Luigi Accardi

New Features for Public Key Exchange Algorithms

18-th International ICWG Meeting
May 9-13, 2011
Hotel Novotel Kraków Centrum
Kraków, Poland

Università di Roma Tor Vergata
Email: accardi@volterra.mat.uniroma2.it
WEB page: http://volterra.mat.uniroma2.it

Plan of the present talk

1) Introduction:
main ideas of the new algorithms
2) General construction and
abstract scheme of the new algorithms
3a) Illustration of the general structure
using toy models
3b) Recovery of some known PKA algorithms
4) Resiliency to attacks
(comparative complexity).

PKA (asymmetric) algorithms

Basic problem:
A wants to send a secure message to B.

The best known Public Key Agreement (PKA) cryptographic algorithms are asymmetric with respect to the information possessed by A and B.

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

Strongly asymmetric PKA algorithms

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.

Main new features

– Public information is split among **multiple public keys**

– B (**the receiver**) has one set of public keys

– The unique public key used by A (**the sender**) depends on those of B.

The splitting of the public information implies levels of:

– security

– flexibility

– variety of concrete realizations

which cannot be found in the standard PKA algorithms.

Implementation complexity
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

– easier to implement
– quicker.

Patent pending No. RM2011A000062, 11/02/2011 (joint with Massimo Regoli)

Notations and Public Ingredients:

– $\mathbb{N}$, the natural integers

– $\mathcal{P}$, a semigroup

(noted multiplicatively, with 1)

– $\alpha \in \mathcal{P}$, an element of $\mathcal{P}$

$$\{\mathbb{N} \ ; \ \mathcal{P} \ ; \ \alpha\}$$

$$\mathcal{P}_0(\alpha) \equiv \mathcal{P}_0(\alpha) := \{\alpha^n \ : \ n \in \mathbb{N}\} \subseteq \mathcal{P}$$

the (commutative) semigroup generated by α.

B (the receiver) constructs the following maps:

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

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

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

arbitrary functions satisfying the **compatibility conditions**

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

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

$$\pi(xy) = \pi(x)\pi(y) \quad ; \quad \forall x, y \in \mathcal{P}_0(\alpha)$$

$$\pi(1) = 1$$

Step (1) Using these functions B constructs:
The Secret Key of B, i.e. the function:

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

The Public Keys of B, i.e. the functions:

$$\widehat{x}_{B,1} N_{B,1}^{-1} \tag{1}$$

$$N_{B,3}^{-1} \widehat{x}_{B,4} \tag{2}$$

and the element of $\mathcal{P}$

$$N_{B,1} \widehat{x}_{B,2}(\alpha) \tag{3}$$

Step (2)

B sends his public keys to A

Step (3a) A chooses her Secret Key:

$$\text{a natural integer } x_A \in \mathbb{N}$$

Step (3b)
using α, x_A and the public key $N_{B,3}^{-1}\widehat{x}_{B,4}$ of B, A computes her public key

$$N_{B,3}^{-1}\widehat{x}_{B,4}(\alpha^{x_A}) =: y_A$$

Step (4): A

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

Crucial! to calculate κ: A uses public keys of B different from the one used to produce y_A.

$$x_{B,1}N_{B,1}^{-1}[N_{B,1}x_{B,2}(\alpha)]^{x_A} =$$

$$x_{B,1}N_{B,1}^{-1}[N_{B,1}x_{B,2}(\alpha^{x_A})] = x_{B,1}x_{B,2}(\alpha^{x_A}) = \kappa$$

Step (5B): B

$$\widehat{x}_B(y_A) = x_{B,3}N_{B,3}(y_A) =$$

$$x_{B,3}N_{B,3}(N_{B,3}^{-1}x_{B,4})(\alpha^{x_A}) =$$

$$x_{B,3}x_{B,4}(\alpha^{x_A}) = \kappa$$

Scalar toy model (1)

Public ingredients

A finite field

$$\mathbb{F} = \mathbb{Z}_p \quad \text{or} \quad \mathbb{F} = GF(p)$$

$$A \in \mathbb{F}$$

$$(\alpha \to A)$$

Definition of the functions

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

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

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

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

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

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

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

1–**st Compatibility condition**:

$$\widehat{x}_{B,1}\widehat{x}_{B,2}(y) = \widehat{x}_{B,1}(y^{x_2}) = (y^{x_2})^{x_1} = y^{x_2x_1}$$

$$\widehat{x}_{B,3}\widehat{x}_{B,4}(y) = \widehat{x}_{B,3}(y^{x_4}) = (y^{x_4})^{x_3} = y^{x_4x_3}$$

Therefore:

$$\widehat{x}_{B,1}\widehat{x}_{B,2} = \widehat{x}_{B,3}\widehat{x}_{B,4} \Leftrightarrow x_1x_2 = x_3x_4 =: \bar{x}$$

2–**d Compatibility condition**:

$$N_{B,1}\widehat{x}_{B,2}(A^n) = \widehat{x}_{B,2}(A^n) = (A^n)^{x_2} = A^{nx_2} =$$

$$= (A^{x_2})^n = (x_{B,2}(A))^n = N_{B,1}\widehat{x}_{B,2}(A)^n$$

Thus

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

Public Keys of B:

$$\widehat{x}_{B,1}N_{B,1}^{-1}(y) = \widehat{x}_{B,1}(y) = y^{x_1}$$

$$N_{B,3}^{-1}\widehat{x}_{B,4}(y) = N_{B,3}^{-1}(y^{x_4}) = y^{x_4}$$

$$N_{B,1}\widehat{x}_{B,2}(A) = \widehat{x}_{B,2}(A) = A^{x_2}$$

Secret Key of B:

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

$$\widehat{x}_B \equiv x_3$$

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:

$$x_{B,1}N_{B,1}^{-1}[N_{B,1}x_{B,2}(A)]^{x_A} = x_{B,1}[x_{B,2}(A)]^{x_A} =$$

$$= x_{B,1}x_{B,2}(A^{x_A}) = A^{x_A x_1 x_2} = \kappa$$

B constructs the SSK:

$$\widehat{x}_B(y_A) = \widehat{x}_B(A^{x_A x_4}) = A^{x_A x_4 x_3} = \kappa$$

The SSK is the same
because of the compatibility condition

$$x_1 x_2 = x_4 x_3$$

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.

A pedagogical example

With the further specializations:

$$A = a^{x_B^{-1}} \alpha$$

$$x_4 = 1 \Leftrightarrow \bar{x} = x_B = x_3$$

we find:

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 $y_{B,1}$:

$$y_{B,1}^{x_A} = (a\alpha^{x_B})^{x_A} = a^{x_A}\alpha^{x_A x_B}$$

and B computes

$$y_A^{x_B} = (a^{x_A x_B^{-1}}\alpha^{x_A})^{x_B} = a^{x_A}\alpha^{x_A x_B} = \kappa$$

Strongly asymmetric scheme!

The Diffie–Hellman algorithm
is recovered by choosing

$$a = 1$$

which gives

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

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

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

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

Beyond the discrete logarithm: a simple example

B fixes the functions:

A polynomial of degree n

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

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

$$N_{B,3} \ , \ n_2 \in \mathbb{N} \setminus \{0\} \qquad ; \qquad x_{B,3} \in \mathbb{F}$$

With these ingredients B constructs:

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

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

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

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

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

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

Compatibility conditions

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

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

Public Keys of B

$$\alpha$$

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

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

$$\widehat{N}_{B,3}^{-1}\widehat{x}_{B,4} \equiv (c^{N_{B,3}^{-1}a_n}\ ,\ \ldots\ ,\ c^{N_{B,3}^{-1}a_0})$$

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

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

Public Key of A

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

SSK

$$\kappa = \widehat{x}_{B,1}\widehat{x}_{B,2}(\alpha^{x_A}) = \widehat{x}_{B,3}\widehat{x}_{B,4}(\alpha^{x_A})$$

$$= c^{x_{B,3}Q_n(\alpha^{x_A})}$$

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 $n \geq 5$.

Many 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.