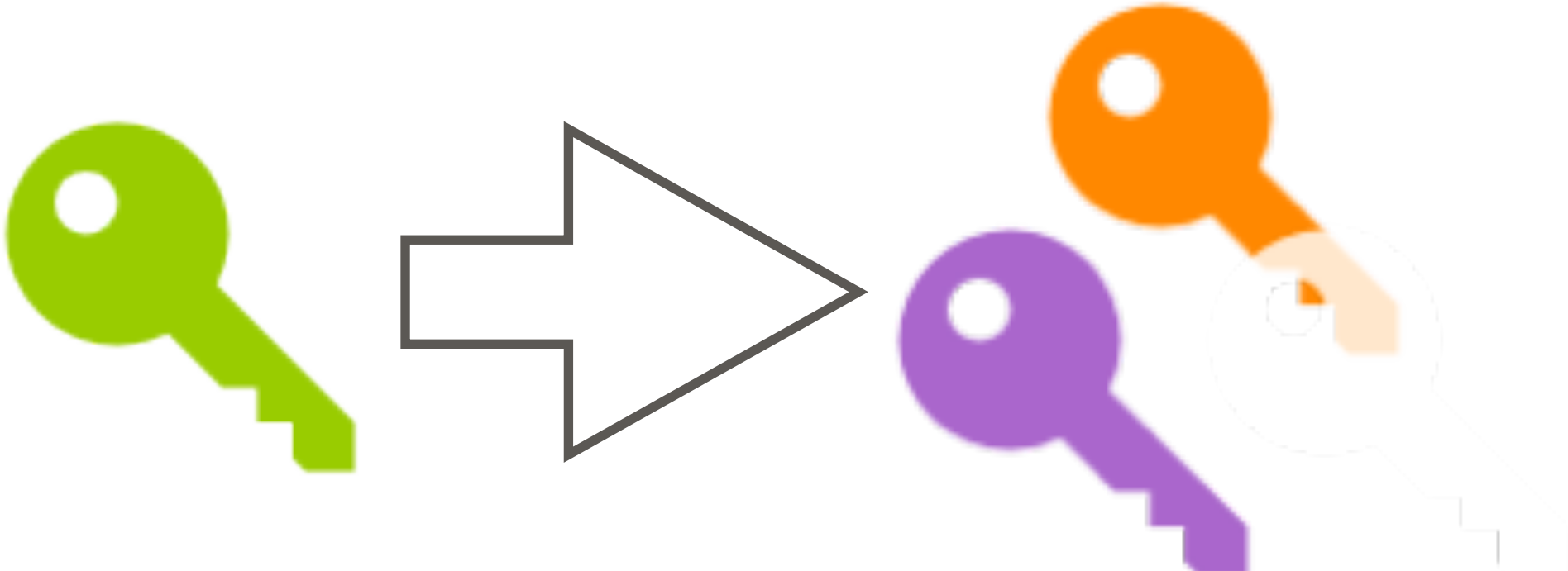
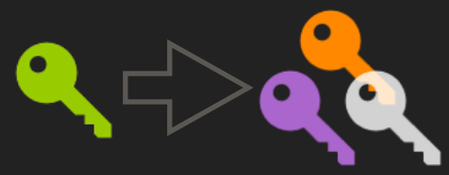
# KEY DERIVATION 2: FROM 1 TO N

# PATTERNS

69

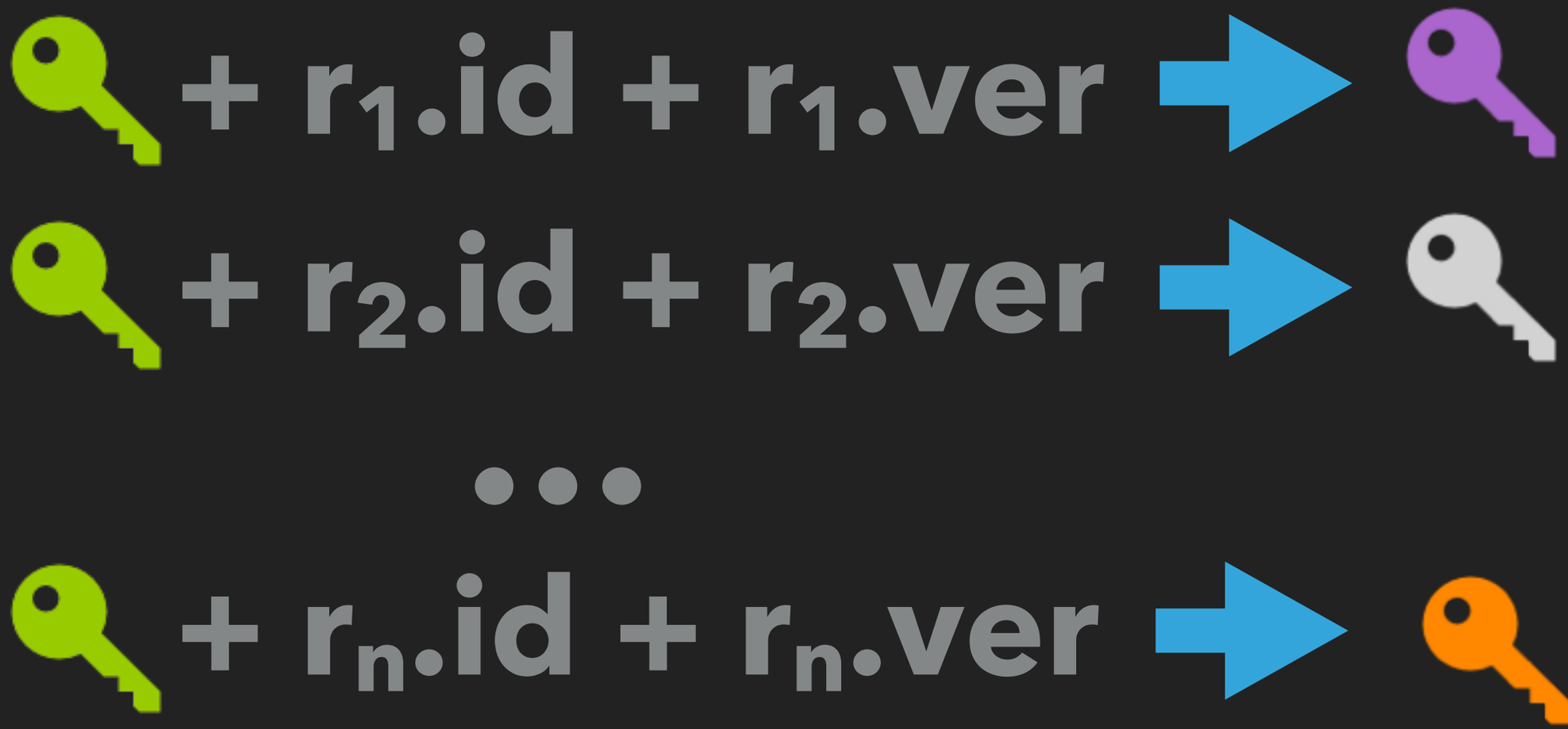


# DERIVE PER RECORD KEYS



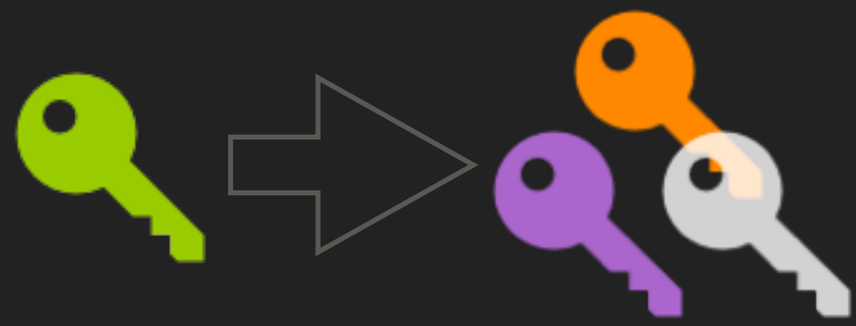
**Problem:** Use different keys for different records, only store master key.

**Solution:** Use key derivation to derive per-record keys.




IMPORTANT: NEVER USE THE SAME KEY/IV TO ENCRYPT DIFFERENT DATA

MAKE SURE THAT THE MASTER KEY HAS ENOUGH ENTROPY FOR DERIVED KEY AND DERIVED IV



PATTERNS

# KEY DERIVATION 2: FROM 1 TO N