Zurich University
of Applied Sciences

School of
Engineering

InES Institute of
Embedded Systems

A Quantitative Comparison Between Renesas's Trusted Secure IP Cryptographic Hardware and Secure Elements

Benchmarking Crypto Acceleration for IoT (cont.)

Mario Noseda, Simon Künzli

Abstract – IoT is an increasingly tempting target for attackers due to its exponential growth. Besides pure software vulnerabilities (like weak or hardcoded passwords, insecure data transfer and storage), the OWASP IoT Top Ten[1] lists hardware-related vulnerabilities such as the lack of physical hardening and the omission of a secure update mechanism. Mitigating these challenges requires additional hardware, as many of these devices are physically exposed and thus at a higher risk than conventional IT devices. More types of hardware solutions that implement the required functionality are entering the market; however, there are few to no performance comparisons. This lack further hinders the adoption of adequate solutions on a per-project basis. This white paper compares the performance of Renesas RX72N's on-chip security engine to secure elements that connect to the host MCU over a serial bus.

This whitepaper is the direct successor to "Crypto Acceleration for IoT: A Quantitative Comparison of Internal and External Solutions[2]", which compares the Secure Crypto Engine 9 (SCE9) contained in the Renesas RA6M4 with the Infineon OPTIGA Trust M and NXP SE050 secure elements. This project repeats the same measurements using the RX72N instead of the RA6M4. Therefore, we kept the firmware structure, the measurement setup and the whitepaper as identical as possible, and we have reused complete paragraphs where applicable. It is important to note that we also had to repeat the measurements with the secure elements, as their performance is also impacted by switching the host MCU.

Compared to conventional IT devices, IoT devices need to catch up in terms of security. The rapid increase of deployed IoT devices drastically increases the attack surface, affecting not only the IoT devices themselves, but also all related infrastructures, as the IoT devices might be used as an attack entry point. Energy-constrained devices are a major focus of attention, as various cryptographic algorithms cannot be used without significantly impacting power consumption.

Fortunately, more and more semiconductor manufacturers are addressing this problem. For several years now, secure elements have offered the capability of storing sensitive data (e.g., credentials and root certificates) in tamper-resistant memory and improving algorithms' energy and time efficiency through dedicated hardware. In addition, most of these secure elements are certified, which means that they are suitable for highly regulated devices. However, adding such a device does not come without its drawbacks. Even though the SPI/I2C communication can be encrypted, the lack of tamper-resistant memory in the MCU exposes the key on the host side to a determined attacker. Additionally, it is still possible to set up the communication completely unencrypted, although this is only intended for the development phase. Even though such a setting has an obvious right to exist, it could still lead to potential problems, e.g., forgetting to enable the encryption for the production build, similar to the well-known issue of forgetting to disable the debug ports.

In contrast, there are MCUs that have a cryptographic engine integrated as a peripheral. In direct comparison, they do not have the problem with the openly accessible interface, since the complete communication of the processor and the peripheral is handled via an internal bus. The on-chip solution also has a clear advantage regarding the data rate, since a significantly higher clock frequency can be used for internal buses. Although such MCUs usually do not contain tamper-resistant memory, the sensitive data is wrapped (encrypted and authenticated) with a special procedure within the crypto engine before being stored in standard flash memory. Compared to the tamper-resistant memory of secure elements, such security-focused MCUs offer a multiple of the storage capacity with a far superior wear-out characteristic.

[1] https://owasp.org/www-project-internet-of-things/
[2] https://doi.org/10.21256/zhaw-25123

There are a lot of other features (updateability, provisioning, certification, ...) that differentiate these two device classes. This white paper focuses on a performance comparison in terms of execution time and energy consumption.

For this, we designed a benchmark composed of various cryptographic primitives, conducted time and energy measurements, and then performed a statistical analysis of the gathered data.

The benchmark is composed of the following cryptographic primitives:

- Generating random numbers (32 / 64 / 128 / 256 / 512 / 1024 bytes)
- Calculation of SHA256 hashes of the previously generated random numbers
- Generation of ECC (secp256r1) and RSA (1024 / 2048 bits) key pairs
- Calculation of ECDSA and RSA digital signatures
- Verification of ECDSA and RSA digital signatures

RSASSA-PKCS1-v1_5 was used as the RSA signature scheme for the complete project. For the remainder of the white paper, expressions like "RSA signature" in text, tables, or figures refer to this scheme.

As for the devices, we compared the Trusted Secure IP (TSIP) contained in the Renesas RX72N[3] to the Infineon OPTIGA Trust M[4] and the NXP SE050[5] secure elements by measuring the respective execution time and energy consumption using a power analyzer during the benchmark.

Project Structure

We used the Renesas Starter Kit+ for RX72N (RSK+RX72N) for benchmarking the performance of the TSIP. The various cryptographic primitives were executed sequentially with an auxiliary GPIO set high during every test. The rising and falling edges allowed the exact calculation of the execution time and energy consumption during the post-processing of the power analyzer data.

Secure elements must be connected to a host MCU. To keep the benchmarks comparable, we kept the RSK+RX72N and added our custom Secure Element Shield (SE-Shield), which contains, among other chips, the OPTIGA Trust M and the SE050. Again, we used the rising and falling edge of the auxiliary GPIO for processing the data.

The firmware has been written using the Renesas e^2 studio and their Firmware Integration Technology (FIT) modules. Concerning the secure elements, we utilized the software development kit (SDK) provided by their respective manufacturer.

We applied basic optimization to the application (i.e., all unused clocks set to the lowest possible frequency and all unused peripherals turned off), but we were not able to optimize for both speed and energy consumption with a single setup. Therefore, clock speeds, prescalers, and the use of sleep modes were specifically configured for the operational aspect being evaluated.

Regarding optimization, the TSIP is a fairly self-contained peripheral and only allows clock speeds to be adjusted, as shown in Table 1. The instruction clock of the core (ICLK) was set to the maximum of 240 MHz when optimizing for execution time. In contrast, it was reduced to 7.5 MHz when optimizing for energy consumption. In both cases, the PCLKB

[3] https://www.renesas.com/rx72n
[4] https://www.infineon.com/cms/en/product/security-smart-card-solutions/optiga-embedded-security-solutions/optiga-trust/optiga-trust-m-sls32aia/
[5] https://www.nxp.com/products/security-and-authentication/authentication/edgelock-se050-plug-trust-secure-element-family-enhanced-iot-security-with-maximum-flexibility:SE050

(clock source of the TSIP) was set to the maximum frequency of 60 MHz. These frequencies yielded the best results for each corresponding metric.

Table 1: Selected settings for optimizing the TSIP.

TSIP Optimization	Time	Energy
Oscillator	Main	Main
PLL	Div. x1, Mul. x10	Div. x1/2, Mul. x10
Clock source	PLL	PLL
ICLK	240 MHz	7.5 MHz
PCLKB	60 MHz	60 MHz

The optimization of the secure elements was determined empirically. We found that the I2C timing requirements could not be achieved for I2C fast-mode+ (1 MHz) without using extremely small pull-up resistors due to the length and capacitance of the traces. Since this only led to a marginal improvement in execution time and significant degradation in energy consumption, it was not used for either optimization. Thus, we used the I2C fast-mode (400 kHz) for both cases. Table 2 shows the configuration we determined for the secure elements. The ICLK was left at the maximum of 240 MHz for the time-optimized tests, since any reduction resulted in an increased execution time.

In contrast, for energy optimization, the phase-lock-loop (PLL) was completely disabled. Furthermore, the ICLK and the PCLKB (clock source of the I2C peripheral) were connected directly to the high-speed on-chip oscillator (HOCO). This comparatively slow 16 MHz clock speed resulted in the best compromise between supply current and execution time, leading to the lowest energy consumption.

Lastly, both secure element SDKs contain various wait loops, in which the host MCU periodically (in the single-digit millisecond range) polls the secure element via I2C to determine whether or not the operation has been completed. If the MCU is put to sleep in between polling, additional energy can be conserved in exchange for a slight reduction in speed.

Table 2: Selected settings for optimizing the secure elements.

SE Optimization	Time	Energy
Oscillator	Main	HOCO
PLL	Div. x1, Mul. x10	Disabled
Clock source	PLL	HOCO
ICLK	240 MHz	16 MHz
PCLKB	60 MHz	16 MHz

In terms of energy optimization, various settings have been determined so that the TSIP as well as the secure elements consume as little energy as possible. However, optimizing the secure elements required a reduction of 93% from the maximum ICLK frequency and putting the MCU into a sleep mode whenever possible, which might not be feasible depending on your type of application. The reduction of the ICLK yields a significant performance penalty for the rest of the application. This could potentially be mitigated by dynamically switching the ICLK frequency before and after cryptographic calculations;

however, this requires additional effort to maintain the functionality of all running peripherals (readjusting prescalers, etc.). Lastly, entering a sleep mode might not be possible due to high-availability constraints (e.g., hard real-time applications).

Measurement Setup

Figure 1 shows the setup used for measuring the performance of the three DUTs.

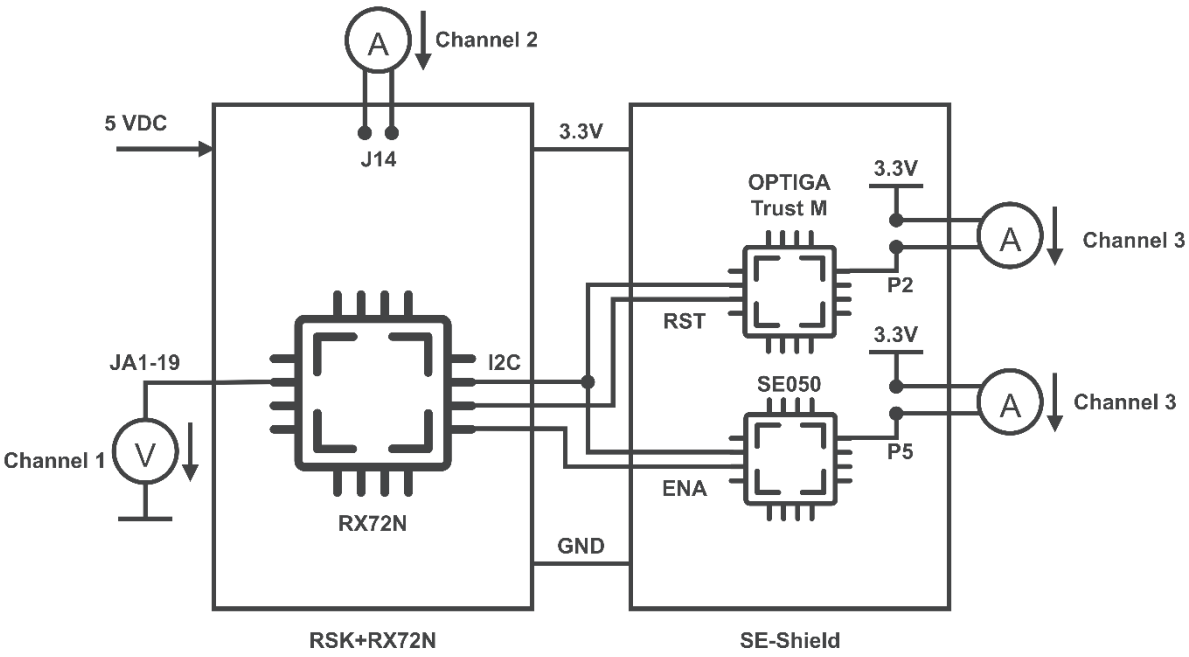

Figure 1: Measurement setup used for all benchmark measurements.

Channel 1 of the Keysight N6705B DC power analyzer was set up as a voltmeter and used to record the voltage of the JA1-19 pin, which signaled the active execution of a benchmark test with a logic "1". Channel 2 was set up as an ammeter and connected to the test pins on J14, which are intended to measure the supply current of the RX72N (only the MCU without anything else on the RSK+). For the OPTIGA Trust M and the SE050, channel 3 was set up as an ammeter and connected to either the P2 or P5 header on the SE-Shield for measuring the current consumption of the respective secure element.

A custom Python package allowed the automation of the measurements. It set up the power analyzer, started the measurement, reset the DUT, and finally exported the measurement results as a CSV file to a USB thumb drive plugged into the power analyzer. Afterwards, the package parsed all the CSV files and calculated all the conducted repetitions' execution time and energy consumption. Finally, it exported the statistical analysis for all the tested cryptographic primitives.

Results

The following two statements are essential to prevent misunderstandings:

- The RSA key generation is a probabilistic operation (finding random large prime numbers is non-deterministic); therefore, the resulting measurements are only a general indication of the performance.
- The sampling period of the power analyzer was set to 81.92 µs (the fastest possible setting for this setup). Consequently, all median values approaching the sampling period must be regarded as neither accurate nor precise measurements, but rather as an approximation.

Absolute Performance

In order to measure the best possible values, the time-optimized setup was used for the execution time measurements and the energy-optimized setup for the energy consumption measurements. Table 3 and Table 4 list the resulting absolute values of the benchmark, where each value is the median of all measured repetitions.

As mentioned at the beginning of this section, values close to the sampling period of 81.92 µs could not be measured accurately with the power analyzer. The measurements of the asymmetric algorithms performed with the TSIP were affected by this limitation and are marked accordingly. Furthermore, random generation and hashing with the TSIP were so fast (less than one sampling period) that the power analyzer couldn't measure them adequately. In order to still compare it to the secure elements regarding the execution time, random generation and hashing with the TSIP were measured using a logic analyzer.

Relative Performance

To better compare the performance of the TSIP and the secure elements, Figure 2 shows the relative difference between the DUTs. It contains the ratios of the measurement results of the secure elements to those of the TSIP. For example, the OPTIGA Trust M takes 6.98 times longer than the TSIP to generate a 1024-bit RSA signature. Similarly, the SE050 needs 0.642 times as much energy as the TSIP to generate a 2048-bit RSA signature. For a quicker overview, the colors of the individual cells indicate the order of magnitude of the calculated ratios.

Table 3: Absolute execution time and energy consumption of the complete node during the random and hash benchmarks (median of values, rounded to 3 significant digits, n=100)

		TSIP[1]		Trust M[2]		SE050[2]	
Primitive	Bytes	Time [s]	Energy [J]	Time [s]	Energy [J]	Time [s]	Energy [J]
Random	32	7.79e-06	-	6.23e-03	4.37e-04	1.45e-02	7.45e-04
	64	1.54e-05	-	7.95e-03	5.23e-04	1.52e-02	7.81e-04
	128	3.06e-05	-	1.52e-02	6.83e-04	1.65e-02	8.54e-04
	256	6.10e-05	-	1.89e-02	9.58e-04	2.15e-02	1.11e-03
	512	1.22e-04	-	3.68e-02	1.86e-03	3.16e-02	1.52e-03
	1024	2.43e-04	-	7.23e-02	3.74e-03	6.31e-02	3.04e-03
Hash	32	5.63e-06	-	4.40e-02	3.03e-03	3.09e-02	1.52e-03
	64	1.01e-05	-	4.63e-02	3.52e-03	3.38e-02	1.60e-03
	128	1.42e-05	-	4.66e-02	3.70e-03	3.74e-02	1.84e-03
	256	1.72e-05	-	5.66e-02	4.55e-03	4.48e-02	2.35e-03
	512	2.30e-05	-	6.94e-02	5.76e-03	5.94e-02	3.21e-03
	1024	3.48e-05	-	1.00e-01	8.47e-03	3.31e-01	1.54e-02

1. Only execution time measurements have been performed due to limitations of the measurement equipment (see Section Absolute Performance).
2. The energy consumption is calculated from the current consumption of the secure element and the host MCU (RX72N).

Table 4: Absolute execution time and energy consumption of the complete node during the asymmetric crypto benchmarks (median of values, rounded to 3 significant digits, n=100)

		TSIP[1]		Trust M[2]		SE050[2]	
Primitive	Operation	Time	Energy	Time	Energy	Time	Energy
ECDSA	Key Gen.	(*) 1.23e-03	1.30e-04	6.38e-02	3.98e-03	2.10e-01	9.41 e-03
	Sign	(*) 1.47e-03	1.46e-04	6.55e-02	4.20e-03	4.45e-02	2.46 e-03
	Verify	2.79e-03	2.80e-04	8.09e-02	5.34e-03	4.46e-02	2.57 e-03
RSA1024	Key Gen.	3.40e-01	3.32e-02	6.92e-01	3.97e-02	7.07e-01	4.84 e-02
	Sign	1.03e-02	1.04e-03	7.21e-02	4.65e-03	6.16e-02	3.75 e-03
	Verify	(*) 1.64e-04	2.84e-05	2.23e-02	1.66e-03	3.76e-02	2.09 e-03
RSA2048	Key Gen.	3.06e+00	2.10e-01	3.99e+00	2.97e-01	3.77e+00	2.72 e-01
	Sign	2.17e-01	1.93e-02	2.98e-01	1.85e-02	1.79e-01	1.24 e-02
	Verify	(*) 1.15e-03	1.25e-04	2.99e-02	2.78e-03	5.23e-02	2.78 e-03

1. The energy consumption is calculated from the current consumption of the RX72N.
2. The energy consumption is calculated from the current consumption of the secure element and the host MCU (RX72N).
*: Value is less than 20 sampling periods of the power analyzer. Consider this execution time as well as the corresponding energy consumption as approximations.

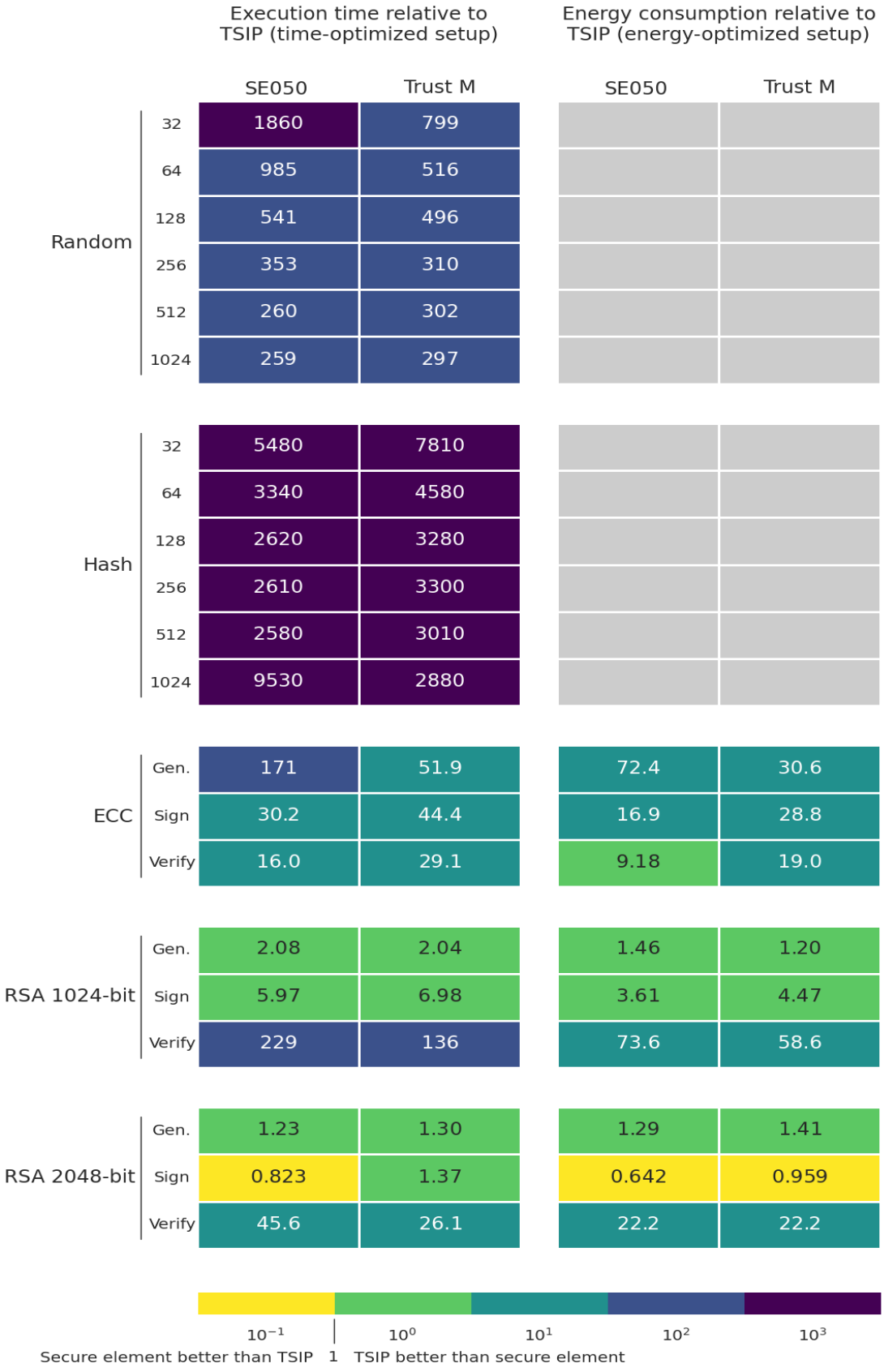

Figure 2: Execution time and energy consumption of the secure elements relative to the TSIP (ratio of median values, rounded to 3 significant digits, n=100). See Section Absolute Performance for information about the missing energy consumption values during random generation and hashing.

Distribution

The highest spread, with a relative standard deviation (RSD)[6] of around 45 to 65%, occurred during the two RSA key generation tests, as expected from a non-deterministic algorithm. Furthermore, all tests in which the median is very close to the sampling period are bound to have a high RSD. Thus, we exclude these tests from our discussion on the distribution of the measured values, as this would arbitrarily increase the observed RSD.

Table 5 and Table 6 list the highest RSDs of the remaining tests for each DUT regarding the time and energy benchmarks, respectively.

Table 5: Execution time measurements with the highest RSD after excluding RSA key generation and justified outliers.

TSIP	Trust M	SE050
1.3% ECDSA Verify	18% Random 128 Bytes	0.28% Random 32 Bytes
0.35% RSA1024 Sign	6.6% Hash 32 Bytes	0.25% Random 128 Bytes
0.18% Hash 32 Bytes	6.3% RSA1024 Verify	0.19% Random 256 Bytes

Table 6: Energy consumption measurements with the highest RSD after excluding RSA key generation and justified outliers.

TSIP[1]	Trust M	SE050
0.92% ECDSA Verify	8.6% RSA1024 Sign	0.2% Random 32 Bytes
0.19% RSA1024 Sign	7.2% RSA1024 Verify	0.19% Random 64 Bytes
0.067% RSA2048 Sign	5.4% Random 64 Bytes	0.19% Random 128 Bytes

1. *Without random generation and hash calculation (missing energy measurements)*

As described in Section Results, the TSIP was too fast for the power analyzer in the random and hash measurements, and only the execution time was measured. Therefore, we excluded these tests in the RSD evaluation of the TSIP regarding energy consumption. The remaining tests show a very high uniformity in execution time and energy consumption, with a maximum RSD of 1.3% and 0.92%, respectively.

Generating 128 bytes of random data with the Trust M resulted in the highest RSD overall, with 18%. A closer look at the raw measurement data shows that most measurements took either 10 ms or 15 ms, which coincides with the host MCU polling the Trust M with a 5 ms interval. We assume that the actual random generation takes about 10ms and sometimes finishes before the next poll and sometimes just misses it. Understandably, this also leads to a high RSD of the energy consumption during the same test. Otherwise, the secure element also shows a very constant behavior with RSDs of 7.1% and lower.

The consistency of the execution time with the SE050 is surprisingly high at 0.28% RSD. It can be assumed that this is due to particularly stringent protection measures against timing attacks.

Ratio between RX72N and Secure Elements

Another observation we have made is the distribution of energy consumption between the secure elements and the host MCU RX72N. Since secure elements always need to be connected to a host MCU, the selection of this MCU has a strong influence on the total energy consumption during the execution of one of the tested cryptographic primitives.

[6] RSD = 100 * σ / μ σ: standard deviation μ: arithmetic mean

Figure 3 shows the ratios with which the MCU and the secure elements contribute to the measured energy consumption.

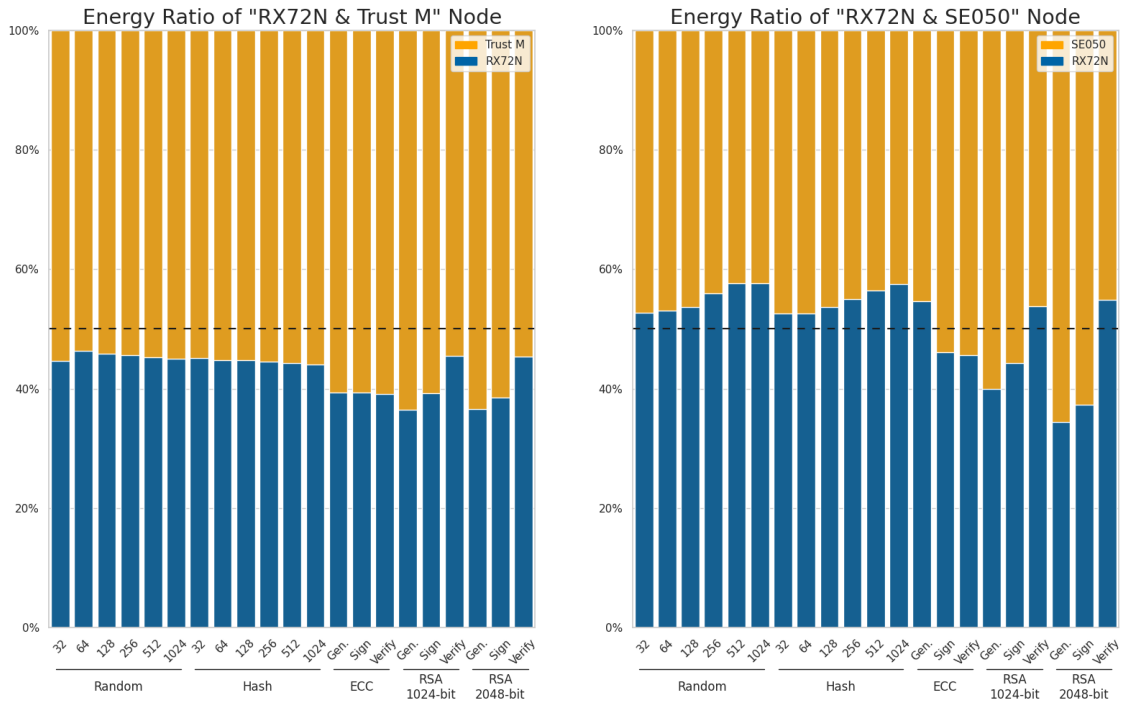

Figure 3: Energy ratio of the host MCU (RX72N) and the secure elements while benchmarking the secure elements.

While the secure element executes the desired operation, the MCU waits and checks periodically (Trust M: 5 ms, SE050: 1 ms) whether the secure element has completed the operation. Thus, the sleep current and the time needed to enter and leave the desired sleep mode are significant when selecting the host MCU. If you want to use one of the two evaluated secure elements in a project with limited power availability, we recommend using a more energy-efficient MCU if possible, as the MCU should not account for a third to even more than half of the total energy consumption.

Conclusion

This white paper provides basic measurements of the TSIP contained in the Renesas RX72N MCU, and the Infineon OPTIGA Trust M and NXP SE050 secure elements during the execution of cryptographic primitives. The results show that the different device types differ not only in their functionality and usage, but also in their performance in terms of execution time and energy consumption. Moreover, the devices used in this evaluation could not be optimized for both execution time and energy consumption simultaneously. Thus, the information contained in this document aims to support developers in finding an adequate solution for their given project by providing them with adequate measurement results.

Zurich University
of Applied Sciences

School of Engineering

The **Institute of Embedded Systems (InES)** is a leading research centre in the field of embedded systems with more than 50 employees as well as a state-of-the-art development and measurement infrastructure. Our services include:

- Design of system concepts and feasibility studies
- Consulting on the choice of technology
- Rapid prototyping and proof-of-concept
- Selection of radio components
- Realization of exhibition demonstrators
- Design of printed circuit boards (PCB)
- Writing microcontroller firmware: radio, protocols, sensors, actuators
- Interfacing to gateways and service platforms (cloud)
- Verification: Long-term tests and stress testing
- Embedded security: Threat analysis and protection measures

Mario Noseda, Simon Künzli
Technikumstrasse 9
CH-8400 Winterthur

mario.noseda@zhaw.ch
simon.kuenzli@zhaw.ch

www.zhaw.ch/ines

This research was funded by Renesas Electronics Europe GmbH.