BIO GRAPHY

Business Plan

Roberto Tinelli

Lorenzo Rossi

Michele Mascherpa

Alessia Pisano

Maximilian Kullmann

Christian Knoll

Table of content

1. Description of the Business Idea

Private data is getting increasingly important in our everyday life. As data collection levels are reaching new heights and information is the key to power, also data breaches and theft are on the rise.

Bio-Graphy introduces a new encryption process to offer corporations, governments and defense departments the kind of data security that is needed to prevent these damaging actions from happening. Thus, it protects an entity's most confidential data. It augments the trust of its clients by safely securing their most valuable information and at the same time reducing anticipated cost due to weak data/information protection.

Our **Vision** is to become an internationally competitive and acknowledged new encryption standard for file and folder encryption.

The, to our knowledge, worldwide **new symmetric encryption process** is called **PBE** (Protein Based Encryption). In a first step, every letter of the alphabet, numbers and symbols are matched with a specific (artificial) amino acid. For the encryption of a plaintext (message or other data), the "translated" amino acids will build a chain which then can be virtually folded through a computational process into a 3D tertiary protein structure. The folded protein, containing our encrypted information, can be sent to any receiver or be stored in an internal database. Additionally, this process also allows our method to go one step further, since multiple tertiary structures can be combined in one larger quaternary structure. This can be elaborated through an example: a company encrypts a vital business report through our process into a quaternary structure, containing multiple tertiary structures. Each of these tertiary structures contain a specific folder filled with information relating to specific aspects of the business. Storing this information in a quaternary structure allows the company to grant specific employees access to individual parts of the report, keeping the other parts of the report encrypted and safe from exposure.

By unfolding the protein via a process, similar to "Rosetta", the original chain of amino acids will be derived and can be translated back into the original plaintext. This is the **basic idea**. In order to perform the process more efficiently, a protein will not be folded every time in a completely new way but the folding will be partially matched with some "base-proteins", located in a database. This matching process allows to fold different parts of the amino acid chain in a similar way as the matched "base-proteins" are folded. To unfold the virtual

protein, it will be again compared to the partially matched "base-proteins" and unfolded in the way it was folded. As it is a symmetric key encryption, the key must be shared (the way on how the protein was folded) with other individuals for them to access the encrypted data.

Furthermore our method enables us to encrypt already encrypted messages, for example of RSA, thus adding a second layer of security that would make the encrypted unreadable to any hostile purpetrator.