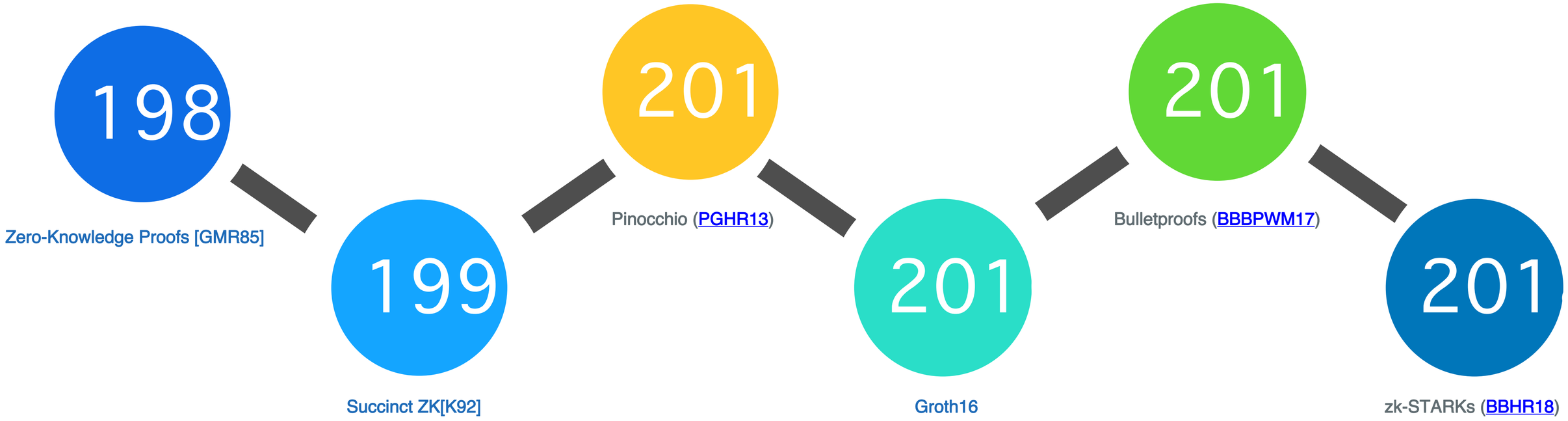
zk-SNARK入门

Star.LI@2019

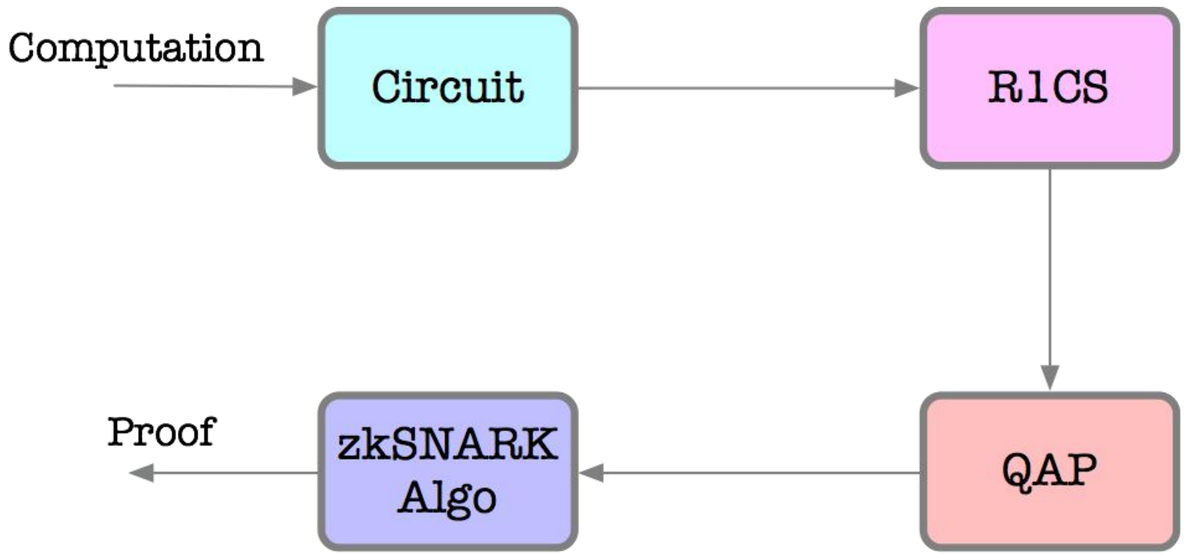
ZKP History


198
Zero-Knowledge Proofs [GMR85]
199
Succinct ZK[K92]
201
Pinocchio (PGHR13)
201
Groth16
201
Bulletproofs (BBBPWM17)
201
zk-STARKs (BBHR18)

What’s zk-SNARK?

- **zk** - Zero Knowledge
- S - Succinct: 证明数据量小
- N - Non-interactive: 无交互
- AR - ARguments: 计算可靠性下的证明
- K - Knowledge: 不泄露任何知识

How zk-SNARK works?



What's QAP?

- P问题 - 多项式时间可解
- NP问题 - 多项式时间不可解，但是多项式时间可验证
- NPC问题 - NP问题，所有NP问题都可规约到一个NPC问题

QAP问题是NP问题

What's QAP?

QAP问题是这样一个NP问题：给定一系列的多项式，以及给定一个目标多项式，找出多项式的组合能整除目标多项式。输入为n位的QAP问题定义如下：

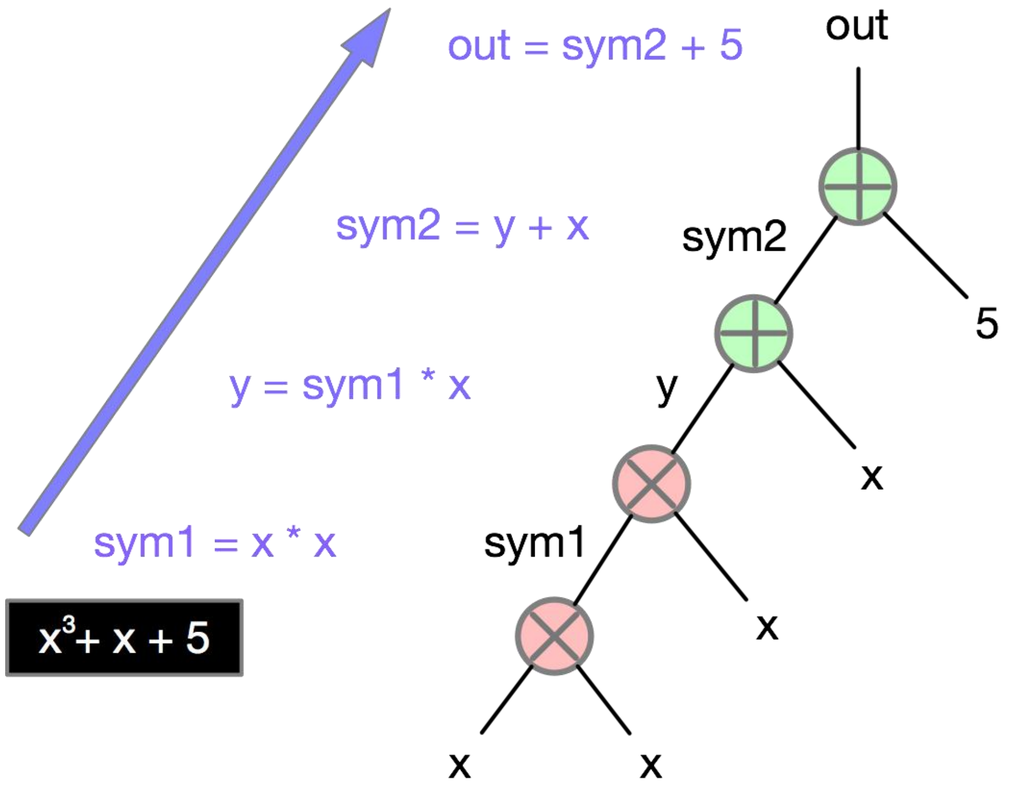
- 给定多个多项式：$v_0, \ldots, v_m, w_0, \ldots, w_m, y_0, \ldots, y_m$
- 目标多项式：t
- 映射函数：$f : \{(i,j) | 1 \leq i \leq n, j \in 0,1\} \rightarrow \{1, \ldots m\}$（确定输入对应的序号）

给定一个证据u（由Statement，Witness以及中间门电路的输出组成），满足如下条件，即可验证u是QAP问题的解：

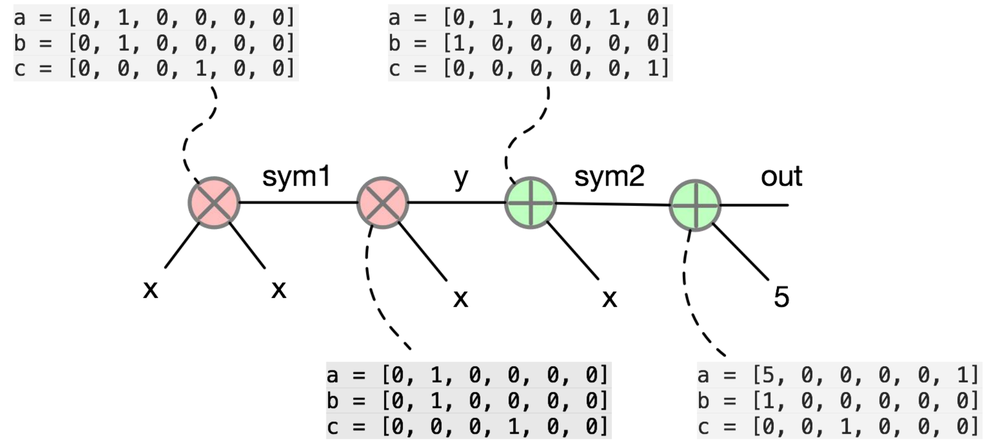
- $(v_0(x) + \sum_{k=1}^{m} a_k \cdot v_k(x)) \cdot (w_0(x) + \sum_{k=1}^{m} b_k \cdot w_k(x)) - (y_0(x) + \sum_{k=1}^{m} c_k \cdot y_k(x))$能整除 $t(x)$

对一个证据u，多项式之间的系数（$a_1, \ldots, a_m$，和$b_1, \ldots, b_m$，以及$c_1, \ldots, c_m$ 相等）。

Circuit Flattening



R1CS - Rank-1 Constraint System



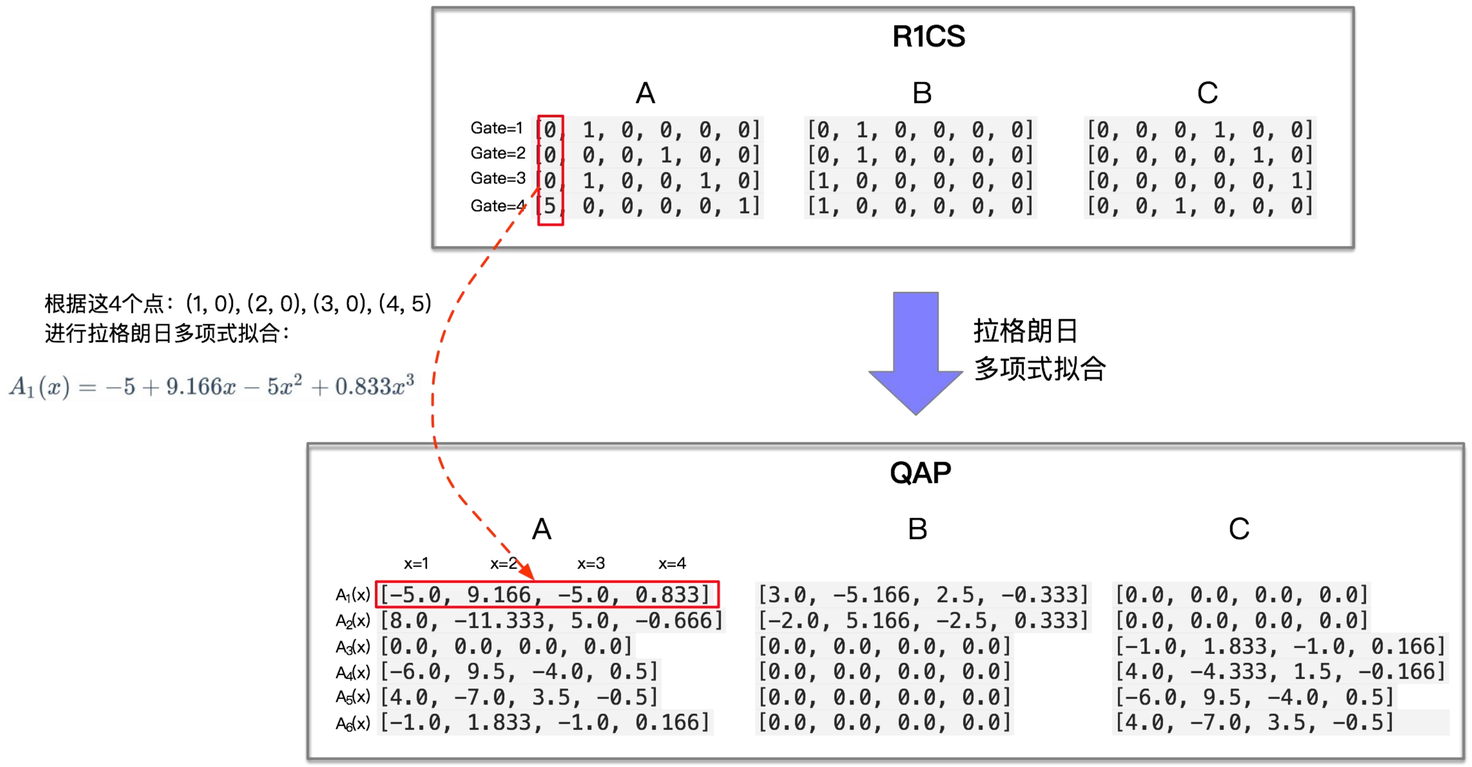
s = [one, x, out, sym1, y, sym2]

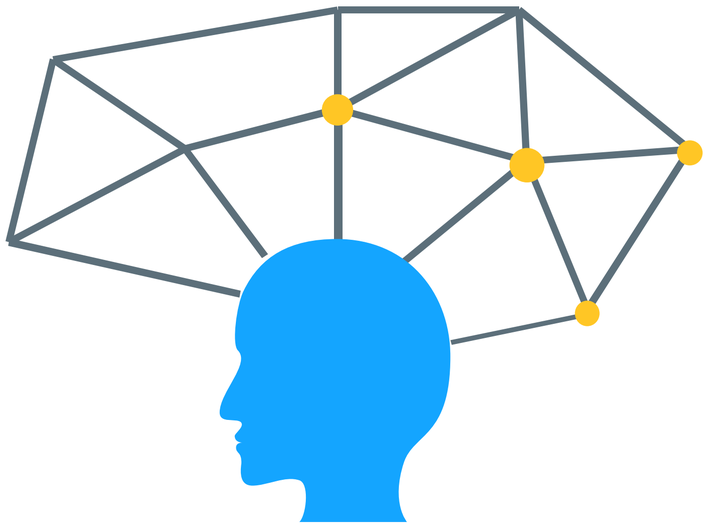
s.a * s.b - s.c = 0

R1CS

	A	B	C
Gate1	[0, 1, 0, 0, 0, 0]	[0, 1, 0, 0, 0, 0]	[0, 0, 0, 1, 0, 0]
Gate2	[0, 0, 0, 1, 0, 0]	[0, 1, 0, 0, 0, 0]	[0, 0, 0, 0, 1, 0]
Gate3	[0, 1, 0, 0, 1, 0]	[1, 0, 0, 0, 0, 0]	[0, 0, 0, 0, 0, 1]
Gate4	[5, 0, 0, 0, 0, 1]	[1, 0, 0, 0, 0, 0]	[0, 0, 1, 0, 0, 0]

QAP


R1CS
A
B
C
Gate=1 [0, 1, 0, 0, 0, 0] [0, 1, 0, 0, 0, 0] [0, 0, 0, 1, 0, 0]
Gate=2 [0, 0, 0, 1, 0, 0] [0, 1, 0, 0, 0, 0] [0, 0, 0, 0, 1, 0]
Gate=3 [0, 1, 0, 0, 1, 0] [1, 0, 0, 0, 0, 0] [0, 0, 0, 0, 0, 1]
Gate=4 [5, 0, 0, 0, 0, 1] [1, 0, 0, 0, 0, 0] [0, 0, 1, 0, 0, 0]
根据这4个点：(1, 0), (2, 0), (3, 0), (4, 5)
进行拉格朗日多项式拟合：
$A_1(x) = -5 + 9.166x - 5x^2 + 0.833x^3$
拉格朗日
多项式拟合
QAP
A
B
C
x=1 x=2 x=3 x=4
A1(x) [-5.0, 9.166, -5.0, 0.833] [3.0, -5.166, 2.5, -0.333] [0.0, 0.0, 0.0, 0.0]
A2(x) [8.0, -11.333, 5.0, -0.666] [-2.0, 5.166, -2.5, 0.333] [0.0, 0.0, 0.0, 0.0]
A3(x) [0.0, 0.0, 0.0, 0.0] [0.0, 0.0, 0.0, 0.0] [-1.0, 1.833, -1.0, 0.166]
A4(x) [-6.0, 9.5, -4.0, 0.5] [0.0, 0.0, 0.0, 0.0] [4.0, -4.333, 1.5, -0.166]
A5(x) [4.0, -7.0, 3.5, -0.5] [0.0, 0.0, 0.0, 0.0] [-6.0, 9.5, -4.0, 0.5]
A6(x) [-1.0, 1.833, -1.0, 0.166] [0.0, 0.0, 0.0, 0.0] [4.0, -7.0, 3.5, -0.5]



What’s t?

Groth16

QAP的定义为"**R**elation"：$R=(p,G_1,G_2,G_T,e,g,h,\ell,\{u_i(X),v_i(X),w_i(X)\}_{i=0}^m,t(X))$。在一个域$Z_p$中，**statements**为$(a_1,\ldots,a_\ell)\in Z_p^\ell$， **witness**为$(a_{l+1},\ldots,a_m)\in Z_p^{m-\ell}$，并且$a_0=1$的情况下，满足如下的等式（$t(X)$的阶为n）：

$$\sum_{i=0}^m a_iu_i(X)\cdot\sum_{i=0}^m a_iv_i(X)=\sum_{i=0}^m a_iw_i(X)+h(X)t(X)$$

三个有限群G_1,G_2,G_T, 对应的生成元分别是$g,h,e(g,h)$。G_1有限群的计算用$[y]_1=g^y$表示，G_2有限群的计算用$[y]_2=h^y$表示。

1. 设置过程：随机选取$\alpha,\beta,\gamma,\delta,x\leftarrow Z_p^*$，生成$\sigma,\tau$。

   $$\tau=(\alpha,\beta,\gamma,\delta,x)$$

   $$\sigma=([\sigma_1]_1,[\sigma_2]_2)$$

   $$\sigma_1=(\alpha,\beta,\delta,\{x^i\}_{i=0}^{n-1},\{\frac{\beta u_i(x)+\alpha v_i(x)+w_i(x)}{\gamma}\}_{i=0}^{\ell},\{\frac{\beta u_i(x)+\alpha v_i(x)+w_i(x)}{\delta}\}_{i=\ell+1}^{m},\{\frac{x^it(x)}{\delta}\}_{i=0}^{n-2})$$

   $$\sigma_2=(\beta,\gamma,\delta,\{x^i\}_{i=0}^{n-1})$$

2. 证明过程：随机选择两个参数r和s，计算$\pi=\Pi\sigma=([A]_1,[C]_1,[B]_2)$

   $$A=\alpha+\sum_{i=0}^m a_iu_i(x)+r\delta$$

   $$B=\beta+\sum_{i=0}^m a_iv_i(x)+s\delta$$

   $$C=\frac{\sum_{i=\ell+1}^m a_i(\beta u_i(x)+\alpha v_i(x)+w_i(x))+h(x)t(x)}{\delta}+As+rB-rs\delta$$

3. 验证过程：验证如下的等式是否成立。

   $$[A]_1\cdot[B]_2=[\alpha]_1\cdot[\beta]_2+\sum_{i=0}^{\ell}a_i[\frac{\beta u_i(x)+\alpha v_i(x)+w_i(x)}{\gamma}]_1\cdot[\gamma]_2+[C]_1\cdot[\delta]_2$$

Groth16

椭圆曲线，同态隐藏，
双线性映射

Groth16 - CRS

- CRS - Common Reference String
- toxic waste - alpha, beta, x …
- MPC - Zcash using MPC protocol to generate trusted CRS

欢迎关注 星想法

Thanks!