Abstract

Teza de doctorat tratează într-un mod unitar problema securizării datelor în transmisiile wireless, cu exemple de implementare pentru aplicaţiile care rulează pe terminalele mobile. Din multitudinea de aspecte legate de protecţia datelor, s-a ales doar partea legată de autentificare pentru dezvoltarea algoritmilor criptografici. Aceasta reprezintă prima parte din cadrul protocolului de transmisie a datelor şi poate fi efectuată prin mai multe metode, dar cele bazate pe matematica curbelor eliptice prezintă posibilităţi noi de construire a unor scheme, superioare din punctul de vedere al proprietăţilor.

Limbajul Java a fost ales pentru construirea aplicaţiilor, având în vedere multitudinea de protocoale deja implementate în acest limbaj (sub formă de librării) şi mai ales portabilitatea acestuia din punct de vedere hardware prin intermediul sistemului de operare Android. Rularea aplicaţiilor a fost efectuată în mediul real cât şi în mediul simulat.

Fundamentul pentru toţi algoritmii prezentaţi este dat de calcularea ecuaţiei matematice a curbelor eliptice pe baza parametrilor predefiniţi. În acest sens este îmbunătăţită metoda de construire a polinomului Hilbert cu ajutorul căruia se poate extrage determinantul. Pentru metodele care nu utilizează acest polinom s-a dezvoltat o nouă metodă, derivată din algoritmul principal Cocks-Pinch, care tratează curbele cu grad de incluziune egal cu 1, deoarece acestea sunt avantajoase din punctul de vedere al calculelor şi a abordării teoretice.

Dintre metodele de autentificare, cele care nu transmit informaţia privată între părţi (cunoaştere zero) sunt preferate pentru mediul de transmisie wireless. Acestea sunt dezvoltate şi unificate într-un cadru generic. Au fost analizate performanţele faţă de algoritmii publici din domeniu, o reprezentare particulară fiind dată de iniţializarea algoritmului cadru pentru un număr diferit de parametrii. Analiza ţine cont de volumul de calcule şi de numărul de transmisii necesare în vederea efectuării protocolului, acest lucru fiind foarte important pentru terminalele mobile, pentru care energia constituie o resursă limitată.

Algoritmii de securizare prezentaţi prin metoda criptării cu vector ascuns sau a criptării neclare şi anonime reprezintă o nouă ramură în cadrul cercetărilor la nivel mondial referitoare la posibilităţile de construire a protocoalelor din punctul de vedere al protecţiei datelor. Ei au ca fundament teoretic teoria criptării bazate pe identitate, dar nu au aceeaşi structură. Acest tip de algoritmi sunt de dată relativ recentă (după anul 2000) şi utilizează exclusiv proprietăţile operaţiei de împerechere, specifică curbelor eliptice. Ambele tipuri de scheme permit utilizarea atributelor de tip "nu contează", care permit transmiterea mesajelor criptate în modul broadcast. Prin combinarea tehnicilor specifice algorimilor de tip neclar cu cei de bazaţi pe identitate neclară a rezultat un nou tip de algoritmi, care rezolvă problema caracterului anonim al identităţii cerute de partea care emite mesajul. Schema prezentată reprezintă o adăugare care poate fi folosită pentru orice tip de criptare bazată pe identitate.

This PhD thesis treats the problem of data security in wireless transmissions in an unitary way, with examples of implementation for application running on mobile devices. From the multitude of data protection issues, in order to develop cryptographic algorithms was chosen only the authentication part. This is the first one that occurs in the data transmission protocol and can be done through several methods, but those based on elliptic curves mathematics presents new possiblities of building schemas, that are superior from the properties point of view.

Java language was chosen for building applications, given the multitude of protocols already implemented in this language (as libraries) and its portability especially in terms of hardware through the Android operating system. Running of the programs was performed with the real device and in the simulated environment.

Computation of the mathematical equations of elliptic curves, based on pre-defined parameters is the basis for all the presented algorithms. For this it is improved the process of building the Hilbert polynomial from which the elliptic curve determinant can be extracted. For those methods that are not using this polynomial, a new method derived mainly from the main Cocks-Pinch one was developed. It treats the curves with embedding degree 1 because they are advantageous in terms of computing and theoretical approach.

Among the authentication methods, the ones which do not transmit sensitive informations between the involved parties (zero-knowledge) are preferred for wireless transmission medium. These are developed and unified into a generic framework. The performances were analyzed regarding available public domain schemas, a particular representation arising from the generic framework customization with a different number of parameters. The analysis takes into account the volume of calculations and the number of transmissions required to carry out the protocol. This number is very important for mobile devices because in their case the energy represents a limited resource.

Security algorithms represented by the hidden vector or anonymous fuzzy identity based encryption form a new branch in the global research on the possibilities of building protocols in terms of data protection. They present the same underlying theoretical theory, but their structure is different. This kind of algorithms is relatively recent (after 2000) and are based only on the pairing operation properties which is specific to elliptic curves. Both kind of schemas permits "don't care" attributes, which permits the broadcast of the encrypted message. By combining specific techniques like fuzzy ones and the fuzzy identity based encryption results a new family of algorithms which solves the anonymous property of the identity requested by the part that transmits the message. The presented algorithm represents an add-on to the existing identity based schemas.

Tudor Bogdan