北京大学前沿计算研究中心
Center on Frontiers of Computing Studies, Peking University

静园5号院
青 年 讲 座

Correctness Amplification of Functional Encryption

Zehou Wu

Department of Computer Science
University of Waterloo

Host：刘天任 助理教授

2026年4月28日 星期二 15:00

静园五院204室

Abstract

Many cryptographic primitives are defined to allow non-negligible correctness error. When this error is non-negligibly less than one-half, standard parallel repetition techniques can reduce it to negligible levels. For all-or-nothing type primitives, such as attribute-based encryption, correctness can also be amplified whenever it holds with probability non-negligibly greater than that of uniformly guessing the underlying message.

However, these approaches fail in partial-decryption settings, such as functional encryption (FE). In particular, for FE schemes, the best known amplification techniques require correctness to hold with probability non-negligibly greater than one-half. This leaves a large gap when the underlying message space is exponentially large, as is the case with most FE schemes.

We present a generic method for boosting correctness across a broad class of FE schemes, provided that base correctness exceeds the probability of randomly guessing the message by a non-negligible margin. Our results apply to a wide range of FE schemes, including those supporting inner products and quadratic functions.

Biography

Zehou Wu is currently a PhD student in Computer Science at the University of Waterloo. Prior to that he received a Master’s Degree from University of Victoria. He received his Bachelor’s at the University of British Columbia. His research focuses on the intersect between cryptography and theoretical computer science.