(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日:
2002年3月28日(28.03.02)

PCT

(10) 国际公布号:
WO 02/25860 A1

(51) 国际分类号[7]: H04L 9/00

(21) 国际申请号: PCT/CN01/01401

(22) 国际申请日: 2001年9月17日(17.09.01)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
00124551.1 2000年9月20日(20.09.00) CN

(71)(72) 发明人/申请人: 慈孟夫(CI, Mengfu) [CN/CN]; 中国湖南省长沙市新开铺路 39 号, Hunan 410009 (CN)。

(74) 代理人: 广州专利事务所(GUANGZHOU PATENT AGENCY); 中国广东省广州市仓边路87号四楼, Guangdong 510030 (CN)。

(81) 指定国(国家): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, 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, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW

(84) 指定国(地区): ARIPO专利(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), 欧亚专利(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲专利(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI专利(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

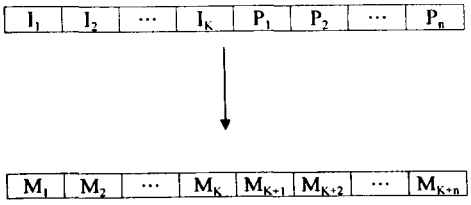
根据细则4.17的声明:
— 关于申请人在国际申请日有权申请并被授予专利(细则4.17(ii))对所有指定国
— 发明人资格(细则4.17(iv))仅对美国

本国际公布:
— 包括国际检索报告。

所引用双字母代码和其它缩写符号，请参考刊登在每期PCT公报期刊起始的"代码及缩写符号简要说明"。

(54) Title: THE DYNAMIC IDENTIFICATION METHOD WITHOUT IDENTIFICATION CODE

(54) 发明名称: 无标识全动态认证方法



(57) **Abstract:** The invention provides a dynamic identification method that has no identification code. A User terminal trnasfers the user's original identification code and ID codes which have been encrypted to the server, and the server confirms the user's ID after decrypting them. The method provided by the invention dynamic encrypts user's original identifier and ID codes, so when user ID is identified every time, because the same user comes to each different results every encryption, there isn't a static identification or character to be distinguished. It makes an attacker have no way to trace, record and analyse a user's ID information. And it makes an attacker who wants to disclose one user's ID information have to disclose all users'. Therefore, the method brings us much more security than before.

[见续页]

WO 02/25860 A1

(57) 摘要

本发明公开了一种无标识全动态认证法，用户终端将用户的原始认证标识码和认证码进行动态加密后传送至服务器，服务器对动态的认证标识码和认证码解密后进行用户身份确认。本发明采用的认证方法，由于对认证标识码和认证码均进行一动态加密，故用户每次进行身份认证时，由于每次加密所得的结果均不相同，没有一个静态标识和特征可供辨识，使攻击者无法对用户的认证信息进行跟踪、记录、分析。实际上造成攻击者破解某一用户的变化规律变成了破解所有用户的变化规律，具有更高的安全性。