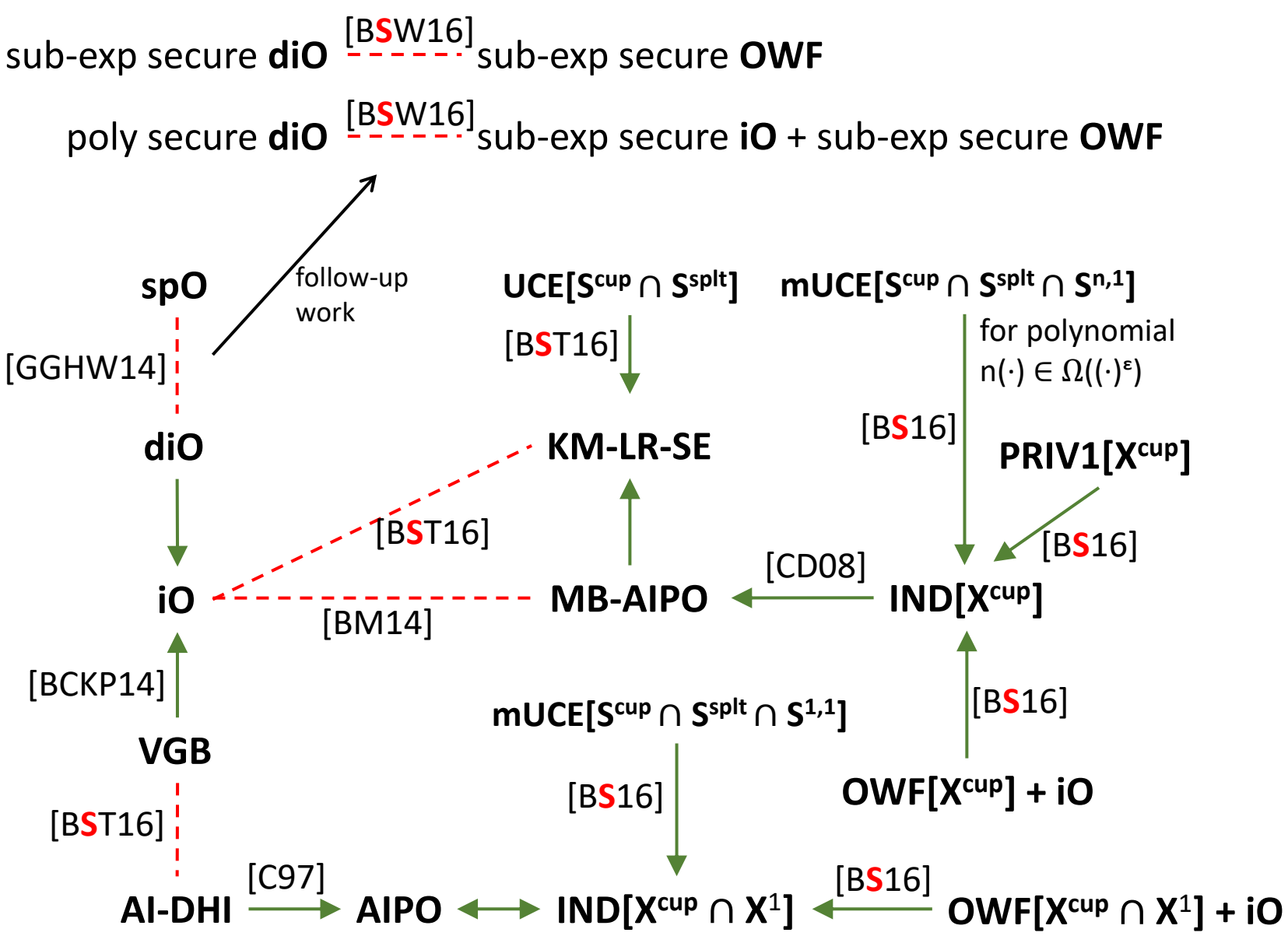
Selected Relations Between Obfuscation Notions

Implication: → Separation: - - -

Igors Stepanovs
August 25, 2017



Obfuscation Security Notions

iO – indistinguishability obfuscation
diO – differing-inputs obfuscation
VGB – Virtual-Grey Box obfuscation
AIPO – auxiliary input point-function obfuscation
MB-AIPO – multi-bit (output) **AIPO**
spO – special-purpose obfuscation
IND – indistinguishability of point-function obf.:
- $\mathbf{X}^{\mathbf{cup}}$ – computationally unpred. target points
- $\mathbf{X}^{1}$ – a single target point

Other Security Notions

AI-DHI – auxiliary input DH inversion
UCE – Universal Computational Extractors, standard-model assumption for random-oracle instantiation (**mUCE** is in multi-key setting):
- $\mathbf{S}^{\mathbf{cup}}$ – computationally unpred. sources
- $\mathbf{S}^{\mathbf{splt}}$ – split sources, leak on inp./out. separately
- $\mathbf{S}^{\mathbf{n,1}}$ – source uses n keys, one query per key

PRIV1 – single-key security of deterministic PKE for multiple users (with auxiliary information)
OWF – multi-key sec. of inj. OWF with aux. inf.
KM-LR-SE – key-message leakage-resilient symmetric encryption