Programme de la journée du département 1
Algorithmique, calcul, image et géométrie
29 mai 2019, A008

9h	Café	
9h30	Jimmy Etienne, MFX	Curved slicing for additive manufacturing
	Gabrielle De Micheli, Caramba	Recovering ECDSA cryptographic keys from partial information
	Charles Duménil, Gamble	Expected size of the Delaunay triangulation of random points on a surface
10h30	Pause	
11h	Aude Le Gluher, Caramba	How much time does it take to factor an integer?
	George Krait, Gamble	Numerical Algorithm for the Topology of Singular Plane Curves
	Semyon Efremov & Thibaut Tricard, MFX	Procedural phasor noise
12h	Déjeuner	
13h30	Remi Decelle, Adagio	Measuring wood quality of logs from low-cost sensors at the sawmill or at the road side
	Paul Huynh, Caramba	NIST's lightweight cryptography initiative

Jimmy Etienne, MFX: Curved slicing for additive manufacturing

3D printing by local material deposition is becoming increasingly important in companies and homes, but many defects mean that these parts are rarely used outside the prototyping phases. The most common defects are:
- delamination (structural weakness created by the deposition of successive flat layers)
- the staircase effect (visual defect created by the deposition of successive layers on the surface)

The approach envisaged is to use existing equipment in the field (3D printers, robotic arms) and to be able to print objects with better structural and/or visual quality. To this end, we plan to develop "curved" slicing techniques in order to avoid the current techniques of slicing by plane (although there is still room for improvement).

In the literature, the approaches never directly address the problems associated with automatic cutting of curved slices. There are proofs of concepts of 3D printing outside the plane, scheduling algorithms for wire-frame objects, objects cut into different printable areas (still on planes), and others print only the outer surface or a thin layer in a curved manner. The scientific objective of this thesis is to revisit the slicing algorithms by allowing deposits along arbitrary curves, in order to improve the quality of the parts (surface condition and/or mechanical resistance). The usual use of planar slices actually simplifies the problem of slicing. When approaching curved slicing, the addition of a large number of degrees of freedom makes the problem difficult to address. We therefore have a progressive approach, which consists in gradually relaxing the flatness constraints to target a generic method at the end of the thesis.

Gabrielle De Micheli, Caramba: Recovering ECDSA cryptographic keys from partial information

A signature algorithm such as ECDSA allows a person to sign some message in order for the receiver to be guaranteed the message is indeed from the right issuer. The Elliptic Curve Digital Signature Algorithm, known as ECDSA, is such a signing algorithm where each signature on some message requires the use of some nonce k. ECDSA, as well as other cryptographic protocols, are known to leak information which can then be used to recover the secret key of the signer. In this work, we look at different ways to recover the secret key used in ECDSA when partial information about the nonce k is known, in particular some consecutive bits. We explain how key recovery can be derived from some difficult lattice problem.

Charles Duménil, Gamble: Expected size of the Delaunay triangulation of random points on a surface

It is well known that a planar triangulation has a linear size. This result is due to the Euler characteristic. In dimension 3 or higher, we can find triangulations that have a size of Θ(n^2).
We compute the size of the triangulation when the points are distributed on surface. For instance, on a cylinder, it is proved that you can have a bad size, O($n\sqrt{n}$), even with a good deterministic sample. But if the points are distributed at random, then a tight bound Θ(n ln n) is reached in expectation. We try to adapt those results on generic surfaces where good samples lead to a triangulation in O(n ln n), and where we expect a linear expected size.

Aude Le Gluher, Caramba: How much time does it take to factor an integer?

The security of some asymetric cryptography relies on the fact that it takes a prohibitive amount of time to factor large enough integers. But how much is "large enough" ? In order to answer the question, I study a factorizing method: the number field sieve (NFS). The goal of my thesis is to get the best estimations possible for its computing time, both from a theoretical and a practical viewpoint. In this talk, I will present a method I designed to assess the asymptotic complexity of NFS.

George Krait, Gamble: Numerical Algorithm for the Topology of Singular Plane Curves

We are interested in computing the topology of plane singular curves. For this, the singular points must be isolated. Numerical methods for isolating singular points are efficient but not certified in general. We are interested in developing certified numerical algorithms for isolating the singularities. In order to do so, we restrict our attention to the special case of plane curves that are projections of smooth curves in higher dimensions. In this setting, we show that the singularities can be encoded by a regular square system whose isolation can be certified by numerical methods. This type of curves appears naturally in robotics applications and scientific visualization.

Semyon Efremov & Thibaut Tricard, MFX: Procedural phasor noise

Procedural pattern synthesis is a fundamental tool of Computer Graphics, ubiquitous in games and special effects. By calling a single procedure in every pixel -- or voxel -- large quantities of details are generated at low cost, enhancing textures, producing complex structures within and along surfaces. Such procedures are typically implemented as pixel shaders.

We propose a novel procedural pattern synthesis technique that exhibits desirable properties for modeling highly contrasted patterns that are especially well suited to produce surface and microstructure details. In particular, our synthesizer affords for a precise control over the profile, orientation and distribution of the produced stochastic patterns, while allowing to grade all these parameters spatially. Our technique defines a stochastic smooth phase field (a phasor noise) that is then fed into a periodic function (e.g. a sine wave), producing an oscillating field with prescribed main frequencies and preserved contrast oscillations. In addition, the profile of each oscillation is directly controllable (e.g. sine wave, sawtooth, rectangular or any 1D profile). Our technique builds upon a reformulation of Gabor noise in terms of a phasor field that affords for a clear separation between local intensity and phase.

Remi Decelle, Adagio: Measuring wood quality of logs from low-cost sensors at the sawmill or at the road side

The thesis focuses on the estimation of wood quality. The analysis of X-ray computer tomography (CT) images has been extensively studied over the past 30 years and more recently. We are interested here in the analysis of RGB images taken by digital cameras (cameras or smartphones).

We only have images of log ends. In the literature, few studies have been carried out for the processing of such images.

The quality of the wood determines its use and price. This quality also influences the physical properties of the log. Several elements highlight this quality, such as the difference between the position of the marrow and the geometric centre of the log or the average thickness of the rings.

Among the features mentioned, an important feature to detect is the pith. Few studies have already been focused on this work on such images. However, these studies make some assumptions, a manual segmentation of the log must be done beforehand or the log is centered in the image. Our first work was to develop an algorithm to locate the pith without these assumptions. Our current work is to study the gap between the pith and the geometric centre of the log (a quality indicator). To do this, we look at the segmentation tools.

Paul Huynh, Caramba: NIST's lightweight cryptography initiative

Driven by the need for cryptographic primitives that can run on devices with very low computing power, small memory and limited power supply, a process to evaluate and standardize these so-called lightweight cryptographic algorithms was recently initiated by the Nation Institute of Standards and Technology (NIST). This presentation intends to give an overview of this initiative and will briefly introduce our submission, "Lilliput-AE".