

18/09/03
200 30 53329

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



162162

(43) International Publication Date
3 October 2002 (03.10.2002)

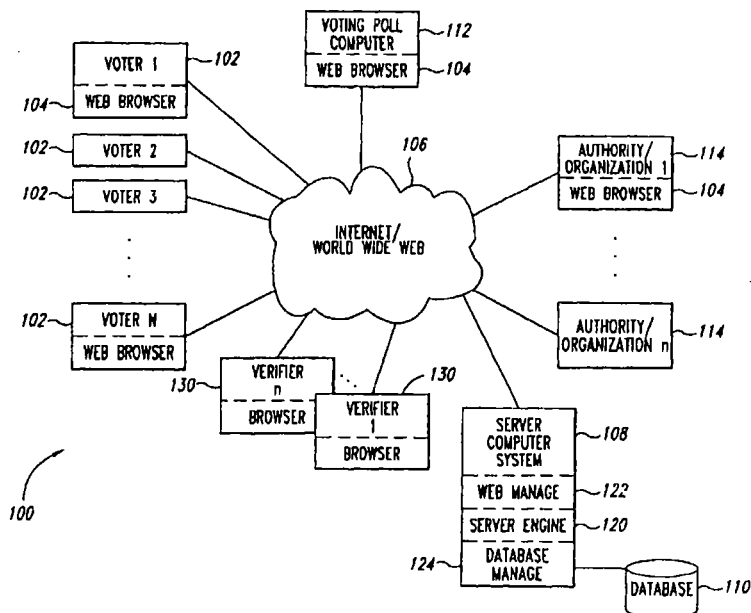
PCT

(10) International Publication Number
WO 02/077929 A3

- (51) International Patent Classification⁷: G07C 13/00, G06F 17/60
- (72) Inventor; and
(75) Inventor/Applicant (for US only): NEFF, Andrew, C. [US/US]; Suite 250, 3101 Northup Way, Bellevue, WA 98004 (US).
- (21) International Application Number: PCT/US02/09264
- (22) International Filing Date: 25 March 2002 (25.03.2002)
- (74) Agents: DALEY-WATSON, Christopher, J. et al.; Perkins Coie LLP, 1201 Third Avenue, Seattle, WA 98101 (US).
- (25) Filing Language: English
- (26) Publication Language: English
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.
- (30) Priority Data:
09/816,869 24 March 2001 (24.03.2001) US
60/311,680 9 August 2001 (09.08.2001) US
60/312,671 15 August 2001 (15.08.2001) US
60/313,003 16 August 2001 (16.08.2001) US
- (71) Applicant (for all designated States except US): VOTE-HERE, INC. [US/US]; Suite 250, 3101 Northup Way, Bellevue, WA 98004 (US).
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: VERIFIABLE SECRET SHUFFLES AND THEIR APPLICATION TO ELECTRONIC VOTING



(57) Abstract: We present a mathematical construct which provides a cryptographic protocol to (verifiably shuffle) a sequence of (k) modular integers, and discuss its application to secure, universally verifiable, multi-authority election schemes. The output of the shuffle operation is another sequence of (k) modular integers, each of which is the same secret power of a corresponding input element, but the order of elements in the output is kept secret. Though it is a trivial matter for the "shuffler" (who chooses the permutation of the elements to be applied) to compute the output from the input, the construction is important because it provides a linear size proof of correctness for the output sequence (i.e. a proof that it is of the form claimed) that can be checked by one or more arbitrary verifiers. The protocol is shown to be honest-verifier zeroknowledge in

a special case, and is computational zeroknowledge in general. On the way to the final result, we also construct a generalization of the well known Chaum-Pedersen protocol for knowledge of discrete logarithm equality ([3], [2]). In fact, the generalization specializes (exactly) to the Chaum-Pedersen protocol in the case $(k)=2$. This result may be of interest on its own. An application to electronic voting is given that matches the features of the best current protocols with significant efficiency improvements. An alternative application to electronic voting is also given that introduces an entirely new paradigm for achieving (Universally Verifiable) elections.

WO 02/077929 A3



ACTION

WO 02/077929 A3

European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

(88) Date of publication of the international search report:

21 November 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.