

LEAKAGE CURRENT MAY BE THE GATE NO ONE THOUGHT TO LOCK
THAT ALLOWS HACKERS TO CRACK HARDENED SYSTEMS.

Leakage-power analysis **ENABLES ATTACKS** on cryptographic devices

BY MILENA JOVANOVIĆ • UNIVERSITY OF MONTENEGRO

Security requirements are increasingly stringent in applications such as e-commerce and electronic banking. Although encryption technology provides robust algorithms, the physical implementation of those algorithms usually leaks information through physical phenomena relating to the electrical operation of the devices, which an attacker could use to detect the secret key. These “side-channel” attacks use information that the hardware implementation of encryption modules leaks. This information could include correlation between data and power consumption or timing (**Reference 1**). Differential-power analysis is a well-documented, powerful side-channel attack because

it allows the attacker to detect secret keys by using a measurement setup employing off-the-shelf components (**Reference 2**). The attacker relies on the fact that standard CMOS logic exhibits a dynamic-power consumption that strongly depends on the input data. For example, consider a simplified model of a CMOS

inverter that receives its load from a capacitance that connects to ground. The model draws its current from a supply only for a zero-to-one output transition. In a one-to-zero transition, the energy in the output capacitance dissipates, and the circuit consumes no power for zero-to-zero and one-to-one transitions.

Engineers have recently proposed many countermeasures employing both software and RTL (register-transfer-level) logic to thwart attacks through dynamic-power analysis (**Reference 3**).

Historically, the primary contributor to power dissipation in CMOS circuits has been dynamic power due to CMOS-switching activity. Dynamic power has a quadratic dependence on supply voltage and a linear dependence on clock frequency. Another important contribution to power consumption in CMOS circuits is leakage power due to parasitic currents in switched-off CMOS devices. That leakage power will most likely soon approach a level comparable with that of dynamic-power consumption (**Reference 4**). Leakage current in a CMOS design strongly depends on the input-data vector, and engineers have used this property to reduce leakage-power dissipation during circuits’ standby periods (**references 5, 6, and 7**). They have also pro-

posed models that can estimate the input vector that produces maximum and minimum leakage current, respectively, in CMOS circuits (Reference 8).

Given leakage current's dependence on input values in CMOS logic, you can use leakage-current measurements to extract information about the secret data in a cryptographic core. After analyzing the dependency of leakage current on input data on a simple cryptographic core using RTL simulations, you can use statistical-analysis techniques to mount attacks. These techniques are similar to those that differential-power analysis uses and allow you to extract the secret key starting from leakage-current measurements, which are, in principle, easier to perform.

DATA DEPENDENCE

The main sources of leakage current are inverse-junction, subthreshold, and

AT A GLANCE

- ▶ Differential-power analysis allows the attacker to detect secret keys by using a measurement setup employing off-the-shelf components.
- ▶ The primary contributor to power dissipation in CMOS circuits is dynamic power due to CMOS-switching activity.
- ▶ You typically use substitution boxes to obscure the relationship between the plain text and the cipher text.
- ▶ You collect side-channel information by measuring some physical quantity.

gate-tunnel current (Reference 9). Subthreshold current is the most important contributor in a MOS transistor biased in a weak inversion region. Designers

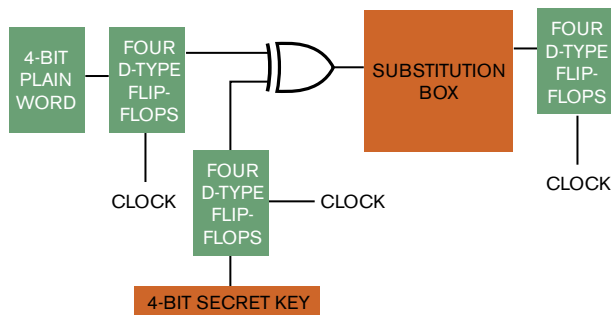


Figure 1 You can build a simple cryptographic core by adding registers to a combinational design.

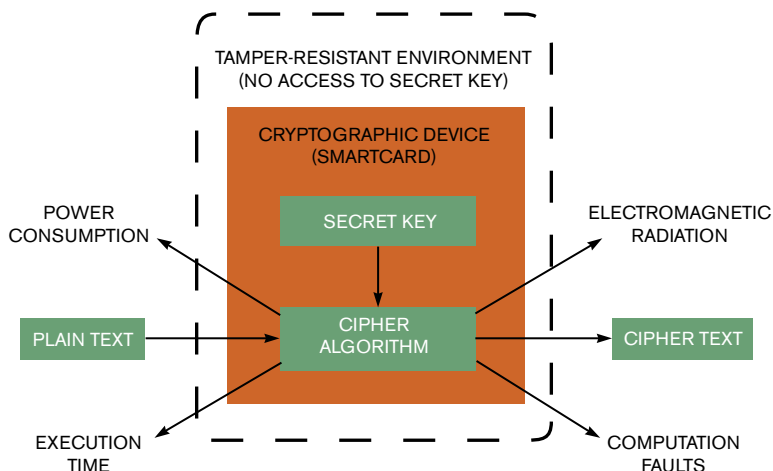


Figure 2 Passive attacks benefit from side-channel information, which you collect by measuring some physical quantity.

of standard-CMOS gates base them on pullup and pulldown networks comprising parallel and series connections. Designers have developed models for the leakage current of MOS devices in series and parallel configurations.

To understand the data dependence of leakage current in standard-CMOS gates, researchers performed simulations on the standard cells of the 90-nm CMOS090 process from STMicroelectronics (www.st.com). These simulations used foundry-supplied models for the Spectre transistor-level simulator, employing five temperatures to verify the temperature dependence of leakage current (Table 1, which is available with the Web version of this article at www.edn.com/090528df). If you sort the leakage currents in the table in ascending order, the same order remains with temperature variations. For example, in a two-input NAND gate, logic input 01 can generate the maximum leakage current for all temperature values. This approach to power analysis exploits the input combination that produces the maximum or minimum leakage current of a cryptographic core. Available literature describes maximum, minimum, and other algorithms to estimate the leakage current.

The basic component of symmetric-key algorithms is the substitution box. When dealing with block ciphers, you typically use substitution boxes to obscure the relationship between the plain text and the cipher text. A substitution box provides a combinational mapping between an N-bit input word and an M-bit output word. These boxes—for example, those with four inputs and four outputs—normally use fixed tables.

Employing a truth table and a 90-nm-CMOS-process library from STMicroelectronics, Cadence (www.cadence.com) researchers synthesized a “serpent” substitution box—one having four inputs and four outputs (Table 2, which is available with the Web version of this article at www.edn.com/090528df). Researchers then performed extensive leakage-current simulations for all possible input combinations of the substitution box. If you sort the input combinations in the table in increasing order of leakage-current consumption, the results remain independent of temperature variations. Thus, you can use any thermal co-



efficient, providing that it remains constant, in simulations or measurements. You can realize a combinational part of a simple cryptographic core by connecting XOR gates to the inputs of a substitution box. XOR gates premix any plain words and secret keys, and a substitution box ciphers the results. You can perform extensive leakage-current simulations on the combinational part of a cryptographic core for all values of keys and inputs. If you put the leakage-current values in ascending order, the order of inputs and outputs will be the same for each key, meaning that leakage current does not depend on the values of the inputs. These simulations also show that the values of leakage current differ for different keys and the same inputs. XOR gates, which are sensitive to the input changes, cause this difference. The substitution box is not the culprit because, for the same input, you can always measure the same current.

You can build a simple cryptographic core by adding registers to a combinational design (**Figure 1**). **Table 3**, which is available with the Web version of this article at www.edn.com/090528df, reports the leakage current of the registers for the input combinations and shows how the leakage current directly relates to the number of ones in a binary word. Simulations on whole cryptographic cores explore all possible combinations

of plain words and keys (**Table 4**, which is available with the Web version of this article at www.edn.com/090528df). The **table** sorts leakage currents in increasing order and groups them by input keys; input columns are the inputs of the substitution box, and output columns are the outputs of the cryptographic core.

LEAKAGE-CURRENT ATTACK

Researchers typically divide attacks on cryptographic algorithms into mathematical and implementation categories, basing the implementation category on passive or active weakness. Researchers are trying to design countermeasures to thwart these powerful attacks (**Reference 10**). Passive attacks benefit from side-channel information, which you collect by measuring some physical quantity (**Figure 2**). Active attacks are more invasive because they introduce faults that result in erroneous calculations, leading to the exposure of a secret key.

The most common side channel for attacks is a device's power consumption. These types of attacks use simple power analysis, differential-power analysis, and correlation-power analysis (**Reference 11**). In a simple-power-analysis attack, an attacker uses the side-channel information from one measurement to directly determine a secret key or parts of a secret key. Differential- and correlation-power analyses are statistical at-

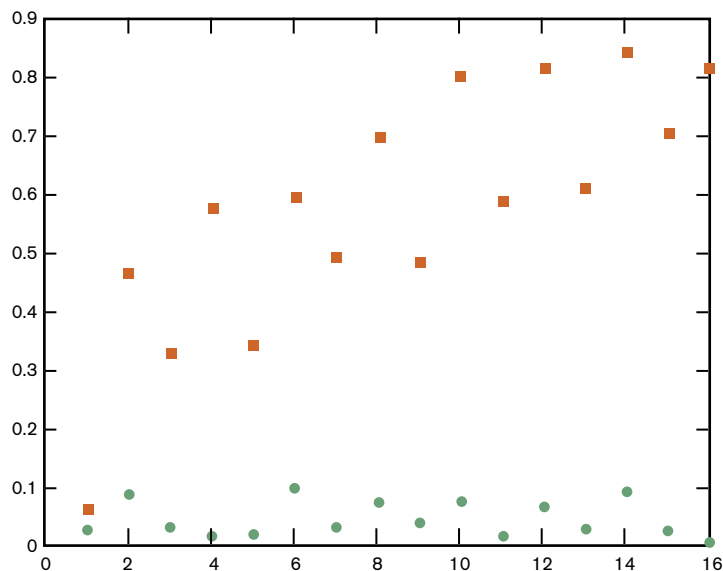


Figure 3 Results from the leakage-power-analysis attack show that all keys but the 0000 key are clearly distinguishable from the leakage-power data.



⊕ Go to www.edn.com/090528df and click on Feedback Loop to post a comment on this article.

⊕ For a list of the references cited in this article, go to www.edn.com/090528df.

tacks and need a lot of measurements and data acquisition. A correlation-power attack involves collecting data and then analyzing the collected data and uses a so-called hypothetical model of the attacked device.

You can use a statistical-analysis tool to detect the key of the cryptographic core. You can also use an attack employing the computation of the correlation coefficient between the vector of acquired leakage currents and a logic vector that uses a hypothesis of the secret key. The method uses the hamming weight, or number of ones in a binary word, of the inputs in the substitution box as a logic vector. You can obtain this weight from a key hypothesis. **Figure 3** shows the computed correlation coefficients. Orange squares denote the right-key hypothesis, and green circles denote a random-key hypothesis. The result is that all keys, except key 0000, are clearly distinguishable by using this kind of attack. Researchers are investigating why you get different results for key 0000.

This preliminary study shows the realistic possibility of using leakage currents to reveal secret keys. The result of the attack employing correlation coefficients suggests that leakage-power analysis could become a problem you should consider during cryptographic-core design, especially for cores in technologies with gates shorter than 0.1 micron that exhibit a high leakage-power consumption. **EDN**

AUTHOR'S BIOGRAPHY

Milena Jovanovic has been a teaching assistant in the electrical-engineering department at the University of Montenegro (Podgorica, Montenegro) since January 2007, teaching courses in electronics, computer peripherals and interfaces, and electrical-engineering materials. Jovanovic has a master's degree in electronics and is currently pursuing a doctorate in electrical engineering at the University of Montenegro. You can reach her at jmilena1983@yahoo.com.