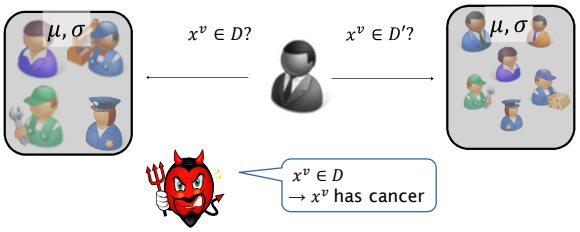
Membership Inference Against DNA Methylation Databases: Attacks and Defenses

Inken Hagestedt[1], Mathias Humbert[2], Pascal Berrang[1], Irina Lehmann[3], Roland Elis[4], Michael Backes[1], Yang Zhang[1]

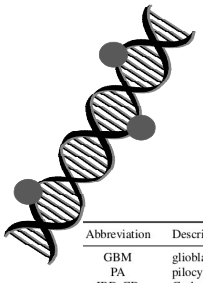
[1]CISPA Helmholtz Center for Information Security [2]Swiss Data Science Center [3]Helmholtz Centre for Environmental Research Leipzig, UFZ, [4]German Cancer Research Center, DKFZ

The Question

Are membership inference attacks possible given only mean μ and standard deviation σ ?



The Data



- DNA methylation: additional molecule (methyl group) attached to DNA
- represented as value in [0, 1]
- methylation patterns vary between tissues, due to environmental factors and due to diseases

Abbreviation	Description	Tissue Type	Number of Patients	GSE identifier
GBM	glioblastoma	brain cancer	136	GSE36278
PA	pilocytic astrocytoma	brain cancer	61	GSE44684
IBD CD	Crohn's disease	blood	77	GSE87640
IBD UC	ulcerative colitits	blood	79	GSE87640
BC	breast cancer	breast cancer	892	-[3]
WGBS	genome and methylation data	blood	75	not publicly available

Statistics-based Attack

→ two statistical tests:

mean only:

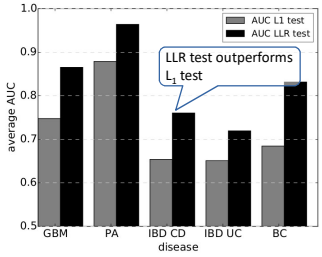
$$L_1(x^j) = |x^j - \mu_r^j| - |x^j - \mu_c^j|$$

$$L_1(x) = \underset{j \in 0,\ldots,n}{\text{ttest}} L_1(x^j)$$

mean reference; mean case; combination of all methylation values with students t-test

mean and standard deviation:

$$LLR(x) = \sum_{j=1}^{n} \frac{\left(x^j - \mu_r^j\right)^2 - \left(x^j - \mu_c^j\right)^2}{2\,(\sigma^j)^2}$$



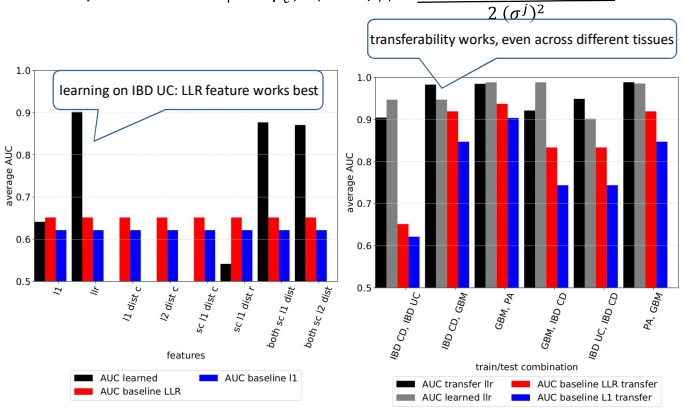
ML-based Attack

→ learn which distance magnitude is informative

distance features: $|x^j - \mu_c^j| \quad \left(x^j - \mu_c^j\right)^2$

scaled versions: $\frac{|x^j - \mu_c^j|}{\sigma^j} \quad \frac{\left(x^j - \mu_c^j\right)^2}{(\sigma^j)^2}$

test-inspired features: $|x^j - \mu_c^j| - |x^j - \mu_r^j| \quad \frac{\left(x^j - \mu_c^j\right)^2 - \left(x^j - \mu_r^j\right)^2}{2\,(\sigma^j)^2}$



Genome-based Attack

→ exploit correlation between genome and methylation:

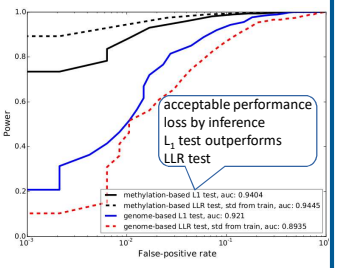
$$f_g(x^j) = p(\mathrm{X_j} = \mathrm{x^j} \mid \mathrm{G} = \mathrm{g}) = \frac{1}{\sqrt{2\pi}\,\sigma_{j,g}} \exp\left(\frac{-(x^j - \mu_{j,g})^2}{(\sigma_{j,g})^2}\right)$$

probability of metylation value modeled by Gaussian

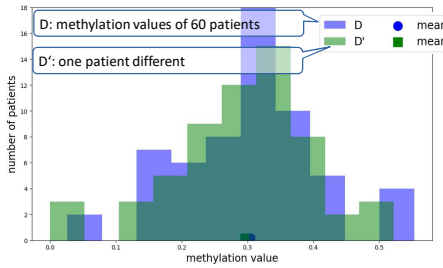
same LLR test on all related positions:

$$LLR(g) = \sum_{j=1}^{m_c} \frac{\left(\mu_{j,g} - \mu_r^j\right)^2 - \left(\mu_{j,g} - \mu_c^j\right)^2}{2\,(\sigma^j)^2}$$

expected methylation value given the genome



Defense with Differential Privacy



difference informative

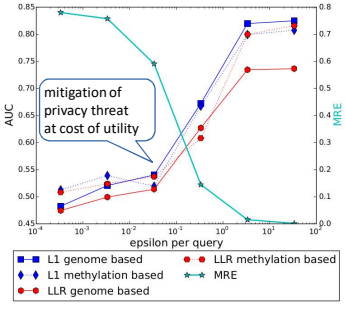
→ output a random mean

that hides the contribution of the changed entry

formally: $\Pr[M(mean(D)) = \mu] \leq e^{\epsilon} \Pr[M(mean(D')) = \mu]$

where $M(mean(D)) = mean(D) + Lap\left(\frac{m}{n}\right)$

number of positions here: 300.000; number of patients here: 60; privacy parameter



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY
SDSC
HELMHOLTZ ZENTRUM FÜR UMWELTFORSCHUNG UFZ
dkfz. GERMAN CANCER RESEARCH CENTER IN THE HELMHOLTZ ASSOCIATION

inken.hagestedt@cispa.saarland
yang.zhang@cispa.saarland