

From: [Foti, James \(Fed\)](#)
To: [Kerman, Sara J. \(Fed\)](#)
Subject: Master list of Journals --RE: CSRC New Publications (Journals/Conferences)
Date: Tuesday, February 26, 2019 12:14:49 PM
Attachments: [External-Cyber-Pubs-Master.xlsx](#)

Hi Sara-

Thanks so much for all that! I have gone ahead and published them. Just included some notes below, for future guidance/reference. Let me know if you have any questions!

Jim

From: Kerman, Sara J. (Fed)
Sent: Tuesday, February 26, 2019 8:30 AM
To: Foti, James (Fed) <james.foti@nist.gov>
Subject: CSRC New Publications (Journals/Conferences)

Hi Jim,

Welcome back! I entered the following publications into CSRC. The last four pubs have some missing authors in CSRC admin.

These have all been checked in and ready for your review.

The Trouble with Terms

CSRC Topics: General Security & Privacy

-For journal articles, in the Publication Date field we include the issue date as it's indicated by the journal. E.g., this one is "November/December 2018" instead of just "December 2018". If you are not sure about the proper format for it (each journal does their own thing, it seems), you can either a) refer to the image of the journal cover, or b) see if that journal is already included in our database —for that, I'm attaching a spreadsheet of our "external pubs". Eventually we'll add pick lists to the pubs interface...SOMETIME... :-0)

Toward Cyberresiliency in the Context of Cloud Computing

CSRC Topics: security measurement; cloud & virtualization

-Added "threats" topic.

-Pub Date: November/December 2018

Comprehensive Security Assurance Measures for Virtualized Server Environments [FYI – this is a book chapter. DOI points to "book" not chapters]

CSRC Topics: cloud & virtualization; hardware, servers

-DOI: changed to chapter-specific DOI.

-Series Title: Lecture Notes in Computer Science

-Added topics: assurance; threats

-Removed Chapter #, since none is specified in the book itself.

-Changed Abstract to match what's on the publisher's site.

A Layered Graphical Model for Cloud Forensic and Mission Impact Analysis [FYI – this proceedings was not “published” until late last year/early this year, but I used the Pub Date and Release date as it correlated with the conference]

CSRC Topics: forensics, Security and Privacy, risk management, threats; Technologies; cloud & virtualization; networks

-Publication Date: January 3-5, 2018 [dates of conference]

-Proceedings Title: shortened to just “Advances in Digital Forensics XIV” – these are a little tricky, but if the subtitle info also appears in our Publication Date and Conference Location fields, then I tend to leave them out and keep the Proceedings title concise. This also helps prevent repetition in a reference that is automatically generated from reference manager software like EndNote.

-DOI: used the paper-specific DOI

-Added topic: modeling

Parallel Self-Testing of the GHZ State with a Proof by Diagrams

CSRC Topics: cryptography

-Publication and Release Dates: Since this was part of a conference, I kept the dates consistent with that conference. When users go to the DOI, they’ll see any newer releases (like this v2 from January 2019).

The New Randomness Beacon Format Standard: An Exercise in Limiting the Power of a Trusted Third Party

CSRC Topics: cryptography; random number generation

-Hmmm...I don’t see this one at all. What’s the release date? What pub series?

-----need authors entered-----

On the complexity and verification of quantum random circuit sampling

CSRC Topics: cryptography

None of the authors were listed, can you add? *I also couldn’t find Univ of CA, Berkeley either*

- Bouland, Adam; University of California, Berkeley
- Fefferman, William J. ; NIST
- Nirkhe, Chinmay; University of California, Berkeley
- Vazirani, Umesh; University of California, Berkeley

SPHINCS-Simpira: Fast Stateless Hash-based Signatures with Post-quantum Security <- *I did this as a white paper (eprint.iacr.org)*

CSRC Topics: cryptography; post-quantum cryptography; digital signatures

- Shay Gueron (Intel is already available)

Elliptic Curves Arising from Triangular Numbers

CSRC Topics: cryptography

- Shiv Kumar (his affiliation is already in the database)

A Method-Level Test Generation Framework for Debugging Big Data Applications

CSRC Topics: Security Measurement Technologies: Big Data

Huadong Feng (both with Univ of Texas at Arlington – which is already in database)

- Jagan Chandrasekaran