Simple Semirings and Post-Quantum Cryptography

Jens Zumbrägel

Institut für Algebra, Fachbereich Mathematik
TU Dresden

Laboratory for Cryptologic Algorithms
EPFL, Lausanne

AAA 93 · Bern, Feb 2017
Outline

Introduction to Simple Semirings

Semigroup Actions and Post-Quantum Cryptography

Finite Simple Semirings

Open Problems and Further Research
Semirings

Consider the natural numbers $\mathbb{N} = \{0, 1, 2, 3, \ldots \}$ with the usual operations $+$ and $\cdot$. For $a, b, c \in \mathbb{N}$ there holds:

\[
(a + b) + c = a + (b + c) \quad \text{: (}$\mathbb{N}$, $+$) is a commutative semigroup
\]
\[
a + b = b + a
\]

\[
(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{: (}$\mathbb{N}$, $\cdot$) is a commutative semigroup
\]
\[
a \cdot b = b \cdot a
\]

\[
(a + b) \cdot c = a \cdot c + b \cdot c \quad \text{: distributive laws}
\]
\[
a \cdot (b + c) = a \cdot b + a \cdot c
\]

\[
0 + a = a, \quad 0 \cdot a = 0 = a \cdot 0 \quad \text{: zero element}
\]

$(\mathbb{N}, +, \cdot, 0)$ is a commutative semiring with zero
Semirings

Definition

A semiring is an algebraic structure \((R, +, \cdot)\) such that:

- \((R, +)\) is a commutative semigroup,
- \((R, \cdot)\) is a semigroup,
- the distributive laws hold.

The semiring is called commutative if \((R, \cdot)\) is commutative.

A semiring \((R, +, \cdot, 0)\) with zero is a semiring with some \(0 \in R\) such that \(0 + a = a\) and \(0 \cdot a = 0 = a \cdot 0\) for all \(a \in R\).

Examples

1. \((\mathbb{N}_{>0} = \{1, 2, 3, \ldots\}, +, \cdot)\) is a commutative semiring
2. \((\mathbb{R}, \text{min}, +)\) is a commutative semiring
3. \((\text{Mat}_{n \times n}(\mathbb{N}), +, \cdot, 0)\) is a semiring with zero
Simple semirings

Definition
A semiring $R$ (with zero) is called simple if any homomorphism $f : R \rightarrow S$ into a semiring $S$ (with zero) is constant or injective. Equivalently, if the only congruences on $R$ are $\Delta_R$ and $\nabla_R$.

Example (Congruences on $\mathbb{N}$)
On $(\mathbb{N}, +, \cdot, 0)$ each congruence $\rho \neq \Delta_{\mathbb{N}}$ is generated by $(k, k+m)$ for some $k, m \in \mathbb{N}$, $m > 0$, and then has index $k+m$.

Examples (Simple semirings)
1. $(\mathbb{B} = \{0, 1\}, \lor, \land, 0)$, the Boolean semiring
2. $(\mathbb{R}, \min, +)$, the tropical semiring
3. $(\mathbb{R}_{>0}, +, \cdot)$
4. $(\text{Mat}_{n \times n}(\mathbb{B}), +, \cdot, 0)$
Outline

Introduction to Simple Semirings

Semigroup Actions and Post-Quantum Cryptography

Finite Simple Semirings

Open Problems and Further Research
“Classical” modern cryptography

Let $g$ be a primitive root modulo a prime $p$. The **discrete logarithm problem (DLP)** is the problem to invert the map

$$\mathbb{Z}_{p-1} \to \mathbb{F}_p^*, \quad a \mapsto g^a.$$

The computational hardness of the DLP is used in public-key cryptography, e.g., in the Diffie-Hellman key exchange protocol.

- Alice: $a \in \mathbb{Z}_{p-1}$
  - $g^a$
  - $g^b$

- Bob: $b \in \mathbb{Z}_{p-1}$

$$k_A = (g^b)^a \quad \quad k_B = (g^a)^b$$
“Interest in [...] quantum-resistant cryptography has recently increased, due to milestones in the development of quantum computing hardware [...]. Consequently, NIST is beginning to prepare for the transition to quantum-resistant cryptography now.”
Quantum attacks

Today’s public-key cryptosystems (key exchange, encryption, digital authentication) rely on

- the *discrete logarithm problem* in a group,
- the *integer factorisation* problem.

In 1994 Shor showed that quantum computers render each of these problems completely broken!

The quantum attacks are based on the *hidden subgroup problem* in finite *abelian groups*.
One-way semigroup actions

Exponentiation can be generalised to *semigroup actions*, where the usual attacks do not apply (Maze, Monico, Rosenthal, 2007).

**Definition**

Let \((A, \cdot)\) be a semigroup and \(X\) be a set. A **one-way action** is an action \(\varphi: A \times X \rightarrow X\) of \(A\) on \(X\) such that

- \(\varphi\) is efficiently computable,
- for random \(x, y \in X\) it is hard to find \(a \in A\) such that \(\varphi(a, x) = y\) (provided that such an \(a\) exists).

**Example (Exponentiation in groups)**

- \(A = (\mathbb{Z}_n, \cdot)\)
- \(X = (G, \cdot)\) is a group of order \(n\) (with hard DLP)
- \(\varphi: (\mathbb{Z}_n, \cdot) \times G \rightarrow G, \quad \varphi(a, x) := x^a.\)
A generalisation of the DLP

Let $\varphi: A \times X \to X$ be a one-way action. Consider the problem:

- given $x, y \in X$ such that there exists $\tilde{a} \in A$ with $\varphi(\tilde{a}, x) = y$
- find $a \in A$ such that $\varphi(a, x) = y$

Algorithms

- **Brute-force search**
  
  \textit{Running time} $O(\min\{|A|, |X|\})$

- **Pollard’s rho** in the “group part” of the semigroup $(A, \cdot)$:
  
  A collision $\varphi(a, x) = \varphi(b, y)$ implies $\varphi(b^{-1}a, x) = y$.
  
  \textit{Running time} $O(\sqrt{|X|})$

Does there exist a square root attack in general?
Generalised Diffie-Hellman

Let \( \varphi : A \times X \to X, (a, x) \mapsto a \cdot x \) be a one-way action. Also, let \( C_A, C_B \subseteq A \) be subsets such that \( ab = ba \) for all \( a \in C_A, b \in C_B \).

Protocol (Z., 2008)

<table>
<thead>
<tr>
<th>Alice</th>
<th>public</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>choose ( a \in C_A )</td>
<td>( x \in X )</td>
<td>choose ( b \in C_B )</td>
</tr>
<tr>
<td>( a \cdot (b \cdot x) )</td>
<td>( a \cdot x \in X )</td>
<td>( b \cdot (a \cdot x) )</td>
</tr>
<tr>
<td>( b \cdot x \in X )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The common key is \( a \cdot (b \cdot x) = ab \cdot x = ba \cdot x = b \cdot (a \cdot x) \).

Relevant problem for security:

• given \( x, y_A = a \cdot x, y_B = b \cdot x \) such that \( ab = ba \)
• find \( k = ab \cdot x \)
Example: Conjugacy in braid groups

Example
Let \( A = X = (G, \cdot) \) be a group and \( \varphi(a, x) := a \cdot x \cdot a^{-1} \).

In particular, braid groups were considered (Ko, Lee et al, 2000). For \( n \geq 2 \) define the braid group \( B_n \) on \( n \) strands by the finite presentation

\[
B_n := \langle \sigma_1, \ldots, \sigma_{n-1} \mid \begin{align*}
\sigma_i \sigma_j &= \sigma_j \sigma_i & \text{if } |i - j| \geq 2 \\
\sigma_i \sigma_j \sigma_i &= \sigma_j \sigma_i \sigma_j & \text{if } |i - j| = 1 \rangle.
\]

Then, \( C_A = \langle \sigma_1, \ldots, \sigma_{m-1} \rangle \) and \( C_B = \langle \sigma_{m+1}, \ldots, \sigma_{n-1} \rangle \) are commuting subsets.
Example: Matrices over semirings

Example (Maze, Monico, Rosenthal, 2007)

Let $R$ be a semiring, and let $M_n(R)$ be the semiring of $n \times n$ matrices. Consider the following \textit{two-sided} semigroup action

$$
\rho: \left( M_n(R) \times M_n(R)^{\text{op}} \right) \times M_n(R) \to M_n(R),
$$

$$
((A_1, A_2), X) \mapsto A_1XA_2.
$$

Restrict the semigroup action to a commutative semigroup $(U, \cdot) \leq (M_n(R), \cdot)$. For example:

$$
U = C[A] = \left\{ \sum_{i=0}^{n} \lambda_i A^i \mid \lambda_i \in C \right\},
$$

where $A \in M_n(R)$ is any matrix and $C$ is the center of $R$. 
Example: Matrices over semirings

Let $U \leq M_n(R)$ be a commutative subsemigroup and let $D \in M_n(R)$ be public.

By commutativity of $U$ we have $K_A = K_B$. 

$K_A = A_1(B_1DB_2)A_2$ 

$K_B = B_1(A_1DA_2)B_2$
Why (simple) semirings?

- **few structure for attacks**
  weakest algebraic structure such that matrix multiplication is associative

- **Pohlig-Hellman-type reduction attack**
  if there exists a nonzero semiring homomorphism

  \[ f : R \rightarrow S \]

  into a smaller semiring \( S \), this induces a homomorphism

  \[ M_n(R) \rightarrow M_n(S) \]

Most interesting are simple semirings.
Outline

Introduction to Simple Semirings

Semigroup Actions and Post-Quantum Cryptography

Finite Simple Semirings

Open Problems and Further Research
Finite simple rings

A semiring \((R, +, \cdot, 0)\) with zero is a ring if \((R, +, 0)\) forms an abelian group, otherwise the semiring is called proper.

A ring \(R\) is simple iff \(\{0\}\) and \(R\) are its only ideals.

**Theorem (cf. Wedderburn-Artin)**

A finite ring \(R\) is simple if and only if one of the following holds:

i) \(R\) is a zero-multiplication ring of prime order,

ii) \(R\) is a matrix ring \(\text{Mat}_{n \times n}(\mathbb{F}_q)\) over a finite field \(\mathbb{F}_q\).
Proper simple semirings

- El Bashir, Hurt, Jančařík, Kepka, 2001: Classification of simple commutative semirings.
- Monico, 2004: Partial classification of finite simple semirings; necessity of idempotent addition \((a + a = a)\) for all \(a \in R\).

Examples

A) \[\begin{array}{ccc}
+ & 0 & 1 & 2 \\
\cdot & 0 & 0 & 0 \\
1 & 1 & 2 & 0 & 1 & 2 \\
2 & 2 & 2 & 2 & 2 & 2
\end{array}\]

B) \[\begin{array}{ccc}
+ & 0 & 1 & 2 \\
\cdot & 0 & 0 & 2 \\
1 & 1 & 2 & 0 & 1 & 2 \\
2 & 2 & 2 & 0 & 2 & 2
\end{array}\]

C) \[\begin{array}{ccc}
+ & 0 & 1 & 2 & 3 & 4 \\
\cdot & 0 & 1 & 0 & 1 & 4 \\
1 & 1 & 3 & 3 & 4 & 0 & 1 & 4 & 4 & 4 \\
2 & 3 & 2 & 3 & 4 & 2 & 3 & 2 & 3 & 4 \\
3 & 3 & 3 & 3 & 4 & 2 & 3 & 4 & 4 & 4 \\
4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4
\end{array}\]

D) \[\begin{array}{ccc}
+ & 0 & 4 & 4 & 4 & 4 \\
\cdot & 0 & 1 & 4 & 4 & 4 \\
4 & 1 & 4 & 4 & 4 & 4 & 4 & 0 & 1 & 4 \\
4 & 4 & 2 & 4 & 4 & 4 & 2 & 3 & 4 & 4 & 4 \\
4 & 4 & 2 & 4 & 3 & 4 & 4 & 4 & 2 & 3 & 4 \\
4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4
\end{array}\]
Proper simple semirings

Examples (cont.)

E) \[\begin{array}{cccccc}
+ & 0 & 1 & 2 & 3 & 4 & 5 \\
0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 2 & 3 & 4 & 5 \\
2 & 2 & 2 & 4 & 4 & 5 \\
3 & 3 & 4 & 3 & 4 & 5 \\
4 & 4 & 4 & 4 & 4 & 5 \\
5 & 5 & 5 & 5 & 5 & 5 \\
\end{array}\] \[\begin{array}{cccccc}
\cdot & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 2 \\
0 & 1 & 2 & 1 & 2 & 2 \\
0 & 0 & 0 & 3 & 3 & 5 \\
0 & 1 & 2 & 3 & 4 & 5 \\
0 & 3 & 5 & 3 & 5 & 5 \\
\end{array}\]

F) \[\begin{array}{cccccc}
+ & 0 & 1 & 2 & 3 & 4 & 5 \\
0 & 0 & 0 & 3 & 3 & 5 \\
1 & 1 & 2 & 3 & 4 & 5 \\
2 & 2 & 2 & 4 & 4 & 5 \\
3 & 3 & 4 & 3 & 4 & 5 \\
4 & 4 & 4 & 4 & 4 & 5 \\
5 & 5 & 5 & 5 & 5 & 5 \\
\end{array}\] \[\begin{array}{cccccc}
\cdot & 0 & 0 & 0 & 3 & 3 & 5 \\
0 & 1 & 2 & 3 & 4 & 5 \\
2 & 2 & 2 & 4 & 4 & 5 \\
0 & 3 & 5 & 3 & 5 & 5 \\
2 & 4 & 5 & 4 & 5 & 5 \\
5 & 5 & 5 & 5 & 5 & 5 \\
\end{array}\]
Residuated maps of lattices

Definition
A map \( f : X \to Y \) of ordered sets \((X, \leq)\) and \((Y, \sqsubseteq)\) is residuated if there is a map \( g : Y \to X \) such that for \( x \in X, y \in Y \) it holds

\[
f(x) \sqsubseteq y \iff x \leq g(y).
\]

If \((X, \leq), (Y, \sqsubseteq)\) are finite lattices with least elements \(0_X\) and \(0_Y\), then \((X \vee 0_X), (Y \sqcup 0_Y)\) are idempotent commutative monoids.

\( f \) is residuated \iff \[
\begin{cases}
f(0_X) = 0_Y, \\
f(x \vee z) = f(x) \sqcup f(z) \text{ for } x, z \in X.
\end{cases}
\]
The semiring of residuated maps

**Proposition**

For any finite lattice \((L, \leq)\) the set

\[ \text{Res}(L, \leq) = \text{End}(L, \lor, 0) \]

of all residuated maps \(L \rightarrow L\) forms a simple semiring with zero.

**Example**

\[ R_6 = \text{Res}(\{0, 1, 2\}, \leq) \]
Finite simple semirings with zero

**Theorem (Z., 2008)**

Let $R$ be a finite proper semiring with zero, $|R| > 2$. T. f. a. e.:

i) $R$ is simple,

ii) there is a non-trivial irreducible $R$-module,

iii) $R$ is a dense subsemiring of $\text{Res}(L)$ for a finite lattice $L$, i.e., containing for all $a, b \in L$ the mapping $e_{a,b}$ defined as

$$e_{a,b}(x) := \begin{cases} 0 & \text{if } x \leq a, \\ b & \text{otherwise.} \end{cases}$$

**Remark**

For *distributive* lattices $L$, a dense subsemiring $S \subseteq \text{Res}(L)$ is already the full semiring, i.e., $S = \text{Res}(L)$. 

Remark
Let $R$ be a finite proper simple semiring.

1. There is an *additively absorbing* element $\infty \in R$, i.e., such that $a + \infty = \infty$ for all $a \in R$.

2. If $R$ has no zero then the element $\infty$ satisfies at least one of

   \[
   \begin{align*}
   \infty \cdot a &= \infty \quad \text{for all } a \in R \quad (\text{left-absorbing}) \\
   a \cdot \infty &= \infty \quad \text{for all } a \in R \quad (\text{right-absorbing})
   \end{align*}
   \]

Proposition
For any finite lattice $L$, where $1_L$ is the greatest element, the set

\[
\text{Res}_1(L) := \{ f \in \text{Res}(L) \mid f(1_L) = 1_L \}
\]

forms a simple semiring with right- but not left-absorbing infinity.
Finite simple semirings without zero

Theorem (Kendziorra, Z., 2013)

Let $R$ be a finite simple semiring, $|R| > 2$, with right- but not left-absorbing infinity. T. f. a. e.:

i) $R$ is simple,

ii) $R$ is a subsemiring of $\text{Res}_1(L)$ for a finite lattice $L$ such that:

\[
\forall a \in L\setminus\{1\} : e_{a,1} \in R
\]

\[
\forall f \in R \exists a \in L\setminus\{1\} : e_{a,1} \leq f
\]

\[
\forall a \in L\setminus\{0,1\} \forall b \in L \exists f \in R : f(a) = b
\]

Example

$R_3 = \text{Res}_1(\{0, 1, 2\})$

\[
\begin{array}{ccc}
B & + & 0 & 1 & 2 \\
0 & 1 & 2 & 0 & 0 & 2 \\
1 & 1 & 2 & 0 & 1 & 2 \\
2 & 2 & 2 & 0 & 2 & 2
\end{array}
\]
Proof via irreducible modules

For any $R$-module $M$ we have a semiring homomorphism

$$T: R \rightarrow \text{End}(M), \quad r \mapsto T_r \quad \text{with} \quad T_r: x \mapsto rx.$$ 

The $R$-module $M$ is called

- **trivial** if $|M| = 1$,
- **id-quasitrivial** if $rx = x$ for all $r \in R$, $x \in M$,
- **quasitrivial** if $T$ is constant, i.e., $rx = sx$ for $r, s \in R$, $x \in M$.

**Proposition**

For any finite simple semiring there is an **irreducible** module, i.e.,

- it is non-quasitrivial,
- it has only id-quasitrivial proper submodules,
- it has only trivial proper quotient-modules.


A **complete semiring** \((R, \Sigma, \cdot)\) is a set \(R\) with complete summation \(\Sigma\) and an associative operation \(\cdot\) which distributes over \(\Sigma\).

**Theorem (Katsov, Nam, Z., 2014)**

A complete semiring \((R, \Sigma, \cdot)\) with \(|R| > 2\) is simple if and only if \(R\) is a dense subsemiring of \(\text{Res}(L)\) for a complete lattice \(L\).

A **topological semiring** \((R, +, \cdot)\) is a Hausdorff topological space \(R\) with continuous semiring operations \(+, \cdot : R \times R \to R\).

It is called **simple** if every continuous homomorphism \(f : R \to S\) into a topological semiring \(S\) is either constant or injective.

**Theorem (Schneider, Z., 2016)**

*Every simple compact semiring with zero is finite.*
Outline

Introduction to Simple Semirings

Semigroup Actions and Post-Quantum Cryptography

Finite Simple Semirings

Open Problems and Further Research
Open problems and further research

Semiring structure theory

- Complete the classification of finite simple semirings with an absorbing infinity.
- Work towards a classification of ideal-simple semirings.
- Characterise general (semisimple) semirings in terms of simple semirings.

Cryptography

- How hard is the general semigroup action problem?
- Generate large commuting subsets of matrices over semirings.
- Exploit other ideas to construct semigroup actions for cryptography.
References


