A Glimpse of Zero-Knowledge Proof

Stone@Earth 2018.09

零知识证明(Zero-Knowledge Proof)

- A知道某个秘密，给出证明
- 群众能从A的证明中确信A知道那个秘密
- 群众无法得到A的那个秘密

隐藏秘密的方法

- 通过特定约束条件，构造同态映射
  - 三色问题，经典数独问题
- 通过“极难求解却极易验证”的难题
  - 大数分解，二次剩余
- 通过同态计算
  - 有限域离散对数问题(DLP)
  - 椭圆曲线离散对数问题(ECDLP)
  - 椭圆曲线配对映射求逆问题(PBC)

零知识证明“固件时代”

1980~2012

- 针对特定问题
- 无法实现算法证明

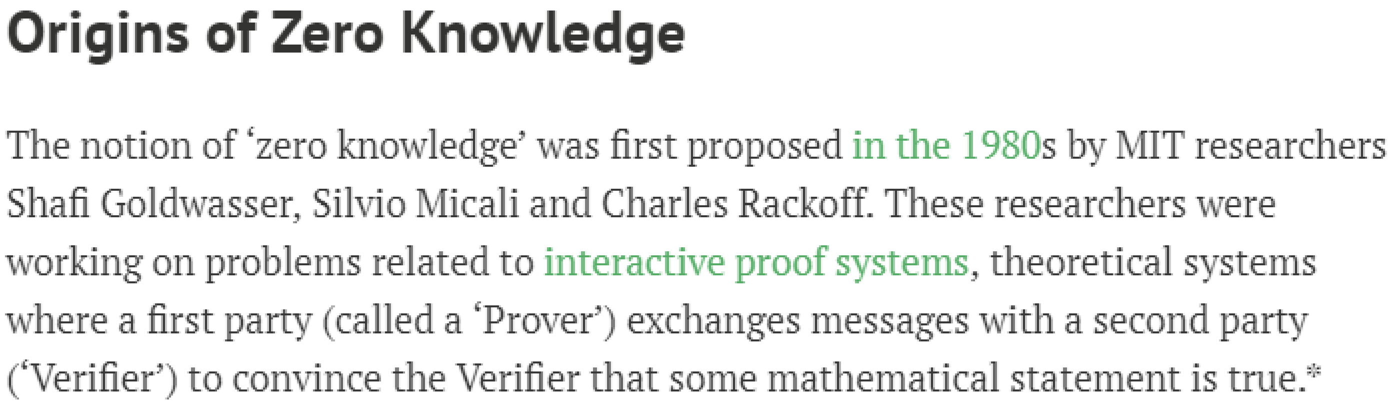
零知识证明一撇(1)

- 1980年 Goldreich, Micali and Wigderson

The Knowledge Complexity of Interactive Proof-Systems

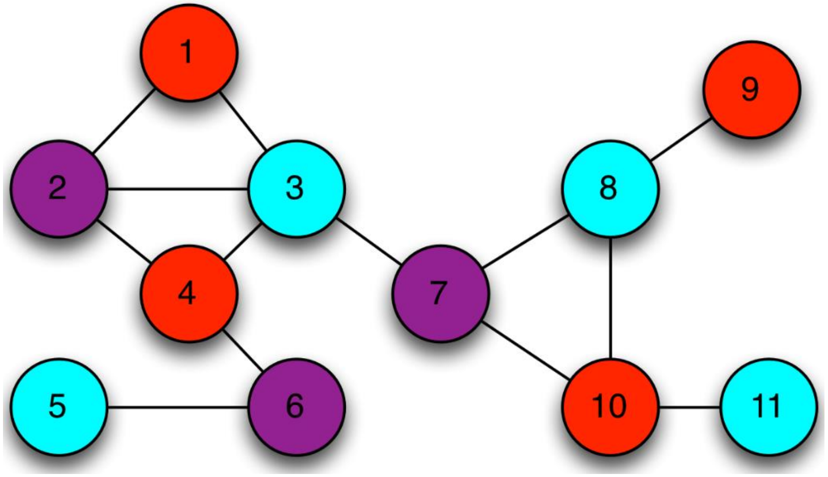
1985 ACM 0-89791-151-2/85/005/0291

https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/



Origins of Zero Knowledge

The notion of ‘zero knowledge’ was first proposed in the 1980s by MIT researchers Shafi Goldwasser, Silvio Micali and Charles Rackoff. These researchers were working on problems related to interactive proof systems, theoretical systems where a first party (called a ‘Prover’) exchanges messages with a second party (‘Verifier’) to convince the Verifier that some mathematical statement is true.*

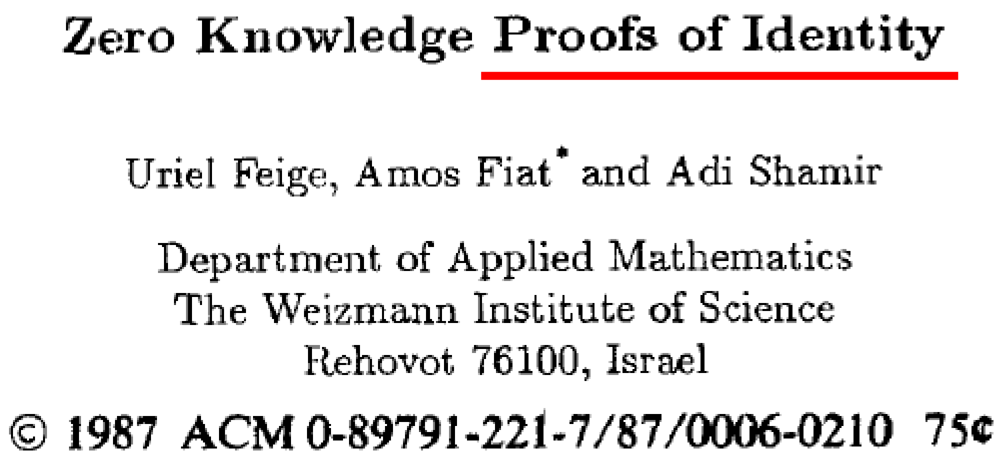


零知识证明一撇(2)

- 1987年 Feige, Fiat, Shamir

通过大数分解和二次剩余隐藏秘密

https://www.slideserve.com/hashim/zero-knowledge-proofs-of-identity

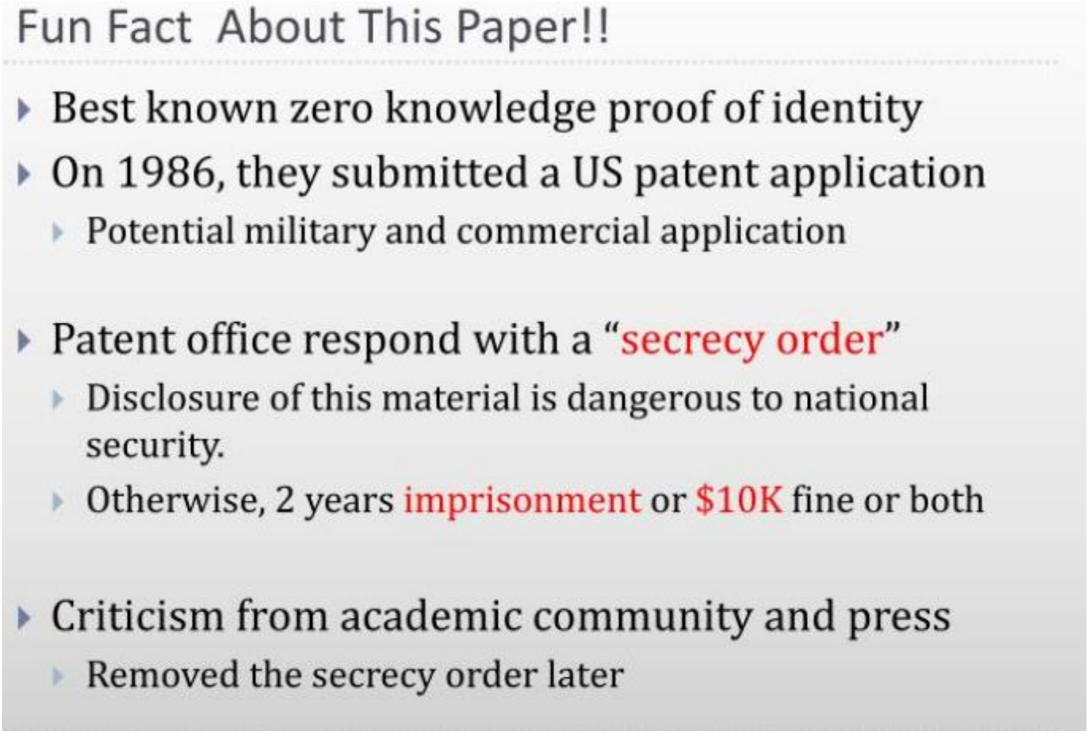


Zero Knowledge Proofs of Identity

Uriel Feige, Amos Fiat* and Adi Shamir

Department of Applied Mathematics
The Weizmann Institute of Science
Rehovot 76100, Israel

© 1987 ACM 0-89791-221-7/87/0006-0210 75¢



Fun Fact About This Paper!!

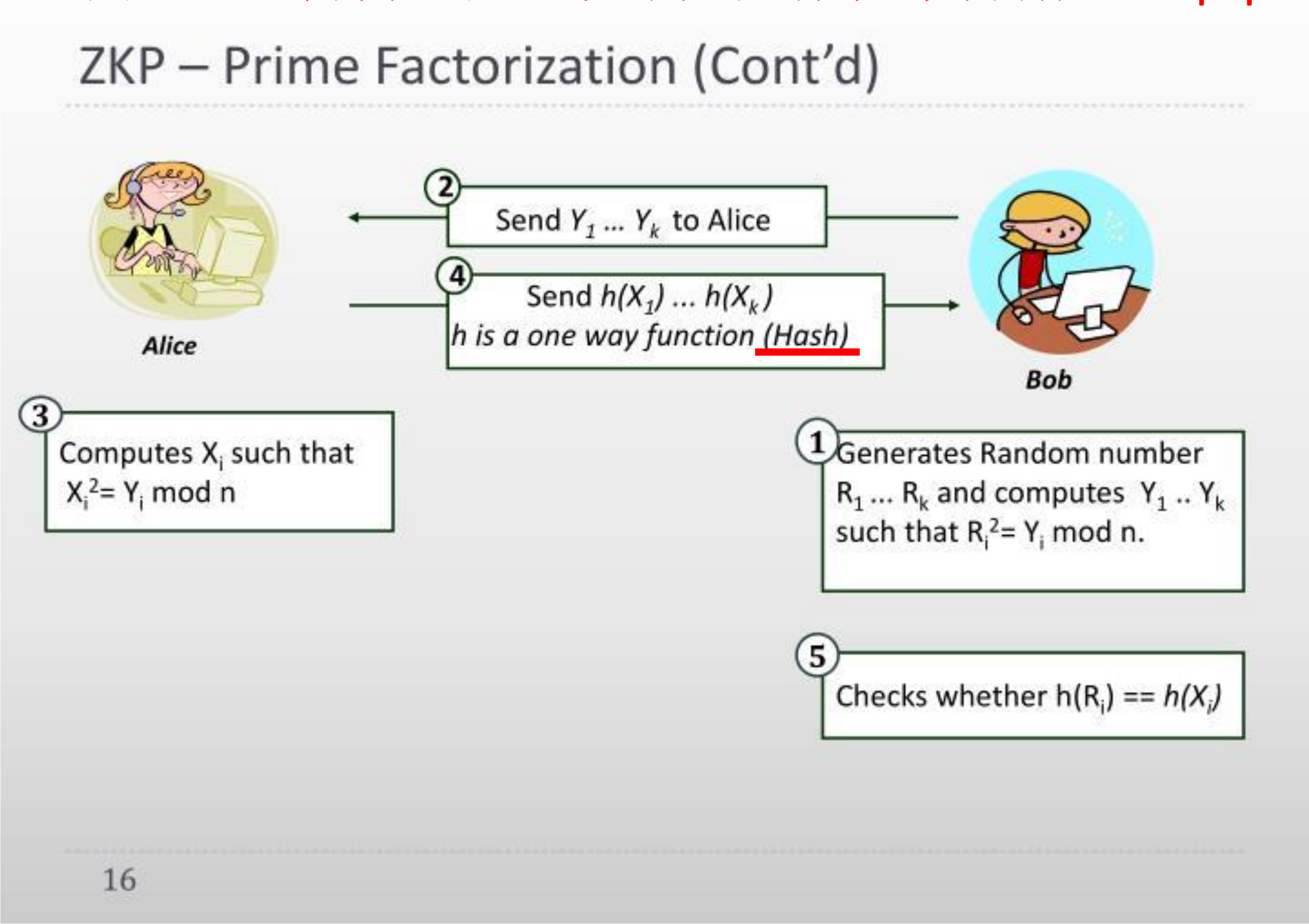
- Best known zero knowledge proof of identity
- On 1986, they submitted a US patent application
  - Potential military and commercial application
- Patent office respond with a “secrecy order”
  - Disclosure of this material is dangerous to national security.
  - Otherwise, 2 years imprisonment or $10K fine or both
- Criticism from academic community and press
  - Removed the secrecy order later

美国专利局回复：

解密本资料危及国家安全，
或遭受2年牢狱及一万美元罚款

零知识证明一撇(2)

Alice向Bob证明自己知道如何对n作质数分解，n=pq，其中p和q为质数



ZKP – Prime Factorization (Cont’d)

② Send Y_1 … Y_k to Alice

④ Send $h(X_1)$ … $h(X_k)$
h is a one way function (Hash)

③ Computes X_i such that $X_i^2 = Y_i \bmod n$

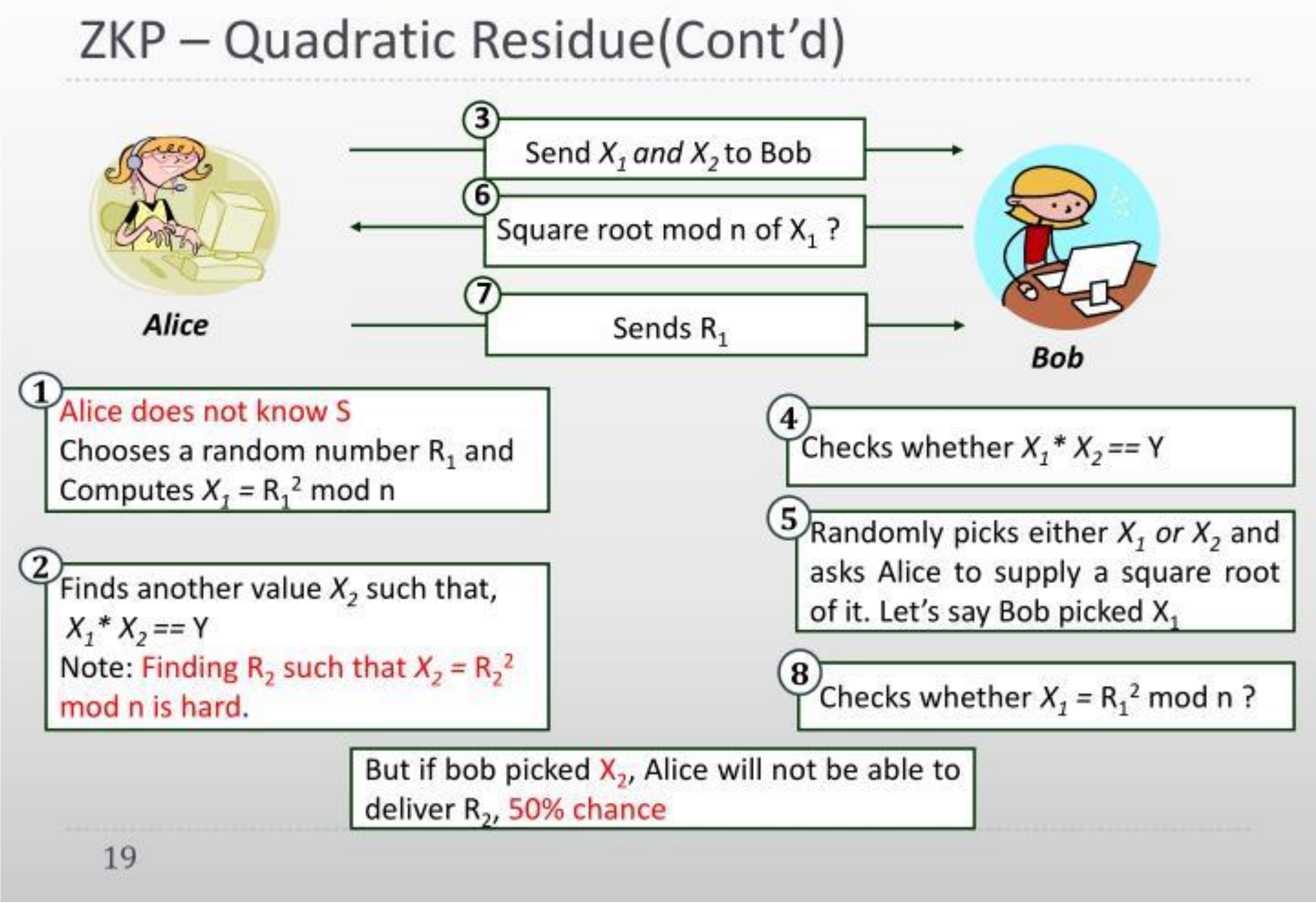
① Generates Random number R_1 … R_k and computes Y_1 .. Y_k such that $R_i^2 = Y_i \bmod n$.

⑤ Checks whether $h(R_i) == h(X_i)$

零知识证明
非概率证明

零知识证明一撇(2)

Alice向Bob证明自己知道 S 满足$S^2 = Y \ mod \ n$



ZKP – Quadratic Residue(Cont’d)

Alice

Bob

3 Send X_1 *and* X_2 to Bob

6 Square root mod n of X_1 ?

7 Sends R_1

1 Alice does not know S
Chooses a random number R_1 and
Computes $X_1 = R_1^2$ mod n

2 Finds another value X_2 such that,
$X_1 * X_2 == Y$
Note: Finding R_2 such that $X_2 = R_2^2$ mod n is hard.

4 Checks whether $X_1 * X_2 == Y$

5 Randomly picks either X_1 *or* X_2 and asks Alice to supply a square root of it. Let’s say Bob picked X_1

8 Checks whether $X_1 = R_1^2$ mod n ?

But if bob picked X_2, Alice will not be able to deliver R_2, 50% chance

19

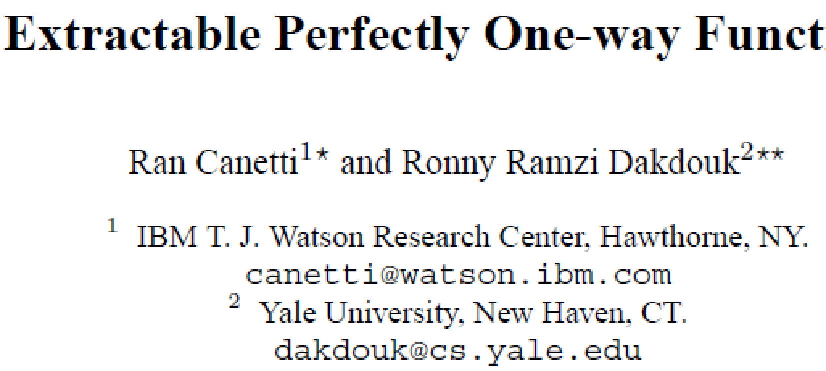
零知识证明
概率证明(PCP)

PCP: Probabilistically Checkable Proof

零知识证明一撇(3)

- 2006年 Canetti, Dakdouk

https://crypto.stanford.edu/portia/papers/CanettiExtractable.pdf



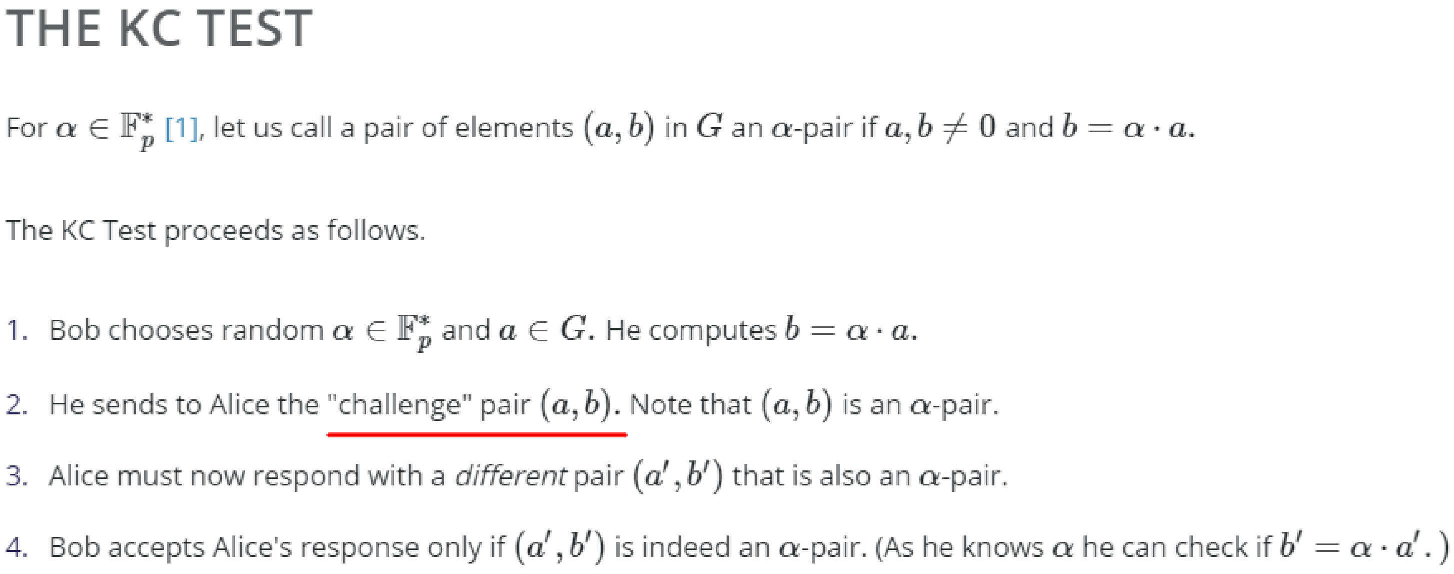
Extractable Perfectly One-way Functions

Ran Canetti[1]* and Ronny Ramzi Dakdouk[2]**

[1] IBM T. J. Watson Research Center, Hawthorne, NY.
canetti@watson.ibm.com
[2] Yale University, New Haven, CT.
dakdouk@cs.yale.edu

Extractable One-way Function
A给出函数计算结果
B能确信A知道某个秘密
B无法从A的计算结果中得到该秘密
Hash函数算不算EOWF？
H1=HASH(x)
(g^x, g^{xy})是EOWF？

https://blog.z.cash/snark-explain3/



THE KC TEST

For $\alpha \in \mathbb{F}_p^*$ [1], let us call a pair of elements (a, b) in G an α-pair if $a, b \neq 0$ and $b = \alpha \cdot a$.

The KC Test proceeds as follows.

1. Bob chooses random $\alpha \in \mathbb{F}_p^*$ and $a \in G$. He computes $b = \alpha \cdot a$.
2. He sends to Alice the "challenge" pair (a, b). Note that (a, b) is an α-pair.
3. Alice must now respond with a *different* pair (a', b') that is also an α-pair.
4. Bob accepts Alice's response only if (a', b') is indeed an α-pair. (As he knows α he can check if $b' = \alpha \cdot a'$.)

白板演示

基于“可提取函数”的零知证明

零知识证明“软件时代”

2013~

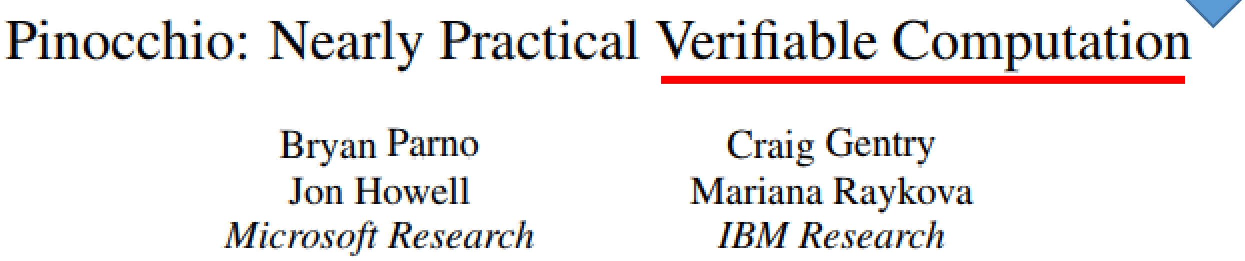
- 算法证明
- 简约紧致证明
- 公开证明

适用于区块链

零知识证明一撇(4)

- 2013年 Parno, Gentry

https://eprint.iacr.org/2013/279.pdf



Pinocchio: Nearly Practical Verifiable Computation

Bryan Parno
Jon Howell
Microsoft Research

Craig Gentry
Mariana Raykova
IBM Research

VC计算比ZK证明更困难。两种场景：
(1) 数据资源公开，证明计算过程可信
(2) 数据资源不公开，证明计算结果可信(科幻？)

由于需要交付计算结果，因此需要传输证明PoD

PoD: Proof of Delivery

破冰之作，ZK证明由“固件时代”进入“软件时代”
最近5年的ZK文章，如果你没有足够时间，那就只读这一篇

关于VC计算，多说一句

近日，在“暗网交易市场”网站上，一个暗网用户售卖顺丰快递数据，卖家称掌握了顺丰快递客户数据总量高达3亿条，售价两个比特币。这些数据包括顺丰快递寄、收件人的姓名、地址、电话等信息，可以先“验货”，验货数据量为10万条，验货费用0.01个比特币。目前，已有10个账号验货。顺丰公司已报警。

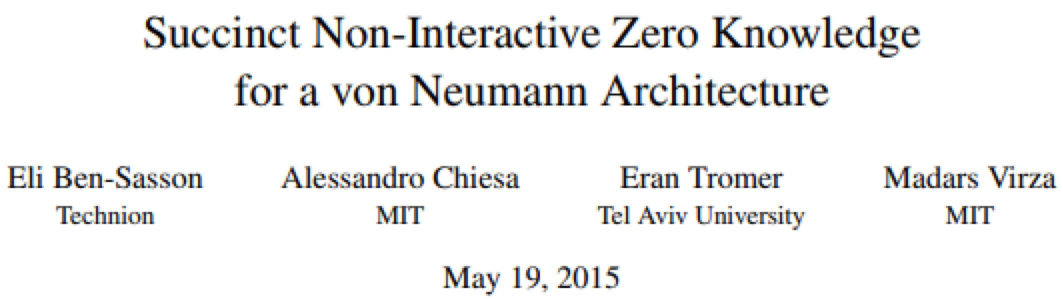
信任的鸿沟

- 验货能不能做到“零信息泄露”？
- 买家怎么知道黑客其实只有10万条真实数据，其余的都是编造的？
- 买家收到货时，怎么知道自己收到的3亿条就是黑客手里的3亿条？

零知识证明一撇(5)

- 2014年 Eli Ben-Sasson

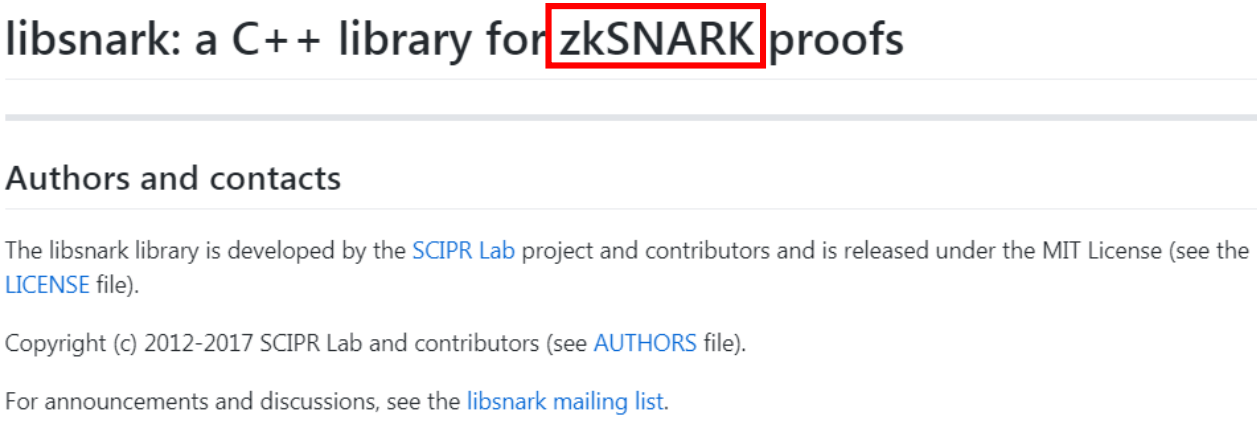
https://eprint.iacr.org/2013/879.pdf



Succinct Non-Interactive Zero Knowledge
for a von Neumann Architecture

Eli Ben-Sasson	Alessandro Chiesa	Eran Tromer	Madars Virza
Technion	MIT	Tel Aviv University	MIT

May 19, 2015



libsnark: a C++ library for zkSNARK proofs

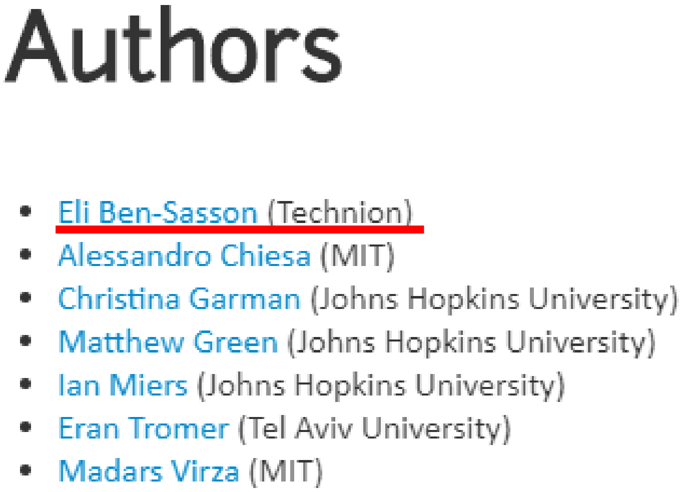
Authors and contacts

The libsnark library is developed by the SCIPR Lab project and contributors and is released under the MIT License (see the LICENSE file).

Copyright (c) 2012-2017 SCIPR Lab and contributors (see AUTHORS file).

For announcements and discussions, see the libsnark mailing list.

Zerocoin Project



Authors

- Eli Ben-Sasson (Technion)
- Alessandro Chiesa (MIT)
- Christina Garman (Johns Hopkins University)
- Matthew Green (Johns Hopkins University)
- Ian Miers (Johns Hopkins University)
- Eran Tromer (Tel Aviv University)
- Madars Virza (MIT)

ZCASH举行避嫌仪式

https://z.cash.foundation/blog/powers-of-tau/

The Zcash Foundation

ZAPPS

Announcing the world's largest multi-party computation ceremony

Zcash在setup阶段有不可公示的秘密
Common Reference String

避嫌：setup是多方协作完成的，每一方都不掌握所有秘密——不能排除共谋

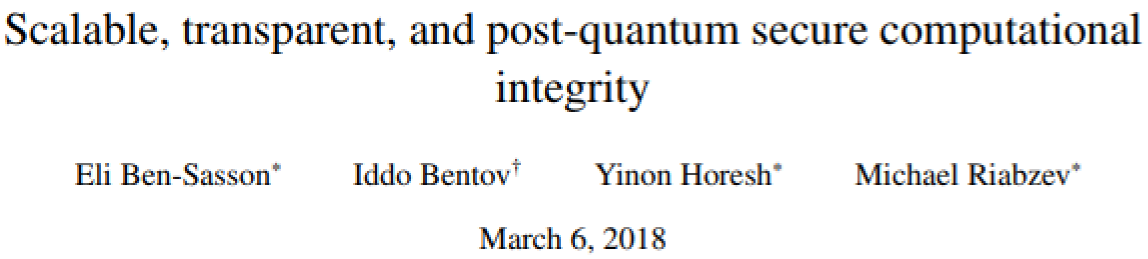
零知识证明一撇(6)

- 2018年 Eli Ben-Sasson

https://eprint.iacr.org/2018/046.pdf

zkStark在setup阶段没有秘密
代价： proof由288B增加到100kB

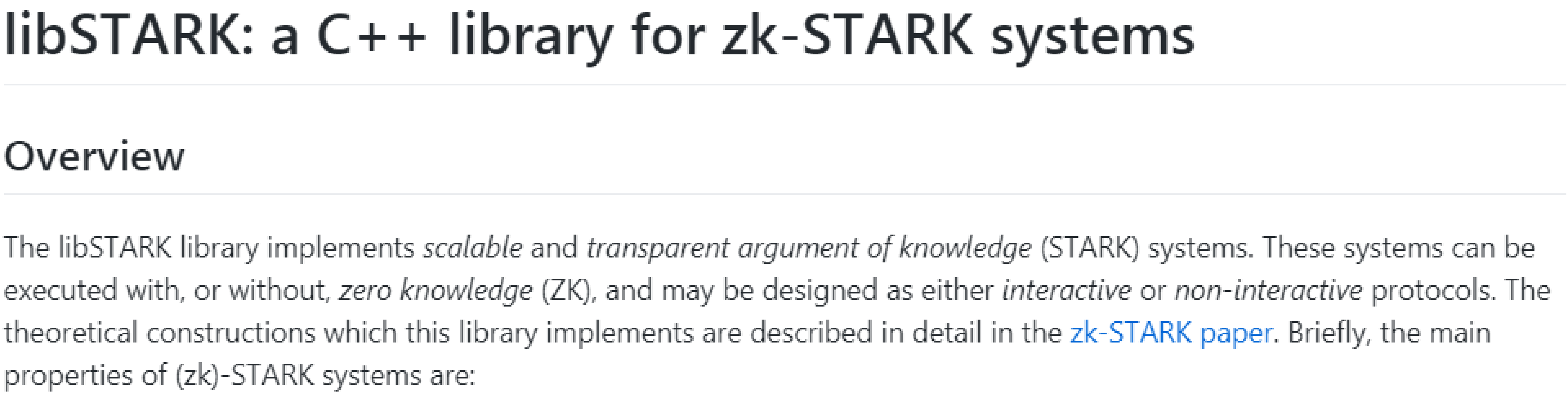
基于通信编码理论实现概率证明
而非基于PBC同态计算



Scalable, transparent, and post-quantum secure computational integrity

Eli Ben-Sasson* Iddo Bentov† Yinon Horesh* Michael Riabzev*

March 6, 2018



libSTARK: a C++ library for zk-STARK systems

Overview

The libSTARK library implements *scalable* and *transparent argument of knowledge* (STARK) systems. These systems can be executed with, or without, *zero knowledge* (ZK), and may be designed as either *interactive* or *non-interactive* protocols. The theoretical constructions which this library implements are described in detail in the zk-STARK paper. Briefly, the main properties of (zk)-STARK systems are:

零知识证明应用

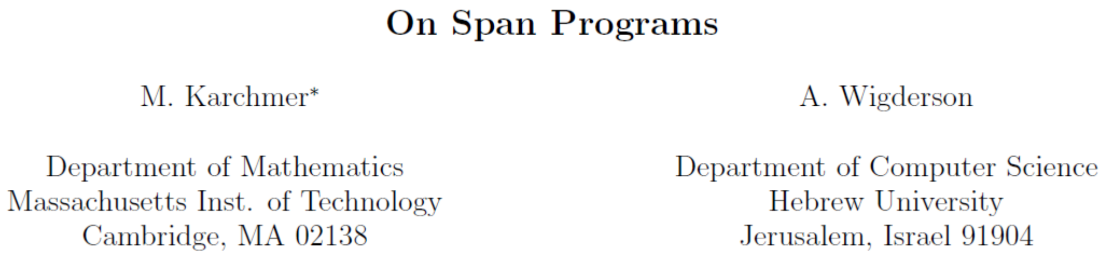
- 信息灰度上链
  - 数据持有证明
- 全网统一登录
  - 登录某网站时，不在网站上注册帐号，而是证明自己是链上某帐号
- 数据交易平台
  - 传输证明
  - 打通数据孤岛，增强企业协作
- 可信计算
  - 敏感数据计算服务
  - 全民数据淘金 (类似google trends)

接下来是枯燥的细节

SP→QSP→QAP

SP, QSP, QAP

https://link.springer.com/content/pdf/10.1007%2F978-3-642-38348-9_37.pdf



On Span Programs

M. Karchmer*

Department of Mathematics
Massachusetts Inst. of Technology
Cambridge, MA 02138

A. Wigderson

Department of Computer Science
Hebrew University
Jerusalem, Israel 91904

Span Program

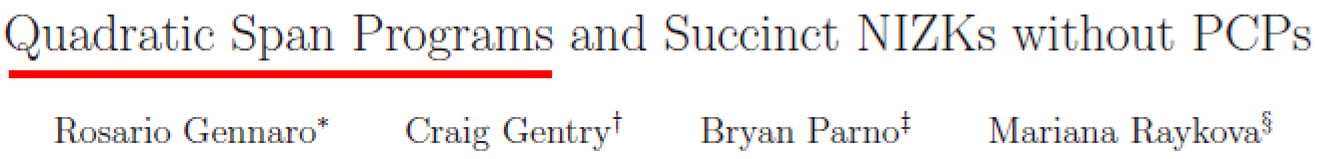
判断3维向量σ满足F(σ)=1 (其中向量σ的每个元素都是0或1)

$$\hat{M} = \begin{bmatrix} m_{11}^{0(1)} & m_{12}^{0(1)} & m_{13}^{0(1)} \\ m_{21}^{0(1)} & m_{22}^{0(1)} & m_{23}^{0(1)} \\ m_{31}^{0(1)} & m_{32}^{0(1)} & m_{33}^{0(1)} \end{bmatrix}$$

矩阵$\hat{M}$相当于F(x)的算法电路图
每个gate有两种状态

F(x)算法用矩阵$\hat{M}$表示
矩阵$\hat{M}$的每个元素有两个值，根据输入参数σ来选择启用哪个算法：
固定某个向量v (target vector)
对于输入参数向量σ，确定矩阵$\hat{M}$每一个元素的值，得到M
用M来span向量空间，具体做法是用任意三维向量s对M作左乘，得到新的向量w=sM，所有这样得到的新向量的集合称作由M span得到的向量空间。如果之前固定的那个v在这个新的向量空间里面，那么就等价于F(σ)=1。

SP->QSP



Quadratic Span Programs and Succinct NIZKs without PCPs

Rosario Gennaro[*] Craig Gentry[†] Bryan Parno[‡] Mariana Raykova[§]

判断3维向量σ满足F(σ)=1 (其中向量σ的每个元素都是0或1)

$$\hat{M} = \begin{bmatrix} m_{11}^{0(1)} & m_{12}^{0(1)} & m_{13}^{0(1)} \\ m_{21}^{0(1)} & m_{22}^{0(1)} & m_{23}^{0(1)} \\ m_{31}^{0(1)} & m_{32}^{0(1)} & m_{33}^{0(1)} \end{bmatrix}$$

F(x)算法用矩阵$\hat{M}$表示
矩阵$\hat{M}$的每个元素有两个值，根据输入参数σ来选择启用哪个算法：
固定某个向量v (target vector)
对于输入参数向量σ，确定矩阵$\hat{M}$每一个元素的值，得到M
用M来span向量空间，具体做法是用任意三维向量s对M作左乘，得到新的向量w=sM，所有这样得到的新向量的集合称作由M span得到的向量空间。如果之前固定的那个v在这个新的向量空间里面，那么就等价于F(σ)=1。

QSP

F(x)的算法电路图
每个gate构造两个多项式u(x)和w(x)

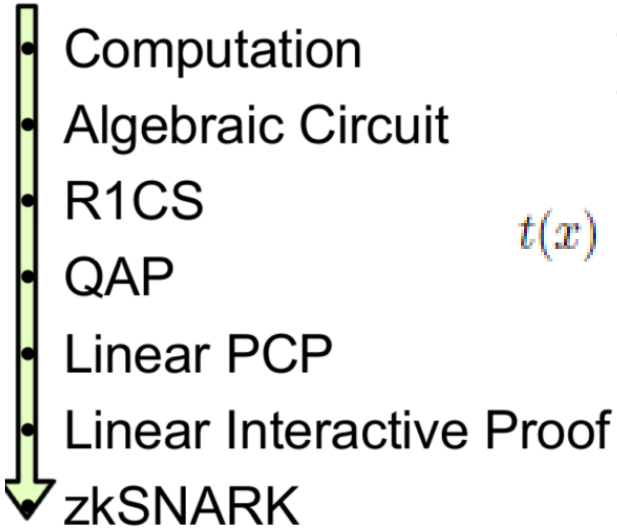
QSP

判断固定的目标多项式t(x)，是否能被$\hat{M}$和σ共同决定的多项式v(x)和w(x)整除

$$t(x) \quad \text{divides} \quad \left(v_0(x) + \sum_{k=1}^{m} a_k \cdot v_k(x)\right) \cdot \left(w_0(x) + \sum_{k=1}^{m} b_k \cdot w_k(x)\right)$$

QAP(Quadratic Arithmetic Programs)

https://medium.com/@VitalikButerin/quadratic-arithmetic-programs-from-zero-to-hero-f6d558cea649



- Computation
- Algebraic Circuit
- R1CS
- QAP
- Linear PCP
- Linear Interactive Proof
- zkSNARK

QAP的输入参数u的取值不限于0或1

QAP对于算法电路图的乘法gate构造三个多项式

$$t(x) \quad \text{divides} \quad \left(v_0(x) + \sum_{k=1}^{m} a_k \cdot v_k(x)\right) \cdot \left(w_0(x) + \sum_{k=1}^{m} a_k \cdot w_k(x)\right) - \left(y_0(x) + \sum_{k=1}^{m} a_k \cdot y_k(x)\right)$$

R1CS→QAP

① 把每个gate的流入、流出的信息视为约束向量a,b,c

② 所有gate生成的约束向量构成向量集合A,B,C

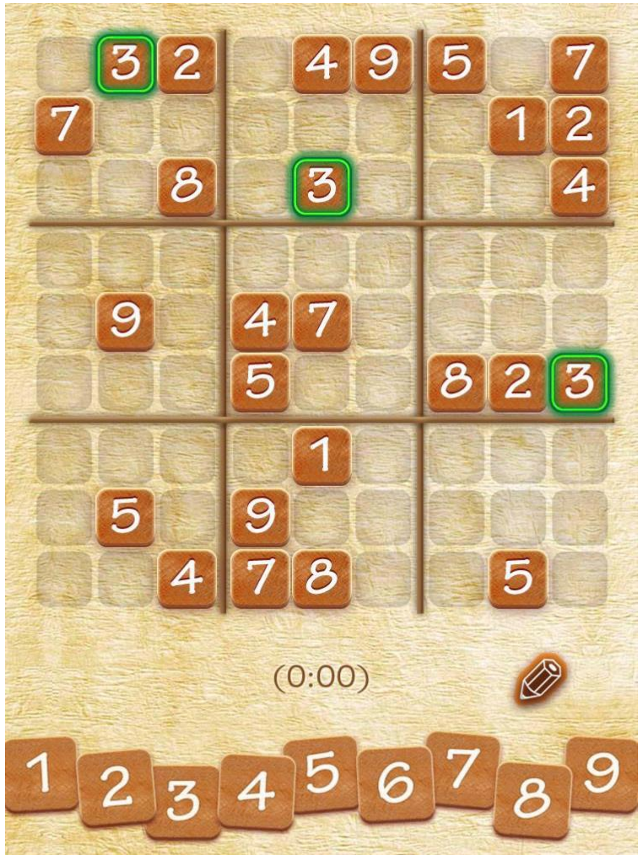
③ 把向量集合A,B,C转换为多项式集合v(x), w(x), y(X) 且满足 v(x)*w(x)-y(x)=H(x)*t(x)，其中t(x)预先给定

问题：如何零知证明自己知道一个能整除x-1的多项式P(x) ？

白板演示

“数独” 零知证明

“幻方” 零知证明



	3	2		4	9	5		7
7							1	2
		8		3				4
	9		4	7				
			5			8	2	3
				1				
	5		9					
		4	7	8			5	

(0:00)

x11	x12	X13
x21	17	X23
x31	x32	x33

总结

- 零知证明始于1980年，皮诺槽论文发表于2013年，zerocoin/zcash是成功应用
- zk-snark
  - 通过指数隐藏秘密（基于椭圆曲线）
  - 基于“椭圆曲线配对映射”实现同态计算证明(概率证明？)
  - 证明简洁，setup不够完美
- zk-sTark
  - 通过指数隐藏秘密（基于有限域）
  - 基于通信编码理论实现概率证明
  - 证明不够简洁

多谢观注！