A metric space of test distributions for DPA and SZK proofs*

C.T.J. Dodson

Department of Mathematics, UMIST, Manchester M60 1QD, UK

S.M. Thompson

platform^7 seven, 1-2 Finsbury Square, London EC2A 1AA, UK

April 18, 2000

Abstract

Differential Power Analysis (DPA) methods and Statistical Zero-Knowledge (SZK) proofs depend on discrimination between noisy samples drawn from pairs of closely similar distributions. In some cases the distributions resemble truncated Gaussians; sometimes one distribution is uniform. A log-gamma family of probability density functions provides a 2-dimensional metric space of distributions with compact support on $[0, 1]$, ranging from the uniform distribution to symmetric unimodular distributions of truncated normal-type with arbitrarily small variance. Illustrative calculations are provided.

In a recent review, Kocher et al. [3] show the effectiveness of Differential Power Analysis in breaking encryption procedures using correlations between power consumption and data bit values during processing, claiming that most smart cards reveal their DES keys using fewer than 15 power traces.

Chari et al. [1] provided a probabilistic encoding (secret sharing) scheme for effectively secure computation. They obtained lower bounds on the number of power traces needed to distinguish distributions statistically, under certain assumptions about Gaussian noise functions. DPA attacks depend on the assumption that power consumption in a given clock cycle will have a distribution depending on the initial state; the attacker needs to distinguish between different 'nearby' distributions in the presence of noise. Zero-Knowledge proofs allow verification of secret-based actions without revealing the secrets. Goldreich et al. [2] discussed the class of promise problems in which interaction may give additional information in the context of Statistical Zero-Knowlege. They invoked two types of difference between distributions: the 'statistical difference' and the 'entropy difference' of two random variables. In this context, typically, one of the distributions is the uniform distribution.

Thus, in the contexts of DPA and SZK tests, and particularly in testing encryption devices for security, it is necessary to compare two nearby distributions on bounded domains. Here, we establish the following result, which provides a range of suitable model distributions for performing such tests using maximum-likelihood Riemannian geometric methods, and discuss applications.

Proposition *The family of probability density functions for random variable $N \in [0, 1]$ given by*

$$g(N, \mu, \beta) = \frac{\frac{1}{N}^{1-\frac{\beta}{\mu}} \left(\frac{\beta}{\mu}\right)^{\beta} \left(\log\frac{1}{N}\right)^{\beta-1}}{\Gamma(\beta)} \quad \text{for } \mu > 0 \text{ and } \beta \geq 1 \tag{1}$$

determines a metric space of distributions with the following properties

- *it contains the uniform distribution*
- *it contains approximations to truncated Gaussian distributions*
- *the difference structure is given by the information-theoretic metric*
- *as a Riemannian 2-manifold it is an isometric isomorph of the manifold of gamma distributions.*

Examples are provided of applications in DPA and SZK, with some illustrative calculations and graphs. These new information geometric methods may be useful for comparison with existing methods in testing encryption devices for security. For example, some data on power measurements from a smartcard leaking information during processing of a '0' and a '1', at a specific point in process time, yielded two data sets C, D. These had maximum likelihood parameters ($\mu_C = 0.7246$, $\beta_C = 1.816$) and ($\mu_D = 0.3881$, $\beta_D = 1.757$). We see that here the dominant parameter in the information metric is μ.

References

[1] S. Chari, C.S. Jutla, J.R. Rao and P. Rohatgi. Towards sound approaches to counteract power-analysis attacks. In **Advances in Cryptology-CRYPTO '99**, Ed. M. Wiener, Lecture Notes in Computer Science 1666, Springer, Berlin 1999 pp 398-412.

[2] O. Goldreich, A. Sahai and S. Vadham. Can Statistical Zero-Knowledge be made non-interactive? Or, on the relationship of SZK and NISZK. In **Advances in Cryptology-CRYPTO '99**, Ed. M. Wiener, Lecture Notes in Computer Science 1666, Springer, Berlin 1999 pp 467-484.

[3] P. Kocher, J. Jaffe and B.Jun. Differential Power Analysis. In **Advances in Cryptology-CRYPTO '99**, Ed. M. Wiener, Lecture Notes in Computer Science 1666, Springer, Berlin 1999 pp 388-397.

*Submission for Poster/Rump Session, Eurocrypt 2000, Bruges, 14-19 May 2000