An Algebra for Assessing Trust in Authentication Chains

Audun Jøsang

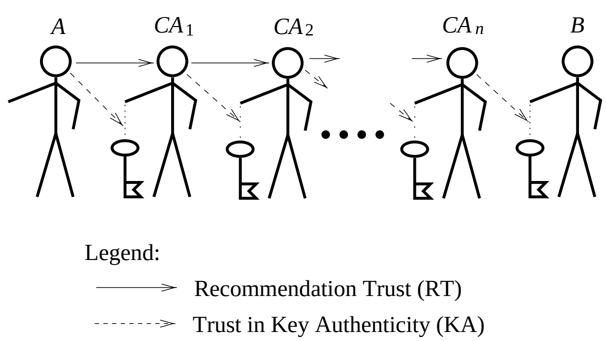
Norwegian University of Science and Technology

Key authenticity based on chains of trust

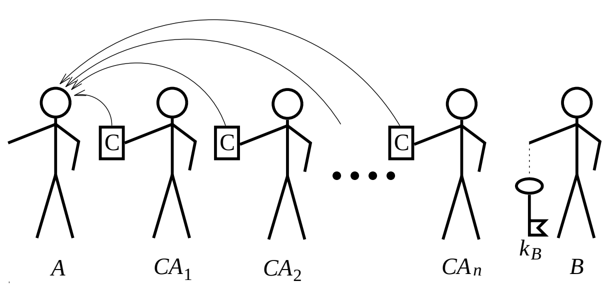
Two types of trust:

1. Trust in key authenticity (key-to-owner binding).

2. Recommendation trust (agent co-operation).



Agent A must determine the authenticity of k_B based on recommendations in the form of certificates.

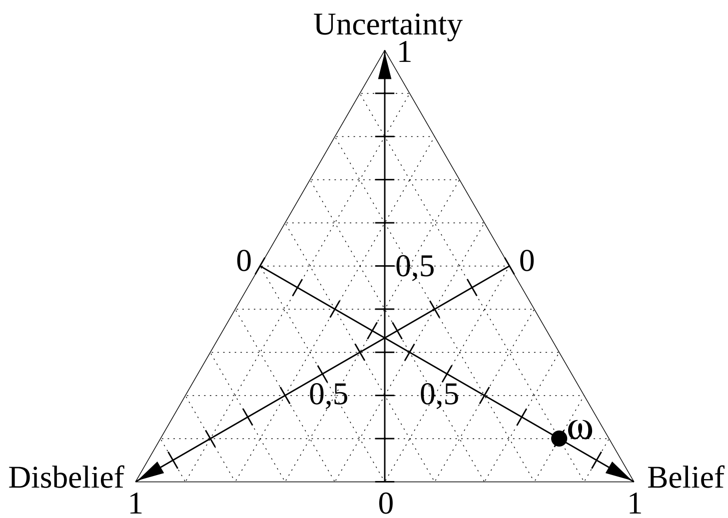


The belief model

An *opinion* is a triplet $\{b, d, u\}$ which satisfies

$$b + d + u = 1, \quad \{b, d, u\} \in [0, 1]^3$$

b: belief
d: disbelief
u: uncertainty



- Any point in the triangle represents an opinion.

- Example, $\omega = \{0.8, 0.1, 0.1\}$ is represented as a dot in the triangle.

Subjective Logic

- Opinions can be interpreted as imprecise probabilities of binary events.

- Subjective Logic is reduced to probability calculus when $u = 0$.

- Subjective logic is reduced to binary logic when $b = 1$ or $d = 1$.

- Ownership of opinions is assigned to individuals.

observing agent

opinion ω_p^A

statement

The operators of Subjective Logic

1. AND $\omega_p^A \wedge \omega_q^A$

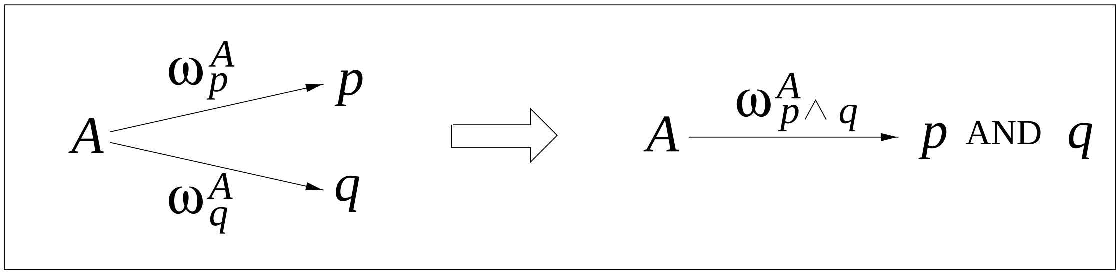
2. OR $\omega_p^A \vee \omega_q^A$

3. Negation $\neg\omega_p^A$

4. Recommendation $\omega_p^A \otimes \omega_p^B$

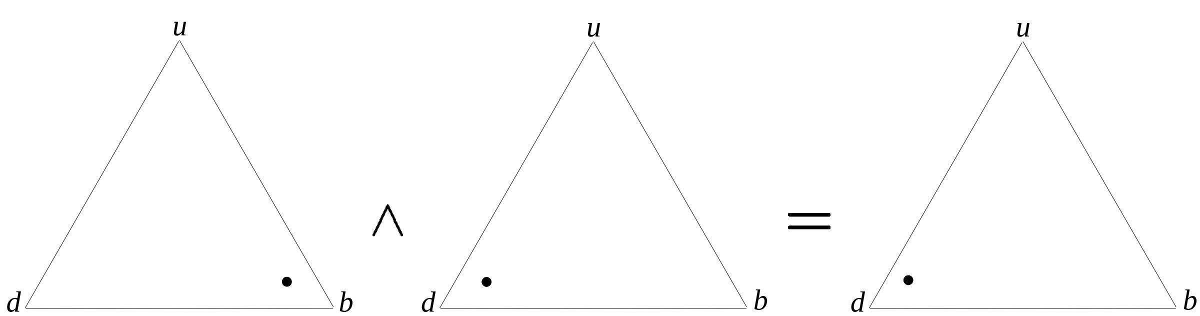
5. Consensus $\omega_p^A \oplus \omega_p^B$

AND

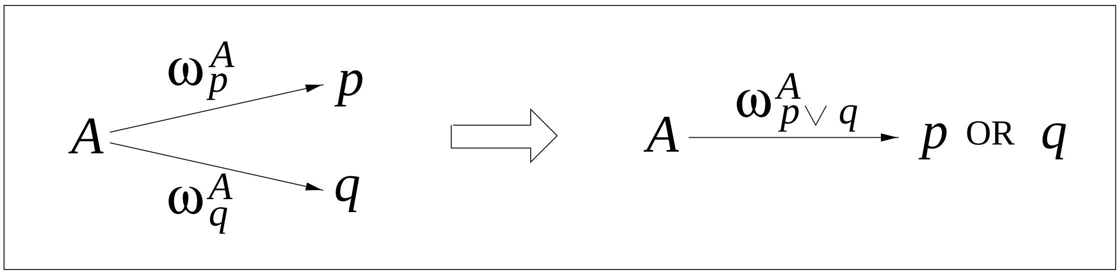


- notation: $\omega_p^A \wedge \omega_q^A = \omega_{p\wedge q}^A$
- commutative
- associative
- opinion independence assumed
- not idempotent: $\omega_p^A \wedge \omega_p^A$ is undefined
- becomes product of probabilities i.c.o. zero ignorance
- becomes ‘binary logic AND’ i.c.o. absolute opinions

Ex: $\{0.8, 0.1, 0.1\} \wedge \{0.1, 0.8, 0.1\} = \{0.08, 0.82, 0.10\}$

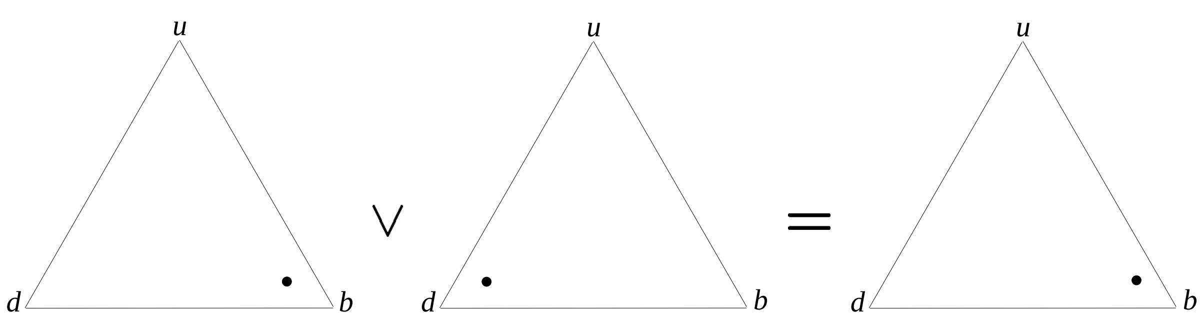


OR



- notation: $\omega_p^A \vee \omega_q^A = \omega_{p \vee q}^A$
- commutative
- associative
- opinion independence assumed
- not idempotent: $\omega_p \vee \omega_p$ is undefined
- becomes co-product of probabilities i.c.o. zero ignorance
- becomes 'binary logic OR' i.c.o. absolute opinions

Ex: $\{0.8, 0.1, 0.1\} \vee \{0.1, 0.8, 0.1\} = \{0.82, 0.08, 0.10\}$

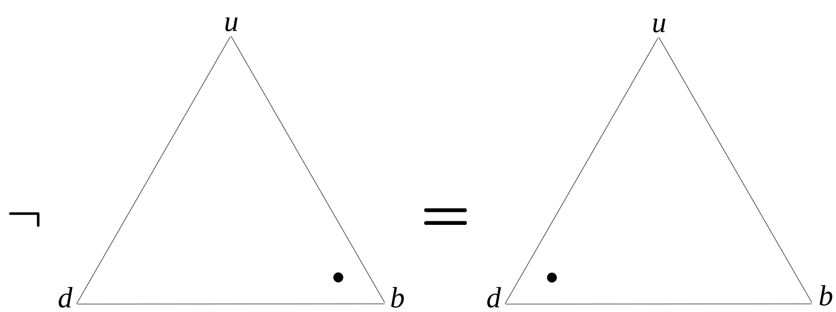


Negation

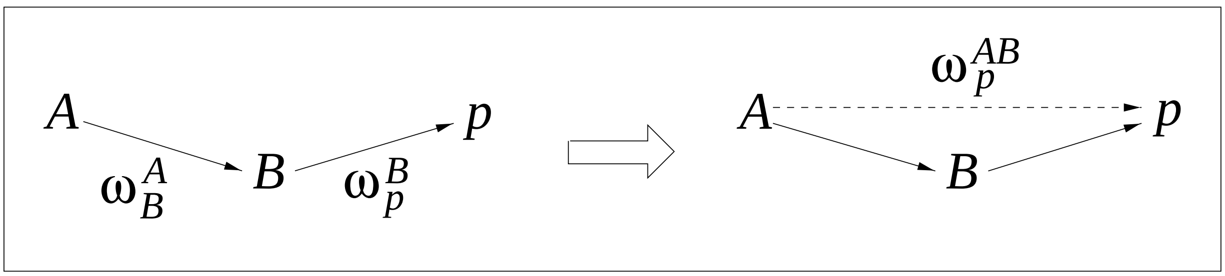
$$A \xrightarrow{\omega_p^A} p \quad \Longrightarrow \quad A \xrightarrow{\omega_{\neg p}^A} \text{NOT } p$$

- notation: $\neg\omega_p^A = \omega_{\neg p}^A$
- Negation is involutive so that $\neg(\neg\omega_p^A) = \omega_p^A$

Ex: $\neg\{0.8, 0.1, 0.1\} = \{0.1, 0.8, 0.1\}$

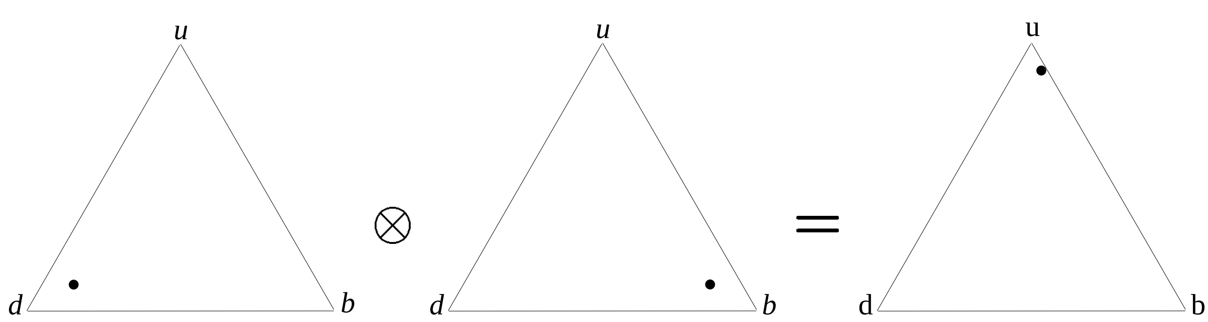


Recommendation

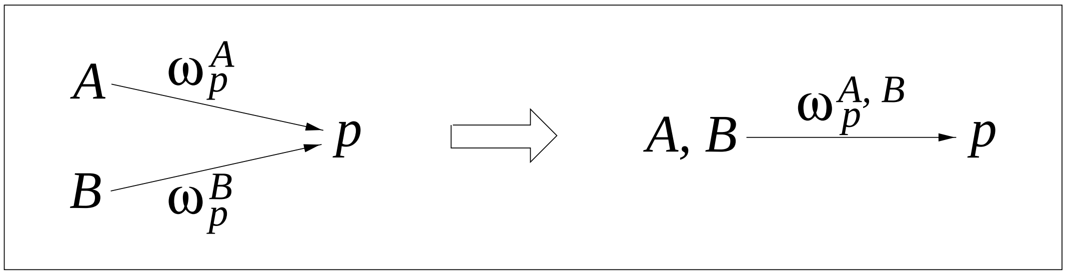


- notation: $\omega_p^{AB} = \omega_B^A \otimes \omega_p^B$
- associative
- non-commutative
- opinion independence assumed
- transitivity assumed

Ex: $\{0.1, 0.8, 0.1\} \otimes \{0.8, 0.1, 0.1\} = \{0.08, 0.01, 0.91\}$

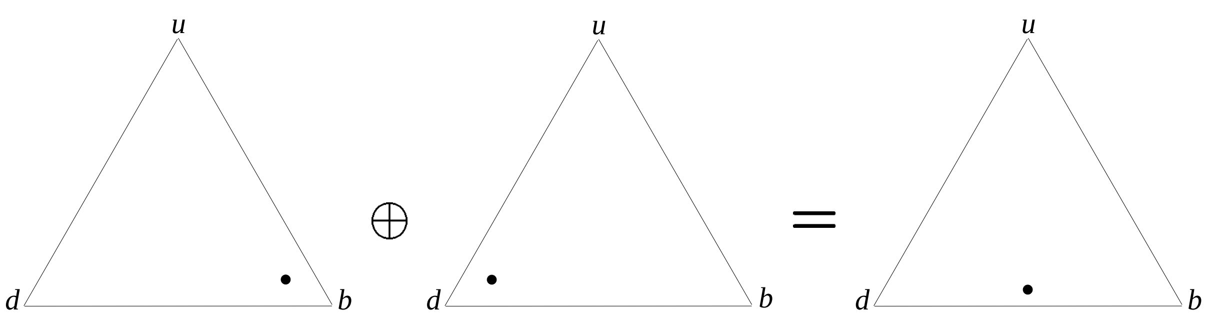


Consensus



- notation: $\omega_p^{A,B} = \omega_p^A \oplus \omega_p^B$
- commutative
- associative
- opinion independence assumed
- opinions without ignorance can not be combined

Ex: $\{0.8, 0.1, 0.1\} \oplus \{0.1, 0.8, 0.1\} = \{0.47, 0.47, 0.06\}$

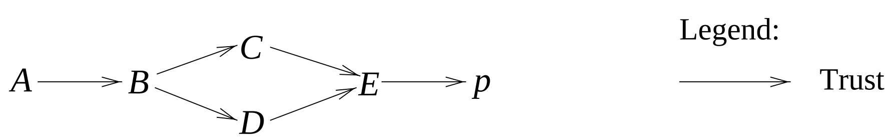


The problem of dependence

'AND' and 'OR' are not distributive on each other:

$$\omega_p \wedge (\omega_q \vee \omega_r) \neq (\omega_p \wedge \omega_q) \vee (\omega_p \wedge \omega_r)$$

Recommendation is not distributive on consensus:



$$\omega^A_B \otimes ((\omega^B_C \otimes \omega^C_E) \oplus (\omega^B_D \otimes \omega^D_E)) \otimes \omega^E_p$$
$$\neq$$
$$(\omega^A_B \otimes \omega^B_C \otimes \omega^C_E \otimes \omega^E_p) \oplus (\omega^A_B \otimes \omega^B_D \otimes \omega^D_E \otimes \omega^E_p)$$

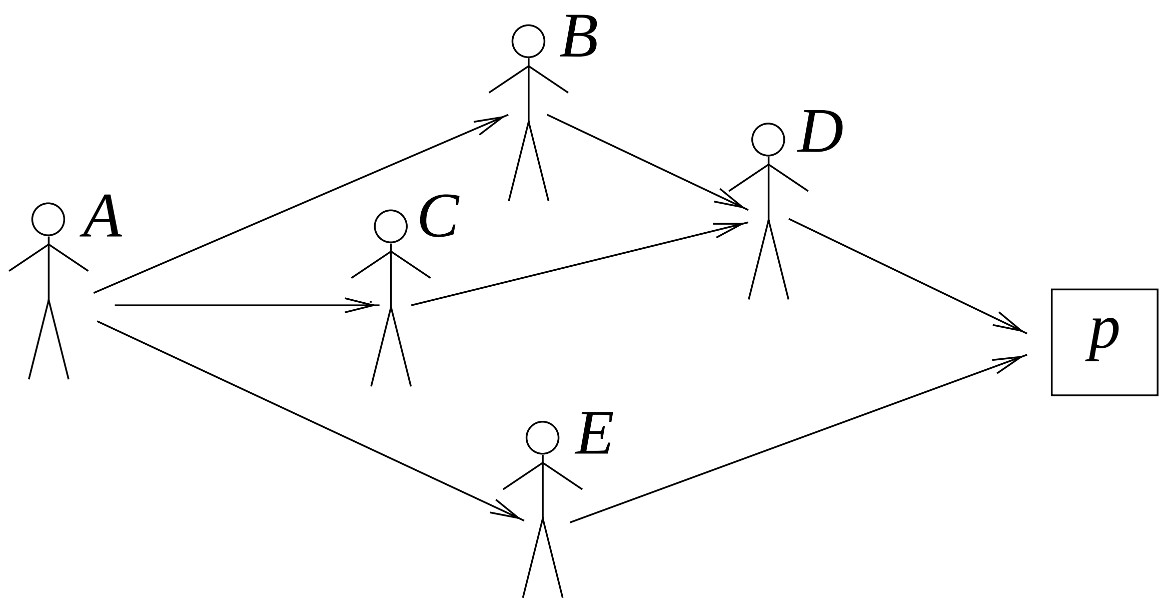
Modelling trust

p: "*The system will resist malicious attacks.*"
q: "*The agent will cooperate.*"
r: "*The key is authentic.*"

ω_p, ω_q, and ω_r are trust parameters.

Trust models can be constructed using subjective logic.

Propagation of trust in social networks



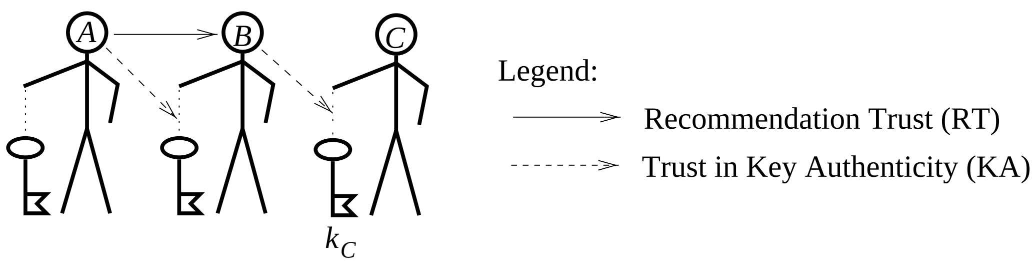
$$\omega_p^{(AB,AC)D,AE}$$

$$=$$

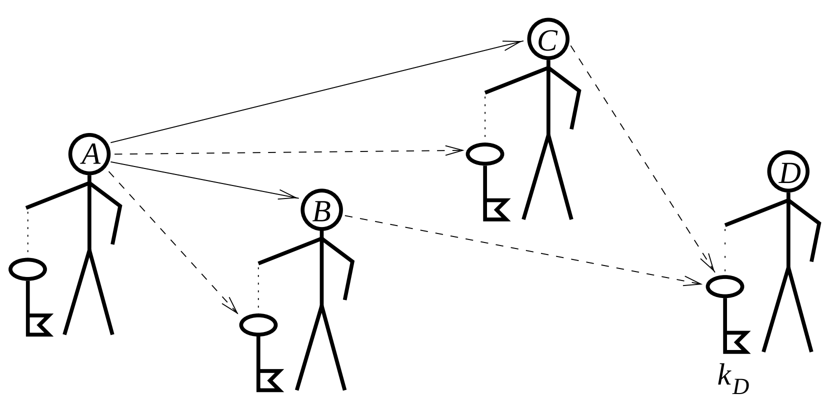
$$((\omega_B^A \otimes \omega_D^B) \oplus (\omega_C^A \otimes \omega_D^C) \otimes \omega_p^D) \;\oplus (\omega_E^A \otimes \omega_p^E)$$

Computation of key authenticity based on trust

Notation: $\omega_B^A = (\omega_{\mathsf{RT}(B)}^A \wedge \omega_{\mathsf{KA}(k_B)}^A)$

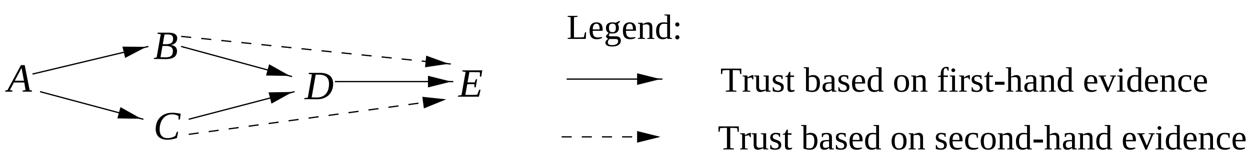


$$\omega_{k_C}^{AB} = \omega_B^A \otimes \omega_{k_C}^B$$



$$\omega_{k_D}^{AB,AC} = (\omega_B^A \otimes \omega_{k_D}^B) \oplus (\omega_C^A \otimes \omega_{k_D}^C)$$

Warning: First-hand trust only!



If B and C recommends their second-hand trust to A, then A would think:

$$\omega_E^{AB,AC} = (\omega_B^A \otimes \omega_E^B) \ \oplus (\omega_C^A \otimes \omega_E^C)$$

Whereas in reality A would compute:

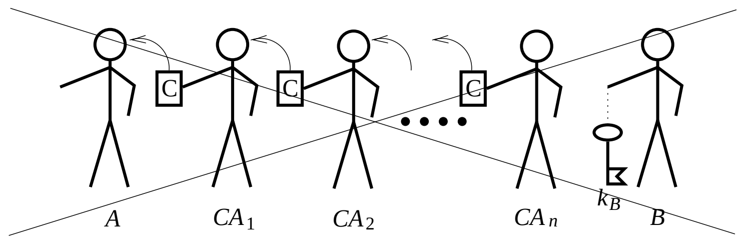
$$\omega_E^{ABD,ACD} = (\omega_B^A \otimes \omega_D^B \otimes \omega_E^D) \oplus (\omega_C^A \otimes \omega_D^C \otimes \omega_E^D)$$

The correct way is to recommend first-hand trust only:

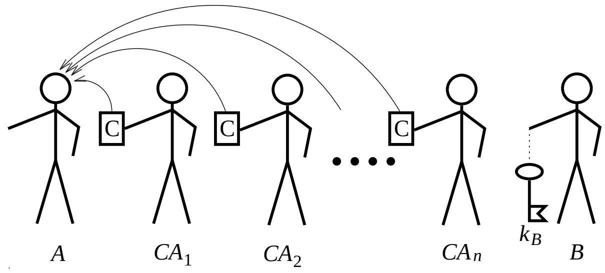
$$\omega_E^{(AB,AC)D} = ((\omega_B^A \otimes \omega_D^B) \oplus (\omega_C^A \otimes \omega_D^C)) \otimes \omega_E^D$$

Direct routing of certificates

Indirect routing and re-computation of trust would lead to recommendation of second-hand trust.

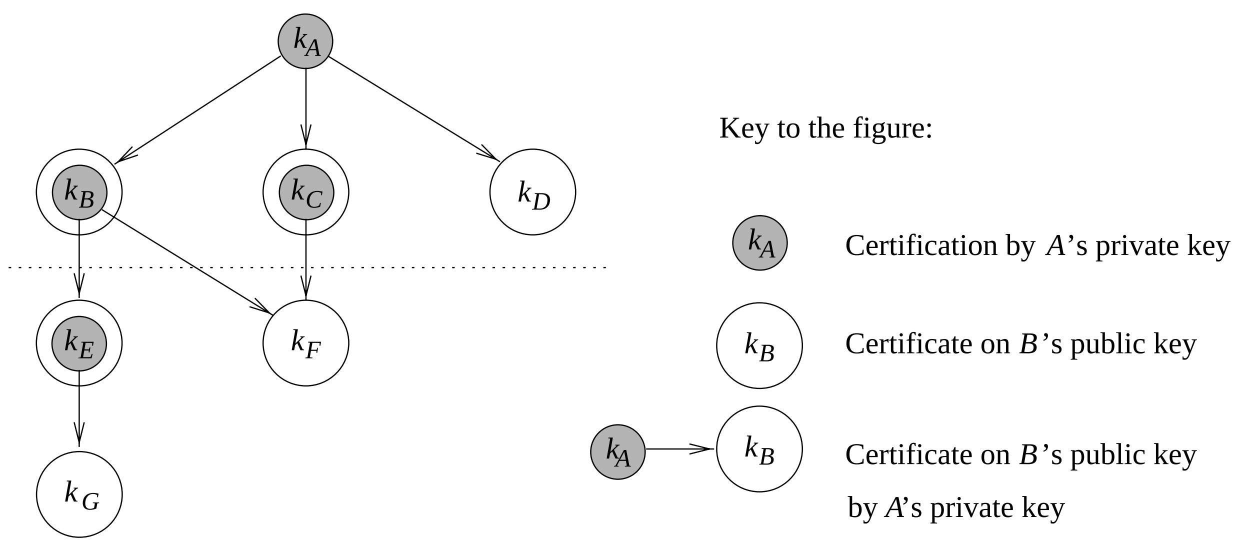


Recommendation of first-hand trust requires direct routing to the final recipient.

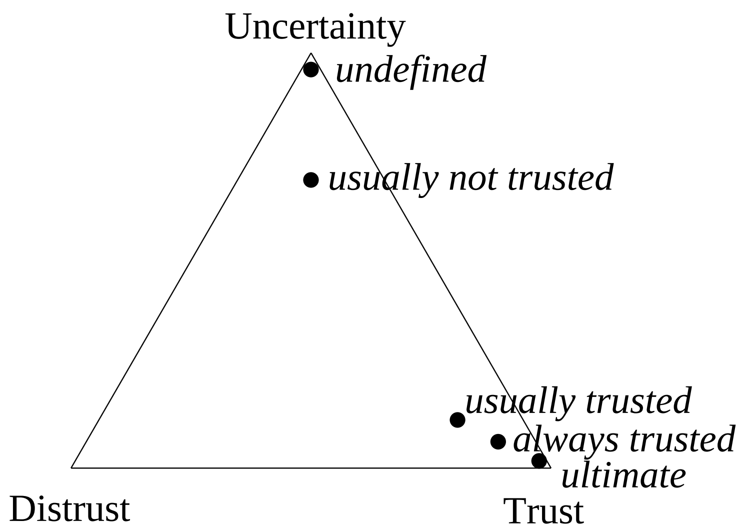


Building a database of certified keys

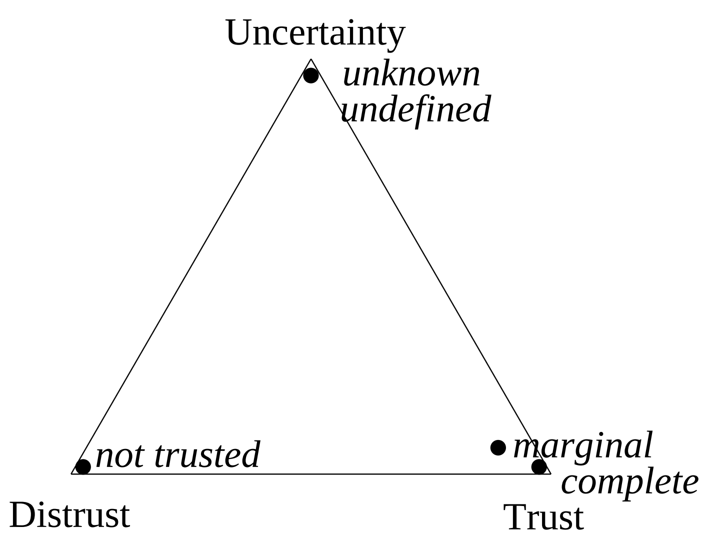
- Public keys can be exchanged manually or electronically.
- Electronically received keys must be certified.
- Each agent decides which other agents she will trust.



Expressing PGP trust values

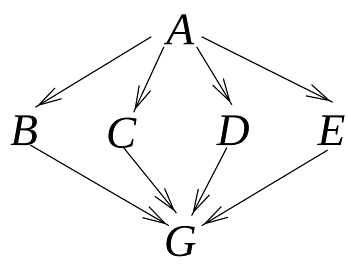


a) "Owner Trust" and "Signature Trust"

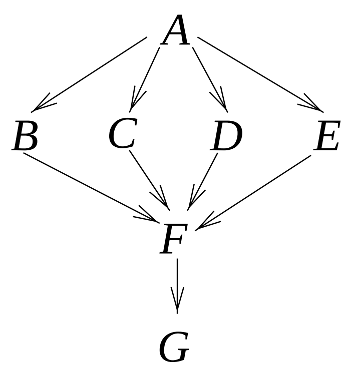


b) "Key Legitimacy"

Hidden dependencies in PGP trust values



a) The situation that A sees



b) The real situation which is hidden for A

A thinks $\omega^{AB,AC,AD,AE}_{\mathsf{KA}(k_G)}$,

but computes $\omega^{ABF,ACF,ADF,AEF}_{\mathsf{KA}(k_G)}$.

A should have computed $\omega^{(AB,AC,AD,AE)F}_{\mathsf{KA}(k_G)}$.

Concluding remarks

- The presented trust model is more complete than previously proposed models because it can express degrees of uncertainty.

- Subjective Logic can be used directly for reasoning about trust in practical security applications.

- A key certificate must contain:
  1) recommendation about key authenticity,
  2) recommendation about key owner.

- Recommendation of trust must be based on first-hand evidence only.