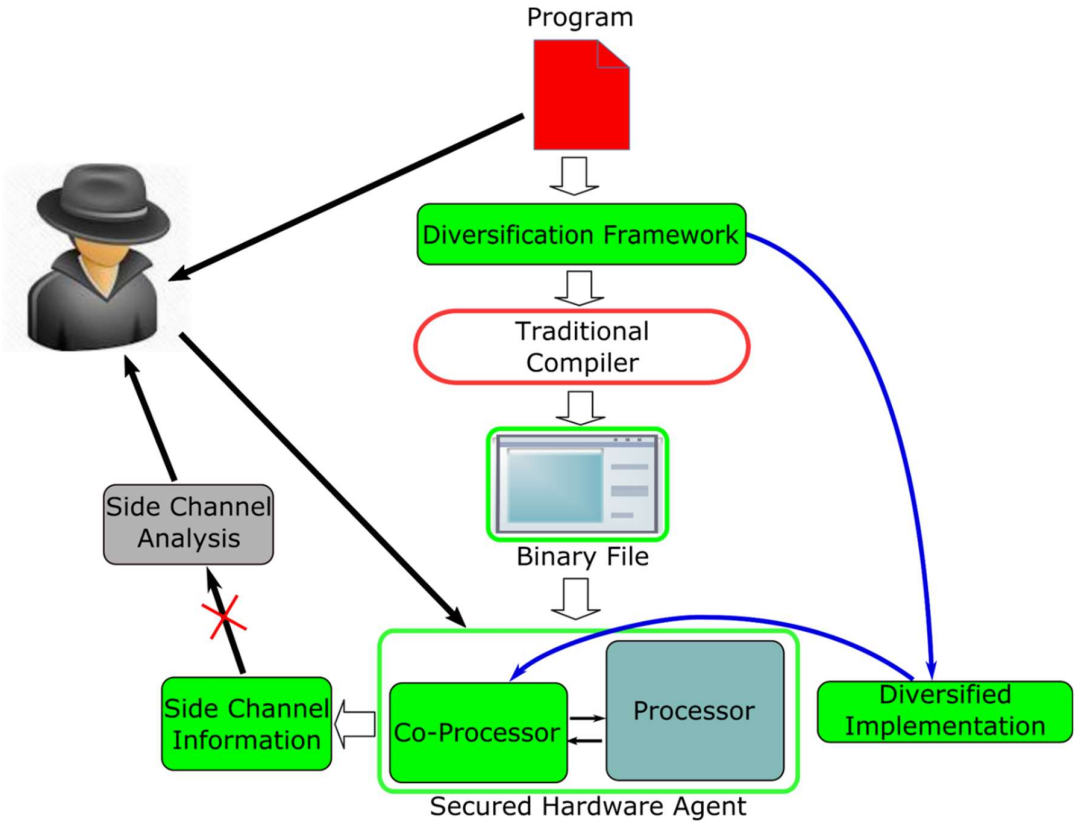
Exploiting Custom Instructions for Program Diversification to Protect Against Timing Side Channel Attacks

We propose to use diversity to vary the side channel characteristics of the program during execution. In particular, we will develop novel techniques for dynamic hardware diversification of the cryptographic primitives using custom instructions to prevent timing side-channel attacks. We envisaged that the proposed techniques will introduce significantly lesser overheads compared to existing methods.



Principal Investigators	Asst. Prof. Lam Siew Kei *(SCSE, NTU)*
Researchers	Dr. Arnab Kumar Biswas Dr. Pham Hung Thinh Dr. Alexander Fell
School / Department	School of Computer Science and Engineering
Source of Funding	National Research Foundation, Singapore