业务专家技术分享

重磅来袭……

课 堂 守 则

1.手机关机或者静音，交给工作人员保管

2.分享过程不要来回走动，有特殊情况请举手示意主持人

3.认真听讲，参与过程互动提问

有多少投入就有多少收获!!!

轻松一下，破冰游戏来一个

真假难辩

游戏规则：

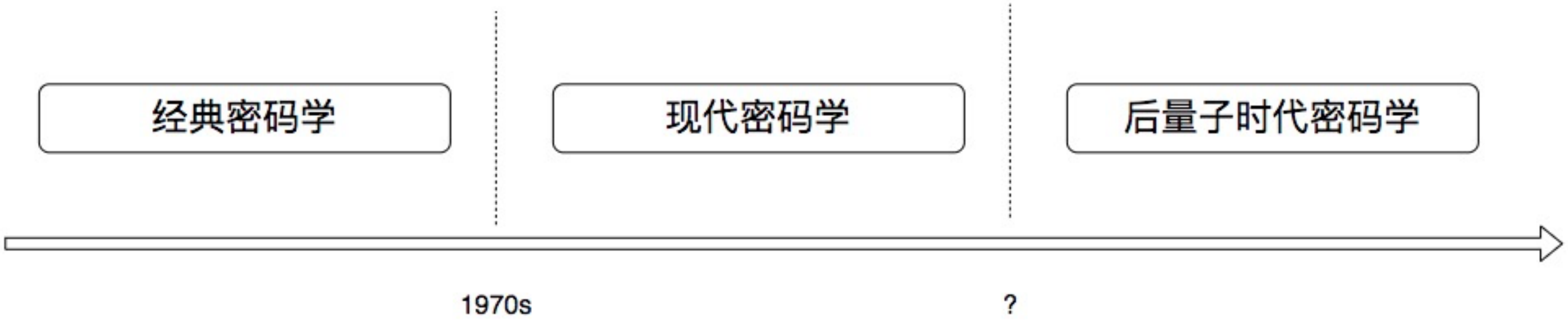
1、将参与者进行分组，每组4人;

2、为每组发放4个一次性杯子，在这4个杯子里有3杯装的是矿泉水，而有一杯装的是白酒;

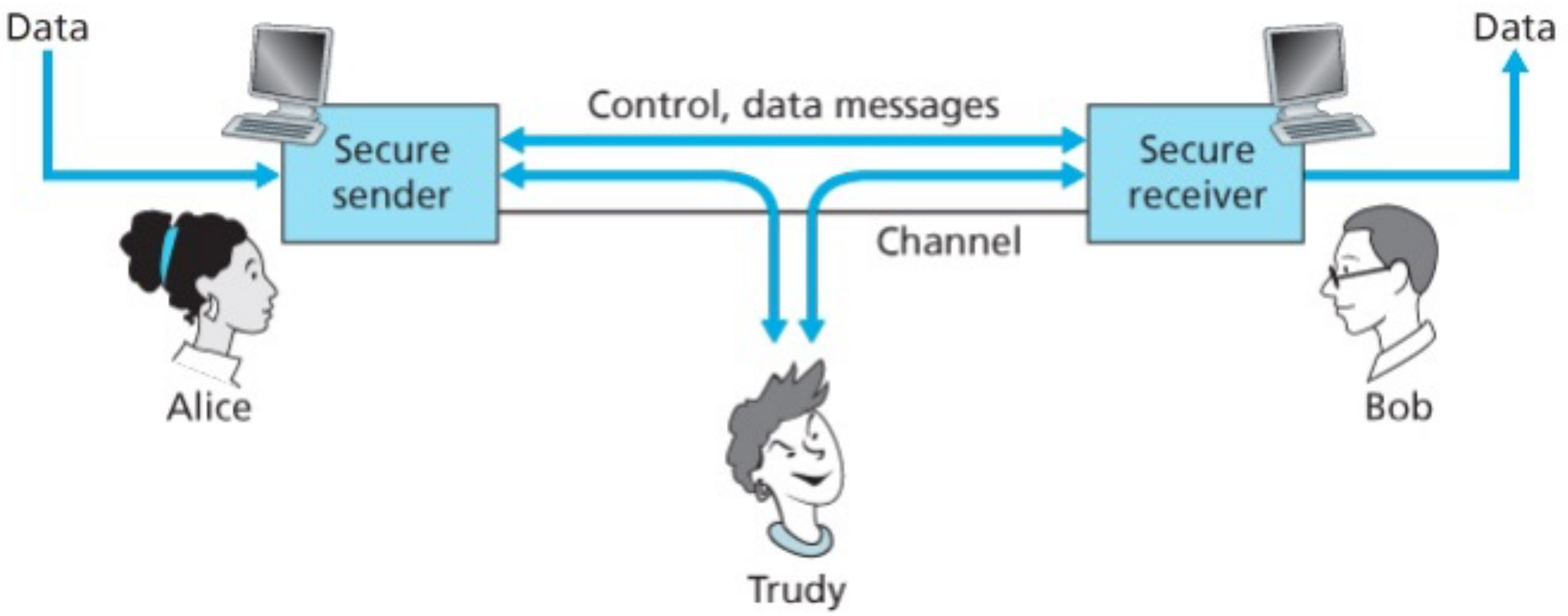
3、两两之间进行比拼，一个队先喝，另外一队猜谁喝的白酒，被猜中的队伍淘汰出局，未被猜中的队伍剪刀石头布PK，赢得队伍有奖励。

初探零知识证明

1. 公钥密码学发展简述
2. 零知识证明解决的问题以及目前的进展

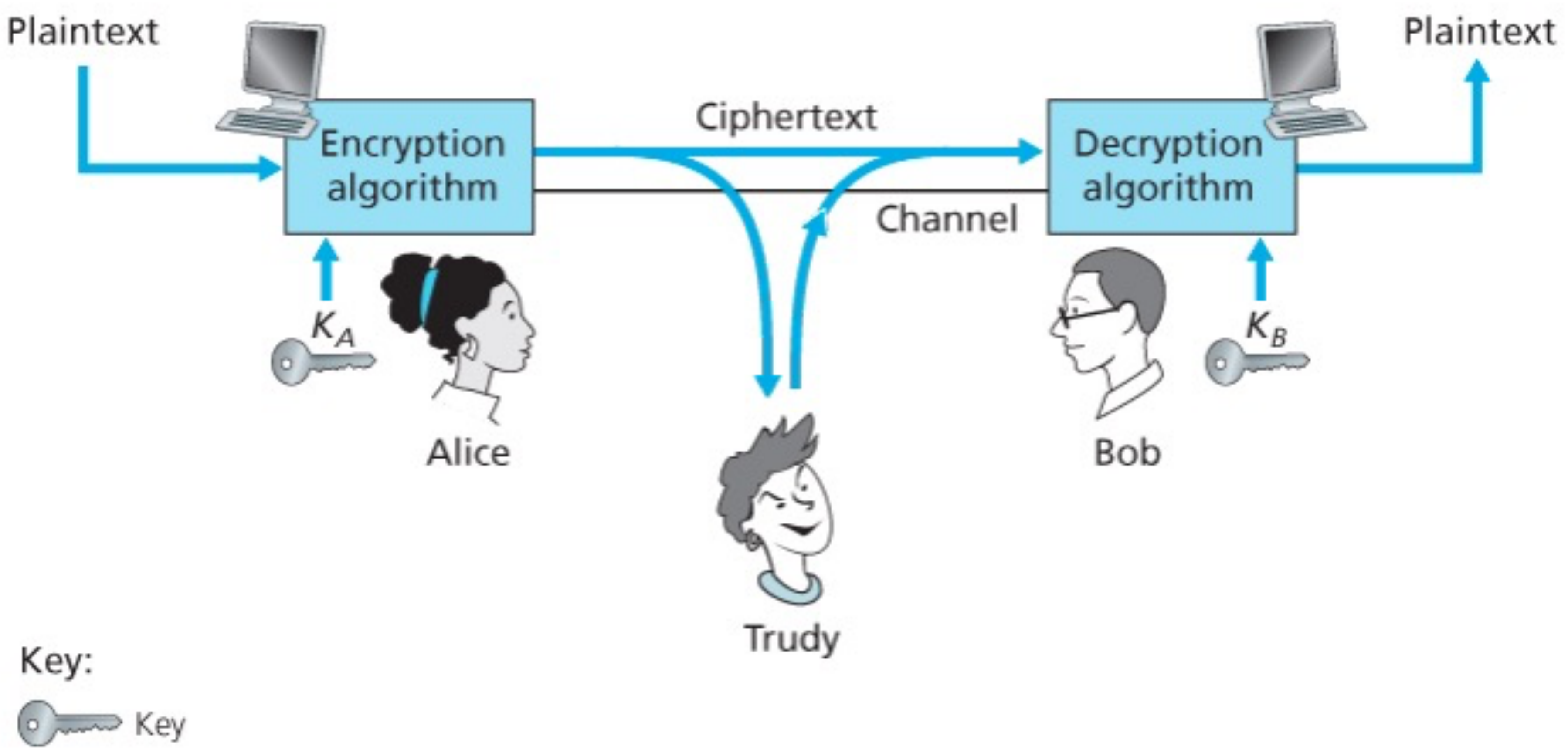

经典密码学
现代密码学
后量子时代密码学
1970s
?

场景设置

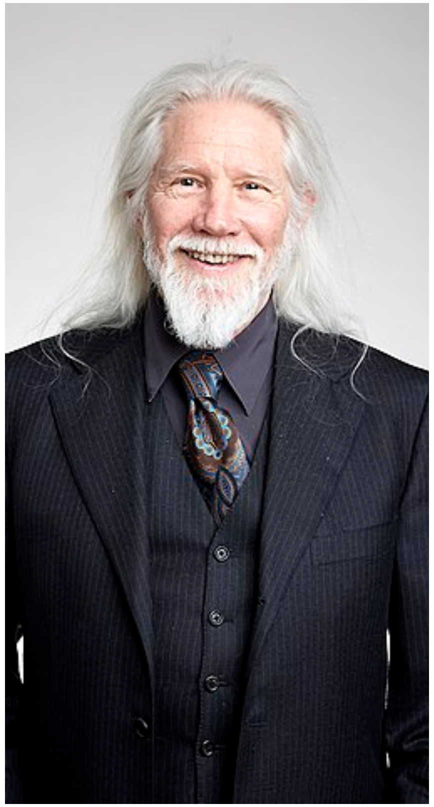

Data
Control, data messages
Data
Secure sender
Secure receiver
Channel
Alice
Bob
Trudy

- 恩尼格玛密码机

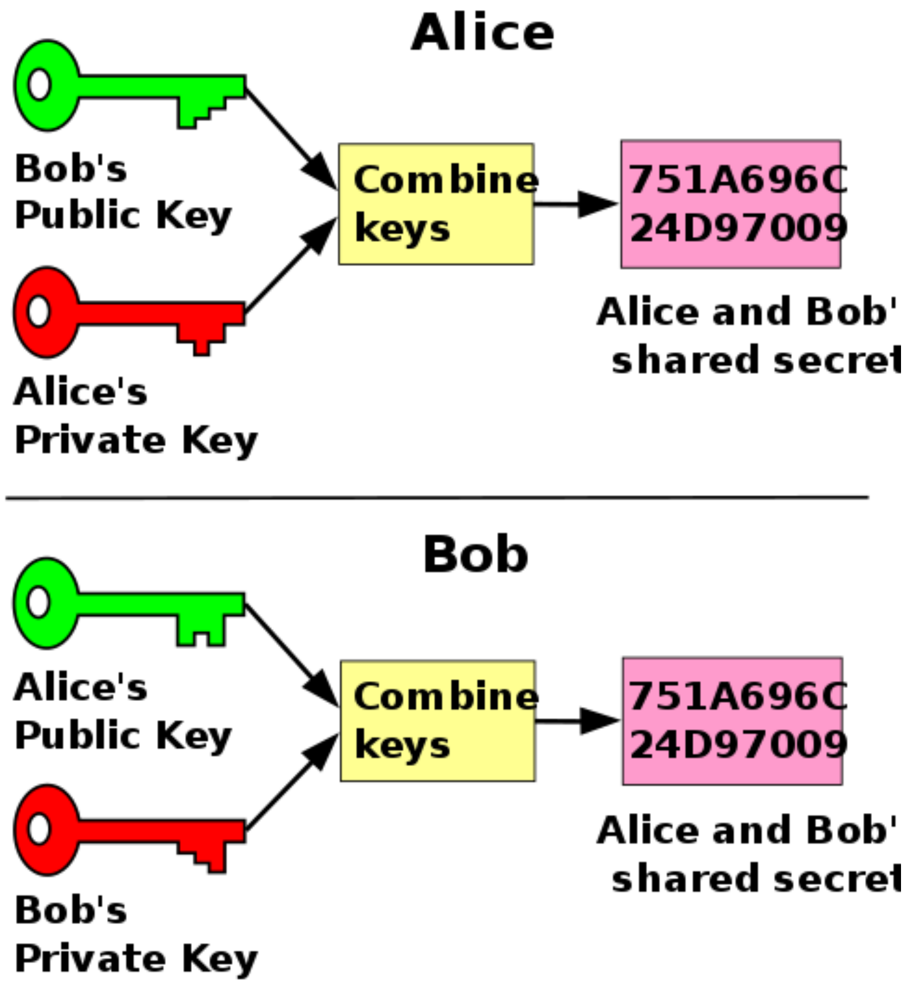

Plaintext
Encryption algorithm
K_A
Alice
hannel
Decryption algorithm
K_B
Bob
Plaintext

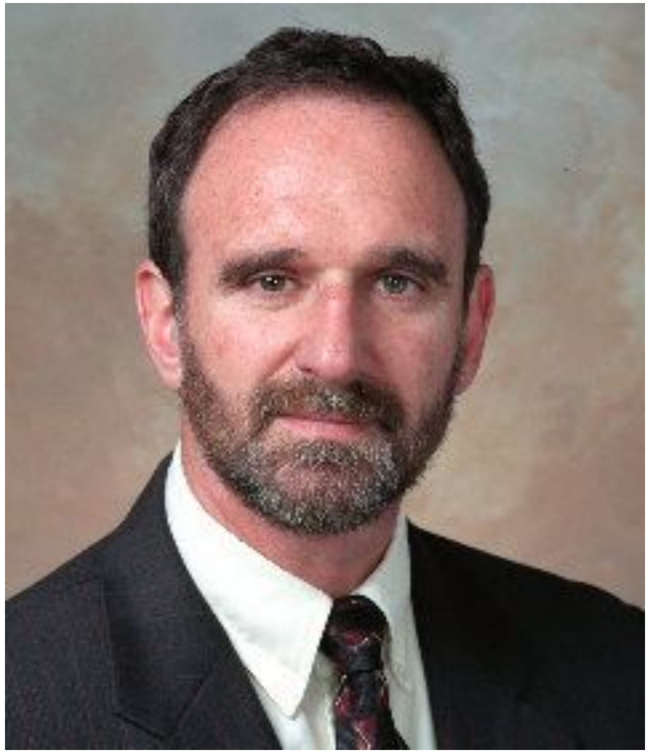

Plaintext
Encryption algorithm
Ciphertext
Channel
Decryption algorithm
Plaintext
K_A
K_B
Alice
Trudy
Bob
Key:
Key

DH key exchange 协议



Whitfield Diffie





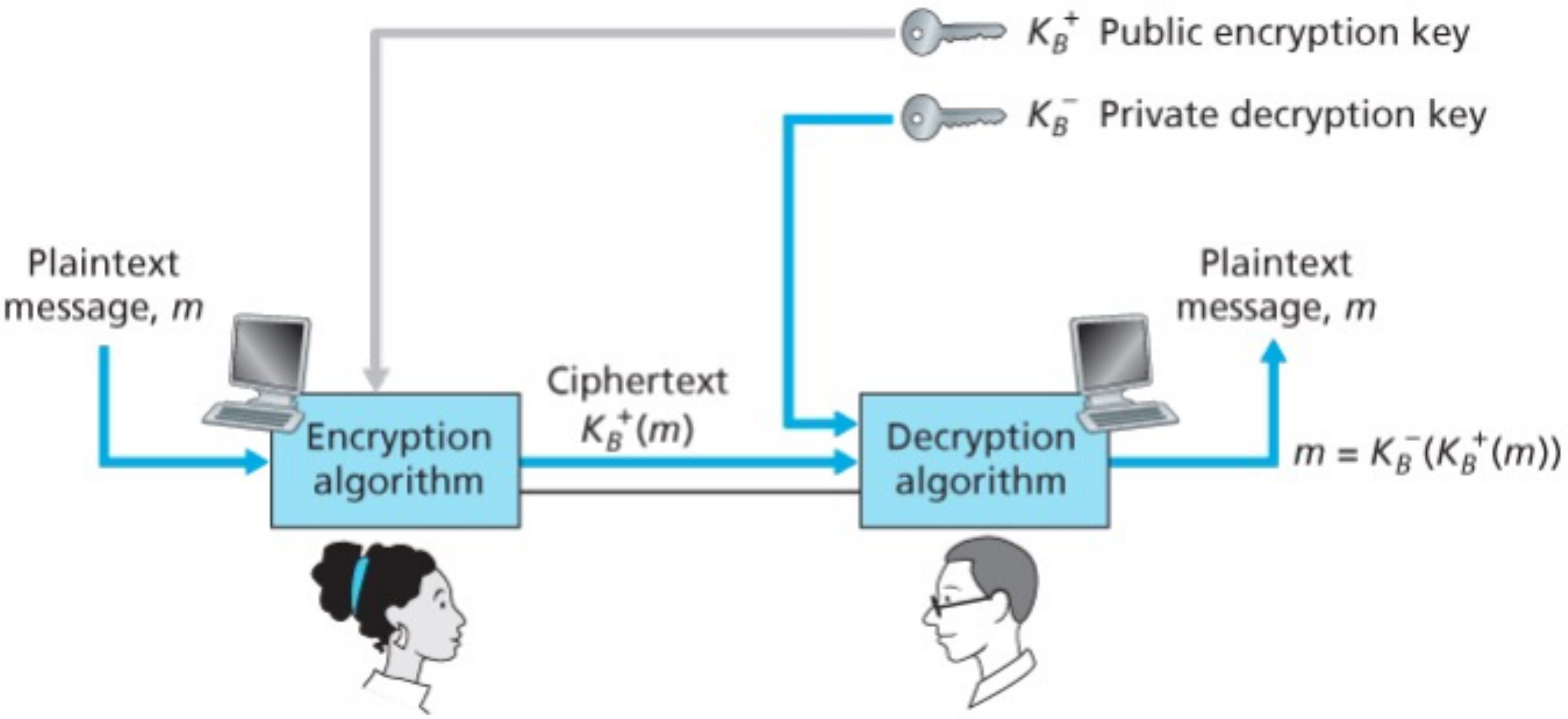
Martin Hellman

RSA

Adi Shamir

Leonard Adleman

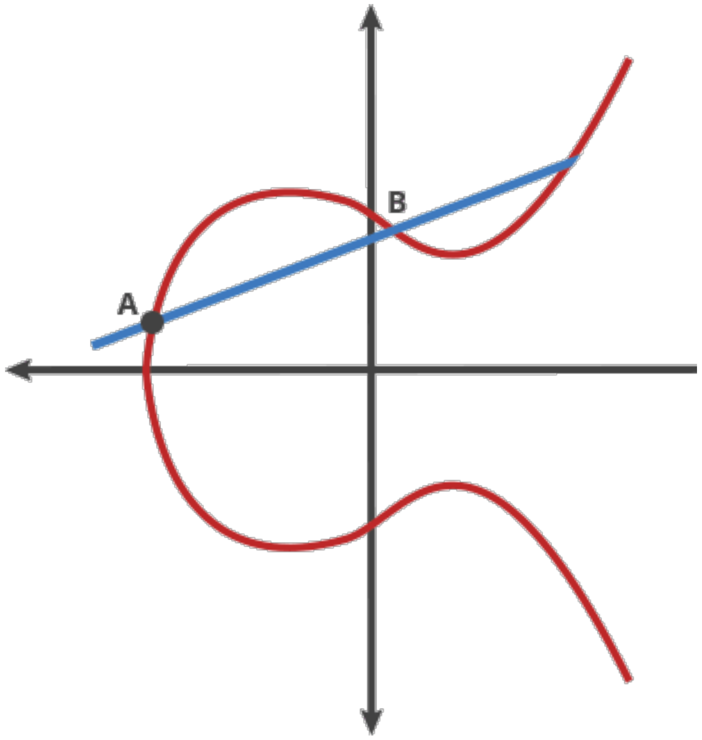
Ron Rivest



K_B^+ Public encryption key
K_B^- Private decryption key
Plaintext message, m
Encryption algorithm
Ciphertext $K_B^+(m)$
Decryption algorithm
Plaintext message, m
$m = K_B^-(K_B^+(m))$

一条椭圆曲线就是一组被 y^2 = x^3 + ax + b 定义的且满足 4a^3 + 27b^2 ≠ 0 的点集

- **ECC 椭圆曲线**



椭圆曲线离散对数问题(**E**lliptic **C**urve **D**iscrete **L**ogarithm **P**roblem, **ECDLP**)

椭圆曲线上的两个点P和Q，k为整数。

$$Q = kP.$$

椭圆曲线加密的数学原理：

点P称为基点（base point）；k为私有密钥（private key）；Q为公开密钥（public key)

- 则给定k和P，根据加法法则，计算Q很容易。
- 但给定P和Q，求k非常困难（实际应用ECC，质数p取得非常大，穷举出k非常困难）。

2. 求解$E_p(a,b)$

设$E_p(a,b)$表示**椭圆曲线上的点集**：

$$\{(x,y)|0 \le x \le p,\ 0 \le y \le p,\ 且x,y均为整数\} \sqcup 0$$

求$E_p(a,b)$点集步骤：

(1)、对每一个x($0 \le x < p$ 且x为整数)，计算$x^3+ax+b \pmod p$.

(2)、决定(1)中求得的值在模p下是否有平方根，计算$y^2 \pmod p$.
- 如果没有，则曲线上没有与这一相对应的点；
- 如果有，则求出两个平方根。

$y=0$时只有一个平方根.

例1：$E_{11}(1,6)$表示椭圆曲线$y^2 = x^3+x+6$. 则点集$E_{11}(1,6)$如下表：

(2, 4)	**(2, 7)**	(3, 5)	(3, 6)	(5, 2)	(5, 9)
(7, 2)	(7, 9)	(8, 3)	(8, 8)	(10, 2)	(10, 9)

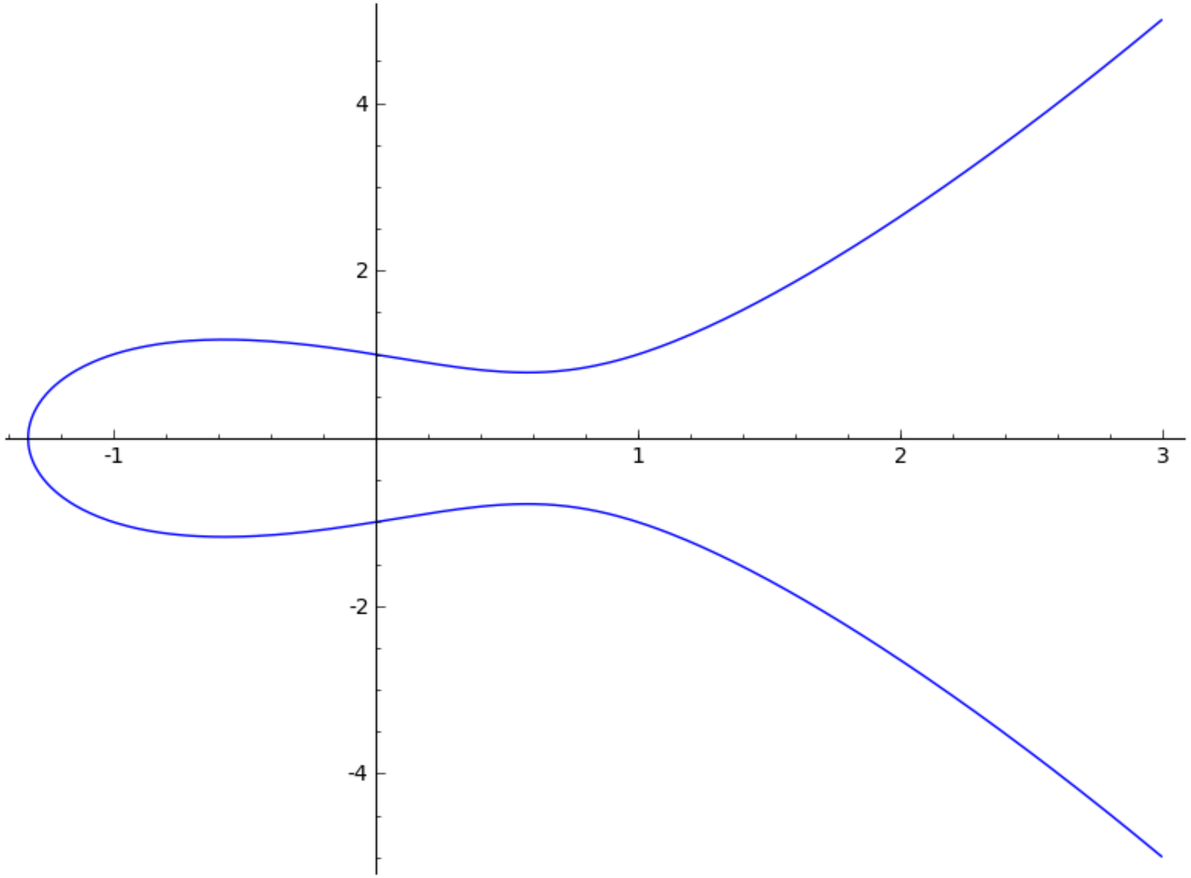
$2^3+2+6 \pmod{11} = 5$
$4^2 \pmod{11}$=5
$7^2 \pmod{11}$=5

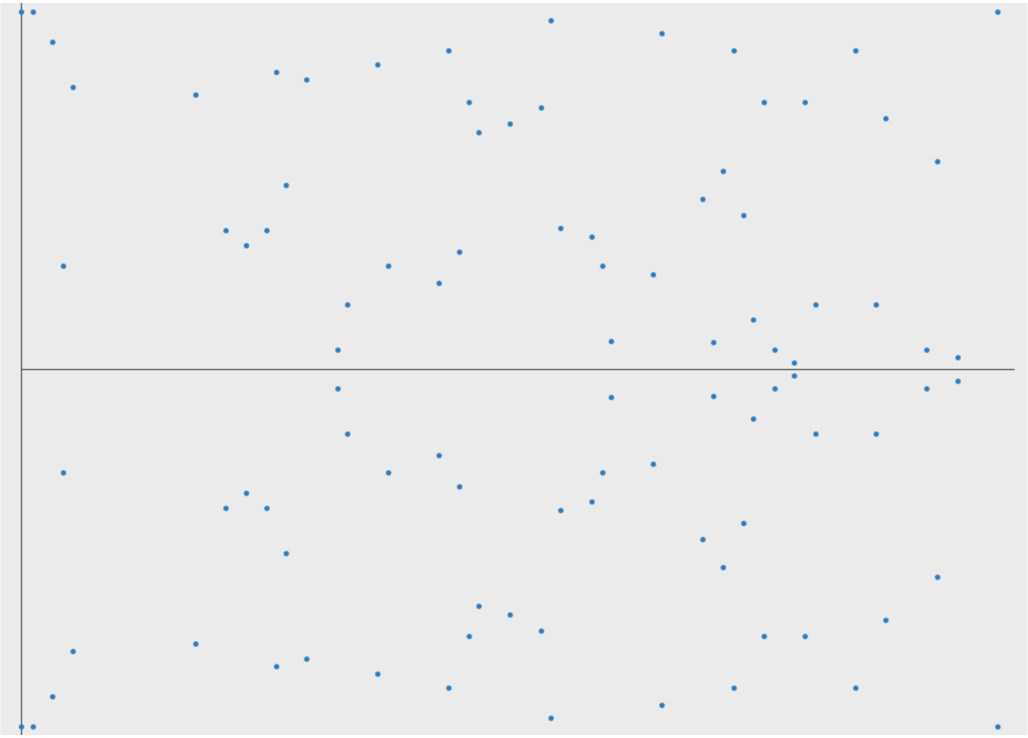
$y^2 = x^3 - x + 1$

$$x^3 + ax + b \quad (mod) \quad p$$

a = -1

b = 1



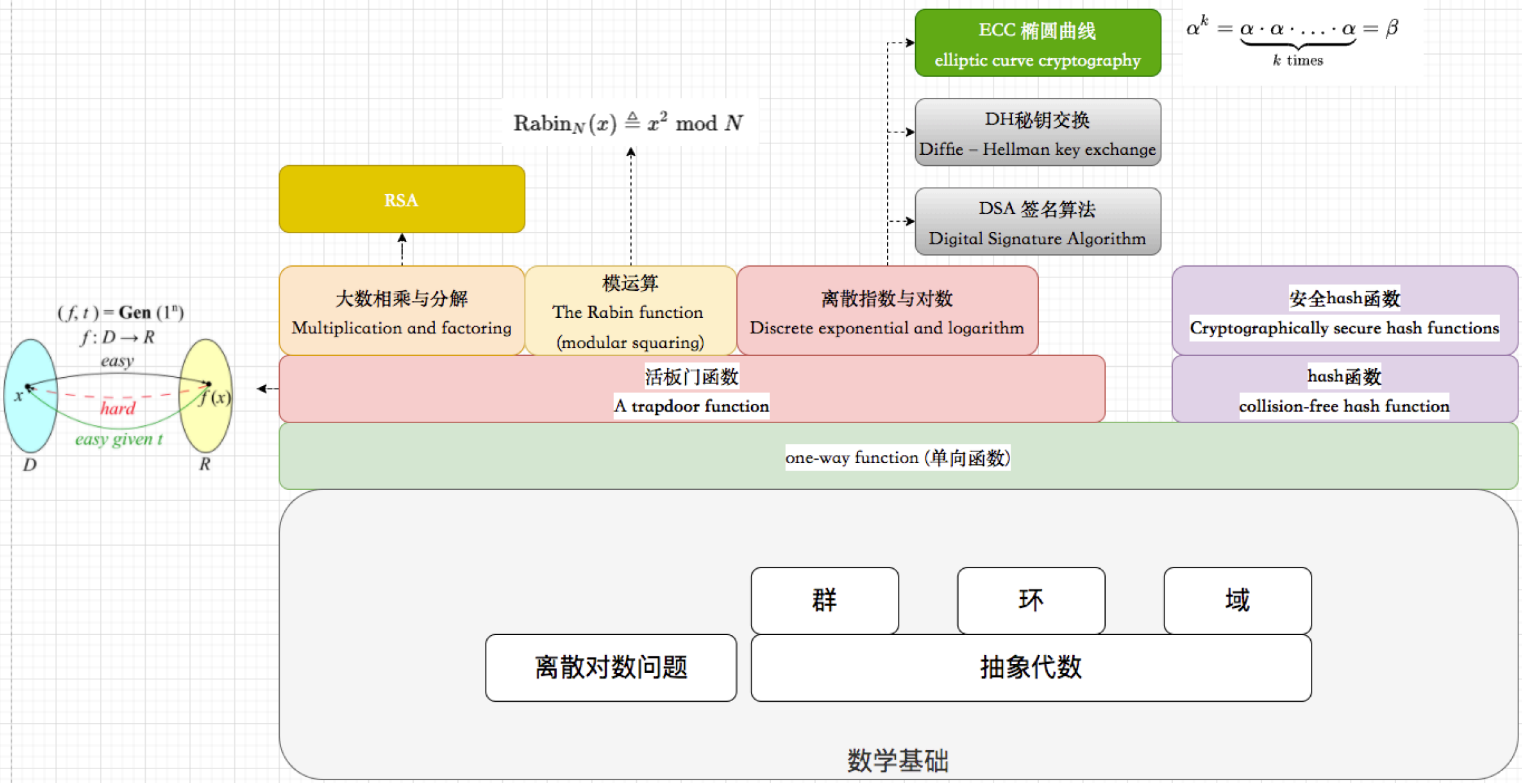


P=97

破解 228位 不同算法需要烧开多少量的水相当[6]

RSA

ECC



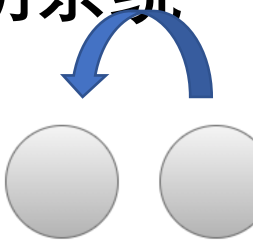
ECC 椭圆曲线
elliptic curve cryptography
$\alpha^k = \underbrace{\alpha \cdot \alpha \cdot \ldots \cdot \alpha}_{k \text{ times}} = \beta$
DH秘钥交换
Diffie – Hellman key exchange
$\mathrm{Rabin}_N(x) \triangleq x^2 \bmod N$
DSA 签名算法
Digital Signature Algorithm
RSA
大数相乘与分解
Multiplication and factoring
模运算
The Rabin function
(modular squaring)
离散指数与对数
Discrete exponential and logarithm
安全hash函数
Cryptographically secure hash functions
$(f, t) = \mathbf{Gen}(1^n)$
$f: D \to R$
easy
hard
easy given t
x
$f(x)$
D
R
活板门函数
A trapdoor function
hash函数
collision-free hash function
one-way function (单向函数)
群
环
域
离散对数问题
抽象代数
数学基础

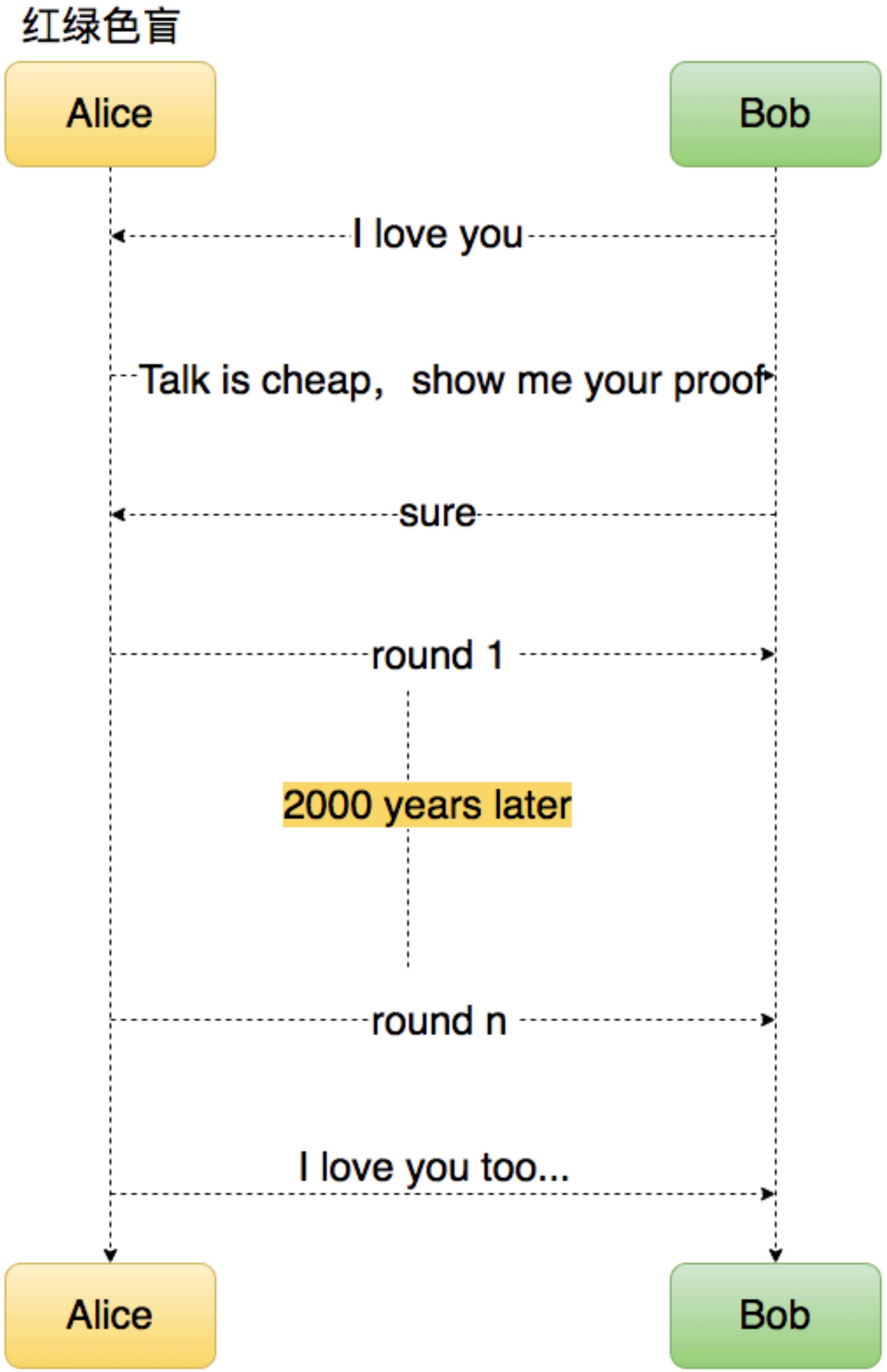
零知识证明是一种 能够让示证方 给验证方证明 自己的一个承诺 但不透漏额外的任何信息

零知识证明系统

- 一个小游戏

零知识证明系统





红绿色盲
Alice
Bob
I love you
Talk is cheap，show me your proof
sure
round 1
2000 years later
round n
I love you too...
Alice
Bob

零知识证明系统定义

Silvio Micali

Shafi Goldwasser

Charles Rackoff

The_Knowledge_Complexity_Of_Interactive_Proof_Systems[8]

1. 授权系统（Authentication systems）

2. 区块链（Blockchains）

3. 数据隐私保护（data private）

……

性质：
完备性（Completeness）
可靠性（Soundness）
零知识性（Zero-knowledgeness）

如何实现零知识证明的

Zero-knowledge succinct non-interactive arguments of knowledge (*zk-SNARK*)

模运算　　指数运算

$$\text{encryption}: \; 5^3 = 6 \pmod 7$$
$$\text{multiplication}: \; 6^2 = (5^3)^2 = 5^6 = 1 \pmod 7$$
$$\text{addition}: \; 5^3 \cdot 5^2 = 5^5 = 3 \pmod 7$$

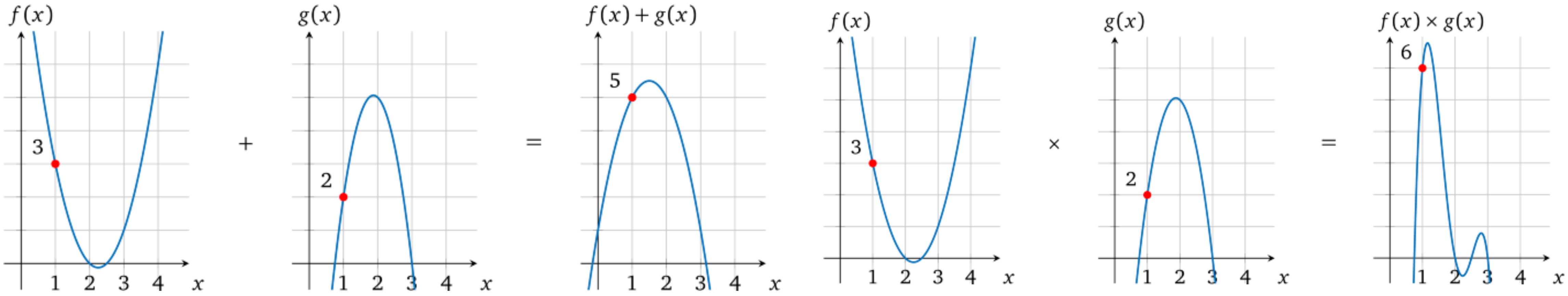
Algorithm 1: Operation depends on an input

```
function calc(w, a, b)
    if w then
        return a × b
    else
        return a + b
    end if
end function
```

$$f(w, a, b) = w(a \times b) + (1 - w)(a + b)$$

多项式

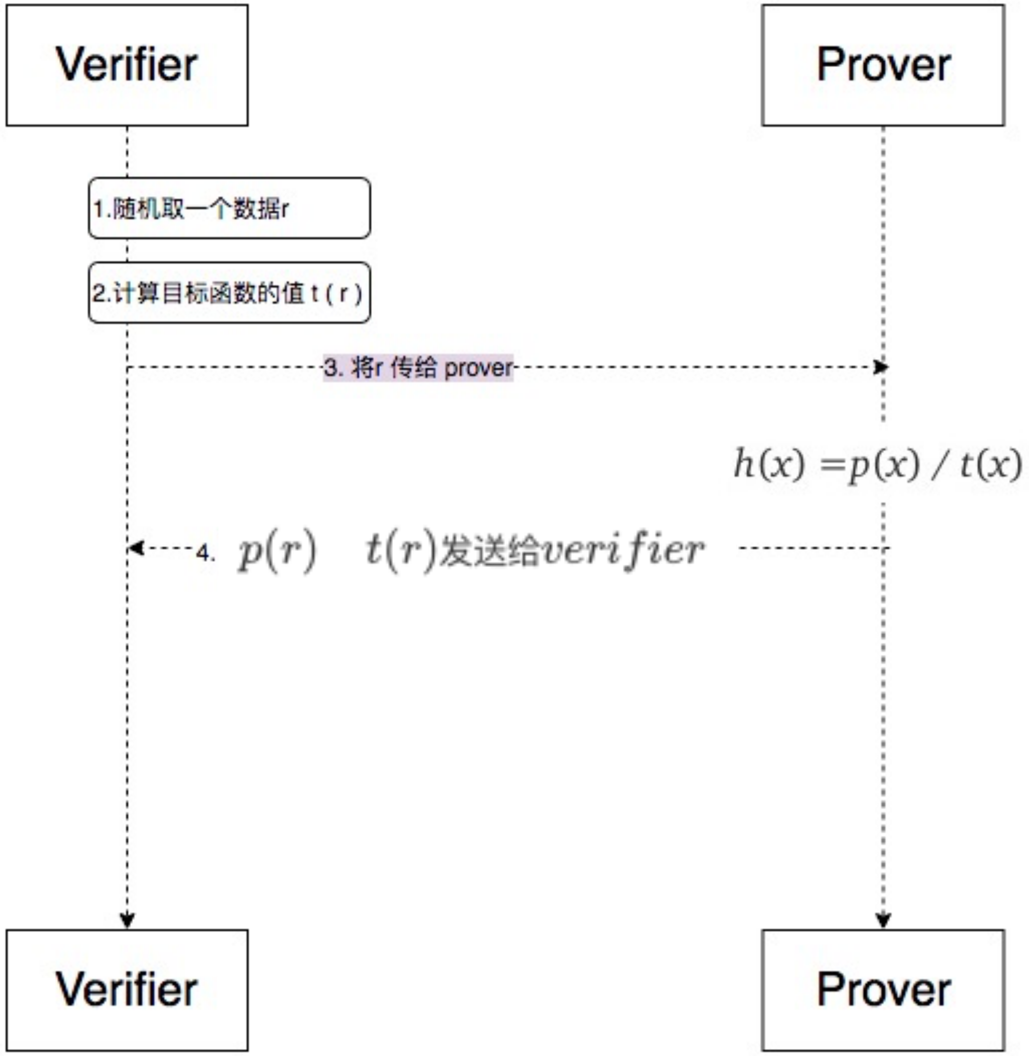
一个多项式有解，一定可以分解成 $(x-a_0)(x-a_1)...(x-a_n)=0$

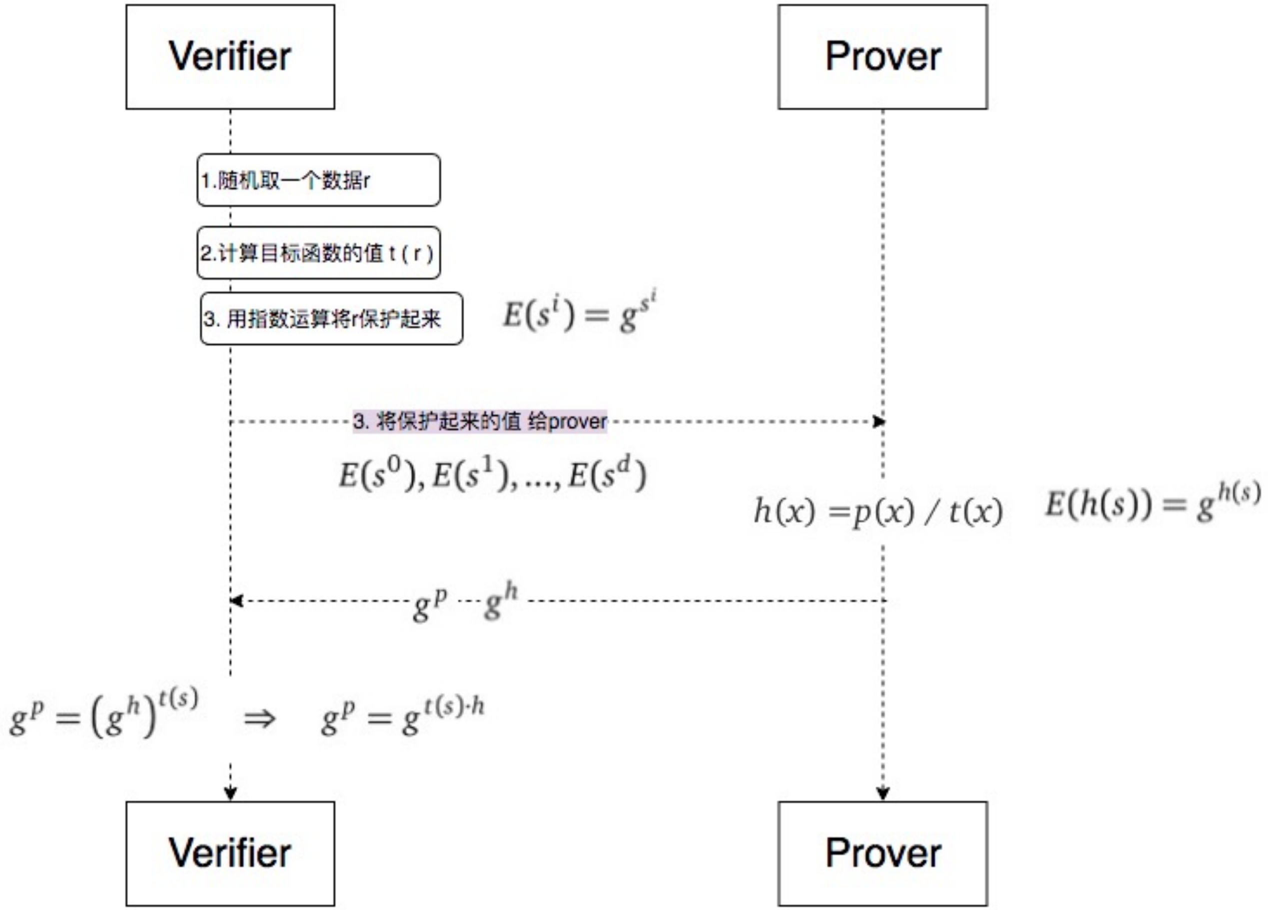


- 问题描述 prover 想向verifier 证明 他知道一个多项式有解s1 和 s2
- 但是不想直接告诉verifier 多项式是什么样子的，那么他需要将多项式转换一下

$$t = (x - s1)(x - s2)$$

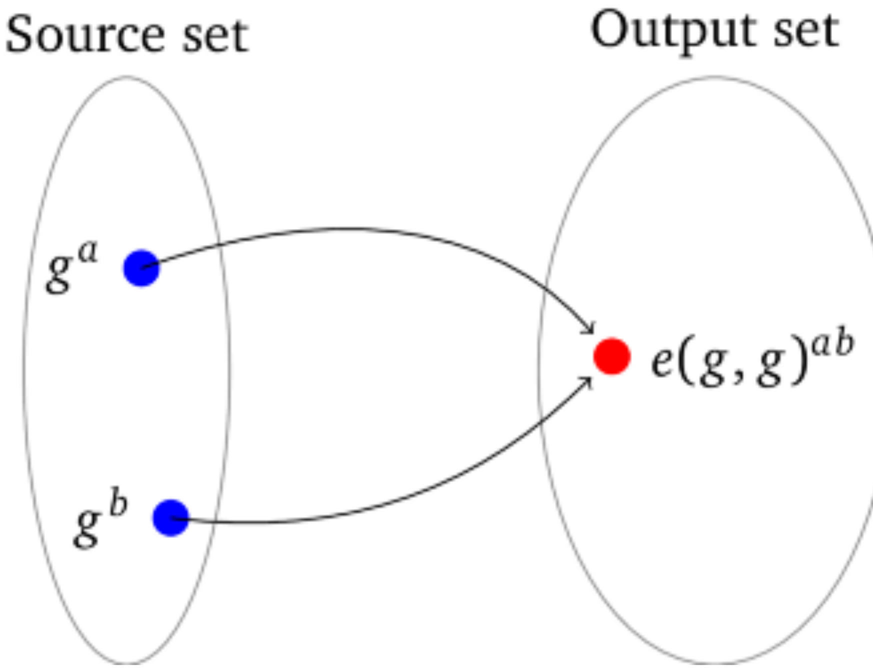
$$p(x) = h(x)t(x)$$

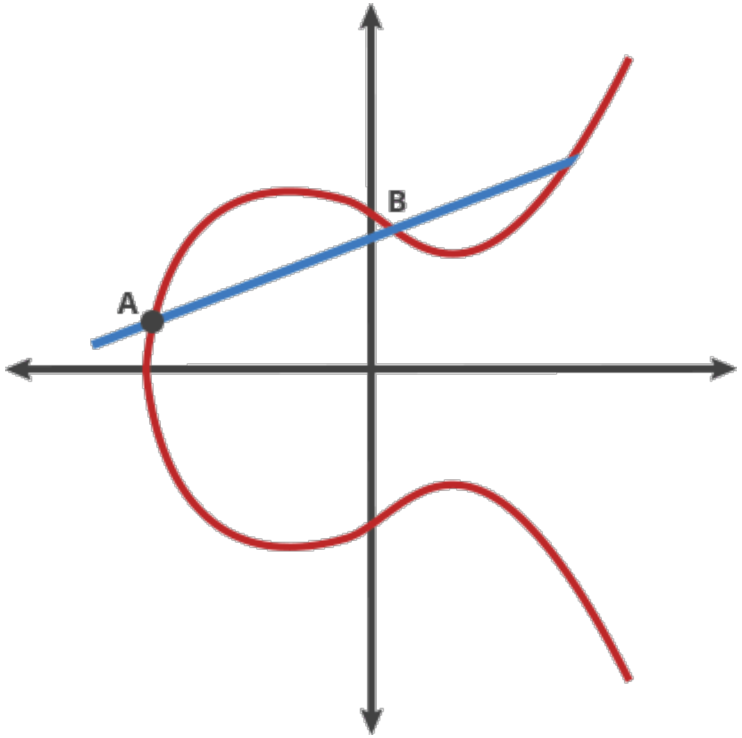




Verifier
Prover
1.随机取一个数据r
2.计算目标函数的值 t (r)
3. 用指数运算将r保护起来
$E(s^i) = g^{s^i}$
3. 将保护起来的值 给prover
$E(s^0), E(s^1), ..., E(s^d)$
$h(x) = p(x) / t(x)$
$E(h(s)) = g^{h(s)}$
g^p
g^h
$g^p = (g^h)^{t(s)} \Rightarrow g^p = g^{t(s) \cdot h}$
Verifier
Prover

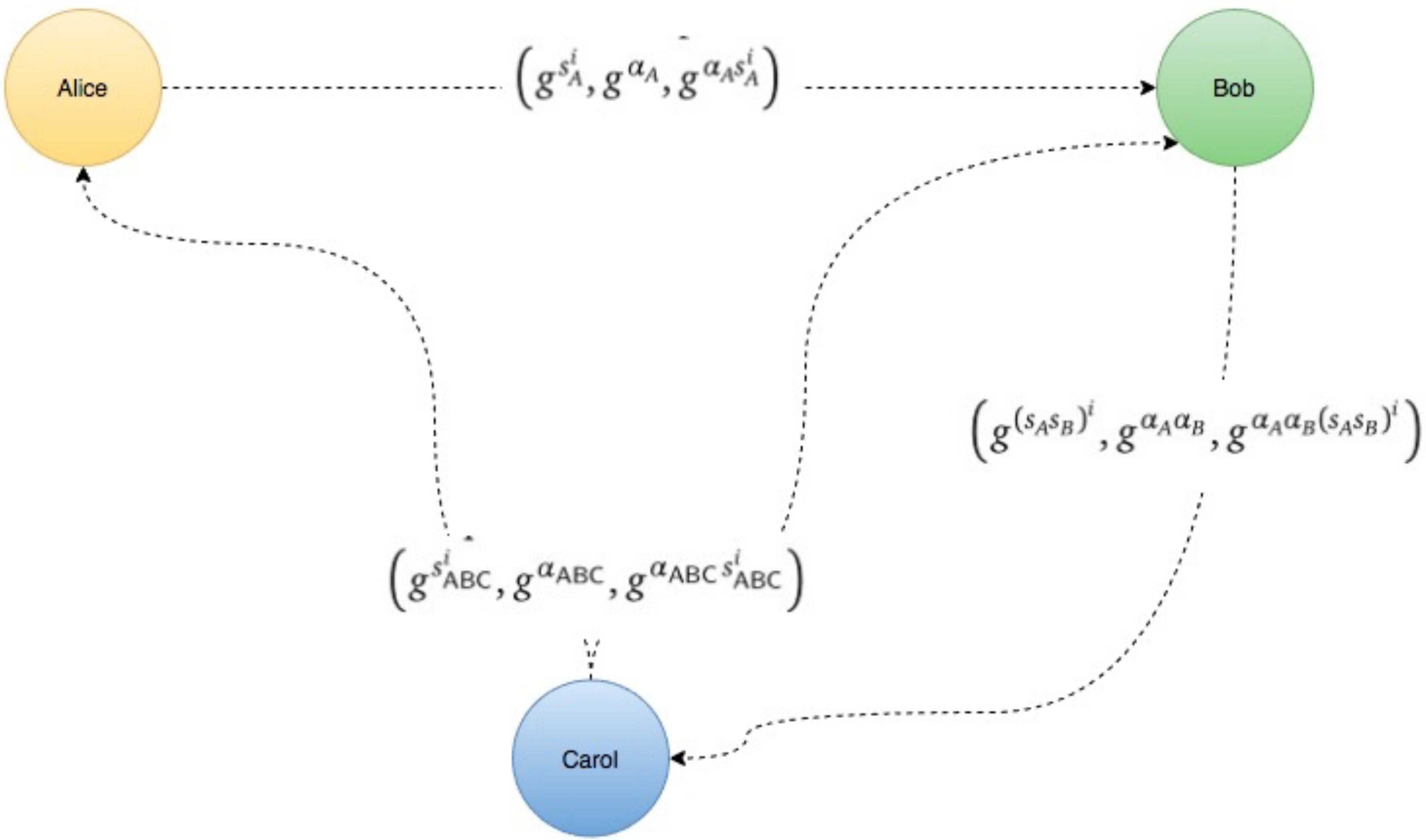
双线性映射





$$e(g^a, g^b) = e(g^b, g^a) = e(g^{ab}, g^1) = e(g^1, g^{ab}) = e(g^1, g^a)^b = e(g^1, g^1)^{ab} = \ldots$$

$p = t \cdot h$ → $e(g,g)^p = e(g,g)^{t \cdot h}$

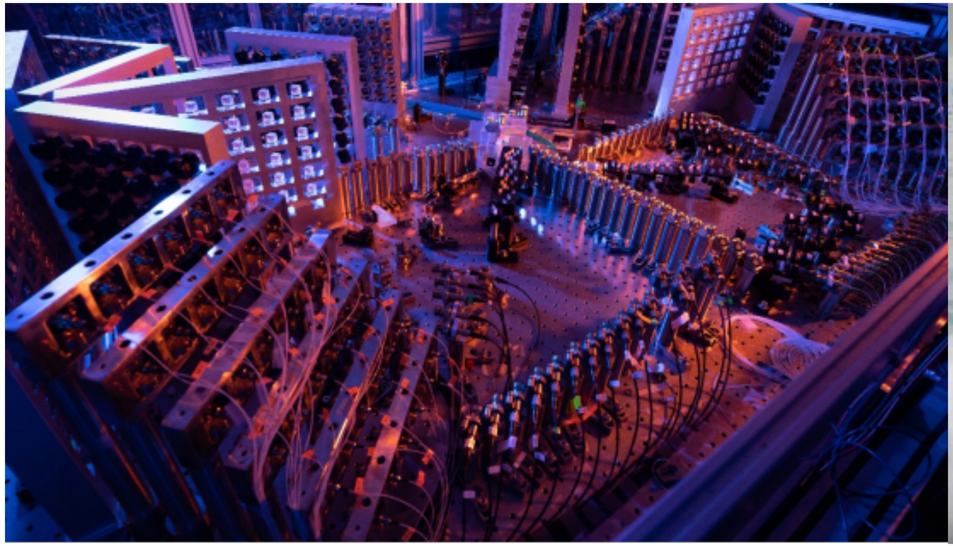

Alice
Bob
Carol
$\left(g^{s_A^i}, g^{\alpha_A}, g^{\alpha_A s_A^i}\right)$
$\left(g^{(s_A s_B)^i}, g^{\alpha_A \alpha_B}, g^{\alpha_A \alpha_B (s_A s_B)^i}\right)$
$\left(g^{s_{ABC}^i}, g^{\alpha_{ABC}}, g^{\alpha_{ABC} s_{ABC}^i}\right)$

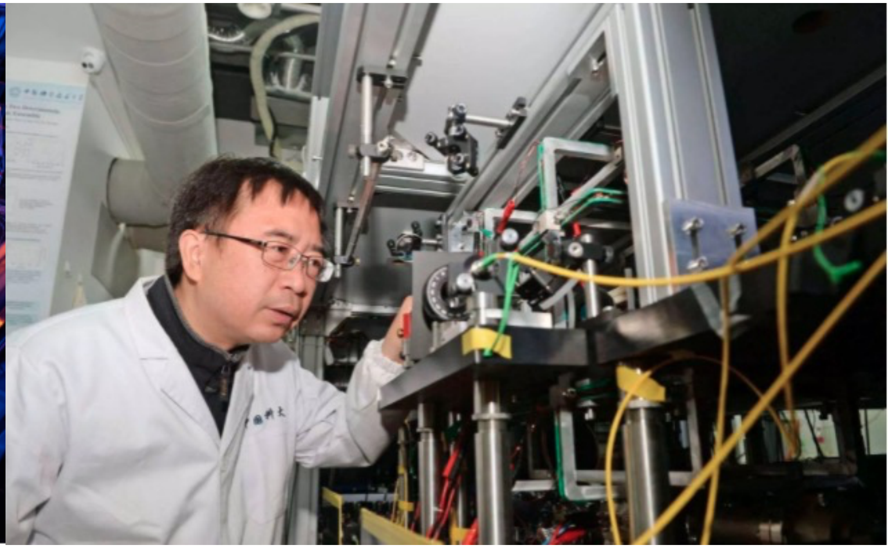
- Setup
  - sample random values s, α
  - calculate encryptions g^{α} and $\left\{g^{s^i}\right\}_{i\in[d]}, \left\{g^{\alpha s^i}\right\}_{i\in\{0,\dots,d\}}$
  - proving key: $\left(\left\{g^{s^i}\right\}_{i\in[d]}, \left\{g^{\alpha s^i}\right\}_{i\in\{0,\dots,d\}}\right)$
  - verification key: $\left(g^{\alpha}, g^{t(s)}\right)$
- Proving
  - assign coefficients $\{c_i\}_{i\in\{0,\dots,d\}}$ (i.e., knowledge), $p(x) = c_d x^d + \cdots + c_1 x^1 + c_0 x^0$
  - calculate polynomial $h(x) = \frac{p(x)}{t(x)}$
  - evaluate encrypted polynomials $g^{p(s)}$ and $g^{h(s)}$ using $\left\{g^{s^i}\right\}_{i\in[d]}$
  - evaluate encrypted shifted polynomial $g^{\alpha p(s)}$ using $\left\{g^{\alpha s^i}\right\}_{i\in\{0,\dots,d\}}$
  - sample random δ
  - set the randomized proof $\pi = \left(g^{\delta p(s)}, g^{\delta h(s)}, g^{\delta \alpha p(s)}\right)$
- Verification
  - parse proof π as $\left(g^{p}, g^{h}, g^{p'}\right)$
  - check polynomial restriction $e\left(g^{p'}, g\right) = e\left(g^{p}, g^{\alpha}\right)$
  - check polynomial cofactors $e\left(g^{p}, g\right) = e\left(g^{t(s)}, g^{h}\right)$

Zero-knowledge proof (ZKP) systems

ZKP System	Publication year	Protocol	Transparent	Universal	Plausibly Post-Quantum Secure	Programming Paradigm
Pinocchio[31]	2013	zk-SNARK	No	No	No	Procedural
Geppetto[32]	2015	zk-SNARK	No	No	No	Procedural
TinyRAM[33]	2013	zk-SNARK	No	No	No	Procedural
Buffet[34]	2015	zk-SNARK	No	No	No	Procedural
ZoKrates[35]	2018	zk-SNARK	No	No	No	Procedural
xJsnark[36]	2018	zk-SNARK	No	No	No	Procedural
vRAM[37]	2018	zk-SNARG	No	Yes	No	Assembly
vnTinyRAM[38]	2014	zk-SNARK	No	Yes	No	Procedural
MIRAGE[39]	2020	zk-SNARK	No	Yes	No	Arithmetic Circuits
Sonic[40]	2019	zk-SNARK	No	Yes	No	Arithmetic Circuits
Marlin[41]	2020	zk-SNARK	No	Yes	No	Arithmetic Circuits
PLONK[42]	2019	zk-SNARK	No	Yes	No	Arithmetic Circuits
SuperSonic[43]	2020	zk-SNARK	Yes	Yes	No	Arithmetic Circuits
Bulletproofs[44]	2018	Bulletproofs	Yes	Yes	No	Arithmetic Circuits
Hyrax[45]	2018	zk-SNARK	Yes	Yes	No	Arithmetic Circuits
Halo[46]	2019	zk-SNARK	Yes	Yes	No	Arithmetic Circuits
Virgo[47]	2020	zk-SNARK	Yes	Yes	Yes	Arithmetic Circuits
Ligero[48]	2017	zk-SNARK	Yes	Yes	Yes	Arithmetic Circuits
Aurora[49]	2019	zk-SNARK	Yes	Yes	Yes	Arithmetic Circuits
zk-STARK[50]	2019	zk-STARK	Yes	Yes	Yes	Assembly
Zilch[30] [51]	2021	zk-STARK	Yes	Yes	Yes	Object-Oriented

后量子密码学时代





USD | All Categories | Filter

#	Coin			Price	1h	24h	7d	24h Volume	Mkt Cap	Last 7 Days
☆ 1	Bitcoin	BTC	Buy	$44,176.12	0.2%	1.1%	-0.1%	$18,236,369,703	$837,565,313,276	
☆ 2	Ethereum	ETH	Buy	$3,141.08	0.2%	3.9%	0.3%	$13,349,156,209	$375,247,568,040	
☆ 3	Tether	USDT		$1.00	0.1%	0.1%	0.0%	$40,707,696,596	$78,801,593,653	
☆ 4	BNB	BNB	Buy	$431.04	0.0%	1.5%	5.3%	$1,937,746,921	$72,477,977,702	
☆ 5	USD Coin	USDC	Buy	$1.00	0.2%	0.1%	0.0%	$2,864,643,148	$52,650,255,820	
☆ 6	XRP	XRP	Buy	$0.836708	0.3%	1.7%	-5.1%	$2,939,654,126	$40,056,979,130	
☆ 7	Cardano	ADA		$1.10	0.3%	2.2%	-7.3%	$958,810,510	$35,117,607,008	
☆ 8	Solana	SOL	Buy	$103.41	0.9%	2.4%	-9.2%	$1,528,154,813	$32,958,326,534	

All owned by Trudy

丁津泰

Rainbow Signature

https://www.abccoin.cc/abc

Experience

Director of Ding Lab in Privacy Protection and Blockchain
Beijing Institute of Mathematical Sciences and Applications
Sep 2020 - Present · 1 yr 6 mos
Beijing, China

Professor at Yau Cener
Tsinghua University
Sep 2020 - Present · 1 yr 6 mos
Beijing, China

Charles Phelps Taft Professor
University of Cincinnati
Sep 1998 - Present · 23 yrs 6 mos

Education

Yale University
Ph.D.

人物介绍

丁津泰，美国耶鲁大学博士，曾任辛辛那提大学威廉·塔福特教授，现任清华大学数学科学中心和北京雁栖湖应用数学研究院双聘教授。早期主要从事量子仿射代数、表示论的研究工作，目前的研究方向是后量子密码学。曾三次担任国际后量子密码学会议的联席主席，是国际上多变量密码学著名学者之一。

Algorithm	Type	Public Key ⬍	Private Key ⬍	Signature ⬍
NTRU Encrypt[37]	Lattice	766.25 B	842.875 B	
Streamlined NTRU Prime	Lattice	154 B		
Rainbow[38]	Multivariate	124 KB	95 KB	
SPHINCS[19]	Hash Signature	1 KB	1 KB	41 KB
SPHINCS+[39]	Hash Signature	32 B	64 B	8 KB
BLISS–II	Lattice	7 KB	2 KB	5 KB
GLP–Variant GLYPH Signature[10][40]	Ring–LWE	2 KB	0.4 KB	1.8 KB
New Hope[41]	Ring–LWE	2 KB	2 KB	
Goppa–based McEliece[14]	Code–based	1 MB	11.5 KB	
Random Linear Code based encryption[42]	RLCE	115 KB	3 KB	
Quasi–cyclic MDPC–based McEliece[43]	Code–based	1,232 B	2,464 B	
SIDH[44]	Isogeny	564 B	48 B	
SIDH (compressed keys)[45]	Isogeny	330 B	48 B	
3072–bit Discrete Log	**not PQC**	384 B	32 B	96 B
256–bit Elliptic Curve	**not PQC**	32 B	32 B	65 B

参考资料

[1] https://en.wikipedia.org/wiki/Classical_cipher
[2] https://en.wikipedia.org/wiki/Post-quantum_cryptography
[3] https://en.wikipedia.org/wiki/Shor%27s_algorithm
[4] https://en.wikipedia.org/wiki/Whitfield_Diffie
[5] https://en.wikipedia.org/wiki/Zero-knowledge_proof
[6] https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/
[7] https://www.nist.gov/
[8] http://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Ir
[9] https://csrc.nist.gov/publications/detail/journal-article/2017/pqc-a-new-opportunity-for-mathematics-community

Q&A

披星戴月奖

下期分享

等你揭晓

扫一扫留下你的建议