(Presentation submission)

Post-Quantum Signatures from Threshold Computation in the Head

Thibauld Feneuil and Matthieu Rivain

CryptoExperts, Paris, France

1 Short abstract

The submitted presentation is about the *Threshold Computation in the Head* (TCitH) framework that we propose in [FR22] (Asiacrypt 2023) and improve in a recent preprint [FR23b]. This framework extends common MPC-in-the-Head techniques by using threshold secret sharing (and in particular Shamir's secret sharing) instead of additive sharing. For some MPCitH-based post-quantum signatures, this approach can achieve significant improvements in terms of sizes and timings.

The proposed presentation would focus on the results of [FR22, FR23b]. The agenda of the presentation would typically be:

- Recall of "standard" MPC-in-the-Head techniques,
- Presentation of the TCitH framework:
  - How threshold sharing impacts MPCitH.
  - The Merkle-tree variant of the TCitH framework.
  - The GGM-tree variant of the TCitH framework.
- Applications:
  - Speeding up MPCitH-based NIST post-quantum signature candidates.
  - Making signature shorter for some candidates.

Examples of slides (only covering [FR22]) that would be extended are available here: `https://www.matthieurivain.com/files/slides-oxford23.pdf#page=51`.

2 Technical abstract

The MPC-in-the-Head (MPCitH) paradigm introduced in [IKOS07] is a versatile paradigm to build zero-knowledge proof systems from secure multi-party computation (MPC). This paradigm can be summarized as follows: By emulating an MPC protocol verifying a witness and by opening some (verifier chosen) parties, the prover convinces the verifier they know the witness with soundness error around $1/N$, for N the number of parties involved in the MPC protocol. In the traditional MPCitH approach, the bottleneck in running times comes from the emulation of the N parties. Recent works have shown how this bottleneck can be mitigated. The hypercube technique proposed at Eurocrypt 2023 [AGH$^+$23] improves the "traditional setting" (additive sharing with GGM tree commitments) by decreasing the emulation phase to $1+\log_2 N$ parties with no extra communication cost. On the other hand, MPCitH based on threshold secret sharing [FR22] (Asiacrypt 2023), here called Threshold Computation in the Head (TCitH), only requires the emulation of a (small) constant number of parties. Specifically TCitH requires $\ell+1$ parties for an $(\ell+1, N)$-threshold sharing (which is 2 parties for $\ell = 1$). Due to the use of Merkle trees in place of GGM trees for the commitments of shares, the original TCitH framework enjoys a particularly fast verification, dropping the verifier complexity from $O(\lambda N)$ to $O(\lambda)$ (for a small constant ℓ). However, it suffers some communication penalties since Merkle authentication paths are twice larger than GGM sibling paths (this overhead typically represents 2 KB for non-interactive arguments with 128-bit security). The improved TCitH framework of [FR23b] extends the original framework as follows:

1. *TCitH with GGM trees.* By using techniques from [CDI05], we can generate and commit Shamir's secret shares with the communication cost of a GGM tree (as in the traditional approach) while benefiting the low-cost MPC emulation of TCitH. Using this "TCitH with GGM tree" setting, one can further overcome a limitation of the original TCitH framework which is that the number of parties N should be at most the size of the field $|\mathbb{F}|$. The obtained variant supports any N and $|\mathbb{F}|$ with an emulation phase of $1 + \lceil \log N / \log |\mathbb{F}| \rceil$ parties (for a soundness error of $\approx 1/N$).

2. *Extended TCitH framework.* The extended TCitH framework supports (threshold) MPC protocols locally computing quadratic (or higher degree) functions instead of being restricted to linear functions. The extended framework comes with two variants depending on the used method to generate and commit the shares: GGM tree (more compact) vs. Merkle tree (faster verification). By supporting higher-degree MPC computation, the extended framework is amenable to many potential applications. We notably apply it to derive succinct arguments for low-degree arithmetic circuits providing a very competitive alternative to post-quantum zero-knowledge arguments for small-size arithmetic circuits [AHIV17, DOT21]. The extended TCitH framework is conceptually close to the Ligero proof system [AHIV17] but while the latter targets "average-size computation" the TCitH framework achieves better sizes for "small-size computation" typically arising in the design of (post-quantum) signature schemes.

3. *Applications.* The TCitH framework is instrumental to various applications and notably for post-quantum (ring) signatures. We show that our basic (non-extended) TCitH framework with GGM tree can improve the performances of nearly all the recent NIST candidates based on the MPCitH paradigm. We then apply our extended framework to proposed improved variants of these candidates. For most of them, we save between 9% and 35% of the signature size. In particular, our framework applied to the non-structured multivariate quadratic (MQ) problem provides signature sizes of 4.2 KB which is to compare with the 6.3 KB of MQOM signatures (previously the smallest based on non-structured MQ) and 4.8 KB of Biscuit signatures (MPCitH scheme based on a structured MQ instance) [FR23a, BKPV23]. We also apply our TCitH framework to design efficient post-quantum ring signatures from any one-way function. We propose concrete instances relying on the MQ and syndrome decoding (SD) problems. For a ring of 1000 users, both schemes have a running time below 10 ms, while achieving sizes around 5 KB for MQ and 9 KB with SD, which greatly improves the current state of the art.

References

AGH$^+$23. Carlos Aguilar Melchor, Nicolas Gama, James Howe, Andreas Hülsing, David Joseph, and Dongze Yue. The return of the SDitH. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part V*, volume 14008 of *LNCS*, pages 564–596. Springer, Heidelberg, April 2023.

AHIV17. Scott Ames, Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. Ligero: Lightweight sublinear arguments without a trusted setup. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017*, pages 2087–2104. ACM Press, October / November 2017.

BKPV23. Luk Bettale, Delaram Kahrobaei, Ludovic Perret, and Javier Verbel. Biscuit: Shorter MPC-based Signature from PoSSo, 2023. `https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/Biscuit-spec-web.pdf`.

CDI05. Ronald Cramer, Ivan Damgård, and Yuval Ishai. Share conversion, pseudorandom secret-sharing and applications to secure computation. In Joe Kilian, editor, *TCC 2005*, volume 3378 of *LNCS*, pages 342–362. Springer, Heidelberg, February 2005.

DOT21. Cyprien Delpech de Saint Guilhem, Emmanuela Orsini, and Titouan Tanguy. Limbo: Efficient zero-knowledge MPCitH-based arguments. In Giovanni Vigna and Elaine Shi, editors, *ACM CCS 2021*, pages 3022–3036. ACM Press, November 2021.

FR22. Thibauld Feneuil and Matthieu Rivain. Threshold linear secret sharing to the rescue of MPC-in-the-head. Cryptology ePrint Archive, Report 2022/1407, 2022. `https://eprint.iacr.org/2022/1407`.

FR23a. Thibauld Feneuil and Matthieu Rivain. MQOM: MQ on my Mind – Algorithm Specifications and Supporting Documentation. Version 1.0 – 31st May 2023, 2023. `https://mqom.org/docs/mqom-v1.0.pdf`.

FR23b. Thibauld Feneuil and Matthieu Rivain. Threshold computation in the head: Improved framework for post-quantum signatures and zero-knowledge arguments. Cryptology ePrint Archive, Paper 2023/1573, 2023. `https://eprint.iacr.org/2023/1573`.

IKOS07. Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-knowledge from secure multiparty computation. In David S. Johnson and Uriel Feige, editors, *39th ACM STOC*, pages 21–30. ACM Press, June 2007.