THE UNIVERSITY OF
MELBOURNE

Opportunity

To accelerate development of the chip design methodology through licensing or co-development, contact:

Eric Höfgen
T: +61 3 8344 4519
E: heric@unimelb.edu.au

Chip design methodology

Improving cybersecurity of low-power devices such as smart cards

The technology

- The chip design methodology uses an application-specific integrated circuit (ASIC) to hide a chip's encryption operations. This prevents cybersecurity breaches via side-channel attacks.

Market need

- Low-power devices such as smart cards store sensitive personal data. More robust cybersecurity is needed to prevent unauthorised access.

Technology status

- A chip created with the new methodology outperformed standard encryption methods. A patent has been filed for the design methodology.

Market need

More secure hardware and software are needed to protect low-power devices such as smart cards from cyberattacks.

Low-power devices that store sensitive data for identification – such as smart cards that control access to buildings, public transport and bank accounts – use cybersecurity to prevent unauthorised access to the data. These devices cannot use conventional cryptographic methods to encrypt data, because they do not have the necessary computational power. Instead, they rely on lightweight ciphers. This makes the devices vulnerable to cyberattacks known as 'side-channel' attacks. They break encryption by reading information from the processing chip embedded in the card – such as its power consumption or operating time. A new design approach is needed to create chips that can prevent these attacks.

The global market for smart cards was estimated at more than US$8 billion in 2019 and is expected to reach more than US$11 billion by 2025. Smart cards are used for credit cards, access-control cards, identification badges, electronic passports and driver licenses. As many as 50 billion smart cards are in circulation today.

Technology and IP status

The chip design is currently optimised for use in application-specific integrated circuit (ASIC) applications. A patent has been filed for the chip design, and further development is ongoing.

The research team is working to enhance the chip design's field-programmable capabilities, so that it can be configured by customers after manufacture. They are particularly interested in collaborating with a licensee to adjust the ASIC design for specific applications.

Solution

A methodology for designing chips that prevent side-channel attacks has been developed by a team led by Professor Udaya Parampalli. It prevents two common types of side-channel attack: propagation-delay and power-analysis attacks.

Propagation-delay attacks measure the time between different inputs to the chip. This information can reveal how a chip works, thus enabling encryption to be broken. Chips created with the new design methodology take the same amount of time to complete logical operations such as 'AND', 'XOR' and 'XNOR', thus preventing propagation-delay attacks. The design performed the same or better than existing encryption approaches.

Power-analysis attacks measure variations in the chip's power consumption to break encryption. The peak power variance of the new chip design is 103–104 times lower than that of other encryption algorithms, including substitution-box (S-box) algorithms like Lucifer and PRESENT. The research team also compared the new chip design to other basic chip designs, such as those using dual path binary decision diagrams (DPBDD), secure differential multiplexer logic (SDMLp) and wave dynamic differential logic (WDDL). Their tests showed that the peak power variance is negligible for algorithms and basic chip designs produced by the new methodology. The new designs also use 2–7 times less average power than other designs, thus enhancing the chips' lifespan.

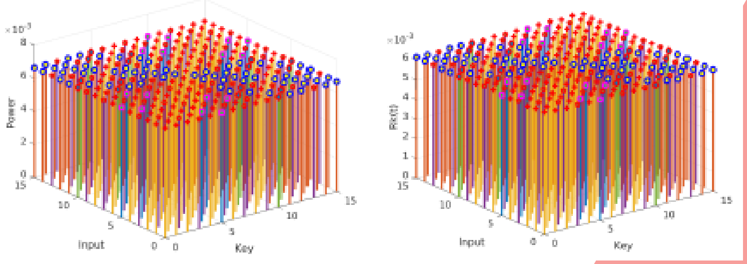

Figure: Correlation Power Analysis attack on a) Present transmission gate S-Box design and b)Lucifer transmission gate based S-box design demonstrating that there is no noticeable difference between inputs. Author: Partha De

Tech name and number:	2020-080 Secure Path Balanced based Approach to Counter Power and Timing Attacks
Researchers:	Professor Udaya Parampalli, Dr Ranjith Unnithan, Partha De
Patents:	Provisional patent in preparation
Publications:	Manuscript in preparation
Keywords:	cybersecurity, internet of things, side-channel attacks, smart cards