RAPOR

Hazırlayan: Şeyma ÇALIŞKAN

İncelenen Yayınlar:

1) A High-Performance Hardware Accelerator for ECC in GF(p) over Generic Weierstrass Curves (2024)
2) A Compact Elliptic Curve Cryptography Accelerator Over Prime Field for System-on-Chips (2024)
3) High-Speed and Secure ECC Processor for Chinese SM2 using Modified Karatsuba Multiplier based on FPGA (2024)
4) A Dual-Core High-Performance Processor for Elliptic Curve Cryptography in GF(p)Over Generic Weierstrass Curves (2022)
5) Flexible FPGA-Based Architectures for Curve Point Multiplication over GF(p) (2016)
6) A 521-bit Dual-Field Elliptic Curve Cryptographic Processor with Power Analysis Resistance (2010)
7) A High Speed Coprocessor for Elliptic Curve Scalar Multiplications over Fp (2010)
8) Ultra High Performance ECC over NIST Primes on Commercial FPGAs (2008)
9) Hardware Elliptic Curve Cryptographic Processor Over GF(p): (2006)
10) A Parallel Processing Hardware Architecture for Elliptic Curve Cryptosystems (2006)

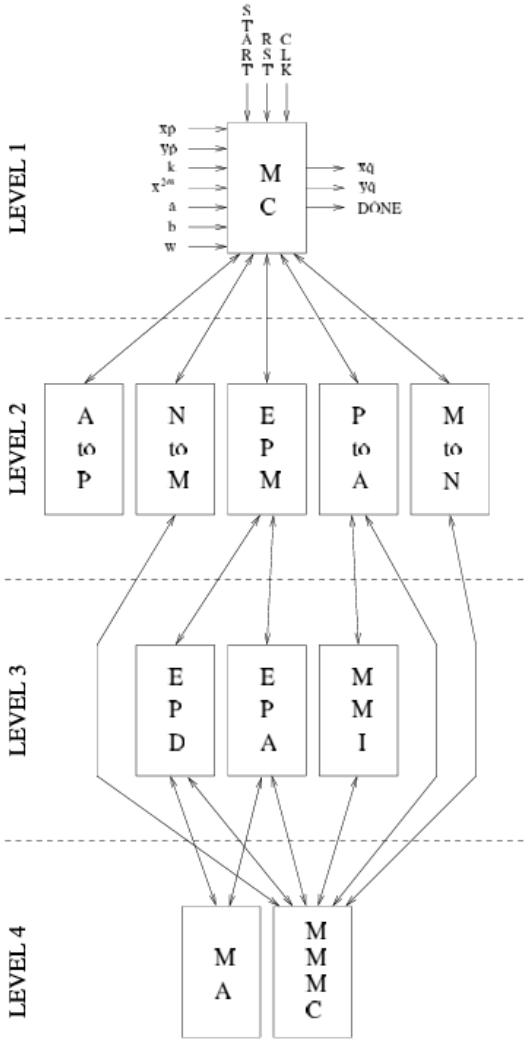

Figure 4.22: Block diagram of the elliptic curve point multiplier circuit over $GF\,(2^m)$

Görselde verilen diagram kullanılarak sistem için bir yol çizilebilir.

Makalelerin Kısaca Katkıları:

1. **A High-Performance Hardware Accelerator for ECC in GF(p) over Generic Weierstrass Curves (2024)**

Temel Katkılar

- **Radix-128 Montgomery Çarpımı (N-R128MMM):**
  Final indirgeme adımını kaldırarak çarpıcı verimliliğini artıran yeni bir modular çarpım yapısı önerildi.
- **Combined-Addition (CA):**
  Modüler indirgeme işlemlerini tek adımda ve hızlı bir şekilde gerçekleştiren yardımcı bir birim tasarlandı.
- **Paralel Mimari:**
  4 N-R128MMM, 2 modüler toplama (MA) ve 2 CA birimi paralel çalışacak şekilde entegre edilerek yüksek performans sağlandı.

---

2. **A Compact Elliptic Curve Cryptography Accelerator Over Prime Field for System-on-Chips (2024)**

Temel Katkılar:

- **Dahili veri depolama birimleri kullanılmadan**, sistem SRAM üzerinden veri erişimi sağlanarak donanım alanı ciddi ölçüde azaltılmıştır.
- **Adder-subtractor (toplama-çıkarma) birimi yeniden kullanılarak** işlem maliyeti düşürülmüştür.
- 256-bit ECC nokta çarpımı:
  - **FPGA'da**: 18.0 ms @ 156.9 MHz (589 slice ile)
  - **ASIC (22nm CMOS)**: 7.1 ms @ 400 MHz (yalnızca 31K gate)
- **Modüler toplama, çıkarma ve kaydırma** işlemleriyle tüm ECC işlemleri desteklenir.

---

3. **High-Speed and Secure ECC Processor for Chinese SM2 using Modified Karatsuba Multiplier based on FPGA (2024)**

Temel Katkılar:

- **2 seviyeli Karatsuba çarpanı** geliştirilmiştir. Bu sayede 256-bit çarpma, iki aşamalı olarak daha küçük bit genişliklerinde hesaplanır ve DSP kaynakları verimli kullanılır.
- **Geliştirilmiş Montgomery skaler çarpım algoritması** ile **nokta toplama ve nokta ikiye katlama** işlemleri paralel gerçekleştirilir.
- **SPA (Simple Power Analysis) saldırılarına karşı dayanıklıdır.**

Hızlı modüler indirgeme algoritması ile Mersenne benzeri asal sayılar üzerinde hızlı hesaplama yapılır.

---

4. **A Dual-Core High-Performance Processor for Elliptic Curve Cryptography in GF(p)Over Generic Weierstrass Curves (2022)**

Ana Katkılar:

- **Radix-128 Montgomery modüler çarpımı**: Sadece **6 clock cycle** sürer.
- **Ayrı PD (point-doubling) ve PA (point-addition) çekirdekleri** ile paralel hesaplama yapılır.
- **Optimize edilmiş veri aktarımı**: Sadece **256-bit kayıtçı** ile PD ve PA çekirdekleri arasında veri aktarımı sağlanır.
- **Geliştirilmiş zamanlama algoritmaları** ile yüksek hız elde edilir.

---

5. **Flexible FPGA-Based Architectures for Curve Point Multiplication over GF(p) (2016)**

Temel Katkılar:

- **Montgomery çarpımı** için **geliştirilmiş bir boru hattı (pipeline) mimarisi** kullanılmıştır.
- **ECPM (Elliptic Curve Point Multiplication)** işlemi için **paralel** PADD (nokta toplama) ve PDBL (nokta ikiye katlama) hesaplamaları gerçekleştirilmiştir.
- **Projeksiyon koordinatları (Jacobian)** ile sadece 1 modüler tersleme gerektiren yapı kullanılmıştır.
- **Arbitrary prime field ve key size desteği** vardır (1024-bit'e kadar), FPGA yeniden yapılandırmasına gerek kalmaz.

Öne Çıkan Özellik:

- Literatürde **parametre boyutu ve asal alanlarda bu kadar esnek çalışabilen ilk donanım mimarilerinden biri**.
- Hem **verimli** hem de **uyarlanabilir** bir çözüm sunar; özellikle çeşitli ECC standartlarını destekleyen sistemler için uygundur.

---

6. **A 521-bit Dual-Field Elliptic Curve Cryptographic Processor with Power Analysis Resistance (2010)**

Temel Katkılar:

- **Yeni birleştirilmiş bölme algoritması** (unified division) ile hem Montgomery hem de klasik modüler bölme işlemleri hızlandırılmıştır.
- **Tüm ECC işlemleri için entegre ve pipelined Galois Field Arithmetic Unit (GFAU)** geliştirilmiştir.
- **Ön hesaplama (pre-computation) gerektirmeyen mimari** ile gerçek zamanlı çalışma sağlanır.
- **Power analysis saldırılarına karşı dirençli**: "Key-blinding" ve "dummy operation" teknikleriyle hem SPA hem DPA saldırılarına karşı koruma sağlanmıştır.

---

7. **A High Speed Coprocessor for Elliptic Curve Scalar Multiplications over Fp (2010)**

Temel Katkılar:

- **Residue Number System (RNS)** kullanılarak, taşımasız (carry-free) ve **yüksek derecede paralel** çalışabilen bir mimari geliştirilmiştir.
- Altera FPGA'lar üzerinde uygulama yapılmış, sonuçlar gösterilmiştir.
- Tasarım, **side-channel saldırılarına (SPA/DPA) karşı dayanıklıdır**.
- 160 bitlik skaler çarpımı **1 ms'den daha kısa sürede** gerçekleştirebilen ilk genel donanım mimarisi olmuştur.

---

8. **Ultra High Performance ECC over NIST Primes on Commercial FPGAs (2008)**

Temel Katkılar:

- **Tüm ECC aritmetiği, FPGA içindeki DSP bloklarında** (sinyal işleme için optimize donanım) gerçekleştirilmiştir.

- **NIST prime sayıları (P-224 ve P-256)** için özel modüler indirgeme algoritmaları kullanılmıştır.
- **Alan kullanımı düşük, hız çok yüksek** olacak şekilde tasarlanmış **çok çekirdekli (multi-core)** bir mimari sunulmuştur.
- 16–18 ECC çekirdeği tek FPGA üzerinde çalıştırılabilmiştir.

---

9. Hardware Elliptic Curve Cryptographic Processor Over GF(p): (2006)

Yenilikler:

- Klasik ve Montgomery terslemeyi tek yapıda gerçekleştiren **birleşik modüler tersleme algoritması**
- **Full-word Montgomery çarpma donanımı** ile daha az saat döngüsü ve yüksek hız
- FPGA'da 256-bit ECC işlemi **3.86 ms** sürede tamamlanmıştır

Avantaj:

- **4 farklı tersleme türünü** destekleyen ilk ECC işlemcisi

---

10. A Parallel Processing Hardware Architecture for Elliptic Curve Cryptosystems (2006)

Temel Katkılar:

- **Birden fazla modüler aritmetik birim (MALU)** kullanılarak paralel hesaplama yapılır.
- Donanım, **Instruction-Level Parallelism (ILP)** kontrolü ile dinamik olarak paralel komutları tespit edip yürütür.
- **Hem GF(p) hem de GF(2^m)** alanları desteklenir.
- 2 veya 3 MALU kullanıldığında performans **1.5 ila 1.6 kat** artar.
- Daha fazla MALU eklemek ek bir fayda sağlamaz.

1) **A High-Performance Hardware Accelerator for ECC in GF(p) over Generic Weierstrass Curves (2024)**

Genel Weierstrass Eğrileri Üzerinde GF(p)'de Eliptik Eğri Kriptografisi için Yüksek Performanslı Donanım Hızlandırıcısı. Makale, 256-bitlik bir eliptik eğri kriptografisi (ECC) donanım hızlandırıcısının tasarımını ve performansını ele alıyor.

Makale, eliptik eğri kriptografisi (ECC) sistemlerinde kullanılan temel bir işlem olan **eliptik eğri nokta çarpımı (ECPM)** işlemini hızlandırmak için yeni bir donanım hızlandırıcı öneriyor. Bu hızlandırıcı, özellikle **genel Weierstrass eğrileri** üzerinde GF(p) (sonlu alan) tabanlı sistemler için tasarlanmış. Weierstrass eğrileri, Montgomery veya Edwards eğrilerine kıyasla daha az performanslı olsa da, SM2, NIST ve Brainpool gibi güvenlik standartlarında hala yaygın olarak kullanılıyor. Makale, bu eğriler üzerinde yüksek performans elde etmeyi hedefliyor ve bunu ASIC (90 nm teknolojisi) üzerinde 0.014 milisaniyede 256-bit ECPM işlemi gerçekleştirerek başarıyor.

Makale, performans artışı sağlamak için üç ana yenilik sunuyor:

Yeni Radix-128 Montgomery Modüler Çarpma (N-R128MMM):

- Geleneksel Montgomery modüler çarpma (MMM) işleminde son indirgeme (final reduction) adımı, çarpanların kullanım verimliliğini düşürüyor. Örneğin, önceki bir tasarımda [5], MMM 6 saat döngüsü (clock cycle) gerektirirken çarpan sadece 5 döngüde aktifti.
- Bu makalede önerilen **radix-128 MMM**, son indirgeme adımını kaldırarak çarpanların kullanımını optimize ediyor. İki adet 128-bit çarpan paralel çalıştırılarak 256-bit MMM işlemi 5 saat döngüsünde tamamlanıyor.

Birleşik Toplama (Combined-Addition - CA):

- MMM'nin son indirgeme adımını telafi etmek için bir **CA yöntemi** geliştirilmiş. Bu yöntem, ardışık MMM işlemlerinin saat döngülerini azaltıyor ve aynı zamanda dört ayrı modüler indirgeme işlemi olarak da yeniden kullanılabiliyor.
- Bu, işlemleri daha hızlı ve verimli hale getiriyor.

Yüksek Paralellikli Montgomery Merdiveni Hızlandırıcı:

- ECPM işlemini hızlandırmak için Montgomery merdiveni algoritması temel alınmış. Bu tasarımda, dört N-R128MMM, iki CA ve iki modüler toplama birimi paralel çalışıyor.
- Sonuç: Bir Montgomery merdiveni işlemi 16 saat döngüsünde, bir ECPM işlemi ise 4.4 bin saat döngüsünde tamamlanıyor.

Matematiksel Temel

Weierstrass eğrileri, şu denklemle tanımlanır:
E: y^2 = x^3 + ax^2 + b \mod p
Burada a ve b, (4a3+27b2)mod p≠0 koşulunu sağlayan GF(p) elemanlarıdır.
ECPM, bir nokta P=(xP,yP) ile bir skaler k kullanılarak Q=[k]P=P+P+⋯+P (k kez toplama) şeklinde hesaplanır. Bu işlem, Montgomery merdiveni algoritmasıyla sabit zamanda gerçekleştirilerek basit güç analizine (SPA) karşı direnç sağlanır.

Montgomery Merdiveni Algoritması

Makalede, Hamburg'un 2020'de önerdiği geliştirilmiş Montgomery merdiveni formülü kullanılıyor. İşlem üç aşamada gerçekleşiyor:

1. **Kurulum (Setup Ladder):** Afin koordinatlar P=(xP,yP) P = (x_P, y_P) P=(xP,yP) Hamburg merdiveni durumuna dönüştürülüyor.
2. **Merdiven Adımı (Ladder):** Her döngüde noktalar güncelleniyor; bu adım paralel modüler işlemlerle optimize edilmiş.
3. **Sonuç (Final Ladder):** Hesaplama tamamlandığında sonuç projektif koordinatlardan afin koordinatlara çevriliyor.

Donanım Uygulaması

- **Modüler İşlemler:**
  - **Modüler Toplama/Çıkarma (MA):** 258-bitlik iki toplama birimiyle 1 saat döngüsünde hesaplanıyor.
  - **Modüler Ters (MI):** Radix-4 Öklid algoritmasıyla 256 saat döngüsünde hesaplanıyor (256-bit ECPM'de bir kez kullanılıyor).
  - **N-R128MMM:** Bölme ve çıkarma yerine kaydırma işlemleri kullanılarak 5 döngüde tamamlanıyor.
- **Paralel Mimari:** Dört N-R128MMM, iki CA ve iki MA birimiyle yüksek paralellik sağlanmış.

---

2) **A Compact Elliptic Curve Cryptography Accelerator Over Prime Field for System-on-Chips (2024)**

2024'te 9. Uluslararası Entegre Devreler ve Mikrosistemler Konferansı'nda sunulmuş. Bu makale, Eliptik Eğri Kriptografisi (ECC) için maliyet odaklı Sistem-Üzerinde-Çip (SoC) tasarımlarına yönelik kompakt bir donanım hızlandırıcı öneriyor.

Sorun ve Çözüm

- **Sorun:** Mevcut ECC hızlandırıcılar yüksek performans için tasarlanmış, ama genellikle büyük alan kaplıyor (örneğin, geniş dahili bellek birimleri kullanıyorlar). Bu, düşük maliyetli SoC'lar için uygun değil.
- **Çözüm:** Bu makalede önerilen hızlandırıcı:
    1. **Dahili Bellek Yok:** Verileri sistem SRAM'inden otobüsle alıyor, böylece alan tasarrufu yapıyor.
    2. **Tekrar Kullanım:** Toplama-çıkarma birimini (adder-subtractor) tekrar kullanarak maliyeti düşürüyor.
    3. **Esneklik:** Farklı algoritmaları destekliyor (örneğin, ECDSA, ECDH).

ECC'nin Üç Seviyesi

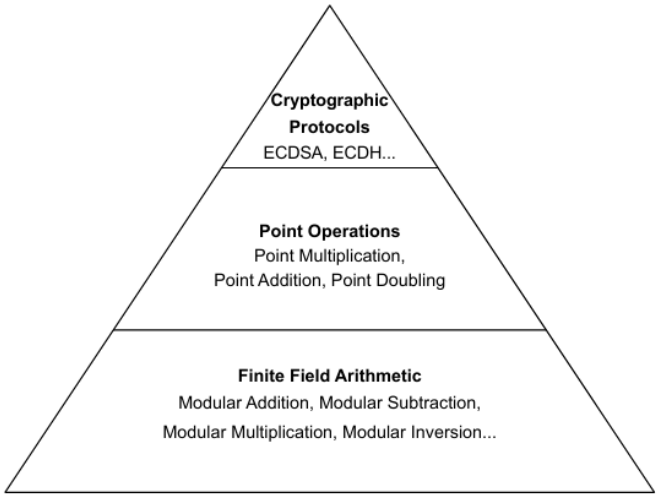

Fig. 1. Three levels of ECC.

Makale, ECC'yi üç katmana ayırıyor (Şekil 1):

1. **Üst Seviye:** Kriptografik protokoller (ECDSA, ECDH).
2. **Orta Seviye:** Nokta işlemleri (point addition, doubling, multiplication).
3. **Alt Seviye:** Asal alan aritmetiği (modüler toplama, çıkarma, çarpma).

Bu hızlandırıcı, alt seviyede çalışarak üst seviyelere temel sağlıyor.

Asal Alan Aritmetiği

Asal alan (prime field), büyük bir asal sayı p p p ile tanımlı GF(p) GF(p) GF(p) kümesidir. ECC'de kullanılan temel işlemler:

1. **Modüler Toplama:** A+B mod p
    - A+B < p ise sonuç A+B
    - A+B ≥ p ise A+B−p
2. **Modüler Çıkarma:** Benzer mantıkla, A−B mod p

3. **Modüler Çarpma:** Daha karmaşık, genellikle “shift-and-add” yöntemiyle yapılıyor (radix-2 interleaved multiplication).
    - Şekil 3’te gösterilen algoritma: Her bit için toplama ve modüler azaltma yapılıyor. Sonuç 0 0 ile 3p arasında olabilir, bu yüzden 2 kez çıkarma gerekebilir.

Hızlandırıcı, bu işlemleri donanımda yaparak hız kazanıyor.

Tasarım Mimarisi

Hızlandırıcı, üç ana bileşenden oluşuyor (Şekil 4):

1. **Bus Slave Arayüzü:** Konfigürasyon (örneğin, modül seçimi) ve aritmetik talimatları alıyor. Talimatlar FIFO’ya sıralanıyor.
2. **Bus Master Arayüzü:** Sistem SRAM’inden veri okuyup yazıyor.
3. **Hesaplama Çekirdeği:** Asıl işi yapıyor (Şekil 5).

Hesaplama Çekirdeği

- **Bileşenler:** (N+1) (N+1) (N+1)-bit toplama-çıkarma birimi, (N+1) (N+1) (N+1)-bit kayıtçı (register), veri yolları.
- **İşleyiş:**
    - Modüler toplama/çıkarma: İlk döngüde toplama/çıkarma, ikinci döngüde modüler azaltma.
    - Modüler çarpma: 2N 2N 2N ila 3N 3N 3N döngü alıyor (örneğin, 256-bit için 512-768 döngü).
- **Kontrol:** Bir durum makinesi (finite-state machine) işlemleri yönetiyor.

Esneklik

- Hesaplama çekirdeği, otobüsten bağımsız bir saatle çalışıyor (asynchronous clock). Bu, sistem saatinden farklı hızlarda çalışmasını sağlıyor.

Neden Daha İyi?

1. **Alan Tasarrufu:** Dahili bellek birimleri yerine otobüsle veri alıyor. Veri erişimi toplam sürenin %9’undan azını oluşturuyor, bu yüzden performans kaybı minimum.
2. **Esneklik:** Herhangi bir asal alanda çalışabiliyor (örneğin, NIST dışı eğriler).
3. **Güvenlik:** Sabit döngü seçeneğiyle yan kanal saldırılarını zorlaştırıyor.

---

3) High-Speed and Secure ECC Processor for Chinese SM2 using Modified Karatsuba Multiplier based on FPGA (2024)

Eliptik Eğri Kriptografisi (ECC) üzerine Çin’in SM2 standardını FPGA üzerinde hızlı ve güvenli bir şekilde uygulamayı ele alıyor.

SM2: Çin'in ECC tabanlı standardı; dijital imza, anahtar değişimi gibi alanlarda kullanılır.

Bu makale, ECC'nin (özellikle Çin'in SM2 standardı) FPGA üzerinde yüksek hızlı bir işlemciyle uygulanmasını hedefliyor. Ana odak:

Sorun: ECC'de skaler çarpma (scalar multiplication) gibi işlemler hesaplama açısından yoğun ve yavaş olabiliyor.

Çözüm:

- **Karatsuba Çarpanı:** Hızlı çarpma için Radix-4 Karatsuba algoritmasının çıkarımsal (subtractive) bir versiyonu kullanılıyor.
- **Montgomery Skaler Çarpma:** Nokta toplama ve ikiye katlama işlemlerini paralel hale getirerek hız artırılıyor.

Skaler Çarpma

- kP=P+P+⋯+P (k kez): Bir noktayı bir skalerle çarpmak, ECC'nin temel işlemidir.
- Nokta toplama (P+Q) ve ikiye katlama (2P) ile yapılır.

Karatsuba Algoritması

- Büyük sayıları çarpmak için kullanılan bir yöntem.
- **Schoolbook:** O(N^2) karmaşıklığı var (her basamak her basamakla çarpılır).
- **Karatsuba:** O(N^(log23/log2)) ≈ O(N^(1.585)), daha az çarpma ile hız sağlar.
- Örnek: XY=(X1Y1)2^k+(X1Y2+X2Y1)2^(k/2)+X2Y2.

Makalenin Yenilikleri

1. 2 Seviyeli Karatsuba Çarpanı

- **Hedef:** 256-bit çarpma yapmak.
- **Yöntem:**
    - 256-bit sayı, 64-bit parçalara bölünür (1. seviye).
    - 64-bit sayı, 16-bit parçalara bölünür (2. seviye), bu da FPGA'nın 18x25 DSP'lerine uyar.
- **Çıkarımsal Karatsuba:**
    - Klasik toplama yerine çıkarma kullanılır:

$$X1Y2+X2Y1=X1Y1+X2Y2-(X1-X2)(Y1-Y2).$$

    - İşaret problemi: Çıkarma signed (işaretli) sayılar üretir, bu da bit genişliğini artırır.
- **Çözüm:** İşaret ön-işleme (sign preprocessing):
    - Mutlak değer alınarak signed sayılar unsigned'a çevrilir, bit genişliği sabit tutulur (örneğin 65-bit → 64-bit).

2. Geliştirilmiş Montgomery Skaler Çarpma

- **Klasik Yöntem:** Nokta toplama ve ikiye katlama sırayla yapılır, y-koordinatı her adımda gerekir.
- **Yeni Yöntem:**
    - Paralel işlem: Nokta toplama ve ikiye katlama aynı anda yapılır.
    - y-koordinatı sadece son adımda hesaplanır.
    - Proje koordinat sistemi kullanılır (bölme işlemleri azalır).
- **Avantaj:** SPA (Simple Power Analysis) saldırılarına karşı dirençli.

3. Donanım Mimarisi

- **Birimler:**
    - **FSM Kontrolör:** İşlem akışını yönetir.
    - **Hesaplama Birimi:** 2 set Karatsuba çarpanı, modüler toplama/çıkarma ve azaltma birimleri içerir.
    - **Nokta Toplama/İkiye Katlama:** Paralel çalışır.
    - **Modüler Ters Alma:** Extended Euclidean algoritmasıyla yapılır.
- **Zamanlama:** 11 çarpma + 1 modüler azaltma süresiyle tamamlanır.

Nasıl Çalışır?

Algoritma 1: 2 Seviyeli Karatsuba

- **Giriş:** 64-bit X ve Y.
- **Adım:**
    - 16-bit parçalara bölünür.
    - Çarpımlar DSP'lerle yapılır (17-bit signed, 18x25'e uyar).
- **Çıkış:** 128-bit sonuç.

Algoritma 2: İşaret Ön-İşleme

- **Sorun:** 256-bit çarpımda 65-bit signed ara sonuçlar çıkar.
- **Çözüm:** |X1−X2| ve |Y1−Y2| alınır, işaret XOR ile belirlenir.
- **Sonuç:** 64-bit unsigned çarpımlar.

Algoritma 3: Montgomery Skaler Çarpma

- **Giriş:** Nokta PPP, skaler kkk.
- **Adım:**
    - k'nin her biti için: Eğer 1 ise Q=Q+P,P=2P; değilse P=P+Q,Q=2Q
    - Paralel çalışır, yyy-koordinatı kullanılmaz.
- **Çıkış:** Q=kP

Algoritma 5: Modüler Ters Alma

- **Yöntem:** Extended Euclidean algoritması.
- **Amaç:** T=(2yZ1^(2)Z2)^−1 mod p hesaplanır.
- **Sonuç:** Afin koordinatlara dönüş.

---

4) A Dual-Core High-Performance Processor for Elliptic Curve Cryptography in GF(p)Over Generic Weierstrass Curves (2022)

Makale, Eliptik Eğri Kriptografisi (ECC) için asal alan GF(p) GF(p) GF(p) üzerinde çalışan, genel Weierstrass eğrilerini destekleyen yüksek performanslı bir çift çekirdekli işlemci sunuyor.

ECC'nin güvenli iletişim için önemli bir yöntem olduğunu, ancak nokta çarpımı (PM) gibi işlemlerin hesaplama açısından yoğun olduğunu belirtiyor. Bu sorunu çözmek için:

- **Önerilen Çözüm:** Çift çekirdekli bir işlemci tasarlanmış.
    - Bir çekirdek **nokta ikiye katlama (PD)**, diğer çekirdek **nokta toplama (PA)** işlemlerini yapıyor.
    - Yeni bir **radix-128 Montgomery modüler çarpma (R128MM)** algoritması geliştirilmiş.
- **Performans:** 256-bit PM işlemi:
    - ASIC'te (90 nm): 0.017 ms (17 µs).
    - FPGA'da (Virtex-6): 0.056 ms (56 µs).
- **Avantaj:** Hızlı, herhangi bir Weierstrass eğrisinde çalışabiliyor ve alan-zaman (AT) performansında diğer tasarımlardan üstün.

Weierstrass Eğrileri: y^2 = x^3 + ax + b denklemiyle tanımlı eğriler. a ve b, GF(p) (asal alan) içinde ve 4a3+27b2mod p≠0 olmalı.

Ana Yenilik: R128MM Algoritması

- **Ne Yapıyor?** Modüler çarpma (MM), PM'nin en zaman alan kısmı. R128MM, Montgomery çarpma algoritmasını 128-bit tabanla optimize ediyor.
- **Nasıl Çalışıyor?** (Algoritma 2)
    - İki 256-bit sayıyı (örneğin x x x ve y y y) 128-bit parçalara bölüyor.
    - 6 saat döngüsünde (clock cycle) çarpma ve modüler azaltmayı tamamlıyor.
    - İki paralel birim (Unit1 ve Unit2) kullanıyor, böylece hız artıyor.
- **Avantaj:** Geleneksel yöntemlere göre daha az döngüyle hızlı sonuç veriyor.

Donanım Mimarisi

PD (Nokta İkiye Katlama)

- **Algoritma 3:** Tekrarlanan PD'yi optimize ediyor.
    - 21 döngüde bir PD tamamlanıyor.
- **Donanım:** (Şekil 1)
    - 4 paralel birim: PD-GF(p)-0/1/2/3.
    - Toplam alan: 578K kapı (gates).

- Tablo I'de döngü planı var

PA (Nokta Toplama)

- **Algoritma 4:** P1+P2 işlemini yapıyor.
  - Z^2 yi PD'den alıyor, tekrar hesaplamıyor.
  - 25 döngüde tamamlanıyor.
- **Donanım:** (Şekil 2)
  - Alan: 418K kapı.
  - Daha az sıklıkta kullanılıyor (256-bit PM'de maksimum 128 kez).

Çift Çekirdekli PM

- **Algoritma 5:** NAF (Non-Adjacent Form) ile optimize edilmiş.
  - PD çekirdeği sürekli ikiye katlama yapıyor.
  - PA çekirdeği gerektiğinde toplama yapıyor.
  - Toplam 5.9K döngüde 256-bit PM tamamlanıyor.

Neden Daha İyi?

1. **Hız:** R128MM ile modüler çarpma 6 döngüye iniyor.
2. **Paralellik:** PD ve PA çekirdekleri aynı anda çalışıyor.
3. **Esneklik:** Herhangi bir Weierstrass eğrisinde çalışabiliyor (NIST gibi özel eğrilere bağlı değil).
4. **Verimlilik:** Daha az kayıt (256-bit) ve optimize döngülerle AT performansı üstün.

---

5) Flexible FPGA-Based Architectures for Curve Point Multiplication over GF(p) (2016)

Bu makale, eliptik eğri kriptografisi (ECC) denen bir şifreleme yöntemini daha hızlı ve esnek bir şekilde çalıştırabilmek için FPGA (Field Programmable Gate Array - Programlanabilir Kapı Dizisi) tabanlı bir donanım tasarımı sunuyor. Özellikle, asal alanlar (GF(p)) üzerinde çalışan bir sistem geliştirilmiş. Bu sistem, farklı standartlardaki eliptik eğrileri destekliyor ve 1024 bit'e kadar parametre boyutlarıyla çalışabiliyor.

Tamamen donanım tabanlı bir sistemdir.

Makalede Ne Yapılmış?

Makale, ECC'nin en önemli ve zaman alan kısmı olan "elips eğrisi nokta çarpımı" (ECPM - Elliptic Curve Point Multiplication) işlemini hızlandırmak için bir donanım tasarımı öneriyor. Bu tasarımın öne çıkan özellikleri şunlar:

1. **Esneklik:** Farklı standartlardaki eğrileri (örneğin, NIST, Brainpool) ve kullanıcı tanımlı eğrileri destekliyor. Ayrıca, parametre boyutu (örneğin, 192 bit, 256 bit, 521 bit) değiştirilebiliyor ve donanımı yeniden yapılandırmaya gerek kalmıyor.

2. **Hız:** Xilinx Virtex-7 FPGA üzerinde test edildiğinde, 512 bitlik bir çarpım işlemi 9.7 milisaniyede tamamlanıyor.
3. **Verimlilik:** Az yer kaplıyor. Sadece 20 DSP dilimi ve 6816 LUT (Logic Unit Table) kullanıyor. Bu, diğer benzer sistemlere göre daha az kaynakla daha iyi performans demek.

Montgomery Çarpımı

Makalede, bu yöntemi FPGA'ya uygun hale getirmek için "Iterative Digit-Digit Montgomery Multiplication" (IDDMM) denen bir algoritma geliştirilmiş ve optimize edilmiş

Paralel İşlem:

- Nokta toplama ve ikiye katlama işlemleri, iki Montgomery çarpanı ve bir toplama/çıkarma birimiyle paralel olarak yapılıyor. Bu, işlemleri hızlandırıyor.

Güvenlik: Sistem, "basit güç analizi" (SPA) saldırılarına karşı savunmasız olabilecek bir algoritma kullanıyor. Ancak, bunu önlemek için "double-and-add-always" denen bir yöntem önerilmiş

Kullanılan Temel Algoritmalar ve Teknikler:

- **Montgomery Çarpımı**:
  - Modüler aritmetiği (özellikle modüler çarpma işlemini) hızlı gerçekleştirmek için kullanılır.
  - İşlemler daha hızlı yapılır ve modüler indirgeme kolaylaşır.
- **Jacobian Koordinatları**:
  - Eğri üzerindeki işlemleri hızlandırmak için affine koordinatlar yerine Jacobian koordinatları kullanılmıştır.
  - Bu dönüşüm sayesinde hesaplama sırasında pahalı modüler ters alma işlemlerinin sayısı azalır.

Jacobian Koordinatları Nasıl Bir Projektif Koordinat Türüdür?

Jacobian koordinatları, projektif koordinatların özel bir şeklidir. Jacobian koordinatlarda dönüşüm şöyledir:

$$x = \frac{X}{Z^2}, \quad y = \frac{Y}{Z^3}$$

- Jacobian koordinatlarının özelliği, modüler ters işlemlerinin sayısını en aza indirmesidir.

- Jacobian koordinatlar, özellikle Montgomery çarpımı ile birlikte çok iyi performans sağlar.

Mimari Yapısı:

Mimari, aşağıdaki bileşenlerden oluşur:

1. **Montgomery Çarpım Ünitesi (IDDMM)**:
    - İşlemleri paralelleştiren, 8 aşamalı boru hattı (pipeline) yapısıyla hızlandırılmıştır.
    - Farklı bit uzunluklarını destekler ve yüksek saat hızlarında çalışır.
2. **PADD (Nokta Ekleme) ve PDBL (Nokta Katlama)**:
    - Eğri üzerinde gerçekleştirilen temel işlemlerdir.
    - İki Montgomery çarpıcı ile paralel işlemler gerçekleştirilir ve hesaplama hızı artar.
3. **Sonlu Durum Makinesi (FSM)**:
    - ECC algoritmalarını koordine eder ve hesaplamaları kontrol eder.

Sonuç Olarak:

Donanım: ECPM'nin tüm matematiksel işlemleri (Montgomery çarpımı, PADD, PDBL, ters alma) FPGA'da donanım olarak yapılıyor. Sistem, bağımsız bir şekilde çalışacak şekilde tasarlanmış.

Yazılım: Çalışma zamanında aktif bir yazılım yok. Yazılım, sadece FPGA' yı programlamak, parametreleri yüklemek ve test yapmak gibi yardımcı rollerde kullanılmış.

---

6) A 521-bit Dual-Field Elliptic Curve Cryptographic Processor with Power Analysis Resistance (2010)

Eliptik eğri kriptografisi (ECC) için 521-bitlik bir donanım işlemcisi tasarımı sunuyor. Bu işlemci, hem GF(p) hem de GF(2^n) alanlarında çalışıyor, enerji verimli, hızlı ve güç analizi saldırılarına karşı dayanıklı.

Bu makale, ECC'nin temel işlemi olan **nokta çarpımı (ECSM - Elliptic Curve Scalar Multiplication)** için bir donanım işlemcisi öneriyor. Öne çıkan özellikler:

- **Dual-Field Desteği:** Hem GF(p) (asal alan) hem GF(2^n) (ikili alan) üzerinde çalışıyor.
- **Hız ve Verimlilik:** Yeni bir bölme algoritması ve tam boru hattı (pipelined) tasarımı ile optimize edilmiş.
- **Güç Analizi Direnci:** SPA (Simple Power Analysis) ve DPA (Differential Power Analysis) saldırılarına karşı koruma sağlıyor.

- **Uygulama:** 90 nm CMOS teknolojisiyle üretilmiş, 521-bit GF(p)'de 19.2 ms, GF(2^409)'da 8.2 ms işlem süresi sunuyor.

Ana Yenilikler

Makale, üç büyük yenilik sunuyor:

1. **Yeni Birleşik Bölme Algoritması:**
    - Geleneksel Montgomery bölme, ters alma (inversion) ve ardından çarpma gerektiriyor (n ~ 3n iterasyon). Bu yavaş ve enerji harcıyor.
    - Yeni algoritma, çarpma ve bölmeyi tek bir birimde birleştiriyor, iterasyon süresini azaltıyor ve enerji tasarrufu sağlıyor.
2. **Ücretsiz Ön Hesaplama (Free Pre-Computation):**
    - Nokta koordinatlarını Montgomery alanına çevirmek veya geri döndürmek için ek işlem gerekmiyor. Bu işlemler, GFAU (Galois Field Arithmetic Unit) tarafından anlık olarak yapılıyor.
3. **Güç Analizi Koruması:**
    - **Double-and-Add-Always:** Her zaman çiftleme ve toplama yaparak işlem düzenini sabit tutuyor (anahtar sızıntısını önlüyor).
    - **Key-Blinding:** Anahtara rastgele bir sayı eklenerek gizleniyor, böylece güç izlerinden anahtar çıkarılamıyor.

Sistem Mimarisi

İşlemci, şu bileşenlerden oluşuyor:

1. **Galois Field Arithmetic Unit (GFAU):**
    - Montgomery çarpma, bölme, toplama ve çıkarmayı bit düzeyinde birleştiriyor.
    - **CSA (Carry-Save Adder) + CPA (Carry-Propagate Adder):** İteratif işlemleri hızlandırıyor. GF(2^n) için CSA'nın XOR özelliği paylaşılıyor.
    - **Tam Boru Hattı:** Kritik yol (critical path) iki aşamaya bölünüyor (UV karşılaştırması ve RS hesaplama), bu da hızı artırıyor (Şekil 2).
2. **EC Kontrol Birimi:**
    - 521-bit verileri register'larda tutuyor ve GFAU'ya yönlendiriyor.
    - 32-bit döngüsel kaydırma register'ları kullanılarak alan tasarrufu sağlanıyor (multiplexer karmaşası azalıyor).
3. **Güç Analizi Koruması:**
    - Anahtar körleme (key-blinding) ve düzenli hesaplama (Şekil 4), donanımda uygulanıyor.

Matematiksel Temel

- **Montgomery Çarpma (Algorithm 1):** $\text{MonMul}(A,B) \equiv a \cdot b \cdot r^{-1} \bmod p$, $r = 2^n$
- **Montgomery Bölme:** Yeni algoritma (Algorithm 3), R ve S operandlarını iteratif olarak hesaplıyor. UV karşılaştırması ve RS güncellemesi boru hattında yapılıyor.
- **Alan Dönüşümü:**
    - Integer → Montgomery: $\text{MonDiv}(a,1) \equiv a \cdot 2^{n} \bmod p$

- Montgomery → Integer: MonMul(a·2^n, 1)≡amod p

Performans ve Ölçüm Sonuçları

- **Üretim:** 90 nm CMOS 1P9M, 0.26 mm^2 çekirdek alan tasarrufu (döngüsel register'larla %60'tan %88 kullanım).
- **ECSM Süreleri:**
  - GF(p_521): 19.2 ms, 58.5 mW.
  - GF(2^409): 8.2 ms, 86.4 mW.
  - GF(2^409, sadece ikili alan): 2.37 ms, 96K kapı (dummy işlem olmadan).
- **Güç Analizi Testleri:**
  - Korunmasız çip: SPA'da 112 mV/57 mV tepe farkı, DPA'da 500 izle sızıntı.
  - Korumalı çip: SPA'da <20 mV (gürültü altı), DPA'da 120K izle bile sızıntı yok (Şekil 7, 8).

---

7) A High Speed Coprocessor for Elliptic Curve Scalar Multiplications over Fp

Bu makale, eliptik eğri skaler çarpımını (scalar multiplication) asal alanlar (Fp) üzerinde hızlı bir şekilde gerçekleştirmek için FPGA tabanlı bir yardımcı işlemci (coprocessor) mimarisi sunuyor. Makale, Residue Number System (RNS) kullanarak yüksek hız ve yan kanal saldırılarına karşı direnç sağlamayı hedefliyor.

Makalenin Amacı Nedir?

Makale, eliptik eğri kriptografisi (ECC) için skaler çarpım işlemini ([k]G) genel asal alanlar (Fp) üzerinde FPGA'da çok hızlı bir şekilde gerçekleştirmeyi amaçlıyor. Ana hedefler:

- **Hız:** 160 bitlik bir eğri için 1 ms'nin altında (örneğin, 0.32 ms) skaler çarpım yapmak.
- **Esneklik:** NIST gibi özel asallara bağlı kalmadan, herhangi bir asal p için çalışmak.
- **Güvenlik:** Yan kanal saldırılarına (SPA ve DPA) karşı dirençli bir tasarım sunmak.
- **Rekor:** Genel Fp üzerinde FPGA'da en hızlı skaler çarpım mimarisi olduğunu iddia ediyor.

Bu tasarım, özellikle IPSEC gibi yüksek hız, düşük gecikme ve güvenlik gerektiren uygulamalar için düşünülmüş.

Temel Kavramlar

Eliptik Eğri Skaler Çarpımı ([k]G)

- ECC'nin en zaman alan işlemi: Bir eğri üzerindeki noktayı (G) bir tamsayı (k k k) ile çarpmak ([k]G=G+G+⋯+G, k kez).
- Matematiksel olarak: $y^2 = x^3 + a_4 x + a_6 \mod p$ denklemiyle tanımlı bir eğri üzerinde çalışıyor.
- Güvenlik: "Eliptik Eğri Ayrık Logaritma Problemi"ne (ECDLP) dayanıyor.

Residue Number System (RNS)

- Büyük sayıları temsil etmenin alternatif bir yolu: Sayılar, birbiriyle asal olan küçük modüller (kanallar: m1,m2,...,mn) üzerinden temsil ediliyor.
- Örnek: X sayısının RNS gösterimi {|X|m1,|X|m2,...,|X|mn}.
- Avantaj: Toplama, çıkarma ve çarpma işlemleri her kanalda bağımsız ve taşıma (carry) olmadan yapılıyor, bu da paralel hesaplamayı kolaylaştırıyor.
- Dezavantaj: Modüler redüksiyon ve taban dönüşümü (base extension) karmaşık.

Montgomery Redüksiyonu

- Büyük sayıları p moduna indirgemek için kullanılan bir algoritma.
- RNS ile birleştirildiğinde (Algorithm 1), çarpma sonrası redüksiyonu hızlandırıyor.
- Çıktı: $S = |X .M^{-1}|_p$ ve $S<2p$.

Makalede Ne Yapılmış?

1. RNS Tabanlı Mimari

- **Fikir:** Klasik çok hassasiyetli (multi-precision) aritmetik yerine RNS kullanılıyor. Bu, çarpma işlemlerini "neredeyse bedava" hale getiriyor çünkü her kanalda bağımsız yapılıyor.
- **Kawamura'dan İlham:** Daha önce RSA için önerilen RNS tabanlı Cox-Rower mimarisi [10], ECC için yeniden tasarlanmış.
- **Yenilik:**
    - ECC'ye uygun hale getirilmiş: Nokta toplama ve ikiye katlama işlemleri için AB+CD gibi desenler tek redüksiyonda hesaplanıyor.
    - Daha derin pipeline (6 aşama) ile yüksek saat frekansı (örneğin, 165 MHz).
    - Genel eğriler için çalışması sağlanmış (NIST'e bağımlı değil).

2. Donanım Tasarımı

- **Rower Modülleri:** Her kanal için bir işlem birimi. Çarpma ($|x \cdot y|_m$) ve toplama işlemlerini tek döngüde yapıyor.
- **Cox Modülü:** Taban dönüşümünde yaklaşık hesaplama (γ) için yardımcı birim.
- **Pipeline:** 6 aşamalı bir pipeline, işlemlerin %90'ını dolu tutuyor (Şekil 2).
- **GPR (General Purpose Registers):** Her kanal için 16 kayıt, yerel değişkenleri tutuyor ve paralel hesaplamayı destekliyor.

3. Algoritmalar

- **Montgomery Ladder (Algorithm 2):** SPA'ya dirençli bir skaler çarpım algoritması. Her bit için bir toplama ve bir ikiye katlama yapıyor.
- **Nokta İşlemleri:** Proje koordinatları kullanılarak inversiyon (ters alma) önleniyor. Formüller RNS için optimize edilmiş (Tablo, Sayfa 5).
- **RNS-Radix Dönüşümü:** Klasik sayı temsiline dönüş ücretsiz yapılıyor (3.4).

4. Güvenlik

- **SPA Direnci:** Montgomery Ladder sayesinde her bit için aynı işlem sırası, zamanlama sızıntısını önlüyor.
- **DPA Direnci:** Rastgele koordinat değişimi (GG'nin temsili değiştiriliyor) ve k'ya rastgele ekleme ile güç analizi zorlaştırılıyor.

Nasıl Çalışıyor?

Matematiksel Temel

- **RNS Temsili:** $M=m1 \cdot m2 \cdots mn$ ve $X<M$ için $X=\{|X|_{m1},\ldots,|X|_{mn}\}$.
- **Montgomery Redüksiyonu (Algorithm 1):**
  - Giriş: $X<\alpha p^{(2)}$ (örneğin, $\alpha=45$).
  - Çıkış: $S = |X .M^{-1}|_p$ ve $S<2p$.
  - İki taban (B ve $\bar{B}$) arasında dönüşüm yaparak çalışıyor.
- **Nokta Toplama ve İkiye Katlama:** AB+CD gibi ifadeler tek redüksiyonda hesaplanıyor, bu RNS'nin avantajını artırıyor.

Donanım Mimarisi

- **Rower:** Her kanal için $|x \cdot y+acc|_m$ işlemini yapıyor. 5-6 aşamalı pipeline ile yüksek frekans elde ediliyor (Şekil 2).
- **Cox:** Taban dönüşümünde γ'yı yaklaşık hesaplıyor.
- **ROM ve GPR:** Ön hesaplamalar (örneğin, p^{-1}, M_i^{-1}) ROM'da tutuluyor, değişkenler GPR'da işleniyor.
- **Taban Seçimi:** $m_i = 2^r - \epsilon i$ (pseudo-Mersenne) şeklinde, çarpma ve redüksiyonu kolaylaştırıyor.

Performans

- **Stratix II (90 nm):** 160 bit için 0.32 ms (165 MHz), 256 bit için 0.68 ms (157 MHz).
- **Stratix (130 nm):** 160 bit için 0.57 ms (92 MHz), 256 bit için 1.17 ms (90 MHz).

Sonuçlar Ne Gösteriyor?

- **Hız:** 160 bitlik bir eğri için 0.32 ms (Stratix II), literatürdeki genel Fp tasarımlarından (örneğin, [11]'de 1 ms) daha hızlı.
- **Kaynak Kullanımı:** Örneğin, 256 bit için 9177 ALM ve 96 DSP (Stratix II).
- **Karşılaştırma:**
    - **[23] (RNS):** 1.77 ms (160 bit), daha yavaş ve büyük.
    - **[11] (Multi-precision):** 1 ms (160 bit), daha yavaş ama alan/hız oranı iyi.
    - **[7] (NIST-specific):** 0.36 ms (224 bit), daha hızlı ama sadece NIST asalları için.

RNS'nin avantajı, büyük eğrilerde (örneğin, 512 bit) bile hızın düşmemesi.

Neden Önemli?

- **Hız ve Esneklik:** Genel Fp üzerinde rekor hız sunuyor, eğri seçimi özgürlüğü sağlıyor.
- **Güvenlik:** Yan kanal saldırılarına karşı doğal direnç.
- **Gelecek Potansiyeli:** ASIC'e geçiş için uygun bir temel.

---

8) Ultra High Performance ECC over NIST Primes on Commercial FPGAs (2008)

Bu makale, eliptik eğri kriptografisi (ECC) için FPGA tabanlı ultra yüksek performanslı bir mimari sunuyor ve özellikle NIST asal alanları (P-224 ve P-256) üzerinde çalışıyor.

Bu makale, ECC'nin temel işlemi olan "nokta çarpımı" (point multiplication) işlemini FPGA üzerinde çok hızlı bir şekilde gerçekleştirmek için yeni bir donanım mimarisi öneriyor. Özellikle, asal alanlar (GF(p)) üzerinde çalışan ECC sistemlerini hedefliyor ve NIST standartlarındaki P-224 ve P-256 asallarını kullanıyor. Ana hedef:

- **Hız:** Tek bir FPGA çipinde saniyede 37.000'den fazla nokta çarpımı yapmak.
- **Verimlilik:** FPGA'nın DSP (Digital Signal Processing) bloklarını kullanarak kaynak tüketimini azaltmak.
- **Standart Uyumluluğu:** Avrupa ve ABD'de tercih edilen NIST asallarını desteklemek.

Makalede Ne Yapılmış?

1. Yenilik: DSP Bloklarının Kullanımı

- Modern FPGA'larda (örneğin, Xilinx Virtex-4) bulunan DSP blokları, normalde sinyal işleme için tasarlanmış çarpma, toplama ve çıkarma birimleridir.
- Bu makalede, ECC'nin tüm aritmetik işlemleri (modüler çarpma, toplama, çıkarma ve redüksiyon) bu DSP bloklarına taşınmış. Böylece, FPGA'nın genel lojik elemanları (LUT'lar) yerine hazır donanım birimleri kullanılmış.
- Avantaj: Daha yüksek hız (yaklaşık 500 MHz) ve daha az kaynak tüketimi.

2. Mimari Tasarım

- **Modüler Aritmetik:** ECC'nin temel işlemleri (nokta toplama ve ikiye katlama), modüler çarpma, toplama ve çıkarma gerektiriyor. Bunlar DSP bloklarında paralel olarak yapılıyor.
- **NIST Redüksiyonu:** NIST asalları (P-224 ve P-256) için özel redüksiyon algoritmaları kullanılmış. Bu algoritmalar, pahalı bölme işlemini ortadan kaldırıp sadece toplama ve çıkarma ile çalışıyor (Algorithm 1 ve 2).
- **Proje Koordinatları:** Ters alma (inversion) işlemini pahalı bulan yazarlar, affine yerine projective (Chudnovsky) koordinatları tercih etmiş. Bu, donanımda daha verimli.

3. Performans Sonuçları

- **Tek Çekirdek:** Küçük bir FPGA'da (XC4VFX12), P-256 için bir nokta çarpımı 620 µs'de tamamlanıyor (1614 işlem/saniye).
- **Çok Çekirdek:** Büyük bir FPGA'da (XC4VSX55), 16-18 çekirdek paralel çalıştırılarak P-224 için 37.700 işlem/saniye elde edilmiş.
- Bu, literatürdeki diğer FPGA tabanlı ECC implementations'larından çok daha hızlı.

Donanım Tasarımı

1. **DSP Kullanımı:**
    - Her DSP bloğu, 18-bit çarpma ve 48-bit toplama/çıkarma yapabiliyor.
    - Büyük sayılar (224 veya 256 bit) için DSP'ler kaskad (cascade) halinde bağlanıyor.
    - Pipeline register'lar kullanılarak maksimum frekans (500 MHz) elde ediliyor.
2. **Modüler İşlemler:**
    - **Toplama/Çıkarma:** Algorithm 3'te gösterildiği gibi, iki DSP bloğuyla paralel yapılıyor. Carry (taşma) yönetimi için ek lojik kullanılmış.
    - **Çarpma:** Schoolbook yöntemiyle, n2 n^2 n2 karmaşıklıkta, DSP'lerde paralel hesaplanıyor (Şekil 3 ve 4).
    - **Redüksiyon:** NIST algoritmaları (Algorithm 1 ve 2) DSP'lerde toplama/çıkarma zinciriyle uygulanıyor. Look-Ahead Logic (LAL) ile overflow/underflow önceden tahmin ediliyor (Şekil 5).

3. **ECC Çekirdeği:**

- Çarpma ve toplama/çıkarma birimleri, BRAM (RAM modülleri) ve bir durum makinesi (state machine) ile birleştirilmiş (Şekil 6).
- Çekirdek, k·P k \cdot P k·P ve k·P+r·Q k \cdot P + r \cdot Q k·P+r·Q gibi işlemleri destekliyor (ECDSA için önemli).

Paralellik

- DSP bloklarının az lojik eleman kullanması, birden fazla çekirdeğin aynı FPGA'ya sığmasını sağlıyor. XC4VSX55'te 512 DSP bloğuyla 16-18 çekirdek çalışıyor.

---

9) **Hardware Elliptic Curve Cryptographic Processor Over GF(p): (2006)**

Bu makale, eliptik eğri kriptografisi (ECC) için GF(p) (sonlu alan) üzerinde çalışan bir donanım işlemcisi tasarımı sunuyor. Makalenin temel amacı, ECC sistemlerinde kullanılan temel matematiksel işlemleri (modüler ters alma, çarpma, toplama ve çıkarma) hızlandıran bir mimari geliştirmek.

Bu makaledeki işlemci:

- **Modüler ters alma** (inversion) ve **Montgomery modüler çarpma** gibi temel işlemleri optimize ediyor.
- Bir FPGA üzerinde 256-bitlik bir skaler nokta çarpımını (point multiplication) **3.86 milisaniyede** gerçekleştiriyor; bu, o tarihte FPGA için rapor edilen en hızlı süre.

Makale, iki büyük yenilik sunuyor:

1. **Birleşik Modüler Ters Alma Algoritması (Unified Inversion Algorithm):**
   - Geleneksel yöntemler (örneğin Fermat'nın Küçük Teoremi), modüler ters alma için çok fazla işlem (modüler üs alma gibi) gerektiriyor ve bu yavaş.
   - Yeni algoritma, hem klasik ters almayı (a^{-1} \mod p) hem de Montgomery ters almayı (a^{-1} 2^k \mod p) tek bir yapıda hesaplıyor.
   - Eski yöntemlere göre Montgomery çarpma sayısını %33 azaltıyor ve donanımda yer tasarrufu sağlıyor (%50'ye kadar).
2. **Tam Kelime Montgomery Çarpma (Full-Word Montgomery Multiplication):**
   - Klasik Montgomery çarpma, bit bazında çalışır ve çok saat döngüsü (clock cycle) gerektirir.
   - Bu tasarımda, tam kelime (örneğin 256-bit) çarpanlar kullanılıyor. Bu, daha az saat döngüsüyle (32 döngü) çarpma işlemini tamamlıyor ve yüksek veri hızı sağlıyor.

Bu iki yenilik, işlemciyi hem hızlı hem de esnek hale getiriyor. Ayrıca dört farklı modüler ters alma türünü destekliyor, bu da farklı ECC uygulamalarına uyum sağlıyor.

Matematiksel Temel: ECC ve GF(p)

Eliptik eğri kriptografisi, şu Weierstrass denklemiyle tanımlı eğriler üzerinde çalışıyor:

E: y^2 = x^3 + ax + b \mod p

- p : Büyük bir asal sayı (örneğin 256-bit).
- a,ba, ba,b: Denklem parametreleri, 4a^3 + 27b^2 ≠0 mod p olmalı.
- Nokta çarpımı (eP): Bir nokta P'yi e kez kendisiyle toplamak (örneğin eP=P+P+⋯+P).

Bu işlem, **double-and-add** algoritmasıyla yapılıyor:

- eee'nin ikili (binary) gösterimine bakarak toplama ve iki katına çıkarma (doubling) adımları uygulanıyor.
- Afin koordinatlarda her toplama/çiftleme için modüler ters alma gerekiyor; bu yüzden projektif koordinatlar tercih ediliyor (sadece son adımda bir ters alma).

Donanım Mimarisi

İşlemci, şu bileşenlerden oluşuyor:

1. **Modüler Ters Alma Birimi:**
    - Yeni birleşik algoritma kullanıyor (Algorithm 6).
    - 256-bitlik bir ters alma, 586 saat döngüsünde 14.64 μs'de tamamlanıyor.
    - FPGA'da tek bir devreyle hem klasik hem Montgomery ters almayı yapıyor.
2. **Montgomery Çarpma Birimi:**
    - Tam kelime çarpma kullanıyor; 256-bit çarpma 32 döngüde 0.70 μs'de bitiyor.
    - Geleneksel bit bazlı yöntemlere göre daha az döngü, benzer gecikme (critical path delay).
3. **Toplama ve Çıkarma Birimleri:**
    - Basit işlemler; 2 döngüde 51 ns'de tamamlanıyor.
4. **ECC İşlemcisi:**
    - Tüm bu birimleri birleştiriyor. 256-bit skaler nokta çarpımı 151,360 döngüde 3.86 ms'de tamamlanıyor.
    - Xilinx Virtex2 Pro FPGA'da uygulanmış (39.46 MHz, 15,755 dilim).

---

10) A Parallel Processing Hardware Architecture for Elliptic Curve Cryptosystems (2006)

Bu makale, eliptik eğri kriptografisi (ECC) için paralel işlemci mimarisi öneriyor ve EC nokta çarpımını (point multiplication) hızlandırmayı hedefliyor.

Bu makale ECC'nin temel işlemi olan nokta çarpımını yavaş bulamaktadır. Yaptığı işlemler:

- Birden fazla **Modüler Aritmetik Mantık Birimi (MALU)** kullanarak paralel işlem yapıyor.
- **Komut düzeyinde paralellik (ILP)** dinamik olarak kontrol edilerek performansı artırıyor.
- Sonuç: Tek bir işlem birimine kıyasla **1.6 kat hız artışı** sağlıyor (GF(p) ve GF(2^m) üzerinde)

Makale, şu yenilikleri öne çıkarıyor:

1. **Paralel MALU Kullanımı:**
    - Birden fazla MALU (örneğin 2, 3 veya 4) aynı anda çalışabiliyor.
    - Önceki çalışmalar sadece iki birimi paralel kullanıp sabit algoritmalarla sınırlıydı (örneğin nokta toplama ve çiftleme). Bu tasarım ise esnek: herhangi bir nokta çarpım algoritmasına uyum sağlıyor.
2. **Dinamik ILP Kontrolü:**
    - İşlemci, komutları çalıştırırken bağımlılıkları (data dependency) anlık olarak kontrol ediyor ve paralel çalışabilecek işlemleri birden fazla MALU'ya dağıtıyor.
    - Bu, modern RISC CPU'lardaki **super-scalar** mimariye benziyor.
3. **Esnek ve Birleşik Tasarım:**
    - Hem GF(p) (asal alan) hem GF(2^m) (ikili alan) üzerinde çalışıyor.
    - MALU'ların sayısı ve yapılandırması ayarlanabilir, bu da performansı optimize etmeyi kolaylaştırıyor.

Sistem Mimarisi

İşlemci şu bileşenlerden oluşuyor (Şekil 1'e dayanarak):

1. **Ana Kontrolör:**
    - Komutları sabit aralıklarla gönderiyor (her döngüde bir komut).
    - Normal bir CPU yerine özel bir kontrolör kullanılıyor; bu, daha hızlı ve kompakt.
2. **Modüler Aritmetik Mantık Birimleri (MALU'lar):**
    - Birden fazla MALU, işlemleri paralel yapıyor.
    - Her MALU, Montgomery modüler çarpma algoritmasını destekliyor.

3. **Paylaşımlı SRAM (RAM):**
    - Tüm MALU'lar tek bir RAM'e erişiyor. Veri ve komutlar ayrı veri yollarıyla (Harvard mimarisi) taşınıyor.
4. **Komut Kuyruk Tamponu (IQB):**
    - Komutları tamponluyor ve ILP'yi kontrol ederek MALU'lara dağıtıyor.
    - Hız farklarını dengeliyor (komut gönderme vs. işlem hızı).
5. **Veri ve Komut Yolları:**
    - Veri Otobüs Kontrolörü (DBC): RAM ile kontrolör arasında veri transferini yönetiyor.
    - Komut Otobüs Kontrolörü (IBC): Komutları IQB'ye yönlendiriyor.

Program ROM'u, 596 bayt ile hem GF(p) hem GF(2^m) için tüm komutları saklıyor.

MALU Tasarımı

MALU'nun veri yolu (Şekil 2), Montgomery modüler çarpma için tasarlanmış:

- **Carry-Save Adder (CSA) Aşaması:**
    - Dört girişi (xy, mn, vs, vc) toplayan 4-2 CSA'lar kullanıyor.
    - Çıktı, yedekli CS formunda (2vc + vs) ve her çarpma sonucu bir bit sağa kaydırılıyor.
    - GF(p) ve GF(2^m) için bit-seri Montgomery çarpma yapıyor.
- **Carry-Propagate Adder (CPA) Aşaması:**
    - CS formunu normal sayıya çeviriyor (sadece GF(p) için).
    - CPA, performansı artırmak için ayrı bir birim olarak eklenmiş.
- **Esneklik:**
    - Digit boyutu (d) ve alan boyutu (k) ayarlanabilir.
    - Denklem: MALU_N(XR,YR,SR)=(XY±S)RmodN
        - R = 2^{k+4}, son indirgeme adımlarını önlüyor.

Bir MALU işlemi şu adımlardan geçiyor (Şekil 3):

1. Komut alma ve çözme (IF, ID).
2. RAM'den veri yükleme (R).
3. CS aşaması ([(k+4)/d] döngü).
4. CP aşaması (GF(p) için l döngü).
5. RAM'e yazma (W).

Komut Düzeyinde Paralellik (ILP)

- **Strateji:** IQB'de iki veya daha fazla komut varsa, veri bağımlılığı kontrol ediliyor.
- **Kural:** Bir MALU komutu (R=X,Y,S) dört adres içeriyor. Eğer iki komutun adresleri çakışmıyorsa (örneğin R1≠X2,Y2,S2) paralel çalışabiliyor.
- **Örnek (Şekil 3):** GF(p) üzerinde birden fazla komut paralel yürütülüyor, ancak RAM çakışmasını önlemek için 3 döngü bekleme süresi var.

Performans Değerlendirmesi

Tablo 1, 160-bit ve 256-bit ECC için döngü sayılarını gösteriyor:

- **GF(p):**
  - 1 MALU: 160-bit için 128,519 döngü, 256-bit için 330,759 döngü.
  - 4 MALU: 160-bit için 80,249 döngü, 256-bit için 206,149 döngü.
  - Hız artışı: ~1.6 kat.
- **GF(2^m):**
  - Benzer şekilde, 4 MALU ile 1.6 kat hız artışı.

Makale, eliptik eğri kriptografisi (ECC) için bir paralel işlemci tasarlıyor ve bu işlemci, iki farklı matematiksel alan üzerinde çalışacak şekilde esnek bir yapıya sahip:

1. **GF(p):** Bu, asal bir sayıya (p) dayalı sonlu bir alan. Örneğin, ppp büyük bir asal sayı olabilir (160-bit veya 256-bit gibi). ECC'de genellikle daha yaygın kullanılır ve işlemler modüler aritmetikle (mod ppp) yapılır.
2. **GF(2^m):** Bu, 2 tabanlı bir polinom alan (binary field). mmm, alanın derecesini temsil eder (örneğin 160 veya 256). Burada işlemler polinomlar üzerinden yapılır ve modüler indirgeme farklı bir şekilde işler (bir indirgenemez polinom kullanılır).

Makaledeki **Modüler Aritmetik Mantık Birimi (MALU)**, bu iki alan için Montgomery modüler çarpma algoritmasını destekliyor. Yani, aynı donanım hem GF(p) hem de GF(2^m) işlemlerini yapabiliyor, ancak bazı farklılıklar var:

- **GF(p) için:** MALU, hem **Carry-Save (CS)** aşamasını hem de **Carry-Propagate (CP)** aşamasını kullanıyor. CP aşaması, yedekli CS formunu normal bir sayıya çevirmek için gerekli (çünkü GF(p)'de tam sayı sonuçlar lazım).
- **GF(2^m) için:** CP aşaması atlanıyor. Çünkü ikili alanda taşıma (carry) yayılımına gerek yok; işlemler polinomlar üzerinden XOR gibi basit operasyonlarla yapılıyor.

Nasıl Çalışıyor?

- **Esneklik:** MALU'nun veri yolu, digit boyutu (d) ve alan boyutu (k) ayarlanabilir şekilde tasarlanmış. Bu, hem GF(p) hem GF(2^m) için uygun hale getiriyor.
- **Montgomery Çarpma:** Her iki alan için de temel işlem MALU_N(XR,YR,SR)=(XY±S)RmodN şeklinde ifade ediliyor. N, GF(p) için asal sayı p, GF(2^m) için ise indirgenemez polinom oluyor.
- **Mode Seçimi:** Sistemde bir **Mode register** var; bu, hangi alanda çalışılacağını belirtiyor (GF(p) veya GF(2^m)).

Kaynakça:

1) Örs Yalçın, S. B. (2005). *Hardware design of elliptic curve cryptosystems and side-channel attacks* (Doctoral dissertation, Katholieke Universiteit Leuven, Belgium)
2) Xie, Y., Yan, R., Liu, Y., Zheng, X., Cai, S., & Xiong, X. (2024). A high-performance hardware accelerator for ECC in GF(p) over generic Weierstrass curves. *IEEE Embedded Systems Letters*.
3) Chen, J., & Tan, N. (2024). A compact elliptic curve cryptography accelerator over prime field for system-on-chips. In *Proceedings of the 2024 9th International Conference on Integrated Circuits and Microsystems (ICICM)* (pp. 820–825). IEEE.
4) Xu, X., Song, M., & Zeng, X. (2024). High-speed and secure ECC processor for Chinese SM2 using modified Karatsuba multiplier based on FPGA. *IEICE Transactions on Communications*. Advance online publication.
5) Xie, Y., Liu, Y., Zheng, X., Zhu, W., Li, J., Cai, S., & Xiong, X. (2022). A dual-core high-performance processor for elliptic curve cryptography in GF(p) over generic Weierstrass curves. *IEEE Transactions on Circuits and Systems II: Express Briefs, 69*(11), 4523–4527
6) Amiet, D., Curiger, A., & Zbinden, P. (2016). Flexible FPGA-based architectures for curve point multiplication over GF(p). In *Proceedings of the 2016 Euromicro Conference on Digital System Design (DSD)* (pp. 107–114). IEEE.
7) Lee, J.-W., Chen, Y.-L., Tseng, C.-Y., Chang, H.-C., & Lee, C.-Y. (2010). A 521-bit dual-field elliptic curve cryptographic processor with power analysis resistance. In *Proceedings of the 2010 IEEE Asian Solid-State Circuits Conference (A-SSCC)* (pp. 206–209). IEEE
8) Guillermin, N. (2010). A high speed coprocessor for elliptic curve scalar multiplications over Fp. In *Proceedings of the 2010 Workshop on Cryptographic Hardware and Embedded Systems (CHES)* . Springer, IACR
9) Güneysu, T., & Paar, C. (2008). Ultra high performance ECC over NIST primes on commercial FPGAs. In *Proceedings of the 10th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2008)* (pp. 62–78). Springer, IACR
10) McIvor, C. J., McLoone, M., & McCanny, J. V. (2006). Hardware elliptic curve cryptographic processor over GF(p). *IEEE Transactions on Circuits and Systems I: Regular Papers, 53*(9), 1946–1957
11) Sakiyama, K., De Mulder, E., Preneel, B., & Verbauwhede, I. (2006). A parallel processing hardware architecture for elliptic curve cryptosystems. In *Proceedings of the 2006 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. III–904–III–907). IEEE