Error Correcting Codes: Combinatorics, Algorithms and Applications (Spring 2011)

Lecture 17: Fuzzy Vaults in Biometrics

Feb 28, 2011

Lecturer: Atri Rudra *Scribe: Eric Mikida*

1 Quick Recap of Reed-Solomon codes

Let $\bar{m} = (m_0, \ldots, m_{k-1}) \in \mathbb{F}_q^k$ be a message, and $S = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_q^n$ be the evaluation set. The $[n, k, n-k+1]_q$ RS code is given by:

$$RS_s(\bar{m}) = (P_{\bar{m}}(\alpha_1), \ldots, P_{\bar{m}}(\alpha_n))$$

where $P_{\bar{m}}$ is the polynomial $P_{\bar{m}}(x) = \sum\limits_{i=0}^{k-1} m_i x^i$

For today's lecture it will be useful to note that an RS code can also be represented in the set form:

$$RS_s(\bar{m}) = \{(\alpha_1, P_{\bar{m}}(\alpha_1)), \ldots, (\alpha_n, P_{\bar{m}}(\alpha_n))\}$$

Note that unlike in vector form, order does not matter.

Theorem 1.1. *For any $[n, k, n-k+1]_q$ RS code, it can be decoded in $O(n^3)$ time for up to $\left(\frac{n-k}{2}\right)$ errors*

We will hold off on the proof of this theorem until later, but note that it is equivalent to the following remark:

Remark 1.2. *Given n pairs, $(\alpha_1, y_1), \ldots, (\alpha_n, y_n)$, if $\exists$ a polynomial $P(x)$ of degree at least $k-1$, such that $P(\alpha_i) = y_i$ for at least $\left(\frac{n+k}{2}\right)$ values of $i \in [n]$, then $P(x)$ can be computed in $O(n^3)$ time.*

2 The Fuzzy Vault Problem

Say you have a secret, s, and you want to store it in a secure way. Instead of using a password, you want to use your fingerprint, f. You want the locked version of your secret to have two properties:

Properties:

(i) You should be able to unlock s

(ii) No one else should be able to unlock s

Naive Solution: Use f as a key in any secure symmetric key crypto-system (*ie.* AES).

To see the issues with out naive solution, we first need to know a little bit about how fingerprints are stored. The standard way to store a fingerprint is a collection of triples, called minutia. The i^{th} minutia is the triple (x_i, y_i, θ_i), where x_i and y_i are the x and y coordinates of a point on the finger, and θ_i is the angle of the line tangent to that point.

The main issue with our naive solution is that two fingerprint readings will never be exactly the same; even if the same finger is used. For any two fingerprint readings, the following may occur:

Issues:

(*i*) Translation and rotation of the fingerprint

(*ii*) Varying pressure will cause local errors

(*iii*) Not a complete overlap of the fingerprint region

(*iv*) The minutia need not form a vector, just a set

We can now see that the naive solution is not adequate. Even if we could somehow correct for the first 3 issues, symmetric key cryptosystems require a vector, not a set, so our naive solution will fail.

Remark 2.1. *The 4 problems that came up in our naive solution will come up with any solution we propose. The technology is not yet at a point where we can eliminate these issues. Because of this, we are able to achieve property* (i) *of our system, but property* (ii) *is still mainly unsolved. We can test whether a certain fingerprint is a good enough match, but we cannot necessarily keep others out. The reason fingerprinting works for government agencies, such as the police or FBI, is that there is a trust that the government will keep your data secure. With a commercial entity, that trust is not there which is why commercial systems don't quite exist yet.*

3 Formal Problem Statement

The first thing we need to do is quantize the measurements of the minutia. We cannot be infinitely precise in our measurements anyways, so let's assume that all quantized minutia, (x_i, y_i, θ_i) are in $\mathbb{F}_q$. Theoretically this can also help to correct the first two issues from our naive solution. We could go through all possible Δ values in $\mathbb{F}_q$ to get rid of translation and rotation errors. We can also do some local error correction to a quantized value.

Formal Problem:

- Secret $s \in \mathbb{F}_q^k$
- Fingerprint $f \in \binom{\mathbb{F}_q}{t}$ *(Here $\binom{\mathbb{F}_q}{t}$ means subsets of size t of $\mathbb{F}_q$)*
- LOCK : $\mathbb{F}_q^k \times \binom{\mathbb{F}_q}{t} \to \binom{\mathbb{F}_q}{n}$, $t \leq n$
- UNLOCK : $\binom{\mathbb{F}_q}{t} \times \binom{\mathbb{F}_q}{n} \to \mathbb{F}_q^k$

Properties:

(i) **c-completeness:** Let $f, f' \in \binom{\mathbb{F}_q}{t}$ such that $|f - f'| \leq c < t$
UNLOCK(LOCK(s, f), f') $= s$

(ii) **soundness:** ”Hard” for an adversary to get s from LOCK(s, f) if its f' is ”far” from f
The notion of ”Hard” and ”far” will be formally defined later