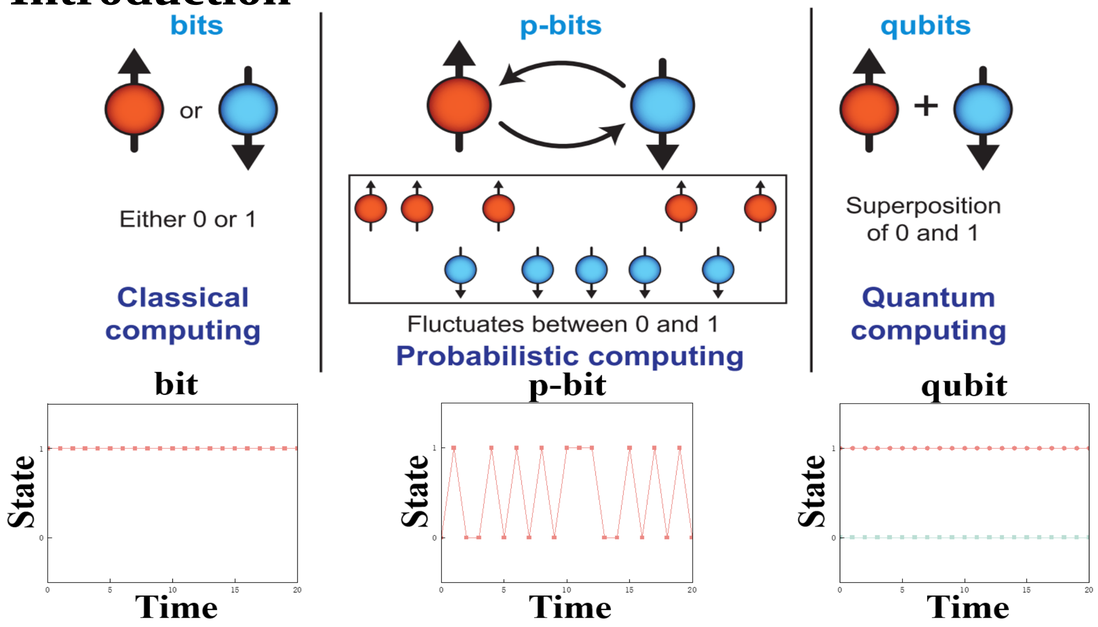
Restricted Boltzmann machine as a probabilistic Enigma

Bin Chen (陈斌)[1,2] and Weichao Yu (余伟超)[1,3]

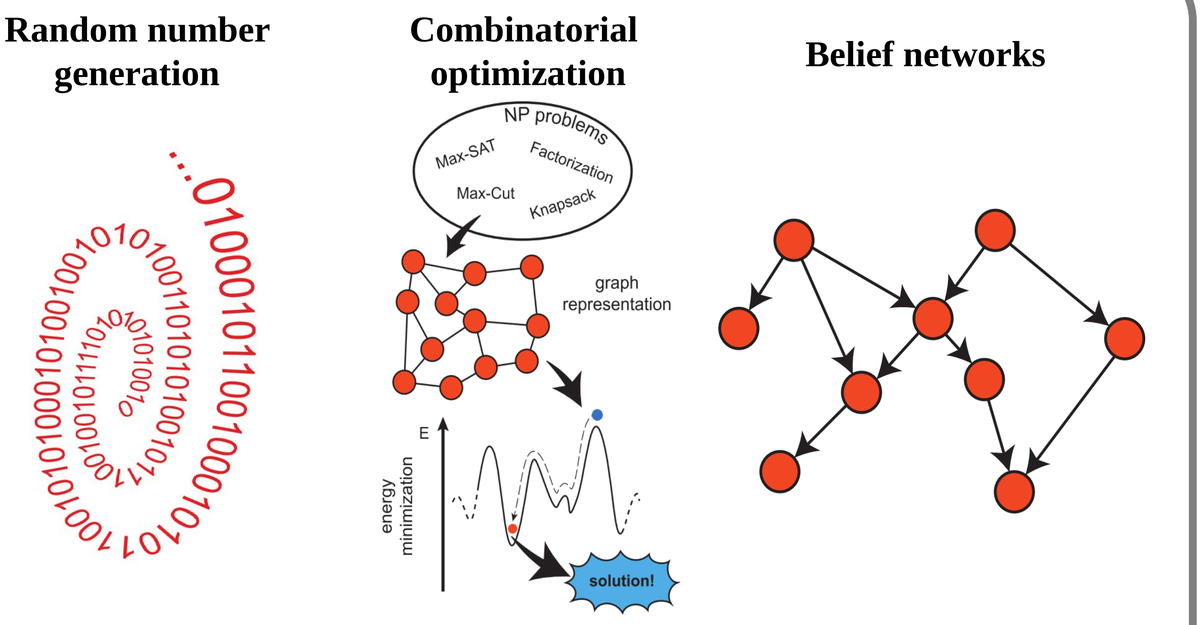
[1]State Key Laboratory of Surface Physics and Institute for Nanoelectronic Devices and Quantum Computing, Fudan University, Shanghai 200433, China
[2]Department of Physics, Fudan University, Shanghai 200433, China
[3]Zhangjiang Fudan International Innovation Center, Fudan University, Shanghai 201210, China

Abstract: We propose an encryption scheme that represents 0 and 1 using high and low probabilities in the marginal distribution of a Restricted Boltzmann Machine(RBM) and trains the weights via gradient descent. Encryption is achieved by shuffling the learned weights. This scheme satisfies the three key characteristics of an effective encryption algorithm: strong diffusion properties, security based on a computationally hard mathematical problem, and hardware acceleration. Magnetic tunnel junctions (MTJs) can be utilized to implement RBM.

Introduction



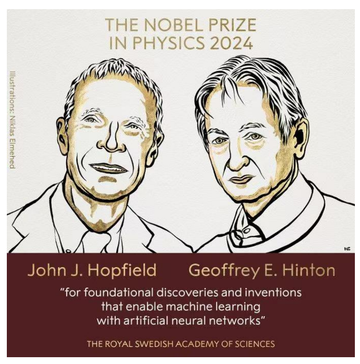
A p-bit refers to a physical entity that rapidly switches between the 0 and 1 states with an adjustable probability.



A probabilistic computer composed of p-bits is capable of solving combinatorial optimization problems such as integer factorization.

Restricted Boltzmann Machine

The RBM has demonstrated capabilities in combinatorial optimization, pattern recognition , and as building blocks for deep belief network.

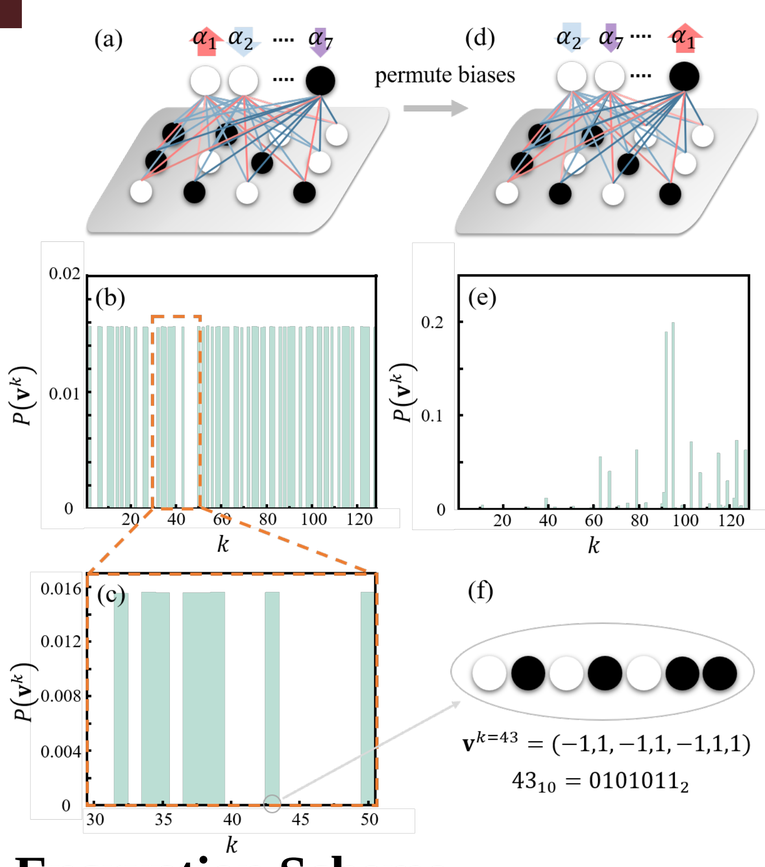


$$E = -(h_i^k W_{ij} v_j^k + \alpha_j v_j^k + \beta_i h_i^k)$$

$$P(\mathbf{v}^k, \mathbf{h}^k) = \frac{1}{Z}\exp(-E(\mathbf{v}^k, \mathbf{h}^k))$$

Encryption Principle

A given set of weights corresponds to a unique marginal distribution. Shuffling the weights alters the marginal distribution.



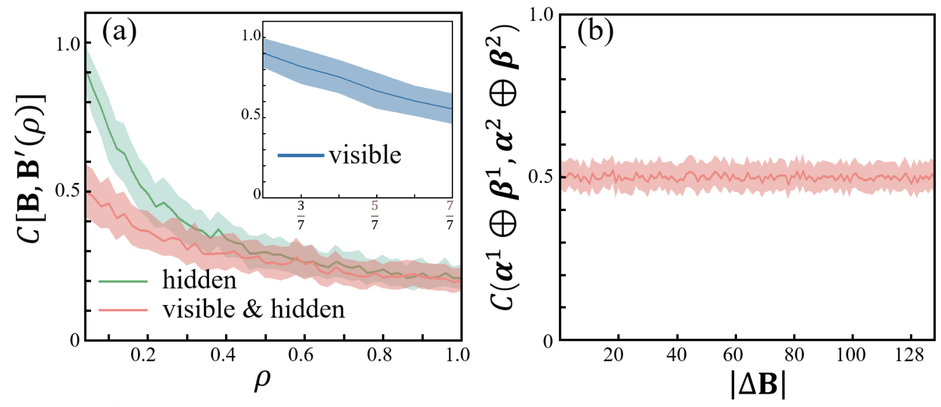
Encryption Scheme

Plaintext ⟶ Marginal Distribution ⟶ {W、α、β}

Receiver ⟶ successfully decrypts

Eavesdropper ⟶ unsuccessfully decrypts

Performance



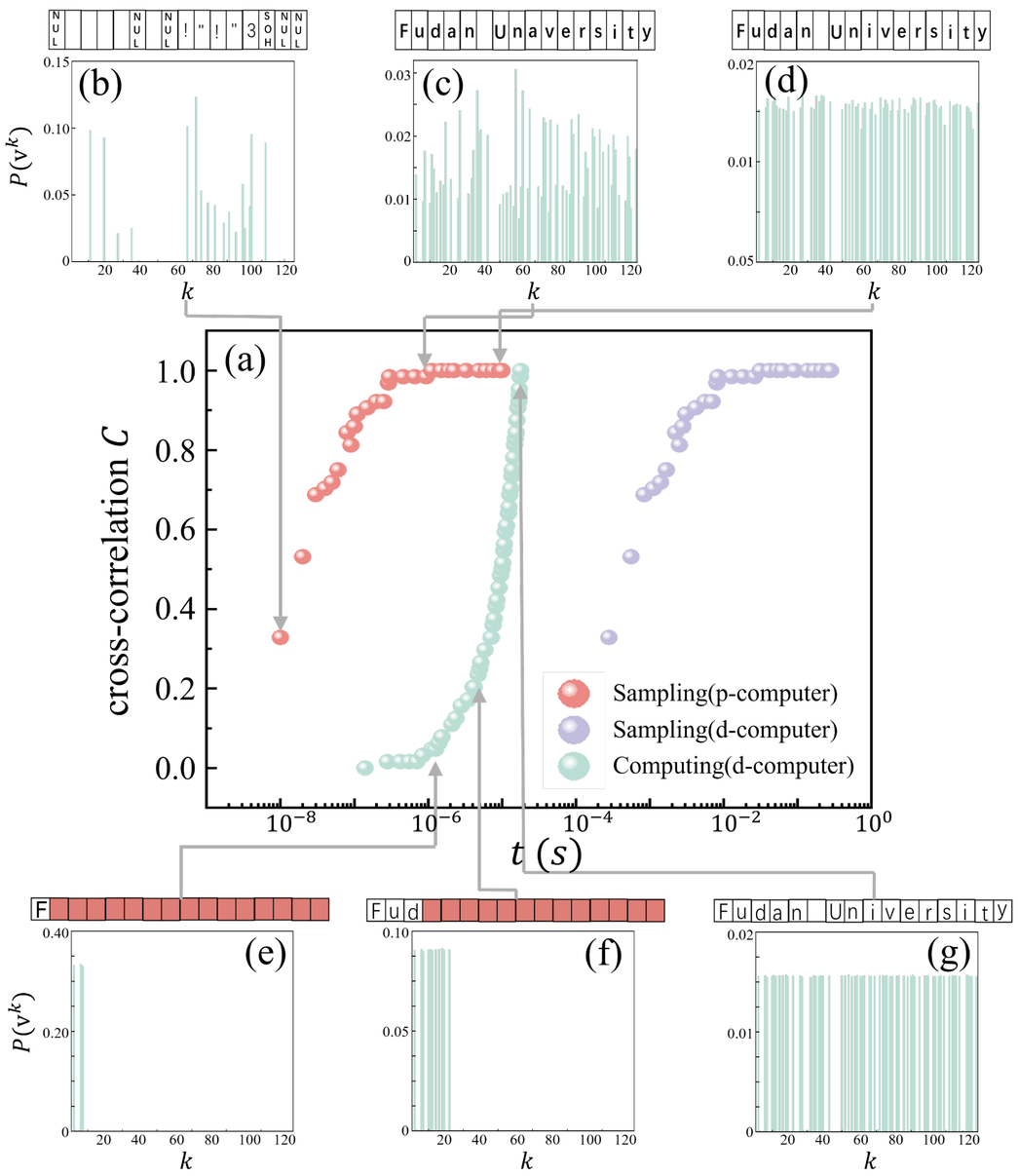
$$C(\rho) = \frac{\sum_{i=1}^{2^n} B_i \times B_i(\rho)}{\sum_{i=1}^{2^n} B_i \times B_i}$$

The similarity between plaintext and pseudo plaintext

The proportion of shuffled biases

$$\rho = \frac{m_{permute}}{m}$$

When ρ reaches 20%, the C of our proposal is lower than that of AES



Hardware-implemented Boltzmann machines accelerate decryption by two to three orders of magnitude compared to general-purpose computers.

Reference

[1] Bin Chen, Weichao Yu. Restricted Boltzmann machine as a probabilistic Enigma(Accepted by Physical Review Applied)
[2] Yadi Wang*, Bin Chen* , et al. *National Science Review* Volume 12, Issue 3, March 2025, nwae338.
[3] Borders W A, Pervaiz A Z, Fukami S, et al. Nature, 2019, 573(7774): 390-393.
[4] D. H. Ackley, G. E. Hinton, and T. J. Sejnowski, Cognitive science 9, 147 (1985).
[5] Chowdhury S, et al. IEEE Journal on Exploratory Solid-State Computational Devices and Circuits, 2023, 9(1): 1-11.

25110190005@m.fudan.edu.cn