Madrid - meeting of the Project

Administration, Plan for the next 6 month ...

SPS G5448

"Secure Communication in the Quantum Era"

Presenters:

Karol Nemoga, NATO Project Evaluator

Otokar Grošek, NPD

September 24-26, 2019

Project Administration

- Payment
- Reporting and Assessment
- Steps and Outcomes
- Dissemination
- Criteria for Success
- Budget
- Various

Payment

- payment for the twelve months of project work has been transferred to the NPD's institutional account and were spread among partners.

Reporting and Assessment

- A financial and technical report will be due for Milestone Two within six months from now. Further progress reports will be linked to technical milestones, as defined in the Project Plan.

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 or FAU?**	18M
M3	**Implementation of selected AGKE, including protection against implementation-level attacks; Workshop at UM**	30M
Final R.	**Final technical and financial report**	36M

Reporting…

- We will start to work on M2 Report at the beginning of March 2020…
- Two pertinent things:
- **Spending of money**
- **Deliverables of the Project**

Step 1-A: Choice of security model (Lead: URJC, contributors: FAU, UM)

Deliverable (D1): A formal security model for quantum-safe AGKE, along with a foundation for a suitable specification language to capture relevant AGKE properties for runtime verification.

Outcomes

BAI, S., **MILLER, S.** and **WEN, W.**: A Refined Analysis of the Cost for Solving LWE via uSVP. AFRICACRYPT 2019: AFRICACRYPT 2019, pp 181-205.

ZAJAC, P.: Code-based signature scheme derived from a MRHS representation of an AES encryption. In Central European Conference on Cryptology 2019 : Telč, Czech Republic. June 12-14, 2019. Brno : Masaryk University, 2019, S. 39-42.

Hai Pham, Rainer Steinwandt and Adriana Suárez Corona: Integrating Classical Pre-processing into an Optical Encryption Scheme. Entropy 2019, 21(9), 872.

Step 1-B: Implementation security of cryptographic primitives (Lead: STU, contributors: FAU)

Deliverable (D2): Implementation guidelines for side-channel resistant quantum-safe signing and for realizing basic operations as occurring in a quantum-safe 2-party key establishment (e.g., with a key encapsulation mechanism).

Outcomes

COLOMBO, C. et al.: Applying Runtime Verification to Group Key Establishment. Computer Science Annual Workshop, Malta - November 2018.

ZAJAC, P.—ŠPAČEK, P.: Preventing potential backdoors in BIKE algorithm, Tatra Mt. Math. Publ. 73 (2019), 193–207.

José Ignacio Escribano Pablos, **María Isabel González Vasco**, **Misael Enrique Marriaga and Ángel Luis Pérez del Pozo:** The Cracking of WalnutDSA: A Survey. Symmetry 2019, 11(9), 1072.

GROŠEK, O. - **FABŠIČ, T.**: Computing multiplicative inverses in finite fields by long division. In Journal of Electrical Engineering. Vol. 69, No. 5 (2018), s. 400-402. ISSN 1335-3632

Step 2-A: Identify candidate protocol (Lead: URJC, contributors: FAU)

Deliverable (D3): A complete design for a quantum-safe AGKE protocol, including security analysis with strong provable guarantees.

Outcomes

BOHLI, J.-M., **GONZÁLEZ VASCO, M. I.** and **STEINWANDT, R.**: Password-authenticated Group Key Establishment from Smooth Projective Hash Functions. Int. J. Appl. Math. Comput. Sci., vol. 29, no. 4, 2019.

Dissemination

- PQC WIKI. A platform for NIST post-quantum cryptography standardization.
- cca 20 media interviews (newspapers, radio, TV, web-magazines)
- 7 public talks (conferences, seminars, summer schools)
- supervision of 4 Master's theses 2019 (2 Zajac, 2 Fabsic,…), others?

Criteria for Success

Criterion	Relative Weight
Project Kickoff Meeting	5%
Launch Project Website	5%
Complete Equipment Purchases	4 out of 7%
Annual Meeting of all Project Partners	7%
Milestone Step 1-A	10%
Milestone Step 1-B	10%
Milestone Step 2-A	10%
Milestone Step 2-B	10%
Milestone Step 3-A	10%
Milestone Step 3-B	10%
Culminating Workshop at University of Malta	9%
Final Report	7%
Total	41 out of 100%

Budget

- Modifications to the project budget, within budget ceiling, are possible in the course of the project. Changes which, alone or together, are less than 5% of the overall budget must be approved by the NPD who must also promptly notify the SPS Office.
- Larger changes must be recommended by all co-directors and approved in advance by the SPS Office. All approved changes, will be incorporated into the project budget, and subsequent reporting shall reflect them.

Budget - cont.

After each Report unspent money are lost… or it is possible to propose a change of budget … and “NATO will make a subsequent payment in accordance with this updated schedule.“

But, as we could see, everything is possible…

Various

- Attack on our web-page…

  On 17 June 2019, our NATO project website was attacked by injecting malicious code into core CMS files stored on our FTP server. During the period when the website was infected, visitors were redirected to various sites containing malware and advertisements. The website was restored from backup and all passwords were updated. CMS system core was up to date at the time of the attack.

Various…

- Peter Spacek is going to visit UM through National Scholarship Programme of the Slovak Republic
- Dr. Misael Enrique Marriaga Castillo – a new member of the Universidad Rey Juan Carlos partner

Q. From yesterday…

training expenses for project participants including necessary travel and accommodation; training may include, but is not limited to, instruction on new equipment or techniques with the manufacturer or in the laboratory of another project participant, or a seminar/institute organized within the framework of the project to train multiple project participants simultaneously

Publication & communication

Banner… Christian = 1000EUR… for M2

Training SK in Malta

November 2019 3 people…

Meeting - USA

Daily allowance 60 $/day

If breakfast -15 $/day

Pocket money 24 $/day

Budget 5 days in a hotel …

Money 5 x (45+24) = 345 $

Hotel 5 x (120 … 200) = 600 … 1000 $

Air ticket 1000$, shuttle ???

In total 2200 – 2600$ plus car …




Thank you for your attention!