Egyetemi doktori (PhD) értekezés tézisei

Titkosítási rendszerek CCA-biztonsága
Encryption systems CCA-security

szerző: MÁRTON Gyöngyvér
témavezető: Dr. Pethő Attila

Debreceni Egyetem
Természettudományi Doktori Tanács
Informatikai Tudományok Doktori Iskola

Debrecen, 2013

Tartalomjegyzék

1. fejezet

Eredmények

Jelen értekezés a titkosító rendszerek választott nyílt szöveg alapú támadással (chosen plaintext attack), illetve választott rejtjelezett szöveg alapú támadással (chosen ciphertext attack) szembeni biztonságát tárgyalja ([24], [37]).

A két támadási típus közül a választott rejtjelezett szöveg alapú támadás tesz erősebb megkötéseket egy titkosító rendszerre. Sokáig a választott rejtjelezett szöveg alapú támadási forma csak az elméleti kriptográfiának jelentett problémát, azonban a gyakorlatban kivitelezett támadási stratégiák, például az 1998-as RSA [57] elleni sikeres Bleichenbacher-támadás [9], azt mutatták meg, hogy szükséges a használatban levő titkosító rendszerek átalakítása. Természetesen a rendszerek átalakítása nem egyszerű feladat, hiszen minden átalakítás a rendszerek hatékonyságának a csökkenésével jár, éppen ezért ezek az átalakítások a jelen kriptográfia aktív kutatási területét képezik ([6], [7], [13], [20], [36]).

Azokat a rendszereket, amelyek biztonságosak a választott nyílt szöveg típusú támadással szemben CPA-biztonságú rendszereknek, azokat a rendszereket pedig, amelyek biztonságosak a választott rejtjelezett szöveg típusú támadással szemben CCA-biztonságú rendszereknek nevezzük.

CCA-biztonságú titkosító rendszerek, pontosabban CCA-biztonságú hibrid rendszerek szerkesztése azt jelenti, hogy a tulajdonképpeni információ titkosításához CCA-biztonságú egyszeri szimmetrikus titkosítási technikát (one-time symmetric encryption technic), a titkosításhoz szükséges titkosító kulcs cseréjéhez, pedig CCA-biztonságú aszimmetrikus titkosítási technikát kell alkalmazni [21]. Az újabb szakirodalom az aszimmetrikus titkosítási technikára a kulcsbeágyazás megnevezést vezeti be ([20], [36]).

Jelen értekezés legfőbb eredménye egy új kulcsbeágyazási mechanizmus CPA, illetve CCA-biztonságú verziójának a bemutatása. A kulcsbeágyazási mechanizmus alapjául a Rabin-titkosító [56] és a Hofheinz és társai [36] által szerkesztett rendszerek szolgáltak. A CCA-biztonságú kulcsbeágyazási mechanizmus a [50] cikkben került publikálásra.

Az értekezés keretén belül megadjuk az új mechanizmus specifikációját, helyességét, hatékonyságát, illetve bizonyítjuk a rendszer biztonságát. Az értekezésben kitérünk még a szakirodalom által számon tartott CCA-biztonságú kulcsbeágyazási mechanizmusok specifikációira, összehasonlítva ezen rendszereket, hatékonyság szempontjából, az új kulcs beágyazási mechanizmus hatékonyságával: megadjuk C++ programozási környezetben a rendszerek mindegyikének implementációját, futási időket mérve a megfelelő algoritmusok esetében.

A tárgyalt rendszerek a következőek, ahol vizsgáljuk az eredeti titkosító rendszert, és annak CCA-biztonságú verzióját:

- az ElGamal- és Cramer–Shoup-rendszer ([27], [20]),
- az RSA- és RSA–OAEP-rendszer ([57], [6]),
- a Rabin- és SAEP-rendszer ([56], [14]),
- a Blum–Goldwasser és Hofheinz és társai rendszere ([12], [36]).

Az elhanyagolható függvény fogalma alatt, melyre szükségünk lesz a továbbiakban a következőket fogjuk érteni ([21], [18], [66]):

1. definíció. *Egy $f(\cdot)$ függvény elhanyagolható (negligible), ha bármely $\epsilon(\cdot)$ polinom esetében létezik egy k_0 egész szám úgy, hogy bármely $k > k_0$ egész számra fennáll: $f(k) < \frac{1}{\epsilon(k)}$.*

Az értekezésben használt jelölések közül, pedig fontosnak tartjuk megemlíteni az alábbiakat ([21][37]).

1. Ha A egy halmaz, akkor $x \xleftarrow{R} A$ jelöli, hogy x véletlenszerűen, egyenletes eloszlás esetén lett kiválasztva.
2. Ha A egy probabilisztikus algoritmus, akkor az $x \xleftarrow{R} A$ jelölés azt jelenti, hogy az A algoritmus x kimenetét véletlenszerűen határozta meg.
3. Az 1^k, k darab egymás mellé írt 1-est jelöl. Ezt a jelölést akkor alkalmazzuk, amikor azt szeretnék jelezni, hogy az algoritmus futási ideje akkor is polinomiális k szerint, ha nincs az algoritmusnak bemenete vagy ez nagyon rövid.

A továbbiakban bemutatjuk az új kulcsbeágyazási mechanizmus részletes specifikációját.

A kulcsbeágyazás mindkét verziója a következő *Gen* kulcsgeneráló algoritmust használja:

1. algoritmus. *A Gen kulcsgeneráló algoritmus az 1^k bemeneten meghatározza az (N, P, Q) számhármast: $(N, P, Q) \xleftarrow{R} Gen(1^k)$ úgy, hogy:*

- $N = P \cdot Q$, *ahol* P, Q *prímszámok, úgy hogy*
  - $P \equiv Q \equiv 3 \pmod 4$, *és*
  - $P = 2 \cdot p + 1, Q = 2 \cdot q + 1$, *ahol* p, q *szintén prímszámok,*
- *A* p *és a* q *bithossza* $k/2 - 1$,

Mindkét verzióban használjuk a kvadratikus maradékok, illetve a kvadratikus maradékok leszűkített halmazát. Jelöljük $\mathbb{QR}_N$-nel a kvadratikus maradékok halmazát, illetve $\mathbb{QR}_N^+$-nel a kvadratikus maradékok leszűkített halmazát, amelyeket formálisan a következőképpen definiálhatunk [63]:

$$\mathbb{QR}_N = \{x \in \mathbb{Z}_N^* : \exists y, y^2 \equiv x \pmod N\}, \text{ és}$$

$$\mathbb{QR}_N^+ = \{|x| : x \in \mathbb{QR}_N\}, \text{ ahol } |x| \text{ az } x \text{ szám abszolút értékét jelöli.}$$

A $\mathbb{QR}_N^+$ halmaznak, kriptográfiai szempontból több fontos tulajdonsága is van, amelyeket az értekezésben megadott bizonyításokban használtunk, [36]. Ezek a következőek:

- $\mathbb{QR}_N^+$ a multiplikatív műveletre nézve ciklikus csoportot alkot, amelynek rendje $\phi(N)/4$, ahol $\phi(N) = (P-1) \cdot (Q-1)$,
- hatékonyan eldönthető, hogy egy elem hozzátartozik a $\mathbb{QR}_N^+$ halmazhoz vagy sem: az adott elemről ellenőrizni kell, hogy benne van-e az $\{1, \ldots, (N-1)/2\}$ halmazban, illetve, hogy a Jacobi szimbóluma $\pmod N$ szerint 1-e.
- a $\mathbb{QR}_N^+$ halmazon belüli kvadratikus maradékok meghatározása problémájának nehézsége ekvivalens a faktorizációs problémával,
- a $\mathbb{QR}_N^+$ halmazon belüli négyzetreemelés függvény egy permutáció lesz a $\mathbb{QR}_N^+$-ben,

- egy egyenletes eloszlás szerint, véletlenszerűen generált $g \in \mathbb{QR}_N^+$ elem nagy valószínűséggel generátor elem lesz; annak a valószínűsége, hogy a g nem lesz generátor elem, a következő:

$$(p+q-1)/(p \cdot q) \leq 2^{-k+2}.$$

1. megjegyzés. *Megjegyezzük, hogy a fenti korlát bizonyításánál fontos szerepet kap, az hogy* $P = 2 \cdot p + 1, Q = 2 \cdot q + 1$, *ahol* p, q *is prímszámok [36], éppen ezért az új kulcsbeágyazási mechanizmushoz, a fenti módon előállított prímeket fogjuk használni.*

A CCA-biztonságú rendszer specifikációja a következő:

A $Gen_{KEM}^{cca}(1^k)$ egy probabilisztikus kulcsbeágyazási algoritmus, amely egyenletes eloszlás szerint, véletlenszerűen az 1^k bemeneten a következőképpen generálja a pk nyilvános kulcsot és az sk titkos kulcsot:

- generál egy N összetett számot a Gen kulcsgeneráló algoritmussal,
- generálja g-t és α-t a következőképpen: $g \xleftarrow{R} \mathbb{QR}_N^+$, $\alpha \xleftarrow{R} \{1, \ldots, (N-1)/4\}$, majd meghatározza X-t: $X = (g^{\alpha \cdot 2^{l_H}})^2 \pmod N$,
- $pk = (N, g, X)$, és $sk = \alpha$.

Az Enc_{KEM}^{cca} kulcsbeágyazási algoritmus az N, g, X bemeneti értékeken a következőket végzi:

- generálja r-t: $r \xleftarrow{R} \{1, \ldots, (N-1)/4\}$,
- meghatározza: $K = g^{r \cdot 2^{l_H}} \pmod N$, és $key = G(K)$, ahol $G : \mathbb{QR}_N^+ \to \{0,1\}^{l_G}$ cél-ütközésmentes hash függvény,

- meghatározza $S = (g^h \cdot X)^r \pmod N$, ahol $h = H(K^2)$, és $H : \mathbb{QR}_N^+ \to \{0,1\}^{l_H}$, cél-ütközésmentes hash függvény,
- meghatározza az $R = K^2 \pmod N$ értéket,
- az algoritmus kimeneti értéke $(key, cipher)$, ahol $cipher = (R, S)$.

A Dec_{KEM}^{cca} kulcskibontási algoritmusnál kétféle módon is meg lehet adni a visszafejtési lépéssorozatot aszerint, hogy bemeneti értéknek az $(\alpha, cipher)$ vagy $(\alpha, P, Q, cipher)$ értékeket adjuk meg.

Ha a bemenetnek az $(\alpha, P, Q, cipher)$, ahol $cipher = (R, S)$ értékeket adjuk meg, akkor hatékonyabb visszafejtési algoritmust kapunk. Megjegyezzük, hogy a rendszer implementálásánál is ezzel a visszafejtési algoritmussal dolgoztunk.

Ebben az esetben a visszafejtés a következőket végzi:

- ha a következő tartalmazás nem áll fenn:

$$(R, S) \in \mathbb{QR}_N^+ \times \mathbb{QR}_N^+,$$

  akkor az algoritmus REJECT elutasító kimeneti értékkel leáll, ellenkező esetben
  - meghatározza a $h = H(R)$ értéket,
  - ha a következő egyenlőség nem áll fenn:

$$S^{2^{1+l_H}} \equiv R^{h+\alpha \cdot 2^{1+l_H}} \pmod N, \qquad (1.1)$$

    akkor az algoritmus REJECT elutasító kimeneti értékkel leáll, ellenkező esetben
    - a kínai maradéktételt alkalmazva meghatározzuk a K értékét, megoldva a következő kongruencia rendszert:

$$K \equiv R^{(P+1)/4} \pmod P,$$
$$K \equiv R^{(Q+1)/4} \pmod Q,$$

$*$ az algoritmus kimeneti értéke a $key = G(K)$ lesz.

A rendszer CCA-biztonsága a faktorizációs feltételezésen, és az alkalmazott hash függvény cél ütközésmentes tulajdonságán alapszik, amelyek formálisan a következőket jelentik:

A faktorizációs feltételezés szerint bármely probabilisztikus polinomiális idejű **A** algoritmus esetében, létezik egy $f(k)$ elhanyagolható függvény úgy, hogy [24]:

$$\mathrm{Adv}_{FAC,\mathbf{A}}(k) = \Pr[\mathbf{A}(N) = (P, Q)] \leq f(k),$$

Egy hash függvény cél-ütközésmentes tulajdonsága, azt jelenti, hogy bármely probabilisztikus polinomiális **B** támadó algoritmus esetén létezik egy $f_{\mathbf{B}}(k)$ elhanyagolható függvény úgy, hogy [7]:

$$Adv_{CR1,\mathbf{B}}(G) = Pr[x \xleftarrow{R} \mathbb{QR}_N, y \xleftarrow{R} \mathbf{B}(x) : x \neq y, G(x) = G(y)] \leq f_{\mathbf{B}}(k).$$

A rendszer CCA-biztonságának bizonyításához a következő kísérletet értelmeztük, amely kísérlet egy polinomiális idejű probabilisztikus **A** támadó és a környezete, a kihívó között zajlik:

1. kísérlet.

1. *A kihívó futtatja a* $Gen^{cca}_{KEM}(1^k)$ *kulcsgeneráló algoritmust, meghatározza az* N, g, X, α *értékeket, majd az* N, g, X *értékeket, átadja az* **A** *támadónak,*
2. *az* **A** *támadó tetszőleges számú alkalommal meghívja a kihívó* $Dec^{cca}_{KEM}(\alpha, \cdot)$ *és* $G(\cdot)$, $H(\cdot)$ *algoritmusait,*
3. *a kihívó elvégzi a következőket:*
   - *meghatározza* $(key^*, cipher^*) \leftarrow Enc^{cca}_{KEM}(N, g, X)$,
   - *generál egy u értéket:* $u \xleftarrow{R} \mathbb{QR}^+_N$,

- *a* (key^*)*-t* c_0*-val jelöli,*
- *a* $(G(u))$*-t* c_1*-gyel jelöli,*
- *átadja az* **A** *támadónak a* $(c_b, cipher^*)$ *értékpárt, ahol* $b \xleftarrow{R} \{0,1\}$*,*

4. *az* **A** *támadó tetszőleges számú alkalommal, különböző cipher értékekre meghívja a kihívó* $Dec^{cca}_{KEM}(\alpha, cipher)$ *és* $G(\cdot)$*,* $H(\cdot)$ *algoritmusait, azzal a megkötéssel, hogy* $cipher \neq cipher^*$*,*
5. *az* **A** *támadó meghatároz egy* $\hat{b} \in \{0,1\}$ *kimeneti értéket.*

Az alábbi tételben $Expr(0)$-val jelöljük azt az eseményt, amikor a támadó által meghatározott kimeneti érték 1, azon feltétel mellett, hogy a kihívónak $b = 0$ volt a választása, és $Expr(1)$-gyel jelöljük azt az eseményt, amikor a támadó által meghatározott kimeneti érték 1, azzal a feltétellel, hogy a kihívó a $b = 1$ értéket választotta.

A tétel, amely ezek után kijelenthető, a következő:

1. tétel. *Ha a fenti kísérletben a* H *és* G *cél-ütközésmentes hash függvények, és ha a faktorizációs feltételezést elfogadjuk, akkor az új kulcsbeágyazási mechanizmus CCA-biztonságú, azaz létezik egy* $f(k)$ *elhanyagolható függvény úgy, hogy bármely* **A** *probabilisztikus polinom idejű támadó esetén:*

$$\mathrm{Adv}^{cca}_{KEM,A}(k) = \tfrac{1}{2}|\Pr[Expr(0)] - \Pr[Expr(1)]| \leq f(k).$$

A fenti tétel bizonyításához további két tételt jelentettünk ki és bizonyítottunk be. Ezek a következőek:

2. tétel. *Ha elfogadjuk a faktorizációs feltételezést, és ha a* G *hash függvény cél-ütközésmentes tulajdonságú, akkor létezik egy*

$f(k)$ elhanyagolható függvény úgy, hogy bármely probabilisztikus polinomiális idejű D támadó algoritmus esetén fennáll:

$$\mathrm{Adv}_{DDS,D}(k) =$$

$$|\Pr[D(N, K^2, G(K)) = 1] - \Pr[D(N, K^2, G(u)) = 1]| \leq f(k),$$

ahol K a kulcsbeágyazási algoritmus során meghatározott érték és $u \xleftarrow{R} \mathbb{QR}_N^+$.

A továbbiakban ezt a típusú algoritmust D-tulajdonságú algoritmusnak fogjuk hívni.

3. tétel. *Ha* **A** *egy probabilisztikus, polinomiális idejű támadó algoritmus, amely feltöri az új rendszer CCA-biztonságát, akkor szerkeszthető egy probabilisztikus polinomiális idejű D algoritmus, amely D-tulajdonságú vagy szerkeszthető egy probabilisztikus polinomiális idejű B algoritmus, amely feltöri a H függvény ütközésmentes tulajdonságát.*

Formálisan ez a következőket jelenti:

$$\mathrm{Adv}^{cca}_{KEM,A}(k) \leq \mathrm{Adv}_{DDS,D}(k) + \mathrm{Adv}_{CR1,B}(k) + f(k),$$

ahol $f(k)$ elhanyagolható függvény.

2. fejezet

Results

This thesis examines the security of encryption systems, it focuses mainly on two types of attacks on chosen plaintext attack and chosen ciphertext attack ([24], [37]).

Between the two types of attacks the chosen ciphertext attack poses a stronger restriction on the construction of encryption systems. At first reading it may seem that chosen ciphertext security signifies problems only for theoretical cryptography, but successful attacks presented in practice, for example the Bleichenbacher attack [9] against RSA [57], show that it is necessary to transform encryption systems. Naturally, transforming encryption system is not an easy task, because the transformed system becomes less efficient, so this area of cryptography constitutes an active research field ([6], [7], [13], [20], [36]).

In the thesis we will call CPA-secure encryption systems those systems which are secure against chosen plaintext attack and CCA-secure encryption systems those systems which are secure against chosen ciphertext attack.

Constructing a CCA-secure encryption system, more exactly CCA-secure hybrid encryption system, means that for encryption of actual data we use symmetric encryption technics and asymmetric encryptions are used to generate and interchange the encryption key of two remote parties. Recent literature introduces the data encapsulation, respectively key-encapsulation terms for these [21].

The main result of the dissertation is a CPA and CCA version of a new key encapsulation mechanism. The mechanism is based on Rabin-encryption [56] and on the system constructed by Hofheinz et al. [36]. The new CCA-secure key encapsulation mechanism was published in [50].

Within the framework of the thesis we give a detailed description of the proposed mechanism, we present the soundness, the efficiency and the proof of CCA security of the proposed CCA-secure mechanism. In the thesis we present some CCA-secure key encapsulation mechanisms, which are considered important in the recent area of cryptography, and we compare these systems with the new key encapsulation mechanism. We give the C++ implementations of the systems, we measure the running times of the corresponding algorithms.

The asymmetric encryption systems and there corresponding CCA-secure versions, which we implement, are the following:

- the ElGamal and Cramer–Shoup system ([27], [20]),
- the RSA and RSA–OAEP system ([57], [6]),
- the Rabin and SAEP system ([56], [14]),
- the Blum–Goldwasser and Hofheinz et al. system ([10], [36]).

In the followings, we need the concept of negligible function, so we define it([21], [18], [66]):

Definition 1. A function $f(\cdot)$ is negligible if for every polynomial $\epsilon(\cdot)$ there exists an integer k_0 such that for all integers $k > k_0$ it is true: $f(k) < \frac{1}{\epsilon(k)}$.

We considered it important to mention the following general notations ([21][37]).

1. If A is a set, then $x \xleftarrow{R} A$ denotes that x is chosen uniformly at random A.
2. If A is a probabilistic algorithm, then $x \xleftarrow{R} A$ denotes that A returns x when executed with fresh coins.
3. 1^k denotes the string comprised of k ones.

Now we are presenting the new key encapsulation mechanism's detailed specifications.

Both versions of the key encapsulation mechanism use the following *Gen* key generation algorithm.

Algorithm 1. The $Gen(1^k)$ is a probabilistic polynomial time algorithm that returns N, P, Q with the following properties:

- $N = P \cdot Q$,
- $P = Q = 3 \pmod 4$, namely P and Q are Blum integers,
- $P = 2 \cdot p + 1, Q = 2 \cdot q + 1$, where p, q are odd prime numbers, namely P and Q are safe primes,
- the bit length of p and q is $k/2 - 1$: $|p| = |q| = k/2 - 1$.

Now we can define the following two groups: we denote the group of quadratic residue as $\mathbb{QR}_N$, and we denote the group of signed residue as $\mathbb{QR}_N^+$. Formally, this means the followings:

$$\mathbb{QR}_N = \{x \in \mathbb{Z}_N^* : \exists y, y^2 \equiv x \pmod N\}, \text{ and}$$

$\mathbb{QR}_N^+ = \{|x| : x \in \mathbb{QR}_N\}$, where $|x|$ denotes the absolute value of x.

The $\mathbb{QR}_N^+$ group has some interesting properties, related to cryptography, which we use in the security proof of our mechanisms. They are the following:

- $\mathbb{QR}_N^+$ with multiplication is a group, and the group order is $\phi(N)/4$, where $\phi(N) = (P-1)\cdot(Q-1)$,
- membership in $\mathbb{QR}_N^+$ can be decided efficiently: tests if an element is in the set: $\{1,\ldots,(N-1)/2\}$, and if the Jacobi symbol modulo N is equal with 1.
- computing square roots in $\mathbb{QR}_N^+$ is equivalent to factoring N,
- squaring in $\mathbb{QR}_N^+$ is a permutation over $\mathbb{QR}_N^+$,
- a uniformly at random generated g element: $g \stackrel{R}{\leftarrow} \mathbb{QR}_N^+$ will be a generator except with probability:

$$(p+q-1)/(p\cdot q) \leq 2^{-k+2}.$$

Remark 1. We mention that it is important to choose P and Q as safe primes, namely $P = 2\cdot p+1$ and $Q = 2\cdot q+1$, where p, q are prime numbers too, to prove the former bound [36].

The proposed CCA-secure scheme's key generation, key-encapsulation and key-decapsulation algorithms are the following:

The key generation algorithm $Gen_{KEM}^{cca}(1^k)$ is a randomized algorithm which generates uniformly at random on input 1^k, the public-key pk and the secret-key sk as follows:

- let N be a composite number generated by Gen,
- let $g \stackrel{R}{\leftarrow} \mathbb{QR}_N^+$, and $X = (g^{\alpha\cdot 2^{l_H}})^2 \pmod N$, where $\alpha \stackrel{R}{\leftarrow} \{1,\ldots,(N-1)/4\}$,
- the algorithm's output is $pk = (N, g, X)$, and $sk = \alpha$.

The key encapsulation algorithm Enc_{KEM}^{cca} operates on input N, g, X and does the following:

- choose $r \xleftarrow{R} \{1, \ldots, (N-1)/4\}$,
- computes: $K = g^{r \cdot 2^{l_H}} \pmod N$, and $key = G(K)$, where $G : \mathbb{QR}_N^+ \to \{0,1\}^{l_G}$ target collision-resistant hash function,
- computes $S = (g^h \cdot X)^r \pmod N$, where $h = H(K^2)$, and $H : \mathbb{QR}_N^+ \to \{0,1\}^{l_H}$, target collision-resistant hash function,
- computes $R = K^2 \pmod N$,
- the algorithm's output is $(key, cipher)$, where $cipher = (R, S)$.

The key decapsulation algorithm Dec_{KEM}^{cca} operates on input $(\alpha, cipher)$ or $(\alpha, P, Q, cipher)$.

If we give as input the values $(\alpha, P, Q, cipher)$, where $cipher = (R, S)$ we obtain a more efficient decapsulation algorithm. We mention that in implementation we work with these values.

In this case, the decapsulation algorithm does the following:

- if $(R, S) \in \mathbb{QR}_N^+ \times \mathbb{QR}_N^+$ does not hold, the algorithm outputs REJECT and stops, otherwise
  - computes $h = H(R)$,
  - if
$$S^{2^{1+l_H}} \equiv R^{h+\alpha \cdot 2^{1+l_H}} \pmod N, \qquad (2.1)$$
    does not hold, the algorithm outputs REJECT and stops, otherwise
    - with the Chinese remainder theorem we are calculating the value of K, solving the following system of congruences:
$$K \equiv R^{(P+1)/4} \pmod P,$$
$$K \equiv R^{(Q+1)/4} \pmod Q,$$

$*$ the algorithm's output is $key = G(K)$.

The security of the system relies in the factoring assumption and the underlying target collision-resistant hash function.

The factoring assumption assumes the existence of an $f(k)$ negligible function such that for all probabilistic polynomial-time **A** algorithm it is true [24]:

$$\mathrm{Adv}_{FAC,\mathbf{A}}(k) = \Pr[\mathbf{A}(N) = (P, Q)] \leq f(k),$$

The target collision-resistance property of a hash function means that for all probabilistic polynomial-time **B** algorithm exists an $f_{\mathbf{B}}(k)$ negligible function such that [7]:

$$Adv_{CR1,\mathbf{B}}(G) = Pr[x \xleftarrow{R} \mathbb{QR}_N, y \xleftarrow{R} \mathbf{B}(x) : x \neq y, G(x) = G(y)] \leq f_{\mathbf{B}}(k).$$

To demonstrate the CCA security of the system we need to define the following experiment, where the experiment takes place between a probabilistic, polynomial time **A** adversary and a challenger.

Experiment 1.

1. The challenger runs $Gen^{cca}_{KEM}(1^k)$ to obtain N, g, X, α,
2. the adversary **A** is given N, g, X and he may query $Dec^{cca}_{KEM}(\alpha, \cdot)$ and $G(\cdot)$, $H(\cdot)$,
3. the challenger does the following:
   - determines $(key^*, cipher^*) \leftarrow Enc^{cca}_{KEM}(N, g, X)$,
   - generates $u \xleftarrow{R} \mathbb{QR}^+_N$,
   - denotes as c_0 the value of (key^*),
   - denotes as c_1 the value of $(G(u))$,
   - the adversary **A** is given $(c_b, cipher^*)$, where $b \xleftarrow{R} \{0, 1\}$,

4. the adversary **A** may query arbitrary $Dec^{cca}_{KEM}(\alpha, \cdot)$ and $G(\cdot)$, $H(\cdot)$, with the only constraint that $cipher \neq cipher^*$,
5. the adversary **A** outputs $\hat{b} \in \{0, 1\}$.

Let $Expr(0)$ denote the event that the adversary outputs 1 on condition that $b = 0$, and let $Expr(1)$ denote the event that the adversary outputs 1 on condition that $b = 1$.

Henceforward the following function can be defined:

$$\mathrm{Adv}_{KEM,\mathbf{A}}(k) = \tfrac{1}{2}|\Pr[Expr(0)] - \Pr[Expr(1)]|.$$

Definition 2. We call the proposed key encapsulation mechanism CCA-secure if for all probabilistic polynomial time adversaries **A** the function $\mathrm{Adv}_{KEM,\mathbf{A}}(k)$ is negligible in k.

Now the following theorem can be stated:

Theorem 1. If in the above experiment H and G are target collision-resistant hash functions and the factoring assumption holds, then the function $\mathrm{Adv}_{KEM,\mathbf{A}}(k)$ is negligible in k, for all probabilistic polynomial time adversaries **A**.

To prove the former theorem we need to state two additional theorems.

Theorem 2. If D is an algorithm that distinguishes between $(N, K^2, G(K))$ and $(N, K^2, G(u))$, where K is the value obtained in key encapsulation, and $u \overset{R}{\leftarrow} QR^+_N$, and G is target collision-resistant hash function, then it can construct an algorithm that factors N. In the following we say that such an algorithm has D-property.

Formally this means the following: if the function $\mathrm{Adv}_{DDS,D}(k)$ is negligible in k, where

$$\mathrm{Adv}_{DDS,D}(k) =$$

$$|\Pr[D(N, K^2, G(K)) = 1] - \Pr[D(N, K^2, G(u)) = 1]| \leq f(k),$$

then such a D algorithm does not exits.

Theorem 3. If A is an adversary that breaks the proposed system CCA-security then we can construct a D algorithm that has D-property or a B algorithm that breaks the target collision-resistant property of H.

Formally this means the following:

$$\mathrm{Adv}_{KEM,A}(k) \leq \mathrm{Adv}_{DDS,D}(k) + \mathrm{Adv}_{TCR,B}(k) + f(k),$$

where $f(k)$ is a negligible function.

Irodalomjegyzék

[1] M. Abdalla – M. Bellare – P. Rogaway: The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES. 2001., *Topics in Cryptology - CT-RSA 2001, LNCS 2020*, 143–158. p.

[2] M. Ajtai – C. Dwork: A public-key cryptosystem with worts-case/awerage-case equivalence. 1999., *In STOC '97 (El Paso, TX), ACM (electronic)*, 284–293. p.

[3] A. Bege – Z. Kása: *Algoritmikus kombinatorika és számelmélet*. 2006, Presa Universitară Clujeană.

[4] M. Bellare – R. Canetti – H. Krawczyk: Keying hash functions for message authentication. 1996., *Advances in Cryptology, CRYPTO '96*.

[5] M. Bellare – P. Rogaway: Random oracles are practical: A paradigm for designing efficient protocols. 1993., *Proceedings of 1st ACM Conference on Computer and Communications Security*, 62–73. p.

[6] M. Bellare – P. Rogaway: Optimal Asymmetric Encryption. 1994., *Advances in Cryptology, EUROCRYPT '94*, 92–111. p.

[7] M. Bellare – P. Rogaway: *Introduction to Modern Cryptography.* 2005.

[8] D.J. Bernstein: The salsa20 family of stream ciphers. http://cr.yp.to/snuffle/salsafamily-20071225.pdf.

[9] D. Bleichenbacher: Chosen Ciphertext Attacks Against Protocols Based on the RSA encryption Standard PKCS#1. 1998., *Advances in Cryptology, Proceedings of CRYPTO '98*, 1–12. p.

[10] L. Blum – M. Blum – M. Shub: Comparison of two pseudo-random number generators. 1982., *Advances in Cryptology, Proceedings of CRYPTO '82*, 61–78. p.

[11] M. Blum – P. Feldman – S. Micali: Proving Security Against Chosen Ciphertext Attacks. 1984., *Advances in Cryptology, Proceedings of CRYPTO '88*, 256–268. p.

[12] M. Blum – S. Goldwasser: An effcient probabilistic public-key encryption scheme which hides all partial information. 1985., *Advances in Cryptology, Proceedings of CRYPTO '84*, 289–302. p.

[13] D. Boneh: Twenty Years of attacks on the RSA cryptosystem. 46 (2). évf. (1999), *Notices of the American Mathematical Society*, 203–213. p.

[14] D. Boneh: Simplified OAEP for the RSA and Rabin functions. 213. évf. (2001), *Lecture Notes in Computer Science, Proceedings of CRYPTO '01*, 275–291. p.

[15] A. Bérczes – J. Folláth – A. Pethő: On a family of collision-free functions. 47. évf. (2010), *Tatra Mountains Mathematical Publications*, 1–13. p.

[16] A. Bérczes – J. Ködmön – A. Pethő: A one-way function based on norm form equations. 49. évf. (2004), *Periodica Mathematica Hungarica*, 1–13. p.

[17] J.A. Buchmann: *Introduction to cryptography.* 2002, Springer.

[18] L. Buttyán – T. Vajda: *Kriptográfia és alkalmazásai.* 2004, Typotex.

[19] D. Coppersmith: Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. 10 (4). évf. (1997), *Journal of Cryptology*, 233–260. p.

[20] R. Cramer – V. Shoup: A practical practical public-key cryptosystem provably secure against adaptive chosen ciphertext attack. 33. évf. (1998), *Advaces in Cryptology, Proceedings of CRYPTO '98*, 13–25. p.

[21] R. Cramer – V. Shoup: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. 2003., *SIAM Journal of Computing*, 167–226. p.

[22] J. Daemen – V. Rijmen: The Block Cipher Rijndael. 2000., *Proceedings of the The International Conference on Smart Card Research and Applications*, 277–284. p.

[23] W. Dai: Crypto++ Library. http://www.cryptopp.com/.

[24] H. Delfs – H. Knebl: *Introduction to cryptography. Principles and Applications.* 2002, Springer.

[25] W. Diffie – M.E. Hellman: New Directions in Cryptography. IT–22. évf. (1976), *IEEE Transactions on Information Theory*, 644–654. p.

[26] Y. Dodis – J. Katz: 3378. évf. (2005). Chosen-Ciphertext Security of Multiple Encryption, 188–209. p.

[27] T. ElGamal: A Public-Key Cryptosystem and a Signatures Scheme Based on Discrete Logarithms. IT–31. évf. (1985), *IEEE Transactions on Information Theory*, 469–472. p.

[28] S.R. Fluhrer – I. Mantin – A. Shamir: Weaknesses in the Key Scheduling Algorithm of RC4. 2001., *Proceeding SAC '01 Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*, 1–24. p.

[29] J. Folláth – A. Huszti – A. Pethő: *Informatikai biztonság és kriptográfia*. 2010.
http://www.inf.unideb.hu/∼pethoe/Jegyzet_PA_20110508.pdf.

[30] R. Freud – E. Gyarmati: *Számelmélet*. 2000, Nemzeti Tankönyvkiadó.

[31] B. Gladman: SHA1, SHA2, HMAC and Key Derivation in C.
http://gladman.plushost.co.uk/oldsite/cryptography_technology/sha.

[32] S. Goldwasser – S. Micali: Probabilistic encryption. 28(2). évf. (1984), *Journal of Computer and System Sciences*, 270–299. p.

[33] L. Goubin – C. Mauduit – A. Sárközy: Construction of large families of pseudorandom binary sequences. 106. évf. (2004), *J. Number Theory*, 59–69. p.

[34] J. Hastad: On using RSA with Low Exponent in a Public Key Network. 1985., *CRYPTO '85 Advances in Cryptology*, 403–408. p.

[35] J. Hoffstein – J. Pipher – J.H. Silverman: *An Introduction to Mathematical Cryptograhy*. 2008, Springer.

[36] D. Hofheinz – E. Kiltz – V. Shoup: Practical Chosen Ciphertext Secure Encryption from Factoring. 2011., *Journal of Cryptology, Online First*^{TM}.

[37] J. Katz – Y. Lindell: *Introduction to Modern Cryptograhy*. 2008, Chapman & HallCRC Press.

[38] A. Kerckhoffs: La cryptographie militaire. IX. évf. (1883), *Journal des sciences militaires*, 5–38. p.

[39] N. Koblitz – A. J. Menezes: A survey of public-key cryptosystems. 46. évf. (2004), *SIAM Review*, 599–634. p.

[40] L. Lovász: *Algoritmusok bonyolultsága*. 2001, Nemzeti Tankönyvkiadó.

[41] A. J. Menezes – P. C. van Oorschot – S.A. Vanstone: *Handbook of applied cryptography*. Boca Raton, Florida, 1997, CRC Press.

[42] R. C. Merkle: A fast software one-way hash function. 3. évf. (1990), *Journal of Cryptology*, 43–48. p.

[43] R. C. Merkle – M. Hellman: Hiding information and signatures in trapdoor knapsacks. 24 (5). évf. (1978), *Information Theory, IEEE Transactions*, 525–530. p.

[44] S. Micali – C. Rackoff – B. Sloan: The notion of security for probabilistic cryptosystems. 1988., *SIAM Journal on Computing*, 412–426. p.

[45] Gy. Márton: *Kriptográfiai alapismeretek*. 2008, Scientia Kiadó.

[46] Gy. Márton: Kriptográfiában alkalmazható feladatok. 2009., *Számokt 2009 konferenciakötet, 19. Nemzetközi számítástechnika és oktatás konferencia*, 289–292. p.

[47] Gy. Márton: Nyilvános kulcsú kriptorendszerek biztonságához kapcsolodó értelmezések. 2010., *Számokt 2010 konferenciakötet, 20. Nemzetközi számítástechnika és oktatás konferencia*, 183–187. p.

[48] Gy. Márton: Public-key cryptography in functional programming context. 2. évf. (2010), *Acta Universitatis Sapientiae, Informatica*, 99–111. p.

[49] Gy. Márton: Üzenethitelesítő kódok és a CCA támadás. 2011., *Számokt 2011 konferenciakötet, 21. Nemzetközi számítástechnika és oktatás konferencia*, 229–233. p.

[50] Gy. Márton: CCA-secure key-encapsulation mechanism based on the factoring assumption. 53. évf. (2012), *Tatra Mountains Mathematical Publications*, 137–146. p.

[51] Gy. Márton: A faktorizációs problémán alapuló titkosító rendszerek biztonsága. 2012., *Számokt 2012 konferenciakötet, 22. Nemzetközi számítástechnika és oktatás konferencia*, 314–315. p.

[52] M. Naor – M. Yung: Public-key cryptosystems provably secure against chosen ciphertext attack. 1990., *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, 427–437. p.

[53] A. M. Odlyzko: Discrete logarithms: The past and the future. 19. évf. (2000), *Designs, Codes, and Cryptography*, 129–145. p.

[54] B. Preneel: Analysis and Design of Cryptographic Hash Function. PhD thesis, Katholieke Universiteit Leuven.

[55] B. Preneel: The state of cryptographic hash functions. 1561. évf. (1999), *Lecture Notes in Computer Science*, 158–182. p.

[56] M. O. Rabin: Digitalized Signatures and Public-Key Functions as Intractable as Factorization. 1979., *MIT Laboratory for Computer Science LCS/TR-212*.

[57] R.L. Rivest – A. Shamir – L.M. Adleman: A method for obtaining digital signatures and public-key cryptosystems. 21 (2). évf. (1978), *Communications of the ACM*, 120–126. p.

[58] L. Rónyai – G. Ivanyos – R. Szabó: *Algoritmusok*. 2004, Typotex.

[59] A. Shamir: A polynomial-time algorithm for breaking the basic Merkle - Hellman cryptosystem. 30 (5). évf. (1984), *Information Theory, IEEE Transactions*, 699–704. p.

[60] V. Shoup: A library for doing number theory. http://www.shoup.net/ntl/.

[61] V. Shoup: Searching for primitive roots in finite fields. 58. évf. (1992), *Mathematics of Computation*, 369–380. p.

[62] W. Stallings: *Cryptography and Network Security. Principles and Practice*. 2010, Prentice Hall.

[63] D. R. Stinson: *Cryptography. Theory and Practice*. 2006, Chapman & HallCRC Press.

[64] U.V. Vazirani – V. Vazirani: Efficient and secure pseudo-random number generation. 1985., *Advances in cryptology, Proceedings of CRYPTO 84*, 193–202. p.

[65] G.S. Vernam: Cipher printing telegraph systems for secret wire and radio telegraphic communications. 55. évf. (1926), *Journal of the IEEE*, 109–115. p.

[66] V. Villányi: RSA signatures schemes with sublimal-free public-key. 41. évf. (2008), *Tatra Mountains Mathematical Publications*, 19–32. p.

[67] M.J. Wiener: Cryptanalysis of short RSA secret exponents. 36 (3). évf. (1990), *Information Theory, IEEE Transactions*, 553–558. p.

[68] M.J. Wiener: Safe prime generation with a combined sieve. 2003., *Crypto Eprint Archive entry 2003: 186.*

A függelék

Referált nemzetközi folyóiratban megjelent cikkek

1. MÁRTON Gyöngyvér: Public-key cryptography in functional programming context, Acta Universitatis Sapientiae Informatica, vol 2. Nr. 1, 2010, 99-112, ISSN 1844-6086 [Zbl 1197.68043]

2. KÁTAI Zoltán, KOVÁCS Lehel István, KÁSA Zoltán, MÁRTON Gyöngyvér, FOGARASI Kinga and FOGARASI Ferenc: Cultivating algorithmic thinking: an important issue for both technical and HUMAN sciences, Teaching Mathematics and Computer Science, 2011, 9/1. [Zbl MathEduc 2012a.00772]

3. MÁRTON Gyöngyvér: CCA-secure key-encapsulation mechanism based on factoring assumption, Tatra Mountains Mathematical Publications, vol 53, 2012, 137–146, ISSN 1210-3195 [Zbl 06135378]

B függelék

Lektorált egyetemi jegyzet

1. MÁRTON Gyöngyvér: Fundamentals of cryptography (in Hungarian), Sapientia-EMTE, Scientia, Cluj-Napoca, 2008, ISBN 978-973-1970-00-4

C függelék

Tudományos konferencia kötetben megjelent cikkek

1. MÁRTON Gyöngyvér, The security of electronic voting, Proceedings of Számokt 2007, 17th International Conference on Computers and Education, Oradea (Nagyvárad), Romania, 2007, ISSN 1842-4546.

2. MÁRTON Gyöngyvér, Recursion, dynamic programming, functional programming, Proceedings of Számokt 2008, 18th International Conference on Computers and Education, Sumuleu Ciuc (Csíksomlyó), Romania, 2008, ISSN 1842-4546.

3. MÁRTON Gyöngyvér, Methods and tools for teaching cryptography, Proceedings of Infodidact 2009, 2th Methodological Conference on Informatics, Szombathely, Hungary, 2009.

4. MÁRTON Gyöngyvér, Eligible problems in cryptography, Proceedings of Számokt 2009, 19th International Conference on Computers and Education, Tg.Mures (Marosvásárhely), Romania, 2009, ISSN 1842-4546.

5. MÁRTON Gyöngyvér, Definitions related to the security of public-key cryptosystems, Proceedings of Számokt 2010, 20th International Conference on Computers and Education, Satu-Mare (Szatmárnémeti), Romania, 2010, ISSN 1842-4546.

6. MÁRTON Gyöngyvér, Message authentication codes and CCA-attack, Proceedings of Számokt 2011, 21th International Conference on Computers and Education, Cluj-Napoca (Kolozsvár), Romania, 2011, ISSN 1842-4546.

7. MÁRTON Gyöngyvér, Security of Encryption Systems based o Factoring Assumptions, Proceedings of Számokt 2012, 22th International Conference on Computers and Education, Alba-Julia (Gyulafehérvár), Romania, 2012, ISSN 1842-4546

D függelék

Tudományos konferenciákon elhangzott előadások

1. MÁRTON Gyöngyvér: Functional programming and cryptography, "The day of science in Transylvania" conference, Miercurea Ciuc, Romania, 2006.
2. MÁRTON Gyöngyvér: Experience in teaching functional programming, "MINICONF" conference, Tg-Mures, Romania, 2007.
3. MÁRTON Gyöngyvér: The role of functional programming in cryptography, Central European Functional Programming School, Cluj Napoca, Romania, 2007.
4. GYŐRFI Eugen, MÁRTON Gyöngyvér: Algebra of the 2D and 3D Cutting/Packing patterns, 6th ESICUP international conference, Valencia, Spain, 2009.

5. MÁRTON Gyöngyvér: Cryptography based on problems of graph theory, 1st "Sapientia MatInfo" International Conference, Tg.Mures, Romania, 2009.

6. MÁRTON Gyöngyvér: Technics used in cryptosystems to achieve CCA-security, 2nd "Sapientia MatInfo" international conference, Tg.Mures, Romania, 2011.

7. MÁRTON Gyöngyvér: Remarks on Blum-Goldwasser public-key encryption system, 11th Central European Conference on Cryptology, Debrecen, Hungary, 2011.

8. MÁRTON Gyöngyvér: Chosen ciphertext security of public-key encryption systems, 9th Joint Conference on Mathematics and Computer Science, Siófok, Hungary, 2012.

9. MÁRTON Gyöngyvér: CCA-secure key-encapsulation mechanism based on the factoring assumption, 12th Central European Conference on Cryptology - TatraCrypt, Smolenice, Slovakia, 2012.