

Analyzing side-channel attack vulnerabilities at RTL

Lai, Xinhui; Jenihhin, Maksim 2023 IEEE 24th Latin American Test Symposium (LATS) 2023 / 2 p. : ill
<https://doi.org/10.1109/LATS58125.2023.10154497>

SCAAT: Secure cache alternative address table for mitigating cache logical side-channel attacks

Shalabi, Ameer; Ghasempouri, Tara; Ellervee, Peeter; Raik, Jaan 2020 23rd Euromicro Conference on Digital System Design (DSD), 26-28 August 2020, Kranj, Slovenia 2020 / art, 20035366, p. 213–217 <https://doi.org/10.1109/DSD51259.2020.00043>

Side-channel attacks on triple modular redundancy schemes

Almeida, Felipe; Aksoy, Levent; Raik, Jaan; Pagliarini, Samuel Nascimento 2021 IEEE 30th Asian Test Symposium ATS 2021 : proceedings 2021 / p. 79-84 : ill <https://doi.org/10.1109/ATS52891.2021.00026> [Conference Proceedings at Scopus](#) [Article at Scopus](#) [Article at WOS](#)

Side-channel Trojan insertion - a practical foundry-side attack via ECO

Perez, Tiago Diadami; Imran, Malik; Vaz, Pablo; Pagliarini, Samuel Nascimento 2021 IEEE International Symposium on Circuits and Systems (ISCAS), Daegu, Korea, May 22-28, 2021 : proceedings 2021 / 5 p. : ill <https://doi.org/10.1109/ISCAS51556.2021.9401481> [Conference Proceedings at Scopus](#) [Article at Scopus](#) [Article at WOS](#)

Verifying cache architecture vulnerabilities using a formal security verification flow

Ghasempouri, Tara; Raik, Jaan; Paul, Kolin; Reinbrecht, Cezar; Hamdioui, Said; Taouil, Mottaqiallah Microelectronics reliability 2021 / art. 114085 <https://doi.org/10.1016/j.microrel.2021.114085> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)