Competing for Attention: An Interview Study with Participants of Cryptography Competitions

Ivana Trummová
trummiva@fit.cvut.cz
Czech Technical University in Prague, Czechia
Leibniz University Hannover, Germany

Juliane Schmüser
juliane.schmueser@cispa.de
CISPA Helmholtz Center for
Information Security, Hannover, Germany

Nicolas Huaman
huaman@sec.uni-hannover.de
Leibniz University Hannover, Germany

Sascha Fahl
fahl@cispa.de
CISPA Helmholtz Center for
Information Security, Hannover, Germany

Abstract

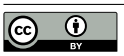
Cryptography competitions often contribute to the development and standardization of new cryptographic schemes. They help select primitives and algorithms that solve specific cryptographic problems securely and efficiently from a list of candidate submissions. Over the last decades, several competitions held by NIST and other research and regulatory organizations resulted in standards for, e.g., symmetric and asymmetric encryption, hashing, digital signatures, and, most recently, quantum-secure cryptography. However, while these competitions fostered much technical research on the submitted schemes, little is currently known about the human aspects of their processes, how they shape the competition results, and their perceived impact on cryptography security.

To investigate human aspects of cryptography competitions, we interviewed 20 experienced cryptography competition participants about their experiences, their assessment of the competitions' impact and its determinants, and their suggestions for future events.

We find that competitions bring attention to a cryptography area, provide research focus and motivation, and establish trust in schemes through community scrutiny and collaboration. Our participants highlighted the criticality of transparency, fairness, and trustworthiness of the competition organizer, emphasizing a need for clear and open communication. Based on these findings, we suggest strategies for future competitions to maximize engagement and provide transparent, trustworthy processes and results. We recommend stronger moderation of social conduct on official channels to ensure fairness and prevent putting off potential contributors. We also find that substantial industry involvement and systematic feedback collection are critical. Transparent organization and evaluation elevate the competition and foster secure and well-adopted standards.

CCS Concepts

• **Security and privacy → Social aspects of security and privacy**.



CCS '25, Taipei, Taiwan

ACM ISBN 979-8-4007-1525-9/2025/10
https://doi.org/10.1145/3719027.3765201

Keywords

Cryptography, Competitions, Participants, Teams, Submissions, Standardization, Selection, Attention, Transparency, Trust, Fairness

ACM Reference Format:
Ivana Trummová, Juliane Schmüser, Nicolas Huaman, and Sascha Fahl. 2025. Competing for Attention: An Interview Study with Participants of Cryptography Competitions. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25), October 13–17, 2025, Taipei, Taiwan.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3719027.3765201

1 Introduction

For the past 30 years, cryptography competitions have facilitated cryptography standardization. Competitions helped establish and widely adopt impactful algorithms, including AES [22] and SHA-3 [9]. These standards lay the cryptographic foundation of information and computer security and secure protocols. Competitions formulate a problem or need that requires new cryptographic approaches, such as quantum-resistant cryptography, and then pick and highlight algorithms to solve this problem. However, conditions vary widely, and these differences influence the choice of algorithms and, therefore, their adoption on a large scale, which is why there have been heated debates about the conditions in previous competitions.

In the past, most of the globally influential competitions were organized by the National Institute of Standards and Technology (NIST): *"NIST works to publish the strongest cryptographic standards possible,"* the agency said in a statement. *"We use a transparent, public process to rigorously vet our recommended standards. If vulnerabilities are found, we work with the cryptographic community to address them as quickly as possible."* [13] NIST succeeded in their work: The AES winner, which became the successor to DES, is used globally for encryption in various areas of application, e.g., in TLS, cloud storage, and goverment communications. While other stakeholders like academics, IETF, or ISO contribute to standards, none matches NIST's track record. However, the stream cipher Salsa20 [6] from the eSTREAM final portfolio [50] became widely adopted in TLS, messaging apps, VPNs, and other applications. Although NIST has undoubtedly been the strongest authority for cryptography competitions, their reputation for integrity was damaged by the National Security Agency's (NSA) actions in the case of the Dual EC_DRBG generator standardization [8], when NIST recommended

a backdoored algorithm [37]. While the Dual EC_DRBG was a significant setback to NIST's trustworthiness, many believe that organizing the AES and SHA-3 competitions substantially restored its reputation [51].

Hence, it is critical to study the human aspects of cryptography competitions and how they influence the competition results and their impact. While cryptography competitions have been integral to the cryptographic ecosystem for decades, the scientific literature lacks insights into the community's perceptions and experiences. To the best of our knowledge, we are the first to investigate the methods and processes of cryptography competitions from the participants' perspective. By interviewing cryptography competition participants who have extensive experience with the processes of cryptography competitions, we provide deep insights into their motivation to participate, experiences during competitions, and views on controversies. We identify concerns and challenges that they encounter with both NIST and non-NIST approaches. We also delve into participant perspectives on fairness, transparency, and trust and how these influence the impact and adoption of competition results. A key motivation for our work derives from Bernstein [7] who observes: *"It is surprisingly difficult to find literature systematically analyzing the security risks in various algorithm-selection processes, and systematically working on designing processes that reduce these risks."* By having a mutual discussion with participants of most of the large cryptography competitions, we aim to pinpoint the security risks and the key design mechanisms that reduce them.

We address the following research questions in our paper:

RQ1 *What are the experiences participants of cryptography competitions had in the past?* Experiences of competition participants in the past 30 years (starting with NIST AES).
- **A:** *What motivates people to compete?*
- **B:** *How do competition participants perceive the process and the outcomes?*

RQ2 *How do cryptography competition participants assess their impact?* Opinions of competition participants about transparency, fairness, and perceived level of security achieved.
- **A:** *How do competitions impact the crypto community?*
- **B:** *How does the community impact the design and security of competitions?*

RQ3 *What are the participants' suggestions for improving future cryptography competitions?* Lessons learned from the past competitions and suggestions for future ones.

With this work, we make the following contributions:

In-Depth Insights into Participants' Experiences. We conducted and analyzed 20 semi-structured interviews with participants of the 9 most influential cryptography competitions of the last 30 years. We gathered experiences from both winning and non-winning submitters and their teams and captured their motivations, competition reflections, and views on how future competitions can be improved.

Competitions Overview. We provide a systematic overview of the cryptography competitions our participants submitted to.

Competition Process. We discuss improved competition processes, from identifying the need for new cryptography to standards adoption. We provide detailed insights into how participants envisioned the competition process and stakeholder responsibilities (cf. Figure 3).

Path Forward. Based on our results, we provide recommendations to future organizers and participants of cryptography competitions and the community.

2 Cryptography Competitions

Cryptography competitions have emerged as a structured process to define problems, collect and evaluate potential solutions, and finally highlight and often standardize one or multiple schemes that solve the problem securely and efficiently. This section aims to give an overview of typical competition procedures and circumstances, focusing on competitions relevant to our results.

Procedure. Competitions are often international events and typically span multiple years. Participants are expected not just to submit a scheme conforming to requirements by a set deadline, but to actively participate throughout the whole process, defend their submission, and incorporate feedback. Therefore, a community is created in the process, and continuous discourse happens over centralized platforms. The most important communication platform in competitions are mailing lists, where most discussion takes place. Some competitions organize meetings and workshops where people can meet, discuss, and get to know each other's work. Submitted schemes are subjected to cryptanalysis by other participants and the wider community and the evaluation committee typically uses the analysis outcome to eliminate candidates over the course of multiple rounds. Optional resources are sometimes given, e.g., a benchmarking tool, API and compilation server, API specification, or Linux distribution with tools.

Requirements. Competitions and their requirements are motivated by a specific need for a new cryptography solution, such as a broken standard, new application needs, or new threats. For example, the first cryptography competition (NIST AES [40]) started in 1997 and ended in a standard widely used today: The selected Rijndael [21] became the symmetric Advanced Encryption Standard (AES) that replaced the broken DES scheme. Vulnerabilities discovered in MD5 [23], SHA-0 [15], and SHA-1 [59] led to the competition for a distinct and non-similar hash function SHA-3, won by Keccak in 2012 [16]. Cryptography competitions also selected better solutions for encryption and hashing in environments with constraints that limit performance [57], such as CAESAR [1] and NIST LWC with Ascon [24]. Most recently, multiple competitions focused on the emerging threat of quantum computing breaking traditional cryptography [2, 3, 19, 45]. NIST's PQC competition and the Korean effort KpqC selected multiple KEM/PKE and signatures schemes, and NIST extended their call for signatures, which at the time of writing this paper considers 14 submissions in the second round [3].

Typical requirements in cryptographic competitions include security and performance requirements as well as information about implementation and portability. In some competitions, requirements are prescribed by the organizer, whereas others synthesize requirements from community discussion and feedback. Security requirements typically include supposed resistance to various types of attacks, formal security definitions and proofs, clear specification

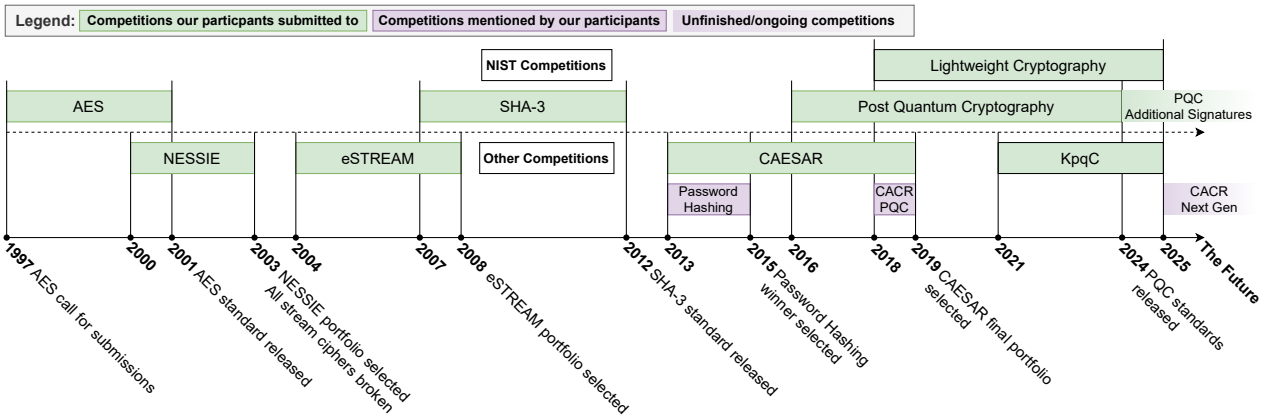


Figure 1: Timeline of cryptography competitions from start to standard or portfolio selection. We include competitions that our participants submitted to, as well as other competitions they mentioned.

of security margins (e.g., key size or number of rounds), and elimination criteria. Performance requirements reflect the intended use case of the standard implementation. Competitions can also require reference implementations, design rationale, and documentation [5, 38, 41, 42, 43, 46, 47, 50, 61].

Organizations. Since the late 1990s, the US federal agency NIST has played a key role in the cryptography ecosystem. It is the standardization body that introduced cryptography competitions, starting with the AES competition, to choose algorithms that become ubiquitous standards [40]. NIST has since continued to use and develop the successful competition format of selecting one scheme for standardization in the SHA-3 and LWC competitions, extending their reporting and community involvement [16, 57]. With their recent PQC competitions, NIST selected a portfolio of schemes for standardization for the first time [2].

Other organizations and researchers followed the example set by the AES standardization process. The New European Schemes for Signatures, Integrity, and Encryption project (NESSIE) began in January 2000 and concluded with the publication of its results in 2003. In contrast to the agency-run NIST competitions, it was set up as a research project with European funding, and it aimed to give recommendations, rather than produce new standards [49]. NESSIE selected a portfolio of algorithms in several categories, noticeably lacking a stream cipher since all candidate schemes were broken. The eSTREAM project was created as a follow-up to advance the understanding of the design and analysis of secure stream ciphers and to identify a portfolio of promising stream ciphers [50].

KpqC is the Korean counterpart of NIST's PQC standardization efforts [19]. KpqC's scope was smaller, the goal being to prepare quantum-safe standards, and to ensure that the effort is not dependent on the USA. The competition was semi-national (at least one team member had to be Korean for each submission), organized by Korea's National Intelligence Service and Security Research Institute, and part of the country's plan to transition to PQC [55]. The CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) competition to create authenticated encryption scheme designs, conducted between 2013 and 2019, is an example for a competition organized by an international team of cryptologists rather than an effort backed by geopolitical interests. The final CAESAR portfolio comprises three use cases: lightweight applications for resource-constrained environments, high-performance applications, and defense in depth [1].

Other national efforts - like the Chinese CACR PQC, CACR Next Gen, and Password Hashing competition - were occasionally mentioned by the participants of our study. However, as the participants had not submitted to those competitons, they are not relevant for our results.

3 Related Work

We discuss related work on the design of cryptography competitions and insights into the cryptography competitions ecosystem.

Designing and Improving Cryptography Competitions. In the background section, we already described the brief history of individual cryptography competitions. In addition, there have been papers that have studied their processes and quality and considered competition design. In 2020, Bernstein [7] published a comprehensive overview of cryptography competitions, where the relationship between speed and security is closely reviewed. Among other topics, the work discusses the conflicting incentives of publishing papers versus creating stable cryptography. Since AES (the first modern cryptography contest), NIST has been the leading organizer of international standardization efforts, and the design of the competition process has remained roughly the same.

In our interviews, we asked the participants to subjectively estimate the security of winning schemes and the most critical moments in the processes of competitions regarding security. Other works focus on the level of security and quality achieved in competitions. Preneel [48] presents a brief overview of the state of hash functions 30 years after their introduction and discusses the progress of the SHA-3 competition. Kannwischer et al. [33] describe the state of implementation quality of NIST PQC submissions. Bock et al. [11] propose a new competition framework for evaluating white-box cryptographic implementations based on their resilience to real-world attacks. Klein [36] highlights and gives examples of how

political and security agency pressures have historically influenced cryptographic standards, often weakening encryption for surveillance purposes, and underscores the importance of independent, transparent cryptography competitions to ensure security-driven rather than politically motivated design choices.

Insights into the Cryptographic Ecosystem. Regarding interviews with cryptographic experts, work has focused on developers and how they implement cryptography in, e.g., companies or open-source tools. This section provides an overview of recent interview papers and their findings for improving cryptographic processes. Prominently, Jancar et al. interviewed 44 developers of 27 popular cryptography libraries about mitigating timing attack side channels in cryptography implementations. Regarding the standard organizations, they found that they need to encourage automated evaluation of timing attacks for submissions and avoid using algorithms susceptible to timing attacks in any published set of standards [32]. Similarly, Haney et al. present interviews with 21 representatives of organizations that use cryptography. They found that these organizations tend to put high emphasis on their security. Concerning standard organizations, they recommend that these organizations improve their support and supplementary resources for implementers and users of these standards. They should also communicate the reasons and justifications for their decisions on standardizing cryptography in order to help implementers understand how to implement the standards and what to focus on [28]. Schmüser et al. conducted interviews with developers of cryptographic libraries, finding that they turn to cryptographic standards for guidance, but those often leave room for interpretation and design decisions based on the developers' opinions [53]. In 2024, Huaman et al. studied standards and their usability. Their work examines the products of competitions (or other processes) but does not focus on the process that precedes creating the standards. They found that working with and implementing standards faces multiple challenges, such as updates to standards potentially breaking compatibility, laws and patents discouraging the use of standards, and the community sometimes providing a problematic environment for participation in open standardization processes like competitions. They also identified key properties of good standards, like provided test vectors and well-documented reference implementations [29]. Also in 2024, Fischer et al. conducted an interview study with cryptography experts studying the path of cryptography adoption. They state that interviewees' collective sentiment towards open standardization processes, like the IETF's Internet Standard Drafting Process and open cryptography competitions run by NIST, was favorable compared to more closed processes like those of ISO or ETSI. At the same time, some interviewees said that NIST processes could be improved, questioning the competition requirements set by the organizers or being concerned about NIST's collaboration with the NSA [26].

As part of their findings, these papers illustrate essential shortcomings of the existing standardization processes. In our work, we obtain in-depth perspectives on the identified issues and give detailed recommendations for future standard competitions.

4 Methodology

To investigate the experiences and opinions on cryptography competitions, we conducted semi-structured interviews with 20 participants of cryptography competitions between July 2024 and February 2025. We elaborate on our interview design, recruitment, sample demographics, and data analysis to provide context for our results. We also discuss ethical implications and limitations for the interviews and how we addressed them.

4.1 Interview Design

We developed the interview guide based on our research questions and insights from related work on cryptography competitions [7]. We tested the interview guide in 2 pilot interviews. We made only minor changes to the wording to improve clarity based on participant feedback and included the pilot interviews in our final dataset. The final interview guide contains an introduction, five main sections, and an outro. We present an overview in Figure 2 and the complete guide in our supplementary materials (cf. Availability). The interviews lasted 61 minutes on average.

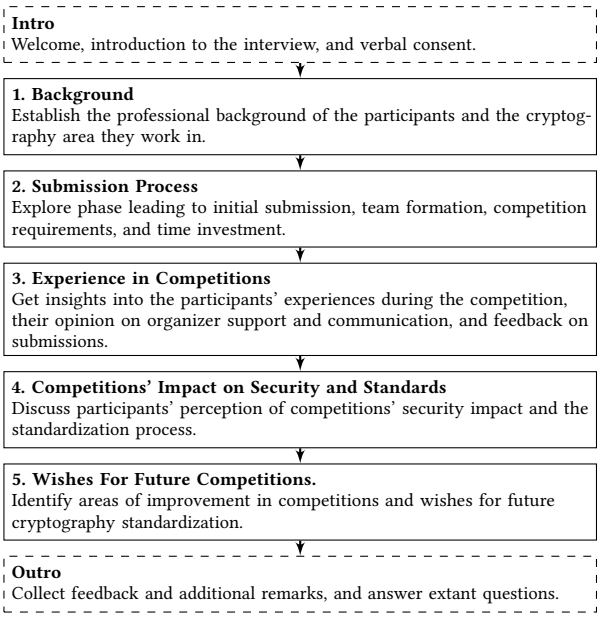


Figure 2: Illustration of our interview guide: We covered participants' background, the submission process, experiences with competitions, views on competitions' impact on cryptography security, and ideas to improve future competitions.

Intro. We briefly introduced the research project, assuring the participants that we were interested in their experiences and opinions and would not judge their answers. We obtained consent for recording.

Background. For context and to warm up the participants, we asked them to describe their educational and professional background and the area of cryptography they worked on.

Submission Process. Next, we asked about the time before the initial submission. This included questions on the competition's requirements, team formation and roles, time commitment, motivation for participating, and initial challenges.

Experiences in Competitions. In this section, we investigated the participants' experiences during the competition. We covered the organizers' role, communication, and support provided during the competition. We discussed the submission's success, the feedback participants received from the organizers and the public, and what happened after the submission was chosen. Finally, we asked the participants to compare competitions if they had participated in more than one and if they considered participating again in the future.

Competitions' Impact on Security and Standards. In addition to participants' general perception of if and how competitions contribute to secure cryptography, we asked about specific processes such as selecting candidates during the competition and the standard drafting afterward. We asked participants about factors influencing their perception of security and what they believed was the best process for creating new standards.

Wishes For Future Competitions. In the final part of the interview, we focused on desired changes for future competitions. Topics included motivating and supporting participants and cryptanalysts and possible alternatives and supplements to competitions. Last, we asked the participants how they would design a competition.

Outro. We debriefed the participants at the end of each interview, allowing them to make additional comments and ask questions, either during or after the recording.

4.2 Recruitment

We recruited participants who had participated in at least one cryptography competition. Initially, we considered the following competitions: NIST PQC, NIST PQC Additional Digital Signature Schemes, NIST LWC, SHA-3, AES, CAESAR, eSTREAM, and NESSIE. We subsequently added the KpqC, CACR PQC, and Password Hashing competitions after participants brought them to our attention. We reached out to 90 participants from publicly available lists of competition entrants, contacting them in waves of 15-20. We only contacted each person once to reduce the burden of cold emailing. We also posted in two mailing lists. We prioritized participants who had competed in multiple competitions, including both winners and non-winners. Since most competitions take place in the US and Europe, we covered competitions organized in these regions, with one exception of South Korea (which we chose to compare two different post-quantum efforts). Our participants' geographic diversity reflects this, which is a limitation of competitions in general. Our participants set consists of 16 people identifying as male and 4 as female, which reflects the gender gap of crypto community. Our invitation email contained a link to our project website, which provided further information on the researchers involved and the project, and a link to our demographics survey. After consenting to our study procedure, confirming that they had participated in at least one cryptography competition, and providing demographic information in the survey, the participants were redirected to schedule an interview slot using calendly[1]. We determined thematic saturation as the point at which no new topics or themes emerged from analyzing additional interviews [52]. We reached this after 16 interviews and proceeded to conduct four additional interviews, confirming saturation. We provide our invitation email, consent form, and demographic survey in our replication package (cf. Availability).

4.3 Qualitative Data Analysis

We used the GDPR-compliant transcription service Amberscript[2] to transcribe the interview audio recordings, and we manually reviewed the transcripts for any mistakes during analysis. We then conducted thematic analysis as described by Braun and Clarke [12]. To develop an initial codebook, three researchers independently conducted inductive open coding on the first interview and merged the three resulting codebooks in a collaborative session. We then used the initial codebook to independently code further interviews with two researchers each, leaving the researchers free to add to and change the codebook. We reviewed and merged changes to the codebook in collaborative sessions in multiple rounds after each 1-3 interviews. We provide the final codebook in our replication package (cf. Availability). Two researchers independently coded each interview transcript and resolved disagreements in a joint discussion, achieving a theoretical agreement of 100%. Therefore, we do not report inter-rater reliability (IRR) [39]. We assigned 1,976 codes, corresponding to a median of 94 codes per interview. Finally, all coders conducted an interactive affinity diagramming [10] session to extract themes from the final set of codes.

We refrain from reporting counts to reflect the qualitative nature of our analysis. Instead, we follow the example of recent interview studies [4, 25, 27, 53, 58, 60] and use qualifiers to estimate prevalence among our participants in our reporting (cf. Figure 4).

4.4 Limitations & Ethics

To contextualize our results, we discuss ethical implications concerning our study and its participants, as well as the limitations of our study.

Authors. None of the authors has competed in cryptography competitions. Our backgrounds are in cryptography, computer science, and usable security.

Ethical Considerations. Our institution's Ethical Review Board (ERB) approved our study design, which follows the ethical guidelines laid out in the Menlo Report [35]. We obtained informed consent from all participants, and we highlighted in our consent form (cf. Availability), as well as at the beginning of each interview, that participation was voluntary, any questions could be skipped, and that the participants could leave the interview at any time. We assured participants that we would not judge their answers and would handle their data confidentially. We used only short, anonymous quotes in our publication and provided the participants with a preprint to review our use of their quotes. Our data handling procedure is compliant with the general data protection regulation (GDPR). All participant data was encrypted and stored internally, with only the research team having access, aside from transcription,

[1] https://calendly.com/
[2] https://www.amberscript.com/

which was done by a GDPR-compliant transcription service. We offered all participants $60 to compensate them for their time.

Limitations. Some limitations inherent to qualitative interview studies apply to our work. Data collection includes under-, over-, and self-reporting bias, recall bias, and social desirability bias, all of which could lead to participants' reports differing from reality. We sought to mitigate these biases by carefully probing our participants for elaborate answers and reassuring them that we did not judge their answers in any way and would only report them anonymously. In addition, we do not assume that a participant not reporting a specific thought or behavior equates to not having it in the interpretation of our results. Participants in cryptography competitions are a small and hard-to-recruit expert population. Given the expertise and experience required to design a cryptographic scheme, it is unsurprising that our sample comprises highly educated cryptographers with multiple years of experience in the field. As is common with qualitative studies, our sample and, thus, our results may not be representative and do not necessarily generalize to all participants of all cryptography competitions. We recruited from the participant lists of cryptography competitions. While we carefully researched them and extended our list whenever we became aware of a competition (e.g., when it was mentioned in an interview), we may have missed some less popular competitions. Our participants self-selected for our study, and advertising a study on the impact of cryptography competitions may have led to participants who are more or less satisfied with the current competition format than the average competition participant. Finally, our qualitative data analysis using semi-open coding and thematic analysis may include researcher bias. However, we mitigated this by creating three independent codebooks, which we then merged in a discussion between three researchers, and by independently double-coding each interview before resolving disagreements in a discussion.

5 Results

We now report the results of our 20 semi-structured interviews, based on the thematic analysis. Our analysis and all results are qualitative and should not be interpreted as quantitative or representative findings. We report on our participants' experiences with the cryptography competitions, including their role and experiences with the organizer, participants' motivations and blockers for participating, and the competitions' perceived impact on cryptography and cryptographic security.

5.1 Participant Demographics

We present the participants' demographics in Table 1. Most were highly educated and had extensive experience in cryptography. To protect their anonymity, we can report some demographics only in an aggregated form. Of our 20 participants, 5 had won a competition, and 3 had reached the final round. 11 had submitted to multiple competitions, ranging from 2 to 6 participations.

5.2 Participants Are Motivated, but the Balance of Rewards and Cost for Competing Is Off

Although all participants chose to compete, they reported various incentives and blockers, and only some would join another competition. Many said they would consider it under specific circumstances, such as when coordinating a motivated team or with realistic chances to win, and some said they would not join another competition. About half of our participants reported that to better motivate people to participate in competitions, they needed better rewards for cryptanalysis, recognition of their contributions for academic credit, or more funding.

Table 1: Summary of our participants' demographic information: We report the years of experiences with cryptography competitions, participants' education, whether they work in academia or industry, and the competitions they submitted to.

Alias	**Experience** (years)	**Education**	**Field**[◇]
P1	10 - 14	PhD, Cryptography	A
P2	15 - 19	PhD, Computer Science	A
P3	10 - 14	PhD, Cryptography	A, I
P4	30+	PhD, Cryptography	I, A
P5	15 - 19	PhD, Cryptography	A
P6	5 - 9	PhD, Cryptography	I,A
P7	10 - 14	PhD, Cryptography	A
P8	10 - 14	PhD, Cryptography	I
P9	25 - 29	PhD, Cryptography	A
P10	25 - 29	PhD, Cryptography	A
P11	20 - 24	M.Sc., Cryptography	I
P12	30+	PhD, Cryptography	A
P13	5 - 9	PhD, Cryptography	A
P14	5 - 9	PhD, Cryptography	I
P15	30+	PhD, Cryptography	A, I
P16	5 - 9	Master, Unrelated	I
P17	25 - 29	PhD, Maths	A
P18	5 - 9	PhD, Cryptography	I
P19	10 - 14	PhD, Cryptography	A
P20	10 - 14	PhD, Cryptography	A
Gender	*Female:* 4	*Male:* 16	
Submissions	*Participants with selected or winning submissions:* 5		
Competitions[*]	*NIST PQC: 9, NIST PQC ADS*[▽]*: 4, NIST AES: 3, NIST SHA-3: 5, NIST LWC: 3, KpqC: 2, CAESAR: 3, NESSIE: 3, eSTREAM: 1*		
Team Size[**]	*Small (1-3):* 12	*Big (4+):* 10	

[◇] A: Academia, I: Industry; primary listed first.
[*] Several participants competed in multiple competitions. We only show total numbers of participants who submitted to a competition to keep the participants anonymized.
[▽] NIST PQC Additional Signature Schemes.
[**] Several participants were part of multiple teams.

Competitions Motivate and Provide a Research Focus. Competitions motivated our participants to work on and submit relevant algorithms for many reasons.

A majority of our participants emphasized that competitions focus attention on a particular area of cryptography. This resulted in motivating factors that can primarily be split into two groups. First, these participants argued that the increased attention from competitions led to a higher impact of their research. Many said it motivated them to work on an interesting cryptography area with an active community, with some saying that it enabled them to receive more feedback on their work and some saying that they liked to contribute to the community's scientific progress. One participant stated: *"Competitions are usually in a very hot area of cryptography that is seeing quite a lot of change. [...] There is usually quite some research advances that you want to be part of."* (P1) Many participants said the attention drew interest from collaborators and industry, with some reporting more practical use of their research. Second, the participants described increased attention helpful for

their work and careers. Many said they competed to highlight their research and algorithms and show their work to a broader audience. A few described how this could lead to new job opportunities, and many noted positive outcome for academic careers such as published papers, increased citations, and the possibility to secure more funding. One participant summarized: *"It's a great way of advertising your research. I would say that exposure was the number one motivation. […] From a career perspective, it's just a great thing to do."* (P8)

Apart from the increased attention, their teams and colleagues motivated participants to submit to a competition. A few reported their supervisor had decided their participation. Many said that competitions fit well with doing a PhD in cryptography with regards to time frame, workload, and publication output, either being grateful for their participation during their PhD or that it was something they could encourage their PhD students to do: *"These competitions tend to be for three, four years, which is pretty ideal for someone like a PhD student […] They'll find their topic in there and it is bleeding edge."* (P9) Finally, the majority of our participants reported personal motives for joining competitions, such as being competitive, having fun, and extending their knowledge and skills.

Participating in Competitions is a Lot of Effort that Is Not Always Adequately Rewarded. According to our interviewees, competing required much time, effort, and skills. Our participants' estimates of time spent in a competition range from a couple of months to more than ten years. Most struggled to estimate the time, as competition work overlapped with their regular jobs. About half had also begun work on their schemes way ahead of the competition and said that a lot of that work was needed for their submission but not explicitly done for the competition:

> *"There is some work that is really specific to the actual submission. […] There is a lot of work that went into the scientific papers that are associated with it, which would have happened otherwise as well but are also relevant to the submission"* — P5

Almost all participants worked in teams, typically with two to eight core contributors per submission. While some said that all team members did a bit of everything, most participants reported a split between the many skills and tasks required to participate in a competition. Initially, participants reported performing requirements engineering, considering the competition's requirements, their own design goals, current trends in cryptography, and the plans of other submitters: *" We also, in this phase discussed a bit with other colleagues in the research area about their plans and tried to get a feeling what people would submit there."* (P1)

In the phase leading up to the submission, participants considered discussing and developing the algorithm design a core task, often modifying a pre-existing design based on the requirements. Almost all participants additionally reported needing the algorithm implemented for the submission, and most viewed design and implementation as distinct tasks and areas of expertise. The design was seen as more theoretical, requiring a deep understanding of mathematics and cryptography theory. Some participants mentioned needing someone to formalize the design. Implementation was regarded as a more practical task requiring programming, architecture, and optimization expertise. For the submission, participants typically had to prepare a set of documents, including a write-up of their algorithm design and motivation for design choices. Some said that at least one team member needed to be a good writer.

During the competition rounds, the focus shifted to cryptanalysis. About half of our participants reported that they or their team analyzed the other submissions to the competition. Many said that there were debates about the submissions and attacks, centered mainly around the practicality of attacks and when to consider a scheme broken. A few said it was essential to participate in these debates to defend and argue for their submission. A few also reported that they were allowed to make minor changes to address the findings of cryptanalysis during the rounds.

Across all phases, the majority of our participants said that a competition team needed someone to assume the role of team leader and coordinator, overseeing and organizing the team effort. Many participants described this as a significant challenge:

> *"The idea is that you have many aspects that you need to fulfill. [Design is] very different work from implementing the scheme for instance. I had to be aware of everything to coordinate people because when people were selecting parameters it also had an impact on the implementations et cetera. The big challenge was to manage people."* — P13

Our participants did not report receiving many resources from the competition organizers to support them with these many and complex tasks. The majority said that organizers provided mailing lists and organized conferences or workshops to foster communication. Only a few participants mentioned websites and documentation, though this may be because those were taken for granted. Only one or two participants each reported additional resources, including an API, a benchmarking tool, a Linux distribution with tooling, and funding. Still, participants voiced few complaints about this lack of resource provision. Only one or two participants missed additional guidelines, a contact person for questions, a benchmarking tool, and a programming and testing framework. More typical was a lack of time, which many participants complained about. However, only some participants attributed this to the organizer, saying the timeline had been inconsistent and delayed. Communication was an area in which many participants thought the organizer could improve support.

Apart from improving their communication, the participants felt the organizer should better moderate the community communication, especially on mailing lists. They observed that some conversations derailed or turned hostile, distracting from scientific discourse, and wished for the organizer to keep the discourse focused and civil:

> *"This was a personal drama, but this had a massive impact because they started shooting down everyone who spoke up, and this entirely kept junior people out. […] The organizer should moderate communication, making sure that everyone is heard and not just a few. […] Otherwise, ban people from the mailing list if they act disrespectfully towards other participants. There were some things that were just not okay. This needs a strong moderator in the end."* — P3

Without this moderation feedback from junior researchers, industry and other third-party sources on algorithms may be discouraged, leading to potentially worse algorithms. There are also other reasons why many participants described competitions as stressful. As

academics with many projects and obligations, they lacked sufficient funding and time to spend on them. For many participants, a lack of recognition of the associated effort was a significant reason why they did not spend more time or budget on competitions. They thought that contributions to the competition, both submissions and cryptanalysis, were not sufficiently rewarded and did not translate to academic credit well enough. A key challenge for cryptanalysis was the inherent risk of not finding a viable attack, meaning the invested time would not lead to a publication:

> *"In analysis you always have the risk that you don't find anything and then don't have anything publishable. Giving an incentive on the analysis is something that competitions are well suited to, but that also needs to be taken up. If that doesn't work out well for some reason, then it can be very detrimental to the security of the results."* — P1

For submissions, their success in the competition was essential for resulting recognition. However, even for selected schemes, translation to academic credit did not always work well:

> *"The problem is, if you submit something to a competition, then it becomes a standard, then people cite the standard. If you're in academia, […] then you need citations. However, someone citing the standard, I don't get a citation from that. […] It does not contribute to my citation index."* — P4

One participant suggested to address these issues by awarding funding based on competition efforts:

> *"It would be great if these publications would be considered by the sort of research funding bodies. When we do a lot of work where you might get a journal publication out of it, but it would be great if the grant and approving parties would, like, recognize this kind of activity as the top tier activity of cryptography that this is."* — P9

Key Insights: Motivation, Effort and Rewards.
Competitions motivated our participants and helped them focus their research, but they required a lot of work and expertise that participants did not always feel was adequately rewarded.
This section addresses RQ1, especially RQ1A, by highlighting participants' motivations, and perceptions of the competition process.

5.3 Role of Standardization Organizations

The impact of an organizer was a major factor in the participants' assessment. About half believed organizers should at least be stakeholders with a significant impact on cryptographic standardization. Many said that NIST is historically a good fit. As one participant put it:

> *"It's huge because only very few organizations have the power to make sure that the algorithms that get selected in the end will be used on the scale that we start seeing now for the new post-quantum algorithms. Maybe ISO would be getting close. IETF also has a lot of power in selecting things that then actually get used."* — P5

Among the mentioned organizations, NIST was the major organization conducting competitions (cf. Figure 1), so it was the focus for almost all participants. We report on participant expectations for organizers, focusing on transparency, the selection and communication processes, and the post-competition path to standardization.

Organizers Need to Be Transparent and Trustworthy. Trust is an essential condition for organizations that conduct competitions. The majority of our participants mentioned that trust in the organizer is generally critical. Impactful standards require trusted, transparent and influential organizations with a good reputation. About half of the participants considered transparency critical, especially for the selection process. Thus, the organizer must openly communicate the timeline, reasons for decisions, and motivations for requested changes and ensure that political or third-party influence is appropriately managed or disclosed. NIST is generally perceived as transparent, according to about half of our participants. However, in many cases, participants also reported intransparent behavior. One participant described their experience with NIST:

> *"NIST did publish a report. It was transparent in the sense that they had a public document that motivated their decisions. Then, of course, they had all these internal discussions that we didn't see. It's not completely transparent because we don't see everything, but it is to a large extent."* — P8

Most participants expressed concerns about third-party involvement, reporting on stories about it, like the NSA in the U.S., leading to a lack of clarity in decisions and reduced trust in the standard. More generally, political backgrounds and misaligned incentives damage trust, both for NIST and other organizers close to governments, as reported by about half of our participants:

> *"When the Russian Federation tries to bring a block cipher to ISO or IETF or whatever, we cannot assume this is done in good faith. The procedures were not designed to handle such a behavior. If you ask me, what would be the best thing to do? It would be to look at how NSA screwed up dual CDBG in ISO and the IETF and in all other places."* — P10

Justifying reports and decisions builds transparency and trust, especially in how schemes are chosen for future rounds.

Most Participants Perceived the Selection Processes as Fair. The winner selection process is key to the quality of the resulting standards. Almost all participants saw the selection processes as fair or appropriate to the competition's goals. Some saw the selection as unfair, noting that big teams or teams with well-known participants, which may have a funding advantage, typically had an easier time developing and defending submissions. These seemingly unfair conditions were widely accepted, as it was assumed that the advantages lead to stronger submissions. However, they may discourage less experienced or smaller teams. With NIST leading many competitions, fairness issues like having to fight with language barriers and bias could have affected some international participants. One participant mentioned:

> *"Is it a fair competition? I think so, but there's going to be some bias. […] Many schemes were very similar. Some were done by people in Europe, some were done by people in South Korea or China. The schemes by people in South Korea got eliminated and the ones by people in Europe advanced to the next round. I know that some South Korean people […] felt that it was unfair."* — P8

Many participants also viewed decision processes as arbitrary or flawed, noting issues like no opportunities for rebuttal if an algorithm fails and elimination for reasons fixable with more time. About half of our participants reported limited or no feedback from organizers about their submissions, They found not understanding

the selection process frustrating and unfair: *"The evaluation process is very unclear. […] The decision is from NIST, we don't know why. They don't explain why. They just say we've picked this one or that one and that's all."* (P2) While this seems to apply to algorithm selection in general, participants could name criteria for selecting specific algorithms. Some participants mentioned the obtained security with factors like key length and robustness, referring to basing algorithms on well-researched cryptographic areas and performance as common criteria. Versatility, or the ability to cover optional or light requirements of a call for participation, also mattered. The most frequently mentioned criterion for elimination, however, was simply the publication of attacks or other ways to break the algorithms.

Clear Communication Is Essential for Transparency and Fairness. Beyond communicating reasons for changes or algorithm selection and providing feedback for submissions, participants also reported on more general communication requirements for the organizer. Some participants highlighted the importance of communicating the timeline and goals of submissions. In many cases, the timeline and requirements for the resulting standards changed as research in the competition was advancing. For example, new attack vectors and defenses can require changes to many submissions, or new requirements can emerge, resulting in delays or changing requirements. While many participants felt that requirements should change as the competition and surrounding research evolve, they also believed that changes must be well communicated. Participants need to be provided with enough time to adapt. For example, P11 recalls an instance of changing requirements that may have been unfair:

> *"NIST wanted to change the requirements but then some authors were very angry and said that was unfair, and if NIST had said that in the beginning, they would have designed their algorithms differently."* — P11

Post-Competition Changes in Standards Are Controversial. For organizations like NIST, the purpose of competition is creating a new standard using the selected submissions [41, 42, 43, 47]. However, changes implemented without transparent reasoning can reduce trust in resulting standards, hindering adoption. Among the standards our participants were involved with, there were a few cases in which they were unhappy with the results. For example, in the SHA-3 competition, the winning algorithm (Keccak) was a simple scheme with variable-length output, as a participant reported. However, NIST released multiple variants of SHA-3 with fixed length as the standard version of Keccak. One participant noted this change being quite controversial, causing the standard to become complex and delaying release. Our investigation revealed limited trust in the chosen fixed-length variants, as the lowest variant was perceived as insecure [20, 54]. A statement by the Keccak team later provided the reasoning for tradeoffs [34]. This further demonstrates the requirement for transparency and communication from the organizer to build trust in standards.

> **Key Insights: Role of the Organizer.**
> Trustworthiness and transparency are viewed as critical features of competitions. NIST is widely recognized as a uniquely powerful standardization body, and while it is generally seen as transparent, there are limits. While most participants perceive the selection processes as fair, some noted biases, limited feedback, and poor communication. Post-competition revisions to the resulting standards may spark controversy. **This section responds primarily to RQ2, highlighting how the community views fairness, transparency, and the role of standardization bodies.**

5.4 Perceived Impact of Competitions on Cryptography Security

Competitions and standardization efforts have a significant role in shaping the focus of cryptographers. Not only do they influence research directions and foster collaboration, but they are profoundly shaped by the community's needs, maturity, and involvement.

Cryptographic Community and Competitions Shape Each Other. Competitions influence each other. They can either be a model to follow: *"[NIST competitions] were very much I think a model for some of the other competitions from Europe that came after that."* (P15) Or they can justify a follow-up, like eSTREAM after NESSIE: *"We knew we needed a good stream cipher because the NESSIE project ended. […] NESSIE didn't recommend any stream cipher because all the [stream cipher] candidates were broken."* (P10) Because competitions don't exist in isolation, they can heavily influence future projects. They can increase community bonds and connect theoretical and applied parts of the cryptographic community, guide researchers, and make it easier for the industry to use existing solutions.

> *"Competitions are the perfect opportunity for [different players] in the field to come together and listen to one another. Sometimes researchers don't even know that they're deviating from what are current needs. Sometimes the industry people are tinkering around and creating their own solutions for things that have been solved already a long time ago in academia. It works in both directions."* — P12

Competitions also have the power to shift the community's focus on a new niche area, as with PQC, facilitating a consensus in large parts of the community. *"[Post-quantum cryptography] was a very niche area at the time. NIST said that they wanted to standardize it. All of a sudden it gained a different status."* (P20) A majority of participants noted that competitions build trust and confidence in schemes by attracting attention and cryptanalysis.

> *"One person can know enough, but if you just have the whole world you motivated as a competition, look at your thing and transparently, then that's the best you can do. Probably. Security wise, I think I have much more faith in something that passes through a competition than anything else."* — P9

The relationship between cryptography competitions and the community is mutually influential. Competitions emerge from community needs, and their quality reflects the community's maturity. For example, NIST PQC included a key feedback round before the competition even began:

> *"They said in early 2016 they wanted to run such a competition, and then later in 2016, they had this draft, call for proposals online saying, "Hey, we appreciate feedback." They received some feedback, and then [published a] call for proposals."* — P5

Apart from openness and transparency, most participants noted the importance of significant involvement of the research community. Feedback from researchers is essential in creating the process and developing the requirements for a competition, and also for

the competing teams to further their research and scheme development, since the majority of participants reported a lack of feedback from the organizer. Additionally, the competitions rely heavily on cryptanalysts to eliminate candidates:

> *"[Recognizing (in)secure schemes] is mainly the responsibility of the cryptanalysts in the community to really invest quite a bit of work into the analysis of the schemes. […] If that doesn't work out well for some reason, then it can be very detrimental to the security of the results."* — P1

Competitions Are Perceived as the Best Path to Secure Standards, but Can Still Be Improved. Most participants mentioned that competitions are a good idea or said they are the best approach to secure cryptographic standards. The majority of participants were familiar with non-competitive standardization processes like IETF and ISO. None of them reported a clear preference for the non-competition approach in general. A few said that it is difficult to compare, but many mentioned various issues with non-competition processes, such as insufficient security guarantees or a lack of clarity about who is deciding in IETF: *"[…] it's not clear who's making the decisions right in the IETF. Everyone who appears on the mailing list can vote. This is quite vulnerable also to an unknown party controlling the outcome."* (P3) Many participants also spoke about IETF as being more closed-off and among themselves, not easily accessible for the community: *" In the IETF, you have to go to these IETF meetings, otherwise you don't know what's happening. These IETF things are always on a different continent."* (P4) One participant mentioned that such inaccessibility can create bias:

> *" It's a bit unfair in that not all of the people can attend these meetings and vote or generate consensus, so it's a very small subset of the community that can attend. The majority of the time it is very centered on people from North American countries that are men."* — P16

Among those who could compare, the majority either disliked a consensus-based decision process for standard selection or criticized the processes as very political and not scientific enough.

Although perceived as great tools to get standards, many participants emphasized that competitions are not universally applicable. Competitions are only effective when there is a clear but non-urgent need, a mature community, and a capable, well-funded organizer. A participant's take on competition timing: *"First identify a need. Going back for a second for the urgent, because the competition takes time, you cannot address urgent needs. This is something that you know you will need four years from now."* (P10) Many participants noted the risk of competitions taking too long, as the resulting standard may already be outdated by the time it is published. However, if competitions are too short, there is not enough time for teams to complete their submissions, for extensive cryptanalysis, and for the community to mature, which increases the risk of overlooked vulnerabilities.

> *"Competitions are nice to select, but this only works if you already have contestants there. This means you have to build a community before that. [PQC] would not have worked if there wasn't a whole crypto community that was started by a bunch of people in the early 2000s."* — P3

Almost all participants expressed their ideas about improving competitions, with the common suggestion being to strengthen the collaboration aspect of competitions. Some participants were motivated by competing against other teams, but many expressed the importance of a collaborative approach. A participant compared academia and industry perspectives:

> *"Coming from a company, I think collaborative approaches may be much better, but it's hard to get any academic credit and publish a paper in a collaborative approach to standardize and make the world better."* — P11

Some participants suggested assessing the security of the actual deployment as opposed to only focusing on security of the scheme: *"When it is deployed, it shows that one particular type of approach is feasible. It also gives information on the use case."* (P8) Others suggested thoroughly considering possible use cases and adding them to the requirements. A few participants mentioned specific, minor changes, like adding a toy version of a scheme to test attacks against or adding a participation certificate to motivate the teams and help them with their cryptographic careers.

Key Insights: Competitions' Impact.
Cryptography competitions play a crucial role in shaping research priorities, fostering collaboration, and establishing trust in new standards by attracting intense scrutiny and cryptanalysis. While competitions are seen as the best approach for securing cryptographic standards, their effectiveness depends on timing, transparency, and community involvement. **This section adresses RQ2A and RQ2B by exploring the broader impact of competitions on the cryptographic community and vice versa, and also RQ3 by reflecting on lessons learned for improving future competitions.**

6 Discussion

In this section, we discuss the implications of our findings, including recommendations for organizers and participants of future competitions and suggestions for future work.

6.1 Implications of Our Findings

Competitions were described as an overall positive experience and the best tool for developing and standardizing novel cryptography. Participants' primary motivations were highlighting their work, attracting attention to their names, and contributing their expertise to the community. Competing requires much effort and time, and rewards are sometimes inadequate. We also sought participants' views on the competition's impact, transparency, fairness, and level of security. We found that competitions significantly impact the visibility of competing cryptographic schemes and that their key feature is capturing the attention of the cryptographic community. By fostering cryptanalysis and providing feedback, the community contributes to the security of results. If the whole process is transparent, trust in the winning schemes is built by design. The fairness of the competition process is also relevant, but since the goal is to provide the best cryptography and not to decide who is the best cryptographer, it is not perceived as critical. Most participants valued transparency and feedback from the organizers and would like to see this improved in future competitions. Clear communication from the organizer's side was a frequently mentioned issue, along with stronger moderation of communication channels. Figure 3 depicts an ideal competition process as envisioned by our participants, showcasing the competition's different stages, from a need for new cryptography to the eventual adoption

of a standard, and the actions required from different stakeholders. We constructed it by grouping insights from the code categories "Designing Own Competition" and "Competition Future" and other codes that concerned criticism and improvement of current competition elements, such as the selection process and the requirements. The figure highlights that participants essentially have a shared vision of the competition process that is overall not dissimilar to the competitions they participated in but calls for more engagement of different stakeholders in, e.g., the requirement specification and standardization process. However, there are some controversial elements, such as whether requirements or schemes should be allowed to change during the often multi-year competition process. We discuss these controversies in more depth below.

Contextualizing Our Findings. Bernstein [7] provides a conceptual and critical framework for understanding competitions as a tool for information cryptography standards. He analyses historical competitions, including DES, and considers risks associated with emphasizing performance and the potential influence of state authorities, which he suggests are essential factors in future competitions. Our study empirically extends Bernstein's work. While many participants' experiences and opinions resonate with Bernstein's paper, e.g., views on trust and third-party involvement, their perspectives focus on social and organizational dynamics, motivations, and a comparison of NIST and non-NIST competitions.

Our paper extends previous work (mainly two studies of Huaman et al. [29] and Fischer et al. [26]) and may bridge standards development and broader cryptography development and adoption processes. While prior work has identified socio-technical barriers in cryptography adoption and the view of standard implementers about the usability of current standards, our work shifts focus to how the process of creating new schemes looks ahead of standardization. Some of our participants expressed that formal verification is necessary, which extends Huaman's results. Several also mentioned patents and their negative consequences when they hinder standardization efforts, unlike public and open-source resources. Our results also align with Fischer et al.'s findings about misaligned incentives; for example, funding significantly incentivizes cryptography researchers. The first step in Figure 3 refers to identifying new cryptography needs. This step is crucial because a correctly identified need with contributions from all relevant stakeholders is required to bridge the gap of misalignment, which is one of the gaps Fischer et al. mention in their work.

Competitions Have Improved Over Time. The AES competition marked a pivotal moment in the standardization of cryptography. It was the first open international cryptography competition and has served as a blueprint for modern competitions and standardization efforts. Some participants recalled AES as somewhat improvised and vaguely defined, or that the requirements for a 128-bit block size were already outdated. However, many praised its unprecedented openness, professionalism, and lasting effect on the field. Subsequent competitions have used the structure established by AES, including public evaluation and multiple rounds of feedback.

Over time, competitions have evolved in both structure and communication. Participants recognized that providing meetings, workshops, and feedback is essential for each round. Recent competitions have notably improved in these areas. Nevertheless, trust in the organizer remains central. Being a large stakeholder with enough resources, NIST continues to dominate as the most impactful and liked organizer, primarily due to its global authority and influence. Non-NIST competitions like CAESAR or NESSIE have made contributions but are seen as less influential and less visible.

In contrast to previous standardization efforts driven by open cryptography competitions, NIST's new Accordion Mode [17] project might mark an interesting shift toward a collaborative, less competitive approach. The project aims to define a new secure and flexible cipher mode and is in the phase of the requirements proposal, collecting feedback from the community. Projects such as this raise the question of balancing collaboration and competition. An optimal competition result is desirable, but the most suitable process it is not immediately clear. On the one hand, adapting and accommodating changes enables reactions to new developments and improvements on novel schemes that may otherwise have to be discarded due to easily remedied flaws. This may help foster collaboration on schemes within the cryptography research community. On the other hand, the competitive spirit and the opportunity to win recognition and renown are significant motivators for participating in competitions, investing time and effort in design, analysis, and attempting to break candidate schemes. This increased attention and scrutiny is a significant security and trustworthiness benefit of competition that is critical to maintain.

If successful, the Accordion Mode project [44], and to a certain extent also the PQC project, which shows efforts toward transparency and collaboration, could serve as a model for new standardization efforts in the future, blending collaboration, open consultation, and technical skills. We believe that organizers of future competitions should balance maintaining motivation through fair competition with allowing for revisions and collaboration to achieve an optimal solution for the underlying cryptography need.

Controversies About How Competitions Should Work. We collected insights on what participants liked and disliked about the competition process, what they would like to see improved in future competitions, and how they would design an own competition. While our results showed that competitions were perceived as a suitable format for producing cryptographic standards, we also identified room for improvement, and the participants did not always agree on the best path. Figure 3 depicts the competition process, its steps, and stakeholders as envisioned by our participants, with dashed elements representing controversial parts.

The first controversial part of the process was whether the organizer should update the requirements during a competition. Supporters of requirement updates argued that over the multiple years competitions often take, new requirements emerge, and requirements might change or become obsolete based on research advances or changing conditions in industry. They felt it was important that competitions react to such changes to produce a relevant, helpful result when the competition ends. In contrast, opponents of requirement updates believed that such changes moved the goalposts, made it hard for competing teams to plan and optimize, and unfairly altered the course of the competition. Similarly, it was controversial whether authors should be able to update their submissions based

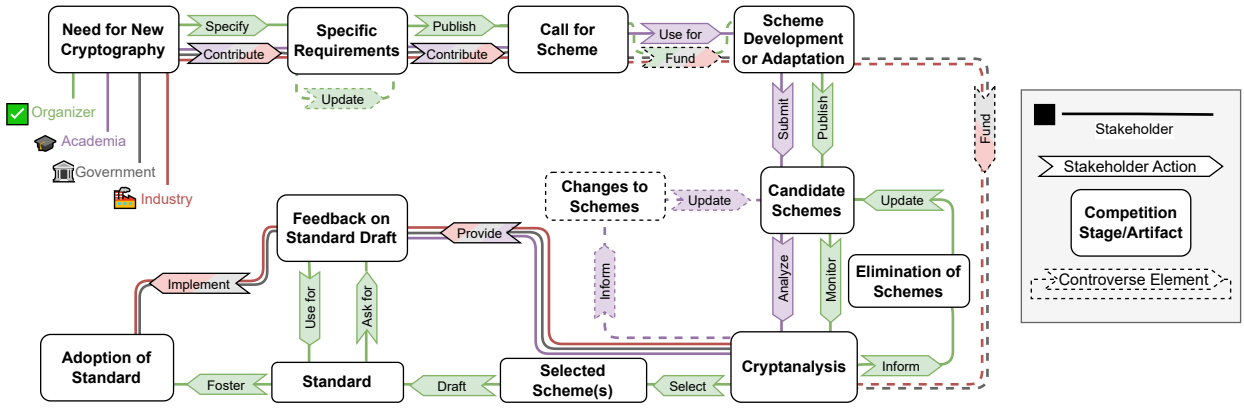


Figure 3: The ideal competition process as envisioned by our participants, with dashed elements representing controversial elements on which participants expressed opposing opinions. We present stages of the process, and the corresponding tasks of different stakeholders.

on the community feedback and cryptanalysis results they received during competition rounds, which some competitions allow. Supporters believed it was in the interest of the best possible result to allow improvements of submissions in light of new insights and collaborations to merge different submissions into a scheme that united their strengths. Opponents again felt submissions should be final to avoid unfair treatment and appropriation of other peoples' work. Both of these controversies reveal an underlying tension between providing stable and fair conditions for competition participants and adapting flexibly to changing conditions to produce the best possible resulting scheme, which proves challenging to navigate.

Another less clear aspect is how to fund competition efforts. Currently, funding for competition participation is heavily intertwined with general research funding. While we find that competitions can help to argue for funding, the associated publications do not always translate well into criteria of academic funding, such as the h-index. Competition organizers could award funding to participants. However, they might struggle to secure funding for the considerable effort required to conduct the competition in the first place. Given that the cryptography research community appears to agree that standards resulting from competitions should be freely accessible, there is an argument to be made for governments and industry to give back to the community with funding.

6.2 Recommendations and Future Work

Based on our findings, we make the following recommendations:

Recommendations to Organizers. According to our participants, the organizer of a competition and the way the competition is handled are key in determining what impact a resulting standard will have. While NIST is one of the most influential organizers we identified in our results (cf. Section 5), any organizer can take key steps to ensure the cryptography community will trust the scheme developed throughout the competition. Organizer transparency, for example through reports that describe in detail the decision-making process behind scheme selection and provide reasons for disqualifying unfit schemes, critically impacts the perception of the winning scheme. Therefore, we recommend providing well-explained reasoning for each step of the competition and ensuring good communication with its participants, especially regarding any delays and disqualifications. Even an organizer as big as NIST can generate mistrust in for any standards if reasons seem foggy or influence through an undisclosed third party like the NSA is uncovered after the announcement of a competition's results. We suggest making competitions international efforts that are open to anyone to participate in, scrutinize, and use the results. Even though some aspects of IETF standardization have been criticized for lack of clarity, tools like the IETF Datatracker [30] and mailing lists [31] provide a strong example of how transparency can be maintained by documenting every step of the decision-making process, while public mailing lists enable broad participation and scrutiny.

Our participants criticized political bias, especially in other, non-competition standardization approaches like ISO standards and competitions that restricted participation based on nationality. It might be sensible for any country's government not to rely on policy choices made abroad. Still, an international effort is a better use of limited resources. It can capture much more attention and likely achieve better security based on the increased input. It can also avoid undue or hidden political biases through transparency and equal opportunities for participation.

Discrimination of submissions, whether perceived or real, remains a complex challenge. While anonymous submissions, as used in academic peer review, might seem like a fair solution, they pose serious risks, particularly the potential for introducing undetectable backdoors or avoiding accountability. Instead, raising awareness within the community about implicit biases, and geographical or institutional favoritism, as well as reinforcing fair evaluation, can foster a more inclusive environment. Similarly, organizers need to ensure the proper conduct of participants and any reviewing researchers in official communication. Our participants reported that heated debates often break out on mailing lists, and conduct may become inappropriate as these discussions evolve. This can discourage more junior participants, who reported generally evading

contact and relying on a senior team member or outright refusing to communicate when such a senior member is unavailable. According to our participants, moderating these mailing lists to prevent personal insults or discussions from getting out of hand is nontrivial but necessary. To support this, we recommend that organizers adopt a clear and enforceable code of conduct, such as the Linux Kernel Code of Conduct [18], to provide a shared framework for acceptable behavior and formal procedures for handling violations.

Regarding more general recommendations, organizers need to ensure their goals are clear and that the requirements help achieve them. Our participants report that, in some cases, their schemes were eliminated by technicalities such as not having optimized for unconventional and presumably unspecified architectures. In other cases, entire standardization efforts failed because the field they targeted was not yet mature enough to provide satisfying solutions, e.g., in the case of the eSTREAM competition (cf. Section 2), where none of the submissions was selected due to vulnerabilities. Competitions can still advance the field in situations like these, but their impact is limited by their inability to provide ideal solutions.

Finally, we make recommendations regarding allowing other stakeholders' involvement. Organizers should provide target APIs, testing setups, and other infrastructure components to ensure participants can test their implementations and match requirements, submitting the best possible version of their schemes. In addition, we recommend that organizers require contributions that support standard adoption by industry stakeholders. This could, for example, include multiple implementations with goals like optimization and ease of implementation. For instance, Keccak (SHA-3) offers a strong precedent, with optimized, simplified, and third-party implementations with thorough documentation on its website [56]. Another approach could be to involve industry stakeholders as reviewers or to invite them to test implementations during competition rounds. By implementing these recommendations, organizers can elevate competitions and ensure that all submissions are considered appropriately, that all feedback is collected, and that the resulting standard fits stakeholders' requirements.

Recommendations for Future Participants. Our recommendations for participants mainly focus on the ecosystem of cryptography research. Participating teams must ensure they have all the required skills: To ensure optimal chances for the submission, the public-facing side, marketing their algorithm, and communicating with reviewers and organizers must be handled well. They need hardware and software experience to ensure that factors like side channels and hardware acceleration or optimization of schemes can be addressed. All teams also need clear leading positions that coordinate the effort and make decisions when individual team members disagree. Furthermore, they should be aware of the time a competition takes, often multiple years, including the development of schemes ahead of the competition and the feedback period involved in eventual standardization afterward.

Finally, submissions that are not selected can still have an impact. A unique approach has merit on account of not being broken along with other approaches with different base assumptions. NIST relies on this for the PQC Addition Digital Signatures call [43]. We also have reports of schemes used in later competitions that better fit their approach. In a more extreme case, where the competition results raised suspicions among our interview participants, schemes later got used through standard-equivalent means like IETF informationals [14]. Therefore, we believe participating in cryptography competitions is a worthwhile effort to promote research, collect feedback, and contribute to the cryptographic community.

Community Recommendations and Future Work. We recommend that the cryptography community come together, build bridges, welcome new people, and embrace a spirit of friendly competitiveness that helps push each other toward the best possible research. We believe the community should be allowed to give feedback and actively participate in designing future competition formats. To complement our results and provide further input for such a design process, future work should investigate the processes and effects of non-competition approaches, which we touched on but did not focus on and about which we can only provide limited insights. Additionally, future work could quantitatively investigate the relationship between competition transparency, trust, and result impact. Based on the practical impact of competitions, there could be applications for standardization efforts in research areas outside of cryptography. However, further research is required on how this approach could benefit other areas.

7 Conclusion

Cryptography competitions continue to be one of the most effective and trusted methods for developing secure standards with great large-scale adoption potential. In this work, we provide an in-depth, participant-centered view of the dynamics of cryptography competitions. Our interviews with experienced cryptography competitors allowed us to identify their the strengths and weaknesses of competitions. Our participants mostly viewed competitions as the best way forward, especially when well-timed, transparent, and supported by a mature community. Still, our findings reflect areas for improvement: better recognition of participants' efforts, more precise and clear communication, and stronger content moderation of the main communication channels. We also observed a shift towards a collaborative approach and a strong reliance on attention used as a precondition to trust.

Acknowledgments

We would like to thank all the participants for their time and for sharing their views with us. We also thank the reviewers and the shepherd for help improving the paper. This research was partially funded by VolkswagenStiftung Niedersächsisches Vorab (ZN3695). This work was also supported by the Grant Agency of the Czech Technical University in Prague, grant No. SGS23/211/OHK3/3T/18 funded by the MEYS of the Czech Republic. The views presented in the paper are those of the authors and do not necessarily reflect the views of any funding agencies.

References

[1] Farzaneh Abed, Christian Forler, and Stefan Lucks. 2016. General classification of the authenticated encryption schemes for the CAESAR competition. *Computer Science Review*, 22, 13–26. DOI: https://doi.org/10.1016/j.cosrev.2016.07.002.

[2] Gorjan Alagic, D Apon, D Cooper, Q Dang, T Dang, J Kelsey, J Lichtinger, C Miller, D Moody, R Peralta, et al. 2023. Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process. (2023).

[3] Gorjan Alagic, Maxime Bros, Pierre Ciadoux, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, et al. 2024. Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process. *NIST IR*, 8528.

[4] Sabrina Amft, Sandra Hölltervennhoff, Rebecca Panskus, Karola Marky, and Sascha Fahl. 2024. Everyone for Themselves? A Qualitative Study about Individual Security Setups of Open Source Software Contributors. In *In 45th IEEE Symposium on Security and Privacy, IEEE S&P 2024, May 20-23, 2024*. IEEE Computer Society. https://www.ieee-security.org/TC/SP2024/accepted-papers.html.

[5] D. J. Bernstein. [n. d.] CAESAR call for submissions, final (2014.01.27). Retrieved Apr. 11, 2025 from https://competitions.cr.yp.to/caesar-call.html.

[6] Daniel J Bernstein. 2008. The Salsa20 family of stream ciphers. In *New stream cipher designs: the eSTREAM finalists*. Springer, 84–97.

[7] Daniel J. Bernstein. 2020. Cryptographic competitions. Cryptology ePrint Archive, Paper 2020/1608. https://eprint.iacr.org/2020/1608. (2020). DOI: 10.1007/s00145-023-09467-1.

[8] Peter Y. A. Ryan, David Naccache, and Jean-Jacques Quisquater, (Eds.) 2016. *Dual EC: A Standardized Back Door. The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Springer Berlin Heidelberg, Berlin, Heidelberg, 256–281. DOI: 10.1007/978-3-662-49301-4_17.

[9] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. 2013. Keccak. In *Annual international conference on the theory and applications of cryptographic techniques*. Springer, 313–314.

[10] Hugh Beyer and Karen Holtzblatt. 1997. *Contextual Design: Defining Customer-Centered Systems*. Morgan Kaufmann Publishers Inc.

[11] Estuardo Alpirez Bock, Alessandro Amadori, Chris Brzuska, and Wil Michiels. 2020. On the security goals of white-box cryptography. *IACR transactions on cryptographic hardware and embedded systems*, 327–357.

[12] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, 2, 77–101.

[13] Alex Byers. [n. d.] NSA encryption info could pose new security risk - NIST weighs in - Rosenworcel: Refunds for long retrans blackouts. Retrieved Sept. 4, 2025 from https://www.politico.com/tipsheets/morning-tech/2013/09/nsa-encryption-info-could-pose-new-security-risk-nist-weighs-in-rosenworcel-refunds-for-long-retrans-blackouts-011574.

[14] Brian Carpenter. [n. d.] Choosing between Informational and Experimental Status. Retrieved Sept. 4, 2025 from https://www.ietf.org/process/process/informational-vs-experimental/.

[15] Florent Chabaud and Antoine Joux. 1998. Differential collisions in SHA-0. In *Annual International Cryptology Conference*. Springer, 56–71.

[16] Shu-jen Chang, Ray Perlner, William E Burr, Meltem Sönmez Turan, John M Kelsey, Souradyuti Paul, and Lawrence E Bassham. 2012. Third-round report of the SHA-3 cryptographic hash algorithm competition. *NIST Interagency Report*, 7896, 121.

[17] Yu Long Chen, Michael Davidson, Morris Dworkin, Jinkeon Kang, John Kelsey, Yu Sasaki, Meltem Sönmez Turan, Donghoon Chang, Nicky Mouha, and Alyssa Thompson. 2024. Proposal of Requirements for an Accordion Mode: Discussion Draft for the NIST Accordion Mode Workshop 2024.

[18] The Linux Kernel Community. 2025. Linux Kernel Code of Conduct. https://www.kernel.org/code-of-conduct.html. Accessed: 2025-07-25. (2025).

[19] Jolijn Cottaar, Kathrin Hövelmanns, Andreas Hülsing, Tanja Lange, Mohammad Mahzoun, Alex Pellegrini, Alberto Ravagnani, Sven Schäge, Monika Trimoska, and Benne de Weger. 2023. Report on evaluation of KpqC candidates. *Cryptology ePrint Archive*.

[20] Paul Crowley. [n. d.] Why I support the US Government making a cryptography standard weaker. Retrieved Apr. 14, 2025 from https://web.archive.org/web/20160324235504/http://www.lshift.net/blog/2013/10/01/why-i-support-the-us-government-making-a-cryptography-standard-weaker/.

[21] Joan Daemen and Vincent Rijmen. 1999. AES proposal: Rijndael.

[22] Joan Daemen and Vincent Rijmen. 2000. Rijndael for AES. In *AES Candidate Conference*, 343–348.

[23] Hans Dobbertin. 1996. Cryptanalysis of MD5 compress. *rump session of Eurocrypt*, 96, 71–82.

[24] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. 2014. Ascon. *Submission to the CAESAR competition: http://ascon. iaik. tugraz. at*.

[25] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, 1–12. https://doi.org/10.1145/3290605.3300764.

[26] Konstantin Fischer, Ivana Trummová, Phillip Gajland, Yasemin Acar, Sascha Fahl, and Angela Sasse. 2024. The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts. In *Proc. 33rd Usenix Security Symposium (SEC'24)*. USENIX.

[27] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, 1–12. https://doi.org/10.1145/3313831.3376511.

[28] Julie M Haney, Mary Theofanos, Yasemin Acar, and Sandra Spickard Prettyman. 2018. "We make it a big deal in the company": Security Mindsets in Organizations that Develop Cryptographic Products. In *Proc. 14th Symposium on Usable Privacy and Security (SOUPS'18)*. USENIX.

[29] Nicolas Huaman, Jacques Suray, Jan H. Klemmer, Marcel Fourné, Sabrina Amft, Ivana Trummová, Yasemin Acar, and Sascha Fahl. 2024. "You have to read 50 different RFCs that contradict each other": An Interview Study on the Experiences of Implementing Cryptographic Standards. In *Proc. 33rd Usenix Security Symposium (SEC'24)*. USENIX.

[30] Internet Engineering Task Force. 2025. IETF Datatracker. https://datatracker.ietf.org/. Accessed: 2025-07-25. (2025).

[31] Internet Engineering Task Force. 2025. IETF Mailing Lists. https://www.ietf.org/participate/lists/. Accessed: 2025-07-25. (2025).

[32] Jan Jancar, Marcel Fourné, Daniel De Almeida Braga, Mohamed Sabt, Peter Schwabe, Gilles Barthe, Pierre-Alain Fouque, and Yasemin Acar. 2022. "They're not that hard to mitigate": What Cryptographic Library Developers Think About Timing Attacks. In *Proc. 43rd IEEE Symposium on Security and Privacy (SP'22)*. IEEE. DOI: 10.1109/SP46214.2022.9833713.

[33] Matthias J. Kannwischer, Peter Schwabe, Douglas Stebila, and Thom Wiggers. 2022. Improving Software Quality in Cryptography Standardization Projects. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 19–30. DOI: 10.1109/EuroSPW55150.2022.00010.

[34] Team Keccak. [n. d.] Yes, this is Keccak! Retrieved Apr. 14, 2025 from https://keccak.team/2013/yes_this_is_keccak.html.

[35] Erin Kenneally and David Dittrich. 2012. The Menlo Report: Ethical principles guiding information and communication technology research. *SSRN Electronic Journal*.

[36] Gunnar O Klein. 2014. Standardization of Cryptographic Techniques–The Influence of the Security Agencies. In *IFIP Conference on History of Nordic Computing*. Springer, 321–327.

[37] Susan Landau. 2015. NSA and Dual EC_DRBG: Déjà Vu All Over Again? *The Mathematical Intelligencer*, 37, 72–83.

[38] Katholieke Universiteit Leuven. [n. d.] NESSIE - Call for Cryptographic Primitives. Retrieved Apr. 11, 2025 from https://web.archive.org/web/20010430081435/http://www.cosic.esat.kuleuven.ac.be/nessie/call/.

[39] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *ACM on Human-Computer Interaction*, 3, CSCW, 1–23, 72.

[40] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, and E Roback. 2001. Report on the Development of the Advanced Encryption Standard (AES). en. (June 2001). https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151226.

[41] NIST. [n. d.] Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA–3) Family. Retrieved Apr. 11, 2025 from https://www.govinfo.gov/content/pkg/FR-2007-11-02/pdf/E7-21581.pdf.

[42] NIST. [n. d.] Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard. Retrieved Apr. 11, 2025 from https://www.govinfo.gov/content/pkg/FR-1997-09-12/pdf/97-24214.pdf.

[43] NIST. [n. d.] Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process. Retrieved Apr. 11, 2025 from https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf.

[44] NIST. [n. d.] Proposal of Requirements for an Accordion Mode. Retrieved Apr. 14, 2025 from https://csrc.nist.gov/files/pubs/other/2024/04/10/proposal-of-requirements-for-an-accordion-mode-dis/iprd/docs/proposal-of-requirements-for-an-accordion-mode-discussion-draft.pdf.

[45] NIST. [n. d.] Status Report on the Fourth Round of the NIST Post Quantum Cryptography Standardization Process. Retrieved Sept. 4, 2025 from https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf.

[46] NIST. [n. d.] Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process. Retrieved Apr. 11, 2025 from https://csrc.nist.gov/csrc/media/Projects/lightweight-cryptography/documents/final-lwc-submission-requirements-august2018.pdf.

[47] NIST. [n. d.] Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. Retrieved Apr. 11, 2025 from https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

[48] Bart Preneel. 2010. The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition. In *Topics in Cryptology - CT-RSA 2010*. Josef Pieprzyk, (Ed.) Springer Berlin Heidelberg, Berlin, Heidelberg, 1–14.

[49] Bart Preneel. 2002. The NESSIE project: towards new cryptographic algorithms. In *3rd International Workshop on Information Security Applications, WISA*. Citeseer, 16–33.

[50] Vincent Rijmen. 2010. Stream Ciphers and the eSTREAM Project. *ISeCure*, 2, 1.
[51] Michael Rogers and Grace Eden. 2017. The Snowden disclosures, technical standards and the making of surveillance infrastructures. *International Journal of Communication*, 11, 802–823.
[52] Benjamin Saunders, Julius Sim, Tom Kingstone, Shula Baker, Jackie Waterfield, Bernadette Bartlam, Heather Burroughs, and Clare Jinks. 2017. Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & Quantity*, 52, 1893–1907. https://doi.org/10.1007/s11135-017-0574-8.
[53] Juliane Schmüser, Philip Klostermeyer, Kay Friedrich, and Sascha Fahl. 2025. "I'm pretty expert and I still screw it up": Qualitative Insights into Experiences and Challenges of Designing and Implementing Cryptographic Library APIs. In *In 46th IEEE Symposium on Security and Privacy, IEEE S&P 2025, May 12-14, 2025*. IEEE Computer Society, (May 2025). https://www.ieee-security.org/TC/SP2025/program-papers.html.
[54] Bruce Schneier. [n. d.] Will Keccak = SHA-3? Retrieved Apr. 14, 2025 from https://www.schneier.com/blog/archives/2013/10/will_keccak_sha-3.html.
[55] PQ Shield. [n. d.] South Korea announces winners of KpqC competition. Retrieved July 15, 2025 from https://pqshield.com/south-korea-announces-winners-of-kpqc-competition/.
[56] Keccak Team. 2025. Keccak Team – Cryptographic Hash Function Keccak. https://keccak.team/. Accessed: 2025-07-25. (2025).
[57] Meltem Sonmez Turan, Meltem Sonmez Turan, Kerry McKay, Donghoon Chang, Lawrence E Bassham, Jinkeon Kang, Noah D Waller, John M Kelsey, and Deukjo Hong. 2023. *Status report on the final round of the NIST lightweight cryptography standardization process*. US Department of Commerce, National Institute of Standards and Technology.
[58] Warda Usman, Jackie Hu, McKynlee Wilson, and Daniel Zappala. 2023. Distrust of big tech and a desire for privacy: Understanding the motivations of people who have voluntarily adopted secure email. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. USENIX Association, 473–490. https://www.usenix.org/conference/soups2023/presentation/usman.
[59] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. 2005. Finding collisions in the full SHA-1. In *Advances in Cryptology–CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005. Proceedings 25*. Springer, 17–36.
[60] Shikun Zhang, Yuanyuan Feng, Yaxing Yao, Lorrie Faith Cranor, and Norman Sadeh. 2022. How usable are ios app privacy labels? *Proceedings on Privacy Enhancing Technologies*.
[61] 양자내성암호연구단. [n. d.] 양자내성암호 국가공모전[KpqC 공모전] 제안요청서(Request For Proposal). Retrieved Apr. 11, 2025 from https://www.kpqc.or.kr/contents/03_exhibit/board.htmlboard_id=board_competition&mode=view&no=6&cate=.

Availability

To support research transparency and reproducibility, we provide our study materials at https://osf.io/7wkdr/?view_only=18dd1b4ba45744a99863451b7a4aae14. The materials include our interview guide, codebook, demographics questionnaire, invitation email, and consent form.

A Qualifiers

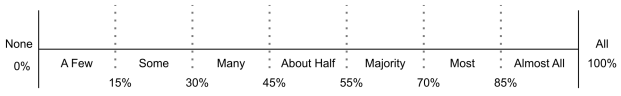


Figure 4: Overview of qualifiers and corresponding shares of the 20 participants as used in result reporting.

B Codebook

The table below presents a streamlined version of our codebook, containing the main code categories used in the analysis. While support codes, specifically Demographics and Helper Codes, have been excluded, all codes that informed the results are included.

Table 2: A simplified version of our codebook - code categories with descriptions.

Code	Description
Participants	Section 5.2 covers codes from this category.
Do It Again	Statements about participants' willingness of submitting in a competition again in the future or reasons not to.
Participants Motivation	Statements that show and describe different motivations of competing again, such as their team and community, money, showing their name and their work, research impact, or reporting having no motivation to compete again.
Participants Tasks	Reported experiences of tasks teams need to fulfill during the competition phases - preparation, submission, rounds, etc.
Organizer	Section 5.3 covers codes from this category.
Fairness	Participants evaluate fairness of competitions they experienced and talk about factors that make a competition fair or unfair.
Organizer Tasks	Summary of organizer tasks during the competition process - communication, resources, requirements, selection, standard specification. Participants also comment on tasks organizer should do.
Communication	Participants evaluate organizers' communication and content.
Missing Resources	Suggestions of resources that were not provided but could help, such as moderating communication, benchmarking facilities, etc.
Provided Resources	Comments on provided resources that helped the teams in the competition process, such as opportunities to meet, communication channels, etc.
Requirements	Evaluation of requirements of competitions, and suggestions for improvement.
Selection	Participants comment on selection criteria, risks, tasks and their consequences, and suggestions for improvement.
Standard Specification	Participants describe the late stages of competitions, their experience contributing to the final standards.
Transparency	Statements that refer to the importance of transparency, factors that influence transparency or experiences with competitions not being transparent.
Trust	Reported experiences of gaining or losing trust in competitions and the outcomes.
Trust Damage	Participants report on factors causing losing trust.
Trust Politics	Participants describe how different countries and nationality of institutions influence trust in standards.
Competitions	Section 5.4 covers codes from this category.
Community Impact	Participants describe how crypto community influences competition design and security, the effects of personal animosities and community maturity level.
Competition Future	Participants compare different competitions formats, evaluate their processes and suggest improvements.
Competition Impact	Participants assume the impact of failed submissions, and describe how competitions influence the level of security of cryptography and how competitions form the community.
Designing Own Competition	Comments on how would participants design their own competition, if they would do so.