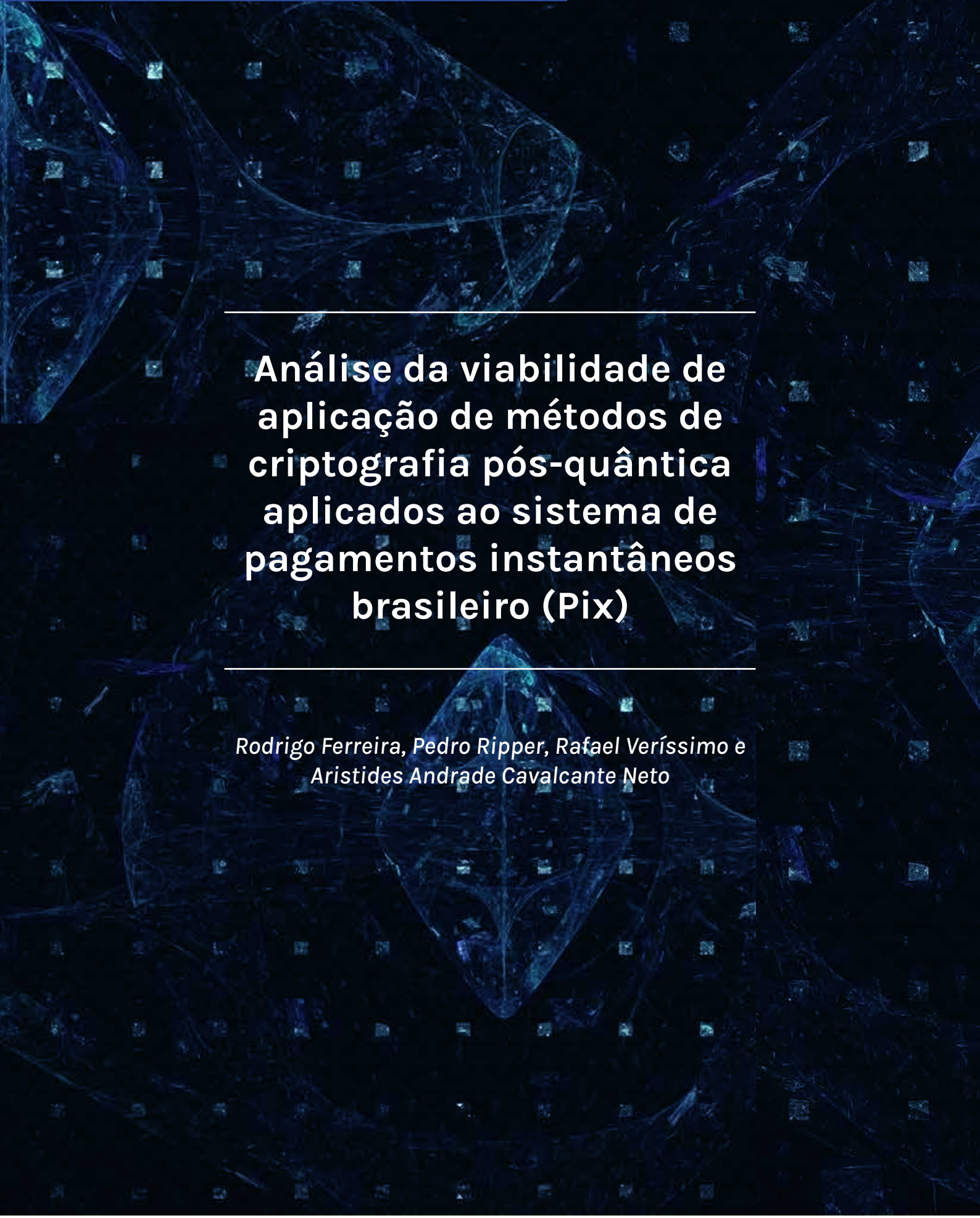


Análise da viabilidade de aplicação de métodos de criptografia pós-quântica aplicados ao sistema de pagamentos instantâneos brasileiro (Pix)

Rodrigo Ferreira, Pedro Ripper, Rafael Veríssimo e Aristides Andrade Cavalcante Neto

Autoria

BANCO CENTRAL DO BRASIL

Parceria

Brazil Quantum

Microsoft

Apoio

Fenasbac

Análise da viabilidade de aplicação de métodos de criptografia pós-quântica aplicados ao sistema de pagamentos instantâneos brasileiro (Pix)

Rodrigo Ferreira[1], *Pedro Ripper*[1], *Rafael Veríssimo*[1] *e Aristides Andrade Cavalcante Neto*[2]

E-mail
contato@brazilquantum.com

Facilitador da pesquisa
Aristides Andrade Cavalcante Neto

1 *Brazil Quantum, São Paulo, SP, Brasil*
2 *Banco Central do Brasil, Brasília, DF, Brasil*

Análise da viabilidade de aplicação de métodos de criptografia pós-quântica aplicados ao sistema de pagamentos instantâneos brasileiro (Pix)

Aristides Andrade Cavalcante Neto (aristides.andrade@bcb.gov.br)
Pedro Ripper (pedro.ripper@brazilquantum.com)
Rafael Veríssimo (rafael.verissimo@brazilquantum.com)
Rodrigo Ferreira (rodrigo.ferreira@brazilquantum.com)

Abstract

Developing quantum computers creates new opportunities and challenges simultaneously. Their high information processing has motivated the creation of post-quantum cryptography (PQC), which contemplates cryptographic methods resistant to potential quantum attacks. In such a context, this study analyzes the feasibility of implementing post-quantum algorithms into the Brazilian Instant Payment Scheme (Pix). To achieve that goal, we analyze the current state of PQC and Pix cryptography. We then perform implementation tests of the Picnic scheme as well as results and future work discussions.

Resumo

O desenvolvimento de computadores quânticos proporciona, simultaneamente, novas oportunidades e desafios. O elevado processamento de informação motivou o surgimento da criptografia pós-quântica (CPQ), a qual contempla métodos criptográficos resistentes aos eventuais ataques de computadores quânticos. Nesse contexto, o presente estudo analisa a viabilidade de implementação de algoritmos pós-quânticos no Sistema de Pagamentos Instantâneos Brasileiro (Pix). Para tanto, parte-se de uma análise do estado atual da CPQ e da criptografia vigente no Pix. Em seguida, realiza-se testes de implementação do método Picnic, discussão dos resultados e proposta de trabalhos futuros.

1. Introdução

Nos últimos anos, o investimento na Computação Quântica vem crescendo vertiginosamente. As expectativas sobre o que um computador quântico pode fazer vem atraindo novos investidores e proporcionando o desenvolvimento de novas empresas, as quais já estão se destacando no mercado. Um bom exemplo disso é a startup IonQ que, em 2021, se tornou a primeira empresa de capital aberto focada em Computação Quântica - com *valuation* de 2 bilhões de dólares [16].

Neste momento, o cenário da Computação Quântica é tal que os sistemas são bastante limitados por operações ruidosas e interações com o ambiente. Esse período é chamado de Era NISQ (*Noise Intermediate-Scale Quantum)* [17], nome que faz referência às tecnologias quânticas de escala intermediária e ruidosas.

Os computadores quânticos deste estágio não apresentam, ainda, qualquer aplicação no mundo real. Esses impedimentos técnicos vêm sendo atacados tanto pela academia quanto pela indústria. Assim, em meio a tal fomento, os computadores quânticos estão evoluindo cada vez mais rápido, com algumas aplicações práticas tornando-se possíveis em um horizonte de 5 a 10 anos [22].

Tal desenvolvimento acelerado também está associado à ameaça que os computadores quânticos poderão oferecer aos sistemas criptográficos atuais. Alguns algoritmos quânticos são capazes de quebrar certos protocolos, como é o caso do Algoritmo de Shor [18] para fatoração de números primos - capaz de quebrar o sistema criptográfico RSA (amplamente utilizado) para uma quantidade suficientemente grande de *qubits*.

Como se sabe, na atual Era NISQ, os computadores quânticos não representam, ainda, uma ameaça tangível à criptografia vigente. Entretanto, em meio à eventual adversidade (exposição repentina de décadas de *backlog* de criptografia RSA), estudos já têm sido conduzidos a fim de encontrar sistemas criptográficos resistentes aos algoritmos quânticos.

A chamada Criptografia Pós-Quântica (CPQ) - também conhecida como *quantum safe* ou *quantum resistant* - apresenta-se como solução para tal questão. Ela consiste em um conjunto de problemas matemáticos clássicos que são desafiadores o suficiente até mesmo para computadores quânticos. Dessa forma, como não há ganho substancial de velocidade na resolução desses problemas via computação quântica, os sistemas tornam-se resistentes a ataques quânticos.

Alguns protocolos de criptografia já existentes, junto com novos que vem sendo desenvolvidos, compõem o grupo de algoritmos pós-quânticos. Diante desse panorama, o *National Institute of Standards and Technology* (NIST), dos EUA, criou um processo de padronização de criptografia pós-quântica, em parceria com empresas e universidades ao redor do mundo [6].

Em meio a essa iniciativa internacional e à postura de vanguarda tecnológica assumida pelo Banco Central do Brasil (BCB), foi proposto um estudo de viabilidade sobre a aplicação de alguns desses algoritmos visados pelo programa do NIST no sistema Pix (sistema de pagamento instantâneo brasileiro), desenvolvido pelo BCB. Esse trabalho foi desenvolvido pela equipe da Brazil Quantum, com apoio da Microsoft no Brasil e do time técnico do BCB.

O estudo desenvolvido iniciou-se com a seleção dos algoritmos *quantum-safe* (dentre os candidatos viáveis do NIST) adequados ao contexto do Pix, visando os critérios: segurança, performance e cripto-agilidade (facilidade de transição de um sistema criptográfico clássico para outro pós-quântico). Em seguida, foram feitas as implementações, tomando como base o tráfego padrão de mensagens pelo Pix. Assim, foi possível realizar uma comparação

entre a performance atual (via métodos clássicos) e aquela que seria obtida em um cenário de sistemas criptográficos pós-quânticos.

O presente artigo consiste em uma breve introdução à CPQ, seguida de uma revisão do seu estado atual. Posteriormente, resume-se o estado atual da criptografia utilizada no Pix, bem como a análise dos algoritmos pós-quânticos e sua implementação. Por fim, são expostos os resultados obtidos a partir das simulações realizadas e a discussão acerca das conclusões e das próximas etapas do trabalho desenvolvido.

2. Fundamentos de Criptografia Pós-Quântica

Apresentada anteriormente, a Criptografia Pós-Quântica é a área que estuda algoritmos presumidamente *quantum safe*, ou seja, resistentes a ataques de computadores quânticos. Uma importante questão a ser levada em conta sobre a Criptografia Pós-Quântica é que não se sabe exatamente o poder que a Computação Quântica de larga escala e resistente a erros irá possuir. Nesse sentido, alguns algoritmos denominados hoje como pós-quânticos podem, em alguns anos, perder sua classificação.

Tal cenário evidencia a importância do projeto do NIST [6], o qual vem examinando uma gama de diferentes algoritmos pós-quânticos desde dezembro de 2016. Esses algoritmos variam em dois principais aspectos. Primeiramente, podem ser divididos pelo seu propósito final: criptografia de chave pública ou assinatura digital.

Além disso, são categorizados segundo o problema matemático no qual eles são baseados, formando, assim, as diferentes famílias de algoritmos pós-quânticos, dentre as quais destacam-se:

- ***Hash-Based:*** sistemas criptográficos em *hash* têm sua segurança fundamentada na resistência de colisão e na inversibilidade de suas funções *hash*. A criptografia *Hash-Based* é largamente usada em protocolos de assinatura digital. Assim, sendo dependente apenas de uma função de *hash* segura, assinaturas digitais *Hash-Based* não apresentam grandes custos computacionais. Dentre os algoritmos *Hash-Based*, tem-se como exemplo o SPHINCS+ [19,20,21].
- ***Code-Based:*** a criptografia *Code-Based* tem como primitiva a teoria de código de correção de erros. Ela oferece como vantagem pequenas assinaturas sob um custo de chaves extensas. Nesse grupo de algoritmos se destacam Classic McEliece, BIKE e HQC [19,20].
- ***Lattice-Based:*** a criptografia *Lattice-Based* (baseada em reticulados) faz uso de problemas matematicamente difíceis dentro do estudo de reticulados. É a família de algoritmos pós-quânticos com maior número de candidatos na Terceira Rodada do programa de padronização de CPQ do NIST, como NTRU, Saber e Frodo-KEM [19,20].

Cabe destacar que a existência de algoritmos de CPQ não é suficiente para garantir a segurança de sistemas. Em alguns anos, com a eventual construção de um computador quântico poderoso o suficiente para executar algoritmos capazes de quebrar protocolos de criptografia como o RSA, não bastaria apenas realizar uma troca por um algoritmo pós-quântico. Isso se deve ao fato de que a CPQ ainda possui muitas questões a serem analisadas, como a eficiência dos seus algoritmos, sua segurança e portabilidade para diferentes tecnologias.

Diante desse panorama, o processo de padronização do NIST é de grande importância, sendo essencial para aperfeiçoar e selecionar os algoritmos classificados como pós-quânticos mais aptos para impedir ameaças à segurança digital vigente.

3. Estado atual da Criptografia Pós-Quântica

O processo da padronização da CPQ pelo NIST [6] revelou-se um importante marco na área. Esse projeto é baseado em rodadas, nas quais diferentes algoritmos são disponibilizados para serem avaliados, a fim de encontrar falhas e pontos de melhoria. Os sistemas criptográficos submetidos têm toda sua documentação disponível em código aberto, a fim de democratizar o seu acesso e entendimento.

Com a primeira rodada iniciada no final de 2016, o processo encontra-se, hoje, em sua terceira etapa. Nesse período, alguns algoritmos foram descartados devido a fraquezas encontradas. Outros, por outro lado, formaram uma lista de possíveis alternativas, podendo ainda ser revisitados no futuro. Os melhores algoritmos selecionados em cada etapa vão sendo adaptados segundo aperfeiçoamentos sugeridos e passam para a próxima fase.

É importante salientar, novamente, que mesmo os algoritmos que vêm apresentando bons resultados pelo NIST ainda podem ser descartados em eventuais etapas futuras do processo. Devido ao avanço consistente da pesquisa em CPQ, novas abordagens e tentativas de ataques são descobertas constantemente, o que pode alterar a perspectiva de decisão final de padronização do NIST.

4. Resumo da criptografia atual do Pix

O sistema de pagamentos instantâneos brasileiro (Pix) possui a segurança como um dos elementos primordiais de seu funcionamento. Para assegurá-la, é necessário estabelecer uma série de protocolos que definem as interações entre todas as partes do sistema de pagamentos [2].

Tais protocolos contemplam a criptografia da comunicação, a autenticação, os processos de assinatura digital e de gestão dos certificados digitais. Ademais, também deve ser realizada a manutenção de *logs* de auditoria a fim de prover rastreabilidade das transações realizadas na rede do Pix [1].

Nesse sentido, tem-se que a comunicação entre cada Provedor de Serviços de Pagamento (PSP) e as *API*s do Pix é realizada por meio da Rede do Sistema Financeiro Nacional (RSFN). Tal comunicação deve obedecer às normas estabelecidas pelo Manual de Redes do SFN [2].

A conexão entre o PSP e as *API*s disponíveis ocorre por meio do protocolo *HTTP* (*Hypertext Transfer Protocol*) 1.1, portando criptografia *TLS* (*Transport Layer Security*) versão 1.2 ou superior, com autenticação mútua obrigatória no momento da conexão. Os algoritmos utilizados nessa criptografia estão dispostos na tabela seguinte.

Tabela 1. Funções e respectivos algoritmos na criptografia TLS utilizada no Pix.

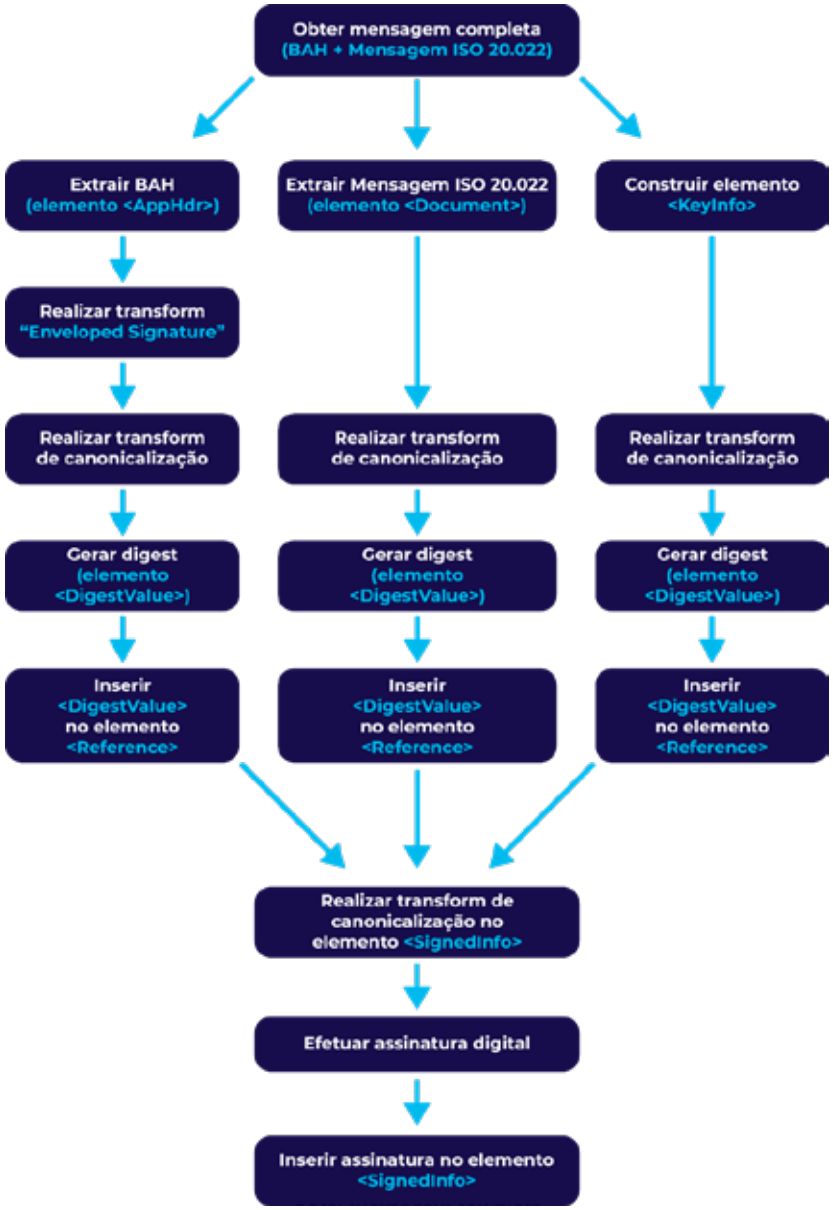
Função	Algoritmo
Troca de Chaves	ECDHE
Autenticação	RSA
Criptografia Simétrica	AES-128, modo GCM
MAC (*Message Authentication Code*)	SHA-256

Vale ressaltar que tanto o BCB quanto o PSP devem utilizar certificados ICP-Brasil [3] (padrão SPB). Além disso, os clientes *HTTP* do PSP necessitam respeitar o *TTL* (*Time To Live*) dos servidores *DNS*, de modo a garantir a disponibilidade de acesso às *API*s do Pix no momento desejado.

Para garantir a integridade das transações no Pix, as mensagens trafegadas no Sistema de Pagamentos Instantâneos (SPI) necessitam ser assinadas digitalmente pelo emissor [1]. Independentemente da operação realizada (considerando os diferentes tipos de mensagens utilizadas [1,2]), tanto no SPI quanto no DICT (Diretório de Identificadores de Contas Transacionais), a resposta do BCB para o PSP sempre será assinada.

No Pix, o padrão de assinatura digital utilizado é o *XMLDSig* [4] e, no SPI, as mensagens devem ser do tipo *ISO 20.022* [5]. Nesse contexto, as informações que devem ser assinadas são: a mensagem *ISO 20.022* (elemento <*Document*>), o cabeçalho *BAH* (elemento <*AppHdr*>) e o elemento <*KeyInfo*>. A figura 1 [1] ilustra o processo de assinatura digital das mensagens no SPI.

Figura 1. Fluxograma da assinatura digital de mensagens no SPI.



5. Criptografia pós-quântica no contexto do Pix

Para a análise da CPQ no contexto do Pix, utilizou-se como referência o *NIST Post-Quantum Cryptography Standardization Process* [6]. Em seu segundo *round*, o NIST selecionou 26 algoritmos ao total. Referente a troca de chaves, tem-se os algoritmos: Classic McEliece, CRYSTALS-KYBER, NTRU, SABER, BIKE, FrodoKEM, HQC, NTRU Prime, SIKE, LAC, LEDAcrypt, NewHope, NTS-KEM, ROLLO, Round5, RQC e Three Bears. Por outro lado, os algoritmos de assinatura digital foram: CRYSTALS-DILITHIUM, FALCON, Rainbow, GeMSS, Picnic, SPHINCS+, LUOV, MQDSS e qTESLA [6].

No terceiro *round* do processo de padronização do NIST, foram selecionados 15 algoritmos, os quais foram categorizados como candidatos "finalistas" ou "alternativos". Os ditos "finalistas" são algoritmos que o NIST considera com maior potencial de estandardização ao término do terceiro *round*. Por sua vez, os candidatos "alternativos" são percebidos pelo NIST como potenciais padrões futuros, após outras rodadas de avaliação [14]. A relação dos candidatos finalistas e alternativos pode ser observada nas tabelas 2 e 3, respectivamente [14].

Tabela 2. Candidatos finalistas do terceiro *round*.

Troca de Chaves	Assinatura Digital
Classic McEliece	CRYSTALS-DILITHIUM
CRYSTALS-KYBER	FALCON
NTRU	Rainbow
SABER	

Tabela 3. Candidatos alternativos do terceiro *round*.

Troca de Chaves	Assinatura Digital
BIKE	GeMSS
FrodoKEM	Picnic
HQC	SPHINCS+
NTRU Prime	
SIKE	

Alinhado aos critérios de avaliação destacados pelo NIST, os autores consideraram os seguintes parâmetros em seu estudo:

- **Segurança**: o fator mais importante para o NIST [6], o qual definiu cinco níveis de segurança com base na quantidade de recursos computacionais necessários para realizar um ataque força bruta;
- **Custo e performance**: segundo aspecto mais relevante, considerando os custos computacionais e de transferência de dados, bem como o desempenho dos algoritmos na geração de chaves ou autenticação de assinaturas digitais;
- **Cripto-agilidade:** fator crucial para a implementação de criptografia pós-quântica no Pix, uma vez que os algoritmos selecionados devem ser facilmente implementados aos sistemas já existentes (a transição deve ser facilitada).

De posse de tais condições e do suporte oferecido pela Microsoft, a Brazil Quantum optou pela análise dos algoritmos desenvolvidos pelo time da *Microsoft Research*: FrodoKEM, SIKE, qTESLA (de troca de chaves) e Picnic (de assinatura digital) [7].

Após deliberação conjunta com a equipe desenvolvedora do Pix, concluiu-se que a forma como o sistema foi construído inviabiliza uma análise do tempo e custo computacional da troca de chaves isoladamente. Isto ocorre porque, no Pix, as mensagens não são criptografadas individualmente, mas sim na camada de transporte – uma vez que elas são transmitidas via HTTP.

Tal cenário proporcionou, portanto, o estudo direcionado à assinatura digital de mensagens no SPI. Dessa forma, a equipe da Brazil Quantum dedicou-se a implementar o algoritmo Picnic (considerando as configurações atuais de criptografia do Pix) e a analisar os resultados obtidos tendo como base a performance atual do Pix.

6. Picnic

Picnic é um algoritmo *quantum-safe* (CPQ) de assinatura digital desenvolvido por pesquisadores da Universidade de Aarhaus, AIT GmbH, DFINITY, Universidade de Tecnologia de Graz, *Georgia Tech*, *Microsoft Research*, Universidade Northwestern, Universidade de Princeton, Universidade Técnica da Dinamarca e Universidade de Maryland [8]. A segurança oferecida pelo Picnic é oriunda de um sistema de *zero-knowledge proof* (ZKP), no qual o emissor consegue demonstrar ao receptor que sabe a mensagem que foi encriptada, sem necessitar revelá-la.

Além do ZKP, o Picnic também utiliza estruturas como cifras de bloco e funções *hash* [9], garantindo uma segurança em nível pós-quântico ao algoritmo. Com isso, procede-se para a análise dos componentes criptográficos do Picnic (*LowMC,* função *hash*, função de derivação de chave) [10] a fim de determinar qual configuração melhor atende às demandas do Pix:

- ***LowMC***: uma cifra de bloco parametrizável utilizada na simulação de um protocolo MPC (*Multi-Party Computation*), a qual é definida a partir da ordem *n* das matrizes binárias e do número *r* de rounds do *LowMC;*
- **Função *hash*:** um algoritmo que mapeia dados de comprimento variável para uma saída de comprimento fixo e que, no caso do Picnic, pode ser SHAKE128 ou SHAKE256 (a depender do nível *L* de segurança considerado);
- **Função de derivação de chave (KDF):** ao criar e verificar assinaturas digitais, é necessário expandir um pequeno valor aleatório (*seed*) de 128 a 512 *bits* de tamanho para um maior (de cerca de 1 kB), o que pode ser feito por meio de uma função SHAKE. Para o Picnic, emprega-se a mesma função (SHAKE128 ou SHAKE256) para o *hashing* e derivação de chave.

Ademais, as implementações do *zero-knowledge proof* do Picnic podem ser feitas com base nas transformações Fiat-Shamir (FS) ou Unruh (UR) [10], gerando duas variantes do Picnic que devem ser testadas em cada nível de segurança. Tais níveis foram denominados (pelo NIST) L1, L3 e L5 [11] como sendo correspondentes à segurança oferecida por AES-128, AES-192 e AES-256, respectivamente.

Neste estudo, também foi realizada a análise da 3ª versão do algoritmo (*Picnic3*), a qual apresenta diferenças sutis em sua implementação. A seguinte tabela resume os parâmetros

criptográficos presentes em cada tipo do Picnic, incluindo os *S bits* de segurança esperados (*S* para ataques clássicos e, no mínimo, *S/2* para ataques quânticos):

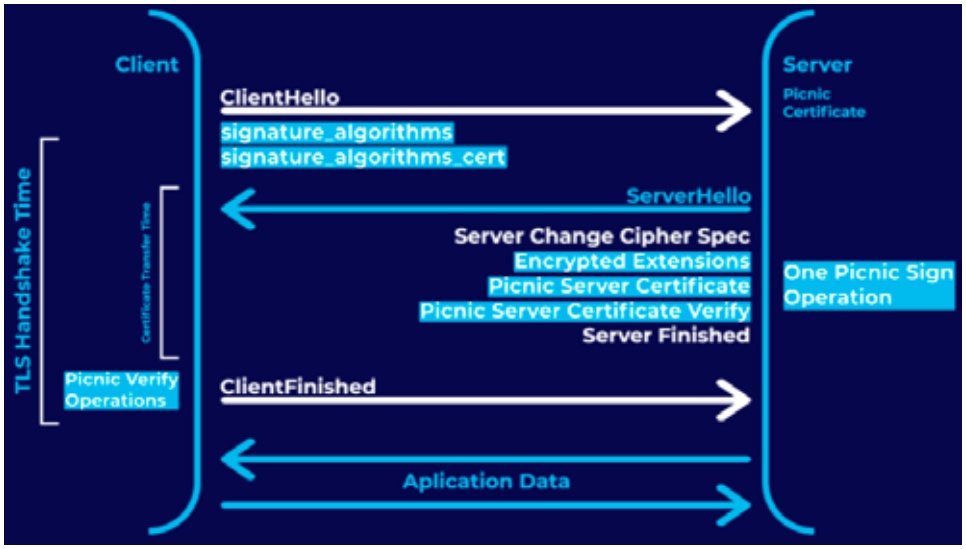
Tabela 4. Tipos de Picnic e seus respectivos parâmetros criptográficos.

Tipo Picnic	*S[bits]*	*n[bits]*	*r[rounds]*	*k[bits]*	*Hash/KDF*
Picnic L1	128	128	20	128	SHAKE128
Picnic L3	192	192	30	192	SHAKE256
Picnic L5	256	256	38	256	SHAKE256
Picnic3 L1	128	129	4	128	SHAKE128
Picnic3 L3	192	192	4	192	SHAKE256
Picnic3 L5	256	255	4	256	SHAKE256

Note que o tamanho *k* indicado na Tabela 4 corresponde ao tamanho da chave (*keysize*), em *bits*, empregada no algoritmo. Além disso, os valores dos parâmetros criptográficos mantêm-se os mesmos para ambas as versões de Picnic (Picnic-FS e Picnic-UR).

A Figura 2 ilustra a arquitetura (em alto nível) de funcionamento do Picnic, contemplando a interação entre cliente e servidor. A telemetria adotada nesse caso foi o *TLS Handshake time*.

Figura 2. Arquitetura em alto nível do funcionamento do Picnic em uma interação cliente-servidor.



7. Implementação

Ao analisar as possíveis opções dos parâmetros criptográficos do Picnic, a realizou-se a implementação e testes das versões Picnic L3 e Picnic3 L3, uma vez que estas apresentam similaridades com a configuração atual do Pix (com foco na cripto-agilidade). Com isso, foram investigadas potenciais mudanças que poderiam ser realizadas no contexto do Pix para torná-lo *quantum-safe* em seu processo de assinatura digital.

Tais adaptações incluem precisamente a mudança do algoritmo RSA-SHA256 para o Picnic, o que pode ser obtido ao editar o elemento <*SignatureMethod*> do Pix. Conforme indica a literatura [12], espera-se que o Picnic possa ser, de fato, uma opção viável para o

futuro da assinatura digital, por ser consideravelmente mais resistente a ataques quânticos do que os métodos tradicionais.

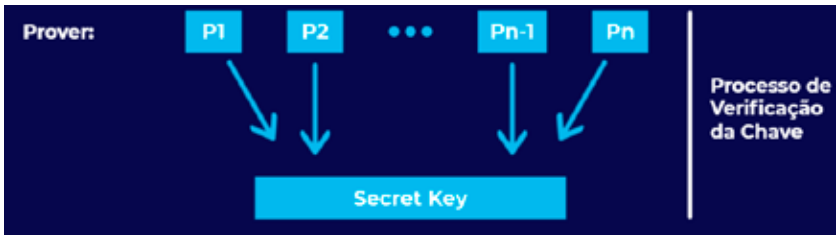
Dessa forma, procedeu-se o estudo para a etapa de testes do Picnic L3 (FS e UR) e Picnic3 L3. O teste realizado é composto por quatro etapas: geração da chave, assinatura da mensagem, verificação da assinatura e serialização das chaves. O processo é ilustrado na figura seguinte.

Figura 3. Procedimento de teste realizado no Picnic.

Conforme indica a Figura 3, o *signer* (de posse da chave secreta) consegue gerar sua prova de conhecimento (*proof of knowledge*), a qual será combinada com a mensagem, constituindo o processo de assinatura digital. Em seguida, ocorre a serialização que, em essência, reduz o espaço que a assinatura ocupa na memória.

Na etapa de verificação da assinatura, tem-se a simulação de *N* partes – cada uma contendo uma fração da chave secreta. Tais partes necessitam, então, juntar suas respectivas frações a fim de formar a chave secreta desejada e verificar se ela satisfaz o problema da prova de conhecimento.

Figura 4. Verificação de chave no teste do Picnic.



Para a realização dos testes, ainda resta definir o tamanho das mensagens. Para tanto, considerou-se as mensagens comumente trafegadas no SPI, sejam elas de uma operação (tabela 5) ou múltiplas operações (tabela 6), como é o caso da *Pacs. 008* [1,2]. Assim, considerou o intervalo de tamanho de mensagens entre o mínimo e máximo trafegado para a realização dos testes do Picnic.

Tabela 5. Tipos e tamanhos de mensagem comumente trafegadas no ambiente Pix.

Tipo de Mensagem	Tamanho (kB)
Admi. 002	2,7
Pibr. 001	2,4
Pibr. 002	2,4
Pacs. 002	2,6

Tipo de Mensagem	Tamanho (kB)
Pacs. 004	3,0
Pacs. 008	3,5
Camt. 040	2,7
Camt. 052	2,8
Camt. 053	3,0
Camt. 054	3,8
Camt. 060	2,7
Reda. 014	2,6

Tabela 6. Quantidade de operações Pacs. 008 e tamanho em KB.

Quantidade de operações [Pacs. 008]	Tamanho (kB)
1	3,5
2	4,4
3	5,3
4	6,2
5	7,1
6	8,0
7	8,9
8	9,8
9	10,7
10	11,6

8. Resultados

Conforme ilustrado nas tabelas 5 e 6, o tamanho das mensagens comumente trafegadas oscila entre 2 KB e 12 KB. Dessa forma, foram realizadas 100 iterações para cada versão considerada (Picnic L3 FS, Picnic L3 UR, Picnic3), com a medição de todos os tempos obtidos. Em seguida, foi plotado o tempo médio para cada tamanho de mensagem. Note que todos os casos foram bem-sucedidos, isto é, realizaram as quatro etapas do teste com êxito.

Figura 5. Tempo de assinatura médio em função do tamanho das mensagens.

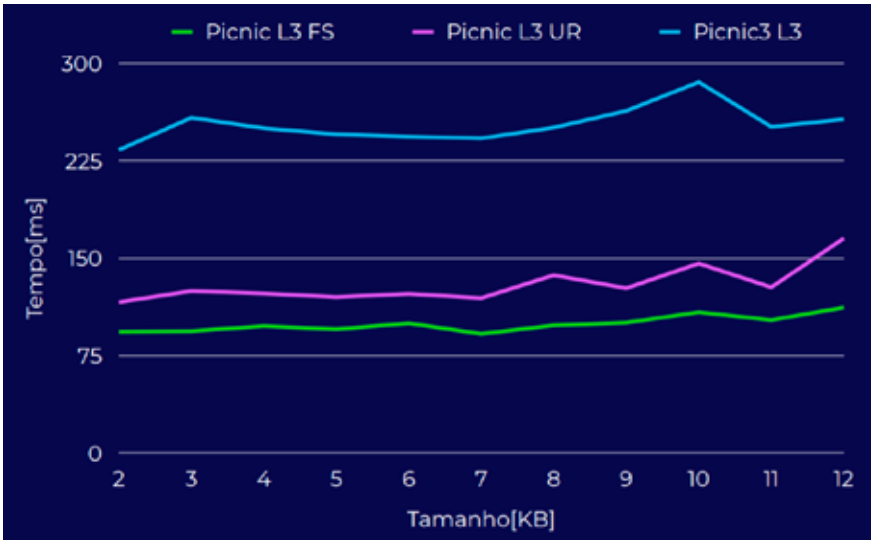


Figura 6. Tempo total médio em função do tamanho das mensagens.

Os resultados ilustrados nas Figuras 5 e 6 foram obtidos em ambiente de programação com processador Intel Core i7-8550U 1.99 GHz e compilador GNU GCC 5.4.72 (WSL2). O guia de uso, bem como o *docker* de testes, pode ser encontrado na página da Brazil Quantum no GitHub [13].

Tais resultados foram comparados com os dados dos testes de carga fornecidos pelo BCB. Portanto, como referência, tem-se os tempos (em milissegundos) para processar cada tipo de mensagem (pacs.002, pacs.004, pacs.008, admi.002, camt.052, camt.053 e pibr.002) desde a sua leitura até a confirmação de escrita. O tempo medido também inclui a criação e assinatura da mensagem XML.

O teste realizado simulou aproximadamente 2000 tps (*transactions per second*) por um tempo de 10 minutos com os diferentes tipos de mensagens sendo trafegadas. Em seguida, coletou-se os tempos mínimo, médio, máximo, além das latências P5, P50, P95 e P99. Uma amostra de tais resultados pode ser observada na tabela 7.

Tabela 7. Propriedades de mensagens trafegadas no ambiente Pix.

Tipo de mensagem	Quantidade de operações	Número de mensagens	Menor tempo	Tempo médio	Maior tempo	P5	P50	P95	P99
Admi.002	1	524	9	23	107	13	22	31	52
Camt.052	1	9	14	21	28	15	22	26	28
Camt.053	1	342	9	26	171	15	24	45	91
Pacs.002	7	2720	11	27	171	18	25	43	60
Pacs.004	2	2	24	27	29	24	27	29	29
Pacs.008	5	1657	13	29	237	20	26	44	64
Pibr.002	1	400	12	26	199	15	24	37	70

Empregando a mesma métrica (tempo total médio), os resultados do teste de carga para o Pix foram de valores entre 22 e 32 milissegundos, a depender do tamanho da mensagem (entre 2 kB e 12 kB). Em comparação ao desempenho das versões do Picnic, nota-se que esta abordagem apresenta o tempo total significativamente maior.

9. Conclusões

A implementação das versões Picnic L3 FS, Picnic L3 UR e Picnic3 L3 no ambiente com processador Intel Core i7-8550U 1.99 GHz via compilador GNU GCC fornece resultados que comprovam a incompatibilidade com as demandas atuais do Pix, o qual requer um piso de 2000 mensagens por segundo (com tempo esperado de até 50 milissegundos por mensagem).

Nesse contexto, os testes de assinatura da mensagem via Picnic L3 FS apresentaram um tempo de processamento de 4 a 5 vezes maior. Destaca-se, também, que os resultados obtidos nesta simulação estão de acordo com a literatura atualizada acerca da performance do Picnic [26].

Contudo, é importante notar que as condições de operação dos sistemas criptográficos comparados não são as mesmas. Internamente, o Pix faz uso de um HSM (*Hardware Security Module*) da DINAMO Networks [23] que possibilita até 4000 operações por segundo. No mercado atual, já existem soluções de HSM suportando cenários de criptografia *quantum-safe*, conforme ofertado por empresas como Thales [24] e Utimaco [25].

10. Discussões e Trabalhos Futuros

De acordo com os resultados obtidos, pode-se perceber que, apesar de certas vantagens (maior segurança e menores chaves públicas), as aplicações do Picnic L3 ou Picnic3 L3 são significativamente mais lentas. De modo geral, a abordagem proposta no Picnic é consideravelmente nova e está em constante evolução, sendo necessário, ainda, um amadurecimento do estudo (em especial das cifras de bloco *LowMC*) antes que seja tomado como padrão pelo NIST [14].

Por outro lado, a diversidade do Picnic (pelo fato de não ser baseado em um problema algébrico ou reticulado complexo) é percebida como um fator positivo em uma padronização futura. Por esses motivos, o Picnic foi considerado como um candidato alternativo pelo NIST [14], o que revela que, com determinados aperfeiçoamentos, é promissor para o uso em larga escala em assinaturas digitais.

Um desdobramento natural do estudo realizado seria a investigação de ataques via canais laterais no esquema proposto pelo Picnic. A literatura do assunto [12] indica que implementações diretas provavelmente apresentariam altas incidências de ataques laterais – o que deveria ser ponderado e contornado considerando o contexto de aplicação no Pix.

Ademais, a fim de promover uma comparação consistente do desempenho dos sistemas criptográficos, um próximo passo seria, idealmente, implementar o algoritmo Picnic descrito no mesmo *hardware* utilizado no Pix. Na impossibilidade de fazer tal teste, uma alternativa viável consiste na reprodução do ambiente via *Microsoft Azure* [15], com a descrição adequada do projeto (objetivo, *sizing*, arquitetura, componentes, tempo, etc.). Dessa forma, pode-se obter estimativas mais realistas do custo de adoção de uma API *quantum-safe* no Pix.

Outra abordagem possível consiste na análise de compatibilidade de HSMs (atuantes em cenários pós-quânticos) com o Picnic. Em seguida, deve-se estudar tanto a disponibilidade comercial destes dispositivos quanto os seus limites atuais de operação. O uso de tais aplicações pode aproximar a performance do Picnic daquela demandada pelos padrões atuais do Pix.

11. Referências

[1] Manual de Segurança do Pix Versão 3.3
URL: https://www.bcb.gov.br/content/estabilidadefinanceira/cedsfn/Manual%20de%20Seguranca%20do%20PIX%20v3.3.pdf

[2] Manual de Redes do SFN Versão 9.2
URL: https://www.bcb.gov.br/content/estabilidadefinanceira/cedsfn/Manual_de_Redes_do_SFN_Ver_9.2.pdf

[3] ICP Brasil - Infraestrutura de Chaves Públicas Brasileira
URL: https://www.gov.br/iti/pt-br

[4] *W3C Recommendation - XML Signature Syntax and Processing.*
URL: https://www.w3.org/TR/2008/REC-xmldsig-core-20080610/

[5] Padrão *ISO 20.022*
URL: https://www.iso20022.org/

[6] *NIST Post-Quantum Cryptography Standardization Process.*
URL: https://csrc.nist.gov/projects/post-quantum-cryptography

[7] *Post-quantum cryptography – Microsoft Research*
URL: https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/

[8] *Picnic – Microsoft Research*
URL: https://www.microsoft.com/en-us/research/project/picnic/

[9] *Picnic – A Family of Post-Quantum Secure Digital Signature Algorithms*
URL: https://microsoft.github.io/Picnic/

[10] *The Picnic Signature Algorithm Specification*
URL: https://github.com/Microsoft/Picnic/tree/master/spec

[11] *NIST – Submission requirements and evaluation criteria*
URL: https://beta.csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

[12] Gellersen, T., Seker, O., Eisenbarth, T., (2020) Differential Power Analysis of the Picnic Signature Scheme. ***Cryptology ePrint Archive Preprint.***
URL: https://eprint.iacr.org/2020/267.pdf

[13] *GitHub – Brazil Quantum*
URL: https://github.com/brazilquantum/PQC-Pix

[14] *Status Report on the Second Round of the NIST PQC Standardization Process*
URL: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf

[15] Serviços de Computação em Nuvem – Microsoft Azure
URL: https://azure.microsoft.com/pt-br/

[16] *IonQ Takes Quantum Computing Public With A $2 Billion Deal*
URL: https://www.forbes.com/sites/moorinsights/2021/03/23/ionq-takes-quantum-computing-public-with-a-2-billion-deal/?sh=b62db775d062

[17] *Quantum Computing in the NISQ era and beyond*
URL: https://arxiv.org/abs/1801.00862

[18] *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*
URL: https://arxiv.org/abs/quant-ph/9508027

[19] *Post-Quantum Cryptography*
URL: https://www.springer.com/gp/book/9783540887010

[20] *Post-Quantum Cryptography: Current state and quantum mitigation*
URL: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

[21] *Hash-based Signatures: An Outline for a New Standard*
URL: https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/papers/session5-hulsing-paper.pdf

[22] *IBM's Roadmap for Scaling Quantum Technology*
URL: https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/

[23] *Hardware Security Module (HSM) - DINAMO Networks*
URL: https://www.dinamonetworks.com/hardware-security-module-hsm/

[24] *Using Thales Luna HSMs with quantum-safe security to protect IoT*
URL: https://www.isara.com/downloads/solution_brief/ISARA_Quantum_Safe_Thales.pdf

[25] *Post-quantum crypto agility – Utimaco HSMs*
URL: https://hsm.utimaco.com/solutions/applications/post-quantum-crypto-agility/

[26] Kales, D., Zaverucha, G., (2020) Improving the Performance of the Picnic Signature Scheme. *Cryptology ePrint Archive Preprint.*
URL: https://eprint.iacr.org/2020/427.pdf