SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Computational Irrelevancy: Bridging the Gap between Pseudo- and Real Randomness in MPC Protocols

Nariyasu Heseri [*] Koji Nuida [†]

Keywords: secure multiparty computation, MPC, pseudorandom generators, PRG, relativisation

Abstract

Due to the fact that classical computers cannot efficiently obtain random numbers, it is common practice to design cryptosystems in terms of real random numbers and then replace them with (cryptographically secure) pseudorandom ones for concrete implementations.

However, as pointed out by [1], this technique may lead to compromise of security in secure multiparty computation (MPC) protocols. Although this work suggests using information-theoretically secure protocols and pseudorandom generators (PRGs) with high min-entropy to alleviate the problem, yet it is preferable to base the security on computational assumptions rather than the stronger information-theoretical ones.

By observing that the contrived constructions in the aforementioned work use MPC protocols and PRGs that are closely related to each other, we notice that it may help to alleviate the problem by using protocols and PRGs that are "unrelated" to each other. In this paper, we propose a notion called "computational irrelevancy" to formalise the term "unrelated" and under this condition provide a security guarantee under computational assumptions.

Main Theorems

Definition 1. Let π be an n-party protocol. We say π is secure against party $\mathcal{P}_i$ *relative to* $\mathcal{O} = \{\mathcal{O}_i\}_{i \in I} \subset \mathcal{PTM}$ if $\exists \mathcal{S} \in \mathcal{PPT}$ s.t. $\forall \mathcal{D} \in \mathcal{NUPPT}$,

$$\left|\Pr\left[\mathcal{D}^{\mathcal{O}}\left(\mathcal{S}(1^{\lambda}, x_i, f_i(\vec{x})), \vec{f}(\vec{x})\right) = 1\right] - \Pr\left[\mathcal{D}^{\mathcal{O}}\left(x_i, r_i, \vec{m}_i(1^{\lambda}, \vec{x}; \vec{r}), \pi(1^{\lambda}, \vec{x}; \vec{r})\right) = 1\right]\right|$$

is negligible where $\mathcal{D}^{\mathcal{O}}$ means $\mathcal{D}$ is given oracle access to all $\mathcal{O}_i$.

Definition 2. Let π be an n-party protocol that is secure against $\mathcal{P}_i$ with simulator $\mathcal{S}$. We say $\mathcal{S}$ is with *raw randomness* if $\exists \mathcal{T} \in \mathcal{PPT}$, s.t. $\forall \lambda \in \mathbb{N}$,

$$\mathcal{S}(1^{\lambda}, x_i, f_i(\vec{x}); r_i, \tau_i) = \left\langle r_i, \mathcal{T}(1^{\lambda}, x_i, f_i(\vec{x}), r_i; \tau_i)\right\rangle$$

where the notation $\langle r_i, y\rangle$ means that components of the tuple (r_i, y) are rearranged such that r_i corresponds to the simulated random tape part.

Theorem 3. *Let π be an n-party protocol. Let $\mathcal{R}$ be a PRG and $\mathcal{I}_{\mathcal{R}}$ be its inverter. For $i \in \{1, 2, \ldots, n\}$, if*

- *π is secure against party $\mathcal{P}_i$ relative to $\mathcal{I}_{\mathcal{R}}$ with raw randomness.*
- *$\epsilon_1(\lambda) := \frac{|\mathrm{range}(\mathcal{R},\lambda)|}{2^{l_{out}(\lambda)}}$ is noticeable.*
- *$\mathcal{R}$ is non-uniformly indistinguishable in its range relative to $\mathcal{I}_{\mathcal{R}}$, i.e. any $\mathcal{NUPPT}$ algorithm cannot distinguish between the output of $\mathcal{R}$ and the uniform distribution over the range of $\mathcal{R}$'s output even given oracle access to $\mathcal{I}_{\mathcal{R}}$.*

then $\pi \circ_i \mathcal{R}$ is secure against party $\mathcal{P}_i$ relative to $\mathcal{I}_{\mathcal{R}}$ with raw randomness.

In this abstract, we only presented the result for the model of 1 adversary using a PRG, while similar results can be shown for 1 adversary with several PRGs used as well as for multiple colluding adversaries with multiple PRGs. For these results, in addition to the assumption that the protocol itself is computationally irrelevant to the PRGs used, we also added assumptions that PRGs are pairwise irrelevant or overall irrelevant respectively. We refer the reader to the full version of this paper for more detail.

References

[1] Koji Nuida. "Cryptographic Pseudorandom Generators Can Make Cryptosystems Problematic". In: *Public-Key Cryptography – PKC 2021*. Ed. by Juan A. Garay. Cham: Springer International Publishing, 2021, pp. 441–468. ISBN: 978-3-030-75248-4.

[*] Graduate School of Information Science and Technology, The University of Tokyo, nariyasu@g.ecc.u-tokyo.ac.jp

[†] Kyushu University / AIST, nuida@imi.kyushu-u.ac.jp