979-8-3503-1894-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/FOCS57990.2023.00147

New York University
New York, USA
marshall@cs.nyu.edu

Cornell Tech
New York, USA
yl2866@cornell.edu

Cornell Tech
New York, USA
noammaz@gmail.com

Tel Aviv University & Cornell Tech
Tel Aviv, Israel & New York, USA
rafaelp@tau.ac.il

***Abstract*—Only a handful candidates for computational assumptions that imply secure key-agreement protocols (KA) are known, and even fewer are believed to be quantum safe. In this paper, we present a new hardness assumption—the *worst-case hardness* of a promise problem related to an *interactive* version of Kolmogorov Complexity. Roughly speaking, the promise problem requires telling apart tuples of strings (π, x, y) with relatively (w.r.t. $\mathsf{K}(\pi)$) low time-bounded *Interactive Kolmogorov Complexity* (IK^t), and those with relatively high Kolmogorov complexity, given the promise that $\mathsf{K}^t(x|y) < s, \mathsf{K}^t(y|x) < s$ and $s = \log n$, and where $\mathsf{IK}^t(\pi; x; y)$ is defined as the length of the shortest pair of t-bounded TMs (A, B) such that the interaction of (A, B) lead to the transcript π and the respective outputs x, y.**

We demonstrate that when t is some polynomial, then not only does this hardness assumption imply the existence of KA, but it is also *necessary* for the existence of secure KA. As such, it yields the first natural hardness assumption characterizing the existence of key-agreement protocols.

We additionally show that when the threshold s is bigger (e.g., $s = 55 \log n$), then the (worst-case) hardness of this problem instead characterizes the existence of one-way functions (OWFs). As such, our work also clarifies exactly what it would take to base KA on the existence of OWFs, and demonstrates that this question boils down to demonstrating a worst-case reduction between two closely

I. Introduction

The notion of a *key-agreement* (a.k.a. *key-exchange*) protocol, introduced by Diffie and Hellman [9] in their seminar paper "New Directions in Cryptography" from the 1976 ushered in a new era for Cryptography. Key Agreement (KA) protocols enable two parties—Alice and Bob—that have never previously met to use communication to establish a secret key (which later can be used to securely communicate), with the guarantee that an eavesdropper (referred to as Eve) who observes the transcript of communication between Alice and Bob cannot learn the secret key.

Key agreement protocols are perhaps the most important primitive enabling secure communication on the Internet—it is safe to say that a majority of electronic commerce applications would not be possible without secure key agreement protocols. However, despite the importance of key-exchange protocols, and so-called "public-key cryptography" in general (or "Cryptomania" in language of Impagliazzo [16]), we only know of a handful of candidate hard problems from which KA protocols can be constructed. More specifically, these

2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS) | 979-8-3503-1894-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/FOCS57990.2023.00147