社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

Strongly Asymmetric Public Key Agreement Algorithms

LuigiACCARDI[†]　入山　聖史[††]　MassimoREGOLI[†]　大矢　雅則[††]

† Università di Roma ”Tor Vergata”　Via Columbia, 2, 00133, Rome, Italy
†† 東京理科大学　〒 278-8510 千葉県野田市山崎 2641
E-mail: †accardi@volterra.mat.uniroma2.it, ††{iriyama,ohya}@is.noda.tus.ac.jp, †††regoli@uniroma2.it

あらまし　Our goal is to discuss the main ideas, general construction and abstract scheme of a new class of cryptographic algorithms. Using toy model realizations we will illustrate the above abstract scheme showing how some known PKA algorithms and variants of them can be recovered from the above mentioned construction. Finally we discuss the resiliency of the above scheme to attacks (comparative breaking complexity).

キーワード　asymmetric public key agreement, key conjugation, publick key distribution

Strongly Asymmetric Public Key Agreement Algorithms

Luigi ACCARDI[†], Satoshi IRIYAMA[††], Massimo REGOLI[†], and Masanori OHYA[††]

† Università di Roma ”Tor Vergata”　Via Columbia, 2, 00133, Rome, Italy
†† Tokyo University of Science　2641 Noda City, Chiba, Japan
E-mail: †accardi@volterra.mat.uniroma2.it, ††{iriyama,ohya}@is.noda.tus.ac.jp, †††regoli@uniroma2.it

Abstract　Our goal is to discuss the main ideas, general construction and abstract scheme of a new class of cryptographic algorithms. Using toy model realizations we will illustrate the above abstract scheme showing how some known PKA algorithms and variants of them can be recovered from the above mentioned construction. Finally we discuss the resiliency of the above scheme to attacks (comparative breaking complexity).

Key words　asymmetric public key agreement, key conjugation, publick key distribution

1. Strongly asymmetric PKA algorithms

In Public Key Agreement (PKA) algorithms two interlocutors A and B produce a secret shared key (SSK) by exchanging public information and combining it with private one.
Such cryptographic algorithms are called *asymmetric* because the private informations possessed by A and B are different and not shared.

However the operations performed by A and B, to construct the secret shared key (SSK), are quite similar.

In the present talk a new method to construct PKA algorithms is discussed in which this residual form of symmetry is eliminated, hence the name: *strongly asymmetric PKA algorithms*.

Rather than a new class of PKA algorithms, the method yields *a machine to produce PKA algorithms*.

The main new features of this new class of PKA algorithms are the following:
– Recipient public keys are distinguished from sender public keys
– B (**the receiver**) has more than one public key (*multiple public keys*)
– The unique public key used by A (**the sender**) depends on those of the recipient.
The splitting of the public information into multiple public keys implies levels of:
– security
– flexibility
– variety of concrete realizations
which cannot be found in the standard PKA algorithms.
The construction of these algorithms does not depend on sophisticated mathematical structures (e.g. groups associated to elliptic curves or complex theorems of number theory). This implies a drastic decrease in implementation complexity and increase in velocity.
The present scheme has been submitted for patent (joint with Massimo Regoli, No. RM2011A000062, 11/02/2011).

1.1 Notations and Public Ingredients

Let $\mathbb{N}$ be the natural integers, $\mathcal{P}$, a semigroup (noted multiplicatively, with 1) and $\alpha \in \mathcal{P}$, an element of $\mathcal{P}$ which is the (commutative) semigroup generated by α: $\mathcal{P}_0(\alpha) \equiv \mathcal{P}_0(\alpha) := \{\alpha^n \ : \ n \in \mathbb{N}\} \subseteqq \mathcal{P}$

1.2 Steps of the algorithm

Step (0) B (the receiver) constructs the following maps:

$$N_{B,1} : \mathcal{P} \to \mathcal{P} \quad \text{easily invertible map}$$

$$N_{B,3} : \mathcal{P} \to \mathcal{P} \text{ easily invertible map}$$

$$\hat{x}_{B,1} \ , \ \hat{x}_{B,2} \ , \ \hat{x}_{B,3} \ , \ \hat{x}_{B,4} : \mathcal{P} \to \mathcal{P}$$

arbitrary functions satisfying the *compatibility conditions*

$$\hat{x}_{B,1}\hat{x}_{B,2}|_{\mathcal{P}_0} = \hat{x}_{B,3}\hat{x}_{B,4}|_{\mathcal{P}_0}$$

$$N_{B,1}\hat{x}_{B,2}|_{\mathcal{P}_0} \text{ is an homomorphism} : \mathcal{P}_0 \to \mathcal{P}$$

Step (1) Using the functions constructed in Step (0), B constructs:

(i) *The Secret Key of* B, i.e. the function:

$$\hat{x}_B := \hat{x}_{B,3}N_{B,3}$$

(ii) *The Public Keys of* B, i.e. the functions:

$$\hat{x}_{B,1}N^{-1}_{B,1}$$

$$N^{-1}_{B,3}\hat{x}_{B,4}$$

and the element of $\mathcal{P}$

$$N_{B,1}\hat{x}_{B,2}(\alpha)$$

Step (2) B sends his public keys to A

Step (3a) A chooses her *Secret Key*: a natural integer $x_A \in \mathbb{N}$.

Step (3b) using α, x_A and the public key $N^{-1}_{B,3}\hat{x}_{B,4}$ of B, A computes her public key: $N^{-1}_{B,3}\hat{x}_{B,4}(\alpha^{x_A}) =: y_A$

Step (4): A sends her public key y_A to B.

Step (5): *Computation of the SSK*: $\kappa = x_{B,1}x_{B,2}(\alpha^{x_A}) = x_{B,3}x_{B,4}(\alpha^{x_A})$

Step (5A): A computes:

$$\begin{aligned} x_{B,1}N^{-1}_{B,1}[N_{B,1}x_{B,2}(\alpha)]^{x_A} &= x_{B,1}N^{-1}_{B,1}[N_{B,1}x_{B,2}(\alpha^{x_A})] \\ &= x_{B,1}x_{B,2}(\alpha^{x_A}) \\ &= \kappa \end{aligned}$$

Remark Notice that, in order to calculate κ, A uses public keys of B different from the one used to produce y_A.

Step (5B): B computes

$$\begin{aligned} \hat{x}_B(y_A) &= x_{B,3}N_{B,3}(y_A) \\ &= x_{B,3}N_{B,3}(N^{-1}_{B,3}x_{B,4})(\alpha^{x_A}) \\ &= x_{B,3}x_{B,4}(\alpha^{x_A}) \\ &= \kappa \end{aligned}$$

2. Scalar toy model (1)

Public ingredients:

– Any field $\mathbb{F}$ in which, for each $x \in \mathbb{F}$, the computation of x^{-1} is efficient. A typical choice is $\mathbb{F} = \mathbb{Z}_p$

– an element $A \in \mathbb{F}$ (A is denoted α in the abstract scheme).

Step (0): Definition of the functions

Fix $x_1, x_2, x_3, x_4 \in \mathbb{F}$ and define:

$$\hat{x}_{B,2}(y) := y^{x_2}$$

$$\hat{x}_{B,1}(y) := y^{x_1}$$

$$\hat{x}_{B,3}(y) := y^{x_3}$$

$$\hat{x}_{B,4}(y) := y^{x_4}$$

$$N_{B,1} := id$$

$$N_{B,3} := id$$

1–**st Compatibility condition**:

$$\begin{aligned} \hat{x}_{B,1}\hat{x}_{B,2}(y) &= \hat{x}_{B,1}(y^{x_2}) \\ &= (y^{x_2})^{x_1} \\ &= y^{x_2x_1} \end{aligned}$$

$$\begin{aligned} \hat{x}_{B,3}\hat{x}_{B,4}(y) &= \hat{x}_{B,3}(y^{x_4}) \\ &= (y^{x_4})^{x_3} \\ &= y^{x_4x_3} \end{aligned}$$

This gives the easily satisfiable condition:

$$\begin{aligned} \hat{x}_{B,1}\hat{x}_{B,2} &= \hat{x}_{B,3}\hat{x}_{B,4} \Leftrightarrow \\ x_1x_2 &= x_3x_4 =: \bar{x} \end{aligned}$$

2–**d Compatibility condition**:

$$\begin{aligned} N_{B,1}\hat{x}_{B,2}(A^n) &= \hat{x}_{B,2}(A^n) \\ &= (A^n)^{x_2} \\ &= A^{nx_2} \\ &= (A^{x_2})^n \\ &= (x_{B,2}(A))^n \\ &= N_{B,1}\hat{x}_{B,2}(A)^n \end{aligned}$$

Thus $N_{B,1}\hat{x}_{B,2}|_{\mathcal{P}_0}$ is an homomorphism, as required.

Public Keys of B:

$$\begin{aligned} \hat{x}_{B,1}N^{-1}_{B,1}(y) &= \hat{x}_{B,1}(y) \\ &= y^{x_1} \\ N^{-1}_{B,3}\hat{x}_{B,4}(y) &= N^{-1}_{B,3}(y^{x_4}) \\ &= y^{x_4} \\ N_{B,1}\hat{x}_{B,2}(A) &= \hat{x}_{B,2}(A) \end{aligned}$$

$$= A^{x_2}$$

Secret Key of B:

$$\hat{x}_B(y) = \hat{x}_{B,3}N_{B,3}(y) = y^{x_3}$$

Thus to give the function $\hat{x}_B$ is equivalent to give the number x_3.
Secret Key of A:

$$x_A \in \mathbb{N}$$

Public Key of A:

$$y_A = N_{B,3}^{-1}\hat{x}_{B,4}(A^{x_A}) = A^{x_A x_4}$$

A constructs the SSK:

$$\begin{aligned} x_{B,1}N_{B,1}^{-1}[N_{B,1}x_{B,2}(A)]^{x_A} &= x_{B,1}[x_{B,2}(A)]^{x_A} \\ &= x_{B,1}x_{B,2}(A^{x_A}) \\ &= A^{x_A x_1 x_2} \\ &= \kappa \end{aligned}$$

B constructs the SSK:

$$\begin{aligned} \hat{x}_B(y_A) &= \hat{x}_B(A^{x_A x_4}) \\ &= A^{x_A x_4 x_3} \\ &= \kappa \end{aligned}$$

The SSK is the same because of the compatibility condition $x_1x_2 = x_4x_3$.

Breaking complexity

The eavesdropper, called Eve (E) knows the public parameters and the public keys:

$$A \in \mathbb{F} \ ; \ x_1 \in \mathbb{F} \ ; \ x_4 \in \mathbb{F} \ ; \ A^{x_2} \in \mathbb{F} \ ; \ y_A = A^{x_A x_4} \in \mathbb{F}$$

If E can compute the logarithm in $\mathbb{F}$, then she can recover $x_A x_4 = lg_A y_A$. Since E knows x_4, she recovers x_A knowing A^{x_2}, x_1, x_A, she can compute the SSK

$$(A^{x_2})^{x_A x_1} = A^{x_A x_1 x_2} = \kappa$$

Thus the breaking complexity of this algorithm is equivalent to the logarithm in $\mathbb{F}$. This means that the above toy realization does not bring a real gain with respect to the standard PKA algorithms.

2. 1 A strongly asymmetric version of the Diffie–Hellman algorithm

The public keys of B are

$$y_{B,1} := a\alpha^{x_B}$$

$$y_{B,2} := a^{x_B^{-1}}\alpha$$

The secret key of A is: $x_A \in \mathbb{N}$.
The public key of A is: $y_A := y_{B,2}^{x_A}$.
Finally the SSK κ is: $\kappa := a^{x_A}\alpha^{x_A x_B}$.
A computes the SSK using $y_{B,1}$: $y_{B,1}^{x_A} = (a\alpha^{x_B})^{x_A} = a^{x_A}\alpha^{x_A x_B}$.
B computes the SSK using y_A: $y_A^{x_B} = (a^{x_A x_B^{-1}}\alpha^{x_A})^{x_B} = a^{x_A}\alpha^{x_A x_B} = \kappa$.

2. 2 The Diffie–Hellman algorithm

The Diffie–Hellman algorithm is recovered by choosing $a = 1$, which gives

$$y_{B,1} =: y_B := \alpha^{x_B}$$

$$y_{B,2} = \alpha$$

$$y_A = \alpha^{x_A}$$

$$\kappa = \alpha^{x_A x_B}$$

3. Beyond the discrete logarithm: a simple example

B fixes the following functions:
– A polynomial of degree n

$$Q_n(y) = \sum_{j=0}^{n} a_j y^j \ ; \ a_j \in \mathbb{F} \ , \ j \in \{0, 1, \dots, n\}$$

– A polynomial of degree 1

$$P_2(y) := a_2 y + b_2 \ ; \ a_2, b_2 \in \mathbb{F}$$

– Two natural integers and a scalar

$$N_{B,3} \ , \ n_2 \in \mathbb{N} \setminus \{0\}$$

$$x_{B,3} \in \mathbb{F}$$

With these ingredients B constructs:

$$\hat{x}_{B,2}(y) = P_2(y^{n_2}) = a_2 y^{n_2} + b_2$$

$$\hat{x}_{B,3}(z) = z^{x_{B,3}}$$

$$\hat{x}_{B,4}(y) = c^{Q_n(y)} = c^{\sum_{j=0}^{n} a_j y^j}$$

$$\hat{N}_{B,3}(z) = z^{N_{B,3}}$$

$$\hat{N}_{B,1} = P_2^{-1} \Leftrightarrow \hat{N}_{B,1}^{-1} = P_2$$

$$\hat{x}_{B,1}(z) = c^{x_{B,3}Q_n\left(\left(\frac{z}{a_2} - \frac{b_2}{a_2}\right)^{n_2^{-1}}\right)}$$

This choice satisfies the compatibility conditions:

$$\hat{x}_{B,3}\hat{x}_{B,4}(y) = c^{x_{B,3}Q_n(y)} = \hat{x}_{B,1}\hat{x}_{B,2}(y)$$

$$\hat{x}_{B,1}\hat{x}_{B,2} = \hat{x}_{B,3}\hat{x}_{B,4}$$

Public Keys of B: the public parameter α and

$$\hat{N}_{B,1}\hat{x}_{B,2}(\alpha) = P_2^{-1}P_2(\alpha^{n_2}) = \alpha^{n_2}$$

$$\hat{N}_{B,3}^{-1}\hat{x}_{B,4}(y) = \prod_{j=0}^{n}(c^{N_{B,3}^{-1}a_j})^{y^j}$$

B sends to A the $n+1$ numbers: $\hat{N}_{B,3}^{-1}\hat{x}_{B,4} \equiv (c^{N_{B,3}^{-1}a_n}, \ldots, c^{N_{B,3}^{-1}a_0})$.

$$\hat{x}_{B,1}\hat{N}_{B,1}^{-1}(y) = \prod_{j=0}^{n}(c^{x_{B,3}a_j})^{y^{jn_2^{-1}}} \Leftrightarrow$$

$$\hat{x}_{B,1}\hat{N}_{B,1}^{-1} \equiv (c^{N_{B,3}^{-1}a_n}, \ldots, c^{N_{B,3}^{-1}a_0}, n_2)$$

Public Key of A

$$y_A = \hat{N}_{B,3}^{-1}\hat{x}_{B,4}(\alpha^{x_A}) = \prod_{j=0}^{n}(c^{N_{B,3}^{-1}a_j})^{(\alpha^{x_A})^j}$$

SSK

$$\kappa = \hat{x}_{B,1}\hat{x}_{B,2}(\alpha^{x_A}) = \hat{x}_{B,3}\hat{x}_{B,4}(\alpha^{x_A}) = c^{x_{B,3}Q_n(\alpha^{x_A})}$$

Breaking complexity : Taking the following $n+2$ logarithms

$$\log\alpha\ ,\ \log c^{N_{B,3}^{-1}a_n}\ ,\ \ldots\ ,\ \log c^{N_{B,3}^{-1}a_0}$$

E reduces the problem to the algebraic equation

$$\log y_A = \sum_{j=0}^{n}(\log c^{N_{B,3}^{-1}a_j})(\alpha^{x_A})^j$$

of degree n in the unknown $y = \alpha^{x_A}$. E knows:
– the coefficients of the equation
– that at least one solution in the field $\mathbb{F}$ exists.
Therefore E has to:
– find all solutions of this equation in $\mathbb{F}$
– for each of them (at most n) compute the logarithm $\log\alpha^{x_A}$.
From this she deduces a possible candidate for x_A:

$$x_A = \frac{\log\alpha^{x_A}}{\log\alpha}$$

After that, she proceeds by exhaustive search.
Comparative complexity : Supposing zero cost for:
– the logarithms
– the exhaustive search,
then the breaking complexity is equivalent to find all the roots in the finite field $\mathbb{F}$ of the algebraic equation of degree n with coefficients in $\mathbb{F}$. No general solution method is known for $n \geqq 5$.

4. Conclusions

Many non toy realizations of the general scheme have been constructed. They are structurally different: not variants of each other. The emphasis of the present talk is on the unlimited potentiality of realizations which are apparent already from the (simplest) scalar models. The non scalar models are much richer in structures and possibilities and for some of them the breaking complexity is at the moment unknown.

文　献

[1] Luigi Accardi: Algoritmi fortemente asimmetrici per la distribuzione pubblica di chiavi crittografiche.
Talk given at the seminar "Algoritmi a colazione" Dipartimento Ingegneria dell'Informazione, Università di Roma "Tor Vergata".

[2] Luigi Accardi: New Features for Public Key Exchange Algorithms,
18-th International ICWG Meeting, May 9-13, 2011, Kraków, Poland.

[3] Luigi Accardi, Massimo Regoli: Strongly asymmetric Public Key Agreement Algorithms and the double parametrization method, in preparation.

[4] Luigi Accardi, Masanori Ohya, Massimo Regoli, Satoshi Iriyama: New realizations of strongly asymmetric Public Key Agreement Algorithms, in preparation.