SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

RELATÓRIO DE EXAME TÉCNICO

N.° do Pedido:	BR102015028061-0	**N.° de Depósito PCT:**
Data de Depósito:	06/11/2015	
Prioridade Unionista:	-	
Depositante:	UNIVERSIDADE FEDERAL DE MINAS GERAIS (BRMG)	
Inventor:	JEROEN ANTONIUS MARIA VAN DE GRAAF	
Título:	“Método de compartilhamento de dados criptografados entre um grupo através de chaves do tipo cifra de uso único ”	

PARECER

O presente pedido refere-se a um método de compartilhamento de dados criptografados entre um grupo, utilizando chaves de uso único, ou seja, chaves do tipo cifra de uso único (do inglês, one-time pad /OTP). O método requer que todos os usuários estejam de posse de uma chave-mestra, que corresponde a uma tabela T de R linhas de S bits gerados de forma realmente aleatória, proveniente de um processo físico, à qual uma pessoa, que não pertença ao grupo, não tenha acesso. A chave K, do tipo cifra de uso único, que cifrará a mensagem, será gerada através da operação lógica XOR entre N linhas da chave-mestra escolhidas de forma probabilística. Essas posições serão transmitidas juntamente com a mensagem cifrada, de forma descentralizada, uma vez que não há a necessidade de uma entidade central, entre os usuários do grupo.

Em 24/10/2023, por meio da petição 870230094198, o Depositante apresentou argumentações no pedido em resposta ao parecer emitido no âmbito da Resolução Nº 240/2019, notificado na RPI 2743 de 01/08/2023 segundo a exigência preliminar (6.22). Não foram apresentadas modificações no pedido.

Em 10/05/2024, por meio da petição 870240039795, a Requerente apresentou modificações no pedido em resposta ao parecer emitido, notificado na RPI 2771 de 15/02/2024 (despacho 7.1). Estas modificações estão consideradas no Quadro 1.

Quadro 1 – Páginas do pedido examinadas

Elemento	Páginas	n.º da Petição	Data
Relatório Descritivo	1 a 11	870240039795	10/05/2024
Quadro Reivindicatório	1 e 2	870240039795	10/05/2024
Desenhos	--	--	--
Resumo	1	870170037217	02/06/2017

Quadro 2 – Considerações referentes aos Artigos 10, 18, 22 e 32 da Lei n.º 9.279 de 14 de maio de 1996 – LPI		
Artigos da LPI	**Sim**	**Não**
A matéria enquadra-se no art. 10 da LPI (não se considera invenção)		**X**
A matéria enquadra-se no art. 18 da LPI (não é patenteável)		**X**
O pedido apresenta Unidade de Invenção (art. 22 da LPI)	**X**	
O pedido está de acordo com disposto no art. 32 da LPI	**X**	

Comentários/Justificativas: --

Quadro 3 – Considerações referentes aos Artigos 24 e 25 da LPI		
Artigos da LPI	**Sim**	**Não**
O relatório descritivo está de acordo com disposto no art. 24 da LPI	**X**	
O quadro reivindicatório está de acordo com disposto no art. 25 da LPI		**X**

Comentários/Justificativas:

1. Argumentações da requerente:

    1. Argumentação da Requerente: "*Constata-se, portanto, que mesmo um indivíduo que não seja técnico no assunto é capaz de gerar números verdadeiramente aleatórios utilizando tecnologias comercialmente disponíveis baseadas em processos físicos, pois esse conhecimento e essa técnica são comuns e estão disponíveis de forma corriqueira.*

    Ademais, a geração de números verdadeiramente aleatórios NÃO é a técnica sobre a qual versa o pedido de patente BR102015028061-0, tampouco refere-se ao problema técnico que se pretende solucionar com a tecnologia proposta no pedido de patente BR102015028061-0. Apenas tira-se proveito da técnica Physical-RNG para aprimorar a segurança de uma metodologia de compartilhamento de dados criptografados entre um grupo."

    2. Análise da argumentação: A partir da explicação do requerente ficou claro que o pedido é descrito de forma suficiente, apesar de genérico, dessa forma não mais incidindo no Art. 24 da LPI.

    3. Argumentação da Requerente: "Com relação à afirmativa do Examinador de que não há especificação acerca do termo utilizado no relatório descritivo: "Chave-mestra", a Requerente esclarece que há no relatório descritivo inúmeras informações que especificam, descrevem e detalham a "Chave-mestra", por exemplo: 1) A chave mestra corresponde a uma tabela T de R linhas de S bits gerados de forma realmente aleatória proveniente de um processo físico; 2) A chave mestra é compartilhada (no grupo) através de um canal seguro; 3) A chave mestra é utilizada para obtenção da chave secreta K do tipo one-time pad."

4. Análise da argumentação: Os trechos do relatório descritivo citados são especificados pelo resultado alcançado, sem características técnicas da chave. Exemplo: A chave mestra é compartilhada (no grupo) através de um canal seguro. Qual é o grupo a ser compartilhado, pessoas, dispositivos móveis, algoritmos, quaisquer pessoas? O que é um canal seguro, uma comunicação criptografada já existente (HTTPS) ou uma entrega secreta pessoal, um canal de comunicação que “ninguém tem acesso”? Ainda que tais características citadas pela requerente definissem de forma clara e precisa, tais trechos não foram incorporados à reivindicação 1, dessa forma a mesma se mantém imprecisa e não clara.

2. Continuando a análise do pedido de patente:

    1. As características “gerados de forma realmente aleatória e proveniente de um processo físico” e “que foi compartilhada anteriormente entre o grupo através de um canal seguro” usadas na definição da matéria pleiteada na reivindicação 1 são genéricas, impossibilitando a definição clara e precisa da matéria objeto da proteção, o que contraria o disposto no Art. 25 da LPI e na Instrução Normativa nº 30/2013 – Art. 4º (III).
    2. A reivindicação 1 contém trechos explicativos com relação às vantagens e ao simples uso da matéria reivindicada, tais como “ gerados de forma realmente aleatória e proveniente de um processo físico, que foi compartilhada anteriormente entre o grupo através de um canal seguro”, contrariando o disposto no Art. 25 da LPI e na Instrução Normativa nº 30/2013 – Art. 4º (VIII).
        1. No trecho “gerados de forma realmente aleatória e proveniente de um processo físico” não é claro o que é a “forma realmente aleatória”, não trazendo nenhuma característica técnica ao leitor de como é gerada tal forma aleatória. O trecho “proveniente de um processo físico”, que deveria ser usado para especificar tal geração aleatória, é uma simples afirmação, que faz parte do estado da técnica, de como é realizado o uso do gerador.
        2. O trecho “que foi compartilhada anteriormente através de um canal seguro” não apresenta características técnicas para definir o compartilhamento. Somente é explicitado que é realizada uma transferência de dados de um processo físico inacessível a pessoas que não pertençam ao grupo, caracterizando como um simples uso da matéria reivindicada.
    3. A reivindicação independente 1 contraria o disposto no Art. 25 da LPI e na Instrução Normativa nº 30/2013 – Art. 5º (IV e V), pois não possui preâmbulo e define na parte caracterizante, i.e. após a expressão “caracterizado por”, características já compreendidas no estado da técnica, sem evidenciar as características técnicas essenciais e particulares, não compreendidas no estado da técnica.
    4. O trecho explicativo “e à qual o adversário não tenha acesso ” foi removido.
    5. As equações foram corrigidas de forma satisfatória.

Quadro 4 – Documentos citados no parecer

Código	**Documento**	**Data de publicação**
D1	EP1841122	30/12/1899

Comentários/Justificativas: --

Quadro 5 – Análise dos Requisitos de Patenteabilidade (Arts. 8.º, 11, 13 e 15 da LPI)		
Requisito de Patenteabilidade	**Cumprimento**	**Reivindicações**
Aplicação Industrial	Sim	1 a 2
	Não	--
Novidade	Sim	1 a 2
	Não	--
Atividade Inventiva	Sim	--
	Não	1 a 2

Comentários/Justificativas

1. Argumentações da requerente:

    1. Argumentação da Requerente: ”*A Requerente esclarece que as chaves do tipo OTP (one-time pad) não são enviadas aos destinatários, tampouco no modo “plaintext” se for esse o significado que o Examinador tentou denotar com a expressão “de forma plana”. Essa característica é ausente na invenção e sua identificação pelo Examinador é equivocada. A Requerente considera que as afirmativas feitas pelo Examinador envolvendo os conceitos de chave OTP e chave mestra estão incorretas.*”

    6. Análise da argumentação: De fato, a chave OTP não é enviada da maneira como foi descrito no parecer anterior. Esse trecho do argumento foi mal apresentado, entretanto as questões principais do argumento permanecem não respondidas pela requerente. O argumento inicial da requerente é (grifo nosso): "*Dessa forma, **nenhuma informação sobre as OTPs** e os processamentos envolvidos na comunicação ficam concentradas em um ponto de vulnerabilidade a acessos maliciosos, seja pela rede de comunicação entre os membros do grupo e um servidor centralizado, seja fisicamente em um dispositivo centralizado.*"

    7. Entretanto, do descrito, as informações para criar a chave OTP (N posições aleatórias para gerar a chave K) são mandadas em "plaintext" juntamente com as mensagens, conforme já apontado e descrito no relatório descritivo: “*A mensagem cifrada C é enviada aos destinatários juntamente com as N posições das linhas da tabela T, que os possibilitará reconstruir a chave K, já que eles possuem a chave-mestra T*” (Parágrafo 0016). Tal argumento não é rebatido pela requerente.

    8. O argumento anterior diz que "a chave é criada em um equipamento físico único, distribuído de forma manual. Qualquer pessoa com acesso ao equipamento que gera a

chave-mestra é capaz de obter a chave utilizada." Tal argumento não é rebatido pela requerente.

9. Ao juntar essas duas informações é claro que as informações sobre as OTPs são compartilhadas (o contrário de nenhuma informação sobre as OTPs). A OTP não é compartilhada, entretanto todas as informações necessárias para a sua produção são acessíveis ou compartilhadas por algum meio físico, seja o meio físico da rede ou mídias físicas.

2. Argumentação da Requerente: *"Foi evidenciado pela Requerente na resposta ao parecer de exame técnico no despacho 6.22 que a vantagem em custo computacional é um efeito técnico que decorre da seguinte particularidade da invenção" [..] "A Requerente esclarece que o quadro reivindicatório apresentado não reivindica vantagens da invenção, mas sim características técnicas que culminam em tais vantagens."*

3. Análise da argumentação: Conforme exposto pela requerente, tal custo computacional não é reivindicado em nenhuma reivindicação. No caso, a simples vantagem em custo computacional em relação a D1 não é capaz de trazer atividade inventiva ao presente pedido, pois não foram apresentados dados que mostrem tal superioridade em relação ao estado da técnica, sendo uma breve explicação do funcionamento do método.

4. Os argumentos do parecer do parecer anterior não foram totalmente analisados pela requerente. Os argumentos 1 (geração de chaves mestras) e argumentos 3 (OTPs não circulam na rede de comunicação) não foram analisados pela requerente. Os argumentos em relação à falta de atividade inventiva não foram apresentados.

2. Não foram apresentadas argumentações em relação à atividade inventiva frente a D1, somente foram apresentados argumentos em relação ao quadro 3 e em resposta à argumentação da requerente, conforme apresentado na seção acima. As alterações no quadro reivindicatório se restringiram a correção de inconformidades em relação ao Art. 25 apresentadas no parecer anterior. Foi retirado uma parte de um trechos explicativos e foi deslocado o caracterizado por.

1. Dessa forma, mantemos o mesmo entendimento anteriormente apresentado. Sendo assim, a reivindicação independente 1 é óbvia frente a D1. As demais reivindicações (dependentes) estão absorvidas ou são óbvias frente a D1 e aos conhecimentos de um técnico no assunto. Portanto, a matéria pleiteada nas reivindicações 1 e 2 é mera decorrência do estado da técnica, não apresentando atividade inventiva e estando em desacordo com os artigos 8º e 13 da Lei nº 9.279/96 (LPI).

Conclusão

Assim sendo, de acordo com o Art. 37, indefiro o presente pedido, uma vez que:

- não atende ao requisito de atividade inventiva (Art .8º combinado com Art. 13 da LPI)

- as reivindicações estão indefinidas e/ou não estão fundamentadas no relatório descritivo (Art. 25 da LPI)

De acordo com o Art. 212 da LPI, o depositante tem prazo de 60 (sessenta) dias, a partir da data de publicação na RPI, para interposição de recurso.

Publique-se o indeferimento (9.2).

Rio de Janeiro, 12 de junho de 2024.

Daniel de Souza Dias
Pesquisador/ Mat. Nº 2041265
DIRPA / CGPAT III/DITEL
Deleg. Comp. - Port. INPI/DIRPA Nº 007/16