
بسم الله الرحمن الرحيم

رمزنگاری احراز اصالت شده: گذشته، حال و آینده

نصور باقری

دانشگاه تربیت دبیر شهید رجایی

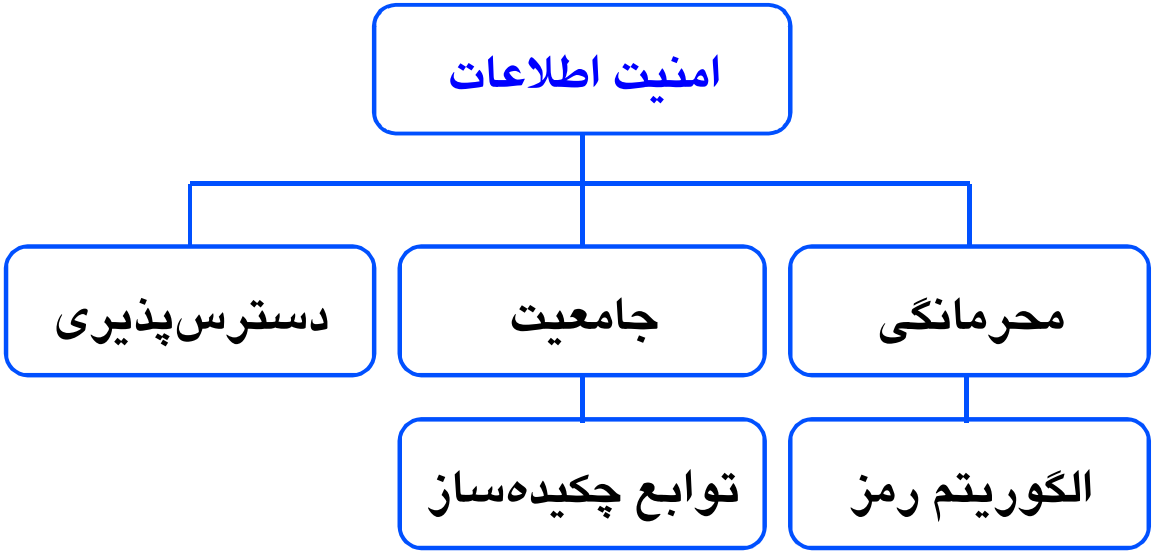
Nbagheri@srttu.edu

با تشکر از آقای مهندس جواد علیزاده برای تهیه بخش اعظم اسلایدها

فهرست مطالب

فهرست مطالب

مقدمه و تعاریف

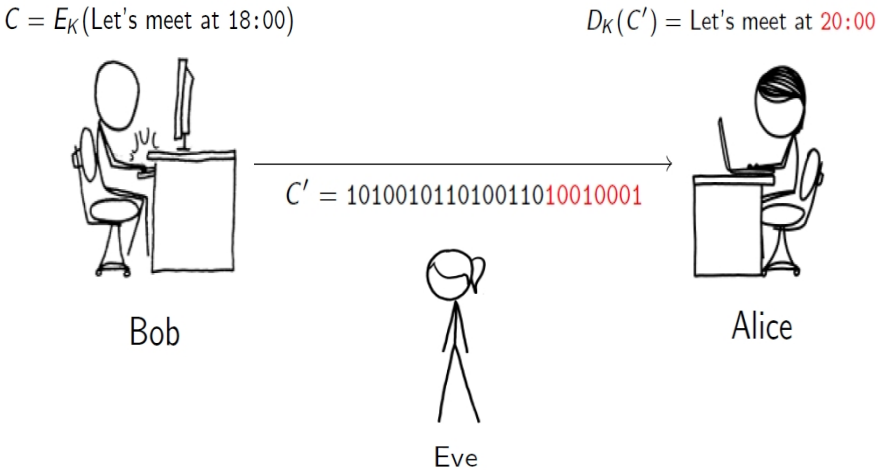


مواردی وجود دارد که برای حفظ امنیت، محرمانگی و احراز اصالت پیام، به طور همزمان لازم هستند.

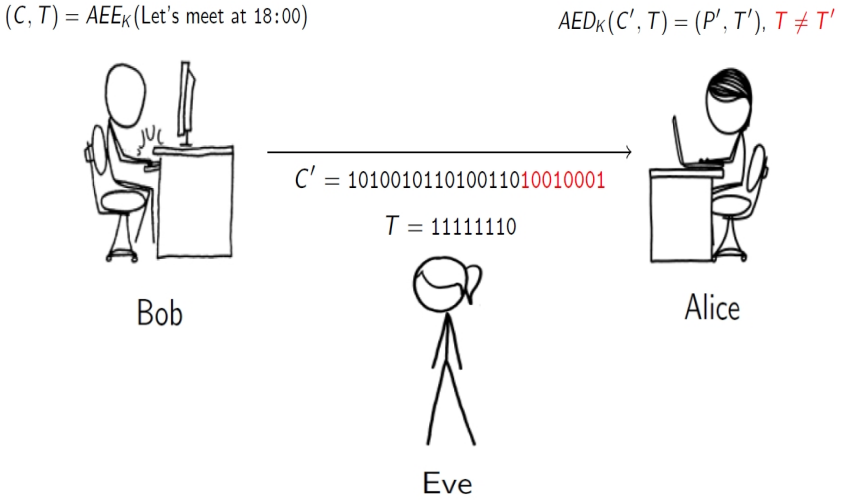
مثال: پروتکل‌های SSL و IPSec

مقدمه و تعاریف

رمزگذاری بدون احراز اصالت

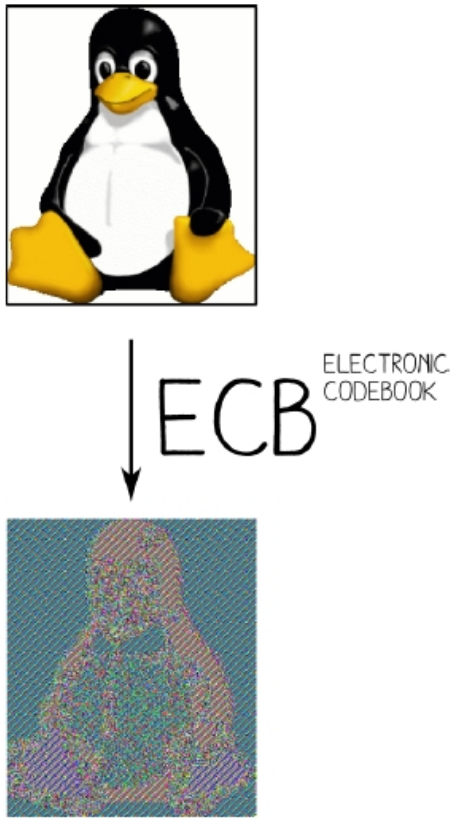


رمزگذاری همراه با احراز اصالت



Aumasson, J.P., Jovanovic, P., Neves, S.: NORX: Parallel and Scalable AEAD. In: ESORICS 2014.

ECB

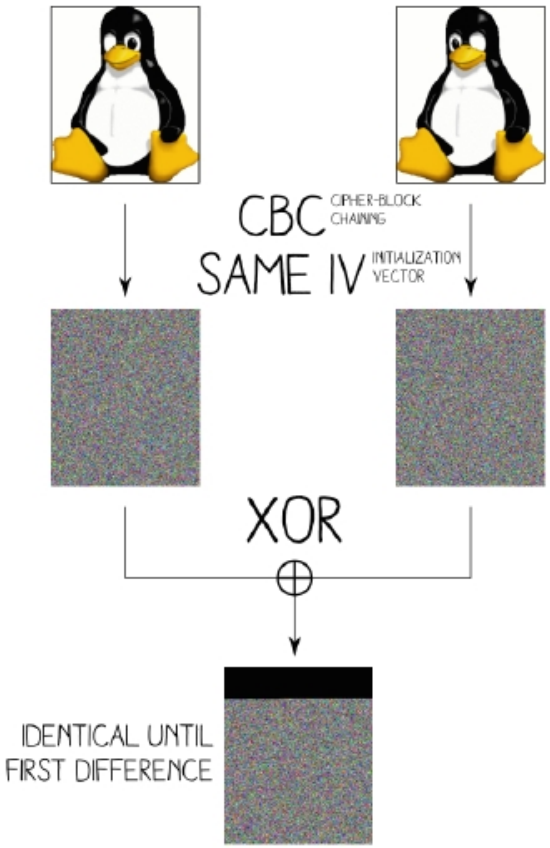


Picture credits: Ange Albertini (@angealbertini, @corkami)

https://code.google.com/p/corkami/

Aumasson, J.P., Jovanovic, P., Neves, S.: NORX: Parallel and Scalable AEAD.

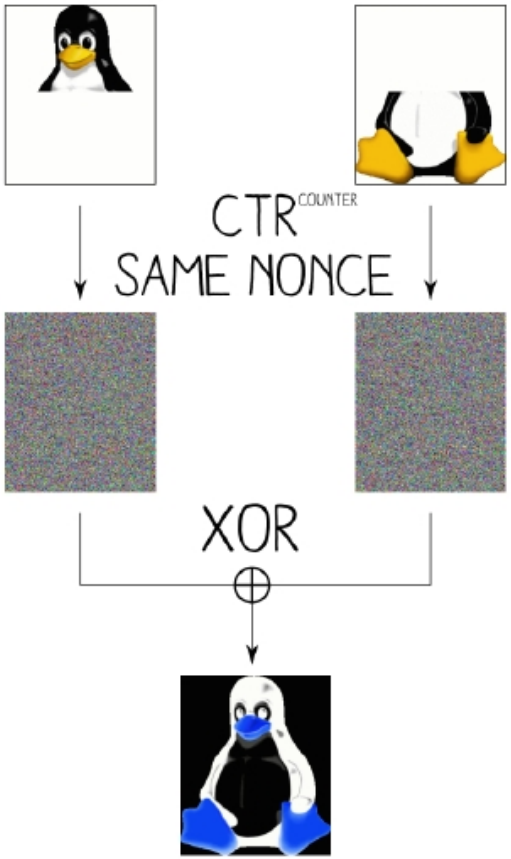
CBC



Picture credits: Ange Albertini (@angealbertini, @corkami)

https://code.google.com/p/corkami/

CTR



Picture credits: Ange Albertini (@angealbertini, @corkami)

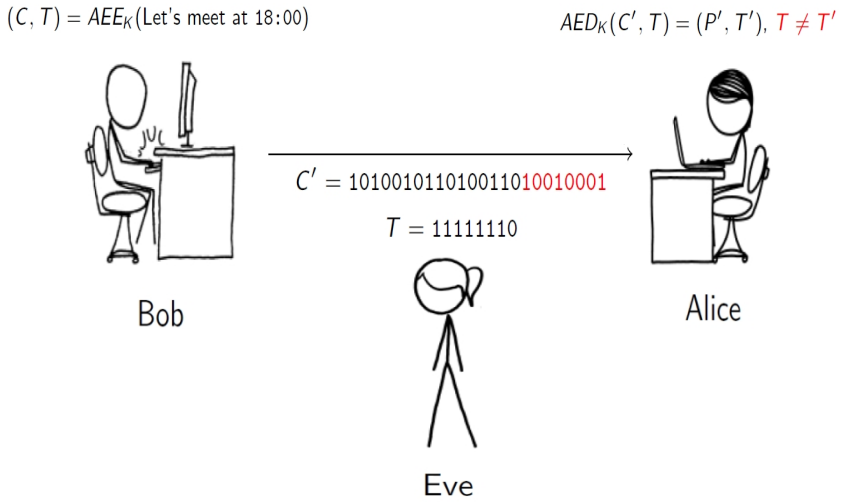
https://code.google.com/p/corkami/

معایب مدهای رمز قالبی

- غالبا در برابر حملات فعال آسیب پذیر هستند.
- به راحتی می توان متن رمز شده را تغییر داد بدون اینکه گیرنده متوجه شود.
- گسترش خطا

راه کار : استفاده از رمزگذاری احراز اصالت شده

رمزگذاری همراه با احراز اصالت



Aumasson, J.P., Jovanovic, P., Neves, S.: NORX: Parallel and Scalable AEAD. In: ESORICS 2014.

تعاریف

تعریف

طرح‌های رمزگذاری احراز اصالت شده (AE)، طرح‌هایی هستند که محرمانگی و احراز اصالت پیام را به طور هم‌زمان برآورده می کنند.

$$AE: (N, A, M) \rightarrow (N, A, C, T)$$

روش عام

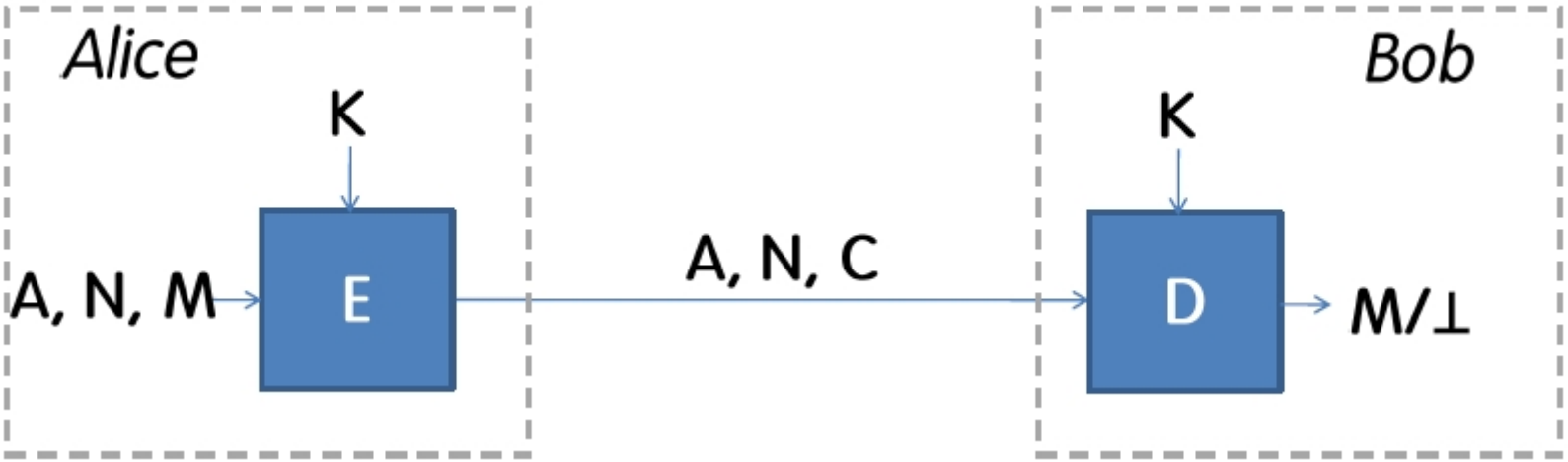
الگوریتم رمز + کد احراز اصالت پیام = رمزگذاری احراز اصالت شده

Bellare and Namprempre (2000)

	Privacy			Integrity	
Composition Method	IND-CPA	IND-CCA	NM-CPA	INT-PTXT	INT-CTXT
Encrypt-and-MAC	insecure	insecure	insecure	secure	insecure
MAC-then-Encrypt	secure	insecure	insecure	secure	insecure
Encrypt-then-MAC	secure	secure	secure	secure	secure

مزی

استفاده از رمزگذاری احراز اصالت شده مبتنی بر تک شمار



Nonce dependent AE: Security fails when N repeats
Nonce MR AE: Provide security when N repeats

E: $C \leftarrow E_K(A, N, M)$

D: $M/\perp \leftarrow D_K(A, N, C)$

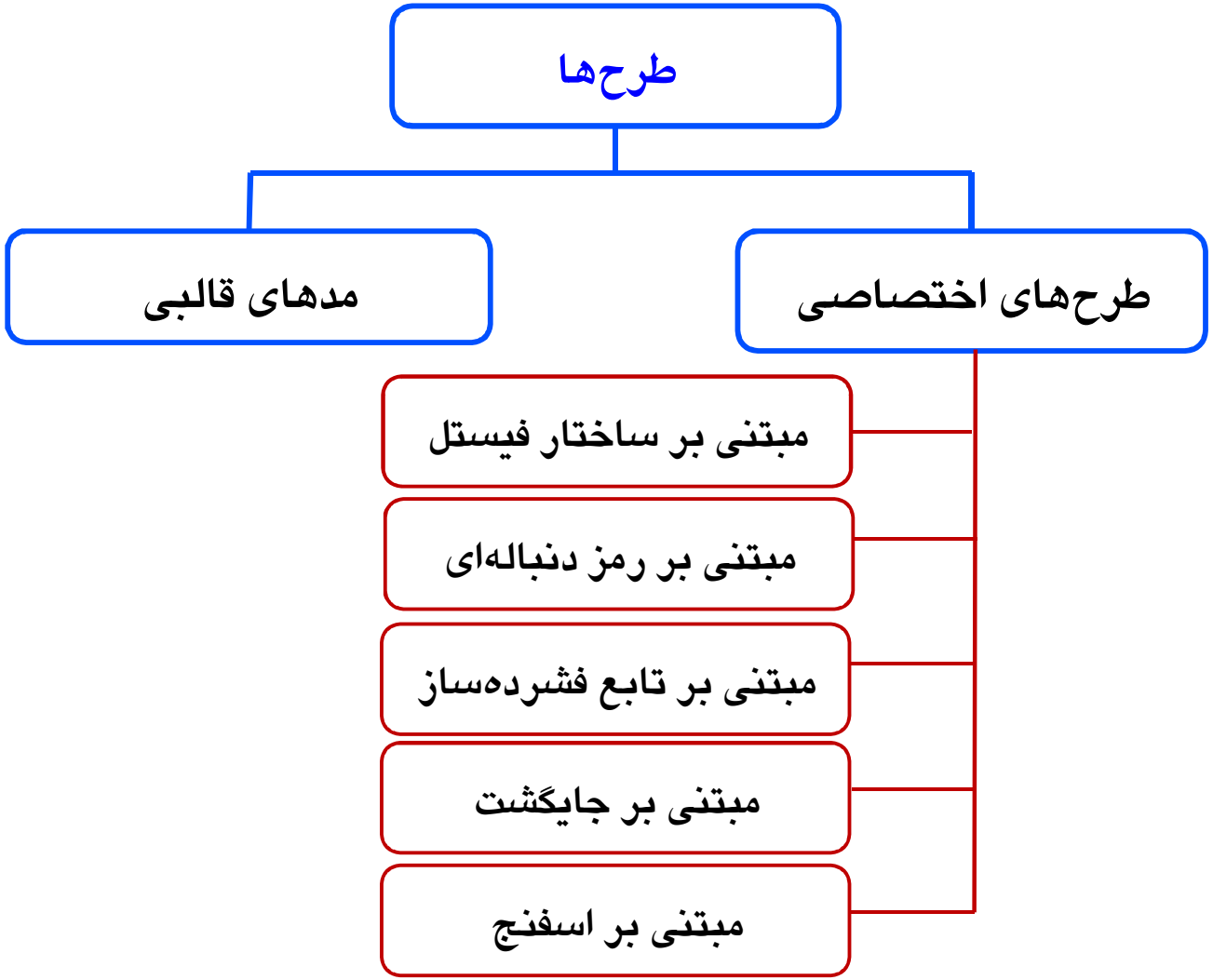
Correctness: $\mathbf{D}_K(A, N, \mathbf{E}_K(A, N, M)) = M$

رمزگذاری احراز اصالت شده اختصاصی قبل از CAESAR

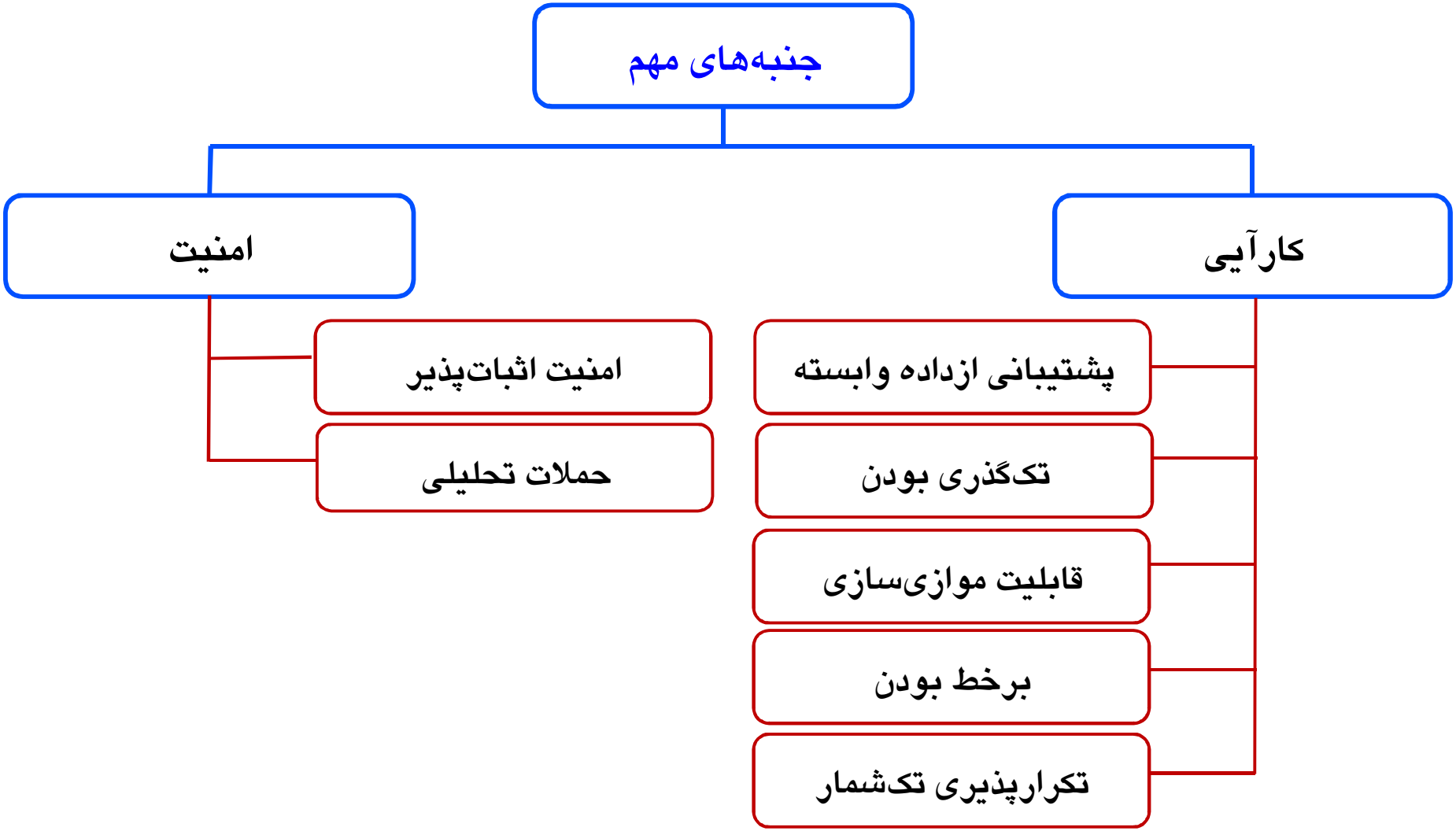
Primitive	Nonce dependent	Nonce MR
Block cipher	IAPM*, OCB*, XECB*, CCM, GCM, OTR*, CLOC	SIV, BTM, McOE-G, POET, COPA
Permutation	Sponge Wrap Ketje&Keyak, NORX	APE

Elena Andreeva: Authenticated Encryption and the CAESAR Competion, ESC 2015

رویکردها در طراحی رمزگذاری احراز اصالت شده اختصاصی



معیارهایی برای ارزیابی یک طرح اختصاصی



فهرست مطالب

- ✓ معرفی رمزگذاری احراز اصالت شده
  - ✓ مقدمه و تعاریف
  - ✓ طرح‌های رمزگذاری احراز اصالت شده و ویژگی‌های آنها
- ✓ مسابقه CAESAR
  - ✓ وضعیت نامزدهای دور اول
- ❑ الگوریتم ARTEMIA
  - مد عمل : JHAE
  - تابع جایگشت
- ❑ چالش های مهم در حوزه رمزگذاری احراز اصالت شده
- ❑ جمع‌بندی و نتیجه‌گیری

مسابقه CAESAR

برگزاری: تحت حمایت NIST

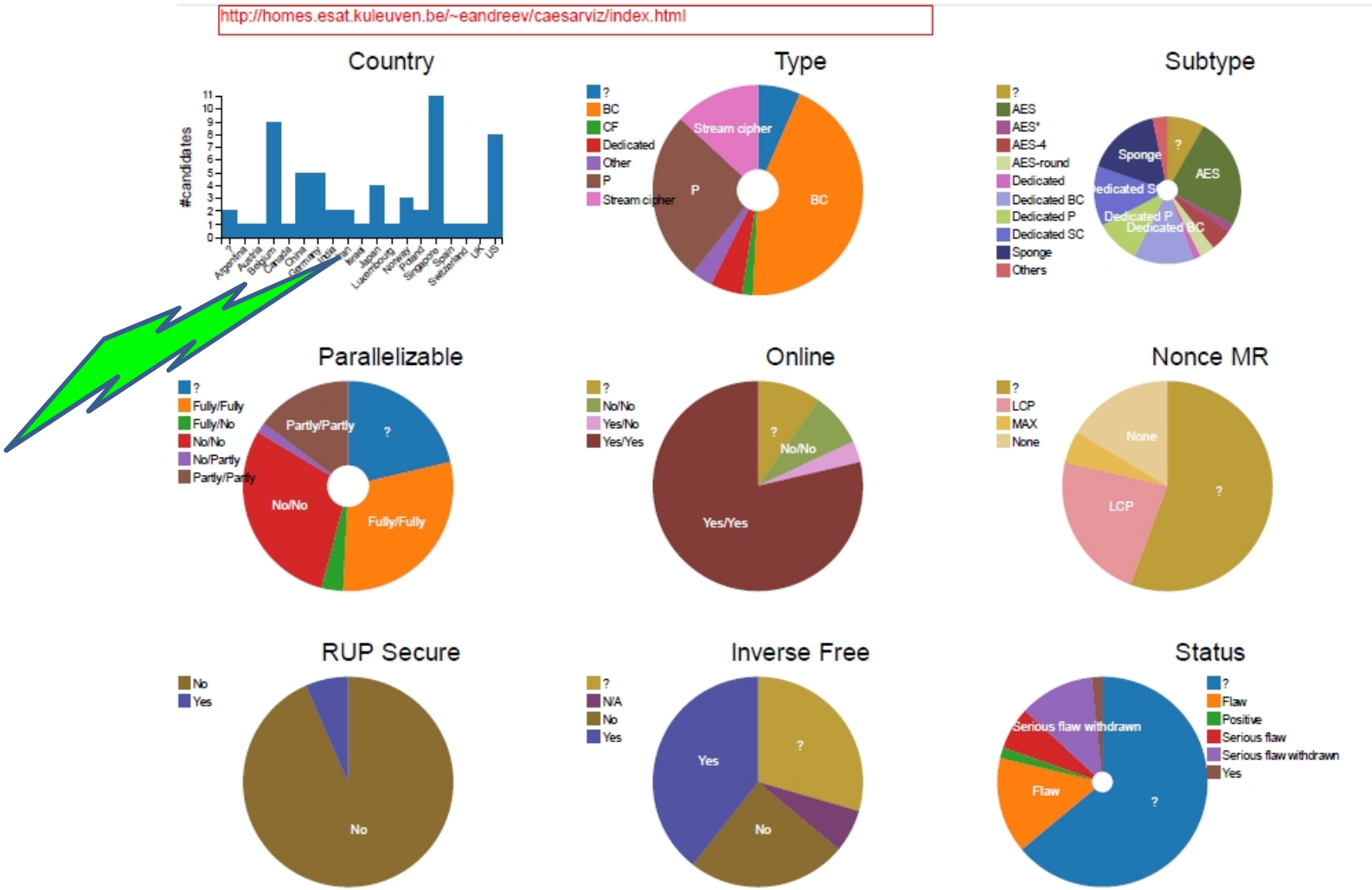
تاریخ	روی-داد
2012.07.05–06	کارگاه آموزشی DIAC (Directions in Authenticated Ciphers)– استکهلم سوئد
2013.01.15	اطلاعیه شروع مسابقه CAESAR
تابستان 2013	برگزاری DIAC 2013
2014.01.15	اتمام مهلت زمانی برای ارسال نامزدهای دور اول مسابقه (تمدید تا 2014.03.15)
2014.05.15	اتمام مهلت زمانی برای پیاده‌سازی نرم‌افزاری
2014.08.23–24	برگزاری DIAC 2014
2015.03.15	اعلام نامزدهای دور دوم مسابقه
2015.04.15	اتمام مهلت زمانی برای بهبود نامزدهای دور دوم
تابستان 2015	برگزاری DIAC 2015
2015.12.15	اعلام نامزدهای دور سوم مسابقه
2016.01.15	اتمام مهلت زمانی برای بهبود نامزدهای دور سوم
تابستان 2016	برگزاری DIAC 2016
2016.12.15	اعلام نامزدهای دور نهایی مسابقه (فینالیست-ها)
2017.01.15	اتمام مهلت زمانی برای بهبود نامزدهای دور نهایی
تابستان 2017	برگزاری DIAC 2017
2017.12.15	اعلام رتبه-های نهایی (و اتمام مسابقه CAESAR)

نامزدهای دور اول

ACORN	++AE	AEGIS	AES-CMCC	AES-COBRA
AES-COPA	AES-CPFB	AES-JAMBU	AES-OTR	AEZ
Artemia	Ascon	AVALANCHE	Calico	CBA
CBEAM	CLOC	Deoxys	ELmD	Enchilada
FASER	HKC	HS1-SIV	ICEPOLE	iFeed[AES]
Joltik	Julius	Ketje	Keyak	KIASU
LAC	Marble	McMambo	Minalpher	MORUS
NORX	OCB	OMD	PAEQ	PAES
PANDA	π-Cipher	POET	POLAWIS	PRIMATEs
Prøst	Raviyoyla	Sablier	SCREAM	SHELL
SILC	Silver	STRIBOB	Tiaoxin	TriviA-ck
Wheesht	YAES			

کل نامزدها	مبتنی بر AES	مبتنی بر اسفنج	مد عمل	طراحی اولیه	امنیت اثبات پذیر
۵۷	۲۱	۵	۲۸	۲۳	۲۷

مقایسه نامزدهای دور اول



The dataviz has been created by Xavier Dutoit.

نامزدهای دور اول

طرح‌های مبتنی بر رمزهای قالبی			
++AE	AVALANCHE	KIASU	Silver
AES-CMCC	CBA	LAC	YAES
AES-COBRA	CLOC	Marble	
AES-COPA	Deoxys	OCB	
AES-CPFB	ELmD	POET	
AES-JAMBU	iFeed[AES]	SCREAM	
AES-OTR	Joltik	SHELL	
AEZ	Julius	SILC	

سایر طرح‌ها			
ACORN	HKC	NORX	Prøst
AEGIS	HS1-SIV	OMD	Raviyoyla
Artemia	ICEPOLE	PAEQ	Sablier
Ascon	Ketje	PAES	STRIBOB
Calico	Keyak	PANDA	Tiaoxin
CBEAM	McMambo	π-Cipher	TriviA-ck
Enchilada	Minalpher	POLAWIS	Wheesht
FASER	MORUS	PRIMATEs	

انصرافی ضعف جدی ضعف قابل رفع مشاهده تحلیل توسط طرحان

کل نامزدها	خارج شده	ضعف (قرمز)	ضعف (نارنجی)	مورد بحث (سبز)	باقیمانده
۵۷	۸	۵	۱۰	۱۰	۳۴

فهرست مطالب

آرتمیا

آرتمیا، یک خانواده از طرح‌های AE اختصاصی است.

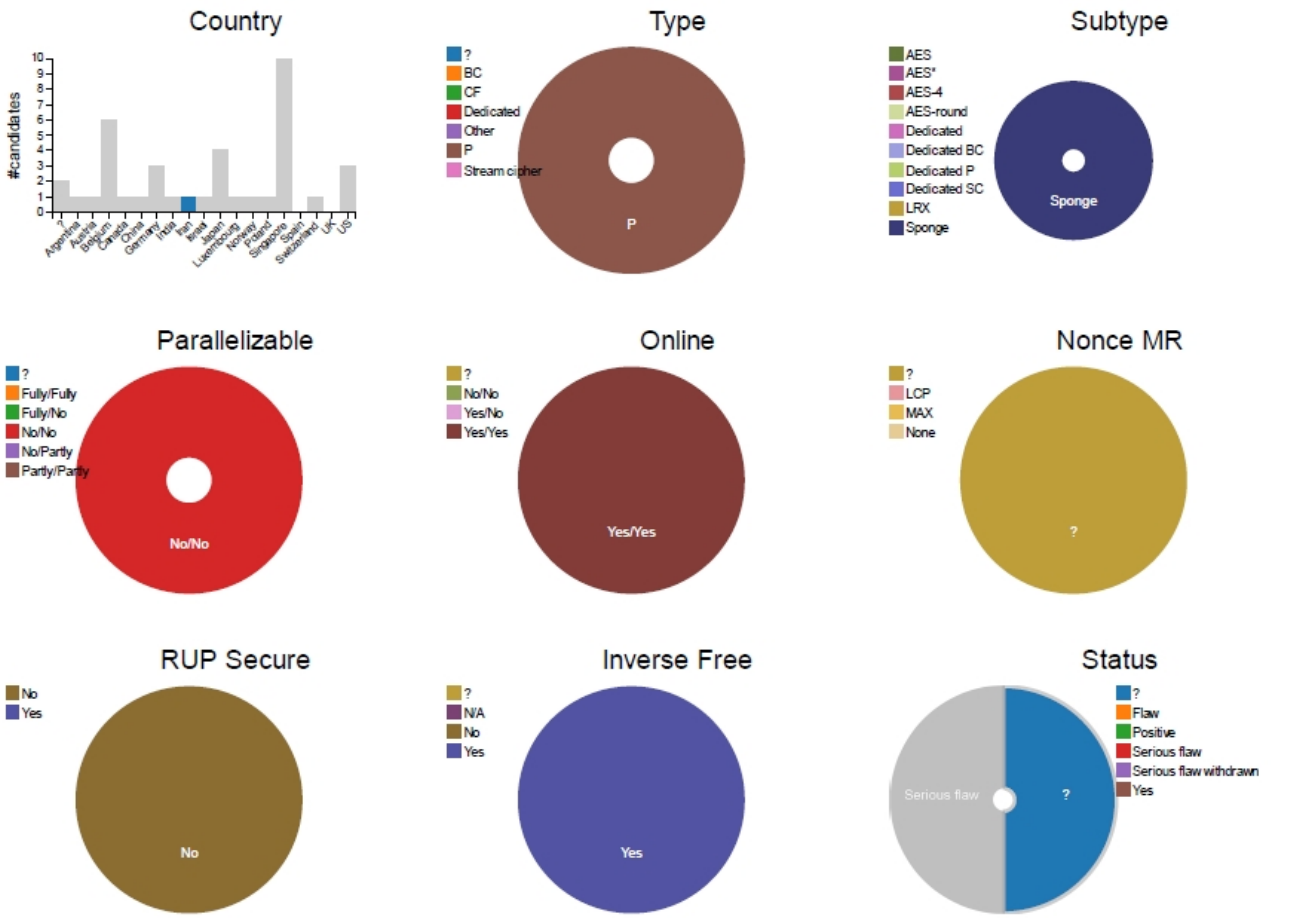
Dedicated *AE*	Provable Security	AD	online	Nonce Misuse Resistance	Inverse-Freeness of π (or f)
ASC-1	Yes	No	No	No	Yes
ALE	No	Yes	Yes	No	Yes
AEGIS	No	Yes	Yes	No	Yes
FIDES	No	Yes	Yes	No	Yes
CBEAM	No	Yes	Yes	No	Yes
APE	Yes	Yes	Enc only	Yes	No
Artemia	Yes	Yes	Yes	No	Yes

دو مولفه اصلی دارد:

۱- مد عمل JHAE ۲- جایگشت آرتمیا

	lenght of permutation $(2n)$	*length of key* (n)	*maximum length of nonce* (n)	*length of tag* (n)
Artemia-256	512	256	≤ 256	256
Artemia-128	256	128	≤ 128	128

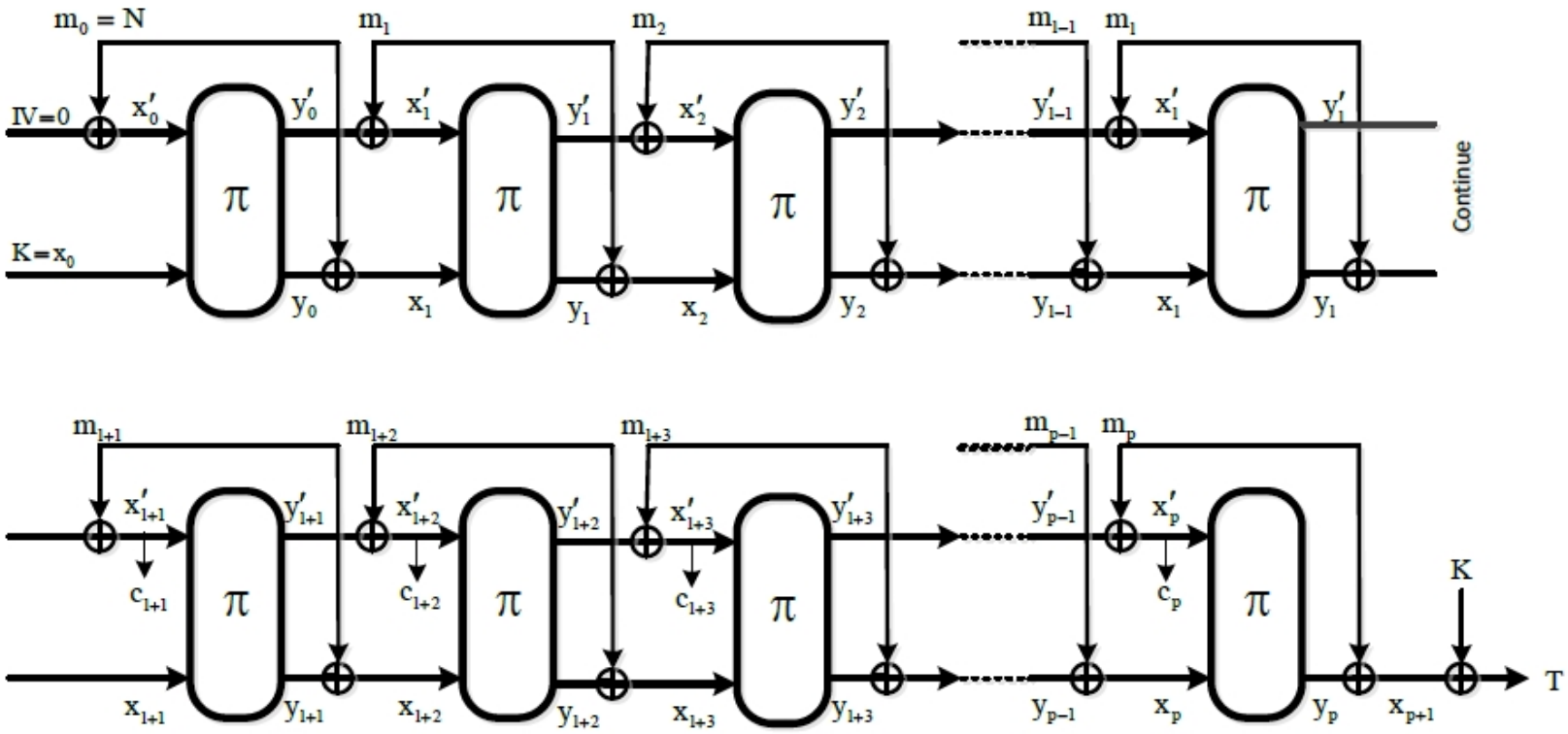
آرتمیا



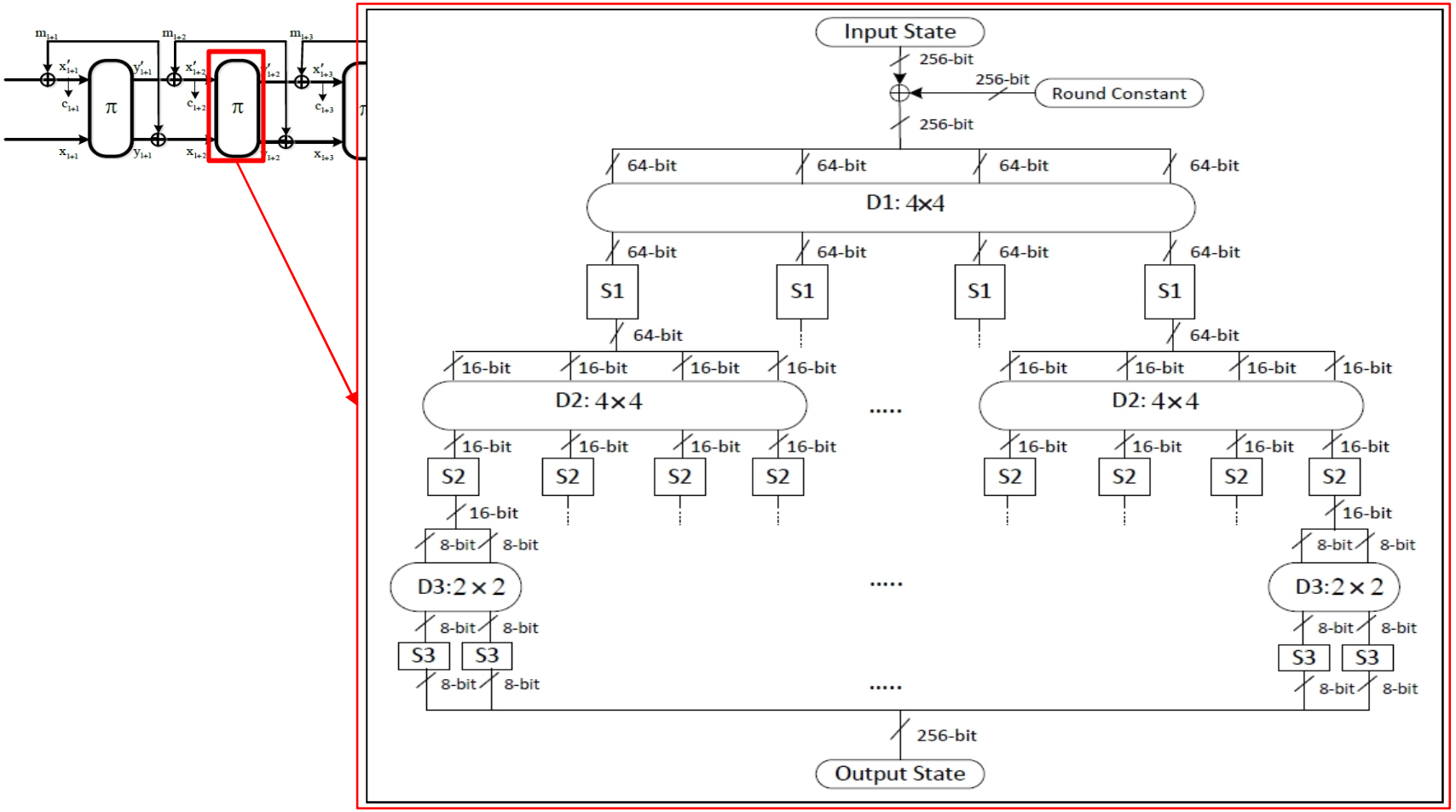
Name	Country	type	subtype	parallelizable	online	nonce MR	decryption Misuse	Inverse Free	status
Artemia	Iran	P	Sponge	No/No	Yes/Yes		No	Yes	

The dataviz has been created by Xavier Dutoit.

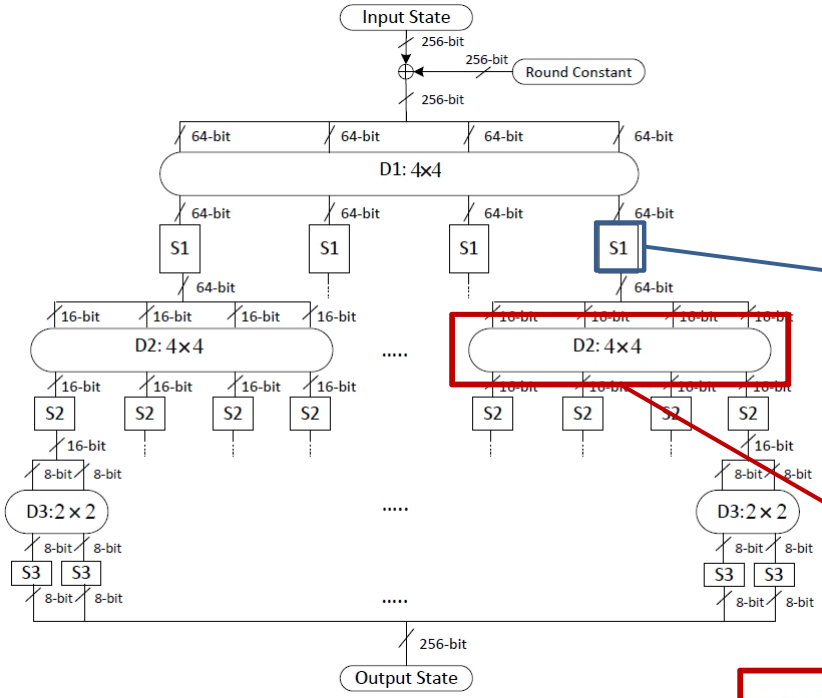
آرتمیا


$m_0 = N$
m_1
m_2
m_{l-1}
m_l
IV=0
x'_0
y'_0
x'_1
y'_1
x'_2
y'_2
y'_{l-1}
x'_l
y'_l
π
K=x_0
y_0
x_1
y_1
x_2
y_2
y_{l-1}
x_l
y_l
Continue
m_{l+1}
m_{l+2}
m_{l+3}
m_{p-1}
m_p
x'_{l+1}
y'_{l+1}
x'_{l+2}
y'_{l+2}
x'_{l+3}
y'_{l+3}
y'_{p-1}
x'_p
c_{l+1}
c_{l+2}
c_{l+3}
c_p
K
T
x_{l+1}
y_{l+1}
x_{l+2}
y_{l+2}
x_{l+3}
y_{l+3}
y_{p-1}
x_p
y_p
x_{p+1}

آرتمیا


Input State
256-bit
256-bit
Round Constant
256-bit
64-bit
64-bit
64-bit
64-bit
D1: 4×4
64-bit
64-bit
64-bit
64-bit
S1
S1
S1
S1
64-bit
64-bit
16-bit
16-bit
16-bit
16-bit
D2: 4×4
.....
D2: 4×4
16-bit
16-bit
16-bit
16-bit
S2
S2
S2
S2
16-bit
16-bit
8-bit
8-bit
D3:2 × 2
.....
D3:2 × 2
8-bit
8-bit
S3
S3
8-bit
8-bit
.....
256-bit
Output State

آرتمیا



	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

$$
\left.
\begin{aligned}
Y_0 &= X_0 \oplus X_2 \oplus X_3 \oplus L(X_1 \oplus X_3) \\
Y_1 &= X_1 \oplus X_3 \oplus Y_0 \oplus L(X_2 \oplus Y_0) \\
Y_2 &= X_2 \oplus Y_0 \oplus Y_1 \oplus L(X_3 \oplus Y_1) \\
Y_3 &= X_3 \oplus Y_1 \oplus Y_2 \oplus L(Y_0 \oplus Y_2)
\end{aligned}
\right\}
$$

اهداف امنیتی

Goal	Artemia-256 bits of security	Artemia-128 bits of security
Confidentiality of the secret key	128	64
Confidentiality of the plaintext	128	64
Integrity of the plaintext	128	64
Integrity of the associated data	128	64
Integrity of the nonce	128	64

تحلیل و ارزیابی آرتمیا

مد JHAE:

Theorem 1. *JHAE based on an ideal permutation* $\pi : \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ *is* (t_A, σ, ϵ)*-indistinguishable from an ideal AE based on a random function RO and an ideal permutation* π' *with the same domain and range, for any* t_A*, then* $\epsilon \leq \frac{\sigma(\sigma-1)}{2^{2n-1}} + \frac{\sigma^2}{2^{2n}} + \frac{\sigma^2}{2^n}$*, where* σ *is the total number of blocks in queries to* $JHAE - E$*,* π*, and* π^{-1}*, by* $\mathcal{A}$*.*

Theorem 2. *For any adversary* $\mathcal{A}$ *that makes* σ *block queries to* $JHAE - E$*,* π*, or* π^{-1} *in total, JHAE based on an ideal permutation* $\pi : \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ *is* (t_A, σ, ϵ)*-unforgeable, then* $\epsilon \leq \frac{3\sigma^2}{2^n} + \frac{3q}{2^n}$.

جایگشت آرتمیا:

Artemia	# Rounds	# Minimum active SBoxes	Maximum probability of a differential characteristic	Maximum bias of a linear characteristic
$Artemia-512$	2	45	2^{-270}	2^{-180}
$Artemia-512$	4	90	2^{-540}	2^{-360}
$Artemia-256$	2	35	2^{-210}	2^{-140}
$Artemia-256$	4	70	2^{-420}	2^{-280}

ارزیابی آرتمیا در دور اول

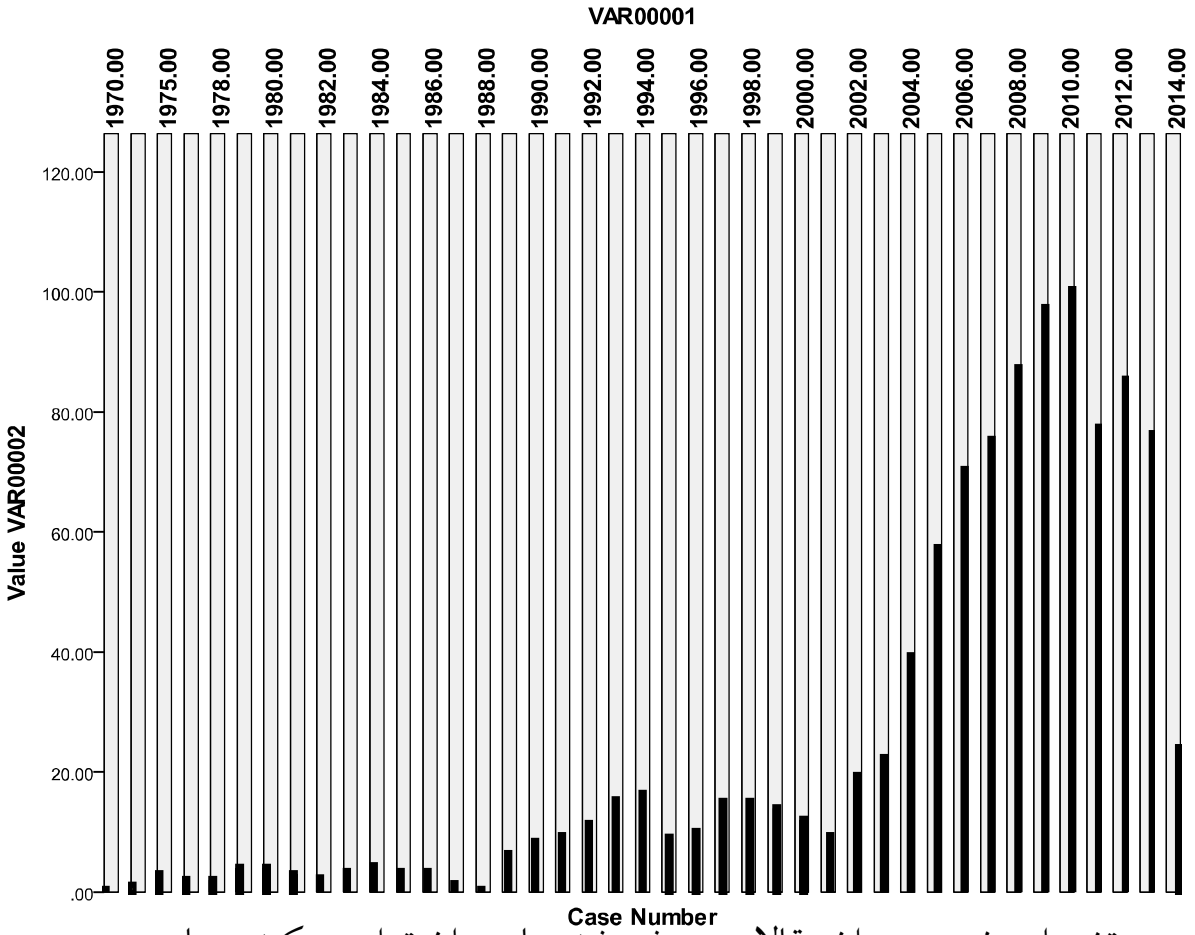
- ✓ **Philipp Jovanovic, Atul Luykx, and Bart Mennink, "Beyond 2^{c/2} Security in Sponge-Based Authenticated Encryption Modes", ASIACRYPT 2014.**

Abstract. The Sponge function is known to achieve $2^{c/2}$ security, where c is its capacity. This bound was carried over to keyed variants of the function, such as SpongeWrap, to achieve a $\min\{2^{c/2}, 2^{\kappa}\}$ security bound, with κ the key length. Similarly, many CAESAR competition submissions are designed to comply with the classical $2^{c/2}$ security bound. We show that Sponge-based constructions for authenticated encryption can achieve the significantly higher bound of $\min\{2^{b/2}, 2^{c}, 2^{\kappa}\}$ asymptotically, with $b > c$ the permutation size, by proving that the CAESAR submission NORX achieves this bound. Furthermore, we show how to apply the proof to five other Sponge-based CAESAR submissions: Ascon, CBEAM/STRIBOB, ICEPOLE, Keyak, and two out of the three PRIMATEs. A direct application of the result shows that the parameter choices of these submissions are overly conservative. Simple tweaks render the schemes considerably more efficient without sacrificing security. For instance, NORX64 can increase its rate and decrease its capacity by 128 bits and Ascon-128 can encrypt three times as fast, both without affecting the security level of their underlying modes in the ideal permutation model.

It is expected that the security proofs also generalize to the modes of Artemia [1] and π-Cipher [17]. However, they deviate slightly more from the other designs. Artemia is based on the JH hash function [30] and XORs data blocks in both the rate and capacity part. It does not use domain separations, rather it encodes the lengths of the inputs into the padding at the end [5]. Therefore, a generalization of the proof of NORX to Artemia is not entirely straightforward.

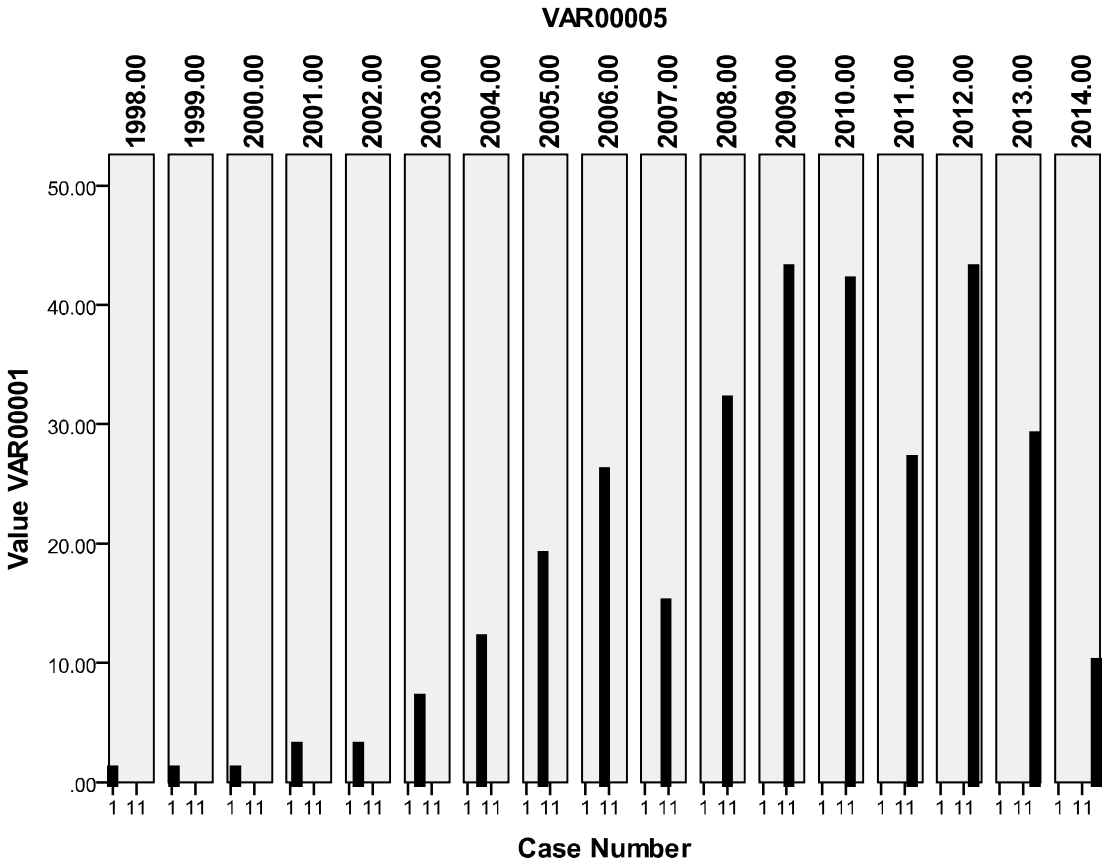
فهرست مطالب

تاثیر مسابقات در حوزه رمز بر تحقیقات (مثال SHA-3)



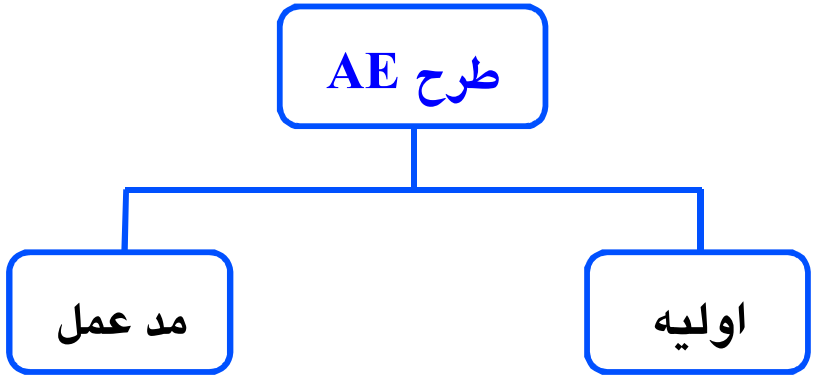
تغییرات نسبی میزان مقالات منتشر شده با عنوان توابع چکیده-ساز

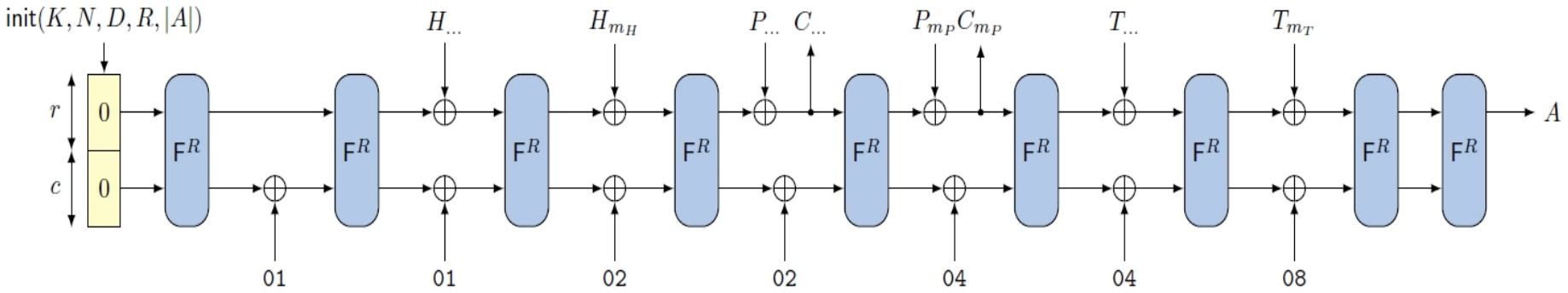
ارزیابی امنیتی کاندیدا ها(مخصوصا کاندیداهای دور دوم در این مرحله)



تغییرات نسبي ميزان مقالات منتشر شده با عنوان برخورد و پيش-تصوير/دوم

امنیت اثبات‌پذیر طرح‌های رمزگذاری احراز اصالت شده





CHES 2010: Santa Barbara, CA, USA:

•Olivier Benoît, Thomas Peyrin: Side-Channel Analysis of Six SHA-3 Candidates. 140-157

•Luca Henzen, Pietro Gendotti, Patrice Guillet, Enrico Pargaetzi, Martin Zoller, Frank K. Gürkaynak: Developing a Hardware Evaluation Method for SHA-3 Candidates. 248-263

•Kris Gaj, Ekawat Homsirikamol, Marcin Rogawski: Fair and Comprehensive Methodology for Comparing Hardware Performance of Fourteen Round Two SHA-3 Candidates Using FPGAs. 264-278

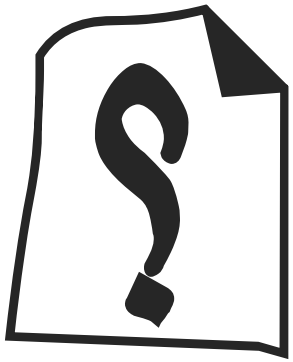
• view export ask others Joppe W. Bos, Deian Stefan: Performance Analysis of the SHA-3 Candidates on Exotic Multi-core Architectures. 279-293

•Christian Wenzel-Benner, Jens Gräf: XBX: eXternal Benchmarking eXtension for the SUPERCOP Crypto Benchmarking Framework. 294-305

جمع‌بندی و نتیجه‌گیری

- در اینجا مباحث مربوط به طرح‌های رمزگذاری احراز اصالت شده و امنیت اثبات‌پذیر مرور شد.
- در حال حاضر جامعه جهانی رمزنگاری توجه خاصی به موضوع رمزگذاری احراز اصالت شده دارند.
- به نظر می رسد این حوزه زمینه مناسبی برای انجام تحقیقات در لبه دانش حداقل تا پایان مسابقه CAESAR است.

با تشکر از صبر و حوصله شما عزیزان



نصور باقری

Nbagheri@srttu.edu