Proposta de Carimbo do Tempo Descentralizado e Preciso para a ICP-Brasil utilizando Sistemas Embarcados e Criptografia Pós-Quântica

Gabriel Estevam[1], **Martín Vigil**[1]

[1]Engenharia de Computação - Universidade Federal de Santa Catarina (UFSC)
Araranguá – SC – Brasil

gabriel.estevam@grad.ufsc.br, martin.vigil@ufsc.br

Abstract. *In Brazil, legally binding timestamping is based on a trusted third party known as Time Stamping Authority and is regulated by the Brazilian Public Key Infrastructure (ICP-Brasil). However, concerns arise from system centralization and timestamps requests. This work proposes a new, low cost, and compact time stamping device using post-quantum cryptography. The device is proposed to promote decentralization in the ICP-Brasil and increase time precision in time stamping. Moreover, we provide a proof of concept and conduct experiments showing our proposal is feasibility and effective.*

Resumo. *O modelo de Carimbo do Tempo aceito juridicamente no Brasil é o baseado em Autoridades de Carimbo do Tempo (ACT), regulamentadas pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Contudo, o modelo está sujeito a problemas causados pela centralização e pelo método de obtenção do carimbo. Diante disso, este trabalho propõe um dispositivo de carimbo do tempo compacto, de baixo custo e com criptografia pós-quântica. O dispositivo é apresentado como uma modificação no modelo de carimbo do tempo da ICP-Brasil com o objetivo de minimizar a centralização e aumentar a precisão de tempo. Por fim é apresentado uma prova de conceito e uma série de experimentos que mostram a factibilidade e eficácia do dispositivo.*

1. Introdução

Carimbo do tempo é a prova que uma informação digital existia em uma determinada data e hora. Os carimbos do tempo são documentos eletrônicos emitidos por Autoridades de Carimbo do Tempo (ACT) regulamentadas pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Segundo o Instituto Nacional de Tecnologia da Informação (ITI), o carimbo do tempo confere as propriedades de integridade e tempestividade a documentos digitais [ITI 2020]. Integridade garante que o documento não foi alterado [Vigil et al. 2015] e tempestividade estabelece data e hora confiáveis para a existência do documento.

O uso do carimbo do tempo foi regulamentado pela ICP-Brasil em 2008. A iniciativa permitiu inserir datação com validade legal em documentos assinados, trazendo um nível a mais de segurança além da certificação digital comum. A solução passou a ser utilizada por instituições públicas e privadas, como órgãos do judiciário, prefeituras, secretarias, laboratórios médicos, entre outros [ITI 2008]. Atualmente o carimbo do tempo é aplicado em atividades de registros de: apólices de seguro, direitos autorais, diplomas digitais, ponto eletrônico e inúmeras outras aplicações [Santiago 2019]. Um caso em que

é indispensável o carimbo do tempo é o projeto do Diploma Digital do Ministério da Educação. Em 2019, a Universidade Federal de Santa Catarina (UFSC) foi a pioneira ao implantar um projeto-piloto para emissão de diplomas assinados digitalmente. Segundo Sergio Roberto de Lima e Silva Filho - consultor comercial da BRy Tecnologia - "O carimbo do tempo é a tecnologia que comprova a data e a hora que o documento foi emitido, e o certificado digital, a que garante a autenticidade do diploma". A BRy Tecnologia em conjunto com o Laboratório de Segurança em Computação (LabSEC) implementaram o projeto-piloto na UFSC.

Almeja-se no futuro que a tecnologia de carimbo do tempo seja difundida a ponto de tornar-se invisível ao usuário, estando presente em computadores, smartphones, câmeras de vigilância, automóveis, *Internet of Things* (IoT), entre outros. Com o crescimento das aplicações de IoT aumentou-se a demanda por segurança, como certificação de bombas de combustíveis e relógios medidores de energia [CryptoID 2020].

A preocupação com a validade na datação de documentos é justificada pela facilidade de manipulação dos relógios dos computadores. Contudo, no Brasil segundo o ITI existem apenas oito ACT credenciadas em 2020 [ITI 2017a] e apenas uma empresa que fornece Sistema de Carimbo do Tempo (SCT) homologado pela ICP-Brasil [ITI 2017b], o que implica em uma alta centralização. A centralização pode provocar problemas de indisponibilidade de serviço, escalabilidade, necessidade de infraestrutura avançada, entre outros [Coulouris et al. 2013]. Além disso, o mundo vive um movimento rumo à descentralização de processos. Como exemplo as criptomoedas e a tecnologia de blockchain. Outro problema deste modelo é a latência. A forma mais usual de obter um carimbo do tempo é através da Internet, porém implica em um atraso na marcação do tempo. Segundo [Kurose and Ross 2013], no melhor dos casos o atraso de rede é da ordem de milissegundos mas pode chegar a casa décimos de segundo ou mais. No entanto, aplicações como leilões online e mercado de ações necessitam de carimbos do tempo com precisão na ordem de milissegundos e algumas vezes microssegundos, como relata [Broby et al. 2019].

Diante disso, este trabalho propõe um dispositivo de carimbo do tempo utilizando um hardware compacto, de baixo custo e com criptografia pós-quântica. O dispositivo é apresentado como uma modificação no modelo de carimbo do tempo da ICP-Brasil com o objetivo de minimizar os problemas da centralização e aumentar a precisão de tempo.

O restante deste artigo é organizado da seguinte forma. Na seção 2 são apresentados conceitos básicos para o entendimento do trabalho. Na seção 3 são apresentados trabalhos relacionados. Na seção 4 é apresentado o modelo de carimbo do tempo da ICP-Brasil. Na seção 5 é apresentado o modelo proposto. Na seção 6 é apresentado uma prova de conceito. Na seção 7 são apresentados os experimentos realizados e na seção 8 as considerações finais.

2. Referencial Teórico

Nesta seção são apresentados conceitos importantes para o entendimento deste trabalho.

2.1. Função de Hash Criptográfico

Uma função de hash mapeia um conjunto de bits de tamanho arbitrário para um conjunto de bits de tamanho fixo. É definida por $h : \{0,1\}^* \rightarrow \{0,1\}^m$, sendo m um inteiro

positivo [Buchmann et al. 2013]. Funções de hash criptográfico possuem a propriedade de resistência a colisão por ser inviável encontrar e e e' distintos tal que $h(e) = h(e')$. Esta propriedade permite que as funções de hash criptográfico sejam utilizadas para verificação de integridade de documentos [Buchmann et al. 2013].

2.2. Assinatura Digital e XMSS

A assinatura digital assegura integridade, autenticidade e não repúdio a documentos digitais. Integridade garante que o documento não foi alterado. Autenticidade permite identificar a origem do documento. E não-repúdio impede que o remetente refute a autoria do documento [Vigil et al. 2015]. Algoritmos de assinatura digital proveem procedimentos de geração de chaves pública e privada, assinatura e verificação. A chave privada é utilizada para emitir a assinatura e a chave pública é utilizada para a verificação da assinatura [Vigil et al. 2015]. Um exemplo de algoritmo de assinatura digital é o RSA[1].

Neste trabalho utilizou-se o *eXtended Merkle Signature Scheme* (XMSS), algoritmo de assinatura digital baseado em função de hash. O XMSS não emprega problemas matemáticos clássicos, e.g., RSA com fatoração de número grandes. Ao invés disso, dispõe da propriedade de resistência a colisões das funções de hash, o que o torna resistente a ataques de computadores quânticos [IRTF 2020]. O XMSS baseia-se no algoritmo *Winternitz One-Time Signature Scheme* (WOTS). No WOTS, cada par de chaves produz apenas uma assinatura. Para o gerenciamento das múltiplas chaves o XMSS utiliza uma Árvore de Merkle (Para mais detalhes sobre XMSS, WOTS e Árvore de Merkle vide [Bernstein et al. 2009]).

2.3. Microcontrolador ESP32

Um microcontrolador é um dispositivo que integra um microprocessador e periféricos como memórias voláteis e não-voláteis, temporizadores, conversores analógico-digital, entre outros. O ESP32[2] é um microcontrolador que possui um *Real Time Clock* (RTC) interno, comunicação Wi-Fi e comunicação serial do tipo *Universal Serial Bus* (USB). O ESP32 também conta com o módulo *Cryptographic hardware acceleration* que realiza aceleração em hardware das funções criptográficas AES, SHA e RSA. Segundo a Espressif, fabricante do ESP32, a aceleração em hardware permite executar operações significativamente mais rápido do que se fossem implementadas somente em software [Espressif 2020].

3. Trabalhos Relacionados

Muitos trabalhos propuseram soluções alternativas de carimbos do tempo. A maioria destes trabalhos são focados na descentralização do modelo de carimbo do tempo. Como é o caso de [Harmann 2019] com a utilização de múltiplos servidores e verificação cruzada, [Neumann et al. 2014] com a utilização de servidores de DNS (*Domain Name System*) e diversos trabalhos utilizando blockchain como [Gipp et al. 2015]. Contudo, em todos estes trabalhos os carimbos do tempo possuem acurácia de múltiplos segundos a minutos, que é inferior ao pretendido pelo presente trabalho.

[1]RSA - Algoritmo criptográfico criado por [Rivest et al. 1978].

[2]https://www.espressif.com/en/products/socs/esp32/overview

Na vertente de dispositívos físicos de carimbo do tempo o assunto é pouco explorado, encontrando-se poucos artigos na literatura. Na busca percorreu-se mais de dez mil artigos nas plataformas *Xplore Digital Library* do *IEEE*, *Springer Link*, *Science Direct*, *ACM Digital Library*, *Research Gate* e *Google Scholar*. Apenas os dois artigos apresentados a seguir alinharam objetivos com este trabalho.

[Kakei et al. 2012] propuseram uma solução de carimbo do tempo *off-line* utilizando *Trusted Platform Module* (TPM). O TPM é um chip seguro, resistente a violação, montado diretamente na placa-mãe de um computador. Desta forma, o carimbo do tempo é gerado e assinado com criptografia RSA dentro do TPM, prevenindo a falsificação do tempo no carimbo. O TPM insere no carimbo um tempo relativo contado desde sua última atualização. A atualização é feita através de uma ACT via internet, que registra o tempo absoluto da atualização do TPM. Para obter o tempo absoluto do carimbo deve-se resgatar o tempo da correspondente atualização na ACT e somar com tempo fornecido pelo TPM. No entanto, esta abordagem utiliza a frequência do relógio do computador para a contagem relativa de tempo, que pode ser um ponto de vulnerabilidade. Além disso, necessita de uma adaptação de hardware para instalação do TPM. Ademais, os autores não revelaram dados de experimentos de acurácia, apenas que o carimbo do tempo leva pouco mais de um segundo para ser gerado.

Por fim, [Starnberger et al. 2010] propuseram um dispositivo de carimbo do tempo utilizando *smart cards* para leilões online. Um *smart card* é composto por um circuito integrado montado sobre um cartão plástico, capaz de processar e armazenar dados. A proposta se preocupa com a centralização e possíveis ataques em leilões online. No modelo proposto, o *smart card* utiliza um protocolo seguro de sincronização de tempo e emite uma assinatura que é gerada dentro do dispositivo, semelhante ao caso anterior. Mas nesse caso, o *smart card* possui um oscilador próprio, independente do computador a qual é conectado. No entanto, a baixa capacidade de processamento dos *smart cards* foi um fator impeditivo para a sincronização do relógio e precisão do tempo.

4. Modelo de Carimbo do Tempo da ICP-Brasil

A ICP-Brasil possui um conjunto de documentos que regulamentam a geração e uso de carimbos do tempo no Brasil. Os documentos são disponibilizados pelo ITI e foram utilizados para estudo neste trabalho. A Figura 1 representa uma visão geral da estrutura de carimbo do tempo da ICP-Brasil.

O Comitê Gestor da ICP-Brasil é responsável pelas normas e implantação do modelo. A Autoridade Certificadora Raiz (AC-Raiz) credencia, fiscaliza e audita entidades da ICP-Brasil e atua como Entidade de Auditoria de Tempo (EAT). As Autoridades Certificadoras (AC) são responsáveis por emitir, renovar e revogar os certificados dos SCT e do Sistema de Auditoria e Sincronismo (SAS) da AC-Raiz. As ACT são as entidades responsáveis pela emissão dos carimbos do tempo. As ACT devem operar um ou mais SCT, conectados à Rede de Carimbo de Tempo (RCT). O Subscritor é o cliente pessoa física ou jurídica que solicita o carimbo do tempo. E a Terceira Parte é a pessoa ou entidade na qual é apresentado o carimbo do tempo, podendo verificar sua validade. O modelo utiliza um mecanismo para garantir o sincronismo dos relógios e a rastreabilidade do tempo nos equipamentos. O relógio atômico da ICP-Brasil fornece a hora *Universal Time Coordi-*

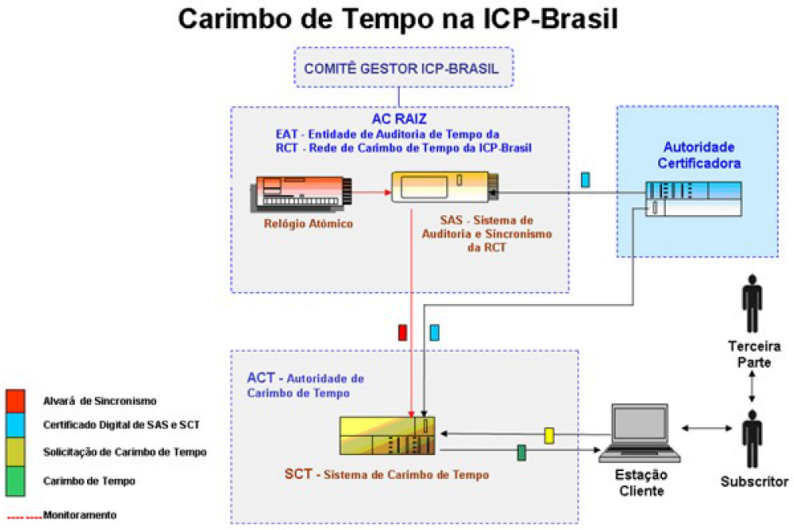

Figura 1. Modelo de Funcionamento do Carimbo do Tempo da ICP-Brasil. (Fonte [ICP-Brasil 2015])

nated (UTC)[3] para o SAS da AC-Raiz. E o SAS dissemina a hora para os equipamentos das ACT e emite o alvará de sincronismo.

A ICP-Brasil define duas formas de obtenção do carimbo do tempo: solicitação presencial através de uma mídia física diretamente na ACT; e solicitação remota por meio de uma rede privada ou pela Internet. A ICP-Brasil exige que as ACT utilizem um Módulo de Segurança Criptográfico para a geração de chaves criptográficas e assinatura digital. Além disso é exigido um rígido controle de segurança física, procedimental e de pessoal aos SCT. Incluem-se níveis de acesso físico, sistemas de detecção, normas de armazenamento de dados, qualificação de pessoal, restrições de acesso, etc.

O modelo de carimbo do tempo da ICP-Brasil apresenta altíssimo nível de segurança, contudo o modelo implica em limitações como centralização e atraso na marcação do tempo. A centralização é ocasionada pelo número reduzido de ACT e pelo custo elevado para dispor de um SCT. Entre os problemas que podem ser causados pela centralização estão: indisponibilidade de serviço, escalabilidade, necessidade de infraestrutura avançada, etc [Coulouris et al. 2013]. E o atraso na marcação do tempo é devido aos métodos de obtenção do carimbo do tempo. Mesmo quando a solicitação é feita via Internet o atraso no melhor dos casos é da ordem de milissegundos, mas na prática pode atingir décimos de segundo ou mais [Kurose and Ross 2013].

5. Modelo Proposto - Dispositivo de Carimbo do Tempo

Nesta seção é apresentada uma modificação no modelo da ICP-Brasil. A modificação consiste em adicionar ao modelo o novo componente proposto, o Dispositivo de Carimbo do Tempo (DCT).

5.1. Visão Geral

Na Figura 2 é apresentado a modificação na estrutura do modelo.

[3]Tempo decorrido em segundos desde 1 de Janeiro de 1970.

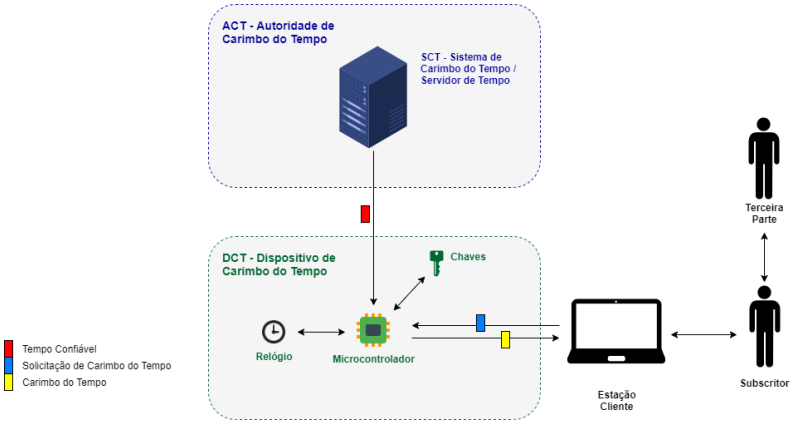

Figura 2. Modelo Proposto. (Fonte o Autor)

O DCT presente na Figura 2 é um equipamento capaz de emitir carimbo do tempo e tem a finalidade de ser uma extensão dos SCT das ACT. Neste modelo a geração e assinatura do carimbo do tempo é feita dentro do DCT, que é de posse do subscritor. O DCT possui um microcontrolador, um relógio interno e um conjunto de chaves públicas e privadas. As chaves privadas são geradas dentro do microcontrolador e não são acessíveis em nenhum momento. O microcontrolador ajusta o relógio com o tempo fornecido pelo servidor de tempo da ACT e emite certificados de carimbo do tempo assinados. É de responsabilidade das ACT: homologar, auditar, certificar, sincronizar e eventualmente comercializar os DCT.

5.2. Características Técnicas

O DCT deve ter tamanho compacto, menor que um cartão de crédito, o que o permite ser portável ao usuário. O dispositivo deve ter baixo custo, para facilitar a aquisição pelos usuários e consequentemente amenizar os problemas de centralização. São restrições técnicas para o DCT:

- Possuir um relógio de tempo real (RTC).
- Possuir interface de comunicação de rede.
- Possuir interface de comunicação serial USB.
- Ser capaz de armazenar as chaves criptográficas.
- Ser capaz de executar um algoritmo de assinatura digital.

5.3. Sincronização do Tempo

O relógio interno do DCT deve ser sincronizado periodicamente por um servidor de tempo da ACT. A sincronização acontece via Internet. Se o DCT perder a conexão com a Internet, depois de um período de tempo determinado pela ACT a sincronização perderá sua validade e o dispositivo deixará de emitir carimbos do tempo até uma nova sincronização. Para realizar a sincronização do relógio, deve-se estabelecer um canal de comunicação entre a ACT e o DCT que garanta a autenticidade das informações enviadas.

A sincronização do relógio segue o *Network Time Protocol* (NTP) estabelecido pelo [NTP.BR 2020]. No esquema define-se uma troca de mensagens para que o cliente descubra o deslocamento (*offset*) do seu tempo em relação ao tempo do servidor.

Segundo o [NTP.BR 2020] a troca de mensagens tem a seguinte forma (vide Figura 3):

- O cliente marca o seu tempo atual **a**.
- O cliente envia a Mensagem 1 ao servidor com o tempo **a**.
- O servidor recebe a mensagem e marca o tempo em que recebeu como **x**.
- O servidor envia a Mensagem 2 com **a**, **x** e seu tempo atual **y**.
- O cliente recebe a mensagem com **a**, **x** e **y** e marca seu tempo atual **b**.

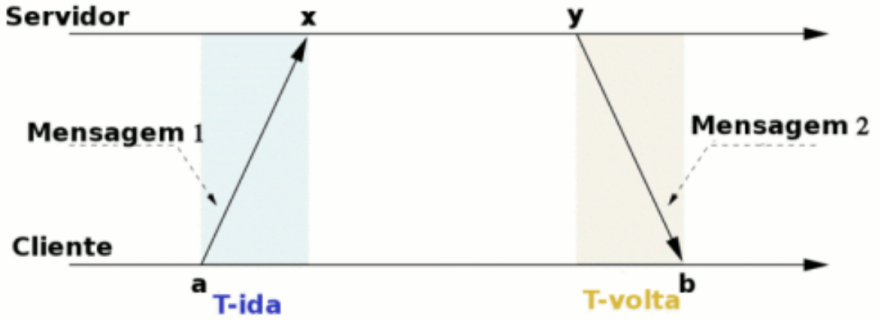

Figura 3. Troca de Mensagens. (Fonte [NTP.BR 2020])

Por simplificação o esquema considera o tempo de ida da mensagem igual ao tempo de volta. Desta forma, o atraso (*delay*) da mensagem é definido como:

$$delay = \frac{(x - a) + (b - y)}{2}.$$

E o deslocamento é definido da seguinte forma:

$$offset = x - (a + delay) = \frac{x - a + y - b}{2}.$$

O *offset* é utilizado para ajustar do relógio local. Se o *offset* for positivo o relógio local está atrasado. Se o *offset* for negativo o relógio local está adiantado.

5.4. Obtenção do Carimbo do Tempo

Neste modelo estabelece-se uma nova forma de obtenção do carimbo do tempo. Consiste em o usuário conectar o DCT a uma porta USB de um computador e utilizar uma aplicação para solicitar a emissão do carimbo do tempo. Desta forma, o carimbo do tempo é gerado localmente.

5.5. Aspectos de Segurança do DCT

Para garantir a integridade e tempestividade nos carimbos de tempo emitidos pelos DCT são necessárias medidas que previnam eventuais vulnerabilidades de segurança do dispositivo. Por isso, nesta seção é descrito um modelo de ameaça para o DCT e algumas medidas que podem ser tomadas para corrigir ou amenizar as vulnerabilidades de segurança.

5.5.1. Modelo de Ameaças

O modelo de ameaças é um estudo do cenário, ambiente, contexto e circunstâncias que o sistema em questão está ou pode ser submetido. Tem o objetivo de levantar possíveis vulnerabilidades de segurança do sistema e prever ataques [Shostack 2014].

No modelo proposto o DCT é de posse do subscritor, que é um usuário no mundo real. Este usuário pode levar o DCT para qualquer lugar e aplicar qualquer técnica que tenha disponível para tentar violar a segurança do dispositivo. Sendo que os dois principais pontos levantados como possiveis vulnerabilidades de segurança do DCT são:

- Adulteração de dados ou descoberta das chaves criptográficas por acesso a memória interna.
- Avanço ou retrocesso do RTC.

Quanto ao avanço ou retrocesso do RTC do dispositivo, tem-se conhecimento de técnicas que podem manipular a frequência do relógio. A frequência do relógio é suscetível a temperatura, tensão de alimentação e radiação eletromagnética. E quanto a adulteração ou descoberta de dados por acesso a memória interna pode ser realizada lendo os sinais diretamente nos pinos do microcontrolador com equipamento adequado.

No entanto, neste trabalho impede-se o subscritor de explorar as vulnerabilidades de acesso à memória, conforme medidas de segurança mencionadas na seção a seguir. Quanto às vulnerabilidades de avanço ou retrocesso de relógio, assume-se aqui que elas não são exploradas. Meios para impedi-las efetivamente são deixados para trabalhos futuros.

5.5.2. Medidas de Segurança

A ICP-Brasil define requisitos para a homologação de *tokens* criptográficos em um de seus manuais de condutas técnicas [ICP-Brasil 2017]. *Tokens* criptográficos são hardwares com conexão USB, com capacidade para gerar e armazenar chaves criptográficas e realizar processamento criptográfico [ICP-Brasil 2017]. Diferente dos DCT, os *tokens* criptográficos não possuem RTC. Contudo, podem compartilhar os requisitos técnicos de segurança.

Dentre os requisitos estabelecidos definem-se restringir acesso físico aos circuitos integrados com a finalidade de deter a observação, sondagem, manipulação e a substituição ou remoção de componentes do módulo. Para isso, o circuito integrado do módulo deve ser protegido por um invólucro que evidencie sinais de tentativas de violação [ICP-Brasil 2017].

Além dos requisitos já estabelecidos deve-se também acrescentar a blindagem térmica e eletromagnética, com o intuito de prevenir o ataque à manipulação da frequência do RTC do dispositivo. Atender tais requisitos são trabalhos futuros.

6. Prova de Conceito

Nesta seção será apresentada uma Prova de Conceito (PoC - *Proof of Concept*) para o modelo proposto. A PoC consistiu em analisar a viabilidade técnica do modelo quanto aos critérios de implementação e segurança. O critério de implementação avalia se é possível cumprir as funcionalidades esperadas para o DCT por meio do desenvolvimento de hardware e software. E o critério de segurança avalia se é possível alcançar os requisitos de segurança necessários para o DCT. A PoC apresentada não se preocupa em atender todos os requisitos estabelecidos no modelo, apenas mostrar que é possível construir um DCT. Portanto, foram assumidas algumas simplificações sem comprometer resultado da

análise. O trabalho conta com o desenvolvimento de um dispositivo de carimbo do tempo, a implementação do firmware para o dispositivo, a implementação da aplicação e um servidor de tempo.

O microcontrolador utilizado para a construção do DCT foi o ESP32 na versão de desenvolvimento. O microcontrolador foi escolhido por possuir um RTC interno, comunicação serial USB, comunicação Wi-Fi e tamanho compacto. Para o invólucro do dispositivo propõe-se o encapsulamento com resina epóxi. A resina epóxi possui uma composição química que proporciona alta adesão, resistência mecânica elevada, resistência a altas temperaturas e baixa absorção de umidade [Fan and Wong 2001]. Esta técnica já é utilizada para encapsulamento de circuitos integrados, como mostra [Hadizadeh et al. 2019]. O encapsulamento não foi realizado neste trabalho por falta de recursos, contudo não afeta a prova de conceito.

O firmware do dispositivo foi implementado na linguagem C e incorpora bibliotecas específicas para o microcontrolador. As bibliotecas permitem realizar a comunicação Wi-Fi e utilizar as funções criptográficas SHA[4] que contam com aceleração em hardware. A seguir são descritas as funcionalidade implementadas no firmware:

- **Emitir carimbo do tempo**: solicitação de carimbo do tempo para o hash de um documento que se deseja carimbar.
- **Consultar chave pública**: permite consultar a chave que identifica unicamente o dispositivo. A chave pública permite consultar se o DCT é certificado.
- **Alterar nome e senha da rede Wi-Fi**: permite informar o nome e senha da rede Wi-Fi que o DCT irá utilizar para sincronização do relógio.
- **Consultar status da rede**: informa se é possível estabelecer uma conexão de rede.

A sincronização do relógio do DCT é realizada periodicamente, caso seja possível conectar-se ao servidor de tempo da ACT através da rede Wi-Fi a qual o nome e senha são informados pelo usuário. Quando o procedimento de sincronização é realizado com sucesso, a validade da sincronização do relógio do DCT é renovada por um período de tempo estabelecido pela ACT. A escolha do período de validade é determinada pela acurácia do relógio do DCT. A acurácia indica o desvio que a hora do relógio pode ter ao longo do tempo.

O certificado de carimbo do tempo emitido pelo DCT possui os atributos a seguir:

- **Hash do dado** (*DataHash*): identificação do documento carimbado.
- **Data e hora** (*Timestamp*): marcação temporal no momento da solicitação.
- **Chave pública** (*PublicKey*): permite verificar a assinatura do carimbo.
- **ACT** (*AuditEntity*): nome da ACT responsável pelo DCT.
- **Última sincronização** (*LastSync*): data e hora da última sincronização.
- **Servidor de tempo** (*TimeServer*): endereço do servidor de tempo.

Para interagir com DCT desenvolveu-se uma aplicação, que é um programa de computador escrito em linguagem Python 3. Permite enviar solicitações para o DCT via comandos no terminal. Foi implementado também na aplicação o esquema de assinatura XMSS, que permite verificar a assinatura e a autenticidade da chave do dispositivo. A autenticidade da chave garante que a assinatura foi gerada pelo dispositivo.

[4]Recomendado por [Cooper et al. 2019] para *Hash-Based Signature Scheme*, incluindo XMSS.

Um servidor de tempo foi implementado em NodeJS para fornecer data e hora confiáveis para a sincronização do relógio do DCT. No modelo proposto a responsabilidade pelo servidor de tempo é da ACT. O DCT se conecta ao servidor de tempo por comunicação HTTP, sendo esta suficiente para a PoC. Posteriormente podem ser explorados outros métodos de comunicação, como UDP. A resposta do servidor de tempo é assinada via XMSS e é verificada dentro do DCT, garantindo autenticidade na comunicação.

7. Experimentos e Análise de Resultados

Nesta seção são apresentados alguns experimentos realizados para análise do protótipo do DCT desenvolvido. Foram realizados experimentos de latência, tempo de resposta, precisão, sincronização e acurácia. Nos experimentos utilizou-se a estimativa de média populacional como em [Triola 2013]. O cálculo da margem de erro indica o intervalo de confiança e também sugere se o tamanho da amostra foi suficiente.

Os equipamentos utilizados nos experimentos foram: um ESP-WROOM-32 (daqui em diante chamado de dispositivo); um computador Intel(R) Core(TM) i7-5500U CPU @ 2.40GHz-3.0GHz, 16 GB de memória RAM e Sistema Operacional Linux Ubuntu 18.04.4 LTS x64; um computador Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz-2.70GHz, 8 GB de memória RAM e Sistema Operacional Windows 10 x64; e um *switch*[5] Intelbras SF 800Q. Nos experimentos que demandaram apenas 1 computador foi utilizado o computador com sistema operacional Linux.

O experimento de latência aferiu o tempo despendido na comunicação entre um computador e o dispositivo (Cenário 1 - Figura 4). O tempo despendido indica o atraso na marcação de tempo do carimbo. O experimento consistiu em medir o tempo necessário para uma mensagem ser enviada de um computador até o dispositivo. Considerando que o tempo de ida e de volta são aproximadamente iguais, metade do valor obtido é o tempo que a mensagem levou para ser enviada do computador até o dispositivo. Essa abordagem permite aferir o tempo despendido na comunicação sem a necessidade de os relógios do computador e do dispositivo estarem sincronizados. Ainda no experimento de latência mediu-se o tempo necessário para comunicação entre dois computadores (Cenário 2 - Figura 4) utilizando comunicação HTTP. O objetivo deste experimento foi aferir o tempo mínimo despendido na comunicação HTTP, a fim de comparar com o tempo despendido na comunicação serial do DCT.

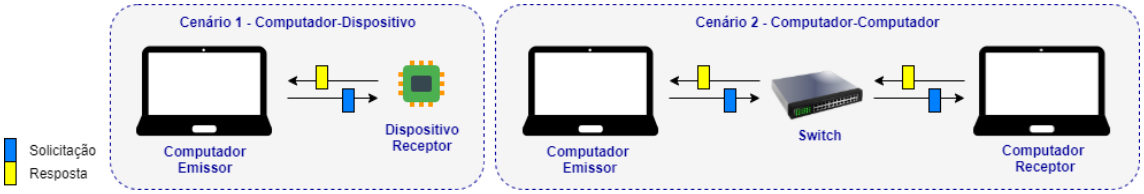

Figura 4. Cenários do experimento de Latência. (Fonte o Autor)

O experimento de tempo de resposta, diferente do experimento de latência, mediu o período desde a solicitação de carimbo do tempo pela aplicação até a obtenção resposta com o certificado de carimbo do tempo assinado. O objetivo deste experimento foi aferir

[5]Equipamento que permite comunicação de dispositivos em redes de computadores.

a performance do dispositivo quanto a emissão de certificados de carimbo do tempo e da assinatura digital.

O experimento de precisão mediu o tempo necessário pelo microcontrolador para fazer uma marcação de tempo. No experimento o RTC do dispositivo é consultado ininterruptamente e a cada consulta é anotado a diferença entre o valor retornado e o anterior.

O experimento de sincronização mediu a defasagem do relógio logo após a sincronização. O objetivo foi analisar a eficiência do método de sincronização. No experimento um computador consulta via comunicação serial o tempo do relógio do dispositivo e marca a diferença de tempo em relação ao relógio do computador.

O experimento de acurácia mediu a defasagem do relógio ao longo de um período de tempo. A acurácia implica na frequência de sincronização a ser mantida para garantir a confiabilidade do ancoramento temporal. No experimento um computador consultou o relógio do dispositivo logo após a sincronização, aguardou 1 minuto, consultou novamente e anotou a diferença dos tempos retornados.

Em todos os experimentos foram executados 5 ensaios com 100 amostras, totalizando 500 amostras cada experimento. Os resultados dos experimentos podem ser vistos na Tabela 1. A margem de erro e o intervalo de confiança foram construídos com parâmetro de confiança de 95%. O experimento de latência mostrou que o atraso na marcação do tempo utilizando o DCT é em média mais de 100 vezes menor do que utilizando a solicitação de carimbo via HTTP, e esse número ainda pode ser muito maior em cenários com redes maiores. O experimento de tempo de resposta mostrou que o DCT pode emitir até 110 carimbos por minuto. O experimento de precisão mostrou que a máxima granularidade de tempo do dispositivo é de aproximadamente 17 μs. O experimento de sincronização mostrou uma defasagem média de 126.41 μs, contudo o desvio padrão foi de 729.49 μs. Acredita-se que a defasagem é causada pelo método de sincronização que adota a simplificação de simetria no tempo de ida e volta das mensagens. Além disso, em redes maiores as filas de espera nos enlaces podem aumentar ainda mais a defasagem na sincronização. Por fim o experimento de acurácia mostrou que o dispositivo tem uma acurácia aproximada de 34 ppm (partes por milhão). Esse valor representa um atraso no relógio de aproximadamente dois milissegundos por minuto.

Experimento	Média	Desvio P.	Erro	Intervalo
Latência Cenário 1	31.33 μs	3.70 μs	0.32 μs	31.01 - 31.61 μs
Latência Cenário 2	5.09 ms	326 μs	28.58 μs	5.06 - 5.12 ms
Tempo de Resposta	542.00 ms	7.42 ms	0.65 μs	541.35 - 542.65 ms
Precisão	16.91 μs	1.38 μs	0.12 μs	16.79 - 17.03 μs
Sincronização	126.41 μs	725.49 μs	63.59 μs	62.82 - 190.00 μs
Acurácia	2027.58 μs	49.17 μs	9.64 μs	2017.94 - 2037.22 μs

Tabela 1. Resultado dos experimentos.

8. Considerações Finais

O objetivo principal deste trabalho foi propor um dispositivo de carimbo do tempo utilizando um hardware compacto, de baixo custo e com criptografia pós-quântica. O dispositivo é apresentado como uma modificação no modelo de carimbo do tempo da ICP-Brasil,

visando minimizar a centralização e aumentar da precisão de tempo. Para a realização do trabalho estudou-se o modelo da ICP-Brasil, elaborou-se um modelo modificado, fez-se uma revisão bibliográfica de trabalhos relacionados, implementou-se uma prova de conceito e por fim realizaram-se alguns experimentos.

O principal resultado obtido neste trabalho é o atraso da marcação de tempo pelo DCT ser em média mais de 100 vezes menor do que no modelo que utiliza comunicação de rede, como é o caso do modelo da ICP-Brasil. Esse resultado é importante pois considera-se a latência o fator limitante na precisão de tempo do carimbo. O atraso na marcação do tempo na ordem de centésimos de milissegundos possibilita carimbos do tempo com precisão de milissegundos ou até décimos de milissegundos. No experimento de precisão, a granularidade na marcação de tempo encontrada para o dispositivo é menor que o valor obtido para latência, portanto não é um fator limitante. Os resultados dos experimentos de acurácia e sincronização foram abaixo do esperado, contudo, para a acurácia é possível obter melhores resultados com a substituição do relógio do dispositivo e para a sincronização acredita-se ser possível em um trabalho futuro melhorar o método de sincronização com repetição de consultas ou redundância de servidores de tempo.

Quanto a descentralização, o método de obtenção do carimbo localmente minimiza os problemas de indisponibilidade de serviço, escalabilidade e necessidade de infraestruturas avançadas por parte das ACT. Acredita-se também que um dispositivo com baixo custo é capaz de introduzir novos usuários e adoção em novas tecnologias.

Como trabalhos futuros, pretende-se comparar os SCT das ACT e os Módulos de Segurança Criptográfico por eles utilizados com o DCT desenvolvido através de experimentos. Além disso, buscar-se-ão alternativas para expandir a descentralização do sistema. Por exemplo, a utilização de servidores de tempo independentes, com sistema de homologação do dispositivo e processo de auditoria contínua. Um outro possível trabalho futuro é o estudo de carimbo do tempo em IoT. Nesse caso o subscritor é uma máquina que realiza as solicitações de forma automatizada e possivelmente com alta frequência. Portanto faz necessário o aprofundamento da análise da performance do dispositivo e do método criptográfico neste cenário.

Referências

Bernstein, D. J., Buchmann, J., and Dahmen, E. (2009). *Post-Quantum Cryptography*. Springer, Berlin, 2009 edition. 248p.

Broby, D., Basu, D., and Arulselvan, A. (2019). The role of precision timing in stock market price discovery when trading through distributed ledgers. *Journal of Business Thought*, 10. DOI: 10.18311/jbt/2019/23355.

Buchmann, A. J., Karatsiolis, E., and Wiesmaier, A. (2013). *Introduction to Public Key Infrastructures*. Springer, New York - Dordrecht - London, 1 edition. 194 p.

Cooper, D. A., Apon, D. C., Dang, Q. H., Davidson, M. S., Dworkin, M. J., and Miller, C. A. (2019). Recommendation for stateful hash-based signature schemes. *Draft NIST Special Publication 800-208*. DOI: 10.6028/NIST.SP.800-208-draft.

Coulouris, G., Dollimore, J., Kindberg, T., and Blair, G. (2013). *Sistemas Distribuídos - Conceitos e Projetos*. Bookman, Porto Alegre, 5 edition. 1055p.

CryptoID (2020). *IoT começa a demandar certificação digital*. Disponível em: https://cryptoid.com.br/identidade-digital-destaques/iot-comeca-a-demandar-certificacao-digital/. Acesso em 23 de janeiro de 2020.

Espressif (2020). *ESP32 - Technical Reference Manual*. Disponível em: https://www.espressif.com/sites/default/files/documentation/esp32_technical_reference_manual_en.pdf. Acesso em 05 de setembro de 2020.

Fan, L. and Wong, C. P. (2001). Thermosetting and thermoplastic bisphenol a epoxy/phenoxy resin as encapsulant material. *Proceedings International Symposium on Advanced Packaging Materials Processes, Properties and Interfaces*, pages 230–235. DOI: 10.1109/ISAOM.2001.916580.

Gipp, B., Meuschke, N., and Gernandt, A. (2015). Decentralized trusted timestamping using the crypto currency bitcoin. Disponível em: https://arxiv.org/abs/1502.04015. Acesso em: 02 de julho de 2020.

Hadizadeh, R., Laitinen, A., Molinero, D., Cunningham, S., Vockerberger, C., and Weis, G. (2019). Embedded component packaging for wafer-level encapsulated and integrated rf mems. *2019 20th International Conference on Solid-State Sensors, Actuators and Microsystems & Eurosensors XXXIII*, pages 1615–1618. DOI: 10.1109/TRANSDUCERS.2019.8808808.

Harmann, P. (2019). Distributed trusted timestamp. *Master's Thesis, Masaryk University*. Disponível em: https://is.muni.cz/th/bgmmw/Trusted_Timestamping_v3_is.pdf. Acesso em: 02 de julho de 2020.

ICP-Brasil (2015). *DOC-ICP-11 versão 1.3 - VISÃO GERAL DO SISTEMA DE CARIMBOS DO TEMPO NA ICP-BRASIL*. Disponível em: https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-11-versao-1-3-visao-geral-do-sist-de-cts-na-icp-brasil-30-09-2015-pdf. Acesso em 23 de fevereiro de 2020.

ICP-Brasil (2017). *Manual de Condutas Técnicas 3 – Volume I - Requisitos, Materiais e Documentos Técnicos para Homologação de Tokens Criptográficos no Âmbito da ICP-Brasil*. Disponível em: http://iti.gov.br/images/repositorio/legislacao/manuais-de-conduta-tecnica/MCT3_Vol.I.pdf. Acesso em 20 de fevereiro de 2020.

IRTF (2020). *Request for Comments: 8391 - XMSS: eXtended Merkle Signature Scheme*. Internet Research Task Force. Disponível em: https://tools.ietf.org/html/rfc8391. Acesso em 02 de julho de 2020.

ITI (2008). Uso do carimbo do tempo é oficial no brasil. Disponível em: https://www.iti.gov.br/noticias/68-iti-na-midia/1602-uso-do-carimbo-do-tempo-e-oficial-no-brasil. Acesso em 20 de janeiro de 2020.

ITI (2017a). Autoridades de carimbo do tempo. Disponível em: https://www.iti.gov.br/icp-brasil/autoridades-de-carimbo-do-tempo. Acesso em 21 de janeiro de 2020.

ITI (2017b). Equipamentos certificados. Disponível em: https://www.iti.gov.br/homologacao/64-homologacao/212-equipamentos-homologados. Acesso em 21 de janeiro de 2020.

ITI (2020). Certificado digital - saiba mais. Disponível em: https://aquitemcd.iti.gov.br/certificado-digital/1. Acesso em 29 de janeiro de 2020.

Kakei, S., Mohri, M., Shiraishi, Y., and Noguchi, R. (2012). Offline time-stamping system: Its design and implementation. *2012 IEEE International Conference on Control System, Computing and Engineering*, pages 404–409. DOI: 10.1109/ICCSCE.2012.6487179.

Kurose, J. and Ross, K. (2013). *Computer Networking - A Top-Down Approach*. Pearson, United States of America, 6 edition. 998p.

Neumann, C., Heen, O., and Onno, S. (2014). Dnstamp: Short-lived trusted timestamping. *Computer Networks. 2014, vol. 64*, pages 208–224. DOI: 10.1016/j.comnet.2014.02.016.

NTP.BR (2020). *O NTP*. Disponível em: https://ntp.br/ntp.php. Acesso em 20 de fevereiro de 2020.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126. DOI: 10.1145/359340.359342.

Santiago, C. (2019). Soluti responde - act: o que é e como aplicar um carimbo do tempo? Disponível em: https://solutiresponde.com.br/act-o-que-e-e-como-aplicar-um-carimbo-do-tempo/. Acesso em 20 de janeiro de 2020.

Shostack, A. (2014). *Threat Modeling: Designing for Security*. Wiley, Indianapolis - USA, 1 edition. 590p.

Starnberger, G., Froihofer, L., and Goeschka, K. M. (2010). Using smart cards for tamper-proof timestamps on untrusted clients. *2010 International Conference on Availability, Reliability and Security*, pages 96–103. DOI: 10.1109/ARES.2010.78.

Triola, M. F. (2013). *Introdução à estatística: atualização da tecnologia*. LTC, Rio de Janeiro, 11 edition. 707p.

Vigil, M., Buchmann, J., Cabarcas, D., Weinert, C., and Wiesmaier, A. (2015). Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: A survey. *Computers & Security*, 50:16–32. DOI: 10.1016/j.cose.2014.12.004.