Smolenice - meeting of the Project

Writing M2 Report, Plan for the next 12 month ...

SPS G5448

"Secure Communication in the Quantum Era"

Presenters:

Karol Nemoga, NATO Project Evaluator

Otokar Grošek, NPD

March 2-4, 2020

Project Administration

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

Reporting and Assessment

- A financial and technical report will be due for Milestone 2, i.e. by March 30, 2020.
- We can declare expenditures if all the transaction was finalized, and we have relevant documents.
- We should be able to declare as much as possible to be able to get next payment in maximal amount for Milestone 3 ...

Reporting - cont.

Back-up documentation: Receipts must be provided with your financial report, clearly indicating on the receipt the item number ("financial record" tab, column A) to which it corresponds, with explanation/translation if required. All receipts should be in numerical order and sent as one file.

Reporting – cont.

- **Stipends**: template attached
-**Travel costs**: a mission report with expense breakdown signed by the traveler (you do not need to submit every single receipt)
-**Project Management cost**: a statement from the Institute is required for each milestone period on the expended amount for that milestone, without any breakdown…
-**Various costs**: standard invoices

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 in Smolenice**	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 are starting to work on M2 Report …
- Two pertinent things:

- **Spending of money**
- **Deliverables of the Project**
- **Changing in the teams – members...**
- **Outline of our next work...**
- Modifications to the project budget...

Step 1-A: Choice of security model

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 - papers

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

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 - papers

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

Outcomes - presentations

HROMADA, V.: Acoustic Side-Channels in Cryptography. CYBERSEC CEE 2019 – 5th European Cybersecurity Forum. Katowice, Poland. 29. - 30. 10. 2019

Step 2-A: Identify candidate protocol

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

Outcomes - papers

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.

PERSICHETTI, E., STEINWANDT, R. and **SUÁREZ CORONA, A.:** From Key Encapsulation to Authenticated Group Key Establishment – a Compiler for Post-Quantum Primitives, Entropy – Special Issue Blockchain: Security, Challenges, and Opportunities, vol. 21, no. 12, 1183, 2019.

Outcomes - papers

BOHLI, J.-M. - GONZÁLEZ VASCO, M.I. - STEINWANDT, R.:
Building Group Key Establishment on Group Theory: A Modular Approach, Symmetry – Special Issue on Interactions between Group Theory, Symmetry and Cryptology) 2020, 12(2), 197.

Step 2-B: Identify protocol-level security mechanisms

Deliverable (D4): Guidelines for securing an implementation of a quantum-safe AGKE against a substantial class of implementation-level attacks on a relevant target platform.

Outcomes - papers

COLOMBO, C. - VELLA, M.: Towards a Comprehensive Solution for Secure Cryptographic Protocol Execution based on Runtime Verification. In: ForSE, Valletta, Malta, 2020.

.

Outcomes - presentations

SPACEK, P. - COLOMBO, C. - VELLA, M.: Using TEE and RV in PQ-TLS Communication. CSAW'19. Department of Computer Science. University of Malta. 29. 11. 2019

SPACEK, P. - COLOMBO, C. - VELLA, M.: Combining HSM and RV to secure communication. Department of Computer Science. University of Malta.

Step 3-A: Protocol and parameter optimization

Deliverable (D5): A quantum-safe AGKE protocol where all parameter choices are fully specified for relevant security levels. Parameter recommendations must be derived from theoretical results or/and validated through experimental data.

Preliminary work started by examining efficiency of selected proposed post-quantum system, and estimated cost of realizing quantum attacks.

Outcomes - papers

MATHEIS, K., STEINWANDT, R. and **SUÁREZ CORONA, A.:** Algebraic Properties of the Block Cipher DESL, Symmetry, vol. 11, no. 11, 1411, 2019

BAI, S. - BOUDGOUST, K. - DAS, D. - ROUX-LANGLOIS, A. - WEN, W. - ZHANG, Z.: Middle-Product Learning with Rounding Problem and Its Applications. In: Galbraith S., Moriai S. (eds) Advances in Cryptology -- ASIACRYPT 2019, Lecture Notes in Computer Science, vol. 11921, pp. 55-81, Springer, 2019.

LANGENBERG, B. - PHAM, H. - STEINWANDT, R.: Reducing the Cost of Implementing AES as a Quantum Circuit, IEEE Transactions on Quantum Engineering, 2020.

Step 3-B: Deploy implementation-level security mechanisms

Deliverable (D6): A fully operational quantum-safe AGKE, including protection against implementation-level attacks.

Outcomes - papers

PERNICKÝ, Ľ. - ZAJAC, P. Integration of post-quantum cryptography to Android application (in Slovak). In *Santa's Crypto 2019 : proceedings. Praha, Czech Republic. 5.-6.12.2019*. 1. ed. Bílovice nad Svitavou : Trusted Network Solutions, 2019, S. 37-38.

Summary of our solutions

- Altogether we have published 15 papers and 11 presentations at leading conferences.
- We have started to work on HW implementation of the proposed protocol.

Dissemination

- We have **a list of 41 public talks** (conferences, seminars, summer schools), media interviews (newspapers, radio, TV, web-magazines) including
- PQC WIKI. A platform for NIST post-quantum cryptography standardization.

Criteria for Success

Criterion	Relative Weight
Project Kickoff Meeting	5%
Launch Project Website	5%
Complete Equipment Purchases	7%
Annual Meeting of all Project Partners	7%
Milestone Step 1-A	10%
Milestone Step 1-B	10%
Milestone Step 2-A	4 out of 10%
Milestone Step 2-B	2 out of 10%
Milestone Step 3-A	2 out of 10%
Milestone Step 3-B	10%
Culminating Workshop at University of Malta	9%
Final Report	7%
Total	52 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.

NEW: from Klavdija

It is not necessary to spend all money allocated for the reporting milestone, as this can be adjusted when forecasting requirements for future milestones (eg. if you expect to spend less than initially approved please reflect that with your next report on the Milestone 2 tab (green columns))

Budget - cont.

- Please also note that your reporting account balance will reflect your next tranche (eg. if you reporting account balance is 50K and your expenditure forecast is 100K, we will only transfer 50K for your next tranche).
- Please note that each Progress report requires a separate technical report, but the excel file used throughout the course of the project stays the same.

Various…

- P. Spacek visited UM through National Scholarship Programme of the Slovak Republic
- T. Fabsic, V. Hromada, O. Gallo and P. Melo visited UM to work on HW implementation of the proposed protokol…
- Dr. Misael Enrique Marriaga Castillo – a new member of the Universidad Rey Juan Carlos partner

Various…

- Floyd Johnson from FAU visit to URJC (Jan 20th to Feb 21st)
- E. Antal, M. Jokay, M. Vojvoda new members of the STU team

Publication & communication

- 2 Banners, cups in SK,
- Video in SP




Thank you for your attention!