Commitment Schemes and Diophantine Equations

Felipe Voloch

ANTS XIV

July 2020

UC
UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

Abstract

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.

Motivation

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. (As it is possibly quantum resistant)

An encryption system based on this principle was proposed by Akiyama and Goto, then broken by Ivanov and V., fixed, broken again, fixed again,... Current status unclear.

Commitment scheme

Commit a message without revealing it (e.g. vote, auction bid) by making public a value obtained from the message and check, after message is revealed, that the value confirms the message.

Using such one-way functions for commitment schemes was proposed by Boneh and Corrigan-Gibbs.

Commitment scheme II

Encode message as point P over some field F. Make public a variety V/F with $P \in V$, from some fixed family. To check, verify that P satisfies the equations of V. We need:

- 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 $\#V(F) = 1$.

The last condition is important to prevent cheating. It proves that P was indeed the committed message.

Injective maps I

Answering a question of Friedman, Poonen proved:

Theorem 1

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

For $P = (a,b)$, take $V : f(x,y) = f(a,b)$. It is very hard to find $V(\mathbb{Q})$. Indeed, the proof is non-constructive! (So we don't know f)

Injective maps II

Zagier suggested $f(x,y) = x^7 + 3y^7$. With exponent 13 instead of 7, the abcd conjecture implies that it's injective. Boneh and Corrigan-Gibbs suggested using this modulo an RSA modulus N. It will not be quantum resistant.

Question

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

Pasten: There exists affine surface S with $S(\mathbb{Q})$ Zariski-dense and a morphism $S \to \mathbb{A}^1$ inducing an injection $S(\mathbb{Q}) \to \mathbb{Q}$.

$S(\mathbb{Q})$ is too sparse to be cryptographically useful.

Injective maps III

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

Question

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

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

Injective maps IV

abcd conjecture holds for function fields of char p for functions of degree at most p, so $x^{13} + ty^{13}$ injective in the set of pairs of elements of $K(t) - K$ of degree at most $p/13$ if $13 \nmid p(p-1)$. Enough for application to commitment schemes by taking a sufficiently large finite field K.

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

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

Curves on surfaces I

Rational curve P parametrized by $(f_0 : f_1 : f_2 : f_3)$ in $\mathbb{P}^3$ over a finite field $\mathbb{F}_q$, f_i polynomials of degree at most m. Such a curve will be our message and our commitment will be a smooth surface $S/\mathbb{F}_q$ of degree d containing P.

Curves on surfaces II

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

Curves on surfaces III

To check if Picard number is two, compute L-function of S.

Theorem 2

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 $m < 2d(d-4)/(d-2)$.

Curves on surfaces IV

H hyperplane section and , D_1, D_2 two smooth rational curves of degree m, $D_1D_2 = \delta$

$$\begin{vmatrix} H^2 & HD_1 & HD_2 \\ D_1H & D_1^2 & D_1D_2 \\ D_2H & D_2D_1 & D_2^2 \end{vmatrix} =$$

$$\begin{vmatrix} d & m & m \\ m & -(2+(d-4)m) & \delta \\ m & \delta & -(2+(d-4)m) \end{vmatrix}$$

Curves on surfaces IV

Only vanishes for $\delta = -(2 + (d - 4)m) < 0$ or $\delta = 2m^2/d + (2 + (d - 4)m) > m^2$. Neither can be $D_1 D_2$.

THANK YOU