We propose to develop Distribution-Sensitive Cryptography (DSC), a new framework for cryptographic tool design that will connect and improve upon several existing primitives and produce entirely new ones. DSC guides the creation of context-specific cryptography, leveraging statistical modeling of applications to achieve better security than possible with generic cryptographic tools. Using DSC, we will explore real-world problems for which good solutions have historically been elusive, including:

\* Brute-force attacks against password-based encryption: Conventional encryption is vulnerable to brute-force attacks when keys are weak, as is typical for keys derived from human-chosen passwords. We will develop new solutions for this problem inspired by honey encryption (HE). HE, a primitive recently introduced by the PIs, in principle enables evasion of brute-force attacks. Broad, practical application of HE, however, will demand innovations in formal definitions and empirical modeling that we propose to pursue.

\* Censorship of encrypted protocols: Nation-states use deep-packet inspection to identify and block conventionally encrypted network protocols. Existing steganographic schemes are too slow for practical use, though, and possibly over-engineered for fielded censorship tools in high-traffic settings. Inspired by the PIs' experience with format-transforming encryption (FTE), a promising anti-censorship tool limited by a lack of distributional sensitivity, we will experimentally study real-world adversarial abilities and drive toward a more advanced approach that we call Distribution-Sensitive Encryption (DSE). DSE will strike a new balance in steganographic design, achieving distributional security in a provable-security sense against real-world adversaries as well as high performance.

\* Securing human-generated authentication secrets: Human-generated secrets are noisy; passwords are mistyped, biometric readings are fuzzy, etc. Conventional cryptographic primitives cannot accommodate such ambiguity; prior solutions, such as fuzzy extractors, target security for arbitrary use cases and thus often leak too much information about secrets. We propose to explore a new primitive, called a Distribution-Sensitive Secure Sketch (DSSS), that will leverage application-specific modeling to achieve better security.

In each case, we will both refine our cross-cutting DSC framework and apply it to guide the construction and validation of our solutions. The DSC framework dictates the steps of formulating empirical estimates of appropriate distributions; conceiving suitable formal, provable security definitions; building schemes; and evaluating schemes both formally and via experimentation. A key design principle is robustness, ensuring “fallback” security in case distribution estimates are incorrect.

Intellectual Merit: Our work will require new methodologies and theoretical advances to integrate real-world insights from empirical, data-driven study with formal analysis in the provable security paradigm of modern cryptography. We believe that a new approach will result for developing secure cryptographic tools tailored to particular application settings. Our work will of necessity build connections with other disciplines, including sampling theory, natural language processing, learning theory, and more.

Broader Impact: We have formulated our research program to maximize potential for broad impact on a number of groups. We have experience transitioning our research into tools for the anti-censorship activist community and supporting safe Internet use by activists, dissidents, and others. Our proposed work will aim for similar impact. We will also actively engage industry partners, both to glean real-world requirements and to transition our new tools into practice. Our work will also aim to build bridges between the practitioner and academic communities through workshop development, exposure of academics to research questions of applied value, and educational activities stemming from our research. Finally, we expect that our proposed DSC framework will support a broad array of future research efforts in cryptography.

Keywords: censorship, distribution-sensitive cryptography, fuzzy cryptography, passwords