Improving Onion Notation

Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Presented at: PET2003,
Dresden, 26th March 2003

Why does notation matter?

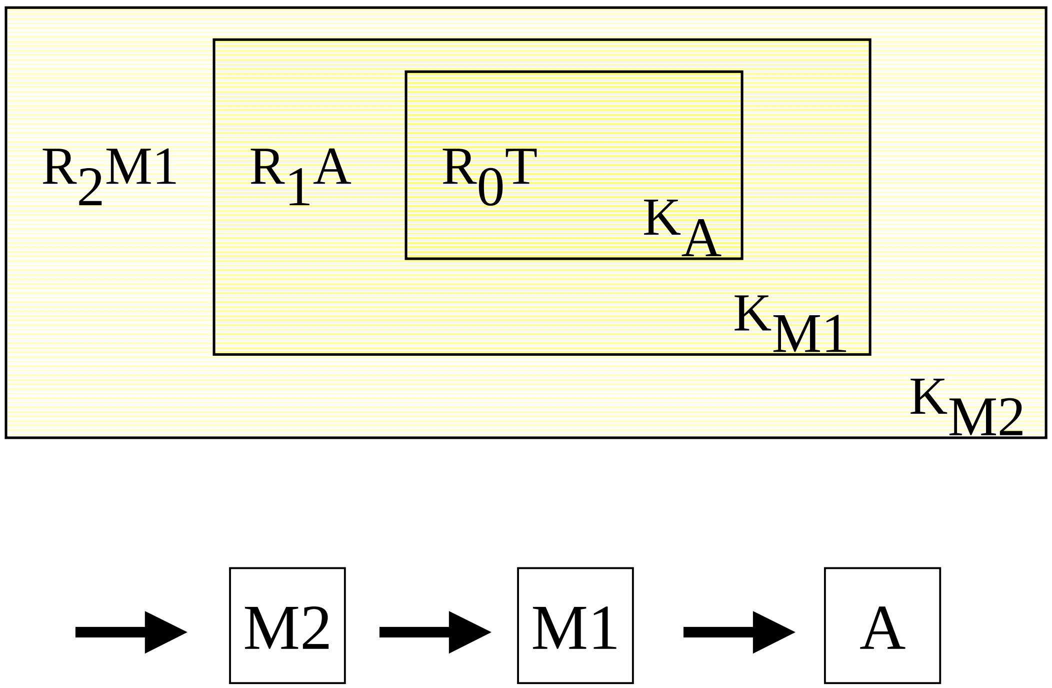
In signs one observes an advantage in discovery which is greatest when they express the exact nature of a thing briefly and, as it were, picture it; then indeed the labour of thought is wonderfully diminished.

Leibniz, 1646–1716

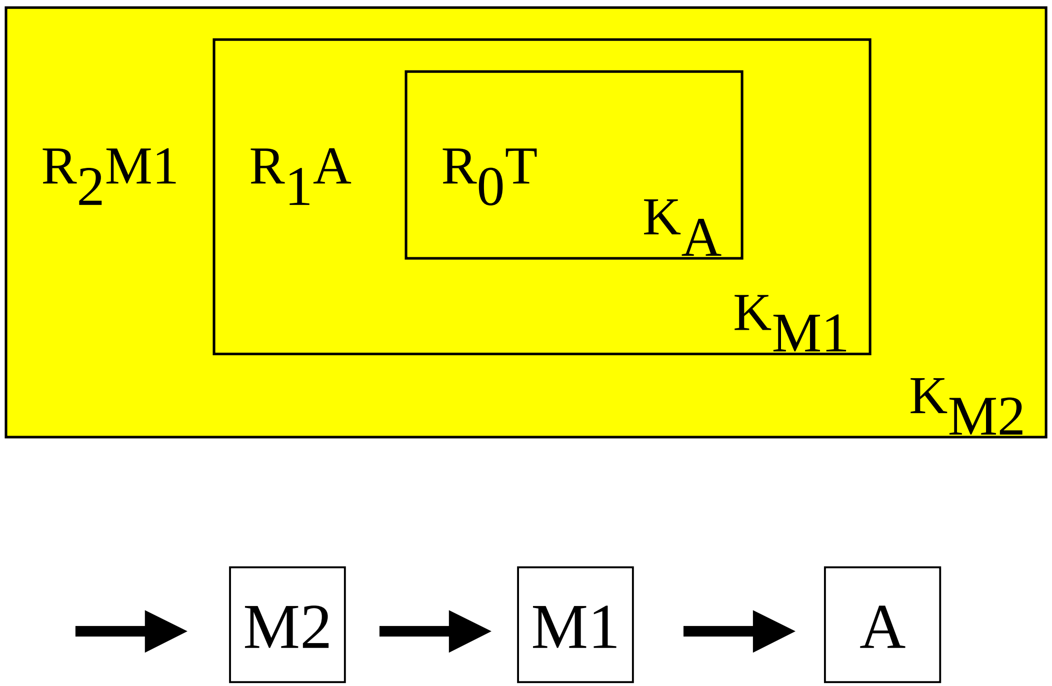
Summary

- Current onion notation
- What’s important about a notation?
- A new notation
- Using the new notation
- Discussion
- Lunch!

Sending message T to Alice



Sending message T to Alice



Onion notation

- MIXs invented by David Chaum, 1981
- $K_i(x)$ means “seal” x with key K_i
- Hence an “onion” [Goldschlag et al 1996] for text T destined for node A (owner of key K_a) sent via MIX M_1 (owner of key K_1) is, with the addition of nonces R_1 and R_0:

$$\mathbf{K_1(R_1,K_a(R_0,T),A)}$$

Onion notation II

- Ohkubo & Abe, 2000
- use $\mathcal{E}_{K_i}(x)$ to mean "encrypt" x with key K_i
- Hence an "onion" for text T destined for node A (owner of key K_a) sent via MIX M_1 (owner of key K_1) is, with the addition of nonces R_1 and R_0:

$$\boldsymbol{\mathcal{E}_{K_1}(R_1, \mathcal{E}_{K_a}(R_0, T), A)}$$

Onion notation III

- Serjantov, 2003, following BAN tradition
- $\{x\}_{K_i}$ means "encrypt" x with key K_i
- Hence an "onion" for text T destined for node A (owner of key K_a) sent via MIX M_1 (owner of key K_1) is, with the addition of nonces R_1 and R_0:

$$\mathbf{\{R_1,\{R_0,T\}_{K_a},A\}_{K_1}}$$

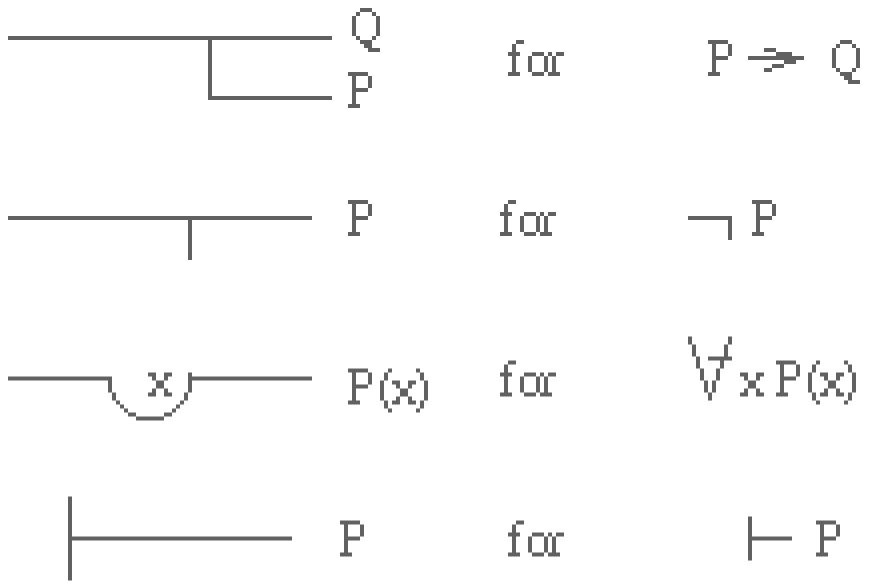
Assessing notations

A) Make it fit on one line

Frege, 1879

Begriffsschrift

The start of the age of symbolic logic. His contemporaries failed to cope!



Assessing notations

B) Make it easy to write

eg: “$\varepsilon_{K_i}(x)$” has custom subscript, font size and line spacing

C) Make it easy to read

can you read $_{\text{subscript}}$ from the back ?

Assessing notations

D) Will it allow errors to be detected ?

E) Will it allow simple generalisation

F) Will it be easy to comprehend

so what of this example?

$$K_n(R_n\ldots\underline{(R_2,\underline{K_1(R_1,\underline{K_a(R_0,T)},A)},M_1)}\ldots M_{n-1})$$

There must be a better way!

$| R_0,T \# K_a | R_1,*,A \# K_1$

| is the start of a section of the onion

#K means encrypt this section with key K

* is the result of the previous encryption

There's no nesting to unpick!

- Three MIXs:

  $| R_0,T \# K_a|R_1,*,A \# K_1|R_2,*,M_1 \# K_2$

- n MIXs:

  $| R_0,T \# K_a|R_1,*,A \# K_1|\ldots|R_n,*,M_{n-1} \# K_{n-1}$

Pfitzmann & Waidner 1986

- Avoid end-to-end retransmission on failures

$X_a \quad K_a(T)$

$X_n \quad K_n(k_n, A), k_n(X_a)$

$X_i \quad K_i(k_i,M_{i+1},k_{i+1},M_{i+2}),k_i(X_{i+1})$

ie: besides normal information, each MIX is told about next but one MIX and can route around a failure. The sender also encrypts with k_i values and tells appropriate MIXs their values.

In the new notation

$X_a \quad |T \# K_a$

$X_n \quad |k_n, A \# K_n|X_a \# k_n|*_0*_1$

$X_i \quad |k_i, M_{i+1},k_{i+1},M_{i+2} \# K_n|X_{i+1} \# k_i|*_0*_1$

where $*_0$ is the result of encrypting the previous section and $*_1$ the result of encrypting the section before that

Avoiding the induction

$|T \# k_a$

$|k_n, A \# K_n |*_0 *_1 \# k_{n-1}$

$|k_{n-1}, M_n, k_n, A \# K_{n-1} |*_0 *_1 \# k_{n-2}$

$|k_{n-2}, M_{n-1}, k_{n-1}, M_n \# K_{n-2}|*_0 *_1 \# k_{n-3}$

$|k_{n-3}, M_{n-2}, k_{n-2}, M_{n-1} \# K_{n-3} | *_0 *_1 \# k_{n-4}$

…

and can now reason about security properties

Questions for a discussion

- Is it worthwhile making the notation resemble the implementation, or should it resemble Encryption(functions) ?
- Do we actually have trouble reading nested brackets? or lots of $_{\text{subscripts}}$? or … ellipses?
- If this notation isn't useful, should we start to ruthlessly stamp out the new-fangled notations that are appearing ?

Why does notation matter?

In signs one observes an advantage in discovery which is greatest when they express the exact nature of a thing briefly and, as it were, picture it; then indeed the labour of thought is wonderfully diminished.

Leibniz, 1646–1716

Discussion

$| R_0, T \# K_a | R_1, *, A \# K_1 | \ldots | R_n, *, M_{n-1} \# K_{n-1}$

| is the start of a section of the onion

K means encrypt this section with key K

* is the result of the previous encryption

More ideas

- Brackets:

$$| K_a (R_0,T) | K_1(R_1,*,A) | K_2(R_2,*,A)$$

- Arrows:

$$| R_0,T>K_a|R_1,*,A>K_1|\ldots|R_n,*,M_{n-1}>K_{n-1}$$

or

$$| R_0,T\rightarrow K_a|R_1,*,A\rightarrow K_1|\ldots|R_n,*,M_{n-1}\rightarrow K_{n-1}$$

And a functional notation (Grothoff)

$F(a, b)(x) := E_{ka}(R_a, x, b)$

$(f(A,B) \circ f(B,C) \circ f(C,C))\ (T)$

Power notation (Serjantov)

cf: $\prod$ or $\sum$ (Euler's notation)

$$\underset{i=0}{\overset{n}{\Omega}} R_i \text{ , *, } M_i$$

- where A is M_0 and the "initial" * is empty

More discussion ?

- At lunch ?
- Or later in the workshop !

richard.clayton@cl.cam.ac.uk

http://www.cl.cam.ac.uk/~rnc1/