Flash Memory Summit

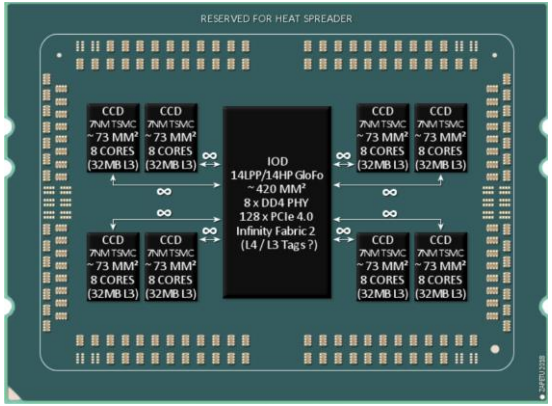
UCIe™ Chiplet Management & Security

Presenters:
Jérôme Glisse Manageability/Security Work Group Co-Chair and Engineer at Google

Peter Onufryk Manageability/Security Work Group Co-Chair and Intel Fellow at Intel

Why Chiplets?

- Chiplets enable construction of devices that exceed maximum reticle size
- Reuse of chiplets reduces device design time and cost
- Breaking a monolithic device into smaller chiplets improves silicon yield and reduces cost
- Chiplets manufactured using different semiconductor processes reduces device cost and enables greater levels of integration
- Use of chiplets designed by different teams/companies enables innovation to be scaled through specialization



AMD EPYC Rome

Eight compute chiplets in 7 nm

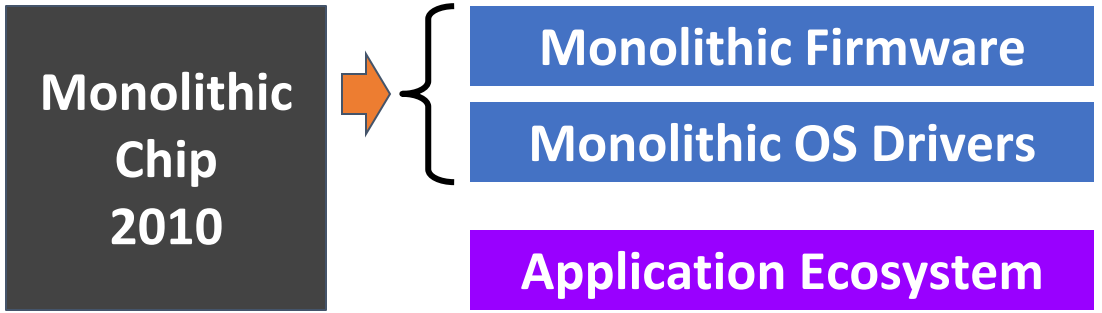
One I/O chiplet in 12 nm

Stage of Chiplet Ecosystem

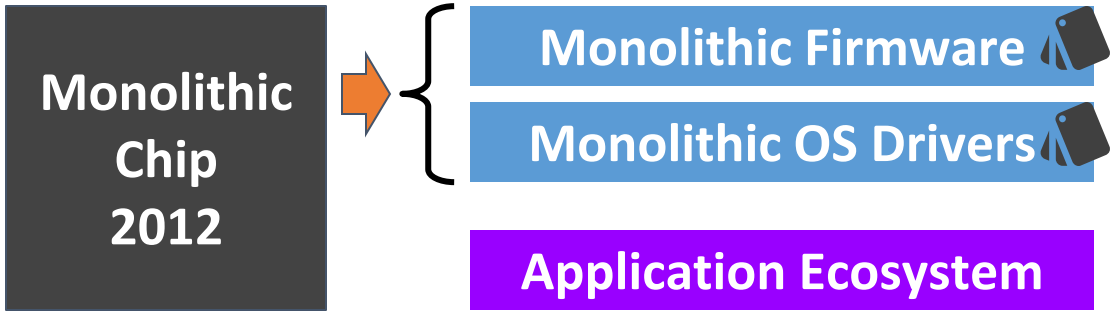
Monolithic Chip Management & Security

Flash Memory Summit

Monolithic Hardware
⇒ Monolithic Software

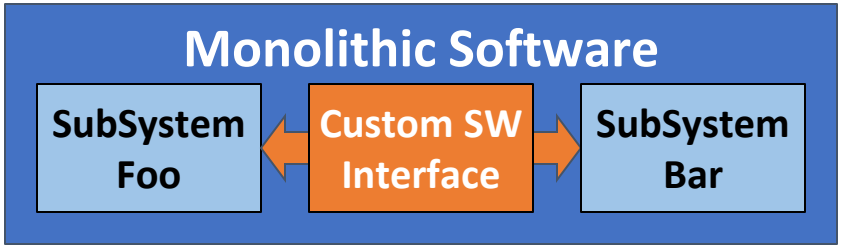


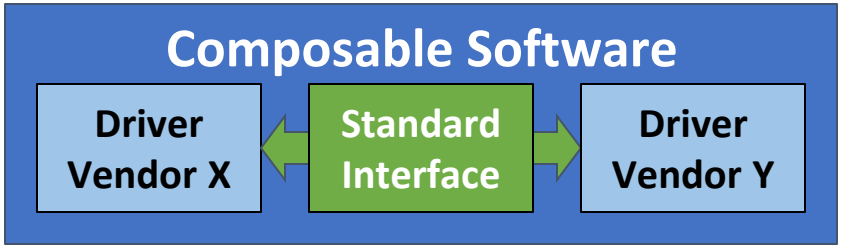
Update Hardware
⇒ Patch Software



Composable Chip⇒Composable Software

- Chiplet because we want High Velocity ⇒ Need Software Reuse
- Software Reuse ⇒ Standardize How to Compose Software
- Standardize at the protocol layer ⇒ How Chiplet Communicates
- Leverage existing industry standard such as one from DMTF ⇒ TTM



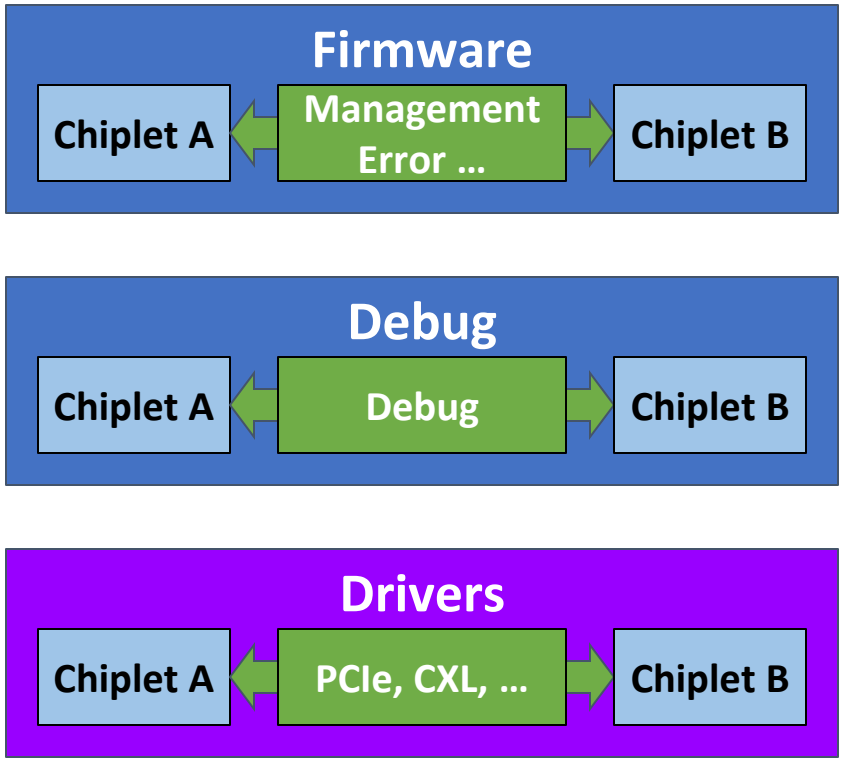


Software Composability at Every Levels

From Firmware
(low level Hardware Management)

Through Debug
(Standard debug interface, …)

To User facing Software
(Drivers, Frameworks, …)



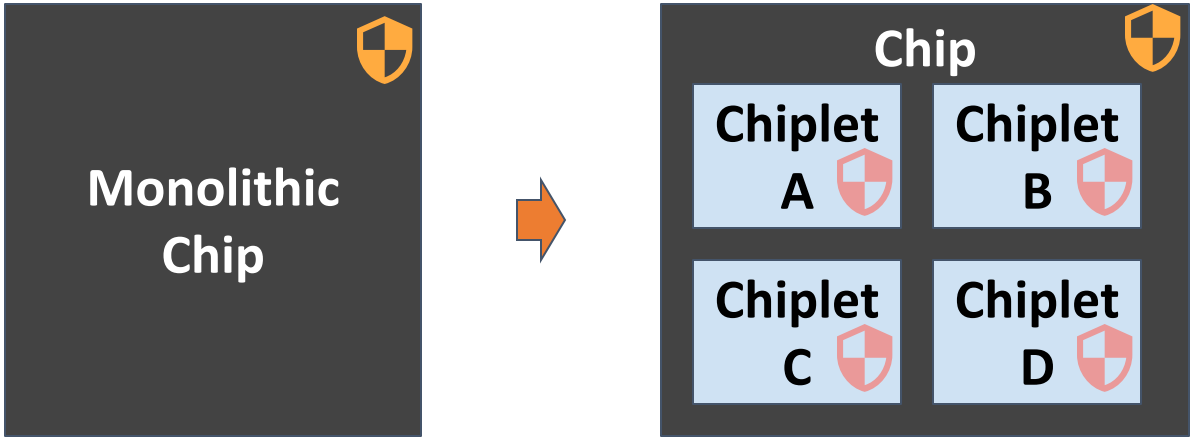
Security: Monolithic to Composable

Flash Memory Summit

Proprietary Security do not work and do not interoperate !

Keep Chip secure ⇒ Each Chiplet in a package must be Secure

Need to use common standard across Chiplets
(Chiplet Identity Configuration and Debug States)



Flash Memory Summit

UCIe™
Universal Chiplet Interconnect Express

THANK YOU

www.UCIexpress.org