Submission Data for 2017 CORE conference Re-ranking process
Workshop on Cryptographic Hardware and Embedded Systems

Submitted by: Yuval Yarom zz-linkedin@qwerty.co.il
Supported by: Yuval Yarom

Conference Details

Conference

Title: Workshop on Cryptographic Hardware and Embedded Systems
Acronym : CHES
Rank: C

Requested Rank

Requested Rank: A

Recent Years

Most Recent Year

Year: 2017
URL: https://ches.iacr.org/2017/
Papers submitted: 130
Papers published: 33
Acceptance rate: 25
Source for acceptance rate: http://www.springer.com/gp/book/9783319667867

Program Chairs

Name: Wieland Fischer Affiliation: Infineon Technologies H index: -1 Google Scholar URL: DBLP URL: http://dblp.uni-trier.de/pers/hd/f/Fischer:Wieland
Name: Naofumi Homma Affiliation: Tohoku University H index: 19 Google Scholar URL: https://scholar.google.com.au/citations?user=NuguztsAAAAJ&hl=en DBLP URL: http://dblp.uni-trier.de/pers/hd/h/Homma:Naofumi

General Chairs

Name: Bo-Yin Yang Affiliation: Academia Sinica H index: 30 Google Scholar URL: https://scholar.google.com.au/citations?user=hI3a_oIAAAAJ&hl=en DBLP URL: http://dblp.uni-trier.de/pers/hd/y/Yang:Bo=Yin
Name: Chen-Mou Cheng Affiliation: National Taiwan University H index: 18 Google Scholar URL: https://scholar.google.com.au/citations?user=WKmNG2sAAAAJ&hl=en DBLP URL: http://dblp.uni-trier.de/pers/hd/c/Cheng:Chen=Mou

Second Most Recent Year

Year: 2016
URL: https://www.iacr.org/workshops/ches/ches2016/start.php
Papers submitted: 148
Papers published: 30
Acceptance rate: 20
Source for acceptance rate: http://www.springer.com/gp/book/9783662531396

Program Chairs

Name: Axel Poschmann Affiliation: NXP H index: 22 Google Scholar URL: https://scholar.google.com.au/citations?user=7dzeXRoAAAAJ&hl=en DBLP URL: http://dblp.uni-trier.de/pers/hd/p/Poschmann:Axel
Name: Benedikt Gierlichs Affiliation: KU Leuven H index: 25 Google Scholar URL: https://scholar.google.com.au/citations?user=Znj7XP8AAAAJ&hl=en DBLP URL: http://dblp.uni-trier.de/pers/hd/g/Gierlichs:Benedikt

General Chairs

Name: Erkay Savas Affiliation: Sabanci University H index: 25 Google Scholar URL: https://scholar.google.com.au/citations?user=biKy5tsAAAAJ&hl=en DBLP URL: http://dblp.uni-trier.de/pers/hd/s/Savas:Erkay
Name: Çetin Kaya Koç Affiliation: University of California Santa Barbara H index: 41 Google Scholar URL: https://scholar.google.com.au/citations?user=pd-IjLcAAAAJ&hl=en DBLP URL: http://dblp.uni-trier.de/pers/hd/k/Ko=ccedil=:=Ccedil=etin_Kaya

Third Most Recent Year

Year: 2015
URL: https://www.iacr.org/workshops/ches/ches2015/
Papers submitted: 128
Papers published: 34
Acceptance rate: 27
Source for acceptance rate: http://www.springer.com/gp/book/9783662483237#aboutBook

Program Chairs

Name: Tim Güneysu Affiliation: University of Bremen H index: 26 Google Scholar URL: https://scholar.google.com.au/citations?user=QrXiIS0AAAAJ&hl=en DBLP URL: http://dblp.uni-trier.de/pers/hd/g/G=uuml=neysu:Tim
Name: Helena Handschuh Affiliation: Cryptography Research H index: 21 Google Scholar URL: https://scholar.google.com.au/citations?user=b_xI-SwAAAAJ&hl=en DBLP URL: http://dblp.uni-trier.de/pers/hd/h/Handschuh:Helena

General Chairs

Name: Emmanuel Prouff
Affiliation: ANSSI
H index: 26
Google Scholar URL: https://scholar.google.com.au/citations?user=2KSRvI8AAAAJ&hl=en
DBLP URL: http://dblp.uni-trier.de/pers/hd/p/Prouff:Emmanuel

Name: Matthieu Rivain
Affiliation: CryptoExperts
H index: 22
Google Scholar URL: https://scholar.google.com.au/citations?user=9sCtc54AAAAJ&hl=en
DBLP URL: http://dblp.uni-trier.de/pers/hd/r/Rivain:Matthieu

Name: Guenael Renault
Affiliation: UPMC
H index: 11
Google Scholar URL: https://scholar.google.com.au/citations?user=B85idEMAAAAJ&hl=en
DBLP URL: http://dblp.uni-trier.de/pers/hd/r/Renault:Gu=eacute=na=euml=l

External Ranks

Google Scholar Rank

Sub-category URL:
https://scholar.google.com.au/citations?view_op=top_venues&hl=en&vq=eng_computersecuritycryptography
Position in sub-category: 14
h5-index of 20th item in subcategory: 28
h5-index of this conference: 32
Next conference above portal link: http://portal.core.edu.au/conf-ranks/1815/
h5-index of above conference: 34
Next conference below portal link: http://portal.core.edu.au/conf-ranks/61/
h5-index of below conference: 31

LiveSHINE rank

Class: A+
H-index: 68
RankH-index: 69
Avg citations: 50
RankAvgCitations: 39
ClassAvgCitations: A++
Publications: 347
Citations: 17472

Microsoft Academic rank

Class: A+
FiledRating: 86
RankFieldRating: 103
ClassFieldRating: A
Avg citations: 48
RankAvgCitations: 32
ClassAvgCitations: A++
Publications: 642
Citations: 30795

Where others publish

General Report

File: http://portal.core.edu.au/core/media/conf_rank_report/CHES-report_yi5cEf9.txt
List of people with h-indices:

No.	Name	h index	url
1	Ingrid Verbauwhede	63	https://scholar.google.com.au/citations?user=ZyG1ZGgAAAAJ&hl=en
2	François-Xavier Standaert	51	https://scholar.google.com.au/citations?user=JvBXO48AAAAJ&hl=en
3	Christof Paar	57	https://scholar.google.com.au/citations?user=w81afLAAAAAJ&hl=en
4	Daniel J. Bernstein	46	https://scholar.google.com.au/citations?user=ToxxF5oAAAAJ&hl=en
5	Joos Vandewalle	75	https://scholar.google.com.au/citations?user=Swa4FrsAAAAJ&hl=en
6	Bart Preneel	68	https://scholar.google.com.au/citations?user=omio-RsAAAAJ&hl=en
7	Moti Yung	87	https://scholar.google.com.au/citations?user=ScL8iFQAAAAJ&hl=en
8	Ari Juels	71	https://scholar.google.com.au/citations?user=uf0D-uoAAAAJ&hl=en
9	Jean-Jacques Quisquater	63	https://scholar.google.com.au/citations?user=KXkSNy4AAAAJ&hl=en
10	Nigel P. Smart	54	https://scholar.google.com.au/citations?user=Qvm3k64AAAAJ&hl=en
11	Paul C. van Oorschot	67	https://scholar.google.com.au/citations?user=CMRzTi8AAAAJ&hl=en
12	Sourav Das	70	https://scholar.google.com.au/citations?user=sB4D_HIAAAAJ&hl=en
13	Michael Luby	79	https://scholar.google.com.au/citations?user=OCzTJZ8AAAAJ&hl=en
14	Joseph H. Silverman	50	https://scholar.google.com.au/citations?user=FPa_qFgAAAAJ&hl=en
15	Alfredo De Santis	49	https://scholar.google.com.au/citations?user=Wt7Y3-oAAAAJ&hl=en
16	Michael J. Fischer	49	https://scholar.google.com.au/citations?user=YVy_ry8AAAAJ&hl=en
17	Michael Waidner	57	https://scholar.google.com.au/citations?user=AyRNYLoAAAAJ&hl=en
18	Wade Trappe	51	https://scholar.google.com.au/citations?user=muk0-U4AAAAJ&hl=en
19	Robert H. Deng	55	https://scholar.google.com.au/citations?user=OPbZGPsAAAAJ&hl=en
20	Salil P. Vadhan	54	https://scholar.google.com.au/citations?user=37frPb8AAAAJ&hl=en

Keyword:
Reference Item:

2. Cryptographic Hardware and Embedded Systems (CHES)

This conference was published at 68 times by 9 of 20 experts in the last 10 years.

The experts that publish at this conference are: Nigel P. Smart(2), Jean-Jacques Quisquater(5), Ingrid Verbauwhede(21), Christof Paar(15), Moti Yung(1), Franois-Xavier Standaert(19), Ari Juels(1), Bart Preneel(5), Daniel J. Bernstein(5)

In 2005, there were 6 publications by 6 experts: Nigel P. Smart, Jean-Jacques Quisquater, Ingrid Verbauwhede, Franois-Xavier Standaert, Bart Preneel, Christof Paar
In 2006, there were 6 publications by 6 experts: Jean-Jacques Quisquater, Ingrid Verbauwhede, Bart Preneel, Franois-Xavier Standaert, Ari Juels, Christof Paar
In 2007, there were 5 publications by 4 experts: Franois-Xavier Standaert, Bart Preneel, Jean-Jacques Quisquater, Christof Paar
In 2008, there were 6 publications by 5 experts: Franois-Xavier Standaert, Ingrid Verbauwhede, Bart Preneel, Daniel J. Bernstein, Christof Paar
In 2009, there were 9 publications by 3 experts: Franois-Xavier Standaert, Christof Paar, Ingrid Verbauwhede
In 2011, there were 7 publications by 4 experts: Franois-Xavier Standaert, Christof Paar, Daniel J. Bernstein, Ingrid Verbauwhede
In 2012, there were 9 publications by 4 experts: Bart Preneel, Franois-Xavier Standaert, Daniel J. Bernstein, Ingrid Verbauwhede
In 2013, there were 6 publications by 4 experts: Franois-Xavier Standaert, Christof Paar, Daniel J. Bernstein, Ingrid Verbauwhede
In 2014, there were 5 publications by 4 experts: Nigel P. Smart, Franois-Xavier Standaert, Daniel J. Bernstein, Ingrid Verbauwhede
In 2015, there were 9 publications by 4 experts: Moti Yung, Franois-Xavier Standaert, Christof Paar, Ingrid Verbauwhede

9 out of the 20 experts published at this conference in 1 or more years
7 out of the 20 experts published at this conference in 2 or more years
6 out of the 20 experts published at this conference in 3 or more years
5 out of the 20 experts published at this conference in 5 or more years
3 out of the 20 experts published at this conference in 8 or more years
2 out of the 20 experts published at this conference in 9 or more years
1 out of the 20 experts published at this conference in 10 or more years

Specialised Report

File: http://portal.core.edu.au/core/media/conf_rank_report/CHES-report2.txt
List of people with h-indices:

No.	Name	h index	url
1	Lars R. Knudsen	41	https://scholar.google.com.au/citations?user=YayQtGUAAAAJ&hl=en
2	Marten van Dijk	41	https://scholar.google.com.au/citations?user=byCWPiwAAAAJ&hl=en
3	Marc Joye	41	https://scholar.google.com.au/citations?user=aHRLgDcAAAAJ&hl=en
4	Serge Vaudenay	42	https://scholar.google.com.au/citations?user=ub25b48AAAAJ&hl=en
5	Alex Biryukov	42	https://scholar.google.com.au/citations?user=tP5rH0wAAAAJ&hl=en
6	Ingrid Verbauwhede	63	https://scholar.google.com.au/citations?user=ZyG1ZGgAAAAJ&hl=en
7	François-Xavier Standaert	51	https://scholar.google.com.au/citations?user=JvBXO48AAAAJ&hl=en
8	Christof Paar	57	https://scholar.google.com.au/citations?user=w81afLAAAAAJ&hl=en
9	Ahmad-Reza Sadeghi	56	https://scholar.google.com.au/citations?user=p66Ie-YAAAAJ&hl=en
10	Daniel J. Bernstein	46	https://scholar.google.com.au/citations?user=ToxxF5oAAAAJ&hl=en
11	Bart Preneel	68	https://scholar.google.com.au/citations?user=omio-RsAAAAJ&hl=en
12	Moti Yung	87	https://scholar.google.com.au/citations?user=ScL8iFQAAAAJ&hl=en
13	Ari Juels	71	https://scholar.google.com.au/citations?user=uf0D-uoAAAAJ&hl=en
14	Jean-Jacques Quisquater	63	https://scholar.google.com.au/citations?user=KXkSNy4AAAAJ&hl=en
15	Nigel P. Smart	54	https://scholar.google.com.au/citations?user=Qvm3k64AAAAJ&hl=en
16	Adi Shamir	-1	http://amturing.acm.org/award_winners/shamir_2327856.cfm
17	Srinivas Devadas	78	https://scholar.google.com.au/citations?user=-yrzguMAAAAJ&hl=en
18	Arjen K. Lenstra	51	https://scholar.google.com.au/citations?user=rVqdVR4AAAAJ&hl=en
19	Ruby B. Lee	44	https://scholar.google.com.au/citations?user=odeKATgAAAAJ&hl=en
20	Vincent Rijmen	47	https://scholar.google.com.au/citations?user=zBQxZrcAAAAJ&hl=en

Keyword:
Reference Item:

1. Cryptographic Hardware and Embedded Systems (CHES)

This conference was published at 93 times by 19 of 20 experts in the last 10 years.

The experts that publish at this conference are: Nigel P. Smart(2), Jean-Jacques Quisquater(5), Ingrid Verbauwhede(21), Arjen K. Lenstra(1), Marc Joye(5), Adi Shamir(4), Christof Paar(15), Lars R. Knudsen(2), Vincent Rijmen(1), Serge Vaudenay(2), Srinivas Devadas(2), Alex Biryukov(2), Ruby B. Lee(1), Moti Yung(1), Franois-Xavier Standaert(19), Ahmad-Reza Sadeghi(7), Ari Juels(1), Bart Preneel(5), Daniel J. Bernstein(5)

In 2005, there were 9 publications by 9 experts: Nigel P. Smart, Marc Joye, Jean-Jacques Quisquater, Ingrid Verbauwhede, Franois-Xavier Standaert, Bart Preneel, Ahmad-Reza Sadeghi, Adi Shamir, Christof Paar
In 2006, there were 8 publications by 8 experts: Marc Joye, Jean-Jacques Quisquater, Ingrid Verbauwhede, Bart Preneel, Franois-Xavier Standaert, Ahmad-Reza Sadeghi, Ari Juels, Christof Paar
In 2007, there were 9 publications by 8 experts: Jean-Jacques Quisquater, Alex Biryukov, Christof Paar, Bart Preneel, Marc Joye, Franois-Xavier Standaert, Lars R. Knudsen, Ruby B. Lee
In 2008, there were 9 publications by 7 experts: Ingrid Verbauwhede, Franois-Xavier Standaert, Ahmad-Reza Sadeghi, Adi Shamir, Bart Preneel, Daniel J. Bernstein, Christof Paar
In 2009, there were 10 publications by 4 experts: Franois-Xavier Standaert, Serge Vaudenay, Christof Paar, Ingrid Verbauwhede
In 2010, there were 6 publications by 5 experts: Ahmad-Reza Sadeghi, Marc Joye, Adi Shamir, Lars R. Knudsen, Serge Vaudenay
In 2011, there were 10 publications by 6 experts: Srinivas Devadas, Ingrid Verbauwhede, Franois-Xavier Standaert, Ahmad-Reza Sadeghi, Christof Paar, Daniel J. Bernstein
In 2012, there were 10 publications by 6 experts: Vincent Rijmen, Ingrid Verbauwhede, Bart Preneel, Ahmad-Reza Sadeghi, Franois-Xavier Standaert, Daniel J. Bernstein
In 2013, there were 7 publications by 5 experts: Ingrid Verbauwhede, Franois-Xavier Standaert, Ahmad-Reza Sadeghi, Christof Paar, Daniel J. Bernstein
In 2014, there were 6 publications by 5 experts: Nigel P. Smart, Ingrid Verbauwhede, Franois-Xavier Standaert, Arjen K. Lenstra, Daniel J. Bernstein
In 2015, there were 9 publications by 4 experts: Moti Yung, Franois-Xavier Standaert, Christof Paar, Ingrid Verbauwhede

19 out of the 20 experts published at this conference in 1 or more years
12 out of the 20 experts published at this conference in 2 or more years
9 out of the 20 experts published at this conference in 3 or more years
7 out of the 20 experts published at this conference in 4 or more years
6 out of the 20 experts published at this conference in 5 or more years

4 out of the 20 experts published at this conference in 7 or more years
3 out of the 20 experts published at this conference in 8 or more years
2 out of the 20 experts published at this conference in 9 or more years
1 out of the 20 experts published at this conference in 10 or more years

Comparator Conferences

IFIP WG 11.3 Working Conference on Data and Applications Security (also known as DBSEC)
IEEE Computer Security Foundations Symposium (was CSFW)
Theory of Cryptography Conference

Other Information

Proposers

First name: Yuval
Last name: Yarom
Affiliation: The University of Adelaide
Email: yval@cs.adelaide.edi.au

Attachments

N/A

Summary Argument:

The CHES conference focuses on the security of cryptographic implementations and as such it straddles two related domains: cryptography and security. Because the conference is relevant across two domains, I chose to compare it to three A level conferences: DBSec, CSF and TCC. The former two are security conferences and the latter is a cryptography conference. Of the three, DBSec and CSF are clearly inferior to CHES, whereas TCC is only slightly inferior to CHES, with some aspects being stronger than CHES.

The two strong aspects of CHES are the acceptance rate and participants numbers. The CHES acceptance rate for the past three years is consistently below 30% with an average of 24%. In contrast, the acceptance rate of all three comparator conferences is consistently above 30%, with an average of 35%-40%.

Over the years, CHES has become a popular event. For the past eight years, attendance has been above 300 registered participants (https://ches.iacr.org/statistics.shtml), and for the last five years the number of registered participants is consistently over 350. Such levels of attendance are well above all of the other A level conferences in either security or cryptography. (See http://jianying.space/conference-ranking.html for detailed information). In particular, the comparator conferences, CSF and TCC, only attract 100-150 participants. I could not find the numbers for DBsec.

The strength of CHES publications is further demonstrated by the citation rates. It is one of the top-20 cited venues in Google Scholar metrics. Of the three comparator conference only TCC is in the list, showing similar citation rates. The h5-index for the other two conferences is well below that of CHES.

The CHES conference is a centre of an ecosystem, including annual workshops (FDTC and PROOFS), less regular workshops (WISE 2015, WhibOx 2016), tutorials, and a community journal (JCEN see http://jcen.info/guidelines.html).

CHES enjoys regular publications by outstanding researchers, including IACR and IEEE fellows (Ingrid Verbauwhede, Christof Paar and Bart Preneel). In that respect, similar patterns can be seen in DBsec and in CSF, however CHES is slightly weaker than TCC in this respect.

In summary, CHES has a lower acceptance rate and higher attendance than any of the comparator conferences. It also has similar or better citation records. Clearly, CHES is superior to CSF and to DBSec - both A level conferences, and both in CHES main area (FoR 0803). It is also similar or slightly superior to TCC. It further displays the characteristics of A level conferences. As such, I believe that CHES should be reranked as an A level conference.

Additional Notes

The "where people publish" tool fails to recognise some names even when they match DBLP. These include Paul C. van Oorschot, Marten Van Dijk, Michael Backes and Sabrina De Capitani Di Vimercati.

For both the General Report and the Specialised Report I aimed to list authors who both match the criteria and publish in the relevant conference. In particular, I manually scanned all of the authors who published three or more times in each of the conferences. In the General Report I included all those that have an h-index above 45 (i.e. 46 and higher) and have the exact relevant keyword in the profile (i.e. for the keyword "cryptography" I used the search term "label:cryptography", excluding authors with the keyword "applied cryptography"). For the Specialised report I included authors with h-index above 40 (i.e. 41 and higher).

Prof Adi Shamir is included although he does not have a Google Scholar profile and, consequently, I do not know what his h-index is. Being a Turing award winner I assume noone would doubt that he is an outstanding computer scientist. I further verified that he has more than 40 publications that have at least 41 citations each. Hence, had he maintained a Google Scholar profile, his h-index would clearly be more than 40.