Department of Electrical Engineering - ESAT

KATHOLIEKE UNIVERSITEIT LEUVEN

Computing in the Encrypted Domain

Brecht Wyseur, Mina Deng, Thomas Herlea

Katholieke Universiteit Leuven
Department ESAT/SCD-COSIC

RE-TRUST 5th Quarterly Meeting
December 2007, Leuven

Outline

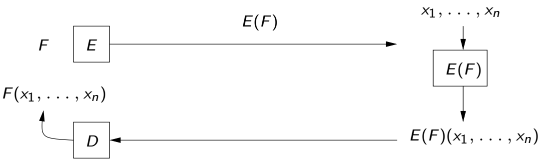
1. RE-TRUST
   - Motivation
2. Homomorphic crypto schemes
3. DCRA-cryptosystems
   - Goldwasser-Micali
   - Benaloh
   - Naccache-Stern
   - Okamoto-Uchiyama
   - Paillier
   - Damgård-Jurik
4. New directions
   - Pairings
   - Evaluating 2-DNF formulas on Ciphertexts
5. Conclusion

Motivation

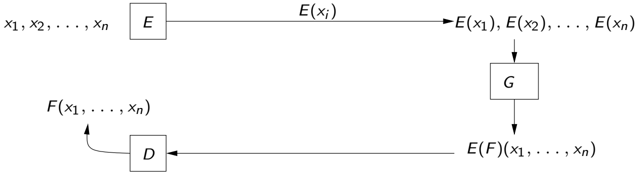
- RE-TRUST WP3 Task 3.3 “Encrypted code execution”
  - Computing with Encrypted Functions (CEF)
  - Computing with Encrypted Data (CED)
- Partners: Gemalto, K.U.Leuven
- M9-M33 (June 2007 - June 2009)

CED/CEF

Computing with Encrypted Functions



Computing with Encrypted Data



Computing with Encrypted Data

- Secure Function Evaluation
  Yao's Garbled Circuits, cryptocomputing, ...
- Homomorphic cryptosystems

Homomorphic cryptosystems

An encryption scheme E_k is said to be *homomorphic* if for any k, it satisfies the following property:

$$\forall m_1, m_2 \in \mathcal{M} : E(m_1 \bigotimes m_2) = E(m_1) \bigoplus E(m_2)$$

for some operators $\bigotimes$ in $\mathcal{M}$ and $\bigoplus$ in $\mathcal{C}$.

Quadratic Residue

Quadratic residue

An element x is said to be a quadratic residue module n if

$$\exists y \vdash x \equiv y^2 \mod n$$

The Jacobi Symbol captures the quadratic residuosity:

$$\left(\frac{x}{n}\right) = \begin{cases} 1 & \text{if } \exists y \vdash x \equiv y^2 \mod n \\ 0 & \text{if } n|x \\ -1 & \text{else} \end{cases}$$

and can easily be computed given the factorisation of n.

$$\left(\frac{x}{\prod_i p_i}\right) = \prod_i \left(\frac{x}{p_i}\right) \qquad \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$$

Decisional Composite Residuosity Assumption (DCRA)

x is a n'th residue in $\mathbb{G}$, if $\exists y \vdash x \equiv y^n \mod ord(\mathbb{G})$.

Decisional Composite Residuosity Assumption (DCRA)

Let A be a probabilistic polynomial time algorithm. Assume A knows the order of $\mathbb{G}$, which is k bits. A gets input x and outputs bit $b = 1$ if x is an n'th residue in $\mathbb{G}$, $b = 0$ otherwise. Let $p(A, k, x)$ be the probability that $b = 1$. Then

$$|p(A, k, x) - p(A, k, x^n)| < neg(k)$$

Deciding n'th residuosity is believed to be intractable.

QR and QNR computation

Some more properties

- **Inversion:** If a is a QR $\mod n$, then $(-1) \cdot a \mod n$ is a QNR $\mod n$ (and vice versa).
- **Multiplication** $\mod n$**:**

a	b	$a \cdot b \mod n$
QR	QR	QR
QR	QNR	QNR
QNR	QR	QNR
QNR	QNR	QR

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Observe that

$$QR/QNR, \cdot \cong \mathbb{Z}_2, +$$

Goldwasser-Micali

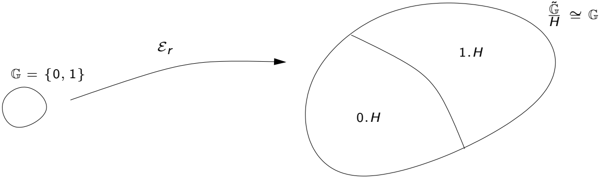


Figure: Goldwasser-Micali homomorphic mapping

Each element of $\mathbb{G}$ is mapped onto a random element of a coset of the factor group $\frac{\tilde{\mathbb{G}}}{H}$, with $H \subset \tilde{\mathbb{G}}$ all quadratic residues.

Remark: We need to deploy a *probabilistic* encryption scheme.

Goldwasser-Micali

$$\begin{cases} b = 0 & \rightarrow & c \ \mathrm{QR} \\ b = 1 & \rightarrow & c \ \mathrm{QNR} \end{cases}$$

Prerequisites:

- g a quadratic non-residue $\in \mathbb{Z}_n^*$.
- $n = pq$, where p and q are prime.

Encryption: Let b be the bit to be encrypted. Choose $r \stackrel{R}{\longleftarrow} \mathbb{Z}_n^*$ a random element.

$$c = \mathcal{E}_r(b) = g^b r^2 \mod n$$

Decryption:
Compute the Jacobi symbol of the ciphertext with respect to n.
Hard when factorisation of $n = pq$ is unknown. Easy when p, q are known.

Benaloh

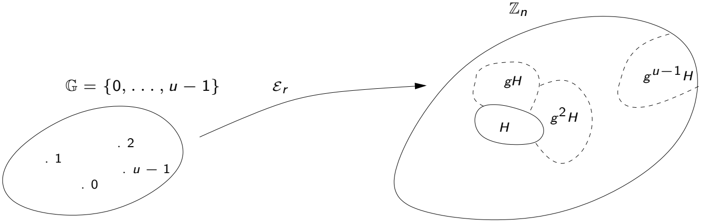


Figure: Benaloh homomorphic mapping

Benaloh

Prerequisites:

- Choose a blocksize u, and two large primes p and q, such that $u|(p-1)$, and $gcd(q-1,u)=1$. Set $n=pq$.
- Choose $g \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ such that $y^{(p-1)(q-1)/u} \neq 1 \mod n$.
- Public key is (g,n), private key is the two primes (p,q).

Encryption: $m \in \frac{\mathbb{Z}}{u\mathbb{Z}}$ message. $r \leftarrow^R \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$.

$$c = \mathcal{E}_r(m) = g^m r^u \mod n$$

“Decryption”:

$$c^{\phi(n)/u} \equiv 1 \mod n \Leftrightarrow m \equiv 0 \mod u$$

Benaloh

Decryption:

- $E(m)E(i) = E(m+i \mod u) = E(0 \mod u)$, Hence

$$c^{i\phi(n)/u} \equiv 1 \mod n \Leftrightarrow m \equiv -i \mod u$$

- Precompute $T_M = g^{M\phi(n)/u} \mod n$.

$$\forall z \in E_r(M) : z^{(p-1)(q-1)/u} \equiv T_M \mod n$$

- *Baby step-giant step* method: Precompute T_M for each $M \approx k\sqrt{u}$, with $k = 0..\sqrt{u}$.

$$c^{i\phi(n)/u} = T_M \Leftrightarrow m \equiv M - i \mod u$$

Naccache-Stern

Prerequisites:

- Similar to Benaloh
- u is B-smooth and square-free (i.e., $u = \prod_i p_i$, with $p_i < B$ and $p_i \neq p_j$ for $i \neq j$).

Encryption:

$$c = \mathcal{E}_r(m) = g^m r^u \mod n$$

Decryption: For each p_i: compare $c^{\phi(n)/p_i} \mod n$ with $g^{i\phi(n)/p_i} \mod n$. Find m using the Chinese Remainder Theorem for $m \equiv i \mod p_i$.

Okamoto-Uchiyama

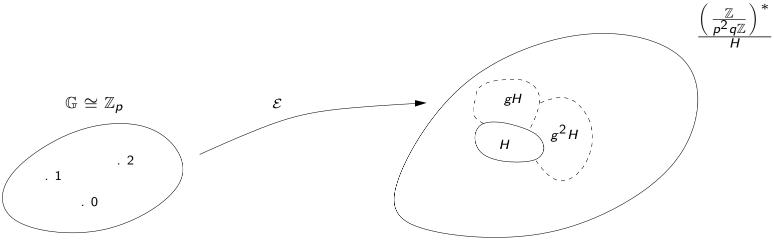


Figure: Damgård-Jurik homomorphic group mapping

$\left(\frac{\mathbb{Z}}{p^2q\mathbb{Z}}\right)^* \cong \left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^* \times \left(\frac{\mathbb{Z}}{q\mathbb{Z}}\right)^*$ has a unique subgroup of order $p \Rightarrow \left(\frac{\mathbb{Z}}{p^2q\mathbb{Z}}\right)^* \cong \mathbb{Z}_p \times H$.

Okamoto-Uchiyama

Prerequisites:

- Generate large primes p, q, and set $n = p^2 q$.
- Choose $g \in (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ such that g has order $(p-1)p$ in the subgroup $(\frac{\mathbb{Z}}{p^2\mathbb{Z}})^*$.
- Let $h = g^n \mod n$.

Encryption: Select $r \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ at random. $m \in \mathbb{Z}_p$.

$$c = g^m h^r \mod n$$

Decryption:

Define $L(x) = \frac{x-1}{p}$ on $G = \{x : x \equiv 1 \mod p\}$. Then

$$m = \frac{L(c^{p-1} \mod p^2)}{L(g^{p-1} \mod p^2)} \mod p$$

Paillier

Prerequisites:

- Choose two large primes p, q.
- Compute $n = pq$ and $\lambda = lcm(p-1, q-1)$.
- Select a random $g \in \mathbb{Z}^*_{n^2}$, such that $\mu = (L(g^\lambda \mod n^2))^{-1} \mod n$ exists, with $L(x) = \frac{x-1}{p}$.
- The public key is (n, g), the private key λ.

Encryption: Let $m \in \mathbb{Z}_n$ be the message to be encrypted. Select $r \in \mathbb{Z}^*_n$ at random.

$$c = g^m r^n \mod n^2$$

Decryption:

$$m = \frac{L(c^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} \mod n$$

Paillier

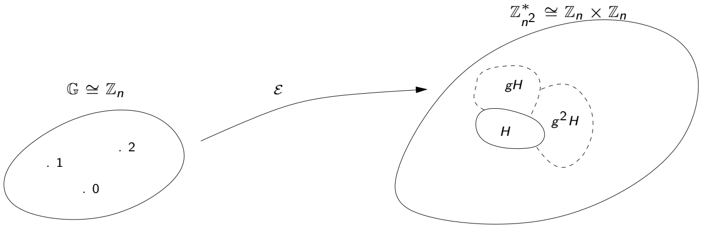


Figure: Paillier homomorphic group mapping

$$\mathbb{Z}_{n^2}^* \cong \mathbb{G} \times H, \text{ with } H = \{x \in \mathbb{Z}_{n^2} \mid x^\lambda \equiv 1 \mod n\} \cong \mathbb{Z}_n.$$

Damgård-Jurik

Generalisation of Paillier's cryptosystem.
$\mathbb{Z}^*_{n^{s+1}} \cong G \times H$, with G a cyclic group of order n^s, and $H \cong \mathbb{Z}^*_n$.

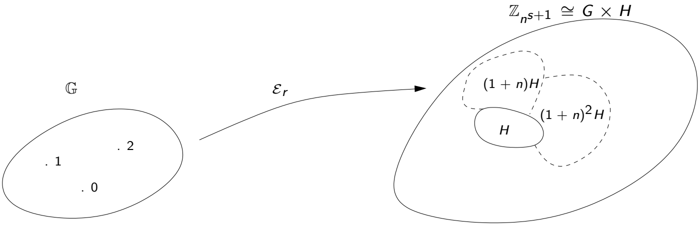


Figure: Damgård-Jurik homomorphic group mapping

Lemma

For any $s < p, q$: $(1+n)$ has order n^S in $\mathbb{Z}_{n^{s+1}}$.

Damgård-Jurik

Prerequisites:

- Choose primes p and q, compute $n = pq$, $\lambda = lcm(p-1, q-1)$.
- Choose $g \in \mathbb{Z}^*_{n^{s+1}}$ such that $g = (1+n)^j x \mod n^{s+1}$, with $gcd(j, n) = 1$, and $x \in H$.
- Choose d such that $d \mod n \in \mathbb{Z}^*_n$ and $d \equiv 0 \mod \lambda$.
- The public key is (n, g), the private key d.

Encryption: $m \in \mathbb{Z}_{n^s}$, and $r \xleftarrow{R} \mathbb{Z}^*_{n^{s+1}}$.

$$c = g^m r^{n^s} \mod n^{s+1}$$

Decryption:

$$c^d = (1+n)^{jmd \mod n^s} \mod n^{s+1}$$

Damgård-Jurik

Decryption:

$$c^d = (1+n)^{jmd \mod n^s} \mod n^{s+1} \tag{1}$$

Let $L(a) = \frac{a-1}{n}$, then

$$L((1+n)^i = \mod n^{s+1} = (i + \binom{i}{2} n + \dots \binom{i}{s} n^{s-1}) \mod n^s$$

We can compute $i_j \equiv i \mod n^j$ using

$$L((1+n)^i = \mod n^{j+1} = (i + \binom{i}{2} n + \dots \binom{i}{j} n^{j-1}) \mod n^j$$

Hence we are able to obtain jmd from (1), and the message $m = (jmd) \cdot (jd)^{-1} \mod n^s$.

DCRA homomorphic crypto schemes

$$\mathcal{E}_{r_1}(m_1)\mathcal{E}_{r_2}(m_2) \mod a \equiv \mathcal{E}_r(m_1 + m_2 \mod b)$$

	a	b
Goldwasser-Micali	n	1
Benaloh	n	r
Naccache-Stern	n	r
Okamoto-Uchiyama	p^2q	p
Paillier	n^2	n
Damgård-Jurik	n^{s+1}	n^s

Where $n = pq$.
Bandwith expansion: $\frac{a}{b}$.

Pairings

A *pairing* is a function

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_3.$$

All pairings that we consider (as a primitive for homomorphic encryption schemes), satisfy the following additional properties:
Bilinearity For all $P, P' \in \mathbb{G}_1$, and all $Q, Q' \in \mathbb{G}_2$ we have

$$e(P+P', Q) = e(P, Q)e(P', Q), \text{ and } e(P, Q+Q') = e(P, Q)e(P, Q')$$

Non-degeneracy

- For all $P \in \mathbb{G}_1$, with $P \neq 0$, there is some $Q \in \mathbb{G}_2$ such that $e(P, Q) \neq 1$.
- For all $Q \in \mathbb{G}_2$, with $Q \neq 0$, there is some $P \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$.

Deploy a Pairing between homomorphic groups

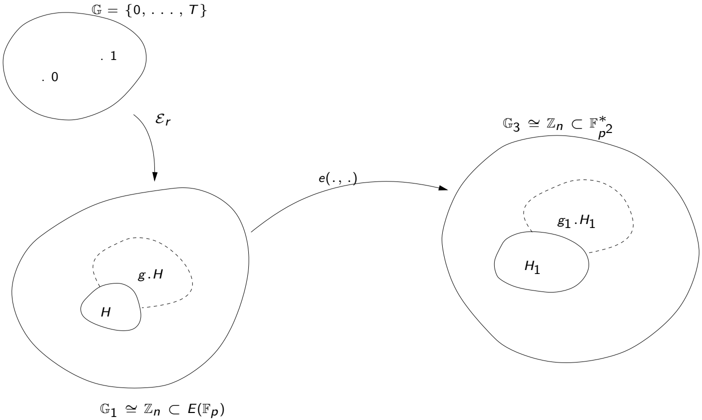


Figure: Paired homomorphic groups

Boneh's Construction

Construction:

- Let $n = q_1 q_2 \in \mathbb{Z}$, with q_1, q_2 two random τ-bit primes.
- Find the smallest positive integer $l \in \mathbb{Z}$ such that $p = ln - 1$ and $p = 2 \mod 3$.
- Construct the group of points on the elliptic curve $y^2 = x^3 + 1$ over $\mathbb{F}_p$. Hence $\#E(\mathbb{F}_p) = p + 1 = ln$. Define $\mathbb{G}_1$ as a subgroup of order n generated by g.
- Construct a modified Weil pairing on the curve $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_3$, with $\mathbb{G}_3$ a subgroup of $\mathbb{F}^*_{p^2}$ of order n, with generator $e(g, g)$.

Decision problem: Given $(n, \mathbb{G}_1, \mathbb{G}_3, e)$, it is hard to decide if $x \in \mathbb{G}_1$ is an element of $\mathbb{Z}_{q_1}$ without knowing the factorization of n.

Crypto system

Prerequisites:

- $g, u \xleftarrow{R} \mathbb{G}_1$
- $h = u^{q_2}$, random generator of subgroup of $\mathbb{G}_1$ of order q_1.
- Public key $(n, \mathbb{G}_1, \mathbb{G}_2, e, g, h)$, private key q_1.

Encryption: $m \in \{0, \ldots, T\}$ with $T < q_2$, $r \xleftarrow{R} \mathbb{Z}_n$.

$$c = g^m h^r \in \mathbb{G}_1$$

Decryption:

$$c^{q_1} = (g^{q_1})^m$$

Let $\hat{g} = g^{q_1}$. To recover m, compute discrete log of c^{q_1} base $\hat{g}$.

Homomorphic properties

Additive For any $c_1, c_2 \in \mathbb{G}_1$, encryptions of $m_1, m_2 \in \{0, \ldots, T\}$, with $r \in \mathbb{Z}_n$:

$$c = c_1 c_2 h^r \leftrightarrow m_1 + m_2 \mod n$$

Multiplicative

$$c = e(c_1, c_2) h_1^r = g_1^{m_1 m_2} h_1^{\tilde{r}} \in \mathbb{G}_3$$

with $g_1 = e(g, g)$, $h_1 = e(g, h)$, and
$\tilde{r} = m_1 r_2 + m_2 r_1 + \alpha q_2 r_1 r_2 + r$, where $h = g^{\alpha q_2}$ for some (unknown) $\alpha \in \mathbb{Z}$.

2-DNF evaluation conclusion

- "Infinite" amount of additions in the encrypted domain
- *Once* a multiplication
  $\Rightarrow$ Quadratic polynomials $F(x_1, \ldots, x_u)$ can be evaluated in the encrypted domain.
- However, knowledge of a certain polynomial size interval needed for decryption of the result.

Conclusion and future work

- Task started with state-of-the-art study of a family of Homomorphic Encryption Schemes (DCRA-based), and the theory of *Secure Function Evaluation (SFE)*.
- We only discussed about *computation on encrypted data (CED)*, not about *computing with encrypted functions (CEF)*. $\rightarrow$ Operations are not obfuscated.
- Practical applicability for the benefit of the project needs to be studied further.