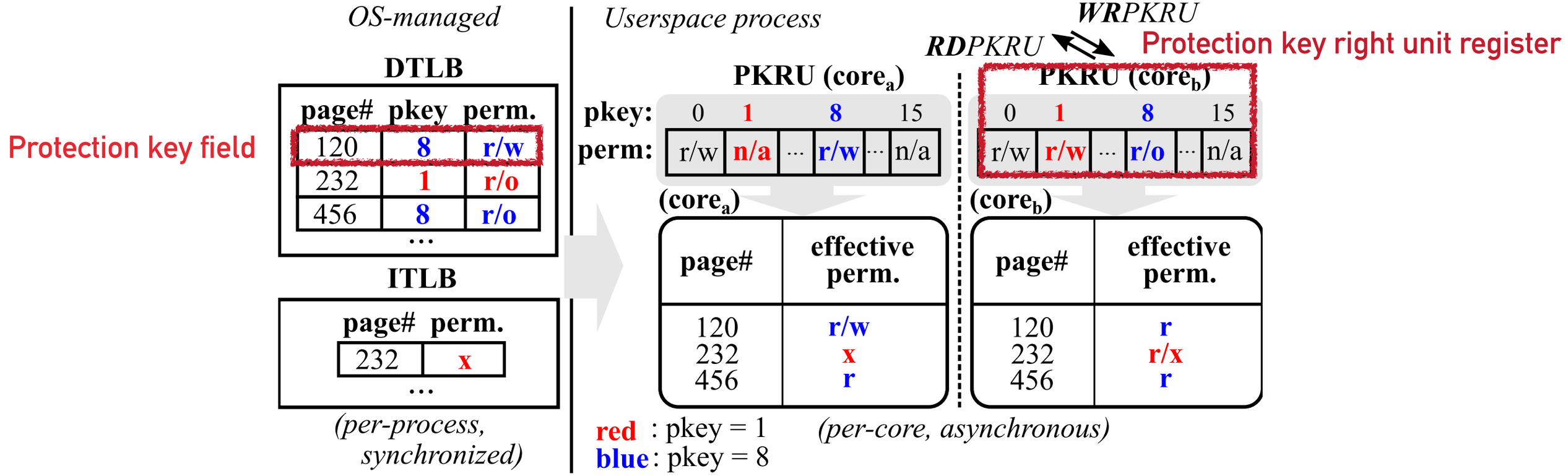
LIBMPK: SOFTWARE ABSTRACTION FOR INTEL MEMORY PROTECTION KEYS (INTEL MPK)

Soyeon Park, Sangho Lee, Wen Xu, Hyungon Moon and Taesoo Kim

INTEL MEMORY PROTECTION KEYS

- Available from Intel Skylake-sp processor
- Support fast permission change for page groups with single instruction
- Execute-only memory



CHALLENGES AND LIBMPK

- Potential Security Hazard : key-use-after-free
  - pkey_free does not perfectly free the protection key
- Non-scalable Hardware Resources
  - 32-bit PKRU register, supporting only 16 keys

- Key virtualization can solve both by decoupling physical keys from user interface and supporting key indirection.

- Asynchronous permission change
  - Permission change with MPK is thread-local intrinsically

- libmpk provides permission synchronization API to resolve this challenge

CONCLUSION

July 10th 16:10 Track II Security #1: Kernel

Application	Protected target	Performance
OpenSSL	Private key	0.53% slowdown
Memcached	slab	0.01% slowdown
Chakracore	JIT cache	4.39% improvement
V8	JIT cache	0.81% slowdown

- *libmpk is a **secure, scalable, and synchronizable** abstraction of MPK for supporting fast memory protection and isolation with little effort.*