Hardware accelerators for cybersecure V2X connectivity
ESTABLISHED IN 2014

UNIVERSITY OF PISA SPIN-OFF

ITALIAN SME COMPANY

INGENIArs

The Art of Engineering

INNOVATIVE START-UP

ONGOING ISO9001 & ISO13485 CERTIFICATION

© 2019 IngeniArs S.r.l. All rights reserved - Confidential
We offer **High Quality Products and Services** to promote **Innovation** in the Aerospace, Healthcare and Automotive fields.
• ELECTRONICS, MICRO-ELECTRONICS AND EMBEDDED HW/SW SYSTEMS

• FPGA & ASIC DIGITAL DESIGNS

• COMPLEX DSP ALGORITHMS MODELLING

• VHDL & VERILOG IP CORES

• DESKTOP APPLICATIONS

• WEB & MOBILE APPS
• CYBER SECURITY IP MACRO-CELLS
• INNOVATIVE TOOLS & ALGORITHMS
• DESIGN SERVICES
Hardware accelerators for cybersecure V2X connectivity - Outline

• Automotive systems and cybersecurity weaknesses

• Security solutions for automotive wireless networking

• Results and discussion
Automotive networks - today
Automotive networks - tomorrow
Wireless automotive networks applications

**V2V** - Vehicle-to-Vehicle.
Alerts one vehicle to the presence of another. Cars “talk” using DSRC technology.

**V2D** - Vehicle-to-Device.
Vehicles communicate with cyclists’ V2D device and vice versa.

**V2P** - Vehicle-to-Pedestrian.
Car communication with pedestrian with approaching alerts and vice versa.

**V2I** - Vehicle-to-Infrastructure.
Alerts vehicles to traffic lights, traffic congestion, road conditions, etc.

**V2G** - Vehicle-to-Grid.
Smart grid controls vehicle charging and return electricity to the grid.

**V2H** - Vehicle-to-Home.
Vehicles will act as supplement power supplies to the home.
Cybersecurity services needed

- Data Confidentiality
  - E.g.: driver’s privacy (GPS position)

- Data Integrity
  - Ensuring the operations of the on-board systems

- Authentication
  - Only certificated entities shall use the on-board networks

- Data Availability
  - The communication must be guaranteed (safety critical systems)
Automotive context requirements

• Safety Vs. Security trade-off
  • Security introduces overhead on the communication

• Automotive systems can be latency-critical
  • Real-time data security is needed

• Low-power constraints
  • Power saving

Hardware Accelerators
Hardware accelerators for cybersecure V2X connectivity - Outline

• Automotive systems and cybersecurity weaknesses

• Security solutions for automotive wireless networking

• Results and discussion
Cybersecurity solutions

- Data Confidentiality
- Data Integrity
- Authentication
- Additional Services

- AES IP Core
  (Advanced Encryption Standard)
- SHA IP Core
  (HASH Engine for SHA-2 / SHA-3)
- ECC Accelerators
  ECDSA / ECIES IP Core
  (Elliptic Curve Cryptography)
- TRNG IP Core (Proof of Concept)

© 2019 IngeniArs S.r.l. All rights reserved - Confidential
AES IP core

- Symmetric key data encryption / decryption
- Compliant with NIST FIPS 197 standard
- Fast decryption support
- Configurable architecture:
  - Encryption or merged encryption/decryption
  - AES-128 and/or AES-256 support
  - Internal stage cascading for throughput increasing
  - Fast / Slow decryption support

<table>
<thead>
<tr>
<th></th>
<th>Std-cell 45 nm ASIC**</th>
<th>Intel Stratix IV FPGA***</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logic Complexity *</td>
<td>&lt; 18 kGE</td>
<td>&lt; 2250 ALMs</td>
</tr>
<tr>
<td>Frequency</td>
<td>560 MHz</td>
<td>160 MHz</td>
</tr>
<tr>
<td>Throughput (AES-128)*</td>
<td>7.17 Gbps</td>
<td>2.05 Gbps</td>
</tr>
<tr>
<td>Throughput (AES-256)*</td>
<td>5.12 Gbps</td>
<td>1.46 Gbps</td>
</tr>
</tbody>
</table>

* Data for single stage AES IP Core
** NanGate FreePDK45 OCL, post-synthesis results
*** Not using dedicated RAM blocks

For further technical details please contact:
info@ingeniars.com

© 2019 IngeniArs S.r.l. All rights reserved - Confidential
SHA IP Core

- HASH Engine for SHA-2 and SHA-3 algorithms
- Compliant with FIPS-180 and FIPS-202 standards
  - All algorithms
- Configurable architecture:
  - Selection of SHA algorithms (SHA-2 or SHA-3)
  - Multiple output digest width (224 – 256 – 384 – 512)
  - Internal byte-oriented padding module (optional)

For further technical details please contact:
info@ingeniars.com

<table>
<thead>
<tr>
<th></th>
<th>Std-cell 45 nm ASIC**</th>
<th>Intel Stratix IV FPGA***</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logic Complexity*</td>
<td>&lt; 28 kGE</td>
<td>&lt; 3200 ALMs</td>
</tr>
<tr>
<td>Frequency</td>
<td>1100 MHz</td>
<td>100 MHz</td>
</tr>
<tr>
<td>Throughput SHA3-512</td>
<td>&gt; 26 Gbps</td>
<td>&gt; 2.4 Gbps</td>
</tr>
<tr>
<td>Throughput SHA3-384</td>
<td>&gt; 38 Gbps</td>
<td>&gt; 3.4 Gbps</td>
</tr>
<tr>
<td>Throughput SHA3-256</td>
<td>&gt; 48 Gbps</td>
<td>&gt; 4.5 Gbps</td>
</tr>
<tr>
<td>Throughput SHA3-224</td>
<td>&gt; 50 Gbps</td>
<td>&gt; 4.8 Gbps</td>
</tr>
</tbody>
</table>

*  Data for SHA-3 algorithm
** NanGate FreePDK45 OCL, post-synthesis results
*** Not using dedicated RAM blocks
ECDSA / ECIES IP Core

- Elliptic Curve Cryptography support
  - ECDSA / ECIES schemes
- Compliant with NIST FIPS 186-4 standard
- Configurable architecture:
  - Multiple NIST P Curves Support (P-256 / P-521)

<table>
<thead>
<tr>
<th></th>
<th>Std-cell 45 nm ASIC**</th>
<th>Intel Stratix IV FPGA***</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logic Complexity*</td>
<td>&lt; 325 kGE</td>
<td>&lt; 19000 ALMs</td>
</tr>
<tr>
<td>Frequency</td>
<td>350 MHz</td>
<td>60 MHz</td>
</tr>
<tr>
<td>Throughput ECDSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signature Generation</td>
<td>&gt; 5000 Gen/s</td>
<td>&gt; 950 Gen/s</td>
</tr>
<tr>
<td>Throughput ECDSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signature Verification</td>
<td>&gt; 3500 Ver/s</td>
<td>&gt; 660 Gen/s</td>
</tr>
</tbody>
</table>

* Data for ECDSA over NIST-P256R1
** NanGate FreePDK45 OCL, post-synthesis results
*** Not using dedicated RAM blocks

For further technical details please contact:
info@ingeniars.com
Hardware accelerators for cybersecurity V2X connectivity - Outline

- Automotive systems and cybersecurity weaknesses
- Security solutions for automotive wireless networking
- Results and discussion
Demonstrator on FPGA platform

- Stratix IV FPGA
- SoC Architecture
  - Dedicate PLL clock
  - Synchronization IF

![Diagram of FPGA platform components]

- Master clock
- NIOS II Processor
- Wi-Fi device
- PLL
- (T)RNG
- AES core
- SHA2 engine
- ECC arithmetic accelerator

- ECIES algorithms
- ECDSA algorithms
- AES-ECB functions
Demonstrator (System architecture)

- System Application
- Secure Library
- HW Device Drivers
- SW-Secure Library (wolfCrypt/wolfSSL)
- HW modules

© 2019 IngeniArs S.r.l. All rights reserved - Confidential
## HW vs. SW Implementation

### HW ECDSA vs. SW ECDSA

<table>
<thead>
<tr>
<th>Service</th>
<th>Function</th>
<th>HW or SW?</th>
<th>Test</th>
<th>Elapsed Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECDSA</td>
<td>Signature generation</td>
<td>HW</td>
<td>PASSED</td>
<td>-&gt; 6.65 ms @ 50 MHz</td>
</tr>
<tr>
<td>ECDSA</td>
<td>Signature verification</td>
<td>HW</td>
<td>PASSED</td>
<td>-&gt; 7.59 ms @ 50 MHz</td>
</tr>
<tr>
<td>ECDSA</td>
<td>Signature generation</td>
<td>SW</td>
<td>PASSED</td>
<td>-&gt; 29127.42 ms @ 50 MHz (~4381.1 slower)</td>
</tr>
<tr>
<td>ECDSA</td>
<td>Signature verification</td>
<td>SW</td>
<td>PASSED</td>
<td>-&gt; 32909.06 ms @ 50 MHz (~4336.0 slower)</td>
</tr>
</tbody>
</table>

© 2019 IngeniArs S.r.l. All rights reserved - Confidential
OUR TEAM

6 PhD Scientists
8 Engineers
1 Economist