Numbers at Work and Play

Igor E. Shparlinski

Background

Number theory targets the most fundamental object of a human's mind: integer numbers. Its questions can be explained to high school students, while getting answers requires very deep and convoluted arguments. Its internal beauty has always been an irresistible attraction for mathematicians, computer scientists, engineers, and enthusiastic amateurs. Furthermore, its primal motivation has always been our natural intellectual curiosity rather than everyday practical needs.

Cryptography is a key technology widely deployed by private, commercial, and governmental users to ensure privacy and authenticity in secure electronic data communication. Its research directions are often driven by practical demands. For example, recently, various issues of privacy and electronic voting entered the world of cryptography. While most of us would agree that these activities are not the most pure and beautiful in our lives, cryptography has its own irresistible attraction and intrinsic motivation for further developments.

The goal of this article is twofold. We hope to convince cryptographers that number theory still has much to offer in terms of concrete results and that they can also extend their toolbox with a variety of little-used, yet powerful, methods. We also hope that number theorists will gain new interest in such an exciting area as cryptography, which guarantees to keep them supplied with new challenges. The dull, politically correct cliché that different cultures are to be explored and enjoyed rather than treated as hostile may actually be correct.

Cryptography is the best-known area of applications of number theory, but it is not the only one. The others include computer science, dynamical systems, physics, and even molecular chemistry. There are also recently emerging applications of number theory to quantum computing and financial mathematics. Nevertheless, here we concentrate only on the interplay between number theory and cryptography and on what they have given and can give to each other.

Igor E. Shparlinski is professor of mathematics at Macquarie University, Australia. His email address is igor@comp.mq.edu.au; http://www.comp.mq.edu.au/~igor/.

Honeymoon

Prior to pioneering works of Whitfield Diffie and Martin Hellman, Ralph Merkle and Martin Hellman, and Ron Rivest, Adi Shamir, and Leonard Adleman, which essentially invented public key cryptography (see [30]), number theory had always been considered as the most conservative and closed part of mathematics with only occasional and short-lasting affairs outside.

We briefly remind readers how the Diffie-Hellman and RSA schemes work.

In the *Diffie–Hellman scheme*, two communicating parties, say C (for a Cryptographer) and $\mathcal{M}$ (for a Mathematician) agree on a cyclic group G, generated by $g \in G$. Then C and $\mathcal{M}$ choose secret numbers x and y and compute g^x and g^y, respectively. The values of g^x and g^y are now made publicly available. It is easy to see that both C and $\mathcal{M}$ can compute

$$(g^y)^x = g^{xy} = (g^x)^y.$$

Note that g^{xy} does not carry any meaningful information. However, it can be used to derive (via a publicly known algorithm) a common key for

some pre-agreed private key cryptosystem, which $\mathcal{C}$ and $\mathcal{M}$ can now use for their communication. It is believed that the problem of finding g^{xy} from given values of g^x and g^y is hard, and solving the corresponding *discrete logarithm problem* is the only feasible line of attack. That is, the attacker simply tries to recover x from the given value of g^x (or does the same for y). We also recall that the order of $\mathcal{G}$ needs to be prime (to prevent the so-called Pohlig-Hellman attack of reducing the problem to prime order subgroups).

In *RSA*, $\mathcal{C}$ chooses two primes p and q and computes $N = pq$; note that the Euler function $\varphi(N) = (p-1)(q-1)$ can easily be evaluated. Then, $\mathcal{C}$ also chooses an *encryption exponent* e with $\gcd(e, \varphi(N)) = 1$ and computes the *decryption exponent* d such that

$$de \equiv 1 \pmod{\varphi(N)}.$$

Now the values of N and e are made public, while d is kept private. To encrypt a message m (represented by an integer in the reduced residue system modulo N), $\mathcal{M}$ simply computes and transmits

$$c \equiv m^e \pmod{N}.$$

The decryption is as easy:

$$c^d \equiv (m^e)^d \equiv m^{de} \equiv m \pmod{N},$$

since by the *Euler Theorem*

$$a^{\varphi(N)} \equiv 1 \pmod{N}$$

for any integer a with $\gcd(a, N) = 1$. It is also believed that, in order to attack this cryptosystem, one must find d, which in turn requires $\varphi(N)$, which is equivalent to finding the factors p and q of N.

As we have just seen, both the Diffie-Hellman key exchange protocol and RSA cryptosystem are based on very simple number-theoretic facts, which date back centuries. But certainly it was not the mathematics behind these constructions that made number theorists so excited. It was the realization that attacking these schemes required very deep insight into some fundamental properties of integers.

The sudden discovery of the great potential of number theory for very practical applications immediately got the attention of many leading researchers in number theory. Such distinguished number theorists as Neal Koblitz, Jeffrey Lagarias, Hendrik Lenstra, Andrew Odlyzko, Carl Pomerance, Hugh Williams, and many others started to actively work in this area and achieved a series of fundamental results and also established new directions.

Midlife Crisis

Unfortunately, over the years the tight links and mutual interest have somewhat diminished. Much of the cryptographic research became occupied with protocol designs. Although this is undeniably highly important and interesting, it is, typically, a not so mathematically rich part of cryptography. Certainly this must not be held against protocol design; using mathematics is not a goal, it is a way to achieve a goal. There is nothing wrong if some areas do not need much of it. Furthermore, there have been many really delightful exceptions, such as zero-knowledge proofs and the identity-based cryptosystem of Boneh and Franklin; short signatures of Boneh, Lynn, and Shacham; and the tripartite key exchange protocol of Joux. See [1] for a detailed description of these schemes.

However, due to increased applied orientation, researchers with more advanced knowledge of engineering and of actual demands of practical cryptography, but lesser fundamental mathematical background, moved into the area. In turn, this led to relying on a somewhat lightweight approach to proofs, led to creating oxymorons such as "*heuristic proof*", and developing a frequently used argument that "if we do not understand some object well enough, it behaves as a uniformly distributed random variable." Unfortunately, one of the effects of this was that mathematicians, both several individual researchers and the whole community, have somewhat distanced themselves from cryptography. The creation of NTRU [18] in the mid-1990s by number theorists Jeffrey Hoffstein and Joseph Silverman and harmonic analyst Jill Pipher was one of the few very welcome exceptions, but it did not change the trend of somewhat abstained position among most of the mathematicians. On the bright side, theoretical computer scientists have moved in, bringing with them new paradigms such as zero-knowledge proofs, secure computation, privacy protection, pseudorandomness, and many other insights which greatly expanded the scope of cryptographic research.

So, by all means, the word "crisis" in the title of this section refers only to the relations between cryptography and mathematics, but not to the progress in each individual area, which has been truly remarkable.

Surprisingly enough, in many cases it was exactly the practical aspect of cryptography which suffered first from that lack of broad mathematical background.

For example, since Neal Koblitz and Victor Miller independently invented elliptic curve cryptography (see [1]), its well-known Achilles heel was the encryption/decryption speed. The idea is based on the fact that the set of rational points on an elliptic curve over a finite field form an Abelian group under an appropriate composition law.

Traditionally, the group of points on an elliptic curve is written additively, so we talk about addition rather than multiplication, doubling rather than squaring, and multiplication by a scalar rather than exponentiation. Furthermore, typically it is easy to choose a curve for which this group contains a large cyclic subgroup of prime order. So many standard constructions such as the Diffie–Hellman key exchange scheme can be implemented over an elliptic curve, too. So far, no efficient general attack has been found on this scheme; however, this security advantage is somewhat offset by higher computational costs. Another potential weakness (which is elliptic-curve-specific) is that typically doubling a point and adding two points on an elliptic curve follow different formulas and thus take different amounts of time. This can be efficiently exploited by the so-called timing or power attacks. There is an extensive literature, where a number of very clever tricks have been suggested to remedy the situation (see [1, Chapter 29]). Unfortunately, being carried away by the race to reduce the number of arithmetic operations in computational formulas (and also balancing them between doubling and additions), the cryptographic community missed the fact that a readily available solution already existed in literature. The insight came from a number theorist. Namely, it was the paper of Edwards [16] that changed the whole game here. Since then, *Edwards curves* have become a hot topic in elliptic curve cryptography. Let us hope that history will not repeat itself and the new spiral of incremental adjustments on the original idea of Edwards curves will not distract from searching for (and finding!) new fundamental improvements.

There are also strong trends within cryptography, motivated by both inner dynamics and practical demands, to make it more rigorous. Overall, this is a very positive development; the idea goes in the right direction. Research in this area has led to such remarkable achievements as the Cramer-Shoup cryptosystem [12]. This and many other papers follow the same standards of rigor as a typical mathematical paper.

However, the quest for provable security occasionally takes too extreme forms. Nowadays, it is very hard for a newly proposed cryptographic scheme to get accepted for publication if the authors do not say something about "provable security". In turn it sometimes leads to hastily composed proofs which have gaps or simply do not address the statement they are supposed to prove. As a result, there have been quite a few completely broken "provably secure" cryptosystems. Recently, similar concerns have been expressed by Koblitz [23], albeit in maybe a too radical form; see also [25] for the follow-up discussion.

Even linguistically, the word "provable" is slightly overemphasized, as all known proofs are nothing but reductions between various problems. No one in complexity theory calls an NP-complete problem "provably hard". Nowadays, we may only dream of such a proof (and probably these dreams will last for a long time…). In any case, the author personally would put much more trust into a protocol which remains unscathed after it has been carefully examined by several well-known "code-breakers" rather than in any "provably secure" scheme.

Living Happily Ever After?

There is no reason not to! Actually there are strong indications that this may really happen. Over the last several years one could see a large group of researchers, of different academic ages, who started their careers in classical or computational number theory and moved toward cryptography. In turn the modern cryptographic community seems to be ready to embrace mathematicians.

Although this is still mostly limited to elliptic curve cryptography, this is a really delightful development. These mathematicians represent different generations and areas of number theory and hopefully will also diversify the area of applications to cryptography.

Furthermore, most mathematicians probably limit the involvement of mathematics in cryptography to only *public key cryptography*. There is, however, much more out there. For example, secret sharing, which we describe below, gives an example of such unjustly lesser-known applications. Quantum cryptography is yet another direction which is rapidly becoming very practical, too.

In fact, the main point of this article is to exhibit great opportunities for both disciplines and give several concrete examples where such joint work may start. Number theory still has a lot to offer, while cryptography provides a constant stream of new beautiful problems and points of view. Both sides just need to take a step toward each other and become more accepting:

$$\text{Number Theory} + \text{Cryptography} - \text{Prejudice} = \text{Love}$$

Although typically number theory plays a service role, simply responding to challenges and requests coming from cryptography, there are also examples when cryptographic techniques have directly led to very interesting number-theoretic results. Below we try to give a brief outline of several recent activities and achievements which have been cross-fertilized by, and belong to, both number theory and cryptography. Our intention has been to give a diverse scope of possible directions for further collaboration, as well as to formulate some specific problems. Unfortunately the space limitations forced us to leave out many exciting topics, such as, for example, constructions of expanders

from isogeny maps on elliptic curves and their applications to constructing hash functions and investigating of the security of discrete logarithm problems on elliptic curves (see [8, 20]).

It is important to remember that number theory is not the only branch of mathematics which is related to cryptography. For instance, recently we have witnessed very exciting developments in the group-theory-based cryptography as well as recently emerged links between cryptography and polynomial algebra.

The author is indebted to Joachim von zur Gathen for the observation that three out of seven Clay Millennium problems—P vs. NP, Birch and Swinnerton-Dyer Conjecture, and Riemann Hypothesis—deal with objects of cryptographic relevance: hard computational problems, elliptic curves, and prime numbers; see http://www.claymath.org/millennium/.

Current Developments and Perspectives

In RSA We Trust!

RSA cryptosystem is based on the *Euler Theorem*, which is one of the most well-known and fundamental number-theoretic facts. However, it has always excited number theorists, not because of the way it works, but because we think that despite (or maybe because of) the simplicity of the underlying mathematics, it is very hard to break. Designing attacks on RSA and evaluating their strength is exactly where most of the interplay between number theory and cryptography has happened.

Certainly the modulus factorization attack is the most general way of breaking RSA. All factorization algorithms, heuristic and rigorous, are based on our knowledge and understanding of the behavior and distribution of smooth numbers and thus have very strong number theory contents (see [13, 30]). We recall that an integer n is called y-smooth if n has no prime divisor $p > y$. Furthermore, the elliptic curve factoring algorithm of Lenstra [24] is based on some deep facts on the distribution of elliptic curves over finite fields and class numbers.

Yet, despite very significant and concentrated efforts, integer factorization remains a very hard computational problem, which is poorly understood theoretically and practically. One of the possible ways to gain more understanding of this problem is to ask how much "help" one should request from an all-powerful oracle in order to be able to factor a given integer N. Two most impressive achievements in this direction are due to Maurer [27] and Coppersmith [10]. Maurer [27] has proved, conditionally on some natural conjecture on the density of very smooth numbers in a short interval, that for any $\varepsilon > 0$ one can request (adaptively) at most $\varepsilon \log n$ bits of information and then factor n in polynomial time. In the approach of Coppersmith [10] more information is requested, but it is limited to specific bits of prime factors of n. For example, if $n = pq$, where $p < q < 2p$ are primes, then about $0.25 \log n / \log 2$ of the most significant bits of p are enough to factor n; see also [28] for an exhaustive survey of follow-up developments. Both approaches contain a number of open problems of rich number-theoretic contents and certainly deserve more attention from number theorists.

Finally, there are also attacks on RSA that are based on an unlucky or careless choice of the modulus. For example, such is the *cyclic attack* on RSA analyzed by Friedlander, Pomerance, and Shparlinski on the basis of the results on the distribution of the Carmichael function of shifted prime numbers; see [33, Chapter 15].

Similarly, the problem of the distribution and frequency of so-called *strong primes* (see [30, Section 4.4.2]), has been resolved in [2]. In both cases, it is shown that the overwhelming majority of the moduli is perfectly safe against both threats. And also in both cases there are several exciting directions for further research and collaboration between number theorists and cryptographers.

Geometry of Numbers and Lattice-Based Cryptography

In 1978 Merkle and Hellman suggested a cryptosystem based on a very elegant idea of using a *superincreasing knapsack*, that is, a sequence of integers $a_1, \dots, a_n$ with $a_i > a_{i-1} + \dots + a_1$, $i = 2, \dots, n$ (see [30, Section 8.6]). Although in general the Knapsack Problem is NP-complete, a superincreasing knapsack is easy: Given the sum

$$A = \sum_{i=1}^{n} a_i x_i,$$

with a binary vector $(x_1, \dots, x_n) \in \{0,1\}^n$, one can recover $x_n, \dots, x_1$ consecutively by using a simple "greedy" algorithm. One, however, may try to hide the superincreasing structure by choosing a prime $p > a_n$, a random $\lambda \not\equiv 0 \pmod p$, an element π of the symmetric group S_n, and then publishing a permutation

$$c_1 = b_{\pi(1)}, \dots, c_n = b_{\pi(n)}$$

of the residues

$$b_i \equiv \lambda a_i \pmod p, \qquad i = 1, \dots, n.$$

Then a binary vector $(y_1, \dots, y_n) \in \{0,1\}^n$ is encrypted by

$$C = \sum_{i=1}^{n} c_i y_i,$$

which can be decrypted by anyone who knows p, λ, and the permutation π by computing $A \equiv \lambda^{-1} C \pmod p$, recovering $(x_1, \dots, x_n)$ for the corresponding superincreasing knapsack, and then computing $y_i = x_{\pi^{-1}(i)}$, $i = 1, \dots, n$. This idea is

very attractive and encryption/decryption are both very fast. However, unfortunately, this scheme and its various extensions have all been broken by an appropriate application of the famous LLL algorithm of Lenstra, Lenstra, and Lovász; see [32]. This series of unsuccessful attempts to build a reliable cryptosystem based on hard lattice problems was quite frustrating, and for quite some time this direction was put on the back burner.

The first theoretical breakthrough, which reignited interest in lattice-based cryptosystems, happened in 1997 when Ajtai and Dwork and Goldreich, Goldwasser, and Halevi reinstated this direction. Although these cryptosystems and their variations are either impractical or under attack (or both) (see [31, 32]), they proved the vitality of the idea of using hard problems of the geometry of numbers for cryptographic purposes. Furthermore, at around the same time, the highly practical NTRU was invented by Hoffstein, Pipher, and Silverman [18]. A decade of attacks on NTRU has led to a series of modifications and adjustments of the original scheme, but it seems that it has survived the storm and provides a very secure and efficient cryptosystem.

Nowadays there is a strong and active group of cryptographers who are combining practical aspects of lattice-based cryptography with a deep and original mathematical insight; see the surveys [28, 31, 32].

There are, however, many unexplored directions. For example, is it possible to salvage the original Merkle-Hellman idea by mixing a superincreasing knapsack with some other types of easily recoverable knapsacks? It is known that iterating the modular multiplication hiding trick does not help here, but what about a more general affine transformation

$$b_i \equiv \lambda a_i + \mu \pmod{p}, \qquad i = 1, \dots, n,$$

and then insisting that the encoded message is always of the same weight $w \sim n/2$ (so the total additive shift is $w\mu$)?

There are many other possibilities to investigate and certainly an unlimited field of action for number theory.

Anatomy of Integers and Cryptographic Attacks[1]

As we have mentioned, our insight on the behavior of prime divisors of a "typical" integer underlies all modern integer factorization algorithms. There are, however, several more important, albeit not so well-known, cryptographic constructions which rely on some delicate properties of prime and integer divisors of integers.

[1] *The author admits that the title of this section is greatly influenced by [14].*

However, these algorithms are not the only applications of number-theoretic results on the fine structure of integers. Here we recall a few more cryptographic constructions and algorithms with a rich and nontrivial number theoretic content. In particular, many cryptographic attacks target "atypical" integers, and it is important to know how rare they are.

The traditional Discrete Logarithm Problem (DLP) is the problem of finding x from a given value of g^x where g is a generator of a cyclic group G. There are, however, several cryptographic protocols which rely on the presumed hardness of finding x from given values of $g^x, \dots, g^{x^n}$ (or, sometimes, just of two values g^x and g^{x^n}). Intuitively it may seem that this extra information cannot help much and the problem is not easier than the original DLP (corresponding to $n = 1$).

Quite surprisingly, this intuition has turned out to be wrong. In particular, Cheon [9] has shown that, ignoring some logarithmic factors:

- given g^x and g^{x^d} for some $d \mid p-1$, one can find x in time about $\mathcal{O}\left(\sqrt{p/d} + \sqrt{d}\right)$ (which is $\mathcal{O}\left(p^{1/4}\right)$ for $d \sim \sqrt{p}$);
- given $g^x, \dots, g^{x^d}$ for some $d \mid p+1$, one can find x in time about $\mathcal{O}\left(\sqrt{p/d} + d\right)$ (which is $\mathcal{O}\left(p^{1/3}\right)$ for $d \sim p^{1/3}$).

This gives rise to the question of estimating the probability with which a random prime p is such that $p \pm 1$ has a divisor d of a given size.

Fortunately, readily available results and methods, such as the classical Brun sieve as well as some more recent results, give almost perfect answers to this and related questions and imply that the above attacks apply to a rather dense set of primes. We refer to [9] for more details.

In [29], Menezes introduces the *Large Subgroup Attack* on some cryptographic protocols over a prime field $\mathbb{F}_p$. The attack can be applied, if for some $q \mid p-1$, the ratio $n = (p-1)/(2q)$ has a smooth divisor $s > q$. Banks and Shparlinski [3] have used their asymptotic formula on the probability $\eta(k, \ell, m)$ that a k-bit integer n has a divisor $s > 2^m$ which is 2^ℓ-smooth to give some insight on the frequency with which this attack succeeds on "random" primes, assuming that shifted primes $p-1$ behave like "random" integers.

One of the most interesting choices of parameters is:

$$k = 863, \qquad m = 160, \qquad \ell = 80$$

(which produces a 1024-bit prime p), in which case it has been shown in [3] that (heuristically) the attack succeeds with probability $\eta(863, 80, 160) \approx 0.09576 > 9.5\%$.

Pell Equations and Pairing-Based Cryptography

Elliptic curve cryptography is yet another confirmation of the great practicality of deep mathematical theories. Recently, the area enjoyed a second wave of activity in which elliptic curves are not merely used as just an example of a finite group but in a much more subtle way, which has no analogue in other groups such as $\mathbb{F}_q^*$. Namely, following the pioneering works of Boneh and Franklin, Boneh, Lynn and Shacham, Joux, Joux and Nguyen, Menezes, Okamoto and Vanstone, a diverse scope of cryptographic applications of the Tate, Weil, and other pairings on elliptic curves has been discovered (see [1, Chapters 22 and 24] for an exhaustive survey).

A background on elliptic curves can be found in [1, 36]; however, for our purposes it is quite enough just to recall that an elliptic curve in the affine model is essentially the set of solutions (x, y) in the algebraic closure of a finite field $\mathbb{F}_q$ of q elements to the Weierstrass equation

$$Y^2 = X^3 + aX + b$$

, where the coefficients $a, b \in \mathbb{F}_q$ avoid a certain surface in $\mathbb{F}_q^2$ (and also $\gcd(q, 6) = 1$; otherwise, the Weierstrass equation takes a slightly more complicated form).

In modern applications of elliptic curves in cryptography, the notion of *embedding degree* plays one of the central roles. Recall that an elliptic curve $\mathbf{E}$ over the finite field $\mathbb{F}_q$ of q elements has embedding degree k with respect to the subgroup $\mathcal{G}$ of the group $\mathbf{E}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on $\mathbf{E}$, if $\#\mathcal{G} \mid q^k - 1$, and k is the smallest positive integer with this property. Typically, only subgroups $\mathcal{G}$ of prime order ℓ of $\mathbf{E}(\mathbb{F}_q)$ are of interest.

The above applications have naturally led to two mutually complementary directions:

- Estimating the probability that a "random" elliptic curve (in some natural sense) has a small embedding degree with respect to a subgroup $\mathcal{G}$ of $\mathbf{E}(\mathbb{F}_q)$ of large prime order ℓ.
- Finding explicit constructions of elliptic curves $\mathbf{E}$ having a small embedding degree with respect to some subgroup $\mathcal{G}$ of $\mathbf{E}(\mathbb{F}_q)$ of large prime order ℓ.

There are results of various flavors which show that a "random" curve (for different types of randomization) tends to have a large embedding degree with respect to large prime order subgroups of $\mathbf{E}(\mathbb{F}_q)$ (see [21, 26]). In particular, this means that the so-called *MOV attack* of Menezes, Okamoto and Vanstone (see [1, Section 22.2]) is not likely to succeed on a "random" curve. On the other hand, this also means that "random" curves are useless for the purposes of pairing-based cryptography, thus making the second problem even more important.

Both directions still have many open questions with a strong number theory context, even if in many cases only conditional results, under the Generalized Riemann Hypothesis and/or the Bateman-Horn Conjecture on primes in polynomial values. For example, in [26], an approach is given to getting a heuristic upper bound on the number of the pairing-friendly MNT curves, named after Miyaji, Nakabayashi and Takano; see [1, Section 24.2.3.a], (who surprisingly enough, invented this very elegant construction even before applications of pairing-friendly curves had been found). However, to get precise results one needs to estimate the order of magnitude (as the function of the parameter $z > 1$) of the series

$$S(z) = \sum_{\substack{s \le z \\ s \text{ squarefree}}} \sum_{\substack{n^2+8=3sm^2 \\ n \equiv 1 \pmod 6 \\ n \ge 2}} \frac{1}{(\log n)^2},$$

where the inner sum is taken over positive solutions $n \equiv 1 \pmod 6$, $n \ge 2$ to the *Pell* equation $n^2 + 8 = 3sm^2$ (see [19] for a background on the Pell equation). It is believed that, typically such solutions grow exponentially and the jth solution is of order of magnitude $\exp(c\sqrt{s}j)$ for some absolute constant $c > 0$ (in particular, the first solution is exponential in $\sqrt{s}$). This may lead to a suggestion that $S(z) = z^{o(1)}$. However, Karabina and Teske [22] noticed that there is a thin set of exceptional values of $s = 12k^2 + 4k + 3$, satisfying $3s = (6k + 1)^2 + 8$, for which there is a very small solution of order $\sqrt{s}$. This implies that

$$S(z) \ge C \frac{\sqrt{z}}{(\log z)^2}$$

for some absolute constant $C > 0$. In [21] this bound has been slightly improved, but the question about the precise behavior of $S(z)$ is still wide open and is of great interest for both number theory (because of the new methods it is likely to require to develop) and cryptography (because of the application to such a "hot" topic as pairing-based cryptography). Let us reiterate that so far even heuristically the situation is poorly understood.

Similar questions can be asked for other constructions (see [17] for a survey), giving unlimited opportunities for collaboration between both communities.

Secret Sharing and Algebraic Number Theory

Since Shamir introduced the first secret sharing scheme (SSS) (see [30, Section 12.7.2]), this area has enjoyed a tremendous amount of attention and work. We recall that, in the simplest settings, a "t-out-of-n" SSS is a way of distributing some information, derived from a secret key X, between n participants so that any $t + 1$ of them can recover X, but no coalition of t participants can gain any knowledge about X. The initial scheme of Shamir already used a very elegant idea of

polynomial interpolation over finite fields. Later, much deeper tools of polynomial algebra and algebraic number theory were applied to improve the existing schemes. These schemes also cover many more access scenarios of threshold secret sharing over an arbitrary abelian group when given only blackbox access to the group operations and to blackbox randomness (while the original scheme of Shamir is essentially limited to secret sharing over finite fields). In turn this generality required use of much deeper number-theoretic tools. For example, Desmedt and Frankel [15] constructed a scheme based on cyclotomic fields and discussed the relations between their construction and the *Lenstra constant*. We recall for an algebraic number field $\mathbb{K}$ the Lenstra constant $L(\mathbb{K})$, introduced as a tool to study Euclidean number fields, is defined as the largest number m of algebraic integers $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}_{\mathbb{K}}$ such that the differences $\alpha_i - \alpha_j$, $1 \le i < j \le m$, belong to the unit group of $\mathbb{K}$. Unfortunately, $L(\mathbb{K})$ tends to be rather small.

In fact, the construction of [11], which builds upon some previous ideas of Cramer and Fehr, is still based on using algebraic numbers, but its effectiveness is not limited by the size of the Lenstra constant.

We also note that algebraic geometry, in particular constructions of curves with many rational points over finite fields, has also been used for the same purpose [7]. There is very little doubt that experts in algebraic number theory may find (and solve!) a wealth of challenging problems in this area and thus greatly contribute to its further development.

Exponential Sums and Pseudorandomness

Exponential sums, and more generally character sums, form a well-developed number-theoretic tool to show that certain objects behave similarly to uniformly distributed random variables. So there is no surprise they can be of invaluable help for analyzing cryptographic primitives; see [33] for some examples.

For example, let $g \in \mathbb{F}_q^*$ be an element of order t. The Diffie–Hellman problem (that is, recovering g^{xy} from g^x and g^y) is nowadays usually called the *Computational Diffie–Hellman Problem*, CDH. One can also consider a variant of this problem that is known as the *Decisional Diffie–Hellman Problem*, DDH, which is about distinguishing a stream of Diffie–Hellman triples (g^x, g^y, g^{xy}) from a stream of triples (g^x, g^y, g^z) where x, y, z are chosen uniformly at random from the interval $[0, t-1]$. The complexity status and interrelations between the CDH and DDH are mostly unknown, but both are presumed to be hard. One, however, may try to get some indirect evidence in support of their hardness. Motivated by this point of view, the uniformity of distribution of (g^x, g^y, g^{xy}) has been established by Canetti, Friedlander and Shparlinski and then improved by Canetti, Friedlander, Konyagin, Larsen, Lieman and Shparlinski (see [33, Chapter 3]). Finally, Bourgain [5], using very powerful methods of additive combinatorics, has greatly extended the range of t for which such a result holds. Yet one can still find here many open questions and unexplored directions.

There are also more direct applications of exponential sums. For instance, Boneh and Venkatesan [4] introduced the following problem, known as the *Hidden Number Problem*, HNP:

> *For a prime p, recover $\alpha \in \mathbb{F}_p$, given the ℓ most significant bits of $\alpha t_i \pmod p$ for k elements $t_1, \ldots, t_k \in \mathbb{F}_p$, chosen independently and uniformly at random.*

Certainly when ℓ is large (say, larger than the bit length of p), the problem is trivial. Boneh and Venkatesan [4] have given a probabilistic polynomial time algorithm which works for much smaller values of ℓ, namely $\ell \approx \sqrt{\log p}$. They have also shown that the HNP has close links with the bit security property of the Diffie-Hellman key. The latter means that recovering even a small portion of the bits of g^{xy} is as hard as recovering the whole key. This property is crucial to guarantee that when only some bits of g^{xy} are used to establish a common key for a private key cryptosystem, this does not introduce any additional weakness in the protocol. Recall that the bit length of such keys (80-120 bits) is significantly shorter than the bit length of the Diffie-Hellman key (500-1,000 bits). One of the facts used in the proof was the observation that if $t \in \mathbb{F}_p$ is chosen uniformly at random, then the probability that $\alpha t \pmod p$ belongs to a prescribed interval of length h inside of $[0, p-1]$ is about h/p.

However, it has turned out that for the above application the multiplier t is chosen from a multiplicative subgroup of $\mathbb{F}_p$, and thus the above uniformity of distribution property had to be re-established, and this is exactly where exponential sums came into the picture (see [34]).

The HNP algorithm of Boneh and Venkatesan [4], reinforced with bounds of exponential sums, has also been used for a very "destructive" purpose, namely to attack the Digital Signature Scheme (see [33, Chapter 20]). The exponential sums which appear here are of a type which does not appear in any "pure" number theory applications, and their estimating required a combination of various techniques.

Even more surprisingly, the modification suggested in [35] to the HNP algorithm of [4] has tight links with the Waring problem in finite fields and allows the study of very general sequences of

multipliers; see [34] for a survey of algorithms for several other variants of the HNP.

Finally, just to give a brief taste of the diversity of application of exponential sums to cryptography, we also mention:

- The construction of Bourgain [6] of so-called randomness extractors, a very important object in theoretic cryptography and computer science. Obtaining explicit forms of the estimates of [6] is a natural, interesting, but not easy, question.
- Results of Jao, Miller and Venkatesan [20] on the reducibility between the discrete logarithm problem on different elliptic curves with the help of bounds of character sums (implied by the Generalized Riemann Hypothesis). A natural direction of research would be to apply the large sieve technique in order to establish a similar result for almost all primes (instead of all primes as in [20]) but unconditionally.

Conclusion

By no means is this paper intended to be a survey of all links, both existing and potential, between cryptography and number theory. Many important topics and directions are left out. We still hope it says enough to exhibit the richness and potential of the two interacting galaxies of cryptography and number theory. In particular, we have tried to show to mathematicians there is much more in cryptography than RSA and other classical schemes of public key cryptography, where they can apply their knowledge and experience. On the other hand, the intent was to show to cryptographers that there is much more in mathematics than congruences and prime numbers, which can be of great value for cryptography

The author does hope that the title of this section refers only to the paper, and not to the story. In fact, we have strong reasons to expect that we are just at the beginning of a new chapter with many more exciting twists and an elaborate plot. We anticipate this will bring a lot of success and enjoyment to all its participants and interested viewers.

Acknowledgments

The author is very grateful to many cryptographers and mathematicians for providing various specific and general comments on the preliminary draft and also for supplying additional references. Unfortunately, not all of them could be included due to size limitations; on the other hand, some passages in the text are almost direct quotations of their comments. This especially applies to Jung Hee Cheon, Ronald Cramer, Joachim von zur Gathen, Jorge Jimenez Urroz, Carl Pomerance, Joseph Silverman, and Edlyn Teske.

Very special thanks go to Steven Galbraith who, besides making many critical remarks and useful suggestions, also helped with language editing.

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren, *Elliptic and Hyperelliptic Curve Cryptography: Theory and Practice*, CRC Press, 2005.

[2] W. Banks, J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, Multiplicative structure of values of the Euler function, *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Fields Institute Communications, vol. 41, Amer. Math. Soc., 2004, 29–48.

[3] W. D. Banks and I. E. Shparlinski, Integers with a large smooth divisor, *Integers* **7** (2007), # A17, 1–11.

[4] D. Boneh and R. Venkatesan, Hardness of computing the most significant bits of secret keys in Diffie–Hellman and related schemes, *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1109** (1996), 129–142.

[5] J. Bourgain, Estimates on exponential sums related to Diffie–Hellman distributions, *Geom. and Func. Anal.* **15** (2005), 1–34.

[6] J. Bourgain, On the construction of affine extractors, *Geom. and Func. Anal.* **17** (2007), 33–57.

[7] I. Cascudo, H. Chen, R. Cramer, and C. Xing, Asymptotically good ideal linear secret sharing schemes with strong multiplication over any fixed finite field, *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin (to appear).

[8] D. X. Charles, E. Z. Goren, and K. E. Lauter, Cryptographic hash functions from expander graphs, *J. Cryptology* (to appear).

[9] J. Cheon, Discrete logarithm problems with auxiliary inputs, *J. Cryptology* (to appear).

[10] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, *J. Cryptology* **10** (1997), 233–260.

[11] R. Cramer, S. Fehr, and M. Stam, Primitive sets over number fields and absolutely optimal black-box secret sharing, *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **3621** (2005), 344–360.

[12] R. Cramer and V. Shoup, Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack, *SIAM J. Comp.* **33** (2003), 167–226.

[13] R. Crandall and C. Pomerance, *Prime numbers: A Computational Perspective*, Springer-Verlag, New York, 2005.

[14] J.-M. De Koninck, A. Granville, and F. Luca (eds.), *Anatomy of integers*, CRM Proc. and Lect. Notes, vol. 46, Amer. Math. Soc., Providence, RI, 2008.

[15] Y. Desmedt and Y. Frankel, Homomorphic zero-knowledge threshold schemes over any finite Abelian group, *SIAM J. Discr. Mathem.* **7** (1994), 667–679.

[16] H. M. Edwards, A normal form for elliptic curves, *Bull. Amer. Math. Soc.* **44** (2007), 393–422.

[17] D. Freeman, M. Scott, and E. Teske, A taxonomy of pairing-friendly elliptic curves, *J. Cryptology* (to appear).

[18] J. HOFFSTEIN, J. PIPHER, and J. H. SILVERMAN, NTRU: A ring based public key cryptosystem, *Lect. Notes in Comp. Sci.*, vol. 1433, Springer-Verlag, Berlin, 1998, 267–288.

[19] M. J. JACOBSON and H. C. WILLIAMS, *Solving the Pell Equation*, Springer-Verlag, Berlin, 2009.

[20] D. JAO, S. D. MILLER, and R. VENKATESAN, Expander graphs based on GRH with an application to elliptic curve cryptography, *J. Number Theory* **129** (2009), 1491–1504.

[21] J. JIMÉNEZ URROZ, F. LUCA, and I. E. SHPARLINSKI, On the number of isogeny classes of pairing-friendly elliptic curves and statistics of MNT curves, *Preprint*, 2008

[22] K. KARABINA and E. TESKE, On prime-order elliptic curves with embedding degrees $k = 3, 4$ and 6, *Lect. Notes in Comp. Sci.*, vol. 5011, Springer-Verlag, Berlin, 2008, 102–117.

[23] N. KOBLITZ, The uneasy relationship between mathematics and cryptography, *Notices of the Amer. Math. Soc.* **54** (2007), 972–979.

[24] H. W. LENSTRA, Factoring integers with elliptic curves, *Ann. Math.* **126** (1987), 649–673.

[25] Letters to the Editor, *Notices of the Amer. Math. Soc.* **54** (2007), 1454–1456.

[26] F. LUCA and I. E. SHPARLINSKI, Elliptic curves with low embedding degree, *J. Cryptology* **19** (2006), 553–562.

[27] U. M. MAURER, On the oracle complexity of factoring integers, *Computational Complexity* **5** (1996), 237–247.

[28] A. MAY, Using LLL-reduction for solving RSA and factorization problems, *Proc. Conf. in Honour of the 25th Birthday of the LLL algorithm, LLL+25* Caen, France, 2007 (to appear).

[29] A. J. MENEZES, Another look at HMQV, *J. Math. Cryptology* **1** (2007), 47–64

[30] A. J. MENEZES, P. C. VAN OORSCHOT, and S. A. VANSTONE, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1996.

[31] D. MICCIANCIO and O. REGEV, Lattice-based cryptography, *Post-Quantum Cryptography*, Springer-Verlag, 2009, 147–191.

[32] P. Q. NGUYEN, Public-key cryptanalysis, *Recent Trends in Cryptography*, Contemp. Math., vol. 477, Amer. Math. Soc., 2009 (to appear).

[33] I. E. SHPARLINSKI, *Cryptographic Applications of Analytic Number Theory*, Birkhäuser, 2003.

[34] I. E. SHPARLINSKI, Playing "Hide-and-Seek" with numbers: The hidden number problem, lattices and exponential sums, *Proc. Symp. in Appl. Math.*, Amer. Math. Soc., Providence, RI, **62** (2005), 153–177.

[35] I. E. SHPARLINSKI and A. WINTERHOF, A hidden number problem in small subgroups, *Math. Comp.* **74** (2005), 2073–2080.

[36] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Springer-Verlag, Berlin, 1995.