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 0000 de 01/08/2023 segundo a exigência preliminar (6.22). Não foram apresentadas modificações no pedido.

Quadro 1 – Páginas do pedido examinadas

Elemento	Páginas	n.º da Petição	Data
Relatório Descritivo	1 a 8	870170027534	26/04/2017
Quadro Reivindicatório	1	870170027534	26/04/2017
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. O relatório descritivo do presente pedido não descreve suficientemente a invenção de forma a possibilitar sua realização por um técnico no assunto, contrariando o disposto no Art. 24 da LPI. No trecho “O método requer que todos os usuários possuam uma cópia da chave-mestra, que corresponde a uma tabela T de R linhas de S bits gerados de forma realmente aleatória, provenientes de um processo físico inacessível a pessoas que não pertençam ao grupo.”, citado no parágrafo 0012, não é descrito qual processo físico é utilizado para gerar a chave-mestra. Não é identificado qual processo é capaz de gerar uma chave “realmente aleatória”, o que é uma das questões centrais em qualquer problema de cifragem. Não é apresentado tal processo e, não é possível afirmar que tal processo não será único e não copiável, o que vai contra o escrito no trecho “provenientes de um processo físico inacessível a pessoas que não pertençam ao grupo”.

2. A reivindicação 1 não atende ao disposto no Art. 25 da LPI e na Instrução Normativa nº 30/2013 – Art. 4º (III), pois a matéria pleiteada não está definida de maneira clara, precisa e positiva pelas seguintes razões:
    1. O termo “Chave-mestra” não é especificado, principalmente em relação a sua estrutura. Não é explicitado o que é a chave-mestra, podendo esta estar relacionada a quaisquer tipos de chaves presentes na literatura, como por exemplo uma chave mestra pública, chave mestra privada, entre outras.
3. 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 através de um canal seguro e à qual o adversário não tenha acesso”, 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 de como é realizado o uso do gerador.

2. O trecho "que foi compartilhada anteriormente através de um canal seguro e à qual o adversário não tenha acesso" 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.

4. As reivindicações 1 e 2 contrariam o disposto no Art. 25 da LPI e na Instrução Normativa nº 30/2013 – Art. 4º (V), pois faz referência ao relatório descritivo. Os termos " através da equação 2" e " aplicando a equação 3" fazem referência a equações que estão no relatório descritivo.

5. 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.

Quadro 4 – Documentos citados no parecer		
Código	**Documento**	**Data de publicação**
D1	EP1841122	03/10/2007

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 e 2
	Não	--
Novidade	Sim	1 e 2
	Não	--
Atividade Inventiva	Sim	--
	Não	1 e 2

Comentários/Justificativas

1. Análise da Argumentações da requerente:

   1. *A tecnologia BR102015028061-0 elabora uma chave one-time pad (OTP) de forma probabilística por meio de um processo físico inacessível a pessoas que não pertençam ao grupo. Dessa forma, elimina-se a possibilidade de duas chaves iguais serem geradas, tornando segura a comunicação entre um grupo de pessoas.*

      1. Análise: Conforme apresentado no quadro 3 deste parecer, não é descrito de forma suficiente o processo para gerar a chave-mestra e a chave OTP, não sendo possível identificar se tal processo é capaz de gerar chaves únicas. Dessa forma,

somente as afirmações, sem parte técnica, não são capazes de trazer nenhuma atividade inventiva ao pedido.

2. *A tecnologia BR102015028061-0 provê meios de obtenção das OTPs de forma descentralizada, utilizando-se uma chave mestra compartilhada. 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.*

    1. Análise: O presente pedido versa, no parágrafo 0014, sobre a forma descentralizada de obtenção: “A chave-mestra deve ser compartilhada pessoalmente entre os usuários através de um meio confiável como, por exemplo, CD-ROM, pen drive ou HD portável.”. Tal chave deve ser criada de forma centralizada, em um equipamento “físico” único. A OTP é gerada ao “selecionar N posições aleatórias da chave-mestra” (parágrafo 0013) e tal chave OTP é enviada de forma plana aos destinatários “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).

    2. Dessa forma não é possível afirmar que “*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.*” já que as informações de OTP são enviadas de forma plana e 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.

3. *A tecnologia BR102015028061-0 possui um recurso adicional de segurança que pode ser alcançado referenciando-se as OTPS de forma indireta por suas posições na chave mestra juntamente com a mensagem cifrada. Dessa forma as OTPs não circulam na rede de comunicação utilizada.*

    1. Análise: O trecho do presente pedido versa de outra forma: “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”

4. *A tecnologia BR102015028061-0 também possui um custo computacional muito menor se comparada com D1, uma vez que D1 utiliza duas chaves OTP e inúmeras operações lógico-matemáticas adicionais, tais como permutação, duas etapas de aplicação da operação XOR, e muitas outras operações.*

1. Análise: No caso proposto, a simples vantagem em custo computacional em relação a D1 não é capaz de trazer atividade inventiva ao presente pedido. Não foi destacada nenhuma vantagem computacional da proposta do presente pedido.

2. Em exame do quadro reivindicatório e diante da anterioridade selecionada constata-se:
    1. As características presentes da reivindicação independente 1 estão antecipadas por D1 pois:
        1. D1 descreve um método para cifrar uma mensagem M em que a partir de uma primeira sequência aleatória de bits subdividir a referida mensagem M em sub-strings, para cada sub-string é executar uma operação XOR da referida cadeia de mensagem unitária com uma sequencia de bits da primeira sequência aleatória de bits, gerando sub-string cifrada. Em seguida são concatenadas as sub-strings para gerar uma mensagem cifrada. Ver: Resumo, parágrafos 0008, 0012, 0013, 0015, 0017, 0026.
    2. As características presentes da reivindicação dependente 2 estão antecipadas por D1 pois:
        1. O documento D1 descreve o uso de uma porção de tamanho definido (Is), que faz relação direta com o tamanho da string a ser enviada, a partir de um número aleatório grande como chave criptográfica, aplicando a operação XOR para obter o resultado (Ver parágrafo 0008 de D1).
3. 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

Diante ao exposto nesse parecer, o presente pedido não atende às disposições dos Art. 24, Art. 25 e Art. 8º combinado com o Art. 13 da LPI, conforme apontado na seção de comentários/ justificativas dos Quadros 3 e 5 deste parecer.

O depositante deve se manifestar quanto ao contido neste parecer em até 90 (noventa) dias, a partir da data de publicação na RPI, de acordo com o Art. 36 da LPI.

Publique-se a ciência de parecer (7.1).

Rio de Janeiro, 2 de fevereiro de 2024.

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