Outline

1. Introduction

2. Benaloh’s Dense Probabilistic Encryption
   - Original scheme
   - A small problematic example

3. Consequences in applications

4. Corrected version

5. A precise analysis of the problem
   - Probability of failure
   - Message space reduction
1. Introduction

2. Benaloh’s Dense Probabilistic Encryption
   - Original scheme
   - A small problematic example

3. Consequences in applications

4. Corrected version

5. A precise analysis of the problem
   - Probability of failure
   - Message space reduction
Homomorphic Encryption

Definition (additively homomorphic)

\[ E(m_1) \otimes E(m_2) \equiv E(m_1 \oplus m_2). \]

Applications

- Electronic voting
- Secure Function Evaluation
- Private Multi-Party Trust Computation
- Private Information Retrieval
- Private Searching
- . . .
## A partial history of homomorphic cryptosystems

<table>
<thead>
<tr>
<th>Year</th>
<th>Name</th>
<th>Security hypothesis</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>1982</td>
<td>Goldwasser-Micali</td>
<td>quadratic residuosity</td>
<td>( \log_2(n) )</td>
</tr>
<tr>
<td>1994</td>
<td>Benaloh</td>
<td>higher residuosity</td>
<td>( &gt; 2 )</td>
</tr>
<tr>
<td>1998</td>
<td>Naccache–Stern</td>
<td>higher residuosity</td>
<td>( &gt; 2 )</td>
</tr>
<tr>
<td>1998</td>
<td>Okamoto–Uchiyama</td>
<td>( p )-subgroup</td>
<td>3</td>
</tr>
<tr>
<td>1999</td>
<td>Paillier</td>
<td>composite residuosity</td>
<td>2</td>
</tr>
<tr>
<td>2001</td>
<td>Damgård—Jurik</td>
<td>composite residuosity</td>
<td>( \frac{d+1}{d} )</td>
</tr>
</tbody>
</table>
Outline

1. Introduction

2. Benaloh’s Dense Probabilistic Encryption
   - Original scheme
   - A small problematic example

3. Consequences in applications

4. Corrected version

5. A precise analysis of the problem
   - Probability of failure
   - Message space reduction
Outline

1. Introduction

2. Benaloh’s Dense Probabilistic Encryption
   - Original scheme
   - A small problematic example

3. Consequences in applications

4. Corrected version

5. A precise analysis of the problem
   - Probability of failure
   - Message space reduction
Key Generation

- Choose a block size $r$ and two large primes $p$ and $q$ such that:
  - $r$ divides $(p - 1)$.
  - $r$ and $(p - 1)/r$ are relatively prime.
  - $r$ and $q - 1$ are relatively prime.
  - $n = pq$, $\varphi(n) = (p - 1)(q - 1)$.

- Select $y \in (\mathbb{Z}_n)^* = \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}$ such that
  $$y^{\varphi(n)/r} \not\equiv 1 \mod n$$

The public key is $(y, r, n)$, and the private key is the two primes $p$ and $q$. 
Original cryptosystem

**Encryption**
For $m$ in $\mathbb{Z}_r$:

$$E_r(m) = \{ y^m u^r \mod n : u \in (\mathbb{Z}_n)^* \}.$$  

**Homomorphic property**

$$E_r(m_1) \times E_r(m_2) = E_r(m_1 + m_2).$$
Original cryptosystem

Decryption

\[(y^m u^r)^{(p-1)(q-1)/r} = y^{m(p-1)(q-1)/r} \cdot u^{(p-1)(q-1)}
= y^{m(p-1)(q-1)/r} \mod n.\]

- Find \(m \in \mathbb{Z}_r\) such that
  \[(y^{-m} c)^{(p-1)(q-1)/r} = 1 \mod n.\]

- \(\rightarrow\) discrete logarithm to perform in the subgroup of order \(r\) of \(\mathbb{Z}_p^*\).
- usual index-calculus methods
- efficient algorithm when \(r\) is smooth.
- \(p - 1\) should still have a large co-factor.
Outline

1. Introduction

2. Benaloh’s Dense Probabilistic Encryption
   - Original scheme
   - A small problematic example

3. Consequences in applications

4. Corrected version

5. A precise analysis of the problem
   - Probability of failure
   - Message space reduction
Example

Parameters

- Take \( n = pq = 241 \times 179 = 43139 \), \( r = 15 \), \( y = 27 \).
- \( r \) divides \( p - 1 = 240 \)
- \( r \) and \( (p - 1)/r = 16 \) are coprime.
- \( r \) and \( (q - 1) = 2 \times 89 \) are coprime.
- \( y \) and \( n \) are coprime.
- \( y^{(p-1)(q-1)/r} = 40097 \neq 1 \) mod \( n \).

Example encryption

\[
24187 = y^{112} \in E_r(1) \\
= y^{64} \in E_r(6).
\]
Analysis of the example

Ambiguous encryption

\[ y^5 = 27^5 \]
\[ = 8 \]
\[ = 41^{15} \]
\[ = 41' \mod n. \]

→ the cleartext space is now \( \mathbb{Z}_5 \) instead of \( \mathbb{Z}_{15} \).
Outline

1. Introduction

2. Benaloh’s Dense Probabilistic Encryption
   - Original scheme
   - A small problematic example

3. Consequences in applications

4. Corrected version

5. A precise analysis of the problem
   - Probability of failure
   - Message space reduction
Presidential Election

- Maximum number of ballots $< r = 15$.
- Vote for Nicolas $\in E_r(0)$
- Vote for Ségolène $\in E_r(1)$
- Actual result $R \in E_r(11)$
- Computed result $R \in E_r(11) = E_r(1)$

Ségolène is elected
Nicolas is elected
Problem

- $n$ users in a network
- each user trusts each other with a given trust value.
- Alice wants to know the global trust of the network in Bob.
- Maybe Alice will grant Bob access to (critical) resources based on the computed value.
Private Trust Computation

Algorithm

- each user splits its trust value $t$ into $n - 1$ shares:
  
  $$ t = s_1 + s_2 + \ldots + s_{n-1} \mod r.$$ 

- each user has a Benaloh keypair with the same parameter $r$.

- a share from each user is given to every other user, encrypted under the receiving user’s key.

- the encrypted values are combined and decrypted locally, then combined globally.
Problematic example

- the queried user Bob is a newcomer (trust = 0).
- Charlie uses a faulty $y$ parameter with $r_{\text{true}} = r/3$.
- Charlie’s recombined value should have been $-1$.
- Charlie’s actual contribution will be $r_{\text{true}} - 1 \approx r/3$.

Analysis

- uses Benaloh’s cryptosystem for a common $r$.
- Naccache–Stern’s cryptosystem could be used instead.
Secure Card Dealing

[Goile 2005]

Online Poker

- Need to collaboratively compare $m_1$ and $m_2$ from $E(m_1)$ and $E(m_2)$.
- Encryption performed using Benaloh’s cryptosystem with $r = 53$.
- Not vulnerable to the flaw, with luck (53 is prime).
Outline

1. Introduction

2. Benaloh’s Dense Probabilistic Encryption
   - Original scheme
   - A small problematic example

3. Consequences in applications

4. Corrected version

5. A precise analysis of the problem
   - Probability of failure
   - Message space reduction
Key Generation (recall)

\[
\begin{align*}
    r & \mid (p - 1) \\
    \gcd(r, (p - 1)/r) &= \gcd(r, q - 1) = 1 \\
    y^{\varphi(n)/r} &\neq 1 \mod n
\end{align*}
\]

Let \( g \) be a generator of the group \((\mathbb{Z}_p)^*\), and since \( y \) is coprime with \( n \), let \( \alpha \) be the value in \( \mathbb{Z}_{p-1} \) such that \( y = g^\alpha \mod p \).

Main theorem

The following properties are equivalent:

a) decryption works unambiguously;

b) for all prime factors \( s \) of \( r \), we have \( y^{(\varphi(n)/s)} \neq 1 \mod n \);

c) \( \alpha \) and \( r \) are coprime.
Proof

(c) ⇒ (a) (contrapositive)

- Assume

\[ y^{m_1}u_1^r = y^{m_2}u_2^r \mod n. \]

- Reducing mod \( p \) we get:

\[ g^{\alpha(m_1 - m_2)} = (u_2/u_1)^r \mod p \]

- There exists some \( \beta \) such that

\[
\begin{align*}
g^{\alpha(m_1 - m_2)} &= g^{\beta r} \mod p \\
\alpha(m_1 - m_2) &= \beta r \mod p - 1 \\
\alpha(m_1 - m_2) &= 0 \mod r.
\end{align*}
\]

- Recall \( r \) and \( \alpha \) are coprime
Proof

\((a) \Rightarrow (c)\) (contrapositive)

Assume \(\alpha\) and \(r\) are not coprime and let \(s = \gcd(\alpha, r)\), \(r = sr'\), \(\alpha = s\alpha'\).

\[
yr' = g^{\alpha r'} \mod p
= (g^{\alpha'})^r \mod p.
\]

- \(yr'\) is an \(r\)-th power mod \(p\).
- \(yr'\) is an \(r\)-th power mod \(q\).
- \(yr'\) is a valid encryption of 0 and of \(r'\).
Proof

(c) ⇒ (b)  (contrapositive)

Assume that there exists some prime factor \( s \) of \( r \) such that

\[ y^{\varphi(n)/s} = 1 \text{ mod } n. \]

Reduce mod \( p \):

\[ \alpha \frac{\varphi(n)}{s} = 0 \text{ mod } p - 1. \]

So

\[ \alpha \frac{\varphi(n)}{s} = (p - 1) \frac{\alpha(q - 1)}{s} \]

is a multiple of \( p - 1 \) and \( s \) divides \( \alpha(q - 1) \). Since \( s \) does not divide \( q - 1 \), \( s \) divides \( \alpha \) and \( \alpha \) and \( r \) are not coprime.
Proof

\[(b) \implies (c)\] (contrapositive)

Assume \(\alpha\) and \(r\) are not coprime and denote by \(s\) some common prime factor. Then

\[
y^{(\phi(n)/s)} = g^{\alpha \phi(n)/s} \mod p \\
= g^{(\alpha/s) \phi(n)} \mod p = 1 \mod p.
\]

And by construction of \(r\), \(s \nmid q - 1\) so \(y^{(\phi(n)/s)} = 1 \mod q\).
Outline

1. Introduction

2. Benaloh’s Dense Probabilistic Encryption
   - Original scheme
   - A small problematic example

3. Consequences in applications

4. Corrected version

5. A precise analysis of the problem
   - Probability of failure
   - Message space reduction
Outline

1. Introduction

2. Benaloh’s Dense Probabilistic Encryption
   - Original scheme
   - A small problematic example

3. Consequences in applications

4. Corrected version

5. A precise analysis of the problem
   - Probability of failure
   - Message space reduction
Probability of failure

Incorrect condition

\[ y^{\varphi(n)/r} \neq 1 \mod n \iff r \nmid \alpha. \]

Assume that \( r \) divides \( \alpha \): \( \alpha = r\alpha' \). So

\[
\begin{align*}
y^{\varphi(n)/r} & = g^{\alpha \varphi(n)/r} \mod p \\
& = (g^{\alpha'})^{\varphi(n)} \mod p \\
& = 1 \mod p.
\end{align*}
\]

Since \( r \) divides \( p - 1 \), \( y^{\varphi(n)/r} = 1 \mod q \).
Conversely, if \( y^{\varphi(n)/r} = 1 \mod n \), then

\[
g^{\alpha\varphi(n)/r} = 1 \mod p
\]

\[
\alpha \frac{\varphi(n)}{r} = 0 \mod p - 1.
\]

Since \( r \) divides \( p - 1 \) and is coprime with \( \frac{\varphi(n)}{r} \) (by definition), we have \( r \mid \alpha \). □
Estimating the proportion $\rho$ of faulty $y$’s

- Incorrect condition on $y$: $r \nmid \alpha$.
- Proper condition on $y$: $\alpha$ and $r$ are coprime.

\[
\rho = 1 - \frac{\varphi(r)}{r - 1} \\
= 1 - \frac{r \varphi(r)}{r - 1} \\
= 1 - \frac{r}{r - 1} \prod_i \frac{p_i - 1}{p_i} \\
\approx 1 - \prod_i \frac{p_i - 1}{p_i}
\]
Probability of error

Practical example

\[ p = 2 \times (3 \times 5 \times 7 \times 11 \times 13) \times p' + 1 \]

\[ p' = \begin{align*}
&4464804505475390309548459872862419622870251688508955 \\
&5037374496982090456310601222033972275385171173585381 \\
&3914691524677018107022404660225439441679953592 \\
&5033292671082791323022555160232601405723625177570767 \\
&523893639864538140315412108959927459825236754568279.
\end{align*} \]

\[ q = \begin{align*}
&1005585594745694782468051874865438459560952436544429 \\
&5033292671082791323022555160232601405723625177570767 \\
&523893639864538140315412108959927459825236754568279.
\end{align*} \]

\[ \#p = \#q = 512 \text{ bits.} \]
Probability of error

Practical example (cont’d)

\[
gcd(q - 1, p - 1) = 2
\]

\[
r = (3 \times 5 \times 7 \times 11 \times 13) \times p'
\]

\[
\rho = 1 - \frac{r}{r - 1} \times \frac{2}{3} \times \frac{4}{5} \times \frac{6}{7} \times \frac{10}{11} \times \frac{12}{13} \times \frac{p' - 1}{p'}
\]

\[
\rho > 61\%.
\]
1 Introduction

2 Benaloh’s Dense Probabilistic Encryption
   - Original scheme
   - A small problematic example

3 Consequences in applications

4 Corrected version

5 A precise analysis of the problem
   - Probability of failure
   - Message space reduction
Consequence of a faulty $y$

Let $u = \gcd(\alpha, r)$. Then $r' = \frac{r}{u}$. Moreover if $r' \neq r$, this faulty value of $y$ goes undetected by the initial condition as long as $u \neq r$. 

Cleartext space reduction
DSMP

Let $G$ be an abelian group with subgroups $K$, $H$ such that $G = KH$ and $K \cap H = \{1\}$. The Decisional Subgroup Membership Problem is to decide whether a given $g \in G$ is in $K$ or not.

Examples

- Goldwasser-Micali
- Naccache-Stern
- Okamoto-Uchiyama
- Paillier:

$$E_u(m) = (1 + n)^m u^n \mod n^2$$

- ciphertext space is $G = (\mathbb{Z}_{n^2})^* \simeq (\mathbb{Z}_n)^* \times \mathbb{Z}_n$
- $H$ is the subgroup of order $n$ (generated by $g = 1 + n$)
- $K$ is the set of the invertible $n$-th powers mod $n^2$. 

Application to Benaloh’s corrected scheme

- $G = (\mathbb{Z}_n)^*$
- $H$ the cyclic subgroup of order $r$ of $G$
- $K$ the set of invertible $r$-th powers in $G$
- the public element $y$ must generate $H$.

The semantic security of our corrected scheme is therefore equivalent to the DSMP for $K$, that is, being able to distinguish $r$-th powers modulo $n$. 
A slight change of description caused an error.
Undetected for 16 years.
Used verbatim in several protocol papers, even from last year.
A huge probability of failure for suggested parameters $r = 3^k$.
Quite possibly never implemented.