da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

ATHENE
National Research Center
for Applied Cybersecurity

Indexing Protected Deep Face Templates by Frequent Binary Patterns

D. Osorio-Roig et al

Biometrics Security and Privacy Group, IdiapResearch Institute
da/sec–Biometrics and Security Research Group, Hochschule Darmstadt

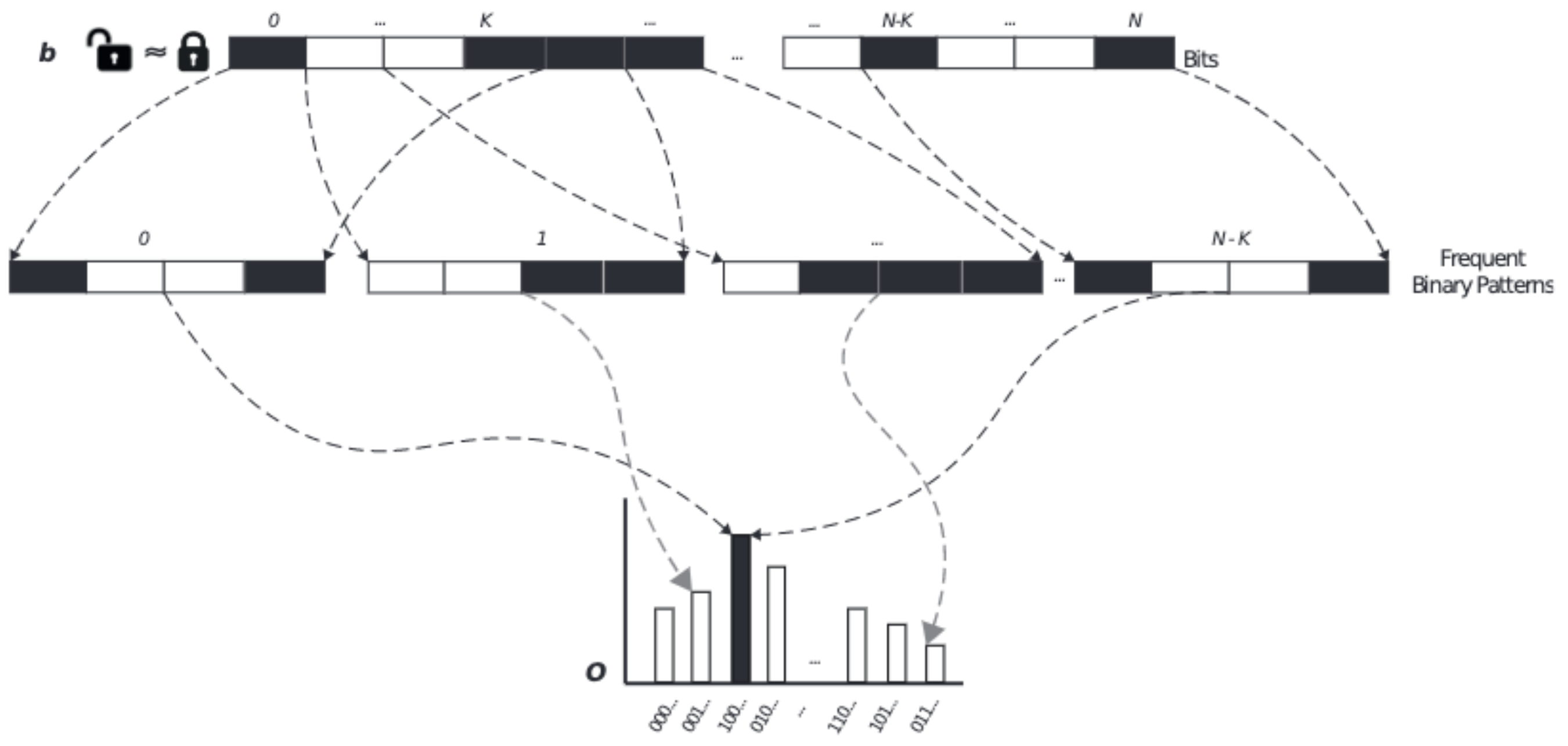
Introduction

In the context of face biometrics, researches have mainly focused on cancelable biometrics for identification systems. Some observations can be analysed:

- computational costs in these schemes, which apply a typical exhaustive search-based identification, tend to grow linearly with the number of enrolled subjects.
- most of the cancelable schemes introduce the randomness to fulfill BTP requirements defined by the ISO/IEC 24745 standard (i.e. renewability, unlinkability, irreversibility) yielding binary representations-based features.

i. Explore whether the most frequent binary patterns over cancelable templates could be most stable and sufficient for indexing.
ii. First proposal of search space-reducing ***Workload Reduction*** scheme for deep face templates protected by well-known cancelable biometric schemes.
iii. Experimental results showcase that the proposed scheme is agnostic w.r.t the applied cancelable schemes.

Proposed Scheme



- Frequent binary pattern extraction: a set **P** of binary patterns are extracted from N bits; subsequently, frequent patterns are defined to their corresponding number of occurrences in N.

Computational Workload Reduction

$$\mathcal{W} = \sum_{i=1}^{z} |l_i|$$

Experimental Setup

Cancelable schemes

- BioHashing
- IoM with Uniformly Random Permutation (IoM-URP)
- IoM with Gaussian Random Projection (IoM-GRP)
- Original face embeddings are used as baseline (unprotected system)

Identification experiments

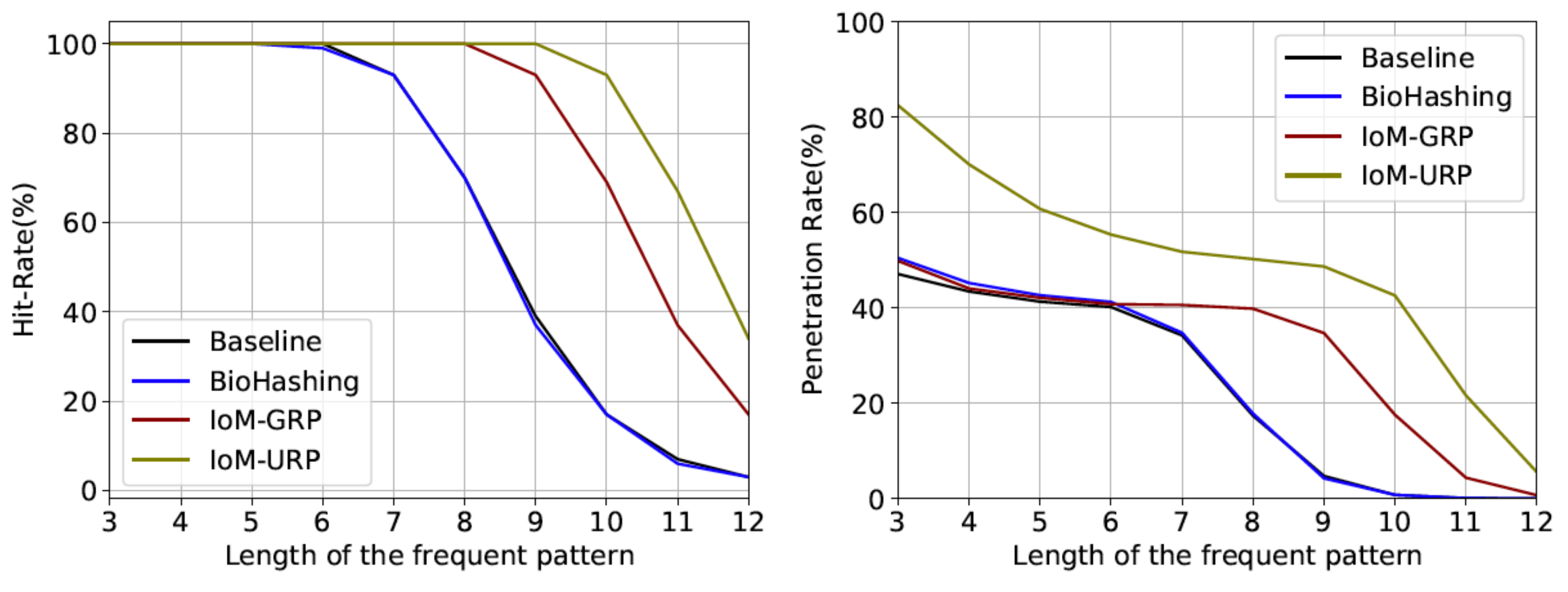
- Closed-set scenario (sub-sampling of 10 rounds)
- Open-set scenario (10-folds cross-validation)
- Normal and stolen-token scenarios
- Baseline workload of an identification system is considered to be an exhaustive search, i.e. a biometric probe is compared against all references enrolled in the database.
- Experiments are conducted on LFW database containing 1,680 in enrolment

Metrics

- **Biometric performance**: for closed-set scenario, the hit-rate(H-R); for open-set scenario, the detection error trade-off (DET) curves.
- **Computational workload**: penetration rate (P-R) and the necessary number of comparisons per identification transaction.

Experimental Results

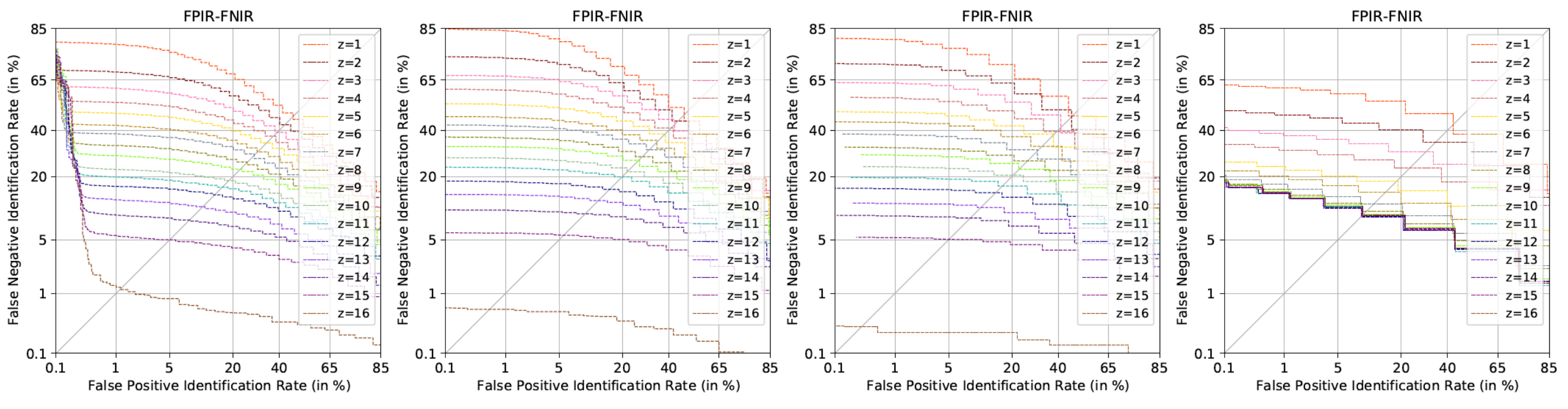
Closed-set scenario evaluation



(a) H-R – Normal scenario (b) P-R – Normal scenario

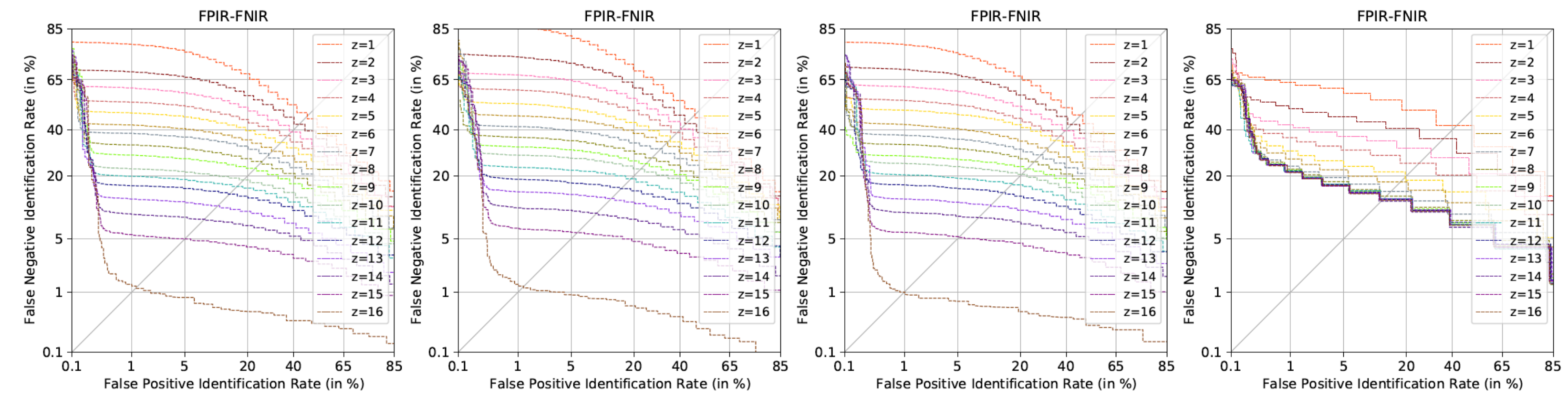
- It can be perceived that the curves can be maintained at almost 100% H-R up to a certain length of the frequent pattern depending on the cancellable scheme.
- P-R can be reduced to approximately half (i.e. P-R < 52%) of the baseline workload, while maintaining a high H-R.

Open-set scenario evaluation



(a) Unprotected baseline (b) BioHashing (c) IoM-GRP (d) IoM-URP

Normal Scenario



(a) Unprotected baseline (b) BioHashing (c) IoM-GRP (d) IoM-URP

Stolen-token Scenario

- Evaluating the effect of the parameter z over challenging scenarios.
- A fixed length of frequent pattern, i.e. $K = 4$, and z ranging in [1,16].
- Biometric performance improves as the maximum number of visited bins corresponding to the most frequent binary patterns from the probe (z) increase.

BTP approach	Normal-scenario			Stolen-token-scenario		
	FNIR@FPIR=1.0%	z	P-R(%)	FNIR@FPIR=1.0%	z	P-R(%)
Unprotected baseline	19.76	11	66.08	19.76	11	66.08
BioHashing	23.30	11	66.27	23.14	11	66.44
IoM-GRP	19.57	11	66.28	20.37	11	66.61
IoM-URP	22.33	5	87.90	29.99	5	88.59

- Summary of the best results over open-set evaluation for normal and stolen-token scenarios, respectively.
- For a FNIR@FPIR = 1.0%, the system achieves a rejection rate for genuine identification transactions of less than 24%, while reducing to approximately 66% of the workload over open-set scenarios.

Future work

- Extend the proposed system to multi-biometrics where frequent binary patterns will be extracted from multiple biometric characteristics.

Participate in the survey "*Protecting your data in biometric systems*"

EAB - Protecting Your Data in Biometric Systems

Acknowledgment: This work has in part received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 860813 - TReSPAsS-ETN and the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE..