Post-quantum cryptography research at UIM FEI STU

Tomáš Fabšič Ondrej Gallo Otokar Grošek Viliam Hromada **Pavol Zajac** [1]

June 29, 2022

[1]This work was supported the NATO Science for Peace and Security Programme under grant G5448.

Outline

Impact of quantum computing

Quantum computing has a significant impact on cryptography:

- Grover's Algorithm (and related): weakens symmetric cryptography, implications for lightweight cipher designs
- Shor's Algorithm (and related): breaks public key cryptography primitives (RSA, DSA, ECDSA, ...)

Post-quantum cryptography

Post-quantum cryptography (PQC) aims to replace (mostly) public key cryptographic schemes with new ones that resist quantum attacks.

- Code-based
- Lattice-based
- Hash-based
- SIDH-based

Our PQC research projects

- 2012 – 2016: Secure Implementation of Post-Quantum Cryptography, NATO SfP 984520
- 2017 – 2020: Secure Post-quantum Cryptography, VEGA 1/0159/17
- 2018 – 2021 (extended to 2022): Secure Communication in the Quantum Era, NATO SPS Project G5448

Secure Implementation of Post-Quantum Cryptography

- Research focused on secure implementation and resistance against side-channel attacks.
- Led by Otokar Grošek, in cooperation with France, USA and Israel.
- November 2018: best project of decade of NATO Science for Peace and Security Programme in the area of cyber security.

Secure Post-quantum Cryptography

- Slovak research (VEGA), led by Pavol Zajac.
- Continuation of ”Secure Communication in the Quantum Era” with focus on more adoption of secure post-quantum cryptography.

Secure Communication in the Quantum Era

- Practical research with the main goal of secure group communication for quantum future.
- Led by Otokar Grošek, Slovak University of Technology in Bratislava, in cooperation with:
  - Rainer Steinwandt, Florida Atlantic University/The University of Alabama in Huntsville (UAH), USA,
  - Christian Colombo, University of Malta,
  - Maria Isabel Gonzales Vasco, Universidad Rey Juan Carlos, Spain.
- More information: `re-search.info`

Secure Communication in the Quantum Era: Main results

- Protocol design

  María Isabel González Vasco, Ángel L. Pérez del Pozo, Rainer Steinwandt, Group Key Establishment in a Quantum-Future Scenario, Informatica 31(2020), no. 4, 751-768, DOI 10.15388/20-INFOR427

- Protocol implementation and runtime verification

  ABELA, R. - COLOMBO, C. - MALO, P. - SÝS, P. - FABŠIČ, T. - GALLO, O. - HROMADA, V. - VELLA, M.: Secure implementation of a quantum-future GAKE protocol. In ZHOU, Jianying.Security and Trust Management : 17th International Workshop, STM 2021. Darmstadt, Germany. October 8, 2021. Cham : Springer, 2021, S. 103-121. ISBN 978-3-030-91858-3. V databáze: DOI: 10.1007/978-3-030-91859-0_6 ; SCOPUS: 2-s2.0-85121907279.

- Total: 32 (+3) Publications, 18 Presentations and Abstracts, 51 dissemination activities for the public

Secure Communication in the Quantum Era: SK results

Our contributions:

- new post-quantum research,
- implementation work,
- dissemination of knowledge in Slovakia.

SK outcomes:

- Publications: 13 (+2 submitted)
- Presentations: 8
- Dissemination: 27
- Theses: 22 Ing / 5 Bc

Secure Communication in the Quantum Era: SK results

Major publications (by P. Zajac):

- ZAJAC, P. - ŠPAČEK, P.: A new type of signature scheme derived from a MRHS representation of a symmetric cipher. In Infocommunications journal. Vol. 11, No. 4 (2019), s. 23-30. ISSN 2061-2079 (2019: 0.141 - SJR, Q4 - SJR Best Q).
- ZAJAC, P. - ŠPAČEK, P.: Preventing potential backdoors in BIKE algorithm. In Tatra Mountains Mathematical Publications : Number theory, algebra and cryptology '18. Vol. 73, (2019), s. 179-193. ISSN 1210-3195 (2019: 0.214 - SJR, Q4 - SJR Best Q). V databáze: SCOPUS: 2-s2.0-85072285502 ; DOI: 10.2478/tmmp-2019-0013.
- ZAJAC, P.: Ephemeral keys authenticated with Merkle trees and their use in IoT applications. In Sensors. Vol. 21, iss. 6 (2021), Art. no. 2036 [17] s. ISSN 1424-8220 (2020: 3.576 - IF, Q1 - JCR Best Q, 0.636 - SJR, Q2 - SJR Best Q). V databáze: DOI: 10.3390/s21062036 ; CC: 000652714500001 ; WOS: 000652714500001 ; SCOPUS: 2-s2.0-85102358756.

Secure Communication via Classical and Quantum Technologies

- Proposed new NATO SPS project led by Rainer Steinwandt.
- Main aim is to integrate PQC and QKD as available on the distributed network infrastructure.
- Two partners from Slovakia:
  - UIM FEI STU for PQC part,
  - FU SAV for QKD part.

We hope for support from QUTE.sk community and Slovak research authorities.