CA Algorithms

Stream cypher: QP-DYN

CA QP-DYN is a family of symmetric encryption algorithms that can be used for real time encryption - decryption of variable length messages. Its primary application scenario is the encryption of arbitrarily long data streams (Surveillance, Communications, entertainment, …).
The Initialization Key can be either fixed or negotiated on the spot via Public Key Agreement. The generated key stream is as long as the data stream to be encrypted and has very good statistical properties. This allows a One Time Pad encryption/decryption mode which, according to Shannon's theorem, achieves the maximum level of attainable cryptographic strength.
Inspired by this class of algorithms, recently a new, specific for hardware, class of algorithms has been developed with much higher performances.

Public Key Agreement (PKA): QP-KEX

Extremely flexible Public Key Agreement method which allows the creation of a Secret Shared Key (SSK) through publicly exchanged information between two subjects.
In addition to CA QP-Kex several innovative families of algorithms of PKA are under active study and some among them have the qualities to become candidate new standards in the Public Key Agreement scenario.

Identification: Muncher

Muncher is a suite of highly innovative identification algorithms, including both OTP (One Time Password) and CBI (Challenge Based Identification) protocols, scalable, resistant to statistical, algebraic and crypt analytical attacks. In its standard implementation, it uses a 128bit key to send 80bit messages.
At prototype level it has been implemented in USB, embedded systems, FPGA and RFID devices.
Originally tailored to the needs of the automotive market, it has now been implemented on software for Mobile Payments (Android).
OTP based identification: in this mode, when the user activates the device, on its screen a string of characters appears to be used as access code.
CBI: in this mode the process is activated by an access request emitted by the device. In response to this request the access controller sends a signal (Challenge) which is always different from the previous one. The device elaborates the answer and sends it back to the controller who verifies it and authorizes access only if the answer is correct.

A higher level of security, decoupling the identity from the ownership of the device, is obtaining introducing a PIN (Personal Identification Number) which activates the device. The price for this is a considerable loss in speed of the identification process.

Personalization: used algorithms are proprietary, many of them are published since several years. The list is annually updated and enriched in international conferences or journals.

References

Vittorio Ottaviani, Alberto Zanoni, Massimo Regoli: CONJUGATION AS PUBLIC KEY AGREEMENT PROTOCOL IN MOBILE CRYPTOGRAPHY - SECRYPT 2010 - http://secrypt.icete.org

L. Accardi, M. Ohya, M. Regoli: THE QP-DYN ALGORITHMS - Quantum Bio--Informatics IV - World Scientific, QP-PQ Series vol. 28 (2011) 1-15 - ISBN/ISSN: 978-981-4343-75-6

Accardi, L., Markus Gaebler: Statistical Analysis of Random Number Generators In: Quantum Bio-Informatics IV - World Scientific, QP-PQ Series vol. 28 (2011) 117-128 - ISBN/ISSN: 978-981-4343-75-6

CryptAlarm s.r.l.
Operating Headquarters
Centro Interdipartimentale V.Volterra
Facoltà di Economia - Edificio Ricerca
Università di Roma "Tor Vergata"
Via Columbia 2, 00133 Roma, Italy
Tel. (+39) 06 2022498