

Eurocrypt 2020 Chair<eurocrypt2020programchairs@iacr.org>

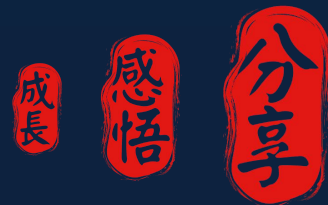
To: Fuchun Guo

Cc: eurocrypt2020programchairs@iacr.org

REJECTED

Dear Fuchun Guo;

We are sorry to inform you that your submission



如何提升你那 1% 的 IACR 中稿率

Research and Writing:

Why



Killed My Submission

Fuchun Guo

郭福春

fuchun@uow.edu.au



DSPP 2025



UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Outline

- Perspective
- Research
- Writing
- Conclusion



something I learnt, something I found



1. Perspective: IACR Papers are Important



IACR Papers

If **(Many)**
then



1. Perspective: IACR Papers are Challenging

- People in every research field are **people-mountain-people-sea.**



The image shows a screenshot of a Zhihu (Chinese Quora) post. The post title is "为什么你会觉得密码学很难了?" (Why do you find cryptography so difficult?). The text below the title reads: "现在一听到是学密码的，就开始仰望大佬的姿态了？密码学到底为什么难？是刻板印象么，就像大家" (Now, as soon as you hear someone is studying cryptography, you start to look up to the big guys? Why is cryptography so difficult? Is it a stereotype, like everyone...). To the right of the text is a photograph of a crowded beach, identified as Bondi Beach, Sydney, Australia.

- Growing topics:** new security, new foundations, and new primitives.
- Finding simple and interesting topics has become more difficult. Most topics must consider **multiple factors.**
- Short papers are harder to produce now, with research often requiring multiple contributions and resulting in **longer papers** (60 pages).



1.Perspective: Traps in the Path to IACR



Accepted








REJECTED

Understand why IACR says “no” through **research contribution** and **academic writing** will help boost the success chance (at least 1% 😊)



1.Perspective: Fuchun's Experience

- 20 years in cryptologic research (started in Sep.2005 at 福建师大). 
- Have had **many rejected** submissions (first submission in 2008). 
- Served on some IACR PC and have analyzed many samples. 
- Deep thinking on what cryptologic research is when booking. 
- Spent two months summarizing writing tricks together with AI. 



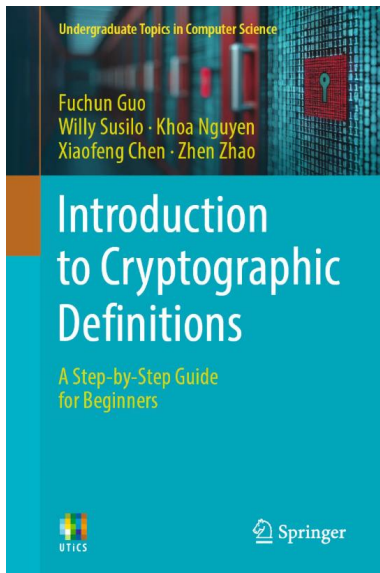
2. Research

Whether a research contribution is good enough for IACR



2. Research: Above and Beyond (1/3)

Cryptography is studied by humans, for humans only.



C.
I.
A.

不好意思

郭老师他又夹带私活了。

。。。



2. Research: Above and Beyond (2/3)

- When conducting cryptologic research, we might be able to change the world, **but** for most of time we only advance human knowledge (超越人类的认知极限) even when publishing IACR papers.
- Advance human knowledge = Above and Beyond
- Above and Beyond = Benefits (**Impact**) and Novelty (**Intelligent**)
- Benefits = **F**unctionality + **S**ecurity + **E**fficiency (FSE 😊)

下一页很重要



2. Research: Above and Beyond (3/3)



	Benefits (Impact)	Novelty (Intelligent)
Level 1	Wow, this is good! (卧槽卧槽, 大大的不错)	Solid (硬核式, 真的很不一样)
Level 2	Well, just so so! (确实不错, 但就那样了)	Incremental (增量式, 这里有些东西)
Level 3	It could be good! (这个应该好像可能不错)	New (新意式, 有不同的地方)



IEEE Trans

卧村密码学报



2. Research: Level 3 (1/3)

ElGamal Encryption

Enc(pk, m):

1. Choose a random r
2. Compute $C_1 = g^r$
3. Compute $C_2 = h^r * m$
4. Return $CT = (C_1, C_2)$



Guo Encryption

Enc(pk, m):

1. Choose a random r
2. Compute $C_1 = h^r * m$
3. Compute $C_2 = g^r$
4. Return $CT = (C_1, C_2)$



2.Research: Level 3 (2/3)



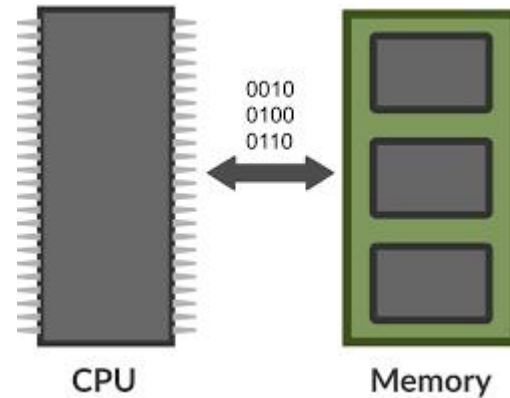
Guo Encryption

Enc(pk, m):

1. Choose a random r
2. Compute $C_1 = h^r * m$
3. Compute $C_2 = g^r$
4. Return $CT = (C_1, C_2)$

Contribution: We propose a new PKE.

- **Novelty:** New because it is different
- **Benefits:** ???



2.Research: Level 3 (3/3)

These research **belong to Level 3** due to less convincing benefits:

- 1.Our proposed algorithms are **simpler**.
- 2.We solve a **new** research problem that hasn't been solved.
- 3.Our scheme allow users to have the controlling **capabilities**.
- 4.Our scheme can be secure against X attacks by **Fuchun Guo**.
- 5.We use a new building block to construct this primitive.
- 6.The KeyGen algorithm in our scheme has better security.
- 7.We successfully propose a secure scheme for this new primitive!





2. Research: Level 1 vs Level 2 (1/10)



	Benefits (Impact)	Novelty (Intelligent)
Level 1	Wow, this is good! (卧槽卧槽, 大大的不错)	Solid (硬核式, 真的很不一样)
Level 2	Well, just so so! (确实不错, 但就那样了)	Incremental (增量式, 这里有些东西)


HARD

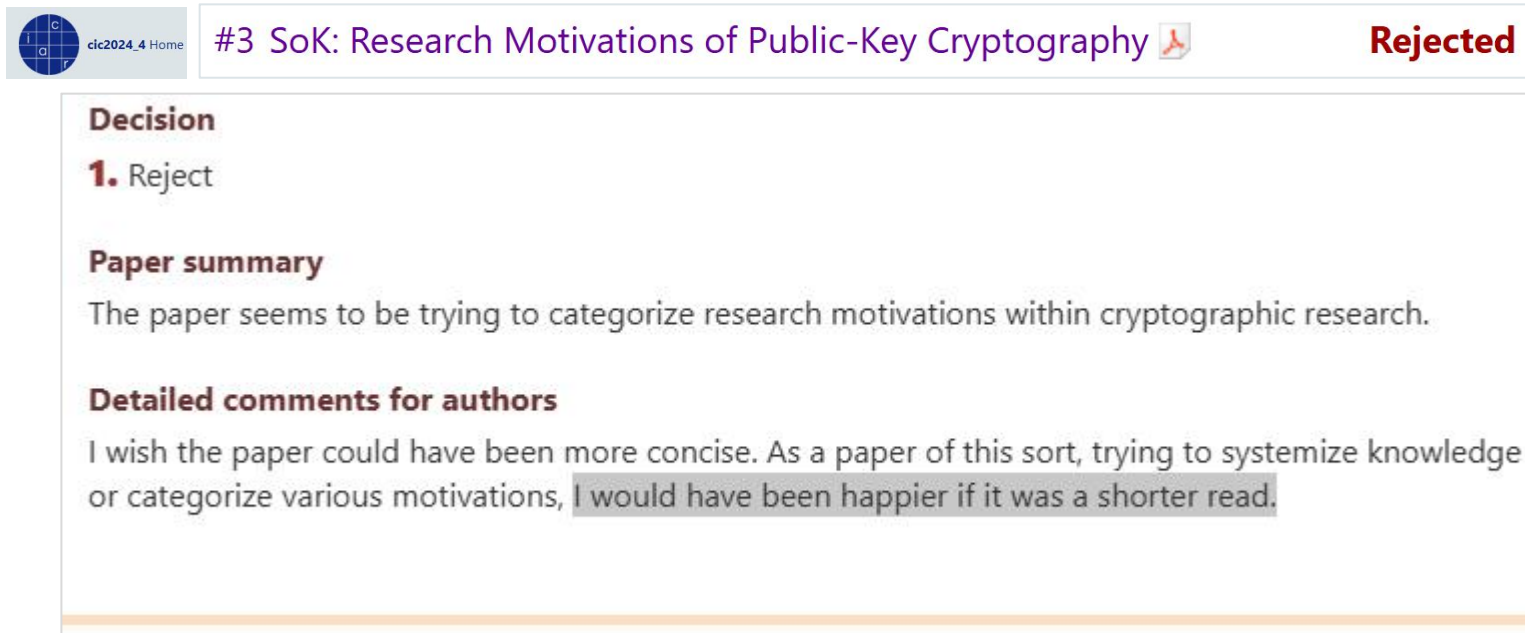
 **Authors:** If they (PC) read our papers carefully and think hard, they will see that our research belongs to Level 1.


 **Authors:** We “prove” that our research belongs to Level 1.




2. Research: Level 1 vs Level 2 (2/10)

 **Authors:** If they (PC) read our papers carefully and think hard, they will see that our research belongs to Level 1.



 clic2024.4 Home

#3 SoK: Research Motivations of Public-Key Cryptography 

Rejected

Decision

1. Reject

Paper summary

The paper seems to be trying to categorize research motivations within cryptographic research.

Detailed comments for authors

I wish the paper could have been more concise. As a paper of this sort, trying to systemize knowledge or categorize various motivations, I would have been happier if it was a shorter read.



2. Research: Level 1 vs Level 2 (3/10)



Authors: We “prove” that our research belongs to Level 1.

A submission belongs to **incremental** if

- **Some Optimization** (缝缝补补), or
- **Tradeoff** (拆东补西), or
- **Limited Applications** (杯水车薪), or
- **Dependent** (狐假虎威), or
- **Not Surprising** (循规蹈矩) .

REJECTED

顶会之路很艰（扯）难（淡）……



2. Research: Level 1 vs Level 2 (4/10)

REJECTED

Some Optimization (缝缝补补)

Example:

We proposed a more efficient/secure scheme based on [12].

Truth:

We achieve this via double encryption based on [12].



2. Research: Level 1 vs Level 2 (5/10)

REJECTED

Tradeoff (拆东补西)

Example:

We first time achieve $O(1)$ size ciphertext for X primitive.

Truth:

We achieve this in a very weak security model.



2. Research: Level 1 vs Level 2 (6/10)

REJECTED

Limited Applications (杯水车薪)

Example:

We proposed a new primitive that is very useful for X application.

Truth:

The construction requires the application with perfect setting (e.g. all users must be online at the same time).



2. Research: Level 1 vs Level 2 (7/10)

REJECTED

Dependent (狐假虎威)

Example:

We solve the X open problems proposed in Crypto 1995.

Truth:

We actually solve it by using [12] after a simple modification.



2. Research: Level 1 vs Level 2 (8/10)

REJECTED

Not Surprising (循规蹈矩)

Example:

We first time propose an efficient scheme for X in standard model.

Truth:

We add some well-known tricks to the scheme in [12] using RO for X to obtain our scheme in standard model.



2. Research: Level 1 vs Level 2 (9/10)

✔ **Authors:** We “prove” that our research belongs to Level 1.

A submission belongs to **“Well, just so so”** if

- the benefit in this submission is not what other researchers are concerned about.



2. Research: Level 1 vs Level 2 (10/10) **REJECTED**

Small Impact (有些鸡肋)

Example:

We propose the first $O(1)$ -size digital signature scheme with tight security under DL assumption in standard security model.

Challenge from PC:

So what? I don't think this problem is important!



2. Research: Summary (1/2)

SoK: Research Motivations of Public-Key Cryptography

- **Efficiency**: Storage/Computational/Communication Efficiency
- **Security**: Better (Foundations, Security Model, Security Proof)
- **Functionality**: Decentralized, Boundable, Traceable, Revocable, Hierarchical, Provable, Robust, Verifiable, Fuzzy, Partially, Fully, Proxy, Aided, Convertible, Dynamic, Multiple, Batch,



The number of research problems is increasing, but they **all look similar** following a pattern.



2. Research: Summary (2/2)

Fuchun's Personal View

Compared to 20 years ago, it is **harder** to prove “Level-1” because:

- Most tricks (novelty) look similar from here to there.
(创新技巧看起来闻起来换汤不换药，哪儿哪儿都像旧药材。)
- Increased number of research problems and most problems are losing their importance.
(研究问题数量激增，重要性被稀释，大多数问题变得不重要)



3. Writing

Whether a manuscript is ready for IACR submission.



3. Writing: A Fake Email (1/3)



Dear  International Association
for Cryptologic Research

Based on the number of papers submitted to eprint, it is evident that the population of cryptologic researchers is growing, with many striving to have their submissions accepted by the IACR.

I propose that the IACR should increase its acceptance rate to accommodate the rising number of researchers. Having their papers accepted would boost their confidence, encouraging them to make further contributions to the cryptology community.

Thanks & Regards,
Fuchun

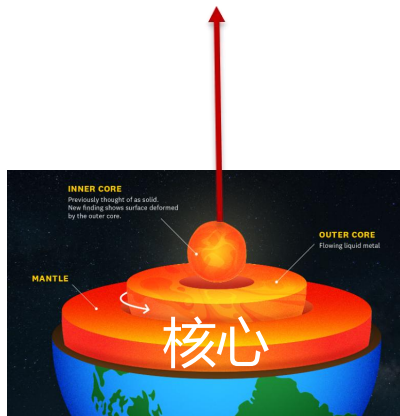


3. Writing: A Fake Email (2/3)



1. increase acceptance rate

2. cryptologic researchers are growing



3. further contributions from them to this community



3. Writing: A Fake Email (3/3)



3. Writing: Structure (1/4)

In academic writing, all text can be categorized into two main purposes:

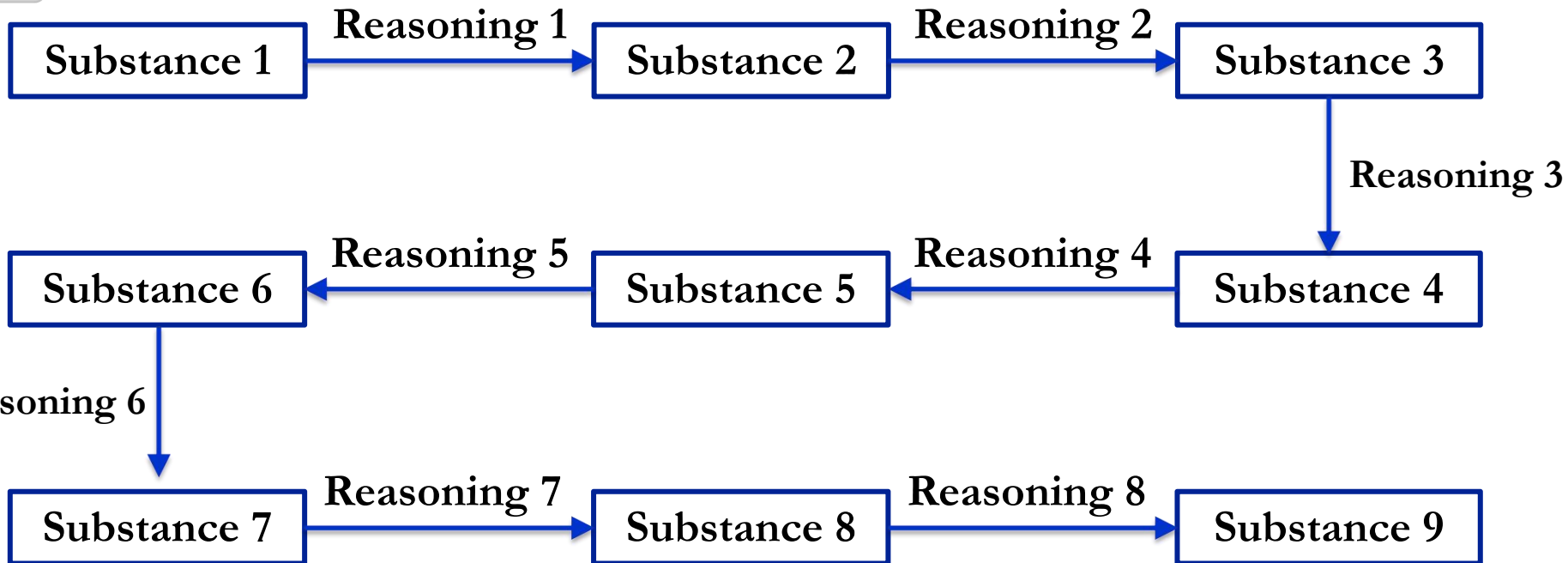
- **Substance:** This includes the **core content(核心内容)** of the paper, such as background (A), proposals (B), and contributions (C). It represents the what of the research, what the paper is about, what it argues, and what it concludes.
- **Reasoning:** This refers to the **logical connections (逻辑推理)** between A, B, and C. It explains how the paper moves from background to proposal and from proposal to contributions, using deduction, induction, analogy, or validation.

A well-structured paper ensures that substance is clearly presented and reasoning is well-articulated, making the argument both persuasive (说服力) and coherent(连贯性).



3. Writing: Structure (2/4)

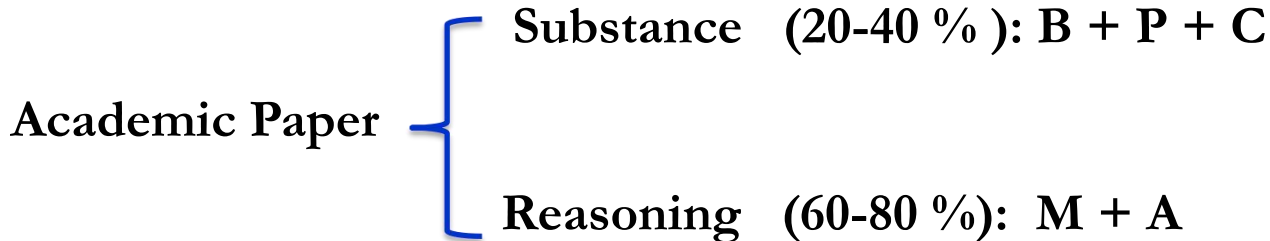
START



STOP



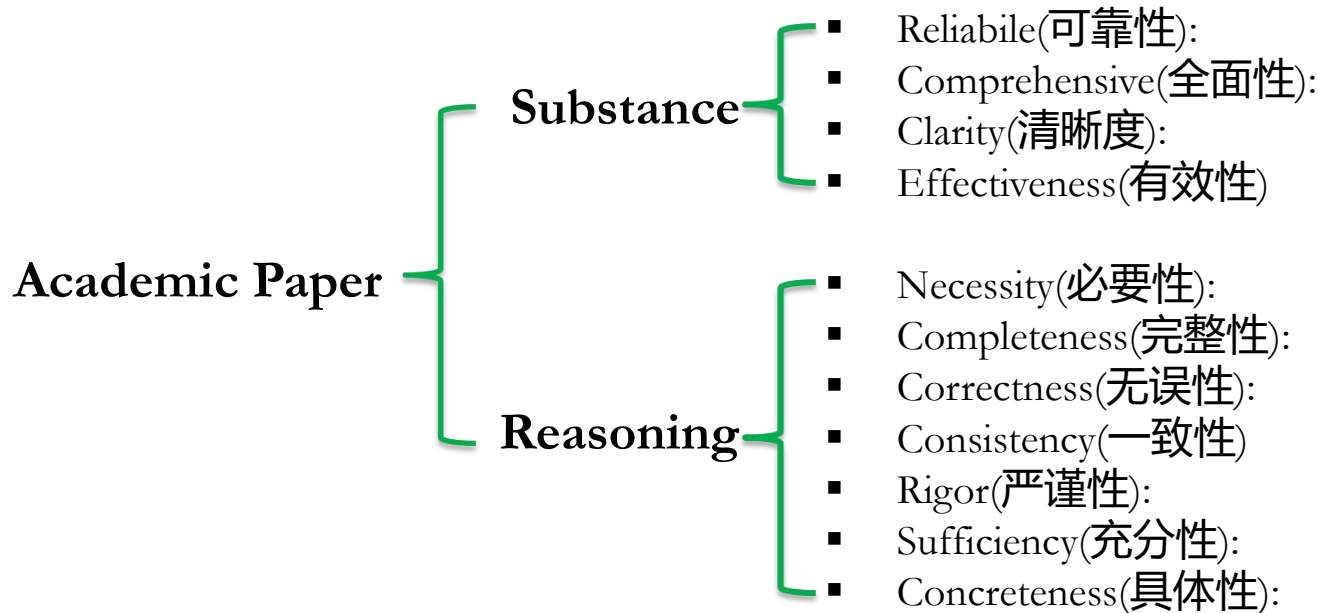
3. Writing: Structure (3/4)



下一页很重要……



3. Writing: Structure (4/4)



3. Writing: One-by-One (1/8)

Substance(Background)

- **Reliable(可靠性):**

1. The paper has a severe misunderstanding about XXX in every section.

- **Comprehensive(全面性):**

1. The recent work of [XXX] on YYY should have certainly been mentioned, since they also obtain ZZZZ like this paper.
2. The authors fail to consider the most recent works on the topic, namely the articles of Asiacrypt 2020 and 2022 from XXX et al. [X] and [Y] respectively.



3. Writing: One-by-One (2/8)

Substance(Proposal)

- Clarity(清晰度):
 1. A high-level description is missing and it would improve this paper considerably.

- Effectiveness(有效性)
 1. The construction seems over-complicated.
 2. The correctness error is so high that the protocol is really inefficient, when repeating it to boost correctness.



3. Writing: One-by-One (3/8)

Reasoning(Motivation)

- Necessity(研究意义的必要性):
 1. The motivation of the paper is unclear, and the reasoning behind the research goal is not well explained.
 2. The problem trying to solve is not scientifically challenging.
 3. Improving the concrete efficiency of MPC protocols is an important research question.



3. Writing: One-by-One (4/8)

Reasoning(Proposal and Analysis)

- **Completeness(表述完整性):**
 1. The X algorithm is not defined in Definition 2.
 2. The proof of Lemma 2 is incomplete. Why is XXX a valid forgery against the scheme?
 3. What is a “strong adversary”? How is it different from a “weak adversary”? The authors didn’t explain it in the paper.



3. Writing: One-by-One (5/8)

Reasoning(Proposal and Analysis)

▪ Correctness(表述无误性):

1. I don't think the protocol achieves the X properties claimed because.....
2. Equation (8) in the proof of Theorem seems wrong because...

▪ Consistency(表述一致性)

1. In the security model, Adv is said to make all queries in advance, but later Adv is said to adaptively query the signing oracle.
2. The input of algorithm X in definition and scheme are not consistent.



3. Writing: One-by-One (6/8)

Reasoning(Proposal and Analysis)

- Rigor(表述严谨性):
 1. It is easy to see that
 2. The scheme and security definitions should be formalized...
 3. The security definitions are not stated formally (even though this is supposed to be a contribution).
 4. The paper lacks rigorous security definitions and proofs. There are significant concerns about the scheme's security against X attacks.



3. Writing: One-by-One (7/8)

Reasoning(Proposal and Analysis)

- Sufficiency(表述充分性):

1. The formal security proof is lacking sufficient details.
2. I would also have liked a more thorough and systematic description of how the parameters are chosen and a more precise description of the attacks that are taken into account.
3. The technical part seems correct but is really missing some explanations.



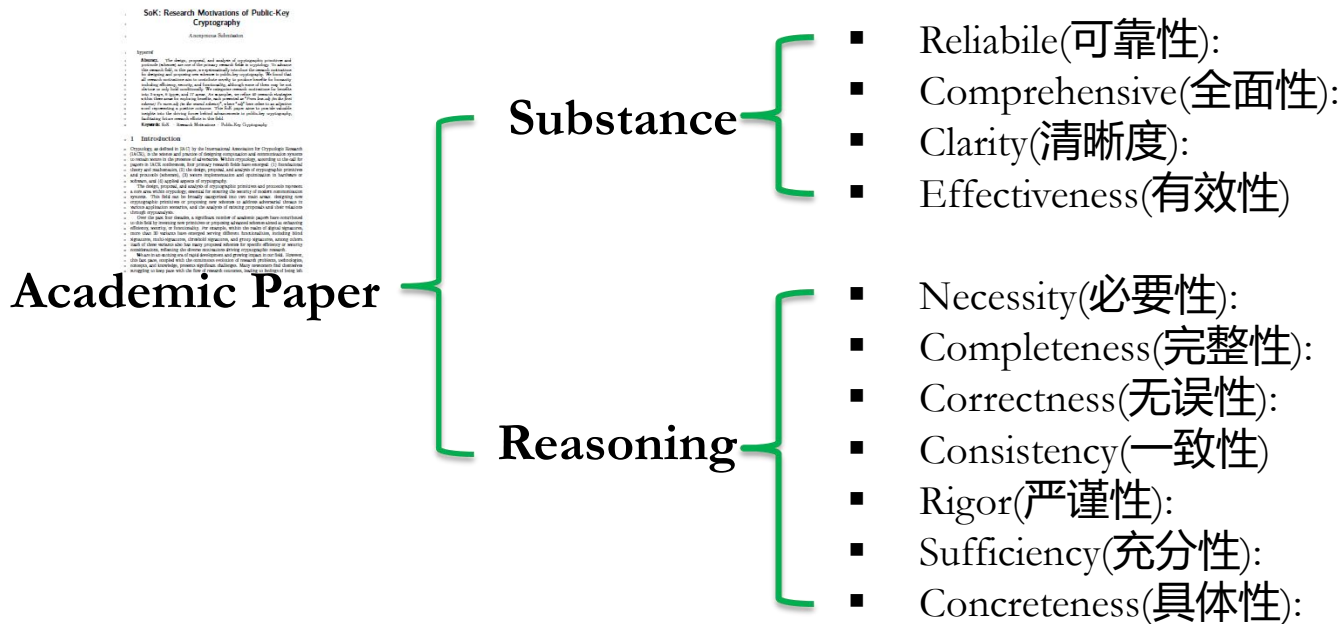
3. Writing: One-by-One (8/8)

Reasoning(Proposal and Analysis)

- **Concreteness(表述具体性):**
 1. In Section 5 I would have liked to get a slightly more intuitive description of what a conditional XXX is.
 2. It needs more intuition how the result (theorem 3.1) improves over the analysis of the sampler in XXX.



3. Writing: Summary



It is not easy to complete a well-written paper. Rejection makes perfect!

听说过很多道理，仍然写不好论文。多被拒几次(复盘几次)就好了！





4. Conclusion



Driving Test in AU



Driver Knowledge Test



Learner licence
Max 90km/h



Driving Test



Provisional (P1) licence
Max 90km/h



Hazard Perception Test



Provisional (P2) licence
Max 100km/h




Driver Qualification Test



Full licence
Maximum 110km/h



**To pass the driving test we must
(1) score at least 90%, and
(2) have no fail items.**

Class C Car Driving Test 

Test started Applicant's signature

24 hour time

Test vehicle plate no. Name of driving instructor

State Name of driving school

DI Licence number Driving school number

Instructor's vehicle Other vehicle Automatic Manual

Termination

1 2 3 4 5 6 7 8 9 10

Test not conducted/terminated/immediate fail because: Manager verifying reason

Assessments							
S	P	D	Z	H	R	C	NOTES
S	P	D	1	H	R	C	
S	P	D	2	H	R	C	
S	P	D	3	H	R	C	
S	P	D	4	H	R	C	
S	P	D	5	H	R	C	
S	P	D	6	H	R	C	
S	P	D	7	H	R	C	
S	P	D	8	H	R	C	
S	P	D	9	H	R	C	
S	P	D	10	H	R	C	
S	P	D	11	H	R	C	
S	P	D	12	H	R	C	
S	P	D	13	H	R	C	
S	P	D	14	H	R	C	
S	P	D	15	H	R	C	
S	P	D	16	H	R	C	
S	P	D	17	H	R	C	
S	P	D	18	H	R	C	
S	P	D	19	H	R	C	
S	P	D	20	H	R	C	
S	P	D	21	H	R	C	
S	P	D	22	H	R	C	
S	P	D	23	H	R	C	
S	P	D	24	H	R	C	
S	P	D	25	H	R	C	
			YES				
			NO				
25	25	25				25	
							Totals

F IF Fail and immediate Fail items

1. Driving for the wrong way or road markings.

2. Failing to give way when necessary.

3. Colliding with a vehicle, pedestrian or object.

4. Performing an illegal act or manoeuvre.

5. Exceeding the speed limit.

6. Action requiring testing officer intervention.

7. Causing a dangerous situation.

8. Failing to maintain proper control of the vehicle.

9. Failing to exercise due care to avoid an accident.

10. Failing to give way to an emergency vehicle.

11. Disobeying directions from a person controlling traffic.

12. Frequently not signalling intention. TOTAL

13. Refusing to attempt any part of the test.

14. Repeated or deliberate failure to follow directions.

15. Unreasonably obstructing other vehicles or pedestrians.

16. Receiving external advice or instruction during the test.

17. Not parking to the required standard.

18. Failing to maintain a safe following distance.

19. Frequently not making required observation checks. TOTAL

My result has been explained to me

Applicant's signature Date

day / month / year

OFFICE USE ONLY Test finished I certify that I have tested the applicant in accordance with Transport for NSW procedures. CSRDT's signature

PERCENTAGE RANGE

45071250 (11/20) Form1408

Results PASS FAIL Number of FAIL items



4. Conclusion: Research + Writing (1/2)

A submission belongs to **incremental** if

- Some Optimization (缝缝补补), or
- Tradeoff (拆东补西), or
- Limited Applications (杯水车薪), or
- Dependent (狐假虎威), or
- Not Surprising (循规蹈矩).

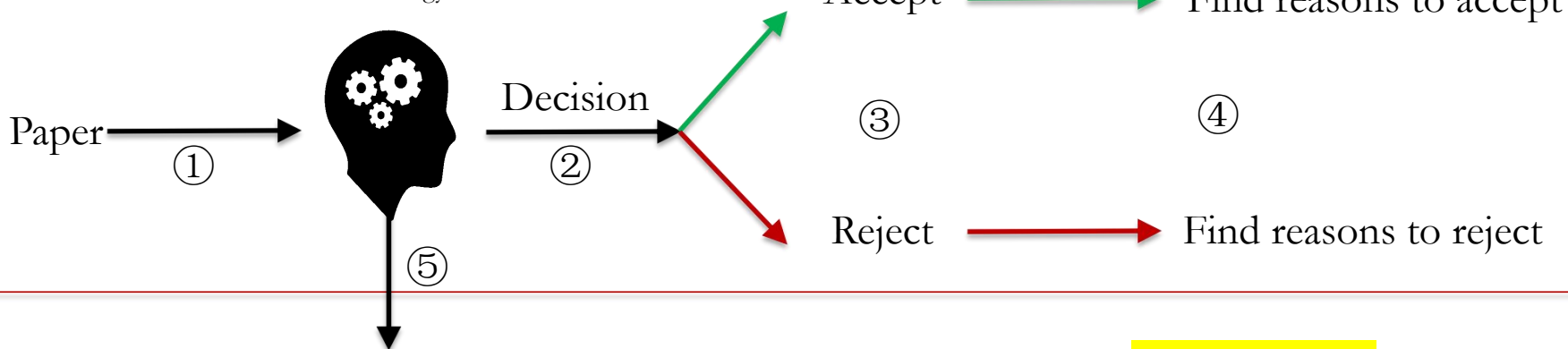
REJECTED

Academic Paper

- Substance
 - Reliable(可靠性):
 - Comprehensive(全面性):
 - Clarity(清晰度):
 - Effectiveness(有效性)
- Reasoning
 - Necessity(必要性):
 - Completeness(完整性):
 - Correctness(无误性):
 - Consistency(一致性)
 - Rigor(严谨性):
 - Sufficiency(充分性):
 - Concreteness(具体性):

Instinct (本能)

Fast for Energy-save



It is therefore important to prove novelty **effectively!**



4. Conclusion: Research + Writing (2/2)

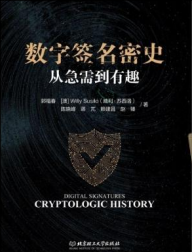
We can **qucikly prove** that the novelty in our work is solid.

We can **prove** that the novelty in our work is solid.

The novelty in our work is solid.

酒香不~~也~~怕巷子深，因为PC腿力有限走不远！





THE END

Dear author,

We are sorry to inform you that your submission

Title: Fully Tight Security Reduction for Unique Signatures

Authors: Fuchun Guo (University of Wollongong)

Willy Susilo (University of Wollongong)

was not accepted to Eurocrypt 2021.

We received many good submissions, but could only accept a small number of them to the program.

图 1-2 欧密会 (Eurocrypt) 于 2021 年 1 月发出的一封拒稿信

如果论文审稿者是和隔壁邻居老奶奶一样慈祥，且比人类高出三个科技文明等级的外星人就好了，可惜的是实际情况不是这样的。时间有限、精力有限、水平有限的论文作者，需要通过有限的篇幅，向时间、精力、水平也都有有限的审稿者讲清楚研究内容和研究贡献不是一件容易的事情，但这是论文作者一生都必须认真对待的一件事。

7

