



Oleshchuk's Public-Key Cryptosystem

Based on Church-Rosser String-Rewriting Systems

Heiko Stamer <stamer@theory.informatik.uni-kassel.de>

76F7 3011 329D 27DB 8D7C 3F97 4F58 4EB8 FB2B E14F



⋮⋮⋮ Introduction and Preliminaries

Definition 8 *Nonempty set $C \subseteq \Sigma^*$ is a code, if $\forall x_{i_1}, \dots, x_{i_n}, x_{j_1}, \dots, x_{j_m} \in C$ holds*

$$x_{i_1} \dots x_{i_n} = x_{j_1} \dots x_{j_m} \Rightarrow x_{i_1} = x_{j_1}$$

By Induction: $\forall 1 \leq k \leq n : x_{i_k} = x_{j_k}$ and $n = m$

Corollary 2 (unique presentation)

If C is a code then any sequence from C^ can be uniquely presented as concatenation of words from C .*

For finite set C the code property is effectively decidable.



⋮⋮⋮ Classical (Secret Key) Cryptosystem

- Plaintext alphabet: w.l.o.g. $\Sigma = \{0, 1\}$
 - Cryptotext alphabet: Δ , e.g. with $|\Delta| > |\Sigma|$
1. Choose secret SRS T with Church-Rosser property.
 2. Choose two words $u_0, u_1 \in \text{IRR}(T)$ for elements of Σ , such that $u_i u_j \in \text{IRR}(T)_{i,j=0,1}$ and $\{u_0, u_1\}$ is a code.
 3. Letter $x_i \in \Sigma$ is encrypted as word $w_i \in \Delta^*$ such that

$$w_i \xrightarrow{T^*} u_i \quad \text{i.e. } w_i \in [u_i]_T .$$

$$\text{Enc}(x_{i_1} x_{i_2} \dots x_{i_n}) = y \quad \text{with } y \in [u_{i_1} u_{i_2} \dots u_{i_n}]_T$$

Decryption is unique, due to Church-Rosser and code properties!

⋮⋮⋮ Classical (Secret Key) Cryptosystem

Example 1 (don't use) $\Sigma = \{0, 1\}, \Delta = \{a, b, c\}$

Rules of confluent SRS T on Δ : $(abc, ab), (bbc, cb)$

$u_0 = abb \in \text{IRR}(T) \quad u_1 = acb \in \text{IRR}(T)$

$u_0u_0 = abbabb \in \text{IRR}(T), u_0u_1 = abbacb \in \text{IRR}(T)$

$u_1u_0 = acbabb \in \text{IRR}(T), u_1u_1 = acbacb \in \text{IRR}(T)$

trivial check: $\{abb, acb\}$ is a (fixed-length) code

encoding of $170_{\text{dez}} = 10101010_{\text{bin}} \rightsquigarrow (acbabb)^4$

↓ one possible (weak!) encryption ↓

$abbcabcbbcacbabbbcbcbcbabbcbcbabb$ $\in [(u_1u_0)^4]_T$

$\rightarrow_T^5 (acbabb)^4 \rightsquigarrow 10101010_{\text{bin}} = 170_{\text{dez}}$

Public Key Cryptosystem (Usage)

Alice

One letter case: $\text{Enc}(x_i) = w_i$ with $w_i \in [L_i]_S$
 $\text{Enc}(x_{i_1}x_{i_2} \dots x_{i_n}) = y$ with $y \in [L_{i_1}L_{i_2} \dots L_{i_n}]_S$

Eve

She wants to find $w \in \{L_0 \cup L_1\}^*$ with $w \leftrightarrow_S^* y$,
but S may have undecidable word problem.

Bob

$\exists w \in \text{IRR}(T)$ such that $y \rightarrow_T^* w$
and $w = u_{i_1}u_{i_2} \dots u_{i_n}$ with $u_{i_j} \in R_{i_j}$

Public Key Cryptosystem (Example)

Example 2 (don't use) $\Sigma = \{0, 1\}$, $\Delta = \{a, b, c\}$
Rules of secret Church-Rosser SRS T on Δ :

$$(abc, ab), (bbc, cb)$$

$$u_0 = abb, u_1 = acb, u_2 = bab, u_i \in \text{IRR}(T)$$

trivial check: $\{abb, acb, bab\}$ is a code

$$R_0 = \{abb, bab\}, R_1 = \{acb\}$$

$$L_0 = \{abccbcb, babccccc\}, L_1 = \{abcbbcc\}$$

Rules of public (non confluent) SRS S on Δ :

$$(abcc, abc), (cbbca, ccba), (cabcc, cab), (cbbcbbc, cccb)$$

Public Key Cryptosystem (Example)

Example 2 (don't use)

$$10_{\text{dez}} = 1010_{\text{bin}} \rightsquigarrow \overbrace{abcbbcc}^{\in L_1} \overbrace{babcccc}^{\in L_0} \overbrace{abcbbcc}^{\in L_1} \overbrace{abccbbc}^{\in L_0}$$

↓ *one possible (weak!) encryption* ↓

$$\underbrace{abc^2b^2cb^2cab c^6abc^2b^2c^2abc^3b^2cbc} \in [L_1L_0L_1L_0]S$$

$$\rightarrow \frac{1}{T} acbbabacbabbb \rightsquigarrow 1010_{\text{bin}} = 10_{\text{dez}}$$



Public Key Cryptosystem (Analysis)

OLESHCHUK's arguments why cryptanalysis is difficult:

1. Let S be non-monadic SRS and $\text{Enc}(x_i) = w_i$ with

$w_i \in \langle L_i \rangle_S$, where

$\langle L_i \rangle_S = \{w \mid \exists u \in L_i \text{ such that } w = w_t \leftrightarrow_S w_{t-1} \leftrightarrow_S \dots \leftrightarrow_S w_0 = u \text{ and } \forall 0 \leq i \leq t : |w_i| \leq |w_{i+1}|\}$.

By construction: $\underbrace{\langle L_i \rangle_S}_{\in \text{CSL}} \subseteq [L_i]_S$

CS-Grammar G_i with $L(G_i) = \langle L_i \rangle_S$ is constructable.

Decryption of $y \in \langle L_i \rangle_S$ (without trapdoor) is equivalent to test $y \in L(G_i)$, which is P-SPACE-complete (detCSG).

2. Advantage: no boundary markers between symbols

Eve has to find the boundaries in $2^{|y|-1}$ possibilities.

Public Key Cryptosystem (Analysis)

OLESHCHUK's arguments why cryptanalysis is difficult:

3. Any Church-Rosser T' such that

(i) S refines T'

(ii) $[L_0]_{T'} \cap [L_1]_{T'} = \emptyset$

(iii) $([L_0]_{T'} \cup [L_1]_{T'}) \cap \text{IRR}(T')$ is a code

(iv) for any $u'_0, u'_1 \in ([L_0]_{T'} \cup [L_1]_{T'}) \cap \text{IRR}(T')$ holds
 $u'_i u'_j \in \text{IRR}(T')$ for $i, j = 0, 1$

can be used to decrypt a message y .

(a) T cannot be derived from S directly, since S doesn't contain all information about T in general.

Public Key Cryptosystem (Analysis)

OLESHCHUK's arguments why cryptoanalysis is difficult:

(b) There exists no algorithm to decide whether a finite SRS S is equivalent to finite Church-Rosser SRS T' .
(O'DUNLAING, 1983)

(c) But property (i) can be tested in linear time:

Q: How many Church-Rosser Systems T' might be analyzed (brute force)?

A: 'almost all' one-rule SRS are Church-Rosser
(BOOK, SQUIER, 1984)

Conjecture: Number of n -rule Church-Rosser SRS T' on Δ grows exponentially with growing $|\Delta|$ and n .

References

- [Olk95] VLADIMIR A. OLESHCHUK: *On Public-Key Cryptosystem Based on Church-Rosser String-Rewriting Systems*, COCOON'95, LNCS 959 (1995)
- [BO93] RONALD V. BOOK, FRIEDRICH OTTO: *String-Rewriting Systems*, Springer NY, ISBN 3-540979654, 1993