

“Preview Writeup”: In anticipation of a package submission to the NIST Threshold Call

Title: MiniMPC: Threshold Schemes for (and from) MiniCrypt

Version: 1.0 (2026-01-12)¹

Team name: MPC MINlons

Team members: Hongrui Cui, Chun Guo, Xiaojie Guo, David Heath, Jonathan Katz, Vladimir Kolesnikov, Alex Malozemoff, Samuel Ranellucci, Mike Rosulek, Lawrence Roy, Xiao Wang, Chenkai Weng, Kang Yang, Yu Yu

Abstract: This submission aims to provide a suite of cryptographic protocols in Minicrypt for securely evaluating any Boolean circuit, thus making it highly suitable for supporting threshold operations of Minicrypt primitives (i.e., N3 and S3). The protocol suite supports two or more parties, assuming a static adversary corrupting at most all but one party. The submission includes building blocks at different levels, providing modular composition without sacrificing efficiency. It includes definitions and constructions for correlation robustness, oblivious transfer extension, authenticated Boolean triples, and authenticated garbling. Many of these tools could be of independent interest to submissions in other contexts.

Proposed crypto-systems:

- S-mTCCRL: simulation-secure correlation robust hash function (Category S7),
- SoftspokenOT: oblivious transfer extension from minicrypt (Category S7),
- Authenticated Beaver triple (Category S7),
- Authenticated Garbling: actively secure MPC for Boolean circuits (Categories S3, and N3).

Keywords: Threshold Cryptography; NIST Threshold Call

¹Preliminary version submitted to NIST-MPTC for review

Preview writeup. This document is provided to NIST for online publication, to foster public awareness and support public discussion within the scope of the NIST First Call for Multi-Party Threshold Schemes [NIST-IR8214C]. This “preview writeup” represents a good-faith plan for a subsequent “package submission”. However, until the deadline for package submission, the team may still modify its own composition and the submission plan, including possible changes to the technical scope, and/or the used techniques or achieved results.

Team members: Hongrui Cui^{i1,a1}, Chun Guo^{i2,a3}, Xiaojie Guo^{i3,a2}, David Heath^{i4,a9}, Jonathan Katz^{i5,a12}, Vladimir Kolesnikov^{i6,a5}, Alex Malozemoff^{i7,a7}, Samuel Ranellucci^{i8,a13}, Mike Rosulek^{i9,a4}, Lawrence Roy^{i10,a10}, Xiao Wang^{i11,a6}, Chenkai Weng^{i12,a8}, Kang Yang^{i13,a11}, Yu Yu^{i14,a1,a2}

Open Researcher and Contributor Identifiers (ORCID):

i1 (0000-0002-6203-413X); i2 (0000-0002-8520-6301); i3 (0000-0001-5295-2781); i4 (0000-0001-9589-5182); i5 (0000-0001-6084-9303); i6 (0000-0002-0211-1244); i7 (0009-0009-0744-2366); i8 (0009-0007-1429-6622); i9 (0009-0003-5206-6191); i10 (0009-0003-8436-0029); i11 (0000-0002-5991-7417); i12 (0000-0003-2436-9366); i13 (0000-0002-7453-4043); i14 (0000-0002-9278-4521)

Affiliations:

^{a1} School of Computer Science, Shanghai Jiao Tong University @ Shanghai, China

^{a2} Shanghai Qi Zhi Institute @ Shanghai, China

^{a3} School of Cyber Science and Technology, Shandong University @ Jinan, China

^{a4} School of Electrical Engineering and Computer Science, Oregon State University @ Corvallis, OR, USA

^{a5} School of Cybersecurity and Privacy, Georgia Institute of Technology @ Atlanta, GA, USA

^{a6} Department of Computer Science, Northwestern University @ Evanston, IL, USA

^{a7} Galois Inc. @ Portland, OR, USA

^{a8} School of Computing and Augmented Intelligence, Arizona State University @ Tempe, AZ, USA

^{a9} Siebel School of Computing and Data Science, University of Illinois Urbana-Champaign @ Urbana, IL, USA

^{a10} Aarhus University @ Aarhus, Denmark

^{a11} State Key Laboratory of Cryptology @ Beijing, China

^{a12} Google @ USA

^{a13} Coinbase @ Canada

Main contacts:

- **Team mailing list:** minimpc@googlegroups.com
- **Primary technical contact person:** Xiao Wang, wangxiao1254@gmail.com

Produced by humans. The team hereby confirms that the content in this preview writeup: (i) was produced by the team members, and (ii) was not produced by generative artificial intelligence (AI), with the possible exception of AI-proposed grammar improvements, minor integrated suggestions, or some well-identified and short localized portions of auxiliary content (e.g., some illustration); and (iii) was proofread by the team members.

1. Introduction

This submission aims to provide a suite of cryptographic protocols for evaluating any Boolean circuit with practical efficiency. The proposed protocols assume a small set of base oblivious transfers already executed among parties, and they only require MiniCrypt primitives in the subsequent computation. As such, the proposed building blocks can all be instantiated securely using NIST-approved primitives and can perform flexible modes of threshold operations for all NIST-approved symmetric-key primitives. We believe the proposed building blocks in this submission will also have independent application in practical protocols for secure multi-party computation.

In more detail, the proposed submission includes 1) definition and constructions of correlation-robust hash functions with simulation security, 2) correlated oblivious transfer (OT) extension, 3) authenticated Boolean Beaver triples, and 4) authenticated garbling for evaluating any Boolean circuit, all constructed assuming an ideal cipher and a random oracle. We plan to provide details of the protocol, proof, implementation, and evaluation in our final submission.

The overall protocol targets categories N3 and S3 (Symmetric). Some building blocks can fall in category S7 (Gadgets).

2. Specification

2.1. Organization

From a high-level view, our proposed system takes a small number of oblivious transfer correlations and builds a protocol for securely evaluating any Boolean circuit with active security. Each component of our proposed system only requires MiniCrypt tools (e.g., ideal cipher, random oracle, and PRG). By leaving out the initial oblivious transfer correlations, we allow for a flexible choice of computational assumptions between classical assumptions (e.g., DDH) and post-quantum assumptions (e.g., LWE). Our proposed system includes four modular building blocks:

1. **Correlation-robust (CR) hash functions for simulation security.** In this part, we built upon prior works from the team [GKWY20; GKWWY20; GWYY25] and extended them so that they can be used as a modular component in higher-level protocols. Details of this new definition can be found in a recent technical report [CGGWYY25]. In particular, we proposed a new definition for a correlation robust hash function that comes with a simulator so that it can be securely composed with other protocols for simulation security in both the standalone model [Can00] and the universal composability model [Can01]. In this submission, we will use a block-cipher-based construction that can be proven secure in the ideal-cipher model. It would be instantiated using the NIST-approved AES block cipher.
2. **Oblivious transfer extension in MiniCrypt.** To preserve the conservativeness of assumptions in the suite of protocols presented in our submission, this part includes the state-of-the-art oblivious transfer (OT) extension protocol based solely on symmetric-key primitives [Roy22], which improves the IKNP OT extension [IKNP03].

3. **Authenticated Boolean Beaver Triples.** This part includes protocols that transform correlated oblivious transfer of independent values into authenticated Boolean Beaver Triples. Based on a long series of prior works [NNOB12; FKOS15; WRK17a; WRK17b; KRRW18; YWZ20; BLNNOOSS21], we further 1) incorporated an optimization to reduce memory movement during the bucketing process, 2) replaced random oracle to the above CR hash function for improved efficiency, and 3) provided a detailed end-to-end proof with concrete security loss.
4. **Authenticated Garbling.** This part includes protocols for authenticated garbling [WRK17a; WRK17b; KRRW18; YWZ20; CWYY23] built on top of the above protocols with random oracles replaced by the above CR hash functions for improved efficiency. We further incorporated a row-reduction optimization from [DIL02].

The flexibility of a general framework allows us to support various input/output patterns. Furthermore, one can evaluate any Boolean circuit on top of it. In this submission, we focus on symmetric-key primitives approved (N3) or not approved (S3) by NIST.

2.2. System Model

By default, we assume a set of parties holding a secret sharing of the private/signing key. For other inputs and outputs, our protocol supports secret-shared input (SSI) and secret-shared output (SSO). We assume a synchronous network.

The proposed protocol requires a random oracle, an ideal cipher, and the availability of a small number of oblivious transfer correlations for further OT extension. The initial set of OT correlation is out of the scope of this submission and could require more trusted setups. The proposed protocol always assumes that all-but-one parties can be corrupted, i.e., $f = n - 1$. The protocol could support any number of parties (n), and we plan to benchmark for at least up to $n = 32$ parties.

2.3. Security

Our protocol can be proven secure in the UC paradigm, assuming a static, active adversary corrupting up to all but one party. It achieves security with abort and assumes a synchronous network in our proof. We plan to examine security against adaptive adversaries and/or in the asynchronous setting, though it is not clear if our protocol can be proven secure in these settings without reducing its efficiency. Our proof targets concrete security, and we expect to achieve $\kappa - O(1)$ bits of computational security when using κ -bit strings for garbled labels.

3. Open-Source Implementation

3.1. Code structure

We will have two implementations: (1) an implementation of the multi-party authenticated garbling protocol in C++ as part of EMP-toolkit (<https://github.com/emp-toolkit>), and (2) an implementation of the two-party authenticated garbling protocol in Rust as part of Swanky (<https://github.com/GaloisInc/swanky>).

For (1), the majority of the code will be written in C++, built with CMake, and compilable with the latest versions of Clang and GCC. It will provide individual modules for each of the above four parts of the protocol, with the intention that other submissions (e.g., ones with OT extension using other assumptions) could drop in easily. The code only requires static linking of OpenSSL, and we will bundle a version of SSE2NEON for compatibility on ARM platforms.

For (2), the code will be written in Rust. As above, it will provide individual modules for each component of the protocol.

3.2. Code progress and availability

The code is still under development. There is currently no early version for testing. However, the code is partially based on and improved upon the EMP-toolkit available on GitHub.

3.3. Implementation of the networking model

Our protocol works in the security-with-abort model and hence does not need a full-blown broadcast. However, we implement an echo broadcast for our protocol. Our protocol assumes an authenticated channel; we plan to address this in our implementation.

4. Experimental Performance Evaluation

We do not have performance numbers reportable from our current implementation yet. We expect the end-to-end performance to be better than that reported in [WRK17a; WRK17b; YWZ20].

5. Licensing, Patent Claims, and Funding

5.1. Licenses

We plan to release our code under the MIT or the Apache License. Our implementation statically links to `OpenSSL`, which is under the Apache v2 License. The implementation on ARM CPUs further depends on `sse2neon`, which is under the MIT license.

5.2. Related Patent

The team is not aware of any active or provisional patent that overlaps with the content in this submission.

5.3. Funding Acknowledgment

Yu Yu is supported by the National Natural Science Foundation of China (Grant Nos. 92270201 and 62125204). Chun Guo is supported by the National Natural Science Foundation of China (Grant 62372274). David Heath is supported in part by NSF award CNS-2246353. Vladimir Kolesnikov is supported in part by NSF awards CNS-2246354 and CCF-2217070. Mike Rosulek is supported in part by NSF award CNS-2150726. Lawrence Roy is supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under grant agreement number 101124977 (DECRYPSIS). Xiao Wang is supported in part by NSF CNS-2236819.

References

- [BLNNOOSS21] Sai Sheshank Burra, Enrique Larraia, Jesper Buus Nielsen, Peter Sebastian Nordholt, Claudio Orlandi, Emmanuela Orsini, Peter Scholl, and Nigel P. Smart. “High-Performance Multi-party Computation for Binary Circuits Based on Oblivious Transfer”. In: *Journal of Cryptology* 34.3 (July 2021), p. 34. DOI: [10.1007/s00145-021-09403-1](https://doi.org/10.1007/s00145-021-09403-1). Also at ia.cr/2015/472.
- [Can00] Ran Canetti. “Security and Composition of Multiparty Cryptographic Protocols”. In: *Journal of Cryptology* 13.1 (January 2000), pp. 143–202. DOI: [10.1007/s001459910006](https://doi.org/10.1007/s001459910006). Also at ia.cr/1998/018.
- [Can01] Ran Canetti. “Universally Composable Security: A New Paradigm for Cryptographic Protocols”. In: *42nd FOCS*. IEEE Computer Society Press, October 2001, pp. 136–145. DOI: [10.1109/SFCS.2001.959888](https://doi.org/10.1109/SFCS.2001.959888). Also at ia.cr/2000/067.
- [CGGWYY25] Hongrui Cui, Chun Guo, Xiaojie Guo, Xiao Wang, Kang Yang, and Yu Yu. *Simulation-based Security Notion of Correlation Robust Hashing with Applications to MPC*. Cryptology ePrint Archive, Paper 2025/1818. 2025. URL: <https://eprint.iacr.org/2025/1818>.
- [CWYY23] Hongrui Cui, Xiao Wang, Kang Yang, and Yu Yu. “Actively Secure Half-Gates with Minimum Overhead Under Duplex Networks”. In: *EUROCRYPT 2023, Part II*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14005. LNCS. Springer, Cham, April 2023, pp. 35–67. DOI: [10.1007/978-3-031-30617-4_2](https://doi.org/10.1007/978-3-031-30617-4_2). Also at ia.cr/2023/278.
- [DIL022] Samuel Dittmer, Yuval Ishai, Steve Lu, and Rafail Ostrovsky. “Authenticated Garbling from Simple Correlations”. In: *CRYPTO 2022, Part IV*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13510. LNCS. Springer, Cham, August 2022, pp. 57–87. DOI: [10.1007/978-3-031-15985-5_3](https://doi.org/10.1007/978-3-031-15985-5_3). Also at ia.cr/2022/836.
- [FKOS15] Tore Kasper Frederiksen, Marcel Keller, Emmanuela Orsini, and Peter Scholl. “A Unified Approach to MPC with Preprocessing Using OT”. In: *ASIACRYPT 2015, Part I*. Ed. by Tetsu Iwata and Jung Hee Cheon. Vol. 9452. LNCS. Springer, Berlin, Heidelberg, November 2015, pp. 711–735. DOI: [10.1007/978-3-662-48797-6_29](https://doi.org/10.1007/978-3-662-48797-6_29). Also at ia.cr/2015/901.
- [GKWWY20] Chun Guo, Jonathan Katz, Xiao Wang, Chenkai Weng, and Yu Yu. “Better Concrete Security for Half-Gates Garbling (in the Multi-instance Setting)”. In: *CRYPTO 2020, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. LNCS. Springer, Cham, August 2020, pp. 793–822. DOI: [10.1007/978-3-030-56880-1_28](https://doi.org/10.1007/978-3-030-56880-1_28). Also at ia.cr/2018/578.
- [GKWY20] Chun Guo, Jonathan Katz, Xiao Wang, and Yu Yu. “Efficient and Secure Multiparty Computation from Fixed-Key Block Ciphers”. In: *2020 IEEE Symposium on Security*

- and Privacy*. IEEE Computer Society Press, May 2020, pp. 825–841. DOI: [10.1109/SP40000.2020.00016](https://doi.org/10.1109/SP40000.2020.00016). Also at ia.cr/2019/074.
- [GWYY25] Chun Guo, Xiao Wang, Kang Yang, and Yu Yu. “On tweakable correlation robust hashing against key leakages”. In: *Designs, Codes and Cryptography* (2025), pp. 1–38. DOI: [10.1007/s10623-025-01641-9](https://doi.org/10.1007/s10623-025-01641-9). Also at ia.cr/2024/163.
- [IKNP03] Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. “Extending Oblivious Transfers Efficiently”. In: *CRYPTO 2003*. Ed. by Dan Boneh. Vol. 2729. LNCS. Springer, Berlin, Heidelberg, August 2003, pp. 145–161. DOI: [10.1007/978-3-540-45146-4_9](https://doi.org/10.1007/978-3-540-45146-4_9). Also at <https://www.iacr.org/archive/crypto2003/27290145/27290145.pdf>.
- [KRRW18] Jonathan Katz, Samuel Ranellucci, Mike Rosulek, and Xiao Wang. “Optimizing Authenticated Garbling for Faster Secure Two-Party Computation”. In: *CRYPTO 2018, Part III*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10993. LNCS. Springer, Cham, August 2018, pp. 365–391. DOI: [10.1007/978-3-319-96878-0_13](https://doi.org/10.1007/978-3-319-96878-0_13). Also at ia.cr/2018/578.
- [NNOB12] Jesper Buus Nielsen, Peter Sebastian Nordholt, Claudio Orlandi, and Sai Sheshank Burra. “A New Approach to Practical Active-Secure Two-Party Computation”. In: *CRYPTO 2012*. Ed. by Reihaneh Safavi-Naini and Ran Canetti. Vol. 7417. LNCS. Springer, Berlin, Heidelberg, August 2012, pp. 681–700. DOI: [10.1007/978-3-642-32009-5_40](https://doi.org/10.1007/978-3-642-32009-5_40). Also at ia.cr/2011/091.
- [Roy22] Lawrence Roy. “SoftSpokenOT: Quieter OT Extension from Small-Field Silent VOLE in the Minicrypt Model”. In: *CRYPTO 2022, Part I*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13507. LNCS. Springer, Cham, August 2022, pp. 657–687. DOI: [10.1007/978-3-031-15802-5_23](https://doi.org/10.1007/978-3-031-15802-5_23). Also at ia.cr/2018/578.
- [WRK17a] Xiao Wang, Samuel Ranellucci, and Jonathan Katz. “Authenticated Garbling and Efficient Maliciously Secure Two-Party Computation”. In: *ACM CCS 2017*. Ed. by Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu. ACM Press, October 2017, pp. 21–37. DOI: [10.1145/3133956.3134053](https://doi.org/10.1145/3133956.3134053). Also at ia.cr/2017/030.
- [WRK17b] Xiao Wang, Samuel Ranellucci, and Jonathan Katz. “Global-Scale Secure Multiparty Computation”. In: *ACM CCS 2017*. Ed. by Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu. ACM Press, October 2017, pp. 39–56. DOI: [10.1145/3133956.3133979](https://doi.org/10.1145/3133956.3133979). Also at ia.cr/2017/189.
- [YWZ20] Kang Yang, Xiao Wang, and Jiang Zhang. “More Efficient MPC from Improved Triple Generation and Authenticated Garbling”. In: *ACM CCS 2020*. Ed. by Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna. ACM Press, November 2020, pp. 1627–1646. DOI: [10.1145/3372297.3417285](https://doi.org/10.1145/3372297.3417285). Also at ia.cr/2019/1104.
- [NIST-IR8214C] Luís T. A. N. Brandão and René Peralta. *NIST First Call for Multi-Party Threshold Schemes*. (National Institute of Standards and Technology) NIST Internal Report (NISTIR) 8214C. 2026. DOI: [10.6028/NIST.IR.8214C](https://doi.org/10.6028/NIST.IR.8214C).