PROPUESTA
TRABAJO DE FIN DE GRADO – GRADO EN INGENIERÍA INFORMÁTICA

Prof. Simone Santini
Correo electrónico: simone.santini@uam.es Teléfono: +34 91 497 2209
En calidad de: Profesor del departamento de Ingeniería Informática

Propone el siguiente TRABAJO DE FIN DE GRADO, a fin que sea difundido en la Escuela Politécnica Superior, según la normativa vigente, para su posterior asignación y elaboración.

☐ Marcar en caso de que la propuesta esté vinculada a Prácticas Externas Curriculares.

<table>
<thead>
<tr>
<th>Título</th>
<th>Tagging privacy: cryptographic methods for avoiding statistical inference in personal data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tutor</td>
<td>Simone Santini</td>
</tr>
</tbody>
</table>

**Breve descripción de la motivación y objetivos**

These days, it is quite common to post pictures in a social network tagging them with information such as the names of the people therein depicted. This information, apparently harmless, reveals, to the companies that control the social network, a lot about the people that appear in the photographs. The sheer volume of reliably replicated data can be used as the basis for techniques such as network tomography in order to extract much more information than the user originally intended to give.

In this project, we shall study the use of one-way trapdoor functions for hiding the identity and the repeated presence of people in tagged images. The idea is to devise a method so that the same tag (e.g. the name of a person) will be encoded each time as a different encrypted tag, in such a way that it will be very hard for the unauthorized person to determine whether two encrypted tags correspond to the same person or not. Only the owner of the information (the person depicted in the photograph) and other authorized agents will possess the decryption algorithm necessary to realize whether different tags are, in fact, about him or not.

In this way, malicious agents (e.g. the companies that own the social networks) will not be able to perform any statistical deduction on the tagged data, since it will be impossible to identify the name of the same person in different pictures. Only the people authorized by the owner of the information will be able to do so.

For more information, come and see me in my office (B-350) and/or write to me: simone.santini@uam.es

**Requisitos y conocimientos del estudiantes, tanto deseadable como indispensables**

Good programming skills (in any language you like);
Curiosity, creativity, and the capacity to look for new solutions;
Good capacity for mathematical reasoning (although no specific knowledge of advanced mathematics is required);
A basic knowledge of cryptography is a plus (but not necessary: the math involved is quite easy);
This is a very publishable work, so a reasonable knowledge of English and a good capacity for expressing ones thoughts in a clear and concise manner will be very useful;
A good sense of humor is required for a fruitful interaction with the project advisor.

**Lugar de realización del proyecto y horario tentativo**

Any corner of the EPS, the cafeteria, your home, my office... apart from regular meetings to discuss progress, you are pretty much free to work in any place you like: a laptop with Linux on it is all you need.

Free schedule: be your own boss, and work at your own rythm.

**En caso de existir una beca o posibilidad de la misma, indicar cuantía y entidad financiadora.**

<table>
<thead>
<tr>
<th>Entidad Financiadora</th>
<th>Cuantía</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Plazo de la solicitud**

Open

Marcar con una X las Competencias de Tecnología Específica a las que se adscribe (BOE 4 agosto 2009):

- [ ] Ingeniería del Software
- [ ] Ingeniería de Computadores
- [X] Computación
- [ ] Sistemas de Información
- [ ] Tecnologías de la Información

Madrid 15 de Mayo de 2013

(Firma)