Kollisioonivabadel räsifunktsioonidel põhinevate piiranguteta ajatempliskeemide võimalikkusest

Margus Niitsoo

juhendaja prof. Ahto Buldas

11. november 2008. a.

Mis on ajatembeldus?

- Patendiamet ja notarid
- Pahatahtliku ametnikuga seonduvad probleemid
- Infoühiskonna vajadused

Krüptograafilised templid

- Kontroll faili muutmise vastu
- Räsifunktsioon - konstrueerib dokumendi põhjal väikese kontrollväärtuse

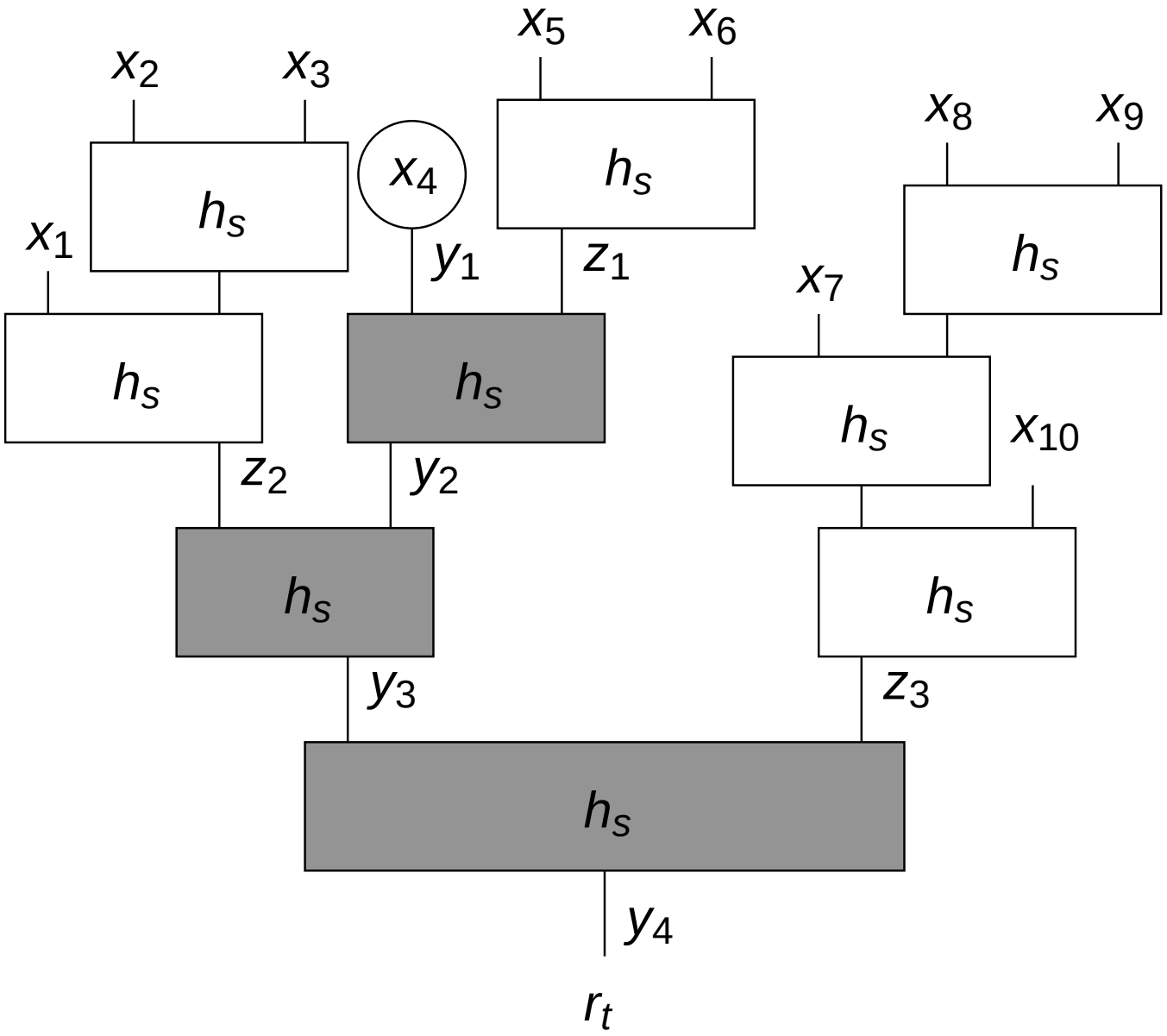
Kollisioonikindlus

- Kaks dokumenti peaks ideaalis alati andma erineva räsiväärtuse
  - Dokumente aga rohkem kui väärtuseid
- Kollisioonikindlus - raske leida kaht dokumenti, mis annaks sama väärtuse
  - Selliste dokumentide paari nimetatakse kollisiooniks

Harberi ja Stornetta ajatempliskeem

- Idee - avaldada väike räsiväärtus iga päev ajalehes
- Kolm osapoolt: kliendid, ametnik, ajaleht
- Kliendid loovad oma dokumentidest räsiväärtused ja saadavad ametnikule
- Ametnik kombineerib need räsiväärtused kokku üheks väiksemaks

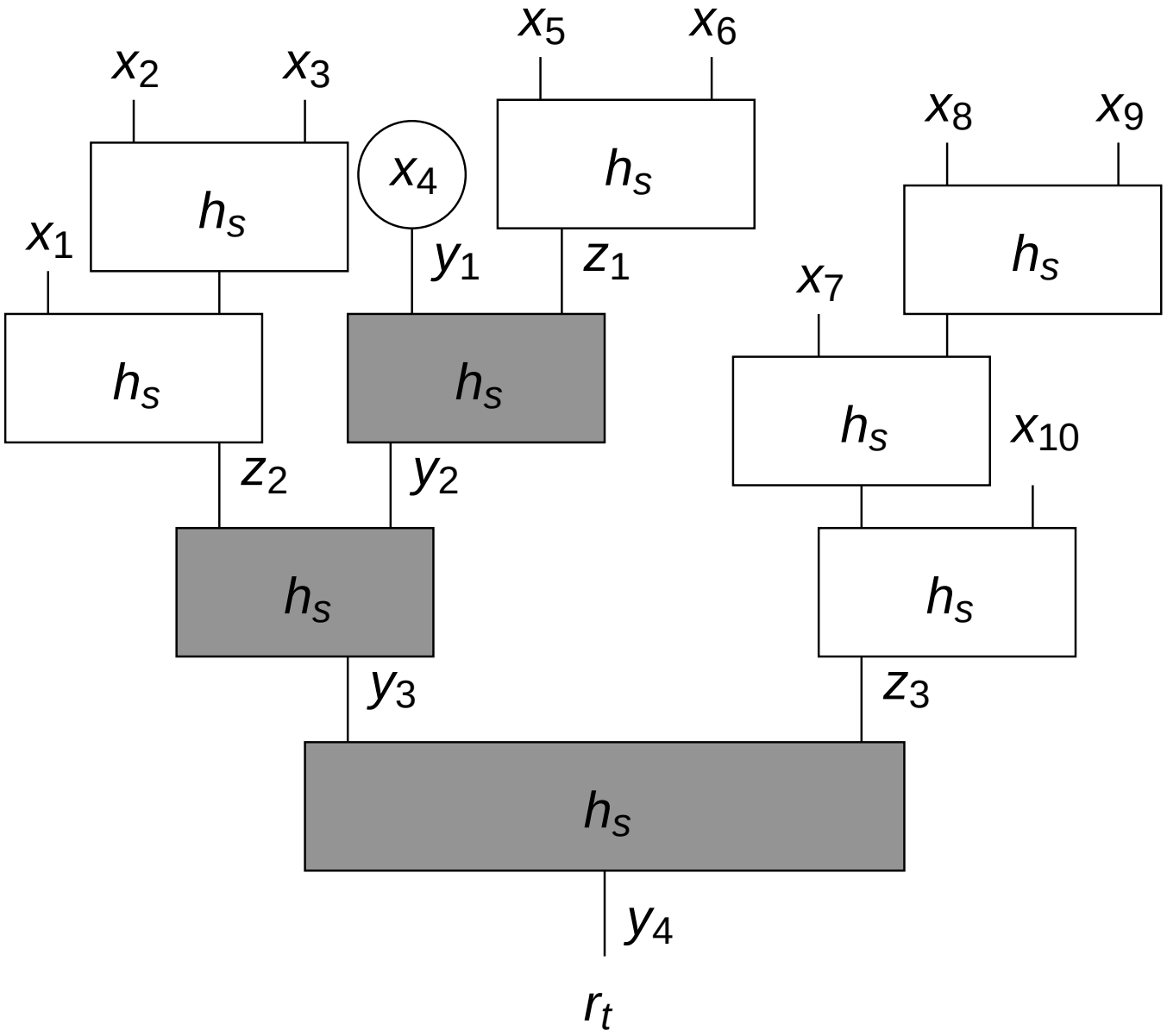
Räsiväärtuste kombineerimine



Ajatempliskeemi turvalisus

- Tahaksime, et poleks võimalik dokumendile anda eilset templit
- Piisab, kui vaatleme dokumente, mida me eile veel ei teadnud
- Eeldame, et ajatempleid lööv ametnik võib olla ebaaus

Ahelakindlus



Seni teada olev

- Kui puu kuju on üheselt fikseeritud, piisab kui kasutada kollisioonikindlat räsifunktsiooni
- Kui puu kuju võib aga olla suvaline, see ei kehti
- Ahelakindlus on kollisioonikindlusest mingis mõttes sõltumatu
- On aga võimalik, et kollisioonikindlast funktsioonist saab konstrueerida ahelakindla funktsiooni.

Antud töö tulemused

- Üritasin välistada sellise konstruktsiooni olemasolu

Antud töö tulemused

- Üritasin välistada sellise konstruktsiooni olemasolu
- Paraku lõplikult see ei õnnestunud.
  - Näitasin, et kui konstruktsioon olemas on, peaks ta olema oluliselt keerulisem või kavalam, kui valdav enamus seni tuntud Krütpoloogilisi konstruktsioone

Antud töö tulemused

- Üritasin välistada sellise konstruktsiooni olemasolu
- Paraku lõplikult see ei õnnestunud.
  - Näitasin, et kui konstruktsioon olemas on, peaks ta olema oluliselt keerulisem või kavalam, kui valdav enamus seni tuntud Krütpoloogilisi konstruktsioone
- Autori enda arvamus on endiselt, et konstruktsiooni pole.

Tänan kuulamast

Küsimused on teretulnud!