Serial vs. Parallel Elliptic Curve Crypto Processor Designs

Abdul-Aziz Tabakh, Ayed Al-Qahtani, Alaaeldin Amin
King Fahd University of Petroleum & Minerals (KFUPM)

Outline

- Introduction
  - Crypto-systems
  - Elliptic curve cryptography (ECC)
  - Aladdin Modulo Multiplier
  - Architecture & Development
  - Experiment results & Comparison
- Achievements & Conclusions

Classic Cryptography

- Substitution (Caesar)
  - Transposition
  - Enigma Machine
  - Vigenere
  - Block (Hill)
- Vernam (one time pad)
  - DES
  - AES

Symmetric-key algorithms

- Symmetric-key cryptography
  - encryption/decryption is performed using one secret key:
    e.g. DES and AES.
  - Advantage: they are faster in execution
    - straightforward transformations.
    - can be pipelined to give better performance.
  - Problem is to find efficient method to exchange keys securely: key distribution problem.
  - If secret key is disclosed during key exchange >>> whole symmetric key crypto algorithm >>> >>> completely vulnerable.
Simple Example of PKC

Non-mathematical

- Bob has a box and a padlock which only he can unlock once it is locked
- Alice wants to send a message to Bob
- Bob sends its box and the padlock unlocked to Alice
- Alice puts its message in the box and locks the box using Bob’s padlock and sends it to Bob – thinking that the message is safe since it is Bob that can unlock the padlock and accesses the contents of the box.
- Bob receives the box, unlocks the padlock and reads the message

Public-key cryptography

- Public-key crypto algorithms (asymmetric cryptographic algorithms) e.g. RSA use separate public and private keys to perform encryption and decryption.
- The public key is made widely available and is used by communicating parties to encrypt data. Only the party with the correct corresponding private key can decrypt data.
- Public-key algorithms are the most secure cryptographic algorithms because they are based on an underlying mathematically hard-to-solve problem like integer factorization problem, discrete logarithm problem etc.
- They are also substantially slower than symmetric-key cryptography algorithms.
- Public key algorithms are commonly used in practice for the transport of keys subsequently used for bulk data encryption and decryption by symmetric-key algorithms and other applications.

Other Cryptographic Applications

- Digital Signatures: allows electronically sign (personalize) the electronic documents, messages and transactions
- Identification: is capable of replacing password-based identification methods with more powerful (secure) techniques
- Key Establishment: To communicate a key to your correspondent (or perhaps actually mutually generate it with him) whom you have never physically met before
- Secret Sharing: Distribute the parts of a secret to a group of people who can never exploit it individually

Why Elliptic Curve Cryptography (ECC)?

- Integer factorization problems (RSA)
- Discrete Logarithm problems (Diffie-Helman, ElGamal)
- Elliptic Curve Cryptosystems (ECC)

<table>
<thead>
<tr>
<th>Algorithm Family</th>
<th>Bit Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integer Factorization (IF)</td>
<td>1024</td>
</tr>
<tr>
<td>Discrete Logarithm (DL)</td>
<td>1024</td>
</tr>
<tr>
<td>Elliptic Curve Crypto (ECC)</td>
<td>160</td>
</tr>
</tbody>
</table>
Elliptic curve cryptography (ECC)

- Elliptic curve in GF(P)
  - $y^2 = x^3 + ax + b$
- Enc/Dec:
  - Enc:
    - Choose a random integer $C$
    - ECC doubling and adding operations done,
  - Dec:
    - Use Aladdin modular multipliers.
    - Elimination of inversion => Projective Coordinates.
    - Show the gain obtained using VHDL.

Aladdin Modulo Multiplier

- It is required to compute $P = A \cdot B \mod N$ where $A, B, N$ are $n$-bits unsigned integers.

Study

- ECC doubling and adding operations done,
  - In sequence.
  - In parallel.
- Performance, speed, and area comparison.
- Show the gain obtained using VHDL.
- Use Aladdin modular multipliers.
**Architecture & Development**
- VHDL is used to model the algorithms.
- Synthesize it of FPGA.
- Evaluate the speed and find out the space occupied.
  - Speed and space is the most important metrics for evaluating any digital design.

**Registers contents – point adding**

<table>
<thead>
<tr>
<th>Port No</th>
<th>Component</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data</td>
<td>00000000</td>
</tr>
<tr>
<td>2</td>
<td>Control</td>
<td>00000000</td>
</tr>
<tr>
<td>3</td>
<td>Multiplier</td>
<td>00000000</td>
</tr>
<tr>
<td>4</td>
<td>Multiplier</td>
<td>00000000</td>
</tr>
</tbody>
</table>

**Experiment results & Comparison**
- The maximum clock frequency is 20.547MHz.
- The maximum clock period is 48.669ns.
- The total size of the design is equivalent to 394,472 gates.
  - **Data Path** = 344,876 gates
  - **Control Unit** = 1,419 gates (<1%)
  - **Buffering** = 48,177 gates

**Registers contents – point doubling**

<table>
<thead>
<tr>
<th>Port No</th>
<th>Component</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data</td>
<td>00000000</td>
</tr>
<tr>
<td>2</td>
<td>Control</td>
<td>00000000</td>
</tr>
<tr>
<td>3</td>
<td>Multiplier</td>
<td>00000000</td>
</tr>
<tr>
<td>4</td>
<td>Multiplier</td>
<td>00000000</td>
</tr>
</tbody>
</table>

**Experiment results & Comparison**
- Multipliers occupy the largest portion of the design (almost 35% is serial design and 42% is the parallel design).
- **Portion of designs** = parallel design is 3.3 times larger than the serial design.
Experiment results & Comparison

<table>
<thead>
<tr>
<th></th>
<th>Serial Design</th>
<th>Parallel Design</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT</td>
<td>2,039,797.5</td>
<td>1,724,380</td>
</tr>
<tr>
<td>AT²</td>
<td>39,776,051.25</td>
<td>8,621,900</td>
</tr>
<tr>
<td>A/T</td>
<td>2.1373x10¹⁰</td>
<td>5.94697x10¹⁰</td>
</tr>
</tbody>
</table>

- Parallel design is better in most cases.
- Serial is better when area is very important.

Achievements & Conclusions

- We implement Aladdin modulo multiplier
- We investigate the cost (Area & Time) tradeoffs for serial and parallel multiplier for ECC possessor.
- Exploiting parallelism boost up performance
- Parallel is better in most cases - excluding when hardware area is important

Thanks for the opportunity

Questions?