Common Randomness Amplification: A Constructive View

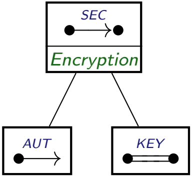
Grégory Demay and Ueli Maurer

ETH Zürich

September 3rd, 2012

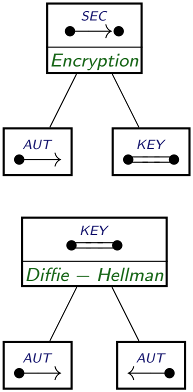
Composable Security Definitions Are Essential

Composable Constructions



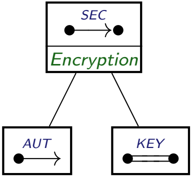
Composable Security Definitions Are Essential

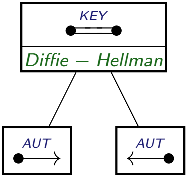
Composable Constructions

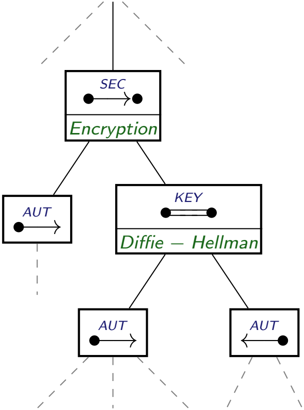


Composable Security Definitions Are Essential

Composable Constructions

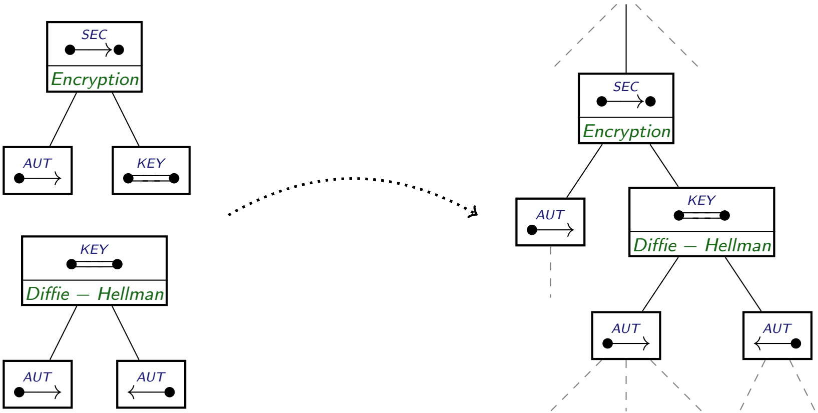






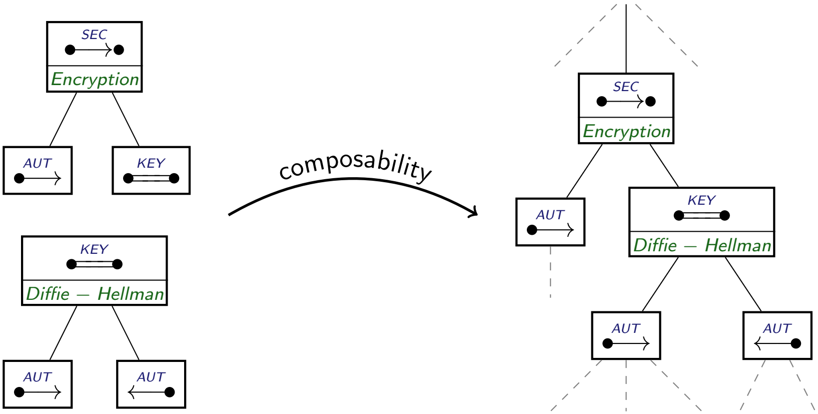
Composable Security Definitions Are Essential

Composable Constructions



Composable Security Definitions Are Essential

Composable Constructions

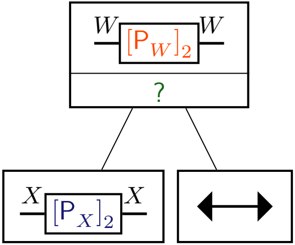


Secure Amplification of Common Randomness

- Can two *distrustful* parties create more common randomness than they initially share?

Secure Amplification of Common Randomness

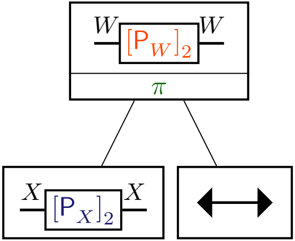
- Can two *distrustful* parties create more common randomness than they initially share?



and $H(W) > H(X)$

Secure Amplification of Common Randomness

- ~~Can two distrustful parties create more common randomness than they initially share?~~



$$\Longrightarrow H(W) \lessapprox H(X)$$

Thank You!