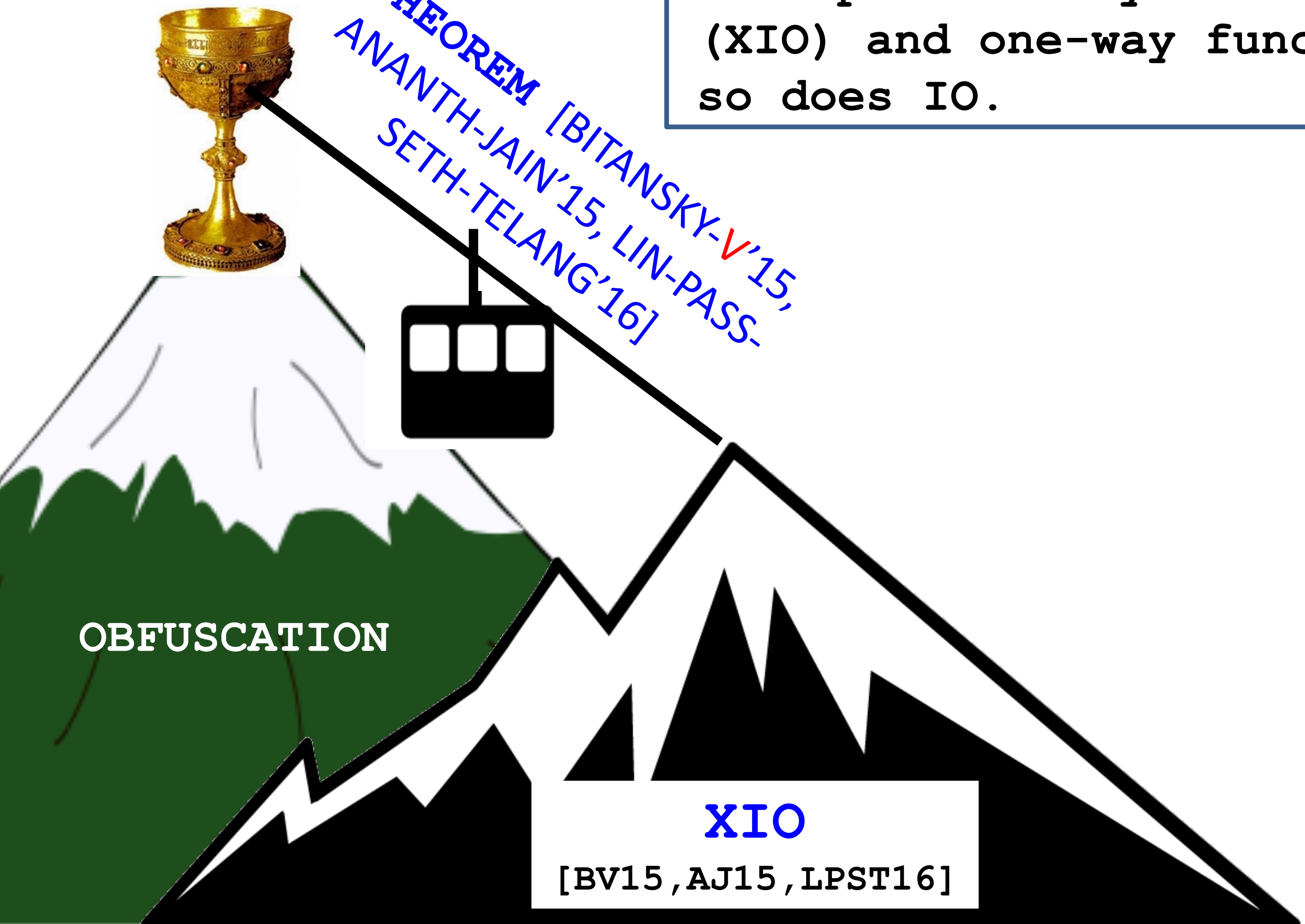
Constructing Program Obfuscators

[Garg-Gentry-Halevi-Raykova-Sahai-Waters'13]

Break, Fix, Break, Fix, …

Constructing Program Obfuscators

THEOREM 1:
If exponentially inefficient IO (XIO) and one-way functions exist, so does IO.



THEOREM [BITANSKY-V’15, ANANTH-JAIN’15, LIN-PASS-SETH-TELANG’16]

OBFUSCATION

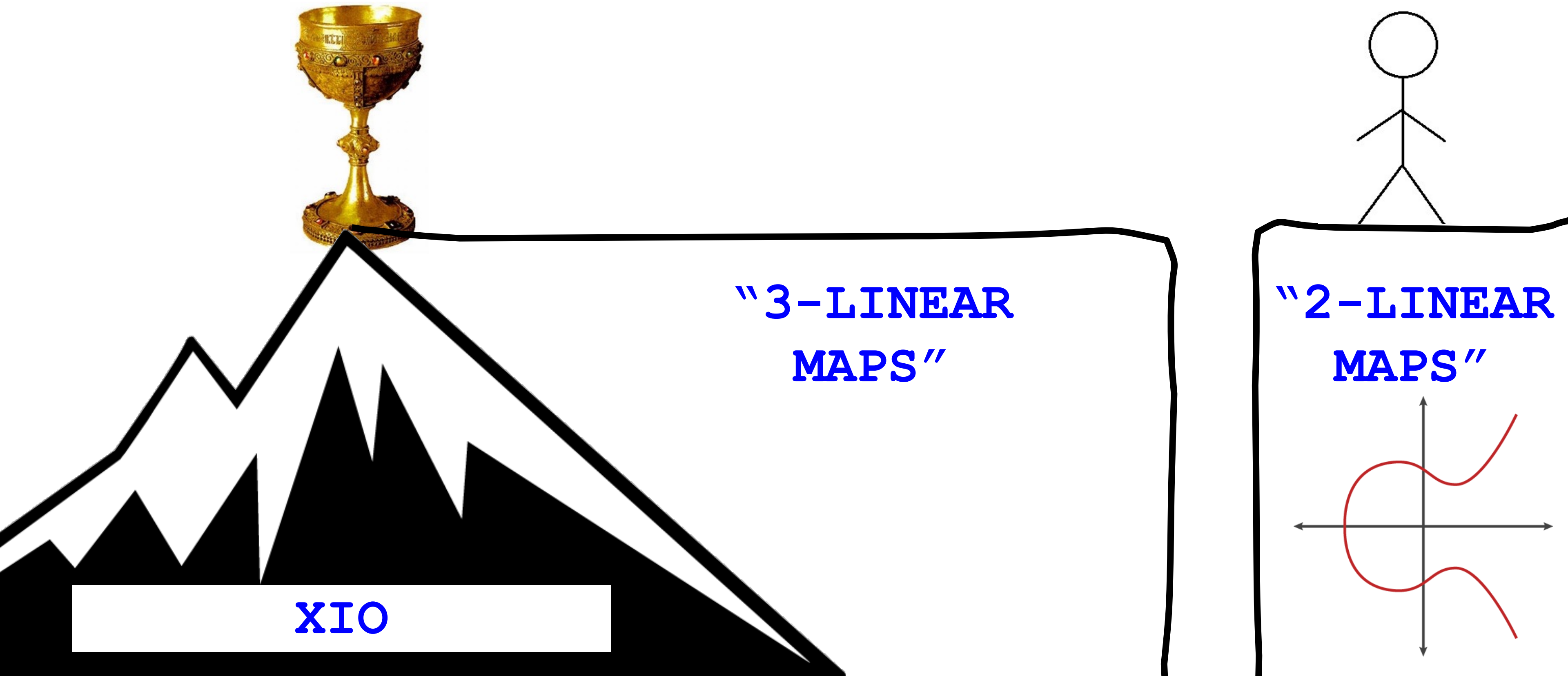
XIO

[BV15,AJ15,LPST16]

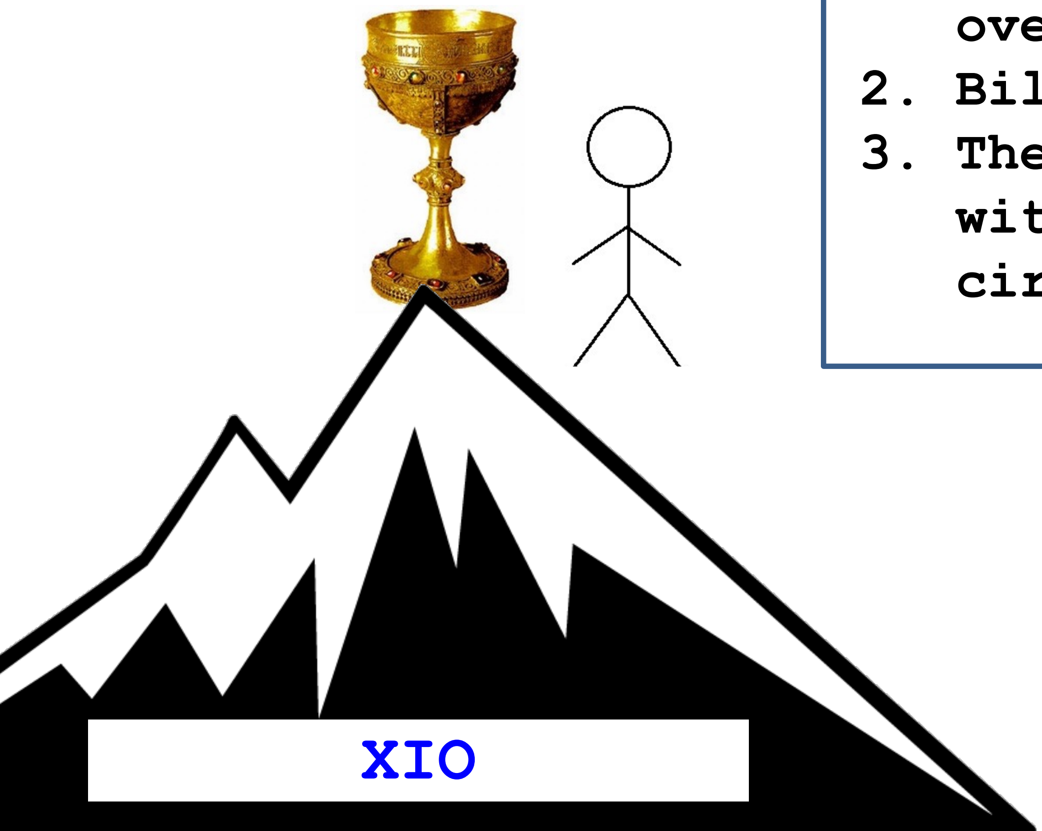
Constructing Program Obfuscators

THEOREM 1.5 [Lin-V’16, Lin’17, Ananth-Sahai’17, Lin-Tessaro’17]

If 3-linear maps exist*, so does XIO, and therefore, IO.



Constructing Program Obfuscators



THEOREM 2 [Jain-Lin-Sahai'21, '22]

XIO exists assuming that

1. Learning parity with noise over large fields is hard;
2. Bilinear maps exist ☺
3. There are PRGs computable with constant depth circuits.