El Gamal mix-nät och implementering av en verifierare

Kandidatexamensarbete - SA104X - VT2013

Erik Larsson Carl Svensson
Handledare: Douglas Wikström

KTH, Skolan för datavetenskap och kommunikation

Praktiskt med elektronisk folkomröstning

- Rösta säkert & hemligt
- Verifierbart
- Robust

Praktiskt med elektronisk folkomröstning

- Rösta säkert & hemligt
- Verifierbart
- Robust
- Kanske ingen valvaka

Innehåll

Mixnät - översiktligt

(bild 1) Skapandet av kryptotextslistan är utanför vårt arbete. Listan går igenom noderna och krypteras om och blandas. Vi får ut en lista med röster och kan inte veta vem som röstat på vad. För att kunna gå igenom detaljer behövs lite krypto.

- Tombola-beskrivning?

Innehåll

Kryptografi

(bild: två kopior av samma nyckel)
Översiktlig beskrivning av kryptografi. Caesar-chiffer Förut fanns bara symmetriska, gemensam nyckel. xxxx bc. - 1976

Public Key Cryptography

¡bild: ett hänglås, en nyckel¿
En nyckel för kryptering, en för dekryptering

El Gamal

$$y := g^x mod p$$

Givet y, g och p. Vad är x? Svårt! Tack vare detta så kan vi skapa El Gamal.

$$y := g^x srandomc = (g^s, y^s * m) = (u, v)m = u^- x * v = g^{(}-s * x) * y^s * m =$$

Förklara hur lätt logaritm =¿ knäckt krypto.
Homomorfism, lager på lager
Detta kan generaliseras till valfri cyklisk grupp.

- Public key crypto

Zero-knowledge proof

Bevisa att man besitter information utan att avslöja informationen.
Exempel med sten, sax, påse genom kryptering.
¡bild: sten-sax-påse¿

Innehåll

Krypteringsnät

¡bild 1¿ ¡bild 4¿ ¡bild 1¿
Förklara detaljerna i varje server

- El gamal

Verifierbarhet

¡bild 2¿ Det skapas extra data.

- Verifiering
- Zero-knowledge

Verifiering

¡bild 3¿

Verificatum

Implementation, Wikström, titel, CSC

Innehåll

Implementation

Vi implementerade en verifierare

- C++
- GMP, OpenSSL
- Representera matematiska objekt

Innehåll

Hur gick det?

Programmets struktur kunde varit bättre. Vi hittade fel i specifikationen. Det var genomförbart men vi kom fram med några förslag till förbättringar på dokumentet.

Innehåll

Roligt på slutet

Det är möjlig att skapa ett elektroniskt röstningssystem. Vi är inte riktigt där än. Verificatum kommer (antagligen) användas i nästa norska val.

Tack! Frågor?