Logical system with negligible probability

Takeuti Izumi
7 March 2015

Formalisation of proofs

– Academic significance

Not to prove a new theorem

To analyse the proof

To clarify the essence of inferences

– Industrial significance

Not to provide a new cryptgraphic function

To make the proof less mistaken and more dependable

To make the proof machine-checkable

To enable the proof to be circulated in non-mathematicians

The notion of 'negligibly small probability' often occurs in arguments of cryptograhpy.

For instance:

1. The difference of the probabilities of X and Y is negligibly small.
2. The difference of the probabilities of Y and Z is also negligibly small.
3. Therefore, the difference of the probabilities of X and Z is also negligibly small.

Formal definition of negligibly small probability:

A value ϵ depending on the security parameter is *negligibly small* iff for any positive polynomial $p(\ )$, there is a number N such that for any security parameter $n > N$, it holds $\epsilon < 1/p(n)$.

The argument with negligibly small probability is often like the following:

1. Put an arbitray polynomial $p(\ )$.
2. $|\,\mathbf{Pr}[X] - \mathbf{Pr}[Y]| < 1/2p(n)$ for large n.
3. Also $|\,\mathbf{Pr}[Y] - \mathbf{Pr}[Z]| < 1/2p(n)$ for large n.
4. Hence $|\,\mathbf{Pr}[X] - \mathbf{Pr}[Z]| < 1/p(n)$ for large n.
5. Therefore the difference of probabilities $|\,\mathbf{Pr}[X] - \mathbf{Pr}[Z]|$ is negligibly small.

This argument uses a method of mathematical analysis.

A method of mathematical analysis is not easy.

It sometimes induces mistakes in proofs.

A method of symbolic processing is better than it.

Negligible probability ofren appear in the following form:

'$|\mathbf{Pr}[\boldsymbol{P}] - \mathbf{1/2}|$ is negligibly small.'

We regard this as a modality for $\boldsymbol{P}$.

We propose a formal logical system with this modality,
and prove a useful theorem in the formal system.

Aim: To propose a logical system with negligible probability
which proves privacy in Kawamoto voting protocol

All the other systems deal with only rigid probabilities.

Thus they can formalise the discussion below:

1. $\mathbf{Pr}[\boldsymbol{X}]$ is exactly equal to $\mathbf{Pr}[\boldsymbol{Y}]$.
2. $\mathbf{Pr}[\boldsymbol{Y}]$ is exactly equal to $\mathbf{Pr}[\boldsymbol{Z}]$.
3. Therefore, $\mathbf{Pr}[\boldsymbol{X}]$ is exactly equal to $\mathbf{Pr}[\boldsymbol{Z}]$.

On the other hand, they cannot formalise the following discussion:

1. $\mathbf{Pr}[\boldsymbol{X}]$ is close to $\mathbf{Pr}[\boldsymbol{Y}]$.
2. $\mathbf{Pr}[\boldsymbol{Y}]$ is close to $\mathbf{Pr}[\boldsymbol{Z}]$.
3. Therefore, $\mathbf{Pr}[\boldsymbol{X}]$ is close to $\mathbf{Pr}[\boldsymbol{Z}]$.

Our system can formalise this discussion.

$\mathbf{2} = \{0, 1\}$, $\mathbf{2}^* = \cup_{n=0}^{\infty} \mathbf{2}^n$, $\mathbf{2}^{<n} = \{x \in \mathbf{2}^* | \; |x| < n\}$,

$(\,) \in \mathbf{2}^0$ denotes the empty word.

$1^n \in \mathbf{2}^n$ denots a sequence of 1 of length n.

$0^n \in \mathbf{2}^n$ denots a sequence of 0 of length n.

$x \in \mathbf{2}^m \subset \mathbf{2}^{<n}$ is encoded as $\phi_n(x) = x \; 1 \; 0^{n-m-1} \in \mathbf{2}^n$

$y \in \mathbf{2}^n$ is decoded as $\psi_n(y) = x \in \mathbf{2}^m$ for $y = x \; 1 \; 0^{n-m-1}$,

and $\psi_n(y) = (\,)$ for $y = 0^n$

For a PTIME function f over $\mathbf{2}^*$, the following holds.

There is polynomials p and q such that,

for each positive integer n,

there is a sequnce of logical circuites $C_1, C_2, ..., C_{q(n)}$ such that,

the size of C_i is less than $p(n)$ for each $i = 1, 2, ..., q(n)$,

and

for any $x \in \mathbf{2}^{<n}$,

$$f(x) = \psi_{q(n)}(C_1(\phi_n(x))C_2(\phi_n(x))...C_{q(n)}(\phi_n(x)) \in \mathbf{2}^{<q(n)}$$

$Circ_{n_1,n_2,...,n_k}(...)$ is an emulator of circuit, that is:

Let C be a circuit, and $c \in 2^*$ be the code of C.

For any $x_1 \in 2^{<n_1}, x_2 \in 2^{<n_2}, ..., x_k \in 2^{<n_k}$,

$$Circ_{n_1,n_2,...,n_k}(c, x_1, x_2, ..., x_k) = C(\phi_{n_1}(x_1)\phi_{n_2}(x_2)...\phi_{n_k}(x_k))$$

The code c of a circuit C is as large as a polynomial of the size of C.

$Circ_{...}(\ )$ is a PTIME function.

There are PTIME functions f, f', f'' such that

$$Circ_{...}(f(c), x, y) = Circ_{...}(c, y),$$

$$Circ_{...}(f'(c, y), x) = Circ_{...}(c, x, y).$$

$$Circ_{...}(f''(c), x, y) = Circ_{...}(c, y, x).$$

Encryption Scheme (G^E, G^D, E, D):

– $G^E(x, y)$: encryption key of seed x and nonce y.

– $G^D(x, y)$: the decryption key for $G^E(x, y)$.

– $E(x, y, z)$: encryption function with key x, message y and nonce z.

– $D(x, y)$: decryption function with key x from encrypted message y.

G^E, G^D, E and D are functions over 2^* such that

$$D(G^D(s, r), E(G^E(s, r), m, r')) = m.$$

When nonces are regarded as probabilistic variables,

these G^E, G^D, E and D are regarded as probabilistic algorithm.

An encryption scheme (G^E, G^D, E, D) is
a *Encryption Scheme with Bound* p iff

– All of G^E, G^D, E, D are PTIME functions over 2^*.

– p is a polynomial.

– The computation times of $G^E(x, y)$, $G^D(x, y)$ and $D(x, y)$ are bounded by $p(|x|)$ independently to y.

– The computation time of $E(x, y, z)$ is bounded by $p(\max(|x|, |y|))$ independently to z.

– There is a PTIME function f over 2^* such that the computation time of $f(x, y, z)$ is bounded by

$$p(\max(|x|, |y|, |z|)),$$

and that
for any $c \in 2^*$, $s, m, r, r' \in 2^{<n}$, $x \in 2^{<p(n)}$,

$$Circ_{n,p(n),p^2(n),p^2(n)}(c, G^E(s, r), E(G^E(s, r), m, r'), x) = Circ_{p(n),p^2(n)}(f(c, m, r'), G^E(s, r), x)$$

An encription scheme (G^E, G^D, E, D) with bound p has *indistinguishable encryption*, or is *ciphertext-indistinguishable*, iff

for any positive polynomials q, q', q'' where $q'(n) \geq n$,
for any sequence $\{c_1, c_2, c_3, ...\}$ where $|c_n| < q''(n)$,
there is a number N such that,
for any $u > N$, for any $x_1, x_0 \in 2^{<q'(u)}$,

$$\#\{(i, r, r') \in 2 \times 2^{<p(u)} \times 2^{<p(q'(u))} | \\ i = Circ(c_u, G^E(1^u, r), E(G^E(1^u, r), x_i, r'))\} \\ < (1/2 \ + \ 1/q(u)) \cdot \#(2 \times 2^{<p(u)} \times 2^{<p(q'(u))})$$

Kawamoto Voting Protocol

$$\begin{array}{rcl}
 & A & \\
e_{A1} = E(k_{V1}, s_{A1}, n_{A1}) & \swarrow \ \searrow & e_{A2} = E(k_{V2}, s_{A2}, n_{A2}) \\
 & & \\
\begin{array}{r} s_{A1} = D(k_{V1}^{-1}, e_{A1}) \\ e_1 = E(k_C, \langle v_1, s_{A1} \rangle, n_1) \end{array} & V_1 \qquad V_2 & \begin{array}{l} s_{A2} = D(k_{V2}^{-1}, e_{A2}) \\ e_2 = E(k_C, \langle v_2, s_{A2} \rangle, n_2) \end{array} \\
 & & \\
e_1' = E(k_{MIX}, e_1, n_1') & \searrow \ \swarrow & e_2' = E(k_{MIX}, e_2, n_2',) \\
 & MIX & \\
e_1 = D(k_{MIX}^{-1}, e_1') & \downarrow\downarrow & e_2 = D(k_{MIX}^{-1}, e_2') \\
 & C & \\
v_1 = left(D(k_C^{-1}, e_1)) & \downarrow\downarrow & v_2 = left(D(k_C^{-1}, e_2)) \\
 & BB &
\end{array}$$

Suppose that the intruder can look at both encrypted messages, but cannot send any message of identity fraud.

The privacy of that votes is provided by the indistingushability of $E(k_{MIX}, e_1, n'_1)$ from $E(k_{MIX}, e_2, n'_2)$.

That is formalised into that:

for any positive polynomials q, q', q'' where $q'(n) \geq n$,

for any sequence $\{c_1, c_2, c_3, ...\}$ where $|c_n| < q''(n)$,

there is a number N such that,

for any $u > N$, for any $x_1, x_0 \in 2^{<q'(u)}$,

$$\begin{aligned}
&\#\{(i, r, r_0, r_1) \in 2 \times 2^{<p(u)} \times (2^{<p(q'(u))})^2 | \\
&\quad i = Circ(c_u, G^E(1^u, r), \\
&\qquad\qquad E(G^E(1^u, r), x_i, r_i), E(G^E(1^u, r), x_{1-i}, r_{1-i}))\} \\
&< (1/2 \ + \ 1/q(u)) \cdot \#(2 \times 2^{<p(u)} \times (2^{<p(q'(u))})^2)
\end{aligned}$$

Informal proof — Hybid argument

Each line is indisdinguishable to the next:

$$Circ(c_u, G^E(1^u, r), E(G^E(1^u, r), x_1, r_1), E(G^E(1^u, r), x_0, r_0))$$

$$Circ(c_u, G^E(1^u, r), E(G^E(1^u, r), x', r'), E(G^E(1^u, r), x_0, r_0))$$

$$Circ(c_u, G^E(1^u, r), E(G^E(1^u, r), x', r'), E(G^E(1^u, r), x_1, r_1))$$

$$Circ(c_u, G^E(1^u, r), E(G^E(1^u, r), x_0, r_0), E(G^E(1^u, r), x_1, r_1))$$

The target is to formalise this proof.

Algebra

Types: $\mathbf{b} \subset \mathbf{p}^0 \subset \mathbf{p}^1 \subset \mathbf{p}^2 \subset ...$

Denotation of Types :

$$D_u(\mathbf{b}) = 2,\ D_u(\mathbf{p}^0) = 2^{<u},\ D_u(\mathbf{p}^1) = 2^{<p(u)},$$
$$D_u(\mathbf{p}^2) = 2^{<p(p(u))},\ D_u(\mathbf{p}^3) = 2^{<p(p(p(u)))}, ...,$$
$$D_u(\mathbf{p}^n) = 2^{<p^n(u)}, ...$$

where u is the security parameter and p is the bounding polynomial.

Bivalent algebra

Constants and function symbols:

$$\mathbf{0} : \mathbf{b},\ \mathbf{1} : \mathbf{b},\ \sqcap : \mathbf{b} \times \mathbf{b} \to \mathbf{b},\ \oplus : \mathbf{b} \times \mathbf{b} \to \mathbf{b},$$

$$\mathbf{cond} : \mathbf{b} \times \boldsymbol{\tau} \times \boldsymbol{\tau} \to \boldsymbol{\tau}.$$

Rules:

$(\mathbf{0},\ \mathbf{1},\ \sqcap,\ \oplus)$ is a Boolean ring.

(Bivalance) $\mathbf{1} \neq \mathbf{0}$. Either $\boldsymbol{t} = \mathbf{0}$ or $\boldsymbol{t} = \mathbf{1}$ for $\boldsymbol{t} : \mathbf{b}$.

$$\mathbf{cond}(1, \boldsymbol{t}, \boldsymbol{u}) = \boldsymbol{t},\ \mathbf{cond}(0, \boldsymbol{t}, \boldsymbol{u}) = \boldsymbol{u}.$$

Cryptographic algebra

Function symbols:

$$\mathbf{ge}, \mathbf{gd} : \mathbf{p}^0 \times \mathbf{p}^1 \to \mathbf{p}^1$$

$$\mathbf{enc} : \mathbf{p}^1 \times \mathbf{p}^n \times \mathbf{p}^{n+1} \to \mathbf{p}^{n+1},\ \mathbf{dec} : \mathbf{p}^1 \times \mathbf{p}^{n+1} \to \mathbf{p}^n$$

Rules: $\mathbf{dec}(\mathbf{gd}(\boldsymbol{x}, \boldsymbol{y}), \mathbf{enc}(\mathbf{ge}(\boldsymbol{x}, \boldsymbol{y}), \boldsymbol{m}, \boldsymbol{n})) = \boldsymbol{m}$

Circuit Algebra

Function symbol: **circ** $: \tau \times ... \times \tau' \to$ **b**

Semantics: $[\![\mathbf{circ}(c, x_1, ..., x_n)]\!] = Circ(c, x_1 x_2 ... x_n)$

Rules:

– For $c : \mathbf{p}^n$, there is $c' : \mathbf{p}^{n+1}$ depending only on c such that

$$\mathbf{circ}(c', x_1, .., x_n) = \mathbf{circ}(c, x_{i(1)}, ..., x_{i(n)})$$

where $(i(1), ..., i(n))$ is a permutation of $(1, ..., n)$

– For $c, y : \mathbf{p}^n$, there is $c' : \mathbf{p}^{n+1}$ depending only on c, y and r such that

$$\mathbf{circ}(c', k, x) = \mathbf{circ}(c, k, x, \mathbf{enc}(k, y, r))$$

Syntax

Variables: V^τ for each type τ, $V = \coprod_\tau V^\tau$: a finite set.

All variable are regarded as probabilistic variables.

A non-probabilistic variable x is regarded as a probabilisitic variable such that $\mathbf{Pr}[x = c] = 1$ for some constant value c.

If the value of a variable x is determined to be 1 or 0

in a nondeterministic process,

then, we regard that either $\mathbf{Pr}[x = 1] = 1$ or $\mathbf{Pr}[x = 0] = 1$,

which is determined nondeterministically

Function symbols: The constants and function symbols of algebras.

Terms: constucted with variables and functoin symbols.

Unmodalled formulae: $F^U ::= \; t = u | \neg F^U | F^U \wedge F^U | \forall v F^U$

Modalled formulae:

$$F^M ::= \; \mathsf{N}(t; t_1, t_2, ..., t_n) | \oslash F^U | \Box F^U | \neg F^M | F^M \wedge F^M | \forall v F^M$$

where t and u are terms and $v \in V$.

$\mathsf{N}(t; t_1, t_2, ..., t_n)$: The proabilistic distributions of t is even and independent to those of $t_1, t_2, ..., t_n$.

$\oslash F$: The diffenece between 1/2 and the probability of F is negligible.

$\Box F$: The probability of F is equal to 1.

Abbrebiations:

$$t \sqcup u \equiv t \oplus u \oplus t \sqcap u, \; {\sim} t \equiv 1 \oplus t,$$

$$\mathsf{N}(t_1, t_2, ..., t_n; t'_1, t'_2, ..., t'_m) \equiv$$
$$\mathsf{N}(t_1; t_2, ..., t_n, t'_1, ..., t'_m) \wedge \mathsf{N}(t_2, t_3, ..., t_n; t'_1, ..., t'_m)$$
$$(n \geq 2),$$

$$F \supset G \equiv \neg(F \wedge \neg G), \; F \vee G \equiv \neg F \supset G,$$

$$F \supset\subset G \equiv (F \supset G) \wedge (G \supset F),$$

$$\exists x F \equiv \neg \forall x \neg F$$

The strength of connetive powers is in the order:

$$\neg, \; \forall, \; \exists, \; \oslash, \; \Box, \; \wedge, \; \vee, \; \supset, \; \supset\subset.$$

Semantics

An asignment w and a distribution μ

of parameter u and bounding polynomial p

For a type τ, $D_u(\tau)$ is defined as: $D_u(\mathsf{b}) = 2,\ D_u(\mathsf{p}^n) = 2^{<p^n(u)}$.

$w \in W_u = \{w : \prod_\tau V^\tau \to D_u(\tau)\}$. Note that W_u is finite.

$\mu : W_u \to [0,1],\ \sum_{w \in W_u} \mu(w) = 1$

We extend the domain of μ into the power set of W_u as:

$\mu(E) = \sum_{w \in E} \mu(w)$ for $E \subset W_u$.

A model M of polynomial p is

an infinite sequence $M = (\mu_1, \mu_2, \mu_3, \ldots)$

where μ_i is a distribution of parameter u_i and bounding polynomial p

for an incleasing sequence of integers $u_1 < u_2 < u_3 < \ldots$

For $v \in V^\tau,\ e \in D_u(\tau)$, and $w \in W_u$,

the notation $w[e/v] \in W_u$ is defined as

$w[e/v](v) = e$ and $w[e/v](v') = w(v')$ for $v' \neq v$

For $v \in V$ and $w, w' \in W_u$, the relation $w \sim_v w'$ is defined as

$w = w'[w(v)/v]$

For $v \in V^\tau$ and $\mu, \mu' : W_u \to [0, 1]$,

the relation $\mu \sim_v \mu'$ is defined as, for any $w \in D_u$,

$\sum_{e \in D_u(\tau)} \mu(w[e/v]) = \sum_{e \in D_u(\tau)} \mu'(w[e/v])$

that is, $\mu(\{\omega | \omega \sim_v w\}) = \mu'(\{\omega | \omega \sim_v w\})$

$\sim_v$ denotes the relation that two behave the same except for v

For $M = (\mu_1, \mu_2, ...)$ and $M' = (\mu'_1, \mu'_2, ...)$

$M \sim_v M' \iff$ for any i, $\mu_i \sim_v \mu_i$

Lemma $\sim_v$ is an equivalence relation.

Lemma For $v, v' \in V$ and $\mu_1, \mu_2 : W_u \to [0, 1]$,

if $\mu_1 \sim_v \mu_3 \sim_{v'} \mu_2$ for some μ_3,

then $\mu_1 \sim_{v'} \mu_4 \sim_v \mu_2$ for some μ_4.

Put an encryption scheme $S = (G^E, G^D, E, D)$

Function sysmbols **ge**, **gd**, **enc** and **dec** are interpreted into G^E, G^D, E and D.

Other constants and function symbols are interpreted in the standard way.

For a term $t : \tau$ and $w \in D_u$,
the interpretation $[\![t]\!](w) \in D_u(\tau)$ is defined in the usual way.

The interpretation of an unmodalled formula

$$w \models F^U$$

is defined as follows, where $w \in W_u = \prod_\tau V^\tau \to D_u(\tau)$

$$w \models t = t' \iff [\![t]\!](w) = [\![t']\!](w)$$

$$w \models \neg F \iff w \not\models F$$

$$w \models F \wedge G \iff w \models F \ \&\ w \models G$$

$$w \models \forall x F \iff w' \models F \text{ for any } w' \sim_x w$$

The interpretation of a modalled formula

$$M \models F^M$$

is defined as follows, where $M = (\mu_1, \mu_2, ...)$ is a model:

$$M \models \neg F \iff M \not\models F$$

$$M \models F \wedge G \iff M \models F \,\&\, M \models G$$

$$M \models \forall x F \iff M' \models F \text{ for any } M' \sim_x M$$

$M \models \mathsf{N}(t; t', t'', ...) \iff$

For any j, the following holds:

Let $\tau, \tau', \tau''...$ be the types of $t, t', t'', ...$.

For any $e \in D_{u_j}(\tau), e' \in D_{u_j}(\tau'), e'' \in D_{u_j}(\tau''), ...,$

$$\mu_j(\{\omega \in W_{u_j} | [\![t]\!](\omega) = e, [\![t']\!](\omega) = e', [\![t'']\!](\omega) = e'', ...\})$$
$$= (1/\#D_{u_j}(\tau)) \cdot \mu_j(\{\omega \in W_{u_j} | [\![t']\!](\omega) = e', [\![t'']\!](\omega) = e'', ...\})$$

$M \models \oslash F \iff$

for any polynomial $q(\ )$,

there is an integer N such that,

for any $j \geq N$,

$$\left| \mu_j(\{w \in W_{u_j} | w \models F\}) - 1/2 \right| < 1/q(j).$$

$M \models \Box F \iff$

for any j and any $w \in W_{u_j}$, $w \models F$.

$S \models F \iff$

$M \models F$ for any M

where the function symbols $\mathbf{ge}, \mathbf{gd}, \mathbf{enc}, \mathbf{dec}$ are interpreted into S.

Axioms

Detachment: $\boldsymbol{F} \supset \boldsymbol{G},\ \boldsymbol{F} \vdash \boldsymbol{G}$.

Generalisation: $\boldsymbol{F} \vdash \forall \boldsymbol{x} \boldsymbol{F}$.

Substitution: $\boldsymbol{t} = \boldsymbol{t}' \vdash \boldsymbol{F}^{\boldsymbol{M}}[\boldsymbol{t}/\boldsymbol{x}] \supset \boldsymbol{F}^{\boldsymbol{M}}[\boldsymbol{t}'/\boldsymbol{x}]$.

Necessity: $\boldsymbol{F}^{\boldsymbol{U}} \vdash \Box \boldsymbol{F}^{\boldsymbol{U}}$.

Variable generation: $\mathsf{N}(\boldsymbol{x}; \boldsymbol{x}_1, \boldsymbol{x}_2, ..., \boldsymbol{x}_n) \supset \boldsymbol{F}^{\boldsymbol{M}} \vdash \boldsymbol{F}^{\boldsymbol{M}}$,

where all the probabilistic variables in $\boldsymbol{F}^{\boldsymbol{M}}$ are listed in $\boldsymbol{x}_1, \boldsymbol{x}_2, ..., \boldsymbol{x}_n$.

Initial formulae:

Tautologyes,

Axioms on equation: $\boldsymbol{t} = \boldsymbol{t}$,,

$\boldsymbol{t} = \boldsymbol{t}' \supset \boldsymbol{F}^{\boldsymbol{U}}[\boldsymbol{t}/\boldsymbol{x}] \supset \boldsymbol{F}^{\boldsymbol{U}}[\boldsymbol{t}'/\boldsymbol{x}]$,

Axioms on quantification:

$\forall \boldsymbol{x}(\boldsymbol{F} \supset \boldsymbol{G}) \supset \boldsymbol{F} \supset \forall \boldsymbol{x} \boldsymbol{G}$, where $\boldsymbol{x}$ does not appear in $\boldsymbol{F}$,

$\forall \boldsymbol{x} \boldsymbol{F} \supset \boldsymbol{F}[\boldsymbol{t}/\boldsymbol{x}]$.

Initial formulae:

Rules of algebras, where we formalise informal rules such as bivalence.

Dependencies are descripted as follows:

$$\mathsf{N}(y_1, y_2, ..., y_m; c, x_1, x_2, ..., x_n, z_1, z_2, ..., z_l) \supset$$
$$\exists c'.\ \mathsf{N}(y_1, y_2, ..., y_m; c, c', x_1, x_2, ..., x_m, z_1, z_2, ..., z_l)$$
$$\wedge\ \mathsf{circ}(c, x_1, x_2, ..., x_n) = \mathsf{circ}(c', x_{i_1}, x_{i_2}, ..., x_{i_n})$$

Where $(i_1, i_2, ..., i_n)$ is a permutation of $(1, 2, ..., n)$

Initial formulae:

And that,

$$\mathsf{N}(z_1, ..., z_l; c, x_1, ..., x_m, y_1, ..., y_n, r, z'_1, ..., z'_k) \supset$$
$$\exists c'.\ \mathsf{N}(z_1, ..., z_l; c, c', x_1, ..., x_m, y_1, ..., y_n, r, z'_1, ..., z'_k)$$
$$\wedge \forall kx.\ \mathsf{circ}(c', x_1, ..., x_m) = \mathsf{circ}(c, x_1, ..., x_m, y_1, ..., y_n)$$

$$\mathsf{N}(z_1, z_2, ..., z_l; c, y, r, z'_1, z'_2, ..., z'_m) \supset$$
$$\exists c'.\ \mathsf{N}(z_1, z_2, ..., z_l; c, c', y, r, z'_1, z'_2, ..., z'_m)$$
$$\wedge\ \forall kx.\ \mathsf{circ}(c', k, x) = \mathsf{circ}(c, k, x, \mathsf{enc}(k, y, r))$$

Initial formulae:

Rules on independence:

$$\mathsf{N}(t; t_1, t_2, ..., t_n) \supset \mathsf{N}(t; t_{i_1}, t_{i_2}, ..., t_{i_n}),$$

where $\{i_1, i_2, ..., i_n\} \subset \{1, 2, ..., n\}$.

$$\mathsf{N}(t; t', t_1, t_2, ..., t_n) \supset \mathsf{N}(t'; t_1, t_2, ..., t_n) \supset \mathsf{N}(t'; t, t_1, t_2, ..., t_n)$$

Initial formulae:

Rules on Probability:

$$\Box(F \supset G) \supset \Box F \supset \Box G$$

$$\Box(F \supset\subset G) \supset \oslash F \supset \oslash G$$

Calculation of probability:

$$\mathsf{N}(i; t, u) \supset (\oslash\, 1 = \mathbf{cond}(i, t, u) \supset\subset \oslash\, 1 = \mathbf{cond}(i, t \sqcup u, t \sqcap u)),$$

$$\mathsf{N}(i; t) \supset \mathsf{N}(i; u) \supset \oslash\, 1 = u \supset (\oslash\, 1 = t \supset\subset \oslash\, 1 = \mathbf{cond}(i, t, u)).$$

Soundness

This axiomatic system is sound for the semantices.

It seems that this system is incomplete,
becasue the system mentions nothing on the behaviour of **circc**( ).
The system which proves useful theorems is useful,
even if it is not complete.

The proof of privacy of Kawamoto protocol

The follwoings are equivalent:

– $\boldsymbol{S} = (\boldsymbol{G^E}, \boldsymbol{G^D}, \boldsymbol{E}, \boldsymbol{D})$ has indistinguishable encryption.

– $\boldsymbol{S} \models \mathsf{N}(\boldsymbol{i}, \boldsymbol{r_1}, \boldsymbol{r_0}; \boldsymbol{c}, \boldsymbol{x_1}, \boldsymbol{x_0}) \supset$

$$\oslash\, \boldsymbol{i} = \mathbf{circ}(\boldsymbol{c}, \mathbf{ge}(1^{u}, \boldsymbol{r}), \mathbf{cond}(\boldsymbol{i}, \mathbf{enc}(\mathbf{ge}(1^{u}, \boldsymbol{r}), \boldsymbol{x_1}, \boldsymbol{r_1}), \mathbf{enc}(\mathbf{ge}(1^{u}, \boldsymbol{r}), \boldsymbol{x_0}, \boldsymbol{r_0}))$$

where $\boldsymbol{x_1}, \boldsymbol{x_0} \in \boldsymbol{V}^{\mathsf{p}^1}$, $\boldsymbol{i} \in \boldsymbol{V}^{\mathsf{b}}$, $\boldsymbol{r}, \boldsymbol{r_1}, \boldsymbol{r_0} \in \boldsymbol{V}^{\mathsf{p}^2}$, and $\boldsymbol{c} \in \boldsymbol{V}^{\mathsf{p}^n}$.

We name this formula $\mathbf{IND}$.

The indistinguihsbility supporting Kawamoto protocol's privacy is formalised as the following:

$$\mathbf{N}(i, r, r_1, r_0; c, x_1, x_0) \supset \oslash\ i = \mathbf{circ}(c, \mathbf{ge}(1^u, r),$$
$$\mathbf{cond}(i, \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1), \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0))),$$
$$\mathbf{cond}(i, \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0), \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1)))\ )$$

where $x_1, x_0, c \in V^{\mathsf{p}^1},\ i \in V^{\mathsf{b}},\ r, r_1, r_0 \in V^{\mathsf{p}^2}$.

We name this formula **IND-Priv**.

We will show that we can derive **IND-Priv** form **IND** in our axiomatic system.

This equation is derivable:

$$\mathbf{circ}(c, \mathbf{ge}(1^u, r),$$
$$\mathbf{cond}(i, \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1), \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0))),$$
$$\mathbf{cond}(i, \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0), \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1)))\ )$$

$$= \mathbf{cond}(i, \mathbf{circ}(c, \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1), \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0)),$$
$$\mathbf{circ}(c, \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0), \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1)))$$

Therefore, the target formula is:

$$\mathbf{N}(i, r, r_1, r_0; c, x_1, x_0) \supset \oslash\ i = \mathbf{cond}(i,$$
$$\mathbf{circ}(c, \mathbf{ge}(1^u, r), \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1), \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0)),$$
$$\mathbf{circ}(c, \mathbf{ge}(1^u, r), \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0), \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1)))$$

This equivaence is derivable:

$$i = \textsf{\textbf{cond}}(i, t, u) \supset\subset 1 = \textsf{\textbf{cond}}(i, t, \sim u).$$

Therefore, the target formula is:

$$\begin{aligned}&\textsf{N}(i, c; r, r_1, r_0) \supset \oslash\ 1 = \textsf{\textbf{cond}}(i,\\ &\quad \textsf{\textbf{circ}}(c, \textsf{\textbf{ge}}(1^u, r), \textsf{\textbf{enc}}(\textsf{\textbf{ge}}(1^u, r), x_1, r_1), \textsf{\textbf{enc}}(\textsf{\textbf{ge}}(1^u, r), x_0, r_0)),\\ &\ \sim\textsf{\textbf{circ}}(c, \textsf{\textbf{ge}}(1^u, r), \textsf{\textbf{enc}}(\textsf{\textbf{ge}}(1^u, r), x_0, r_0), \textsf{\textbf{enc}}(\textsf{\textbf{ge}}(1^u, r), x_1, r_1)))\end{aligned}$$

$$\textsf{N}(i; t, u) \supset \oslash 1 = \textsf{\textbf{cond}}(i, t, \sim u)$$

denotes that t is indistinguishable to u.

This relation

$$\textsf{N}(i; t, u) \supset \oslash\ i = \textsf{\textbf{cond}}(i, t, \sim u)$$

between t and u is a equvalence relation, thus transitive.

As preparation, this is devivable:

– $\mathbf{N}(j; i, t_1, t_2, t_3) \wedge \oslash\, j = 1$

$\wedge \oslash\, 1 = \mathbf{cond}(i, t_1, {\sim} t_2) \wedge \oslash\, 1 = \mathbf{cond}(i, t_2, {\sim} t_3)$

$\supset \oslash\, 1 = \mathbf{cond}(j, \mathbf{cond}(i, t_1, {\sim} t_2), \mathbf{cond}(i, t_2, {\sim} t_3))$

These equations are derivable:

– $\mathbf{cond}(i, t_1, {\sim} t_2) \sqcup \mathbf{cond}(i, t_2, {\sim} t_3) = \mathbf{cond}(i, t_1 \sqcup t_2, {\sim} t_2 \sqcup {\sim} t_3)$

$= \mathbf{cond}(i, t_1, {\sim} t_3) \sqcup \mathbf{cond}(i, t_2, {\sim} t_2)$

– $\mathbf{cond}(i, t_1, {\sim} t_2) \sqcap \mathbf{cond}(i, t_2, {\sim} t_3) = \mathbf{cond}(i, t_1 \sqcap t_2, {\sim} t_2 \sqcap {\sim} t_3)$

$= \mathbf{cond}(i, t_1, {\sim} t_3) \sqcap \mathbf{cond}(i, t_2, {\sim} t_2)$

Therefore, this is derivable:

– $\mathbf{N}(j; i, t_1, t_2, t_3) \wedge \oslash\, j = 1 \;\supset$

$(\oslash\, 1 = \mathbf{cond}(j, \mathbf{cond}(i, t_1, {\sim} t_2), \mathbf{cond}(i, t_2, {\sim} t_3))$

$\supset\subset\; \oslash\, 1 = \mathbf{cond}(j, \mathbf{cond}(i, t_1, {\sim} t_3), \mathbf{cond}(i, t_2, {\sim} t_2))\;)$

On the other hand, these are derivable:

– $\mathbf{N}(i;t_2) \wedge \oslash\ i = 1 \supset \oslash\ 1 = \mathbf{cond}(i,1,0)$

– $\mathbf{N}(i;t_2) \wedge \oslash\ i = 1 \supset$

$$(\oslash\ 1 = \mathbf{cond}(i,1,0)\ \ \supset\subset \oslash\ 1 = \mathbf{cond}(i,t_2,\sim t_2))$$

Therefore, these are derivable:

– $\mathbf{N}(i;t_2) \wedge \oslash\ i = 1 \supset \oslash\ 1 = \mathbf{cond}(i,t_2,\sim t_2)$

– $\mathbf{N}(i,j;t_1,t_2,t_3) \wedge \oslash\ i = 1 \wedge \oslash\ j = 1\ \supset$

$$(\ \oslash 1 = \mathbf{cond}(i,t_1,\sim t_3)$$
$$\supset\subset\ \ \oslash\ 1 = \mathbf{cond}(j,\mathbf{cond}(i,t_1,\sim t_3),\mathbf{cond}(i,t_2,\sim t_2))\ )$$

As the consequence, these are derivable:

– $\mathbf{N}(i,j;t_1,t_2,t_3) \wedge \oslash\ i = 1 \wedge \oslash\ j = 1\ \supset$

$$(\ \oslash\ 1 = \mathbf{cond}(i,t_1,\sim t_3)$$
$$\supset\subset\ \ \oslash\ 1 = \mathbf{cond}(j,\mathbf{cond}(i,t_1,\sim t_2),\mathbf{cond}(i,t_2,\sim t_3))\ )$$

– $\mathbf{N}(j,i;t_1,t_2,t_3) \wedge \oslash\ i = 1 \wedge \oslash\ j = 1$

$$\wedge \oslash\ 1 = \mathbf{cond}(i,t_1,\sim t_2) \wedge \oslash\ 1 = \mathbf{cond}(i,t_2,\sim t_3)$$
$$\supset \oslash\ 1 = \mathbf{cond}(i,t_1,\sim t_3)$$

Therefore, by eliminating the variable j:

– $\mathbf{N}(i;t_1,t_2,t_3) \wedge \oslash\ i = 1$

$$\wedge \oslash\ 1 = \mathbf{cond}(i,t_1,\sim t_2) \wedge \oslash\ 1 = \mathbf{cond}(i,t_2,\sim t_3)$$
$$\supset \oslash\ 1 = \mathbf{cond}(i,t_1,\sim t_3)$$

By repitating the same discussion:

– $\mathbf{N}(i; t_1, t_2, ..., t_n) \wedge \oslash\ i = 1$

$\wedge \oslash\ 1 = \mathbf{cond}(i, t_1, \sim t_2)$

$\wedge \oslash\ 1 = \mathbf{cond}(i, t_2, \sim t_3)$

. . .

$\wedge \oslash\ 1 = \mathbf{cond}(i, t_{n-1}, \sim t_n) \ \supset\ \oslash\ 1 = \mathbf{cond}(i, t_1, \sim t_n)$

We will show the indistinguishability of each line to the next:

1. $\mathbf{circ}(c, \mathbf{ge}(1^u, r), \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1), \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0))$
2. $\mathbf{circ}(c, \mathbf{ge}(1^u, r), \mathbf{enc}(\mathbf{ge}(1^u, r), x', r'), \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0)))$
3. $\mathbf{circ}(c, \mathbf{ge}(1^u, r), \mathbf{enc}(\mathbf{ge}(1^u, r), x', r'), \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1)))$
4. $\mathbf{circ}(c, \mathbf{ge}(1^u, r), \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0), \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1)))$

It is suffient to show the first.

We have

$$\exists c'.\forall kxy.\mathbf{N}(\vec{z}; c, x, y, \vec{z}') \supset \mathbf{N}(\vec{z}; c, c', k, x, y, \vec{z}')\wedge$$
$$\Box\ \mathbf{circ}(c', k, x) = \mathbf{circ}(c, k, x, \mathbf{enc}(k, y, r))$$

Hence

$$\exists c'.\forall x_1 x' r_1 r'.\mathbf{N}(r, r_1, r'; c', x_1, x_0, x', r_0) \supset$$
$$\mathbf{N}(r, r_1, r'; c', x_1, x_0, x', r_0)$$
$$\wedge\ \Box\ \mathbf{circ}(c', \mathbf{ge}(1^u, r), \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1))$$
$$= \mathbf{circ}(c, \mathbf{ge}(1^u, r), \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1), \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0))$$
$$\wedge\ \Box\ \mathbf{circ}(c', \mathbf{ge}(1^u, r), \mathbf{enc}(\mathbf{ge}(1^u, r), x', r'))$$
$$= \mathbf{circ}(c, \mathbf{ge}(1^u, r), \mathbf{enc}(\mathbf{ge}(1^u, r), x', r'), \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0))$$

Hence

$$\exists c'.\forall x_1 x' r_1 r'.\mathbf{N}(r, r_1, r'; c', x_1, x_0, x', r_0) \supset$$
$$\mathbf{N}(c'; x_1, x', r_1, r', r)$$
$$\wedge\ \Box\ \mathbf{cond}(i, \mathbf{circ}(c, \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1), \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0)),$$
$$\sim\!\mathbf{circ}(c, \mathbf{enc}(\mathbf{ge}(1^u, r), x', r'), \mathbf{enc}(\mathbf{ge}(1^u, r), x_0, r_0)))$$
$$= \mathbf{cond}(i, \mathbf{circ}(c', \mathbf{ge}(1^u, r), \mathbf{enc}(\mathbf{ge}(1^u, r), x_1, r_1)),$$
$$\sim\!\mathbf{circ}(c', \mathbf{ge}(1^u, r), \mathbf{enc}(\mathbf{ge}(1^u, r), x', r')))$$

By $\mathbf{IND}$,

$$\mathsf{N}(r, r_1, r'; c'', x_1, x') \supset$$

$$\oslash\, 1 = \mathsf{cond}(i, \mathsf{circ}(c'', \mathsf{ge}(1^u, r), \mathsf{enc}(\mathsf{ge}(1^u, r), x_1, r_1)), \sim\mathsf{circ}(c', \mathsf{ge}(1^u, r), \mathsf{enc}(\mathsf{ge}(1^u, r), x', r'))$$

Therefore

$$\mathsf{N}(r, r_1, r'; c', x_1, x_0, x', r_0) \supset$$

$$\oslash\, 1 = \mathsf{cond}(i, \mathsf{circ}(c', \mathsf{ge}(1^u, r), \mathsf{enc}(\mathsf{ge}(1^u, r), x_1, r_1), x_0, r_0), \sim\mathsf{circ}(c', \mathsf{ge}(1^u, r), \mathsf{enc}(\mathsf{ge}(1^u, r), x', r'), x_0, r_0)\ )$$

Therefore

$$\mathsf{N}(r, r_1, r'; c, x_1, x_0, x', r_0) \wedge \oslash\, 1 =$$

$$\mathsf{cond}(i,$$

$$\mathsf{circ}(c, \mathsf{ge}(1^u, r), \mathsf{enc}(\mathsf{ge}(1^u, r), x_1, r_1), \mathsf{enc}(\mathsf{ge}(1^u, r), x_0, r_0)),$$

$$\sim\mathsf{circ}(c, \mathsf{ge}(1^u, r), \mathsf{enc}(\mathsf{ge}(1^u, r), x', r'), \mathsf{enc}(\mathsf{ge}(1^u, r), x_0, r_0))$$

$$)$$

Conclusion

We formalised the inferences on negligibly small probability.

Especially, we formalise trhe dependency of variables

by the predicate $\mathbf{N}(;)$.