UM NOVO PROTOCOLO DE INTEROPERABILIDADE PARA REDES BIOMÉTRICAS, APRIMORANDO A SEGURANÇA E PRIVACIDADE POR MEIO DE TÉCNICAS CRIPTOGRÁFICAS

EDUARDO MAGALHÃES DE LACERDA FILHO

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UM NOVO PROTOCOLO DE INTEROPERABILIDADE PARA REDES BIOMÉTRICAS, APRIMORANDO A SEGURANÇA E PRIVACIDADE POR MEIO DE TÉCNICAS CRIPTOGRÁFICAS

EDUARDO MAGALHÃES DE LACERDA FILHO

ORIENTADOR: VINÍCIUS P. GONÇALVES, DR.

DISSERTAÇÃO DE MESTRADO EM
ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGEE.DM-760/21

BRASÍLIA/DF: DEZEMBRO - 2020

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UM NOVO PROTOCOLO DE INTEROPERABILIDADE PARA REDES BIOMÉTRICAS, APRIMORANDO A SEGURANÇA E PRIVACIDADE POR MEIO DE TÉCNICAS CRIPTOGRÁFICAS

EDUARDO MAGALHÃES DE LACERDA FILHO

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

_____

Prof. Dr. Vinícius P. Gonçalves – ENE/Universidade de Brasília
Orientador

_____

Prof. Dr. Rafael Timóteo de Sousa Junior – ENE/Universidade de Brasília
Membro Interno

_____

Dra. Thienne Johnson – Universidade do Arizona
Membro Externo

BRASÍLIA, 22 DE DEZEMBRO DE 2020.

FICHA CATALOGRÁFICA

LACERDA FILHO, EDUARDO
Um novo protocolo de interoperabilidade para redes biométricas, aprimorando a segurança e privacidade por meio de técnicas criptográficas [Distrito Federal] 2020.
xii, 91p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2020).
Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Biometria	2. Segurança
3. Privacidade	4. Interoperabilidade
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

LACERDA FILHO, E. (2020). Um novo protocolo de interoperabilidade para redes biométricas, aprimorando a segurança e privacidade por meio de técnicas criptográficas . Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGEE.DM-760/21, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 91p.

CESSÃO DE DIREITOS

AUTOR: Eduardo Magalhães de Lacerda Filho
TÍTULO: Um novo protocolo de interoperabilidade para redes biométricas, aprimorando a segurança e privacidade por meio de técnicas criptográficas .
GRAU: Mestre ANO: 2020

É concedida à Universidade de Brasília permissão para reproduzir cópias desta dissertação de mestrado e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. O autor reserva outros direitos de publicação e nenhuma parte dessa dissertação de mestrado pode ser reproduzida sem autorização por escrito do autor.

Eduardo Magalhães de Lacerda Filho

Departamento de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

À Fernanda e ao nosso anjo Miguel

AGRADECIMENTOS

Nessa jornada acadêmica, de muita dedidação, estudo, alegrias e aprendizado, tenho que agradecer, inicialmente, à Deus pela saúde e felicidade da minha família, amigos, colegas, professores e demais que me acompanharam nesta jornada.

Agradecer à minha linda esposa Fernanda, por tudo que fez e faz para minha vida e família. Presente quando eu estava ausente para cuidar dessa jornada, desse ciclo que muitas vezes me tirou do convívio do nosso filho, família e amigos. Eu queria encontrar palavras de agradecimento, mas não consigo expressar minha gratidão a você. Eu te amo.

À minha mãe e ao meu pai. Não há um passo que eu não vá me lembrar das duas pessoas que me proporcionaram chegar até onde cheguei. Ao meu irmão, cunhada, e minha linda e amável sobrinha Olívia, pelo amor incondicional, pela felicidade que é ter vocês nos nossos pensamentos, na qual a distância física nunca afastou essa alegria de poder participar uns dos outros de nossas vidas. Eu amo todos vocês.

À minha família e amigos por serem tão especiais. Obrigado por todos os momentos maravilhosos vividos. Obrigado pela torcida e incentivo.

Ao meu orientador, Professor Vinicius, no qual estendo meus cumprimentos a todo corpo docente do PPGEE e meus colegas. Obrigado, professor, por dedicar seu tempo a esta pesquisa e compartilhar seu conhecimento. Talvez, não há nada melhor para um professor do que ver seu aluno crescendo em suas habilidades e entendimento. Você é responsável direto pelos nossos resultados, publicações e por esta dissertação.

Finalmente, ao meu filho Miguel. Ser pai é o maior momento da minha vida, pelo imenso amor, felicidade, transformação, dedicação, cuidado, preocupações e responsabilidades. Tudo se torna maior e mais relevante por você. Tudo se compreende, tudo se aprende. Quando você, meu filho, puder ler e compreender essas palavras, lembre-se: você é o maior tesouro da minha vida!

RESUMO

Título: Um novo protocolo de interoperabilidade para redes biométricas, aprimorando a segurança e privacidade por meio de técnicas criptográficas
Autor: Eduardo Magalhães de Lacerda Filho
Orientador: Vinícius P. Gonçalves, Dr.
Programa de Pós-Graduação em Engenharia Elétrica
Brasília, 22 de dezembro de 2020

Melhorar a segurança, privacidade e interoperabilidade de redes e protocolos biométricos tem sido um desafio para muitos trabalhos de pesquisa por muitos anos. As várias abordagens propostas ainda precisam integrar essas três características, além de mostrar evidências de segurança para as aplicações biométricas. Nesse sentido, esta pesquisa propõe um esquema probabilístico para cifrar índices de bancos de dados biométricos e uma nova abordagem para interoperabilidade entre sistemas que intercambiam dados biométricos, aprimorando, *e.g.*, o IEEE Biometric Open Protocol Standard. Dessa forma, destaca-se duas melhorias significativas por meio desta pesquisa quando comparada a trabalhos relacionados. A primeira vem das técnicas criptográficas e esquemas de rede propostos. Implica uma probabilidade insignificante de ataques conhecidos terem sucesso contra a proposta, devido às suas evidências de segurança semântica, bem como as dificuldades que impõe aos ataques, dadas as barreiras de alta complexidade que são inviáveis para o invasor quebrar em tempo polinomial. Nestas técnicas, inclui-se um vetor de inicialização modificado e um parâmetro único aleatório para o algoritmo de encriptação. A segunda melhoria compreende o novo protocolo de interoperabilidade, escrito na forma de uma Interface de Programação de Aplicativos, com procedimentos de integridade e controle de solicitações de identificação biométrica que aumentam a confiabilidade do sistema e contribuem para fins de interoperabilidade. Como conclusão deste trabalho, mostra-se a análise de segurança, as provas e os resultados das constribuições, que demonstram que a nova rede biométrica proposta é precisa em relação à integridade e interoperabilidade, preservando o anonimato das pessoas cujos dados biométricos são trocados na rede e armazenados nos bancos de dados relacionados.

Palvras Chave: Biometria, Segurança, Privacidade, Interoperabilidade.

ABSTRACT

Title: A new interoperability protocol for biometric networks, improving security and privacy through cryptographic techniques.
Author: Eduardo Magalhães de Lacerda Filho
Supervisor: Vinícius P. Gonçalves, Dr.
Graduate Program in Electrical Engineering
Brasília, December 22nd, 2020

Improving the security, privacy, and interoperability of biometric networks and protocols has been a challenge for many research papers for many years. The various proposed approaches still need to integrate these three characteristics and show security evidence for biometric applications. In this sense, this research proposes a probabilistic scheme to encrypt biometric database indexes and a new approach for interoperability between systems that exchange biometric data, improving, *e.g.*, the IEEE Biometric Open Protocol Standard. Two significant improvements in this research stand out when compared to related works. The first comes from the proposed cryptographic techniques and network schemes. It implies an insignificant probability of known attacks being successful against the proposal due to its evidence of semantic security and the difficulties it imposes on attacks, given the high complexity barriers that are not viable for the attacker to break in polynomial time. These techniques include a modified initialization vector and a single random parameter for the encryption algorithm. The second improvement comprises the new interoperability protocol, written in the form of an Application Programming Interface, with integrity and control procedures for biometric identification requests that increase system reliability and contribute to interoperability purposes. As a conclusion of this work, it shows the security analysis, evidence, and results that show that the proposed new biometric network is accurate in terms of integrity and interoperability, preserving people's anonymity whose biometric data is exchanged on the network and stored in the related databases.

Keywords: Biometrics, Security, Privacy, Interoperability.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

Sistemas biométricos automatizados para comprovação da identidade de um indivíduo são amplamente utilizados em diversos segmentos de uma sociedade [2]. Esses segmentos, sob controle de entidades públicas e privadas, possuem aplicações com uso de biometria, *e.g.*, na emissão de passaportes e serviços de imigração, na abertura de contas e transações no sistema financeiro, na aquisição de benefícios sociais, no provimento de certificados digitais por meio das Autoridades Certificadoras, na habilitação de eleitores para votação em urna eletrônica, no comércio, entre outros. Nesse sentido, diversos países e organizações normatizaram seus processos biométricos para que, com a acurácia necessária, esses sistemas fossem úteis e eficazes no combate à fraude por falsa identidade e na correta comprovação biométrica de uma pessoa.

Essas normativas descrevem como devem funcionar os sistemas biométricos desde a coleta aos processos de comparação, transação e guarda dos dados biométricos. Esses dados podem ser impressões digitais, face, íris, voz, DNA, entre outras biometrias, com diferentes formatos digitais para cada um deles. Para maior acurária e eficácia de uma identificação (1:n) ou uma verificação (1:1) biométrica é necessário o uso de mais de uma biometria dentro dos motores, *i.e.*, a tecnologia de comparação biométrica, e, por consequência, dos bancos de dados biométricos. A acurácia dos algoritmos de comparação tem aumentado ao longo dos anos, o que permite a ampliação eficiente do uso dessas biometrias na identificação e verificação de pessoas. Ademais, as normativas procuram dotar estes sistemas de algum fator de segurança e privacidade ou interoperabilidade para o conjunto de informações biográficas, *i.e.*, relacionadas ao nome, número social, data de nascimento, entre outras, e biométricas, no intuito de preservar as informações coletadas, transacionadas e armazenadas.

Segurança, privacidade e interoperabilidade são três características desafiadoras para redes biométricas. Para provê-las dentro das redes biométricas são utilizados os denominados Provedores de Serviços Biométricos (PSB), que são as entidades que prestam serviços de identificação e verificação. A dificuldade está em superar esses três desafios ao mesmo tempo dentro de uma rede. Nesse cenário, normalmente um segmento da sociedade ou está usando diferentes tecnologias biométricas sem qualquer procedimento de interoperabilidade e garantia de privacidade entre os dados, ou está usando a mesma tecnologia, *e.g.*, o mesmo esquema de modelos (*templates*) biométricos, que usualmente são proprietários e fechados. Esse cenário é uma consequência da falta de protocolos de comunicação seguros para interoperabilidade entre diferentes tecnologias biométricas e que possam manter, com segurança, a privacidade dos dados biográficos e biométricos dos indivíduos, tanto no seu armazenamento quanto nas transações realizadas.

Alguns esforços para prover esse tipo de solução existem. Cita-se mais destacadamente o protocolo *IEEE Biometric Open Protocol Standard* (IEEE BOPS) [3] e o formato de campos especificado pelo *American National Standard for Information/National Institute of Standards and Technology* (ANSI/NIST) [4]. Entretanto, não há indícios de trabalhos publicados que consigam juntar as questões de interoperabilidade com segurança e privacidade, com evidências que o sistema possui probabilidade insignificante de ser atacado com sucesso. Portanto, torna-se fundamental desenvolver uma abordagem que consiga superar os três desafios ao mesmo tempo, com provas que o sistema biométrico é seguro o suficiente contra qualquer adversário $\mathcal{A}$.

1.1 MOTIVAÇÃO E JUSTIFICATIVA DA PESQUISA

Por muitos anos, a principal abordagem para segurança e privacidade de redes biométricas tem sido a aplicação de técnicas de modelos biométricos [2, 5, 6, 7, 8, 9]. O trabalho de Ross *et al.* [10] promoveu muitas pesquisas para lidar com a proteção de modelos usando criptossistemas biométricos [11, 12, 13, 14, 15, 16, 17, 18] e técnicas de biometria cancelável (*cancelable biometric*) [19, 20, 21, 22], também chamada de transformação de ferramenta biométrica. Alguns desses trabalhos também incluem ferramentas para autenticação, segurança de rede e capacidade de processamento. Apesar da evolução dos trabalhos nesse cenário de modelos biométricos, alguns deles possuem alguns inconvenientes, incluindo falhas na implementação de *hardware*, suscetíveis a ataques de ligação, ataques de força bruta, ataques de canal lateral, problema de nível de privacidade contra a Taxa de Aceitação Falsa (*False Acceptance Rate*), entre outros [23, 24, 25, 26, 27]. Além disso, mesmo com o uso do IEEE BOPS, ou simplesmente do formato ANSI/NIST, não é possível usar cada um desses modelos em diferentes bases biométricas e fazê-los se comunicar, com uma prova de segurança razoável e sem comprometer a privacidade dos dados de uma pessoa.

Outro ponto relevante é que redes e bancos de dados biométricos inseguros e comprometidos, sem a devida prova de segurança, podem irreversivelmente levar ao extravio de identidade. Essa é uma característica intrínseca ao uso de dados biométricos em transações, visto que a biometria útil em sistemas de identificação e verificação automatizados é aquela que tem por caraterística fundamental a perenidade na sua composição. Neste contexto de uso de dados biométricos e crescente preocupação com a privacidade, foram propostas leis para proteger os dados pessoais, impondo soluções para mitigar o problema de ataques e vazamentos aos mesmos [28, 29]. Esse cenário torna-se mais complexo, visto que, e cada vez mais, diferentes bases biométricas, principalmente as públicas, possuem mais de uma biometria armazenada e transacionada. Qualquer estudo, pesquisa, trabalho e implementação que vise a adoção de sistemas biométricos deve, com o devido rigor, endereçar os ditâmes

legais e infralegais impostos para cada país.

Dado o exposto, relata-se a questão que esta dissertação irá endereçar. O problema de pesquisa que direciona este trabalho é a falta de protocolos e esquemas seguros para fazer com que diferentes sistemas biométricos se comuniquem e, ainda sim, garantam a privacidade de dados individuais contra ataques conhecidos. Este trabalho propõe a resolução deste problema com uma nova abordagem que não se concentra na tecnologia de modelos biométricos para resolver as questões de segurança do banco de dados e das transações biométricas. Tampouco utiliza-se somente dos protocolos de comunicação existentes, por ora citados. Este trabalho constrói um esquema que anonimiza os registros nos bancos de dados e transações dos PSB, aprimorando a segurança, mantendo a privacidade, e um conjunto de técnicas de comunicação para interoperabilidade e integridade entre os dados que são transacionados na rede, entre diferentes sistemas biométricos.

Para essa contrução, é criado um esquema que propõe duas aproximações, a saber: a) uso de técnicas criptográficas para encriptação de dados; e, b) um protocolo de comunicação biométrico. Cria-se um algoritmo probabilístico com primitivas de chaves simétricas e usa-se técnicas de primitivas de chaves públicas para o provimento das garantias necessárias à segurança e proteção do sistema. Ademais, implementa-se um novo protocolo de comunicação para interoperabilidade e integridade dos dados, usando concomitantemente protocolos de rede e formatação para troca de dados. O algoritmo destina-se para a anonimização dos dados indexados no armazenamento do banco de dados e das transações na rede. Os cálculos são realizados dentro da área criptográfica protegida dos *Hardware Secure Modules* (HSM), equipamentos especializados no uso de componentes criptográficos, que estão localizados dentro de ambientes seguros e auditáveis, para melhor controle e segurança física e lógica dos componentes utilizados.

A segunda aproximação aborda o novo protocolo de comunicação. Este destina-se a, com integridade das informações trocadas, fazer com que diferentes tecnologias biométricas, que utilizam diferentes modelos biométricos, possam interagir seus dados anonimizados, criados pelo algoritmo mencionado. As especificações podem, *e.g.*, ser inseridas no IEEE BOPS [3]. Para validar o esquema proposto, fez-se uma criptoanálise do algoritmo criado e das técnicas de encriptação com chaves públicas, assim como uma análise dos processos de rede implementados, baseados nas probabilidades de realização de um ataque bem sucedido. Ademais, fez-se uma implementação de um projeto com dois PSB ativos dentro dos laboratórios do Instituto Nacional de Tecnologia da Informação - ITI, convalidando o modelo proposto, nos quais os resultados serão apresentados nesta dissertação.

As provas e avaliações mostrarão a segurança da proposta. As técnicas criptográficas usadas para encriptar todos os registros são invioláveis de serem quebradas em tempo polinomial, mantendo o anonimato de uma pessoa. Além disso, este trabalho tem uma comparação completa entre outros criptossistemas e transformações de ferramentas biométricos que

funcionam para uma melhor visualização da inovação desta pesquisa. Os resultados denotam que a rede biométrica tem boa eficiência quanto a completude e integridade de transações realizadas entre PSB.

A justificativa da pesquisa apresentada pretende entregar um esquema que torna qualquer sistema biométrico anônimo, interoperável e íntegro entre qualquer tecnologia. Isso permite que não hajam mais problemas com: 1) tecnologias proprietárias; 2) vazamento de dados que permitam o extravio da identitidade de uma pessoa; 3) troca de informações de clientes ou cidadãos, visto que agora todas essas são anônimas. Resumindo, pretende-se resolver o desafio que é agregar, ao mesmo tempo, e até onde se tem conhecimento é o primeiro trabalho nesse sentido, segurança, privacidade e interoperabilidade entre diferentes sistemas biométricos.

A presente pesquisa pode ser considerada como uma pesquisa aplicada e de desenvolvimento [1]. É uma pesquisa aplicada visto que se insere no ambiente acadêmico e profissional para resolver um problema que afeta sistemas biométricos de governos e iniciativa privada pelo mundo. Ademais, é uma pesquisa de desenvolvimento visto que agrega aproximações novas tanto no algortimo criptográfico criado como no protocolo de comunicação entre redes biométricas.

1.2 OBJETIVOS

O objetivo da pesquisa é desenvolver um protocolo de comunicação biométrico interoperável que garanta a segurança e privacidade dos dados provinientes das coletas das informações dos indivíduos, tanto no aramzenamento quanto nas transações entre os sistemas biométricos.

1.2.1 Objetivos Específicos

Os objetivos específicos são:

- Criar um algoritmo de primitivas de chaves simétricas para anonimizar os dados indexados dos bancos de dados e transacionados dos PSB;
- Definir um algoritmo de primitivas de chaves públicas para garantia de exportação e importação das chaves secretas e encriptar os dados biométricos que transacionam entre os PSB;
- Desenvolver uma arquitetura de rede entre os PSB para que os processos de identificação e verificação biométricos sejam realizados com os dados anonimizados e que garantam a integridade, privacidade e segurança de todos os dados.

1.3 HIPÓTESE

Descreve-se a hipótese que permeia essa dissertação. Em relação aos objetivos listados na seção anterior, a hipótese principal desta pesquisa é atribuir a redes biométricas privacidade dos dados que são armazenados e transacionados, implementando diversas técnicas para deixar a arquitetura segura, e fazer com que os dados e as transações sejam interoperáveis, com processos que mantenham a integridade das operações. As hipóteses secundárias são:

- Diminuir a dependência de tecnologias e processos proprietários e fechados em redes biométricas;
- Atender aos requisitos impostos por leis de proteção de dados, que versam sobre privacidade e uso dos dados pessoais.

1.4 CONTRIBUIÇÕES

As contribuições desta dissertação são:

(1) Criação de um algoritmo probabilístico de encriptação dos dados de um indivíduo no bando de dados de um PSB, baseado no AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) [30], com chave secreta simétrica `k` de 256 bits (AES-256-CBC), modificado por um vetor de inicialização aleatório (`iv`) e um parâmetro de número único `nonce` para cada entrada, e um algoritmo de *hash* de função unidirecional (SHA-2 - *Secure Hash Algorithm* de 256 bits) [31], embarcado em um HSM [32, 33] FIPS (*Federal Information Processing Standard*) [34], instalado em um ambiente seguro e auditado (ITI).

(2) Uso de um algoritmo de encriptação com primitivas de chaves públicas, baseado no RSA-OAEP (Rivest-Shamir-Adleman-Optimal Asymmetric Encryption Padding) [35], com chave de 2048 bits (RSA-2048-OAEP), para o processo de exportação e importação da chave secreta `k` e das transações entre PSB.

(3) Desenvolvimento um protocolo de comunicação, por meio da construção de uma API (*Application Programming Interface*), que destina-se a dar interoperabilidade e integridade às transações realizadas na rede dos PSB, baseado em HTTPS (Hyper Text Transfer Protocol Secure) [36] e na linguagem JSON [37].

A primeira contribuição cria um algortimo denominado de IDN. Ele se baseia na chave secreta `k`, na identificação social exclusiva de um cidadão, para esta pesquisa o `CPF` (Cadastro de Pessoa Física), e um Número de Código de Tempo (`TCN` - *Time Code Number*) para o cálculo do parâmetro `nonce`. Esse anonimato é garantido usando AES-256-CBC modificado por um `iv` aleatório e gerado localmente, dentro de cada HSM dos PSB, pela chave

secreta k e pelo CPF, além de um parâmetro nonce, também aleatório e gerado localmente, dentro de cada HSM dos PSB, pela chave secreta k e pelo TCN, modificando a saída do AES-256-CBC. Usando o próprio HSM incorporado em um ambiente seguro e com certificação FIPS, os diferentes PSB na rede podem calcular e verificar a mesma sequência de IDN que representa o detentor (CPF) de uma biometria inequivocamente, sem enviar pela rede o iv ou o nonce, o que torna o algoritmo inovador. O propósito do algoritmo é garantir o anonimato de qualquer dado biográfico de uma pessoa na base de dados dos PSB, incluindo a segurança semântica, dada pelas análises e resultados probabilísticos que provam e mantém essa condição.

A segunda contribuição usa conceitos relativos à encriptação utilizando primitivas de chaves públicas. Para tal, usa-se a chave pública do HSM de cada PSB para que se faça uma operação RSA-2048-OAEP. Esta operação destina-se a duas operações, a saber: 1) a primeira relaciona a exportação cifrada da chave secreta k do HSM offline confiável (terceira parte confiável), que gera a mesma, para os HSM de cada PSB; e 2) a segunda relaciona com a comunicação encriptada entre os PSB. Essa operação garante que somente os PSB conhecidos na rede, possam ter a chave secreta k e operar dentro da arquitetura de rede proposta.

A terceira contribuição desenvolve um protocolo de interoperabilidade, permitindo a comunicação segura com diferentes tecnologias de PSB. É garantida a interoperabilidade e integridade entre os sistemas biométricos que trocam o índice criptografado, chamado IDN, mantendo a premissa de não descriptografá-lo. O objetivo deste novo protocolo é produzir melhor desempenho da rede para identificação (1:n) e a construção de um mecanismo de cache que aprimore a agilidade da rede na produção das respostas necessárias. É construída uma API representativa dessa contribuição, apresentada no Apêndice A. A evidência de segurança dos procedimentos de rede e dos resultados provam que o protocolo é seguro o suficiente e é possível interoperar qualquer pacote biométrico no PSB.

Algumas premissas são adotadas para os resultados das contribuições mencionadas. Para os cálculos de registros anônimos (IDN), encriptação de chaves públicas e o armazenamento de chaves simétricas, é obrigatório o uso de dispositivos HSM [33] incorporados em um ambiente seguro e com certificação FIPS [34]. O HSM permite abordar a segurança física e lógica dos ativos digitais armazenados e executa cálculos criptográficos mais rapidamente. Além disso, o HSM possui um recurso importante que não permite que um ativo, uma vez importado, seja copiado ou exportado, habilitando-se, somente, o uso desse ativo (como uma chave simétrica) sem poder modificá-lo. Outra premissa é que o protocolo de comunicação usa o pacote biométrico baseado em ANSI/NIST [4]. Esse padrão é amplamente usado por sistemas biométricos e permite que os formatos e campos de informação sejam integrados, incluindo respostas correspondentes da biometria que passam pelo processo de identificação ou verificação. Por fim, um país, estado ou segmento deve ter um identificador biográfico,

i.e., uma sequência de caracteres individual, como nome, número social, registro de nascimento, entre outros. Um registro de sequência individual permite que o IDN seja o elemento representativo de uma pessoa no compartilhamento entre os sistemas biométricos.

1.5 MÉTODO DA PESQUISA

Este projeto de pesquisa se alicerçou na construção de diferentes fases para consecução dos objetivos. O método de pesquisa que se adequa nesta construção é o baseado no *Design Science* [1]. A Figura 1.1 mostra o processo de pesquisa adotado nesta dissertação.

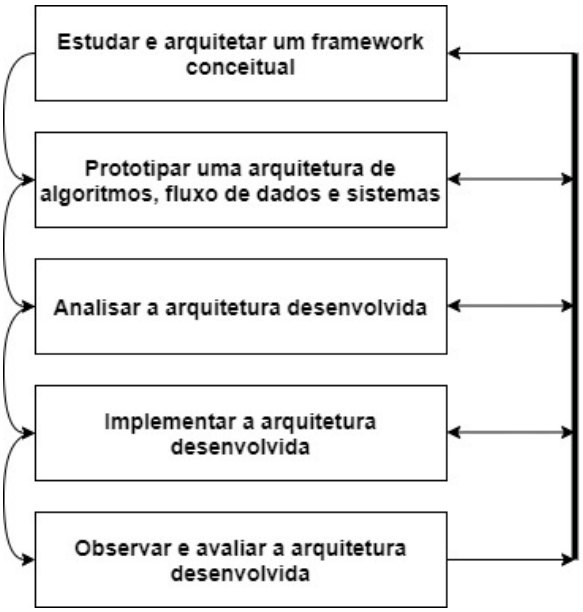

Figura 1.1 – Processos de pesquisa. Adaptado de [1]

Adere-se a linha de pesquisa de múltiplos conceitos. Isso é refletido pelo uso da teoria dos números, teoria da probabilidade, aplicação de criptografia em sistemas e códigos, protocolos de texto, linguagens de programação e biometria. Todos eles são utilizados com o propósito de promover a segurança, a privacidade e a interoperabilidade de dados em uma rede biométrica. As atividades desta pesquisa consistiram em seis fases principais, a saber: (1) definir o escopo do problema que se quer resolver, (2) estabelecer a formalização da estrutura, (3) prototipar a arquitetura do sistema, (4) analisar o sistema, (5) implementar o sistema e (6) analisar os resultados. Neste contexto, segue a descrição detalhada destas fases:

- Fase 1: Descrição da situação atual e dos problemas que afetam as redes biométricas;
- Fase 2: Detalhamento da teoria e da arquitetura conceitual, com aplicação de múltiplos conceitos baseados em criptografia, protocolos de comunicação e linguagem computacional para consecução da pesquisa;

- Fase 3: Escrita dos algoritmos em linguagem de programação definida e prototipação da arquitetura conceitual da rede biométrica;
- Fase 4: Análise conceitual do algoritmo e da arquitetura prototipada;
- Fase 5: Implementação em laboratório da arquitetura proposta; e
- Fase 6: Apresentação e análise dos resultados obtidos em laboratório, inclusive comparativa em relação à outros trabalhos, com os ganhos da perspectiva desta pesquisa.

1.6 ESTRUTURA DO TRABALHO

O restante desta dissetarção está dividida nas seguintes partes:

- O Capítulo 2 descreve, em termos matemáticos e de arquitetura de rede, a teoria utilizada para esta pesquisa. https://www.overleaf.com/project/5f81dc3642667c0001a3cb0c
- O Capítulo 3 apresenta os trabalhos mais relevantes relacionados a esta pesquisa direcionados a aspectos de segurança, privacidade e interoperabilidade de redes biométricas.
- Apresenta-se a proposta da pesquisa no Capítulo 4, em que discorre-se sobre o esquema de encriptação criado e a arquitetura da rede biométrica, com os pacotes relacionados.
- O Capítulo 5 mostra toda a análise de segurança da proposta.
- Os resultados são apresentados e discutidos no Capítulo 6.
- Finalmente, no Capítulo 7, conclui-se o trabalho, indicando trabalhos futuros para sequência desta pesquisa.

2 REFERENCIAL TEÓRICO

Neste Capítulo serão apresentados conceitos teóricos relacionados a esta pesquisa. Essencialmente, serão abordados a teoria de primitivas de chaves simétrica e pública, a algoritmo unidirecional SHA-256, a entropia de um gerador de números aleatórios e a linguagem de programação JSON. O objetivo do Capítulo é positivar a teoria matemática, os conceitos criptográficos e de linguagem de programação que compõem a arquitetura proposta. A metodologia utilizada para este Capítulo foi colacionar definições para os esquemas utilizados.

2.1 PRIMITIVA DE CHAVE SIMÉTRICA

Nesta seção serão definidos os conceitos de encriptação de chave simétrica e sua respectiva segurança. Após, será detalhada a teoria do AES em modo CBC, visto a utilização deste na criação do algoritmo de anonimização dos registros (IDN), conforme será abordado no Capítulo 4.

2.1.1 Esquema de encriptação de chave simétrica

DEFINIÇÃO 2.1 (Esquema de encriptação de chave simétrica [38]) Um esquema de encriptação de chave simétrica é definido por uma chave secreta $\mathtt{k} \in \{0,1\}^k$ e um texto em claro $\mathtt{m} \in \{0,1\}^m$. Um texto encriptado ou cifrado $\mathtt{c} \in \{0,1\}^c$ é um par probabilístico de (Enc, Dec), onde $\mathsf{Enc}(\mathtt{k},\mathtt{m}) \rightarrow \mathtt{c}$, $\mathsf{Dec}(\mathtt{k},\mathtt{c}) \rightarrow \mathtt{m}$ e para qualquer mensagem $\in M$ e $k \in \{0,1\}^k$ leva a $\Pr[\mathsf{Dec}(k, \mathsf{Enc}(k, M)) = M] = 1$.

2.1.2 Segurança da encriptação de chave simétrica

DEFINIÇÃO 2.2 (Segurança da encriptação de chave simétrica [38]) A segurança de um esquema de encriptação simétrica é alcançado quando, *e.g.*, para duas mensagens $\mathtt{m}$, $\mathtt{m'}$, as distribuições de probabilidades de $\mathsf{Enc}(\mathtt{m})$ e $\mathsf{Enc}(\mathtt{m'})$ na execução de um algoritmo são as mesmas, com resultados diferentes.

2.1.3 AES

O AES é um algoritmo simétrico de encriptação. O principal objetivo é trasnsformar um texto em claro (X), em uma saída cifrada (Y), que só possa ser revertida para quem possui uma chave secreta (K). A Figura 2.1 abstrai esse objetivo comentado. O entendimento detalhado deste algortimo se faz necessário, visto que é nele que está baseada o esquema do algortimo IDN criado, assim como a modificação no vetor de inicialização e o parâmetro de número único proposto neste trabalho na saída da cifra AES.

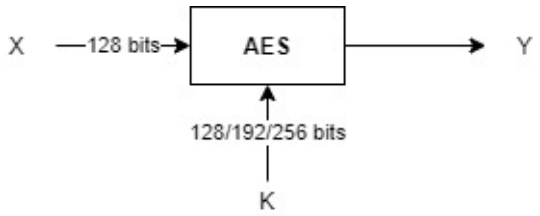

Figura 2.1 – AES.

2.1.3.1 Campos Finitos

Todas as operações internas do AES são baseadas na teoria dos Campos Finitos (*Finite Fields* - FF), também conhecidos como Campos de Galois (*Galois Fields* - GF) [39]. Destaca-se que em criptografia quase sempre necessita-se de uma configuração finita do Campo. Antes da definição do que é Campo, aborda-se o conceito de Grupo.

DEFINIÇÃO 2.3 (Grupo) Grupo é o conjunto de elementos G que, juntos com uma operação "o", combinam dois elementos em G. Um Grupo tem as seguintes propriedades:

- A operação do Grupo "o" é fechada, *i.e*, para todos a, b $\in$ G tem-se que $a\ o\ b = c \in G$;
- É associativo, *i.e*, $a\ o\ (b\ o\ c) = (a\ o\ b)\ o\ c$ para todos a, b, c $\in$ G;
- Existe um elemento neutro, *e.g.*, de valor 1, *i.e*, $a\ o\ 1 = 1\ o\ a = a$ para todos os a $\in$ G;
- Tem propriedade do inverso, *i.e*, $a\ o\ a^{-1} = a^{-1}\ o\ a = 1$;
- É abeliano (comutativo), *i.e*, $a\ o\ b = b\ o\ a$ para todos os a, b $\in$ G.

DEFINIÇÃO 2.4 (Campo) Um Campo é definido como um conjunto de elementos com as seguintes propriedades:

- Todos os elementos de Campo formam um grupo aditivo com a operação do grupo "+" e um elemento neutro 0;
- Todos os elementos do Campo, exceto o 0, formam um grupo multiplicativo com a operação do grupo "x" e o elemento neutro 1;
- Quando as duas operações do grupo se misturam, a lei de distribuição se mantém, *i.e.*, para todos a, b, c $\in FF$:a(b + c) = (ab) + (ac)

Um FF só existe se ele tem p^m elementos, em que p é um número primo e m é um inteiro positivo.

Alguns exemplos de FF:

- Existe um FF com 11 elementos: $GF(11) = GF(11^1)$;
- Existe um FF com 81 elementos: $GF(81) = GF(3^4)$;
- Existe um FF com 256 elementos: $GF(256) = GF(2^8)$, este é usado no Campo AES.

Os tipos de FF podem ser definidos como $GF(p^m)$; quando m = 1, *i.e.*, $GF(p)$, conhecidos como campos primos, ou; quando m $\geq$ 1, *i.e.*, $GF(p^m)$, conhecidos como campos de extensões, que são fundamentais em criptografia, *e.g.*, $GF(2^m)$. A aritmética dos campos primos e campos de extensão são amplamente definidas em muitos trabalhos [40]. Destacam-se os cálculos que são feitos para soma, subtração e multiplicação, usando redução modular, o uso do aglortimo extendido euclidiano para calcular uma inversão, a representação dos GF em polinômios irredutíveis, entre outros.

2.1.3.2 Estrutura do AES

A estrutura do algortimo AES é mostrada na Figura 2.2.

O AES encripta todos os 128 bits dos dados de entrada em uma rodada. O número de rodadas depende do tamanho da chave K usada, conforme mostrado a seguir:

- K = 128 bits $\rightarrow$ 10 rodadas;
- K = 192 bits $\rightarrow$ 12 rodadas;

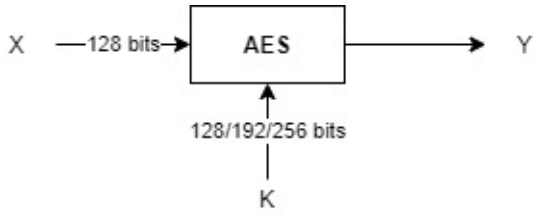

Figura 2.2 – Estrutura do AES.

- K = 256 bits $\rightarrow$ 14 rodadas;

Cada rodada consiste em quatro camadas: a) *Byte Substitution*, promove confusão; b) *Shift Row*, promove difusão; c) *Mix Column*, promove difusão; d) *Key Addition*.

A Figura 2.3 mostra como funciona cada rodada e as camadas no AES.

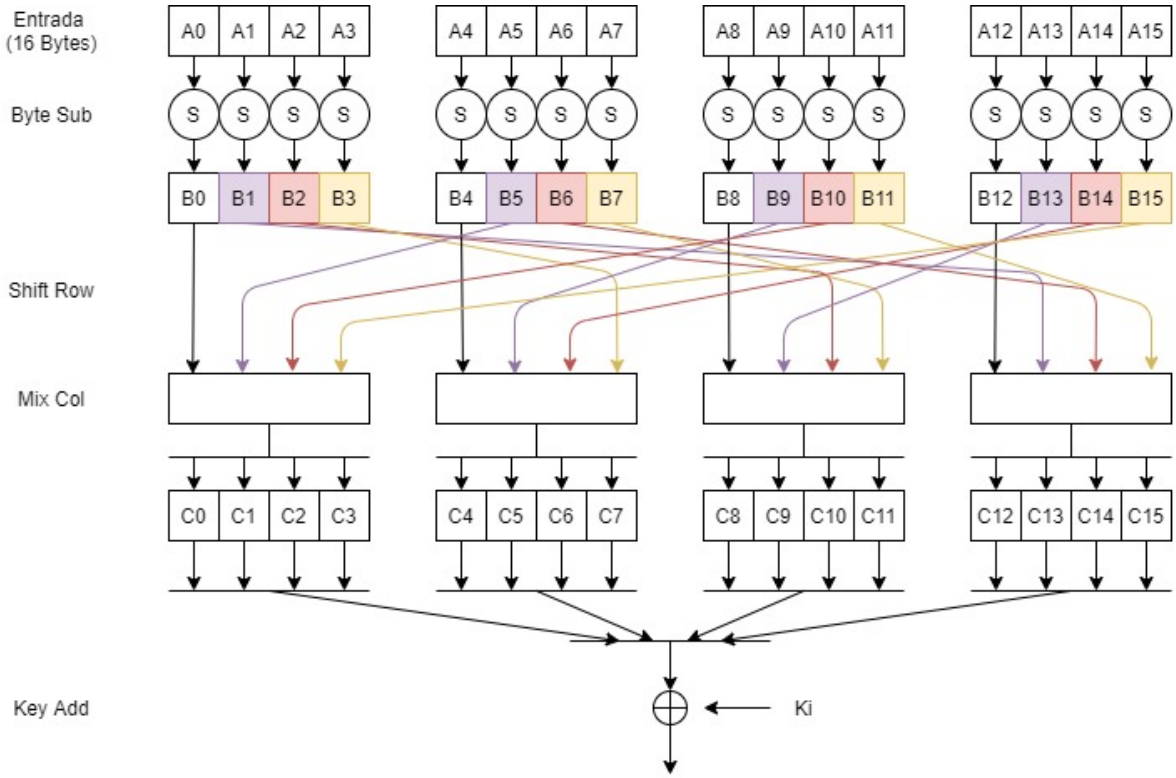

Figura 2.3 – Camadas em uma rodada no AES.

A última rodada não possui a camada de *Mix Column*. Para todo começo (bloco de 128 bits de entrada) e no final é feita uma operação de *Key Whitening*, *i.e.*, uma operação de XOR entre a chave e os bits de entrada e saída. A entrada, então, é dividida em blocos de 16 bytes.

A) Camada Byte Sub

Também conhecida como "S-Box Layer", consiste em $S(A_i) = B_i$, mostrado na Figura 2.4

Todas as dezesseis S-Box são idênticas. A S-Box é uma tabela de coordenadas do padrão

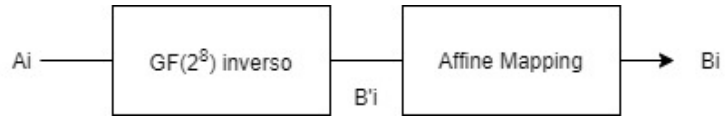

Figura 2.4 – S-Box.

AES que foi construída em princípios matemáticos. A tabela S-Box foi feita assim: considere $A_i \in GF(2^8)$. Então, *e.g.*:
$A_i = 1100\ 0010$
$A_i(x) = x^7 + x^6 + x$
$B_i'(x) = x^5 + x^3 + x^2 + x + 1 = A^{-1}(x)$
$B_i' = 0010\ 1111$

Percebe-se que $(x^7 + x^6 + x)(x^5 + x^3 + x^2 + x + 1) \equiv 1\ mod\ x^8 + x^4 + x^3 + x + 1$, sendo $x^8 + x^4 + x^3 + x + 1$ o polinômio irredutível do AES. Entretanto, o AES não permite que se faça uma descrição matemática certa de uma entrada para sua saída. Então, se faz uma nova transformação que acaba com essa acertividade matemática (*Affine Mapping*), como mostrado na matriz a seguir:

$$\mathrm{B}_i = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \ mod\ 2.$$

Esse é o resultado na camada Byte Sub.

B) Camada Shift Row

Consiste somente em reposicionar os bits de saída da camada Byte Sub. De forma representativa, a Figura 2.5 apresenta esse reposicionamento.

Cada byte é conectado à camada Mix Col, para propósito de difusão.

C) Camada Mix Col

A camada Mix Col faz processos de mutliplicação e adição em $GF(2^8)$ nos bytes de saída da anterior. A seguir mostra-se a matriz derivativa desse processo:

Figura 2.5 – Shift Row.

$$\mathrm{C}_i = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} \equiv \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Todos os c_i, b_i e constantes são bytes. $C_0 = 02 * B_0 + 03 * B_5 + 01 * B_{10} + 01 * B_{15}$, sendo que "*" é propriedade multiplicativa em $GF(2^8)$ e "+" é propriedade aditiva em $GF(2^8)$. A representação se dá assim: $01 = 0000\ 0001 \rightarrow 1$; $02 = 0000\ 0010 \rightarrow x$; $03 = 0000\ 0011 \rightarrow x + 1$.

D) Camada Key Add

Trata-se somente da inclusão da chave secreta na saída dos bytes da Mix Col. Faz-se uma operação de XOR ($\oplus$) em cada byte de saída C_i.

2.1.3.3 Estrutura do modo AES-CBC

Será descrito o modo AES-CBC. O uso de modos no AES tem por objetivo resolver dois problemas: 1) Tornar a encriptação probabilística, *i.e.*, para a mesma entrada essa produzir diferentes saídas, mas que o outro lado que compartilha da chave saiba como descifrar; 2) combinar a encriptação para todos os blocos, *i.e.*, todos seguem a mesma regra.

DEFINIÇÃO 2.5 (Encriptação determinística e probabilística) Um esquema de encriptação é determinístico se um texto em claro (Pt) é mapeado para uma cifra fixa de saída (Ct) caso a chave secreta não mude. Um esquema de encriptação é probabilístico quando esse

usa uma aleatoriedade para alcançar uma geração não-determinística da cifra de saída.

O CBC é um dos modos probabilísticos do AES. A Figura 2.6 demonstra seu funcionamento.

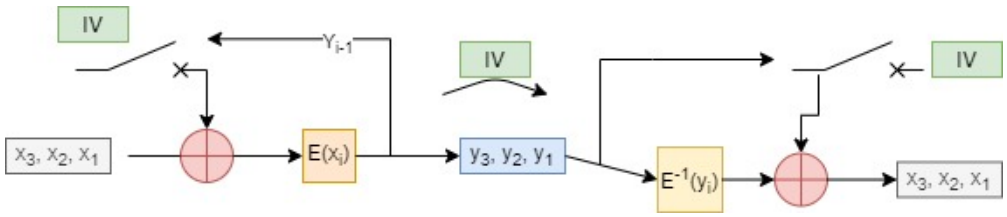

Figura 2.6 – AES-CBC. Processo de cifragem e decifragem.

É importante notar que o oposto de um XOR é outro XOR. O vetor de inicialização (IV) não precisa ser secreto e deve ser um "nonce" (*number used only once*). Para geração do IV é necessário usar números verdadeiramente aleatórios e um contador (guardado aonde gera-se o IV) concatenado com um tempo.

A importância do entendimento de cada camada e do modo CBC é fundamental tanto para a proposta criptográfica desta dissertação, quanto dos ataques colacionados. A pesquisa propõe na entrada em rearranjo do IV, fazendo com que esse seja secreto, aleatório e somente calculado pelas entidades que possuem a chave secreta `k`. O não envio pela rede de IV, e adotando um "nonce" para tornar o esquema probabilístico na entrada e saída do bloco AES-CBC faz com que esta pesquisa mitigue uma série de ataques contra o AES-CBC. Ademais, o entendimento das camadas faz-se necessário porque existem ataques, como serão mostrados, que exploram a vulnerabilidades de construção de cada uma delas, criando subfunções para tornar a saída de cada um determinística, explorando processos com poucas rodadas de confusão e de difusão ou atacando o IV.

2.2 PRIMITIVA DE CHAVE PÚBLICA

Descreve-se o conceito e a segurança da encriptação de chave pública nesta seção. Especificamente sobre o algoritmo RSA com preenchimento utilizando a técnica de OEAP. Os detalhes do uso desta técnica de encriptação podem ser vistos no Capítulo 4.

2.2.1 Esquema de encriptação de chave pública

DEFINIÇÃO 2.6 (Esquema de encriptação de chave pública [41]) O esquema de encriptação de chave pública é dado por $\mathsf{Dec}_{\mathsf{sk}}(\mathsf{Enc}_{\mathsf{pk}}(m_i)) = m_i$, em que Dec é a fase de decriptação usando sk, Enc é a fase de encriptação usando pk, para $(\mathsf{pk}, \mathsf{sk}) \leftarrow KGen(1^n)$ e $m \in M \leftarrow \{0,1\}^*$ espaço da mensagem.

2.2.2 Segurança semântica da encriptação de chave pública

DEFINIÇÃO 2.7 (Segurança semântica de encriptação de chave pública [41]) A segurança semântica é dada considerando um esquema de encriptação de chave pública e adversários de tempo polinomial $\mathcal{A}$ and $\mathcal{A}$'. $\mathsf{Adv}^1_{\mathcal{A}}(k)$ é: $(M,S) \leftarrow \mathcal{A}_1(\mathsf{pk})$; $x \leftarrow M$; $y \leftarrow \mathsf{Enc}_{\mathsf{pk}}(x)$; $(v,f) \leftarrow \mathcal{A}_2(M,s,y)$; se $v = f(x)$, então $d \leftarrow 1$; o contrário $d \leftarrow 0$; e $\mathsf{Adv}^0_{\mathcal{A}'}(k)$ é: $(M,S) \leftarrow \mathcal{A}'_1(\mathsf{pk})$; $x \leftarrow M$; $(v,f) \leftarrow \mathcal{A}'_2(M,s)$; se $v = f(x)$, então $d \leftarrow 1$; o contrário $d \leftarrow 0$; em que $(|x| = |x'|) \in M$, f é uma função algoritmica $M \in \{0,1\}^*$, e $v \in f(M)$. Então, $\mathsf{Adv}_{\mathcal{A},\mathcal{A}'}(k) = \Pr\left[\mathsf{Adv}^1_{\mathcal{A}}(k) = 1\right] - \Pr\left[\mathsf{Adv}^0_{\mathcal{A}'}(k) = 1\right]$, em que o esquema de encriptação de chave pública é seguro se $\mathsf{Adv}_{\mathcal{A},\mathcal{A}'}(k)$ for insignificante.

DEFINIÇÃO 2.8 (IND-CPA, IND-CCA1, e IND-CCA2 - notação de segurança para encriptação de chave pública [41]) A segurança IND é dada considerando um esquema de encriptação de chave pública e um algoritmo de tempo polinomial $\mathsf{Adv}^{\mathrm{f}}_{\mathcal{A}_{1,2}}(k)$. Para qualquer CPA, CCA1 and CCA2 (adaptativo), $\mathsf{Adv}^{\mathrm{f}}_{\mathcal{A}_{1,2}}(k)$ é: $f \in \{0,1\}$; $(x_0, x_1, S) \leftarrow \mathcal{A}^1_1(\mathsf{pk})$; $y \leftarrow \mathsf{Enc}_{\mathsf{pk}}(x_f)$; $d \leftarrow \mathcal{A}^2_2(x_0, x_1, S, y)$; em que x_f é a representação das mensagens, $|x_0| = |x_1|$, e S o estado de encriptação. Considerando o seguinte: $\mathcal{A}^{\epsilon}_1(\mathsf{pk})$ e $\mathcal{A}^{\epsilon}_2(x_0, x_1, S, y)$ para CPA; $\mathcal{A}^{\mathsf{Dec(sk)}}_1(\mathsf{pk})$ e $\mathcal{A}^{\epsilon}_2(x_0, x_1, S, y)$ para CCA1; $\mathcal{A}^{\mathsf{Dec(sk)}}_1(\mathsf{pk})$ e $\mathcal{A}^{\mathsf{Dec(sk)}}_2(x_0, x_1, S, y)$ para CCA2, em que a função ϵ é vazia para $\exists$ de entrada, então $\mathsf{Adv}^{\mathrm{f}}_{\mathcal{A}_{1,2}}(k) = \Pr\left[\mathsf{Adv}^1_{\mathcal{A}_{1,2}}(k) = 1\right] - \Pr\left[\mathsf{Adv}^0_{\mathcal{A}_{1,2}}(k) = 1\right]$, em que o esquema de encriptação de chave pública é seguro se $\mathsf{Adv}^{\mathrm{f}}_{\mathcal{A}_{1,2}}(k)$ for insignificante.

2.2.3 RSA

O algortimo de chave pública RSA (Rivest–Shamir–Adleman) [42], ao contrário dos simétricos, requerem o cálculo de um par de chaves (Kpu, Kpr). Doravante denominados chave pública e chave privada, essas possuem um condão matemático entre si, que faz com que o uso de uma chave impute o uso exclusivamente da outra para a operação inversa (neste

caso usando par de chaves para encriptação/decriptação e não para assinaturas). A segurança no uso do RSA [35], especificamente, deriva-se do problema da fatoração de números grandes, advinda da Teoria dos Números. O algoritmo RSA calcula seu par de chaves assim:

- Escolhe-se dois números primos grandes de forma aleatória (Gerador de Números Aleatórios), p e q;
- $n = p * q$;
- Calcula-se $\phi(n) = (p-1)(q-1)$;
- Escolhe $Kpu = e \in 1, 2, ..., \phi(n) - 1$, tal que o máximo divisor comum $mdc(e, \phi(n)) = 1$, sendo e e $\phi(n)$ relativamente primos;
- Calcula-se $Kpr = d$, tal que, $d * e \equiv 1 \; mod \; \phi(n)$.

Tem-se, então, $Kpu = (n, e)$ e $Kpr = (d)$. É importante destacar que atualmente duas premissas devem ser seguidas, visto os avanços nas técnicas de criptoanálise, devido a capacidade computacional e dos algoritmos em atacar o RSA. A primeira é que $p, q \geq 2^{512}$ e a segunda é que $n \geq 2^{1024}$.

2.2.3.1 RSA-OAEP

DEFINIÇÃO 2.9 O esquema de encriptação RSA-OEAP calcula $s = (m||0^{k_1}) \oplus G(r)$ e $t = r \oplus H(s)$, resultando $c = f(s, t)$, em que r é um inteiro k-bit gerado aleatoriamente, f é uma função unidirecional. O esquema de decriptação RSA-OAEP calcula $(s, t) = g(c)$, em que g é o inverso de f usando sk, $r = t \oplus H(s)$, $M = s \oplus G(r)$. Para k_1 LSB de M e n MSB of M, se $[M]_{k_1} = 0^{k_1}$, o algoritmo de encriptação de chaves públicas retorna $[M]^n$, o contrário “rejeita".

2.3 SHA-256

Funções de resumo unidirecionais, *i.e.*, algoritmos de *hash*, são usados em muitas implementações criptográficas. Para um k inteiro positivo, a função *hash* com um domínio e um codomínio $H : \{0,1\}^* \rightarrow \{0,1\}^k$ endereça uma entrada arbitrária de tamanho $m \in \{0,1\}^*$ para uma saída fixa $y \in \{0,1\}^k$, chamada de resumo da mensagem. Definido pelo NIST, a suíte SHA-2 [31] é composta por seis funções *hash* com respectivos tamanhos em bits:

SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. Descreve-se, resumidamente, os sete passos que incidem no texto de entrada para o texto (*hash*) de saída usando o algoritmo SHA-256.

- Preenchimento de bits. A mensagem é preenchida de forma que seu comprimento seja congruente com $\equiv\ 448\ mod 512$. Este preenchimento é feito adicionando um único 1 bit ao final da mensagem, seguido por quantos zeros forem necessários para que o comprimento dos bits seja igual a $448\ mod 512$.

- Comprimento. Uma representação de 64 bits de comprimento da mensagem é anexada ao resultado. Este passo tem o objetivo de deixar o comprimento da mensagem um múltiplo exato de 512 bits.

- *Parsing*. A mensagem preenchida é transformada em N blocos de mensagem de 512 bits, $M^{(1)}, M^{(2)}, ..., M^{(N)}$, por bloco de 64 bits.

- Inicializar o valor de *hash*. O valor *hash* inicial, $H^{(0)}$, é definido consistindo em oito palavras de 32 bits, em formato hexadecimal.

- Programação de mensagens. O algoritmo SHA-256 usa uma programação de mensagem de sessenta e quatro palavras de 32 bits. As palavras da programação mensagem são rotuladas $W_0, W_1, \ldots, W_{63}$., para:

$$\mathrm{W}_t = \begin{cases} M_t^{(t)} & 0 \leq t \leq 15 \\ \sigma_1^{(256)}(W_{i-2}) + W_{i-7} + \sigma_0^{(256)}(W_{i-16}) + W_{i-16} & 16 \leq t \leq 63 \end{cases}, \text{ em que}$$

$\sigma_1^{(256)}(W_{i-2}) = ((W_{i-2})ROTR\ 17) \oplus ((W_{i-2})ROTR\ 19) \oplus ((W_{i-2})SHR\ 10)$; e
$\sigma_0^{(256)}(W_{i-15}) = ((W_{i-15})ROTR7) \oplus ((W_{i-15})ROTR\ 18) \oplus ((W_{i-15})SHR\ 3)$; sendo que, ROTRk é a rotação a direita por k; e SHRk é o deslocamento a direita por k, com a introdução de quantos 0s forem necessários à esquerda.

Para i = 0 a N (N = o número de blocos preenchidos na mensagem), faz-se:

{

- Inicialização dos registros. Inicia os registradores a; b; c; d; e; f; g; h com o valor de *hash* intermediário $(i-1)^st$ (= o valor de hash inicial quando i = 1):

  $a \leftarrow \mathsf{H}_1^{i-1}$;
  $b \leftarrow \mathsf{H}_2^{i-1}$;
  ...
  $h \leftarrow \mathsf{H}_8^{i-1}$;

- Saída. Aplica-se a função de compressão do SHA-256 para atualizar os registros a; b; ...; h, de tal forma que:

  Para j = 0 a 63
  {
  Calcula-se $Ch(e, f, g)$, $Maj(a, b, c)$, $\sum_0(a)$, $\sum_1(e)$, e W_j, em que

  $Ch(x, y, z) = (x \hat{} y) \oplus (\neg x \hat{} z)$;
  $Maj(x, y, z) = (x \hat{} y) \oplus (x \hat{} z) \oplus (y \hat{} z)$;
  $\sum_0(x) = ROTR^2(x) \oplus ROTR^13(x) \oplus ROTR^22(x)$;
  $\sum_1(x) = ROTR^6(x) \oplus ROTR^11(x) \oplus ROTR^25(x)$;
  $\sigma_0(x) = ROTR^7(x) \oplus ROTR^18(x) \oplus SHR^3(x)$;
  $\sigma_1(x) = ROTR^17(x) \oplus ROTR^19(x) \oplus SHR^10(x)$, sendo que

  "$\oplus$" é o *bitwise* usando porta XOR, " $\hat{}$ " é o *bitwise* usando porta AND, "$\neg$" é o complemento do *bitwise* e "+" é a adição $mod\ 2^{32}$.

  $T_1 \leftarrow h + \sum_1(e) + Ch(e, f, g) + K_j + W_j$;
  $T2 \leftarrow \sum_0(a) + Maj(a, b, c)$;
  $h \leftarrow g$;
  $g \leftarrow f$;
  $f \leftarrow e$;
  $e \leftarrow d + T_1$;
  $d \leftarrow c$;
  $c \leftarrow b$;
  $b \leftarrow a$;
  $a \leftarrow T_1 + T_2$;
  }

Calcula-se o valor do *hash* intermediário i_{th} de $H^{(i)}$:
$H_1^(i)a + H_1^{(i-1)}$;
$H_2^(i)b + H_2^{(i-1)}$;
...
$H_8^(i)h + H_8^{(i-1)}$;

}

Tem-se, então, que $H^(N) = (H_1^{(N)}, H_2^{(N)}, ..., H_8^{(N)})$ é o valor de *hash*, em SHA-256, da mensagem de entrada.

2.4 ENTROPIA DE UM GERADOR DE NÚMEROS ALEATÓRIOS

Entropia denota-se por iniciar um gerador de números aleatórios com dados imprevisíveis. A fonte de entropia deve ser não determinística. Para esta pesquisa, usamos o marcador internacional do NIST para aferir a entropia das chaves secretas geradas pelo HSM, conforme denfinição a seguir.

DEFINIÇÃO 2.10 (Entropia [43]) Entropia, *i.e.*, min-entropia, é um conceito subjacente ao conjunto de aleatoriedade para um Gerador de Números Aleatórios (RNG), de uma variável aleatória $\mathtt{x}$, no conjunto $A = \{x_1, x_2, \ldots, x_k\}$, com probabilidade dada por $\Pr[X = x_i] = p_i$, for $i = 1, \ldots, k$, de acordo com "NIST Special Publication 800-90B - Recommendation for Random Number Generation Using Deterministic Random Bit Generators" [43]:

$$H = \min_{1 \leq i \leq k} (-\log_2 p_i) = -\log_2 \max_{1 \leq i \leq k} (p_i)$$

2.5 JSON

JSON (*JavaScript Object Notation*) [37] é uma linguagem de programação em formato texto para troca de dados. Usa algumas convenções que são familiares às bibliotecas da suíte C, Java, JavaScript, Perl e Python. Possui, em resumo, duas estruturas: i) Uma coleção de pares com nome e valor, *i.e.*, para cada valor atribui-se um nome que descreve o seu significado; e ii) Uma lista ordenada de valores, por meio de um *array*, vetor, lista ou sequência.

É definido sete tipos de valor: string, número, objeto, matriz, verdadeiro, falso e nulo. A linguagem tem algumas regras de sintaxe que devem ser observadas. São elas:

- Um objeto JSON é cercado por chaves "";
- Os pares nome e valor são agrupados por dois pontos ":" e separados por uma vírgula ",";
- Uma matriz é cercado por colchete "[]";
- Os formatos octal e hexadecimal não são permitidos;
- Cada chave dentro do JSON deve ser exclusiva e deve estar entre aspas duplas; e
- O tipo booleano corresponde a apenas dois valores especiais: verdadeiro ou falso. Os valores NULL são representados pelo literal nulo (sem aspas).

Em JSON, quando objetos e matrizes contêm outros, os dados têm uma estrutura semelhante a uma árvore. O cabeçalho HTTP usado para indicar que o conteúdo de uma solicitação ou resposta são dados JSON tem a seguinte sintaxe:

Content-Type: application/json

Para gerar e analisar dados JSON, existem dois modelos de programação semelhantes aos usados em documentos XML. O modelo de objeto cria uma árvore que representa os dados JSON na memória. A árvore pode então ser navegada, analisada ou modificada. O modelo de *streaming* usa um analisador baseado em evento que lê dados de um elemento JSON por vez. O analisador gera eventos e processamento, quando um objeto ou *array* começa ou termina, quando encontra uma chave ou quando encontra um valor.

2.6 CONSIDERAÇÕES FINAIS SOBRE A TEORIA RELACIONADA A ESTA PESQUISA

O Capítulo apresentou as considerações teóricas sobre as técnicas utilizadas nas contribuições propostas nesta dissertação. Ressalta-se que, para algumas técnicas apresentadas, é preciso implementar mecanismos para mitigar os ataques conhecidos, que derivam da exploração de um atacante sobre as vulnerabilidades na implementação da teoria apresentada nos sistemas computacionais. Alguns desses ataques possuem complexidade muito alta de serem realizados, com probabilidade insignificante de sucesso, pela própria formação do algoritmo utilizado. Em outros casos, são necessárias implementações adicionais para que o algortimo possa ser utilizado em propostas como dessa dissertação. No próximo Capítulo será mencionado alguns trabalhos relevantes correlacionados a esta pesquisa, que se utilizam de várias técnicas mencionadas neste Capítulo.

3 TRABALHOS RELACIONADOS

Neste Capítulo, faz-se uma descrição dos trabalhos relacionados a esta pesquisa. Mostra-se estudos que trazem conceitos sobre aspectos relacionados a segurança, privacidade, interoperabilidade e as técincas usadas para proteger uma rede biométrica. No intuito de mostrar a evolução e o que esta dissertação está solucionando, alguns trabalhos serão explicados e, posteriormente, no Capítulo 6, os mesmos serão comparados à proposta feita nesta pesquisa.

3.1 SEGURANÇA E PRIVACIDADE DE DADOS BIOMÉTRICOS

A preocupação com a segurança, a privacidade e a interoperabilidade dos registros biométricos está em várias propostas. Algumas técnicas aprimoram a proteção dos dados biométrico, mas, até o melhor conhecimento, não há indícios que alguma delas integre provas de segurança, privacidade e interoperabilidade simultaneamente como esta pesquisa proposta. Demonstrando como o vazamento de dados biométricos é um problema, em uma dada população, uma pesquisa realizada por Li e Zhang [44] mostra que quase 80% dos participantes têm medo de que informações biométricas pessoais sejam passíveis de roubo após o uso em aplicativos de verificação. Apenas 17% acham que a verificação feita no aplicativo bancário é segura. Com relação à interoperabilidade, já existem alguns esforços úteis de padronização [3, 4] que serão comentados e, como uma das contribuições desta dissertação, melhorados.

3.1.1 Aspectos de segurança e privacidade

Para garantir a segurança da rede e dos bancos de dados biométricos e, também, a privacidade dos dados, é necessário observar vários aspectos. O trabalho sobre privacidade diferencial, apresentado por Dwork [45], mostra que há muitas informações auxiliares que um adversário $\mathcal{A}$ pode obter sem acessar o banco de dados. Portanto, é essencial delimitar as fronteiras do que esta pesquisa estabelece em relação a segurança e privacidade. Neste sentido, registra-se, claramente, sobre os objetivos desta dissertação, *i.e.*, aprimorar a segurança e a privacidade dos dados enquanto estes estiverem dentro da rede e do banco de dados biométricos, usando técnicas criptográficas que possuem comprovação de segurança.

3.1.2 Trabalhos sobre segurança e privacidade biométrica

Existem muitas técnicas criptográficas e de transformações conhecidas para endereçar a segurança e a privacidade dos dados biométricos. A Tabela 3.1 apresenta alguns trabalhos

Tabela 3.1 – Trabalhos de biometria relacionado a segurança e privacidade

Lai *et al.* [17]	Privacy–Security Trade-Offs in Biometric Security Systems-Part I: Single Use Case
Lai *et al.* [18]	Privacy–Security Trade-Offs in Biometric Security Systems-Part II: Multiple Use Case
Nagar *et al.* [16]	Multibiometric Cryptosystems Based on Feature-Level Fusion
Nassir and Perumal [15]	Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm
Rathgeb *et al.* [21]	Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris
Kumar and Kumar [13]	A Cell-Array-Based Multibiometric Cryptosystem
Li *et al.* [14]	A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion
Kaur and Sofat [46]	Fuzzy vault template protection for multimodal biometric system
Zhou and Ren [12]	PassBio: Privacy-Preserving User-Centric Biometric Authentication
Toli and Preneel [11]	Privacy-preserving Biometric Authentication Model for e-Finance Applications
Kaur and Khanna [19]	Random Distance Method for Generating Unimodal and Multimodal Cancelable Biometric Features

relevantes na área.

As partes I e II dos trabalhos de Lai *et al.* [17, 18] apresentam algumas teorias importantes. É descrito o compromisso entre segurança, privacidade e proteção da chave em qualquer sistema biométrico (*template* biométrico), quando no uso de uma biometria, e ao enfrentar a reutilização da mesma informação biométrica em vários locais. Os trabalhos tratam de medidas biométricas específicas para diferentes abordagens ao gerar uma chave em sistemas de autenticação biométrica: (a) abordagem não aleatória; (b) abordagem aleatória.

Nagar *et al.* [16] propõe uma estrutura de fusão no nível do recurso. Foi baseado em um algoritmo incorporado de transformação que modifica um recurso biométrico x_m em uma nova representação binária ou de compromisso z_m. Um módulo fundido que combina a biometria homogênea e um sistema criptográfico biométrico que gera um esboço seguro nos procedimentos de inscrição/coleta. O trabalho proposto apresenta algumas análises de segurança para o modelo biométrico criado e melhoria do desempenho da rede.

O trabalho de Nassir e Perumal [15] usa o ID do usuário e uma senha com os dados biométricos extraídos, convertidos em números decimais. Ao usar algoritmos simétricos e RSA, o trabalho cifra e assina os dados em um pacote. No banco de dados, esse pacote é

decifrado para uma análise de decisão. Algumas avaliações de desempenho foram feitas, mas sem análise de segurança.

O trabalho de Rathgeb *et al.* [21] propõe uma transformação baseada em filtro Bloom para proteger modelos em amostras de rosto e íris. Ele constrói duas matrizes que foram organizadas em um código binário bidimensional, divididas em blocos de tamanho igual, consistindo em $w_F(w_I)$ bits. Uma transformação $\mathtt{h}$ foi aplicada para mapear a coluna binária para seu valor decimal equivalente, cujos locais estavam dentro dos filtros deBloom. Uma função *hash* foi aplicada, levando a face e a íris a ter o mesmo comprimento de transformação e, na última etapa, a face e a íris transformadas foram fundidas, em uma representação, para questões de privacidade.

O artigo de Kumar e Kumar [13] propõe um sistema criptográfico biométrico multimodal baseado em dois modos: (a) modo de recurso; (b) modo de decisão. A construção consiste em três fases, *i.e.*, usando Bose Chaudhuri Hocquenghem (BCH) aplicado na biometria, criando código de paridade, um cálculo de código *hash* do estágio de bloqueio realizado nas modalidades biométricas e o estágio de desbloqueio em que a paridade dO código foi regenerado usando XOR. A análise experimental confirma a superioridade dos sistemas criptográficos multimodais e a fusão no nível de decisão.

Li *et al.* [14] descreve uma nova análise de segurança, propondo uma construção multibiométrica usando uma impressão digital para cifrar a chave. Ao combinar a teoria da informação e segurança, o trabalho usa triangulações, extração de recursos e dois níveis de criptografia, um com funções *hash* e cofres para vincular o modelo de impressão digital transformado, e outro com o esquema de compartilhamento secreto de Shamir para dividir e armazenar os valores de *hash*. Um nível de decisão fundido obteve a identidade de uma amostra.

O trabalho de Kaur e Sofat [46] sobre *fuzzy vault* incorpora uma abordagem de modelo biométrico multimodal. O cofre difuso é uma combinação de impressões digitais e face - pontos de minúcia extraídos usando análise de cruzamento e um componente principal, onde o "fuzzy" é o cofre de entrada, para codificação e interpolação de Lagrange para recuperar a chave do cofre, no âmbito da decodificação. O esquema proposto mostra que a abordagem produz um desempenho satisfatório e fornece a segurança reivindicada.

Zhou e Ren [12] propõe um TPE (*Threshold Predicate Encryption*) usando um esquema de criptografia funcional. O texto sem formatação foi cifrado e uma chave secreta associada a um vetor, usando as instâncias de Criptografia de Produto Interno e Criptografia de Predicado, que decifram um valor de função e não mais o texto sem formatação. Nenhuma informação sensível sobre os vetores podem ser usadas em ataques passivos ou ativos.

O trabalho de Toli e Preneel [11] usa um gravador de autenticação de pseudo-identidade de um cliente de um banco. Com o código PIN do cliente, o pacote biométrico é cifrado e

armazenado no dispositivo, descartando a biometria e o PIN. Para requisitos de segurança, o trabalho proposto usa padrões ISO de dispositivos biométricos, financeiros e criptográficos.

Kaur e Khanna [19] propõe um método de distância aleatória. Considerando a abordagem do modelo biométrico cancelável multimodal, gera-se uma identidade pseudo-biométrica revogável, discriminatória e que preserva a privacidade. O método mapeia, no espaço cartesiano, características biométricas e calcula a distância de alguns pontos, de acordo com o sigilo do usuário. A análise de segurança apresenta alguma resistência a ataques conhecidos.

Poucas técnicas, como o esquema que será mostrado no Capítulo 4, referem-se ao anonimato do registro do índice em um banco de dados biométrico. O uso de técnicas criptográficas junto à sistemas biométricos não é novo [47], mas, até onde se tem conhecimento, não havia sido utilizado para garantir o anonimato com interoperabilidade e integridade nos registros e transações biométricas. Uma das contribuições desta dissertação é a construção de um índice cifrado e não reversível, mas que possa atravessar e ser utlizado pela rede de conexões entre os PSB com segurança.

3.2 PROTOCOLOS DE COMUNICAÇÃO BIOMÉTRICOS

Será abordado alguns trabalhos sobre protocolos de comunicação nas redes biométricas. O foco será no relato do *framework* IEEE BOPS, principalmente na API construída e, como contribuição desta pesquisa, aprimorada.

3.2.1 Interoperabilidade

Os padrões ANSI/NIST [4] e IEEE BOPS [3] são referências em interoperabilidade de componentes em diferentes sistemas biométricos. O ANSI/NIST é um descritivo de campos (um pacote) que se relacionam com os dados biométricos que são transacionados na rede. Deve-se destacar que existem estudos que buscam estabelecer mecanismos de interoperabilidade, como Tolosana *et al.* [48] e Mason *et al.* [49]. No entanto, nenhum estudo comparativo será feito nesta pesquisa sobre esses últimos, porque eles apresentam soluções apenas parciais para dispositivos e dados biométricos, mas não sobre todo o fluxo de uma transação biométrica. Descreve-se a seguir o IEEE BOPS.

3.2.2 Sobre o IEEE BOPS

O IEEE BOPS garante controle de acesso multinível, declaração de identidade, processo de auditoria e permite a interoperabilidade, independente do sistema subjacente. A arquitetura proposta é construída para componentes periféricos, usando linguagens neutras, como

Representational State Transfer (REST), JSON e *Transport Layer Security/Secure Sockets Layer* (TLS/SSL) [3], fornecendo uma interface de comunicação cliente/servidor. O mecanismo BOPS inclui um *software*, um servidor BOPS confiável e um sistema de detecção de intrusão. O BOPS usa uma API para fins de interoperabilidade que será o assunto desta dissertação.

As seções 6 a 9 do documento IEEE BOPS descrevem as considerações de interoperabilidade, incluindo o formato da API. A API executa uma conexão SSL de 2 vias (mútua), que mitiga ataques de repetição, controla os procedimentos de autenticação dos dispositivos e estabelece mensagens JSON entre o servidor BOPS e o cliente. Ela cria cinco tipos de procedimentos (Assertion, Role Gathering, Multi-Level Access Control, Assurance e Auditing) que mantêm a comunicação por uma associação tripla do usuário, dispositivo e sessão.

A API começa com uma mensagem de código de erro JSON para chamadas de conexão. Posteriormente, a documentação do BOPS descreve mensagens JSON sobre a configuração inicial, os dispositivos, a autenticação de sessão - por troca de certificados - e a segurança de comunicação, incluindo um "QROpportunity" que identifica o aplicativo cliente. A parte chamada de "Role Gathering" inclui um fluxo descritivo de parâmetros de entrada e saída sobre a construção, criação, status, dados e término da sessão. Entre as sessões de status e de dados é onde a biometria é capturada e enviada para a rede. O mecanismo de controle dispara uma resposta binária para o "JSONObject" que inclui, ou não, os dados retornados relacionados ao problema de segurança da conexão. Por fim, a API propõe uma garantia e auditoria de mensagens JSON para ações de grupo (leitura/gravação) em qualquer conjunto de dados.

Embora o BOPS trate de detalhes sobre segurança e autenticação, o problema reside no fato de que o IEEE BOPS não ter nenhum mecanismo de integridade eficaz. O controle multinível não oferece mensagens sobre o objeto das transações biométricas. Não inclui lidar com as operações pendentes, *timeout* ou recuperação de conexão entre sistemas para o procedimento de identificação biométrica. Nossa pesquisa usa o pacote ANSI/NIST e propõe uma subseção de integridade na documentação da API, aprimorando o IEEE BOPS.

3.3 CONSIDERAÇÕES FINAIS SOBRE OS TRABALHOS RELACIONADOS

Este Capítulo descreveu relavantes trabalhos na área desta dissertação. Há muito tempo, artigos propõem ideias para dar segurança e privacidade a dados em redes biométricas. Conforme mostrado, no que tange a trabalhos voltados a segurança e privacidade, existem algumas técnicas que fazem uso de ferramentas de transformações, baseada em diferentes aproximções criptográficas. Outros derivam de técnicas de agrupamento difuso, que é um

método que permite que dados biométricos sejam usados como entradas para técnicas criptográficas. Alguns deles possuem consistentes demonstrações de segurança, mas nenhum possui uma linha que faça com que a técnica seja usada de forma interoperável. O trabalho de Toli e Preneel [11] até cita que interoperabilidade é algo fora do escopo daquele artigo.

Sobre interoperabilidade, esta dissertação centrou seus estudos e comparações no padrão IEEE BOPS. Nesse sentido, apontou-se incompletude do padrão internacional, visto a falta de um descritivo sobre integridade das transações. A falta de uma comunicação de reconhecimento da falha ou do sucesso de uma transação, torna este padrão incompleto nas questões de interoperabilidade e segurança do processo biométrico. Não obstante, conforme será apresentado no próximo Capítulo, esta pesquisa resolve a questão da interoperabibilidade, com integridade e segurança, mantendo a privacidade dos dados de um indivíduo dentro de uma rede biométrica. Esta proposta, que se concretiza em uma API (refira-se ao Apêndice A), pode ser incorporada ao padrão IEEE BOPS.

4 PROPOSTA

Neste capítulo, descreve-se a proposta desta dissertação. Explica-se as técnicas criptográficas, o protocolo de comunicação biométrico e as soluções que esta pode endereçar. As técnicas criptográficas que serão apresentadas têm os objetivos de anonimizar o dado indexado de uma pessoa dentro do banco de dados biométricos, mas construindo um algoritmo que permita que essa indexação possa ser usada para identificar pessoas pelos PSB desta rede, e proteger o ciclo de vida da chave secreta `k`. Na seção do protocolo de comunicação biométrico será explicado a rede biométrica. Apresenta-se os elementos e fluxos, assim como o processo que garante interoperabilidade, usando o dado anonimizado (IDN) entre os PSB e criando um mecanismo de integridade para a confirmação da informação pela rede. Neste escopo, será proposto uma suíte de mensagens JSON e um código, em forma de API, que, como uma das contribuições desta pesquisa, podem ser incorporados, *e.g.*, na documentação do IEEE BOPS, melhorando o *framework* citado.

4.1 TÉCNICAS CRIPTOGRÁFICAS PROPOSTAS

4.1.1 O algoritmo do IDN

O esquema de geração do IDN, mostrado no Algoritmo 1, usa o número do Cadastro de Pessoa Física - `CPF`, o Número do Código de Tempo - `TCN`, a chave secreta `k` (`k`=256 bits), o algoritmo AES-256-CBC, um vetor de inicialização - `iv` e um parâmetro de número único - `nonce` aleatórios e calculados localmente dentro do módulo criptográfico do HSM e a função de *hash* SHA256, da seguinte maneira:

- O `CPF` é expandido por concatenação até se obter um comprimento de 256 bits;
- O parâmetro `iv` é calculado, inicialmente, pela concatenação de `k` e `CPF` resultando em um comprimento de 512 bits, chamado de `y`; então, obtêm-se `x` aplicando `x` = SHA256 (`y`), com comprimento de 256 bits; depois, divide-se `x` em duas metades de mesmo comprimento, sendo `a` os primeiros 128 bits e `b` o restante; finalmente tem-se que `|iv|` = `a` $\oplus$ `b`;
- O bloco de entrada com o `CPF` é preenchido (*padding*) até 128 bits e é cifrado, em AES-256-CBC, usando `k` e `iv`, resultando em um texto cifrado `z`, que é uma sequência cifrada de 128 bits;
- O parâmetro `nonce` é calculado de forma semelhante ao `|iv|`, *i.e.*, o `|TCN|`é re-

Algorithm 1 O algoritmo do IDN

Data: CPF, k

Result: IDN

Read the value of k;

Read the value of CPF;

Read the value of TCN;

$k \in \{0,1\}^{256}$;

$CPF \in \{0,1\}^{88}$;

$TCN \in \{0,1\}^{288}$;

x^j is the j^{th}-bit of x;

h^j is the j^{th}-bit of h;

v^j is the j^{th}-bit of v;

foreach *CPF* **do**

$CPFEXT = CPF||CPF||CPF \in \{0,1\}^{256}$

$y = k||CPFEXT \in \{0,1\}^{512}$

$\mathsf{H} \xrightarrow{y} x$

$a \in (x^0, x^1, ..., x^{127})$

$b \in (x^{128}, x^{129}, ..., x^{255})$

$iv = a \oplus b$;

$AES\text{-}256\text{-}CBC(CPF, iv, k) \rightarrow z$

$TCN \in (h^0, h^1, ..., h^{255})$

$u = k||TCN \in \{0,1\}^{512}$

$\mathsf{H} \xrightarrow{u} v$

$c \in (v^0, v^1, ..., v^{127})$

$d \in (v^{128}, v^{129}, ..., v^{255})$

$nonce = c \oplus d$

$IDN = z \oplus nonce$

end

Return IDN

duzido para um comprimento de 256 bits e concatenado com k, gerando uma sequência com comprimento de 512 bits, chamada de u; então, obtêm-se v aplicando v = SHA256 (u), com comprimento de 256 bits; depois, divide-se v em duas metades de mesmo comprimento, sendo c os primeiros 128 bits e d o restante; finalmente tem-se que nonce = c $\oplus$ d;

- Por fim, IDN = z $\oplus$ nonce, viável apenas para o PSB reverter, visto que IDN e TCN são os únicos parâmetros enviados pela rede.

A equação 4.1 representa a geração do IDN.

$$\begin{aligned} \text{IDN} = (\ \ (\text{AES}(k, \text{iv}, \text{CPF})) \oplus (((SHA256(k||TCN)) \in \{0,1\}^{0,\ldots,127}) \\ \oplus ((SHA256(k||TCN)) \in \{0,1\}^{128,\ldots,255}))\ \ ). \end{aligned} \tag{4.1}$$

A Figura 4.1 faz uma abstração de como fica o fluxo de entrada desta modificação no AES-CBC que versa esta pesquisa.

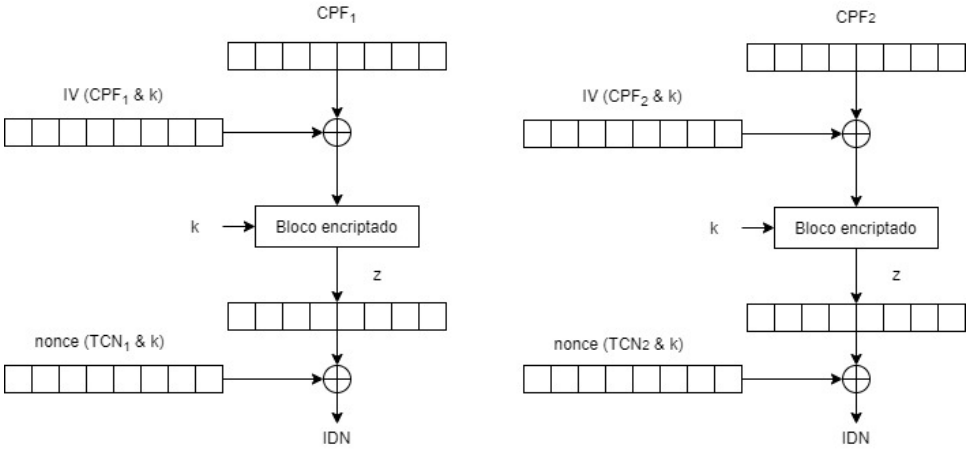

Figura 4.1 – Algoritmo AES-CBC modificado por esta pesquisa.

O mesmo CPF, quando registrado em momentos diferentes, gera IDN distintos, porque cada transação tem um TCN diferente. No entanto, o mesmo CPF, quando entra no Algoritmo 1, *e.g.*, duas vezes, resultando nas tuplas $IDN_1//TCN_1$ e $IDN_2//TCN_2$, gerará o mesmo z, da seguinte maneira:

- Calcula-se nonce com TCN_i;
- Faz-se $IDN_i \oplus nonce$, resultando em z.

Usando o Algoritmo 2, caso z seja o mesmo, *e.g.*, para a tupla armazenada $IDN_1//TCN_1$ e a tupla coletada/transacionada $IDN_2//TCN_2$, isto significa que trata-se do mesmo CPF.

Algorithm 2 z algorithm

Data: IDN$_i$, TCN_i
Result: z
Read the value of IDN$_i$;
$Readthevalueof TCN_i$;
v^j is the j^{th}-bit of v;
foreach *TCN$_i$* **do**
  $u = k||TCN_i \in \{0,1\}^{512}$
  $\mathsf{H} \xrightarrow{u} v$
  $c \in (v^0, v^1, ..., v^{127})$
  $d \in (v^{128}, v^{129}, ..., v^{255})$
  $nonce = c \oplus d$
  $z = IDN_i \oplus nonce$
end
Return z

Somente o PSB que possui `k`, `CPF`, `IDN_i` e `TCN_i` pode alcançar o mesmo `z` para um `CPF`. Destaca-se que todos esses cálculos criptográficos são feitos dentro do módulo criptográfico de cada HSM dos PSB.

4.1.2 Ciclo de vida e proteção da chave secreta k

Descreve-se como esta pesquisa lida com o ciclo de vida e proteção da chave secreta `k`. Para fins de geração, cria-se uma chave simétrica `k` aleatória com 256 bits em um HSM *offline*. Depois de criá-la, exporta-se `k` usando operações em RSA-OAEP, com as chaves públicas (Kpu) de cada HSM dos PSB na rede. Este procedimento produz um envelope criptográfico (Kpu(k)) por cada HSM dos PSB, contendo a chave secreta `k`. Apenas a chave privada (Kpr) de cada HSM pode decifrar o envelope (Kpr(Kpu(k))). A prova de segurança dessas operações será descrita no Capítulo 5. A Figura 4.2 mostra o fluxo ciclo de vida e proteção da chave `k`.

Para exportar e importar a chave `k` (Secret_2.key), usa-se os seguintes comandos, mostrados via OpenSSL script, com preenchimento RSA-2048-OAEP [35, 50]:

Input: "Certificate_from_PSB.cer", "Secret_2.key"
Output: key.key
Initialization:
$ openssl x509 -pubkey -noout -in Certificate_from_PSB.cer > HSM_.pub -inform DER;

$ openssl rsautl -oaep -encrypt -inkey HSM_.pub -pubin -in Secret_2.key -out Key.key;

Input: "HSMprivate.key", "Key.key"
Output: Secret_2.key

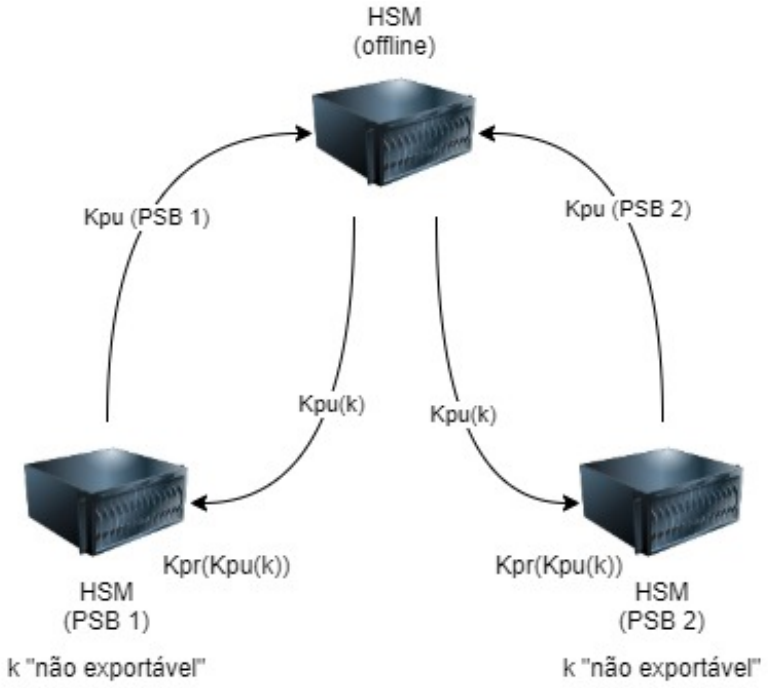

Figura 4.2 – Ciclo de vida e proteção da chave secreta k.

Initialization:
$ openssl rsautl -oaep -decrypt -inkey HSMprivate.key -pubin -in Key.key -out Secret_2.key;

Uma cerimônia com registro de auditoria local deve importar a chave secreta `k` no HSM do PSB com o recurso "não exportável". Não é possível, com este procedimento, copiar ou exportar `k` do HSM dos PSB. Os requisitos de certificação FIPS [34] garantem esta funcionalidade nos HSM. As condições estabelecidas na documentação de testes FIPS também tratam da inviolabilidade do HSM contra ataques de penetração, canal lateral, físicos, químicos e outros. De fato, uma das premissas desta pesquisa, conforme já comentado, é que o HSM deve ser certificado por mecanismos internacionalmente reconhecidos, *e.g.*, FIPS. Todas essas ferramentas e procedimentos tratam da proteção da chave secreta `k` contra violações e ataques.

4.2 PROTOCOLO DE COMUNICAÇÃO BIOMÉTRICO

4.2.1 A rede biométrica

Descreve-se a rede biométrica, mostrada na Figura 4.3, que define o cenário implementado nesta dissertação. Discorre-se sobre os elementos que compõem essa rede.

A Figura 4.3 mostra os dois PSB (*PSB 1* e *PSB 2*) com seus respectivos processos de capturas e elementos internos. O *Processo de Captura* consiste na coleta das biometrias

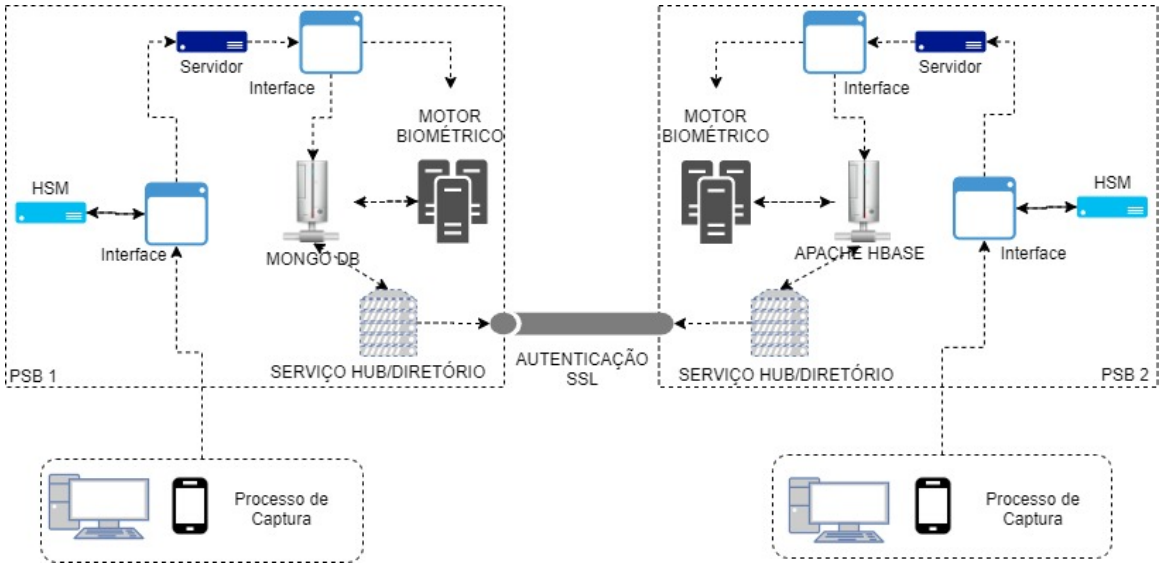

Figura 4.3 – Arquitetura da rede biométrica.

que, para este cenário, resumem-se a impressão digital e a face para cada `CPF`. O *software* de captura, que fornece extração das informações biométricas e uma medição de qualidade das mesmas, prepara um pacote `ANSI/NIST Package 1` com a informação do `CPF` e das biometrias. O `ANSI/NIST Package 1` é enviado por meio de um canal SSL mutuamente autenticado para a *Interface* dos PSB.

A *Interface*, ao recepcionar o pacote, comanda ao módulo criptográfico do *HSM* fazer os cálculos do IDN. Monta-se, então, o pacote `ANSI/NIST Package 2`, com o IDN calculado, extraindo o campo `CPF` do `ANSI/NIST Package 1`. A Figura 4.4 mostra o pacote de referência `ANSI/NIST Package 2` truncado, enfatizando o campo IDN, em uma transação `IDE`. Para detalhes do `ANSI/NIST Package 2`, por favor refira-se ao Apêndice B. No Capítulo 6 será mostrado um IDN real circulando pela rede biométrica.

O pacote `ANSI/NIST Package 2` possui o `TCN` ligado a transação `IDE`. No núcleo de cada PSB existe, no mínimo, um *Servidor* e uma outra *Interface* que funcionam de *worker* entre o *HSM*, o banco de dados e *MOTOR BIOMÉTRICO*. O banco de dados dos PSB trabalha na indexação e armazenamento dos dados e o *MOTOR BIOMÉTRICO* é quem processa as identificações (1:n) e verificações (1:1). O último componente dos PSB são os *SERVIÇO HUB/DIRETÓRIO* que possuem papel de recepcionar os comandos e mensagens entre os PSB, que se conectam por meio do *AUTENTICAÇÃO SSL*. Para a *AUTENTICAÇÃO SSL*, os PSB devem divulgar as seguintes informações:

- ID do PSB;
- Localização/URL do serviço de troca de arquivos ANSI/NIST, *i.e.*, do *SERVIÇO HUB*;
- Localização/URL do *SERVIÇO DIRETÓRIO*; e

Figura 4.4 – O campo IDN no arquivo de referência ANSI/NIST Package 2.

- x509/certificado para fins de autenticação do PSB.

A divulgação é feita em arquivo em formato JSON, seguindo o descrito abaixo:

```
[
{
“PSBioId:”  “NomePSB”,
“nist_endpoint”: “URL PARA ENVIO DE ARQUIVOS ANSI/NIST”,
“directory_endpoint”: “URL PARA SERVIÇO DE DIRETÓRIO”,
“x509”: “BASE64 X.509”
},
{...}
]
```

As configurações dos principais elementos dos PSB, na arquitetura proposta para esta dissertação, são apresentados na Tabela 4.1.

Elemento	*PSB 1*	*PSB 2*
HSM	ASI-HSM AHX5 KNET Cryptographic Module	ASI-HSM AHX5 KNET Cryptographic Module
S.O. do *SERVIÇO HUB/-DIRETÓRIO*	Linux Ubuntu 18.04	Linux CentOS 7
Processador do *SERVIÇO HUB/DIRETÓRIO*	Intel(R) Xeon (R) E5 - 2699	Intel(R) Xeon (R) E5-2650
Tecnologia do *MOTOR BIOMÉTRICO*	NEC Solutions	GPB
Banco de Dados	MongoDB	Apache Hbase
Capacidade do Link	500/500 Mbps	500/500 Mbps

Tabela 4.1 – Configurações dos principais elementos da Rede Biométrica.

4.2.1.1 Cache do PSB

O cache da base biométrica de um PSB (*e.g.*, PSB 1) é uma funcionalidade que permite que os dados do outro PSB (*e.g.*, PSB 2) sejam armazenados localmente. Possui dois mecanismos para garantir a sua consistência e manutenção.

- Construção de cache durante as transações: sempre que uma transação de cadastramento, *i.e.*, `IDE`, é executada, as informações da transação são repassadas para o outro PSB, para que a busca 1:N seja executada. No término do cadastramento, o PSB que recebeu a transação de cadastramento deve informar ao outro o sucesso ou cancelamento da transação, permitindo assim o uso dos dados para construção do cache;
- Reconstrução de cache/manutenção de cache: o PSB pode consultar no *SERVIÇO DIRETÓRIO* do outro PSB uma listagem de IDN e solicitar o envio de pacotes para reconstrução de cache;

Os caches biométricos podem ser utilizados para dois fins:

a) Execução de verificações 1:1, dispensando consultas de verificações no outro PSB; e

b) Execução de consultas 1:N, dispensando a espera (assíncrona) pelo retorno dos demais PSB nas transações de cadastro e atualização;

Quando o PSB precisar criar, recompor ou atualizar seu cache, deverá consultar a lista de IDN do outro PSB. A partir da data da última atualização do registro e do número único da transação (`TCN`) que originou ou atualizou o registro, o PSB solicitante decidirá se precisa ou não inserir ou atualizar esse registro em seu cache.

4.2.2 O protocolo de interoperabilidade

Apresenta-se, nesta subseção, as contribuições desta proposta em relação ao novo protocolo de interoperabilidade, aprimorando e criando mecanismos de integridade para, *e.g.*, as especificações do IEEE BOPS. Primeiro, apresenta-se como funcionam o *SERVIÇO HUB* e o *SERVIÇO DIRETÓRIO*. Em seguida, integra-se todas as mensagens e processos criados em um novo fluxo, que deve ser seguido para fins de integridade e identificação.

4.2.2.1 *SERVIÇO HUB* e *SERVIÇO DIRETÓRIO*

As requisições para o *SERVIÇO HUB* devem seguir o padrão assíncrono, *i.e.*, todas as respostas devem ser retornadas pelo *SERVIÇO HUB* que recebeu a solicitação quando o mesmo tiver a informação disponível. O modelo assíncrono implementado deve seguir o conceito "PULL", *i.e.*, quem recebeu a requisição é responsável por gerar e entregar a requisição de resposta.

Em geral, pela sua característica, o *SERVIÇO HUB* retorna os erros de forma assíncrona. Em algumas situações específicas, pode-se gerar um erro por tempo de execução da requisição. O *SERVIÇO HUB* deve retornar um código de sucesso/erro conforme é demonstrado na API, proposta no Apêndice A

Em caso de recebimento de qualquer um destes erros no envio de uma transação, o PSB de origem não deve incluir a transação na lista de pendências, *i.e.*, `pending_operations`, até que o problema seja sanado.

As requisições para o *SERVIÇO DIRETÓRIO* devem seguir o padrão síncrono, *i.e.*, todas as respostas devem ser retornadas na mesma requisição/resposta. O *SERVIÇO DIRETÓRIO* deve ser oferecido por cada um dos PSB como um mecanismo rápido de consulta.

O *SERVIÇO DIRETÓRIO* deve prover quatro operações básicas:

- Operação de listagem de operações pendentes: permite consultar transações para as quais o outro PSB aguarda resposta;
- Operação de requisição de reenvio de operações pendentes: permite a solicitação de reenvio de uma transação que esteja listada como pendente e não foi recebida pelo PSB;
- Operação de consulta de `z`: permite confirmar a existência ou não de determinado de `z` nos registros do PSB, além de um indicador das biometrias disponíveis;
- Operação de listagem de IDN: permite consultar IDN que existem na base do PSB, para fins de reconstrução de cache biométrico.

O serviço de consulta de IDN e a listagem de operações pendentes serão realizados por meio de "GET" no *endpoint* descrito na API, proposta no Apêndice A. O serviço de requisição de reenvio de operações pendentes será realizado através de "POST" no *endpoint* do arquivo descrito na API, proposta no Apêndice A. Os códigos HTTP utilizados para informar sucesso/erro nas requisições do *SERVIÇO DIRETÓRIO* estão descritos na API, proposta no Apêndice A. As mensagens JSON, com campos de requisição e resposta para cada uma das transações estão descritas na API, proposta no Apêndice A. Esta API é o código que pode ser inserido no IEEE BOPS e permite garantir que as transações dentro de uma rede biométrica, além de interoperáveis, sejam íntegras, com mecanismos de sucesso ou erro para cada transação de cadastro ou verificação, conforme será demonstrado no capítulo **??**.

4.2.3 O fluxo do protocolo de interoperabilidade

Serão apresentados os fluxos detalhados da rede PSB. Os fluxos são:

- `NIST Acceptance`
- `z_query`
- `IDN_List`
- `pending_operations` e `resend_operations`
- `IDE`
- `change_status`

Esses fluxos permitem que a rede biométrica realize suas operações de identificação (1:n) e verificação (1:1) com o indexador cifrado IDN, independentemente da tecnologia empregada no *MOTOR BIOMÉTRICO*. Isso siginifica que não é necessário a construção de modelos biométricos (*templates* biométricos) proprietários e que todos os PSB na rede obrigatoriamente precisam usar. Ademais, permite que os PSB saibam se as transações foram de fato processadas, garantindo integridade dos dados na rede.

A) NIST Acceptance

É o fluxo, mostrado na Figura 4.5, de recebimento do pacote `ANSI/NIST Package 2` oriundo do outro PSB, mostrado na Figura 4.5. Executa-se apenas o processamento mínimo para autenticação da origem, identificação da transação e inclusão da mesma em fila única de processamento. Resulta em retorno síncrono, *i.e.*, *SERVIÇO DIRETÓRIO*, de sucesso ou erro do recebimento. O erro no recebimento retorna uma mensagem HTTP 400 para o PSB de origem, denotando que não foi possível processar o arquivo `ANSI/NIST Package 2`

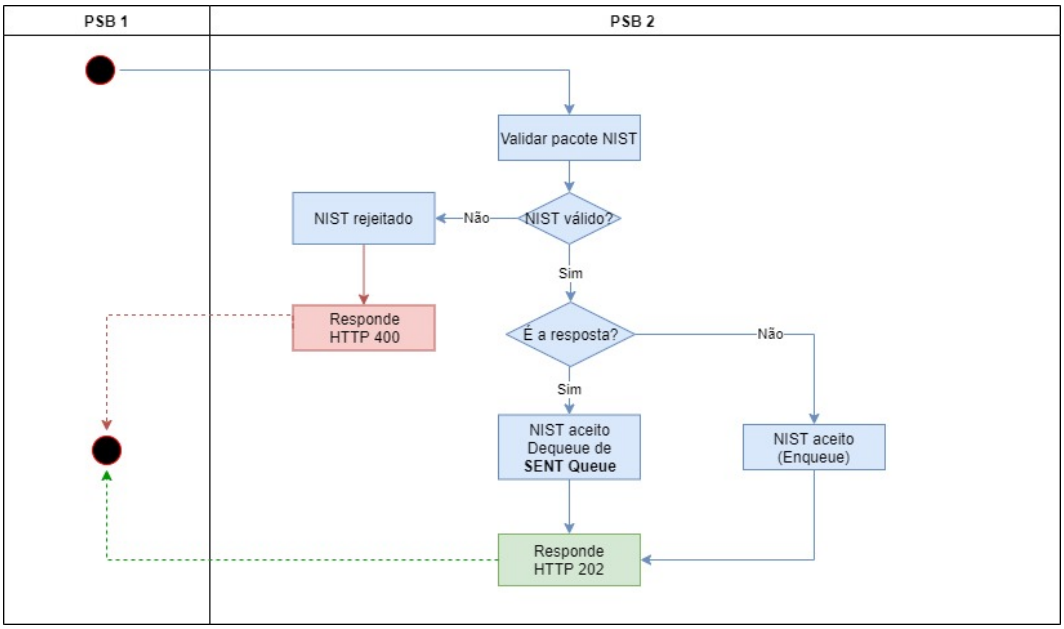

Figura 4.5 – Fluxo do NIST Acceptance.

- obrigando o PSB de origem a verificar o formato no arquivo. Esse erro não gera pendência na rede, mas somente um erro de negócio.

B) z_query

Este fluxo, mostrado na Figura 4.6, verifica se o código `z` está registrado no banco de dados local e cache do PSB e também se existe no outro PSB. O HSM do PSB calcula o parâmetro $nonce_i$, para cada TCN_i que estão armazenados. Depois, retorna a resultante $IDN_i \oplus nonce_i \rightarrow z_i$. Caso um z_i do grupo calculado for igual ao `z` de entrada, gera-se um pacote JSON com argumento $TRUE$, caso não exista, *i.e.*, `CPF` ainda não foi registrado na base, gera-se um pacote JSON com argumento $FALSE$. Se `z` existe, a resposta JSON apresenta quais impressões digitais e face estão registradas (TRUE|FALSE para cada campo representativo), junto com os IDN e `TCN` associados. Os detalhes das mensagens JSON são apresentados na API, proposta no apêndice A.

C) IDN_List

Este fluxo, mostrado na Figura 4.7, tem por objetivo listar os IDN e TCN que estão registrados no outro PSB. Esta tarefa se faz necessária para integridade dos dados em cache de um PSB com os dados do outro PSB. Os detalhes da mensagem de retorno da informação são apresentados na API, proposta no Apêndice A.

4.2.3.1 pending_operations e resend_operations

Este fluxo, mostrado nas Figuras 4.8 e 4.9 garantem a integridade das transações e, consequentemente, dos dados na rede biométrica. No caso de um incidente com um PSB, *e.g.*,

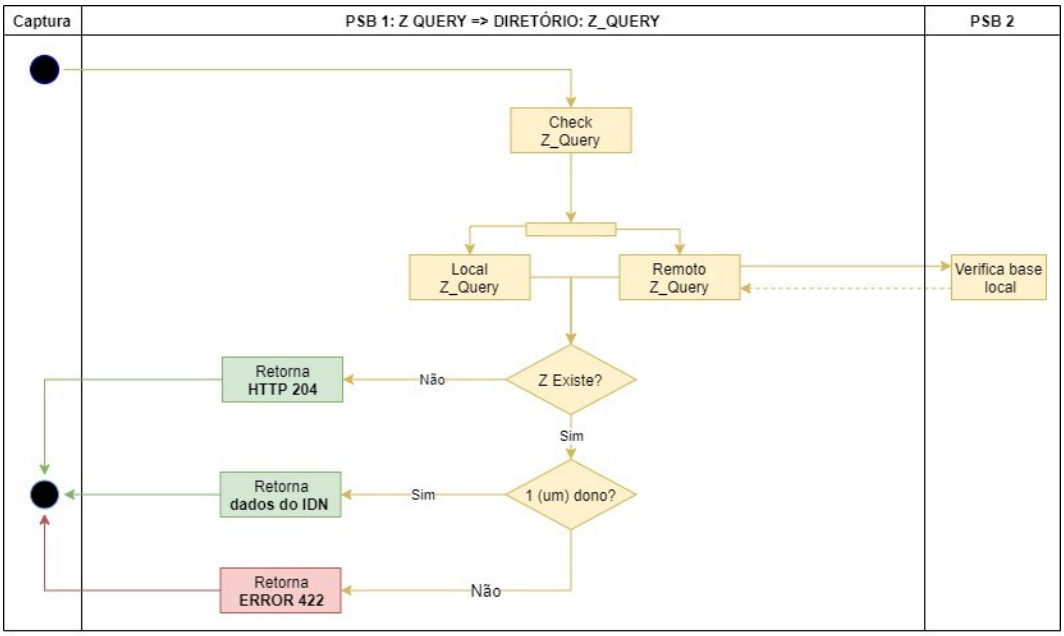

Figura 4.6 – Fluxo do z_query.

timeout, conexão ruim ou manutenção, a transação mostra uma lista de IDN e TCN que requer processamento adicional, mas que não pôde ser feito *on-line*. Depois, o PSB solicita que o outro reenvie as operações apenas para os IDN que não foram processados localmente. De hora em hora, esse tipo de JSON é enviado para garantir que todos os processos tenham sido executados, mantendo a integridade das transações pela rede. Após receber a lista de IDNs pendentes, o PSB pergunta quais operações devem ser realizadas. Esta lista de operações que devem ser realizadas pode ser uma transação de `IDE`, `END` ou `change_status`. Os detalhes da mensagem de retorno da informação são apresentados na API, proposta no Apêndice A.

D) IDE

Este fluxo, apresentado na figura 4.10, mostra a principal transação da rede. É ele que realiza todos os processos de identificação e verificação biométrica do `CPF`. Após diversos processos internos, que serão detalhados na Tabela 4.2, o PSB envia ao outro uma transação `IDE`. O `IDE` é o comando para o outro PSB inicie o processo de identificação. Anexa-se à mensagem o pacote `ANSI/NIST Package 2`, por um canal SSL mutuamente autenticado. A resposta a essa mensagem é um `VRE` transação com o valor `M` ou `X`, conforme detalhado na Tabela 4.2. Os detalhes da mensagem de retorno e de cada erro sobre essa transação são apresentados na API, proposta no Apêndice A.

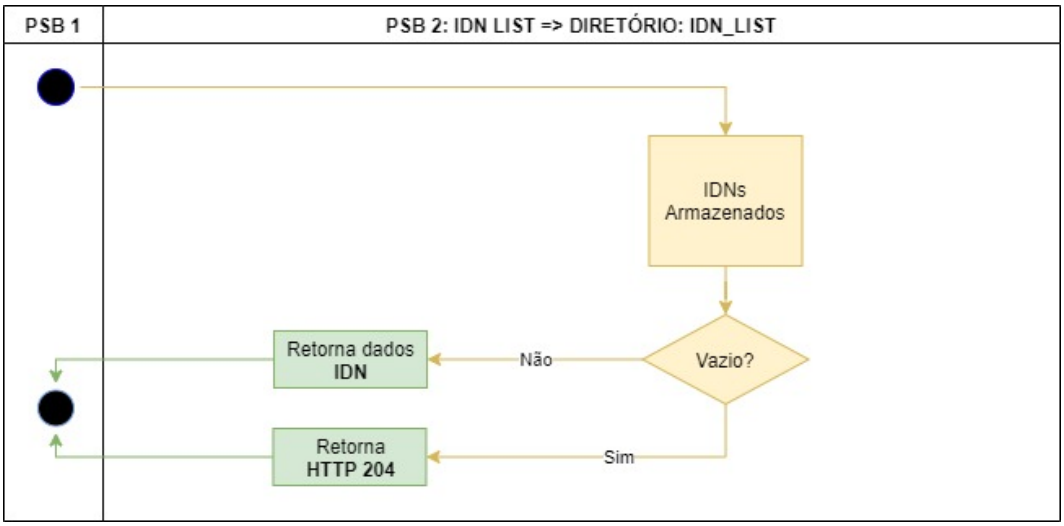

Figura 4.7 – Fluxo do IDN_List.

Tabela 4.2 – Definições dos elementos do fluxo IDE.

Processo de captura	É a entidade responsável pela coleta de dados biométricos e biográficos(`CPF`) de uma pessoa. Também é responsável por resolver exceções ou erros.
NIST Package 1	É o pacote ANSI/NIST com `|CPF|` e os dados biométricos associados.
NIST Acceptance	O pacote ANSI/NIST vai para o PSB 1.
NIST válido?	Verifica se os campos e a qualidade das biometrias estão corretos. Se estiver ok (sim), vai para o HSM. Se não estiver ok (não), o processo termina com um código de erro 999, indicando à entidade de captura que o pacote NIST está incorreto ou corrompido.
HSM	Transforma o `CPF` em IDN, usando Algoritmo 1.
NIST Package 2	É o pacote ANSI/NIST 2 com o IDN e as biometrias do `CPF` cifrado.
z_query	É o comando para verificar se `z`, com o IDN_i e `TCN_i` de entrada, já existe associado ao IDN_i e `TCN_i` armazendados dentro do banco de dados.
Local z_query	Pesquisa `z` dentro da base local, *i.e.*, aqueles `CPF` que teve a biometria coletada dentro do sistema PSB 1 (incluindo o processo de captura). O banco de dados local possui o IDN_i com o `TCN_i` e as biometrias associadas.

Continua na próxima página

Tabela 4.2

Cache z _query	Pesquisa `z` dentro da base do cache, *i.e.*, aqueles `CPF` que teveram a biometria coletada dentro do sistema PSB 2. O banco de dados de cache do PSB 1 possui o IDN_i com o `TCN_i` e biometria associada do PSB 2.
z existe?	Verifica se o `z` ($IDN_i \oplus nonce$), do Algoritmo **??**, é encontrado. Se não, ele vai para a pesquisa 1:N na lista negativa. Caso exista (sim), o processo termina com um código de erro 200, indicando que o `CPF` já foi registrado e que um processo de verificação (1: 1) pode ser realizado.
1:N Blacklist	Verifica se os dados biométricos coletados estão entre os fraudadores já detectados.
Hit?	Se não (não), ele vai para uma pesquisa biométrica 1:N. Se houver acerto/correspondência (sim), os prováveis candidatos são reunidos e apresentados à entidade responsável pelo processo de captura. A entidade deve decidir se é, de fato, um fraudador (interromper o fluxo de trabalho) ou um falso positivo (continuar o fluxo de trabalho).
Gather Candidates	É a lista de candidatos da lista negativa.
1:N Local	Pesquisa (1: N) o banco de dados local para biometria duplicada.
Hit?	Caso seja encontrado o mesmo dado biométrico (sim), os prováveis candidatos são reunidos e apresentados à entidade responsável pelo processo de captura. A entidade deve decidir se é, de fato, um fraudador, *i.e.*, a mesma biometria encontrada para diferentes `z` (interromper o fluxo de trabalho) ou um falso positivo (continuar o fluxo de trabalho). Se nenhuma biometria for encontrada (não), ele vai para a pesquisa 1:N no banco de dados de cache e para um `IDE` ao PSB 2.
Gather Candidates	É a lista de candidatos do Local 1: N.
1:N Cache	Pesquisa (1: N) do banco de dados em cache para biometria duplicada. O banco de dados de cache do PSB 1 e o banco de dados local do PSB 2 devem ser iguais.
HUB:IDE	É a transação de identificação (solicitação 1:N) para processamento no PSB 2. Um pacote ANSI/NIST 2 com o IDN e a biometria associada. Além disso, a solicitação vai com o parâmetro do `TCN`.

Continua na próxima página

Tabela 4.2

IDE - PSB 1	Pesquisa (1:N) o banco de dados local para biometria duplicada em PSB 2.
Respostas	Existem duas respostas: uma é do banco de dados de cache do PSB 1 e a outra é do banco de dados local do PSB 2 (`VRE X` nenhuma biometria foi encontrada; `VRE M` pelo menos uma biometria foi encontrada). O cache do PSB 1 deve ser igual ao banco de dados local do PSB 2, portanto, espera-se as mesmas respostas. A razão de verificar, novamente, esta resposta é para garantir que as respostas estejam as mesmas (*e.g.* calibrar acurária da pesquisa biométrica). Caso contrário, a entidade responsável pela parte de captura deve resolver este problema atualizando o banco de dados de cache ou comunicando-se com a entidade da parte de captura do PSB 2.
Hit?	Caso seja encontrado mesmos dados biométricos (sim), os prováveis candidatos são reunidos e apresentados à entidade responsável pelo processo de captura. A entidade deve atualizar o banco de dados de cache ou se comunicar com a entidade PSB 2 para resolver o problema. Se nenhuma biometria for encontrada (não), chega-se a etapa final deste fluxo que é a publicação do IDN.
Gather Candidates	É a lista de candidatos do cache 1:N ou advindas do PSB 2 no processo do `IDE`.
HUB:Change_Status	É a confirmação para o PSB 2 de que o IDN está pronto para ser registrado, associado a um `TCN` e a sua respectiva biometria.
Cache	PSB 2 armazena o IDN, com o `TCN` e a biometria associada.

F) change_status

É uma mensagem de confirmação do PSB, mostrando o status finalizado de um processo de identificação. Ela garante que o PSB possa armazenar a tupla IDN e `TCN`, associados à biometria, no banco de dados, incluindo o cache. A Figura 4.11 mostra a sequência de eventos entre as transações de `IDE` e `change_status`.

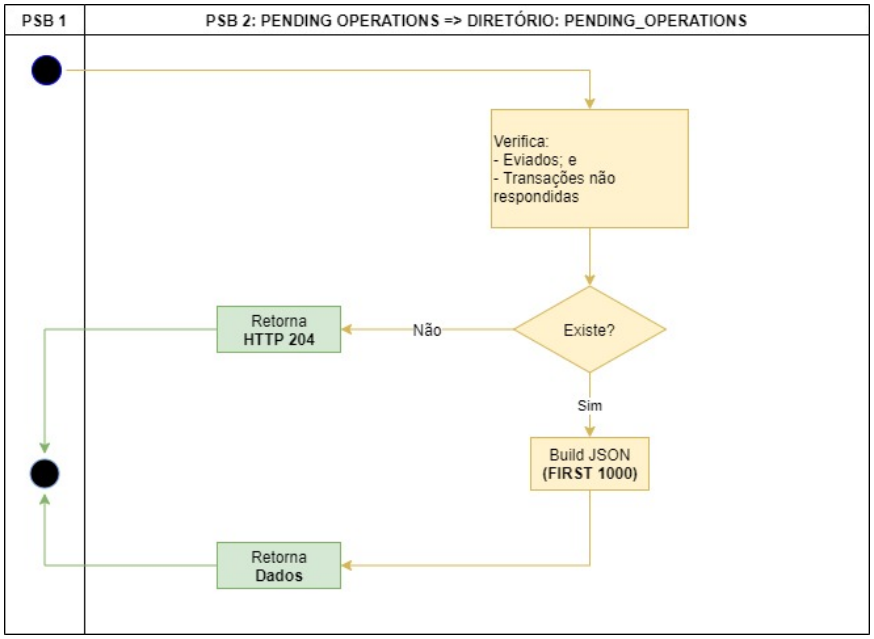

Figura 4.8 – Fluxo do pending_operations.

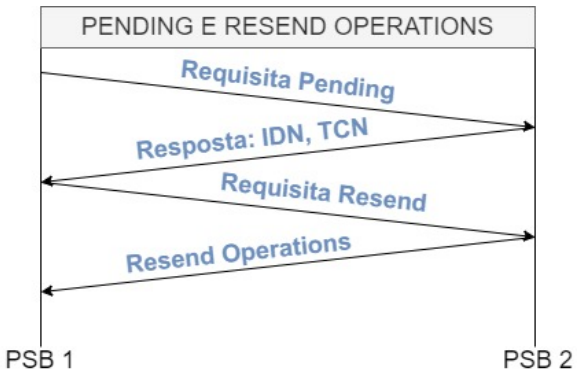

Figura 4.9 – Sequência de eventos para o pending_operations e o resend_operations.

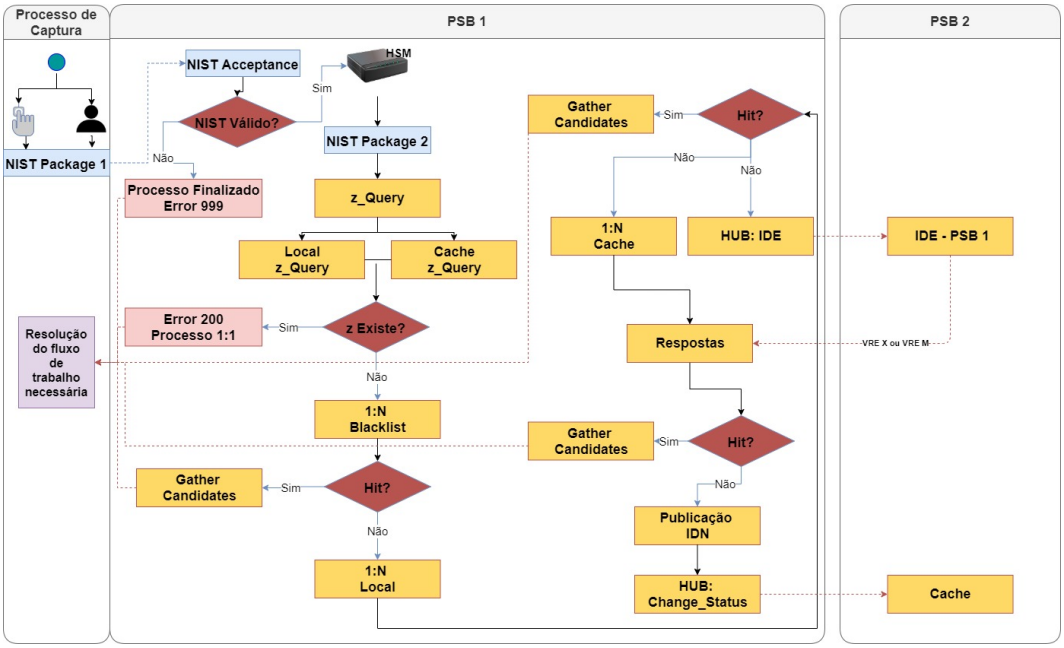

Figura 4.10 – Processo de identificação e verificação na rede biométrica proposta.

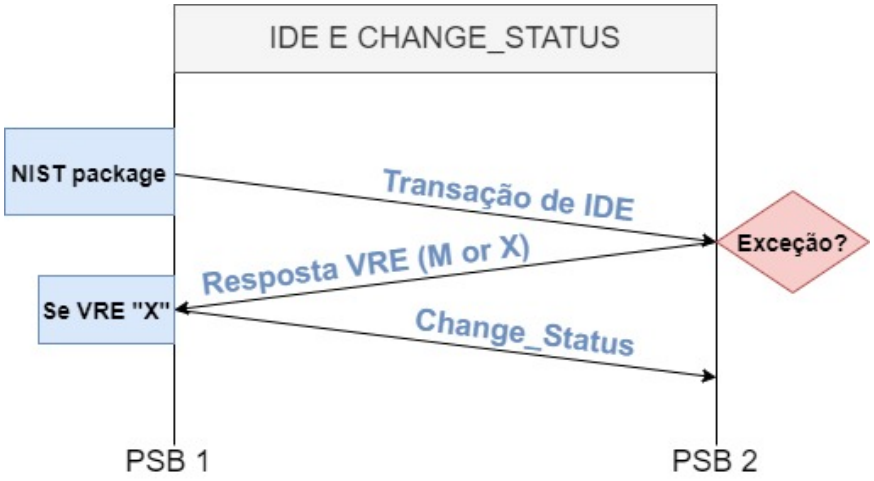

Figura 4.11 – Sequência de eventos para o IDE e o change_status.

4.3 CONSIDERAÇÕES FINAIS SOBRE A PROPOSTA

Nesta subseção, serão feitas considerações finais sobre a proposta colacionada. Em primeiro plano, qualquer rede biométrica pode adotar os conceitos aqui descritos, visto se tratar de processos que se utilizam de algoritmos e bibliotecas abertos, notoriamente conhecidos e com ampla documentação. Uma das funções da proposta é não depender de sistemas proprietários para garantir a segurança de um dado e, ao mesmo tempo, fazer com que os sistemas se comuniquem por meio de um protocolo de comunicação confiável e interoperável, que endereça eventuais problemas em uma rede biométrica. Além deste trabalho garantir a privacidade, a segurança e a interoperabilidade de redes biométricas na arquitetura demonstrada, especificamente, esta pesquisa melhora dois normativos internacionais, comentados a seguir.

A proposta criptográfica tem a capacidade de mudar o item “13.2.4.4.1 N32-f key hierarchy", do “Security architecture and procedures for 5G system (Release 15 - Rel 15)” [51]. O Rel-15 descreve o uso de um esquema criptográfico simétrico, usando o algoritmo AES, para o Non Access Stratum (NAS), para as mensagens de integridade, transferência e proteção do “User Plane” (UP) e “Access Stratum” (AS), e para sinalização de “Radio Resource Control” (RRC). Conforme apresentado, o Rel-15 pode adotar os conceitos do novo `iv` e `nonce` calculados localmente para o algoritmo AES, e que não precisam ser enviados pela rede 5G. Todos os “User Equipments” (UE) e os dispositivos integrados na rede 5G podem calcular o mesmo `iv` e `nonce`, usando o segredo compartilhado `k`, já existente nas redes 5G, e, *e.g.*, o Identificador Permanente de Assinatura (SUPI), ou outro valor conhecido entre os dispositivos fornecidos a ambos os lados da rede, após o processo de autenticação usando chaves públicas. Isso mitigaria uma série de possíveis ataques às redes 5G, além de não ser necessário qualquer envio de dados referente ao usuário, *e.g.*, como o SUPI.

O outro documento normativo que esta pesquisa tem a aderência de melhorar, conforme descrito, é o IEEE BOPS [3]. A API do IEEE BOPS, entre os fluxos “sessionstatus” e “sessiondata”, não possui mensagens que garantam a integridade das transações de dados biométricos entre o cliente/servidor. Sugere-se, então, a inserção de uma subseção sobre “Integridade” no IEEE BOPS, incluindo uma chamada de “sessionIntegrity”, entre “sessionstatus” e “sessiondata”, no procedimento de “Role Gathering”, considerando comandos propostos na API, apresentada no Apêndice A. Esses comandos podem ser imediatamente inseridos no normativo da IEEE, visto que são aderentes e em formato JSON, o mesmo proposto pelo BOPS.

Em continuidade, será apresentado e comentado a análise de segurança desta proposta. Será visto que a mesma possui elementos que permitem anonimizar um indexador utilizando as técnicas propostas, com probabilidade insignificante, e com alta complexidade, de um ataque ser bem sucedido. As evidêndias e provas são suficiente para a segurança da arquitetura implementada.

5 ANÁLISE DE SEGURANÇA

Este capítulo está dividido em três áreas de análise de segurança das propostas desta dissertação. A primeira e a segunda estão focadas na criptoanálise das técnicas criptográficas propostas, principalmente na aleatoriedade da chave secreta [43] e segurança semântica (SS) [52], encaminhada pela notação de segurança indistinguível (IND) [53]. A terceira análise é baseada na segurança das operações de rede. Para as definições de segurança deste documento, a não-maleabilidade (NM) implica IND. Para o ataque adaptável de texto cifrado escolhido (CCA2), IND também implica em NM [53]. SS é equivalente a IND no modelo de ataque de texto em claro (CPA) [52], mas não nos modelos de ataque de texto cifrado escolhido (CCA) [53].

5.1 CRIPTOANÁLISE

5.1.1 Aleatoriedade da chave k

A chave secreta `k` é gerada de forma aleatória [43].

Prova.

Para realizar a análise formal das chaves que são geradas pelo HSM *offline*, usa-se o conjunto de testes NIST [43]. Compilamos os testes “make iid" e‘ ‘make non_iid" usando as bibliotecas “libdivsufsort-dev / libbz2-dev", usando o sistema operacional Ubuntu 18.04, com os seguintes resultados:

```
NIST IID test

./ea_iid -i keys.bin
Calculating baseline statistics...
H_original: 7.886548
H_bitstring: 0.998301
min(H_original, 8 X H_bitstring):
7.886548
** Passed chi square tests
** Passed length of longest
```

```
repeated substring test
Beginning initial tests...
Beginning permutation tests... these
may take some time
** Passed IID permutation tests

NIST Non-IID test

./ea_non_iid -i keys.bin
Running non-IID tests...
Running Most Common Value Estimate...
Running Entropic Statistic Estimates
(bit strings only)...
Running Tuple Estimates...
Running Predictor Estimates...
H_original: 7.718814
H_bitstring: 0.932005
min(H_original, 8 X H_bitstring):
7.456043
```

Este resultado, inclusive com os valores de entropia resultantes, prova que o conjunto de testes oficial do NIST aprova a aleatoriedade das chaves (k) que são geradas para o esquema proposto.

■

5.1.2 SS e IND

DEFINIÇÃO 5.1 (CPF) O CPF é dado por:

$$CPF = (d_0; d_1; d_2; d_3; d_4; d_5; d_6; d_7; d_8; d_9; d_{10}),$$

em que d_n é um dígito decimal que é representado por um bloco de octetos. Nas oito primeiras posições do CPF, cada bloco de octetos possui uma entropia de 4 bits. A nona posição representa uma posição do estado brasileiro. As duas últimas posições são dígitos verificadores, completando os onze dígitos, e são calculadas de acordo com as nove e dez primeiras, *i.e.*, $d_9 = ((\sum_{i=0}^{8} d_i * (i+1))mod11)mod10$; e $d_{10} = (((\sum_{i=0}^{9} d_i * i)mod11)mod10$.

5.1.2.1 Ataques de aniverário e biclique

O IDN é seguro contra os ataques de aniversário [54, 55] e *biclique* [56] para qualquer adversário $\mathcal{A}$.

Prova.

Para provar que o esquema IDN proposto é seguro contra os ataques de aniversário e *biclique*, é necessário detalhar a entropia dos novos, aleatórios e calculados localmente `iv` e `nonce` criados. Para o `iv`, concatena-se o `CPF` de 88 bits até o comprimento de 256 bits e, depois, com a chave `k` de 256 bits, resultando em um comprimento de 512 bits. Usa-se a entropia de uma variável aleatória uniforme e independente do algortimo SHA-256, resultando em uma *string* de 256 bits, o que converge esse resultado a um esforço de saída com entropia de $\log_2((1-1/e)\times 2^{256})$ [55]. Para `nonce` concatena-se os 256 bits mais valiosos do `TCN` com a chave `k` de 256 bits. Calcula-se o SHA-256 dessa concatenação, levando um comprimento de 256 bits. Visto para `nonce` o mesmo nível de segurança do parâmetro `iv`.

O bloco contendo `CPF` é preenchido até 128 bits para entrada no AES-CBC. É feito um XOR com o `iv` aleatório de 128 bits para cada entrada, resultando em um $blockCPF \in \{0,1\}^{128}$ aleatório. Em vez de reiniciar o AES-256-CBC com o resultado anterior e um vetor de inicialização que tem que ser enviado pela rede, nesta proposta faz-se um XOR na entrada do bloco do AES-256-CBC com um vetor de inicialização `iv` aleatório e local de 128 bits para cada entrada (e esse vetor de inicialização não é enviado pela rede), derivado a partir de parâmetros conhecidos (`k` e `CPF`) apenas para o PSB da rede. Este processo leva ao esquema proposto de criptografia a um esforço de entropia de 256 bits. O `nonce` é XOR com o resultado do AES-256-CBC (`z`), gerando o IDN, levando a um esforço de entropia de 128 bits.

$\mathcal{A}$ não pode ter o controle dos bits de entrada calculados pelo XOR dos parâmetros aleatórios `iv` e `nonce`. O esforço do custo computacional, para o nosso esquema de IDNs, para encontrar uma colisão é de aproximadamente $2^{n/2}$ [57], n = 256 (`k`-bit), para ataques de aniversário. Além disso, o esforço dd custo computacional para uma recuperação de chave em ataques *biclique* é superior a 2^{250}-bit, para dados de 2^{40} e em um ataque de pré-imagem é superior a 2^{120}, ambos 14 rodadas do AES [56, 58, 59]. Portanto, este esforço computacional torna os ataques inviáveis em tempo polinomial, *i.e.*, não é possível calcular do texto em claro `CPF` ao IDN ou do IDN ao texto em claro `CPF`, garantindo o anonimato dos dados. ■

Essa abordagem evita outras séries de ataques conhecidos na literatura que serão aborda-

dos em seguida.

5.1.2.2 CCA e CCA2

IDN é seguro contra CCA e CCA2 - [60, 53] para qualquer adversário $\mathcal{A}$.

Prova.

Os parâmetros `iv` e `nonce` não são enviados pela rede. Eles são calculados e usados apenas dentro do módulo criptográfico do HSM do PSB. Portanto, *e.g.*, $\texttt{iv} \oplus t, AES\text{-}256\text{-}CBC(iv \oplus CPF)$ não pode ser calculado por $\mathcal{A}$. A mesma abordagem pode ser feita para o parâmetro `nonce`. As únicas informações enviadas pela rede (e armazenadas nos bancos de dados) são o texto cifrado IDN e o `TCN`. Os cálculos de `iv` e `nonce` no esquema do IDN proposto são inviáveis para qualquer $\mathcal{A}$. Consegue-se demonstrar que, mesmo usando AES-CBC, o IDN é seguro contra CCA e CCA2, visto a modificação que foi realizada nesta pesquisa, de forma inédita, até onde se tem conhecimento, do vetor de inicialização do algoritmo AES-CBC. ■

5.1.2.3 Padding Oracle Attack

IDN é seguro contra POA - [61] para qualquer adversário $\mathcal{A}$.

Prova.

Cada 128-bit `CPF` do bloco de entrada AES-256-CBC é sempre XOR-ed com um elemento aleatório de 128 bits, *i.e.*, o `iv`. Este atua como *One Time Pad* (OTP) para cada mensagem de entrada no bloco AES-256-CBC. Nenhuma cifra do bloco está vinculada às anteriores. Reinicia-se o bloco do esquema proposto não mais com *feedback* da saída anterior do AES-256-CBC, que usa comumente um vetor de inicialização escolhido exclusivo para a rede, mas sim com um `iv` local e aleatório, com 128 bits de comprimento. Como as cifras de bloco não podem ser vinculadas a outras e `iv` e a entrada do bloco é desconhecida para qualquer $\mathcal{A}$, a execução de um ataque de preenchimento (POA) não é viável. ■

5.1.2.4 CPA

IDN é seguro contra CPA - [60] para qualquer adversário $\mathcal{A}$.

Prova.

O esquema proposto gera um AES-256-CBC calculado no módulo criptográfico do HSM de cada PSB, com um `iv` local e aleatório. O resultado do AES-256-CBC é XOR-ed com um `nonce` local e aleatório. Como mostrado, desde que `iv` e `nonce` mantenham aleatórios e não previsíveis, estes não podem ser calculados por um $\mathcal{A}$, *i.e.*, o AES-256-CBC proposto e o IDN resultante não podem ser atacados em tempo polinomial. ■

5.1.2.5 Segurança do processo de encriptação de chave pública - PKE

Para exportar a chave `k` do HSM *offline*, usa-se a operação RSA-OAEP-2048-wrap. Define-se, a seguir, a segurança desta operação.

O RSA-OAEP-2048-wrap proposto é SS [41], encaminhado pelas notações IND-CPA, IND-CCA1, e IND-CCA2 PKE [41], contra qualquer adversário $\mathcal{A}$.

Prova.

Usa-se a estrutura de codificação de preenchimento RSA-2048-OAEP bits, para uma mensagem m, no módulo criptográfico do HSM. Recuperando uma mensagem $m \in \{0,1\}^*$, um $\mathcal{A}$ deve calcular $r = Y \oplus H(X)$, $H : \{0,1\}^{k-k_0} \rightarrow \{0,1\}^{k_0}$ é o Oracle aleatório (RO), $Y = r \oplus H(X)$ e $X = G(r) \oplus m_{padded}$, em que $G : \{0,1\}^{k_0} \rightarrow \{0,1\}^{k-k_0}$ é um RO. A estrutura de codificação fornece $RSA - OAEP(m_b) = RSA(X||Y)$, em que $b \in \{0,1\}$. Como o OAEP inclui um valor aleatório uniforme em m_{padded}, $\mathcal{A}$ não pode recuperar $X||Y$, o que depende da dificuldade do problema de fatoração RSA-2048 bits [35]. Um $\mathcal{A}$ não consegue adivinhar b e $\mathcal{A}[(k)]$ são insignificantes para um CPA.

De acordo com Fujisaki *et al.* [62], supõe-se que y^* seja um texto cifrado de desafio e m_b, r^* seja um número inteiro aleatório e siga a mesma iteração de a criptografia Oracle OAEP comentada. Para um s não consultado pelo RO $H(s)$, tem-se uma distribuição aleatória uniforme de $H(s)$ e $r = t \oplus H(s)$. Portanto, existe uma pequena probabilidade de que $t \oplus H(s)$ seja consultado por um RO G ou se refira a r^*, levando a um $G(r)$ aleatório e há uma probabilidade menor de que 0^{k_1} são calculados, levando as rejeições de descriptografia do Oracle. Ao rejeitar, $\mathcal{A}$ não pode combinar as listas do Oracle para uma pré-imagem de y, indicando que o RSA-OAEP-2048-bit é IND-CCA1 e também IND-CCA2 esquema de criptografia.

A partir da exposição, assume-se que o PKE proposto é SS. A dificuldade de inverter a função RSA de alto expoente e o modelo de segurança RO, *i.e.*, sob a constatação de que as funções *hash* usadas no esquema se comportam como RO, prova que nosso esquema PKE é seguro, considerando a nota encontrada na RFC 8017 [35]. Usa-se o

algoritmo SHA-256 [31] para o esquema proposto. A implementação RSA-2048-OAEP torna $adv[(k)]$ desprezível. ■

5.1.2.6 Outros ataques

Outros ataques e métodos significativos devem ser considerados. Para o algoritmo AES-256-CBC, um ataque de bumerangue amplificado com chave relacionada tem uma complexidade de $2^{99,5}$-bit, em 14 rodadas para dados de $2^{99,5}$ [63]. A diculdade de explorar o RSA-2048, usando *Number Field Sieve*, tem uma complexidade de 2^{112} [64, 65]. Além disso, os HSM *offline* de cada PSB implementam cálculos criptográficos em tempo constante, com núcleos e bibliotecas resistentes à análise de potência diferencial, incorporados em um módulo criptográfico seguro, credenciado pelo conjunto de testes FIPS [34]. Esta abordagem evita ataques de canais laterais, *e.g.*, ataques de tempo [27, 66], análise de potência [67] e análise de falhas [68].

5.2 SEGURANÇA DE REDE

Comenta-se alguns possíveis ataques a dispositivos e redes, apontando as contramedidas de cada um deles. O `k` embrulhado é importado em uma cerimônia local no ambiente de segurança do PSB. Todos os HSMs offline e PSB [34] possuem um recurso que não permite nenhuma cópia ou uso indevido do `k` não exportável. No slot, o administrador principal raiz pode apenas criar ou destruir o espaço lógico, mas nunca obterá a propriedade do slot. Os HSM do PSB têm outros recursos de segurança incorporados, *e.g.*, autenticação de vários níveis, acesso dividido entre operadores, IDS (Intrusion Detection System), violações não-físicas, mecânicas, químicas e proteção contra injeção de Structured Query Language (SQL) [34, 32].

Os canais autenticados mutuamente para toda a comunicação são feitos usando um TLS/ SSL (RSA-2048 bits) [69], que inclui o *processo de coleta* no PSB e entre os PSB. É informado, por uma lista de serviços biométricos confiáveis assinados, cada um dos pontos finais de IP e URL do PSB credenciados. Existem firewalls dedicados que definem apenas o IP da rota de cada PSB. Os pacotes biométricos ANSI/NIST têm o nome do PSB emissor e de destino. Todos os nomes são recuperados do certificado incorporado na lista confiável. Além de todas as partes da rede mencionadas, o PSB usa a sincronização de tempo com uma fonte de tempo confiável com um carimbo de data/hora para troca de transações. A partir dessa exposição, ataques de repetição [70] e ataques de DoS distribuídos [71] podem ser mitigados.

5.3 CONSIDERAÇÕES FINAIS SOBRE A ANÁLISE DE SEGURANÇA

Foram apresentados, neste Capítulo, a criptoanálise e concepções de segurança de rede do esquema proposto. Conforme foi mostrado, a proposta, do ponto de vista criptográfico, gera uma alta complexidade, tornando a probabilidade de um ataque ser bem sucedido insignificante. Desde que a chave seja secreta e usada somente pelos partícipes da rede (premissa dos sistemas de primitivas criptgráficas), no escopo simétrico e assimétrico, os dados indexadores de um indíviduo permanecem anônimos e não é possível derivar um dado biográfico de um indivíduo da sua cifra, e vice-versa. Garante-se, então, mesmo em um caso de vazamento de dados, o anonimato das pessoas nesta rede prototipada.

Ademais, aborda-se os aspectos relativos a segurança da rede. Não é proposta desta pesquisa aprimorar qualquer dessas abordagens, mas consigna-se que foram usados os processos que, pela literatura e certificações internacionais, tornam os equipamentos e comunicações na rede seguros. Em suma, o proposto neste Capítulo, encontra-se aderente, em termos de segurança, a um esquema que visa proteger os dados e interoperá-los. Conforme será mostrado no próximo Capítulo, os resultados demonstram a viabilidade da rede para operação entre entidades biométricas.

6 APRESENTAÇÃO E AVALIAÇÃO DOS RESULTADOS

Inicialmente, neste Capítulo, discorre-se sobre a avaliação de segurança do esquema proposto. Apresenta-se um quadro em que são mostrados os resultados obtidos em termos da complexidade computacional e probabilidade/viabilidade para que cada ataque ocorra. Em seguida, demonstra-se os resultados, passo-a-passo, do IDN proposto utilizando uma chave `k`, um `CPF` e um `TCN` de testes. Por fim, apresenta-se os resultados do novo protocolo de comunicação de interoperabilidade, com um IDN advindo de um `CPF` real.

6.1 AMOSTRA E DISCUSSÃO SOBRE O ALGORITMO DO IDN

6.1.1 Resultados da avaliação de segurança

A Tabela 6.1 mostra os resultados da avaliação de segurança do esquema proposto. Com base no Capítulo 5, mostra-se a complexidade e o método aplicado para uma probabilidade insignificante de cada ataque.

A principal contribuição criptográfica desta pesquisa é a formação dos parâmetros `iv` e `nonce`. O `iv` e `nonce` possuem 128 bits aleatórios e não são enviados pela rede, operando localmente nos PSB e recalculados para cada entrada de `CPF`. Conseqüentemente, um $\mathcal{A}$ não pode prever, calcular ou impor em um tempo polinomial o `iv` e o `nonce`, revogando assim ataques significativos contra o esquema IDN proposto, incluindo o CCA e CCA2 contra o AES-256-CBC, conforme já demonstrado. A complexidade de quebrar o IDN proposto não é viável em um ataque de tempo polinomial. A complexidade da implementação do OAEP se baseia em encontrar uma colisão no RO $\leftarrow$ SHA-256 e na dificuldade de quebrar o RSA-2048-bits. Todo o armazenamento e cálculo são feitos dentro do módulo criptográficos dos HSM FIPS, com a chave`k` também aleatória, aplicando contramedidas contra ataques de canais laterais, com o recurso de ativo não exportável no seu *slot* de armazenamento. O principal resultado do esquema proposto é a segurança, com privacidade em relação aos dados de uma pessoa, que pode-se aplicar em redes e bancos de dados biométricos.

Para operação da rede, garantindo o protocolo de interoperabilidade, práticas conhecidas foram implementadas para mitigar ataques. Canais de comunicação SSL mutuamente reconhecidos, protocolos IPsec, com IP e URL declardos para as configurações de *firewall*, PSB sincronizados com data e hora, entre outros. Esses métodos podem atenuar, *e.g.*, DDoS (*Distributed Denial of Service*) e ataques de repetição.

Tabela 6.1 – Resultado da avaliação de segurança.

Ataques	Complexidade	Probabilidade	Método aplicado
Aniversário	$2^{256/2}$	$\Pr[] \geq 0.5$	Algoritmo do IDN
Related-Key Boomerang	$2^{99.5}$	$\Pr[] = 1$	AES-256-CBC
Biclique	$\sim 2^{254}$; $\sim 2^{126}$	$\Pr[] = 1$; $\Pr[] = 0.63$	AES-256-CBC
CCA	2^{128}	$\Pr[] = 1$	Algoritmo do IDN
POA	2^{128}	$\Pr[] = 1$	AES-256-CBC
CPA	2^{128}	$\Pr[] = 1$	AES-256-CBC, com Algoritmo do IDN `iv`
IND-CPA	$2^{\log_2((1-1/e)\times 2^{256})}$; 2^{112}	$\Pr[] \geq 0.5$; $\Pr[] = 1$; $\mathsf{Adv}^{\mathrm{f}}_{\mathcal{A}_{1,2}}(k) \sim insignificante$	RO $\leftarrow$ SHA-256; RSA-OAEP-2048
IND-CCA1	$2^{\log_2((1-1/e)\times 2^{256})}$; 2^{112}	$\Pr[] \geq 0.5$; $\Pr[] = 1$; $\mathsf{Adv}^{\mathrm{f}}_{\mathcal{A}_{1,2}}(k) \sim insignificante$	RO $\leftarrow$ SHA-256; RSA-OAEP-2048
IND-CCA2	$2^{\log_2((1-1/e)\times 2^{256})}$; 2^{112}	$\Pr[] \geq 0.5$; $\Pr[] = 1$; $\mathsf{Adv}^{\mathrm{f}}_{\mathcal{A}_{1,2}}(k) \sim insignificante$	RO $\leftarrow$ SHA-256; RSA-OAEP-2048
NFS	2^{112}	$\Pr[] = 1$	RSA-2048
Timming	-	insignificante	Tempo-Constante
Power Analysis	-	insignificante	Núcleos e bibliotecas resistentes a DPA
Fault Analysis	-	insignificante	Prevenção contra ataques de Injeção; Redundância de hardware e sincronismo de tempo; *Operation Hiding*; *Blinding Infection*; Proteção de protocolo
(D)DoS	-	insignificante	SSL mútuo; IPsec; IDS; PSB IP e URL de serviço conhecidos
Replay	-	insignificante	SSL mútuo; Âncora e carimbo de tempo

6.1.2 Demonstração da construção do esquema IDN proposto

A seguir, mostra-se o *script* do IDN executado no módulo criptográfico de um HSM, usando bibliotecas do OpenSSL:

Input: “CPF”, “TCN”, “Key.key”

Output: IDN

Initialization:

```
read CPF
read TCN
CPFhex=$(echo -n $CPF | xxd -p)
CPFEXT="$CPFhex$CPFhex$CPFhex"
CPFEXT="${CPFEXT:0:64}"
K="$(echo $(hexdump -v -e '/1 "%02X" ' < Key.key))"
KCPF="$K$CPFEXT"
KCPF="${KCPF:0:128}"
shaX=$(echo -n $KCPF | xxd -p -r | sha256sum | cut -d ' ' -f 1)
A="${shaX:0:32}"
B="${shaX:32:32}"
IV = ""
for ((i=0; i < ${#A}; i+=2 ))
do
Ai = $((16#${A:$i:2}))
Bi = $((16#${B:$i:2}))
xorAB = $(( Ai ^ Bi))
tmp = $(printf '%02x' $xorAB)
IV = "${IV}${tmp}"
done
lData=${#CPFhex}
lPadding=$(( (32 - $lData)/2 ))
blockCPF="${CPFhex}"
tmp=$(printf '%02x' $lPadding)
for ((i=0; i < $lPadding; i++ ))
do
blockCPF="${blockCPF}${tmp}"
done
z=$(echo -n $blockCPF | xxd -p -r | openssl enc -nopad -e -a -nosalt -aes-256-cbc -K $K
-iv $IV)
TCNhex=$(echo -n $TCN | xxd -p)
TCNEXT="${TCNEXT:0:64}"
```

```
KTCN="$K$TCNEXT"
KTCN="${KTCN:0:128}"
shaT=$(echo -n $KTCN | xxd -p -r | sha256sum | cut -d ' ' -f 1)
C="${shaT:0:32}"
D="${shaT:32:32}"
NONCE=""
for ((i=0; i < ${#A}; i+=2 ))
do
Ci=$(( 16#$C:$i:2 ))
Di=$(( 16#$D:$i:2 ))
xorCD=$(( Ci ^ Di ))
tmpnonce=$(printf '%02x' $xorCD)
NONCE="${NONCE}${tmpnonce}"
done
IDN=""
for ((i=0; i < ${#A}; i+=2 ))
do
zi=$(( 16#${z:$i:2} ))
NONCEi=$(( 16#${NONCE:$i:2} ))
xorzNONCE=$(( zi ^ NONCEi ))
tmpidn=$(printf '%02x' $xorzNONCE)
IDN="${IDN}${tmpidn}"
done
```

A tabela 6.2 mostra os cálculos de IDN para o esquema criado. Esses são feitos, seguindo o *script* mostrado, usando um possível (hipotético) `CPF` e `TCN`, com uma chave de teste `k`, gerada a partir do HSM *offline*, para fins experimentais. De acordo com os resultados, `iv`, `nonce`, `z` e IDN não podem ser calculados sem o conhecimento de `k`, associado a `CPF` e `TCN`, *i.e.*, apenas os PSB da rede são capazes de gerar `z` para o mesmo `CPF`. Na subseção 6.2.1 mostra-se um `CPF` real, cifrado para IDN, nesta rede biométrica projetada.

6.1.3 Demonstração da inversão do IDN no texto cifrado z

A seguir, mostra-se o *script* para inversão do IDN no texto cifrado `z`, executado no módulo criptográfico de um HSM, usando bibliotecas do OpenSSL:

Input: "IDN", "TCN", "Key.key"

Output: z

Initialization:

read IDN

Tabela 6.2 – Construção do IDN.

Parâmetro	Valores e Resultados
k	c2ec8d17c0ef9147af75814255513e56d272 31fc73fdd27048240414fbbaa154
CPF	12345678901
TCN	3E59C8E1-F3D2-4F14-B03A-EA45EEF22627
CPFEXT	31323334353637383930313132333435 36 37383930313132333435363738393 0
K||CPFEXT	c2ec8d17c0ef9147af75814255513e56d27231fc73fdd27048240414f bbaa1543132333435363738393031313233343536 37 38393031313233343536373839 30
SHA256 (K||CPFEXT)	0f1d397e009f0f4813b953d5a7688a1f14606ad021d 940a6c8ca97619ed2c042
A	0f1d397e009f0f4813b953d5a7688a1f
B	14606ad021d940a6c8ca97619ed2c042
iv	1b7d53ae21464feedb73c4b439ba4a5d
CPF Block	31323334353637383930310505050505 (padding)
z	c162acd5c93b74e44f35af583d15f497
TCNEXT	33453539433845312D463344322D344631342D42303 3412D4541343545454632
K||TCNEXT	c2ec8d17c0ef9147af75814255513e56d27231fc73fdd27048240414f bbaa1543345353943384531 2D463344322D34463134 2D423033412D454134354545463
SHA256 (K||TCNEXT)	e3b0c44298fc1c149afbf4c8996fb92427ae41e464 9b934ca495991b7852b855
C	e3b0c44298fc1c149afbf4c8996fb924
D	27ae41e4649b934ca495991b7852b855
nonce	c41e85a6fc678f583e6e6dd3e13d0171
IDN	057c2973355cfbbc715bc28bdc28f5e6

```
read TCN
TCNEXT="${TCNEXT:0:64}"
KTCN="$K$TCNEXT"
KTCN="${KTCN:0:128}"
shaT=$(echo -n $KTCN | xxd -p -r | sha256sum | cut -d ' ' -f 1)
C="${shaT:0:32}"
D="${shaT:32:32}"
NONCE=""
for ((i=0; i < ${#A}; i+=2 ))
do
Ci=$(( 16#$C:$i:2 ))
Di=$(( 16#$D:$i:2 ))
xorCD=$(( Ci ^ Di ))
tmpnonce=$(printf '%02x' $xorCD)
NONCE="${NONCE}${tmpnonce}"
done
z=""
for ((i=0; i < ${#A}; i+=2 ))
do
IDNi=$(( 16#${z:$i:2} ))
NONCEi=$(( 16#${NONCE:$i:2} ))
xorIDNNONCE=$(( IDNi ^ NONCEi ))
tmpz=$(printf '%02x' $xorIDNNONCE)
z="${z}${tmpz}"
done
```

A tabela 6.3 mostra os cálculos da inversão do IDN para o texto cifrado `z`. Calcula-se `z` para cada tupla de $IDN//TCN$ de entrada, fazendo o mesmo para cada tupla $IDN_i//TCN_i$ armazenada. De acordo com esses resultados, somente as entidades que possuem `k`, `TCN` e o IDN podem refazer os cálculos e comparar os resultados para as tuplas de entrada e armazenada. Caso `z` seja o mesmo, sabe-se que esse pertence ao mesmo `CPF`.

Tabela 6.3 – Inversão do IDN no texto cifrado z.

Parâmetro	Valores e Resultados
k	c2ec8d17c0ef9147af75814255513e56d272 31fc73fdd27048240414fbbaa154
IDN	057c2973355cfbbc715bc28bdc28f5e6
TCN	3E59C8E1-F3D2-4F14-B03A-EA45EEF22627
TCNEXT	33453539433845312D463344322D344631342D42303 3412D4541343545454632
K||TCNEXT	c2ec8d17c0ef9147af75814255513e56d27231fc73fdd27048240414f bbaa154334535394338453 12D463344322D34463134 2D423033412D454134354545463
SHA256 (K||TCNEXT)	e3b0c44298fc1c149afbf4c8996fb92427ae41e464 9b934ca495991b7852b855
C	e3b0c44298fc1c149afbf4c8996fb924
D	27ae41e4649b934ca495991b7852b855
nonce	c41e85a6fc678f583e6e6dd3e13d0171
z	c162acd5c93b74e44f35af583d15f497

6.2 RESULTADO DO PROTOCOLO DE COMUNICAÇÃO PROPOSTO

6.2.1 O protocolo de comunicação interoperável

Apresenta-se os resultados para o novo protocolo de comunicação de interoperabilidade proposto. A trilha de registro foi extraída do PSB 1, mostrando a comunicação entre o mesmo e o PSB 2, com um IDN (`CPF` cifrado) real e, conforme demonstrado, irreversível. As mensagens das transações de `pending_operation`, com um `IDN_List` e `NIST Acceptance`, de `operation_resend`, e de `IDE`, com um `change_status`, são mostradas.

```
[DIR:RECEIVED] FROM=PSB2; REQUEST=
{"requestType":"pending_operations"}

[DIR:SENT] TO=PSB2; RESULT=
{"pendingOperationsList":[{"operationType":
"1_n_queue","idnList":[{"idn":
"10d548f2fe7559d0a3162bc3db992ff2","tcn":
0BB79BA3-2911-4297-9758-10E0BF975002"}]}]}

[DIR:RECEIVED] FROM=PSB2; REQUEST=
{"requestType":"operation_resend","idn":
```

```
"10d548f2fe7559d0a3162bc3db992ff2",
"tcn":"0BB79BA3-2911-4297-9758-10E0BF975002"}

[DIR:SENT] TO=PSB2;RESULT=
{"response":"IDE","idn":
"10d548f2fe7559d0a3162bc3db992ff2",
"tcn":"0BB79BA3-2911-4297-9758-10E0BF975002"}
```

O `pending_operations` é o mecanismo que garante que todo PSB processe todos os dados transacionados. Ao solicitá-lo, o PSB 2 recebe do PSB 1 toda a lista da tupla IDN e `TCN` que não foram processados. Este comando permite que a rede permaneça íntegra, *i.e.*, sem nenhum processo de identificação ausente. Depois, o PSB 2, que solicitou a operação `pending_operation` e recebeu a lista de IDNs, envia um `operation_resend`, que garante ao PSB 1 que o PSB 2 está pronto para processar as transações ausentes. Imediatamente após indicar que o PSB 2 está pronto, o PSB 1 designado envia, *e.g.*, uma transação de `IDE`.

```
[HUB:SENT] TO=PSB2;TRANSACTION=
{"transaction-type":"IDE","idn":
"66f5a1b3282da4ac74aabf28112c240a","tcn":
"0C490874-B4F5-46ED-B9CB-BEB8E6F71081",
"timestamp":"1575288144418"}

[HUB:RECEIVED] FROM=PSB2;TRANSACTION=
{"transaction-type":"VRE","idn":
"66f5a1b3282da4ac74aabf28112c240a","tcn":
"02FA798D-D81F-43DB-9E44-32489389C470",
"timestamp":"1575288144418","reference-tcn":
"0C490874-B4F5-46ED-B9CB-BEB8E6F71081",
"srf":"X"}

[HUB:SENT] TO=PSB2;REQUEST=
{"requestType":"change_status","idn":"66f5a
1b3282da4ac74aabf28112c240a";
"tcn":"0C490874-B4F5-46ED-B9CB-BEB8E6F71081"}
```

O PSB 1, após executar o processo local mostrado na Figura 4.10, envia uma transação de `IDE`, para o IDN "66f5a1 ...", ao PSB 2. O PSB 2 responde um `VRE` com o valor `X`, *i.e.*, nenhuma biometria foi encontrada no banco de dados biométrico. O PSB 1 en-

via uma mensagem de confirmação `change_status`, concluindo o processo de registro, e o PSB 2 pode armazenar em seu cache. Toda solicitação de `IDE` anexa o pacote `ANSI/NIST Package 2`, com a biometria correspondente para cada IDN. Estes resultados provam que o esquema proposto é seguro, viável e pode ser incorporado ao descritivo do IEEE BOPS, para que esse passe a ter mecanismos de integridade de fluxo de rede.

6.3 COMPARAÇÃO COM OUTROS TRABALHOS

Poucas técnicas, como a proposta desta pesquisa, se referem, ao mesmo tempo, à evidência de segurança e ao anonimato do registro do índice em bancos de dados biométricos. A Tabela 6.4 apresenta trabalhos anteriores publicados para fornecer um esboço informativo das abordagens existentes. Mostra-se que o uso de transformações de recursos e técnicas criptográficas juntamente com sistemas biométricos não é novo. No entanto, até o melhor conhecimento, não havia sido usado para manter a privacidade, com evidências de segurança, e também criar um protocolo de interoperabilidade entre diferentes tecnologias de entidades participantes de uma rede biométrica.

O *framework* IEEE BOPS não possui qualquer mensagem que permita ao dispositivo cliente verificar com sucesso, integridade e possibilidade de recuperação, as transações biométricas. Esta pesquisa, na comparação mostrada na Tabela 6.5, aprimora o IEEE BOPS ao construir mensagens JSON que permitem que as transações biométricas sejam verificadas, processadas e finalizadas, apontando se uma transação não concluiu a tarefa. Além disso, permite utilizar o algoritmo do IDN criado, garantindo o anonimato dos registros que são compartilhados entre os entes partícipes de uma rede biométrica.

Tabela 6.4 – Resumo dos trabalhos relacionados em comparação com a estrutura proposta. Aspectos de segurança, privacidade e interoperabilidade foram considerados.

Trabalhos	Possui uma abordagem de segurança e privacidade dos dados biométricos?	Possui uma abordagem de segurança e privacidade dos dados biográficos?	É seguro contra ataques conhecidos?	A proposta possui algum mecanismo de interoperabilidade?
Lai *et al.* [17]	SIM	NÃO	SIM	NÃO
Lai *et al.* [18]	SIM	NÃO	SIM	NÃO
Nagar *et al.* [16]	SIM	NÃO	SIM	NÃO
Nassir and Perumal [15]	SIM	SIM	NÃO	NÃO
Rathgeb *et al.* [21]	SIM	NÃO	SIM	NÃO
Kumar and Kumar [13]	SIM	NÃO	SIM	NÃO
Li *et al.* [14]	SIM	NÃO	SIM	NÃO
Kaur and Sofat [46]	SIM	NÃO	NÃO	NÃO
Zhou and Ren [12]	SIM	NÃO	SIM	NÃO
Toli and Preneel [11]	SIM	SIM	NÃO	NÃO
Kaur and Khanna [19]	SIM	NÃO	SIM	NÃO
O esquema proposto nesta pesquisa	**SIM**	**SIM**	**SIM**	**SIM**

Tabela 6.5 – Comparação entre o framework IEEE BOPS e esta pesquisa.

Trabalhos	Canal Seguro?	Possui API de interoperabildiade?	Possui mecanismo para verificar integridade dos dados?	Possui mecanismo de recuperação das transações?
IEEE BOPPS [3]	SIM	SIM	NÃO	NÃO
O esquema proposto nesta pesquisa	**SIM**	**SIM**	**SIM**	**SIM**

6.4 AVALIAÇÃO DE DESEMPENHO DA REDE

Descreve-se sobre o desempenho do esquema proposto. Para esta dissertação, desempenho é a eficiência da rede no processamento de transações *on-line*. Os resultados são de uma instância em execução entre o PSB 1 e o PSB 2. Inicialmente, na Tabela 4.1, repisa-se as configurações dos principais componentes usados para esta pesquisa. Em seguida, nominalmente, extrai-se a capacidade criptográfica do HSM. Finalmente, mostra-se o número de `IDE` e `pending_operations` por dia, executando a API proposta ao longo de uma semana. O método aplicado para medir o desempenho foi verificar quantas transações de `IDE` foram enviadas do PSB 1 e quantas transações `pending_operations` o PSB 2 enviou por dia. Esta razão denota a capacidade do PSB 2 de processar transações por demanda dentro do escopo desta pesquisa.

O HSM realiza um auto-teste condicional durante sua operação, de acordo com os parâmetros de certificação FIPS. O número nominal para estabelecer o IDN, rodando o OpenSSL script desta pesquisa, com AES-256-CBC, é superior a 1.000 cifras por segundo. Este desempenho é muito maior do que as transações que são realizadas pela rede proposta. Como será mostrado, a capacidade criptográfica do HSM não prejudica ou interfere no desempenho da rede.

A Figura 6.1 e a Figura 6.2 mostram os resultados obtidos entre transações do PSB 1 e PSB 2. Na Figura 6.1, o PSB 1 enviou (em azul) em média 14.389 transações de `IDE` por dia e recebeu (em laranja), do PSB 2, uma média de 4.284. O total (em cinza) de transações pela rede teve uma média de 18.673. As transações de `pending_operations` do PSB 2 para o PSB 1 tiveram uma média de 266 por dia. O desempenho do esquema proposto, dado pela razão $\frac{nmerodepending\_operations}{nmerodeIDE}$, é de aproximadamente 98,15%.

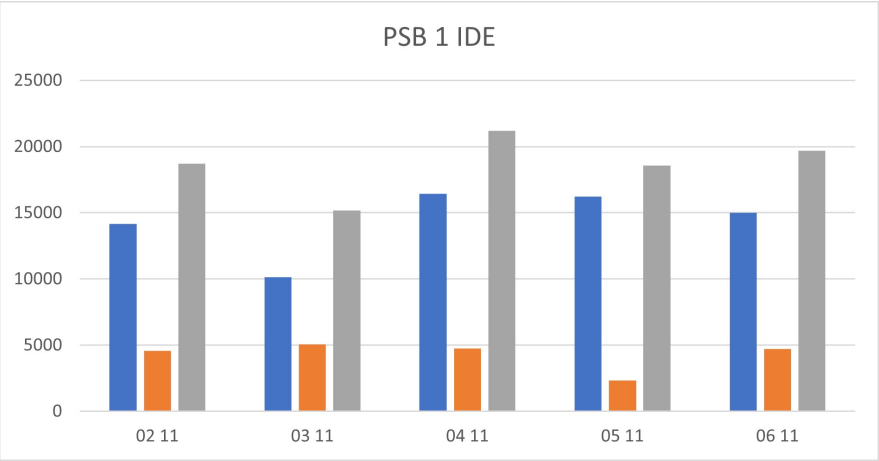

Figura 6.1 – PSB 1: Transações de IDE por uma semana.

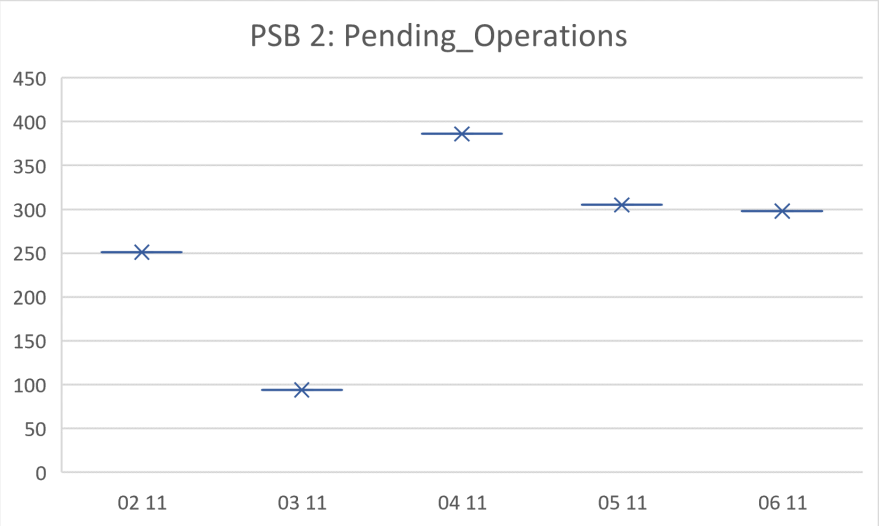

Figura 6.2 – PSB 2: Transações de pending_operation por uma semana.

6.5 CONSIDERAÇÕES FINAIS SOBRE OS RESULTADOS APRESENTADOS

Os resultados demonstram a viabilidade, a segurança e a diferença para os outros trabalhos em relação a proposta apresentada. Destacou-se, inicialmente, a dificuldade relacionada em atacar, com sucesso, esta abordagem em tempo polinomial. A principal contribuição criptográfica dessa dissertação relaciona-se com a mudança na concepção do envio do vetor de inicialização do algoritmo AES em modo CBC. Concebeu-se um novo fluxo para cifrar textos em claro de forma problabílista, endereçando a segurança da chave secreta, sem a necessidade do envio de parâmetros pela rede. Esse fato, para o AES-CBC, mitiga o ataque de CCA e CCA2, tornando este trabalho ainda mais relevante no âmbito criptográfico.

O IDN mostrado, conforme relatado, trata-se de uma informação de um `CPF` real. Nas transações, exibidas por meio de trilhas de auditorias dos serviços, não é possível, em tempo

polinomial, reverter o IDN em `CPF`. Para um adversário, capturar as informações pela rede denotam uma probabilidade insignificante de sucesso na tentativa de expor o texto em claro. O processo apresentado em forma de resultados garante a privacidade do dado pessoal de qualquer indivíduo na rede implementada.

Ademais, mostrou-se a viabilidade de um novo protocolo de interoperabilidade. Esse tem o foco relacionado a comunicação dos dados e a manutenção da integridade das transações realizadas pela rede. Esse fato, conforme pesquisa feita, melhora significativamente as especificações internacionais do IEEE BOPS, padrão de referência em interoperabilidade de transações biométricas.

7 CONCLUSÃO E TRABALHOS FUTUROS

Segurança, privacidade e interoperabilidade devem ser os principais requisitos entre todos os sistemas biométricos implementados. Os bancos de dados e redes biométricos que se comunicam, ou ainda pretendem fazê-lo, devem possuir mecanismos para tratar desses três requisitos, sem que se derive dessa iniciativa soluções proprietárias ou que não possuem evidências de segurança necessárias para proteção dos dados. A operação de sistemas biométricos nessas circunstâncias, *i.e.*, sem condições mínimas de segurança, traz fragilidade à privacidade das informações.

Ademais, deve ser endereçada, em conjunto com a mitigação de possíveis fragilidades, a questão de interoperabildiade entre entidades de uma rede biométrica. Considerando sistemas de identificação e verificação baseados em diferentes estruturas tecnológicas, até esta pesquisa, não se tinha conhecimento de protocolos de comunicação que atendam aos requisitos de troca de dados biométricos pelas redes de forma anônima, protegendo os dados de um indivíduo, com um método de integridade. Em tempos em que leis são editadas e publicadas pelos países com comandos claros para proteção dos dados dos indivíduos e, além, do crescente uso de sistemas biométricos em políticas públicas e iniciativas privadas, resolver esse problema de juntar esses três requisitos torna-se fundamental para qualquer sociedade.

Este trabalho, para resolver o apontado, propôs um novo esquema para juntar segurança, privacidade e interoperabilidade de redes biomértricas. A nova abordagem garante o anonimato de qualquer pessoa dentro de bancos de dados biométricos e ainda permite que eles se comuniquem, executando todos os procedimentos de identificação com segurança. Esquemas de criptografia probabilísticos e um novo protocolo de comunicação foram utilizados para obter privacidade, com evidências de segurança, e interoperabilidade com integridade de transações entre redes biométricas. Para os dados de entrada e uma chave secreta compartilhada entre as entidades participantes da rede, produz-se com sucesso um índice anônimo em todos os bancos de dados representando apenas uma pessoa.

Nesse sentido, esta dissertação apresentou três principais contribuições: (1) Um esquema de encriptação probabilístico de chave simétrica para tratar da segurança e privacidade dos dados; 2) Um esquema de encriptação de chave pública para tratar da proteção da chave simétrica relacionada a (1); e (3) Usando a contribuição (1), uma nova API para garantir a interopearbilidade e integridade dos dados em uma rede biométrica prototipada.

A primeira contribuição cria um algortimo chamado de IDN. O IDN é a forma cifrada que representa uma pessoa em um banco de dados biométrico. Essa cifra se dá pelo uso do algoritmo AES-256-CBC modificado por um vetor de inicialização (`iv`) e parâmetro único

(`nonce`) calculados localmente nas entidades que participam da rede, de forma aleatória, sem que estes sejam enviados pela rede. Significa que além das proteções das comunicações onde trafegam um dado biométrico, na proposta concebida criou-se uma forma de anonimizar (cifrar) os dados de uma pessoa, sem precisar decifrá-los, *e.g.*, como o CPF, adotado neste trabalho. Essa cifra provou-se segurança sufuciente contra diversos ataques efetivos na literatura da criptoanálise.

A segunda contribuição visa proteger o ciclo de vida da chave secreta. Esta pesquisa propôs o uso do alogoritmo RSA-2048-OEAP para criar um envelope cifrado para transporte da chave secreta. Cada HSM das entidades participantes possuem o seu envelope criptográfico que, conforme mostrado, só pode ser aberto por aquele HSM específico. Ademais, o trabalho propôs o uso de um HSM certificado internacionalmente (FIPS, no caso concreto) a fim de usufruir com segurança da função de não exportação da chave secreta. A premissa do uso desses equipamentos trazem uma série de vantagens a segurança do processo, inclusive repelindo ataques conhecidos da literatura contra processadores criptográficos.

A terceira contribuição cria um novo protocolo de comunicação entre entidades biométricas. Independentemente de qual sistema tecnológico biométrico que esteja se utilizando, o novo protocolo é capaz de ofertar que diferentes entes na rede estejam aptos a se comunicar e realizar as operações necessárias, usando, inclusive, o indexador IDN proposto. No âmbito em questão, um dos resultados desta dissertação é uma nova API com funções que garantem, além do processo de identificação, integridade das operações. Essa API, por ser construída em JSON, pode ser incorporada ao conhecido *framework* IEEE BOPS. O padrão internacional IEEE BOPS pode ser aprimorado por meio dessa API, incluindo uma maneira da rede manter suas operações independentemente das contingências, garantindo integridade dos dados e transações.

As análises e resultados mostram que é possível operar redes biométricas conforme proposto. Não é possível, em tempo de execução polinomial, ligar o CPF de uma pessoa ao IDN correspondente, tornando o dado da pessoa totalmente anônimo dentro do banco de dados e das transações biométricas, endereçando privacidade aos dados. Foram adotadas medidas de prevenção de ataques a chave secreta e a rede que, em conjunto com os algortimos utlizados para gerar o anonimato dos dados, endereçam segurança na rede. Por fim, a trilha de logs do protocolo de interoperabilidade estabelce que é possível verificar e encerrar todas as transações que foram realizadas, independentede da contigência que a rede tenha. A propsota mostra-se viável e resolve o problema de aglutinar segurança, privacidade e interoperabilidade em redes biométricas.

Em suma, esta pesquisa produziu com sucesso um índice anônimo e interoperável para todos os bancos de dados representando apenas uma pessoa. Denota-se que o resultado do indexador mantém a privacidade, com relevantes aspectos de segurança, de qualquer dado pessoal de um indivíduo. Ademais, propõe-se que o padrão IEEE BOPS seja aprimorado com o

estabelecimento de uma estrutura adicional para mensagens JSON entre sistemas, incluindo uma maneira de as redes manterem suas operações independentemente de contingências. Esta pesquisa, para além da solução endereçada de promover segurança, privacidade e interoperabilidade em redes biométricas, resolve questões relevantes quanto a implementação que envolve o compartilhamento de dados pessoais, aumentando a segurança e garantindo a privacidade dessas informações.

7.1 PUBLICAÇÕES RELACIONADAS A ESTA PESQUISA

Nesta seção, apresenta-se as publicações dos trabalhos acadêmicos relacionados à presente dissertação. Este estudo, em sua fase inicial de resultados, teve um artigo aceito na *International Conference on Information Systems Security and Privacy* (ICISSP), conforme referência a seguir:

Lacerda Filho, E. and Gonçalves, V. (2020). *Achieving Privacy, Security, and Interoperability among Biometric Networks using Symmetric Encryption*.In Proceedings of the 6th International Conference on Information Systems Security and Privacy - Volume 1: ICISSP, ISBN 978-989-758-399-5, pages 481-489. DOI: 10.5220/0008961504810489.

Este artigo cria o algoritmo IDN, ainda proposto de maneira determinística. Estabelece, também, o procedimento de importação e proteção da chave secreta. Apresenta o conceito da rede biométrica, mas ainda sem especificar todas as mensagens e sem a API formatada. Esse trabalho foi apresentado na Conferência Internacional ICISSP 2020, sediada em Malta, na trilha dos algortimos criptográficos. Posteriormente, seu *proceedings* foi publicado pela Scitepress Digital Library.

Esta pesquisa também foi submetida ao Journal IEEE Access:

Lacerda Filho, E.M; Rocha Filho, G.P; Sousa Junior, R.T. and Gonçalves, V.P. (2020) "Improving Data Security, Privacy, and Interoperability for the IEEE Biometric Open Protocol Standard" is presently being given full consideration for publication in IEEE Access. Impact Factor 3.745. Qualis A1.

Nesta submissão, no qual o *rebutal* foi enviado no dia 23/11/2020, apresentou-se o algortimo IDN de forma probabilística, com uma extensa avaliação de segurança do mesmo. Destacam-se os cálculos dos parâmetros do vetor de inicialização e do valor único (*nonce*). Detalha-se ainda mais o processo do ciclo de vida e proteção da chave privada, com os *scripts* usados para cifrar e decifrar os envelopes de transporte. Apresenta-se de forma definitiva as contribuições sobre o novo protocolo de interoperabilidade, incidindo em uma melhoria de processos do IEEE BOPS. Aponta-se como solução uma API, em linguagem JSON, que pode ser incorporada na documentação do IEEE BOPS.

Ainda no campo das publicações, foi realizado um pedido de registro de software. Esse pedido for registrado sob o protocolo: 870200154940. Esse pedido foi concebido pela criação da API de interoperabilidade, demonstrada a inovação dos procedimentos ali contidos para redes biométricas. A inovação é trazida pelo fluxo de mensagens de reconhecimento do status de uma transação, conforme explicado nesta dissertaçao. A API foi escrita em linguagem JSON.

7.2 LIMITAÇÕES DA PESQUISA

Devido a pandemia relacionada ao vírus COVID-19, houve algumas limitações desta pesquisa no âmbito da extração de dados da fase 6 mencionada no Capítulo 1. O acesso aos laboratórios no ano de 2020, entre o período de 17/03/2020 até a presente fase de entrega desta dissertação, ficou inviabilizado. Isso fez com que a extração dos registros referentes aos ativos da arquitetura implementada, mais especificamente dos HSM e dos motores biométricos, não pudessem ser feitas. Devido à natureza desses equipamentos (equipamentos de segurança), onde estão implementados (O ITI impõe rígidas regras de acesso) e os procedimentos adotados nesta pesquisa, *e.g.*, importação da chave secreta com a característica de "não exportação", os registros só podem ser acessados *in loco*. A Universidade de Brasília não possui equipamentos desta natureza disponíveis para a proposta deste trabalho. Entretanto, não há prejuízo no entendimento, análise, replicação e resultados gerados por esta dissertação, *i.e.*, tão somente não foram expostos as trilhas de registros internos desses equipamentos mencionados.

7.3 TRABALHOS FUTUROS

Como trabalhos futuros, existem algumas considerações e lacunas que esta pesquisa não preencheu. É possível expandir o protocolo de comunicação para realizar atualizações de dados biométricos. Isso seria mais uma funcionalidade da rede, que também funcionaria sobre os mesmos aspectos de privacidade e segurança demonstrados. Um outro ponto relavante é verificar o uso do algoritmo IDN nas representações dos vetores biométricos coletados e armazenados. Esses representam, *e.g.*, as minúcias das impressões digitais ou pontos fiduciais de uma face. Como, normalmente, a coleta e os dados biométricos já armazenados possuem bits diferentes, não necessariamente resultando em duas pessoas diferentes, é necessário criar um vetor médio representativo das mesmas, *e.g.*, impressões digitais coletadas e armazenadas, para fim de comparação. Esse é um trabalho que resolveria diversos problemas encontrados em redes biométricas sobre aplicação de um *template* proprietário e fechado nas soluções.

Além disso, como já comentado, o algoritmo IDN proposto pode fornecer segurança, privacidade e interoperabilidade de uso geral. Qualquer rede de comunicação, principalmente aquelas que usam esquemas de criptografia, como a arquitetura 5G, poderiam se usufruir do esquema apresentado. Esses trabalhos futuros são propostas imediatas das contribuições e resultados que essa dissertação apresentou.

REFERÊNCIAS BIBLIOGRÁFICAS

1 NUNAMAKER, J. J. F.; CHEN, M.; PURDIN, T. D. M. Systems development in information systems research. *J. Manage. Inf. Syst.*, M. E. Sharpe, Inc., Armonk, NY, USA, v. 7, n. 3, p. 89–106, 0/91. ISSN 0742-1222. Disponível em: <http://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=5748024&loginpage=Login.asp&site=ehost-live>.

2 JAIN, A. K.; NANDAKUMAR, K.; ROSS, A. 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, v. 79, p. 80–105, 2016.

3 IEEE. IEEE Standard for Biometric Open Protocol, Redline. *IEEE Std 2410-2019 (Revision of IEEE Std 2410-2017), Redline*, p. 1–134, June 2019.

4 MANGOLD, K. Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information ANSI/NIST-ITL 1-2011 NIST Special Publication 500-290 Edition 3. In: . [S.l.: s.n.], 2016.

5 CHOUDHARY, S. K.; NAIK, A. K. Multimodal Biometric Authentication with Secured Templates — A Review. In: *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. [S.l.: s.n.], 2019. p. 1062–1069.

6 GOMEZ-BARRERO, M. et al. General Framework to Evaluate Unlinkability in Biometric Template Protection Systems. *IEEE Transactions on Information Forensics and Security*, v. 13, n. 6, p. 1406–1420, June 2018.

7 SANDHYA, M.; PRASAD, M. Biometric Template Protection: A Systematic Literature Review of Approaches and Modalities. In: ____. [S.l.: s.n.], 2016.

8 NGO, D. C. L.; TEOH, A. B. J.; HU, J. *Biometric Security*. United Kingdom: Cambridge Scholars Publishing, 2015. ISBN 1443871834, 9781443871839.

9 CAMPISI, P. *Security and Privacy in Biometrics*. [S.l.]: Springer Publishing Company, Incorporated, 2013. ISBN 1447152298, 9781447152293.

10 ROSS, A.; SHAH, J.; JAIN, A. K. From Template to Image: Reconstructing Fingerprints from Minutiae Points. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, v. 29, n. 4, p. 544–560, April 2007. ISSN 0162-8828.

11 TOLI, C.-A.; PRENEEL, B. Privacy-preserving biometric authentication model for e-finance applications. In: *ICISSP*. [S.l.: s.n.], 2018.

12 ZHOU, K.; REN, J. PassBio: Privacy-Preserving User-Centric Biometric Authentication. *IEEE Transactions on Information Forensics and Security*, v. 13, n. 12, p. 3050–3063, Dec 2018.

13 KUMAR, A.; KUMAR, A. A Cell-Array-Based Multibiometric Cryptosystem. *IEEE Access*, v. 4, p. 15–25, 2016.

14 LI, C. et al. A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion. *IEEE Transactions on Information Forensics and Security*, v. 10, n. 6, p. 1193–1206, June 2015.

15 NASIR, M.; PERUMAL, P. Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm. *International Journal of Innovative Research in Computer and Communication Engineering*, v. 3297, 11 2013.

16 NAGAR, A.; NANDAKUMAR, K.; JAIN, A. K. Multibiometric Cryptosystems Based on Feature-Level Fusion. *IEEE Transactions on Information Forensics and Security*, v. 7, n. 1, p. 255–268, Feb 2012.

17 LAI, L.; HO, S.; POOR, H. V. Privacy–Security Trade-Offs in Biometric Security Systems—Part I: Single Use Case. *IEEE Transactions on Information Forensics and Security*, v. 6, n. 1, p. 122–139, March 2011.

18 LAI, L.; HO, S.; POOR, H. V. Privacy–Security Trade-Offs in Biometric Security Systems—Part II: Multiple Use Case. *IEEE Transactions on Information Forensics and Security*, v. 6, n. 1, p. 140–151, March 2011. ISSN 1556-6021.

19 KAUR, H.; KHANNA, P. Random Distance Method for Generating Unimodal and Multimodal Cancelable Biometric Features. *IEEE Transactions on Information Forensics and Security*, v. 14, p. 709–719, 2019.

20 PUNITHAVATHI, P.; GEETHA, S.; SHANMUGAM, S. Cloud-Based Framework for Cancelable Biometric System. In: *2017 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*. [S.l.: s.n.], 2017. p. 35–38.

21 RATHGEB, C. et al. Towards Cancelable Multi-Biometrics based on Bloom Filters: A Case Study on Feature Level Fusion of Face and Iris. In: *3rd International Workshop on Biometrics and Forensics (IWBF 2015)*. [S.l.: s.n.], 2015. p. 1–6.

22 RATHA, N. K.; CONNELL, J. H.; BOLLE, R. M. Enhancing Security and Privacy in Biometrics-based Authentication Systems. *IBM Syst. J.*, IBM Corp., Riverton, NJ, USA, v. 40, n. 3, p. 614–634, mar. 2001. ISSN 0018-8670. Disponível em: <http://dx.doi.org/10.1147/sj.403.0614>.

23 TOLOSANA, R. et al. Biometric Presentation Attack Detection: Beyond the Visible Spectrum. *IEEE Transactions on Information Forensics and Security*, v. 15, p. 1261–1275, 2020. ISSN 1556-6021.

24 NATGUNANATHAN, I. et al. Protection of Privacy in Biometric Data. *IEEE Access*, v. 4, p. 880–892, 2016.

25 HIRANO, T. et al. A Practical Attack to AINA2014's Countermeasure for Cancelable Biometric Authentication Protocols. In: *2016 International Symposium on Information Theory and Its Applications (ISITA)*. [S.l.: s.n.], 2016. p. 315–319.

26 QUAN, F. et al. Cracking Cancelable Fingerprint Template of Ratha. In: *2008 International Symposium on Computer Science and Computational Technology*. [S.l.: s.n.], 2008. v. 2, p. 572–575.

27 KOCHER, P. C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*. London, UK, UK: Springer-Verlag, 1996. (CRYPTO '96), p. 104–113. ISBN 3-540-61512-1. Disponível em: <http://dl.acm.org/citation.cfm?id=646761.706156>.

28 WOLTERS, P. T. J. The security of personal data under the GDPR: a harmonized duty or a shared responsibility? *International Data Privacy Law*, v. 7, n. 3, p. 165–178, 2017. Disponível em: <http://dx.doi.org/10.1093/idpl/ipx008>.

29 BUSTARD, J. The Impact of EU Privacy Legislation on Biometric System Deployment: Protecting citizens but constraining applications. *IEEE Signal Processing Magazine*, v. 32, n. 5, p. 101–108, Sep. 2015.

30 DWORKIN, M. J. *SP 800-38A 2001 Edition. Recommendation for Block Cipher Modes of Operation: Methods and Techniques*. Gaithersburg, MD, United States, 2001.

31 DANG, Q. *Secure Hash Standard (SHS)*. pub-NIST:adr, 2015. v + 30 p.

32 YU, W. et al. A study of HSM based key protection in encryption file system. In: *2016 IEEE Conference on Communications and Network Security (CNS)*. [S.l.: s.n.], 2016. p. 352–353.

33 KIM, D.; JEON, Y.; KIM, J. A secure channel establishment method on a hardware security module. In: *2014 International Conference on Information and Communication Technology Convergence (ICTC)*. [S.l.: s.n.], 2014. p. 555–556. ISSN 2162-1233.

34 SCHAFFER, K. B. *Security Requirements for Cryptographic Modules*. pub-NIST:adr, 2019.

35 MORIARTY, K. et al. *PKCS #1: RSA Cryptography Specifications Version 2.2*. RFC Editor, 2016. RFC 8017. (Request for Comments, 8017). Disponível em: <https://rfc-editor.org/rfc/rfc8017.txt>.

36 RESCORLA, E. *HTTP Over TLS*. RFC Editor, 2000. RFC 2818. (Request for Comments, 2818). Disponível em: <https://rfc-editor.org/rfc/rfc2818.txt>.

37 BRAY, T. *The JavaScript Object Notation (JSON) Data Interchange Format*. RFC Editor, 2017. RFC 8259. (Request for Comments, 8259). Disponível em: <https://rfc-editor.org/rfc/rfc8259.txt>.

38 KATZ, J.; LINDELL, Y. *Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series)*. [S.l.]: Chapman & Hall/CRC, 2007. ISBN 1584885513.

39 WOLKERSTORFER, J.; OSWALD, E.; LAMBERGER, M. An asic implementation of the aes sboxes. In: SPRINGER. *Cryptographers' Track at the RSA Conference*. [S.l.], 2002. p. 67–78.

40 SHPARLINSKI, I. *Finite Fields: Theory and Computation: The meeting point of number theory, computer science, coding theory and cryptography*. [S.l.]: Springer Science & Business Media, 2013. v. 477.

41 WATANABE, Y.; SHIKATA, J.; IMAI, H. Equivalence Between Semantic Security and Indistinguishability Against Chosen Ciphertext Attacks. In: DESMEDT, Y. G. (Ed.). *Public Key Cryptography — PKC 2003*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002. p. 71–84. ISBN 978-3-540-36288-3.

42 RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, Association for Computing Machinery, New York, NY, USA, v. 21, n. 2, p. 120–126, fev. 1978. ISSN 0001-0782. Disponível em: <https://doi.org/10.1145/359340.359342>.

43 TURAN MELTEM S.AND BARKER, E. B. et al. *SP 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation*. Gaithersburg, MD, United States, 2018.

44 LI, Q.; ZHANG, L. The Public Security and Personal Privacy Survey: Biometric Technology in Hong Kong. *IEEE Security Privacy*, v. 14, n. 4, p. 12–21, July 2016. ISSN 1540-7993.

45 DWORK, C. Differential Privacy. In: *Proceedings of the 33rd International Conference on Automata, Languages and Programming - Volume Part II*. Berlin, Heidelberg: Springer-Verlag, 2006. (ICALP'06), p. 1–12. ISBN 3-540-35907-9, 978-3-540-35907-4. Disponível em: <http://dx.doi.org/10.1007/11787006_1>.

46 KAUR, M.; SOFAT, S. Fuzzy Vault template protection for Multimodal Biometric System. In: *2017 International Conference on Computing, Communication and Automation (ICCCA)*. [S.l.: s.n.], 2017. p. 1131–1135.

47 BARNI, M.; DROANDI, G.; LAZZERETTI, R. Privacy Protection in Biometric-Based Recognition Systems: A marriage between cryptography and signal processing. *IEEE Signal Processing Magazine*, v. 32, n. 5, p. 66–76, Sept 2015. ISSN 1053-5888.

48 TOLOSANA, R. et al. Preprocessing and Feature Selection for Improved Sensor Interoperability in Online Biometric Signature Verification. *IEEE Access*, v. 3, p. 478–489, 2015. ISSN 2169-3536.

49 MASON, S. et al. Interoperability between Fingerprint Biometric Systems: An Empirical Study. In: *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. [S.l.: s.n.], 2014. p. 586–597. ISSN 1530-0889.

50 BELLARE, M.; ROGAWAY, P. Optimal Asymmetric Encryption. In: SANTIS, A. D. (Ed.). *Advances in Cryptology — EUROCRYPT'94*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995. p. 92–111. ISBN 978-3-540-44717-7.

51 3GPP. *Security architecture and procedures for 5G system (Release 15)*. [S.l.], 2019. Version 15.6.0. Disponível em: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169>.

52 GOLDREICH, O. *Foundations of Cryptography: Basic Tools*. New York, NY, USA: Cambridge University Press, 2000. ISBN 0521791723.

53 BELLARE, M. et al. Relations Among Notions of Security for Public-key Encryption Schemes. In: KRAWCZYK, H. (Ed.). *Advances in Cryptology — CRYPTO '98*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998. p. 26–45. ISBN 978-3-540-68462-6.

54 MCGREW, D. A. Impossible Plaintext Cryptanalysis and Probable-Plaintext Collision Attacks of 64-bit Block Cipher Modes. *IACR Cryptology ePrint Archive*, v. 2012, p. 623, 2012.

55 BELLARE, M.; KOHNO, T. Hash Function Balance and Its Impact on Birthday Attacks. In: CACHIN, C.; CAMENISCH, J. L. (Ed.). *Advances in Cryptology - EUROCRYPT 2004*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004. p. 401–418. ISBN 978-3-540-24676-3.

56 BOGDANOV, A.; KHOVRATOVICH, D.; RECHBERGER, C. Biclique Cryptanalysis of the Full AES. In: *Proceedings of the 17th International Conference on The Theory and Application of Cryptology and Information Security*. Berlin, Heidelberg: Springer-Verlag, 2011. (ASIACRYPT'11), p. 344–371. ISBN 978-3-642-25384-3. Disponível em: <http://dx.doi.org/10.1007/978-3-642-25385-0_19>.

57 DOBRAUNIG, C.; EICHLSEDER, M.; MENDEL, F. Analysis of SHA-512/224 and SHA-512/256. In: *Proceedings, Part II, of the 21st International Conference on Advances in Cryptology — ASIACRYPT 2015 - Volume 9453*. Berlin, Heidelberg: Springer-Verlag, 2015. p. 612–630. ISBN 978-3-662-48799-0. Disponível em: <https://doi.org/10.1007/978-3-662-48800-3_25>.

58 KHOVRATOVICH, D.; RECHBERGER, C.; SAVELIEVA, A. Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 Family. In: CANTEAUT, A. (Ed.). *Fast Software Encryption*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. p. 244–263. ISBN 978-3-642-34047-5.

59 KHOVRATOVICH, D. Bicliques for Permutations: Collision and Preimage Attacks in Stronger Settings. In: . [S.l.: s.n.], 2012. v. 7658, p. 544–561.

60 ROGAWAY, P. *Evaluation of Some Blockcipher Modes of Operation*. 2011. Evaluation carried out for the Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan.

61 KANG, H. et al. New Efficient Padding Methods Secure Against Padding Oracle Attacks. In: KWON, S.; YUN, A. (Ed.). *Information Security and Cryptology - ICISC 2015*. Cham: Springer International Publishing, 2016. p. 329–342. ISBN 978-3-319-30840-1.

62 FUJISAKI, E. et al. RSA-OAEP Is Secure Under the RSA Assumption. *Journal of Cryptology*, v. 17, n. 2, p. 81–104, Mar 2004. ISSN 1432-1378. Disponível em: <https://doi.org/10.1007/s00145-002-0204-y>.

63 BIRYUKOV, A.; KHOVRATOVICH, D. Related-Key Cryptanalysis of the Full AES-192 and AES-256. In: MATSUI, M. (Ed.). *Advances in Cryptology – ASIACRYPT 2009*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. p. 1–18. ISBN 978-3-642-10366-7.

64 BARKER, E. B. et al. *SP 800-57 Part 1 Rev. 4. Recommendation for Key Management, Part 1: General*. Gaithersburg, MD, United States, 2016.

65 BERNSTEIN, D.; LANGE, T. Batch NFS. In: JOUX, A.; YOUSSEF, A. (Ed.). *Selected Areas in Cryptography – SAC 2014: 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers*. Germany: Springer, 2014. (Lecture Notes in Computer Science), p. 38–58. ISBN 978-3-319-13050-7.

66 BONNEAU, J.; MIRONOV, I. Cache-Collision Timing Attacks Against AES. In: *Cryptographic Hardware and Embedded Systems""CHES 2006*. Springer, 2006. (Lecture Notes in Computer Science, v. 4249), p. 201–215. Disponível em: <https://www.microsoft.com/en-us/research/publication/cache-collision-timing-attacks-against-aes/>.

67 KOCHER, P.; JAFFE, J.; JUN, B. Differential Power Analysis. In: WIENER, M. (Ed.). *Advances in Cryptology — CRYPTO' 99*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999. p. 388–397. ISBN 978-3-540-48405-9.

68 BONEH, D.; DEMILLO, R. A.; LIPTON, R. J. On the Importance of Checking Cryptographic Protocols for Faults. In: FUMY, W. (Ed.). *Advances in Cryptology — EUROCRYPT '97*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997. p. 37–51. ISBN 978-3-540-69053-5.

69 RESCORLA, E. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC Editor, 2018. RFC 8446. (Request for Comments, 8446). Disponível em: <https://rfc-editor.org/rfc/rfc8446.txt>.

70 DING, D. et al. A Survey on Security Control and Attack Detection for Industrial Cyber-Physical Systems. *Neurocomputing*, v. 275, p. 1674–1683, 01 2018.

71 YAN, Q. et al. Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges. *IEEE Communications Surveys Tutorials*, v. 18, n. 1, p. 602–622, Firstquarter 2016.

APÊNDICE

A API

Apresenta-se o código da API criada. Cada etapa determina que tipo de chamada é necessária em solicitações e respostas para fins de integridade. Conforme abordado, essa API pode ser incorporada na documentação do IEEE BOPS.

```
swagger: "2.0"
info:
  description: "API"
  version: "1.0.0"
  title: ""
  contact:
    email: "emlacerdaf@gmail.com"
tags:
- name: "directory"
  description: "Synchronous Pattern"
- name: "hub"
  description: "Asynchronous Pattern"

schemes:
- "https"

paths:
  /directory/zquery:
    get:
      tags:
      - directory
      description: "zquery"
      consumes:
      - application/json
      produces:
      - application/json
      parameters:
      - in: query
        name: z
        type: string
        required: true
```

```
      description: "zcode"
    responses:
      200:
        description: "z was found in
        the base"
        schema:
          $ref: "#/definitions/
      zquery"
      204:
        description: "z not found"
      400:
        description: "Bad request"
      401:
        description: "Request without
        certificate"
      403:
        description: "Certificate not
        recognize"

/directory/PendingOperations:
  get:
    tags:
    - directory
    description: "Pending-operations
    listing operation"
    consumes:
    - application/json
    produces:
    - application/json
    responses:
      200:
        description: "Return from
        pending-operations"
        schema:
          $ref: "#/definitions/
          PendingOperations"
      400:
        description: "Bad request"
      401:
```

```
        description: "Request without
        certificate"
      403:
        description: "Unrecognized
        certificate"

/directory/operation-resend:
  get:
    tags:
    - directory
    description: "Operation resubmit
    request pending-operation"
    consumes:
    - application/json
    produces:
    - application/json
    parameters:
    - in: query
      name: tcn
      type: string
      required: true
      description: "TCN code"
    responses:
      202:
        description: "Accepted"
      400:
        description: "Bad request"
      401:
        description: "Request without
        certificate"
      403:
        description: "Unrecognized
        certificate"

/directory/idn-list:
  get:
    tags:
    - directory
    description: "IDN list"
```

```
    consumes:
    - application/json
    produces:
    - application/json
    parameters:
    - in: query
      name: startDate
      type: integer
      description: "UNIX Timestamp
      UTC"
    - in: query
      name: endDate
      description: "UNIX Timestamp
      UTC"
      type: integer
    responses:
      200:
        description: "OK"
        schema:
          $ref: "#/definitions
      /IdnList"
      400:
        description: "Bad request"
      401:
        description: "Request without
        certificate"
      403:
        description: "Unrecognized
        certificate"

/hub:
  post:
    tags:
    - Hub
    description: "Hub operations"
    consumes:
    - application/xml
    - application/octet-stream
    produces:
```

```
      - application/json
      parameters:
        - in: body
          name: NIST
          description: ANSI/NIST
        transaction
          schema:
            type: object
            example:
      responses:
        202:
          description: "Accepted"
        400:
          description: "Bad request"
          schema:
            $ref: "#/definitions
        /HubError"
        401:
          description: "Request without
          certificate"
        403:
          description: "Unrecognized
          certificate"

definitions:
  ZQuery:
    type: object
    properties:
      idn:
        type: string
        example: "IDN code"
      timestamp:
        type: integer
        example: 1234567890123
      exists:
        type: string
        example: "TRUE or FALSE"
      t_14_013_1:
        type: string
```

```
  example: "Corresponding TCN or
  blanck"
t_14_013_2:
  type: string
  example: "TCorresponding TCN or
  blanck"
t_14_013_3:
  type:  string
  example: "Corresponding TCN or
  blanck"
t_14_013_4:
  type: string
  example: "Corresponding TCN or
  blanck"
t_14_013_5:
  type: string
  example: "Corresponding TCN or
  blanck"
t_14_013_6:
  type: string
  example: "Corresponding TCN or
  blanck"
t_14_013_7:
  type:  string
  example: "Corresponding TCN or
  blanck"
t_14_013_8:
  type: string
  example: "Corresponding TCN or
  blanck"
t_14_013_9:
  type: string
  example: "Corresponding TCN or
  blanck"
t_14_013_10:
  type: string
  example: "Corresponding TCN or
  blanck"
t_10:
```

```
      type: string
      example: "Corresponding TCN or
      blanck"

PendingOperations:
  type: object
  properties:
    pendingOperationsList:
      type: array
      maxItems: 1000
      items:
        type: string
      example:
      - "IDN of the pending
      transaction, TCN of the pending
      transaction"
      - "IDN of the pending
      transaction, TCN of the pending
      transaction"


idnList:
  type: array
  items:
    properties:
      idn:
        type: string
        example: ""
      timestamp:
        type: integer
        example: 1234567890123
      t_14_013_1:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_14_013_2:
        type: string
        example: "Corresponding TCN
        or blanck"
```

```
      t_14_013_3:
        type:  string
        example: "Corresponding TCN
        or blanck"
      t_14_013_4:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_14_013_5:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_14_013_6:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_14_013_7:
        type:  string
        example: "Corresponding TCN
        or blanck"
      t_14_013_8:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_14_013_9:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_14_013_10:
        type: string
        example: "Corresponding TCN
        or blanck"
      t_10:
        type: string
        example: "Corresponding TCN
        or blanck"

HubError:
  type: object
```

```
properties:
  errorCode:
    type: integer
    example: 999
  errorMessage:
    type: string
    example: "error"
```

B PACOTE ANSI/NIST - TRANSAÇÃO IDE

Apresenta-se o esquema, em XML, do pacote `ANSI/NIST Package 2`.

<?xml version="1.0" encoding="UTF-8" standalone="true"?>

-<itl:NISTBiometricInformationExchangePackage xmlns:nc="http://niem.gov/niem/niem-core/2.0" xmlns:itl="http://biometrics.nist.gov/standard/2011"

xmlns:biom="http://niem.gov/niem/biometrics/1.0" xmlns:iti="http://iti.gov.br/psb">

-<itl:PackageInformationRecord>

<biom:RecordCategoryCode>1</biom:RecordCategoryCode>

-<biom:Transaction>

-<biom:TransactionDate>

<nc:Date>2020-05-11</nc:Date>

</biom:TransactionDate>

-<biom:TransactionDestinationOrganization>

-<nc:OrganizationIdentification>

<nc:IdentificationID> TransactionDestinationOrganization</nc: IdentificationID>

</nc:OrganizationIdentification>

</biom:TransactionDestinationOrganization>

-<biom:TransactionOriginatingOrganization>

-<nc:OrganizationIdentification>

<nc:IdentificationID> TransactionOriginatingOrganization</nc: IdentificationID>

</nc:OrganizationIdentification>

</biom:TransactionOriginatingOrganization>

-<biom:TransactionControlIdentification>

<nc:IdentificationID> TransactionControlIdentification</nc:IdentificationID>

</biom:TransactionControlIdentification>

-<biom:TransactionControlReferenceIdentification>

<nc:IdentificationID> TransactionControlReferenceIdentification</nc: IdentificationID>

</biom:TransactionControlReferenceIdentification>

-<biom:TransactionImageResolutionDetails>

<biom:NativeScanningResolutionValue>00.00</biom: NativeScanningResolutionValue>

<biom:NominalTransmittingResolutionValue>00.00</biom: NominalTransmittingResolutionValue>

</biom:TransactionImageResolutionDetails>

<biom:TransactionMajorVersionValue>05</biom: TransactionMajorVersionValue>

<biom:TransactionMinorVersionValue>00</biom: TransactionMinorVersionValue>

<biom:TransactionCategoryCode>IDE</biom: TransactionCategoryCode>

-<biom:TransactionContentSummary>

<biom:ContentFirstRecordCategoryCode>1</biom: ContentFirstRecordCategoryCode>

<biom:ContentRecordQuantity>3</biom: ContentRecordQuantity>

-<biom:ContentRecordSummary>

-<biom:ImageReferenceIdentification>

<nc:IdentificationID>2</nc:IdentificationID>

</biom:ImageReferenceIdentification>

<biom:RecordCategoryCode>2</biom:RecordCategoryCode>

</biom:ContentRecordSummary>

-<biom:ContentRecordSummary>

-<biom:ImageReferenceIdentification>

<nc:IdentificationID>1</nc:IdentificationID>

</biom:ImageReferenceIdentification>

<biom:RecordCategoryCode>10</biom:RecordCategoryCode>

</biom:ContentRecordSummary>

-<biom:ContentRecordSummary>

-<biom:ImageReferenceIdentification>

<nc:IdentificationID>0</nc:IdentificationID>

</biom:ImageReferenceIdentification>

<biom:RecordCategoryCode>14</biom:RecordCategoryCode>

</biom:ContentRecordSummary>

</biom:TransactionContentSummary>

</biom:Transaction>

</itl:PackageInformationRecord>

-<itl:PackageDescriptiveTextRecord>

<biom:RecordCategoryCode>2</biom:RecordCategoryCode>

-<biom:ImageReferenceIdentification>

<nc:IdentificationID>2</nc:IdentificationID>

</biom:ImageReferenceIdentification>

-<itl:UserDefinedDescriptiveDetail>

<icp:idn>idn</icp:idn>

<icp:iag>RFB</icp:iag>

<icp:tod>99</icp:tod>

<icp:anf>N</icp:anf>

</itl:UserDefinedDescriptiveDetail>

</itl:PackageDescriptiveTextRecord>

-<itl:PackageFacialAndSMTImageRecord>

<biom:RecordCategoryCode>10</biom:RecordCategoryCode>

-<biom:ImageReferenceIdentification>

<nc:IdentificationID>1</nc:IdentificationID>

</biom:ImageReferenceIdentification>

-<biom:FaceImage>

<nc:BinaryBase64Object>BinaryBase64Object</nc: BinaryBase64Object>

-<biom:ImageCaptureDetail>

-<biom:CaptureDate>

<nc:Date>2020-05-11</nc:Date>

</biom:CaptureDate>

-<biom:CaptureOrganization>

-<nc:OrganizationIdentification>

<nc:IdentificationID>CaptureOrganization</nc: IdentificationID>

</nc:OrganizationIdentification>

</biom:CaptureOrganization>

</biom:ImageCaptureDetail>

<biom:ImageColorSpaceCode>SRGB</biom: ImageColorSpaceCode>

<biom:ImageCompressionAlgorithmText>JPEGB</biom: ImageCompressionAlgorithm-Text>

<biom:ImageHorizontalLineLengthPixelQuantity>480</biom: ImageHorizontalLineLength-PixelQuantity>

<biom:ImageHorizontalPixelDensityValue>1</biom: ImageHorizontalPixelDensityValue>

<biom:ImageScaleUnitsCode>0</biom:ImageScaleUnitsCode>

<biom:ImageCategoryCode>FACE</biom:ImageCategoryCode>

<biom:ImageVerticalLineLengthPixelQuantity>640</biom: ImageVerticalLineLengthPixelQuantity>

<biom:ImageVerticalPixelDensityValue>1</biom: ImageVerticalPixelDensityValue>

<biom:FaceImageAcquisitionProfileCode>13</biom: FaceImageAcquisitionProfileCode>

</biom:FaceImage>

</itl:PackageFacialAndSMTImageRecord>

-<itl:PackageFingerprintImageRecord>

<biom:RecordCategoryCode>14</biom:RecordCategoryCode>

-<biom:ImageReferenceIdentification>

<nc:IdentificationID>0</nc:IdentificationID>

</biom:ImageReferenceIdentification>

-<biom:FingerImpressionImage>

<nc:BinaryBase64Object>BinaryBase64Object</nc: BinaryBase64Object>

<biom:ImageBitsPerPixelQuantity>8</biom: ImageBitsPerPixelQuantity>

-<biom:ImageCaptureDetail>

-<biom:CaptureDate>

<nc:Date>2020-05-11</nc:Date>

</biom:CaptureDate>

-<biom:CaptureOrganization>

-<nc:OrganizationIdentification>

<nc:IdentificationID>CaptureOrganization</nc: IdentificationID>

</nc:OrganizationIdentification>

</biom:CaptureOrganization>

</biom:ImageCaptureDetail>

<biom:ImageCompressionAlgorithmText>WSQ20</biom: ImageCompressionAlgorithm-Text>

<biom:ImageHorizontalLineLengthPixelQuantity>512</biom: ImageHorizontalLineLength-PixelQuantity>

<biom:ImageHorizontalPixelDensityValue>1</biom: ImageHorizontalPixelDensityValue>

<biom:ImageScaleUnitsCode>1</biom:ImageScaleUnitsCode>

<biom:ImageVerticalLineLengthPixelQuantity>512</biom: ImageVerticalLineLengthPixelQuantity>

<biom:ImageVerticalPixelDensityValue>1</biom: ImageVerticalPixelDensityValue>

<biom:FingerprintImageImpressionCaptureCategoryCode>0<biom: FingerprintImageImpressionCaptureCategoryCode>

<biom:FingerPositionCode>3</biom:FingerPositionCode>

</biom:FingerImpressionImage>

</itl:PackageFingerprintImageRecord>

</itl:NISTBiometricInformationExchangePackage>