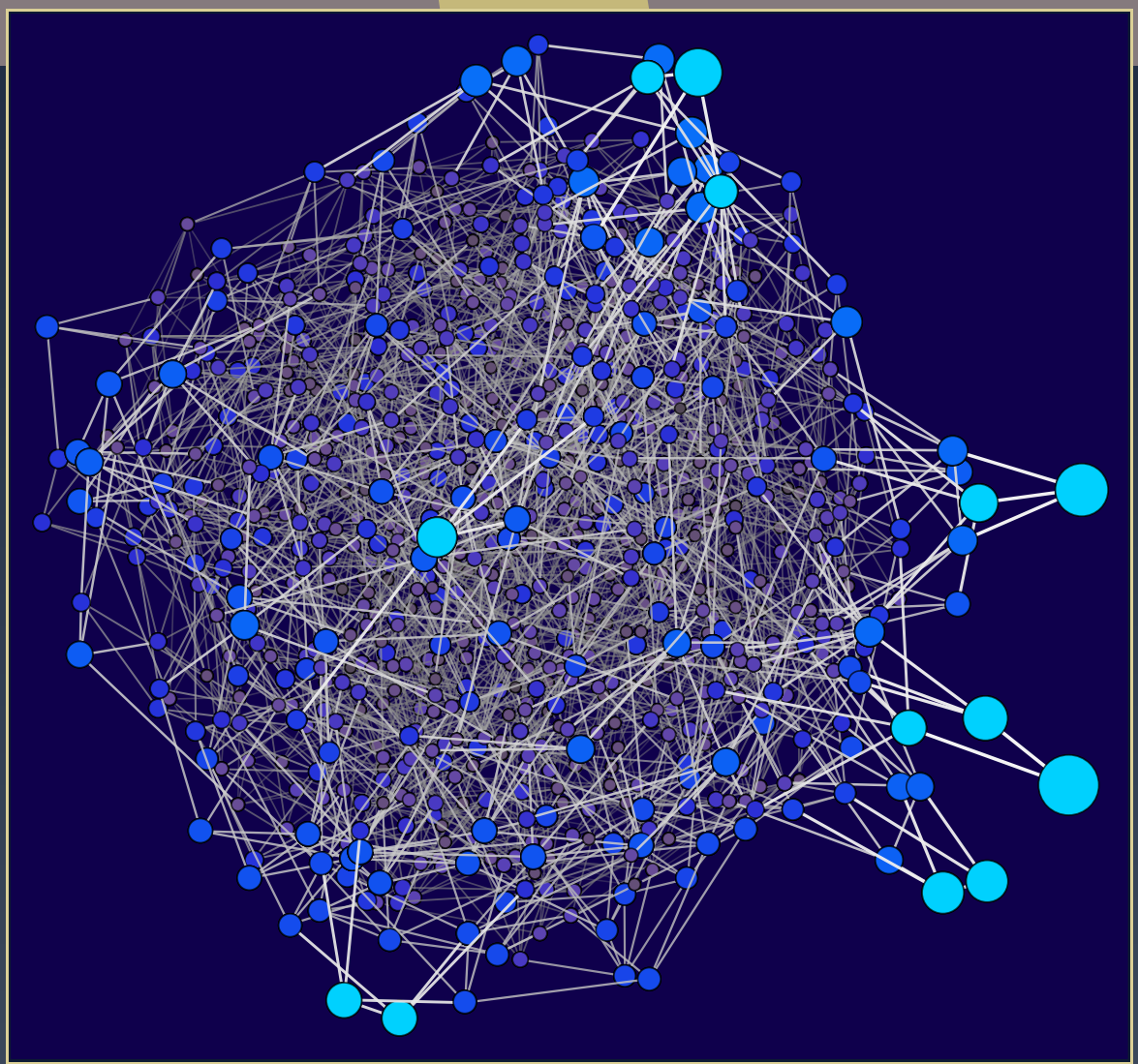
THE OPEN BOOK SERIES 4

ANTS XIV
Proceedings of the Fourteenth Algorithmic Number Theory Symposium

Commitment schemes and diophantine equations

José Felipe Voloch



msp

THE OPEN BOOK SERIES **4** (2020)
Fourteenth Algorithmic Number Theory Symposium
https://doi.org/10.2140/obs.2020.4.1

Commitment schemes and diophantine equations

José Felipe Voloch

Motivated by questions in cryptography, we look for diophantine equations that are hard to solve but for which determining the number of solutions is easy.

1. Commitment schemes

Solving a diophantine equation is typically hard but, given a point, it is typically easy to find a variety containing that point. This is an example of a "one-way function" with potential applications to cryptography. Our current (lack of) knowledge suggests that such a function is possibly quantum resistant and, therefore, cryptosystems based on these could be used for postquantum cryptography [BL17].

An encryption system based on this principle was proposed by Akiyama and Goto [AG06; AG08], then broken by Ivanov and the author [IV09]. It was then fixed, broken again, fixed again... Current status unclear.

The purpose of a commitment scheme is for a user to commit to a message without revealing it (e.g., vote, auction bid) by making public a value obtained from the message in such a way that one can check, after the message is revealed, that the public value confirms the message.

Using such diophantine one-way functions for commitment schemes was proposed by Boneh and Corrigan-Gibbs [BCG14]. They also suggested working modulo an RSA modulus N. This could conceivably weaken the system. It will definitely no longer be quantum resistant. Some partial attacks on this particular system are presented in [ZW17].

Here is the general format of a diophantine commitment scheme. Encode a message as point P over some field F. Make public a variety V/F with $P \in V$, with V taken from some fixed family of varieties. To check the commitment, one verifies that P satisfies the equations of V. We need the following conditions to be satisfied for this to work:

- Given P, it is easy to construct V.
- Given V, it is hard to find $V(F)$ (hence P).
- Given V (and perhaps P), it is easy to verify that $\#V(F) = 1$.

MSC2020: 11D45, 94A60.
Keywords: commitment schemes, diophantine equations, algebraic varieties.

The last condition is important to prevent cheating. It proves that P was indeed the committed message. In general, a commitment scheme consists of two algorithms $\mathsf{Commit(m,r)}$, $\mathsf{Reveal(m,r,c)}$. The first takes as input a message m and a random string r to produce an output c, which is then made public. The second takes as input $\mathsf{m,r,c}$ as before and outputs yes or no, depending on whether c is the correct output of $\mathsf{Commit(m,r)}$. The randomness is needed, e.g., if the list of possible messages is small enough that it can be brute force searched. Note that our requirement that $\#V(F) = 1$ corresponds to the notion of perfect binding for a commitment scheme. There is a weaker notion of computational binding in which the condition is relaxed to only hold with probability close to one. See [BCG14, Section 4.1] for the precise definition of a commitment scheme and some discussion.

These commitment schemes are similar in spirit to the class of multivariate polynomial cryptosystems. In analogy to what is done there, it is conceivable to have encryption by selecting a subset of varieties V/F such that $V(F)$ can be easily found but that V can be disguised as a general member of the collection of varieties. We do not address the interesting problem of doing this for schemes we consider.

2. Diophantine equations

Answering a question of Friedman, Poonen [Poo10] proved:

Theorem 2.1. *Assuming the Bombieri–Lang conjecture, there exists* $f(x, y) \in \mathbb{Q}[x, y]$ *inducing an injection* $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$.

Boneh and Corrigan-Gibbs [BCG14] then use the following construction from such a function. For $P = (a, b)$, take $V : f(x, y) = f(a, b)$ to get a commitment scheme fitting the general setting of Section 1. Unfortunately, Poonen's proof, besides being conditional on a conjecture, is also nonconstructive!

Zagier suggested $f(x, y) = x^7 + 3y^7$ as a polynomial defining an injective function. But we don't have a proof. With exponent 13 instead of 7, the abcd conjecture implies that this function essentially injective.

Question 2.2. Is solving $x^7 + 3y^7 = k$ over $\mathbb{Q}$ hard?

Pasten [Pas20] proved that there exists an affine surface S of the form $U \times U$ with $S(\mathbb{Q})$ Zariski-dense in S and a morphism $S \to \mathbb{A}^1$ inducing an injection $S(\mathbb{Q}) \to \mathbb{Q}$. But, $S(\mathbb{Q})$ is too sparse to be cryptographically useful.

Cornelissen [Cor99], using that the abcd conjecture is true for function fields of characteristic 0, noted that $x^m + ty^m$ is injective in $K(t)$, $\operatorname{char} K = 0$ for m large.

Question 2.3. Is solving $x^m + ty^m = k$ over $\mathbb{Q}(t)$ hard?

My guess is that the answer is no.

Cornelissen also noted that $x^p + ty^p$ is injective in $K(t)$, $\operatorname{char} K = p$. But solving $x^p + ty^p = k$ is easy.

The following was noted in [SV20], with the proof being an extension of [Vol85] (see also [Wan] for a related result without a hypothesis on the degree of the morphism):

Theorem 2.4. *Let F be a function field of a curve C of genus g with field of constants K of characteristic $p > 0$ and let S be a finite set of places of F. If $u_1, \dots, u_t$ are S-units of F, linearly independent over K, such that the degree of the morphism $(u_1 : \cdots : u_t) : C \to \mathbb{P}^{t-1}$ is less than p and satisfy*

$$u_1 + \cdots + u_t = 1$$

then

$$\max\{\deg u_i \mid i = 1, \dots, t\} \le \frac{t(t-1)}{2}(2g - 2 + \#S)$$

The above result implies the injectivity of $x^{13} + ty^{13}$ in the set of pairs of elements of $K(t) - K$ of degree at most $p/13$ if $13 \nmid p(p-1)$.

This is enough for the application to commitment schemes by taking a sufficiently large finite field K and considering the function $x^{13} + ty^{13}$ restricted to the above set where the function is injective.

But the function is not injective in the whole of $K(t)$. Indeed, if $x^{13} + ty^{13} = k$, $q = p^{12}$, then

$$(x^q / k^{(q-1)/13})^{13} + t(t^{(q-1)/13} y^q / k^{(q-1)/13})^{13} = k$$

3. Curves on surfaces

The cryptosystem of Akiyama and Goto [AG06; AG08] actually uses curves on surfaces over finite fields. We now consider the use of rational curves on surfaces in $\mathbb{P}^3$ over a finite field for commitment schemes.

We start with a rational curve P parametrized by $(f_0 : f_1 : f_2 : f_3)$ in $\mathbb{P}^3$ over a finite field $\mathbb{F}_q$, where the f_i are polynomials of degree at most m (i.e., a point in $\mathbb{P}^3$ over $\mathbb{F}_q(t)$). Such a curve will include the message and randomness and our commitment will be a smooth surface $S/\mathbb{F}_q$ of degree d containing P. This is a bit different from previous schemes as the surface is constant (i.e., independent of t). If S is given by an homogeneous equation $F = 0$, the condition that $P \subset S$ is simply $F(f_0, f_1, f_2, f_3) = 0$ which can be viewed as a system of linear equations on the coefficients of F, once the f_i are given. There are $\binom{d+3}{3}$ coefficients and $dm + 1$ equations. One has solutions to the system as soon as there are more coefficients than equations but these are not guaranteed to be smooth. Poonen [Poo08] has proved that, for d large, a positive proportion of those solutions do indeed give smooth surfaces. One expects in practice that, as long as the finite field is big enough, there will be plenty of smooth surfaces.

To guarantee uniqueness of the curve P inside S, we prove the following result.

Theorem 3.1. *Let $S/\mathbb{F}_q$ be a smooth surface in $\mathbb{P}^3$ of degree $d > 3$ with Picard number two. Then S contains at most one smooth rational curve of degree m, if $m < 2d(d-4)/(d-2)$.*

Proof. Let H be a hyperplane section and D_1, D_2 two distinct smooth rational curves of degree m contained in S. We compute the determinant of the matrix of intersection pairings for H, D_1, D_2 and show it is nonzero, hence these curves are independent in the Néron–Severi group, contradicting the hypothesis on the Picard number.

Clearly, $H^2 = d$, $HD_i = m$, $i = 1, 2$. The canonical class of S is $(d-4)H$, so the adjunction formula gives $D_i^2 + (d-4)HD_i = -2$, hence $D_i^2 = -(2 + (d-4)m)$. Let $\delta = D_1 D_2$. The determinant of the

matrix of intersection pairings is therefore

$$\begin{vmatrix} H^2 & HD_1 & HD_2 \\ D_1H & D_1^2 & D_1D_2 \\ D_2H & D_2D_1 & D_2^2 \end{vmatrix} = \begin{vmatrix} d & m & m \\ m & -(2+(d-4)m) & \delta \\ m & \delta & -(2+(d-4)m) \end{vmatrix}$$
$$= -d\delta^2 + 2m^2\delta + d(2+(d-4)m)^2 + m^2(2+(d-4)m).$$

This vanishes precisely when $\delta = -(2+(d-4)m), 2m^2/d + (2+(d-4)m)$. The first value is negative so cannot be D_1D_2 and the second value is bigger than m^2 by our hypothesis but $D_1D_2 \leq m^2$ by Bézout's theorem so cannot be D_1D_2 either. □

To apply the theorem, we need to know that the Picard number of S is at most two. For a given surface, this can be done using the algorithm of [Cos15], for example. This algorithm computes the L-function of S and the Picard number of S is the multiplicity of q as a root of the L-function, conditional on the Tate conjecture. However, the surfaces we construct will have Picard number at least two and a theorem of Tate shows that the multiplicity of q as a root of the L-function is an upper bound for the Picard number. So, if this multiplicity is two, it is verified that the Picard number is two. There is a parity condition coming from the functional equation for L-functions which implies that this will not work if d is odd. It is reasonable to expect that a sizable proportion of such surfaces have Picard number two if d is even, but this is not currently known and is worthy of further investigation.

In sum, our commitment scheme is as follows, with a finite field $\mathbb{F}_q$ and integers m, d selected a priori:

(1) Encode a message as well as some randomness within (f_0, f_1, f_2, f_3), $f_i \in \mathbb{F}_q[t]$, $\deg f_i \leq m$.

(2) Choose a random $F \in \mathbb{F}_q[x_0, x_1, x_2, x_3]$ homogeneous of degree d with $F(f_0, f_1, f_2, f_3) = 0$.

(3) Check whether the surface defined by $F = 0$ is smooth and has Picard number two. If so, publish F as the commitment. If not, pick a different F in step (2).

For an explicit example, consider $m = 3, d = 6$. For a sextic surface to contain a given twisted cubic, one needs to satisfy a system of 19 equations in 84 variables and, hopefully, many of those will give rise to smooth surfaces with Picard number two. The space of available messages depends on 16 variables.

One can also use $m = 3, d = 4$. The inequality in the theorem is not satisfied but the second value for δ is $13/2$, which is not an integer so cannot be D_1D_2 and the result holds. In this case, we have a system of 13 equations in 35 variables for the coefficients of the surface and again, the space of available messages depends on 16 variables.

The expansion from 16 variables to 84 (or 35) from the message to the commitment is potentially wasteful and it is worth investigating whether a priori setting many of these variables to zero will still allow enough variability so that step (3) above succeeds. Another, less explicit way, of achieving the same result is to require that F vanishes at a prespecified set of points Z_0 not lying on the curve P. Poonen (personal communication) informs me that the results of [Poo08] can be adapted to show that, for d large, a positive proportion of the surfaces containing both P and Z_0 are smooth.

Another issue worth studying is the choice of q. In some ways, small q is better for computations. But, if a very small value of q, such as $q = 2$ is chosen, then $m = 3$ is too small, as it allows brute force searching for the rational curve.

Given a surface, to find a rational curve inside it, one can either do a brute force search on the coefficients of the parametrization, or set up a system of equations for these coefficients and try to solve it, e.g., using Gröbner bases. Neither option seem particularly efficient. Neither option also appears to be much improved by the use of quantum computers. There are general algorithms in the literature (e.g., [PTvL15]) that compute the Néron–Severi group of a variety but these make no claim of practicality.

Acknowledgements

This work was supported by MBIE. I would also like to thank Steven Galbraith for suggesting that I look into commitment schemes and for helpful comments as well as Edgar Costa and Bjorn Poonen for suggestions.

References

[AG06] K. Akiyama and A. Goto, *A public-key cryptosystem using algebraic surfaces*, (extended abstract), PQCrypto Workshop Record.

[AG08] K. Akiyama and A.Goto, *An improvement of the algebraic surface public-key cryptosystem*, Proceedings of SCIS.

[BCG14] Dan Boneh and Henry Corrigan-Gibbs, *Bivariate polynomials modulo composites and their applications*, 42–62.

[BL17] Daniel J. Bernstein and Tanja Lange, *Post-quantum cryptography*, Nature **549** (2017), no. 7671, 188–194.

[Cor99] Gunther Cornelissen, *Stockage diophantien et hypothèse abc généralisée*, C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), no. 1, 3–8.

[Cos15] Edgar Costa, *Effective computations of Hasse–Weil zeta functions*, 2015, Ph.D. Thesis, p. 78.

[IV09] Petar Ivanov and José Felipe Voloch, *Breaking the Akiyama–Goto cryptosystem*, 113–118.

[Pas20] Hector Pasten, *Bivariate polynomial injections and elliptic curves*, Selecta Math. (N.S.) **26** (2020), no. 2, Paper No. 22, 13.

[Poo08] Bjorn Poonen, *Smooth hypersurface sections containing a given subscheme over a finite field*, Math. Res. Lett. **15** (2008), no. 2, 265–271.

[Poo10] Bjorn Poonen, *Multivariable polynomial injections on rational numbers*, Acta Arith. **145** (2010), no. 2, 123–127.

[PTvL15] Bjorn Poonen, Damiano Testa, and Ronald van Luijk, *Computing Néron–Severi groups and cycle class groups*, Compos. Math. **151** (2015), no. 4, 713–734.

[SV20] Igor E. Shparlinski and José Felipe Voloch, *Value sets of sparse polynomials*, Canad. Math. Bull. **63** (2020), no. 1, 187–196.

[Vol85] José Felipe Voloch, *Diagonal equations over function fields*, Bol. Soc. Brasil. Mat. **16** (1985), no. 2, 29–39.

[Wan] Julie Tzu-Yueh Wang, *A note on Wronskians and the ABC theorem in function fields of prime characteristic*, Manuscripta Math. **98**, no. 2, 255–264.

[ZW17] Xiaona Zhang and Li-Ping Wang, *Partial bits exposure attacks on a new commitment scheme based on the Zagier polynomial*, 357–366.

Received 3 Aug 2020.

JOSÉ FELIPE VOLOCH: felipe.voloch@canterbury.ac.nz
School of Mathematics and Statistics, University of Canterbury, Christchurch, New Zealand

VOLUME EDITORS

Stephen D. Galbraith
Mathematics Department
University of Auckland
New Zealand
https://orcid.org/0000-0001-7114-8377

The cover image is based on an illustration from the article "Supersingular curves with small noninteger endomorphisms", by Jonathan Love and Dan Boneh (see p. 9).

Electronic copies can be obtained free of charge from http://msp.org/obs/4 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-07-1 (print), 978-1-935107-08-8 (electronic)

First published 2020.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 4

Fourteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place 29 June to 4 July 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.

TABLE OF CONTENTS