Analysis and Conception of Symmetric Key Cryptography Primitives

Highly constrained devices (automotive systems, sensor networks, distributed control systems, IoT, etc.) are getting more and more interconnected and security becomes paramount. Yet, as the majority of modern cryptographic algorithms were designed for desktop/server environments, many of these algorithms cannot be implemented in such constrained devices.

The SYmmetric and Lightweight cryptography Lab at Nanyang Technological University in Singapore works at delivering lightweight cryptographic algorithms, fit for the most constrained devices, while providing high security against latest cryptanalysis advancements. For example, our PHOTON algorithm is the smallest known cryptographic hash function, providing authentication capabilities while being suited even for the smallest RFID tags (now an ISO/IEC 29192-5:2016 standard).

Our team is currently designing new cipher technologies to enable broader security primitives for constrained devices: encryption, authentication, etc.. The final goal is to build a do-it-all cryptographic primitive, easy to implement, flexible, and that can scale to tiny devices, but performs also very well on micro-controllers or high-end servers.

We also work on evaluating the security of various cryptographic algorithms, in different scenarios: from very pure and theoretical cryptanalysis attacks to very practical side-channel cryptanalysis.

Principal Investigators	Asst. Prof. Thomas Peyrin *(SPMS)*
Researchers	Dr. Mohona Ghosh Dr. Ivica Nikolic Dr. Sumit Kumar Pandey
Students	Mr. Siang Meng Sim Mr. Pierre Karpman Mr. Anubhab Baksi Mr. Wang Haoyang Mr. Mustafa Kairallah
School / Department	School of Physical & Mathematical Sciences
Grant Agency	National Research Foundation, Singapore (NRF Fellowship)