

راهنمای تهیه و نگارش مقالات نشریه علمی منادی افتا با استفاده از زی پرشین و لاتک

نویسنده اول^۱، نویسنده دوم^۲ و نویسنده سوم^{*}

^۱بخش، دانشگده، دانشگاه، شهر، ایران

^۲بخش، دانشگده، دانشگاه، شهر، ایران

اطلاعات مقاله	چکیده
کلمات کلیدی:	این چکیده شامل خلاصه‌ای از نتایج تجربی یا نظری حاصل از کار تحقیقاتی شما است. محتوای این بخش
کلمه کلیدی ۱	نباید از ۲۰۰ کلمه تجاوز نماید. در غیر این صورت در فرمت نهایی مقاله شما ما با مشکلات زیادی مواجه
کلمه کلیدی ۲	خواهیم شد. از بحث‌های کلی و مقدماتی در چکیده پرهیز شود. در صورتی که در این بخش از نماد یا کلمات
کلمه کلیدی ۳	اختصاری لاتین استفاده می‌کنید، باید در متن چکیده آن را معرفی نمایید. از ارجاع به مراجع و پانویس در
کلمه کلیدی ۴	بخش چکیده پرهیز شود.
نوع مقاله: پژوهشی	

© ۱۴۰۳ انجمن رمز ایران

۱ مقدمه

دو فصل نامه علمی-ترویجی «منادی افتا» با هدف ترویج و اعتلای سطح دانش نظری و عملی اساتید، دانش پژوهان، مهندسين و دانشجویان در حوزه امنیت فضای تولید و تبادل اطلاعات، از کلیه اساتید، پژوهشگران، مهندسين و دانشجویان رشته‌های مهندسی مخابرات، الکترونیک، کامپیوتر، علوم ریاضی، آمار و سایر رشته‌های مرتبط برای ارائه مقالات علمی-ترویجی در زمینه‌های رمز شناسی، نهان نگاری، امنیت زیرساخت‌های کامپیوتری (نرم افزار، سخت افزار، سیستم عامل، پایگاه داده و ...)، امنیت زیرساخت‌های ارتباطی (امنیت شبکه، مخابرات امن و ...)، امنیت سامانه‌های کاربردی (تجارت الکترونیک، قوانین و مسائل حقوقی افتا و ...) و سایر موضوعات مرتبط دعوت به عمل می‌آورد. این دستورالعمل روش تهیه مقاله برای ارائه به دوفصل نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا) را بیان می‌کند. از نویسندگان و تهیه‌کنندگان محترم مقالات، تقاضا می‌شود، نکات زیر را در تهیه و تنظیم مقالات ارسالی رعایت نمایند:

- (۱) مقالات قابل چاپ در نشریه، باید با بیان جدید و نو در یکی از زمینه‌های مذکور بوده و از نظر جنبه علمی و ترویجی قوی باشد.
- (۲) مقالات نباید در هیچ نشریه علمی داخلی یا خارجی دیگر به چاپ رسیده باشد؛ یا هم‌زمان به نشریه دیگری ارسال شود؛ اما مقالات ارائه شده در کنفرانس‌ها، پس از طی مراحل داوری، قابل پذیرش و چاپ خواهد بود.
- (۳) زبان رسمی نشریه، فارسی (به همراه چکیده انگلیسی) می‌باشد.
- (۴) مقالات ارسالی باید در دو نسخه PDF و Word و یا LaTeX و PDF ارسال شوند.
- (۵) ساختار مقاله باید شامل عنوان، چکیده فارسی، متن اصلی، نتایج و جمع‌بندی، مراجع، شکل‌ها و جدول‌ها (در صورت نیاز) باشد.
- (۶) مقالات ارسالی بایستی حداقل ۸ صفحه و حداکثر ۲۰ صفحه باشند.
- (۷) اصطلاحات و اسامی خارجی با معادل‌های دقیق و رسا در زبان فارسی و نام کامل واژه و عبارت اختصاری به کار رفته در متن، به پانویس ارجاع شوند.
- (۸) مسئولیت مطالب درج شده در مقاله بر عهده نویسنده (یا نویسندگان) آن خواهد بود.
- (۹) دوفصل نامه «منادی افتا»، حق رد یا قبول مقالات را برای خود محفوظ داشته و هیأت تحریریه در انجام ویرایش ادبی با حفظ

*نویسنده مسئول

آدرس‌های رایانامه: email1@some.ac.ir (نویسنده اول)، email2@some.ac.ir (نویسنده دوم)، email3@some.ac.ir (نویسنده سوم)

© ۱۴۰۳ تمامی حقوق متعلق به انجمن رمز ایران است.

(ب) مورد دوم
(ج) مورد سوم
(د) مورد چهارم

۲.۳ محط‌های آماده شده برای قضا

حال به قضیه ۲ ارجاع می‌دهم.
گزاره ۱. یک گزاره بنویسید.
نتیجه ۱. یک نتیجه بنویسید.

اثاث. یک محط اثاث

- لم ۱. یک لم بنویسید.
ادعا ۱. یک ادعا بنویسید.
اصل ۱. یک اصل بنویسید.
حدس ۱. یک حدس بنویسید.
نکته ۱. یک نکته بنویسید.
فرضیه ۱. یک فرضیه بنویسید.
فرض ۱. یک فرض بنویسید.
محک ۱. یک محک بنویسید.
تعریف ۱. یک تعریف بنویسید.
مثال ۱. یک مثال بنویسید.
تذکر ۱. یک تذکر بنویسید.
نماد ۱. یک نماد بنویسید.
مسئله ۱. یک مسئله بنویسید.
اصل ۱. یک اصل بنویسید.

برای نوشتن یک فرمول در داخل متن به صورت $e^{i\pi} + 1 = 0$ عمل کنید. اگر می‌خواهید فرمول بدون شماره در یک خط جدا قرار بگیرد حتماً از کد `شماره استفاده` نمایید:

$$e^{i\pi} + 1 = 0.$$

۱.۲ نصب توزیع لاتک و زی‌پرشین

۲.۲ فونت‌های مورد نیاز

در این قالب از فونت Yas برای متون فارسی و از فونت Times New Roman برای متون انگلیسی استفاده شده است. این فونت‌ها باید حتماً بر روی سیستم عامل شما نصب باشد. فونت Yas در پوشه‌ای در قالب ارائه شده قرار داده شده است که می‌توانند از آن استفاده کنند.

با استفاده از نسخه همین متن به عنوان نسخه پایه مقاله نیازی به تنظیم مجدد و صفحه‌بندی نیست.

اگر نیاز به لیست‌های شماره گذاری شده دارید می‌توانید به طرق زیر عمل کنید.

یک لیست نمونه

- مورد اول
- مورد دوم

یک لیست نمونه

- (۱) مورد اول
(۲) مورد دوم

یک لیست نمونه

توصیف اول مورد اول

توصیف دوم مورد دوم

برای تولید لیست‌های پیچیده‌تر از بسته `enumitem` استفاده کند.

(آ) مورد اول

¹LaTeX ²X_YPersian ³TeXLive ⁴MikTeX

جدول ۱. مقایسه ایده پیشنهادی و مقالات ارائه شده

تکنولوژی	بیت تصادفی (bits)	تأخیر زمانی	مساحت	طرح
UMC 180nm	۸	۳۶	۱,۳۷	[۱]
UMC 180nm	۰	۱۶	۴,۲۰	[۲]
UMC 180nm	۳۲	۸	۲,۳۲	[۳]
UMC 180nm	۱۸	۸	۲,۶۰	[۴]
Nangate 45nm	۵۴	۶	۱,۸۸	[۵]
TSMC 65nm	۶۴	۵	۱,۴۲	[۶]
Nangate 45nm	۱۹	۲ + ۳	۱,۶۹	[۷]
UMC 180nm	۴۸	۴	۴,۲۴	[۸]

ببینید. توضیح هر جدول باید در بالای آن قرار بگیرد. همچنین از بسته tabularx استفاده کنید تا عرض جدول برابر با عرض ستون شود.

همچنین می‌توان یک شکل یا جدول بزرگ را در کل عرض متن جای داد. شکل ۲ را ببینید.

۵.۳ محیط الگوریتم

یک مشاهده طریقه نگارش الگوریتم و ارجاع به آن، الگوریتم ۱ را ببینید.

الگوریتم ۱ روال شناسایی ۱۲ بیت کوچک‌تر بلوک‌های جداول مراجعه

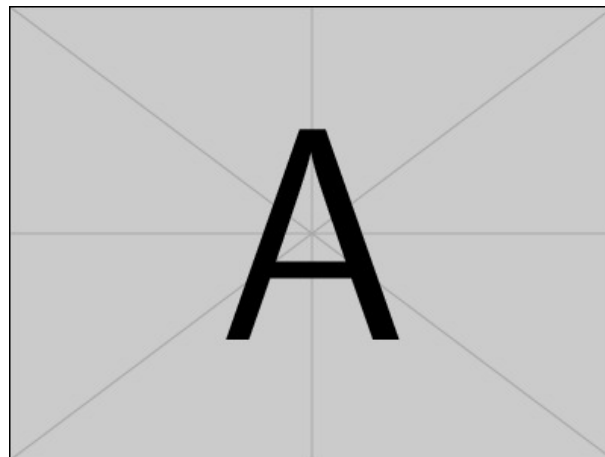
```

1: for ( $i = 0; i < i + +$ )
2:   for ( $o = 0; o < N; o + +$ )
3:      $maccess(M[o]);$ 
4:   end for
5:    $t1 = rdtsc();$ 
6:    $AES^k(x);$ 
7:    $t2 = rdtsc();$ 
8:    $c[x^b][j] + +; \quad b = 0.4.8.12 \quad 0 \leq j < 256$ 
9:    $T[x^b][j] = T[x^b][j] + (t2 - t1);$ 
10: end for
11: for ( $b = 0; b < 16; b + +$ )
12:   for ( $x^b = 0; x^b < 256; x^b + +$ )
13:     for ( $j = 0; j < 256; j + +$ )
14:        $D[x^b][j] = \frac{T[x^b][j]}{c[x^b][j]}$ ;
15:     end for
16:   end for
17: end for

```

۶.۳ مراجع

شماره مراجع هم در متن و هم در بخش مراجع در میان گروه قرار داده می‌شود. شماره اختصاص داده شده به مراجع به ترتیب ظاهر شدن



شکل ۱. یک شکل آزمایشی

برای فرمول‌های یک خطی شماره‌دار از محیط equation استفاده کنید:

$$e^{i\pi} + 1 = 0 \quad (۱)$$

برای ارجاع به فرمول‌های ریاضی، شماره فرمول باید در پرانتز قرار بگیرد. مثلاً فرمول (۱) فرمول اوایلر است.

برای نوشتن فرمول‌های چندخطی از محیط align استفاده کنید. مثلاً فرمول چندخطی شماره‌دار زیر را ببینید که فقط دو فرمول شماره دارند:

$$e^{i\pi} + 1 = 0 \quad (۲)$$

$$e^{i\pi} + 1 = 0 \quad (۳)$$

یا فرمول چندخطی بدون شماره زیر:

$$e^{i\pi} + 1 = 0$$

$$e^{i\pi} + 1 = 0$$

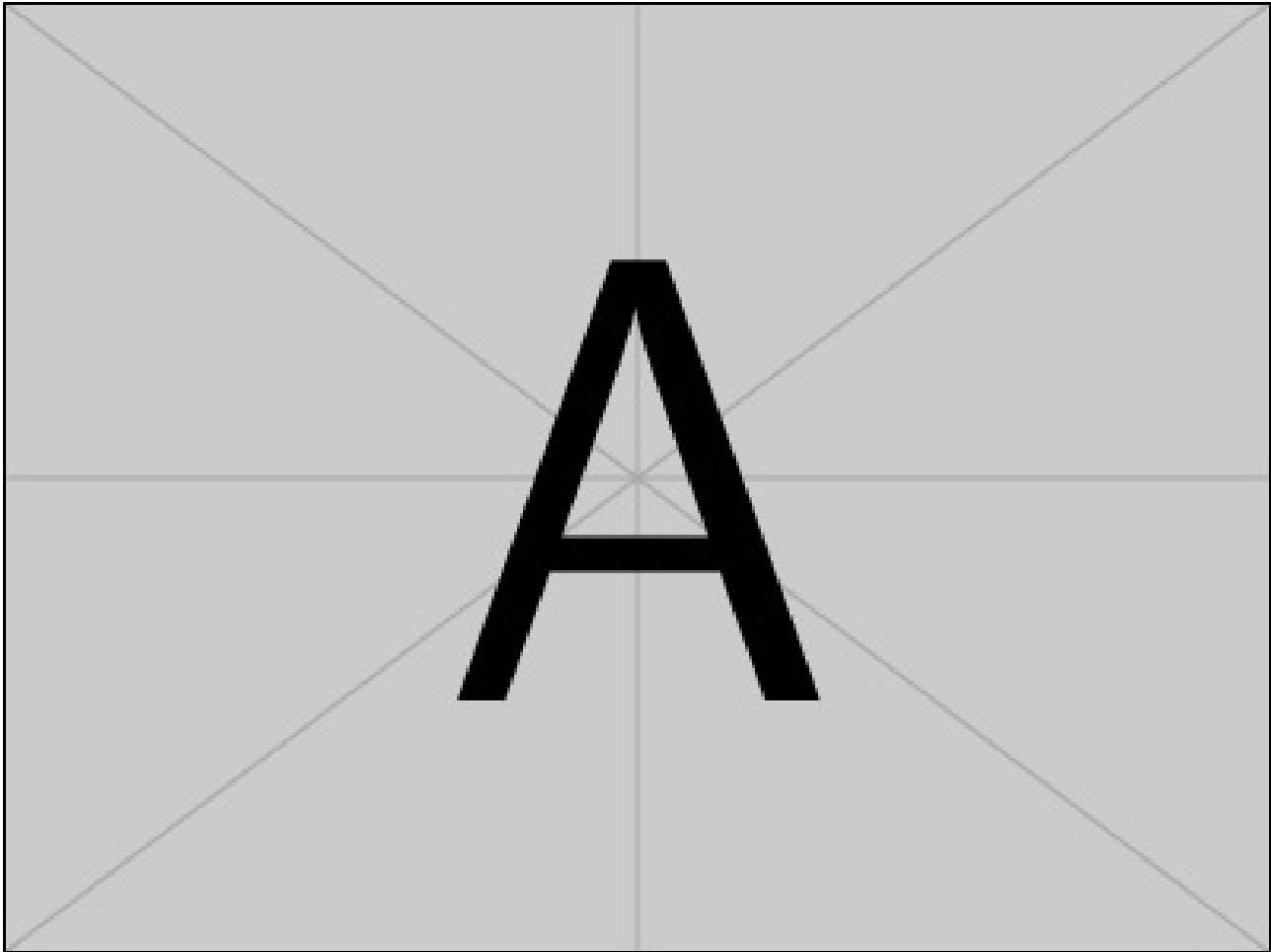
$$e^{i\pi} + 1 = 0$$

$$e^{i\pi} + 1 = 0$$

۴.۳ تصاویر و جداول

در اینجا یک شکل آورده می‌شود. لازم نیست شکل‌ها در همان جایی که در سورس قرار داده می‌شوند، در خروجی هم در همان جا ظاهر شوند. به جای این کار می‌توان به آن‌ها ارجاع داد. به عنوان مثال شکل ۱ را ببینید. زیرنویس شکل‌ها در زیر آنها باید ظاهر شود. عرض تصاویری که در یک ستون قرار می‌گیرند هم باید به اندازه عرض ستون باشد. همچنین بهتر است که اشکال شما با پسوند pdf یا png باشند. اشکال را در پوشه Images ذخیره کنید.

در اینجا یک جدول آورده می‌شود. لازم نیست جدول‌ها در همان جایی که در سورس قرار داده می‌شوند، در خروجی هم در همان جا ظاهر شوند. به جای این کار می‌توان به آن‌ها ارجاع داد. به عنوان مثال جدول ۱ را



شکل ۲. عنوان کلی شکل

sign of Integrated Circuits and Systems, 40(6):1010–1038, 2020.

- [3] Kan Xiao, Domenic Forte, Yier Jin, Ramesh Karri, Swarup Bhunia, and Mohammad Tehranipoor. Hardware trojans: Lessons learned after one decade of research. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 22(1):1–23, 2016.
- [4] Bicky Shakya, Tony He, Hassan Salmani, Domenic Forte, Swarup Bhunia, and Mark Tehranipoor. Benchmarking of hardware trojans and maliciously affected circuits. *Journal of Hardware and Systems Security*, 1(1):85–102, 2017.
- [5] Jonas Krautter, Dennis RE Gnad, and Mehdi B Tahoori. Fpgahammer: Remote voltage fault attacks on shared fpga, suitable for dfa on aes. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 44–68, 2018.
- [6] Jayaram Bhasker and Rakesh Chadha. *Static timing analysis for nanometer designs: A practical approach*. Springer

این مراجع در متن مقاله است. به طور کلی استاندارد ارجاع به مراجع بر مبنای استاندارد IEEE می باشد که جهت مشاهده آن می توانید به دستورالعمل IEEE مراجعه نمایید. توصیه می شود مراجع مقالات چاپ شده در شماره های اخیر نشریه را مشاهده فرمایید تا بتوانید سبک نوشتن مراجع را رعایت نمایید.

سعی کنید مراجع را با استفاده از bibtex بنویسید. با دیدن همین نمونه آماده شده می توانید از این قابلیت لاتک استفاده کنید. در غیر این صورت اگر می خواهید از محیط thebibliography در لاتک استفاده کنید، حتما شیوه نوشتن مراجع را رعایت فرمائید.

مراجع

- [1] Swarup Bhunia and M Tehranipoor. The hardware trojan war. *Cham, Switzerland: Springer*, 2018.
- [2] Wei Hu, Chip-Hong Chang, Anirban Sengupta, Swarup Bhunia, Ryan Kastner, and Hai Li. An overview of hardware security and trust: Threats, countermeasures, and design tools. *IEEE Transactions on Computer-Aided De-*

Science & Business Media, 2009.

- [7] Michael Bushnell and Vishwani Agrawal. *Essentials of electronic testing for digital, memory and mixed-signal VLSI circuits*, volume 17. Springer Science & Business Media, 2004.
- [8] Arash Nejat, David Hely, and Vincent Beroulle. Escalation: Leveraging logic masking to facilitate path-delay-based hardware trojan detection methods. *Journal of Hardware and Systems Security*, 2(1):83–96, 2018.