BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 2(81), 2016, Pages 40–44
ISSN 1024–7696

Asymmetric ID-Based Encryption System, Using an Explicit Pairing Function of the Reciprocity Law

S. V. Vostokov, R. P. Vostokova, I. A. Budanaev

Abstract. In this paper, we describe a new approach for building an asymmetric ID-based encryption (**IBE**) system and an authentication protocol without disclosure, using the idea of Explicit Hilbert Pairing.

Mathematics subject classification: 11A15, 11F33, 11T71.
Keywords and phrases: ID-based systems, Asymmetric Encryption, Explicit Pairing, Reciprocity Law, Hilbert's Ninth Problem, Frobenius Operator, Protocol, Explicit Hilbert Pairing.

1 Introduction

This paper proposes a new approach for creating ID-based systems, using the Explicit Pairing Reciprocity Law from works [1, 2]. The Reciprocity Law was first examined by P. Fermat, when he proved that $x^2 + 1$ is divisible by a prime number p, for some integer x, if and only if $p = 4k + 1$. The Quadratic Reciprocity Law for Legendre exponential symbols was formulated by L. Euler and proved by C. F. Gauss in the 18th century. In the 19th century attempts were made to obtain an explicit formula for the product of the symbols of power residues in an arbitrary number field, containing the necessary roots of 1. Partial results were obtained by Kummer, Dirichlet and Eisenstein. After new insight about the deep analogy of algebraic numbers and algebraic functions was proposed by L. Kroneker, Hilbert implemented this idea and devised a plan to obtain an Explicit Reciprocity Law (Hilbert's 9th problem, 1900). The first part of this plan was the construction of field theory of classes which was completed in the early 20th century by mathematicians such as W. Furtwängler, T. Takagi, E. Artin, and H. Hasse. This theory reduces the calculation of the product of global power residues to the product of local normed residue symbols (pairing or Hilbert symbol). The first explicit, but not complete formula for this pairing in the circumferential extension of the p-adic numbers of field Q_p, were found in 1928 by E. Artin and H. Hasse. In 1950 I. R. Shafarevich constructed the basis of the multiplicative group of a local field (finite extension of the p-adic Q_p numbers), on the elements of which he proposed the method for calculating the Hilbert pairing. Definitive and complete formulas for the Hilbert Pairing were obtained by S. Vostokov in 1978 [1], and later independently by H. Bruckner [3].

In this paper we use the Explicit Hilbert Pairing from [1], in the case of a circular field $Q_p(\xi)$, where ξ is a primitive root of degree p of 1 (see Section 2), for the authentication protocol without disclosure (see Section 3).

2 Explicit Hilbert Pairing

Consider the multiplicative group of power series $U = 1 + XZ_p[X]$. Let Δ be the Frobenius Operator on the ring of Laurent Series $Z_p[X]$, acting on series $f(X)$ of $Z_p[X]$ as follows:

$$\Delta f(X) = f^{\Delta}(X) = f(X^p).$$

Further, we define the function $l(f(X))$ for series $f(X)$ from the group $U(X)$:

$$l(f(X)) = \frac{1}{p} \log \frac{f(X)^p}{f(X)^{\Delta}}.$$

Lemma 1. *The function $l(f)$ has integer coefficients in Z_p. In addition, $l(f)$ has the following properties:*

1. *$l(f(X)g(X)) = l(f(X)) + l(g(X))$*
2. *$l(f(X)^a) = al(f(X))$*

for series $f(X)$ and $g(X)$ of group $U(X)$ and the integer a of Z_p.

Proof. The first property was proven in ([4], *Lemma* 2). The second property follows from the corresponding property of the logarithm and the additive property of the operator Δ. □

We now define the pairing $< *, * >$ on $U(X) \times U(X)$ by the formula

$$< f(X), g(X) >= \{res_x(l(f(X))\frac{d}{dX}\log g(X) - l(g(X))\frac{d}{dX}\frac{\Delta}{p}\log f(X))X^{-p}\} \bmod p.$$

Proposition 1. *The pairing $< *, * >$ has the following properties:*

1. *It is bilinear, i.e.*
   $< f_1 f_2, g >=< f_1, g > + < f_2, g >$,
   $< f^a, g >= a < f, g >$
   for series f_1,f_2,g, of $U(X)$ and an integer a of Z_p, and similar equalities for the second argument.
2. *It is skew-symmetric, i.e.*
   $< f, g > + < g, f >= 0$.

Proof. Bilinearity of the pairing follows from the corresponding properties of the function $l(f)$ and logarithm. Let us now prove the skew-symmetry. We denote

$$\Phi(f, g) = l(f)d\log g - l(g)d\Delta\log f.$$

From the definition of the function $l(f)$ it follows that

$$\Phi(f,g) = l(g)dl(f) - l(g)d\log f + l(f)d\log g,$$

therefore

$$\Phi(f,g) + \Phi(g,f) = l(f)dl(g) + l(g)dl(f) = d(l(f)l(g)).$$

We conclude that

$$< f, g > + < g, f >= \{res_x(d(l(f)l(g))X^{-p}\} \equiv \{res_x(d(l(f)l(g))X(-p)\} \equiv 0 \bmod p$$

and skew-symmetry of the pairing is proved. □

Remark 1. The pairing $< *, * >$ has the property of independence of each of the arguments too. For that, let $Eis(X)$ be the Eisenstein irreducible polynomial of degree $p-1$,

$$Eis(X) = \frac{((1+X)^p - 1)}{X^p},$$

and let $r(X)$ be the remainder from the division of $f(X) - 1$ by polynomial $u(X)$. Then

$$< f(X), g(X) >=< r(X), g(X) > .$$

Remark 2. Properties of the pairing $< *, * >$ from Proposition 2, are similar to those of the Weil pairing and are proven in [1, 2]. For the general case see [5], Chapter VII).

3 Authentication Protocol without Disclosure

Proof of security of the protocol under discussion is determined by the properties of the proposed pairing function and non-polynomial complexity problem of the discrete logarithm in a polynomial ring with integer coefficients, which in general case is polynomially reduced to the discrete logarithm in finite fields [4].

3.1 Protocol Parameters and its Members

Let A (Alice) and V (verifier) be the members of the protocol. The secret known by Alice is some polynomial $a(X)$ of the group $U(X)$. Both parties of the protocol know the number s, the polynomial $Eis(X)$ and the polynomial $A(X) = a^s \mod Eis(X)$. According to the classical problem of authentication protocol without disclosure, Alice must prove to the verifier her knowledge of the secret polynomial $a(X)$, without disclosing it.

3.2 The Choreography of the Protocol

1. Alice selects a random polynomial $r(X)$ and determines the polynomial $R(X) = r(X)^s \mod Eis(X)$
2. Alice sends to the verifier the value of $R(X)$
3. V can request from A one of the following responses
   - the first response is the polynomial
     $$z(X) :< z(X), R(X) >= s < z(X), z(X) >$$
   - the second response is the polynomial
     $$y(X) :< y(X), R(X)A(X) >= s < y(X), y(X) > .$$
4. For the first response, A uses the known polynomial $r(X)$ and forms the polynomial $z(X) = r(X)$. For the second response, Alice uses the secret polynomial $a(X)$ to calculate the polynomial $y(X) = r(X)a(X) \mod Eis(X)$
5. V verifies the correctitude of the answers of A
   - for the first response
     $$< z(X), R(X) >=< r(X), r(X)^s >= s < r(X), r(X) >,$$
   - for the second response:
     $$\begin{aligned} < y(X), R(X)A(X) > &=< r(X)a(X), R(X)A(X) > \\ &= s < r(X)a(X), r(X), a(X) > \\ &= s < y(X), y(X) > . \end{aligned}$$

The above steps are performed until the verifier is convinced that Alice knows the secret polynomial $a(X)$. All the properties of the given protocol correspond to the properties of the classic authentication protocol without disclosure.

4 Final Remarks

In this paper, we propose a new system authentication protocol without disclosure. The system uses the idea of Explicit Hilbert Pairing of the Reciprocity Law (see [1, 2]). Explicit Hilbert pairing is used because it is bilinear and skew-symmetric (see Section 2). These properties make it interesting and paramount to building the system's protocol. The principle described in this paper can not only be used in other applications, like digital signature, but also as an extension to other security models.

Acknowledgments. The first author of the present paper was supported by RFFI grant number 14-01-00393.

References

[1] Vostokov S. V. *Explicit form of the law of reciprocity.* Math. of the USSR-Izvestiya 1979, **13**, No. 3, 557–588 (English Translated: Izvestiya AN SSSR, Ser. Matem., 1978, **42**:6, 1288–1321).

[2] Vostokov S. V. *Hilbert symbol in a discrete valuated field.* Journal of Soviet Mathematics, 1982. **19**, Issue 1, 1006–1019 (English Translated: Zap. Nauchn. Sem. LOMI, 1979, **94**, 50–69).

[3] Brueckner H. *Hilbert symbole zum Exponenten p^n und Pfaffische Formen.* Hamburg, 1979, 788 p.

[4] Markelova A. V. *Discrete logarithm in an arbitrary quotient ring of polynomials of one variable over a finite field.* Diskr. Mat., 2010, **20**, Issue 2, 120–132 (English Translated: Discrete Mathematics and Applications, 2010, **20**, No. 2, 231—246).

[5] Fesenko I. B., Vostokov S. V. *Local Fields and Their Extensions.* Translations of Mathematical Monographs, **121**, AMS, 1993.

Received December 6, 2015

S. V. Vostokov
Sankt-Petersburg State University
E-mail: *s.vostokov@spbu.ru*

R. P. Vostokova
Baltic State Technical University "VOENMEH"
E-mail: *rvostokova@yandex.ru*

I. A. Budanaev
Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
E-mail: *ivan.budanaev@gmail.com*