High-speed FPGA implementation of full-word Montgomery multiplier for ECC applications:

https://www.sciencedirect.com/science/article/pii/S0141933117302843

- Bu makalede
    - **Operantlar "word" (kelime)** denilen daha büyük parçalara ayrılıyor (örneğin 64-bit, 128-bit gibi).
    - Bu kelimeler **blok halinde** işleniyor.
    - Özellikle, **Four-Parts (FP)** ve **Deep Four-Parts (DFP)** bölme teknikleri kullanılıyor.

Nasıl işliyor?

- Sayılar örneğin 256-bit ise:
    - FP yönteminde → 4 parçaya (4 × 64-bit)
    - DFP yönteminde → her bir parça da 4'e bölünüyor (16 × 16-bit gibi)
- Bu bölünmüş word'ler **paralel** olarak çarpılıyor ve toplama işlemleriyle birleştiriliyor.

Her bir parçanın çarpımı, **gömülü FPGA DSP blokları**yla (örneğin 18x25 çarpanlar) çok hızlı yapılabiliyor.

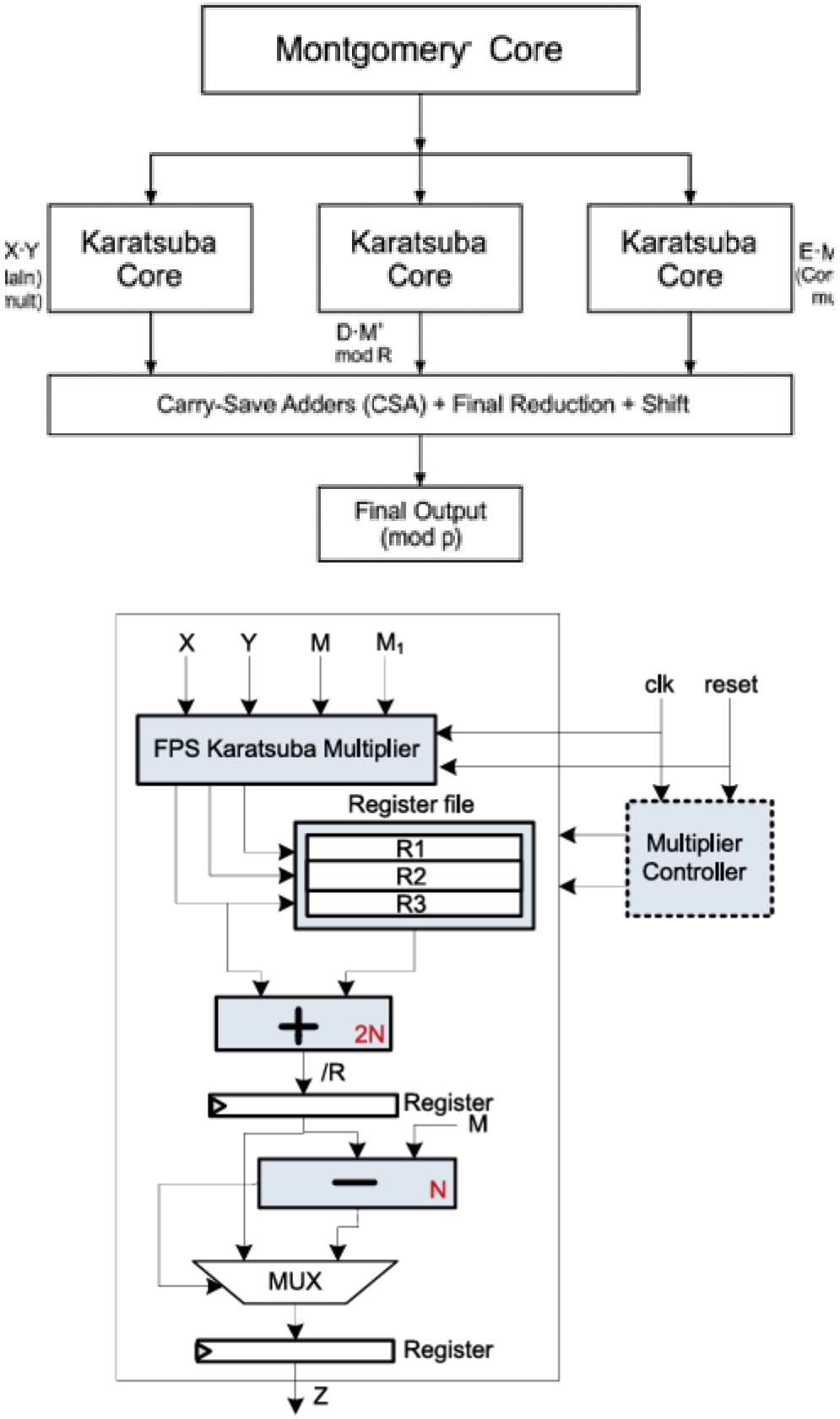

Fig. 5. Montgomery modular multiplier.

Montgomery İşlem Adımları

1. **D = X·Y** → Karatsuba ile yapılır
2. **E = (D·M') mod R**
    - mod R işlemi → sadece alt bitlerin alınması → donanımda **tek gate**
3. **T = (D + E·M) >> k**
    - E·M → Karatsuba çarpımı
    - D + E·M → CSA ile taşımasız toplanır
    - >> k → sadece bit shift

Pipeline Yapısı

Bu sistemde her bileşen bir pipeline stage olarak çalışır:

Stage	İşlem
1	X·Y (Karatsuba)
2	D·M' (Karatsuba)
3	mod R (masking)
4	E·M (Karatsuba)
5	CSA Toplama
6	Shift + düzeltme

Toplama ve Sadeleştirme – CSA + Final Adder + Shift

- D + E·M → bu toplama işlemi **carry-save adder (CSA)** ile yapılır:
    - Avantajı: taşıma gecikmesini engeller
    - Çok sayıda toplamayı paralel şekilde yürütür
- Ardından **sonuç sağa kaydırılır** (/R, yani >> k)
- Gerekirse Z ≥ M düzeltmesi yapılır → Z = Z – M

Pipeline & Performans

Her Karatsuba bloğu ve toplama aşaması **pipeline olarak birbirine bağlanmıştır**.
Bu sayede:

- Toplam işlemin süresi: **29–38 cycle**
- Donanımda her clock’ta yeni bir Montgomery sonucu üretilebilir