100% safe IP Core? – CryptOne as an example of new generation of secured IP Cores

Jacek Hanke, CEO Digital Core Design
Agenda

1. About Digital Core Design
2. Milestones
3. Security vs hardware
4. CryptOne
5. Summary
Digital Core Design has been founded in 1999 and since the early beginnings is focused in IP Cores improvement and System-on-Chip designs,

During these two decades, DCD’s launched more than 70 different architectures, among them e.g. World’s Fastest 8051 – the DQ80251 and royalty-free 32-bit CPU - the D32PRO,

DCD has sold more than 1000 license to various customers like corporations start-ups, R&D offices, universities and so on.
Milestones

- DQ80251, World's Fastest 8051
- DoCD™ Hardware Debugger
- DP8051 XP
- DRPIC 166X IP Core

EDN's Hot Products of 2012 for DQ80251 & DoCD

- DQ80251 Product of the Year Award
- EDN 2013 Hot Business Award

- DQ80251 presented at CeBIT 2013 opening ceremony
- DQ80251 awarded at EDN Hot 100 Products
- D32PRO presented at CeBIT 2013 opening ceremony
- D32PRO named Polish Product of the Future
- DCD among 4 most innovative companies in Poland

- D32PRO, royalty-free 32-bit CPU
- CryptOne, 100% safe crypto CPU
- D32PRO awarded with the „Teraz Polska” Prize

1999 DCD established

DCD’s IP Cores

500 customers
1000 licenses
More than 500,000,000 devices

Pls vote for CryptOne for "Best Innovative IP prize"
DCD’s IP Cores

☑ One of the most experienced companies in IP Core market

☑ More than 70 architectures in portfolio including 8-bit, 16-bit, 32-bit MCU, UART, I2C, SPI, I3C, USB, CAN, CAN-FD LIN, floating points ...

☑ Among them World’s Fastest & World’s Smallest 8051 & 80251

☑ Deeply embedded, royalty-free, fully scalable 32-bit CPU

☑ Technology independent (ASIC & FPGA)

☑ IP Cores tailored to the project needs

☑ Royalty-free solutions
Security, stupid*

There are a range of attack types...

- Physical Attacks: Fault injection: clock or power glitch, alpha ray, Side Channel Analysis (SCA), Probing, Focused in Beam (FIB) etc.
- Life Cycle Attacks: Code downgrading, Excess manufacturing, Integrity vulnerabilities
- Software Attacks: Buffer overflows, Interrupts, Malware etc.
- Communication attacks: Man in the Middle, Weak RNG, Code vulnerabilities
- Physical Attacks: Fault injection: clock or power glitch, alpha ray, Side Channel Analysis (SCA), Probing, Focused in Beam (FIB) etc.

* Paraphrised: Bill Clinton 1993 „It’s the economy, stupid”
### Top IoT Concerns

*What are your top 2 concerns for developing IoT solutions?*

<table>
<thead>
<tr>
<th>Concern</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>39.0%</td>
</tr>
<tr>
<td>Data Collection &amp; Analytics</td>
<td>10.5%</td>
</tr>
<tr>
<td>Integration with Hardware</td>
<td>15.5%</td>
</tr>
<tr>
<td>Connectivity</td>
<td>15.5%</td>
</tr>
<tr>
<td>Interoperability</td>
<td>15.1%</td>
</tr>
<tr>
<td>ROI</td>
<td>14.1%</td>
</tr>
<tr>
<td>Scalability</td>
<td>11.6%</td>
</tr>
<tr>
<td>Privacy</td>
<td>11.2%</td>
</tr>
<tr>
<td>Standards</td>
<td>10.8%</td>
</tr>
<tr>
<td>Performance</td>
<td>10.8%</td>
</tr>
<tr>
<td>Maintenance</td>
<td>10.2%</td>
</tr>
<tr>
<td>Cost</td>
<td>8.2%</td>
</tr>
<tr>
<td>Complexity</td>
<td>7.6%</td>
</tr>
<tr>
<td>Don’t Know</td>
<td>5.4%</td>
</tr>
<tr>
<td>Certification/Conformance</td>
<td>3.6%</td>
</tr>
<tr>
<td>Other</td>
<td>3.0%</td>
</tr>
</tbody>
</table>

Copyright (c) 2018, Eclipse Foundation, Inc. | Made available under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).
Why security in HW is better than SW?

- **Faster**: HW cryptography performs the encryption and decryption many times the speed of SW implementation,
- **Higher Performance, Lesser Code size**, 
- **Application Integrity Assurance**: hardware root of trust is more secure & higher assurance of code integrity over software,
- **Resistance to Reverse Engineering**: SF is more susceptible to RE
  Resistance to Non-intrusive Attacks: SF is more vulnerable to attacks that are based on power consumption analysis
- **Higher level of Key Protection**: keys are stored in HW not in SF
Security vs hardware

When implementing security countermeasures on an IoT device, best done using **hardware** based security.

<table>
<thead>
<tr>
<th>Software attacks</th>
<th>Isolated Security IP (HSM)</th>
<th>HW-based security</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>Micro-architectural attacks</td>
<td></td>
<td>!</td>
</tr>
<tr>
<td>Physical attacks</td>
<td>!</td>
<td>!</td>
</tr>
</tbody>
</table>

Ready for the highest Security level.
CryptOne is a 100% safe crypto CPU, because...

It involves the use of **RSA asymmetric encryption scheme** to realize a cryptosystem with a **one-time pad (OTP)**,

DCD’s solution is a broadly defined crypto system solution based on an asymmetric RSA with a **hidden value of a component of a public key susceptible to crypto analysis and implementing the OTP rules**, 

Nowadays security is the key- that’s why CryptOne OTP offers the advantages of symmetric crypto systems with one-time pad while retaining the advantages of asymmetric systems.
CryptOne core is a universal, fully scalable solution which is able to boost asymmetric cryptographic algorithms like: RSA, Diffie-Hellman and ECC;

It provides the efficient solution for asymmetric cryptography boosting arithmetic operations like: modular exponentiation, multiplication, inversion, GCD finding as also point doubling;

The energy efficient architecture of CryptOne IP core enables the usage of the very small silicon footprint with high processing speeds.
100% safe crypto CPU

- CryptOne can be provided with various different interfaces including AMBA AHB, AXI4, APB;
- Very intuitive interface enables the fast, straightforward system integration;
- The core is resistant to the Differential Power Attacks (DPA) and timing attacks.

Pls vote for CryptOne for "Best Innovative IP prize"
CryptOne’s features:

- **CryptOne constant time algorithms:**
  - Modular exponentiation,
  - Parallel modular exponentiation CRT
  - ECDSA sign/verify
  - ECDH
  - Elliptic curve point multiplication
  - Modular multiplicative inverse
  - GCD
  - Modular reduction
  - Multiplication
  - Division

- **Cryptographic algorithm applications:**
  - ECDSA, ECDH
  - RSA key generation
  - RSA Sign/Verify/Encrypt/Decrypt
  - Diffie-Hellman schemes
  - Miller-Rabin Primality check
  - System applications:

- **Client-server communication:**
  - Sensor networks
  - SSL/TLS stacks
  - IoT devices
  - Embedded security/ID devices

- **AMBA AHB, AXI4, APB** interface ready
- **Rapid & easy development with delivered API**
- **Patent pending architecture**
  - Algorithms resistant against SPA and timing attacks
  - CryptOne elliptic curves with native support:
    - NIST P-192
    - NIST P-224
    - NIST P-256
    - NIST P-384
    - Koblietz P-192
    - Koblietz P-256
    - Koblietz P-384
    - Brainpool P-256
    - Brainpool P-384
    - Brainpool P-512
    - Other/custom curves optional support

- **Software support:**
  - **OpenSSL** engine
  - **MbedTLS** port
  - OS independent crypto library
CryptOne – choose the best for you

CryptOne EC
- Modular Exponentiation constant time operation algorithm support
- Parallel Modular Exponentiation CRT constant time operation algorithm support
- Secure private RSA key computation, no branch inversion
- Easy to use software library interface
- Elliptic Curves point multiplication constant time algorithm
- Constant time modular multiplicative inverse algorithm for private operations
- Boost modular multiplicative inverse algorithm for public operations
- Native support for most popular elliptic curves
- Easy to use software library interface

CryptOne TLS
- Modular Exponentiation constant time operation algorithm support
- Modular Exponentiation CRT constant time operation algorithm support
- Secure private RSA key computation, no branch inversion
- Elliptic Curves point multiplication constant time algorithm
- Constant time modular multiplicative inverse algorithm for private operations
- Boost modular multiplicative inverse algorithm for public operations
- Native support for most popular elliptic curves
- Modular Reduction constant time algorithm
- Greatest Common Divisor algorithm
- MbedTLS and OpenSSL port libraries
- Software interface and examples for building own hardware algorithms with support for:
  - Large vector addition/subtraction
  - Large vector shift right/left
  - Large vector modular multiplication
  - Branch, execution flow controls
100% safe crypto CPU

- CryptOne consists of technologically independent hardware crypto processor in the form of synthesizable IP Core module prepared for integration and implementation in an IC (ASIC or FPGA)

- CryptOne offers both software and hardware cryptography advantages

PLS vote for CryptOne for "Best Innovative IP prize"
CryptOne

- Hardware & software co-design
- Test stimulation vectors are generated with the usage of D32PRO Simulator – the sub-module for RSA crypter is written in C++
- All tests are written in C using D32PRO software – they can be easily used in hardware through D32PRO platform
- Generated stimulation vectors are also used for reference comparison
- All internal data is exchanged through the AXI4-Stream protocol in simple format = higher flexibility
- The internal RSA CRYPT MODULE can work in a separate domain

Pls vote for CryptOne for "Best Innovative IP prize"
**Receiveables**

- C software drivers with API
- Silicon proven architecture
- Hardware code:
  - VERILOG Source Code or
  - FPGA Netlist
- VERILOG test bench environment
- Technical documentation
- Synthesis scripts
- 12 months of free technical support included
Summary

☑ Success stories are the best confirmation for DCD’s quality

"We once licensed DP8051 from DCD. When we needed incorporating a CAN 2.0B controller in another chip, we firstly thought about DCD. After a short period evaluation, we decided to adopt DCD’s DCAN IP and we found the core to be well designed, well documented. We are satisfied in DCD’s support and price.

-- Liuyadong, SOC Director of Bröte Semiconductor

Reference letter for Digital Core Design

Beyond Right

DCD Recommendation

Flowserv purchased and used some DCD IP (DFF13655 with DSP1 and DCM) for a chip that we are using in a product scheduled to launch at the beginning of next year (2018). This project has been underway since 2015. We have had ample time to thoroughly test DCD’s IP and have found it to be solid. We have no known issues.

Flowserv also asked DCD to make minor tweaks to the IP for us and to provide some implementation-specific updates to the documentation they provided and we found DCD to be responsive, helpful, and easy to work with.

Flowserv will have no problem using DCD in the future and would recommend them to other companies considering using their IP.

Thanks,

Nathan Highy
R&D Engineer

Dear Sir,

“As one of the first companies we had the chance to work the newest DCD’s invention - the D32PRO in a project involving implementation of an extensive architecture (D32PRO + DFFAU + DUS82-ULPI + DMAC-RMII + DDSPI + DCM + DCAN + DUN + DIMART) (DLC32).

Despite the complexity of the design, all DCD’s modules turned out to be easy to work on, so we have completed the works without any difficulties or delays. At all times DCD’s team assisted in the process providing reliable and always on time support. Working with DCD proved to be a very rewarding experience for all involved; this should result in a solid foundation for future collaborations.”

Yours sincerely,

[Signature]
Why DCD?

- Two decades of IP Core market experience
Why DCD?

- DCD presented World’s fastest 8051 CPU during CeBIT 2013 official opening ceremony (in front of German Chancellor A. Merkel and EU President D. Tusk)
- D32PRO has been presented during EXPO in Milan and Hannover Messe
Why DCD?

- Innovative products – always step ahead before competitors
- Know-how based on two decades of market experience
- Optimal solutions which answers market needs
- Significant Time-to-market reduction
- Coherent IP Core portfolio
- IP Cores tailored to the project needs
- Complete solution from one company
  
  like e.g.: IP Core + debugger + ...
Thank you!

Any questions?

info@dcd.pl

Pls vote for CryptOne for "Best Innovative IP prize"