National Institute of Information and Communications Technology

暗号理論における ブロックチェーン

NICT
セキュリティ基盤研究室
主任研究員 江村 恵太

自己紹介

- 国立研究開発法人情報通信研究機構
  - National Institute of Information and Communications Technology (NICT)
- サイバーセキュリティ研究所セキュリティ基盤研究室 主任研究員
- 研究テーマ：暗号理論, 暗号応用
  - グループ署名, IDベース/属性ベース/関数型暗号, 検索可能暗号, 準同型暗号など (公開鍵系)

本日の内容

- 暗号理論におけるブロックチェーン
- アブスト：暗号理論では, 様々な暗号要素 (公開鍵/共通鍵暗号, 署名, ゼロ知識証明, 一方向性関数等々) を組み合わせて別の暗号方式を構成する研究 (一般的構成) や, 逆にある暗号要素をどのように組み合わせても所望の暗号方式を作成するのは困難であることを示す研究 (ブラックボックス帰着困難性) が行われている.

- 本講演では, ブロックチェーンを暗号要素の一つとして見た場合, 構成可能性/不可能性の研究においてどのような結果が示されているのかを簡単に紹介する.

本日の内容 (雰囲気)

- ハッシュ関数
  - みなさんのイメージ（私見）：
    - ある値xのハッシュ値 H(x)が与えられてもxはわからない
  - 一方向性 (One-waynesss)　そのハッシュ値yを計算し

$$\mathrm{Adv}_{\mathcal{A}}^{\mathbf{OWF}}(k) := \Pr[H(z) = y | x \xleftarrow{\$} \{0,1\}^k;\ y = H(x);\ z \leftarrow \mathcal{A}(1^k, y)] < \epsilon(k)$$

kビットの値xを適当に選んで

攻撃アルゴリズムAに
与えるとzを出力して

H(z)=yとなる
(z=xかもしれないし衝突を
見つければz≠xでもいい)

確率が無視できる

本日の内容 (雰囲気)

- ハッシュ関数
  - みなさんのイメージ（私見）：
    - x≠zかつH(x)=H(z)となる組 (x,z) を見つけられない
  - 衝突困難性 (Collision Resistance)

$$\mathrm{Adv}_{\mathcal{A}}^{\mathbf{CR}}(k) := \Pr[H(z) = H(x) \wedge x \neq z | (x, z) \leftarrow \mathcal{A}(1^k)] < \epsilon(k)$$

H(z)=H(x) かつ
xとzは違う値となる

攻撃アルゴリズムAが
(x,z) を出力

確率が無視できる

本日の内容 (雰囲気)

- ハッシュ関数
  - 一方向性 (One-waynesss)
  - 衝突困難性 (Collision Resistance)

入出力のインターフェースのみ既知

- 一方向性関数 (正確には置換) から衝突困難ハッシュ関数を (ブラックボックス帰着で) 構成することは困難
  - Daniel R. Simon: Finding Collisions on a One-Way Street: Can Secure Hash Functions Be Based on General Assumptions? EUROCRYPT 1998: 334-345
    - Nonブラックボックスならいける
      Justin Holmgren, Alex Lombardi: Cryptographic Hashing from Strong One-Way Functions (Or: One-Way Product Functions and Their Applications). FOCS 2018: 850-858

本日の内容 (雰囲気)

- 一方向性関数が存在すると疑似乱数生成器が存在する
  - Russell Impagliazzo, Leonid A. Levin, Michael Luby: Pseudo-random Generation from one-way functions (Extended Abstracts). STOC 1989
  - 平文とXORと取れば共通鍵暗号になる.
- 一方向性関数が存在すると署名が存在する
  - Moni Naor, Moti Yung: Universal One-Way Hash Functions and their Cryptographic Applications. STOC 1989
- 鍵共有 (公開鍵暗号) を一方向性関数から (ブラックボックス帰着で) 構成することは困難
  - Russell Impagliazzo, Steven Rudich: Limits on the Provable Consequences of One-Way Permutations. STOC 1989

本日の内容（雰囲気）

余談

これらは実現可能性に関する結果

効率的な構成とはまた別

(一方向関数だけで署名作っても非効率)

例：BLS署名 (Ethereum 2.0でサポート)

ペアリング (a.k.a. 双線型写像) を使用

$\sigma=H(m)^{sk}$, $e(\sigma,pk)=?=e(g_1,g_2)$

(注：H(m)は楕円曲線上の点)

公開鍵暗号どころか, IDベース/属性ベース暗号等の

構成に使われるくらい暗号学的に強い道具

本日の内容 (雰囲気)

- 一
-
-

余談2 (暗号屋さん向け内輪ネタ)

BLS署名提案時 [Boneh-Lynn-Shacham@Asiacrypt 2001]
対称ペアリングでの構成 (遅い)

$e: G \times G \rightarrow G_T$

Ethereumの実装では非対称ペアリング
(BLS曲線 (BLS12-381)) を使用 (速い)

$e: G_1 \times G_2 \rightarrow G_T, G_1 \neq G_2$

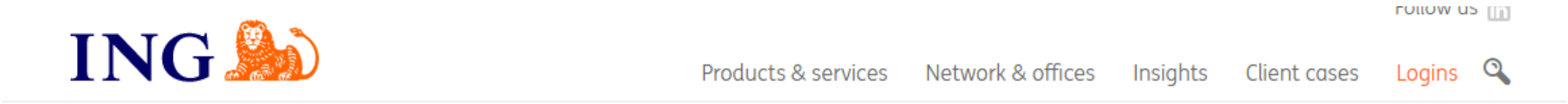
本日の内容 (雰囲気)

- ブロックチェーン＝暗号要素 (公開鍵/共通鍵暗号, 署名, 一方向性関数, 疑似乱数生成器等々) と見たとき何ができるのか？

- 以下の論文を中心に紹介
  - Rishab Goyal, Vipul Goyal: Overcoming Cryptographic Impossibility Results Using Blockchains. TCC 2017 https://eprint.iacr.org/2017/935.pdf

  - ブロックチェーンを用いたゼロ知識証明

ゼロ知識証明（範囲証明）とブロックチェーン

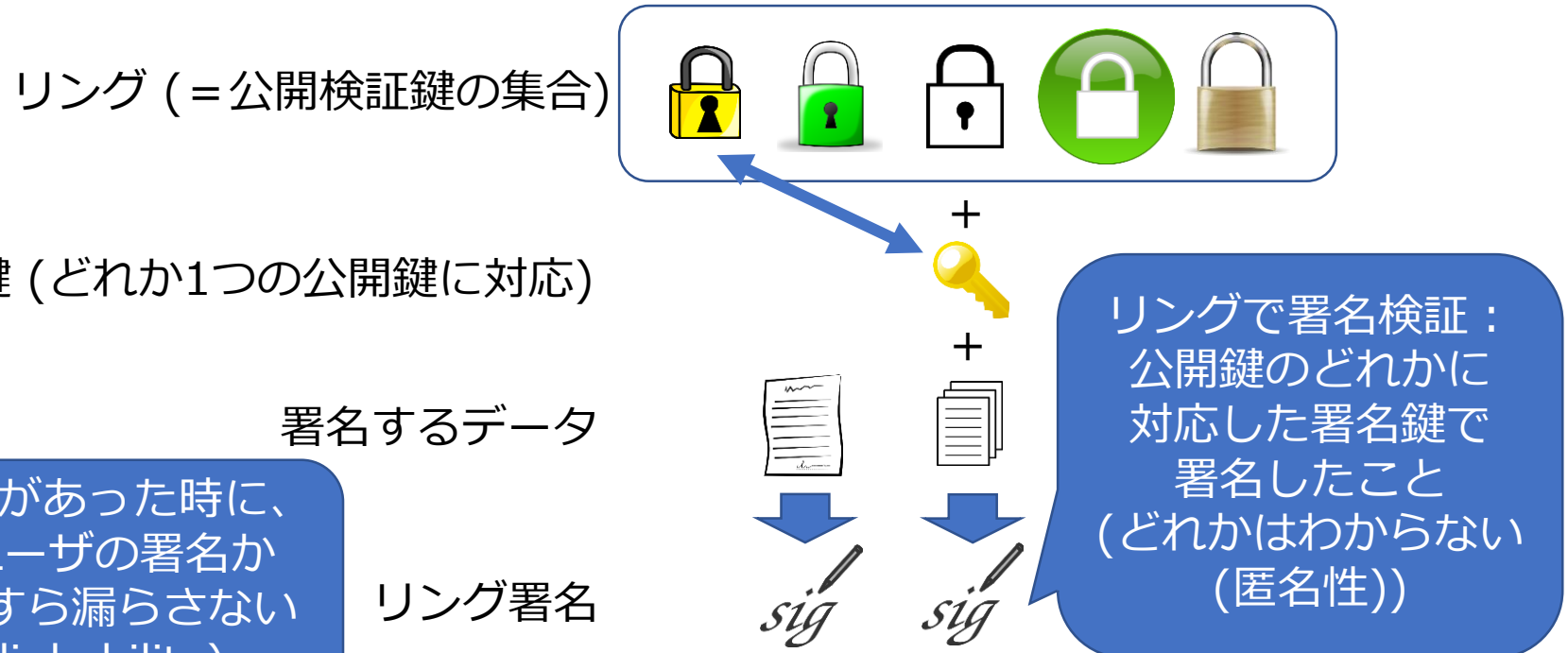


ING launches Zero-Knowledge Range Proof solution, a major addition to blockchain technology

- Prove that their salary sits within a certain range, without revealing the exact figure.
- Prove that a payment amount is within a limit, but it does not show the exact amount.
  - https://www.ingwb.com/themes/distributed-ledger-technology-articles/ing-launches-major-addition-to-blockchain-technology

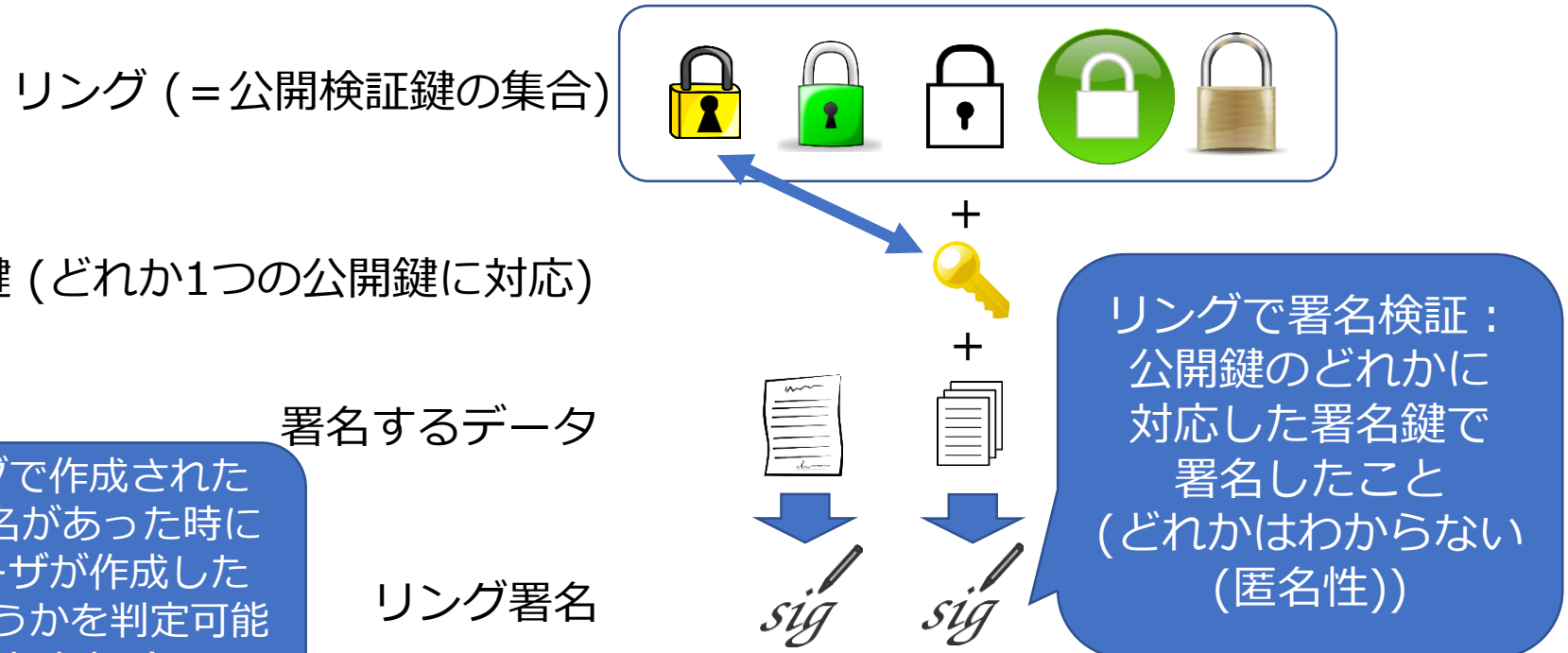
ゼロ知識証明 (所属証明) とブロックチェーン

- リング署名 (Ring Signature)
  - 署名者を明かすことなく, 署名の検証が可能 (Membership proof)
    - Ronald L. Rivest, Adi Shamir, Yael Tauman:
      How to Leak a Secret. ASIACRYPT 2001

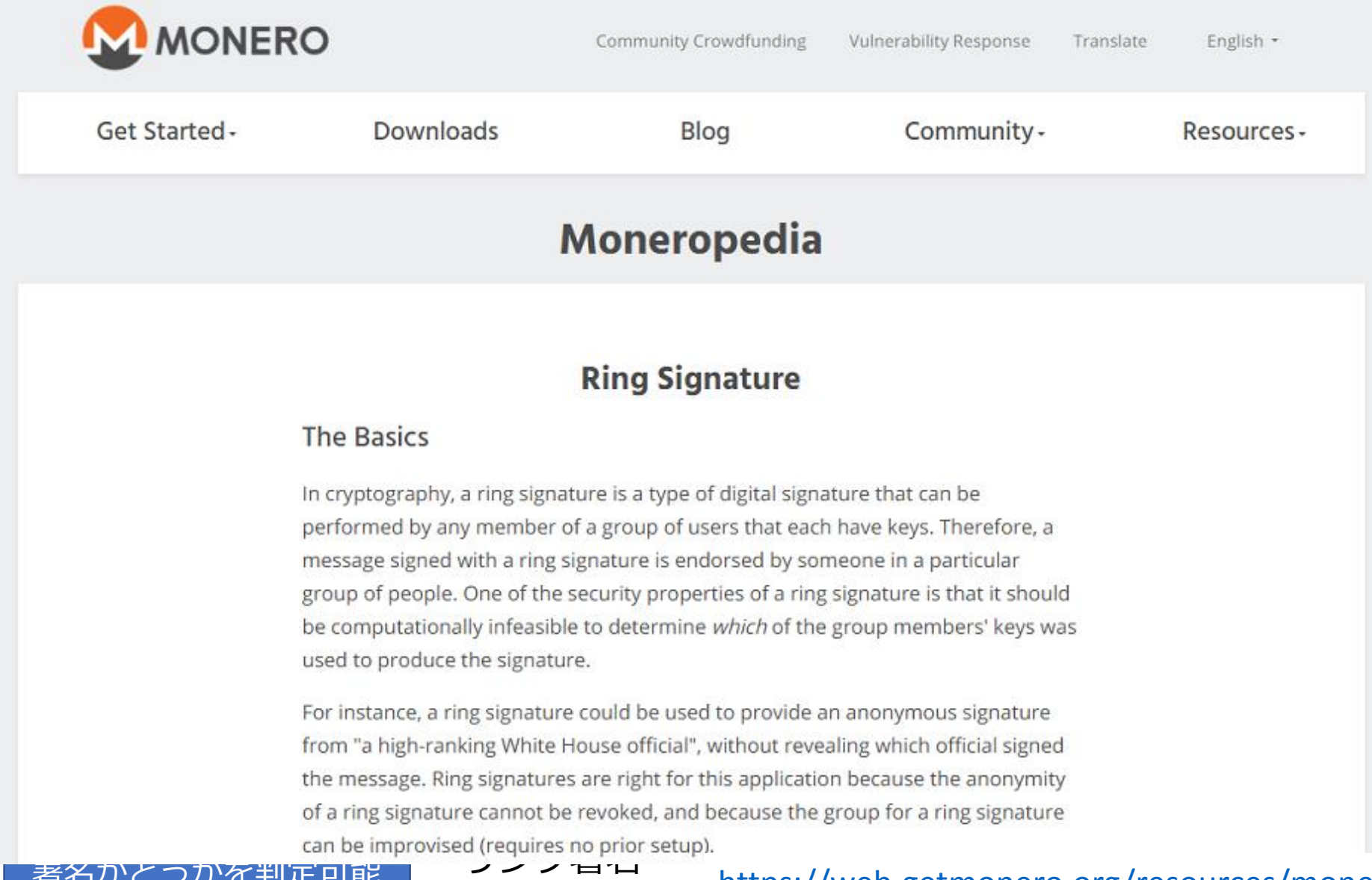


ゼロ知識証明（所属証明）とブロックチェーン

- “Linkable” リング署名
  - 署名者を明かすことなく，署名の検証が可能 (Membership proof)
    - Joseph K. Liu, Victor K. Wei, Duncan S. Wong: Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups (Extended Abstract). ACISP 2004: 325-335



ゼロ知識証明（所属証明）と



署名がどつかを判定可能
(Linkability)

https://web.getmonero.org/resources/moneropedia/ringsignatures.html

非対話ゼロ知識証明 (Non-interactive Zero-Knowledge proof, NIZK)

- (確率的多項式時間攻撃者を考える場合はproof ではなくargument)

$$(\mathcal{K}, \mathcal{P}, \mathcal{V})$$

Keyのようなもの (共通参照情報, Common Reference String: CRS) 生成
Prove (証明): crs, x, w入力, pi 出力
Verify (検証): crs, x, pi入力, 0/1出力

L: NP言語 (Language)

$\omega \in L$: 証拠 (witness)

やりたいことの気持ち
xは公知情報
wは教えないでx=H(w)を
満たすwを知っていることの
証明piを作りたい

Informal example

$$\text{For } x, \text{ define } L \text{ s.t. } \omega \in L \text{ if } H(\omega) = x$$

関係 (Relation) $\mathcal{R}(x, \omega) = 1$

非対話ゼロ知識証明 (Non-interactive Zero-Knowledge proof, NIZK)

Definition 3.4. (NIZK with CRS) A pair of PPT algorithms $(\mathcal{K}, \mathcal{P}, \mathcal{V})$ is a NIZK argument (of knowledge) for a language $\mathcal{L} \in \mathbf{NP}$ with witness relation $\mathcal{R}$ if it satisfies the following conditions:

- (Completeness) For all (x, w) such that $\mathcal{R}(x, w) = 1$, there exists a negligible function $\mathrm{negl}(\cdot)$ such that

$$\Pr[\mathcal{V}(\mathsf{crs}, x, \pi) = 1 : \mathsf{crs} \leftarrow \mathcal{K}(1^\lambda);\ \pi \leftarrow \mathcal{P}(\mathsf{crs}, x, w)] \geq 1 - \mathrm{negl}(\lambda).$$

- (Soundness) For every $x \notin \mathcal{L}$ and all PPT adversaries $\mathcal{A}$, there exists a negligible function $\mathrm{negl}(\cdot)$ such that

$$\Pr[\mathcal{V}(\mathsf{crs}, x, \pi) = 1 : \mathsf{crs} \leftarrow \mathcal{K}(1^\lambda);\ \pi \leftarrow \mathcal{A}(\mathsf{crs}, x)] \leq \mathrm{negl}(\lambda).$$

- (Zero Knowledge) There is a PPT algorithm Sim for the argument system such that for (x, w) subject to $\mathcal{R}(x, w) = 1$, the following holds

$$\{(\mathsf{crs}, \pi) : \mathsf{crs} \leftarrow \mathcal{K}(1^\lambda);\ \pi \leftarrow \mathcal{P}(x, w)\} \approx_c \{\mathsf{Sim}(x)\}$$

[Goyal-Goyal@TCC2017]

非対話ゼロ知識証明 (Non-interactive Zero-Knowledge proof, NIZK)

もしwがxとの関係を満たしていたら

証明piを作成

検証アルゴリズムVが1 (accept) を出力する確率が

crs作成して

ほとんど1

Definiti of PPT algorithms $(\mathcal{K}, \mathcal{P},$ edge)
for a lang ion $\mathcal{R}$ if it satisfies the follow

- (Completeness) For all (x, w) such that $\mathcal{R}(x, w) = 1$, there ... that

$$\Pr[\mathcal{V}(\mathsf{crs}, x, \pi) = 1 : \mathsf{crs} \leftarrow \mathcal{K}(1^\lambda);\ \pi \leftarrow \mathcal{P}(\mathsf{crs}, x, w)] \geq 1 - \mathrm{negl}(\lambda).$$

...ll P... ...ts a negli... ...nction negl(·) such
... = ... $x)] \leq$
...gorithm Sim for the argument system such that for (x, w) subject

...rs $\leftarrow \mathcal{K}(1^\lambda);\ \pi \leftarrow \mathcal{P}(x, w)\} \approx_c \{\mathsf{Sim}(x)\}$

[Goyal-Goyal@TCC2017]

非対話ゼロ知識証明 (Non-interactive Zero-Knowledge proof, NIZK)

Definition 3. PT algorithms $(\mathcal{K}, \mathcal{P}, \mathcal{V})$ is a NIZK argument (of knowledge) for a language if it satisfies the following conditions:

- (Comple $x, w) = 1$, there exists a negligible function $\text{negl}(\cdot)$ such that $\leftarrow \mathcal{K}(1^\lambda);\ \pi \leftarrow \mathcal{P}(c$

- (Soundness) For every $x \notin \mathcal{L}$ and all PPT adversaries $\mathcal{A}$, th $(\cdot)$ such that

$$\Pr[\mathcal{V}(\mathsf{crs}, x, \pi) = 1 : \mathsf{crs} \leftarrow \mathcal{K}(1^\lambda);\ \pi \leftarrow \mathcal{A}(\mathsf{crs}, x)] \leq \text{negl}(\lambda).$$

algo system that for (x, w) subject

crs {Si

でもxは言語に入っていない

攻撃者Aが証明piを作成

検証アルゴリズムVが1 (accept) を出力する確率は

crs作成して

ほとんど 0

[Goyal-Goyal@TCC2017]

非対話ゼロ知識証明 (Non-interactive Zero-Knowledge proof, NIZK)

wを知っていて作成した
piと識別できない
(分布の) ものを作ることができる
(= piからwの情報は漏れない:ゼロ知識)

シミュレータが存在して

rithms $(\mathcal{K}, \mathcal{P}, \mathcal{V})$ is a NIZK argument (of knowledge)
sfies the following conditions:

1,

; π

ies $\mathcal{A}$, ther egligible function $\mathrm{negl}(\cdot)$ such

$1^\lambda)$: $\mathcal{A}(\mathsf{crs}, x)] \leq \mathrm{negl}(\lambda)$.

for the argument system such that for (x, w) subject

$$\{(\mathsf{crs}, \pi) : \mathsf{crs} \leftarrow \mathcal{K}(1^\lambda);\ \pi \leftarrow \mathcal{P}(x, w)\} \approx_c \{\mathsf{Sim}(x)\}$$

wは知らないんだけども

非対話ゼロ知識証明 (Non-interactive Zero-Knowledge proof, NIZK)

- Witness indistinguishability (WI)
  - Zero-knowledgeより弱い概念
  - CRSいらない
  - 気持ち：witnessがw1とw2と複数存在したとき, どちらのwitnessを使用したのかがpiから漏れない

- (Witness Indistinguishability) For any sequence $\mathcal{I} = \{(x, w_1, w_2) : \mathcal{R}(x, w_1) = 1 \wedge \mathcal{R}(x, w_2) = 1\}$

$$\{\pi_1 : \pi_1 \leftarrow \mathcal{P}(x, w_1)\}_{(x,w_1,w_2)\in\mathcal{I}} \approx_c \{\pi_2 : \pi_2 \leftarrow \mathcal{P}(x, w_2)\}_{(x,w_1,w_2)\in\mathcal{I}}$$

[Goyal-Goyal@TCC2017]

非対話ゼロ知識証明 (Non-interactive Zero-Knowledge proof, NIZK)

- Witness indistinguishability (WI)
  - Zero-knowledgeより弱い概念
  - CRSいらない

証拠が2つ (w1とw2)

w1で作成したpiと

- (Witness Indistinguishability) For any sequence $\mathcal{I} = \{(x, w_1, w_2) : \mathcal{R}(x, w_1) = 1 \wedge \mathcal{R}(x, w_2) = 1\}$

$$\{\pi_1 : \pi_1 \leftarrow \mathcal{P}(x, w_1)\}_{(x,w_1,w_2)\in\mathcal{I}} \approx_c \{\pi_2 : \pi_2 \leftarrow \mathcal{P}(x, w_2)\}_{(x,w_1,w_2)\in\mathcal{I}}$$

識別不可能

w2で作成したpiとが

Overcoming Cryptographic Impossibility Results Using Blockchains [Goyal-Goyal@TCC2017]

- 非対話ゼロ知識証明 (Non-interactive Zero-Knowledge proof, NIZK)
- 共通参照情報 (Common Reference String, CRS) が正直に生成される仮定 (Trusted Setup)
  - Setup仮定なしだと言語がBPPに制限される [Ore87, GO94, GK96]
  - (今回はランダムオラクルは考えない)
- 誰がCRSを作るのか問題
  - 特に非中央集権の場合
  - 各参加者がそれぞれCRSを作成し, 参加者の大半が正直であると仮定するmulti-CRSモデル [GO07].
    - [GO07] Jens Groth and Rafail Ostrovsky. Cryptography in the multi-string model. In CRYPTO, volume 4622 of Lecture Notes in Computer Science, pages 323–341, 2007.

Overcoming Cryptographic Impossibility Results Using Blockchains
[Goyal-Goyal@TCC2017]

- ものすごくざっくりとした説明 (詳細は論文参照)
- 証明者はブロックチェーンB (=crs) に対し以下を証明

$\omega \in L$ OR BがForkしたブロックチェーンが存在する

$$c_1 = \mathsf{Commitment}(\omega)$$
$$c_2 = \mathsf{Commitment}(f)\ (f \text{ is all zeros with the length } |\omega|)$$

NIWI argument:

c1は w in L に対するwitness wのコミットメントである, or
c2はBがforkした十分長いブロックチェーンのコミットメントである

Overcoming Cryptographic Impossibility Results Using Blockchains
[Goyal-Goyal@TCC2017]

- ものすごくざっくりとした説明 (詳細は論文参照)
- 証明者はブロックチェーン B に対し以下を証明

$$\omega \in L$$

ーン

コミットメントなので, c1とc2からはwやfの情報は漏れない

$$c_1 = \mathsf{Commitment}(\omega)$$
$$c_2 = \mathsf{Commitment}(f)\ (f \text{ is all zeros with the length } |\omega|)$$

NIWI argument:

c1は w in L に対するwitness wのコミットメントである, or
c2はBがforkした十分長いブロックチェーンのコミットメントである

Overcoming Cryptographic Impossibility Results Using Blockchains
[Goyal-Goyal@TCC2017]

- ものすごくざっくりとした説明 (詳細は論文参照)
- 証明者はブロックチェーンB (=crs) に対し以下を証明

$w \in L$ OR BがForkしたブロックチェーン

$c_1 =$

$c_2 =$

ちゃんと証拠wを知っているのであれば,
OR関係の片側は常に成り立つので証明が通る (Completeness)

NIWI argument:

c1は w in L に対するwitness wのコミットメントである, or
c2はBがforkした十分長いブロックチェーンのコミットメントである

Overcoming Cryptographic Impossibility Results Using Blockchains
[Goyal-Goyal@TCC2017]

- ものすごくざっくりとした説明 (詳細は論文参照)
- 証明者はブロックチェーンB (=crs) に対し以下を証明

ーン

攻撃者がもつstakeがMinority であると仮定, wを知らない場合にforkを作成することはできない (Soundness)

NIWI argument:

c1は w in L に対するwitness wのコミットメントである, or
c2はBがforkした十分長いブロックチェーンのコミットメントである

Overcoming Cryptographic Impossibility Results Using Blockchains
[Goyal-Goyal@TCC2017]

- ものすごくざっくりとした説明 (詳細は論文参照)
- 証明者はブロックチェーンB (=crs) に対し以下を証明

ーン

シミュレータはMajorityである正直な参加者 (＝攻撃者ではない) を利用してforkを作成すれば, 検証に通るpiを “wを知らなくても” 作成できる (Zero-Knowledge)

NIWI argument:

c1は w in L に対するwitness wのコミットメントである, or
c2はBがforkした十分長いブロックチェーンのコミットメントである

最後に

- 本講演では, ブロックチェーンを暗号要素の一つとして見た場合, 構成可能性/不可能性の研究においてどのような結果が示されているのかを簡単に紹介した.

- ブロックチェーンを使ったとしてもこういうことはできないという不可能性の結果？