

Design and verification of secure cache wrapper against access-driven side-channel attacks

Niazmand, Behrad; Azad, Siavoosh Payandeh; Jervan, Gert; Sepulveda, Johanna Euromicro Conference on Digital System

Design : DSD 2019 : 28 - 30 August 2019 Kallithea, Chalkidiki, Greece : proceedings 2019 / p. 672-676 : ill

<https://doi.org/10.1109/DSD.2019.00108>

Design of Cyber Bio-analytical Physical Systems : formal methods, architectures, and multi-system interaction strategies

Ashraf, Kanwal; Le Moullec, Yannick; Pardy, Tamas; Rang, Toomas Microprocessors and microsystems 2023 / art. 104780, 14

p. : ill <https://doi.org/10.1016/j.micpro.2023.104780> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Mapping requirements specifications into a formalized blockchain-enabled authentication protocol for secured personal identity assurance

Leiding, Benjamin; **Norta, Alexander** Future Data and Security Engineering : 4th International Conference, FDSE 2017, Ho Chi Minh

City, Vietnam, November 29 - December 1, 2017 : proceedings 2017 / p. 181-196 : ill https://doi.org/10.1007/978-3-319-70004-5_13

[Conference proceedings at Scopus](#) [Article at Scopus](#) [Article at WOS](#)

Safeguarding a formalized blockchain-enabled identity-authentication protocol by applying security risk-oriented patterns

Norta, Alexander; Matulevičius, Raimundas; Leiding, Benjamin Computers & Security 2019 / p. 253-269

<https://doi.org/10.1016/j.cose.2019.05.017> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Securing verified IO programs against unverified code in FI

Andrici, Cezar-Constantin; Ciobăca, Stefan; Hrițăcu, Catalin; Martínez, Guido; **Rivas Gadda, Exequiel Matías;** Tanter, Éric;

Winterhalter, Théo Proceedings of the ACM on programming languages 2024 / art. 74, 34 p. : ill <https://doi.org/10.1145/3632916> [Journal](#)

[metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

A security verification template to assess cache architecture vulnerabilities

Ghasempouri, Tara; Raik, Jaan; Paul, Kolin; Reinbrecht, Cezar; Hamdioui, Said; Taouil, M. 2020 23rd International Symposium on

Design and Diagnostics of Electronic Circuits and Systems (DDECS), April 22nd – 24th 2020 Novi Sad, Serbia : Proceedings 2020 /

art. 9095707, 6 p <https://doi.org/10.1109/DDECS50862.2020.9095707>

SSProve : a foundational framework for modular cryptographic proofs in Coq

Haselwarter, Philipp G.; **Rivas, Exequiel;** Van Muylder, Antoine; Winterhalter, Théo; Abate, Carmine; Sidorenco, Nikolaj; Hrițăcu,

Cătălin; Maillard, Kenji; Spitters, Bas ACM Transactions on Programming Languages and Systems 2023 / art. 15

<https://doi.org/10.1145/3594735> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [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](#)