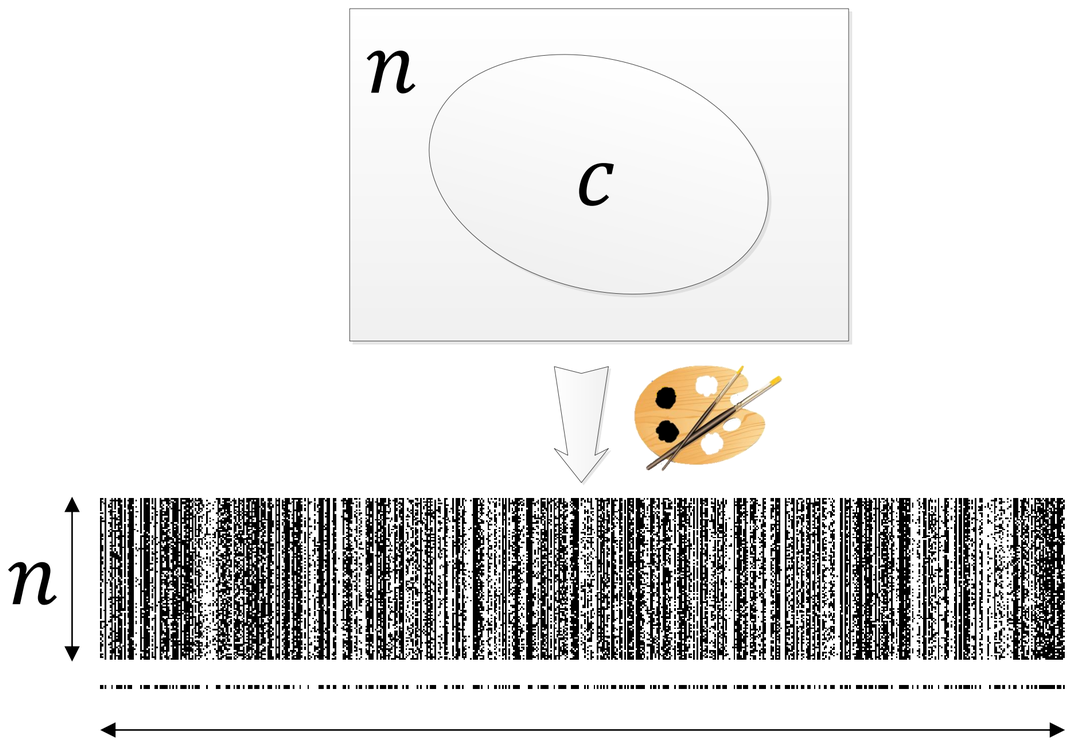
irdeto
TU/e Technische Universiteit Eindhoven University of Technology

Dynamic Traitor Tracing for Arbitrary Alphabets:

Divide and Conquer

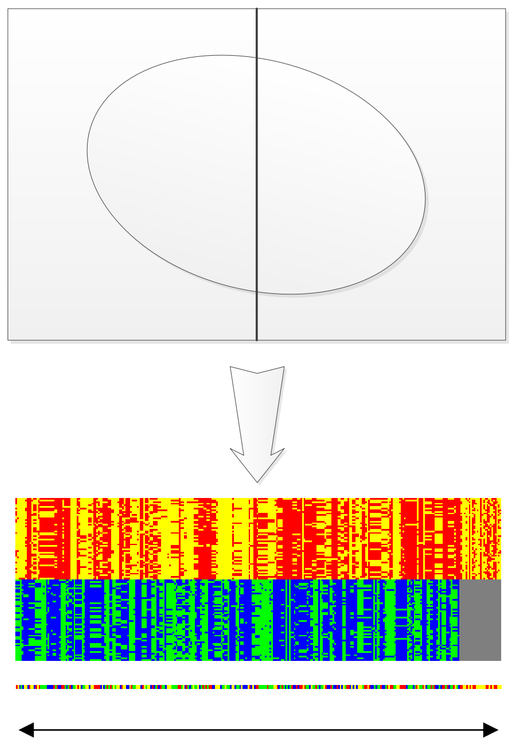
Thijs Laarhoven (TU/e), Jan-Jaap Oosterwijk (TU/e), Jeroen Doumen (Irdeto)

Introduction



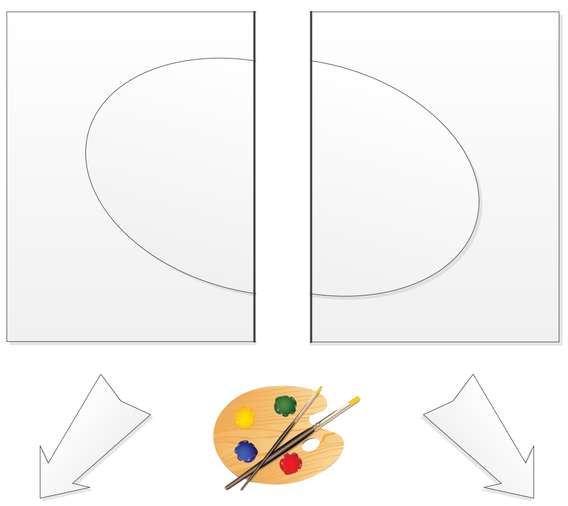
$$l = c^2 \ln\left(\frac{n}{\varepsilon}\right)$$

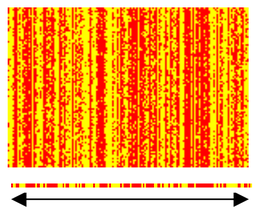
Conquer



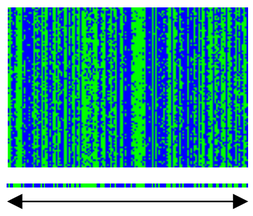
$$l_{NEW} \approx l_L + l_R$$

Divide



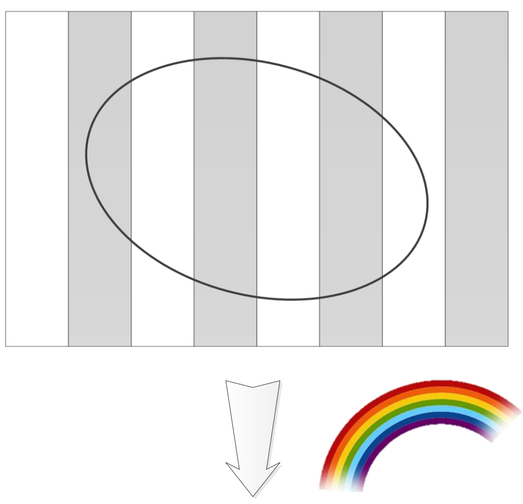


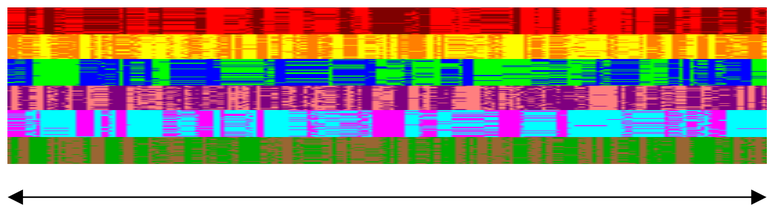
$$l_L \approx \left(\frac{c}{2}\right)^2 \ln\left(\frac{n}{2\varepsilon}\right)$$



$$l_R \approx \left(\frac{c}{2}\right)^2 \ln\left(\frac{n}{2\varepsilon}\right)$$

Generalization





$$l \approx \frac{c^2}{q} \ln\left(\frac{n}{\varepsilon}\right)$$

References

- A. Fiat and T. Tassa, "*Dynamic Traitor Tracing*", *J. Cryptology*, vol. 14, no. 3, 2001.
- T. Laarhoven et al., "*Dynamic Tardos Traitor Tracing Schemes*", submitted for publication. Available at http://arxiv.org/abs/1111.3597
- G. Tardos, "*Optimal Probabilistic Fingerprint Codes*", Proc. 35th ACM Symp. on Theory of Computing, 2003.