A New Signature Scheme Based on $(U|U+V)$ Codes

Thomas Debris Alazard, Nicolas Sendrier, and Jean-Pierre Tillich

https://arxiv.org/abs/1706.08065

Digital Signature from Codes

Public Key: a binary code $\mathcal{C}[n, k]$
Secret Key: the code structure

Complete Decoding: Find the codeword closest to a random word

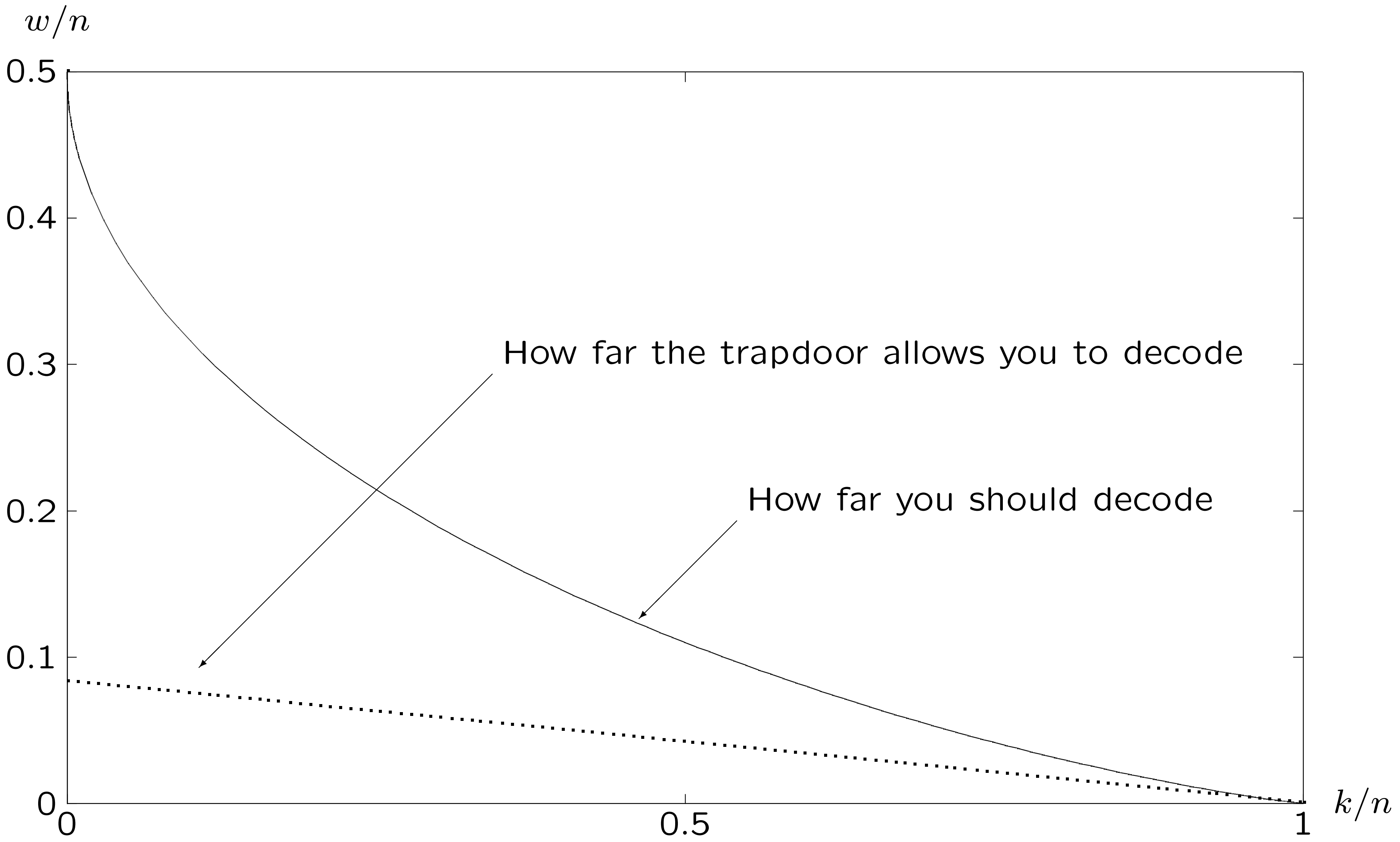
$\rightarrow$ [CFS, 2001], extreme parameters, poor scaling

Source Distortion: Find a codeword close to a random word

$\rightarrow$ find a (secure) family of code for which decoding with an approximation factor is possible

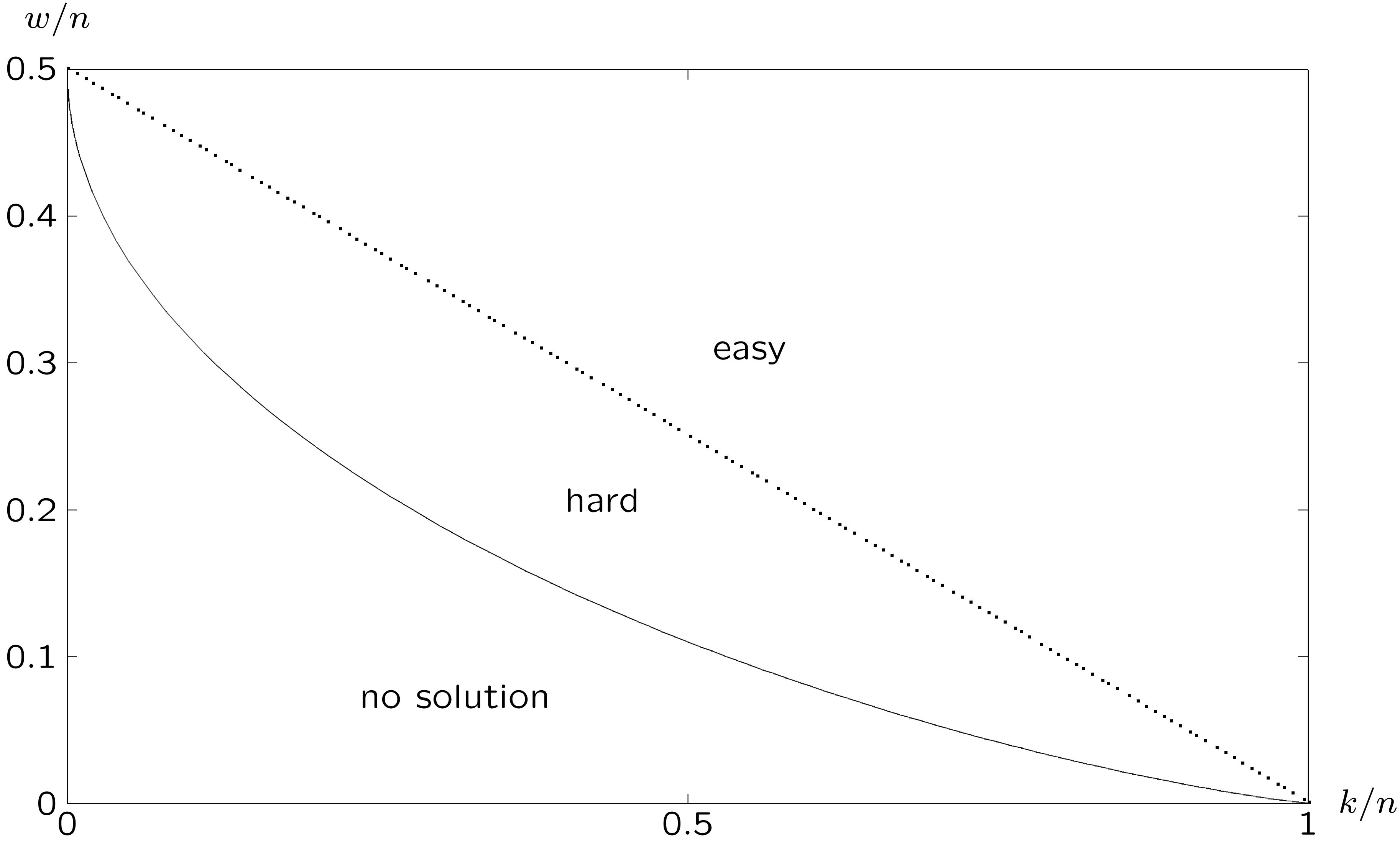
CFS-Like Approach — Complete Decoding

Decoding w errors in an $[n, k]$ code



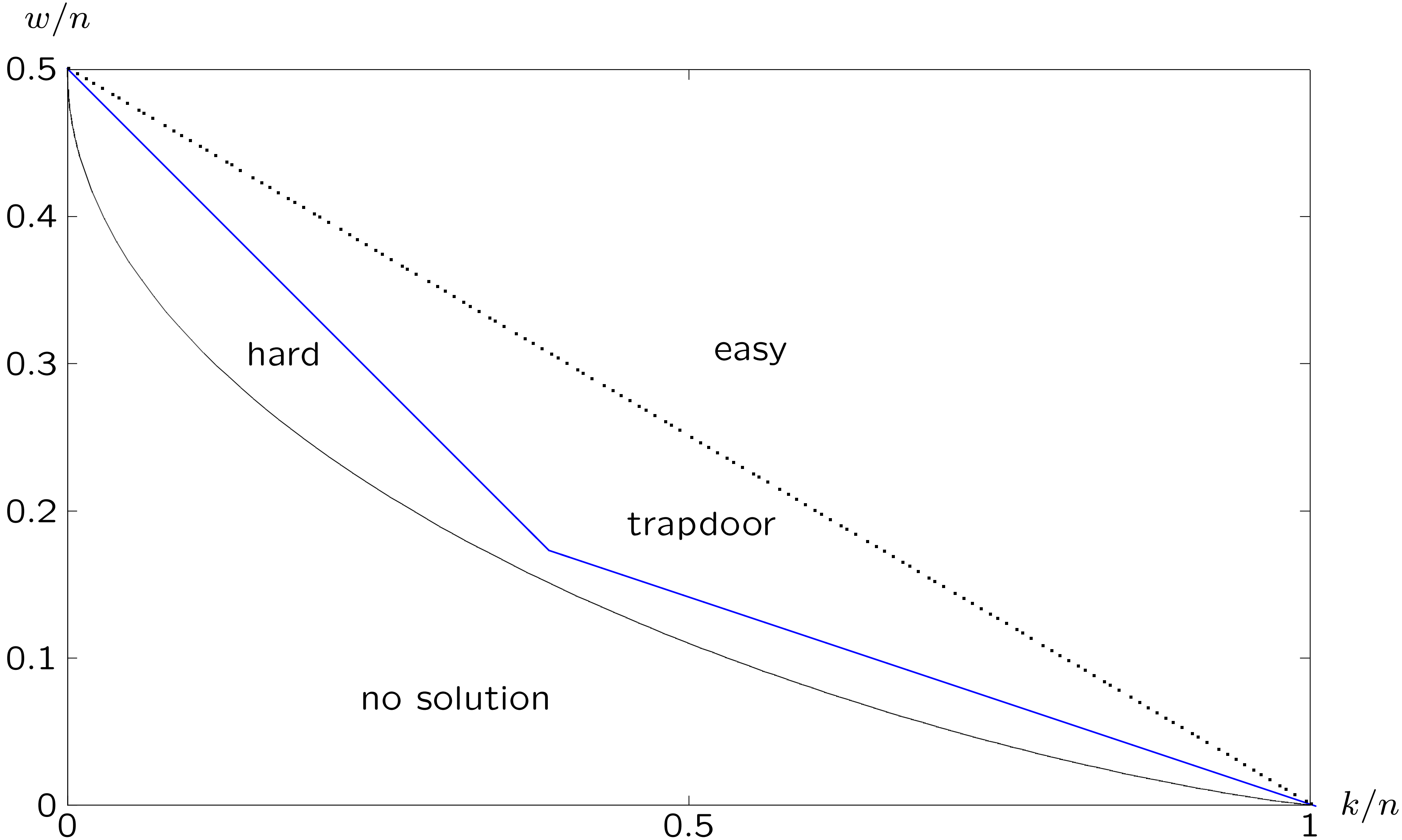
New Approach — Source Distortion

Decoding w errors in an $[n, k]$ code



Source Distortion with $(U|U+V)$ codes

Decoding w errors in an $[n, k]$ code



A New Digital Signature Scheme Based on $(U|U+V)$ Codes

Public Key:

$$G = S \begin{pmatrix} G_U & G_U \\ 0 & G_V \end{pmatrix} P$$

with G_U and G_V random, S non singular, P permutation.

Secret Key: G_U, G_V, and P

Signature: codeword x close to Hash($Message$)

Verification: is x a codeword close to Hash($Message$)?

Security

Existential unforgeability under adaptive chosen message attacks (EUF-CMA) under two assumptions

$$\begin{cases} \text{Indistinguishability of } (U|U+V) \text{ code} \\ \text{Hardness of Decoding One Out of Many (DOOM)} \end{cases}$$

Parameters

Security	80	128	256
Signature length (bits)	4918	7870	15738
Public key size (MBytes)	0.683	1.75	7.00

`https://arxiv.org/abs/1706.08065`

Thank you for your attention