At the Juncture of Cryptography and Humanity

Ari Juels

RSA Laboratories
Bedford, MA 01730, USA
E-mail: ajuels@rsasecurity.com

Cryptographic protocols are almost always geared toward situations involving exact knowledge. A digital signing protocol or decryption protocol, for example, typically assumes possession on the part of the user of a fully specified private key. At the juncture between human beings and security systems, however, assumptions regarding exactitude very often break down. People alter their trust relationships and acquire and forget information (such as passwords) on a regular basis. Even from a biological perspective, human beings present constantly changing information to computer systems. As designers of biometric authentication systems know, images of a finger, iris, or face never look exactly the same way twice.

A strong basis exists for error tolerance in cryptography, with research on secure multiparty computation, public-key cryptosystems, quantum cryptography, and many other topics drawing on constructions such as error-correcting codes, e.g., [1, 3, 10]. The types of errors introduced by ordinary human beings, however, have seen less interest and attention in the cryptographic literature than those of Byzantine adversaries and photons. Ongoing research at RSA Laboratories seeks to develop a set of cryptographic techniques tolerant of the types of errors typically introduced by human beings.

Fuzzy commitment is one algorithm stemming from research at RSA Labs and antecedent work [8, 4, 5]. This is a simple construction employing error-correcting codes in a somewhat unorthodox manner so as to allow encryption and decryption of a ciphertext using keys that are similar in some appropriate metric, but not exactly equivalent. Fuzzy commitment has yielded several practical applications. The first of these is a *visual password system* – briefly stated, an authentication system in which a password consists of a collection of designated points on different images. To specify her password, a user must pick out these designated points; thanks to the underlying use of fuzzy commitment, however, she need not select her points with perfect precision.

A second application is what we refer to as a *fuzzy vault* [7]. The basic principle here is familiar from existing password recovery systems on the Web. To authenticate herself, a user must correctly answer some subset (e.g., 5 out of 7) of "life" questions, such as "What is your mother's maiden name?" or "What was the name of your high school?" A conventionally designed password recovery system stores the answers for each user on a server, which is responsible for checking the correctness of answers submitted during authentication sessions. The aggregation of private user information on publicly accessible servers presents privacy concerns of an obviously serious nature. By contrast, in our fuzzy vault system the answers to life questions are never stored anywhere in explicit form. Instead, the private key of a user is encrypted using a fuzzy commitment scheme under the answers to her life questions. By providing some fraction of correct answers, the user can recover her private key. While at least one fuzzy vault proposal has previously appeared in the literature [6], the lack of rigorous design led to a serious break [2]. Our system, however, possesses provable security properties. We have constructed a prototype with a graphical interface that RSA Security Inc. has plans to incorporate into products this year.

Biometric authentication represents another area of application of fuzzy commitment. The aim here is again to eliminate aggregation of sensitive private information on servers. A typical fingerprint recognition system, for example, involves storage on a server of registered images (or some derivative information) of the fingerprints of users. To authenticate herself, a user transmits a new image of her fingerprint to the server. The server checks that the new image is similar to the registered one (in some appropriate sense), and grants access based on the degree of similarity. Centralized aggregation of fingerprint information on a server introduces a host of privacy and security concerns, not to mention architectural complications. Fuzzy commitment offers an attractive alternative. By storing the private key of a user as a fuzzy commitment under her fingerprint image, a biometric authentication system can avoid the need for explicit storage of fingerprint information and also for server-side processing of fingerprint data.

In a typical fingerprint recognition system, the measure of "similarity" does not correspond to that in our basic fuzzy commitment scheme. In particular, while our original scheme depends upon a notion of similarity like that of Hamming distance, fingerprint recognition often relies on distance metrics involving unordered sets. To address this new scenario, we have developed a fuzzy commitment scheme with the special property

of *order invariance* [9]. In this scheme, the ordering of symbols in keys used to encrypt and decrypt information has no impact on successful operation of the scheme. Like the original fuzzy commitment scheme, the order-invariant one makes use of error-correcting codes, such as Reed-Solomon codes, but involves a rather different construction and set of resulting properties.

Fuzzy commitment schemes can also be used for settings involving privacy-sensitive matching, as considered for example in what we refer to as the *movie lovers' problem*. Alice wishes to find another person with a taste in movies similar to her own. Alice's list of favorite movies is l_A; she wants to find another person with a similar list. Using a fuzzy commitment scheme, Alice can publish to a bulletin board a ciphertext C_A on her telephone number, encrypted under l_A. Bob, who has a list l_B of favorite movies can decrypt Alice's telephone number successfully only if l_A is similar to l_B. With use of a *throttling mechanism*, i.e., a means of preventing off-line attacks, it is possible to consider the movie lovers' problem in low-entropy settings. For example, since movie tastes are similar across large segments of the population, an attacker might try to decrypt C_A by guessing. Alice can prevent this by giving on-line yes/no answers to decryption attempts, and restricting the number of such attempts according to her security goals. The movie lovers' problem can serve as the basis for privacy-preserving protocols distinguishing communities of users with similar tastes or goals.

Fuzzy commitment thus enables the construction of Human Interactive Proofs (HIPs) that distinguish among sets of human beings. An additional interest at RSA Labs has been the problem of creating what might be thought of as an *Automated Turing Test* (ATTs), that is, large sets of problem instances that may be generated efficiently at random and distinguish between human beings and computing devices seeking to pose as human beings. Several Web sites, such as Altavista and iDrive, already employ a crude form of ATT involving the task of recognizing letters that are misaligned and drawn in unusual and heterogeneous fonts. We have found that single algorithms involving optical character recognition are capable of breaking these ATTs very easily. We have investigated a couple of alternatives, including, for example, a simple test in which a photograph is presented at different angles, and the user is asked to select the correct one. We look forward to learning about and plumbing current hardness conjectures from the artificial intelligence community in order to strengthen our development of new ATTs.

References

1. C.H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska. Practical quantum oblivious transfer protocols. In J. Feigenbaum, editor, *Crypto '91*, pages 351–366. Springer-Verlag, 1991. LNCS No. 576.
2. D. Bleichenbacher and P. Nyuyen. Noisy polynomial interpolation and noisy chinese remaindering. In B. Preneel, editor, *Eurocrypt '00*, pages 53–69, 2000. LNCS no. 1807.
3. C. Crépeau and J. Kilian. Achieving oblivious transfer using weakened security assumptions. In *Proceedings of the 29th IEEE Symposium on the Foundations of Computer Science*, pages 42–52, 1988.
4. G.I. Davida, Y. Frankel, and B.J. Matt. On enabling secure applications through off-line biometric identification. In *IEEE Symposium on Privacy and Security*, 1998.
5. G.I. Davida, Y. Frankel, and B.J. Matt. On the relation of error correction and cryptography to an offline biometric based identification scheme. In *Proceedings of WCC99, Workshop on Coding and Cryptography*, 1999.
6. C. Ellison, C. Hall, R. Milbert, and B. Schneier. *Protecting Secret Keys with Personal Entropy*, pages 311–318. 2000.
7. N. Frykholm and A. Juels. Error-Tolerant Password Recovery. In P. Samarati, editor, *Eighth ACM Conference on Computer and Communications Security*, pages 1–8. ACM Press, 2001.
8. A. Juels and M. Wattenberg. A fuzzy commitment scheme. In G. Tsudik, editor, *Sixth ACM Conference on Computer and Communications Security*, pages 28–36. ACM Press, 1999.
9. A. Juels and M. Sudan. A fuzzy vault scheme. 2000. In submission.
10. R.J. McEliece. A public-key cryptosystem based on algebraic coding theory. Technical Report DSN progress report 42-44, Jet Propulsion Laboratory, Pasadena, 1978.
11. F. Monrose, M. K. Reiter, and S. Wetzel. Password hardening based on keystroke dynamics. In G. Tsudik, editor, *Sixth ACM Conference on Computer and Communications Security*, pages 73-82. ACM Press, 1999.