KRISTTOPHER KAYO COELHO

UM SISTEMA PARA GARANTIR A SEGURANÇA DE INFORMAÇÕES MÉDICAS EM REDES CORPORAIS

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação em Ciência da Computação, para obtenção do título de *Magister Scientiae*.

Orientador: José Augusto Miranda Nacif

Coorientadora: Michele Nogueira Lima

VIÇOSA - MINAS GERAIS
2020

Ficha catalográfica preparada pela Biblioteca Central da Universidade Federal de Viçosa - Câmpus Viçosa

T
C672s
2020

Coelho, Kristtopher Kayo, 1989-
Um sistema para garantir a segurança de informações médicas em redes corporais / Kristtopher Kayo Coelho. – Viçosa, MG, 2020.
50f : il. (algumas color.) ; 29 cm.

Inclui apêndice.
Orientador: José Augusto Miranda Nacif.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f.43-48.

1. Redes de área corporal (Eletrônica) - Medidas de segurança. 2. Algoritmos. 3. Criptografia . I. Universidade Federal de Viçosa. Departamento de Ciência da Computação. Programa de Pós-Graduação em Ciência da Computação. II. Título.

CDD 22 ed. 005.1

KRISTTOPHER KAYO COELHO

UM SISTEMA PARA GARANTIR A SEGURANÇA DE INFORMAÇÕES MÉDICAS EM REDES CORPORAIS

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação em Ciência da Computação, para obtenção do título de *Magister Scientiae*.

APROVADA: 20 de fevereiro de 2020.

Assentimento:

Kristtopher Kayo Coelho
Autor

José Augusto Miranda Nacif
Orientador

Dedico este trabalho a Deus e minha família, por serem essenciais em minha vida.

AGRADECIMENTOS

Parte da jornada é o fim. Esta etapa da minha vida não poderia ter chegado a este desfecho sem o precioso apoio de diversas pessoas. Em primeiro lugar, não posso deixar de agradecer aos meus orientadores, professores José Augusto Nacif e Michele Nogueira por toda a paciência, empenho, orientação e motivação no desenvolvimento de cada trabalho realizado durante o mestrado, bem como a colaboração do professor Alex Borges. Os demais agradecimentos serão generalizados, de modo a não cometer a deselegância de negligenciar nomes importantes. Desejo igualmente agradecer a todos os meus colegas de mestrado, laboratório e estudantes da UFV, cujo apoio e amizade estiveram presentes em todos os momentos. Agradeço aos funcionários da universidade que foram sempre prestativos a solucionar alguns obstáculos. Quero ainda agradecer a minha família (genuína e "adotiva") e pelo apoio incondicional que me dedicaram, especialmente aos meus pais e irmãos. Também presto um agradecimento especial aos meus amigos, que apesar das dificuldades e da distância não deixaram de estar presentes, incentivando e motivando. Por fim, gostaria de enfatizar que a opinião de pessoas que duvidaram desta conquista e criticaram minhas escolhas também tiveram papel importante como motivação. A Deus, toda a glória.

"O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001".

"Prefiro ser descrito como um lutador, alguém que jamais desistiu."
(Michael Schumacher)

RESUMO

COELHO, Kristtopher Kayo, M.Sc., Universidade Federal de Viçosa, fevereiro de 2020. **Um Sistema para Garantir a Segurança de Informações Médicas em Redes Corporais**. Orientador: José Augusto Miranda Nacif. Coorientadora: Michele Nogueira Lima.

As redes corporais fazem referência a um grupo de dispositivos eletrônicos vestíveis dispostos junto ao corpo humano para realizar o monitoramento em tempo real de sinais vitais, auxiliando em tratamentos e fornecendo diagnósticos precoces e acurados. Os dispositivos das redes corporais tendem a produzir um elevado volume de dados sigilosos, os quais são comumente transmitidos por tecnologias propensas a interferências, interceptações e ataques. Portanto, desenvolver soluções que atendam aos requisitos de segurança torna-se imprescindível. Entretanto, os dispositivos portáteis impõem restrições de consumo de recursos computacionais, tais como memória, processamento e energia. A criptografia dispõe de métodos para empregar a segurança desejada, impedindo que usuários indevidos acessem mensagens privadas. Este trabalho contribui com a literatura de duas formas: (i) através de uma avaliação prática do impacto de algoritmos criptográficos leves sobre consumo de energia e recursos em dispositivos vestíveis e (ii) com a proposta de um sistema para geração de chaves criptográficas secretas adequado às WBANs. Deste modo, inicialmente, apresenta-se a avaliação empírica e orientada por *hardware* a qual confirma a forte correlação entre a quantidade de operações lógicas/aritméticas, instruções *assembly* e o consumo de energia. Mesmo com os algoritmos criptográficos rápidos, seguros e eficientes ainda existe o compromisso de que uma única chave secreta seja compartilhada a priori entre as entidades comunicantes. Isso demanda que um esquema de acordo de chaves leve e robusto seja implementado. Baseado nos resultados alcançados da avaliação, este trabalho apresenta um sistema seguro para geração e acordo de chaves secretas, baseado em sinais fisiológicos. O sistema tem a proposta de ser leve, eficiente e otimizado, aplicando conceitos de computação aproximada de modo a prover uma redução significativa no consumo energético e de memória. O material criptográfico é obtido através da transformação e quantização de sinais do eletrocardiograma em chaves secretas. Os resultados indicam que este projeto proporciona uma redução do consumo de memória de até 76% em relação a duas técnicas do estado da arte.

Palavras-chave: WBAN. Algoritmos criptográficos. Acordo de chaves.

ABSTRACT

COELHO, Kristtopher Kayo, M.Sc., Universidade Federal de Viçosa, February, 2020. **A Security System to Ensure the Privacy Medical Information on Wireless Body Area Networks**. Advisor: José Augusto Miranda Nacif. Co-advisor: Michele Nogueira Lima.

Wireless Body Area Network refers to a set of wearable electronic devices on the human body to carry out real-time monitoring of vital signs, aiding in treatments and providing early and accurate diagnoses. Devices in Wireless Body Area Networks sense a high amount of sensitive data which is usually transmitted by technologies susceptible to interference, interception and invasion. Therefore, developing solutions to accomplish security requirements is indispensable. However, wearable devices impose restrictions on the consumption of computational resources, such as memory, processing and energy. Encryption offers methods to employ the desired security, preventing unauthorized users from accessing private messages. This work contributes in two ways: (i) with the practical evaluation of light cryptographic algorithms on energy and resource consumption to wearable devices and (ii) with the proposal of a system for cryptographic keys agreement classified by WBANs. Thus, an empirical and hardware-oriented evaluation is presented, which confirms the hard correlation between the number of logical/arithmetic operations, assembly instructions and energy consumption. Even with fast, safe and computationally efficient cryptographic algorithms, there is still a requirement that a single secret key is priority shared between communicating entities. This requires a light and robust key arrangement scheme to be implemented. Based on the results of the evaluation, this work presents a system for generating and establishing secret keys, based on physiological signals. The system is light, efficient and optimized, applying approximate computing concepts to provide a significant reduction in energy and memory consumption. The cryptographic material is obtained by transforming and quantizing ECG signals on secret keys. The results indicate that this project is capable of providing a reduction in absolute memory consumption of up to 76% compared to the state of the art. The commitment to safety during the transmission of the keys occurs by using an alternative communication channel (the human body). Thus, these keys, which are usually the target of attacks, are exchanged through a signal completely confined within the individual.

Keywords: WBAN. Cryptography algorithms. Key agreement.

LISTA DE FIGURAS

1.1 Arquitetura das redes corporais. 12
1.2 Gastos com dispositivos vestíveis dobrarão de 2018 à 2021 [1]. 13

2.1 Power consumption measurement. 24
2.2 Wearable device power state machine (PSM). 25
2.3 Power consumption in milliwatts on the *run* state. 26

3.1 Arquitetura do sistema proposto. 30
3.2 Geração de características a partir do sinal de eletrocardiograma [2]. . . 32
3.3 Geração de chaves proposta. 35
3.4 Interfaces de comunicação. 36
3.5 Protocolos nas interfaces. 37
3.6 Cenário de transmissão de dados. 38

A.1 Data transmission scenario. 50

LISTA DE TABELAS

2.1 Computational complexity vs. memory consumption. 26
2.2 Logic/arithmetic operations vs. assembly instructions. 27
2.3 Battery life expectancy. 27

3.1 Comparação entre protocolos. 33
3.2 Avaliação do consumo de memória. 39

A.1 Signal propagation distances. 50

SUMÁRIO

1 Introdução **11**
- 1.1 Problema . . . 14
- 1.2 Objetivo . . . 15
- 1.3 Contribuições . . . 15
- 1.4 Estrutura da dissertação . . . 17

2 Cryptography Algorithms in Wearable Communication: An Empirical Analysis **19**
- 2.1 Introduction . . . 19
- 2.2 Lightweight Cryptography Algorithms for Wearable Networks . . . 21
- 2.3 Experiments and Methodology . . . 23
- 2.4 Results . . . 24
- 2.5 Conclusion . . . 27

3 Um Sistema Leve e Seguro para Acordo de Chaves Utilizando Comunicação Corporal **28**
- 3.1 Introdução . . . 28
- 3.2 Trabalhos Relacionados . . . 31
- 3.3 Sistema Proposto . . . 33
  - 3.3.1 Geração de Chaves . . . 34
  - 3.3.2 Acordo de Chaves . . . 35
  - 3.3.3 Acoplamento Galvânico . . . 36
- 3.4 Resultados . . . 38
- 3.5 Conclusão . . . 40

4 Conclusão **41**

Referências Bibliográficas **43**

Apêndice A Evaluating the Skin as a Secure Communication Medium **49**
- A.1 Introduction . . . 49
- A.2 Methodology . . . 49
- A.3 Preliminary Results . . . 50
- A.4 Conclusion . . . 50

Capítulo 1

Introdução

A evolução tecnológica dos dispositivos vestíveis para sensoriamento remoto se desenvolveu rapidamente nos últimos anos. Uma de suas áreas inovadoras e promissoras é a de rede de sensores corporais ou *Wireless Body Area Network* (WBAN). Essas redes são definidas por um conjunto de dispositivos eletrônicos que se reúnem para construir um sistema de monitoramento contínuo e proativo de sinais vitais dos pacientes através dos sensores dispostos em seu corpo [3]. Entre as motivações responsáveis por esta expansão da área, destacamos os gastos relacionados à saúde e ao envelhecimento populacional. Estes gastos representam desafios aos países desenvolvidos e em desenvolvimento acelerando a demanda por novos tratamentos médicos com base tecnológica [4]. Alguns fatores diretamente associados ao estilo de vida contemporâneo podem ocasionar o surgimento de diversas doenças, tais como o sedentarismo e a má alimentação, além do consumo excessivo de bebidas alcoólicas e cigarros. Consequentemente, o número de profissionais da área de saúde passou a ser insuficiente ao atendimento da população [5]. As WBANs surgem como uma solução oferecendo um alto grau de mobilidade, cujo principal benefício é tornar o cuidado da saúde disponível em qualquer momento e em qualquer lugar [6, 7].

A Figura 1.1 ilustra a arquitetura de três níveis das redes corporais. O primeiro nível compreende os diversos dispositivos computacionais que podem ser dispostos, estrategicamente, dentro ou em torno do corpo humano. O segundo é referente à unidade central de processamento ou nó coordenador (assistente pessoal ou *smartphone*), responsável por processar os dados provenientes dos sensores e realizar a comunicação com a terceira camada. Os servidores e as máquinas dos médicos e serviços de emergência são responsáveis pelo acompanhamento e cuidados com os usuários. O objetivo deste sistema é monitorar remota e continuamente os sinais vitais, como, por exemplo, a pressão arterial, o eletroencefalografia, a eletrocardiografia (ECG), a frequência cardíaca, o nível de glicose no sangue, a temperatura e o posicionamento corporal e a saturação de oxigênio no sangue. Essas informações são enviadas por dispositivos sem fio para provedores ou monitores de saúde. A partir deste monitoramento é possível antecipar o diagnóstico e, consequentemente, o início do tratamento. Os dispositivos são capazes de identificar os riscos à saúde do usuário fornecendo um

diagnóstico precoce, proporcionando uma redução de custos com tratamento e uma perspectiva maior de cura. A acurácia do diagnóstico tende a ser elevada, uma vez que os dispositivos se encontram diretamente conectados ao corpo, possibilitando aferições precisas e com o mínimo de interferências, e oferecendo aos profissionais de saúde a apresentação de diagnósticos corretos e em tempo real.

Figura 1.1: Arquitetura das redes corporais.

Os dispositivos vestíveis tornaram-se uma das tecnologias mais populares nos últimos anos. A Figura 1.2 ilustra os dados sobre relatórios de pesquisa de mercado, onde estima-se que este mercado alcance US$ 52 bilhões em 2020, um aumento de 27% em relação a 2019 e praticamente o dobro em relação a 2018 (de acordo com a última previsão do Gartner, Inc. em 2019) [1]. Usuários comuns têm direcionado seus interesses principalmente para relógios e roupas inteligentes os quais tendem a assumir a liderança do mercado em 2020. Os principais fatores que impulsionam os gastos com estes dispositivos incluem a maior precisão dos sensores, miniaturização e uma melhor proteção de dados do usuário [8]. Comumente, os dados produzidos por estes dispositivos são transmitidos por meio de tecnologias de comunicação sem fio. Estas tecnologias normalmente utilizam radiofrequências [9, 10], como *RF-Narrowband* (RF-NB), *bluetooth*, *Millimeter Wave* (mmWave) ou *5G mobile networks*. O ambiente em questão apresenta condições de vulnerabilidade, o que torna a comunicação propensa a congestionamento, interferências e ataques, uma vez que seu sinal é propagado pelo ar [3]. Portanto, especialistas sugerem que a privacidade do usuário final continuará a ser um forte fator de influência para o crescimento contínuo do mercado, especialmente para casos de uso em monitoramento de saúde, onde órgãos como HIPAA (EUA) e GDPR (Europa) regulamentam regras de privacidade. No Brasil esta regulamentação é proveniente do decreto que institui o Plano Nacional de Internet das

Coisas aliado ao Marco Civil da Internet [11, 12].

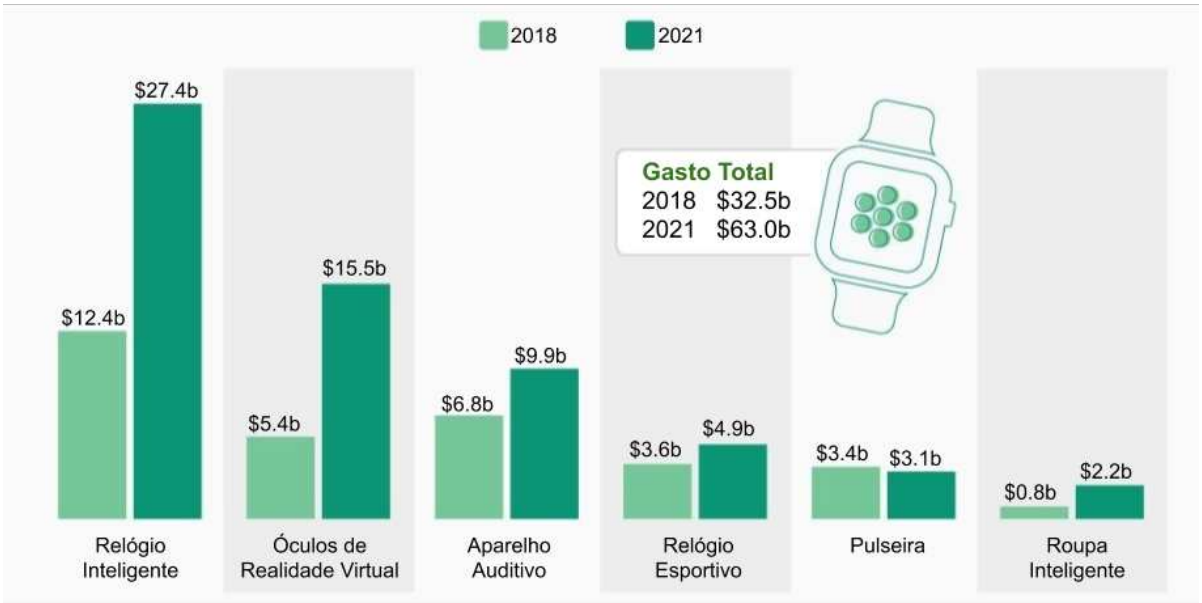


Figura 1.2: Gastos com dispositivos vestíveis dobrarão de 2018 à 2021 [1].

A segurança e a integridade de dados são uma questão fundamental em WBANs, as ameaças pelas quais estas redes de sensores corporais são expostas podem ser classificadas como ataques externos e internos. Em um ataque externo, proveniente do ataque de um dispositivo intruso, técnicas de criptografia são usadas como medidas para impedir que um invasor obtenha acesso especial aos dados da rede de sensores. Neste caso, o invasor pode realizar ataques, como espionagem passiva, onde o atacante escuta a rede com a intenção de descobrir chaves secretas criptográficas. Os ataques de negação de serviço consistem na sobrecarrega da rede com mensagens enviadas por um adversário para que os serviços da vítima sejam interrompidos. Em um ataque de repetição, um nó malicioso captura mensagens legítimas trocadas entre os dispositivos, replicando-as para alterar o comportamento da rede. Em um ataque interno, o atacante possui acesso físico ao *hardware* e, consequentemente, sua memória, a qual armazena os dados brutos. Este cenário é considerado o mais crítico, porém ocorre com menor frequência, uma vez que o invasor necessita de acesso direto ao usuário com os sensores. Deste modo, o atacante possui acesso total e não oficial direto aos dados de saúde, os quais podem ser coletados, editados, corrompidos e falsificados. Além da manipulação de dados, é possível realizar a obstrução a rede, descartando pacotes legítimos que passam pelo nó comprometido, levando a diagnósticos e tratamentos incorretos [13].

Com a popularização dos dispositivos vestíveis e suas aplicações na área de saúde, as necessidades de segurança são mais evidentes do que nunca nos dias atuais. As redes WBANs surgiram como uma padronização de dispositivos e protocolos destinados ao abastecimento de dados à assistência médica onipresente. No entanto, as

restrições de energia, memória e potência de processamento dos dispositivos impõem novos requisitos, restringindo o uso de soluções tradicionais de segurança utilizadas nas redes sensores comuns. Assim, existe uma necessidade em desenvolver soluções criptográficas, juntamente com métodos de acordo chave para mitigar ataques externos. As pesquisas existentes discutem os problemas de segurança e privacidade de uma forma geral, sem concentrar seus esforços nos problemas relativos à geração e ao estabelecimento de chaves, específicos para redes corporais [14].

1.1 Problema

Atualmente, muitas pesquisas estão sendo realizadas sobre os problemas enfrentados pelos dispositivos vestíveis, dada a demanda de desenvolvimento de soluções que atendam aos seus requisitos específicos. Devido à popularidade e à confiança de usuários em dispositivos portáteis, existe um grande volume de tráfego contendo dados com alta sensibilidade, o que pode proporcionar o surgimento de novas formas de ataques. A segurança dos dados é algo essencial para qualquer sistema, porém, quando falamos de dados clínicos, essa segurança precisa ser redobrada.

Geralmente, os algoritmos criptográficos de chave simétrica são rápidos, seguros e eficientes computacionalmente. Entretanto, apresentam algumas desvantagens, como a exigência de que uma chave secreta seja compartilhada entre as entidades comunicantes. Isto exige a distribuição de uma cópia da chave entre os nós da rede de forma segura. Os materiais criptográficos distribuídos pelo meio sem fio estão sujeitos à descoberta por meio da espionagem dos usuários mal intencionados, os quais utilizam de técnicas como ataques de canal lateral ou *sniffers*. Outro método de distribuição é o pré-carregamento, que é oneroso e dependente de conhecimento prévio da topologia da rede, uma vez que é realizado de forma manual. Visto isso as chaves a serem compartilhadas devem ser longas, aleatórias e com variação no tempo, além de existir a recomendação que sejam altamente dependente do usuário, elas ainda devem ser mantidas em segurança durante os processos de distribuição e utilização [15]. O processo da geração, distribuição e armazenamento de chaves é conhecido como gerenciamento ou acordo de chaves.

Ademais, toda a construção das técnicas criptográficas para dispositivos com limitações de recursos computacionais devem passar por uma severa e abrangente análise acerca do consumo de recursos, principalmente objetivando eficiência energética. O consumo demasiado de energia reduz a vida útil da bateria, exigindo uma substituição precoce, que para alguns tipo de sensores podem ser impraticáveis. Outros objetivos os quais devem ser explorados durante o desenvolvimento de soluções para garantir a segurança dos dados é a redução do consumo de memória e tempo de processamento [16].

1.2 Objetivo

Quando se trata de dados sigilosos, o objetivo principal é garantir sua privacidade, protegê-los e assegurar sua integridade. Isto é possível utilizando métodos criptográficos. A criptografia é o estudo de princípios e técnicas para comunicação segura em um meio propenso à interceptação e alteração de dados [17]. A criptografia também refere-se à construção e à análise de protocolos que impeçam usuários indevidos de acessarem mensagens privadas. Infelizmente, a criptografia não oferece essa segurança gratuitamente ou magicamente, para proteger a identidade e a privacidade do usuário, estes métodos necessitam massivamente de recursos de *hardware* como memória e processamento, implicando diretamente em um consumo maior de energia.

Portanto, o objetivo é desenvolver uma solução completa, leve, robusta e eficiente para o problema de gerenciamento de chaves para algoritmos de criptografia simétrica. O sistema de troca de material criptográfico baseia-se em valores fisiológicos utilizando o sinais ECG como fonte para gerar chaves criptográficas. O esquema de acordo de chave apresentado proporciona uma redução do consumo de memória, uma vez que aplica conceitos de computação aproximada para reduzir o custo de armazenamento dos valores utilizados para realizar o cálculo das chaves. O compromisso com a segurança durante a troca das chaves ocorre por meio da utilização de um canal seguro, o próprio corpo humano. A comunicação galvânica, além de prover segurança ao mecanismo de troca de chaves contribui diretamente com o compromisso da redução de consumo de memória, uma vez que elimina todo o *overhead* de segurança dos métodos tradicionais.

Entretanto para alcançar este compromisso, antes fez-se necessário um estudo detalhado sobre as técnicas criptográficas direcionadas a dispositivos vestíveis com recursos limitados. A maioria dos estudos existentes investigam os requisitos pela perspectiva de *software* [18, 19] ou por simulações e modelos analíticos [20, 21]. Apesar da reconhecida importância destes estudos, uma análise empírica é uma maneira de complementá-los, oferecendo *insights* e conhecimentos que podem auxiliar no desenvolvimento de novos projetos para soluções criptográficas mais eficientes e econômicas [22]. A análise apresentada nesta dissertação destaca os impactos da especificidade dos algoritmos criptográficos em dispositivos vestíveis concentrando principalmente no estudo do consumo de energia sobre as técnicas de cifras que utilizam chaves simétricas.

1.3 Contribuições

É crescente a necessidade de prover segurança às informações compartilhadas nos mais diversos tipos de redes. No entanto, as redes amplamente dependentes de dispo-

sitivos com recursos limitados, como as WBANs, apresentam um desafio importante, a reduzida disponibilidade de memória, capacidade de processamento e, principalmente, energia dos mesmos dificulta a utilização de alguns dos principais algoritmos criptográficos considerados seguros atualmente.

As principais contribuições deste trabalho correspondem ao desenvolvimento e apresentação de:

- Uma avaliação empírica orientada por *hardware* dos algoritmos de criptografia mais representativos em relação aos requisitos das redes corporais.
- Um sistema completo, leve e seguro para acordo de chaves utilizando comunicação corporal, avaliado sobre a perspectiva de dispositivos reais.

A análise apresentada neste trabalho é fundamentada sobre apresentar um sistema seguro para transmissão de dados o qual faz uso de técnicas de criptografia simétrica. Nesta arquitetura, os dispositivos comunicantes conhecem *a priori* ou predispõe de um canal seguro para estabelecer uma chave secreta, única e comum empregada na cifra das mensagens durante um intervalo de comunicação. Particularmente, as investigações são direcionadas sobre duas classes diferentes de algoritmos de criptografia leve de chave simétrica, denominadas cifras de bloco [23] e cifra de fluxo [24]. Neste estudo, a literatura referente aos algoritmos de criptografia destinados a dispositivos vestíveis [19, 20, 25] é cuidadosamente analisada. A escolha dos algoritmos se deu com base nas restrições de processamento e memória impostas pelos *hardwares*. Ainda foram consideradas as limitações de energia, característica principal de dispositivos implantáveis e miniaturizados. Estes métodos de criptografia fornecem um nível de segurança elevado mesmo lidando com os limites relacionados à falta de recursos e complexidade computacional dos dispositivos. Portanto, são considerados algoritmos “leves”.

As informações obtidas através da análise supracitada nos permitem desenvolver métodos de gerenciamento de chaves que obedeçam rigorosamente os requisitos referentes ao baixo consumo de recursos computacionais [26]. Portanto, as estratégias para a geração e o acordo chaves devem ser desenvolvidas cuidadosamente, atentando para os princípios de leveza, eficiência energética e ocupação de memória. Além disso, é desejável que o sistema seja automático e de tempo real, ou seja, com o mínimo envolvimento do usuário ou de terceiros. Os esquemas projetados para redes de sensores sem fio de um modo geral não possuem compromisso com os requisitos inerentes das redes WBANs. Portanto, o desenvolvimento de uma solução completa e leve para o problema de gerenciamento de chaves para algoritmos de criptografia simétrica é uma contribuição para o avanço do estado da arte [14].

Pesquisas no campo de estudo de gerenciamento de chaves apontam para soluções que fazem uso de sinais fisiológicos para obter características como aleatorie-

dade, variação temporal e dependência do usuário [14]. Entretanto, mesmo com uma proposta "leve", as soluções são desenvolvidas e avaliadas em simulações, o que impossibilita a avaliação do real custo computacional sobreposto ao *hardware*. Portanto, com o intuito de auxiliar a construção de um sistema de segurança completo e leve para garantir a segurança de informações médicas em redes corporais, esta dissertação apresenta uma metodologia robusta e eficiente para geração e estabelecimento de chaves secretas baseada em sinais de eletrocardiograma. Assim, os materiais criptográficos, que são comumente alvo de ataques, são trocadas por meio de um sinal completamente confinado dentro do próprio indivíduo. Os resultados indicam que este projeto proporcione uma redução do consumo de memória absoluta de até 76% em relação ao estado da arte, mantendo ainda o compromisso com a segurança, ratificado pela transmissão de de dados intra-corpo. O esquema proposto é capaz de isentar o tempo de pré-configuração ou carregamento manual de chaves, atendendo à expectativa de estabelecimento de chaves *plug and play*.

1.4 Estrutura da dissertação

Este dissertação está estruturada em conformidade com o formato de coletânea de artigos científicos normalizado pelo Conselho Técnico de Pós-Graduação da Universidade Federal de Viçosa [27]. Este formato é composto pelas partes básicas: introdução geral (Capítulo 1), artigos científicos (Capítulos 2, 3), conclusões gerais (Capítulo 4) e Apêndice A. Dentre os artigos, o primeiro foi publicado em um periódico científico (*IEEE Communications Letters*) e o segundo será submetido à avaliação para publicação em uma revista científica. O apêndice faz referência ao resumo apresentado no *workshop* da *ESWEEK Medical CPS*, que reúne pesquisadores com interesse em sistemas ciber-físicos (CPS).

A dissertação está organizada da seguinte forma: No Capítulo 2 é apresentado o artigo *Cryptography Algorithms in Wearable Communication: An Empirical Analysis*, o qual expõe uma avaliação empírica orientada por *hardware* dos algoritmos de criptografia simétrica mais representativos, mensurando o impacto sobre consumo de energia e recursos de *hardware* para dispositivos vestíveis com recursos computacionais limitados. O Capítulo 3 discorre sobre o artigo: Um Sistema Leve e Seguro para Acordo de Chaves Utilizando Comunicação Corporal, onde é proposto um sistema completo de estabelecimento de chaves secretas para algoritmos de criptografia simétrica utilizando o próprio corpo humano como canal de comunicação seguro por meio de acoplamento galvânico. No Capítulo 4, são apresentadas as conclusões gerais, discutindo os resultados obtidos e os avanços alcançados. Ainda nesse capítulo, as oportunidades de pesquisa em aberto são apresentadas. O Apêndice A inclui a investigação sobre a viabilidade de usar a pele como um meio de comunicação seguro

entre dispositivos vestíveis em curta distância.

Ainda durante o período de mestrado, além dos trabalhos acima listados, também foram produzidos outras publicações em colaboração com professores e alunos de graduação e mestrado. Entre estas obras pode-se listar ***ADD: Accelerator Design and Deploy - A tool for FPGA high-performance dataflow computing*** [28], o qual apresenta uma ferramenta de alto nível para especificar, simular e implementar aceleradores de fluxo de dados para aplicativos de *streaming* mapeáveis em circuitos FPGA. O trabalho **Gerador Parametrizável de Aceleradores para K-means em FPGA e GPU** [29] apresenta um gerador de código de domínio específico para o K-means capaz de gerar código para GPUs e FPGAs. O trabalho **Minimum Switching Networks** [30] consiste em apresentar um novo esquema para projetar Redes de Interconexão Multiestágio (MINs), com um número reduzido de comutadores, mantendo a roteabilidade das redes. O trabalho **Ensino de Arquitetura e as Predições Tomadas por Desempenho com as Predições não Tomadas pela Segurança: Vulnerabilidades *Meltdown* e *Spectre*** [31] tem como objetivo apresentar uma abordagem para motivar o ensino de arquitetura de computadores de modo a compreender melhor as vulnerabilidades *Meltdown* e *Spectre*.

Capítulo 2

Cryptography Algorithms in Wearable Communication: An Empirical Analysis

In this letter, we assess the practical impact of lightweight block and stream cipher algorithms on power consumption and hardware resources for wearable devices that own low computational resources. Differently from the literature, we present an empirical and hardware-driven evaluation of the most representative encryption algorithms with regard to the requirements of wearable networks. We design and implement a cryptography library useful for wearable devices. Results confirm a strong correlation between the amount of logic/arithmetic operations, assembly instructions and power consumption for the two evaluated platforms, and they highlight the need to design encryption algorithms for wearable devices with high energy consumption efficiency, but strong security level similar to AES.

2.1 Introduction

Market forecasts that worldwide shipments of wearable computing devices will reach 929 million in 2021, presenting as major drivers fitness and healthcare gadgets [32]. Wearable computing devices are smart electronic devices (electronic device with microcontrollers) that can be incorporated into clothing, worn on the body, or implanted in the body, such as fitness trackers, smartwatches, and the "neural dust" implantable sensor. They have rapidly become popular due to advancements in micro and nano-electronics. Wireless communication is essential for these advancements, once it allows the connection between devices in and around the human body, including low-rate devices like pedometers and high-rate devices like augmented-reality glasses. This communication relies on different standards such as those from the IEEE 802.15 family [33] or the next generation mmWave 5G cellular.

Given data sensitiveness in this context, popularity and user-reliance on wearable devices, there has been an emergence of new and varied attack vectors targeting privacy intrusions, that so far cannot be addressed by classical techniques developed for the Internet applications. In this letter, our goal lies in empirically evaluating

the practical impact of the most representative lightweight cryptography algorithms with regard to the requirements of wearable networks, such as high security and low computational resources, considering energy constraints from implantable and non-implantable devices.

Most existing studies have investigated wearable network requirements either from a software perspective [18, 19] or by simulations and analytical models [20, 21]. Despite the importance of those studies, an empirical study complements them offering insights and knowledge closer to the real implementation of those cryptography algorithms, assisting then in the design of more efficient and cost-effective solutions. To the best of our knowledge, ours is the first to follow a hardware-driven and empirical evaluation, highlighting the impacts of the hardware specificity to cryptography algorithms in wearable devices.

Our analysis targets symmetric cryptography, where the communicating wearable devices share (possibly through a pairing or authentication, and key establishment protocol) the session key used to encrypt the messages. Particularly, we focus our investigations on two different classes of symmetric lightweight encryption algorithms, as block ciphers (XTEA, XXTEA, SKIPJACK, RC2, and AES) [23], stream cipher (RC4). For our evaluation approach, we have designed and implemented a cryptography library useful for wireless wearable devices[1]. For power consumption measurements, we have designed an instrumentation circuit and integrated it in the evaluated platforms. The power consumption evaluation has followed a methodology adapted from Bessa *et al.* [34], that allow us to assess the power dissipation from wearable devices while they are in idle and running states. Our analysis has focused on real-life, off-the-shelf wearable platforms which consider the transmission of data and other with greater processing power abstracting communication.

Our results confirm the strong correlation between the amount of logic/arithmetic operations required to encrypt data block or stream, and their respective power consumption [35]. Results indicate that SKIPJACK algorithm can be up to 18.76% more efficient among the evaluated algorithms in terms of power consumption, processing up to 32x fewer instructions. It also consumes up to $\approx$ 3.5x less ROM memory related to AES. Analyzing time vs. power consumption, the XTEA algorithm has a battery consumption almost 6x lower than AES. However, it is worth to highlight the high security level of AES, bringing us to the conclusion that it is necessary efforts to design encryption algorithms for wearable devices with high computational efficiency (i.e., memory usage, energy consumption) and high security level.

This letter presents the lightweight cryptography algorithms for wearable devices (Section 2.2); the designed experiments and methodology (Section 2.3); the discussion of the obtained results (Section 2.4); and conclusions (Section 2.5).

[1] https://github.com/UFV-Alumni/lib_crypto

2.2 Lightweight Cryptography Algorithms for Wearable Networks

A cryptosystem consists of a plaintext space $\mathcal{P}$, a ciphertext space $\mathcal{C}$, and a key space $\mathcal{K}$, an encryption algorithm $Enc : \mathcal{K}$ x $\mathcal{P} \rightarrow \mathcal{C}$, and a decryption algorithm $Dec : \mathcal{K}$ x $\mathcal{C} \rightarrow \mathcal{P}$. For each $k \in \mathcal{K}$ and $p \in \mathcal{P}$, it is $Dec(Enc(p)_k)_k = p$. In the communication model introduced by Shannon [36], a cryptosystem provides confidentiality to the information from an attacker. Hence, a sender and a receiver communicate by a public channel, where they exchange ciphertexts.

Symmetric key cryptography assumes a secure channel used by the communicating parties to establish a secret session key k, not accessible to the adversary. Given p, k, and the cryptosystem, the sender can construct the ciphertext c and send it to the receiver. The receiver can reconstruct the plaintext p, given c, k, and the cryptosystem. Symmetric key cryptography is relevant for wearable networks, that devices and communication have severe resource constraints (e.g., energy, memory, and processing capacity), and applications demand for low response time. The attacker's main goal lies in recovering p or k and, according to Kerckhoff's principle, an attacker knows the specification of the cryptosystem and has access to the ciphertext c.

While in the last decades the progress in the security cryptographic primitives was based in modeling [37], this work focuses on power consumption analysis of established block and stream ciphers. A block cipher is a cryptosystem with $gf(p^n)$, where gf denotes the Galois field in order $n \in \mathcal{Z}+$ and plaintext $p \in \mathcal{P}$. For each key k, the encryption function $Enc(p)_k$ is a permutation. In the most general case, the $\mathcal{K}$ corresponds to the set of permutations of size $2^n!$, where a single k lies in a table of size 2^n. The use of a subset of permutations is reasonable by generating a small key. To encrypt messages longer than the block size, we use a mode of operation, such as Cipher Block Chaining or Counter Mode, and integrity protection, such as Galois Counter Mode [37].

A stream cipher encrypts binary digits of a plaintext one at time. It follows an internal state $x \in \mathcal{X}$, an update function $L : \mathcal{X} \rightarrow \mathcal{X}$, and an output function $f : \mathcal{X} \rightarrow \mathcal{Z}$, where $\mathcal{Z}$ is called the keystream alphabet. An output $z \in \mathcal{Z}$ is produced at time t, according to $zt = f(xt)$, where $xt = Lt(x)$ and x is the initial state. The stream of outputs $z_0, z_1, \ldots$ is called the keystream. Each output symbol is combined to the corresponding plaintext symbol to produce a ciphertext symbol.

In this study, we have analyzed recent literature on wearable cryptography algorithms [20, 19, 25]. We have chosen these algorithms based on power and processing restrictions imposed by wearable devices, considering the energy limitations of implantable and non-implantable devices. XTEA, XXTEA, SKIPJACK, RC2, and AES

are block ciphers; whereas RC4 is a stream cipher. These encryption algorithms provide a security level that can handle thresholds related to low-resource, minimal area, low-memory, and low-power, being well-known as "light" algorithms. In addition to the six lightweight algorithms, briefly described in the next paragraphs, we have initially considered others, e.g., KSEED, TWOFISH, and CAST5. But, they have shown to be impractical for the current wearable device architecture due to the excessive memory use, reported from MSP430 GCC.

The eXtension to TEA (XTEA) and the Corrected Block TEA (XXTEA) encryption algorithms employ a 128-bit key and blocks of 64-bits. XTEA operates in 64 rounds and XXTEA has a variable number of rounds. In both, permutations follow simple operations, *e.g.*, addition, shifting and XOR. For key recovery, the best attack reported on XTEA was a related-key differential attack on 26 out of 64 rounds. The cryptanalysis of XXTEA describes a successful chosen plaintext attack with 2^{59} plain-ciphertext pairs [19].

The SKIPJACK algorithm is a 32-round cipher which applies two distinct rules labeled as A and B. These rules are applied interleaved as A, B, A, B per 8 rounds. Permutations comprise of shifts and Feistel's, which use 32 of the 64 bits from the secret key per permutation. Despite the controversy around SKIPJACK design, cryptanalysis point out a resistance for attacks of 2^{48}, using at least 2^{34} plaintexts [38]. As SKIPJACK, RC2 works on 64-bit blocks and allows a variable key size. It follows the key expansion and encryption steps. Key expansion can extend any key size, in the range of 1 to 128 bytes, up to a 128-byte key. Encryption performs permutations based on a substitution table. Estimates to retrieve a secret key are proportional to the effort for analyzing about 2^{4r} (for $r = 16$) chosen plaintexts [39].

The Advanced Encryption Standard (AES) algorithm has become the primary choice for various security services due to its strong defense against known attacks. The best known attacks against AES are slightly faster than brute-force and require $2^{126.2}$ operations to recover an AES-128 key. In [40], the authors presented an optimized version of AES for devices with low computational capacity and memory resources, while still providing low power consumption.

RC4 is a stream cipher and it comprises of a Key Scheduling Algorithm (KSA) and a Pseudo-Random Generation Algorithm (PRGA). KSA transforms a random key in an initial permutation, whereas PRGA uses this initial permutation to generate a pseudo-random output sequence. Cryptographic transformations applied by the algorithm are linear and simple, using permutations and sums of integer values. However, secure use of RC4 is non-trivial as experienced with Wi-Fi WEP. However, the recovery requires a complex process of about 2^{13} algorithm operations for 256-bit key [24].

2.3 Experiments and Methodology

In this work, the experiments rely on two platforms: (i) wearable devices from the Shimmer platform, model 2R and (ii) a Teensy™ 3.2 microcontroller. The Shimmer devices are equipped with a MSP430 F1611 microcontroller, 16-bit RISC architecture. Each wearable device contains 48KB flash memory and 10KB RAM. These devices sense vital signs and movements from users by accelerometers, magnetometers, and gyroscope, and transmit them to a coordinator device (*e.g.*, a smartphone) through wireless communication. These low-power wireless devices run TinyOS, a Real-Time Operating System (RTOS). The Teensy platform is equipped with an ARM® Cortex®-M4 of 72 MHz CPU and 32-bit architecture. This device also contains a 256KB flash memory and 64KB RAM memory. For Teensy, the algorithms were implemented in C language and deployed using the Arduino interface.

We measure power consumption in different states (*i.e.*, idle, and run). At a glance, we set up the devices to the desired state and continuously monitor it. The devices are automatically placed in a low-power mode when the task queue is empty (*idle* state). Hence, we are able to measure the device power consumption in this state. Finally, to analyze the wearable on the run state, we set up the device to continuously perform a cryptography task — on 64-bits data blocks — using one of the aforementioned cryptography algorithms on both platforms, *run* state). In the Shimmer platform, *run* state, we consider the cost of encrypted data transmission. Finally, unless we tell otherwise, at each state we perform 2,000 samples and present mean confidence interval of 95%.

We have designed and assembled a circuit for power consumption measurement adapted from [34]. The circuit comprises of a low-cost data acquisition board (DAQ - ADALM1000) connected to a wearable, a 0.10 Ω resistor, and a computer (Figure 2.1). We use Active Learning Interface for Circuits and Electronics (ALICE) software to acquire voltage measurements from both terminals of the resistor which are connected to channels CH_A and CH_B of the DAQ. The voltage can be easily transformed to current following the law of Ohm, $V = R$ x I, since the resistance value is known. To make comparisons, we calculate the power consumption by multiplying the current to the voltage. Then, power consumption follows: $P = ((\text{CH\_A} - \text{CH\_B})/0.10) * V$ mW.

DAQ delivers a maximum sampling rate of 100 ksps (kilosamples per second). Therefore, we calculate power consumption, mean, and the total consumption time for the algorithms in each analyzed state of wearable devices. Also, the computational complexity of the algorithms is of great relevance because power consumption bottlenecks occur during data processing and transmission. Hence, we also consider the size of machine code, when it represents a large share of the hardware resource

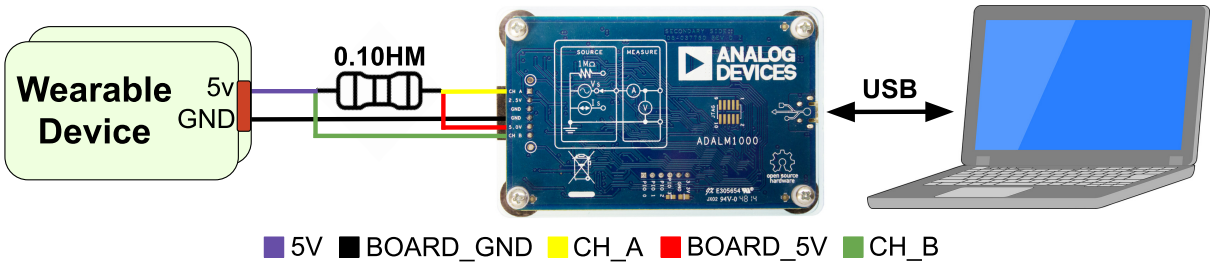


Figura 2.1: Power consumption measurement.

consumption.

We also count the number of Assembly instructions using the Godbolt online compiler and a manual process known as Table Test. The Godbolt compiler converts programs from several languages into Assembly code. For the experiment, we use the MSP430 GCC compiler version 5.3.0 for Shimmer platform and AVR GCC version 4.6.4 for Teensy platform, both without optimization directives. Then, we convert the code to Assembly code. Next, using the Table Test, we have counted the final number of Assembly instructions.

Similarly, we also analyze the main operations in each cryptography algorithm. The considered operations are *shift left*, *shift right*, *and*, *or*, *not*, *xor*, *sum*, *subtraction*, and *multiplication*. We enumerate all these logical and arithmetic operations when we want to confirm if the number of operations can be directly correlated with the final performance and power consumption of each algorithm implementation [35]. Furthermore, since wearable devices are severely constrained in computational resources, and implantable devices have hard limitations for replacement, we analyze the amount of memory the implementation of each algorithm requires. We derive this information to memory consumption (ROM and RAM separately) of each cryptography algorithm using MSPGCC compiler for Shimmer platform and AVR GCC for Teensy platform [20]. To ensure equivalence between measurements, we disregard the overhead produced by TinyOS on the Shimmer platform. Hence, we can assert that the presented data refers exactly to each algorithm.

2.4 Results

Power consumption is one of the critical factors in the design and development of wearable networks for both high-end and low-end embedded devices. Therefore, a comprehensive power efficiency analysis, considering all possible factors is of great relevance. A Power State Machine (PSM) represents the possible states of a device, and a transition between two states means power cost and delay. Thus, low power states have a longer delay between transitions for *run* states. The transition time is presented in [41]. The time for other transitions is considered insignificant and it is

not represented in PSM.

Figure 2.2 represents the PSM of the evaluated devices. In the *idle* state, the employed platforms run automatically under low energy consumption, being attractive because they manage themselves the different levels of suspension and interruptions, which makes easier for the developer. The figure also presents the average power consumption for each cryptographic algorithm and evaluated state and the transition time between states. Thus, we highlight the SKIPJACK algorithm, that improves energy efficiency in 18% compared to AES.

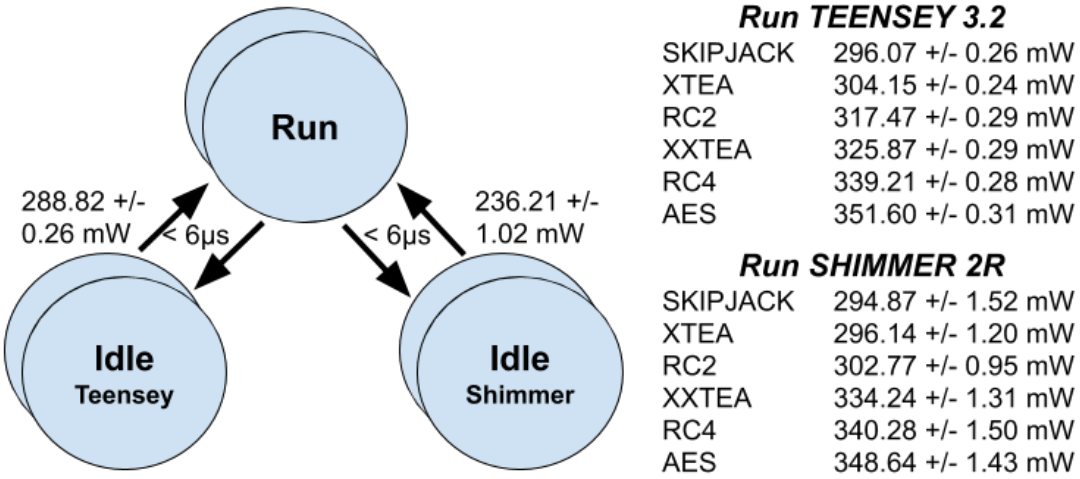
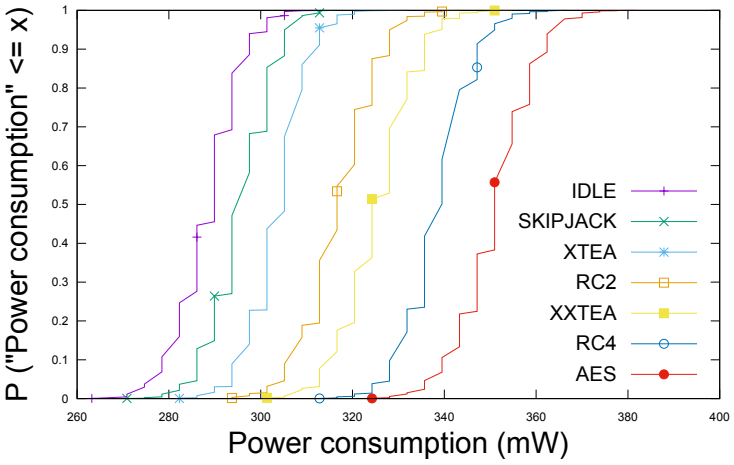


Figura 2.2: Wearable device power state machine (PSM).

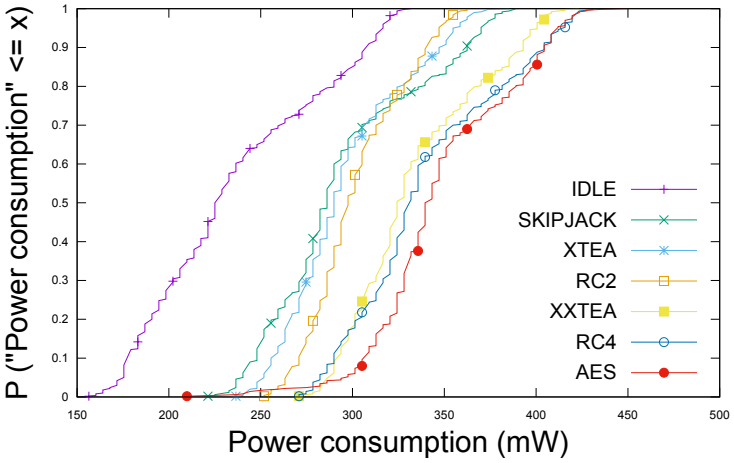
The *run* state asymptotically dominates energy consumption. The analysis of power consumption for the Shimmer platform includes cryptographic processing and radio data transmission. With the Teensey platform, we have excluded the transmission operation and we can observe a similarity in the allusive behavior to the energy consumption of the cryptographic algorithms. Figure 2.3 shows the behavior of the evaluated algorithms in both platforms through the Cumulative Distribution Functions (CDFs). Figure 2.3a illustrates the results for the Teensy platform, and Figure 2.3b presents results for the Shimmer platform.

The computational cost of logical and arithmetic operations has a direct effect on processing time and wearable device power consumption. Table 2.1 shows the number of operations for each evaluated algorithm and their respective complexity. The count is relative to the encryption function, once the wearable device performs this function, but not decryption. Thus, power consumption has a direct correlation with the number of operations. Another correspondence observed is the proportionality of ROM/RAM occupancy between the algorithms, $\approx$ 11%. In addition to finding a ROM memory consumption about $\approx$ 3.5x higher of AES in relation to SKIPJACK, considering the Shimmer platform.

Table 2.2 displays information about the amount of logical/arithmetic operations and assembly instructions performed by each cryptographic algorithm. This allows



(a) Power consumption per state Teensy 3.2.



(b) Power consumption per state Shimmer 2R.

Figura 2.3: Power consumption in milliwatts on the *run* state.

Tabela 2.1: Computational complexity vs. memory consumption.

ALGORITHM	COMPLEXITY	MEMORY CONSUMPTION (BYTES)			
		Shimmer 2R		Teensy 3.2	
		ROM	RAM	ROM	RAM
SKIPJACK	$O(1)$	6,834	608	13,892	4,584
XTEA	$O(1)$	6,772	612	13,360	4,620
RC2	$O(1)$	6,786	726	14,028	4,828
XXTEA	$O(n)$	7,064	604	13,456	4,556
RC4	$O(n)$	6,994	604	13,348	4,556
AES	$O(1)$	24,068	1,978	14,048	4,812

us to draw a direct correlation between these parameters and energy consumption. Hence, we observe that the SKIPJACK algorithm performs fewer operations and, thus, fewer instructions ($\approx$ 32x), requiring less hardware performance and less energy, particularly, when compared to AES.

Taking as a basis the cryptanalysis presented in Section 2.2, we analyze the tradeoff between power consumption and the security level for each algorithm. SKIPJACK and AES are the two extremes. SKIPJACK is the most power efficient; whereas AES has the highest power consumption. However, AES presents the highest security level.

Tabela 2.2: Logic/arithmetic operations vs. assembly instructions.

ALGORITHM	#LOGICAL/ ARITHMETC OPERATIONS	NUMBER OF ROUNDS	Shimmer 2R		Teensy 3.2	
			MAIN LOOP	TOTAL #INSTR.	MAIN LOOP	TOTAL #INSTR.
SKIPJACK	496	32	665	760	1,680	1,908
XTEA	576	32	1,184	1,206	4,256	4,329
RC2	804	16	1,550	1,645	6,832	7,075
XXTEA	1,490	12	5,748	5,776	15,936	16,034
RC4	1,992	8	400	10,677	1,088	30,703
AES	2,704	9	21,636	24,117	48,087	54,552

We could also predict the battery lifetime for the devices, as shown in Table 2.3. We consider an internal battery of 450 mA in the Shimmer platform and a demanding scenario, in which the device performs a data transmission per minute. It is estimated that the device can respond uninterruptedly for up to 67 hours using XTEA as a cryptographic algorithm. This means that the choice of the algorithm can directly influence up to $\approx$ 5.9x the battery lifetime.

Tabela 2.3: Battery life expectancy.

ALGORITHM	TIME (S)	AVERAGE CONSUMPITION (mA)	BATTERY LIFE (HH:MM)
SLEEP MODE	——	0.0011	——
SKIPJACK	33.00	58.974	40:55
XTEA	12.93	59.228	67:00
RC2	14.62	60.554	62:58
XXTEA	39.64	66.848	33:24
RC4	59.47	68.056	24:17
AES	138.00	69.728	11:34

2.5 Conclusion

In this letter, we have investigated block and stream ciphers in terms of resource usage and power consumption for end-to-end wearable devices secure communications. We have performed a hardware-driven power consumption measurement evaluation under two platforms with constrained resources. The SKIPJACK algorithm exhibits the best performance for power consumption and the second least memory usage. The XTEA algorithm presents the longest battery lifetime. However, differently from AES, SKIPJACK and XTEA have potential vulnerabilities pointed out in the literature. Hence, despite the computational and energetic efficiency of SKIPJACK and XTEA for the evaluated wearable devices, AES still presents a high security level, leading us to the conclusion that there is still a need to design encryption algorithms for wearable devices with high energy consumption efficiency and security level similar to AES.

Capítulo 3

Um Sistema Leve e Seguro para Acordo de Chaves Utilizando Comunicação Corporal

Quando trata-se de dados pessoais sigilosos transmitidos em redes propensas a ataques, as necessidades de segurança são mais evidentes. Os dispositivos vestíveis apresentam severas restrições de recursos, restringindo o uso de soluções de segurança padrão. Portanto, neste capítulo apresentamos uma solução visando à segurança e à privacidade na transmissão de dados fisiológicos em redes corporais com o menor consumo de recursos de *hardware*. Os algoritmos criptográficos de chave simétrica são rápidos e seguros, porém necessitam do compartilhamento de uma única chave secreta entre as entidades comunicantes. Assim, este capítulo apresenta um sistema para o acordo de chaves baseado em sinais fisiológicos, eficiente e otimizado, aplicando conceitos de computação aproximada [42] de modo a prover uma redução significativa no consumo de memória. A proposta apresentada melhora efetivamente o consumo de memória absoluta, proporcionando uma redução de até 76% em relação ao estado da arte. O compromisso com a segurança ocorre através da utilização de um canal de comunicação alternativo (o corpo humano), mantendo os dados completamente confinados dentro do próprio indivíduo.

3.1 Introdução

O uso de dispositivos eletrônicos vestíveis representa, nos dias de hoje, um passo evolutivo da tecnologia móvel. Estes dispositivos têm sido adotados massivamente em diversos segmentos como, por exemplo, medicina preventiva e bem-estar físico, pertencendo ao subconjunto da Internet das Coisas (IoT). Estima-se que existam mais de 20 bilhões de "coisas" conectadas, onde cerca de 40% destas, sejam relacionadas à telemedicina, constituindo um mercado de US$ 117 bilhões. Para 2025, acredita-se que este número de dispositivos alcance 75 bilhões [43]. Apesar de ainda em estágio inicial, diversas pesquisas empíricas sobre o uso de soluções tecnológicas e disposi-

tivos vestíveis foram realizadas no contexto da saúde nos últimos anos. No entanto, apesar destas pesquisas, a grande disseminação do uso de novas tecnologias desperta discussões sobre a coleta e o compartilhamento de dados, com foco em proteção, privacidade, precisão e confiabilidade, uma vez que frequentemente os dados de saúde são transmitidos e armazenados em meios físicos vulneráveis a ataques [44]. As atuais tecnologias de transmissão de dados sem-fio utilizam radiofrequências como *RF-Narrowband* (RF-NB), *RF-Ultra Wideband* (RF-UWB), *Millimeter Wave* (mmWave) ou rede móvel 5G. Essas tecnologias são mais suscetíveis a ataques, uma vez que seu sinal é propagado pelo ambiente [9, 10]. Uma técnica alternativa e menos suscetível a ataques é a utilização do corpo do paciente como meio físico e canal de comunicação seguro para a transmissão dos dados. Essa técnica, conhecida como acoplamento galvânico, dificulta a injeção de sinais maliciosos ou a espionagem de dados por meio de ataques de canal lateral ou outras técnicas de "*sniffers*". Isto ocorre devido ao confinamento do sinal dentro do corpo do próprio paciente [45].

Os sistemas de redes corporais (WBAN) exigem certas medidas para garantir a segurança, privacidade, integridade e a confidencialidade dos dados clínicos de um paciente a todo momento. A Segurança e a privacidade são os dois aspectos cruciais para um sistema WBAN [10, 46, 26]. A segurança implica que os dados sejam protegidos contra usuários não autorizados desde a coleta, transmissão e armazenamento, garantindo a privacidade das informações pessoais. Quando aplicações maliciosas conseguem tomar posse e manipular informações pessoais, uma série de problemas é desencadeada. A exposição pública pode gerar danos pessoais severos, tais como perda de emprego ou danos emocionais. Além disso, as informações falsas repassadas aos médicos resultam em alteração de diagnósticos e tratamento, ocasionando até a morte de pacientes. Portanto, é imprescindível adotar um meio de comunicação robusto aliado ao uso de técnicas de criptografia, de modo a garantir a segurança e a privacidade dos dados [22]. Como os dispositivos WBAN possuem recursos limitados em termos de armazenamento, poder de processamento e energia, existem várias restrições acerca do desenvolvimento de projetos de geração e acordo de chaves secretas [26]. Portanto, as estratégias de geração e acordo chaves devem ser leves, eficientes em termos energéticos e consumir pouca memória. Além disso, é desejável que o envolvimento do usuário ou de terceiros seja mínimo, o que inviabiliza o uso dos esquemas projetados para redes de sensores sem fio de um modo geral em WBANs [14].

Neste trabalho, é apresentada uma solução completa e leve para o problema de gerenciamento de chaves para algoritmos de criptografia simétrica, proporcionando um avanço no estado da arte [26] em relação à segurança dos dados coletados e trafegados em redes WBANs, com o menor consumo dos recursos de *hardware*. Deste modo, é proposto um sistema robusto e eficiente para geração e estabelecimento de chaves

secretas, baseado em sinais fisiológicos, particularmente o eletrocardiograma (ECG) entres dispositivos IoT vestíveis. A arquitetura do sistema proposto é ilustrada pela Figura 3.1. O sistema é composto por módulos, de modo que a cada um destes seja atribuída uma função específica. O módulo gerador de chaves proposto toma como base os trabalhos apresentados em [2, 47] aplicando conceitos de computação aproximada [42] de modo a prover otimizações acerca da utilização de memória. Nesta etapa, o sinal fisiológico do ECG sofre uma transformação produzindo características individuais únicas, que posteriormente serão quantizadas de modo a produzir uma chave secreta comum. O processo de troca de chaves secretas é definido por um protocolo simplificado de comunicação e troca de mensagens. Os trabalhos que alicerçam esta pesquisa necessitam da adição de técnicas de segurança, o que consequentemente proporciona uma sobrecarga ao seu protocolo de comunicação, visto que utilizam um meio de transmissão compartilhado e propenso a interceptações. Portanto, com o objetivo de prover uma comunicação segura entre sensores, aliada a redução da sobrecarga de comunicação, o módulo responsável por estabelecer a conexão entre os dispositivos utiliza um canal de comunicação alternativo (o corpo humano). Assim, estas chaves que são comumente alvo de ataques, são distribuídas por meio de um sinal completamente confinado dentro do próprio indivíduo.

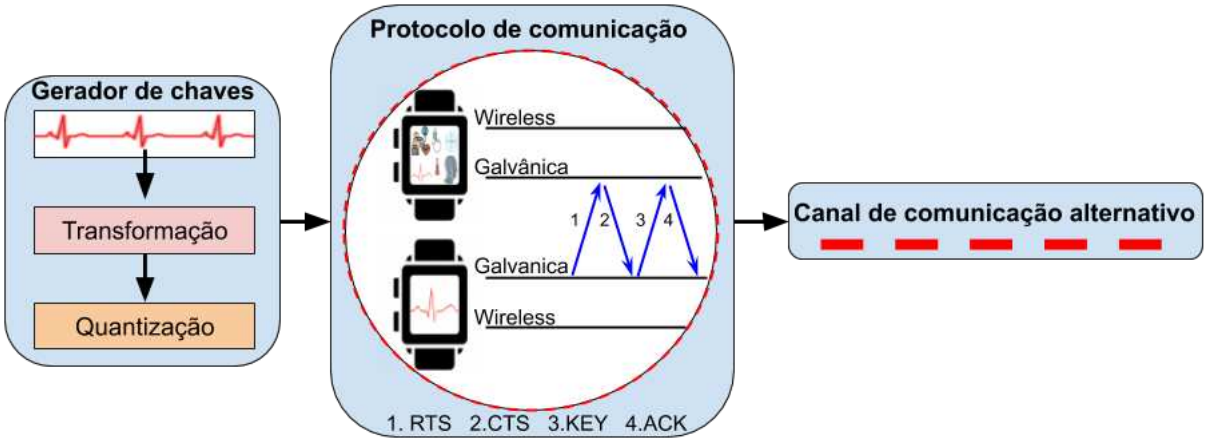


Figura 3.1: Arquitetura do sistema proposto.

O sistema apresentado neste artigo busca atender aos requisitos referentes à consumo de recursos utilizando de técnicas de computação aproximada e privacidade de dados através da comunicação intra-corpo. Os resultados indicam que a proposta é capaz de assegurar uma redução no consumo de memória de aproximadamente 24% reduzindo também o custo na comunicação durante o processo de acordo de chaves. O esquema de acordo de chave proposto, utilizando a comunicação galvânica, isenta o sistema do tempo de pré-configuração ou carregamento manual de chaves, ou seja, os sensores começam a se comunicar com segurança assim que dispostos no corpo. O custo integral para realizar a transmissão de uma chave criptográfica de 128 bits é

próximo de 1 segundo por sessão.

A sequência deste trabalho acompanha a seguinte organização. A Seção 3.2 discute sobre o estado da arte sobre a geração e o acordo de chaves secretas baseados em sinais fisiológicos. Na Seção 3.3, apresentamos o sistema proposto. Na Seção 3.4, são discutidos os benefícios obtidos. Por fim, a seção 3.5 conclui o artigo e direciona os trabalhos futuros.

3.2 Trabalhos Relacionados

Nesta seção são apresentados os principais trabalhos do estado da arte relacionados à geração e estabelecimento de chaves criptográficas utilizando sinais fisiológicos para dispositivos com limitações computacionais [14]. O esquema de acordo de chave EKA (*EKG based Key Agreement*), proposto em [2], utiliza sinais de eletrocardiograma para gerar chaves criptográficas. Presume-se que todos os sensores sejam capazes de aferir os sinais de eletrocardiograma. O processo descrito neste trabalho consiste fundamentalmente em duas etapas, extração de características e acordo de chaves. Na fase de extração de características, ambos dispositivos realizam a leitura do sinal eletrocardiograma simultaneamente. É utilizada a uma taxa de amostragem fixa a 125Hz durante 5 segundos resultando em 650 amostras. Estas amostras são divididas em 5 blocos com 125 amostras cada (ou 1 segundo). Em seguida, é aplicada a Transformada Rápida de Fourier (FFT) de 128 pontos para cada parte. Os primeiros 64 coeficientes provenientes do resultado da FFT de cada uma das 5 partes são concatenados a fim de formar um vetor de característica contendo 320 coeficientes (ponto flutuante de precisão dupla), como ilustrado na Figura 3.2. Para gerar blocos de características, o vetor de característica sofre uma quantização. Esse trabalho aplica a quantização exponencial em 12 etapas, produzindo um valor binário de 4 bits para cada coeficiente, resultando em 20 blocos, 64 bits em cada um dos sensores de comunicação.

A fase de acordo de chaves é subdividida em três etapas, compromisso, processamento e confirmação. Durante o compromisso os blocos contendo 1.280 bits sofrem uma cifra por meio de uma função *hash* e são trocados entre os sensores. Na etapa de processamento os blocos são organizados e classificados de modo a gerar uma matriz que contenha apenas os índices dos blocos que são idênticos em ambos os sensores. Deste modo é possível derivar a chave comum. Para a confirmação os nós trocam uma mensagem entre si mascarando a chave pública com um bloco idênticos através da função XOR. Uma verificação é realizada para a identificação do bloco, se a avaliação for bem-sucedida, as chaves são aceitas.

O esquema apresentado em [47] oferece soluções de modo a otimizar o processo de geração do vetor de características proposto por [2], aplicando a transformada de onduleta discreta (DWT). Uma vez que esta transformada apresenta custo computa-

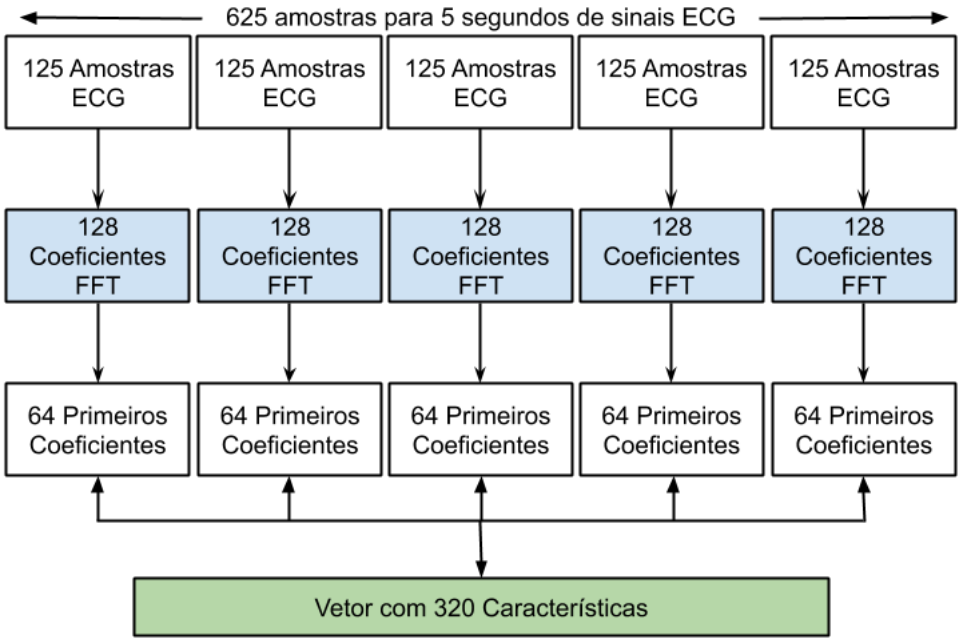


Figura 3.2: Geração de características a partir do sinal de eletrocardiograma [2].

cional linear, enquanto a FFT apresenta um custo linearítmico. Além disso, durante a fase estabelecimento de chaves, a etapa de compromisso é renomeada como para compromisso com marca d'água. Esta alteração consiste em adicionar valores aleatórios obtidos a partir de sinais coletados da íris ou de impressão digital a cada bloco antes de ser enviado. Isso faz com que o tamanho do bloco seja de pelo menos 128 bits, dificultando ataques de força bruta. A íris ou matriz de impressão digital são usadas devido à sua natureza constante e únicas por indivíduo. As demais etapas seguem a arquitetura descrita anteriormente. Assim a análise de desempenho é focada exclusivamente sobre as transformações, onde a DWT apresenta melhor complexidade computacional. Os autores não apresentaram o custo computacional referente a adição do método de marca d'água. Uma vez que este necessita de mais sensores junto aos pacientes e maior processamentos e memória para armazenar dos sinais obtidos por tais sensores. Além de empregar uma sobrecarga à transmissão dos blocos entre os dispositivos.

Os trabalhos citados objetivam apresentar a funcionalidade dos sinais de eletrocardiograma para gerar chaves criptográficas comuns entre dois nós. Ainda sugerem que as chaves geradas sejam longas, aleatórias e com variação de tempo, além de serem altamente depende do usuário. Entretanto, mesmo com uma proposta "leve", os autores desenvolveram suas propostas em MATLAB, o que impossibilita a avaliação real para dispositivos com recursos limitados. Dispositivos como Arduino e Teensy, comumente utilizados em projetos de baixo custo, têm limitações severas de memória, inclusive não dão suporte nativo a ponto flutuante de precisão dupla como no MATLAB. Ademais, ao que se diz respeito à transferência dos blocos, existe uma so-

brecarga exacerbada, inviabilizando a utilização de canais de comunicação de baixa vazão, como a comunicação galvânica.

Portanto, o sistema proposto busca, além das características de segurança já apresentada, implementar uma solução ainda mais otimizada. Objetiva-se reduzir o consumo de memória utilizando computação aproximada, mantendo o desempenho e níveis de segurança já alcançados. Ademais, como pode-se observar na Tabela 3.1, objetiva-se reduzir o conjunto de amostras da entrada em 20%, além de se utilizar a função de transformada com menor complexidade (DWT). Intenciona-se remover a sobrecarga durante a fase da troca de chaves em decorrer da aplicação de técnicas de transmissão que utilizam como meio seguro o próprio tecido humano. E, deste modo, é apresentado um sistema completo e funcional com total compatibilidade a dispositivos reais com recursos limitados.

Tabela 3.1: Comparação entre protocolos.

Trabalhos	Amostras de ECG	Transformada	Sobrecarga no estabelecimento das chaves	Meio de transmissão	Validação
[2]	625	FFT	SIM	Wireless	MATLAB
[47]	625	DWT	SIM	Wireless	MATLAB
Proposto	500	DWT	Não	Galvânico	Dispositivo real

Visto que a transmissão segura das chaves é parte fundamental do processo de acordo de chaves, a adoção de um meio de comunicação que atenda a este requisito deve ser explorada. Deste modo, este trabalho baseia-se na metodologia proposta em [45], onde é proposto um sistema para autenticação de usuários baseada em biometria. Esta abordagem promete proteger a transmissão de dados contra ataques sofisticados de *RF sniffer*. De modo a complementar e prover maior robustez no trabalho proposto, utiliza-se de *hardwares* específicos e construídos especificamente para realizar o acoplamento de sinais em meio iônico [48, 49, 50].

3.3 Sistema Proposto

Esta seção apresenta o sistema proposto para realizar a geração e o acordo de chaves secretas com base em dados fisiológicos, bem como sua distribuição. Propõe-se um algoritmo leve que utiliza computação aproximada [42] para economizar os recursos de *hardware* em dispositivos vestíveis. Por fim, é apresentado um sistema experimental completo de baixo custo para a comunicação galvânica. Este utiliza o corpo humano como canal de transmissão robusto para o estabelecimento de chaves secretas. Ainda respeita-se a legislação de ética vigente, na qual são utilizadas soluções aquosas para apresentar propriedades dielétricas similares ao tecido humano.

3.3.1 Geração de Chaves

O recente avanço das pesquisas na telemedicina tem permitido o desenvolvimento de dispositivos miniaturizados de baixa potência que podem executar o monitoramento e a transmissão dos sinais vitais de pacientes cada vez mais preciso. Entretanto, o emprego de técnicas de segurança deve seguir os requisitos de projeto de modo a minimizar o consumo de recursos [26]. Os modelos apresentados na Seção 3.2 são baseados em sinais fisiológicos, com a finalidade de atender a estes requisitos, o que lhes credenciam como base para desenvolvimento da nossa abordagem. Deste modo, as otimizações foram propostas para atender aos requisitos de consumo de recursos.

O processo de geração de chaves proposto parte da aquisição dos sinais fisiológicos particularmente o ECG. Para isto utilizou-se como fonte os dados ECG filtrados de pacientes disponibilizados pelo banco de dados (ECG-ID) do MIT PhysioBank [51]. O sinal é amostrado em 125Hz, ou seja, 125 amostras por segundo. O tipo de dado adotado para a representação de cada amostra da entrada é um inteiro assinalado de 16 bits. Deste modo, segmenta-se a base em quatro segundos, que são divididos em janelas de 125 amostras cada. Esta redução em intervalos em potência de 2 proporciona uma análise de 500 amostras. As amostras são convertidas do seu domínio original (tempo) para uma representação no domínio da frequência utilizando uma transformada. Como enfatizado em [47], DWT apresenta o melhor desempenho perante a FFT e, portanto existe a preferência em sua utilização. Os métodos de transformada de 128 pontos proporcionam a decomposição da amostra de ECG em uma sequência de valores singulares, onde os 64 primeiros (devido à natureza simétrica do espectro) de cada uma das quatro partes representam as características inerentes de cada intervalo. A criação de uma estrutura que agrupe estes valores em um vetor de características apresenta a maior contribuição deste trabalho referente ao processo de geração de chaves secretas. Como foco principal da inclusão do canal secundário de comunicação através da pele é proporcionar a segurança necessária ao estabelecimento de chaves, não é preciso de fato armazenar todos os 256 coeficientes. Portanto, armazenam-se apenas os 64 primeiros coeficientes provenientes da transformada. Os coeficientes são números reais e neste momento são representados com meia precisão (16 bits) com intuito de reduzir ainda mais o consumo de memória. Como esta representação não é nativa dos *hardwares* de prateleira, ela foi desenvolvida em software. A meia precisão foi implementada obedecendo rigorosamente as descrições do padrão IEEE 754, tendo sua representação binária armazenada dentro do tipo inteiro sem sinal de 16 bits. Portanto, em cada intervalo de 64 características é aplicada a quantização exponencial de 4 etapas para realizar a geração de chaves. A quantização produz um valor binário de 32 bits para cada bloco de 64 coeficientes. Ao fim das quatro iterações, as quais consomem toda a entrada de dados, uma chave secreta baseada

em sinais fisiológicos de 128 bits é produzida. Todo o processo de geração de chaves proposto é ilustrado passo a passo pela Figura 3.3, onde observam-se quatro iterações rotuladas como iteração 0 a 3. Em cada uma das iterações tem-se o processamento de um conjunto de 125 amostras de ECG por meio da transformada. Em seguida os 64 coeficientes característicos resultantes são quantificados em 32 bits.

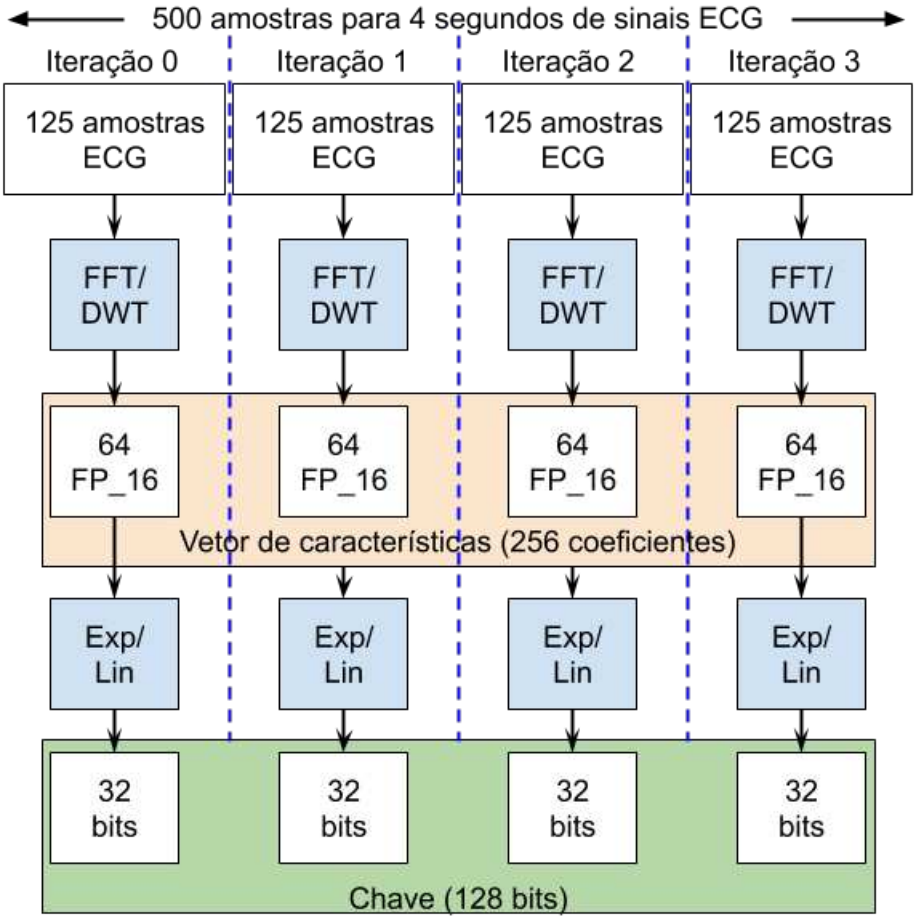


Figura 3.3: Geração de chaves proposta.

3.3.2 Acordo de Chaves

A fase de acordo de chaves ocorre após a vetorização de características ser quantizado gerando a chave secreta a ser compartilhada entre os dispositivos. Esta chave é trocada entre os dispositivos por meio do canal seguro proporcionado pelo acoplamento galvânico. Este canal é ilustrado pela **interface de acordo de chaves** na Figura 3.4. A **interface de dados** é ativada após o estabelecimento das chaves sendo responsável pela transmissão dos dados fisiológicos cifrados entre os dispositivos. Esta interface pode ser implementada sobre qualquer tecnologia de radiofrequência.

O processo de comunicação entre os dispositivos tem início quando um dispositivo deseja estabelecer uma comunicação com o outro (normalmente com maior poder

Figura 3.4: Interfaces de comunicação.

computacional/nó coordenador). Neste momento, é necessário que ambos dispositivos já estejam de posse das chaves de criptografia utilizadas na cifra dos dados. O protocolo de comunicação simplificado utiliza sinalizadores equivalentes aos presentes nas normas do IEEE 802.11, com objetivo de manter uma padronização. Portanto, é enviado um pedido para enviar (RTS - *request to send*) com endereço do destinatário. Se o receptor dispuser de dados a enviar, ele sinaliza com uma mensagem em que "pode enviar" (CTS - *clear to send*). Neste momento, a chave é transmitida e, após a conclusão, o receptor sinaliza o recebimento com a mensagem de confirmação (ACK - *acknowledgement*). Assim, os dispositivos estão aptos a trocar dados sigilosos cifrados. Para isto, o protocolo de transmissão de dados segue os mesmos passos descritos para a troca de chaves, com o envio de RTS, recebimento de CTS, envio dos dados e confirmação por ACK. A Figura 3.5 ilustra todo o processo de comunicação entre os dispositivos utilizando ambas interfaces. O círculo à esquerda, construído por uma linha tracejada em vermelho, representa a fase de estabelecimento de chaves, o qual utiliza a comunicação galvânica para troca de informações entre os dispositivos. Já o círculo à direita, simbolizado em tracejado preto, corresponde à interface de comunicação a qual utiliza radiofrequência para realizar a troca de informações bem como os sinais vitais cifrados.

3.3.3 Acoplamento Galvânico

O sistema de estabelecimento de chaves proposto é fundamentado na comunicação segura através do acoplamento galvânico. Deste modo, existe uma redução significativa na vulnerabilidade a ataques, principalmente quando comparado às de tecnologias de comunicação convencionais por radiofrequência, tais como Bluetooth e Zigbee [45]. A partir deste princípio, descrevemos as principais características da rede, capaz de pro-

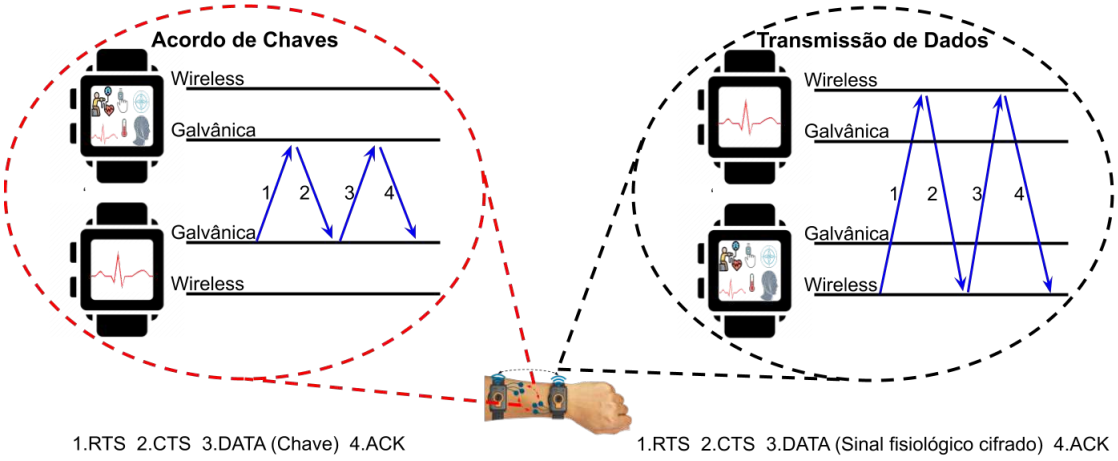


Figura 3.5: Protocolos nas interfaces.

ver uma troca de chaves segura entre dois nós presente em uma rede WBAN.

Neste trabalho, a parte experimental foi desenvolvida sobre a plataforma de prototipagem eletrônica de *hardware* livre Arduino Nano. Esta plataforma é equipada com um microcontrolador ATmega328, 32 KB Memória Flash. Os softwares desenvolvidos para a plataforma foram implementados na linguagem C e implantados nos dispositivos usando o ambiente de desenvolvimento integrado (IDE) do próprio Arduino. Para realizar o acoplamento dos sinais de dados junto ao corpo, foram utilizados *hardwares* de baixo custo desenvolvidos especificamente para esta finalidade [48, 49, 50].

Para codificar os sinais de forma analógica, passíveis de externalização utilizando as portas PWM (*Pulse Width Modulation*) dos microcontroladores, foi implementado em software o protocolo assíncrono UART (*Universal Asynchronous Receiver/Transmitter*). Este protocolo proporciona conversão de dados de paralelo para serial durante a transmissão e de serial para paralelo na recepção. Além de simples, o protocolo proporciona uma comunicação eficiente. Em conjunto, utiliza-se a modulação OOK (*On-off keying*) pois esta consume menos energia e se adequar à natureza *On-Off* dos dispositivos digitais [52, 45]. Estas modulações representam os dados digitais através das variações de amplitude e duração em uma onda portadora. A presença de uma onda por um período de tempo específico tem o valor binário 1, enquanto a ausência da onda portadora por um período de tempo indica valor binário 0.

Os *hardwares* responsáveis pelo acoplamento e recepção dos sinais consistem respectivamente em um *differential drive* e um *sensing amplifier*, os quais possuem descrição aberta à comunidade [1]. De forma resumida, o *driver* diferencial converte pulsos eletrônicos produzidos pelo microcontrolador em corrente elétrica a ser aplicada ao meio físico. Essa corrente produz uma tensão que pode ser identificada por eletrodos receptores dispostos a uma curta distância da fonte. O nó receptor equipado com amplificador de sinal (1000x) torna possível a leitura de dados por dispositivos

[1] https://github.com/adrianosvc/ibc_coupling

analógico de medição, como o osciloscópio ou aquisitor de dados [48, 49, 50]. Para reconstruir o sinal recebido de forma que seja compatível com os microcontroladores de prateleira, é necessária a utilização de uma módulo conversor analógico digital. O módulo ADS115 converte as tensões diferenciais (± 5v) em valores que variam de 0 a 5v, correspondente aos valores de leitura das portas de entradas PWM dos microcontroladores. Entretanto, esta decodificação exige várias operações de ponto flutuante definindo um gargalo na comunicação. Por este motivo, o tempo seguro de bit o qual permite plena decodificação online é de 8 ms, representando uma vazão de dados a 125 bps.

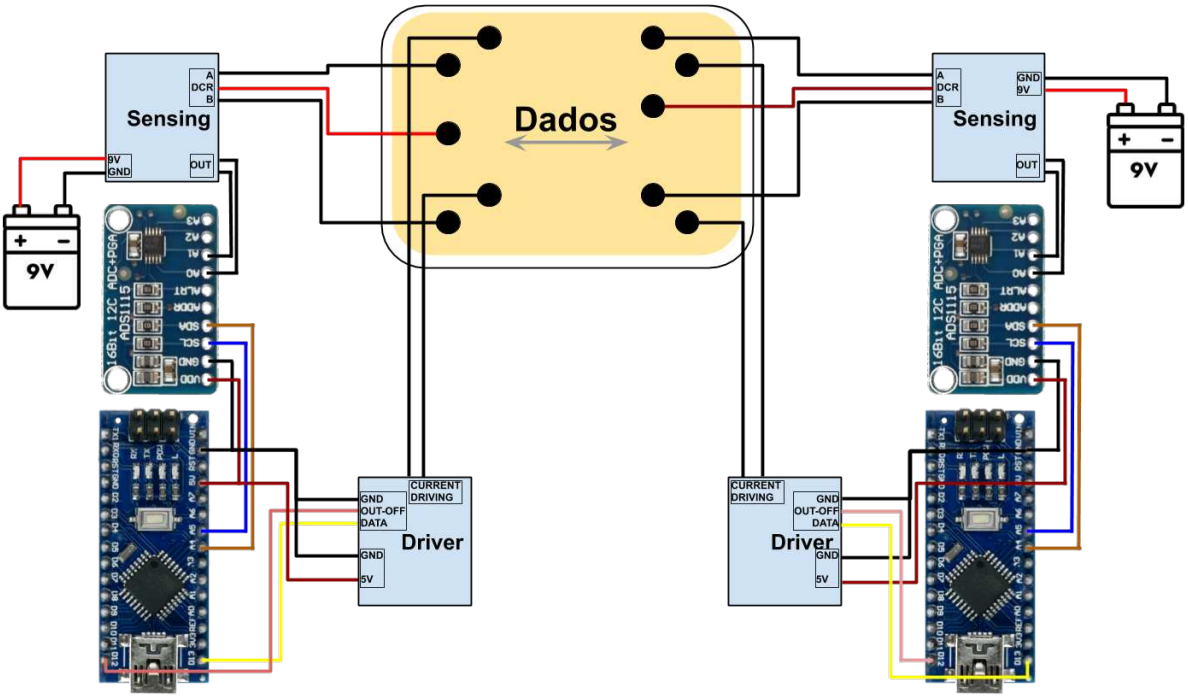


Figura 3.6: Cenário de transmissão de dados.

A Figura 3.6 ilustra o acoplamento do conjunto de *hardwares* acima descritos, os quais são necessários para realizar os procedimentos de geração e acordo de chaves proposto. Neste arcabouço, o sinal é acoplado ao ambiente físico através de uma corrente diferencial de 1 mA. Utilizamos um tecido fantasma (esponja) envolto por uma solução salina (0,9%), representando um meio iônico para propagação do sinal. O comprimento do canal corresponde à distância dos eletrodos transmissores (*differential drive*) e receptores (*sensing amplifier*) mantidos espaçados a 10 cm [45].

3.4 Resultados

O consumo de recursos computacionais como memória é um dos fatores críticos para o projeto e desenvolvimento de soluções de segurança para dispositivos embarcados

aplicados às redes corporais. Assim, uma análise abrangente referente ao seu aproveitamento é de grande relevância. Na análise apresentada a seguir, é considerada a implementação proveniente dos trabalhos apresentados na Seção 3.2 considerando a representação nativa dos *hardwares* para ponto flutuante de precisão simples. Assim é possível traçar um paralelo com a proposta otimizada proposta, a qual utiliza o recurso de computação aproximada para representar números reais em meia precisão.

Como o número 2 é a base do sistema binário e suas potências são relevantes na Ciência da Computação o método proposto utiliza quatro janelas para amostrar o sinal fisiológico do ECG, proporcionando uma entrada de dados 20% menor. Entretanto, a grande contribuição no quesito consumo de memória encontra-se sobre o vetor de características. Ao adicionar o canal secundário de comunicação através da pele é possível realizar a geração direta da chave de 128 bits e enviá-la, sem necessidade de armazenar o vetor de características completo e as demais estruturas de dados. Isto aliado com a representação das características em meia precisão proporciona uma redução de 90% em relação aos algoritmos de geração de chaves tradicionais. Estas otimizações representam uma economia absoluta de aproximadamente 1.37KB somente para o procedimento de geração de chaves.

A comunicação galvânica ainda elimina todo a sobrecarga de armazenamento de dados adicionado à fase de acordo de chaves, uma vez que a chave de 128 bits está pronta para compartilhamento depois de quantizada. Este consumo extra por parte do algoritmo apresentado em [2] compreende as seguintes estruturas: *Quantized Blocks, Copy Hashed blocks, Hashed blocks', W e KeyMat*, onde são consumidos outros 0,93 KB de memória. Por empregar mais segurança com a adição de uma marca d'água proveniente de outro sinal fisiológico, como digital ou íris, o trabalho contido [47] consome ainda mais memória. As estruturas *Copy Hashed blocks, Hashed blocks'e W*, além da matriz com os coeficientes para a composição da marca d'água, possuem o dobro de tamanho. Como o valor desta matriz não é informado, inferimos que ela possua as mesmas dimensões de W devido a suas características. Portanto, esta versão de algoritmo de acordo de chaves consome cerca de 2,16 KB. A Tabela 3.2 apresenta um comparativo sobre o consumo de dados de ambas implementação perante a proposta deste trabalho.

Tabela 3.2: Avaliação do consumo de memória.

Consumo de Memória em Bytes	(Venkatasubramanian et al.)	(Ali et al.)	Proposto
Entrada de dados	1.250	1.250	1.000
Vetor de características	1.253	1.253	128
Acordo de chaves	960	2.215	0
Total	**3.463**	**4.718**	**1.128**

Além dos custos referentes ao consumo de memória, é importante discutirmos

a sobrecarga na transmissão de dados para estabelecimento das chaves. Os mecanismos propostos para incorporar segurança compartilhamento para a utilização de meios de comunicação não segura implicam em excesso de compartilhamento de dados. Podemos citar a troca dos blocos quantizados cifrados, o código de autenticação de mensagens e as chaves aleatórias *Key R* de cada dispositivo. Com a proposta de estabelecimento de chaves *plug and play* deste trabalho, além das mensagens curtas de controle, o pacote útil da mensagem principal é formado basicamente pela chave secreta de 128 bits. Portanto, considerando o sistema completo de transmissão de dados galvânico apresentado, assim como suas respectivas propriedades, e respeitando as severas limitações impostas pelo conversor analógico digital, é possível transmitir a chave em aproximadamente 1 segundo. Entretanto, ao desconsiderarmos este gargalo, o sistema pode atingir um intervalo de tempo de bit de 90 μs, chegando a 11,11 kbps de vazão, o que significa que a chave pode ser enviada em 0,0115 segundo. Limites ainda maiores podem ser alcançados, porém é bem conhecido que a quantidade de poluentes do espectro eletromagnético se eleva abruptamente acima dos 100 kHz, o que é indesejável. Isto reforça a importância da transmissão em baixa frequência. Com base nos objetivos propostos e na metodologia apresentada, pode-se afirmar que o sistema é leve, robusto e seguro suficiente para ser implantado em dispositivos com recursos limitados, como Arduino. Esta afirmação é respaldada pelos resultados referentes ao consumo de memória, tempo de processamento e transmissão de dados.

3.5 Conclusão

Apoiados sobre os resultados inerentes ao consumo de memória apresentado pela presente abordagem, é possível afirmar que as otimizações propostas atendem às aplicações em dispositivos com recursos limitados. Ademais, a partir da redução da sobrecarga durante o processo de estabelecimento de chaves, torna-se possível a utilização da comunicação galvânica como um canal de comunicação seguro para a transmissão de dados sigilosos. Portanto, é possível realizar a geração e estabelecimento *plug and play* de chaves secretas utilizando a pele como meio de comunicação seguro para dispositivos vestíveis que fazem uso de algoritmos de criptografia simétrica. Como trabalhos futuros pretende-se expandir a proposta principalmente direcionando-a para aplicações que exijam autenticação de usuários de forma contínua e não invasiva.

Capítulo 4

Conclusão

Neste manuscrito, foram apresentados dois trabalhos que objetivam introduzir novos métodos para prover a garantia de segurança à informações clínicas coletadas e trafegadas por dispositivos eletrônicos dispostos junto ao corpo humano. O objetivo das soluções apresentadas baseiam-se em atender os requisitos inerentes das redes corporais. Portanto, uma análise abrangente da eficiência energética, considerando todos os fatores possíveis, é de grande relevância, como observado no Capítulo 2. Deste modo, foi investigado o impacto da aplicação de algoritmos criptográficos em dispositivos comerciais, avaliando o consumo de recursos e energia através de uma metodologia eficaz de aferição baseada em *hardware*. Dentre os algoritmos de cifra leve avaliados, o SKIPJACK apresenta o melhor desempenho relativo ao consumo de energia e o segundo menor gasto de memória. Não obstante, o algoritmo XTEA apresenta um desempenho médio melhor, proporcionando uma maior vida útil à bateria dos dispositivos. Contudo, SKIPJACK e XTEA ainda apresentam potenciais vulnerabilidades apontadas na literatura devido suas características de projeto simplistas, direcionados à eficiência e leveza, diferentemente do AES. Portanto, apesar da eficiência computacional e energética apresentada pelos métodos SKIPJACK e XTEA, o algoritmo de cifra AES ainda apresenta um nível superior de segurança, levando à conclusão de que ainda é necessário projetar soluções próprias para dispositivos vestíveis com alta eficiência energética e nível de segurança semelhante ao AES.

Geralmente os algoritmos criptográficos de chave simétrica são rápidos, seguros e eficientes computacionalmente. Entretanto, necessitam que uma chave secreta única seja compartilhada *a priori* entre os dispositivos da rede, processo conhecido como gerenciamento de chaves. O Capítulo 3 deste trabalho destaca a proposta de um sistema leve, otimizado e completo para realizar este estabelecimento de chaves. A proposta é desenvolvida principalmente para atender ao requisito consumo de recursos de *hardware*. Portanto, a partir da redução da sobrecarga durante o processo de estabelecimento de chaves é possível concluir que as otimizações propostas, atendem às necessidade específicas de dispositivos com recursos limitados, uma vez que proporcionam uma redução de até 76% em relação ao estado da arte. Além disso, essa economia de recursos aliada à redução da sobrecarga no processo de envio das cha-

ves permite a utilização da comunicação galvânica como um canal de comunicação seguro para a transmissão de dados sigilosos. Assim como introduzido pelo estudo presente no Apêndice A referente a viabilidade da utilização de tecido vivo para a propagação dos dados. Portanto, é possível realizar a geração e estabelecimento *plug and play* de chaves secretas de forma eficiente e fazendo uso da pele como meio de comunicação seguro para dispositivos vestíveis que fazem uso de algoritmos de criptografia simétrica.

Os resultados alcançados e as conclusões acima apresentadas demonstram que este trabalho atingiu os objetivos propostos. Contudo, apesar dos resultados positivos e apresentação de um sistema seguro e robusto suficiente para ser empregado em redes WBAN, novas questões no âmbito das redes corporais ainda devem ser investigadas. No futuro, gostaríamos de estender nosso estudo a outras vertentes da segurança em redes corporais, como a autenticação de usuários. Apresentando uma versão do sistema que seja capaz de utilizar características de sinais fisiológicos para realizar a autenticação de maneira constante e não intrusiva entre dispositivos. Objetiva-se ainda aprofundar os estudos sobre a propagação dos dados por meio dos tecidos vivos, de modo que seja possível obter uma elevada taxa de transmissão com significativa redução de ruídos.

Apesar deste trabalho contemplar um estudo aprofundado sobre a construção de algoritmos criptográficos, ainda é necessário que novos algoritmos sejam desenvolvidos especificamente para atender aos rigorosos requisitos das redes corporais. Espera-se que esta análise seja estendida sobre os demais esquemas criptográficos, como curva elíptica. Meios alternativos, seguros e eficientes para realizar a transmissão dos materiais criptográficos representam uma área em desenvolvimento. Dentro do campo da comunicação intra-corpo existem diversas questões a serem exploradas, bem como a vazão dos dados, mitigação de interferências, alcance e efeitos colaterais ao tecido vivo. Portanto, o desenvolvimento de *hardwares* específicos e miniaturizados para realizar o acoplamento do sinal junto ao tecido vivo também carecem de atenção.

Referências Bibliográficas

[1] Felix Richter. Consumer spending on wearables to double by 2021. https://www.statista.com/chart/19954/consumer-spending-on-wearable-devices/, nov 2019. Último Acesso: 29-01-2020.

[2] Krishna Kumar Venkatasubramanian, Ayan Banerjee, Sandeep KS Gupta, et al. Ekg-based key agreement in body sensor networks. In *IEEE INFOCOM Workshops 2008*, pages 1–6. IEEE, 2008.

[3] Israa Al_Barazanchi, Haider Rasheed Abdulshaheed, and Madya Safiah Binti Sidek. A survey: Issues and challenges of communication technologies in wban. *Sustainable Engineering and Innovation, ISSN 2712-0562*, 1(2):84–97, 2019.

[4] GK Ragesh and K Baskaran. An overview of applications, standards and challenges in futuristic wireless body area networks. *International Journal of Computer Science Issues (IJCSI)*, 9(1):180, 2012.

[5] Samaneh Movassaghi, Mehran Abolhasan, Justin Lipman, David Smith, and Abbas Jamalipour. Wireless body area networks: A survey. *IEEE Communications Surveys & Tutorials*, 16(3):1658–1686, 2014.

[6] Michele Nogueira Lima. *Saúde Móvel: Conceitos, Iniciativas e Aplicações*. Clube dos Autores, 2010.

[7] Iara Augustin, Giuliano Pereira Ferreira, and Adenauer Corrêa Yamin. Grade computacional como infra-estrutura para a computação pervasiva/ubíqua. *ERAD - Santa Cruz do Sul*, 2008.

[8] Laurence Goasduff. Gartner says global end-user spending on wearable devices to total $52 billion in 2020. https://www.gartner.com/en/newsroom/press-releases/2019-10-30-gartner-says-global-end-user-spending-on-wearable-dev, oct 2019. Último Acesso: 29-01-2020.

[9] William J Tomlinson, Stella Banou, Christopher Yu, Milica Stojanovic, and Kaushik R Chowdhury. Comprehensive survey of galvanic coupling and alternative intra-body communication technologies. *IEEE Communications Surveys & Tutorials*, 21(2):1145–1164, 2018.

[10] Assefa K Teshome, Behailu Kibret, and Daniel TH Lai. A review of implant communication technology in wban: Progress and challenges. *IEEE reviews in biomedical engineering*, 12:88–99, 2018.

[11] Louise Marie Hurel and Luisa Cruz Lobato. Segurança e privacidade para a internet das coisas. 2018.

[12] ASCOM. Decreto que institui o plano nacional de internet das coisas é publicado. http://www.mctic.gov.br/mctic/opencms/salaImprensa/noticias/arquivos/2019/06/Decreto_que_institui_o_Plano_Nacional_de_Internet_das_Coisas_e_publicado.html, 2019. Último Acesso: fevereiro de 2020.

[13] Sagarika Karchowdhury and Mainak Sen. Survey on attacks on wireless body area network. *International Journal of Computational Intelligence & IoT, Forthcoming*, 2019.

[14] Aftab Ali and Farrukh Aslam Khan. Key agreement schemes in wireless body area networks: Taxonomy and state-of-the-art. *Journal of medical systems*, 39(10):115, 2015.

[15] Mahdi Aiash, Glenford Mapp, and Aboubaker Lasebae. A survey on authentication and key agreement protocols in heterogeneous networks. *arXiv preprint arXiv:1208.1918*, 2012.

[16] Deena M Barakah and Muhammad Ammad-uddin. A survey of challenges and applications of wireless body area network (wban) and role of a virtual doctor server in existing architecture. In *Intelligent Systems, Modelling and Simulation (ISMS), 2012 Third International Conference on*, pages 214–219. IEEE, 2012.

[17] Susha Surendran, Amira Nassef, and Babak D Beheshti. A survey of cryptographic algorithms for iot devices. In *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, pages 1–8. IEEE, 2018.

[18] Stéphanie Kerckhof and *et al.* Towards green cryptography: a comparison of light ciphers from the energy viewpoint. In *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2012.

[19] Suzan Sallam and *et al.* A survey on lightweight cryptographic algorithms. In *TENCON 2018-2018 IEEE Region 10 Conference*. IEEE, 2018.

[20] Mickaël Cazorla, Kevin Marquet, and Marine Minier. Survey and benchmark of lightweight block ciphers for wireless sensor networks. In *International Conference on Security and Cryptography (SECRYPT)*, 2013.

[21] Maryam El Azhari, Nadya El Moussaid, Ahmed Toumanari, and Rachid Latif. Equalized energy consumption in wban for a prolonged network lifetime. *Wireless Communications and Mobile Computing*, 2017.

[22] Kristtopher Coelho, Danilo Damião, Guevara Noubir, Alex Borges, Michele Nogueira, and José Nacif. Cryptographic algorithms in wearable communications: An empirical analysis. *IEEE Communications Letters*, 23(11):1931–1934, 2019.

[23] Bassam J. Mohd, Thaier Hayajneh, and Athanasios V. Vasilakos. A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues. *Journal of Network and Computer Applications*, 58, 2015.

[24] Junggab Son and *et al.* Fast and accurate machine learning-based malware detection via rc4 ciphertext analysis. In *IEEE ICNC*, 2019.

[25] Murat Dener. Comparison of encryption algorithms in wireless sensor networks. In *ITM Web of Conferences*, volume 22. EDP Sciences, 2018.

[26] Marko Kompara and Marko Hölbl. Survey on security in intra-body area network communication. *Ad Hoc Networks*, 70:23–43, 2018.

[27] UFV, Conselho Técnico de Pós Graduação da Universidade Federal de Viçosa. Normas de redação de teses e dissertações. http://www.dpi.ufv.br/arquivos/ppgcc/doc/PPG-2015-normascorrigidas.pdf, 2018. Accessed: 2018-06-14.

[28] Jeronimo C. Penha, Lucas B. Silva, Jansen M. Silva, Kristtopher K Coelho, Hector P. Baranda, José Augusto M. Nacif, and Ricardo S. Ferreira. Add: Accelerator design and deploy-a tool for fpga high-performance dataflow computing. *Concurrency and Computation: Practice and Experience*, 31(18):e5096, 2019.

[29] Jeronimo Costa Penha, Lucas Bragança, Kristtopher Coelho, Michael Canesche, Jansen Silva, Giovanni Comarela, José Augusto M Nacif, and Ricardo Ferreira. A gpu/fpga-based k-means clustering using a parameterized code generator. In *2018 Symposium on High Performance Computing Systems (WSCAD)*, pages 61–69. IEEE, 2018.

[30] Ricardo Ferreira, Michael Canesche, Kristtopher Coelho, and Jose Nacif. Minimum switching networks. In *2018 VIII Brazilian Symposium on Computing Systems Engineering (SBESC)*, pages 225–230. IEEE, 2018.

[31] Ana Cláudia MP da Costa, Kristtopher Kayo Coelho, Jeronimo Costa Penha, Ricardo dos Santos Ferreira, and José Augusto M Nacif. Ensino de arquitetura e as predições tomadas por desempenho com as predições não tomadas pela

segurança: Vulnerabilidades meltdown e spectre. *International Journal of Computer Architecture Education (IJCAE)*, 2018.

[32] Christopher C Cheung, Andrew D Krahn, and Jason G Andrade. The emerging role of wearable technologies in detection of arrhythmia. *Canadian Journal of Cardiology*, 34(8):1083–1087, 2018.

[33] Yan Li, Zicheng Chi, Xin Liu, and Ting Zhu. Passive-zigbee: Enabling zigbee communication in iot networks with 1000x+ less power consumption. In *ACM SenSys*, pages 159–171, 2018.

[34] Tarsila Bessa, Christopher Gull, Pedro Quintão, Michael Frank, José Nacif, and Fernando Magno Quintão Pereira. Jetsonleap: A framework to measure power on a heterogeneous system-on-a-chip device. *Science of Computer Programming*, 2017.

[35] Bassam J Mohd and *et al.* Lightweight block ciphers for iot: Energy optimization and survivability techniques. *IEEE Access*, 6, 2018.

[36] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[37] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Second Edition*. Chapman & Hall/CRC, 2nd edition, 2014.

[38] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. *Journal of Cryptology*, 18(4):291–311, 2005.

[39] Lars R Knudsen and *et al.* On the design and security of RC2. In *International Workshop on Fast Software Encryption*. Springer, 1998.

[40] Yehya A Nasser and *et al.* AES algorithm implementation for a simple low cost portable 8-bit microcontroller. In *IEEE ICDIPC*, 2016.

[41] Michel Goraczko and *et al.* Energy-optimal software partitioning in heterogeneous multiprocessor embedded systems. In *Annual Design Automation Conference*, pages 191–196. ACM, 2008.

[42] Piotr Luszczek, Ichitaro Yamazaki, and Jack Dongarra. Increasing accuracy of iterative refinement in limited floating-point arithmetic on half-precision accelerators. In *2019 IEEE High Performance Extreme Computing Conference (HPEC)*, pages 1–6. IEEE, 2019.

[43] Ramakrishna Dantu, Indika Dissanayake, and Sridhar Nerur. Exploratory analysis of internet of things (iot) in healthcare: A topic modeling approach. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[44] Paola Mosconi, Silvia Radrezza, Emanuele Lettieri, and Eugenio Santoro. Use of health apps and wearable devices: Survey among italian associations for patient advocacy. *JMIR mHealth and uHealth*, 7(1):e10242, 2019.

[45] William J Tomlinson, Stella Banou, Christopher Yu, Michele Nogueira, and Kaushik R Chowdhury. Secure on-skin biometric signal transmission using galvanic coupling. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, pages 1135–1143. IEEE, 2019.

[46] Anurag Tewari and Prabhat Verma. Security and privacy in e-healthcare monitoring with wban: A critical review. *International Journal of Computer Applications*, 136(11), 2016.

[47] Aftab Ali and Farrukh Aslam Khan. An improved ekg-based key agreement scheme for body area networks. In *International Conference on Information Security and Assurance*, pages 298–308. Springer, 2010.

[48] Marc Simon Wegmueller, Sonja Huclova, and et al. Galvanic coupling enabling wireless implant communications. *IEEE Transactions on Instrumentation and Measurement*, 58(8):2618–2625, 2009.

[49] Marc Simon Wegmueller, Michael Oberle, Norbert Felber, Niels Kuster, and Wolfgang Fichtner. Signal transmission by galvanic coupling through the human body. *IEEE Transactions on Instrumentation and Measurement*, 59(4):963–969, 2009.

[50] Marc S Wegmüller. *Intra-body communication for biomedical sensor networks*. PhD thesis, ETH Zurich, 2007.

[51] Alistair EW Johnson, Tom J Pollard, Lu Shen, H Lehman Li-wei, Mengling Feng, Mohammad Ghassemi, Benjamin Moody, Peter Szolovits, Leo Anthony Celi, and Roger G Mark. Mimic-iii, a freely accessible critical care database. *Scientific data*, 3:160035, 2016.

[52] Fernando Nakayama, Bruno Cremonezi, Aldri Luiz dos Santos, Michele Nogueira, Kaushik Chowdhoury, Stella Banou, Eduardo Coelho Cerqueira, et al. Autenticação contínua e segura baseada em sinais ppg e comunicação galvânica. In *Anais do XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 707–720. SBC, 2019.

[53] William J *et al.* Tomlinson. Experimental assessment of human-body-like tissue as a communication channel for galvanic coupling. In *IEEE Int. Conference on Wearable and Implantable Body Sensor Networks (BSN)*, 2015.

Apêndice A

Evaluating the Skin as a Secure Communication Medium

A.1 Introduction

Estimations point out that in 2020 there will be more than 20 billion connected "things", where around 40% will be telemedicine-related, making up a $117 billion market. For 2025, this number of devices can reach 75 billion [43]. Furthermore, it is also estimated that 35 zettabytes of clinical data will be produced and often be transmitted and stored on physical media [44], which rises several concerns about security, privacy, integrity, and confidentiality of a patient clinical data at any moment. In this work, we evaluate the skin as a secure channel to transmit sensitive data such as cryptography keys. We can generate these key by using vital signals, such as ECG, and share between devices through a secondary and secure medium (the human skin). In this application scenario, we can provide more security and solve the management problem of secret key cryptographic algorithms.

A.2 Methodology

Fig. A.1 illustrates the complete application model we consider in this work. In the test scenario (A.1B), we have the microcontroller, the Differential Driver and a Sensing Amplifier. The Differential Driver couples the signal to the physical environment through a 1 mA differential current. The Sensing Amplifier provides a gain of one thousand times. We use swine tissue as the physical medium, once it presents similar human tissue dielectric properties [53]. The experiments were performed by varying the electrodes distance by 2, 5, 10, 15, and 20 cm between Driver and Amplifier. In addition, we have varied the physical environment settings between skin-skin, skin-muscle, and muscle-muscle. Online decoding (A.1C) demands several floating-point operations for assessing the filter outputs and adaptive threshold, in order to recover data bits. Such capabilities are not available in cost-effective microcontrolers. For this reason, we conducted our analysis based on offline decoding.

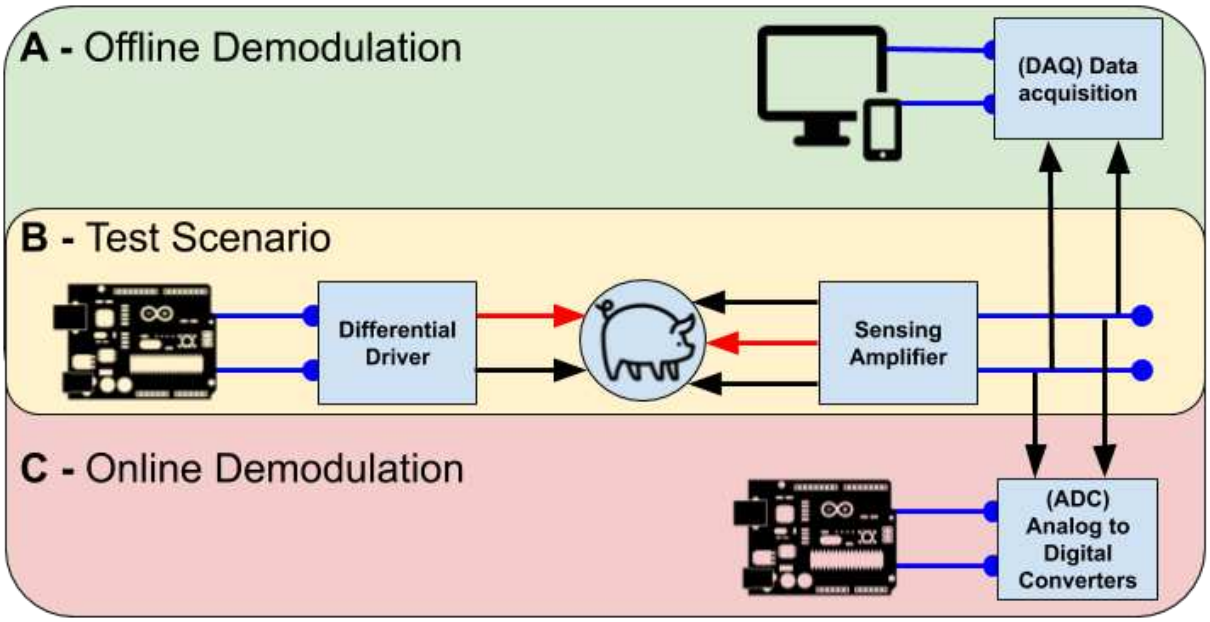


Figura A.1: Data transmission scenario.

A.3 Preliminary Results

Table A.1 presents our preliminary results for communication distances considering skin-skin, skin-muscle, and muscle-muscle physical mediums. We notice that even with variations of physical environment settings, the communication is limited to lengths of less than 15 cm. Besides, the channel presents a data transmission rate of more than 9,600 bps in all physical medium combinations.

Tabela A.1: Signal propagation distances.

Communication medium	Length (cm)
Skin-skin	2-5
Skin-muscle	10
Muscle-muscle	10-15

A.4 Conclusion

In this work, we investigated the feasibility of using the skin as a secure communication medium. In the case of skin-skin communication, for short lengths (2-5 cm), we observe a bandwidth of 9,600 bps. To this end, we used Differential Driver and Sensing Amplifier circuits. As future work, there is the possibility to present an evaluation regarding the error rate, data loss, and signal attenuation. We are also evaluating other options for increasing the data transmission rate for online decoding.