Producing Unique Identifiers and Random Numbers on Basis of Unclonable Parameters of Microcontrollers and Undesired Effects

Josef Strnadel (strnadel@fit.vutbr.cz), Giuseppe Conte (xconte00@stud.fit.vutbr.cz)
Brno University of Technology, IT4Innovations Centre of Excellence, Bozetechova 2, 61266 Brno, Czech Republic

Abstract

Main goal of this poster is to show how unique and distinctive physical properties of component-of-the-shelf (COTS) microcontrollers (MCUs) can be utilized to enhance the security of embedded systems with no necessity to modify the hardware for the purpose. It can be shown that even if each MCU chip is produced by the same procedure and technology, there are some slight changes that make it being both unique and random in some sense. For that purpose, the same piece of a simple code was executed on each MCU with the goal to produce its unique identifier as well as a unique sequence of random numbers based on the physical properties of that MCU.

Introduction

The need for security belongs to typical requirements imposed on recent devices such as MCUs. A very important aspect in the security context is the utilization of unique identifiers (IDs) and random numbers (RNDs) for confidentiality and authentication purposes. Typically, either a special hardware (HW) or software (SW) is utilized to produce the IDs and RNDs. However, this adds extra costs since an extra HW or SW must be added to enhance security of a device.

In relation to this poster, we focus to the device identification (DEVID) problem, which is solved especially in the secured communication area where it is necessary uniquely identify both a sender and a receiver of a message. Typical solutions of the DEVID problem are based on writing a unique (ID) number into a non-volatile memory such as flash, post-production modification of the device, introducing special circuits designed to compute IDs algorithmically or using non-conventional solutions such as a polymorphic chip called REPOMO32. However, if the uniqueness requirement imposed on IDs is extended by non-reproducibility (unclonability) of IDs, many of the above-mentioned solutions fail to meet both the requirements.

Main idea

To minimize costs related to production of unique, non-reproducible IDs and RND sequences, we have decided to utilize inherent properties of common COTS MCUs rather than to utilize a complex circuitry, technology or algorithms for that purpose. Since MCUs are typically digital, synchronous sequential circuits we have focused to inherent properties implying from uniqueness of their inner clock signals. Because of the production process variability, several undesired effects such as jitters can be measured and hopefully, utilized to identify those devices.

Jitter effect

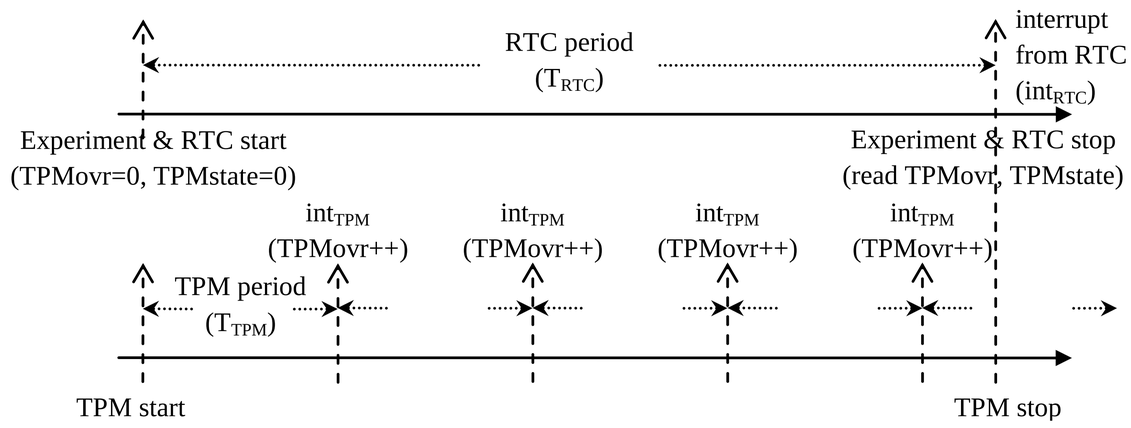
Jitter can be defined as the timing variation of a (real) signal edge from its ideal (simulated, theoretical) occurrence time. However, if a real hardware is utilized then signals such as clock are typically disturbed by factors such a thermal noise, power supply variations, loading conditions, device noise, and interference coupled from nearby circuits. Many types of jitter can be identified in the literature, e.g. Period Jitter, Cycle to Cycle Jitter, Long Term Jitter, Phase Jitter or Time Interval Error Jitter. Further jitter effects such as task-release jitter, response-time jitter etc. can be observed if a SW (e.g., operating system, OS) layer is utilized over the HW.

Experimental platform

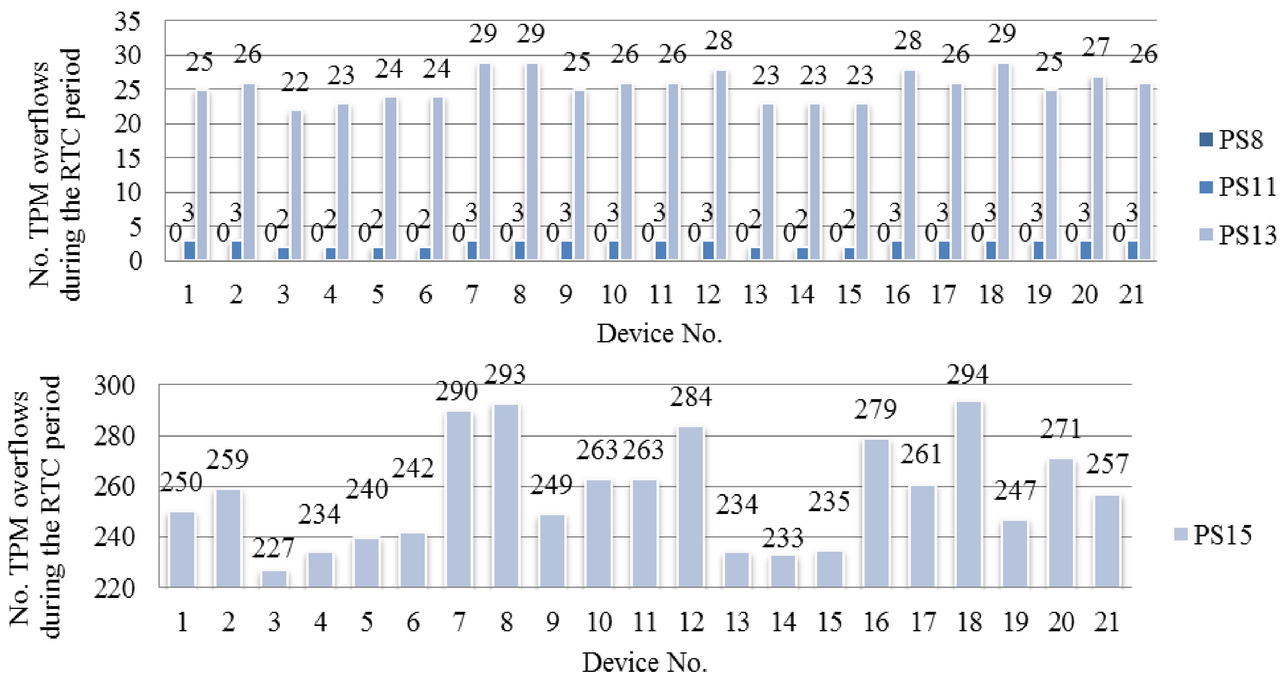
To verify practical applicability of our idea, we have utilized two modules realized on the 8-bit Freescale's MC9S08JM60 COTS MCU: the Real-Time Counter (RTC) configured to be clocked by the LPO (Low-Power Oscillator) and the Time/Pulse-Width Modulator (TPM) configured to be clocked by the BUSCLK (Bus Clock) derived from MCG (Multipurpose Clock Generator). For measurements, it was important that LPO and MCG (as well as BUSCLK) were independent.

Principle

The undesired jitter effect can be e.g. observed by simply counting how many times TPM @ 8MHz overflows (TPMovr value) in a single 100ms period of RTC followed by reading TPM's final state (TPMstate value):

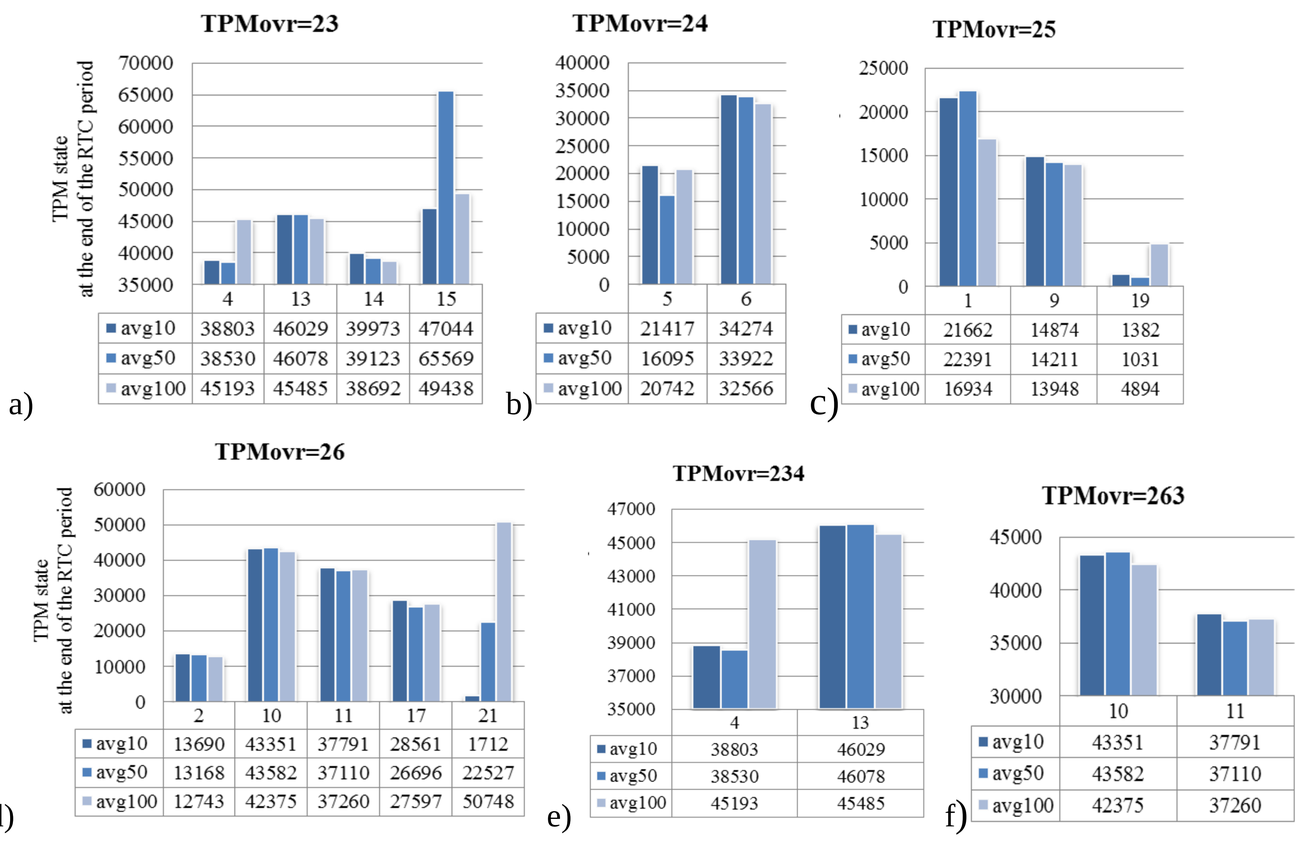


Overall results



Amount of TPM overflows within single RTC period as a function of the RTC prescaler.

Detail results



TPMovr=23	4	13	14	15
avg10	38803	46029	39973	47044
avg50	38530	46078	39123	65569
avg100	45193	45485	38692	49438

TPMovr=24	5	6
avg10	21417	34274
avg50	16095	33922
avg100	20742	32566

TPMovr=25	1	9	19
avg10	21662	14874	1382
avg50	22391	14211	1031
avg100	16934	13948	4894

TPMovr=26	2	10	11	17	21
avg10	13690	43351	37791	28561	1712
avg50	13168	43582	37110	26696	22527
avg100	12743	42375	37260	27597	50748

TPMovr=234	4	13
avg10	38803	46029
avg50	38530	46078
avg100	45193	45485

TPMovr=263	10	11
avg10	43351	37791
avg50	43582	37110
avg100	42375	37260

Devices with the same TPMovr value can be distinguished on basis of the TPMstate value – selected results for the RTCPS=13 (a-d) and for RTCPS=15 (e, f). avg10, avg50 and avg100 means the value was evaluated as a mean value (arithmetical average) from 10 %, 50 % and 100 % of TPMstate data

Conclusion and Acknowledgements

On basis of our experiments, it can be concluded that it is possible to generate both IDs as well RNDs on basis of physical, non-reproducible parameters of digital COTS devices such as microcontrollers (MCUs) with no necessity of utilizing either a complex and/or very specialized software or hardware for the same purpose. Instead, device's inherent effects can be utilized for that, scalability of which can be extended by a simple jitter-measurement technique based e.g. on the ISR-level or task-level executions.

This work has been partially supported by the COST project No. LD14055 (Unconventional Design Techniques for Intrinsic Reconfiguration of Digital Circuits: From Materials to Implementation), the project No. FIT-S-14-2297 (Architecture of parallel and embedded computer systems) and the project No. ED1.1.00/02.0070 (IT4Innovations Centre of Excellence).