The First Official Crypto-World Rankings

Keef M. Martin and Vincent Rijndael
Cosic World,
Kardinaal Mercierlaan 94
B-3001 Heverlee, Belgium
{*keith.martin,vincent.rijmen*}*@esat.kuleuven.ac.be*

Abstract

We announce the first official Crypto-World Rankings in an unbiased attempt to geographically identify the real nations of excellence in the field.

1 Motivation

In a world of increasing international co-operation, expanding communication networks and blurring of national identities, we wish to whip off the "international research community" veil and determine which country is the *best* at cryptology. Which is the most cryptological nation on the planet? Is the United States the super-power? A controversial nationalistic investigation of the current state of the art. An international cryptological version of the Eurovision Song Contest if you like. Will Norway have *nil points*? In which country in the world do you have the best chance of dining in a restaurant where the waiter can find an attack on your authentication protocol? In which country in the world are you most likely to have your block cipher broken by the person in front of you in the supermarket checkout queue? In which country in the world are you most likely to go to a concert and have weaknesses in your hash function pointed out by the saxophonist?

We assessed these issues by investigating six measures deemed by the authors as appropriate indicators of cryptological strength. Each measure is considered in turn, with (where appropriate) the top ten nations being attributed a score. These scores are accumulated and, following the immense popularity and success of the FIFA/Coca-Cola-World Ranking system for soccer [4], the final results are presented in the form of the first official Crypto-World Rankings. We hope that nations will be able to use their Crypto-World Ranking in order to enhance grant applications, buy favours from program committees and settle bar disputes, etc. It is our understanding that statistical results should be accompanied by confidence bounds. Thus we state unequivocally that we are *very confident* in the correctness of the results.

2 Conference paper acceptance

A good national measure of cryptological strength is the ability to have papers accepted at major conferences that have advance refereeing procedures. We investigated the national success rates at recent Eurocrypt and Fast Software Encryption conferences. The results of the two investigations for the 1996 - 1997 period [2, 3, 5, 6] are shown in Table 1. The numbers shown represent the "top ten" in terms of million head of population per occurrence of an author with affiliation from that country.

Country	Rate	Score
Luxembourg	0.420	10
BELGIUM	0.483	9
Switzerland	0.600	8
Denmark	0.883	7
Finland	1.028	6
Israel	1.100	5
Sweden	2.215	4
Netherlands	2.236	3
Australia	2.628	2
France	2.814	1

Table 1: Million head of population per authorship 1996-1997

Following analysis of the results in Table 1, we were tempted to make the practical and entirely reasonable adjustment to the sample space that countries under consideration should be at least the size of Rhode Island. However, after much deliberation, we decided to let the results stand uncorrected.

3 AES submissions

The Advanced Encryption Standard call clearly represents a state of the art cryptological activity [1]. Most of the submitted block cipher algorithms came from single nations, however where more than one nationality was represented on a submission we awarded appropriate fractions of a submission to the countries involved. It seemed to us reasonable that countries experiencing a wet season of at least six months should be excluded, however as this possibly had rather self-destructive implications, we decided to present the results in full in Table 2.

4 High office

There can be fewer honours in a life of cryptological research greater than to be elected by your peers to a position of high office in the IACR. [9]. We thus considered the

Country	Submissions	Rate	Score
Costa Rica	1	3.534	10
Norway	5/6	5.301	9
BELGIUM	1	10.160	8
Israel	1/3	16.500	7
Australia	1	18.400	6
Canada	3/2	20.227	5
Korea	1	45.950	4
U.S.A.	5	53.600	3
France	1	58.600	2
Germany	1	82.100	1

Table 2: Million head of population per AES submission

affiliation of the elected office bearers of the IACR. in 1998 and these results appear in Table 3. We felt that a suitable statistical modification in this case involved exclusion of countries whose flags only feature the rather unimaginative colours red and white, however this led to a complete collapse of Table 3. All results are thus included.

Country	Office bearers	Rate	Score
Denmark	1	5.300	8
Switzerland	1	7.200	7
Canada	3	10.133	6
BELGIUM	1	10.160	5
U.K.	1	57.600	4
U.S.A.	4	67.000	3
Germany	1	82.100	2
Japan	1	125.700	1

Table 3: Million head of population per elected IACR office bearer 1998

5 Program committees

A sign of respect for national cryptological excellence is selection to sit on a program committee. Thus we reviewed these esteemed gatherings for the Crypto, Eurocrypt and Asiacrypt conferences (1996 to 1998). The statistical adjustment felt necessary in this case was that nations with land more than 700 metres above sea level should not qualify. However, we present the unmodified results in Table 4.

Country	Committee members	Rate	Score
Switzerland	13	0.554	10
Denmark	5	1.060	9
Finland	4	1.285	8
BELGIUM	7	1.451	7
Norway	2	2.200	6
Australia	7	2.629	5
Singapore	1	3.400	4
Canada	7	4.384	3
Sweden	2	4.430	2
Israel	1	5.500	1

Table 4: Million head of population per program committee member (1996-1998)

6 Conference hosting

One way of ensuring that there are lots of cryptologists in your neighbourhood is of course to invite them all to come and visit you. This is the cryptological "party scene" and therefore it must be assumed that if cryptologists are willing to visit somewhere in large numbers then there must be at least some cryptology going on there [7, 8]. So in Table 5 we counted national hostings of Crypto, Eurocrypt or Asiacrypt conferences, from the beginnings of time (1981!) until the year 2000. A statistical fine tuning process to exclude nations willing to tolerate raw fish in their diet was considered, but to maintain impartiality, as always, we present the full results.

Country	Conferences	Rate	Score
Singapore	1	3.440	10
Norway	1	4.400	9
BELGIUM	2	5.080	8
Finland	1	5.140	7
Denmark	1	5.300	6
Switzerland	1	7.200	5
Austria	1	8.130	4
Sweden	1	8.860	3
Hungary	1	10.230	2
Czech Republic	1	10.300	1

Table 5: Million head of population per conference hosting (1981-2000)

7 Newsgroup activity

For our final measure we decided to evaluate an activity that hampers cryptological activity. In this special round, nations are “awarded” negative points! As an excellent example of such a negative measure we counted the national origin of recent postings to the newsgroup sci.crypt. To evaluate the results we simply attributed a value to each nation based on the number of recent postings after application of a weight representing the population of that country (a small ratio represents a large number of postings per head of population). The results are shown in Table 6. No statistical correction, modification, cosmetic alterations, or technical adjustments to the raw data were considered necessary.

Country	Weighted ration	Score
Estonia	0.718	-10
Netherlands	1.118	-9
Sweden	1.476	-8
U.S.A.	1.854	-7
Canada	1.861	-6
Norway	2.211	-5
U.K.	4.387	-4
Germany	5.613	-3
France	7.229	-2
Korea	8.185	-1

Table 6: Population weighted ratio of sci.crypt postings

8 Final scores, rankings and conclusions

And now of course, the moment you have all been waiting for! We present the final results and announce the first Crypto-World Rankings. These are calculated by summing the points awarded in each of the six exciting and closely contested rounds. In all, twenty-three nations qualify for a Crypto-World Ranking, and we give permission for these countries to use this rank as an official evaluation of their cryptological strength. To separate countries that were tied in the ranking table, we decided that a most fair and reasonable way of ordering them would be via their FIFA/Coca-Cola-World rank. Hence of relevance are the FIFA rankings (as of November 1998) for Denmark (18), Switzerland (82), Australia (33), Israel (38), Costa Rica (66), Luxembourg (147), Czech Republic (6), France (2), Japan (30), Sweden (17), Germany (3) and the U.K. (average ranking 56.75). It is our great pleasure and humbling honour to formally declare that the first official Crypto-World Rankings are now available for general public domain use and are presented to the research community in Table 7.

Ranking	Country	Score	Ranking	Country	Score
1	BELGIUM	37	13	Korea	3
2	Denmark	30	14	Hungary	2
3	Switzerland	30	15	France	1
4	Finland	21	16	Czech Republic	1
5	Norway	19	17	Sweden	1
6	Singapore	14	18	Japan	1
7	Australia	13	19	Germany	0
8	Israel	13	20	U.K.	0
9	Costa Rica	10	21	U.S.A.	-1
10	Luxembourg	10	22	Netherlands	-6
11	Canada	8	23	Estonia	-10
12	Austria	4			

Table 7: The first official Crypto-World Rankings

Hence from Table 7 it is clear that the country where it is most likely that the person next to you on the bus will be able to generate a blind signature is ... BELGIUM! To put this result to the test we decided to visit the local cafe to find out how many of the clients had heard of Bart Preneel or Jean-Jacques Quisquater, and amazingly there were at least twelve positive responses. Further at least three people had attempted to eat Hasty Pudding during the previous month, and at least one had considered implementing it. This presents extremely strong supporting evidence for the validity of Belgium's number one ranking.

We would like to thank the referees for their kindly words and suggestions for alternative measures of cryptological strength. Per capita spy satellites proved too difficult to count due to Belgium's tendency for overcast nights, per capita companies featuring the buzz syllables *Cert* and *Trust* was deemed linguistically biased, per capita attendance at IACR conferences was too tedious to enumerate, and per capita number of key bits exportable was regarded as currently too volatile.

As to *why* Belgium is the most cryptological country in the world, we can only offer the possible explanation that it is due to the very cryptic nature of the Belgians themselves. Belgians are very secretive people who are very keen to prevent the rest of the world from discovering important facts about Belgium such as which language to speak, which beer to drink, and why anyone would voluntarily eat chicory. It is only through strong cryptography that these secrets can be guaranteed to survive the information age (although the third is probably safe for all time).

References

[1] NIST's AES homepage, `http://www.nist.gov/aes`

[2] *Advances in Cryptology, Proceedings Eurocrypt'96, LNCS 1070*, U. Maurer, Ed., Springer-Verlag, 1996.

[3] *Advances in Cryptology, Proceedings Eurocrypt'97, LNCS 1233*, W. Fumy, Ed., Springer-Verlag, 1997.

[4] `http://www.fifa2.com/`

[5] *Fast Software Encryption, LNCS 1039*, D. Gollmann, Ed., Springer-Verlag, 1996.

[6] *Fast Software Encryption, LNCS 1267*, E. Biham, Ed., Springer-Verlag, 1997.

[7] *Financial Cryptography'97, LNCS 1318,* R. Hirschfeld, Ed., Springer-Verlag, 1997.

[8] *Financial Cryptography'98, LNCS 1465,* R. Hirschfeld, Ed., Springer-Verlag, 1998.

[9] `http://www.iacr.org`