Capítulo 1

Lightweight Cryptography

Alexandre Zucki Baciuk, João Pedro Gava Ribeiro e Rodrigo Belniok Czelusniak

Abstract

This meta-paper describes the style to be used in articles and short papers for SBC conferences. For papers in English, you should add just an abstract and for the papers in Portuguese, we also ask for an abstract in Portuguese ("resumo"). In both cases, abstracts should not have more than 10 lines and must be in the first page of the paper.

Resumo

Este meta-artigo descreve o estilo a ser usado na confecção de artigos e resumos de artigos para publicação nos anais das conferências organizadas pela SBC. É solicitada a escrita de resumo e abstract apenas para os artigos escritos em português. Artigos em inglês, deverão possuir apenas abstract. Nos dois casos, o autor deve tomar cuidado para que o resumo (e o abstract) não ultrapassem 10 linhas cada, sendo que ambos devem estar na primeira página do artigo.

1.1. Introdução

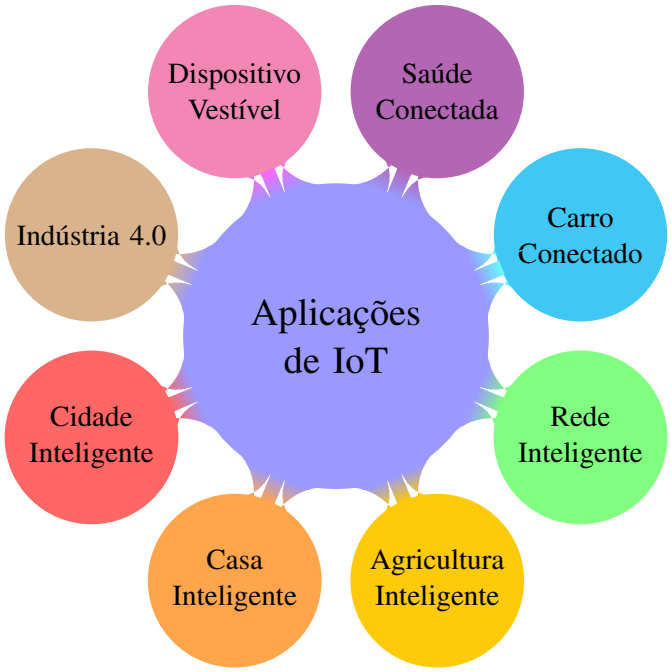
A Internet das Coisas (ou *Internet of Things* – IoT, do inglês) é caracterizada por vários dispositivos interconectados que trocam informações entre si [Dutta et al. 2019]. Esta consolidou-se como uma área de pesquisa robusta e abundante, a partir do avanço de suas aplicações em múltiplos domínios [Thakor et al. 2020], alguns dos quais foram apresentados na Figura 1.1.

Então, para exemplificar, na saúde conectada os sensores de IoT possibilitam um monitoramento contínuo de pacientes e a rápida reação perante anormalidades. Já na casa inteligente, diversos eletrodomésticos, como a iluminação inteligente, simplificam o cotidiano de seus detentores [Sembroiz et al. 2018].

Assim, por mais que o termo tenha sido cunhado em 1999, empresas como a Cisco assumem que o conceito de IoT começou a fazer sentido em 2009, quando a quantidade de

dispositivos conectados (10 bilhões) ultrapassou a população global. De certo modo, esta popularização se deve a melhorias aferidas em termos de eficiência, custo de produção e redução de tamanho de sensores [Sembroiz et al. 2018].

Figura 1.1. Domínios de Aplicação da IoT



Logo, estima-se que em 2024 existiam 18 bilhões de dispositivos conectados na infraestrutura de IoT e projeta-se que existirão 40 bilhões até 2030 [Krishnan et al. 2024]. Nesse sentido, um incremento crescente no número destes dispositivos impõe preocupações atinentes à segurança [Dutta et al. 2019], as quais podem ser expressas como segue:

- Confidencialidade: apenas usuários autorizados podem acessar a informação.
- Disponibilidade: quando necessário, o dispositivo deve conseguir acessar a informação requerida.
- Integridade: deve-se assegurar que os dados são precisos.
- Autenticação: os elementos da rede possuem níveis de acesso diferente. Este é um aspecto complexo de ser implementado em IoT.
- Heterogeneidade: como os elementos da rede se distinguem em complexidade e fabricante, necessita-se de uma rede heterogênea.

Isto posto, surge a motivação para o desenvolvimento de abordagens de Criptografia Leve (ou *Lightweight Cryptography* – LWC), objeto de pesquisa do presente artigo, ou seja, os esquemas criptográficos que dependem de uma complexidade computacional e consumo de memória reduzidos. Sendo assim, a LWC é adequada para sistemas restritos em memória e poder computacional, os quais seriam incapazes de processar em tempo hábil os algoritmos criptográficos convencionais [Aissaoui et al. 2023].

1.2. First Page

The first page must display the paper title, the name and address of the authors, the abstract in English and "resumo" in Portuguese (for papers written in Portuguese). The title must be justified at the left, in 20 point boldface font. Author names must be justified in the same way, as shown in this example.

1.3. CD-ROMs and Printed Proceedings

In some conferences, the papers are published on CD-ROM while only the abstract is published in the Proceedings. In this case, authors are invited to prepare two final versions of the paper. One, complete, to be published on the CD and the other, containing only the first page, with abstract and "resumo" (for papers in Portuguese).

1.4. Sections and Paragraphs

Section titles must be in boldface, 13pt, flush left. There should be an extra 12 pt of space before each title. The first paragraph of each section should not be indented; the first lines of subsequent paragraphs should be indented by 1.27 cm.

1.4.1. Subsections

The subsection titles must be in boldface, 12pt, flush left.

1.5. Figures and Captions

Figures and tables captions should be centered if less than one line (Figure **??**), otherwise justified and indented by 0.8cm on both margins, as shown in Figure **??**. The font must be Helvetica, 10 point, boldface, with 6 points of space before and after each caption.

In tables, do not use colored or shaded backgrounds, and avoid thick, doubled, or unnecessary framing lines. When reporting empirical data, do not use more decimal digits than warranted by their precision and reproducibility. Table caption must be placed before the table (see Table 1.1) and the font used must also be Helvetica, 10 point, boldface, with 6 points of space before and after each caption.

Figure and table references must be composed by the chapter number and a sequence number beginning in one (see the examples of Figure **??**, Figure **??** and Table 1.1).

1.6. Images

All images and illustrations should be in black-and-white, or gray tones. The image resolution on paper should be about 600 dpi for black-and-white images, and 150-200 dpi for grayscale images. Do not include images with excessive resolution, as they may take hours to print, without any visible difference in the result.

Referências

[Aissaoui et al. 2023] Aissaoui, R., Deneuville, J.-C., Guerber, C., and Pirovano, A. (2023). A survey on cryptographic methods to secure communications for UAV traffic management. *Vehicular Communications*, 44. Disponível em:

Tabela 1.1. Variables to be considered on the evaluation of interaction techniques.

Tarefa	Variável	Métrica utilizada
Seleção	Distância do alvo	Virtual cubits
	Direção horizontal e vertical do alvo	Graus do arco
	Distância do objeto oculto	Virtual cubits
	Direção da oclusão	Esquerda/direita/cima/baixo
Posicionamento	Distância inicial	Virtual cubits
	Direções iniciais horizontal e vertical	Graus do arco
	Distância final	Virtual cubits
	Direções finais horizontal e vertical	Graus do arco
	Precisão vertical	Porcentagem de sobreposição
	Precisão horizontal	Porcentagem de sobreposição
Orientação	Distância	Virtual cubits
	Direções horizontal e vertical	Graus do arco
	Orientação inicial (3 angulos)	Graus do arco
	Orientação final (3 angulos)	Graus do arco
	Exatidão/precisão	Graus do arco

https://doi.org/10.1016/j.vehcom.2023.100661. Acesso em: 25 jun. 2025.

[Dutta et al. 2019] Dutta, I. K., Ghosh, B., and Bayoumi, M. (2019). Lightweight Cryptography for Internet of Insecure Things: A Survey. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. Disponível em: https://doi.org/10.1109/CCWC.2019.8666557. Acesso em: 25 jun. 2025.

[Krishnan et al. 2024] Krishnan, A., Taparia, A., Paraskevopoulos, D., Pasqua, E., Brügge, F., Fernandez, J., Sava, J.-A., Baviskar, K., Lueth, K. L., Kulezak, M., Hasan, M., Demir, O., Wegner, P., Kadian, R., Nair, R., Sinha, S., Annaswamy, S., and Myroshnyk, Y. (2024). State of IoT Summer 2024. Technical report, IoT Analytics. Disponível em: https://iot-analytics.com/product/state-of-iot-summer-2024/. Acesso em: 25 jun. 2025.

[Sembroiz et al. 2018] Sembroiz, D., Ricciardi, S., and Careglio, D. (2018). *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*, chapter Chapter 10 - A Novel Cloud-Based IoT Architecture for Smart Building Automation. Elsevier. Disponível em: https://doi.org/10.1016/B978-0-12-811373-8.00010-0. Acesso em: 25 jun. 2025.

[Thakor et al. 2020] Thakor, V. A., Razzaque, M., and Khandaker, M. R. A. (2020). Lightweight Cryptography for IoT: A State-of-the-Art. *Cryptography and Security*. Disponível em: https://doi.org/10.48550/arXiv.2006.13813. Acesso em: 25 jun. 2025.