A Qualitative Study on Ethics Perspectives in Cryptography Research

Maria Hellenthal
hellenthal@cispa.de
CISPA Helmholtz Center for Information Security
Saarbrücken, Saarland, Germany

Thorsten Helfer
helfer@cispa.de
CISPA Helmholtz Center for Information Security
Saarbrücken, Saarland, Germany

Doreen Riepel
riepel@cispa.de
CISPA Helmholtz Center for Information Security
Saarbrücken, Saarland, Germany

Annabelle Walle
walle@cispa.de
CISPA Helmholtz Center for Information Security
Saarbrücken, Saarland, Germany

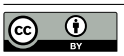
Jannik Zeiser
zeiser@cispa.de
CISPA Helmholtz Center for Information Security
Saarbrücken, Saarland, Germany

Til Dralle
til.dralle@cispa.de
CISPA Helmholtz Center for Information Security
Saarbrücken, Saarland, Germany

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

Abstract

While cryptography is often positioned as inherently pro-social, its methods and deployments can have both beneficial and harmful effects on users and society. Despite the dual-use nature of cryptographic research, it remains unclear whether the cryptographic community shares a common operational account of the ethical responsibilities its researchers adhere to. We conducted semi-structured interviews with 20 cryptography researchers, spanning theory and applied cryptography, and including junior and senior community members. Using qualitative data analysis, we examine how participants relate their research to ethics, the role of normative and ethical considerations in motivating their work, and how they reflect on the broader social and political responsibility of cryptography. Our findings indicate that ethics in cryptographic research is largely implicit, distributed, and conditional rather than explicit. Ethical considerations rarely serve as primary motivations; instead, they emerge situationally, shaped by proximity to application, and by uncertainty about downstream impact. Considerations of responsibility and public good are present but articulated unevenly across participants and contexts. Drawing on participants' perspectives, we outline actionable recommendations and community-level mechanisms, such as venue-specific guidance and repositories of exemplar cases, that encourage ethical reflection and responsibility in cryptographic research while addressing researchers' concerns about potential constraints on scientific progress.



This work is licensed under a Creative Commons Attribution 4.0 International License.
CCS '26, The Hague, Netherlands
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2871-6/2026/11
https://doi.org/10.1145/3830454.3846747

CCS Concepts

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

Keywords

Ethics, Cryptography, Qualitative, Interviews

ACM Reference Format:
Maria Hellenthal, Thorsten Helfer, Doreen Riepel, Annabelle Walle, Jannik Zeiser, Til Dralle, and Sascha Fahl. 2026. A Qualitative Study on Ethics Perspectives in Cryptography Research. In *Proceedings of the 2026 ACM SIGSAC Conference on Computer and Communications Security (CCS '26), November 15–19, 2026, The Hague, Netherlands.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3830454.3846747

1 Introduction

Cryptography research is widely perceived as pro-social, yet it has both positive and negative impacts on humans. Cryptography research output contributes to software and hardware products that can safeguard user privacy and security. This ranges from basic cryptographic primitives, such as public-key encryption and signature schemes [16, 50], to widely deployed communication protocols using those, such as the Signal secure messaging application [56], and dedicated privacy-preserving services, such as the Tor network [59]. However, those cryptographic tools can also facilitate user surveillance, censorship, exclusion, or misuse, depending on how they are designed, deployed, and governed. A prominent example emerged from the Snowden disclosures, which revealed extensive U.S. government surveillance activities and the intentional weakening of standardized cryptographic schemes such as Dual EC [12]. Cryptography is also used offensively in cybercrime, e.g., in the form of cryptographic ransomware [11], as anticipated in academic work introducing the concept of cryptovirology [66].

Does the cryptography research community reflect on these ethical tensions? In an influential essay, Rogaway [51] argues that cryptography has an inherent socio-political and moral dimension that contemporary academic cryptographers tend to overlook - not because they act unethically, but because the field has lost sight of its potential to shape society. Subsequent work echoes and extends this perspective. Some cryptographers highlight the potential of cryptography to support marginalized communities and grassroots movements [35, 52]. Similar developments are evident across the broader cybersecurity landscape, where ethical reflection, supported by frameworks such as the Menlo Principles [18], is gaining prominence but remains unevenly integrated into research practice [57].

Given this growing recognition of cryptography's socio-political implications, is it really the case that – as Rogaway reports – academic cryptographers tend to respond like "a deer in headlights, unsure what such a question could even mean" [51] when asked about their ethical responsibilities?

Our qualitative analysis of 45 cryptography papers published at USENIX Security 2025 [62] revealed an interesting pattern: while our examination of USENIX cryptography papers published between 2021 and 2024 showed that only a small number included an ethics section at all, even after the introduction of a mandatory ethics statement in 2025, many cryptography papers stated, at least implicitly, that their work raised "no ethical concerns."

Authors who discussed ethical concerns in their statements most frequently invoked ethics sections to claim social benefit and procedural compliance, especially responsible disclosure and adherence to the Menlo principles. Substantive engagement with dual-use, surveillance, or downstream harm was rare. [1]

This suggests that ethics sections may, at least in some cases, reflect compliance rather than deeper ethical reasoning, and that compliance audits alone cannot answer the deeper question of how cryptography researchers themselves understand the ethics of their work. What remains unclear, therefore, is how cryptography researchers understand ethics and responsibility beyond such formal requirements. This is critical from a security perspective, as these underlying perceptions shape how threat models are defined, risks are prioritized, and cryptographic systems are ultimately designed and deployed in practice.

To address this gap, we conducted a qualitative interview study with a diverse set of cryptography researchers. Our aim was to move beyond surface-level compliance and examine underlying ethical mindsets, perceptions of responsibility, and views on the broader impact of cryptographic research. This study is guided by the following research questions:

RQ1 *How do cryptography researchers perceive the relationship between their research and ethics?*

RQ2 *To what degree do normative and ethical considerations motivate the research trajectory of cryptographers?*

RQ3 *Do cryptography researchers consider broader social or political responsibility of their work?*

[1] All materials related to our systematic analysis of USENIX Security 2025 cryptography papers and their ethics sections, including an outline of the study and its results, the developed codebook, and the ATLAS.ti file containing the coded data, are available at: https://doi.org/10.5281/zenodo.22658755

The term *ethics* in relation to scientific research is often used in the sense of *good scientific practice* or *scientific integrity*, focusing on the trustworthiness and quality of scientific research itself. In this paper, we are additionally interested in a broader sense of *ethical considerations*: considerations involving judgments about who may benefit from a research project, which outcomes are seen as desirable or harmful, which risks are considered acceptable and for whom, and how assessments of social relevance shape research priorities. This also includes reflections on power relations embedded in technological developments and research agendas, as well as judgments about which research questions or funding sources are out of bounds.

This broad understanding of ethical considerations reflects work in philosophy of science that emphasizes the value-laden nature of scientific practice [20, 21]. It encompasses both general ethical values (such as well-being, autonomy, and justice) and more domain-specific values prevalent in cryptography and computer security, such as privacy and security. It is compatible with views in Science and Technology Studies highlighting the political and economic dimensions of technical artifacts and scientific research (e.g. Winner [64]), and with related concerns about the societal and political implications of cryptography in the contributions by Rogaway [51], Rosenbloom [52], and Kamara [35]. We do not assume or endorse any particular moral theory in this work. Rather, our aim is to capture how researchers themselves articulate and navigate ethical considerations, independent of whether these align with consequentialist, deontological, or other ethical frameworks.

Our findings show that cryptography researchers rarely articulate ethics as an explicit or guiding dimension of their work. Instead, ethical considerations tend to remain implicit and become salient only under specific conditions, such as proximity to application, deployment, or visible downstream consequences. Ethical responsibility is commonly acknowledged but framed as partial, uncertain, and distributed across communities and institutions rather than residing with individual researchers. As a result, ethical engagement in cryptography appears less as a stable orientation and more as a situational, context-dependent practice that varies across areas and research contexts.

Based on our findings we outline actionable recommendations and community-level mechanisms, such as venue-specific guidance, to encourage ethical reflection and responsibility in cryptographic research. Our work supports more systematic ethical reflection, which, in turn, can strengthen scientific outcomes by improving the anticipation of adversarial contexts, reducing dual-use risks, and supporting more robust and responsible deployments of cryptographic systems.

2 Background and Related Work

We discuss related work in two key areas: essays on ethical considerations in cryptography research and work on ethics in the broader security field.

Essays on Ethical Considerations in Cryptography Research. Rogaway [51] argued in 2015 that cryptography has an inherent socio-political and moral dimension warranting greater attention from the research community. With this statement, Rogaway has joined a long tradition of calls for attention within the cryptographic

community: Chaum [14] already warned in 1985 of private and state actors conducting mass surveillance on an unprecedented scale. He suggested cryptographic solutions that would enable society to benefit from digital communication and transactions without sacrificing privacy. Building on such work, the cypherpunk movement in the 1990s was convinced that cryptography is vital in defending social values [28]. They opposed the US government's efforts to restrict strong encryption at the time and believed in cryptography's potential to protect individuals from government overreach and authoritarian control. The WikiLeaks platform embodies the cypherpunk ethos of promoting privacy for ordinary individuals and transparency for powerful institutions [5].

Some cypherpunks' normative visions are radically anarchist or libertarian, which Narayanan [43, 44] suggests limited their broader appeal. But the normative potential of cryptographic research and technology is not restricted to libertarian dreams: Kamara [35] argues that cryptography can be highly helpful to marginalized communities, and that academic researchers can contribute by investigating threat models and solutions tailored to this purpose. In a similar vein, Rosenbloom develops a framework for cryptographers to empower grass-roots movements and marginalized people, referring to a "moral and ethical obligation of all cryptographers to understand the lived impact of their work" [52, p. 32].

Ethics in Security Research. Part of the current attitude of privacy and security researchers is reflected in the demand for ethical reflection within the community. A prominent example is the Menlo Report, developed to support researchers in the ethical assessment of their own work [18]. Although the report has since been archived by the U.S. Department of Homeland Security, calls for increased ethical scrutiny in security research have intensified: Most major security research conferences have introduced their own ethics guidelines [9, 31, 61], revised their calls for papers to explicitly require ethical considerations in submissions [63], or incorporated research ethics committees into the review process [31, 61]. Beyond institutional initiatives, there is a growing body of work examining the ethical challenges inherent in security research and the process of ethical decision-making [17, 38, 40, 48, 49]. However, the systematic study of security researchers' ethical considerations has only recently gained sustained attention. Prior work has largely focused on a limited set of specific issues [19, 26, 37].

Two recent studies are most related to ours. Zhang et al. [67] examined how ethics requirements are operationalized across top-tier security venues, surveying a predominantly Chinese researcher sample. Ramulu et al. [57] analyzed all top-tier security papers published in 2024 and conducted interviews with security researchers. Both papers arrive at the finding that researchers express concern but struggle to integrate ethical reasoning into practice. Our study differs from this prior work in three respects. First, we sample exclusively from cryptography researchers. Roughly two-thirds of that population publish in theory venues with no historical ethics-statement requirement, which is an analytically distinct setting from the above studies. Second, while Ramulu et al. identify differences in ethical engagement across security subfields and highlight cryptography as a field in which ethical concerns are discussed less frequently, our analysis reveals heterogeneity within cryptography itself. Rather than approaching cryptography as a homogeneous field, we systematically examine and identify variation between more theoretical and more applied research. Third, we triangulate our interview findings with an analysis of the required ethics sections in 45 USENIX Security 2025 cryptography papers (cf. https://doi.org/10.5281/zenodo.22658755). This combines a self-report perspective from the interviews with an artifact perspective from the ethics sections for the same community.

3 Methodology

To address our research questions, we conducted a qualitative study using semi-structured interviews with 20 cryptography researchers representing diverse areas of cryptographic research (see Figure 1 for an overview of our study methodology). In line with reproducibility best practices, we adhere to [37] and provide an open science and positionally statement at https://doi.org/10.5281/zenodo.22660582.

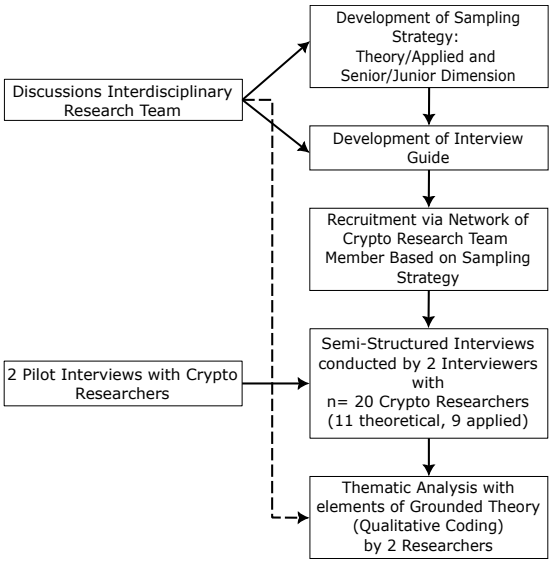


Figure 1: Overview of the qualitative research methodology.

3.1 Sampling and Recruitment

We used maximal structural variation sampling [36] to capture diverse ethical perspectives in cryptography research. We focused on two dimensions: the theory–applied research spectrum and research seniority. These were identified as the most relevant factors through extensive discussion within our interdisciplinary project team, which included researchers in cryptography, cybersecurity, psychology, sociology, and two specialists in research ethics. Together, these dimensions formed a sampling matrix with mutually exclusive cells that guided the identification of cryptography researchers for recruitment (see Table 1).

We operationalized the theory–applied dimension via a two-part categorization of cryptography-relevant iCORE A*/A-ranked venues: First, theory-oriented cryptography and computing venues

such as Crypto [8], Eurocrypt [7], and FOCS [32], and second, venues publishing more applied cryptography research or cryptography applications such as CCS [2], IEEE S&P [33], and USENIX [62] (see the full list of conference venues used in Appendix A). We measured research seniority by the span of publication activity, classifying researchers as senior if they had published for more than seven years and as junior if they had published for seven years or less. We chose the 7-year threshold as a cutoff to distinguish researchers in the typical duration of a PhD/postdoctoral phase from those who have transitioned to more senior roles such as (junior) Faculty positions.

To populate the sampling matrix, we used the Australian CORE conference ranking[2] to quantify publication activity across computing disciplines for researchers who had published at least one cryptography-related paper(s) since 2020. Using the CORE venue classifications, we aggregated publication counts for theory-oriented and applied-oriented venues. Based on the total number of publications and their scores for each venue category, we calculated a publication-orientation score for each researcher. This score was used to classify researchers as:

- Theory-focused: Participants with more than 70% of publications in core cryptography and theory venues
- Applied-focused: Participants with more than 60% in applied venues and "Go-between" participants with a balanced distribution (40–60%) across theory and applied venues

We adjusted these thresholds to ensure adequate representation in each recruitment matrix cell. The Go-between group was included to see whether researchers who publish equally in theory and applied venues exhibit distinct ethical perspectives. However, due to recruitment constraints and the absence of meaningful differences between these participants and applied-focused researchers, we did not treat this group as distinct in the final analysis and included the group in the applied-focused condition.

We calculated research seniority from publication history by comparing the earliest and most recent publication years, both overall and for cryptography-related publications. During this process, we observed that a substantial number of researchers had published in other research fields prior to their first cryptography-related publication. Rather than excluding these individuals, we retained them as a distinct and analytically relevant group, as their prior disciplinary background may contribute to the transfer of ethical perspectives from one research domain to cryptography (Senior-Juniors in Table 1).

Initially, we contacted researchers identified through the sampling matrix via unsolicited email invitations. Due to a very low response rate, we subsequently adapted our recruitment approach. Specifically, we contacted researchers from the sampling list from our professional network – primarily through the cryptography researcher in the author group – using more personalized email invitations. To mitigate potential bias, we deliberately selected participants from a broad professional network spanning multiple institutions and research groups, rather than recruiting primarily from a single academic circle. This approach aimed to reduce the risk of over-representing shared research cultures or ethical perspectives. In the end, we successfully recruited 11 theory-focused participants and nine security/applied-focused researchers.

[2]see https://portal.core.edu.au/conf-ranks/

Theory/Applied Spectrum	**Research Seniority**			
	Senior	Senior-Juniors	Junior	**Total**
Theory-focused	5	2	4	11
Applied-focused	2	4	3	9
Total	7	6	7	20

Table 1: Sampling Matrix and Participants Recruited. Senior-Juniors are senior researchers in other fields of research (> 7 years experience) than cryptography and juniors in cryptography research (≤ 7 years experience)

3.2 Interview Guide and Procedure

The guide for the semi-structured interviews was designed to allow ethical topics to emerge spontaneously, without initial prompting. Participants were not informed in advance that the study focused on ethics; instead, the interviews were introduced as an investigation of the practices and motivations of cryptography researchers.

In the initial phase of the interviews, we began with questions about participants' backgrounds, what cryptography is from their point of view, their key research questions, project selection criteria (including how they assess project relevance and impact), and motivations for conducting cryptographic research.

In the second phase of the interview we addressed ethical considerations explicitly by asking participants whether they viewed their research as contributing to the public good, whether researchers should select projects accordingly, what boundaries they would not cross in their work, how they understood ethics in cryptography research, and whether ethical implications influence their project choices. We began the second interview phase with questions about the public good before explicitly asking about ethics, to assess how participants naturally articulate values and responsibilities in their own term and whether they held implicit ethical motivations for conducting cryptography research. This ordering was intentional to avoid priming participants with the term "ethics," which may carry different interpretations and to better distinguish implicit ethical reasoning from more explicit, post hoc accounts.

In addition, we developed four vignettes that presented hypothetical but realistic scenarios representing ethical dilemmas, such as how participants would proceed if they were to break a widely used encryption scheme (the interview guide can be found at at: https://doi.org/10.5281/zenodo.22663229. The vignettes were intended to make ethical issues more accessible, particularly for participants who had not previously extensively reflected on ethics and might otherwise have found the topic difficult to articulate. We presented the scenarios to participants both visually and verbally, encouraged them to reason through the vignettes, and asked follow-up questions where we felt more context was needed.

The interview guide, including the vignettes, served as a flexible roadmap for the interviewers, allowing questions to be adapted to

each participant's characteristics. Depending on the flow of the interviews, we occasionally added or omitted questions. For instance, we did not present a specific vignette to a participant if they had already elaborated on the issue in a different context. The guide was piloted in two interviews with cryptography researchers from our institution. As these researchers met the sampling criteria and we identified no systematic differences between the pilot interviews and subsequent interviews, we included the pilot interviews in the final data set and analysis. Following the pilot and throughout data collection, we refined the interview guide only minimally. While an adaptive approach is consistent with established methodological recommendations for qualitative interviewing [27, 39, 65], the core questions remained unchanged, and refinements were limited to minor rephrasing and adding sub-questions.

The interviews were conducted remotely between August 2025 and January 2026 and lasted approximately 60 minutes each. Prior to each interview, participants completed an online questionnaire that included informed consent and basic demographic information. All interviews were audio-recorded and transcribed using an in-house AI-based transcription tool based on OpenAI Whisper [46]. The interviews were conducted in English by two researchers - a psychologist and a cryptography researcher. All transcripts were anonymized by removing personal identifiers and institutional and country-specific information. As compensation, we offered all participants an Amazon Gift Card or a PayPal transfer worth $25. Furthermore, the responsible ERB for our institution reviewed and approved our study procedure (a detailed description of this study's ethical considerations can be found at https://doi.org/10.5281/zenodo.22660582).

3.3 Data Analysis

Our analysis combined a top-down approach based on Qualitative Content Analysis [41, 54, 55] with inductive, bottom-up elements inspired by Grounded Theory [13, 24, 58]. An initial coding scheme was derived from the interview guide questions, reflecting the issues participants were explicitly asked to address. To avoid reducing the richness of the data to predefined categories alone, we additionally allowed new codes to emerge inductively through an open-coding process. This hybrid approach enabled us to systematically identify recurring patterns and themes across the interviews. The top-down component was used to derive codes aligned with the interview guide and to obtain direct, structured answers to our interview guide questions. Complementarily, the bottom-up component enabled us to capture emergent phenomena and interpretive themes that were neither explicitly anticipated nor directly prompted by specific interview questions. Together, these approaches allowed us to surface novel insights while situating them within a broader framework defined by the initial coding structure [53].

Two researchers with backgrounds in psychology independently coded the same five interview transcripts to identify text segments relevant to the research questions. To ensure consistency and address interpretive differences, the researchers then engaged in iterative discussions to compare, refine, and align their coding, adapting codes as needed to establish a shared analytical understanding. We did not calculate inter-coder reliability metrics due to the exploratory and partially inductive nature of our study [42]. Instead, we employed a consensus coding approach, in which coding decisions were discussed and iteratively refined until near-complete agreement was achieved - an established practice in qualitative research of this kind [4, 25].

Following this initial phase, we conducted several rounds of descriptive and thematic coding, progressively grouping open codes into broader thematic categories. Through this iterative process, we progressively developed more abstract analytical categories that captured central themes and patterns in the data, resulting in a preliminary codebook. The emerging themes were discussed with two experts in ethics research, who contributed additional interpretive perspectives and helped refine the analytical framework.

The preliminary codebook was then applied to four additional interviews, during which it was further tested, refined, and expanded to incorporate previously omitted or insufficiently specified codes, improving coverage of the data. The resulting codebook was then applied to the remaining 11 interviews and slightly adjusted in response to these data. Last, we used the finalized codebook (please find it at: https://doi.org/10.5281/zenodo.22663229) to reanalyze the first nine interviews. All coding and analysis were conducted using ATLAS.ti [10].

We conducted interviews until all cryptography clusters in our sampling matrix were represented and the analysis indicated thematic saturation with respect to the research questions. To assess saturation, we examined whether newly analyzed interviews introduced novel themes or issues that were not present in the existing data. Once these interviews largely reinforced previously identified themes rather than introducing substantively new ones, we considered thematic saturation to have been reached. We also constructed a comparative matrix to extract research question–relevant information from each interview, enabling systematic comparison and the identification of similarities and differences in how individual researchers addressed the focal issues of this study. Regarding the vignettes, we integrated the elicited themes into the overall analysis, as they largely corresponded to participants' broader ethical reasoning.

3.4 Limitations

Some limitations and biases are typical of interview studies and apply to our work. Below, we discuss three that materially shape the interpretation of our findings.

Sampling and Recruitment. Cold outreach to researchers in our sampling matrix gave us a very low response rate. We therefore recruited primarily through our professional network, using personalized invitations. Hence, no participant was entirely unknown to the research team. To mitigate the risk that a single research culture would dominate our results, we drew on diverse institutions, sub-areas (from theory to applied cryptography), and career stages (from junior to senior). The breadth of perspectives we observed suggests network bias did not constrain thematic coverage.

Generalizability Across Geographies and Demographics. Two participants in our sample identified as female. While this skew reflects the current gender distribution of senior cryptography research, it clearly limits the insights into gendered experiences of ethical reasoning. Future work should intentionally oversample women and gender-minority cryptography researchers to collect

insights into gendered experiences of authority, mentorship, and ethical disagreement. Overall, we recruited participants working in nine countries. When asked about geographic variation in ethical considerations, they reported no notable differences. The international nature of academic cryptography research and the use of English throughout may both contribute to these findings.

Not Disclosing Study Focus. We did not disclose our study's ethical focus during recruitment and presented the interview as an investigation of general research motivation. To limit participant priming, we withheld the word *ethics* until the second interview phase. However, our four vignettes made ethical concerns concrete for participants who had not previously reflected on them. Participants were debriefed after the recording ended. However, a small risk remains that participants inferred the ethical focus during the interview and adjusted their responses accordingly.

4 Results

Below, we report the findings of our interview study with cryptography researchers on their perspectives on ethics in their work. To report our qualitative findings, we use quantifiers (see Table 2).

1-3	4-7	8-11	12-15	16-20
A few	Some	Several	Many	Most
0% 15/20%	35/40%	55/60%	75/80%	100%

Table 2: Quantifiers used to report our qualitative findings

4.1 Participant Demographics

Participants in our study (n = 20) were between 28 to 60+ years old. Two participants identified as female, while all others identified as male. Participants were employed at institutions across nine countries in Asia, Europe, and North America and reported 4 to 30+ years of experience as cryptography researchers. We present selected participant demographics in Table 3. To minimize the risk of participant deanonymization, not all demographic variables are reported or linked to a participant in Table 3. For example, information on the countries or continents in which researchers were employed at the time of the interviews is omitted, as in some cases there may be only a small number of cryptography researchers within a given country publishing in A*/A-ranked venues, increasing the risk of identification.

Apart from one notable exception, no systematic differences emerged in the data based on research seniority and geographic information. The exception concerned very senior researchers with more than 20 years of experience, who tended to take a more complex perspective, manifesting in more explicit and unprompted elaborations of ethical considerations in their research. While we do not stratify our analysis by years of experience, we occasionally note this distinction where relevant. Regarding geographical differences, in addition to having an international sample, we specifically asked participants with international careers whether they had observed differences in ethical practices across countries. Participants reported no meaningful differences, with some suggesting that this similarity may reflect the international nature of academic careers and research practices. In light of this and the absence of systematic geographical differences in our data, we did not pursue geography as a distinct dimension of further analysis. Last, when participants were asked to position themselves on the theory–applied spectrum, their self-assessments largely aligned with their placement in the sampling matrix (see Table 3).

Our findings indicate that ethics in cryptographic research is largely implicit, distributed, and conditional rather than explicit. Below, we unpack and substantiate this high-level observation across multiple analytic dimensions.

Participant	Gender	Research Orientation (sampling/self-reported)	Seniority
P01	Male	Applied/Applied	Sen-Jun
P02	Male	Theory/Theory	Sen
P03	Male	Theory/Theory	Sen
P04	Male	Theory/Theory	Sen-Jun
P05	Male	Theory/Theory	Sen-Jun
P06	Male	Applied/Applied	Jun
P07	Male	Theory/Mixed	Sen
P08	Male	Applied/Applied	Jun
P09	Female	Applied/Applied	Sen-Jun
P10	Male	Theory/Theory	Jun
P11	Female	Theory/Theory	Jun
P12	Male	Applied/Applied	Jun
P13	Male	Applied/Applied	Sen
P14	Male	Applied/Applied	Sen-Jun
P15	Male	Theory/Theory	Jun
P16	Male	Applied/Applied	Sen-Jun
P17	Male	Theory/Mixed	Sen
P18	Male	Theory/Theory	Sen
P19	Male	Theory/Theory	Jun
P20	Male	Applied/Applied	Sen

Table 3: Participant Demographics

4.2 Ethics was not Often the Starting Point in the Interviews

Although there were a few exceptions, ethical considerations rarely emerged spontaneously as a topic of conversation during the initial interview phase when we did not explicitly prompt for them. Ethical considerations were largely absent when we asked participants to describe cryptography research and its primary goals. While some participants characterized cryptography as concerned with protecting privacy or ensuring security, these statements were typically framed in technical or functional terms rather than as explicit ethical commitments.

For some participants, however, ethical considerations became more evident later in the interviews, unprompted, particularly in more specific questioning about how they decide whether a research project is sufficiently relevant to pursue and how they assess the impact of their work. For example, when reflecting on criteria for project relevance, one participant mentioned deliberately avoiding research on *key-escrow* and related chat-control mechanisms, citing ongoing political debates and personal reservations about working on such topics.

	Participant	Explicit ethical considerations without cue	Explicit ethical considerations when cued	Considers ethical implications of research projects	Ethical engagement beyond individual research	Ethics heatmap
Applied	P01	●	●	●	○	
	P06	○	●	●	○	
	P08	○	●	●	○	
	P09	●	●	●	●	
	P12	●	●	●	○	
	P13	●	●	●	●	
	P14	○	●	●	●	
	P16	●	●	●	○	
	P20	○	●	○	○	
Theory	P02	○	○	○	○	
	P03	○	○	○	○	
	P04	●	●	○	○	
	P05	○	○	○	○	
	P07	●	●	●	○	
	P10	○	○	○	○	
	P11	○	●	○	○	
	P15	○	●	●	○	
	P17	●	●	○	○	
	P18	○	○	○	○	
	P19	○	●	●	○	



Table 4: The table captures when ethics entered the conversation and the forms of ethical engagement reported. The accompanying heatmap visualizes the relative salience of ethical reflection expressed during each interview. Each tick represents one indicator and contributes one point to the heatmap score, ranging from 0 (no indicators present; lightest shade) to 4 (all indicators present; darkest shade). Indicator presence was determined through qualitative coding and discussed by two researchers.

Some participants mentioned ethical considerations only when directly prompted by questions about whether their research contributes to the public good. Their responses suggested that although ethical considerations were not at the top of their mind and did not arise spontaneously, participants still engaged with the topic reflectively, indicating that they had previously considered the ethical aspects of their research. In contrast, some participants' responses suggested that ethics was neither a relevant consideration in their research practice nor had been in the past. These participants often struggled to articulate views on social good or ethics. Notably, in a few cases, responses to questions about their understanding of ethics conveyed considerable uncertainty, with participants struggling to formulate or elaborate on an answer. Table 4 provides an overview of participants and the relative salience of ethical considerations in their interviews.

More generally, how and when participants first engaged with ethical concerns in the interview strongly indicated the depth of their subsequent ethical reflections and engagement in their work. Participants who raised ethics unprompted early on engaged more extensively with ethical questions throughout the interview and demonstrated that ethical reflections were already part of their thinking, whereas those who addressed ethics only when prompted tended to provide briefer and more limited responses later on and generally expressed less influence of ethical considerations in their research practices.

> **Key Insights: How and when participants first engaged with ethical issues in the interview was a strong indicator of the depth of their subsequent ethical reflections and engagement in their work.**

4.3 Ethics is Rarely the Primary Driver of Researcher Motivation

Explicit ethical reflections were rarely our participants' initial motivation for their research and do not function as a driver for entering the field or choosing research topics. Only some participants explicitly stated that ethical considerations, such as the broader moral or societal implications of their work, were a core motivation for conducting their research or for shifting their research focus over the course of their careers:

> *"R: ...I think today I would say the motivation is actually still coming from real-world applications. So I would consider myself, maybe call it a real-world cryptographer. So not so much*

> *on the theory side, but really trying to understand how cryptographic systems work in the real world and how we can improve them (...). But so I still find it very fascinating. And the idea that cryptography allows the common people to protect their communications from extremely powerful adversaries, I still find it extremely cool.*" — P13

Rather than being driven by explicit ethical considerations, research motivation and topic choice were primarily shaped by:

Interest and Curiosity. Most interviewees stated that their engagement in cryptographic research was interest- and curiosity-driven, describing it as one of the strongest motivators for their work. This included the desire to explore new ideas, pursue research for fun, and transform ideas into tangible results. Participants selected research projects based on their personal interests, previous work, or existing knowledge, while consciously avoiding topics they found tedious or unappealing. Their engagement was also fueled by the intellectual challenge of the work and a pronounced need for cognition. Participants reported being motivated by the satisfaction of thinking deeply, solving complex problems, and understanding intricate cryptographic systems. For some, the freedom afforded by career stability, such as a tenured position, allowed them to take risks on high-interest questions, and one participant reported pursuing cryptographic research even in their leisure time, reflecting the deeply personal and curiosity-driven nature of their motivations.

Practical Applicability. Many participants emphasized practical applicability and real-world impact as key drivers for their research. They often selected topics and projects based on the potential to transfer cryptography theory to applications, achieve short-term or tangible impact, or target relevant protocols and realistic cryptanalytic attacks. Practical relevance was also linked to industry needs and the balancing of security and efficiency in applied contexts. Some participants described applied research as a way to bridge theory and real-world application, emphasizing that the possibility of concrete application or economic benefit shaped their work. A few researchers mentioned societal protection as a central consideration. However, in general, practical applicability was mentioned in the context of other goals, such as visibility, adoption, and real-world use, rather than explicit ethical goals.

Career and Structural Factors. Some participants described how the academic system incentivizes publication, with researchers feeling pressured to produce results quickly or align their research with topics that support funding opportunities. Job security and long-term employment also influenced project selection, with a few participants choosing research areas based on career prospects, funding availability, or alignment with institutional priorities. For example, post-quantum cryptography was sometimes pursued due to PhD funding opportunities, while other research topics were selected to address existing research gaps or capitalize on overlapping expertise. In this context, practical and scientific interests were sometimes secondary to structural drivers such as career advancement, job stability, and funding constraints. This finding is somewhat illustrated in a statement of P08:

> *"I also kind of, I guess it's hard to say exactly why I work on certain things, but there are different motivations sometimes, like, I guess it's a complicated question, like, working, like, sort of, publish, there's like this sort of pressure to sort of publish that some people feel more or less. And so sometimes you work on problems that you think you can solve, like, in not too much time. Like, so, like, using sort of tools that you know, and so sometimes there's that. Sometimes it's, like, so there's sort of an efficiency element to working to some extent, I find.*" — P08

Social and Community Impact. A fourth motivation stemmed from social and community impact in the research environment. Several participants described how collaborations, supervisors, or student interests guided their choice of research topics, with project relevance shaped by discussions within their teams or the broader community. A few participants emphasized that being part of an interdisciplinary, and collaborative environment motivated them to pursue certain topics. Overall, colleagues, students, and the wider community played an important role in directing attention toward specific problems and sustaining engagement.

> **Key Insights: While there were exceptions in our data set, explicit ethical reflections rarely motivated participants to conduct cryptographic research and were not reported to be drivers for entering the field or choosing research topics.**

4.4 Ethics is Triggered by Proximity

More explicit ethical considerations in cryptographic research seem to enter the reasoning process later, after the primary motivating factors, when research engages with tangible consequences, applied contexts, or user-facing outcomes.

Several interviewees reported that researchers in applied or security-focused areas tend to be more ethically aware, discussing potential misuse and societal consequences. The degree of explicit ethical reflection also depends on the specific research question and context. Ethical considerations are most visible in projects where consequences can be anticipated - when research might influence deployed systems, industry adoption is foreseeable, or policy implications are explicit. In applied fields, responsibility is more readily felt, and ethics is considered in design decisions or when evaluating disclosure.

By contrast, ethical considerations received less attention by our more theoretical cryptography participants, where the potential for misuse is less obvious, the practical impact is harder to judge, and technical and ethical discussions are rarely combined. In this context, ethics is rarely considered during peer-review, and perceived as irrelevant to the work as illustrated in a statement of P02 when being asked what their understanding of ethics in cryptographic research is:

> *"Right. So, the next question for me is that, I think, I don't have to ask myself the question, right? I do theory. I publish, like, theorems, you know, I never code anything. I will not break things or, like, influence by, like, deploy something that's insecure by mistake or something like that. Right. I mean, it's kind of a weird setting.*" — P02

In more theory-driven cryptography research, projects are often conducted *in a bubble*, with few social or political considerations, and little expectation that ethical responsibility should guide the work.

> **Key Insights: Explicit ethical reflections in cryptographic research are situational and contingent, emerging primarily when research is sufficiently close to application or deployment, or involving**

visible societal downstream consequences, and varying strongly across areas and communities within the discipline.

4.5 The Theory–Applied Spectrum Structures Ethical Awareness

In alignment with the previous section, our analysis indicates that the theory–applied spectrum constitutes the strongest organizing dimension shaping how ethical considerations are articulated across interviews. Researchers oriented toward applied cryptography were more likely to mention ethical aspects unprompted and to consider ethical implications when selecting research projects. At the extreme end of the spectrum, this manifested in a high level of ethical engagement that extended beyond individual research projects, including the involvement in official letters to government bodies about cryptography-related concerns or explicitly integrating ethical reflection into teaching, for example, by assigning Rogaway's paper to students. By contrast, theoretical researchers more frequently struggled to address ethical questions and often described ethical considerations as distant, neutral, or irrelevant to their work. At the end of this spectrum, a few interviewees appeared overwhelmed by questions about ethics and explicitly rejected the notion that their work entailed any ethical responsibility beyond standard scientific practice.

At the same time, our data reveal important exceptions that indicate the influence of additional factors beyond the theory–applied spectrum. In particular, the specific research topic within an area emerged as a relevant moderating factor. For example, one participant who predominantly publishes at security conferences and identifies as an applied researcher nevertheless reported little engagement with ethical considerations, emphasizing that their algorithmic work had no direct application or immediate impact. Conversely, a few researchers who primarily published at theory-oriented venues demonstrated substantial ethical awareness due to sustained interest in applied research within the field of cryptography, frequent interaction with applied researchers, or long-standing personal engagement with ethical questions. In these cases, however, ethical reflection was not closely tied to their specific research and rather presented a general interest.

Finally, our data suggest that seniority may play a complementary role in shaping ethical reflection. Participants with more than 20 years of experience consistently articulated more complex, reflective, and experience-based perspectives on ethics. This appears to be less influenced by the research area alone and more related to career stability and long-term exposure to real-world consequences, which may enable senior researchers to take a broader perspective on the societal implications of their work.

Key Insights: The position on the theory–applied spectrum seems to strongly indicate ethical awareness and engagement, with applied researchers being more likely to engage with ethical considerations. Moreover, additional factors, such as specific research topics, personal engagement with ethics, and researcher seniority, appear to influence ethical reflections.

4.6 Public Good is Deferred Rather Than Decisive

A few participants explicitly stated that their own research does not primarily contribute to the public good - describing its benefits as flowing mainly to companies or to relatively narrow expert communities downstream. This is illustrated by P06:

> *"Maybe not to the public, but, to a small community. I guess like, I mean, you have a community and then there's people that, you look up to into, in the community and you, you know, you try to do work that, other people in the community who you look up to would, would think is, is good work..."* — P06

However, most interviewees expressed a general belief that their work, and cryptography as a field more broadly, contributes to the public good. This view was shared by both theory- and applied-focused participants. At the same time, our data indicate variation in how participants articulated their contribution to the public good. Rather than functioning as a clearly defined evaluative criterion, participants typically situated their research at different distances from application with corresponding downstream societal impact.

Public Good as Societal Protection and Practical Impact. For about half of the participants, contributing to the public good was closely associated with societal impact, security, and the protection of users in concrete contexts. These interviewees framed cryptographic research as serving the public good by enabling secure and private communication, protecting common people from adversaries, and safeguarding digital infrastructure. Examples included work on secure messaging, end-to-end encryption, post-quantum security, and standards development. Some emphasized privacy as a fundamental human right and described cryptography as a practical solution for protecting private data, securing everyday communication tools, or preventing large-scale infrastructure failures. Even when potential negative impacts were acknowledged - such as tensions around end-to-end encryption - these were often positioned as secondary to an overall sense of providing security or societal benefit.

Public Good as Advancing Knowledge and the Field Itself. Some participants articulated a more epistemic understanding of the public good. For them, contributing to the public good meant advancing theoretical knowledge, strengthening the cryptographic field, and contributing to academia or the cryptographic research community. In this view, research serves the public good by expanding understanding, producing publishable results, supporting teaching, and maintaining open science practices, regardless of whether immediate applications or societal effects are visible.

Public Good as a Difficult or Indeterminate Concept. Some participants explicitly stated that the public good is difficult to define. Some expressed concerns about differing moral views, political reinterpretation, or the risk of restricting research agendas by imposing narrow or immediate notions of social benefit. A few questioned whether research should be evaluated primarily through the lens of public good at all, emphasizing that predicting societal impact is inherently uncertain.

The Public Good as Deferred and Conditional. Across interviews, even when participants expressed confidence that cryptographic research contributes to the public good, this contribution was rarely described as immediate or direct. Importantly, these

reflections emerged both when participants discussed their own research and when they were asked whether other researchers should consider the public good when choosing research topics. In both contexts, contributions to the public good were typically framed as deferred, indirect, and conditional on developments beyond the individual researcher's control. Many participants emphasized that research precedes adoption and that societal benefits depend on whether ideas are implemented, standardized, or adopted by industry, policymakers, or other downstream actors. As a result, contributing to the public good was often described as a potential rather than an assured outcome. Interviewees highlighted the difficulty of predicting which results would ultimately be deployed, how they might be used, and whether they would have positive or negative effects in practice. Some stressed the importance of a long-term perspective, noting that cryptographic ideas may take years or even decades to materialize in real-world systems, if at all.

This temporal distance from application shaped normative expectations about responsibility. Most participants agreed that theoretical and foundational cryptography research does not and should not have to be guided by considerations of immediate public good. When asked explicitly whether researchers should take public good into account when choosing research topics, interviewees consistently emphasized the legitimacy and necessity of curiosity-driven, foundational work, even without clear societal impact.

> **Key Insights: While most participants stated that cryptographic research does and should contribute to the public good, this contribution is understood in diverse, indirect, and often delayed ways, leaving the public good as a background justification rather than a concrete criterion for research choices.**

4.7 Ethics Means Different Things

When specifically asked about their understanding of cryptography ethics, participants did not converge on a single, shared interpretation of what "ethics" means. Instead, two dominant interpretations emerged - ethics as research integrity and ethics as societal impact - alongside a small number of more specific interpretations.

Ethics as Research Integrity and Good Scientific Practice. One prominent understanding frames ethics primarily in terms of scientific integrity and good research practice. In this view, ethics was associated with honesty, rigor, transparency, responsible disclosure, peer review, (mandated) ethics statements, and open science practices. Some participants emphasized adherence to established norms of scientific conduct, while a few argued that ethical behavior is already deeply embedded in cryptographic practice, much as in other areas of research. When asked about ethical considerations in their work, a few theoretical researchers explicitly referred to following good scientific practice standards, such as careful verification of results, rather than reflecting on broader societal consequences. This finding is illustrated in a statement of P11:

> *"I actually have to say that I, given that I'm so theoretical, I don't think so much about the ethics of the content of my research. To be very honest, like if, like, as I said, everything is online. If people read it, they will understand that I'm not like doing research on people. I, it's like, it's only mathematical objects. I don't think that there's a big ethic problem. What I think, the ethics questions I actually run over most time in my everyday life are more the way how we do research. Like, how, like, how do we talk to each other, like the way when we do reviews, what reviews do I accept on concurrent work..."* — P11

Ethics as Societal Impact. A second, distinct understanding framed ethics in terms of societal impact and broader consequences of cryptographic research. Here, participants referred to issues such as public good, power asymmetries, surveillance, misuse, responsible disclosure, political implications, and downstream social effects. Unlike integrity-based ethics, this interpretation was often described as subjective, difficult to predict, or beyond individual control, particularly in highly abstract or foundational research. Most interviewees held this view, emphasizing uncertainty about how cryptographic work might be used or misused and expressing ambivalence about personal responsibility for future outcomes.

Other Interpretations. Beyond these two dominant framings, a few participants associated ethics with other or more particular meanings. In one case, ethics was linked to experiences of corruption within a researcher's institutional environment, without reference to other aspects of research integrity or broader societal impact. A few theoretical researchers who struggled to articulate ethical considerations in relation to their own work referred to responsible disclosure as one of the few situations in which ethics might play a role at all. One participant explicitly highlighted open science procedures as a central ethical concern, emphasizing transparency and accessibility over questions of impact or misuse.

> **Key Insights: These findings suggest that ethics is not understood as a unified concept, but rather in partially overlapping ways that vary across individuals and areas. As a result, some researchers may perceive themselves as already addressing ethical responsibilities through established scientific practices, even in the absence of explicit engagement with broader societal or political considerations.**

4.8 Ethical Boundaries Exist, but Mainly as Red Lines, not Guiding Principles

We asked participants if there were certain things that they would never do in their research regardless of the potential benefits. Participants articulated a range of situations in which they would not engage in certain types of research, but these limits were typically framed as exceptional cases rather than as criteria shaping everyday research decisions.

Common Refusal Zones and Harm-Based Boundaries. Across interviews, we identified different "red lines" that participants would refuse to cross, primarily motivated by concerns about direct harm to people. These included refusing to build cryptographic backdoors, opposing projects that enable mass surveillance or censorship, and declining research perceived as harming the public. A few participants explicitly stated to reject work connected to war-oriented applications, military projects that could harm civilians, or non-disclosure arrangements tied to military funding.

Integrity- and Methodology-Based Boundaries. In addition to harm-based refusals, participants described ethical boundaries grounded in scientific integrity and research methodology. These included refusing to fabricate or manipulate data, resisting unethical academic practices despite personal or career costs, and

adhering to standards of good scientific practice. Practices such as reproducibility requirements, artifact submission, and open science - particularly in applied cryptography venues - were framed as concrete ethical safeguards already embedded in the field.

Military, Political, and Intellectual Property Boundaries. Ethical boundaries also emerged around military and political involvement. While views varied, some participants expressed discomfort with direct military collaboration, political interference, or privacy-undermining uses. A few described mixed feelings about military use of cryptographic research, noting that acceptance of defense funding depended on context, transparency, and intended use. Others opposed patents and proprietary restrictions, particularly when these limited public benefit or enabled harmful applications.

Absence, Vagueness, and Hypothetical Boundaries. While most participants were able to articulate ethical red lines when explicitly asked to reflect on their boundaries, the majority of these limits referred to hypothetical scenarios rather than lived decisions. Several interviewees reported that they had never actually refused a research project on ethical grounds and many explicitly stated that they did not perceive ethical dilemmas in their work. Several participants did not consider ethics when choosing projects or did not know whether their research would ultimately be used for malicious purposes. Others described ethical boundaries in vague or abstract terms, confining themselves to situations such as avoiding ill-defined grey zones or complying with standard human-subject protections.

> **Key Insights: Ethical boundaries exist, but they are mainly invoked in exceptional situations involving visible harm, integrity violations, or political entanglements, rather than functioning as guiding principles in everyday research practice.**

4.9 Researchers Recognize Responsibility, but Place Clear Limits on it

Across interviews, most participants demonstrated awareness of dual-use risks and potential downstream harm. For a few participants, this awareness emerged early in the interview; for most, it became explicit when ethical questions were raised, and for a few only when discussing the vignettes. Across these contexts, interviewees acknowledged that cryptographic research can be misused, that some technologies have ambiguous effects, and that outcomes may involve both positive and negative consequences. This awareness extended to concerns about surveillance, law enforcement use, blockchain applications, funding from private organizations, and the broader political and societal implications of cryptographic systems. At the same time, a few participants emphasized that misuse of cryptography is unavoidable and that, overall, cryptographic research tends to contribute more to the good than to the bad, even when negative impacts are possible. Participants provided several considerations that substantially qualified individual responsibility:

Responsibility as Conditional and Distributed beyond Individuals. Ethical responsibility was commonly described as conditional rather than absolute. Participants argued that responsibility increases when consequences are directly connected to researchers' actions - for example, in cases of negligent behavior, unethical disclosure, or avoidable harm. By contrast, when outcomes are indirect, mediated through downstream actors, or temporally distant, responsibility was viewed as limited. In this context, the collective nature of cryptographic research and deployment, involving research communities, industry partners, standardization bodies, governments, and users, was highlighted. In this view, individual contributions were often seen as too small or too embedded within larger, socio-technical systems to warrant full personal accountability, as illustrated here:

> *"Okay. So should we take all the physicists and hold them accountable for the atomic bomb? So, no, not all of them. And once you come to a specific abuse, you're chaining, right? You're chaining a lot of things, right? So now we do. I think we'd have to reason backwards from a specific case to even try and get there. It's probably hard to, to pinpoint it to individual people because we're all standing on each other's shoulders for building bigger things. You can't read and disentangle this*" — P14

More generally, community-based consultation, political and democratic processes at the governmental level, shared norms, and peer discussions were often seen as more appropriate mechanisms for ethical reflection than individual responsibility alone.

Responsibility Constrained by Uncertainty and Unpredictability. A second major rationale again concerned the difficulty of predicting future uses and harms. Interviewees repeatedly emphasized uncertainty about how cryptographic research might be applied, misused, or repurposed over time, as well as ambiguity about whether particular consequences should be considered good or bad. Changing definitions, shifting political contexts, and evolving interpretations of cryptographic technologies further complicated ethical evaluation. Because future impact was seen as inherently unpredictable - especially for foundational or theoretical work - several argued that holding individual researchers accountable for downstream effects is not realistic.

> **Key Insights: Responsibility is widely acknowledged but typically understood as conditional, becoming salient mainly in cases of clear harm. Uncertainty about downstream use and the collective nature of cryptographic research often limit individual accountability. As a result, responsibility is more often located at the level of communities or institutions than treated as a guiding principle in everyday research practice.**

4.10 Ethical Discussions Primarily Happen at the Applied End of the Spectrum

Participants described ethical discussions in cryptography as rather unevenly distributed across subcommunities. Ethical reflection and debate were reported to occur primarily within applied and security-oriented venues, while being rare or largely absent in theoretical cryptography communities. Interviewees who regularly submitted to security conferences were more likely to encounter ethical discussions, whether through conference talks, community forums, or informal exchanges. By contrast, participants primarily embedded in theoretical or core cryptography venues emphasized that ethics rarely feature as an explicit topic at conferences, where ethical considerations are typically limited to issues of scientific misconduct and adherence to good research practice.

Shared Normative Assumptions without Explicit Ethical Debate. Despite the lack of formal ethical discussions in many venues, a few participants' statements pointed to shared normative assumptions within the cryptography community. These included the belief that cryptographic technologies are built to protect people, empower users, and resist surveillance or unlawful interception. Such values were described as implicit rather than explicitly articulated or debated. Ethics was thus framed less as a set of guiding principles and more as a background understanding that research should be socially responsible. Some participants emphasized that ethically problematic research should be discussed rather than prohibited, and that ethical reflection should not function as a mechanism to restrict technical inquiry.

Ethics in Peer Review: Discussion without Clear Responsibility. Ethical considerations surfaced most visibly during the peer-review process, though inconsistently and contestedly. Some participants described having raised - or being willing to raise - ethical concerns as reviewers, for example by asking authors to elaborate on potential societal impact or misuse. Others, typical theoretical researchers, emphasized that technical validity and novelty usually outweigh ethical concerns in review decisions. Ethical analysis was frequently described as secondary to technical contribution. However, a few interviewees expressed uncertainty about their role as reviewers, including discomfort with acting as ethical gatekeepers or concerns about being held accountable for allowing potentially harmful research to pass.

Mandatory Ethics Statements: Awareness or Procedural Formality. Mandatory ethics statements - introduced primarily in security venues - elicited mixed responses. These mechanisms were mentioned unprompted by some participants, most often by applied researchers, but also by theory-oriented researchers. Some interviewees viewed ethics statements as useful prompts that draw attention to ethical consequences, particularly for papers with clear societal implications or involving human data, and noted that ethics sections can encourage transparency or reflection. However, some participants - especially those from theoretical backgrounds, but also applied researchers - criticized mandatory ethics statements as unnecessary, burdensome, or largely procedural, with limited substantive influence on review outcomes. Ethics sections were often described as annoying to write, irrelevant for most cryptography papers, or unlikely to meaningfully affect acceptance decisions. One participant (P20) articulated that the growing number of formal submission requirements may dilute, rather than strengthen, ethical reflection. In this view, ethics statements risk becoming another procedural checkbox among many administrative steps, encouraging generic, formulaic responses instead of sustained engagement with the ethical implications of the research.

> **Key Insights: Overall, ethical discussions are concentrated at the applied end, while remaining largely absent from theoretical venues. Where ethics is present, it is often implicit, informal, and unevenly integrated, shaped by venue norms and perceptions of practical impact. Institutional mechanisms such as ethics statements increase visibility but are widely viewed as limited in influence, particularly for theory.**

4.11 Rogaway's Moral Argument as a Shared Reference

At the end of the interviews, we asked participants whether they were familiar with Rogaway's paper on the moral character of cryptographic work. Many participants reported familiarity with the paper including its core arguments while some - primarily theoretical researchers - were not familiar with it. A few applied participants also unpromptedly referenced other ethics-focused work in cryptography (e.g., by Kamara and Rosenbloom), indicating some prior engagement with the broader ethics literature.

Participants familiar with Rogaway's paper generally aligned with its core concerns, particularly its emphasis on the political dimensions of cryptography and the need for greater reflection on social impact. Nevertheless, they expressed ambivalence, mentioning difficulties in defining the public good, uncertainty about downstream consequences, and disagreement over whether such ethical judgments should rest with individual researchers or with political and governmental processes. While Rogaway's work was seen as influential in shaping ethical discourse, a few participants noted that its impact has remained largely discursive, with limited translation into concrete changes in research practices or priorities.

5 Discussion

Below, we briefly answer our research questions, contextualize our work, and provide actionable recommendations for the community.

In relation to RQ1, our participants generally perceived ethics as adjacent to rather than embedded within their research. Ethical reflection was mainly associated with specific moments such as disclosure or application contexts. Rather than being framed as an integral part of everyday research practice, ethical considerations often appeared implicitly (e.g., in references to generally protecting privacy). This was especially evident among theoretical researchers, who rarely expressed explicit ethical considerations connected to their work. Overall, ethical relevance was typically understood in terms of indirect, delayed, or uncertain impacts, leading to a framing of ethics as awareness rather than accountability.

With respect to RQ2, while there are exceptions, normative and ethical considerations played a limited role in motivating cryptographic research or shaping topic choice. Research directions were instead primarily driven by intellectual curiosity and technical challenge. Where ethical commitments existed, they were usually secondary and rarely articulated as initial motivations, becoming salient mainly in response to concrete scenarios or perceived downstream implications.

Regarding RQ3, broader social and political responsibility was widely acknowledged but rarely operationalized. Participants often associated cryptography with societal goods such as privacy and security, but these effects were typically framed as indirect rather than as direct obligations informing research decisions. Some researchers expressed skepticism toward strong individual responsibility claims, instead emphasizing collective or institutional mechanisms for addressing ethical and societal impacts.

Relating our Interview Data Analysis to the USENIX 2025 Ethics Section Analysis. In our analysis of ethics sections in cryptography papers published at USENIX Security 2025 [62] we found

that, despite mandatory ethics statements, many papers implicitly or explicitly stated that their work raised no ethical concerns. Where ethical considerations were discussed, authors primarily emphasized social benefits and procedural compliance, while substantive engagement with issues such as dual use, surveillance, or downstream harms was rare (more information on the results can be found at: https://doi.org/10.5281/zenodo.22658755). Given that we classified USENIX Security as an applied-focused venue, our findings suggest that the greater ethical awareness expressed by applied-focused researchers in our interviews is not necessarily reflected in these ethics statements. However, as theory-focused venues typically do not require ethics statements and such discussions are largely absent from their papers, we could not directly compare them. Nevertheless, these findings indicate that both theory- and applied-focused cryptography researchers should be further encouraged to critically reflect on the potential ethical implications of their work.

Relating to Previous Literature. Our findings align with Ramulu et al's [57] work on ethical decision-making in the broader computer security community, which identifies substantial variation in how ethics are understood, considered, and operationalized across research contexts. In particular, Ramulu et al. observe differences across security subfields: While ethical considerations are more established in areas involving human subjects, researchers with a background in cryptography and mathematics were described as less likely to discuss ethical concerns, in part because of a perceived disconnect between highly technical or mathematical research and real-world impact. Our study provides a more fine-grained perspective of this observation by focusing specifically on cryptography and systematically examining variation along the theory-applied spectrum. We reveal important heterogeneity within cryptography itself: In our interviews, applied-focused work was more readily connected to societal consequences and ethical considerations, whereas theory-focused work was less frequently associated with such considerations. Importantly, as our analysis of ethics statements illustrates, these differences in expressed ethical awareness do not necessarily translate directly into how ethical considerations are addressed in published work. Our results thus extend this line of research by showing that ethical reflection varies both across research orientations and between expressed awareness and its articulation in research outputs, underscoring the need for tailored and context-sensitive approaches to fostering ethical reflection across cryptographic research.

Further, our findings help to assess the impact of Rogaway's call [51] for a more explicit moral orientation in cryptographic research. While many participants were familiar with his arguments and broadly aligned with the view that cryptography has political and societal implications, our data suggest that ethical engagement in practice deviates from Rogaway's normative vision. Rather than functioning as an explicit general guiding framework, ethics in cryptography appears largely implicit, situational, and distributed across communities and institutions. This discrepancy helps to explain why Rogaway's work exerts limited impact on everyday research decisions despite having substantial discursive impact on how ethics in cryptography is discussed in general.

Seen in this light, Rogaway's intervention can be understood as a normative reference point that brings ethical tensions into focus within a field where responsibility is often deferred, contextualized, or collectively externalized.

Recommendations for the Cryptography Community. Our findings suggest that ethical engagement is most effective when situated, contextual, and supported at the community level, rather than imposed through universal or mandated frameworks. Thus, strengthening ethics in cryptography should not aim to constrain research agendas or limit technical exploration, but to lower the threshold for reflection and discussion, thereby making ethical stakes more salient, primarily through awareness-raising.

A Two-Track Ethics-Statement Template for Cryptography Papers. Our findings suggest that the role and purpose of ethics statements in cryptography require clearer communication. Many theory-oriented researchers expressed concerns about mandatory ethics statements, perceiving them as unnecessary, burdensome, or as a form of compliance theater. Rather than functioning as restrictive requirements, ethics statements should be framed as prompts for reflection - even in cases where ethical implications are uncertain or temporally distant. Given that many researchers seem to understand their work as contributing to the public good (e.g., by advancing privacy or theoretical knowledge), ethics statements can provide an opportunity to make these contributions and their underlying normative motivations more explicit.

To accommodate differences across applied- and theory-oriented venues and researchers, we recommend a two-track approach. Theory-leaning papers could adopt template that acknowledges potential long-term or indirect societal relevance, while application-oriented papers could follow a template addressing dual-use risks, deployment contexts, and disclosure practices. Such a differentiated approach may help reduce concerns about compliance as a performance while preserving the reflective intent of ethics statements across diverse forms of cryptographic research.

An Ethical Peer Review Process to Cultivate Ethical Reflection. As a transitional approach, venues could encourage researchers to practice ethical reflection on work from other researchers. For instance, submitting authors could be assigned to another paper and asked to briefly reflect on its societal consequences or ethical tensions, without this evaluation affecting the paper's acceptance. Decoupling ethical reflection from researchers' own work and the standard review process may reduce the perceived need to minimize or defensively frame ethical concerns while also providing a low-stakes opportunity to develop ethical reasoning as a scholarly skill. Such exercises may help to normalize broader moral reflection as part of scientific practice before introducing more formalized ethics requirements.

A Repository of Canonical Dilemmas with Example Cases. A case repository may help shift ethical engagement in cryptography from abstract reflection toward more concrete, shared, and practice-oriented reasoning. This might be particularly beneficial for theoretical researchers, who often perceive little or no direct connection between their work and ethical considerations. By documenting past ethical dilemmas, disclosure decisions, and contested research outcomes, this resource can offer concrete reference points for learning without prescribing norms. We recommend developing

a community-curated repository modeled after responsible disclosure practices, including cases such as debates around chat control or questions of military funding. Each case should be presented concisely, highlighting key decision points faced by researchers. Mentorship practices and community discussion forums can further reinforce this effort by embedding ethical reflection within existing social structures, particularly for early-career researchers.

Venue-level Guidance Rather Than Venue-level Mandates. Although initially perceived as symbolic, repeated engagement with ethical framing may gradually shape norms and expectations within the community, supporting ethical awareness among authors, readers, and especially early-career researchers, without constraining theoretical inquiry or impeding scientific progress. Another possible approach in this direction would be to offer dedicated workshops or discussion sessions at theoretical cryptography venues, creating space to collectively reflect on potential ethical implications of research topics whose relevance may not be immediately apparent. Importantly, new ethics awareness measures should not result in additional formal submission requirements. Excessive proceduralization risks undermining the intended reflective effects by turning ethical engagement into a purely administrative task.

6 Conclusion

We conducted semi-structured interviews with 20 cryptography researchers across theoretical and applied areas to examine how they understand the relationship between their research and ethics. Our analysis shows that ethical considerations are seldom articulated as explicit drivers of research motivation or topic choice. Instead, they tend to surface in specific contexts, such as proximity to application, perceived downstream consequences, and norms within particular research subcommunities. Participants acknowledged that cryptographic research can have ethically relevant impacts and connections to the public good, but these considerations were articulated unevenly, often with reference to uncertainty, indirect effects, or shared responsibility. Based on the results, we suggest that supporting ethical reflection in cryptography may be most effective through lightweight, community-level practices that encourage discussion where ethical stakes become salient, without constraining research agendas or technical exploration.

Acknowledgments

We would like to thank all the participants for their time and for sharing their views with us. We are also grateful to the reviewers and the shepherd for their valuable feedback and suggestions, which helped improve the paper. Finally, we would like to thank our colleague Rafael Mrowczynski from the Empirical Research Support for insightful discussions during the early stages of this study, as well as the Scientific Writing and Presentation team at CISPA for their support.

This paper was edited for grammar and minor sentence shortening to meet page limits using Grammarly, DeepL and ChatGPT.

References

[1] 2026. ACM Asia Conference on Computer and Communications Security (AsiaCCS). Retrieved Apr. 29, 2026 from https://asiaccs2026.cse.iitkgp.ac.in.

[2] 2026. ACM Conference on Computer and Communications Security (CCS). Retrieved Apr. 29, 2026 from https://www.sigsac.org/ccs/CCS2026/.

[3] 2026. ACM Symposium on Theory of Computing (STOC). Retrieved Apr. 29, 2026 from https://acm-stoc.org.

[4] Shubham Agarwal, Rafael Mrowczynski, Maria Hellenthal, and Ben Stock. 2025. " I have no idea how to make it safer": Studying Security and Privacy Mindsets of Browser Extension Developers. In *34th USENIX Security Symposium (USENIX Security 25)*, 2927–2946.

[5] Patrick D. Anderson. 2021. Privacy for the weak, transparency for the powerful: the cypherpunk ethics of Julian Assange. *Ethics and Information Technology*, 23, 3, (Sept. 2021), 295–308. doi:10.1007/s10676-020-09571-x.

[6] 2026. Annual Computer Security Applications Conference (ACSAC). Retrieved Apr. 29, 2026 from https://www.acsac.org.

[7] 2026. Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Retrieved Apr. 29, 2026 from https://eurocrypt.iacr.org.

[8] 2026. Annual International Cryptology Conference (CRYPTO). Retrieved Apr. 29, 2026 from https://crypto.iacr.org.

[9] Association for Computing Machinery. 2018. ACM Code of Ethics and Professional Conduct. Retrieved Feb. 4, 2026 from https://www.acm.org/code-of-ethics.

[10] ATLAS.ti GmbH. 2024. ATLAS.ti | The #1 Software for Qualitative Data Analysis. Online. Retrieved Dec. 21, 2024 from https://atlasti.com/.

[11] Kenan Begovic, Abdulaziz Al-Ali, and Qutaibah Malluhi. 2023. Cryptographic ransomware encryption detection: Survey. *Computers & Security*, 132, 103349. doi:10.1016/j.cose.2023.103349.

[12] Daniel J. Bernstein, Tanja Lange, and Ruben Niederhagen. 2016. Dual EC: A Standardized Back Door. In *The New Codebreakers - Essays Dedicated to David Kahn on the Occasion of His 85th Birthday* (Lecture Notes in Computer Science). Peter Y. A. Ryan, David Naccache, and Jean-Jacques Quisquater, (Eds.) Vol. 9100. Springer, 256–281. doi:10.1007/978-3-662-49301-4_17.

[13] Kathy C. Charmaz. 2006. *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*. Sage, Thousand Oaks, Calif.

[14] David Chaum. 1985. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28, 10, 1030–1044. doi:10.1145/4372.4373.

[15] 2026. Conference on Cryptographic Hardware and Embedded Systems (CHES). Retrieved Apr. 29, 2026 from https://ches.iacr.org.

[16] Whitfield Diffie and Martin E. Hellman. 1976. New directions in cryptography. *IEEE Transactions on Information Theory*, 22, 6, 644–654. doi:10.1109/TIT.1976.1055638.

[17] Alexandra Dirksen, Sebastian Giessler, Hendrik Erz, Martin Johns, and Tobias Fiebig. 2024. Don't Patch the Researcher, Patch the Game: A Systematic Approach for Responsible Research via Federated Ethics Boards. In *Proceedings of the New Security Paradigms Workshop (NSPW 2024)*. Association for Computing Machinery (ACM), Bedford, PA, USA, 126–141. doi:10.1145/3703465.3703475.

[18] David Dittrich and Erin Kenneally. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. Tech. rep. U.S. Department of Homeland Security, Science and Technology Directorate, Cyber Security Division. doi:10.2139/ssrn.2445102.

[19] Kimberly Do, Rock Yuren Pang, Jiachen Jiang, and Katharina Reinecke. 2023. "That's important, but...": How Computer Science Researchers Anticipate Unintended Consequences of Their Research Innovations. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. ACM. doi:10.1145/3544548.3581347.

[20] Heather Douglas. 2023. The importance of values for science. *Interdisciplinary Science Reviews*, 48, 2, 251–263. doi:10.1080/03080188.2023.2191559.

[21] Kevin C. Elliott. 2023. Science and values. en. In *Routledge Encyclopedia of Philosophy*. (1st ed.). Routledge, London, (Aug. 2023). doi:10.4324/9780415249126-Q149-1.

[22] 2026. European Symposium on Research in Computer Security (ESORICS). Retrieved Apr. 29, 2026 from https://sites.google.com/di.uniroma1.it/esorics2026/.

[23] 2026. Financial Cryptography and Data Security (FC). Retrieved Apr. 29, 2026 from https://ifca.ai/fc26/.

[24] Barney G. Glaser and Anselm L. Strauss. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Publishing Company, Chicago.

[25] Lea Gröber, Rafael Mrowczynski, Nimisha Vijay, Daphne A Muller, Adrian Dabrowski, and Katharina Krombholz. 2023. To Cloud or not to Cloud: A Qualitative Study on Self-Hosters' Motivation, Operation, and Security Mindset. In *32nd USENIX Security Symposium (USENIX Security 23)*, 2491–2508.

[26] Florian Hantke, Sebastian Roth, Rafael Mrowczynski, Christine Utz, and Ben Stock. 2024. Where Are the Red Lines? Towards Ethical Server-Side Scans in Security and Privacy Research. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, (May 2024), 4405–4423. doi:10.1109/SP54263.2024.00104.

[27] Cornelia Helfferich. 2019. Leitfaden- und Experteninterviews. In *Handbuch Methoden der empirischen Sozialforschung*. Nina Baur and Jörg Blasius, (Eds.) Springer VS, Wiesbaden, 669–686.

[28] Eric Hughes. 1997. A cypherpunk's manifesto. In *The electronic privacy papers: Documents on the battle for privacy in the age of surveillance*. https://api.semanticscholar.org/CorpusID:167366776.

[29] 2026. IEEE Computer Security Foundations Symposium (CFS). Retrieved Apr. 29, 2026 from https://csf2026.ieee-security.org.
[30] 2026. IEEE European Symposium on Security and Privacy (EuroS&P). Retrieved Apr. 29, 2026 from https://eurosp2026.ieee-security.org.
[31] IEEE Security & Privacy 2026. 2026. Submission Guidelines. Retrieved Apr. 29, 2026 from https://sp2026.ieee-security.org/cfpapers.html.
[32] 2026. IEEE Symposium on Foundations of Computer Science (FOCS). Retrieved Apr. 29, 2026 from https://focs.computer.org.
[33] 2026. IEEE Symposium on Security and Privacy (S&P). Retrieved Apr. 29, 2026 from https://sp2026.ieee-security.org.
[34] 2026. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Retrieved Apr. 29, 2026 from https://asiacrypt.iacr.org.
[35] Seny Kamara. 2020. Crypto for the People. Invited talk. Retrieved Feb. 5, 2026 from https://www.youtube.com/watch?v=Ygq9ci0GFhA.
[36] Gerhard Kleining. 1982. Umriss zu einer Methodologie qualitativer Sozialforschung. *Kölner Zeitschrift für Soziologie und Sozialpsychologie*, 34, 224–253.
[37] Jan H. Klemmer, Juliane Schmüser, Jacques Suray, Jan-Ulrich Holtgrave, Byron M. Lowens, Florian Schaub, and Sascha Fahl. 2025. Transparency Guidelines for Human-Centered Security and Privacy Research. Working paper, version 0.2. (Nov. 2025). doi:10.5281/zenodo.18030545.
[38] Tadayoshi Kohno, Yasemin Acar, and Wulf Loh. 2023. Ethical Frameworks and Computer Security Trolley Problems: Foundations for Conversations. In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 5145–5162. https://www.usenix.org/conference/usenixsecurity23/presentation/kohno.
[39] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. *Research Methods in Human-Computer Interaction*. (2nd ed.). Morgan Kaufmann / Elsevier, Cambridge, MA.
[40] Kevin Macnish and Jeroen van der Ham. 2020. Ethics in cybersecurity research and practice. *Technology in Society*, 63, 101382. doi:10.1016/j.techsoc.2020.101382.
[41] Philipp Mayring. 2000. Qualitative Content Analysis. *Forum: Qualitative Sozialforschung / Forum: Qualitative Social Research*, 1, 2, Art. 20.
[42] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on human-computer interaction*, 3, CSCW, 1–23. doi:10.1145/3359174.
[43] Arvind Narayanan. 2013. What happened to the crypto dream?, part 1. *IEEE security & privacy*, 11, 2, 75–76. doi:10.1109/MSP.2013.45.
[44] Arvind Narayanan. 2013. What happened to the crypto dream?, part 2. *IEEE security & privacy*, 11, 3, 68–71. doi:10.1109/MSP.2013.75.
[45] 2026. Network and Distributed System Security Symposium (NDSS). Retrieved Apr. 29, 2026 from https://www.ndss-symposium.org.
[46] [SW] OpenAI, Whisper: Automatic Speech Recognition 2023. URL: https://github.com/openai/whisper.
[47] 2026. Privacy Enhancing Technologies Symposium (PETS). Retrieved Apr. 29, 2026 from https://petsymposium.org.
[48] Robert Ramirez, Shun Inagaki, Masaki Shimaoka, and Kenichi Magata. 2020. A Cybersecurity Research Ethics Decision Support UI. In *USENIX Association*. USENIX Association. https://www.usenix.org/system/files/soups2020_poster_ramirez.pdf.
[49] Dennis Reidsma, Jeroen van der Ham, and Andrea Continella. 2023. Operationalizing Cybersecurity Research Ethics Review: From Principles and Guidelines to Practice. In *Proceedings of the 2nd International Workshop on Binary Analysis Research (Ethics 2023)*. USENIX Association. doi:10.14722/ethics.2023.237352.
[50] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21, 2, 120–126. doi:10.1145/359340.359342.
[51] Phillip Rogaway. 2015. The moral character of cryptographic work. *Cryptology ePrint Archive*.
[52] Leah Namisa Rosenbloom. 2025. Cryptography and collective power. In *International Conference on Cryptology and Information Security in Latin America*. Springer, 3–39. doi:10.1007/978-3-032-06754-8_1.
[53] Johnny Saldaña. 2014. Coding and Analysis Strategies. In *The Oxford Handbook of Qualitative Research*. Patricia Leavy, (Ed.) Oxford University Press, Oxford. doi:10.1093/oxfordhb/9780199811755.013.001.
[54] Margrit Schreier. 2014. Qualitative Content Analysis. In *The SAGE Handbook of Qualitative Data Analysis*. Uwe Flick, (Ed.) Sage, Los Angeles et al., 170–183. doi:10.4135/9781446282243.n12.
[55] Margrit Schreier. 2012. *Qualitative Content Analysis in Practice*. Sage, Los Angeles et al. doi:10.4135/9781529682571.
[56] Signal Foundation. [n. d.] Signal — Speak Freely. Retrieved Feb. 4, 2026 from https://signal.org/.
[57] Harshini Sri Ramulu, Helen Schmitt, Bogdan Rerich, Rachel Gonzalez Rodriguez, Tadayoshi Kohno, and Yasemin Acar. 2025. Ethics in Computer Security Research: A Data-Driven Assessment of the Past, the Present, and the Possible Future. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security*, 3162–3176. doi:10.1145/3719027.3765071.
[58] Anselm L. Strauss and Juliet M. Corbin. 2008. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. (3rd ed.). Sage Publications, Thousand Oaks, Calif.
[59] The Tor Project, Inc. [n. d.] Tor: Browse Privately, Explore Freely. Retrieved Feb. 4, 2026 from https://www.torproject.org/.
[60] 2026. Theory of Cryptography Conference (TCC). Retrieved Apr. 29, 2026 from https://tcc.iacr.org.
[61] USENIX Security. [n. d.] USENIX Security '25 Ethics Guidelines. Retrieved Feb. 3, 2026 from https://www.usenix.org/conference/usenixsecurity25/ethics-guidelines.
[62] 2026. USENIX Security Symposium. Retrieved Apr. 29, 2026 from https://www.usenix.org/conference/usenixsecurity26.
[63] USENIX Security Symposium. 2026. USENIX Security '26 Call for Papers. Retrieved Apr. 29, 2026 from https://www.usenix.org/conference/usenixsecurity26/call-for-papers.
[64] Langdon Winner. 1980. Do Artifacts Have Politics? *Daedalus*, 121–136.
[65] Andreas Witzel and Herwig Reiter. 2012. *The Problem-centered Interview: Principles and Practice*. Sage, Los Angeles et al.
[66] A. Young and Moti Yung. 1996. Cryptovirology: extortion-based security threats and countermeasures. In *Proceedings of the 17th IEEE Symposium on Security and Privacy (IEEE S&P 1996)*, 129–140. doi:10.1109/SECPRI.1996.502676.
[67] Yiming Zhang, Mingxuan Liu, Mingming Zhang, Chaoyi Lu, and Haixin Duan. 2022. Ethics in Security Research: Visions, Reality, and Paths Forward. In *Proceedings of the 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 538–545. doi:10.1109/EuroSPW55150.2022.00064.

A Conference Venues Used for Sampling

In the following, we list the conferences used to indicate whether a cryptography researcher's work was more theory- or more applied-oriented. We selected the following A*/A-ranked venues as representative of each category.

Venues publishing more applied cryptography research or cryptography applications:

- Annual Computer Security Applications Conference (ACSAC) [6]
- ACM ASIA Conference on Computer and Communications Security (ASIACCS) [1]
- ACM Conference on Computer and Communications Security (CCS) [2]
- IEEE Computer Security Foundations Symposium (CSF) [29]
- European Symposium on Research in Computer Security (ESORICS) [22]
- IEEE European Symposium on Security and Privacy (EuroS&P) [30]
- Financial Cryptography and Data Security (FC) [23]
- Network and Distributed System Security Symposium (NDSS) [45]
- Privacy Enhancing Technologies Symposium (PETS) [47]
- IEEE Symposium on Security and Privacy (S&P) [33]
- USENIX Security Symposium (USENIX Security) [62]

Theory-oriented cryptography and computing venues:

- International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT) [34]
- Annual International Cryptology Conference (CRYPTO) [8]
- Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) [7]
- IEEE Symposium On Foundations Of Computer Science (FOCS) [32]
- ACM Symposium on Theory of Computing (STOC) [3]
- Theory of Cryptography Conference (TCC) [60]
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) [15]