A Note on Lower Bounds for Non-interactive Message Authentication Using Weak Keys

Divesh Aggarwal [*]
Divesh.Aggarwal@epfl.ch

Alexander Golovnev [†]
alexgolovnev@gmail.com

Abstract

In this note, we prove lower bounds on the amount of entropy of random sources necessary for secure message authentication. We consider the problem of non-interactive c-time message authentication using a weak secret key having min-entropy k. We show that existing constructions using $(c+1)$-wise independent hash functions are optimal.

This result resolves one of the main questions left open by the work of Dodis and Spencer [2] who considered this problem for one-time message authentication of one-bit messages.

1 Introduction

1.1 Non-interactive Message Authentication

In this note, we revisit the problem of non-interactive message authentication: where Alice and Bob share a weak secret key $R \in \{0,1\}^n$, and Alice wants to communicate up to c messages authentically to Bob over a channel controlled by the adversary Eve. This problem is known to have an easy solution with ε-security for $\varepsilon < 1$ using one of various possible universal hash functions, or more generally $c+1$-wise independent hash functions (see, for example, [5, 4] that give construction for $c = 1$). These solutions, however, require that the min-entropy $\mathbf{H}_\infty(R)$ of the source R is at least $\frac{cn}{c+1} + \log(\frac{1}{\varepsilon})$.

Dodis and Spencer [2] studied this problem with the goal of finding a lower bound on the min-entropy of R. They showed that for any integer $k \geq \frac{n}{2}$, and any one-round message authentication protocol for one-bit messages, there exists a k-flat source R such that the advantage of the adversary

[*]Department of Computer Science, EPFL
[†]New York University

in forging the tag is at least $2^{n/2-k}$, or in other words, $\mathbf{H}_\infty(R) \geq \frac{n}{2} + \log(\frac{1}{\varepsilon})$. This showed that the construction using universal hash functions is optimal for one-bit messages. However, the bound for many time message authentication is still far from optimal and this was left as one of the main open questions in [2]. Specifically, the authors state that it is interesting to extend their quantitative results for private-key encryption and especially authentication to larger than one-bit message spaces. While this question has subsequently been almost resolved for the case of private-key encryption [1], it has remained open for the case of private-key authentication.

1.2 Our contribution and Comparison with [2]

We answer this open question in the affirmative, i.e., that for any integer $k \geq \frac{cn}{c+1}$, and any c-round message authentication protocol, there exists a k-flat source R such that the advantage of the adversary in forging the tag is at least $2^{cn/(c+1)-k}$, or in other words, $\mathbf{H}_\infty(R) \geq \frac{cn}{c+1} + \log(\frac{1}{\varepsilon})$. Our proof uses a simple idea based on the chain rule for Shannon entropy.

In comparison, the result of [2] was proved by considering a bipartite multigraph with the edges corresponding to the keys and the vertices on each part corresponding to the tags of the bit 0 and 1, respectively. They then partitioned their proof into two cases (i) where there are few tags corresponding to the bit 0, in which case it is easy to guess $\mathsf{Tag}(0, R)$, and (ii) where there are many tags corresponding to the bit 0, but where knowing $\mathsf{Tag}(0, R)$ gives significant information about $\mathsf{Tag}(1, R)$. It seems that one might be able to generalize this idea to prove a lower bound for c-time message authentication by considering $c+1$ cases as opposed to considering two cases for $c = 1$. However, the case analysis becomes significantly more involved due to the combinatorial nature of the proof, and perhaps this is a reason why the question has remained open for so long.

2 Preliminaries

For a set S, we let U_S denote the uniform distribution over S. For an integer $m \in \mathbb{N}$, we let U_m denote the uniform distribution over $\{0,1\}^m$, the bit-strings of length m. For a distribution or random variable X we write $x \leftarrow X$ to denote the operation of sampling a random x according to X. For a set S, we write $s \leftarrow S$ as shorthand for $s \leftarrow U_S$.

2.1 Entropy Definitions

The *prediction probability* of a random variable X is defined as

$$\mathsf{Pred}(X) := \max_x \Pr[X = x].$$

The *min-entropy* of X is defined as

$$\mathbf{H}_\infty(X) := -\log \mathsf{Pred}(X).$$

We say that a random variable X is an (n, k)-*source* if $X \in \{0,1\}^n$ and $\mathbf{H}_\infty(X) \geq k$. We also define *conditional prediction probability* of a random variable X conditioned on another random variable Z as

$$\begin{aligned} \mathsf{Pred}(X|Z) &:= \mathsf{E}_{z \leftarrow Z}\left[\ \max_x \Pr[X = x|Z = z]\ \right] \\ &= \mathsf{E}_{z \leftarrow Z}\left[2^{-\mathbf{H}_\infty(X|Z=z)}\right] . \end{aligned}$$

The *conditional min-entropy* of X is defined as

$$\mathbf{H}_\infty(X|Z) := -\log \mathsf{Pred}(X|Z).$$

Also, the Shannon entropy $\mathbf{H}_1(X)$ of a random variable X is defined as

$$\mathbf{H}_1(X) := -\sum_x \Pr[X = x] \log \Pr[X = x] .$$

The conditional Shannon entropy of a random variable X conditioned on another random variable Z is defined as

$$\begin{aligned} \mathbf{H}_1(X|Z) &:= \mathsf{E}_{z \leftarrow Z} \mathbf{H}_1(X|Z = z) \\ &= -\mathsf{E}_{z \leftarrow Z} \sum_x \Pr[X = x|Z = z] \log \Pr[X = x|Z = z] . \end{aligned}$$

We will need the following standard facts about (conditional) min-entropy, and (conditional) Shannon entropy.

Fact 1. *Let X, Y, Z be arbitrary random variables, and let f be an arbitrary function. Then the following hold*

1. $\mathbf{H}_\infty(X|Z) \geq \mathbf{H}_\infty(f(X)|Z)$, *and* $\mathbf{H}_1(X|Z) \geq \mathbf{H}_1(f(X)|Z)$.
2. $\mathbf{H}_1(X, Y|Z) = \mathbf{H}_1(X|Y, Z) + \mathbf{H}_1(Y|Z)$.
3. $\mathbf{H}_1(X|Z) \geq \mathbf{H}_\infty(X|Z)$.

We remark here that the definition of the conditional Shannon entropy is fairly standard, but there are other alternative definitions in the literature for conditional min-entropy. However, our proposed definition is by now fairly standard. We direct the reader to [3] which contains a comprehensive discussion on conditional entropies, and proves Fact 1 among several other results.

2.2 Message Authentication Codes

In order to define a message authentication code, we first introduce the following game $\mathsf{G}_c(r)$. For a given function $\mathsf{Tag} : \mathcal{M} \times \{0,1\}^n \mapsto \mathcal{T}$ and a fixed secret key $r \in \{0,1\}^n$, an adversary Eve is allowed to make at most c adaptive queries $\mu_1, \ldots, \mu_c$ to $\mathsf{Tag}(\cdot, r)$. We say that Eve wins the game if she outputs a pair (μ_{c+1}, σ), such that $\mathsf{Tag}(\mu_{c+1}, r) = \sigma$ and $\mu_{c+1} \notin \{\mu_1, \ldots, \mu_c\}$. We define the advantage of Eve in this game as

$$\mathsf{Adv}_c^{\mathsf{Eve}}(r) = \Pr[\mathsf{Eve} \text{ wins } \mathsf{G}_c(r)].$$

Definition 1. *A function* $\mathsf{Tag} : \mathcal{M} \times \{0,1\}^n \mapsto \mathcal{T}$ *is called a c-time* (n, k, ε)*-secure message authentication code, if for any distribution* R *on* $\{0,1\}^n$ *with* $\mathbf{H}_\infty(R) \geq k$*, for any computationally unbounded adversary* Eve*,*

$$\mathrm{E}_{r \leftarrow R}[\mathsf{Adv}_c^{\mathsf{Eve}}(r)] \leq \varepsilon.$$

2.3 k-wise Independent Hash Functions

Here we define and give a well-known construction of k-wise independent hash functions.

Definition 2. *A function* $H : \mathcal{X} \times \mathcal{R} \mapsto \mathcal{Y}$ *is said to be a k-wise independent hash function if for all* $y_1, \ldots, y_k \in \mathcal{Y}$*, and all distinct* $x_1, \ldots, x_k \in \mathcal{X}$*,*

$$\Pr_{r \leftarrow \mathcal{R}}(H(x_1, r) = y_1 \ \wedge \ \cdots \ \wedge \ h(x_k, r) = y_k) = \frac{1}{|\mathcal{Y}|^k} \ .$$

Lemma 1 (folklore)**.** *Let* k *be a positive integer, and let* $\mathcal{X} = \mathcal{Y} = \mathbb{F}$*, and* $\mathcal{R} = \mathbb{F}^k$ *for some finite field* $\mathbb{F}$*. Then the function* $H : \mathcal{X} \times \mathcal{R} \mapsto \mathcal{Y}$ *given by*

$$H(x, (r_0, \ldots, r_{k-1})) := r_0 + r_1 \cdot x + \cdots + r_{k-1} \cdot x^{k-1}$$

is a k-wise independent hash function.

3 Tight Bound for c-time MACs

In this section, we prove a lower bound on the error-probability ε for c-time message authentication protocol for deterministic functions Tag.

Theorem 1. *Let* Tag *be a* c*-time* (n, k, ε)*-secure message authentication code where* $\mathsf{Tag} : \mathcal{M} \times \{0,1\}^n \mapsto \mathcal{T}$*. Then we have the following.*

1. *If* $k \le \frac{cn}{c+1}$ *then* $\varepsilon = 1$*;*
2. *If* $k > \frac{cn}{c+1}$ *then* $\varepsilon \ge 2^{\frac{cn}{c+1} - k}$.

Proof. Let U be an n-bit uniformly random string, and let $\mu_1, \ldots, \mu_{c+1} \in \mathcal{M}$ be fixed distinct messages. Note that $\mathbf{H}_1(U) = n$. Using Fact 1 multiple times, we get

$$\begin{aligned}
n =& \mathbf{H}_1(U) \ge \mathbf{H}_1\left(\mathsf{Tag}(\mu_1, U), \ldots, \mathsf{Tag}(\mu_{c+1}, U)\right) \\
=& \mathbf{H}_1\left(\mathsf{Tag}(\mu_1, U)\right) + \mathbf{H}_1\left(\mathsf{Tag}(\mu_2, U), \ldots, \mathsf{Tag}(\mu_{c+1}, U) | \mathsf{Tag}(\mu_1, U)\right) \\
=& \ldots \\
=& \sum_{i=1}^{c+1} \mathbf{H}_1\left(\mathsf{Tag}(\mu_i, U) | \mathsf{Tag}(\mu_1, U), \ldots, \mathsf{Tag}(\mu_{i-1}, U)\right) \\
\ge& \sum_{i=1}^{c+1} \mathbf{H}_\infty\left(\mathsf{Tag}(\mu_i, U) | \mathsf{Tag}(\mu_1, U), \ldots, \mathsf{Tag}(\mu_{i-1}, U)\right) \ .
\end{aligned}$$

Therefore, there exists $i \in \{1, \ldots, c+1\}$, such that

$$\mathbf{H}_\infty\left(\mathsf{Tag}(\mu_i, U) | \mathsf{Tag}(\mu_1, U), \ldots, \mathsf{Tag}(\mu_{i-1}, U)\right) \le \frac{n}{c+1} \ .$$

We fix an i satisfying this ineqaulity. For any $\mathbf{t} = (t_1, \ldots, t_{i-1}) \in \mathcal{T}^{i-1}$, let $\mathcal{E}(\mathbf{t})$ be a shorthand for the event that $\mathsf{Tag}(\mu_j, U) = t_j$ for $1 \le j < i$. From the definition of conditional min-entropy, we get the following.

$$\begin{aligned}
2^{-\frac{n}{c+1}} &\le \mathrm{E}_{\mathbf{t} \in \mathcal{T}^{i-1}} \max_{t_i \in \mathcal{T}} \Pr\left[\mathsf{Tag}(\mu_i, U) = t_i | \mathcal{E}(\mathbf{t})\right] \\
&= \sum_{\mathbf{t} \in \mathcal{T}^{i-1}} \Pr[\mathcal{E}(\mathbf{t})] \cdot \max_{t_i \in \mathcal{T}} \Pr[\mathsf{Tag}(\mu_i, U) = t_i | \mathcal{E}(\mathbf{t})] \\
&= \sum_{\mathbf{t} \in \mathcal{T}^{i-1}} \max_{t_i \in \mathcal{T}} \Pr[\mathsf{Tag}(\mu_j, U) = t_j \text{ for } 1 \le j \le i] \ . \qquad (1)
\end{aligned}$$

For every fixed $\mathbf{t} = (t_1, \ldots, t_{i-1}) \in \mathcal{T}^{i-1}$, let $\mu_{\mathbf{t}}$ be the most probable value of $\mathsf{Tag}(\mu_i, U)$ given $\mathsf{Tag}(\mu_j, U) = t_j$ for $1 \le j < i$. Intuitively, we want to choose a distribution over the set of keys so that $\mathsf{Tag}(\mu_j, U) = t_j$ for $1 \leq j < i$ implies that $\mathsf{Tag}(\mu_i, U) = \mu_{\mathbf{t}}$. Then, given tags for $\mu_1, \ldots, \mu_{i-1}$, we can always guess the tag for μ_i. Let $\mathcal{K}_{\mathbf{t}}$ be the set of keys corresponding to $\mu_{\mathbf{t}}$, i.e.,

$$\mathcal{K}_{\mathbf{t}} = \left\{ r \in \{0,1\}^n | \mathsf{Tag}(\mu_i, r) = \mu_{\mathbf{t}}, \mathsf{Tag}(\mu_j, r) = t_j \text{ for } 1 \leq j < i \right\} .$$

Let also

$$\mathcal{K} = \bigcup_{\mathbf{t} \in \mathcal{T}^{i-1}} \mathcal{K}_{\mathbf{t}}.$$

From inequality (1),

$$|\mathcal{K}| \geq 2^n \cdot 2^{\frac{-n}{c+1}} = 2^{\frac{cn}{c+1}} .$$

If $2^k \leq |\mathcal{K}|$, then let $\mathcal{R}$ be an arbitrary 2^k element subset of $\mathcal{K}$. Otherwise, let

$$\mathcal{R} = \mathcal{K} \cup \mathcal{K}' ,$$

where $\mathcal{K}'$ is a set of arbitrary keys from the set $\{0,1\}^n \backslash \mathcal{K}$, such that $|\mathcal{R}| = 2^k$.

We claim that if R is uniformly distributed on $\mathcal{R}$, then there exists a strategy for Eve such that the advantage in guessing $\mathsf{Tag}(\mu_i, r)$ given $\mathsf{Tag}(\mu_1, r), \ldots, \mathsf{Tag}(\mu_{i-1}, r)$ is at least $2^{\frac{cn}{n+1} - k}$ if $k > \frac{cn}{n+1}$, and 1, otherwise. To see this, notice that for any $r \in \mathcal{K}$, there is a unique value of $\mathsf{Tag}(\mu_i, r)$ given $\mathsf{Tag}(\mu_1, r), \ldots, \mathsf{Tag}(\mu_{i-1}, r)$. Let the strategy of Eve be to guess this unique tag assuming $R \in \mathcal{K}$. Then, Eve succeeds with probability 1 if $R \in \mathcal{K}$, and hence the advantage of Eve is

$$\varepsilon \geq \frac{|\mathcal{R} \cap \mathcal{K}|}{2^k} \geq \frac{\min\left(2^k, 2^{\frac{cn}{c+1}}\right)}{2^k} .$$

The statement of the theorem now follows. □

It is well-known that the bound from Theorem 1 can be achieved by using a family of $c+1$-wise independent hash functions. For the sake of completeness, we present this construction below.

Lemma 2 (folklore)**.** *Let $\mathbb{F}$ be a finite field, and let $\mathcal{M} = \mathcal{T} = \mathbb{F}$, and let the set of keys be $\mathbb{F}^{c+1}$ with $n = (c+1)\log|\mathbb{F}|$. Then the function* Tag : $\mathcal{M} \times \mathbb{F}^{c+1} \mapsto \mathcal{T}$ *defined as:*

$$\mathsf{Tag}\left(\mu, (r_0, \ldots, r_c)\right) := r_0 + r_1 \cdot \mu + \cdots + r_c \cdot \mu^c$$

is a c-time $(n, k, 2^{\frac{cn}{c+1} - k})$-secure message authentication code.

Proof. Let U be uniform in $\mathbb{F}^{c+1}$. For any fixed strategy of Eve, and $r \in \mathbb{F}^{c+1}$, let $f(r)$ denote $\mathsf{Adv}_c^{\mathsf{Eve}}(r)$. Let $\mu_1, \ldots, \mu_{c+1}$ be arbitrary distinct messages in $\mathcal{M}$. By Lemma 1, we have that for any $\sigma \in \mathcal{T}$, the probability that $\mathsf{Tag}(\mu_{c+1}, U) = \sigma$ given $\mathsf{Tag}(\mu_1, U), \ldots, \mathsf{Tag}(\mu_c, U)$ is at most $\frac{1}{|\mathbb{F}|} = 2^{-n/(c+1)}$. Hence,

$$\mathrm{E}_{r \leftarrow U}[f(r)] \leq 2^{-\frac{n}{c+1}} .$$

Now, consider a random key $R \in \mathbb{F}^{c+1}$, such that $\mathbf{H}_\infty(R) \geq k$. Then

$$\begin{aligned}
\mathrm{E}_{r \leftarrow R}[f(r)] &= \sum_{r \in \mathbb{F}^{c+1}} \Pr(R = r) \cdot f(r) \\
&\leq \max_{r \in \mathbb{F}^{c+1}} \Pr(R = r) \sum_{r \in \mathbb{F}^{c+1}} f(r) \\
&\leq 2^{-k} \cdot 2^n \cdot \mathrm{E}_{r \leftarrow U}[f(r)] \\
&\leq 2^{n-k} \cdot 2^{-\frac{n}{c+1}} \\
&= 2^{\frac{cn}{c+1} - k} ,
\end{aligned}$$

as needed. ∎

References

[1] Carl Bosley and Yevgeniy Dodis. Does privacy require true randomness? In *Theory of Cryptography*, pages 1–20. Springer, 2007.

[2] Yevgeniy Dodis and Joel Spencer. On the (non)universality of the one-time pad. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 376–385. IEEE Computer Society, 2002.

[3] Serge Fehr and Stefan Berens. On the conditional Rényi entropy. *Information Theory, IEEE Transactions on*, 60(11):6801–6810, Nov 2014.

[4] Tor Helleseth and Thomas Johansson. Universal hash functions from exponential sums over finite fields and Galois rings. In *Advances in Cryptology—CRYPTO'96*, pages 31–44. Springer, 1996.

[5] Douglas Stinson. Universal hashing and authentication codes. *Designs, Codes and Cryptography*, 4(3):369–380, 1994.