Algorithm $\mathsf{TmmoHash}_n(x)$

A fix-length-input and variable-length output hash constructed following the Tweakable Matyas-Meyer-Oseas (TMMO) construction from [GKWY20], using AES-128 in ECB mode as a permutation π, with $\kappa = 128$ bits. The first block uses an arbitrary initialization vector $IV \in \mathbb{Z}_2^\kappa$.

Inputs: $x \in \mathbb{Z}_2^\kappa$ an input of length κ bits
Outputs: $\boldsymbol{d} \in \mathbb{Z}_2^{n\times\kappa}$, a digest of length $n\kappa$ bits (n blocks of π)

1: $\pi.\mathsf{SetKey}(IV)$
2: **for** $i \in [n]$ **do**
3: $\quad y \leftarrow \pi.\mathsf{Encrypt}(x)$
4: $\quad z \leftarrow \pi.\mathsf{Encrypt}(y \oplus i)$
5: $\quad d_{(i)} \leftarrow z \oplus y$
6: $\quad \pi.\mathsf{SetKey}(d_{(i)})$
return $\boldsymbol{d}$

References

[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 (SP)*, pages 825–841. IEEE, 2020.