J Cryptogr Eng (2018) 8:185–187
https://doi.org/10.1007/s13389-017-0168-3

SPECIAL ISSUE ON MONTGOMERY ARITHMETIC

Special issue in honor of Peter Lawrence Montgomery

Francisco Rodríguez-Henríquez[1] · **Erkay Savaş**[2]

Peter Lawrence Montgomery was born on September 25, 1947. While an undergraduate at the University of California at Berkeley, he became a Putnam fellow in 1967. Montgomery was one of only two contestants able to solve all twelve problems of that year's Putnam examination. In April 1992 he received a Ph.D. from the University of California at Los Angeles. In the biography section of his now famous Karatsuba-like paper [7], one can read what Peter Montgomery concisely wrote about himself,

> He is best known as the inventor of Montgomery multiplication. He has improved integer factorization algorithms.

In fact, Peter Montgomery is well known for a number of very important contributions in a wide range of topics in computational number theory and cryptography. He is credited with inventing the block version of the Lanczos algorithm, which is useful for finding the kernel of a singular matrix over a finite field [6]. This is a crucial step in the index-calculus procedures used for factorizing large integers and for solving the discrete logarithm problem in finite fields or Jacobian groups. Montgomery was also able to speed up Lenstra's ECM factorization algorithm by applying fast Fourier transform (FFT) techniques for the rapid evaluation of polynomials [3–5].

The paper "Speeding the Pollard and elliptic curve methods of factorization" that Peter Montgomery published in 1987 is among his most notable works [2]. In order to speed up Lenstra's ECM factorization algorithm, this paper develops a procedure that can efficiently compute the elliptic curve scalar multiplication operation, $Q = kP$, where $Q, P \in E(\mathbb{F}_p)$, with p a large odd prime. The main idea of the Montgomery procedure, now known as the Montgomery ladder, is that given the x coordinates of the points kP and $(k+1)P$, one can apply *differential* addition and doubling formulas to compute the x coordinates of the points $(2k+1)P$ and $2kP$. Moreover, Montgomery suggested an elliptic curve parametrization, now known as Montgomery curves, which determines a family of curves exceptionally well suited for computing the scalar multiplication operation using the Montgomery ladder procedure. In spite of all those impressive achievements, one can nevertheless see some justification for Montgomery's comment in his aforementioned short autobiography to the effect that he is more widely known for his landmark paper titled "Modular Multiplication Without Trial Division," published in 1985. Excluding the six references in its bibliography, this classic article filled only two pages in the AMS journal "Mathematics of Computation" [1], and yet, as of mid-May 2017, it has over 2650 Google Scholar citations.

Many in the field would agree that very few research works have affected implementations of a broad range of public-key cryptography algorithms used in practice as profoundly as this paper has.

Such algorithms require integer and/or modular arithmetic on large integer operands, and this means that the computational efficiency of public-key cryptography heavily depends on the computational cost of such arithmetic in both hardware and software. In particular, modular multiplication of large numbers, which normally requires an expensive division or reduction operation following an integer multiplication,

✉ Francisco Rodríguez-Henríquez
francisco@cs.cinvestav.mx

Erkay Savaş
erkays@sabanciuniv.edu

[1] CINVESTAV-IPN, Mexico City, Mexico

[2] Sabancı University, Istanbul, Turkey

dominates the time performance of algorithms for popular public-key cryptographic systems such as RSA and ECC.

The Montgomery modular multiplication method eliminates the need for costly division operations by ingeniously replacing them with divisions by a fixed power of two, which is inexpensive or even free of cost in computers and other hardware devices in which the binary number system is the norm. The algorithm, although counterintuitive at first sight, is simple to understand and implement and yet is very efficient, both from a hardware and a software perspective. There are numerous works in the literature that propose different strategies or approaches to finding implementations that are optimized either for speed, or for storage, or for both of these design criteria. Although alternative algorithms for modular multiplication (such as Barrett's method) still survive, there is a consensus that the Montgomery multiplication algorithm is indeed the most advantageous approach in many circumstances.

From a broader perspective, one can define "Montgomery arithmetic" to mean that all arithmetic is performed in the so-called Montgomery domain in which the operands and results are represented in a special way that facilitates the forward transformation of operands and backward transformation of results. Staying in the Montgomery domain as long as possible benefits the entire computation, as the overhead due to the number of transformations is minimized. While this is somewhat straightforward in an RSA implementation, where modular multiplication operations are dominant, in other public-key systems, such as elliptic-curve-based and pairing-based cryptography, a more elaborate layering of arithmetic operations is needed. For instance, the modular inverse can be performed by means of the Montgomery inverse algorithm, which has been shown to be more efficient than the classical binary extended Euclidean algorithm.

In this special issue, we aim to present reasonably easy-to-follow technical explanations of the ingenious ideas behind Montgomery procedures, and to demonstrate best practices in implementing Montgomery algorithms and arithmetic in hardware and software platforms. This issue consists of six contributions written by researchers whose areas of expertise include some of the most relevant aspects of Peter Montgomery's prolific *opus*.

In the first paper, Jean-Claude Bajard, Julien Eynard, and Nabil Merkiche present a comprehensive overview of the use of Montgomery modular reduction in the context of residue number system (RNS) arithmetic. RNS arithmetic has enjoyed an increasing importance in efficient implementation of several public-key cryptosystems, including RSA, elliptic-curve-based, and pairing-based cryptography, and even in emerging schemes, such as quantum-resistant lattice-based cryptography. In all of these applications, the combination of RNS arithmetic with Montgomery reduction becomes crucial for achieving high performance.

In the second paper of this issue, Erkay Savaş and Çetin Kaya Koç outline alternative algorithms for performing the Montgomery inversion operation and give several insightful details on the practical efficiency of each algorithm. This work is especially useful when modular inversion is needed in applications such as elliptic curve cryptography where at least one modular inversion is executed.

In the third paper, Wangchen Dai and Ray C. C. Cheung present a tutorial on spectral arithmetic using Montgomery modular multiplication. Adopting signal processing terminology, while a multiplication operation can be considered an expensive convolution operation in the so-called time domain, in the spectral domain it consists only of simpler component-wise multiplications. From the implementation point of view, this leads to simple modular designs that take advantage of a high level of parallelism in spectral arithmetic. Nevertheless, there remain numerous implementation challenges, such as implementing the fast Fourier transformation (FFT) and the modular reduction operation. Dai and Cheung discuss design issues in detail and provide strategies such as parameter selection criteria to obtain the maximum benefit from the spectral-based Montgomery modular multiplication operation.

In the fourth paper, Craig Costello and Benjamin Smith present a comprehensive tutorial on the Montgomery ladder for large characteristic fields, explaining the main mathematical and algorithmic ideas introduced in his seminal paper [2]. The authors also discuss at length the many ladder variants that have been proposed over the years.

In the fifth paper, Thomaz Oliveira, Julio López, and Francisco Rodríguez-Henríquez present a comprehensive tutorial devoted to the Montgomery ladder operating on elliptic curves defined over binary extension fields. The authors report on a software implementation that achieves speed records for the scalar multiplication operation using ladder procedures in the variable-point scenario.

Finally, in the sixth paper of this issue, Murat Cenk presents a comprehensive survey of the Karatsuba-like formulas and related techniques that provide the most compact formulas for multi-word multiplication computations. The author starts by reviewing Peter Montgomery's seminal ideas on this subject and then presents several important extensions of this line of research, including the use of techniques that crucially rely on the Chinese remainder theorem.

We hope that the collection of articles included in this special issue will give the reader a taste of the influence on high-performance cryptographic implementations that Montgomery's ideas have had during the more than thirty years since the publication of many of his seminal research articles. We also hope that this special issue will be a humble tribute to Peter Montgomery's wonderful research achievements on the occasion of his 70th birthday.

References

1. Montgomery, P.L.: Modular multiplication without trial division. Math. Comput. **44**(170), 519–521 (1985)
2. Montgomery, P.L.: Speeding the Pollard and elliptic curve methods of factorization. Math. Comput. **48**(177), 243–264 (1987)
3. Montgomery, P.L.: Design of an FFT continuation to the ECM method of factorization. AMS Abstr. **10**(4), 278 (1989) Abstract 850-11-25
4. Montgomery, P.L., Silverman, R.D.: An FFT extension to the $P-1$ factoring algorithm. Math. Comput. **54**(190), 839–854 (1990)
5. Montgomery, P.L .: An FFT Extension of the Elliptic Curve Method of Factorization. Ph.D. thesis, University of California at Los Angeles (1992). http://tinyurl.com/ltf6aa4
6. Montgomery, P.L.: A block lanczos algorithm for finding dependencies over GF(2). Adv. Cryptol. EUROCRYPT, LNCS **921**, 106–120 (1995)
7. Montgomery, P.L.: Five, six, and seven-term Karatsuba-like formulae. IEEE Trans. Comput. **54**(3), 362–369 (2005)