UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Računalništvo in matematika – 2. stopnja

Tim Kalan

SKUPINSKO GENERIRANI PODPISI

Magistrsko delo

Mentor: doc. dr. Tilen Marc

Ljubljana, 2024

Zahvala

Neobvezno. Zahvaljujem se ...

Kazalo

Program dela

Mentor naj napiše program dela skupaj z osnovno literaturo.

Osnovna literatura

1. S. Micali, K. Ohta in L. Reyzin, *Accountable-subgroup multisignatures*, v: Proceedings of the 8th ACM conference on Computer and Communications Security (ur. P. Samarati), ACM, Philadelphia, PA, USA, 2001, str. 245–254, DOI: 10.1145/501983.502017, dostopno na https://doi.org/10.1145/501983.502017.

Podpis mentorja:

Skupinsko generirani podpisi

Povzetek

Tukaj napišemo povzetek vsebine. Sem sodi razlaga vsebine in ne opis tega, kako je delo organizirano.

Multisignatures

Abstract

An abstract of the work is written here. This includes a short description of the content and not the structure of your work.

Math. Subj. Class. (2020): 94A60, 11T71
Ključne besede: digitalni podpis, kriptografija
Keywords: digital signature, cryptography

1 Uvod

Odkar se je na svetu pojavil koncept (ročnega) podpisa, je večina primerov uporabe temeljila na pridobivanju podpisov več deležnikov. Odličen primer je npr. Deklaracija neodvisnosti Združenih držav Amerike. SLIKA?.

V prejšnjem stoletju je vzpon računalnika in napredek v kriptografiji privedel do *digitalnih podpisov*. Ti odlično nadomeščajo ročni podpis, prav tako omogočajo, da se skupina podpiše tako, da vsak član poda svoj podpis. Vendar tu lahko z malo matematike poskrbimo, da se skupina lahko podpiše tako, da vsi člani skupaj oddajo en sam podpis, ki priča o podpisu celotne skupine. Tako razbremenimo preverjalca podpisov, kar je ključno v sistemih, kjer je računska moč omejena ali pa draga (npr. pri tehnologiji veriženja blokov).

2 Kriptografske osnove

Preden si lahko pogledamo točno kako lahko skupina generira en sam podpis besedila, si moramo pogledati nekaj kriptografskih osnov. Bolj kompliciranе stvari bodo opisane sproti, ideja tega poglavja je predstaviti stvari, ki so predpogoj za branje kakršnegakoli kriptografskega besedila.

2.1 Kriptografija javnega ključa

2.2 Zgoščevalne funkcije

2.3 Kriptografski podpisi

Ideja *kriptografskih* ali *digitalnih* podpisov je, da služijo kot izboljšava človeškega ročnega podpisa. Za razliko od ročnega podpisa, lahko z digitalnim dosežemo pravo identifikacijo posameznika, ki temelji na njegovem zasebnem ključu. Tako smo lahko za digitalno podpisan dokument prepričani, da ga je res podpisal lastnik točno določenega zasebnega ključa.

Podpis dokumenta poteka nekoliko drugače, kot pri ročnih podpisih. Pri ročnem podpisu ta postane del dokumenta, digitalni podpis pa je od njega ločen, vseeno pa nastane s pomočjo zgostitve podpisanega dokumenta, zato bo podpis za dva različna dokumenta vedno drugačen.

Ostane še vprašanje preverjanja avtentičnosti podpisa. Pri ročnem podpisu to lahko storimo prek primerjave z znanim, preverjeno avtentičnim podpisom. Ta postopek je zamuden in nenatančen, veliko večino ročnih podpisov je moč ponarediti z nekaj prakse. Preverjanje digitalnega podpisa pa temelji na kriptografiji javnega ključa. Ker je podpis nastal s pomočjo podpisnikovega zasebnega ključa, lahko s pomočjo ujemajočega javnega ključa preverimo avtentičnost.

Definicija 2.1. Digitalni ali **kriptografski podpis** $\mathcal{S} = (G, S, V)$ je trojica učinkovitih algoritmov G za ustvarjanje ključa, S za podpisovanje in V za preverjanje podpisa. Definirana je nad končno množico možnih sporočil $\mathcal{M}$, vrnjeni podpis pa leži v v končni množici podpisov Σ.

- G je naključnostni algoritem za ustvarjanje para ključev (pk, sk), ki ne prejme nobenega argumenta. pk je javni kljč za preverjanje avtentičnosti podpisa, sk pa je zasebni ključ za podpisovanje.
- S je naključnostni algoritem, ki za svoja argumenta prejme zasebni ključ sk in sporočilo m, vrne pa podpis σ spročila m z zasebnim ključem sk oz.

$$\sigma = S(\text{sk}, m).$$

- V je deterministične algoritem, ki preverja veljavnost podpisov. Za svoje argumente prejme javni ključ pk, sporočilo m in podpis σ, vrne $veljaven$, če je podpis veljaven in $neveljaven$, sicer. Velja torej

$$V(\text{pk}, m, \sigma) = \begin{cases} veljaven; \sigma = S(\text{sk}, m), \\ neveljaven; \sigma \neq S(\text{sk}, m). \end{cases}$$

2.3.1 Ustvarjanje ključa

2.3.2 Podpisovanje

2.3.3 Preverjanje podpisa

2.3.4 Primer: Schnorrov podpis

3 Matematično ozadje

3.1 Modularna aritmetika

3.2 Multiplikativne grupe modulo n

4 Pregled skupinskih podpisov

5 Skupinsko generirani podpisi na podlagi Schnorrovega podpisa

Povzeto po [1].

6 Skupinsko generirani podpisi v splošnem

Literatura

[1] S. Micali, K. Ohta in L. Reyzin, *Accountable-subgroup multisignatures*, v: Proceedings of the 8th ACM conference on Computer and Communications Security (ur. P. Samarati), ACM, Philadelphia, PA, USA, 2001, str. 245–254, DOI: 10.1145/501983.502017, dostopno na https://doi.org/10.1145/501983.502017.