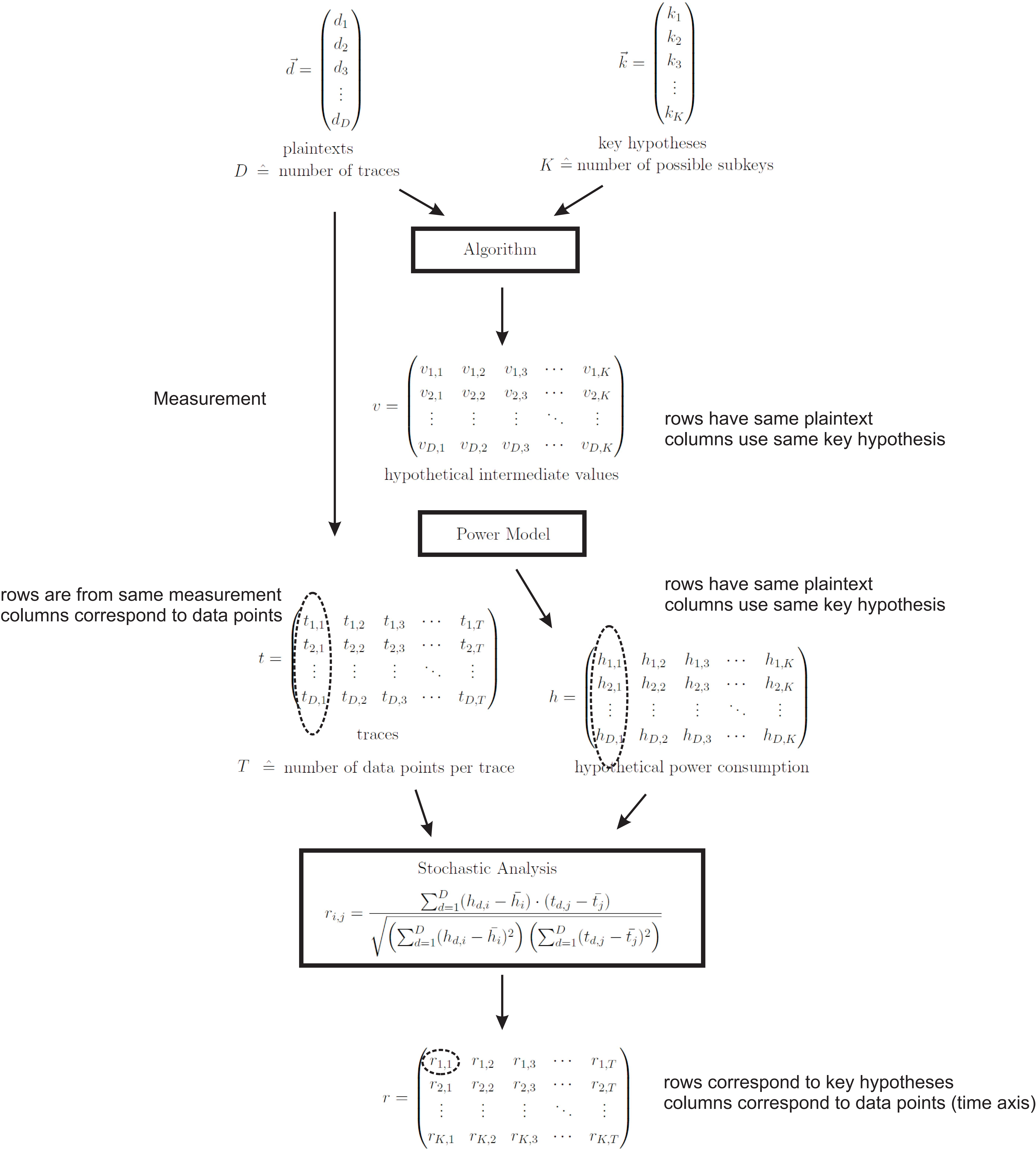

$$\vec{d} = \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ \vdots \\ d_D \end{pmatrix}$$

plaintexts

$D \ \hat{=}$ number of traces

$$\vec{k} = \begin{pmatrix} k_1 \\ k_2 \\ k_3 \\ \vdots \\ k_K \end{pmatrix}$$

key hypotheses

$K \ \hat{=}$ number of possible subkeys

$$v = \begin{pmatrix} v_{1,1} & v_{1,2} & v_{1,3} & \cdots & v_{1,K} \\ v_{2,1} & v_{2,2} & v_{2,3} & \cdots & v_{2,K} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_{D,1} & v_{D,2} & v_{D,3} & \cdots & v_{D,K} \end{pmatrix}$$

hypothetical intermediate values

rows have same plaintext
columns use same key hypothesis

rows are from same measurement
columns correspond to data points

$$t = \begin{pmatrix} t_{1,1} & t_{1,2} & t_{1,3} & \cdots & t_{1,T} \\ t_{2,1} & t_{2,2} & t_{2,3} & \cdots & t_{2,T} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t_{D,1} & t_{D,2} & t_{D,3} & \cdots & t_{D,T} \end{pmatrix}$$

traces

$T \ \hat{=}$ number of data points per trace

rows have same plaintext
columns use same key hypothesis

$$h = \begin{pmatrix} h_{1,1} & h_{1,2} & h_{1,3} & \cdots & h_{1,K} \\ h_{2,1} & h_{2,2} & h_{2,3} & \cdots & h_{2,K} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{D,1} & h_{D,2} & h_{D,3} & \cdots & h_{D,K} \end{pmatrix}$$

hypothetical power consumption

Stochastic Analysis

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i} - \bar{h_i}) \cdot (t_{d,j} - \bar{t_j})}{\sqrt{\left(\sum_{d=1}^{D}(h_{d,i} - \bar{h_i})^2\right)\left(\sum_{d=1}^{D}(t_{d,j} - \bar{t_j})^2\right)}}$$

$$r = \begin{pmatrix} r_{1,1} & r_{1,2} & r_{1,3} & \cdots & r_{1,T} \\ r_{2,1} & r_{2,2} & r_{2,3} & \cdots & r_{2,T} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{K,1} & r_{K,2} & r_{K,3} & \cdots & r_{K,T} \end{pmatrix}$$

rows correspond to key hypotheses
columns correspond to data points (time axis)