Information Processing Letters 115 (2015) 382–385

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Affine-evasive sets modulo a prime

Divesh Aggarwal

Department of Computer Science, New York University, United States

ARTICLE INFO

Article history:
Received 10 June 2014
Received in revised form 16 October 2014
Accepted 17 October 2014
Available online 23 October 2014
Communicated by M. Yamashita

Keywords:
Cryptography
Non-malleable codes
Coding theory
Tamper-resilient cryptography

ABSTRACT

In this work, we describe a simple and efficient construction of a large subset S of $\mathbb{F}_p$, where p is a prime, such that the set $A(S)$ for any non-identity affine map A over $\mathbb{F}_p$ has small intersection with S.

Such sets, called affine-evasive sets, were defined and constructed in [1] as the central step in the construction of non-malleable codes against affine tampering over $\mathbb{F}_p$, for a prime p. This was then used to obtain efficient non-malleable codes against split-state tampering.

Our result resolves one of the two main open questions in [1]. It improves the rate of non-malleable codes against affine tampering over $\mathbb{F}_p$ from $\log\log p$ to a constant, and consequently the rate for non-malleable codes against split-state tampering for n-bit messages is improved from $n^6 \log^7 n$ to n^6.

1. Introduction

Non-malleable codes (NMCs) NMCs were introduced in [5] as a beautiful relaxation of error-correction and error-detection codes. Informally, given a tampering family $\mathcal{F}$, an NMC $(\mathsf{Enc}, \mathsf{Dec})$ against $\mathcal{F}$ encodes a given message m into a codeword $c \leftarrow \mathsf{Enc}(m)$ in a way that, if the adversary modifies m to $c' = f(c)$ for some $f \in \mathcal{F}$, then the message $m' = \mathsf{Dec}(c')$ is either the original message m, or a completely "unrelated value". As has been shown by the recent progress [5,9,4,1,7,6,2,3] NMCs aim to handle a much larger class of tampering functions $\mathcal{F}$ than traditional error-correcting or error-detecting codes, at the expense of potentially allowing the attacker to replace a given message x by an unrelated message x'. NMCs are useful in situations where changing x to an unrelated x' is not useful for the attacker (for example, when x is the secret key for a signature scheme.)

Split-state model NMCs do not exist for the class of all functions $\mathcal{F}_{\mathsf{all}}$. In particular, it does not include functions of the form $f(c) := \mathsf{Enc}(h(\mathsf{Dec}(c)))$, since $\mathsf{Dec}(f(\mathsf{Enc}(m))) = h(m)$ is clearly related to m. One of the largest and practically relevant tampering families for which we can construct NMCs is the so-called split-state tampering family where the codeword is split into two parts $c_1 \| c_2$, and the adversary is only allowed to tamper with c_1, c_2 independently to get $f_1(c_1) \| f_2(c_2)$. A lot of the aforementioned results [9,4,1,3,6] have studied NMCs against split-state tampering. Aggarwal et al. [1] gave the first (and the only one so far) information-theoretically secure construction in the split-state model from n-bit messages to $n^7 \log^7 n$-bit codewords (i.e., code rate $n^6 \log^7 n$). The security proof of this scheme relied on an amazing property of the inner-product function modulo a prime, that was proved using results from additive combinatorics.

Affine-evasive sets and our result One of the crucial steps in the construction of [1] was the construction of NMC against affine tampering modulo p. This was achieved by constructing an affine-evasive set of size $p^{1/\log\log p}$ modulo a prime p. It was asked as an open question whether there exists an affine-evasive set of size $p^{\Theta(1)}$, which will imply constant rate NMC against affine-tampering and rate n^6

E-mail address: divesha@cs.nyu.edu.

http://dx.doi.org/10.1016/j.ipl.2014.10.015
0020-0190/

NMC against split-state tampering.[1] We resolve this question in the affirmative by giving an affine-evasive set of size $\Theta(\frac{p^{1/4}}{\log p})$.

2. Explicit construction

For any set $S \subset \mathbb{Z}$, let $aS + b = \{as + b \mid s \in S\}$. By $S \bmod p \subseteq \mathbb{F}_p$, we denote the set of values of S modulo p.

We first define an affine-evasive set $S \subseteq \mathbb{F}_p$.

Definition 1. A non-empty set $S \subseteq \mathbb{F}_p$ is said to be (γ, ν)-*affine-evasive* if $|S| \le \gamma p$, and for any $(a, b) \in \mathbb{F}_p^2 \setminus \{(1, 0)\}$, we have

$$\left|S \cap \left(aS + b \pmod p\right)\right| \le \nu |S|.$$

Now we give a construction of an affine-evasive set.

Let $Q := \{q_1, \dots, q_t\}$ be the set of all primes less than $\frac{1}{2}p^{1/4}$. Define $S \subset \mathbb{F}_p$ as follows:

$$S := \left\{ \frac{1}{q_i} \pmod p \;\middle|\; i \in [t] \right\}. \tag{1}$$

Thus, S has size $\Theta(\frac{p^{1/4}}{\log p})$ by the prime number theorem.

Theorem 1. *For any prime p, the set S defined in Eq. (1) is $(\frac{1}{2}p^{-3/4}, O(p^{-1/4} \cdot \log p))$-affine-evasive.*

Proof. Clearly,

$$|S| = t \le \frac{1}{2}p^{1/4} = \frac{1}{2}p^{-3/4} \cdot p.$$

Fix $a, b \in \mathbb{F}_p$, such that $(a, b) \ne (1, 0)$. Now, we show that $|S \cap (aS + b \pmod p)| \le 3$. Assume, on the contrary, that there exist distinct $\alpha_i \in Q$ for $i \in \{0, 1, 2, 3\}$ such that $1/\alpha_i \pmod p \in S \cap (aS + b \pmod p)$. We have

$$\frac{a}{\beta_i} + b = \frac{1}{\alpha_i} \pmod p \quad \text{for } i = 0, 1, 2, 3, \tag{2}$$

where $\beta_i, \alpha_i \in Q$ for $i \in \{0, 1, 2, 3\}$, and $\alpha_i \ne \alpha_j$ for any $i \ne j$.

For any i, if $\beta_i = \alpha_i$, then $b \cdot \beta_i = 1 - a \bmod p$, which has at most one solution (since we assume $(a, b) \ne (1, 0)$). Thus, without loss of generality, we assume that $\beta_i \ne \alpha_i$, for $i \in \{1, 2, 3\}$, and $\beta_1 < \beta_2 < \beta_3$.

From Eq. (2), we have that

$$\frac{\frac{a}{\beta_1} + b - \frac{a}{\beta_2} - b}{\frac{a}{\beta_1} + b - \frac{a}{\beta_3} - b} = \frac{\frac{1}{\alpha_1} - \frac{1}{\alpha_2}}{\frac{1}{\alpha_1} - \frac{1}{\alpha_3}} \pmod p,$$

which on simplification implies

$$(\alpha_3 - \alpha_1)(\beta_2 - \beta_1)\beta_3\alpha_2 = (\alpha_2 - \alpha_1)(\beta_3 - \beta_1)\beta_2\alpha_3 \pmod p.$$

Note that both the left-hand and right-hand side of the above equation takes values between $\frac{-p}{16}$ and $\frac{p}{16}$, and hence the equality holds in $\mathbb{Z}$ (and not just in $\mathbb{Z}_p$).

$$(\alpha_3 - \alpha_1)(\beta_2 - \beta_1)\beta_3\alpha_2 = (\alpha_2 - \alpha_1)(\beta_3 - \beta_1)\beta_2\alpha_3. \tag{3}$$

By Eq. (3), we have that β_3 divides $(\alpha_2 - \alpha_1)(\beta_3 - \beta_1)\beta_2\alpha_3$. Clearly, β_3 is relatively prime to α_3, β_2, and $\beta_3 - \beta_1$. Therefore, β_3 divides $(\alpha_2 - \alpha_1)$. This implies

$$\beta_3 \le |\alpha_2 - \alpha_1|. \tag{4}$$

Also, from Eq. (3), we have that α_2 divides $(\alpha_2 - \alpha_1)(\beta_3 - \beta_1)\beta_2\alpha_3$, which by similar reasoning implies α_2 divides $\beta_3 - \beta_1$. Thus, using that $\beta_3 > \beta_1$,

$$0 < \alpha_2 \le \beta_3 - \beta_1 < \beta_3. \tag{5}$$

Similarly, we can obtain α_1 divides $\beta_3 - \beta_2$, which implies

$$0 < \alpha_1 \le \beta_3 - \beta_2 < \beta_3. \tag{6}$$

Eqs. (5) and (6) together imply that $|\alpha_2 - \alpha_1| < \beta_3$, which contradicts Eq. (4). □

3. Affine-evasive function and efficient NMCs

Affine-evasive function We recall here the definition of affine-evasive functions from [1]. Affine-evasive functions immediately give efficient construction of NMCs against affine-tampering.

Definition 2. A surjective function $h : \mathbb{F}_p \mapsto \mathcal{M} \cup \{\perp\}$ is called (γ, δ)-*affine-evasive* if for any $a, b \in \mathbb{F}_p$ such that $a \ne 0$, and $(a, b) \ne (1, 0)$, and for any $m \in \mathcal{M}$,

1. $\Pr_{U \leftarrow \mathbb{F}_p}(h(aU + b) \ne \perp) \le \gamma$.
2. $\Pr_{U \leftarrow \mathbb{F}_p}(h(aU + b) \ne \perp \mid h(U) = m) \le \delta$.
3. A uniformly random X such that $h(X) = m$ is efficiently samplable.

We now mention a result that shows that we can construct an affine-evasive function from an affine-evasive set S.

Lemma 1. *(See [1, Claim 5].) Let $S \subseteq \mathbb{F}_p$ be a (γ, ν)-affine-evasive set with $\nu \cdot K \le 1$, and K divides $|S|$.[2] Furthermore, let S be ordered such that for any i, the i-th element is efficiently computable in $O(\log p)$. Then there exists a $(\gamma, \nu \cdot K)$-affine-evasive function $h : \mathbb{F}_p \mapsto \mathcal{M} \cup \{\perp\}$.*

Note that the above result requires that for any i, the i-th element of S is efficiently computable for some ordering of the set S. This is not possible for our construction since for our construction this would mean efficiently sampling the i-th largest prime. However, this requirement was made just to make sure that h^{-1} is efficiently samplable. We circumvent this problem by giving a slightly modified definition of the affine-evasive function h in the proof of Lemma 2. Before proving this, we state the following result that we will need.

[1] Under a plausible conjecture, this will imply constant rate NMC against split-state tampering. See Theorem 5 for more details.

[2] The assumption K divides $|S|$ is just for simplicity.