Subspace Fuzzy-Vault

Kyle Marshall, Joachim Rosenthal, Davide Schipani, Anna-Lena Trautmann

June 8, 2014

1 Background

Fuzzy vault is the term used by Juels and Sudan in [2] to describe a cryptographic primitive in which a key κ is hidden by a set of features A in such a way that any witness B which is close enough to A under the set difference metric can decommit κ. Fuzzy vault is a generalization of fuzzy commitment [3].

The motivation for fuzzy vault is largely predicated on the growing interest in using fuzzy authentication systems, i.e. systems that do not require an exact match, but rather a partial one, between two sets. Instances include the use of biometric features for authentication, personal entropy systems to allow password recovery by answering a set of questions with a level of accuracy above a certain threshold, privacy-protected matching to allow find a match between two parties without discosing the features in public.

The fuzzy vault scheme proposed in [2] is as follows and will henceforth be called the JS scheme. Let $A \subset \mathbb{F}_q$ and let $\kappa = (k_0, k_1, ..., k_{\ell-1}) \in \mathbb{F}_q^t$ be the secret key. We require that $|A| = t \geq \ell$. Furthermore, choose $r > t$ and select a set $C \subset \mathbb{F}_q$ to consist of $r - t$ points not in A. Construct the polynomial $\kappa(x) = k_0 + k_1 x + ...k_{\ell-1}x^{\ell-1}$ and the sets $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q \times \mathbb{F}_q$ according to

$$\mathcal{A} = \{(x, \kappa(x)) \mid x \in A\},$$
$$\mathcal{B} = \{(y, \kappa(y) + \varepsilon_y) \mid y \in C, \varepsilon_y \neq 0\}.$$

Define $\mathcal{V} = \mathcal{A} \cup \mathcal{B}$. The points $\mathcal{A}$ are called the authentic points, and the points $\mathcal{B}$ are called chaff points. Lastly, an appropriate Reed-Solomon decoder `decode` is selected and $\mathcal{V}$ and `decode` are then made public.

If a witness attempts to gain access to the vault, then the witness submits a set $B \subset \mathbb{F}_q$ which is close to A under the set difference metric and then constructs the polynomial f by interpolating the points of $\mathcal{V}$ whose x-coordinates correspond to B. The witness then uses `decode` to correct f to the nearest codeword in the Reed-Solomon code. If this is given by $\kappa(x)$, then the witness recovers the secret key.

2 A Fuzzy Vault Scheme Using Network Coding

It was shown in [5] that certain reasonable parameters for the fuzzy vault scheme in its original form cause the system to be susceptible to a brute force attack. Choi et al. in [1] speed up the attack by using a fast polynomial reconstruction algorithm. In the JS scheme, the number of keys and thus the complexity of a brute-force attack is determined by the choice of ℓ. Since the number of features must be larger than ℓ, the security, in practice, depends on the number of

features than can be extracted from a biometric. Moon et al. consider the problem of improving the security for small degree polynomials in [6].

Recently, much work has been done in the area of error correcting codes in projective space. These codes turn out to be appropriate for error correction in networks under the setting of Kötter and Kschichang, and are referred to as linear network codes [4]. Extending the construction of the fuzzy vault in the JS scheme to arbitrary linear codes is not entirely straightforward, however, linear network codes can be used to create a fuzzy vault in an analogous way.

In this alternative fuzzy vault scheme, we will utilize techniques from linear network coding and restrict our attention to constant dimension codes [4]. A constant dimension linear network code is a subset of the Grassmanian $\mathcal{G}_q(n,k)$, the set of all k-dimensional subspaces of $\mathbb{F}_q^n$. The subspace distance defines a metric on $\mathcal{G}_q(n,k)$ given by

$$d_S(U,V) = \dim(U+V) - \dim(U \cap V),$$

for $U, V \in \mathcal{G}_q(n,k)$. While finding good linear network codes is still an open research problem, there are many candidates now, including the Reed-Solomon and spread code constructions [4].

In this work, we present the construction of the fuzzy vault based on linear network coding as well as algorithms, security analysis, and considerations for implementation. Furthermore, we show that the fuzzy vault scheme based on linear network coding has several advantages over the JS scheme.

References

[1] Woo Yong Choi, Sungju Lee, Daesung Moon, Yongwha Chung, and Ki Young Moon. A fast algorithm for polynomial reconstruction of fuzzy fingerprint vault. *IEICE Electronics Express*, 5(18):725–731, 2008.

[2] Ari Juels and Madhu Sudan. A fuzzy vault scheme. *Des. Codes Cryptography*, 38(2):237–257, February 2006.

[3] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM conference on Computer and communications security*, CCS '99, pages 28–36, New York, NY, USA, 1999. ACM.

[4] Ralf Koetter and Frank Kschichang. Coding for errors and erasures in random network coding. In *Proc. IEEE Int. Symp. Information Theory*, 2007.

[5] Preda Mihailescu, Axel Munk, and Benjamin Tams. The fuzzy vault for fingerprints is vulnerable to brute force attack. In *BIOSIG*, pages 43–54, 2009.

[6] Daesung Moon, Woo yong Choi, and Kiyoung Moon. Fuzzy fingerprint vault using multiple polynomials. *IEEE International Symposium on Consumer Electronics*, pages 290–293, 2009.