CBCrypto 2024: International Workshop on Code-Based Cryptography

Violetta Weger, Anna-Lena Horlemann, Jean-Christophe Deneuville

September 1, 2023

1. *Name (and possible acronym) of the event*
   5th International Workshop on Code-Based Cryptography (CBCrypto 2024)

2. *Names and contact information of the organizers*

   - **Violetta Weger**, Technical University of Munich, Munich, Germany, violetta.weger@tum.de
   - **Anna-Lena Horlemann**, University of St.Gallen, St. Gallen, Switzerland, anna-lena.horlemann@unisg.ch
   - **Jean-Christophe Deneuville**, École Nationale de l'Aviation Civile, Toulouse, France, jean-christophe.deneuville@enac.fr

3. *Length of event (1-2 days); if 1 day, indicate flexibility for dates*
   2-day event (May 25-26)

4. *A proposed format (workshop with submitted/invited talks, tutorial, panel, etc.) and potential speakers (if applicable, not complete, and no commitment)*
   The event is planned as a hybrid workshop (online and in-person participation) with contributed and invited talks (more details in attached Call for Papers). The following is a list of potential invited speakers, which have not been contacted yet: Philippe Gaborit, Jean-Pierre Tillich, Pierre Loidreau, Antonia Wachter-Zeh, Tanja Lange, Simona Samardjiska, Dustin Moody.

5. *Abstract summarizing the proposed event and its justification*
   With the steady advances in quantum technology, the search for cryptographic schemes which resist attacks on quantum computers became one of the main research topics in coding theory and cryptography over the last decades. One of the most promising directions of post-quantum cryptography is based on algebraic coding theory. Code-based cryptography is denoting any cryptographic system whose security relies on hard coding-theoretic problems, following the seminal work of McEliece in the

late 1970s. In 2017, the National Institute of Standards and Technology (NIST) has initialized a standardization process for post-quantum cryptography, which has now reached its final round and several code-based cryptosystems are in consideration. The research in this direction is, however, far from complete. On the contrary, in 2023 NIST reopened standardization call for post-quantum digital signature schemes, showing the urgency of new solutions. The workshop aims at informing researchers across the community about the newest results in the field and fostering further collaborations. Besides bringing together the existing community, we provide an opportunity to extend the range of participation to researchers approaching this research area for the first time.

6. *In the case of a submission process: a) Potential committee members, b) A draft of the relevant call (including expected dates such as submission deadline, notification, etc.)*
   We plan to confirm the committee of the previous edition. Potential committee members, dates and deadlines can be found in the attached draft of the call for papers / contributions. Please note that the easychair link is not yet functional.

7. *Estimated total number of attendees total and an expected number of student attendees*
   Due to the increasing number of attendees observed within the previous editions, we expect 200 participants = 100 (online) + 100 (in-person), out of which we expect about 100 students.

8. *A one-paragraph biographical sketch for each organizer, describing relevant qualifications, including research and conference/workshop organizing experience*

   - **Violetta Weger**
     Violetta completed her Ph.D. in mathematics at the University of Zurich in 2020 under the supervision of Prof. Joachim Rosenthal. Violetta is a Marie Skłodowska-Curie fellow at the Technical University of Munich. She is working in algebraic coding theory and code-based cryptography since her Master studies. She participated within the NIST standardization call for additional signature schemes, by submitting two code-based schemes. She is in the program committee of CBCrypto since 2023. Violetta has successfully organized several summer schools (ACT'22[1] and ACT'21[2]), in addition to large conferences[3].
   - **Anna-Lena Horlemann**
     Anna-Lena completed her Ph.D. in applied algebra at the University

[1] https://www.math.uzh.ch/act/
[2] https://www.math.uzh.ch/act/index_old.html
[3] https://www.math.uzh.ch/aa/events/joachims-bday-conference

of Zurich in 2013, after which she worked as a researcher and lecturer at the University of Melbourne and Monash University (both Australia), the University of Zurich and the EPF Lausanne (both Switzerland). Since 2017 she is a professor at the University of St.Gallen, where she currently holds the chair for Foundations of Computation at the School of Computer Science. Her main research topics are coding theory and code-based cryptography. In 2020 she received the Sofia-Kovalevskaja award by the Humboldt foundation. She has (co-)organized several conferences in the last years, among others the conference on Coding Theory and Cryptography in Zurich last year. [4]

- **Jean-Christophe Deneuville** completed his Ph.D. in Computer Science in 2016, focusing on Post-Quantum Cryptography, with an emphasis on schemes relying on Coding Theory assumptions. Since 2019, he holds an associate professor position at the French Civil Aviation University in Toulouse, France, where he leads research activities on Cybersecurity and Cryptography. Jean-Christophe has co-authored 6 submissions to the NIST call for PQC standardization process, among which two are still considered (BIKE & HQC). He belongs to the CBCrypto program committee since 2020, and has chaired the 2022 edition.

The previous organizers (Paolo Santini and Andre Esser) declared their intention to support the current chairs whenever necessary.

9. *Funding sources that may be used (and for what purposes)*
We applied for funding of approximately 8000 CHF to the Swiss Mathematical Society. We are eager to find additional funding sources. The funding will be used to cover the expenses of invited speakers and for student grants / waivers. Any left funding will be used for social events.

10. *Information of previous similar events (incl. organizational information such as attendance number), if applicable*
CBCrypto 2023 in Lyon (affiliated with Eurocrypt 2023) had 200 registrations in total.

11. *Link to draft website (if exists)*
`https://www.cb-crypto.org/`

[4] `https://www.math.uzh.ch/aa/events/joachims-bday-conference`