OVERVIEW OF THE DISCRETE LOGARITHM PROBLEM IN CRYPTOGRAPHY

Authors: Abhiroop Sarkar, Deepsubhra Guha Roy, Piyali Datta
Institute of Engineering & Management, Kolkata

Presentation by Abhiroop Sarkar | Paper ID-140

3rd International Conference on Advanced Computing and Applications ICACA | 2024

OUTLINE OF THE PRESENTATION

- Why do we need Public Key Cryptography?
- How can we achieve it?
- A Timeline
- What is the Discrete Log problem?
- Algorithms for solving Discrete log
- Cryptosystems based on discrete log
- Conclusion

INTRODUCTION

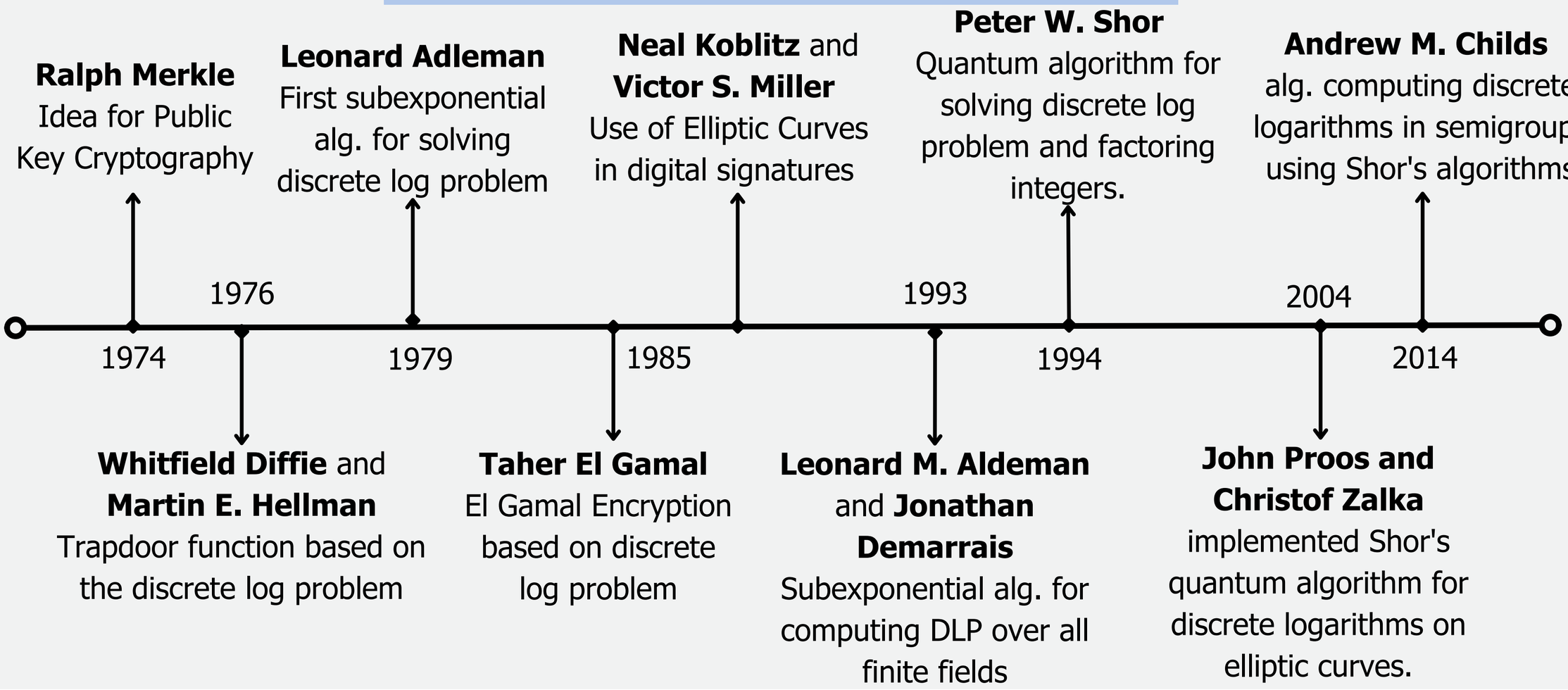
1. What is Public Key Cryptography?
    - **Two** distinct **keys** for encryption and decryption
2. Motivation for Public Key Cryptography:
    - Key Distribution Challenge
    - Scalability Issue
    - Digital Signatures
3. Trapdoor Functions:
    - Functions that are **hard** to invert (without the secret key)

INTRODUCTION

Transition to Cryptosystems:

- Two main one-way functions: **Integer factorization** (RSA) and **Discrete logarithm** (Diffie-Hellman, Elliptic Curves).
- Computational complexity of these problems ensures **High security**.
- Public-key cryptography can be **time-consuming**; a hybrid approach combining both symmetric and asymmetric cryptography is used for efficiency.

HISTORY


1974
Ralph Merkle
Idea for Public Key Cryptography
1976
Whitfield Diffie and Martin E. Hellman
Trapdoor function based on the discrete log problem
1979
Leonard Adleman
First subexponential alg. for solving discrete log problem
1985
Taher El Gamal
El Gamal Encryption based on discrete log problem
1993
Neal Koblitz and Victor S. Miller
Use of Elliptic Curves in digital signatures
1994
Leonard M. Aldeman and Jonathan Demarrais
Subexponential alg. for computing DLP over all finite fields
2004
Peter W. Shor
Quantum algorithm for solving discrete log problem and factoring integers.
2014
John Proos and Christof Zalka
implemented Shor's quantum algorithm for discrete logarithms on elliptic curves.
Andrew M. Childs
alg. computing discrete logarithms in semigroups using Shor's algorithms

MATHEMATICAL CONCEPTS

- Modular Arithmetic: Essential for cryptographic algorithms, involving operations within a finite set of elements.
  - **Fast Exponentiation**: Square and Multiply Algorithm
  - **Euclidean Algorithm**: For Modular Inverse
- Groups in Cryptography:
  - Groups, denoted as (G, $\circ$), are crucial in cryptography for dealing with **finite sets**.
  - Cyclic Groups: All elements can be generated by a primitive element or generator.

Ref: C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer (2010)

THE DISCRETE LOGARITHM PROBLEM

In a finite cyclic group Z*p, the problem of finding x such that 1 <= x <= p-1

$$a^x \equiv b \pmod{p}$$

where a,b belongs to Z*p

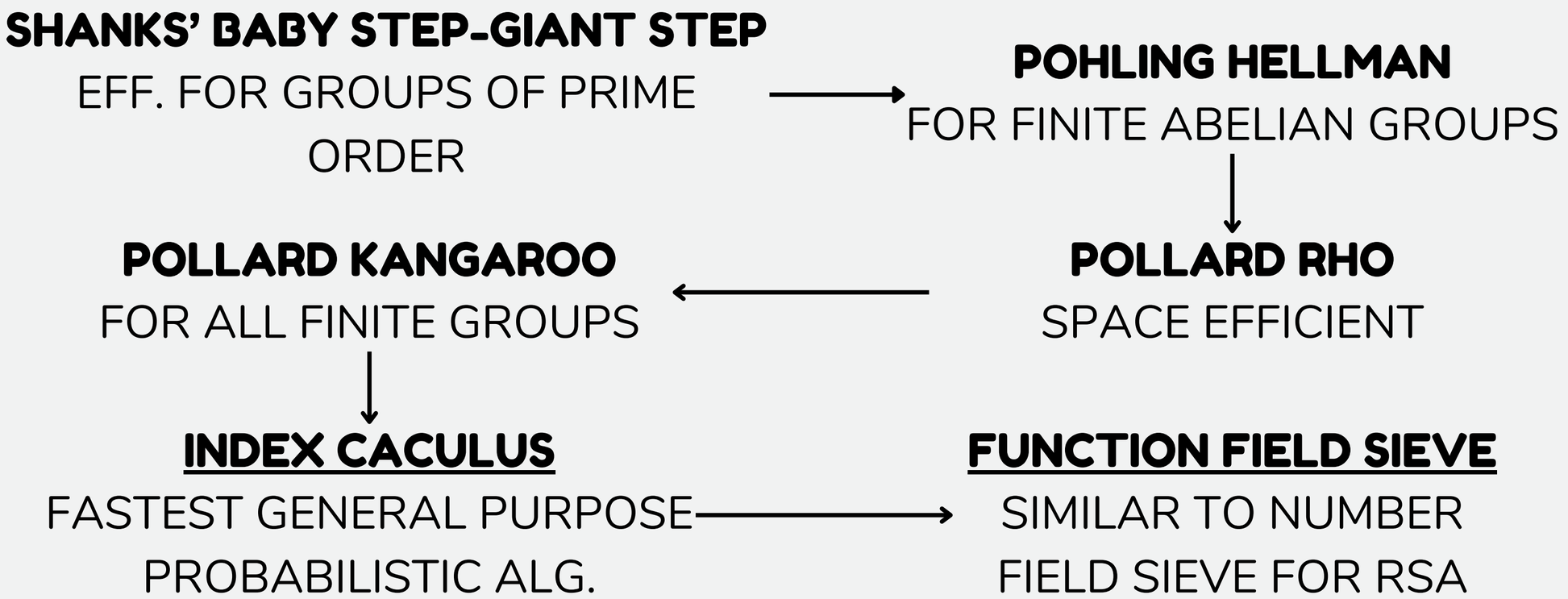
Generalized DLP:

Given a cyclic group G with group operation (.) and cardinality n, and primitive elements a and b, where a, b ∈ G, it is the problem of finding integer x that $1 \leq x \leq n$ such that:

b =a.a.a...x times = a.x

Ref: C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer (2010)

SECURITY OF DISCRETE LOG



Ref:
D. Shanks, Class Number, a Theory of Factorization and Genera. Proceedings of Symposium of Pure Mathematics, Vol. 20, pp. 415-440, (1969)
Stephen, C., Pohlig., Martin, E., Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance (Corresp.). IEEE Trans actions on Information Theory, 24 (1978)
Pollard, By J. M.. Monte Carlo Methods for Index Computation (mod p).Mathematics of Computation, Vol. 32, No. 143, pp. 918-924 (2010)
Kevin S. McCurley, The Discrete Logarithm Problem. Proceedings of Symposia in Applied Mathematics, Vol 22 (1990)
Adleman, L.M. The function field sieve. In: Adleman, L.M., Huang, MD. (eds) Algorithmic Number Theory. ANTS 1994. Lecture Notes in Computer Science, vol 877. Springer, Berlin, Heidelberg (1994)

SHOR'S ALGORITHM

WORKING

- Utilizes entangled quantum registers to compute a^x mod p.
- Applies Quantum Fourier Transform to extract period r.
- Employs classical post-processing to compute discrete logarithm from extracted information.

DEVELOPMENTS

- Increased Efficiency for **Short Discrete Logarithm Problem**
- Implemented on Discrete Log on Elliptic Curves and Semi-Groups.
- Attacking **Hyper Elliptic Curve** is easier than Elliptic Curve Cryptography

Ref:
Peter W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing. 26, 5, 1484 1509 (1997)
Ekerå, M. Quantum algorithms for computing general discrete logarithms and orders with tradeoffs. Journal of Mathematical Cryptology, 15(1), 359-407 (2021)
Huang, Y., Su, Z., Zhang, F., Ding, Y., & Cheng, R. Quantum algorithm for solving hyperelliptic curve discrete logarithm problem. Quantum Information Processing, 19, 1-17 (2020)

CRYPTOSYSTEMS

DIFFIE HELLMAN KEY EXCHANGE

- Secure key exchange over public channels.
- Vulnerable to Meet-in-the-middle attacks
- 3-Participant variant using ECC

EL GAMAL ENCRYPTION

- Combines half-DHKE with symmetric encryption
- Security Flaws (not very practical)
- Identity concealing in group communications

ELLIPTIC CURVE CRYPTOGRAPHY

- Faster than DHKE/RSA
- Smaller Key Size-Less Memory utilization
- Resistance against subexponential time algorithms

Ref:

Joux, A. (2000). A One Round Protocol for Tripartite Diffie–Hellman. In: Bosma, W. (eds) Algorithmic Number Theory.

Khader, A.S., & Lai, D. Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol. 2015 22nd International Conference on Telecommunications (ICT), 204-208 (2015)

David Adrian et. al. 2018. Imperfect forward secrecy: how Diffie Hellman fails in practice. Commun. ACM 62, 1, 106–114 (2019)

M. Mikhail, et. al, Extension and application of El Gamal encryption scheme. World Congress on Computer Applications and Infor mation Systems (WCCAIS), Hammamet, Tunisia, 2014, pp. 1-6 (2004)

Vivek, Kapoor., Vivek, Sonny, Abraham., Ramesh, Singh. Elliptic curve cryptog raphy. ACM Ubiquity, 9, 7 (2008)

Bos, J.W., Halderman et. al, E. Elliptic Curve Cryptography in Practice. Lecture Notes in Computer Science(), vol 8437. Springer, Berlin, Heidelberg (2014)

COMPARISON ECC VS RSA/DHKE

Attack Time (in 10^t years)	ECC	RSA/DHKE
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Ref:
NIST, Special Publication 800-57: Recommendation for Key Management. Part 1: General Guideline, Draft Jan (2003)

CONCLUSION

- Explored the historical significance of the Discrete Logarithm Problem (DLP) in cryptography.
- Discussed solving algorithms including sub-exponential and quantum algorithms.
- Covered key cryptographic schemes such as Diffie-Hellman, El-Gamal, and elliptic curves, highlighting their benefits.

THANK YOU

Presentation by Abhiroop Sarkar

3rd International Conference on Advanced Computing and Applications ICACA | 2024