عنوان مقاله:
یک طرح غیر تعاملی و وارسی پذیر عمومی برای بازیابی قانونی کلید

محل انتشار:
دوازدهمین کنفرانس سالانه انجمن کامپیوتر ایران (سال: 1385)

تعداد صفحات اصل مقاله: 9

نویسندگان:
احسان جهانگیری - *دانشگاه صنعتی شریف - دانشکده مهندسی برق - تهران - ایران*

جواد مهاجری - *دانشگاه صنعتی شریف - پژوهشکده الکترونیک - تهران - ایران*

خلاصه مقاله:
طرح های بازیابی قانونی کلید (Key Escrow) اولین بار در سال 1993 توسط دولت ایالات متحده آمریکا و بمنظور تامین توام محرمانگی کاربران و توانایی شنود مکالمات درمواضع ضروری پیشنهاد شدند. Shamir در سال 1995 برای جلوگیری از رمز گشایی وسیع اطلاعات کاربراین که ارگان های اعمال قانون، مجاز به رمز گشایی اطلاعاتشان نیستند، طرح Prtial Key Escrow را پیشنهاد داد. در این مقاله یک طرح جدید Public Verifiable Partial Key Escrow (PVPKE)) معرفی شده است. این طرح نسبت به طرح PVPKE , Mao ترافیک کمتری را برای شبکه به همراه دارد. طرح پیشنهادی همچنین دارای ویژگی بازیابی متاخر است بدین معنی که حتی هنگامی که TTPها بخش قابل بازیابی (Escrow شده) کلید را بدست اوردند هنوز 2 مرحله برای یافتن کلید محرمانه زمان لازم است. تقلب در این طرح (بعمنی بازیابی راز برای مجموعه غیر مجاز TTP ها) معادل حل مساله Diffie-Hellman است. این طرح علاوه بر عدم نیاز به بر خط بودن تمامی TTPها هنگام Escrow کردن کلید (که از خصوصیات طرح های Publicly Verifiable است)، می تواند بصورت غیر تبادلی پیاده سازی شود.

کلمات کلیدی:
Publicly Verifiable Partial Key Escrow , Publicly Verifiable Secret Sharing , Discrete Logarithm