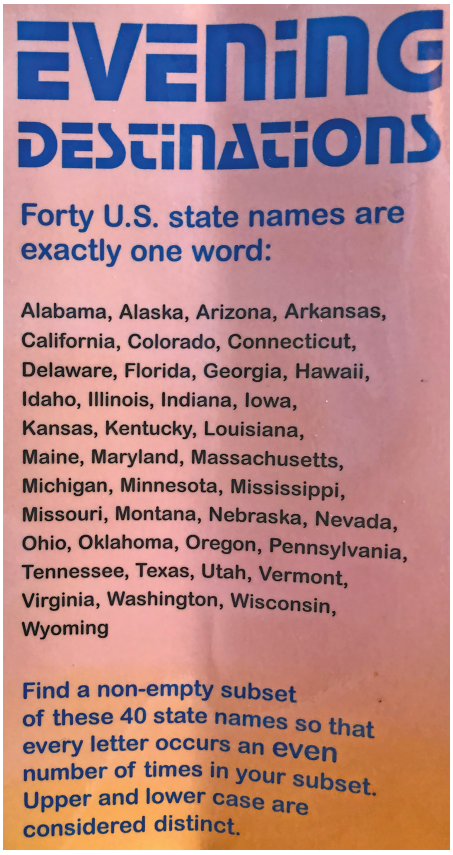

Figure 3. Peter's Techfest puzzle to explain the Number Field Sieve.

cluster of 215 PlayStation 3 game consoles with an interesting instruction set [BKK+12]. This was an effort which is equivalent to about 14 full 56-bit DES key searches. In order to utilize all computational power one had to compute using the single-instruction, multiple data (SIMD) paradigm: performing identical steps on multiple streams of data. During the computation of the binary version of the Euclidean algorithm one needs to compute the trailing zero bit count of a positive integer k (or stated differently, determining the maximum i such that 2^i divides k). This can be done efficiently using a loop but does not work well with SIMD. Peter loved these type of puzzles and studied the instruction set manual of the Cell processor (the one used in the gaming console) and quickly presented an elegant SIMD-friendly solution that the trailing zero bit count of a positive integer k can be computed using the population count of $\bar{k} \wedge (k-1)$ (where $\bar{k}$ is the one's complement of k). These beautiful computational gems contributed to the overall performance of the project.

The collaboration continued when I was a research intern at Microsoft Research in 2011 under the supervision of Peter. The topic was (of course) related to integer factorization and Peter would make sure "his" student would be welcome at MSR and attend all the social events in order to make the most out of his stay.

A typical example of Peter's ability with numbers was when we were investigating some divisibility properties of the cardinality of elliptic curve groups modulo primes. A curve which seems to have favorable properties was defined using a curve parameter $d = -\left(\frac{77}{36}\right)^4$. One morning Peter entered my office and casually remarked on how interesting it was that one could write d as $-\left(\frac{g^2-1}{2g}\right)^4$ (which is indeed true for $g = \frac{9}{2}$). Spotting this pattern in a series of a single element turned out to be the key to prove this particular curve property [BBB+13, Corollary 3.5].

In 2012 I joined MSR's Cryptography Research Group as a post-doctoral researcher and had the opportunity to work with Peter on a daily basis. Over time my wife and I started to assist Peter with weekly chores such as grocery shopping: he always insisted on paying for our lunch that Saturday or Sunday to "even things out."

Peter started weekly bridge lessons to teach me and several other MSR crypto colleagues the basics of the game and the various bidding conventions. It was clear from the start that the ability and experience of Peter playing bridge was well beyond what I could ever hope to achieve. He was a very patient teacher.

Peter was a great mentor, colleague, and friend and I will miss his practical jokes.

4. Betty Montgomery

Peter Lawrence Montgomery was my brother-in-law. He was the oldest of three boys and grew up in a quiet suburb of north San Rafael, California, called Terra Linda. Pete and I were the same age, and I met him when we were 21 when I started dating his younger brother, John. There was no mistaking that Peter was "different." On first meeting, people might have mistakenly thought he was intellectually disabled, but if you took the time to get to know him, you would discover one of the keenest minds imaginable, and one of the kindest people you could ever meet. Pete was childlike in many ways: his language skills, both verbal and written, were like those of a young child, so he was handicapped to some degree in that regard. But, of course, that was balanced by the fact that he was to become one of the greatest mathematical geniuses of our time. He was clearly a savant.

His early life was troubled as he tried to come to terms with a world that didn't understand him, nor did he understand the world. Once he got past his teen years, however, he found his niche in the mathematical world where he was accepted and appreciated. Many years later I would read an article that articulated a condition on the autism

spectrum called Asperger's. It was clear that this condition matched Peter's symptoms, and it gave us an understanding of his condition.

Peter adored my children—his niece Heather and his nephew Page. Whenever we would visit each other, we spent hours on jigsaw puzzles and complicated card games like Liverpool. He would take the kids on long walks around town until he wore them out, and I would get a phone call from some store to come pick them up because the kids were too tired to walk home. No one seemed to mind, though. One thing he liked to do was name all of the states that had a particular letter in their names. When the kids would quickly tire of this, Peter was understanding and would find another way to connect with them. With the adults, he loved to play bridge. It was difficult to play bridge with him, however, because he would memorize each card as it was played and calculate who had what cards. Then, if you were his partner and lost, he would critique what mistakes you made one by one. He didn't really care what people were doing. As long as he was in your company, Peter seemed content.

Pete loved a good joke and had a good sense of humor. Every St. Patrick's Day he would cook breakfast—always the same—scrambled eggs and milk—both dyed green with food coloring, and toast with green mint jelly. He enjoyed practical jokes, and always kept people on their toes. When he received his doctorate from UCLA, the presenter was shorter than Pete, so Pete walked squatted down the length of the stage to receive his diploma at eye level to the presenter.

Peter had a very practical mind and he was eccentric. He never wore glasses but used a magnifying glass instead. We had to encourage him to wear a belt because he thought a rope did just as well. He didn't appreciate entertainment. We took him to Disneyland, but he couldn't understand why people wasted electricity on the opening and closing of the eye on Geppetto's whale. Pete couldn't understand why people needed aquariums, or museums. Nor did he watch any TV or go to movies. His world, his language, was math, and in that world he was in his element and he was happy.

He also had attachments to things. When he moved to the Seattle area, he had a huge collection of nickels that filled a backpack. He couldn't take them on the plane for some reason, so rather than cash them in, he took a bus holding that backpack the entire time. He hoarded everything, even a sandwich sign he once wore every day as he walked to work in an area of Huntsville, Alabama, that didn't have sidewalks. The sign said: "Where's my lane?" He had an article written up about him in the local newspaper where he was fondly spoken of as a well-known and beloved eccentric while living there.

Then came the time some years back when Peter had a seizure and he was left brain damaged. It seemed such a cruel thing to happen to a person with his superior capacity for knowledge. My daughter, who is a clinical neuropsychologist, did what she could to get him the right help in Seattle where she did her residency, but there wasn't much they could do. Pete went to live with his two brothers after that, and he needed 24-hour care for the rest of his life. I mourned for Peter then, I mourned for Peter during those years of incapacity, and I mourn for Peter still. Yet in spite of everything that limited him, Peter did what all of us hope to do, what all of us wish we could say at the end of our days. Peter made a difference.

5. Mathematical Contributions

Peter has made significant contributions to computational number theory which are described in detail in the book dedicated to this topic [BL17]. Let us highlight a subset of Peter's contributions here.

Integer factorization algorithms can be divided into two categories: 1) general purpose integer factorization algorithms where the run-time depends on the size of the integer to be factored; 2) algorithms where the run-time mainly depends on the size of the unknown prime divisor of the integer to be factored. Peter was heavily involved in optimizations, from both a mathematical and an engineering perspective, to obtain new integer factoring records for both categories. Many of his techniques were specifically designed to speed up integer factorization but turned out to have much larger implications in the field of cryptography.

Algebraic-group factorization algorithms. One of the approaches where the run-time depends mainly on the size of the unknown prime divisor was proposed in the 1970s by John Pollard. The idea behind *Pollard's* $p-1$ *integer factorization method* is to find prime factors p of the integer n for which the groups $(\mathbf{Z}/p\mathbf{Z})^*$ have B_1-powersmooth order, so that p can be found in time mostly linear in the largest prime factor of $p-1$. Similarly, Hendrik Lenstra's elliptic curve method (ECM) for integer factorization is the asymptotically fastest method to find relatively small factors of large integers. ECM works analogously to Pollard's method, but replaces the fixed group $(\mathbf{Z}/p\mathbf{Z})^*$ of order $p-1$ by elliptic curve groups with orders behaving like random integers *close to* p.

For these algorithms, one can extend the computation to a second stage by selecting a bound $B_2 > B_1$ and looking for a factor p of n for which the largest prime factor of $p-1$ is $\leq B_2$ and the second largest prime factor of $p-1$ is $\leq B_1$. Pollard already suggested that one could use a circular convolution to evaluate a polynomial along a geometric progression to do this efficiently without providing

further details. These details were made explicit by Montgomery and Silverman in [MS90] for the Pollard $p-1$ method, but they posed an open problem as to how the method could be made to work for ECM. Enabling this fast second stage for the ECM method was the topic of Peter's PhD thesis [Mon92]. Almost 16 years after his dissertation he returned to this topic with Kruppa and looked into further space-efficient optimization techniques [MK08].

Montgomery curves. Inspired by the use of elliptic curves in cryptography for the ECM integer factoring, Koblitz and Miller independently proposed using the group of points on an elliptic curve defined over a finite field as the basis for discrete logarithm cryptosystems, now known as elliptic curve cryptography (ECC). Peter proposed multiple techniques [Mon87] to optimize the ECM method which turned out to have a significant impact on the practical deployment of ECC as well. Peter writes, "The author later discovered an alternative parametrization that requires no inversions." This parametrization, now known as the *Montgomery curve*, in combination with the proposed scalar multiplication algorithm, now known as the *Montgomery ladder*, allows scalar multiplication on the elliptic curve without using both of the curve coordinates. This omission of one coordinate results in record-setting arithmetic counts to implement this scalar multiplication. This resulted in a constant-time speed-up of both ECM and ECC, since for the most commonly used cryptographic schemes, only one coordinate is needed as the outcome of the key-exchange method.

Much later, an efficient and secure Montgomery curve was proposed by Bernstein in [Ber06] and has become the de facto standard in public-key cryptography: it is used to secure your internet connection and your social messaging applications. The regular structure of the Montgomery ladder also turned out to be one of the fundamental tools used to harden cryptographic implementations against *side-channel attacks*: attacks which use physical features of an implementation, such as the elapsed time or power consumption, to break its security.

General factorization algorithms. General purpose integer factorization methods all follow Maurice Kraitchik's variation of Pierre de Fermat's method by looking for a congruence of squares. The idea is to construct pairs of integers x, y such that $x^2 \equiv y^2 \bmod n$. Since n divides $x^2-y^2 = (x-y)(x+y)$ it follows that if $n \neq \pm y \bmod n$, then $\gcd(x-y, n)$ is a nontrivial factor of n. For the (General) Number Field Sieve (NFS), one needs to find good polynomials satisfying certain conditions and with an above-average probability of resulting in smooth integers. Peter played a significant role in polynomial selection and distinguishing more effective parameters for the Number Field Sieve. This has grown into an active area of research (cf. [Cox15] and related work). Next, these polynomials are used to generate a large number of outputs which need to be checked for smoothness. In the early days of the NFS, Peter's optimizations to the line-siever implementation were broadly used in a number of integer factorizations [BMtR+96]. After collecting relations, one needs to find a subset such that their product is a square. This is done by looking at the exponents of the prime factors modulo two and finding dependencies. These exponent vectors are very sparse, and straightforward methods like Gaussian elimination do not take advantage of this sparseness. For example, in the RSA-768 factorization, the exponent vectors had 144 nonzero coefficients out of the $2 \cdot 10^8$ in total. Peter introduced a sequence of subspaces of dimension larger than one for the Lanczos algorithm; this resulted in the block Lanczos method [Mon95] which is very efficient on modern computers and has been used in many factorization records. The final step in the Number Field Sieve is the square root computation of a huge algebraic number given as a product of a lot of small ones. A general efficient solution to compute this in practice was provided by Montgomery in [Mon94].

Montgomery multiplication. Peter is probably most well known for his technique to compute modular multiplication on modern computer architectures without using expensive divisions. Multiplication and division algorithms have significantly different performance characteristics on almost all computer architectures. Multiplication can be up to ten times faster depending on the target architecture. This was the motivation for Montgomery to devise specific code sequences to perform division by invariant integers using multiplication [GM94]. These code sequences are applied in compilers to create faster compiled binaries. Similar motivation gave rise to his arguably most famous work: in order to accelerate modular multiplication on modern computer platforms, and motivated to put unused registers to work [BL17], Montgomery introduced a modular reduction technique now known as *Montgomery reduction* in his seminal 2.5 page article [Mon85]. The main idea behind this approach is to change the representatives of the residue classes and change the modular multiplication accordingly. This change of residue class ensures that the multiplication of two inputs in Montgomery form corresponds to the desired result in Montgomery form. The main idea is to choose a Montgomery radix r larger than and coprime to the modulus m. Then $cr^{-1} \bmod m$ can be computed with

$$d = (c + m(\mu c \bmod r))/r$$

which uses the precomputed value $\mu = -m^{-1} \bmod r$. Whenever $0 \leq c < m^2$, then $0 \leq d < 2m$. The division

by r is an exact division, and when $r = 2^w$, this division by r is a simple right shift by w bits and reduction modulo r is extracting the w least significant bits: both operations are essentially for free on modern computer architectures. This essentially computes a multiplication modulo m at the cost of two multiplications. Due to the overhead of changing representations, Montgomery arithmetic is best when used to replace a sequence of modular multiplications, since this overhead is amortized. A typical use-case scenario is for example when computing a modular exponentiation as required in the widely used RSA cryptosystem.

Cryptographic pairings. When Peter came to Microsoft in the late 1990s, he worked on writing bignum, to provide an implementation of RSA-based cryptosystems. He implemented several approaches to modular multiplication and reduction, including Montgomery multiplication. Starting in 1999, working together with the second author, Peter focused on building and optimizing the Elliptic Curve Library for Microsoft, which started shipping in Windows Vista in 2005. From there it was ported to many other products and we worked on optimizations for different platforms. For example, he wrote optimized assembly code for the ECC library on the ARM platform, which we transferred to the Windows CE mobile division. Although he had enabled Montgomery multiplication as one option, in some of the main instances we chose not to use it based on performance comparisons with other options. Although (weighted) projective coordinates were a common choice at the time due to the highly specialized NIST primes, we often chose configurations with affine coordinates because Peter had implemented an extremely fast modular inversion, and modular multiplication was not that fast for general primes. The ratio of modular inversion to multiplication in his code was more like 5 : 1 instead of 80 : 1 which was reported in external publications at the time.

Just as the Montgomery ladder does not need the y-coordinate of the elliptic curve point for scalar multiplication, in [ELM03] we introduced the double-and-add trick for affine coordinates which saves a multiplication in combined elliptic curve operations by not computing the intermediate y-coordinate. Peter was interested in optimizing scalar multiplication using different bases (such as base-2 or base-3 expansions of a scalar), and in [CJLM06] we presented a combined ternary/binary method to perform efficient scalar multiplication using a variant of the double-and-add trick which is faster whenever a field inversion is more expensive than six field multiplications.

In 2001, new cryptographic applications of pairings on elliptic curves were introduced. Pairings on elliptic curves are bilinear maps from the group of points on an elliptic curve to the multiplicative group of a finite field, most notably the Weil and Tate pairings. Initial applications included one-round tripartite Diffie-Hellman key exchange, identity-based encryption, and short signatures, and additional constructions followed, such as attribute-based encryption, functional encryption, and partial homomorphic encryption. All cryptographic applications of pairings rely on the ability to construct suitable elliptic curves, to compute in the groups involved, and algorithms for the pairing computation itself. In [ELM04] we introduced the squared Weil and Tate pairings for elliptic and hyperelliptic curves, which achieve cancellation of vertical line function contributions because they only depend on the x-coordinates, which are equal for a point and its negative.

Simultaneous inversion. Several other ideas from Peter's work played a role in optimizing algorithms for pairing computation. In addition to fast modular inversion, Peter also introduced the widely used simultaneous inversion trick, which can be applied to pairing computation as explained in [LMN10]. Inversion-sharing for pairing computation can be advantageous for computing multiple pairings or for computing products of pairings, which is useful for batch verification of signatures, for example. Finite field extension arithmetic is required for pairing computation, since the torsion points involved are often defined over an extension of the base field. In [LMN10], we also proposed to compute inverses in extension fields by using towers of extension fields and successively reducing inverse computation to subfield computations via the norm map. This technique drastically reduces the ratio of the costs of inversions to multiplications in extension fields. This technique tips the scales in favor of affine coordinates when the extension degree is large, which is now increasingly the case in the era of quantum computers. Peter wrote the first version of the elliptic curve pairing library for Microsoft.

Peter worked on the IEEE 1363 Elliptic Curve Standard, and we proposed alternate point compression techniques for elliptic curves and Jacobians of hyperelliptic curves for the 1363a 2004 version of the standard. Peter often carried around to meetings his printed out and marked-up versions of the IEEE 1363 Elliptic Curve Standard and/or his printout of the bignum code.

Peter liked to use Maple to experiment, and he had experimented with searching through many possibilities to find advantageous formulas for 5-, 6-, and 7-term Karatsuba formulas ([Mon05]) which were useful for polynomial multiplication and extension field arithmetic.

Peter was well known for his great sense of humor, practical jokes, and his talent with numbers. With his positive attitude he was an example to visiting students and interns. As a mentor, colleague, and friend he was always liked. We will miss him.

References

[BBB+13] Razvan Barbulescu, Joppe W. Bos, Cyril Bouvier, Thorsten Kleinjung, and Peter L. Montgomery, *Finding ECM-friendly curves through a study of Galois properties*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 63–86, DOI 10.2140/obs.2013.1.63. MR3207408

[Ber06] Daniel J. Bernstein, *Curve25519: new Diffie-Hellman speed records*, Public key cryptography—PKC 2006, Lecture Notes in Comput. Sci., vol. 3958, Springer, Berlin, 2006, pp. 207–228, DOI 10.1007/11745853_14. MR2423191

[BKK+12] Joppe W. Bos, Marcelo E. Kaihara, Thorsten Kleinjung, Arjen K. Lenstra, and Peter L. Montgomery, *Solving a 112-bit prime elliptic curve discrete logarithm problem on game consoles using sloppy reduction*, Int. J. Appl. Cryptogr. **2** (2012), no. 3, 212–228, DOI 10.1504/IJACT.2012.045590. MR2952671

[BL17] Joppe W. Bos and Arjen K. Lenstra (eds.), *Topics in computational number theory inspired by Peter L. Montgomery*, Cambridge University Press, Cambridge, 2017. MR3752679

[BMtR+96] Richard P. Brent, Peter L. Montgomery, Herman J. J. te Riele, Henk Boender, Marije Elkenbracht-huizing, Robert Silverman, and Thomas Sosnowski, *Factorizations of* $a^n \pm 1$, $13 \leq a < 100$*: Update 2*, 1996.

[CJLM06] Mathieu Ciet, Marc Joye, Kristin Lauter, and Peter L. Montgomery, *Trading inversions for multiplications in elliptic curve cryptography*, Des. Codes Cryptogr. **39** (2006), no. 2, 189–206, DOI 10.1007/s10623-005-3299-y. MR2209936

[Cox15] Nicholas Coxon, *Montgomery's method of polynomial selection for the number field sieve*, Linear Algebra Appl. **485** (2015), 72–102, DOI 10.1016/j.laa.2015.07.025. MR3394139

[EGM+73] P. Erdős, R. L. Graham, P. Montgomery, B. L. Rothschild, J. Spencer, and E. G. Straus, *Euclidean Ramsey theorems. I*, J. Combinatorial Theory Ser. A **14** (1973), 341–363, DOI 10.1016/0097-3165(73)90011-3. MR316277

[ELM03] Kirsten Eisenträger, Kristin Lauter, and Peter L. Montgomery, *Fast elliptic curve arithmetic and improved Weil pairing evaluation*, Topics in cryptology—CT-RSA 2003, Lecture Notes in Comput. Sci., vol. 2612, Springer, Berlin, 2003, pp. 343–354, DOI 10.1007/3-540-36563-X_24. MR2080147

[ELM04] Kirsten Eisenträger, Kristin Lauter, and Peter L. Montgomery, *Improved Weil and Tate pairings for elliptic and hyperelliptic curves*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 169–183, DOI 10.1007/978-3-540-24847-7_12. MR2137352

[GM94] Torbjörn Granlund and Peter L. Montgomery, *Division by invariant integers using multiplication*, Proceedings of the ACM SIGPLAN'94 Conference on Programming Language Design and Implementation (PLDI), 1994, pp. 61–72.

[LMN10] Kristin Lauter, Peter L. Montgomery, and Michael Naehrig, *An analysis of affine coordinates for pairing computation*, Pairing-based cryptography—Pairing 2010, Lecture Notes in Comput. Sci., vol. 6487, Springer, Berlin, 2010, pp. 1–20, DOI 10.1007/978-3-642-17455-1_1. MR2781813

[MK08] Peter L. Montgomery and Alexander Kruppa, *Improved stage 2 to p±1 factoring algorithms*, Algorithmic Number Theory, 8th International Symposium, ANTS-VIII, Banff, Canada, May 17–22, 2008, Proceedings, 2008, pp. 180–195.

[Mon05] Peter L. Montgomery, *Five, six, and seven-term karatsuba-like formulae*, IEEE Trans. Comput. **54** (2005), no. 3, 362–369.

[Mon85] Peter L. Montgomery, *Modular multiplication without trial division*, Math. Comp. **44** (1985), no. 170, 519–521, DOI 10.2307/2007970. MR777282

[Mon87] Peter L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), no. 177, 243–264, DOI 10.2307/2007888. MR866113

[Mon92] Peter Lawrence Montgomery, *An FFT extension of the elliptic curve method of factorization*, ProQuest LLC, Ann Arbor, MI, 1992. Thesis (Ph.D.)–University of California, Los Angeles. MR2688742

[Mon94] Peter L. Montgomery, *Square roots of products of algebraic numbers*, Mathematics of Computation 1943–1993: a Half-century of Computational Mathematics (Vancouver, BC, 1993), Proc. Sympos. Appl. Math., vol. 48, Amer. Math. Soc., Providence, RI, 1994, pp. 567–571, DOI 10.1090/psapm/048/1314892. MR1314892

[Mon95] Peter L. Montgomery, *A block Lanczos algorithm for finding dependencies over* GF(2), Advances in cryptology—EUROCRYPT '95 (Saint-Malo, 1995), Lecture Notes in Comput. Sci., vol. 921, Springer, Berlin, 1995, pp. 106–120, DOI 10.1007/3-540-49264-X_9. MR1367513

[MS90] Peter L. Montgomery and Robert D. Silverman, *An FFT extension to the* $P-1$ *factoring algorithm*, Math. Comp. **54** (1990), no. 190, 839–854, DOI 10.2307/2008514. MR1011444

Joppe W. Bos

Kristin E. Lauter

Credits

Figure 1 is courtesy of the Montgomery family (left, middle) and Wikipedia (right).

Figures 2 and 3 are courtesy of Kristin E. Lauter.

Photo of Joppe W. Bos is courtesy of Joppe W. Bos.

Photo of Kristin E. Lauter is courtesy of Michael Svoboda.