Meeting on Malta

Initial Progress Report of the 1st Milestone – 6 month ...

SPS G5448

"Secure Communication in the Quantum Era"

Presenter:

Otokar Grošek, NPD

April 2, 2019

Introduction

- This project is a continuation of a very successfull project G4520 "**Secure Implementation of Post-Quantum Cryptography"** (partners SK, IL, FR USA 2013 - 2016)
- Awarded by the ***2018 NATO PARTNERSHIP PRIZE IN THE CYBER SECURITY*** as the best project in the field during last decade…

NATO
OTAN

2018 NATO SPS Partnership Prize

Citation

The 2018 NATO Science Partnership Prize is awarded to the following individuals for their outstanding contribution to science through collaboration:

Professor Otokar Grošek

Director, Institute of Computer and Mathematics, Slovak University of Technology, Bratislava, Slovakia

Doctor Eran Tromer

Senior Lecturer, School of Computer Science, Tel Aviv University, Tel Aviv, Israel

Professor Viktor Fischer

Jean Monnet University, Saint-Etienne, France

Doctor Rainer Steinwandt

Florida Atlantic University, Boca Raton, U.S.A.

For excellence in cooperation in the NATO-sponsored Science for Peace Project on:

Secure Implementation of Post-Quantum Cryptography

The Prize is awarded for their collaboration on post-quantum cryptography research with particular focus on algorithmic and cryptanalytic parameters. The research team worked to identify secure parameter sets, relevant attack vectors for side-channel analyses, and secure implementations for asymmetric cryptographic schemes in a post-quantum setting.
Reliable cryptographic solutions to protect the evolving information technology infrastructure remains vital. With quantum computing on the horizon, new solutions are needed, as key parts of many existing cryptographic solutions are rendered insecure once large-scale quantum computing capabilities are widely available.
A NATO Science for Peace and Security grant was awarded for this project in 2013 and since then the researchers have aptly fulfilled the original objectives of the project and have effectively used the resources at their disposal. The project involved real cooperation between Slovakia and Israeli experts, together with experts from France and the United States.
The project had significant visibility in the public and in the scientific community. From a broader perspective, the project increased the awareness of NATO's research activities in the cyber field. The project has been important in preparing young scientists for post-quantum research, which is now gaining momentum in the scientific community.

Project administration

The Initial Report

- Objectives of the project
- Status
- Next milestone
- Financial progress
- Communication

Objectives of the Project

- The project focuses on the **SPS Key Priority of Cyber defence** – Secure Group Communication
- With QC on the horizon, **new solutions** are needed ...
- ... **Solutions for authenticated group key agreement** – AGKA in Q era.
- ... Also **side-channel attacks**

Status

- **Kick-off Meeting** 30th September – 3rd October 2018
- Implemented the web-page of the Project

  http://re-search.info
- Successful dissemination on Radio/TV, newspapers,... **22 items**
- We have successfuly assembled the working team and started cooperation on the main research...

Status…

- Ch. Colombo in Bratislava, R. Steinwandt in Madrid
- A joint paper presented at Computer Science Annual Workshop at Malta (Colombo)
- Signed ERASMUS contract between STU and University of Malta for realisation of exchanges of young researchers.

Next Milestone

- Step 1-A: Choice of security model, is due: formal security model for quantum-safe AGKE, along with a foundation for a suitable specification language to capture relevant AGKE properties for runtime verification.

Next Milestone

Step 1-B: Implementation security of cryptographic primitives

Step 2-A: building blocks for the protocol, which can be effectively protected against implementation-based attacks, with the focus on side-channel resistant quantum-safe signing and that can be used to realize the basic operations occurring in a quantum-safe 2-party key establishment.

Next Milestone

- Identification of a candidate protocol will have also started, based on the results of milestone 1-A, i.e. by having a well-defined security model, against which the candidate protocol can be evaluated.

Reporting…

Event	Description	Expected date
Kickoff	**Project kickoff meeting**	0
M1	**First progress and Financial Report**	6M
M2	**Completed theoretical analysis of a scalable quantum-safe AGKE; Meeting of all project partners at UM**	18M
M3	**Implementation of selected AGKE, including protection against implementation-level attacks; Workshop at UM**	30M
Final R.	**Final technical and financial report**	36M

Financial Progress

	Equipment	Training	Com&pub	Travel	Consuma	Other	Stipends	ProjMan		sum
Grosek	18664			2746	33			1669		23112
Colombo	2200									2200
Gonzales Vasco				3440						3440
Steinwandt	3661			2147			3929.65			9738
sum	24525			8333	33			1669		38490
plan	33700		500	8000			4800	4000		51000
difference	9175		500	-333	-33		4800	2304		12510

Although we spent 75% there are pending amounts to process…almost 94%

Communication

- Successfully assembled the working team for the project and started cooperation on the main research topics, as demonstrated by two visits and a joint paper presented.
- Successful dissemination phase, informing public about security problems arising from the development of QC and what research work is being done to secure public key infrastructure in the PQE.




Thank you for your attention!