TWC: TTP Option: Medium: Distribution-Matching Encryption

Principal Investigator: Ari Juels (Cornell Tech)
Principal Investigator: Thomas Ristenpart (University of Wisconsin)
Principal Investigator: Thomas Shrimpton (Portland State University)

Solicitation: `http://www.nsf.gov/pubs/2014/nsf14599/nsf14599.htm`

1 Introduction

Contemporary encryption schemes are almost exclusively *distribution-agnostic*. Their security properties are independent of the statistical characteristics of plaintexts and they always yield ciphertexts that are uniformly distributed in the view of an adversary. Distribution-agnostic cryptography is conceptually simple and often convenient in practice. It fails, however, to meet certain basic, common security needs. Password-based encryption using a conventional, distribution-agnostic cipher, for example, is vulnerable to brute-force cracking—especially given the weak passwords typically chosen by users. Ciphertexts produced using distrbution-agnostic encryption are distinguishable from typical plaintext messages and thus fail to conceal the existence of encrypted communications, i.e., support steganography.

There is consequently a growing, unaddressed need for rigorously studied cryptographic primitives that are specifically tailored to non-uniform plaintext and/or ciphertext distributions. This proposal will explore and enlarge the universe of such primitives. It will also draw them together within a unifying formal framework that can inform and expand their range of application, a framework that we call *distribution-sensitive cryptography* (DSC).

The starting point of the proposal and framework will be three thrusts of applied research, each addressing a distinct practical application in which DSC plays a central role. These are: censorship resistance and steganography (focusing on DPI-circumvention), honey encryption (focusing on password-based encryption), and mangement of human secrets (focusing on secure sketches for password typo detection and biometrics). We will leverage the strong interrelationships among these applications to unify them within our formal DSC framework. By combining formal definitions and security proofs with empirical study, and by embellishing systems we have already built and/or fielded, we will publicly deploy artifacts from our research.

The Three Thrusts A number of applications call for DSC schemes dictated by a particular operational environment. Researchers have begin to explore foundational principles for DSC, but until recently, their focus has not been on application-specific settings. As a result, practical tools tend either not to incorporate research-driven concepts or to do so in an ad hoc way without any rigorous means of assessing their security. Our aim is to fill this gap by designing new DSC schemes with *empirically-driven, provable security*. Our three thrusts are:

- *Censorship resistance / steganography:* Several nation states conduct focused or blanket censorship by using deep-packet inspection (DPI) to detect and block particular protocols, such as Tor [1,6,7,17,18,24,25], TLS [5], and Skype VOIP [19, 23]. Recent research in provably secure encryption for this problem has yielded a primitive called format-transforming encryption (FTE). FTE can bypass DPI filters that rely on regular-expression matching, but *cannot* defeat statistically-based traffic filtering. Relevant steganographic techniques are rigorous but impractical [**?**] or practical but lacking strong security assurances [**?**]. We will develop DME techniques that permit fast encoding of packets carrying of ciphertexts to match the statistical properties of normal traffic. We will thereby carry the provable security benefits of FTE into a stronger adversarial model. Our research will benefit on the foundational side from connections with honey encryption by way of our DSC framework; on the empirical side, it will be informed by measurement studies on internet traffic.

- *Honey encryption:* Users tend to select weak passwords. As a result, their password-based encryption (PBE) ciphertexts are vulnerable to brute-force attacks. PBE is commonly used to protect highly sensitive data such as password vaults, both on mobile devices and in the cloud.[1] Honey encryption can strengthen PBE ciphertexts by generating fake plaintexts that statistically resemble real ones—an instance of distribution matching. The first generation of these schemes, however, are narrowly focused (on credit-card numbers and private) and in some cases inefficient, as in the linear ciphertext expansion for RSA private keys in []. We will expand this reperatoire of honey encryption techniques, aiming, for example, to reduce the ciphertext expansion sizes to practical levels. We will also, through connections in our DSC framework, extend honey encryption techniques to enable password-based DPI-circumvention applications.

- *Management of human-generated secrets:* Users make typos when they key in passwords. Biometrics, such as fingerprints, are noisy. Researchers have developed techniques, such as fuzzy extraction [], that permit the use of such noisy data for cryptographic goals. These techniques, however, have not yet seen been rigorously explored in practical settings and thus have not yet been deployed in real-world systems. We will explore the construction of secure sketches for typo detection in support of honey encryption. We will do so through a novel construction that we call a *distribution-matching secure sketch* (DMSS). We will aim to close the gap between theory and practice with an efficient DMSS construction on study of password databases leaked in the wild.

[1] At least one password management service, LastPass, has already suffered a breach in which PBE vaults were apparently exposed [].

Unifying framework We will unify these three disparate threads of research into DSC-related concepts into a single, formal framework. This framework will yield new insights, permit a cross-pollination of concepts and techniques, and spawn new tools and techniques for a range of practical DSC applications. To do so, we will build on the concept of a *distribution-transforming encoder* (DTE), the linchpin of the honey encryption construction in [].

A DTE is a pair $\mathsf{DTE} = (\mathsf{encode}, \mathsf{decode})$ of algorithms, where encode is a mapping from a message space $\mathcal{M}$ to a space $\mathcal{S}$ of what are called *seeds*, and decode maps seeds to messages. In the original DTE definition, a good DTE is one in which, when seeds are selected uniformly at random and encoded, they yield a distribution close to a target one p_m over $\mathcal{M}$. By extending this definition to non-uniform seed spaces and expanding the accompanying security definitions, it is possible to encompass honey encryption, FTE, steganography, and other primitives within the same definitional framework.

A range of new steganographic constructions then come to light that we will explore in this proposal. First, by enabling information-theoretic security in applications that use low-entropy secrets (such as passwords), honey encryption offers potential paths to: (1) Password-based steganography and (2) Steganography for password-based key-agreement protocols. Additionally, as we explain below, a special class of DTEs offers a novel approach in some settings to: (3) Highly efficient yet provably secure steganography.

This expanded view of DTEs also brings into view another foundational connection, between DTE constructions and techniques from simulation-based proofs of security. These proofs often involve "cooking" values returned by an oracle to create an environment that encodes a user secret but is statistically indistinguishable by an adversary from a real environment—a goal analogous to that in DSC settings. In preliminary work, we have found that such techniques, when imported into DTE construction, can substantially improve efficiency in a key class of DTEs (based on rejection sampling). Such improvement can lead to more efficient honey encryption and steganographic schemes.

Experiments and artifact deployment We will inform our explorations into foundations and new constructions with empirical study of deployment environments and the construction of practical tools. The starting point for this work will be statistical evaluation and modeling of packets captured in a large-scale traffic measurement study. For empirically observed traffic, we will aim to design efficient DTEs that can be parlayed into techniques for circumvention of statistical DPI filtering on the internet. Building on our existing, deployed DPI-circumvention tools, we publicly release novel tools resulting from the research in this proposal.

The DTEs in honey encryption cause silent decryption failures when keys contain errors, e.g., when there are typos in passwords. Drawing on real-world password and password-vault breach data we will explore practical improvements to secure sketches that can detect typos in a client with minimal degradation in password entropy. In preliminary work, we have observed structure (high average edit distance) in popular passwords in the wild, an observation that we will leverage to construct a novel form of secure sketch. We will deploy this code in conjunction with SweetPass, a honey-encryption-based password vault under development. We will aim to extend this line of work to biometrics.

Team

Organization

2 DPI-Circumvention and Distribution-Matching Encryption (DME)

2.1 Background: The Censorship Problem

2.2 Our FTE Research and Deployments

2.3 Next Step: Distribution-Matching Encryption (DME) for Censorship-Circumvention

2.4 Challenges in Censorship-Circumvention

In principle, censorship-circumvension systems are fragile. As observed in [**?**], a such a system is detectable by a censor if it fails in even a single observable particular to mimic (parrot) valid traffic of a particular type. Against a sophisticated censor, a censorship-circumvention system mimicking a specific communication protocol must in principle capture a specific implementation of the protocol in its entirety, including its quirks and bugs. This plausible mimicry needs to be sustained, additionally, against active and adaptive probing by the censor.

We believe this challenge to be surmountable *in practice*, despite its theoretical difficulties. We will explore two distinct but complementary approaches:

- *Bounded-adversary models:* As censorship tools must operate at wire speeds, they are computationally highly constrained. Consequently, censors typically perform two-stage processing, in which the first stage makes use of a DPI product tool; while the capabilities of commercial DPI censorship tools are not widely advertised, there is strong evidence that they perform simple regex matching. The second stage of processing may involve more computationally intensive classification, but only involves a very small fraction of suspect traffic identified in the first stage. Existing tools take advantage heuristically of these bounded resources available to censors. We will define and explore DME security within a formal framework that can instantiate concrete bounds in terms of adversarial computational resources or classes of statistical classification methods.

- *Protocol piggybacking:* The techniques we explore in this proposal, such as Distribution Transforming Encoders (DTEs) (see Section **??**) are very general. They may be used to simulate messages in the message layer of a concealing protocol, resulting in a system that *piggybacks on* a target protocol, rather than *mimicking* it. For example, StegoTorus [] embeds client messages in the URIs and cookies in HTTP requests, producing traffic statistically distinguishable from normal. In our approach, steganographic messages might instead, for example, be embedded in the images in a videoconferencing tool. ≪**Ari:** I presume this obvious approach has been explored or is ruled out for some reason. In any case, perhaps we can briefly discuss.≫

3 Honey Encryption

3.1 Background

3.2 Example Applications: SweetPass, GenoGuard

3.3 More Efficient HE

3.4 New HE Applications

4 Human-Generated Secrets

5 Curriculum Development Activities, Outreach, and Dissemination of Results

Our proposed research will be conducted in order to maximize broader impact on education, student development, and the world. This will be facilitated by active engagement with the activist and censorship circumvention practitioner communities as well as community building for academic applied cryptography.

Developing the scientific community. An important part of our work will be development of the applied cryptography research community, which requires integrating better disparate disciplines within computer science. We particularly target expanding the interaction between those building and deploying systems and the cryptographic theory research communities. The PIs are both on the steering committee of a new workshop, Real World Cryptography, to be held next year, and which we intend to continue helping with throughout the lifetime of this grant. This workshop brings together practitioners and academics in order to hear about the latest applied cryptography research as well as industry problems. We hope it will help strengthen the sometimes fractious community of cryptography researchers who (want to) do more applied work.

As part of our proposal, we will develop new methodologies for assessing applied cryptography. In particular, by explicitly building into the design and formal analysis process as well empiricism. We believe this "data-driven" approach will lead to better results, with theory tailored better to the problems of practice relevance. By interaction with the academic community via conferences, workshops, and university visits we will both advertise this methodological approach and gain feedback on it.

Outreach and diversity. We believe that scientific communities are most productive when they include researchers from a wide variety of backgrounds: science disproportionately benefits from a diversity of viewpoints. Towards this end, we will make an effort when attracting students to especially target women and underrepresented minorities. The PIs have already had success in this regard. Shrimpton has mentored Mrs. Tashell Kelly (undergraduate), Ms. Morgan Miller (MS 2010), Ms. Erin Chapman (MS 2012); and served as a committee member for Mrs. Nichole Schimanski (PhD, 2014). Ristenpart is currently advising Ms. Alexis Fisher (MS, expected 2013) and Mrs. Melissa Tress (PhD,

expected 2017). Both PIs are advising or already graduated several other students, now working at Google, Tektronics, Facebook, Sandia National Laboratories, Amazon.

The profile of the students who study computer security at Portland State does not represent the diversity of the surrounding community. To address these issues PI Shrimpton is working with local colleagues to reach potential students earlier in the pipeline. We are currently working on plans for an outreach center that fosters relationships with local K-12 educators.

Curriculum development. A key aspect of our work will be in improving curriculum to ensure students have the right skillsets to tackle problems in the space of applied cryptography and censorship resistance. PI Ristenpart will be developing a new graduate-level security at Wisconsin in Fall 2013. It will focus on preparing students to work at the cutting edge of research in security, and will have a particular emphasis on techniques cutting across the traditional boundaries of theoretical cryptography and systems security. He has already had success developing an undergraduate security course that after just two years is already one of the most popular in the department, and equips students with the perspective needed to find and fix security problems. He has also in the past developed a graduate course on applied cryptography, with an emphasis on theoretical techniques of value to practical cryptography.

During the period of PI Shrimpton's first NSF grant, he developed a graduate course in modern cryptography at Portland State. Motivated by problems he had encountered as part of his research, and frustrations he faced teaching cryptography, he developed "Counting, Probability and Computing" during the period of his second NSF grant. This time, he will develop a course in cryptography suitable for undergraduates. This course will focus much less on proofs and formalisms, much more on applications and developing a good sense of cryptographic hygiene. A major motivation for this new undergraduate course are the continued complaints heard from local employers, especially Intel, about new hires lacking any kind of security-awareness. In fact, Shrimpton will work with Dr. Jesse Walker of Intel to develop this new course.

Technological impact and software dissemination. This project will have its success measured in large part by the degree to which the research impacts real-world censorship circumvention mechanisms. In particular, we intend to implement our new countermeasures in real systems. See the attached supplement on Transitions, which describes our proposed work on building systems based on the FTE and DME technologies. Our goal is that, several years from now, people across the world will be better able to evade censorship due in part to the proposed work.

To facilitate this, we build software prototypes of all new cryptographic schemes. These will be open-sourced and released publicly. The necessary fine-tuning and engineering to ensure deployability will be covered in the Transitions supplement. We note that PI Ristenpart has experience successfully releasing software tools [**?**] that have been used by more than 100,000 people. We are strong believers in the idea that making available software produced in the course of publicly-funded research accelerates scientific advancement, technology transfer, and education.

6 Results of Prior NSF Support

Shrimpton is the PI of NSF Grant #0845610, "CAREER: Design Principles for Cryptographic Hash Functions: Foundations, Primitives and Transforms", for $400,000 and with period 6/2009–6/2014, and also of #nnnnnnn "Tweakable-blockcipher-based Cryptography", for $433,000 and with period mm/yyyy–mm/yyyy. ≪**TomS:** Need to update this, and the following list of pubs.≫ These projects have resulted in a number of top-tier publications [3,4,12,14–16,20–22] and one "Best Paper" award [20]. Many of these papers are about cryptographic hash function designs [3,4,12,20]; [12] and [3] had impact on the designs of several of the NIST SHA-3 entrants. In [15] we explored restrictions of the random-oracle model, and how these restrictions affect provable security. In [22], we uncovered an important, commonly held misunderstanding about the indifferentiability framework [22], and shows how this leads to overconfidence in the security of hash functions. Some of the collaborations fostered by this award have spawned new threads of research. For example, [21] gives the first provable-security treatment of TLS version 1.2 (the current version), showing that it provides length-hiding authenticated encryption. Thinking about length-hiding led to [14], which examines the efficacy of traffic-analysis countermeasures.

Ristenpart is the PI of one current NSF grant #1065134, "TC: Medium: Collaborative Research: Random Number Generation and Use in Virtualized Environments", for total $749.149 and with period of support 9/1/2011 – 8/31/2015. There is no overlap in technical content with the current proposal. The work of this grant has been ongoing for one year. We have so far developed significant portions of the theory underlying new RNGs that will be deployed [2, 10, 11, 13]. We initial results on tools to find further RNG reset vulnerabilities. Two graduated masters students were partially funded by this project. Publications include [2, 8–11, 13].

Topic	Task	Person Years	Supervisor	Timeline Years
FTE	Security notions and proofs	1	Shrimpton	1
FTE	Empirical analysis	1	Ristenpart	1
DME	Formal definitions	2	Shrimpton	2-3
DME	Scheme development	3	Shrimpton	1-3
DME	Empirical analysis	1	Ristenpart	3
Empiricism	Trace collection infrastructure	1	Ristenpart	1
Empiricism	Analysis methods / attacks	3	Ristenpart	1-3

Table 1: Tasks, supervisory roles of different PIs, timeline, and person years required.

7 Collaboration Plan

We have put together a team of two PIs with a long track record of successful collaborations, as well as expertise in the target domain of this proposal. PI Shrimpton is an expert on fast, provably-secure symmetric encryption mechanisms as well as signal processing, signal detection, and communication theory, thereby providing a rare cross-disciplinary perspective relevant to the proposed work. PI Ristenpart works in systems security and both applied and theoretical cryptography, providing a needed perspective on issues of practical import. They have, in the last several years, published six papers together, in top tier security and cryptography venues, including on topics related to this paper [14].

As mentioned, a goal of our proposal is to push improve the scientific methodologies in applied cryptography. In particular, we will place an emphasis on tight integration of empiricism with theory. This will expose PIs, students, and other personnel to new methodologies and cross-disciplinary activities, which we strongly feel will enrich our fields.

7.1 Meetings/Conference Calls/Visits

Communication, a sense of ownership, and overall team cohesion are key to successful collaborations. Frequent use of collaboration tools, including email, Wikis, and instant messaging, will facilitate the former. One-on-one and group meetings as well as cross-institution visits will help with the others.

PI Meetings: The two PIs will have frequent meetings, at least once a week to enable brainstorming, idea development, and execution. The frequency is useful to ensure tight integration between two separate institutional groups, and will facilitate that all of the proposed work will (necessarily) involve involve both PIs.

Institutional Meetings: Each PI will meet individually with his graduate student (and any other personnel) once a week. We will have less frequent group meetings via teleconference.

Visits: We will look for opportunities to perform personnel exchange via summer visits to Wisconsin by the PSU student and vice versa. Depending on student schedules (and interest), we will target visits of one week up to a few months. This will provide student enrichment as well as stoke further collaborations across the two universities.

7.2 Roles, assignments, and timeline

As mentioned and in the spirit of methodological enrichment, both PIs will be involved in all proposed work. That said, we will each be a "supervisor" on certain portions of the project. The goal of the supervisor is to take primary responsibility for progress on the given task and to ensure any potential hurdles are overcome. Table 1 presents a list of tasks, a rough timeline, supervisory roles, and the number of student person-years committed to each task. Note that multiple students may work on a task simultaneously. We have organized the work across the three themes of FTE, DME, and Empiricism, and laid out a timeline that we suspect will properly pipeline tasks.