NOVEL EFFICIENT QUANTUM-SAFE CRYPTOSYSTEM

ITC

MARKET CHALLENGES

Securing governmental, economic or personal data has become a major stake due to their exponential digitalization and the increase in quantity and in sophistication of cyberattacks.
National security agencies have long recommended a set of public-key crypto algorithms for protecting sensitive data, including Diffie–Hellman key-exchange based on elliptic curves and RSA encryption. However, these public-key cryptographic systems that form the bedrock of most modern data protection are harshly threatened by mathematical breakthroughs and the next arrival of powerful quantum computers (anywhere in the next 10 to 50 years according to several experts). That is why, NSA has recently recommended to move as soon as possible to crypto algorithms that will survive upcoming algorithm transition. The demand for quantum-safe cryptographic solutions by governments and industry will likely grow dramatically in the coming years.

INNOVATIVE SOLUTIONS

The innovation relies on the development of a new variant of the HFE (Hidden Field Equations) pattern allowing to guarantee a **very high security level** with regard to the best attacks of the literature, while keeping good practical characteristics (reasonable size of the public key, speed of encryption/signature verification and decryption/signature generation) and by proposing **short and efficient signatures.**

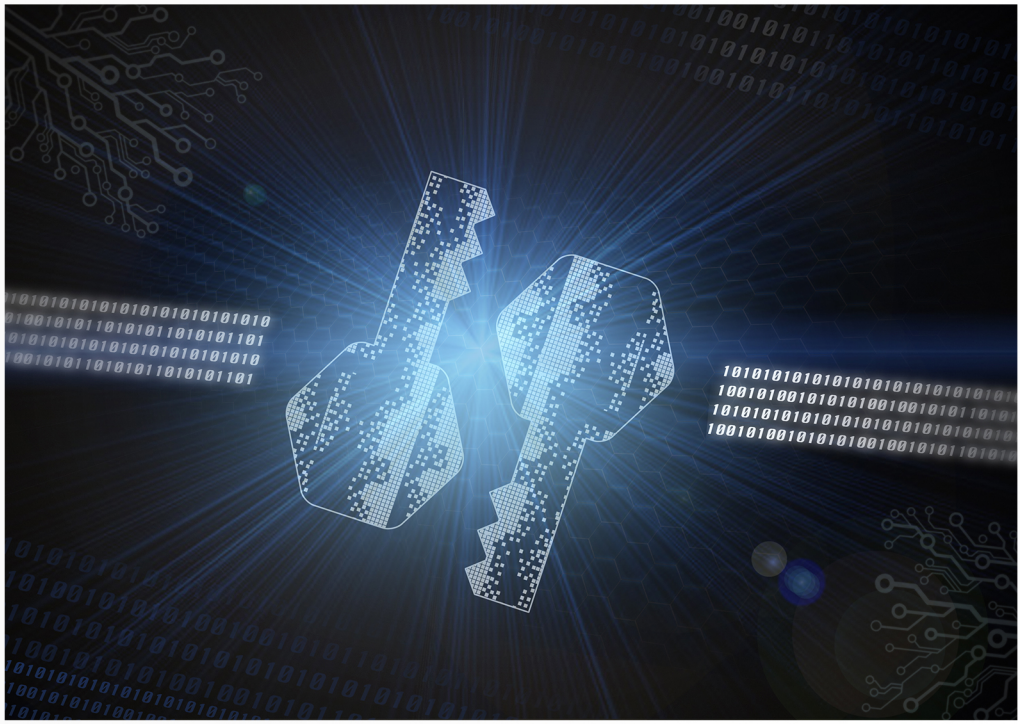
SUGGESTED APPLICATIONS

• **Signature generation and check allowing data authentication** (coming from the person claiming to be the author) and **ensuring data integrity** (prevention of any deliberate or fortuitous change of the message).

• Exchanging data on a network by opening a **secured communication channel**

DEVELOPMENT STATUS

A mobile app under Android which sends encrypted messages and photos has been realized.
It has been tested by the DGA during a field test with army combat units.



COMPETITIVE ADVANTAGES

- Improvement of encryption security
- Faster encryption
- Shorter digital signature
- Possibility of occasionally exchanging highly secured data, without resorting to dedicated equipment

MA00248 IP PROTECTION

KEYWORDS

CRYPTOSYSTEM | ENCRYPTION | DATA AUTHENTICATION
COMMUNICATION CHANNEL | CYBERSECURITY | DIGITAL SIGNATURE

CONTACT
AMANDINE LE GUENNEC
bd@sattlutech.com