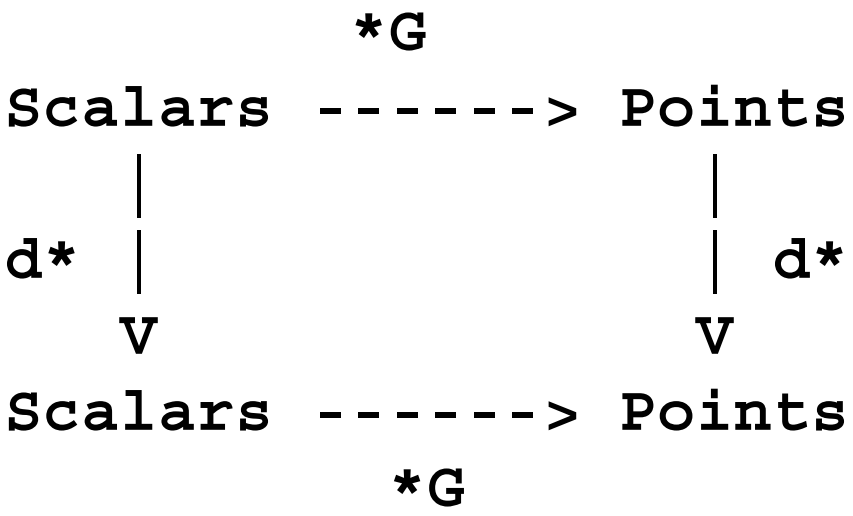
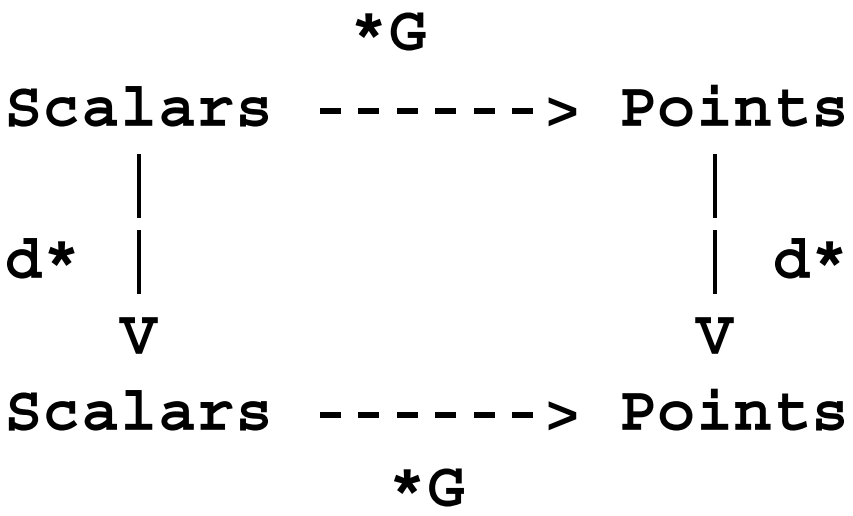
draft-barnes-cfrg-mult-for-7748

Richard Barnes, Joël Alwen, Sandro Corretti

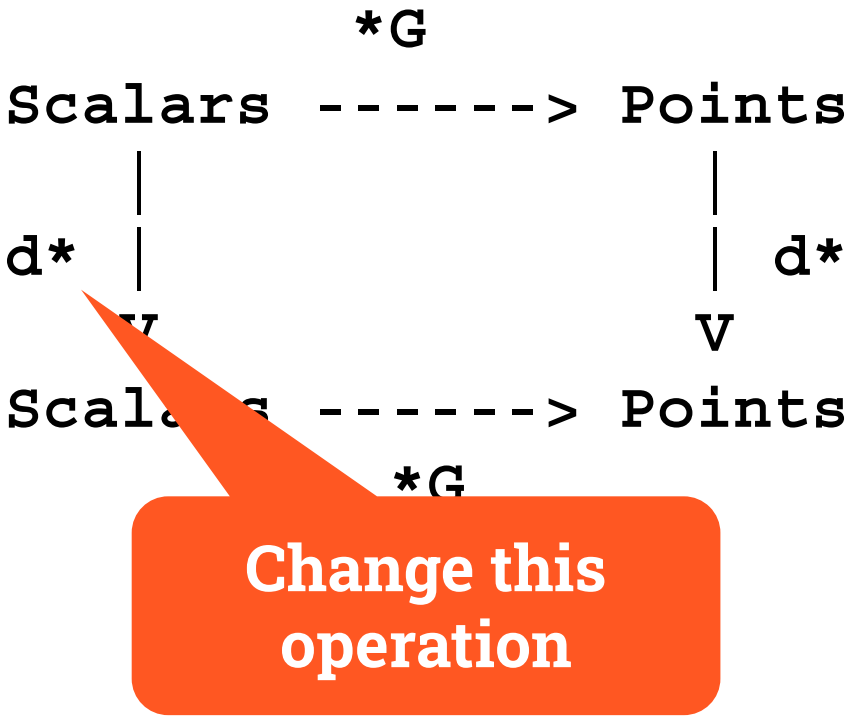


$$d(aG) = (da)G$$



$$d(aG) = (da)G$$

Not true for X25519 / X448!



$$d(aG) = (da)G$$

±multiplication

Problem: “Clamping” -- high order bit is set in decodeScalar()

Observation:

- If x is not clamped, then n - x is almost always clamped
- X25519/X448 operations are not sensitive to sign

So “mult” can just take whichever of (x, n - x) is clamped

Multiplication?

For some x, neither x nor (n - x) is clamped, in which case multiplication fails

Fortunately, this is extraordinarily rare

- X25519: 2^{-125}
- X448: 2^{-222}

Private key holder can detect failure, public key holder cannot

Questions

Interest in this specific question, or updateable PKE that arises from it?

Comments on the technical content? Errors / improvements?

Is this a safe operation? If d is attacker controlled, does attacker gain knowledge of da?

Good material for a CFRG doc?