interview

Dr. Selçuk Köse

"IoT devices are vulnerable to hardware-attacks since they are accessible to attackers"

Dr. Selçuk Köse from the University of South Florida in the United States talks to us about the work behind the paper 'Security implications of simultaneous dynamic and leakage power analysis attacks on nanoscale cryptographic circuits', page 466.

Tell us a little bit about your field of research.

The two primary research thrusts of our group are improving the power efficiency and the trustworthiness of modern integrated circuits. More than 30% of all the power is typically dissipated before even reaching the load circuits during power conversion and delivery. To increase the overall power efficiency, we focus on the source of the problem where we develop circuit, architecture, and system level design methodologies to maximise the voltage conversion efficiency. We have recently proposed a new on-chip power delivery architecture, *regulator-gating*, where we adaptively turn-on and turn-off individual stages of a multiphase voltage regulator based on the workload to improve power efficiency. In our second research thrust, we further leverage the on-chip voltage regulators as a countermeasure against hardware-based side-channel attacks.

What advances have you reported in your *Electronics Letters* paper?

In our Letter, one of my PhD students, Weize Yu, and I have investigated the implications of combining two different hardware-based side-channel attacks: dynamic and leakage power analysis attacks. We have shown that combining two different attacks, can be significantly more powerful than performing individual attacks. The strength of a combined attack increases as the correlation between the obtained information with each individual attack decreases. Intuitively, when an attacker performs an individual attack, each subsequent data will be highly correlated with the preceding data sample. When another attack that provides loosely correlated data samples to the existing attack is performed, combining these two attacks would significantly reduce the number of measurements to disclose.

What is the significance of this?

The work reported in our Letter highlights the security implications of combined side-channel attacks where combining two attacks could be ten times more powerful than an individual attack. This work accentuates the need for more effective countermeasures against hardware-based side-channel attacks.

What are the real world applications?

With the prospected proliferation of Internet-of-Things (IoT) devices with 5G networks, hardware-security will become even more crucial. The research covered in the Letter exemplifies one of the various possible attack scenarios that may target critical information stored in commercial or personal devices. Since people typically tend to use the same password for various devices, the implications of a successful attack could be quite devastating.

IoT devices are quite vulnerable to hardware-attacks since they are typically more accessible to an attacker as compared to the other general purpose computing devices. Additionally, IoT have limited battery power and significant physical constraints. These limitations when combined with the cost constraints make the design of security measures for the IoT quite challenging. Existing countermeasures utilised in general purpose computing devices are mostly not feasible for IoT.

What are you working on now?

Design and management of on-chip power delivery play a central role in our research. While our group is working on several topics at different levels of abstraction for secure and efficient design of next generation power delivery systems, we also leverage on-chip voltage regulators for thermal management and hardware Trojan detection. With the continuous scaling of the transistor size, temperature has recently become a significant design parameter where only a small portion of the transistors can be active at a certain time to not exceed the maximum thermal design power. We are currently working on on-chip thermal management techniques with the help of on-chip voltage regulators.

How do you think the field will develop over the next ten years?

Over the past couple of years, security has become a new design constraint in addition to the existing constraints such as power, noise, speed, and performance. In the next ten years, the importance of security and privacy will continue to increase with the number of connected devices that have become an integral part of our lives. Designing effective security measures at all levels of design abstraction without significant power, performance, and cost overhead will therefore be a significant research area in the next decade.

doi: 10.1049/el.2016.0610