1 Preliminaries

2 A sketch for the boys

2.1 Graph Label Randomization

Say that we have a sparse graph $\mathcal{G} = (V, E)$ such that $|V| = n$ and $\forall v \in V, \deg(v) \leq d$.

We want to "randomize" the labels of the graph via a poly-time embedding function ϕ such that the embeddings are indistinguishable from a truly random embedding, Φ.

We model Φ as function from V to $\{0,1\}^{c \cdot \lambda}$ for some small constant c such that

$$I_{\mathtt{min}}(\phi(V) \mid V = v) \geq 2 \cdot \lambda.$$

Indeed, we do not require that the labels are uniformly random, but rather that each label is "random enough", containing at least 2λ bits of min-entropy.

We can now propose a game to characterize the pseudo-random embedding ϕ. For any PPT adversary, $\mathcal{A}$,

$$\Big| \mathbf{Pr}\left[\mathcal{A}(\phi(v_1), \ldots \phi(v_i)) = 1\right] - \mathbf{Pr}\left[\mathcal{A}(\Phi(v_1), \ldots \Phi(v_i)) = 1\right] \Big| \leq \mathtt{negl}(\lambda) \tag{1}$$

for some $i \in \mathrm{poly}(\lambda)$.

The above game may prove to be uninteresting as we can simply describe ϕ to be a PRF which takes in the vertex label and outputs a pseudo-random string of length $c \cdot \lambda$.

This brings us to our notion of graph-label randomization obfuscation (GRO).

Definition 2.1 (Graph-label randomization obfuscation (GRO, pronounced grow))**.** Given a circuit C_Γ realizing $\phi \circ \Gamma \circ \phi^{-1} : \{0,1\}^{c \cdot \lambda} \to \{0,1\}^{c \cdot d \cdot \lambda}$ (the neighbor function for the embedded space) and any polynomial time adversary,

$$\Big| \mathbf{Pr}\left[\mathcal{A}(\phi(v_1), \ldots \phi(v_i), C_\Gamma) = 1\right] - \mathbf{Pr}\left[\mathcal{A}(\Phi(v_1), \ldots \Phi(v_i), C_\Gamma) = 1\right] \Big| \leq \mathtt{negl}(\lambda) \tag{2}$$

Sparse Graph Obfuscation

September 24, 2023

Abstract

References