Mathematical Research Letters **6**, 287–291 (1999)

AN ALGEBRAIC METHOD FOR PUBLIC-KEY CRYPTOGRAPHY

Iris Anshel, Michael Anshel, and Dorian Goldfeld

Abstract. Algebraic key establishment protocols based on the difficulty of solving equations over algebraic structures are described as a theoretical basis for constructing public–key cryptosystems.

1. Introduction

A *protocol* is a multi–party algorithm, defined by a sequence of steps, specifying the actions required of two or more parties in order to achieve a specified objective. Furthermore, a *key establishment* protocol is a protocol whereby a shared secret becomes available to two or more parties, for subsequent cryptographic applications (see [7]).

We present a compact algebraic key establishment protocol, followed by a group–theoretic illustration, for secret key establishment between two individuals whose only means of communication is a public channel. The foundation of the method lies in the difficulty of solving equations over algebraic structures, in particular groups. The protocol requires each party to perform an algebraic computation (several multiplications followed by rewriting in a monoid or group). The results of the computation are then exchanged between the parties over a public channel and a common shared secret key is then obtained by each party after a second computation is performed. The second computation involves an algorithm to solve the word problem in the monoid or group.

In the case that the protocol is group–based, we show that an adversary (observing all communication over the public channel) can break the scheme and determine the secret key provided a system of conjugacy equations over the associated group is feasibly solvable. This is in contrast to the method proposed in [1]. A very different but loosely related construction (encryption using rewrite systems) is given in [5].

It is known that there exist groups where the word problem is solvable and the conjugacy problem is unsolvable [8]. Further, there are many groups where the word problem is known to be solvable in polynomial time while there is no

Received March 31, 1999.

known polynomial time algorithm to solve the conjugacy problem. An example is the braid group on n strands where the word problem for a word w (of length $|w|$) can be solved in running time $O(|w|^2 n)$ while the best known algorithm for solving the conjugacy problem requires at least exponential running time (see [2]).

Recent developments in mathematical and computational cryptanalysis (see [3,9]) have renewed interest in developing new cryptographic methods. These methods include public–key cryptography based on hidden monomial systems, combinatorial–algebraic systems, and the theories of elliptic and hyperelliptic curves (see [6]).

2. The algebraic key establishment protocol

We now present an algebraic key establishment protocol which, in its most general form consists of a five–tuple $(\mathbf{U}, \mathbf{V}, \beta, \gamma_1, \gamma_2)$ where $\mathbf{U}$ and $\mathbf{V}$ are feasibly computable monoids, and

$$\beta : \mathbf{U} \times \mathbf{U} \longrightarrow \mathbf{V}, \qquad \gamma_i : \mathbf{U} \times \mathbf{V} \longrightarrow \mathbf{V} \quad (i = 1, 2)$$

are feasibly computable functions satisfying the following properties.

(i) For all elements $x, y_1, y_2 \in \mathbf{U}$,

$$\beta(x, y_1 \cdot y_2)) \;=\; \beta(x, y_1) \cdot \beta(x, y_2).$$

(ii) For all elements $x, y \in \mathbf{U}$,

$$\gamma_1(x, \beta(y, x)) = \gamma_2(y, \beta(x, y)).$$

(iii) Suppose $y_1, y_2, \ldots y_k \in \mathbf{U}$ and $\beta(x, y_1), \beta(x, y_2), \ldots, \beta(x, y_k)$ are publicly known for some secret element $x \in \mathbf{U}$. Then, in general, it is infeasible to determine the secret element x.

The users A and B are publicly assigned submonoids, $S_A, T_B \subseteq U$, respectively. Suppose that S_A is generated by the elements

$$\{s_1, \ldots, s_m\},$$

and S_B is generated by $\{t_1, \ldots, t_n\}$. The protocol begins with user A choosing a secret element a in S_A and transmitting the elements

$$\beta(a, t_i) \qquad\qquad i = 1, \ldots, n.$$

Likewise, user B chooses a secret element b in T, transmits

$$\beta(b, s_i) \qquad\qquad i = 1, \ldots, m.$$

It follows from property (iii) that even though the transmission is over a public channel, the secret elements a and b are secure. Property (i) above insures that user A can compute the element

$$\beta(b, a),$$

and

$$\gamma_1(a, \beta(b, a)).$$

Likewise user B can compute $\beta(a, b)$ and $\gamma_2(b, \beta(a, b))$. Recalling property (ii) above we see that

$$\kappa \;=\; \gamma_1(a, \beta(b, a)) \;=\; \gamma_2(b, \beta(a, b))$$

can serve as an established key.

3. A group theoretic protocol

In this illustration the monoid $\mathbf{U} = \mathbf{V}$ is a group, denoted $\mathbf{G}$, and the users A and B are publicly assigned subgroups

$$S_A \;=\; \langle s_1, s_2, \ldots, s_m \rangle, \qquad S_B \;=\; \langle t_1, \ldots, t_n \rangle.$$

Here the function $\beta : \mathbf{G} \times \mathbf{G} \to \mathbf{G}$ is chosen to be conjugation,

$$\beta(x, y) \;=\; x^{-1} y\, x,$$

and the functions γ_1, γ_2 are simply

$$\gamma_1(u, v) = u^{-1} v, \qquad \gamma_2(u, v) = v^{-1} u.$$

Users A and B choose secret elements $a \in S_A$ and $b \in S_B$ respectively, and user A begins the protocol by computing, rewriting, and transmitting the collection of elements

$$a^{-1} t_1 a,\; a^{-1} t_2 a,\; \ldots, a^{-1} t_n a.$$

Similarly, user B computes, rewrites, and transmits

$$b^{-1} s_1 b,\; b^{-1} s_2 b,\; \ldots, b^{-1} s_m b.$$

An adversary observing these transmissions is unable to determine a or b unless (s)he can solve a set of simultaneous conjugacy equations over the base group.

Multiplying two elements in the group can be accomplished by simply concatenating the two expressions representing the elements. The process of rewriting, while not unique, must be chosen so that no adversary can determine the conjugating element from viewing the publicly transmitted conjugates.

Recalling that the conjugate of the product of two elements is the product of the conjugates of those elements (i.e., property (i) of β), users A and B are now in a position to compute, respectively, the elements

$$\beta(b,a) \;=\; b^{-1}ab, \qquad \beta(a,b) \;=\; a^{-1}ba.$$

In order to attain a common key, user A computes

$$\kappa \;=\; \gamma_1(a,\beta(b,a)) \;=\; a^{-1}b^{-1}ab \;=\; [a,b],$$

and user B computes

$$\kappa \;=\; \gamma_2(b,\beta(a,b)) \;=\; [a,b].$$

At this point each user has obtained the key κ in a (usually different) rewritten form.

There are several methods to extract a common (identical) element. If there is a feasible algorithm to put every word in the group in canonical form, the canonical form algorithm can then be applied. There are many groups, however, where the canonical form algorithm has a slow running time while an algorithm to solve the word problem (determine if a word is the identity element) runs considerably faster. In such a case it may be more efficient to obtain a common key by having user B either send a rewritten form of κ or some other random word (not equal to κ) in the group to user A. User A can then use the word problem algorithm to determine if κ was sent or not. If κ was sent then this determines the bit 1, otherwise the bit 0. By iterating m times, an m–bit common key is exchanged. This protocol is probabilistic and generally slower than the canonical form algorithm referred to above. It is also worth noting, that to extract a common key, it suffices to have any well defined easily computable function from $\mathbf{G}$ to any set whose elements have an easily computable canonical form.

The construction of an algebraic key establishment protocol employing braid groups is particularly promising. This is due to the fact that the best known algorithm to solve the conjugacy problem requires at least exponential running time. Furthermore, there are two different algorithmic approaches to the word problem. Both the Birman, Ko, Lee (see [2]) canonical form for elements in the braid group and the Dehornoy method (see [4]) of comparing braids can be employed to rewrite publicly known elements and to obtain a common element once an exchange has been completed.

Acknowledgments

The authors wish to thank Professor Joan Birman of Columbia University for helpful discussions. We also thank the referees for their careful review and suggestions.

The authors wish to gratefully acknowledge the financial support of Arithmetica Inc. in the preparation of this paper. All works and inventions described in this paper were for the benefit of, and were funded by Arithmetica Inc.

References

[1] I.L. Anshel and M. Anshel, *From the Post-Markov theorem through decision problems to public-key cryptography*, Amer. Math. Monthly **100** (1993), 835–844.

[2] J.S. Birman, K.H. Ko, and S.J. Lee, *A new approach to the word and conjugacy problems in the braid groups*, Adv. Math. **139** (1998), 322-353.

[3] D. Boneh, *Twenty years of attacks on the RSA cryptosystem*, Notices Amer. Math. Soc. **46** (1999), 203–213.

[4] P. Dehornoy, *A fast method for comparing braids*, Adv. Math. **125** (1997), 200–235.

[5] Do Long Van, A. Jeyanthi, R. Siromoney, and K.G. Subramanian, *Public key cryptosystems based on word problems*, ICOMIDC Symp. Math. of Computation, Ho Chi Minh City, April 1988.

[6] N. Koblitz, *Algebraic aspects of cryptography*, Algorithms and Computation in Mathematics, 3., Springer-Verlag, Berlin, 1998.

[7] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of applied cryptography*, CRC Press Series on Discrete Mathematics and its Applications., CRC Press, Boca Raton, FL, 1997.

[8] C.F. Miller III, *On group-theoretic decision problems and their classification*, Annals of Mathematics Studies, No. 68., Princeton University Press, Princeton, NJ, 1971.

[9] P.C. van Oorschot and M.J. Wiener, *Parallel collision search with cryptanalytic applications*, J. Cryptology **12** (1999), 1–28.

Arithmetica Inc., 31 Peter Lynas Ct. Tenafly, NJ 07670

Department of Computer Sciences, City College of New York, New York, NY 10031

Department of Mathematics, Columbia University, New York, NY 10027