Efficient Fuzzy Extraction of PUF-Induced Secrets: Theory and Applications

Extended version: Cryptology ePrint Archive, Report 2015/854

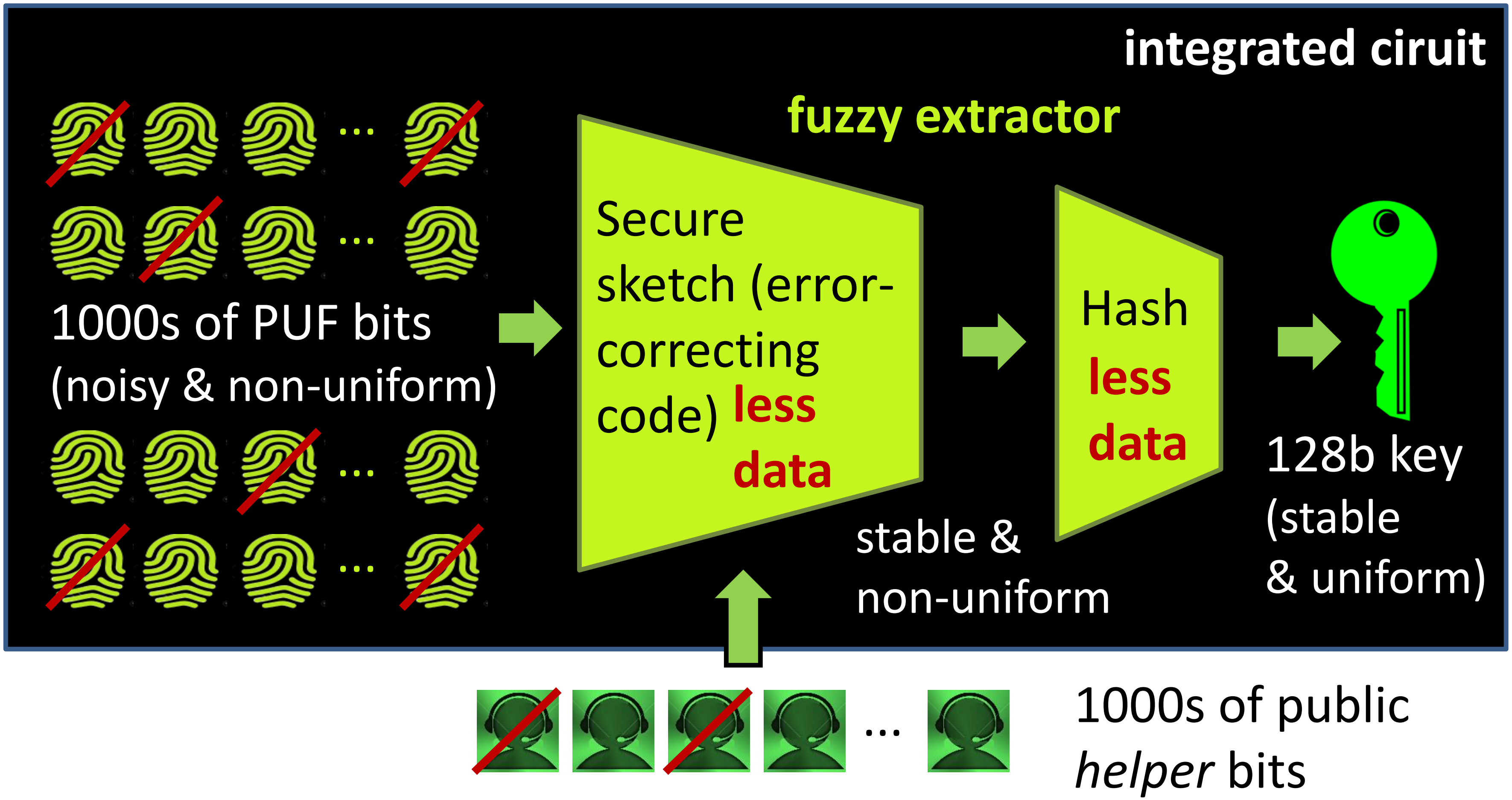
Jeroen Delvaux
Ingrid Verbauwhede
Mandel Yu
Dawu Gu
Matthias Hiller

KU Leuven, COSIC and iMinds
Shanghai Jiao Tong University, LoCCS
Technical University Munich
Verayo and MIT

CHES 2016, Santa Barbara, CA, USA

PUF-Based Key Generation

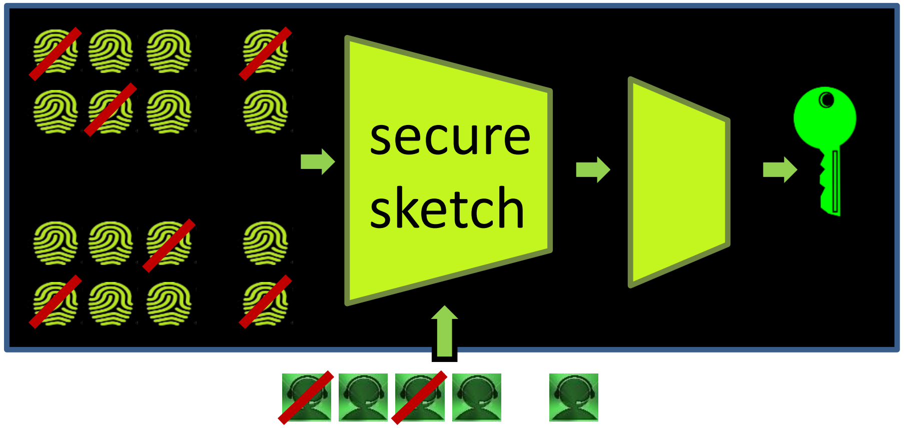
Can we make the default architecture more efficient?



Presentation Outline

(1) Preliminaries: PUF and secure sketch

(2) **THEORY**: tighter bounds on the secure sketch min-entropy loss



sorry, paper only, not here

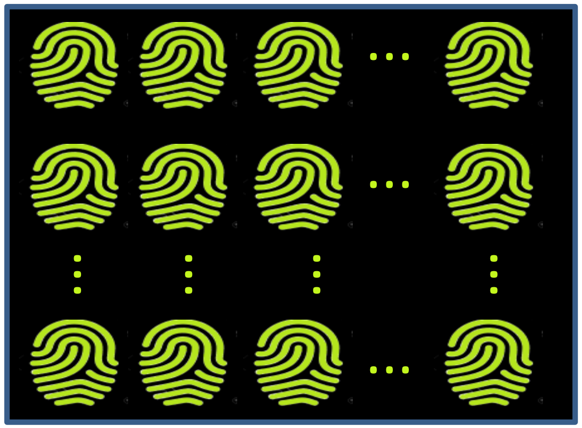
(3) **APPLICATIONS**: *Focus of this talk*

- Reduction in implementation footprint
- Debunk security proof of *reverse fuzzy extractor*
- Proper motivation for debiasing schemes

} 2 CHES 2015 papers

Preliminaries: Array-Based PUFs

Array of identical cells, each producing 1 device-unique bit



* SRAM, DRAM, DFF PUFs (memory-based)
* 1 RO-based PUF
* Coating PUF
* ~~Arbiter PUF and variations~~

issue 1: noisiness

BER 1% - 20% w.r.t. a reference response

issue 2: non-uniformities more 1 than 0, or vice versa

bias

1	0	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	0	1	1	1	1

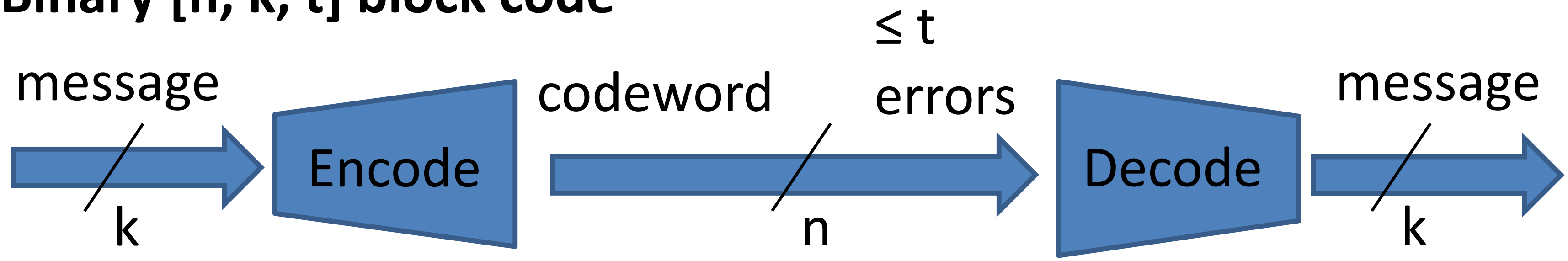
spatial correlations

1	1	1	0	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	1

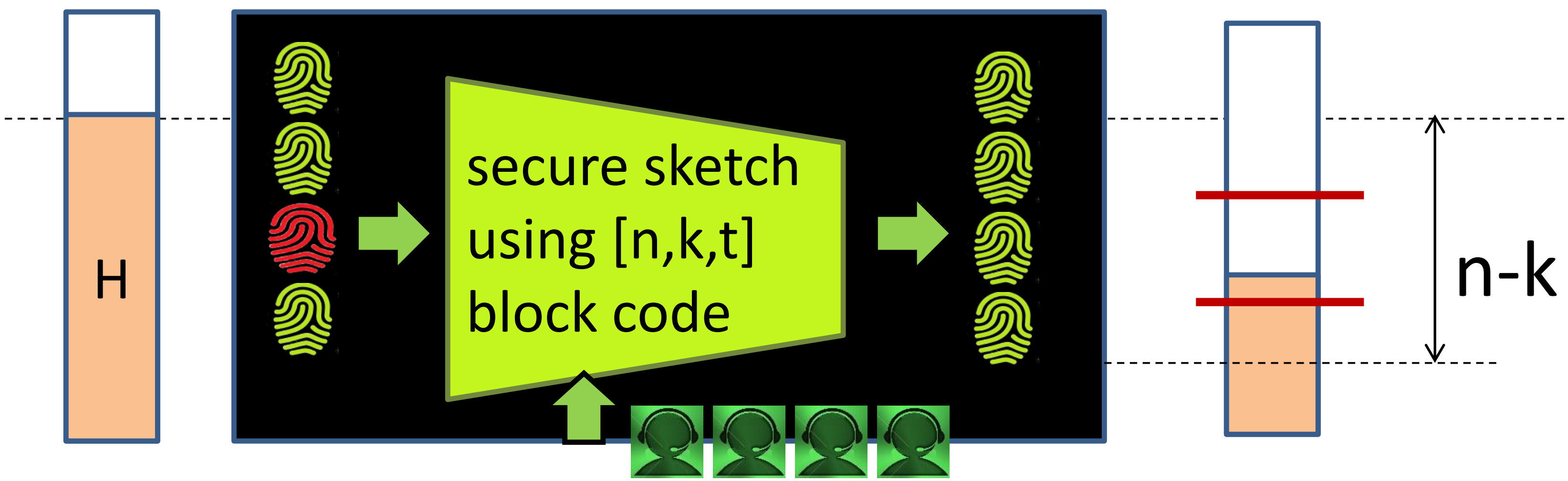
neighboring cells influence each other

Preliminaries: Secure Sketch

Binary [n, k, t] block code



System providers use (**n-k**) **upper bound** on the min-entropy loss



tighter upper/lower bounds (enclosing true value, easy-to-evaluate)

Related work: defeat (*n-k*) bound

- **New research direction**

[Delvaux et al., IEEE TCAD 2014] → [Maes et al., CHES 2015]

so far only repetition codes and i.i.d. PUF bits (bias)

1	0	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	0	1	1

Pr(x(i) = 1) = b with b ∈ [0,1]

- We considerably **extend the scope** on two fronts

<u>1) Large complex codes</u>: BCH, RM, concatenations, ...

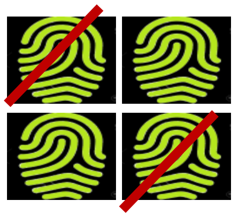
<u>2) Various PUF distributions</u>: bias, spatial correlations, ...

1	1	1	0	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1

Pr(x(i) = x(i+1)) = c with c ∈ [0,1]

Application: reduce implementation footprint

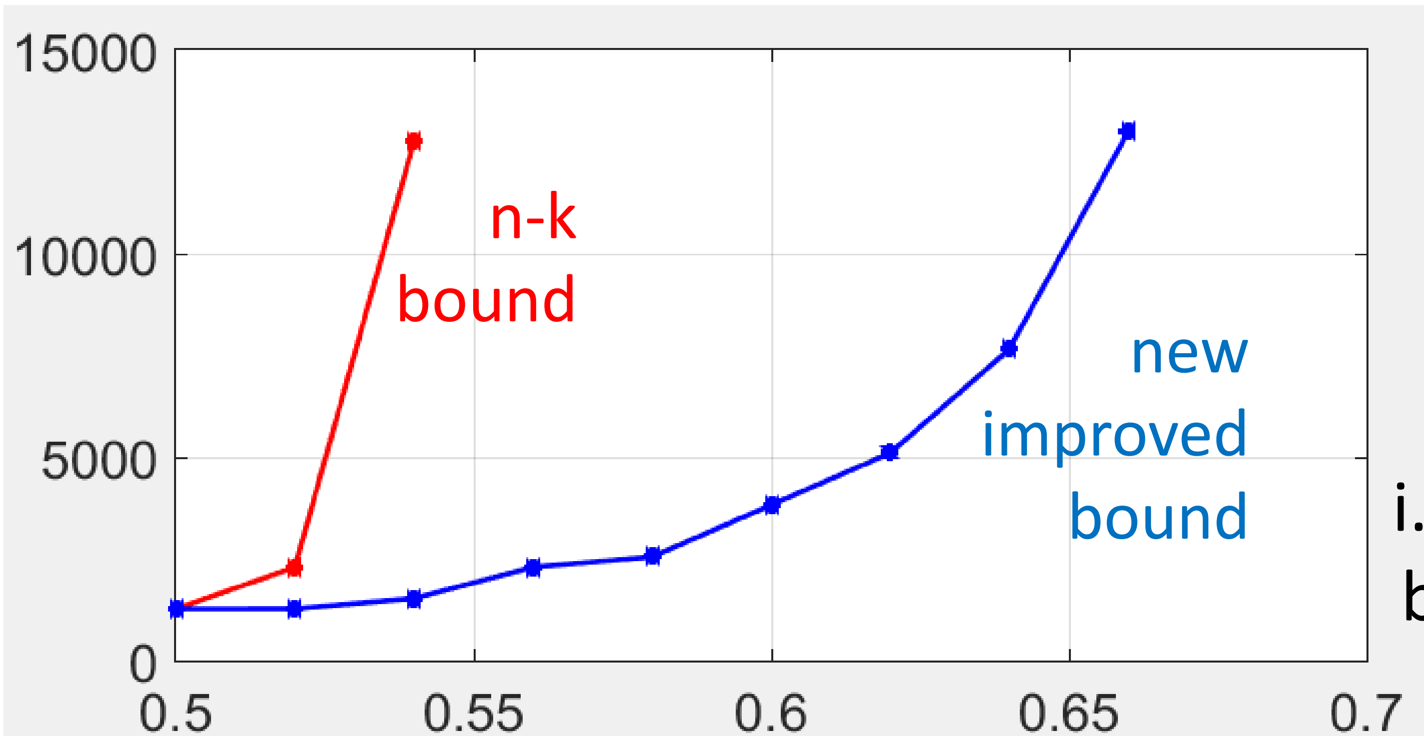
Specs: 128-bit key, BCH+REP code, Pr(error) = 0.1, Pr(fail) ≤ 1E-6



PUF bits

(also less helper bits)

(similar trend for spatially correlated distribution)



i.i.d. bias *b*

1	1	1	1	1
0	0	0	0	0

1	1	1	1	1
1	0	0	0	0

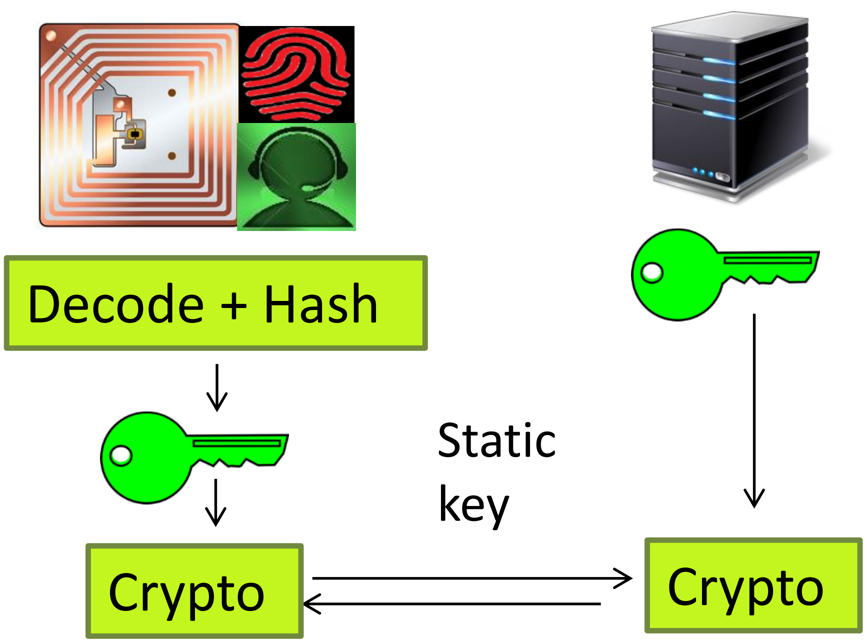
1	1	1	1	1
1	1	0	0	0

Application: Reverse fuzzy extractor (1/2)

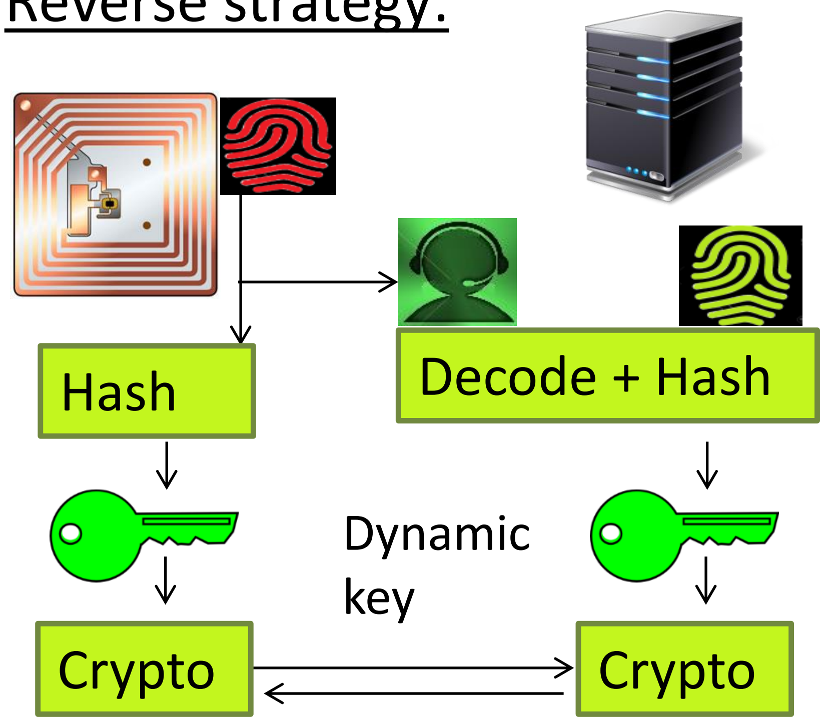
Technique to reduce footprint of PUF-based protocols:

[Van Herrewege et al., FC 2012] → [Maes et al., PhD 2012] → [Aysu et al., CHES 2015, DATE 2016]

Conventional strategy:



Reverse strategy:



Application: Reverse fuzzy extractor (2/2)

Claim: repeated helper data exposure does <u>not</u> result in additional min-entropy loss

~~**Proof:** from [Boyen, ACM CCS 2004]~~ flawed transfer

implicit exposure of individual bit error rates is overlooked

Intuition of unanticipated entropy loss: for biased PUF

PUF error statistics

e.g., [Maes, CHES 2013]

1	0	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	0	1	1	1	1

1	70%	E[BER] ≈ 9%	overall E[BER] ≈ 10%
0	30%	E[BER] ≈ 13%	

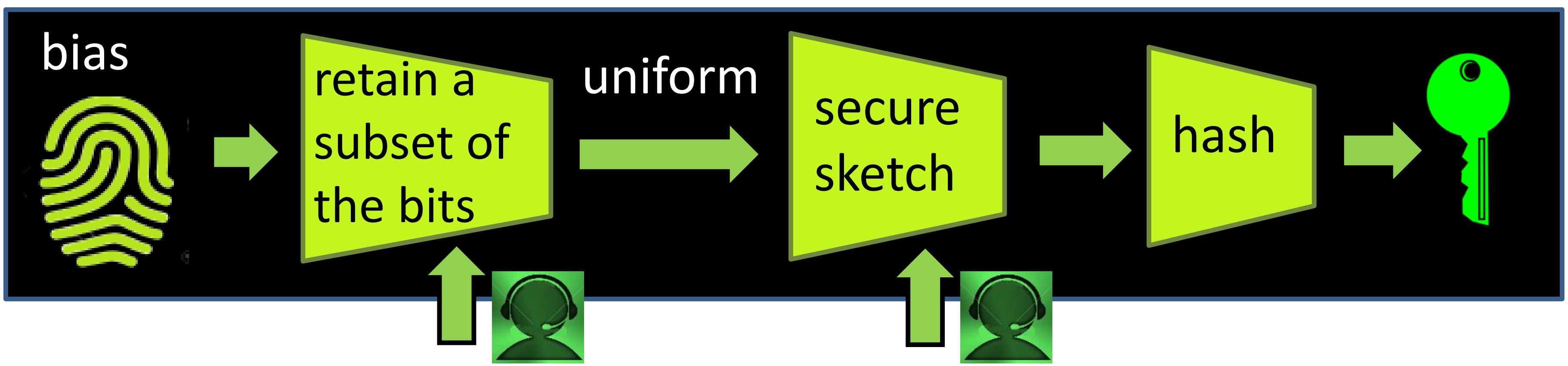
practice: conservative (n-k) bound acts as counterweight

Application: motivation for debiasing schemes

IBS: [Yu et al., IEEE 2010] → [Hiller et al., HOST 2012]

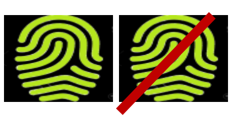
von Neumann: [van der Leest et al., ACM STC 2010] → [Van Herrewege, PhD 2015] → [Maes et al., CHES 2015]

Conjecture that a stand-alone sketch cannot handle bias (which is correct in case the n-k bound is applied)



Application: motivation for debiasing schemes

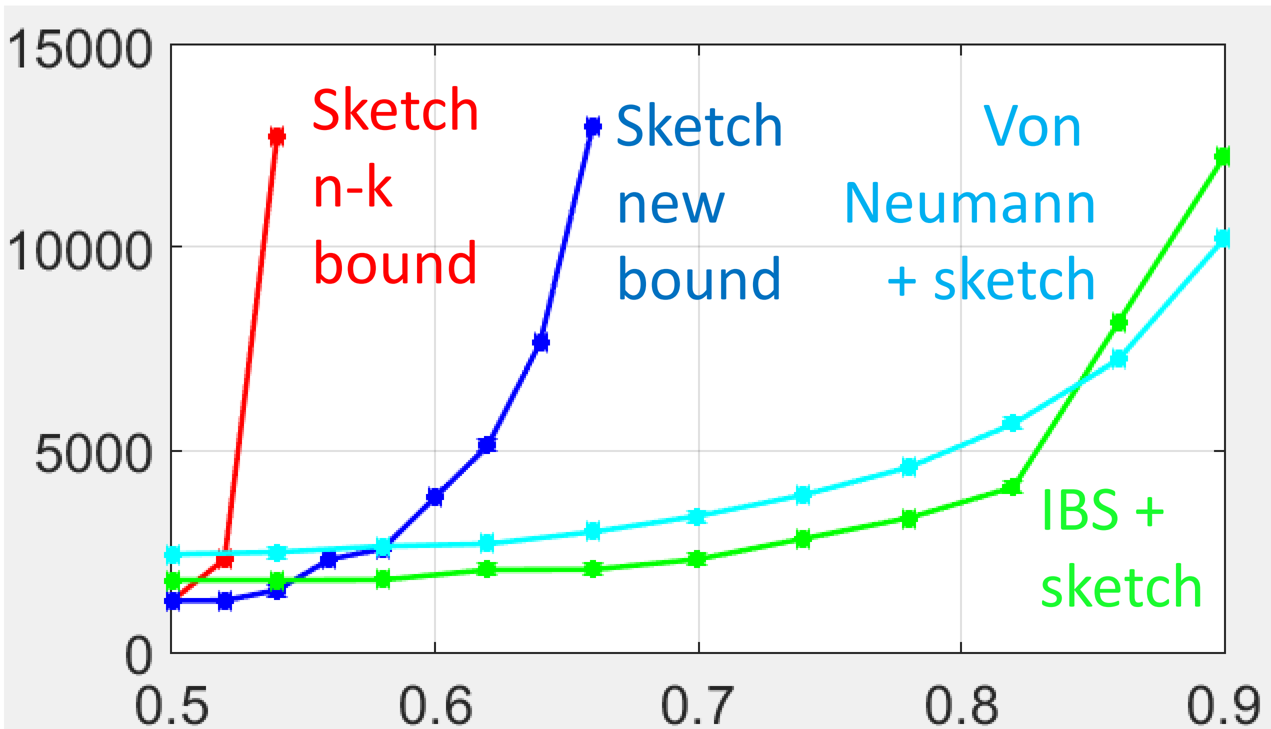
Also in favor of a stand-alone sketch:
1) Debiasing is not for free (circuitry and helper data)
2) Applies to more distributions (other than i.i.d. bias)



PUF bits

new bound is competitive

need for debiasing schemes (or better: PUF redesign)



bias b

Summary

THEORY: **tight bounds** on the secure sketch min-entropy loss for array-based PUFs (new research direction, open for further exploration & improvements)

APPLICATION: reduce fuzzy extrator **implementation footprint**, compared to (n-k) bound

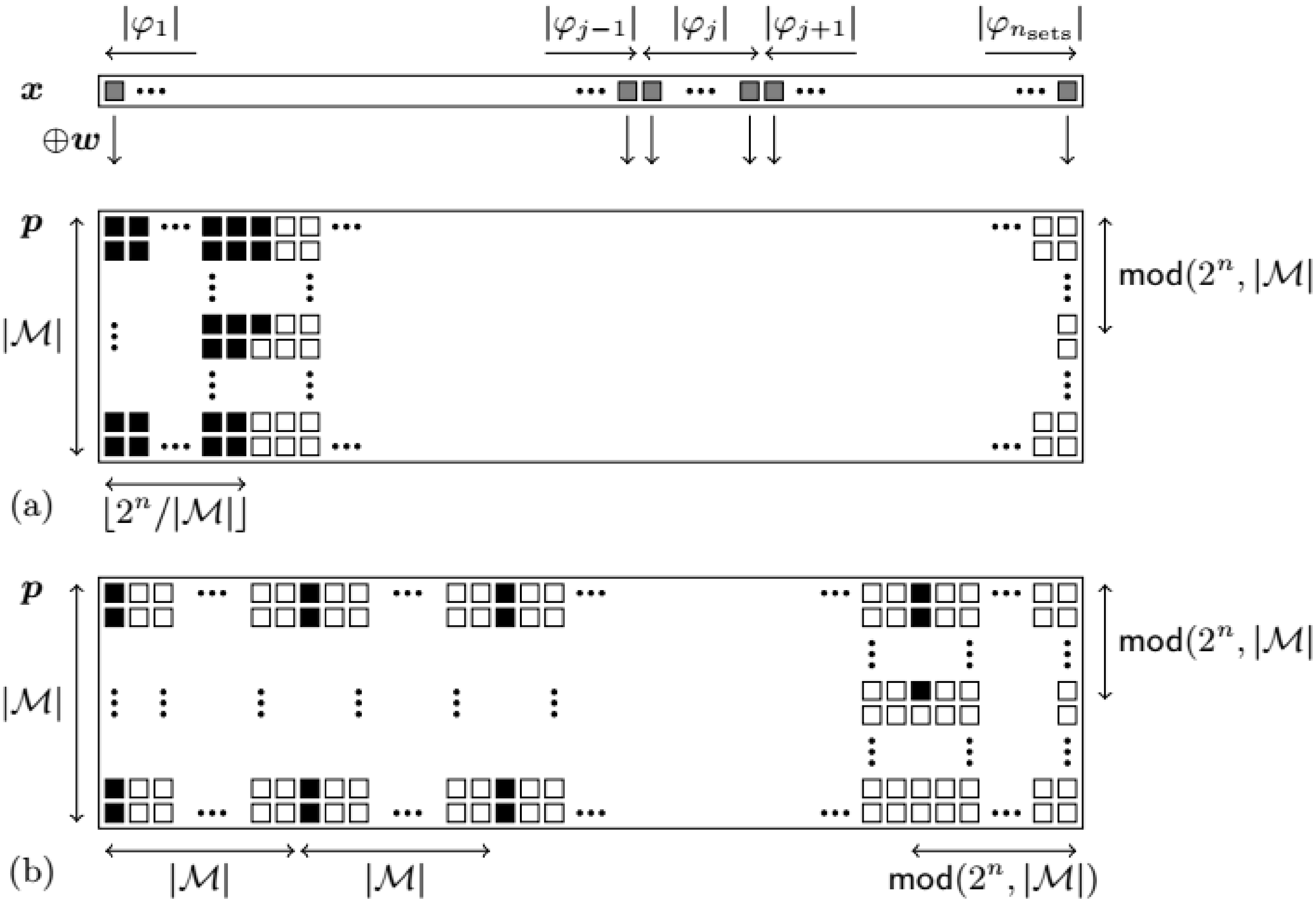
APPLICATION: debunk security proof of **reverse fuzzy extractor** (open for repairs)

APPLICATION: motivate the need for **debiasing schemes** (although low-bias PUFs can do without)

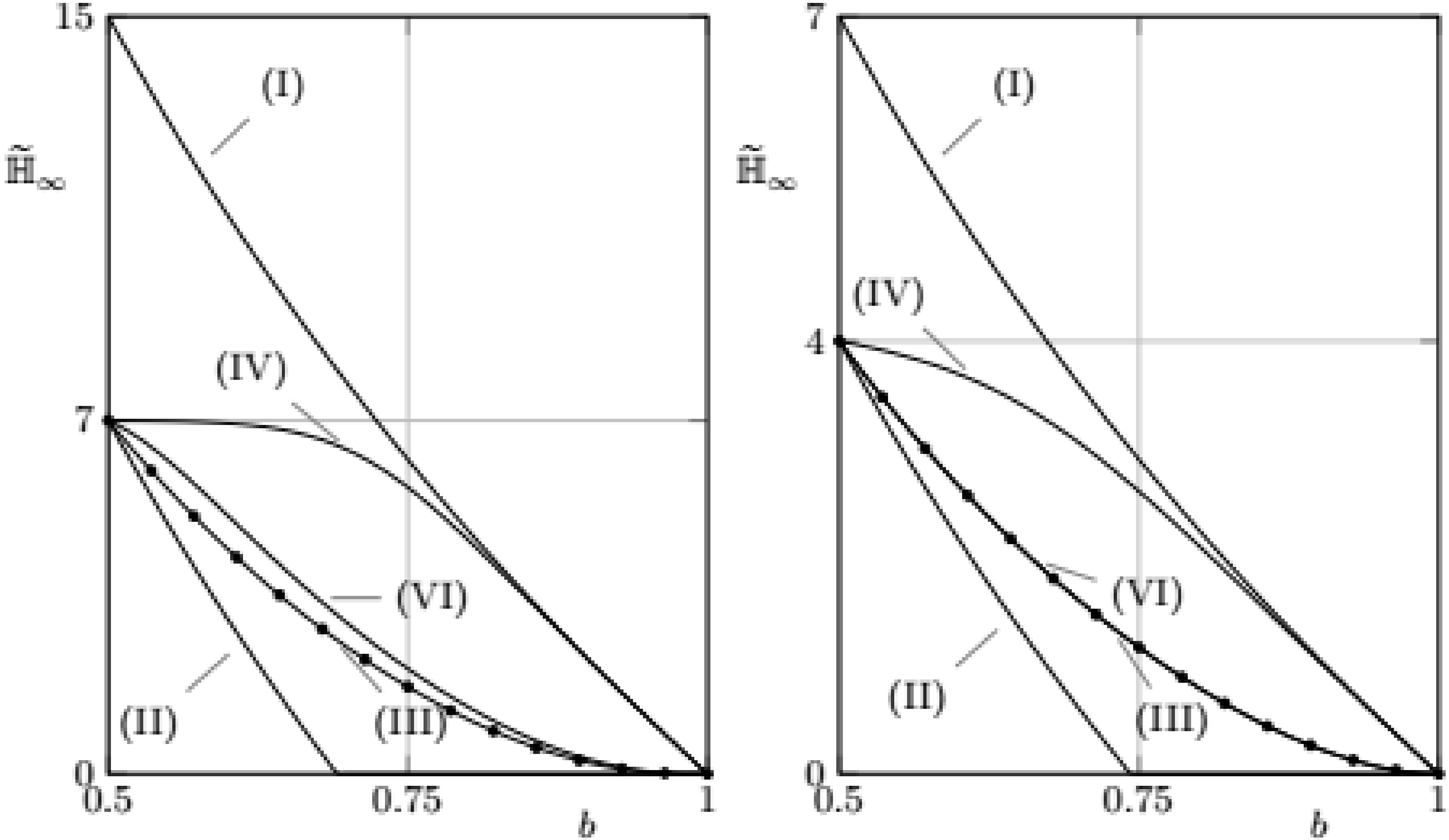
Thank you!

Appendix

All figures and tables

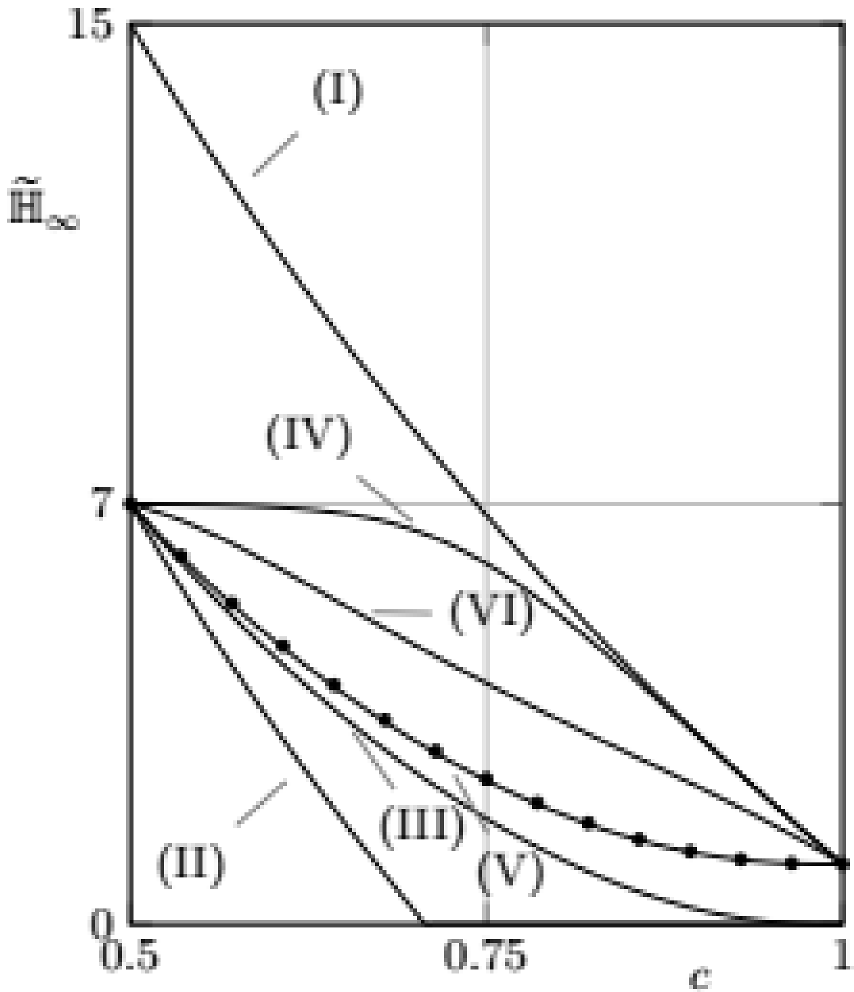


$|\varphi_1|$
$|\varphi_{j-1}|$
$|\varphi_j|$
$|\varphi_{j+1}|$
$|\varphi_{n_{\text{sets}}}|$
$\boldsymbol{x}$
$\oplus \boldsymbol{w}$
$\boldsymbol{p}$
$|\mathcal{M}|$
$\text{mod}(2^n, |\mathcal{M}|)$
(a)
$\lfloor 2^n/|\mathcal{M}| \rfloor$
$\boldsymbol{p}$
$|\mathcal{M}|$
$\text{mod}(2^n, |\mathcal{M}|)$
(b)
$|\mathcal{M}|$
$|\mathcal{M}|$
$\text{mod}(2^n, |\mathcal{M}|)$

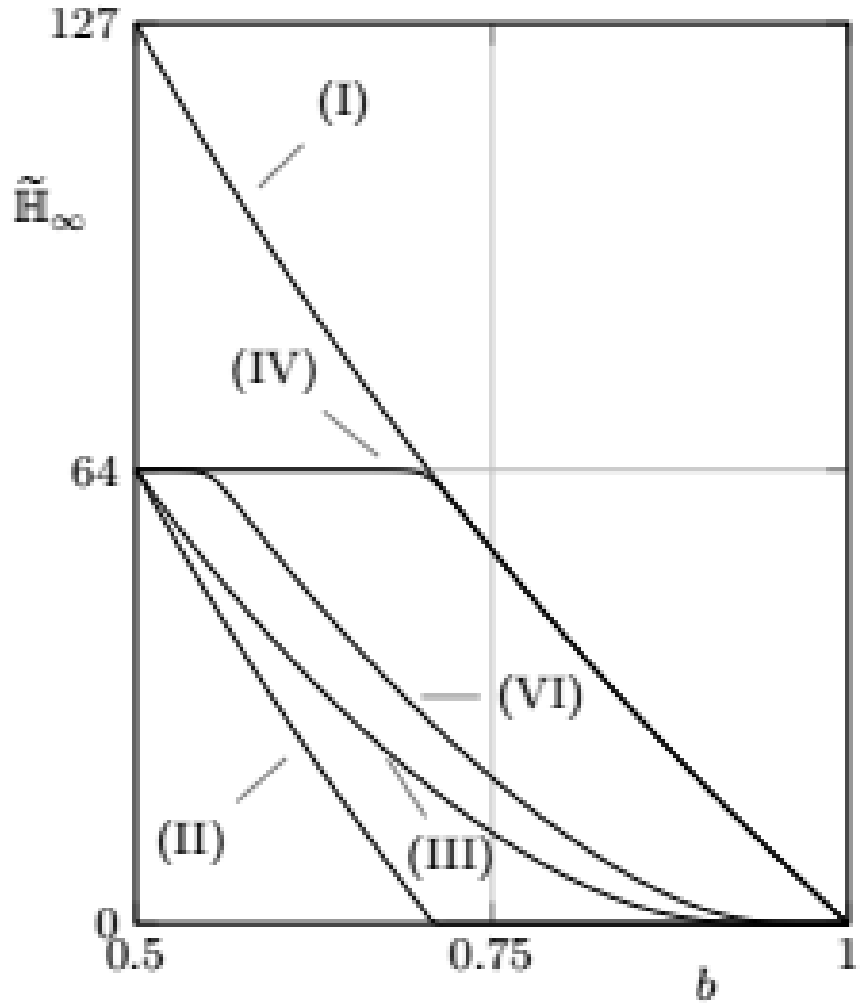


(a) Bias; $[n = 15, k = 7, d = 5]$.

(b) Bias; $[n = 7, k = 4, d = 3]$.

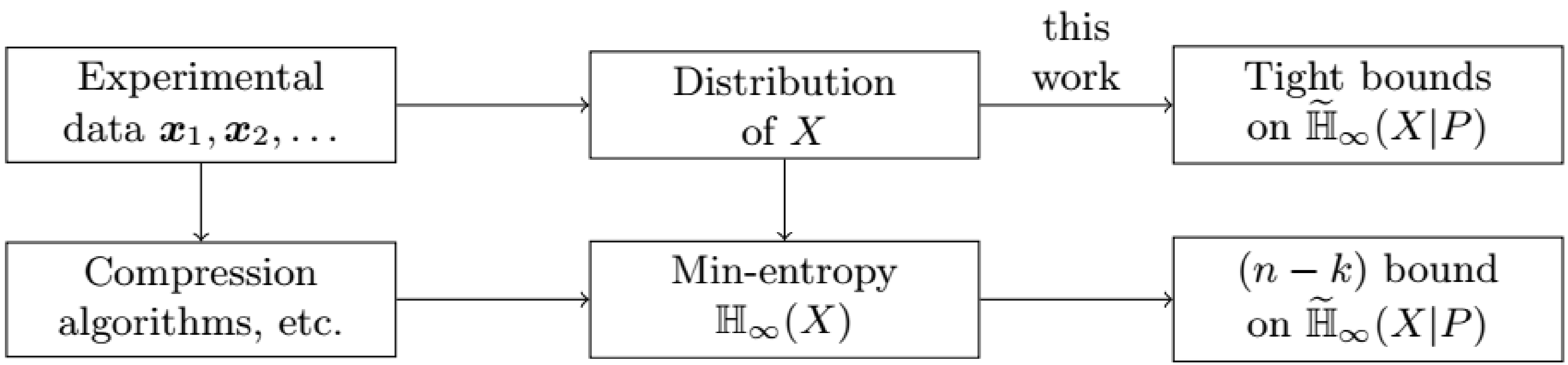


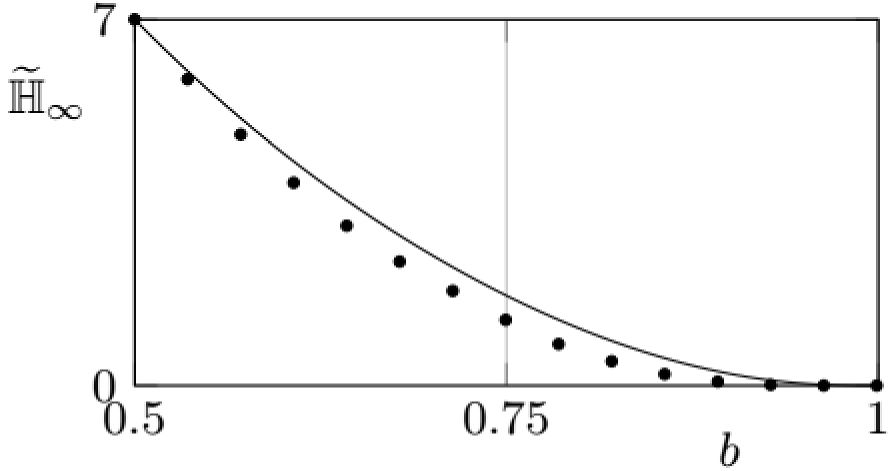
(c) Correlation; $[n = 15, k = 7, d = 5]$.



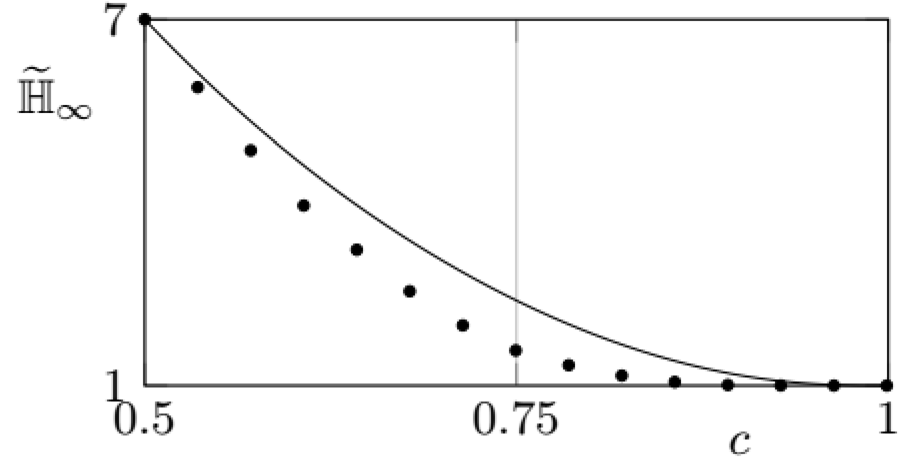
(d) Bias; $[n = 127, k = 64, d = 21]$.

	b	$\mathbb{E}[P_{\text{error}}]$	$z \times [n_2, k_2, d_2] \circ [n_1, k_1, d_1]$	$\widetilde{\mathbb{H}}_\infty(X\|P)$	PUF size n	$\mathbb{E}[P_{\text{fail}}]$
$n-k$ bound	0.50	$\approx 10.0\%$	$2 \times [5,1,5] \circ [127,64,21]$	128	1270	$\approx 3.26\text{E}{-8}$
	0.52	$\approx 10.0\%$	$3 \times [3,1,3] \circ [255,87,53]$	≈ 131.1	2295	$\approx 1.44\text{E}{-8}$
	0.54	$\approx 9.96\%$	$10 \times [5,1,5] \circ [255,155,27]$	≈ 134.4	12750	$\approx 5.56\text{E}{-7}$
	0.56	$\approx 9.90\%$	No code within the search space satisfies the constraints.			
new bound	0.50	$\approx 10.0\%$	$2 \times [5,1,5] \circ [127,64,21]$	128	1270	$\approx 3.26\text{E}{-8}$
	0.52	$\approx 10.0\%$	$1 \times [5,1,5] \circ [255,163,25]$	≈ 134.3	1275	$\approx 4.27\text{E}{-7}$
	0.54	$\approx 9.96\%$	$2 \times [3,1,3] \circ [255,99,47]$	≈ 132.5	1530	$\approx 5.35\text{E}{-7}$
	0.56	$\approx 9.90\%$	$3 \times [3,1,3] \circ [255,87,53]$	≈ 131.3	2295	$\approx 9.90\text{E}{-9}$
	0.58	$\approx 9.81\%$	$2 \times [5,1,5] \circ [255,163,25]$	≈ 130.0	2550	$\approx 4.85\text{E}{-7}$
	0.60	$\approx 9.71\%$	$3 \times [5,1,5] \circ [255,155,27]$	≈ 129.5	3825	$\approx 6.96\text{E}{-8}$
	0.62	$\approx 9.58\%$	$4 \times [5,1,5] \circ [255,163,25]$	≈ 130.4	5100	$\approx 4.42\text{E}{-7}$
	0.64	$\approx 9.42\%$	$10 \times [3,1,3] \circ [255,99,47]$	≈ 132.8	7650	$\approx 3.87\text{E}{-7}$
	0.66	$\approx 9.24\%$	$17 \times [3,1,3] \circ [255,99,47]$	≈ 129.7	13005	$\approx 3.28\text{E}{-7}$

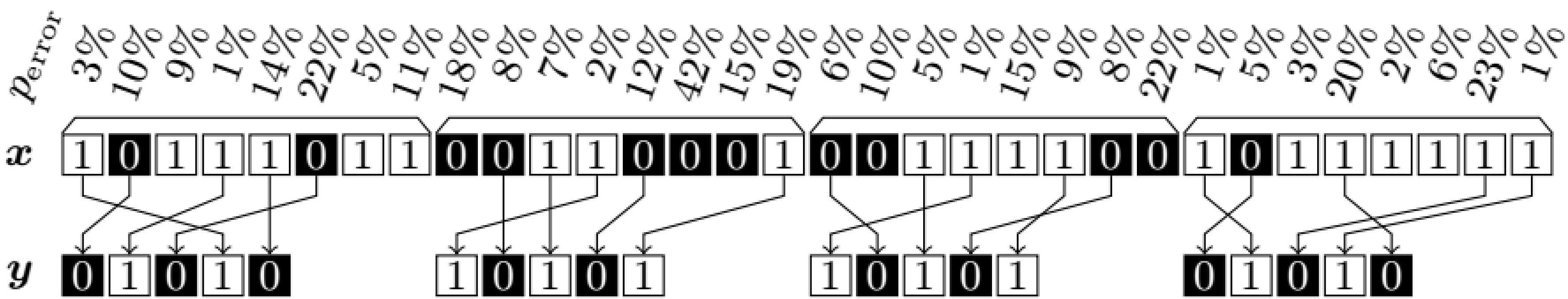

Experimental data $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots$
Distribution of X
this work
Tight bounds on $\widetilde{\mathbb{H}}_\infty(X|P)$
Compression algorithms, etc.
Min-entropy $\mathbb{H}_\infty(X)$
$(n-k)$ bound on $\widetilde{\mathbb{H}}_\infty(X|P)$



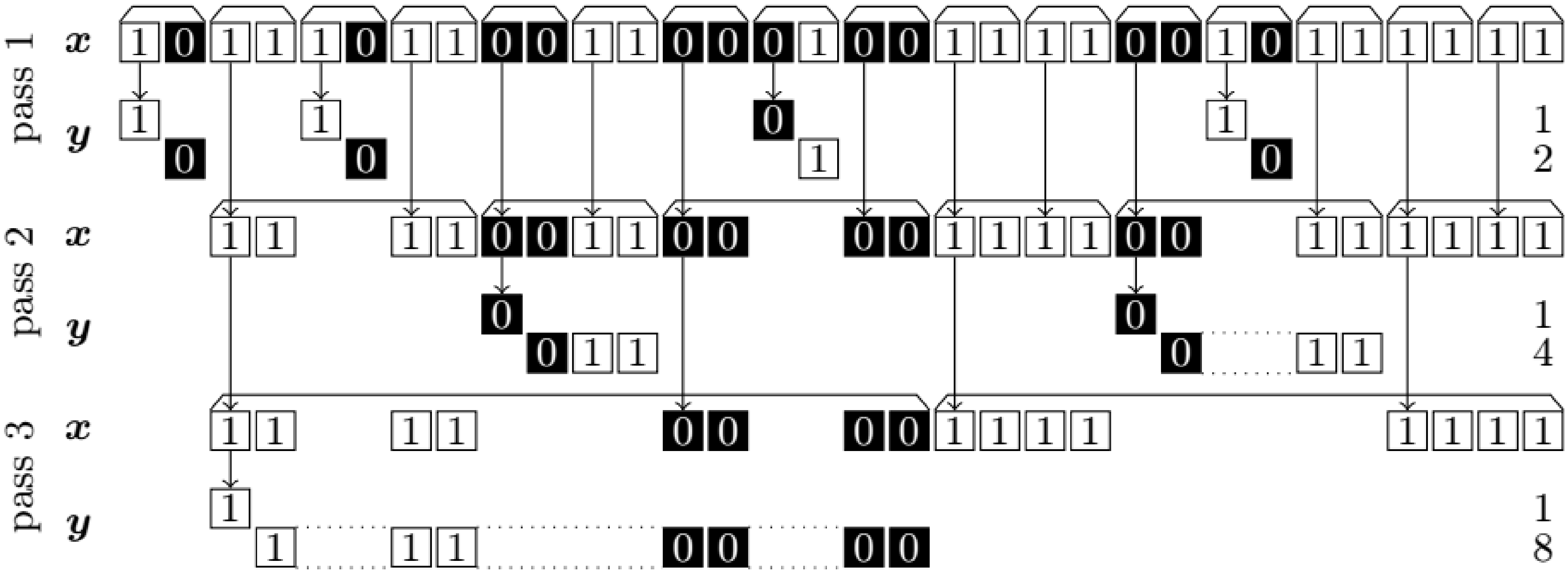
(a) Bias; $[n = 15, k = 7, d = 5]$.

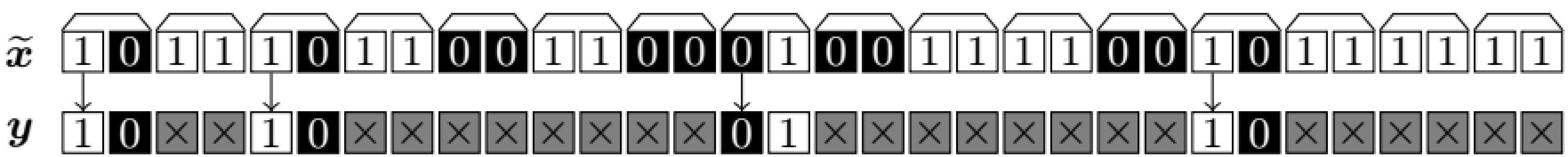


(a) Correlation; $[n = 15, k = 7, d = 5]$.



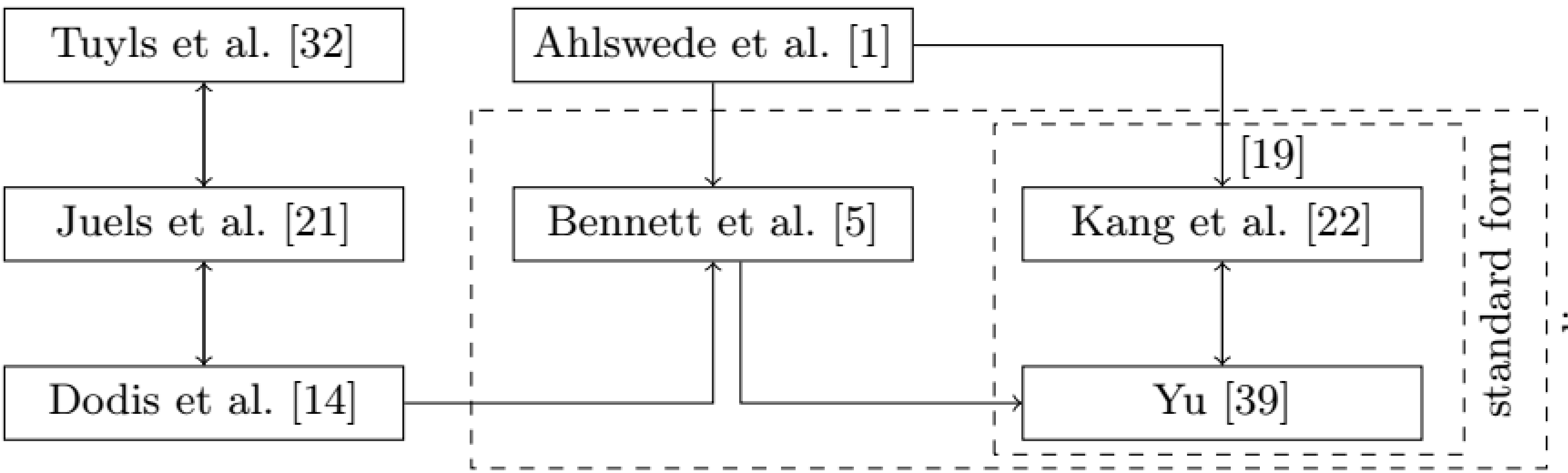
p_{error}
3% 10% 9% 1% 14% 22% 5% 11% 18% 8% 7% 2% 12% 42% 15% 19% 6% 10% 5% 1% 15% 9% 8% 22% 1% 5% 3% 20% 2% 6% 23% 1%
$\boldsymbol{x}$
1 0 1 1 1 0 1 1 0 0 1 1 0 0 0 1 0 0 1 1 1 1 0 0 1 0 1 1 1 1 1 1
$\boldsymbol{y}$
0 1 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 1 0


pass 1
pass 2
pass 3
x
y
1
2
1
4
1
8


x̃
y

	b	$\mathbb{E}[P_{\text{error}}]$	$\mathbb{E}[P_{\text{error}}\|0]$	$\mathbb{E}[P_{\text{error}}\|1]$	Parameters	Retention	$z \times [n_2, k_2, d_2] \circ [n_1, k_1, d_1]$	$\widetilde{\mathbb{H}}_\infty(X\|P)$	PUF size n	$\mathbb{E}[p_{\text{fail},\mathcal{C}_2}]$	$\mathbb{E}[P_{\text{fail}}]$
Generalized IBS	0.50	$\approx 10.0\%$	$\approx 10.0\%$	$\approx 10.0\%$	$n_{\text{index}} = 7$	$\approx 71.4\%$	$2 \times [5,1,5] \circ [127,64,21]$	128	1778	$\approx 1.01\text{E}{-2}$	$\approx 1.70\text{E}{-7}$
	0.54	$\approx 9.96\%$	$\approx 10.6\%$	$\approx 9.40\%$	$n_{\text{index}} = 7$	$\approx 71.4\%$	$2 \times [5,1,5] \circ [127,64,21]$	128	1778	$\approx 1.12\text{E}{-2}$	$\approx 4.57\text{E}{-7}$
	0.58	$\approx 9.81\%$	$\approx 11.2\%$	$\approx 8.79\%$	$n_{\text{index}} = 7$	$\approx 71.4\%$	$1 \times [5,1,5] \circ [255,131,37]$	131	1785	$\approx 1.41\text{E}{-2}$	$\approx 6.46\text{E}{-9}$
	0.62	$\approx 9.58\%$	$\approx 11.8\%$	$\approx 8.18\%$	$n_{\text{index}} = 8$	62.5%	$2 \times [5,1,5] \circ [127,64,21]$	128	2032	$\approx 1.17\text{E}{-2}$	$\approx 7.09\text{E}{-7}$
	0.66	$\approx 9.24\%$	$\approx 12.5\%$	$\approx 7.56\%$	$n_{\text{index}} = 8$	62.5%	$1 \times [5,1,5] \circ [255,131,37]$	131	2040	$\approx 1.83\text{E}{-2}$	$\approx 3.59\text{E}{-7}$
	0.70	$\approx 8.80\%$	$\approx 13.2\%$	$\approx 6.92\%$	$n_{\text{index}} = 9$	$\approx 77.8\%$	$1 \times [7,1,7] \circ [255,131,37]$	131	2295	$\approx 1.90\text{E}{-2}$	$\approx 6.27\text{E}{-7}$
	0.74	$\approx 8.24\%$	$\approx 13.9\%$	$\approx 6.27\%$	$n_{\text{index}} = 11$	$\approx 81.8\%$	$1 \times [9,1,9] \circ [255,131,37]$	131	2805	$\approx 1.62\text{E}{-2}$	$\approx 5.72\text{E}{-8}$
	0.78	$\approx 7.57\%$	$\approx 14.6\%$	$\approx 5.58\%$	$n_{\text{index}} = 13$	$\approx 84.6\%$	$1 \times [11,1,11] \circ [255,131,37]$	131	3315	$\approx 1.65\text{E}{-2}$	$\approx 7.32\text{E}{-8}$
	0.82	$\approx 6.76\%$	$\approx 15.4\%$	$\approx 4.85\%$	$n_{\text{index}} = 16$	$\approx 68.8\%$	$1 \times [11,1,11] \circ [255,131,37]$	131	4080	$\approx 1.66\text{E}{-2}$	$\approx 7.57\text{E}{-8}$
	0.86	$\approx 5.80\%$	$\approx 16.4\%$	$\approx 4.07\%$	$n_{\text{index}} = 16$	$\approx 81.3\%$	$2 \times [13,1,13] \circ [255,71,59]$	142	8160	$\approx 3.57\text{E}{-2}$	$\approx 2.85\text{E}{-8}$
	0.90	$\approx 4.64\%$	$\approx 17.5\%$	$\approx 3.21\%$	$n_{\text{index}} = 16$	$\approx 81.3\%$	$3 \times [13,1,13] \circ [255,45,87]$	135	12240	$\approx 7.51\text{E}{-2}$	$\approx 6.42\text{E}{-7}$
von Neumann	0.50	$\approx 10.0\%$	$\approx 10.0\%$	$\approx 10.0\%$		$\approx 83.4\%$	$4 \times [8,1,8] \circ [63,36,11]$	144	2418	$\approx 2.73\text{E}{-3}$	$\approx 9.85\text{E}{-8}$
	0.54	$\approx 9.96\%$	$\approx 10.6\%$	$\approx 9.40\%$		$\approx 81.6\%$	$4 \times [8,1,8] \circ [63,36,11]$	144	2471	$\approx 2.72\text{E}{-3}$	$\approx 9.73\text{E}{-8}$
	0.58	$\approx 9.81\%$	$\approx 11.2\%$	$\approx 8.79\%$	3 passes	$\approx 77.0\%$	$4 \times [8,1,8] \circ [63,36,11]$	144	2617	$\approx 2.71\text{E}{-3}$	$\approx 9.37\text{E}{-8}$
	0.62	$\approx 9.58\%$	$\approx 11.8\%$	$\approx 8.18\%$		$\approx 70.7\%$	$3 \times [10,1,10] \circ [63,45,7]$	135	2675	$\approx 8.70\text{E}{-4}$	$\approx 9.81\text{E}{-7}$
	0.66	$\approx 9.24\%$	$\approx 12.5\%$	$\approx 7.56\%$	multi-out	$\approx 63.6\%$	$3 \times [10,1,10] \circ [63,45,7]$	135	2971	$\approx 8.52\text{E}{-4}$	$\approx 9.05\text{E}{-7}$
	0.70	$\approx 8.80\%$	$\approx 13.2\%$	$\approx 6.92\%$	$(n_2 \geq 8)$	$\approx 56.2\%$	$3 \times [10,1,10] \circ [63,45,7]$	135	3365	$\approx 8.29\text{E}{-4}$	$\approx 8.12\text{E}{-7}$
	0.74	$\approx 8.24\%$	$\approx 13.9\%$	$\approx 6.27\%$		$\approx 48.6\%$	$3 \times [10,1,10] \circ [63,45,7]$	135	3885	$\approx 8.00\text{E}{-4}$	$\approx 7.06\text{E}{-7}$
	0.78	$\approx 7.57\%$	$\approx 14.6\%$	$\approx 5.58\%$	retention	$\approx 41.4\%$	$3 \times [10,1,10] \circ [63,45,7]$	135	4567	$\approx 7.65\text{E}{-4}$	$\approx 5.91\text{E}{-7}$
	0.82	$\approx 6.76\%$	$\approx 15.4\%$	$\approx 4.85\%$	yield 99%	$\approx 33.5\%$	$3 \times [10,1,10] \circ [63,45,7]$	135	5650	$\approx 7.23\text{E}{-4}$	$\approx 4.72\text{E}{-7}$
	0.86	$\approx 5.80\%$	$\approx 16.4\%$	$\approx 4.07\%$		$\approx 26.1\%$	$3 \times [10,1,10] \circ [63,45,7]$	135	7237	$\approx 6.73\text{E}{-4}$	$\approx 3.55\text{E}{-7}$
	0.90	$\approx 4.64\%$	$\approx 17.5\%$	$\approx 3.21\%$		$\approx 18.5\%$	$3 \times [10,1,10] \circ [63,45,7]$	135	10212	$\approx 6.13\text{E}{-4}$	$\approx 2.45\text{E}{-7}$

$\boldsymbol{p} \leftarrow \mathsf{SSGen}(\boldsymbol{x})$	$\widehat{\boldsymbol{y}} \leftarrow \mathsf{SSRep}(\widetilde{\boldsymbol{x}}, \boldsymbol{p})$	
Random $\boldsymbol{w} \in \mathcal{C}$ $\boldsymbol{p} \leftarrow \boldsymbol{x} \oplus \boldsymbol{w}$	$\widetilde{\boldsymbol{w}} \leftarrow \widetilde{\boldsymbol{x}} \oplus \boldsymbol{p} = \boldsymbol{w} \oplus \boldsymbol{e}$ $\widehat{\boldsymbol{y}} = \widehat{\boldsymbol{w}} \leftarrow \mathsf{Correct}(\widetilde{\boldsymbol{w}})$	(a) Code-offset method of Juels et al. [21].
	$\widetilde{\boldsymbol{w}} \leftarrow \widetilde{\boldsymbol{x}} \oplus \boldsymbol{p} = \boldsymbol{w} \oplus \boldsymbol{e}$ $\widehat{\boldsymbol{y}} = \widehat{\boldsymbol{x}} \leftarrow \boldsymbol{p} \oplus \mathsf{Correct}(\widetilde{\boldsymbol{w}})$	(b) Code-offset method of Dodis et al. [14].
	$\widetilde{\boldsymbol{w}} \leftarrow \widetilde{\boldsymbol{x}} \oplus \boldsymbol{p} = \boldsymbol{w} \oplus \boldsymbol{e}$ $\widehat{\boldsymbol{y}} = \widehat{\boldsymbol{m}} \leftarrow \mathsf{Decode}(\widetilde{\boldsymbol{w}})$	(c) Code-offset method of Tuyls et al. [32].
$\boldsymbol{p} \leftarrow \boldsymbol{x} \cdot \boldsymbol{H}^T$	$\boldsymbol{s} \leftarrow \widetilde{\boldsymbol{x}} \cdot \boldsymbol{H}^T \oplus \boldsymbol{p} = \boldsymbol{e} \cdot \boldsymbol{H}^T$ Determine $\widehat{\boldsymbol{e}}$ $\widehat{\boldsymbol{y}} = \widehat{\boldsymbol{x}} \leftarrow \widetilde{\boldsymbol{x}} \oplus \widehat{\boldsymbol{e}}$	(d) Syndrome method of Bennett et al. [5].
$\boldsymbol{p} \leftarrow \boldsymbol{x}(1:k) \cdot \boldsymbol{A}$ $\oplus\, \boldsymbol{x}(k+1:n)$	$\widehat{\boldsymbol{w}} \leftarrow \mathsf{Correct}(\widetilde{\boldsymbol{x}} \oplus (\boldsymbol{0} \Vert \boldsymbol{p}))$ $\widehat{\boldsymbol{y}} = \widehat{\boldsymbol{x}} \leftarrow \widehat{\boldsymbol{w}} \oplus (\boldsymbol{0} \Vert \boldsymbol{p})$	(e) Systematic method of Yu [39].
	$\widehat{\boldsymbol{y}} = \widehat{\boldsymbol{x}}(1:k) \leftarrow \mathsf{Decode}(\widetilde{\boldsymbol{x}}$ $\oplus (\boldsymbol{0} \Vert \boldsymbol{p}))$	(f) Systematic method of Kang et al. [22].
$\boldsymbol{p} \leftarrow j$ so that $\boldsymbol{x} \in \mathcal{C}_j$	$\widehat{\boldsymbol{y}} = \widehat{\boldsymbol{m}} \leftarrow \mathsf{Decode}_{\mathcal{C}_j}(\widetilde{\boldsymbol{x}})$	(g) Multi-code method of Ahlswede et al. [1].



Tuyls et al. [32]
Ahlswede et al. [1]
[19]
Juels et al. [21]
Bennett et al. [5]
Kang et al. [22]
standard form
linear
Dodis et al. [14]
Yu [39]