SaTC: Medium: Distribution-Matching Encryption

Ari Juels, Thomas Ristenpart, Thomas Shrimpton

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. There is a growing, unaddressed need, however, for rigorously studied cryptographic primitives that are specifically tailored to non-uniform plaintext and/or ciphertext distributions, a notion that we call *distribution-matching encryption* (DME).

This proposal will encompass three main thrusts of research, each addressing a distinct practical application in which DME 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 a single formal framework for DME. 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 DME applications. 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 DME schemes dictated by a particular operational environment. Researchers have begin to explore foundational principles for DME, 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 DME 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 [**?**, **?**, **?**, **?**, **?**, **?**, **?**], TLS [**?**], and Skype VOIP [**?**, **?**]. 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 DME 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 DME 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.

Foundations We will unify these three disparate threads of research into DME-related concepts into a single, formal framework. To do so, we will build on the concept of a *distribution-transforming encoder* (DTE), the linchpin of the honey encryption construction in [].

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

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 is statistically indistinguishable by an adversary from a real environment—a goal analogous to that in DME 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. We will aim to design efficient DTEs for empirically observed traffic 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