Cryptanalysis of MDS-POTI

Yvo Desmedt

Jean-Jacques Quisquater

Moti Yung

Abstract

- MDS-POTI is a new system suggested for global wide use which will strongly affect the practice of cryptography world wide.
- We performed an initial cryptanalysis of the system, employing novel techniques, and found some subtle and critical flaws in its specification & its initial suggested implementation.
- So… what is this system?

MDS-POTI

- It Stands for:

  A More Detailed Strawman for

  Proceedings of the IACR

(and it was suggested by leading members of our community)

New System Acceptance

- Solve the Open Access (first goal)
- (next four more goals): Move to IACR proceedings which is essentially a journal, you can submit when you want, same group of people will review for a while (an editorial board)… All IACR conferences + workshop will fold into a single “proceedings of”….

- We are told: abolish conferences as we know them.. BUT CONFERENCES ARE THE MOST SUCCESSFUL ACHIEVEMENT OF IACR!!! (due to hard work of the boards and many volunteers)

Basic Analysis

- The current system sucks but not broke !!!
- The new system has its inherent flaws, too.
- No conference reviewing by different committees: unfair power to a few reviewers (for a number of years), hard to get in (imagine non-English spoken students writing their first paper: it has to be initially rejected but then accepted with NO STIGMA!).
- Reviewing problem is global in all computer science… Need to incentivize reviewers besides traditional incentives…. (a different problem)..
- Suggested system will make reviewers worse (no deadline): NSF moved to panels since people without definite deadline are too relaxed!!!!
- JoC will be in danger in spite of the intention!

Examples

- The Zero Knowledge paper (GMR) was rejected a few times before accepted (some notions are hard to get right, should not generate stigma and vested interest in ego of reviewers who have rejected the work before).
- The Prof. Wang MD4 5 cryptanalysis was rejected initially: non native speakers cannot always get it right the first time they write… sorry, rejection, improvement, resubmission is a NATURAL cycle (especially for new innovation: reviewers are just as bad as authors – we are all drawn from the same community…)
- IMPACT of NDS-POTI: harder for new ideas (no sequential improved submissions), harder for people with no budget to give talks in other places, people with less funds, newcomers (students in non-English speaking countries), thus: less competition for the establishment. Easier for reviewers (BUT: easier also for stickiness of wrong review/ "same taste reviewers" and easier for stigmatizing a paper.
- Independent committees may be abused by crazy authors. But our conferences and workshop are leading! Why change a leading strategy!? Never worked in history and the risk is not justified!

Potential Negative Impact

- Less innovative papers, more of "natural next step" papers which committees like!
- Innovation will move elsewhere!
- Crypto has 3+4 forums a year but there are other conferences: ACM's CCS, IEEE S&P, STOC, FOCS, PODC, ICALP, ESORICS,…: they accept top papers, they will continue! People will rotate into IACR outside IACR etc. (cannot and should not limit this choice; The IACR should not and cannot become a tyranny limiting idea dissemination!)
- Suggested management structure: quite messy! [honor system]
- Around the model of "crypto conference" a worldwide eco-systems of "look alikes" have emerged, run by members of our community: Indocrypt, Latincrypt, Inscrypt, ISC, Africacrypt, CT-RSA, ICICS, etc. etc. Now we will be killing the basic prototypical successful creation!

- Many revolutions started "in order to serve the common man" but failed to deliver!!! This is not an evolution, this suggestion is a revolution (given the above analysis)! Beware and be Careful !!!!!!!!!

We assert that

- The system of reviewing should be based on fast rotation of reviewers (thus, conferences)
- Deadline rush, competition, and all the other flaws associated with a conference are good for innovation and for newcomers.
- Reviewers suffering through repeated reviews: fact of life (authors suffer through it as well): everyone should learn how to be a good reviewer and serve! People should be open minded to reverse prior opinion as papers evolve for the best; authors who do not respond to reviews are automatically suffering anyway!
- Increased submission: just another success indication for the current conference system!!!!!!!!!! Conference lengths are increasing to accommodate!

Do not touch the publication system

- We have three inherently different publication forums:
  - Eprint: self-publication (open to all by all)
  - Conferences (where the competition, dissemination, and novelty occurs)
  - Journal: archive level, serves people who need academic promotion (journal is often an extended paper with some perspective added to the initial innovation– different from the dissemination role of conferences!)

BTW: in most computer science (outside DB area) this is the model!

We assert the tripodal model works!!

What the bylaws say

- Bylaws: The purposes of the IACR are to advance the theory and practice of cryptology and related fields, and to promote the interests of its members with respect thereto, and to serve the public welfare.
- Advancing theory and practice: Conferences are crucial!
- Promotion of interest: conferences are focal point!

- Andy Clark (former IACR president) uttered (paraphrased): IACR should concentrate, as a priority, on fixing systems that are not working rather than amending existing systems that are working!

If you want to solve open access

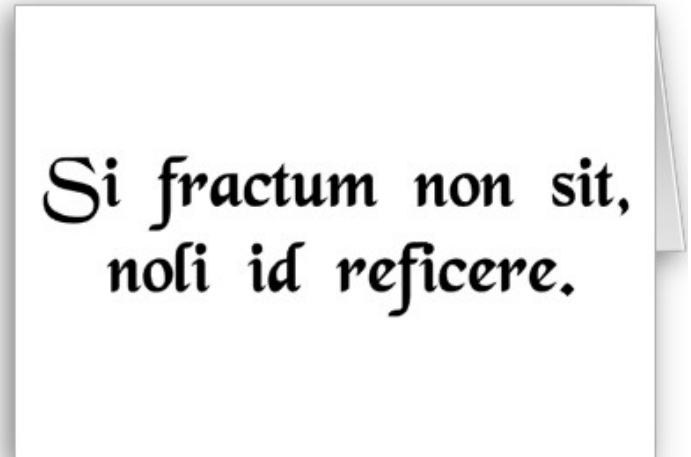
- Do not use the conferences and the current working publication model for doing so! (Open source with its predators and many other issues, and the publishing industry state of business is a problem in itself!)
- Solve the problems you want to solve, one at a time in isolation!!
- Namely, an old Chinese strategy offered:

Do Not deceive the heavens to cross the ocean
(**瞞天過海**／瞒天过海, Mán tiān guò hǎi)

Conclusions: Other old cultures……

- *Primum non nocerum*! (first, do no harm!)
- *Leave well enough alone!*
- *Le mieux est l'ennemi du bien.* (the best is the enemy of the good): [Voltaire]
- *If it ain't broke, don't fix it!*

- Thank You!



It's the IACR as we know it

It's the IACR as we know it

It's the IACR as we know it

And I feel fine

From the rump session of last year at CRYPTO