Toward a PEC Use-Case Suite

*Draft 2021-January-21, for public comments

†Send feedback to pec-suite@nist.gov, by 2021-March-22

Abstract. This document motivates the development of a **p**rivacy-**e**nhancing **c**ryptography (PEC) use-case *suite*. This would constitute a set of proofs of concepts, showcasing the use of cryptographic tools for enabling privacy in various applications. This is not a proposal, but rather a sketch idea to motivate initial public feedback, which can be useful to determine a potential process towards a PEC use-case suite.

Keywords: cryptography, privacy, privacy-enhancing cryptography (PEC), reference material, secure multiparty computation (SMPC), zero-knowledge proof (ZKP).

1 Introduction

1.1 Scope

PEC. **P**rivacy-**e**nhancing **c**ryptography (PEC) refers, in a broad and literal sense, to **c**ryptography (that can be) used to **e**nhance **p**rivacy. PEC tools can serve as enablers of responsible data sharing and interactions, in settings where otherwise (without PEC) one may lack trust to partake in such processes, or be unable to meet privacy regulatory requirements. The technical challenge is often to enable multiple parties to interact meaningfully, towards achieving an application goal, without revealing extraneous private information to one another or to third parties.

Suite. To help identify and assess the potential and pertinence of various PEC tools, it is useful to foster the development of related reference material. This can include reference definitions, descriptions, comparisons, evaluations, security analyzes and

* Luís T. A. N. Brandão. Foreign Guest Researcher at NIST (Contractor via Strativia). Opinions expressed here are by the author and should not be construed as official NIST views.

† Earlier feedback may be useful for an early-improved public draft version.

benchmarking. The sketch idea of a PEC use-case suite arises in this context. Such a suite would constitute a collection of proofs of concept, showcasing the possible use of cryptographic tools for enabling privacy in various applications. The showcased PEC tools can include non-standardized primitives and complex protocols, possibly characterized as advanced cryptography, and they may allow a wide range of tradeoffs. The scope of interest is indeed on the use of currently non-standardized cryptographic techniques and building blocks.

Vision. Over time, the suite can develop into a practical basis of PEC *reference material*, providing insights about security, feasibility, system design, tradeoffs, interoperability and best practices. This would be developed with the collaboration of the international community of stakeholders. From such endeavor would emerge an improved expertise about PEC, useful to assess the pertinence of PEC in conceivable applications, and to develop possible recommendations, for example about future fundamental research and standardization efforts. In the long term, the conceivable benefits of such endeavor also include fostering a responsible promotion of privacy goals in myriad applications. Figure 1 illustrates a corresponding sequence of phases, at a high level.

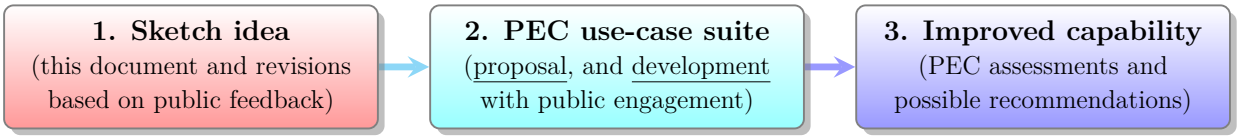

Figure 1: Possible sequence of phases

A large space. Traditional activities of cryptography standardization, for example at NIST, have revolved around *basic* cryptographic primitives, such as block-ciphers, hash functions, random-number generators and regular public-key encryption and signatures. The development of a PEC use-case suite is an approach to tap into the space of more advanced cryptography, where there is a large complexity and range of tradeoffs, many of which to be better understood. It is not on its own intended to derive standards, but to build a (use-case) knowledge basis of how PEC tools can be securely used in the real world. This reference can be useful to characterize the next *basic* level of primitives and protocols, and to support rationale for selecting directions of subsequent engagement. Overall, this is aligned with supporting *the development of innovative security technologies, to address current and future computer and information security challenges.*

Early feedback. While this writeup is informal in nature, the intention is that it serves as a basis for developing future more-technical documentation. Rather than making here a concrete proposal of a PEC use-case suite, the document sketches an idea of what such a suite could be, in order to promote initial external feedback. Such feedback can come from a variety of international stakeholders, including from academia, industry and government sectors. In general, it will be useful to hear about areas of privacy-enhancing applications where advanced cryptographic techniques may be essential enablers. The expected feedback can be useful to steer the idea, with respect to its focuses, format and goals, and for elaborating a subsequent proposal for a PEC use-case suite.

1.2 Cryptographic tools vs. privacy applications

A main aim for considering a PEC use-case suite is to enable assessments about the potential use of cryptographic tools (primitives, techniques, protocols) as privacy enablers. In doing so, taking an application layer into account is essential to better scope the perspectives from which to consider PEC tools, namely to enable a comparison of the potential and of the pertinence across tools.

The scope of interest in PEC in this document can be seen arising from an intersection of cryptography (namely research results in cryptographic tools, here meaning to include primitives, protocols and techniques), privacy (namely potential privacy-enhancing applications), and standardization-like activities (including development of recommendations, guidelines and standards). This intersection is illustrated in Fig. 2.

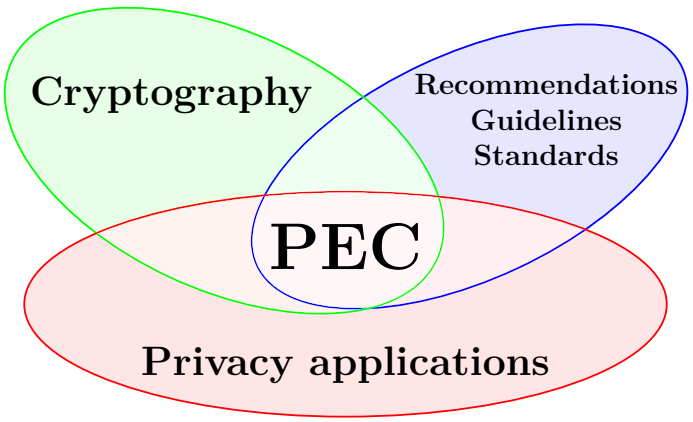

Figure 2: A PEC scope from an intersection of several areas

1.3 Document organization

Section 2 describes various examples of PEC primitives and application areas. Section 3 considers the complementarity of PEC and related areas. Section 4 gives an outline of a possible PEC use-case suite development. Section 5 suggests a structure for the public feedback.

2 Examples of PEC Primitives and Applications

2.1 Example PEC techniques

PEC tools include a variety of cryptographic primitives, protocols and techniques useful for enabling privacy. Relevant representatives include **z**ero-**k**nowledge **p**roofs (ZKPs), **s**ecure **m**ulti**p**arty **c**omputation (SMPC), group signatures and functional encryption.

- **Zero-knowledge proofs (ZKPs).** Allow one party (the prover) to prove to another (the verifier) that a given statement is true, or that some mathematical solution is known to the prover, without revealing any information about the solution.
- **Secure multi-party computation (SMPC).** Allows multiple parties, possibly mutually distrustful, to compute a function (or functionality) of their inputs, as if it were computed by a trusted third party. A party can therefore preserve privacy of their input (i.e., what cannot be derived from the input and output of other parties), even though the input is used in the computation, while also ensuring correctness of outputs. This is achieved without actually needing a trusted party.
- **Group and ring signatures.** Allow a member of a group to digitally sign a message, to prove authenticity/membership with respect to the group (i.e., that it was signed by a group member and it has not been altered theresince), while preserving identity privacy (not revealing the identity of the signatory, apart the group membership predicate, and not allowing linkage to other signatures by the same signatory). In group signatures there is a group manager with a secret key that may enable finding who was the actually signatory.
- **Functional encryption.** A sophisticated encryption scheme that allows producing decryption keys that only decrypt a specific function of whatever plaintext

is encrypted. Two specialized cases are identity-based encryption (IBE) and attribute-based encryption (ABE), where the decryption ability respectively depends on the assigned identity and attributes of the decrypting party (i.e., who has a special decryption key dependent only on the identity and attributes, respectively). For encryption it is sufficient to have a single encryption public key, regardless of how many different functions, attributes or identities may be allowed to perform decryption (with corresponding decryption keys).

Table 1: Examples of PEC primitives/techniques

Primitive	**Description hint (informal)**
Zero Knowledge Proofs (ZKPs)	Prove knowledge of a secret solution to a problem, without revealing the solution.
Secure Multiparty Computation (SMPC)	Jointly compute a function over inputs distributed across several parties, without each party revealing their input.
Group and ring signatures	Produce an unforgeable digital signature, convincingly exhibiting that it has been signed by an unrevealed member of a group.
Functional encryption	Decrypt a function (as specified by a decryption key) of a plaintext that has been encrypted, without learning the clear plaintext.
Fully-Homomorphic Encryption (FHE)	Compute over encrypted data, without learning the plaintext input/output, but ensuring the intended functional transformation.
Private Set Intersection (PSI)	Determine the intersection of sets held by multiple parties, without revealing the non-intersecting components.
Private Information Retrieval (PIR)	Query a key-value database, with the database owner being assured that only one element was queried but not learning which.
Searchable Encryption	Search for a keyword in a database of encrypted documents, obtaining the resulting documents without revealing the keyword.
Blind signatures	Obtain a signature, from a trusted party, without revealing what document has been signed.

Other examples include fully homomorphic encryption (FHE), private set intersection (PSI), private information retrieval (PIR), and blind signatures. This is not an exhaustive list. Table 1 collects these examples, along with very brief description hints. Some PEC techniques may be characterized as "advanced cryptography", as their high dimensionality of variants and tradeoffs may present a challenge for interoperability, and for reflecting on the pertinence of standardization. Yet, they have a clear potential as enablers of enhanced privacy in myriad use-cases.

"Interesting" PEC primitives. There is a wide range of cryptographic techniques and uses that can fit in the PEC scope. These can be used as tools to enable information utility/sharing together with fulfillment of data minimization principles, sometimes in sophisticated and possibly counter-intuitive manners. The exploration proposed in this document is purposely biased toward advanced and non-standardized cryptographic primitives/techniques. Naturally, this characterization is contextual, dependent on the state of development and standardization.

Throughout the proposed process of identifying interesting PEC tools, some basic or standardized primitives may be given less emphasis. Two such examples are regular encryption and signatures, which, although useful, already have well known standardized instantiations. Regular encryption is the paradigmatic tool for enforcing confidentiality of data, which can be useful for enabling privacy in some settings. Regular signatures can in some applications be used as a basis for authorization of data disclosure, sustaining privacy by preventing said authorization from being given by illegitimate parties.

2.2 PEC application areas

The notions of application and use-case are related. In this document, "use-case" typically denotes a representative application. The main elements of the conceived suite are PEC use-cases, which encompass an instantiation of PEC tools (i.e., cryptographic primitives, protocols or techniques) and a description of an application setting (which will inform the privacy requirements and why the proposed PEC tools make sense).

A future suite could identify numerous PEC use-cases, along with a detailed showcasing of cryptography tools that are or can be used to achieve or facilitate them. To prepare a process for a PEC use-case suite, it would be useful to count with initial suggestions of *application areas*, along with a note on the corresponding useful PEC building blocks. There is value in having application areas be first suggested in detailed manner by external stakeholders. The following notes, intended as suggestive and purposely described at a very high level, are based on descriptions in the NIST-PEC project webpage. More details at https://csrc.nist.gov/projects/pec.

2.2.1 Direct disclosure of predicates

A person has a credential, e.g., embedded within a smartcard, issued and digitally signed by a certification authority (CA), and containing **p**rivate **i**dentifiable **i**nformation (PII). The certified PII may include some alphanumeric identifiers, such as full name, birthdate, address, some identification or license number (for some activity) and professional title(s), and possibly also some digitized biometric data (e.g., face photo and fingerprint). In a conceivable application, the person holding the credential uses it to prove some predicate on the PII. For example, it could prove that a real-time digitization of the person's face matches the certified photo, and that the associated data is consistent with having a voting age and having a registered address in a particular voting jurisdiction. Using a practical PEC protocol, e.g., based on ZKPs, the person should be able to convince a verifier that the predicate is satisfied consistently with the identifiers and attributes that the CA has vouched for, yet without revealing extraneous data (e.g., the birthday, the address and even the original photo) and without interacting with the CA.

2.2.2 Brokered authentication

Identity providers (IDPs) can enable users to authenticate to service providers (SPs). Some settings require a broker to mediate this transaction, so as to allow authentication of a passive user (not having specialized software) between the IDPs and SPs, while blinding each IDP and SP from one another. For example, the issuer (identity provider) of an assertion, such as "John Smith is an employee of the Department of Commerce," does not need to know who the consumer of the assertion is. PEC can be used to

further prevent the mediator from learning the assertion, the user attributes and user identity, and even from tracking/linking the same user across various authentications, while at the same time ensuring auditability features to verify the validity of the transactions. Various advanced cryptographic techniques can be used to assist with privacy-preserving brokered identification. For example, SMPC can let the broker verify that the attributes and identity of a user, as held by an IDP, satisfy some predicate required by a SP, but without the IDP (or even the broker) learning what that predicate is, and without the broker or SP learning the attributes and identity.

2.2.3 Public auditability

A Randomness Beacon publishes a random 512-bit number every minute, making it publicly available for free in a digitally signed and time-stamped manner, and chaining it into a backward-immutable chain. Such public randomness can be used to help numerous parties coordinate on future randomness to use, while also allowing post-facto public verification that correct randomness was used. This can fit applications where the probabilistic distribution of the outcome should depend, in a publicly known manner, on committed private attributes. Using PEC, e.g., ZKPs, it is possible to allow such public auditability, while also satisfying privacy requirements. For example, this can allow publicly auditable randomization of clinical trials that depend on patients' data, while also satisfying the patients' privacy.

2.2.4 A wide variety of topics

Topics of PEC applications are likely to have an emphasis on information technology, both in business and non-business sectors. For example, applications can relate to online commerce, banking, health, education, geo-location, encounter metrics, electronic voting, treaty verification, social media and private messaging. They can relate to enabling autonomy of private persons and communities, as well as enabling good practices by collective entities. Also, the range of properties that are being sought along with privacy can be diverse, including auditability and statistics. Some applications, such as identification and authentication, can relate to real uses that extend to a large range of activities.

Use-cases can be motivated by general privacy principles and by the perceived social impact of the solutions. In some other cases the privacy requirements may result more directly from existing regulations. For example: the handling of medical or educational records in the U.S. may be subject to, respectively, the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA); depending on the jurisdiction, there may exist state-level regulations related to consumers' rights over their personal data collected by business; the transmission of data across countries may require compliance with various international regulations.

3 PEC-related areas

When reflecting about a possible PEC use-case suite, it is useful to consider the relation between tools, applications and standards. This interconnection is illustrated in Fig. 3. From a cryptographic-centric perspective, the "tools" are the cryptographic building blocks that can be put together to facilitate an application. The applications are in the level of specification of privacy requirements, which can then be implemented with the help of PEC building blocks. Some PEC tools may be standardized by some organizations, and that may constitute a motivation for their interoperable use in applications. Correspondingly, the use of PEC tools in applications may promote standardization. Both applications and standards related to PEC tools can also promote further development and research toward improved PEC tools.

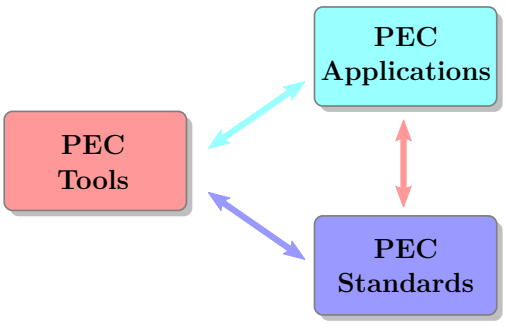

Figure 3: Interconnection between PEC tools, applications and standards

Fig. 4 illustrates a mind map with examples of PEC aspects of interest, in each of the identified perspectives of tools, applications and standards.

The PEC range of interest is very broad and naturally touches on various perspectives of research, applications and standards. Correspondingly, the promotion of PEC can be designed to be complementary or enable synergies with those identified perspectives, rather than constituting a duplication of efforts in separate areas. Taking the NIST-PEC project as a reference point, the following paragraphs consider such possible relations with the perspective of other NIST projects related to cryptography and privacy.

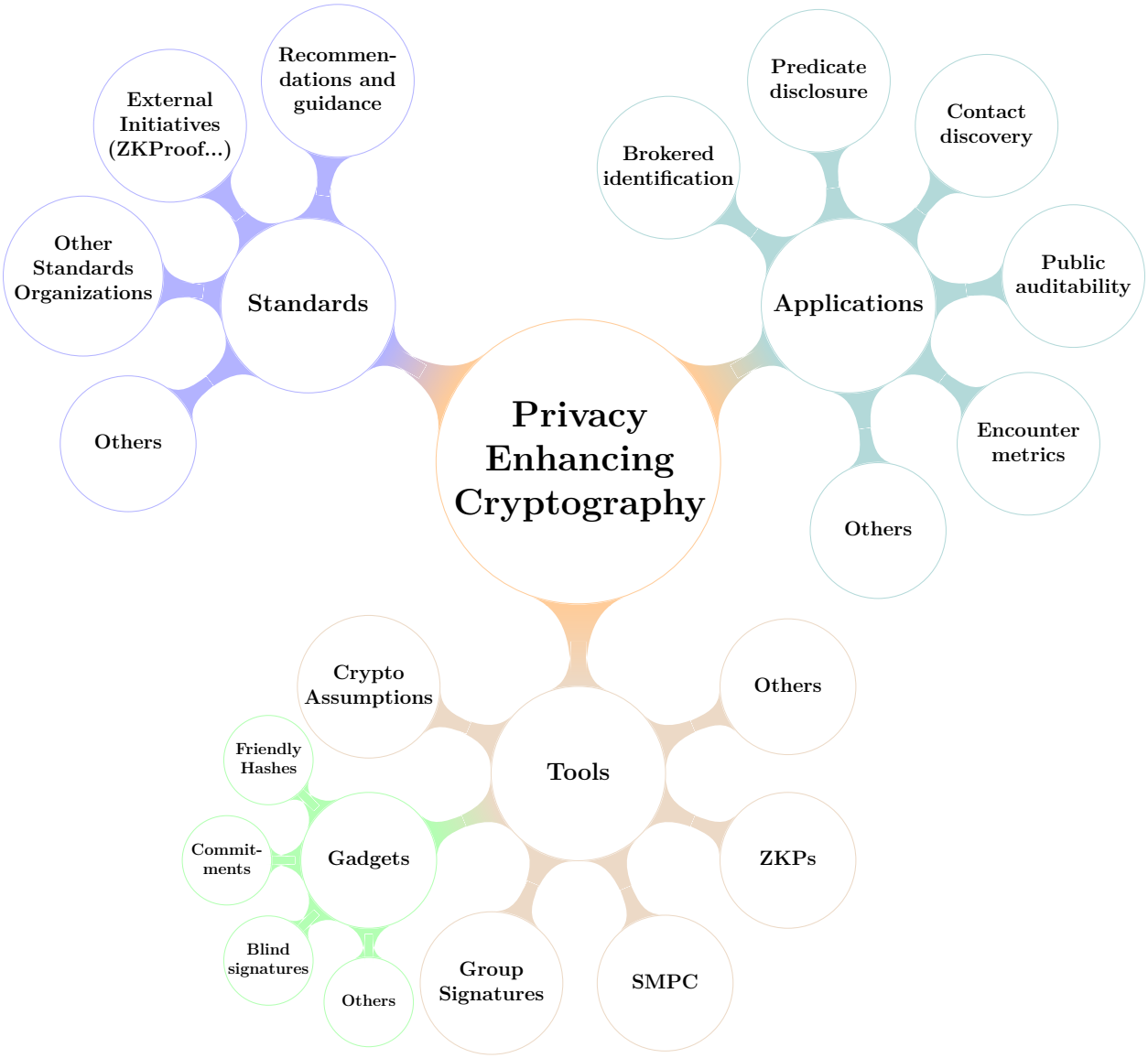

Figure 4: Mind map with examples of conceivable PEC focuses

3.1 Synergies with other cryptography-related projects

- **Threshold Cryptography.** SMPC, a main technique of PEC, is useful for threshold cryptography, where the typical goal is to compute a key-based cryptographic primitive while the secret-key is secret-shared. The PEC project provides a complementary coverage of SMPC techniques, since the reach of SMPC as a general technique is much broader than what the threshold cryptography project encompasses. More details at https://csrc.nist.gov/projects/threshold-cryptography.

- **Interoperable Randomness Beacons.** While a main application of randomness beacons is that of enabling public auditability of randomized processes, achieving such auditability in scenarios with privacy constraints imply the use of PEC. More details at https://csrc.nist.gov/projects/interoperable-randomness-beacons.

- **Post-Quantum Cryptography.** Some post-quantum cryptographic schemes are based on PEC building blocks (e.g., inspired by ZKPs or SMPC paradigms). Conversely, PEC techniques can (should) be developed to achieve post-quantum security, in line with progress in state of the art cryptography. More details at https://csrc.nist.gov/projects/post-quantum-cryptography.

- **Circuit Complexity.** Myriad efficient ZKPs and SMPC depend on good circuits with low complexity, e.g., low number and depth of multiplicative gates/operations. More details at https://csrc.nist.gov/projects/circuit-complexity.

3.2 Complementary privacy-related projects

Privacy is a very broad interdisciplinary area. While PEC is primarily focused on a direct relation between privacy and advanced cryptography, there are other privacy-related techniques, focuses and development activities. The following are some examples of privacy-related projects at NIST.

- **The Privacy Engineering Program (PEP):** "*support the development of trustworthy information systems by applying measurement science and system engineering principles to the creation of frameworks, risk models, guidance, tools,*

and standards that protect privacy and, by extension, civil liberties." More details at https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering.

- **NIST Privacy Framework:** "*A tool to help organizations improve individuals' privacy through enterprise risk management.*" More details at https://www.nist.gov/privacy-framework.

- **Differential Privacy Temporal Map Challenge:** "*develop algorithms and metrics that preserve data utility while guaranteeing individual privacy is protected.*" More details at https://www.nist.gov/ctl/pscr/open-innovation-prize-challenges/current-and-upcoming-prize-challenges/2020-differential

- **National Cybersecurity Center of Excellence (NCCoE).** Maintains several active projects that relate to the enhancement of trust, privacy and security in cyber-security activities. More details at https://www.nccoe.nist.gov

Complementarity example. SMPC, within the scope of the PEC project, is a general cryptographic technique that allows a fine-grained control of the leakage happening in a secure interaction where multiple parties have decided which function (or functionality) to compute from their combined inputs. Differential privacy on the other hand provides insights and metrics to what data transformations are safe to leak, in some contexts. Whether or not these techniques are applied in a complementary way is up to the application design, but they can certainly be considered as complementary building blocks for privacy-enhancing purposes.

4 Envisioning a PEC use-case suite

The promotion of innovation and industrial competitiveness in the area of PEC is useful to enhance economic security and improve quality of life, which is aligned with the mission of NIST. Such promotion is aligned with the following actions:

- Accompany the progress of emerging PEC technologies.
- Assess the potential of cryptography to enable privacy goals.
- Devise guidance about PEC tools and evaluate the pertinence of standardization.

The above should be anchored on a significant understanding of applicable privacy-related use-cases of societal interest, and on the role of cryptographic techniques for the secure design of corresponding privacy-enhancing applications.

4.1 The "reference material" approach

An engagement in the development and characterization of PEC reference material — documents and implementations inspired by real-world and potential use cases — is a way to foster the mentioned needed understanding of PEC. Besides becoming a support for recommendations, such material may also motivate the engagement of the community of stakeholders for further experimentation with PEC, including in research of applied cryptography and development of privacy-enhancing applications.

A conceived instantiation of the reference material approach is to devise a reference set of use-cases from which to learn and based on which to enable exploration of feasible design constructions, sets of important building blocks, benchmark results and possible tradeoffs. That is what this document sketches here as a PEC Use-Case Suite, whose format and development process could be driven by NIST, based on a model that leverages public contributions by stakeholders and where NIST serves as a facilitator.

4.2 The substance of a use-case

In contrast to the very high-level description of examples in this document, the PEC use-cases of a suite would be detailed in various dimensions. Suggested aspects:

1. **Privacy motivation.** Description of an application setting where there are main privacy requirements identified in duality with a sharing or verification utility. This should also include a motivation for the privacy-enhancing solution, possibly based on regulatory requirements or privacy principles, and (possibly informally) its expected potential for social impact.
2. **PEC building blocks.** Enumeration of PEC tools used as building blocks to enable a solution application, and a description of corresponding cryptographic assumptions. Use-cases can depend on currently non-standardized primitives and on assumptions not required in current NIST cryptography standards. These

primitives may for example include the use of pairings (bilinear maps), MPC/ZKP-friendly hashes, commitments, and post-quantum plausibly-secure primitives.

3. **System design.** Description of a real or conceived system design that securely achieves the intended properties of the privacy-enhancing application. This should also include a description of adversarial models and security analysis. Preference should be given to modular designs and analyzes, where PEC tools can be identify as modules, and their composition in the system be proven secure. Availability of implementations, including proofs of concept, can be useful, along with benchmarking and analysys of possible tradeoffs.

Broader considerations. Also relevant in a privacy-enhancing use-case is the identification of privacy in a context broader than cryptography. Beyond the technical dimension of a cryptographic tool, there is the real-world setting where the end users are often humans. For the latter, usability and trust in a technical solution are essential aspects for an application setting to be successful. These aspects can strongly depend on the social settings, and other aspects of real life, including on a personal dimension.

Levels of specification. The envisioned suite would fit a large number of PEC use-cases, developed and specified at various levels. While a complete PEC use-case should specify well the required elements, there is value in taking into account that PEC tools and applications may vary depending on the stages of research, development and deployment. For example, there may exist well defined:

- application settings with privacy challenges "in search of" suitable PEC tools;
- PEC tools "in search of" of applicability in the real world.

The process for developing a PEC use-case suite should enable interconnection between (i) the stakeholders that can propose application settings of real relevance but might not have the corresponding solutions, and (ii) the stakeholders that have the technical expertise on PEC tools but might not be in the role of driving certain applications.

4.3 Enabling a suite

The presented sketch induces some questions about how to drive the process toward a PEC use-case suite, what the incentives for participation are, and what to do after.

A useful perspective for a standards organization is that the PEC use-case suite be developed to become a reference from where to derive useful insights to support recommendations. An apparent challenge relates to the settings where NIST is bound to make recommendations about the use of primitives that have been standardized. With respect to this, the development of a PEC use-case suite is useful from two perspectives:

- It can advance the state of knowledge and experience to assess what future standardization activities are useful. The exploration of PEC use-cases can, for example, make clearer the differentiation of levels of complexity across tools, protocols and techniques. This may facilitate the identification of the next-level basic techniques, whose possible standardization may be pertinent in the future. Such primitives would be beyond the current basic standardized primitives, while still in contrast with more complex cryptographic techniques. Complementary, the process can also support a better understanding of useful techniques for secure composition of those primitives.
- It can help strengthen the ability for other type of recommendations, such as those related to collaboration with other standards bodies and initiatives. It would also enable better informed subsequent recommendations about PEC activities of research and standardization.

Besides the above, the idea of leveraging a PEC use-case suite in collaboration with the community is that there are clear benefits beyond those of the standardization organization. The proponents of use-cases get an opportunity to publicly expose them within a structured program of comparison, evaluation, categorization and possibly incentivization for further development.

4.4 A process

The development of a use-case suite would be initially geared toward improving the understanding of the variety of PEC tools and their potential use, possibly for aiding with the future devising of recommendations.

NIST, as a direct stakeholder of such development, is well placed to promote the endeavor. The role of NIST, namely within the scope of the PEC project, could be that of defining the format and facilitating the process of submissions and security review open to the public. Such facilitation can include:

- defining a structured program that calls external stakeholders to collaborate;
- web-hosting and organizing the reference material provided about PEC use-cases;
- promoting public evaluation and presentations about said material.

Of relevance in this role is the delimitation of the scope of exploration to aspects that matter to cryptographic technology, in the context of information technology applications that rely on the security of computer systems. Challenges exist. For example, an open question at this point is in what way can or should the process encourage a balance of submissions across various areas, or limit submissions based on their technological maturity and/or the relevance of application area.

As in cryptography there is a difference between static and adaptive adversaries, so in this setting seems that an adaptive process is useful, at least on the onset. A proposal for a process would benefit from early feedback from stakeholders (see Section 5).

The endeavor may benefit from an organization in call–evaluation–adaptation phases, possibly with several cycles. The following enumeration is just a sketch:

Phase 1: Call for use-cases.

1. Devise a structure for calling for proposals of PEC use-cases for the suite (see Section 4.2), possibly including diverse categories of submission. The categories should take into account the interplay between tools and applications, the corresponding subsequent analysis.
2. Filter submissions based on admissibility criteria (e.g., material can be publicly posted), and publish the corresponding use-case material, for free accessibility.

Phase 2: Evaluate use-cases.

1. Elaborate and publish an initial summarized and comparative characterization of the received use-cases, enumerating the application areas, PEC tools, cryptographic assumptions, existing implementations and/or standards, notes on potential technological impact, and other aspects of interest.
2. During a publicized period of evaluation, gather public analysis results about the submitted use-cases, including from public presentations (and possibly including a NIST PEC workshop), and proposals of adaptation.

Phase 3: Adapt to results and evolve.

1. Systematize the analysis results into a technical report about the suite, possibly deriving recommendations about the further exploration of PEC tools.
2. Devise a roadmap for the continuation of the suite development process, which may include subsequent improvement and enlargement of the reference set, as well as a possible identification of more specific goals for various focus areas.

5 Intended feedback

A main goal of this document is to motivate feedback from stakeholders external to NIST. The feedback may be used to produce an improved version of this document, and possibly to advance further documentation toward a PEC use-case suite. All feedback will be appreciated. The following are aspects of desired feedback:

1. **Approach.** Comments on the writeup and the overall outlined approach, and in which ways this may be effective for advancing PEC.
2. **Use-case content.** Types of content that should be described in a PEC use-case (see Section 4.2), and whether to differentiate types of use-cases with different submission requirements.
3. **PEC tools.** Suggestions of PEC tools (see Section 2.1), possibly distinguished by complexity, from basic primitives to high-complexity techniques and protocols.
4. **Application areas.** Examples of application areas (see Section 2.2), including those where a privacy requirement exists as a component of enabling information security. This can encompass settings where cryptography has a potential for enabling an essential solution, but the practical cryptography tools and standards currently available to the interested entity might be insufficient.
5. **Process.** The development phases (see Section 4.4), including the process and criteria for organizing submissions and subsequent evaluation. Useful feedback can also include notes about the potential role of the facilitator, of the submitters of use-cases and of the more broad community of stakeholders.

Acknowledgments. Thank you to Lily Chen, René Peralta, Andrew Regenscheid, Angela Robinson and Matthew Scholl from NIST for valuable feedback for this draft.