INSTITUT
DE RECHERCHE
EN INFORMATIQUE
FONDAMENTALE

Université Paris Cité | cnrs

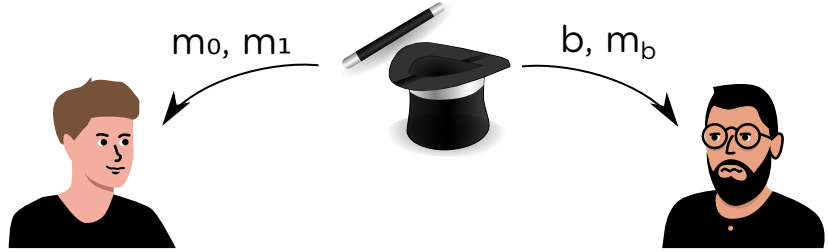
secorvo
security consulting

Pseudorandom Correlation Functions for Garbled Circuits

Theory of Cryptography Conference, TCC 2025 | Aarhus, Denmark

Geoffroy Couteau, Srinivas Devadas, Alexander Koch, Sacha Servan-Schreiber | 2025-11-03

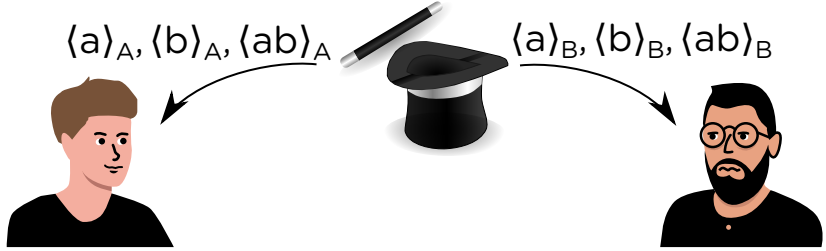
MPC with Correlated Randomness: Random-OT



online:

Efficient online protocol

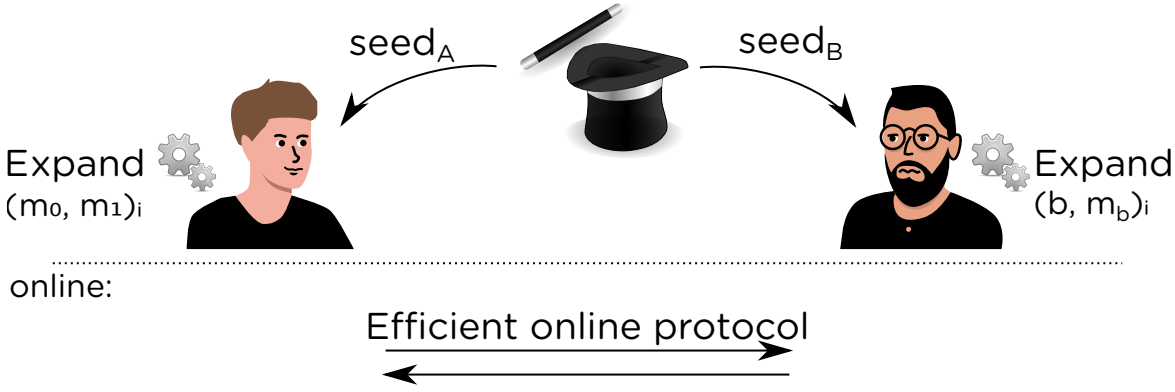
MPC with Correlated Randomness: Beaver-Triples



online:

Efficient online protocol

MPC with Correlated Randomness: using PCGs



MPC with Correlated Randomness: using PCFs

online:

$(m_0, m_1)_i \leftarrow F(k_A, \cdot)$ Efficient online protocol $(b, m_b)_i \leftarrow F(k_B, \cdot)$

MPC with Correlated Randomness: using PCFs

online:

$(\langle \mathcal{C} \rangle_A, \langle \ell \rangle_A)_i \leftarrow F(k_A, \cdot)$ $\qquad$ $(\langle \mathcal{C} \rangle_B, \langle \ell \rangle_B)_i \leftarrow F(k_B, \cdot)$

Shared Garbled Circuit Correlation

Objective: PCFs for the Garbled Circuit Correlation

What?

- after brief preprocessing (generating correlated PCF keys) …
- … allows 2 parties to generate an unbounded number of correlated pairs, i.e. additive shares of a garbled circuit and labels

Why?

- PCFs are a nice way to approach MPC in the correlated randomness model
- The Garbled Circuit correlation enables applications (next), not known without.

Objective: PCFs for the Garbled Circuit Correlation

What?

- after brief preprocessing (generating correlated PCF keys) ...
- ... allows 2 parties to generate an unbounded number of correlated pairs, i.e. additive shares of a garbled circuit and labels

Why?

- PCFs are a nice way to approach MPC in the correlated randomness model
- The Garbled Circuit correlation enables applications (next), not known without.

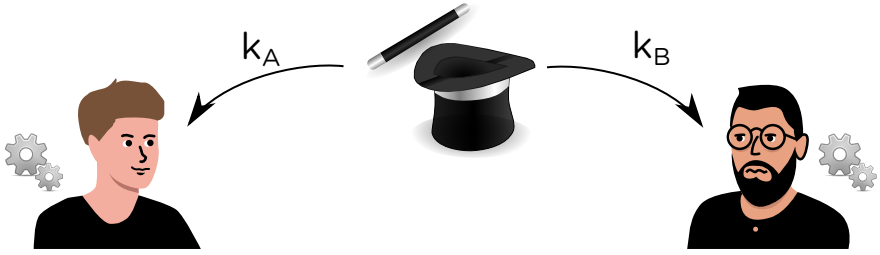
Ingredient: Secret-Sharing-Friendly Garbled Circuits

- BMR-style Garbled Circuits (known from multiparty garbling)
- For each gate entry with $a, b \in \{0,1\}$, we want:

$$\langle g_{ab} \rangle_A \oplus \langle g_{ab} \rangle_B = H(\ell^A_{i,a} \,\|\, \ell^A_{j,b}) \oplus H(\ell^B_{i,a} \,\|\, \ell^B_{j,b}) \oplus \rho_{ab} \,\|\, \ell^A_{k,\rho_{ab}} \,\|\, \ell^B_{k,\rho_{ab}}$$

Application 1: Non-Interactive Secure Computation

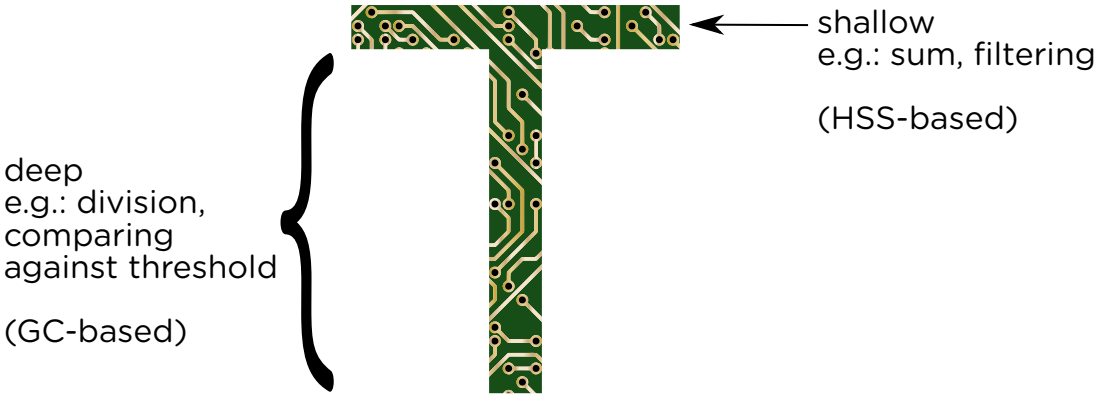
2-round online phase with result reconstructable from bulletin board (semi-honest)



Recap: Homomorphic Secret Sharing (HSS)

- HSS schemes allow to locally evaluate functions on shares, s.t. the resulting shares of the output are short (i.e. featuring “optimal download rate”)
- Only useful for shallow circuits (Exponential cost in the circuit depth)

Application 2: Many Interesting Circuits are T-Shaped



More Specific: Scientific Studies using HSS

And function access control using keys ak that are published, for reproducibility

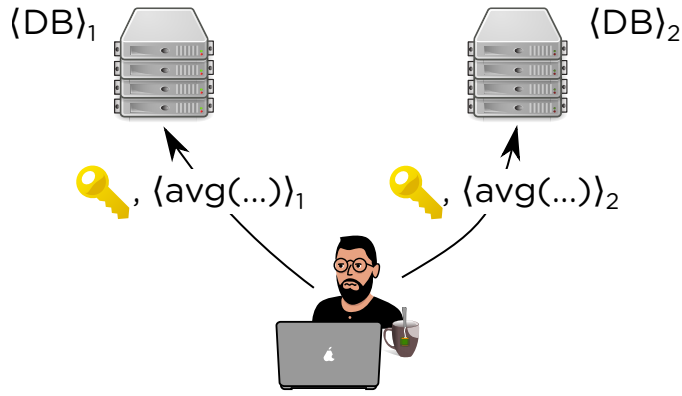


Image “server multiple” by RRZE, CC BY-SA 3.0

More Specific: Scientific Studies using HSS

And function access control using keys ak that are published, for reproducibility

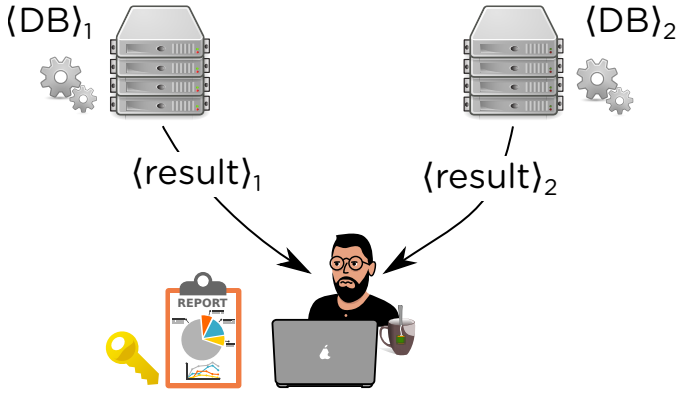


Image “server multiple” by RRZE, CC BY-SA 3.0

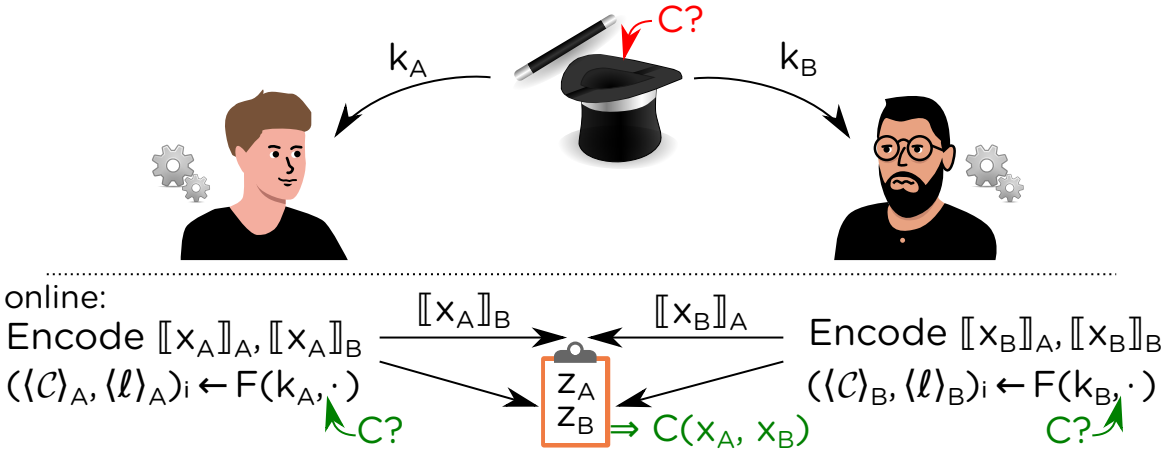
T-Shaped Circuit Savings

	Basic HSS	Our framework
Comm.	$O(k)$	$O(k \cdot d)$
Comp.	$O(n \cdot 2^d)$	$O(n + k \cdot d)$

Input sizes, top part: n, stem part: k, depth: d

Caveat: Our HSS scheme has non-additive reconstruction (garbled circuit evaluation).

Issue: Circuit fixed in advance



Intuition on Construction

We can write the Garbled Circuit correlation as a degree-2 correlation, together with things that parties can compute locally („hashes of labels“)

Issue: Doing this naively fixes the circuit topology.
In the paper: Topology-Adaptive Pseudorandom Correlation Functions (TAPCFs) for Degree-2 Correlations. This allows us to specify the circuit on the fly.

Also there: TAPCFs for “Silent secure computation with function-dependent preprocessing” (to save on bits per AND gate).

And: a relatively efficient construction based on the Expand-Accumulate LPN Assumption (~ 1 GC/sec, for GCs with 10,000 AND gates)