HE-Based On-the-Fly MPC, Revisited

Universal Composability, Approximate/Imperfect Computation, Circuit Privacy

Ganyuan Cao
ganyuan.cao@telecom-paris.fr

Sylvain Chatel
sylvain.chatel@cispa.de

Christian Knabenhans
christian.knabenhansl@epfl.ch

Motivation & Background

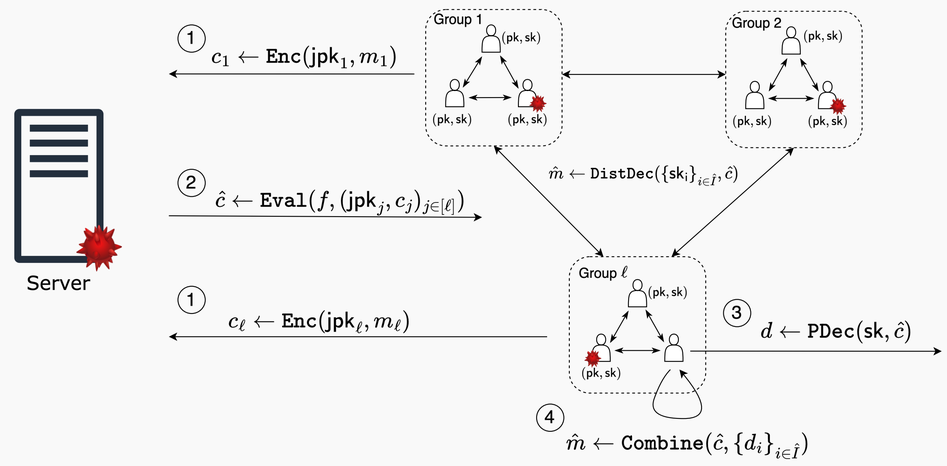
On-the-Fly Multi-Party Computation (OtF-MPC) enables clients to dynamically join a computation without remaining continuously online. OtF-MPC can be realized from multi-party homomorphic encryption, to compute over data encrypted under different keys, combined with non-interactive proofs (NIZKs / zkSNARKs) for verifiability of computation.

Table: A comparison of existing compilers for (on-the-fly) MPC from HE. ●: discussed and analyzed in detail; ◎: informally analyzed or with gaps in the security proof; ○: not considered.

	Imperfect/Approx. HE	Circuit Privacy	(t, n)-Threshold	Composablility
[LTV12]	○	○	○	○
[AJL+12]	●	○	●	◎
[MW16]	○	○	○	◎
[MTBH21]	◎	○	◎	○
[HHK+25]	●	○	◎	○
This Work	●	●	●	●

Security Gaps: existing compilers and security proofs [LTV12] for on-the-fly MPC

- are *not composable*;
- do not handle *threshold* or *multi-group* settings;
- do not capture *approximate* and *imperfect* computations.
- do not model *circuit privacy* for server-side privacy.



Our Contributions:

1. First UC functionality for multi-group HE (MGHE), with imperfect or approximate computation, circuit privacy, and threshold decryption.
2. New security notions for MGHE, capturing client/server privacy, and threshold security under imperfect or approximate computation.
3. Generic compilers for OtF-MPC against malicious adversaries.

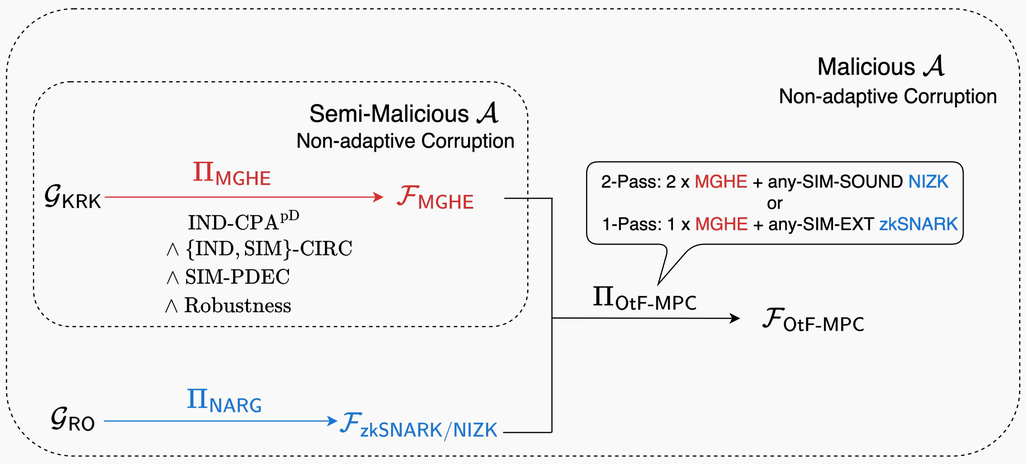


Figure: Roadmap of realizing OtF-MPC; Confidential layer with MGHE that is realizable if the security notions are satisfied; Integrity Layer with zkSNARK/NIZK through verifiability. Two compilers for OtF-MPC that composes MGHE with either any-simulation-sound NIZK or any-simulation-extractable zkSNARK.

Contribution 1: First UC Functionality for Multi-Group HE

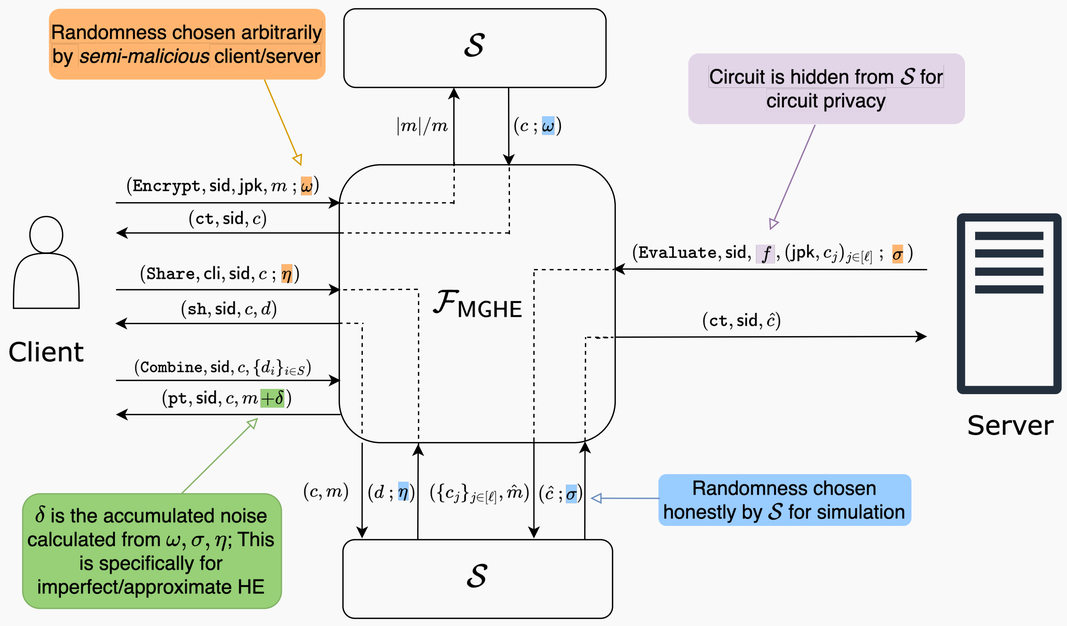


Figure: Illustration of interfaces in $\mathcal{F}_{\text{MGHE}}$.

Contribution 2: New Security Notions for MGHE

For our notions, we consider a *semi-malicious* adversary, who is allowed to choose randomness for the protocol, that *non-adapatively* corrupts a subset of clients and possibly the server.

- *IND-CPA^{pD}* for *Client Privacy*: we allow the adversary to set the randomness for *any* part of the protocol execution. This captures scenarios where both clients and the server are corrupted.

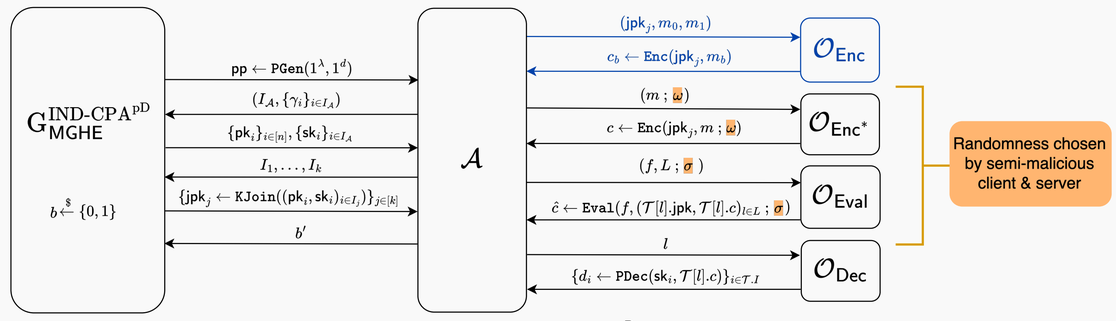


Figure: Illustration of *IND-CPA^{pD}* game for MGHE.

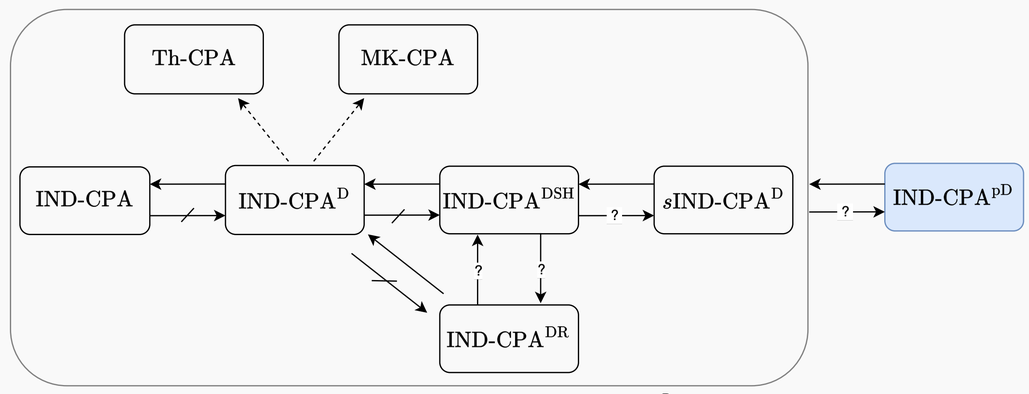


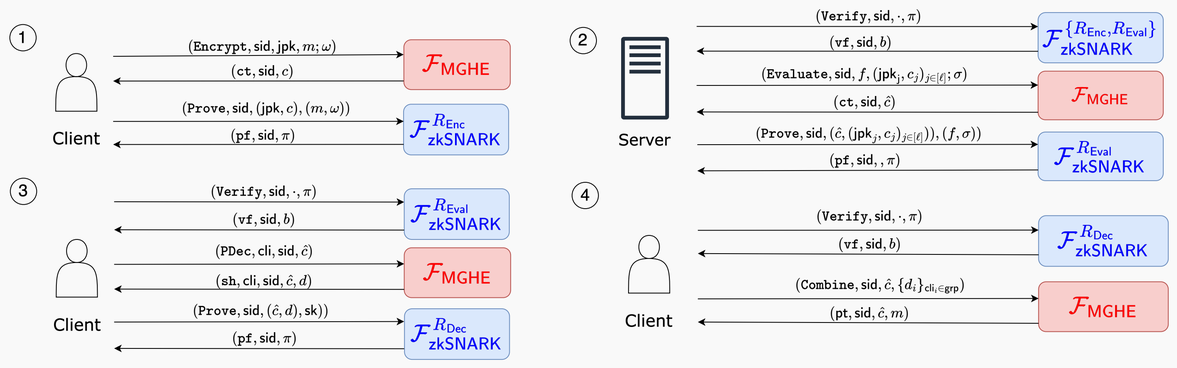
Figure: The relations between our notion *IND-CPA^{pD}* and existing notions.

- $\{SIM, IND\}$-*CIRC* for *Server Privacy*: we examine both simulation-based and game-based formalizations for exact/approximate and perfect/imperfect HE.
- *Threshold Security*: we justify the need for simulatability of decryption share (*SIM-PDEC*) along with *IND-CPA^{pD}* security for MGHE. We also introduce a notion of *robustness*, extending the existing notions to address security under HE evaluation.

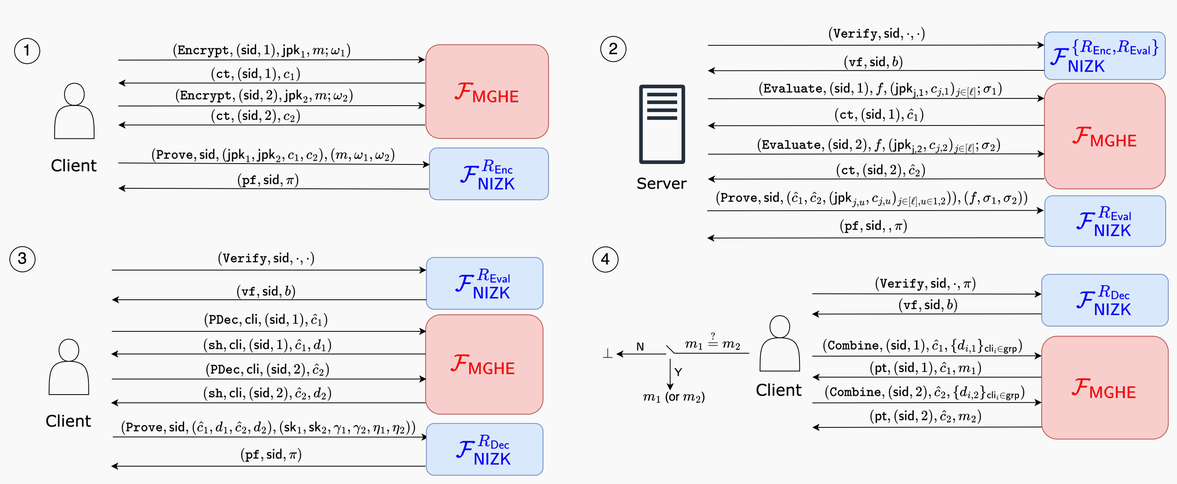
Contribution 3: Compiling MGHE for Malicious Security

We present two compilers that lift MGHE into an on-the-fly MPC protocol against a fully *malicious* adversary that *non-adapatively* corrupts a subset of clients and possibly the server.

- Compiler 1: Single-Encryption with *Any-Simulation-Extractable* zkSNARK



- Compiler 2: Double-Encryption with *Any-Simulation-Sound* NIZK



Gilad Asharov, Abhishek Jain, Adriana López-Alt, Eran Tromer, Vinod Vaikuntanathan, and Daniel Wichs.
Multiparty computation with low communication, computation and interaction via threshold FHE.
In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 483–501. Springer, Berlin, Heidelberg, April 2012.
doi:10.1007/978-3-642-29011-4_29.

Intak Hwang, Yisol Hwang, Miran Kim, Dongwon Lee, and Yongsoo Song.
Provably secure approximate computation protocols from CKKS.
Cryptology ePrint Archive, Report 2025/395, 2025.
URL: https://eprint.iacr.org/2025/395.

Adriana López-Alt, Eran Tromer, and Vinod Vaikuntanathan.
On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption.
In Howard J. Karloff and Toniann Pitassi, editors, *44th ACM STOC*, pages 1219–1234. ACM Press, May 2012.
doi:10.1145/2213977.2214086.

Christian Mouchet, Juan Ramón Troncoso-Pastoriza, Jean-Philippe Bossuat, and Jean-Pierre Hubaux.
Multiparty homomorphic encryption from ring-learning-with-errors.
PoPETs, 2021(4):291–311, October 2021.
doi:10.2478/popets-2021-0071.

Pratyay Mukherjee and Daniel Wichs.
Two round multiparty computation via multi-key FHE.
In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 735–763. Springer, Berlin, Heidelberg, May 2016.
doi:10.1007/978-3-662-49896-5_26.