TWD
INDUSTRIES

TWD Industries AG
Paradiesli 17
CH-8842 Unteriberg
Switzerland
Tel. +41 (0)55 414 2093
Fax +41 (0)55 414 2067

twdi.ch
g-wan.ch
global-wan.ch

SwissPostQuantum

Summary

TWD Industries AG has mathematically demonstrated its **post-quantum symmetric encryption** (PQSE) to the French DRM (Direction du Renseignement Militaire) in year 2007. Encryption standards like AES are expected to show design limits in the near future, notably because of the availability of "quantum computers". TWD's mission is to provably-secure today's critical infrastructure (communications, energy, transports, finance, government) and tomorrow's "Internet of Things" deployments.

Academic Background

To grasp the value of TWD works, let's quote CORDIS, one of the most reputed Academic Research public funding in the world:

> ***Post-quantum cryptography for long-term security*** *(p*roject reference: 645622)
> *Funded under ICT-32-2014 - Cybersecurity, Trustworthy ICT*
> *From **2015**-03-01 to **2018**-03-01, ongoing project (horizon 2020)*
> *Total cost: **EUR 3,964,791.25***
> *EU contribution: EUR 3,851,791.25*
> *Other contributions: EUR 113,000*
>
> *Online banking, e-commerce, telemedicine, mobile communication, and cloud computing depend fundamentally on the security of the underlying cryptographic algorithms. These systems are all broken as soon as large quantum computers are built. The EU and governments around the world are investing heavily in building quantum computers; society needs to be prepared for the consequences, including cryptanalytic attacks accelerated by these computers. Long-term confidential documents such as patient health-care records and state secrets have to guarantee security for many years, but information encrypted with today's standards and stored until quantum computers are available will then be as easy to decipher as Enigma-encrypted messages are today.*
>
> *The challenge is to **find solutions guaranteeing end-to-end security regardless of improvements in attacker hardware or computational capabilities**.*

*WP1: Deliverables include reference **software implementations** and optimized implementations as well as **ASIC designs** and physical security analysis.*

*WP2: Get high-security post-quantum crypto ready **for all common Internet platforms**, including large server CPUs, smaller desktop and laptop CPUs, netbook CPUs (Atom, Bobcat, etc.), and smartphone CPUs (ARM).*

*WP3: Provide **public-key** and **symmetric-key cryptography** for the cloud and protection for files that users store in the cloud, even if the cloud service providers are not trustworthy.*

Technische Universiteit Eindhoven (NL), Bundesdruckerei GmbH (DE), Danmarks Tekkniske Universitet (DK), INRIA (FR), Katholieke Universiteit Leuven (BE), NXP Semiconductors Belgium NV (BE), Ruhr-Universitaet Bochum (DE), Stichting Katholieke Universiteit (NL), Technische Universitaet Darmstadt (DE), Univerisity of Haifa (IL), Academia Sinica (TW).

Consequences on Everybody's Security

Switzerland is absent from this strategic international research project spanning from Europe to... Taiwan.

How serious is the threat of Quantum Computers? According to the CORBIS project:

> *"information encrypted with today's standards and stored until quantum computers are available will then be as easy to decipher as [1920] Enigma-encrypted messages are today."*

This demonstrates the obsolescence of any security based on "computational hardness", the only "truth" taught in Universities today – and the need for provably-secure designs.

Restoring the trust, worldwide, will require *"Tech vendors to embrace higher standards"* as The Economist wrote[1] in *"The Internet of things (to be hacked)"*.

Opportunity for Switzerland

TWD Industries AG has already done most of what the CORBIS consortium is expected to deliver in 2020 – including today's much-needed **symmetric post-quantum encryption**.

Swiss Academic collaboration and investors would let Switzerland establish itself as a world leader in this market – with the accompanying economic growth and international reputation in a *post-Snowden* world:

> In june 2015, Germany installed Patriot missiles on the Turkish-Syrian frontier, in cooperation to the US and Italy. The Spiegel reported that these missiles have been remotely hacked[2].

If military systems are not resilient enough to these new threats, the common critical infrastructure is certainly even more exposed to uncontrolled risks, like the US NASDAQ stolen and taken-down by hackers since 2011[3].

1 http://global-wan.com/en/mission.html

2 http://europe.newsweek.com/german-missiles-hacked-by-foreign-source-329980

3 http://www.nsa.gov/public_info/_files/speeches_testimonies/022315_New_America_Foundation.pdf
http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq