Minutes of the kickoff meeting

Administrative and organizational aspects of the project (discussion lead by O. Grosek)
 - Discussion focused on the rules with respect of the new Handbook and documentation which is required by STU Administration.

Webpage access, communication plan, next visits (discussion lead by O. Grosek)
 - The next meeting is planned in Sept 2019, but after the next NIST workshop, to synchronize final work on Steps 1A, 1B, 2A

Dr Karol Nemoga called attention to keep financial rules and promised to inform us how to use different exchange rates between USD and EURO.

Discussion about Milestone 1A Choice of security model (discussion lead by Rainer Steinwandt)
 - USA: presentation of possible choices, question of how to model security of protocols in post-quantum setting
 - General discussion: should we use quantum random oracles?
 - General discussion: should we focus only on codes or lattices?
 - Slovakia: we might also consider hash based signatures
 - Conclusions: Focus should be on QROM model. We should follow NIST competition and restrict our choices according to NIST recommendations.

Discussion about Milestone 1B Implementation security of cryptographic primitives (discussion lead by Palo Zajac)
 - Slovakia: Presentation of milestone 1B
 - General discussion: What of deliverables should we focus on? Scientific papers, technical reports, implementations?
 - USA: New project with NIST on classification of post-quantum candidates, cooperation can bring added value.
 - USA: How the cooperation with the Slovakian team should work in practice for this milestone?
 - Slovakia: Preferred role: Implementation of specified protocols and attacks (including side-channels). Can operate under guidance from researchers from USA.
 - Conclusions: An overview of implementation security should be done in cooperation with NIST's project on FAU.

Discussion about Milestone 2A Identify candidate protocol (discussion lead by Maribel Vasco)
 - Spain: presented potential two existing options to pursue (compilers from 2-party protocols, adopting existing multiparty protocols)
 - USA: should pursue both directions
 - Slovakia: we can also consider custom protocols not used before, should send a new proposal to participants
 - Conclusions: We should pursue multiple directions and specify final

focus on the next meeting

Knowledge transfer between NATO countries and Malta (discussion led by Ch. Colombo)

- Malta: presentation of techniques of runtime verification
- General discussion: how can we apply these techniques to post-quantum multiparty protocol implementation
- Conclusion: We need existing implementation to apply these techniques, should be done later in the project

Discussion about the involvement of young scientists

- Malta: there is a problem with motivating students to research positions due to pressure from industry jobs
- Spain: seconds the opinion
- Slovakia: we can involve master degree students working on their thesis project as well as PhD students to exchange knowledge.
- Conclusions: We should prepare ERASMUS agreement between STU and University of Malta, and possibly send a master/PhD student to stay on Malta for a longer time and work scientifically on the project topics

Discussion about crypto-courses carried at UM with Department staff (discussion led by Dr Mark Vella). UM is offering a master program in block chaining.