Some applications of idempotent semirings in Public Key Cryptography

Mariana Durcheva
Technical University of Sofia (Bulgaria)

mdurcheva66@gmail.com

Abstract

A set S equipped with two algebraic operations: addition and multiplication is called a *semiring* if the following conditions are satisfied: both operations are associative; the addition is commutative; the multiplication is distributive with respect to the addition

$$a.(b+c) = (a.b) + (a.c) \text{ and } (a+b).c = (a.c) + (b.c) \ \forall a, b, c \in S \ .$$

A semiring S is called an *idempotent semiring* if $a + a = a$ for all $a \in S$.

Employing additively idempotent semirings semirings as a platform for a cryptographic scheme arose several years ago. In the present work we show how to apply different dual pairs of idempotent semirings for constructing new cryptographic protocol. We are interested in four idempotent semirings:

Max-plus semiring: Consider $R_{max} = R \cup \{-\infty\}$. Given $a, b \in R_{max}$, define: $a \oplus b = max\{a, b\}$; $a \odot b = a + b$. If we add the top element $\top = +\infty$ to this set, the resulting semiring is complete and denoted by $\overline{R_{max}}$.

Min-plus semiring: Consider $R_{min} = R \cup \{+\infty\}$. Given $a, b \in R_{+\infty}$, define: $a \oplus b = min\{a, b\}$; $a \odot b = a + b$. If we add the top element $\perp = -\infty$ to this set, the resulting semiring is complete and denoted by $\overline{R_{min}}$.

Max-time semiring: Consider $R_{max,\times} = R^+ \cup \{+\infty\}$ (non-negative real numbers). Given $a, b \in R_{max,\times}$, define: $a \oplus b = max\{a, b\}$; $a \otimes b = a.b$.

Min-time semiring: Consider $R_{min,\times} = R^+ \cup \{+\infty\}$ (non-negative real numbers). Given $a, b \in R_{min,\times}$, define: $a \oplus b = min\{a, b\}$; $a \otimes b = a.b$.

We give a generalization of the Diffie-Hellman key exchange protocol, to the context of semigroup actions. Our protocol in its most general form consists of the following:

two commutative semirings S_1, S_2 act on a set X i.e. $((S_1 \times S_2) \times X) \to X$.

We propose two practical realizations of this scheme based on different dual pairs of idempotent semirings. For the semirings S_1 and S_2 we suggest commutative semirings generated by two given matrices M and N. These semirings are semirings of polynomials in M and N with coefficient of two dual pairs of idempotent semirings. Set X should be selected carefully with respect to the chosen semirings.

In the first protocol: $S_1 = M_n(\overline{\mathbf{R}}_{\mathbf{max}}), S_2 = M_n(\overline{\mathbf{R}}_{\mathbf{min}}), M \in M_n(\overline{\mathbf{R}}_{\mathbf{max}}), N \in M_n(\overline{\mathbf{R}}_{\mathbf{min}}), X \in M_n(\overline{\mathbf{R}})$.

In the second protocol: $S_1 = M_n(\mathbf{R}_{\mathbf{max},\times})$, $S_2 = M_n(\mathbf{R}_{\mathbf{min},\times})$, $M \in M_n(\mathbf{R}_{\mathbf{max},\times})$, $N \in M_n(\mathbf{R}_{\mathbf{min},\times})$, $X \in M_n(\mathbf{R}^+)$.

Keywords

Cryptographic protocol, Idempotent semirings, Semiring action