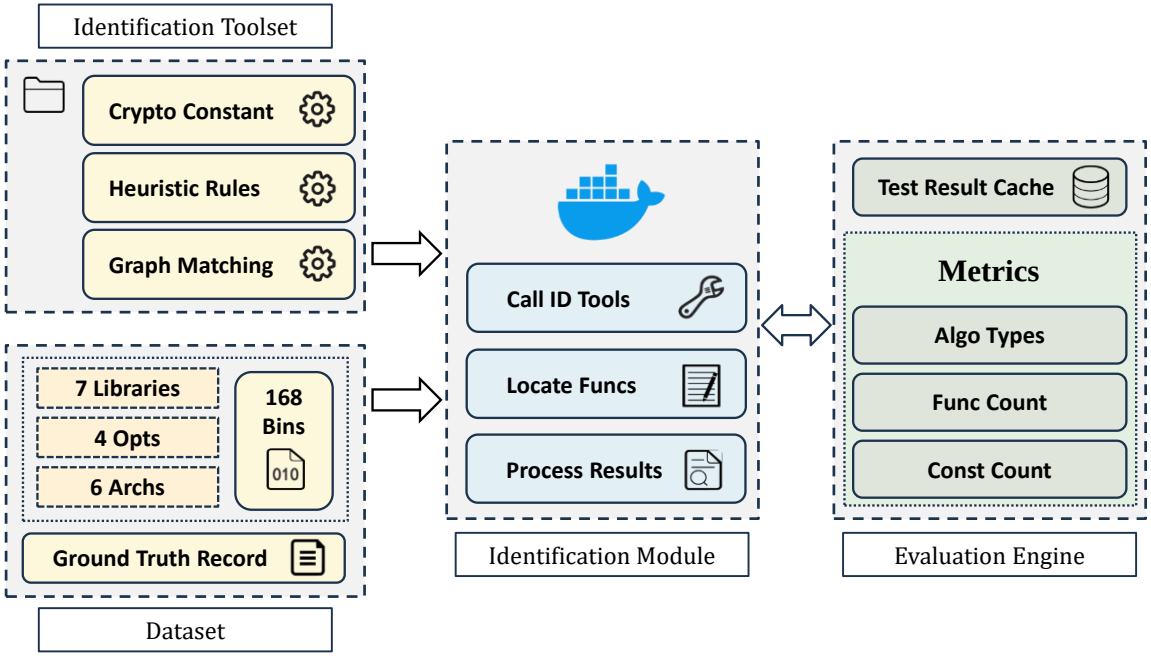
A Unified Evaluation Framework for Cryptographic Algorithm Identification Tools in IoT Firmware

Yifei LI , Xiaoyang ZHUO, Jiewei DU, Chengyu HU, Jin SHI, Shanqing GUO

Frontiers of Computer Science, DOI: 10.1007/s11704-025-50357-5

Problems & Ideas

- Problems of lack of a common assessment framework:
  - A systematic recognition performance evaluation system has not yet been established in the field of IoT firmware cryptographic algorithm recognition.
  - Several basic issues in the field cannot be effectively answered.
- Ideas: A modular recognition performance evaluation framework with multi-dimensional evaluation indicators and diverse test benchmarks.



Main Contributions

- Contributions:
  - Features a modular, extensible architecture with plug-and-play tool integration and standardized 3D quantitative metrics for comparable assessments.;
  - Constructs a multi-layered test suite (7 sources × 6 ISAs × 4 optimizations = 168 binaries) for thorough tool validation.;
  - Evaluated 37 tools across 6 ISAs and 4 optimization levels, then analyzed 20 real firmware samples for practical algorithm usage patterns.

Table 2 The effectiveness of existing tools in identifying cryptographic algorithm types (precision/recall/F1-Score)

Name	cryptlib[27]	libcrypto[28]	libcrypt[29]	libnettle[30]	libtomcrypt[31]	Libgcrypt[32]	wolfssl[33]
Cryfind[13]	0.50/0.31/0.39	0.82/0.48/0.60	0.86/0.38/0.52	0.75/0.39/0.51	0.86/0.46/0.6	0.83/0.44/0.58	0.86/0.31/0.44
Draca[18]	1.00/0.06/0.11	1.00/0.07/0.13	1.00/0.12/0.22	1.00/0.06/0.12	1.00/0.05/0.10	1.00/0.06/0.11	1.00/0.05/0.10
Bfcrypt[17]	1.00/0.18/0.31	0.85/0.20/0.33	1.00/0.25/0.41	1.00/0.19/0.32	1.00/0.31/0.47	0.86/0.17/0.29	1.00/0.15/0.26
Findcrypt3[19]	0.40/0.25/0.32	0.82/0.31/0.45	0.83/0.31/0.45	0.89/0.26/0.40	0.85/0.40/0.57	0.78/0.37/0.54	0.75/0.30/0.43
IDAscope_const[8]	0.60/0.25/0.36	0.80/0.28/0.41	1.00/0.25/0.40	0.81/0.29/0.43	0.94/0.38/0.55	0.78/0.32/0.46	0.80/0.20/0.32
Signsrch[15]	0.70/0.44/0.54	0.79/0.52/0.63	0.63/0.31/0.42	0.76/0.41/0.54	0.83/0.51/0.63	0.79/0.56/0.66	0.85/0.30/0.44
Sigscan[16]	0.75/0.19/0.3	0.88/0.24/0.37	0.80/0.25/0.38	0.71/0.16/0.26	0.92/0.31/0.46	0.77/0.29/0.43	1.00/0.20/0.33
IDAscope_heuristic[8]	0/0/0	1.0/0.03/0.06	1.00/0.19/0.31	1.00/0.52/0.68	0/0/0	1.00/0.12/0.21	0/0/0
Where's crypto[7]	1.00/0.50/0.67	1.0/0.45/0.62	1.00/0.10/0.19	1.00/0.54/0.70	1.00/0.26/0.41	1.00/0.12/0.21	1.00/0.15/0.26

The effectiveness of existing cryptographic algorithm identification tools in identifying cryptographic algorithm types (AES\RSA\DES) by precision, recall, and F1-Score.