Criptografia Homomórfica

Gustavo Henrique Muriel Zanon

Instituto de Matemática e Estatística

Supervisor: Prof. Dr. Marcos Antonio Simplicio Junior
Cosupervisor: Prof. Dr. Paulo Sérgio Licciardi Messeder Barreto

Introdução

A computação na nuvem processa grandes volumes de dados, e muitos desses dados precisam ser manipulados sem perda de confidencialidade. Uma proposta de solução para esse problema consiste no uso da criptografia homomórfica.
Sistemas parcialmente homomórficos, como o criptossistema de Paillier [3], são conhecidos há algum tempo. O trabalho de Gentry [1], envolvendo reticulados, mostrou pela primeira vez a viabilidade de cifração totalmente homomórfica. Contudo, o sistema de Gentry e refinamentos derivados são inviáveis para uso prático. Isso, porém, não impede que suas ideias centrais encontrem utilidade prática.
O estado da arte em criptografia homomórfica permite obter sistemas ligeiramente homomórficos em que a complexidade das operações sobre dados cifrados (efetuadas na nuvem) é especificada de antemão, com desempenho razoável, embora grandes desafios persistam nesse sentido.
Este trabalho visa a descrever alguns dos esquemas mais simples de criptografia homomórfica: o criptossistema de Paillier e o criptossistema NTRU homomórfico.

Conceitos

Em um criptossistema homomórfico, operações algébricas possíveis entre dados legíveis podem ser aplicadas igualmente a dados cifrados, produzindo as formas cifradas dos resultados dessas operações. Tais criptossistemas podem ser classificados em:

- **Parcialmente Homomórficos** *(PHE – Partially Homomorphic Encryption)*: Permitem operação de adição ou de multiplicação sob criptogramas.
- **Ligeiramente Homomórficos** *(SHE – Somewhat Homomorphic Encryption)*: Permitem adição e multiplicação de criptogramas, porém com um número limitado de operações permitidas.
- **Totalmente Homomórficos** *(FHE – Fully Homomorphic Encryption)*: Permitem adição e multiplicação de criptogramas, com número de ilimitado de operações.

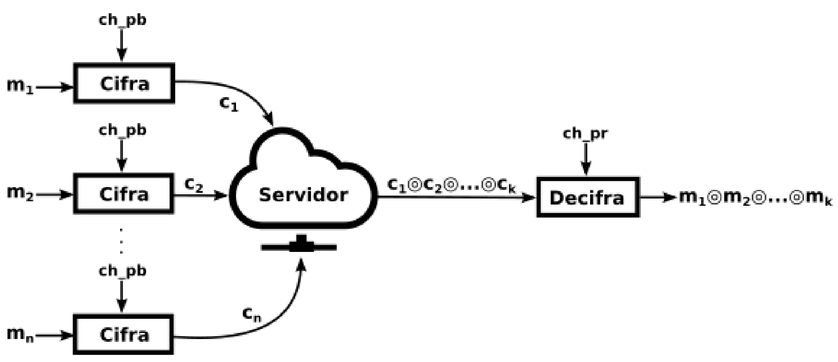

Fig. 1: Exemplo de criprossistema totalmente homomórfico

Paillier

É um esquema de criptografia de chave pública e parcialmente homomórfico. Sua segurança é baseada na intratabilidade do problema dos resíduos quadráticos, não mais difícil que resolver o RSA [3, 4].
A função de encriptação e os componentes do algoritmo são:

$$e_g : \mathbb{Z}_n \times \mathbb{Z}_n^* \to \mathbb{Z}_{n^2}^*$$
$$e_g(x, y) \to g^x \cdot y^n \pmod{n^2}$$

- *Chave pública*: Par (n, g), onde $n = pq$ com p, q primos.
- *Chave privada*: Par $(\lambda(n), \mu)$, onde $\lambda(n) = \text{MMC}(p-1, q-1)$ e $\mu = (\frac{(g^{\lambda(n)} \pmod{n^2})-1}{n})^{-1} \pmod{n}$.
- *Encriptação*: $c = e_g(m, r)$, r aleatório.
- *Decriptação*: $m = (\frac{(c^{\lambda(n)} \pmod{n^2})-1}{n}) \cdot \mu \pmod{n}$.

Homomorfismo Aditivo

Podemos somar duas mensagens m_1, m_2 ao realizar o produto entre seus respectivos criptogramas, cifrados com a chave pública (n, g):

$$\begin{aligned} c_1 \cdot c_2 &\equiv (g^{m_1} r_1^n) \cdot (g^{m_2} r_2^n) \pmod{n^2} \\ &\equiv (g)^{m_1+m_2} (r_2 r_2)^n \pmod{n^2} \end{aligned}$$

O resultado obtido é equivalente a cifrar a mensagem $m_1 + m_2 \in \mathbb{Z}_n$ com um número aleatório $r_1 r_2 \in \mathbb{Z}_n^*$, isso é, $e_g(m_1 + m_2, r_1 r_2)$

NTRU

O NTRU [2] é um criptossistema ligeiramente homomórfico de chave pública. É construído sobre reticulados convolucionais modulares e sua segurança advém da dificuldade de obter vetores curtos, com norma $O(\sqrt{N})$ em vez de $O(q\sqrt{N})$.
O algoritmo considera anéis polinomiais quociente $\mathcal{R}_{N,q} = (\mathbb{Z}/q\mathbb{Z})[x]/\langle x^N - 1\rangle$ e $\mathcal{R}_{N,p} = (\mathbb{Z}[x]/p\mathbb{Z})/\langle x^N - 1\rangle$, onde N e p são primos, e $q \gg p$. Em ambos os anéis a multiplicação é dada pela convolução cíclica $\circledast$.
Os componentes do criptossistema são:

- *Chave privada*: Polinômio $f = p \cdot f' + 1$. O polinômio f' é um polinômio ternário aleatório.
- *Chave pública*: $h = f_q \circledast g$. onde $g = p \cdot g'$, $f_q = f^{-1} \in \mathcal{R}_{N,q}$ e g' é um polinômio ternário aleatório.
- *Encriptação*: $c = h \circledast r + m$, onde r é um polinômio ternário aleatório.
- *Decriptação*: $m' = f \circledast c \in R_{N,q}$ e obtemos $m = m' \in \mathcal{R}_{N,p}$.

Homomorfismo Aditivo e Multiplicativo

Podemos somar duas mensagens m_1, m_2 ao realizar a soma entre seus respectivos criptogramas, cifrados com a chave pública h:

$$\begin{aligned} f \circledast (c_1 + c_2) &= f \circledast (h \circledast r_1 + m_1 + h \circledast r_2 + m_2) \\ &= g \circledast (r_1 + r_2) + f \circledast (m_1 + m_2) \in \mathcal{R}_{N,q} \\ &= m_1 + m_2 \in \mathcal{R}_{N,p} \end{aligned}$$

De forma similar, podemos multiplicar duas mensagens ao realizar a convolução entre seus criptogramas, cifrados com a chave pública h:

$$\begin{aligned} f^2 \circledast (c_1 \circledast c_2) &= f^2 \circledast ((h \circledast r_1 + m_1) \circledast (h \circledast r_2 + m_2)) \\ &= g^2 \circledast (r_1 \circledast r_2) + f \circledast g \circledast (r_1 \circledast m_2 + r_2 \circledast m_1) + f^2 \circledast m_1 \circledast m_2 \in \mathcal{R}_{N,q} \\ &= m_1 \circledast m_2 \in \mathcal{R}_{N,p} \end{aligned}$$

Ambas operações são limitadas pelo parâmetro p do anel $\mathcal{R}_{N,p}$.

Experimentos

A partir da implementação de ambos os algoritmos em linguagem C, foi possível validar a teoria coberta.
Durante a decifração do NTRU, falhas podem ocorrer caso q não não seja suficientemente maior que p. Para somas homomórficas, foi possível observar na prática que $q \in O(p^2)$.

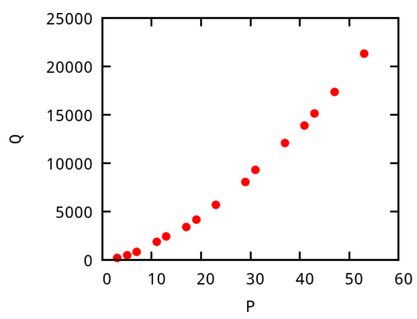

Fig. 2: Valores de q obtidos após 1000 repetições bem sucedidas de $p-1$ somas homomórficas, onde $N = 61$

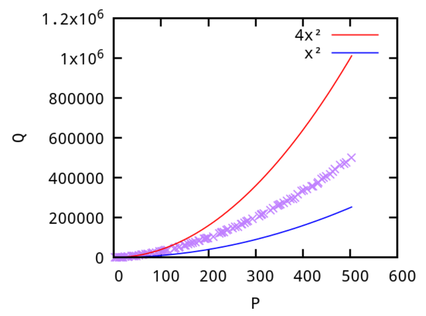

Fig. 3: Valores de q obtidos após 100 repetições bem sucedidas de $p-1$ somas homomórficas, onde $N = 19$. Os resultados obtidos sugerem que $q \in \Theta(p^2)$

Conclusão

Os criptossistemas estudados dificilmente suprirão todas as necessidades da computação na nuvem. Entretanto, isso não impossibilita seu uso em aplicações específicas e de menor porte.
O Paillier nos permitiu realizar o cálculo de médias simples e médias ponderadas com pesos de ponderação públicos. Apesar de ser capaz de realizar grande número de somas de criptogramas na prática, é limitado em aplicações reais que exigem cálculos mais complexos.
O criptossistema NTRU mostrou-se viável para aplicações que exigem número limitado de operações. Vimos empiricamente que, para evitar falhas durante o processo de decifração, o parâmetro q deve crescer à medida que comportamos maior número de operações homomórficas. Contudo, determinar parâmetros seguros constituí área de pesquisa futura.

Referências

[1] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing*, STOC '09, pages 169–178, New York, NY, USA, 2009. ACM.

[2] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *Algorithmic Number Theory: Third International Symposiun, ANTS-III Portland, Oregon, USA, June 21–25, 1998 Proceedings*, chapter NTRU: A ring-based public key cryptosystem, pages 267–288. Springer Berlin Heidelberg, Berlin, Heidelberg, 1998.

[3] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques*, volume 1592 of *Lecture Notes in Computer Science*, pages 223–238. Springer, 1999.

[4] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.