WHITE PAPER

Chronos Security- Hiding the Power Signature

By G. Rinaldi & S. Giaconi, Chronos Tech

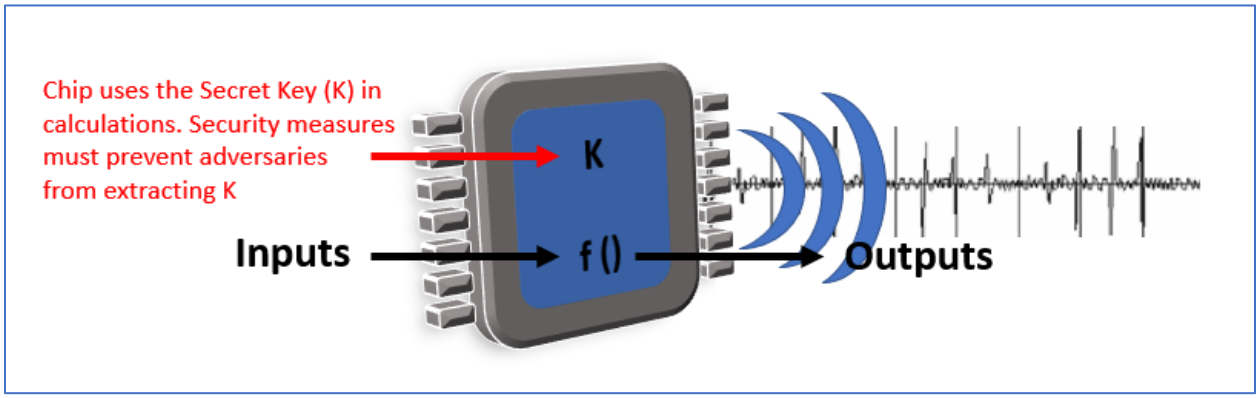
Description:

Security is one of the hottest topics in technology nowadays. Cryptography, for example, is widely used to prevent an attacker from getting access to private information and it is seamlessly used everywhere (Wi-Fi, Credit Card, GSM, CDMA, etc.).

Software attacks are the most common, but usually can be easily mitigated by implementing frequent software updates. Unfortunately, there is another class of attacks that are more difficult to prevent and make the cryptography shield much less effective: hardware attacks.

One of the common assumptions in cryptography is that no information about the keys is known to the attacker and that the cypher implementation is behaving like a black box with only the "ciphertext" as output. Unfortunately, many internal hardware characteristics are easily observable and can be measured to detect the secret keys.

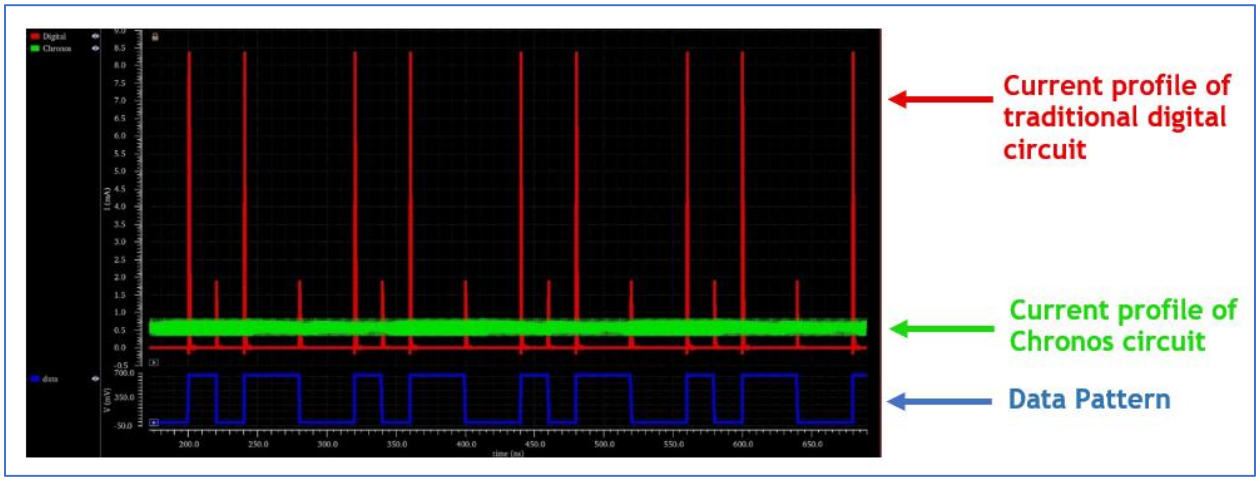
Some examples of what are commonly called side channels are: power consumption, electromagnetic radiation, and timing variations.



If the attacker can correlate this side channel information with the secret key, security can be compromised. Side channel attacks leave no trace, and can often be performed quickly using consumer-level equipment. Once the secret keys have been extracted, attackers can gain unauthorized access, decrypt or forge messages, steal identities, clone devices, create unauthorized signatures, and perform other unauthorized transactions.

One of the most well-known and effective side-channel attacks today is the information leaked through the power consumption of the chip. Differential Power Analysis (DPA), for example, makes use of effective statistical algorithm to retrieve internal information to be used to break the security of the system.

Chronos technology is very effective in mitigating DPA attacks due to its unique power consumption profile. This is a consequence of Chronos' patented Delay Insensitive channels with clockless temporal compression.



In the previous example a simulation shows the difference between the power profile of a simple digital channel vs. the power profile of the same channel implemented with Chronos Technology. As shown, the total current profile of the traditional channel shows very high current peaks which are correlated to the data pattern of the data being transmitted. In the case of Chronos instead, the current profile shows a very even behavior during the transaction and there is no direct correlation between the current profile and the data being transmitted. Another measurable effect of the change in power profile is the significant reduction in Electromagnetic Interference (EMI), the electromagnetic emission of a Chronos channel has much lower power peaks with energy more evenly spread out through the frequency spectrum. The result of adding Chronos Technology to a communication channel is a significant increase in security.