CRYPTOGRAFIE MOET STEMMEN TELLEN CONTROLEERBAAR MAKEN

Mensen en potloden

• *Stemmen in Rotterdam voor de verkiezing van de Provinciale Staten, 2003.*
FOTO DIRK-JAN VISSER

Woensdag zullen sommigen nog een rood potlood gebruiken. Maar over een paar jaar stemmen we misschien thuis op de pc. Of met beveiligd ponspapier. *Bram Vermeer*

OOK BIJ DE verkiezingen voor de Provinciale Staten op 7 maart zullen er weer potloodgemeenten zijn, met geïmproviseerde houten hokjes en vuilnisbakken die zijn omgebouwd tot stembus. Stemmachines staan ter discussie. Het debat gaat vooral over het elektronisch afluisteren tijdens het stemmen. Maar bij verkiezingen gaat het niet alleen om stemgeheim. We willen ook weten dat onze stem goed wordt meegeteld.
Bij de jongste generatie stemmachines kan het tellen gecontroleerd worden: veel nieuwe stemcomputers leggen de stemmen ook op papier vast. In de Duitse deelstaat Hamburg zullen de kiezers volgend jaar hun stembiljet met een *scan*pen invullen. De pen geeft de stem elektronisch door aan de stemcomputer, de kiezer deponeert zijn papieren biljet in een gewone stembus. Bij twijfel over de elektronische uitslag kunnen zo later altijd de papieren stemmen worden geteld.

PAPIERSPOOR Er zijn dan wel afspraken nodig voor het geval papier en elektronica een ander resultaat geven. Hamburg heeft laten weten in dat geval de voorkeur te geven aan de elektronische uitslag. Logisch, het Hamburgse kiesstelsel is zo ingewikkeld, dat handmatig tellen lastig foutloos is uit te voeren. Maar de papieren stem wordt zo gereduceerd tot een zinloos ritueel.
Een *paper trail* biedt dus niet genoeg garantie. Meer wordt verwacht van cryptografische technieken, die verwant zijn aan de bescherming van betalingen op internet. De cryptografie die banktransacties en afschermt, gebruikt speciale wiskundige sommen. Het veelgebruikte RSA-algoritme is gebaseerd op het ontbinden van een groot getal in twee priemgetallen. Het ontbinden vergt extreem veel rekentijd, tenzij je een van die priemgetallen al kent. Ingewijden kunnen de rekensom daardoor snel oplossen en het bericht lezen, maar voor buitenstaanders is dat vrijwel onmogelijk – en dat idee is de basis van alle cryptografische bescherming.
Maar voor stemmachines is dat nog niet genoeg. Onze internetbank mag weten hoeveel geld we overmaken, maar de stemcomputer mag onze stem niet achterhalen. Stemmachines moeten dus niet alleen beschermd worden tegen het afluisteren door buitenstaanders. Ze moeten ook garanderen dat direct betrokkenen geen misbruik maken van onze stem.
De Amerikaanse cryptograaf David Chaum heeft daarvoor een elegant cryptografisch systeem bedacht. In de jaren tachtig werkte hij in Nederland en maakte toen naam met een techniek voor anonieme betalingen. Hij bedacht een systeem voor onder meer anonieme tolheffing. Op welke tolweg je hebt gereden valt daarmee niet te achterhalen, maar wel of je daarvoor betaald hebt.

Chaum bouwt op dat idee voort bij zijn 'Punchscan-stemsysteem'. Alles draait daarin om een stembiljet, dat uit twee vellen papier bestaat, die op elkaar liggen. Op het onderste zijn alleen cijfers gedrukt. Die cijfers zijn zichtbaar door gaten in het bovenste vel papier, dat verder (een stuk boven of onder de gaten) bij elk cijfer de naam van een kandidaat weergeeft. De kiezer maakt het cijfer van de kandidaat van zijn keuze door het gat en rondom het gat rood met een dikke stift. Daarna vernietigt hij een van de twee velletjes en geeft het andere aan de voorzitter van het stembureau. Die kan daaruit niet opmaken wat de kiezer gestemd heeft, want de nummers worden op elk stembiljet op een andere manier aan kandidaten gekoppeld.
Het bewaarde vel wordt ingescand en verder elektronisch verwerkt. Als alle scans zijn verzameld kunnen kiezers de stemmen inzien via internet. Iedereen kan dan controleren of zijn elektronische stem er hetzelfde uitziet als op het bewaarde vel van zijn stembiljet.
Pas bij de telling worden de nummers weer aan namen van kandidaten gekoppeld. En hier zit het cryptografische vernuft van het systeem. Er wordt een cryptografische procedure gevolgd, waarmee dat alleen groepsgewijs kan, met enkele honderden stemmen tegelijk, waarbij niet te achterhalen valt hoe op afzonderlijke biljetten is gestemd maar wel hoe de totalen uitvallen.
Het cryptografische systeem van David Chaum zit vol subtiliteiten, geheime sleutels en digitale handtekeningen. De patenten die hij daarvoor indiende zijn zelfs voor cryptografen lastig te begrijpen. "Niet iedereen hoeft het precies te begrijpen, zolang de experts het maar kunnen controleren", reageert hij desgevraagd. "De werking van de software voor de huidige stemmachines loopt in elk geval ver achter bij de mogelijkheden die de wetenschap biedt voor controle."
Doordat manipulatie ook achteraf kan worden uitgesloten, is voor Punchscan geen afgeschermde hardware nodig, aldus Chaum. "Gewone pc's die op school worden gebruikt zijn perfect bruikbaar." Dat maakt de techniek goedkoop en geschikt voor grootschalig gebruik. Er is alleen speciale hardware nodig om gaten te maken in het papier, maar apparaten daarvoor kunnen makkelijk gefabriceerd worden. "Als je volgende week in heel Amerika verkiezingen wilt houden met Punchscan, kan dat technisch", meent Chaum. Voorlopig wordt Punchscan gebruikt voor universiteitsverkiezingen in de VS. Het concurrerende systeem Votehere is ingezet voor verkiezingen in Washington.
Een andere manier om achteraf je stem te controleren is door te stemmen via internet en vanaf je eigen pc. "Zulke verkiezingen zijn in principe makkelijker te controleren", meent Berry Schoenmakers, cryptograaf aan de Technische Universiteit Eindhoven. "Een stemmachine op een stembureau kun je niet open maken. Maar je bent baas over je eigen pc."

CYBERVOTE Schoenmakers ontwierp de cryptografische software voor Cybervote, een systeem voor online stemmen. Rond 600.000 Franse expats gebruikten het vorig jaar voor lokale verkiezingen. Cybervote is gebaseerd op een zogeheten homomorfe techniek, waarmee stemmen opgeteld kunnen worden zonder dat de inhoud van afzonderlijke stemmen bekend is. Op de pc van de kiezer wordt de stem eerst cryptografisch ingepakt, waarna in de centrale computer geen terugvertaling meer nodig is om de verkiezingsuitslag te kunnen bepalen. Het stemgeheim en de einduitslag zijn controleerbaar in dit systeem.
Online stemmen brengt echter andere veiligheidsrisico's met zich mee. Tijdens verkiezingen moeten alle netwerkspecialisten paraat zijn om het internet af te speuren naar hackers. Trojaanse paarden zijn een bedreiging, evenals pogingen om verkiezingscomputers plat te leggen. De enige echte oplossing daarvoor is het gebruik van speciale computers die geen andere programma's kunnen uitvoeren en die verbonden zijn met een controleerbaar deel van het internet. En er is meer, zegt Schoenmakers. "Verschillende technieken concurreren nu met elkaar. Er moeten keuzes gemaakt worden voor protocollen in standaarden. Dat moet rijpen, voordat gebruikers er vertrouwen in krijgen. Zoals dat eerder gebeurde met de cryptografische bescherming van dataverkeer. Banken gebruiken nu een bepaald beveiligingsalgoritme, omdat dit vastligt in standaarden en iedereen het erover eens is dat dit voldoende bescherming biedt. Zover is het met stemprocedures nog niet." De nieuwe technieken bieden in ieder geval een grotere bescherming dan met de huidige stemmachines mogelijk is, vinden de experts.