SAS

MIZOGUCHI Koki[1]

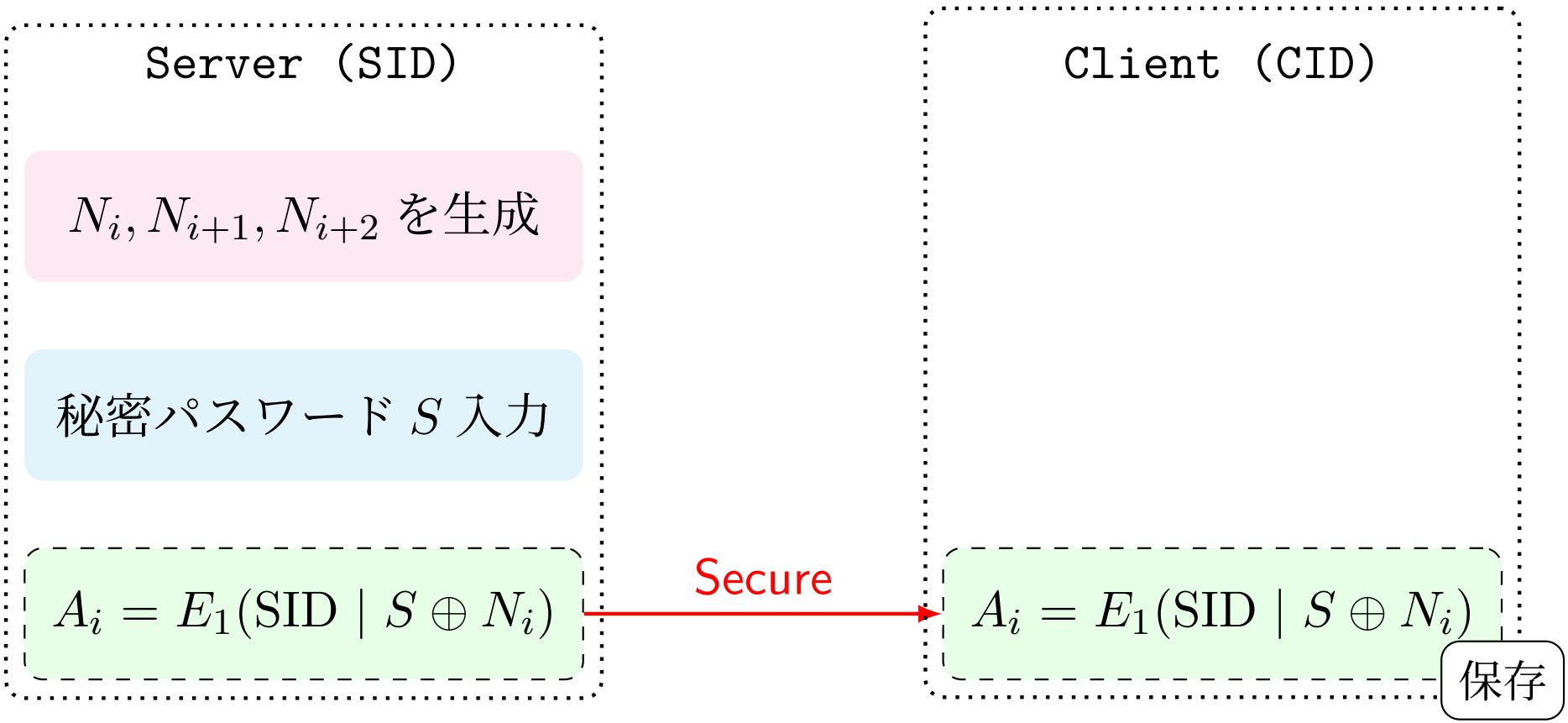
Kochi University of Technology

November 14, 2022

KOCHI UNIVERSITY OF TECHNOLOGY

[1]清水研究室

認証手順


Server (SID)
N_i, N_{i+1}, N_{i+2} を生成
秘密パスワード S 入力
$A_i = E_1(\mathrm{SID} \mid S \oplus N_i)$
Secure
Client (CID)
$A_i = E_1(\mathrm{SID} \mid S \oplus N_i)$
保存

Server が生成するデータ

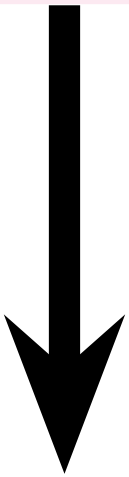
$$A_i = E_1(\mathrm{SID} \mid S \oplus N_i)$$

$$A_{i+1} = E_1(\mathrm{CID} \mid S \oplus N_{i+1})$$

$$A_{i+2} = E_1(\mathrm{SID} \mid S \oplus N_{i+2})$$

Server から Client へデータを送信

$$E_1\left(A_i \oplus A_{i+1}\right)$$



Client

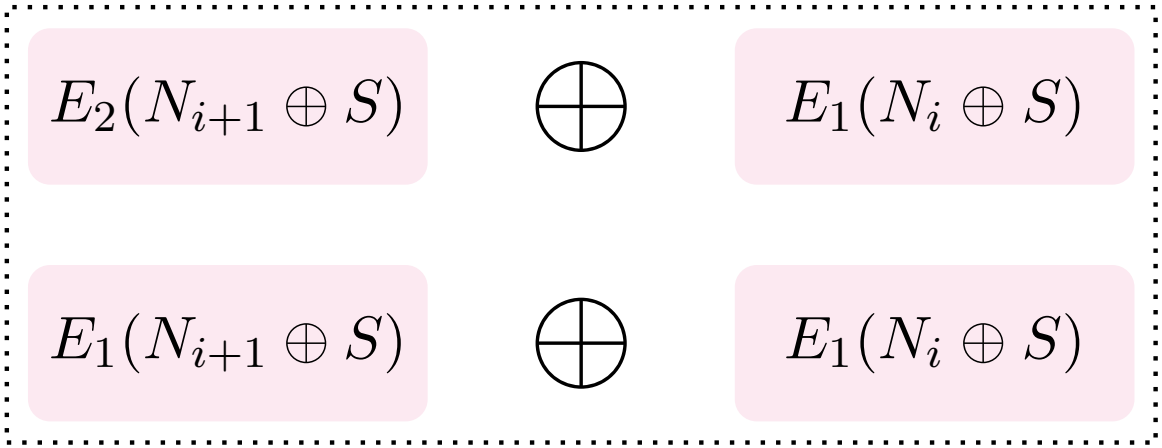
Server 側の処理

認証情報
$E_1(N_i \oplus S)$
$E_2(N_{i+1} \oplus S)$
$E_1(N_i \oplus S)$
$E_1(N_{i+1} \oplus S)$
$E_1(N_i \oplus S)$
受信データ

Server 側の処理

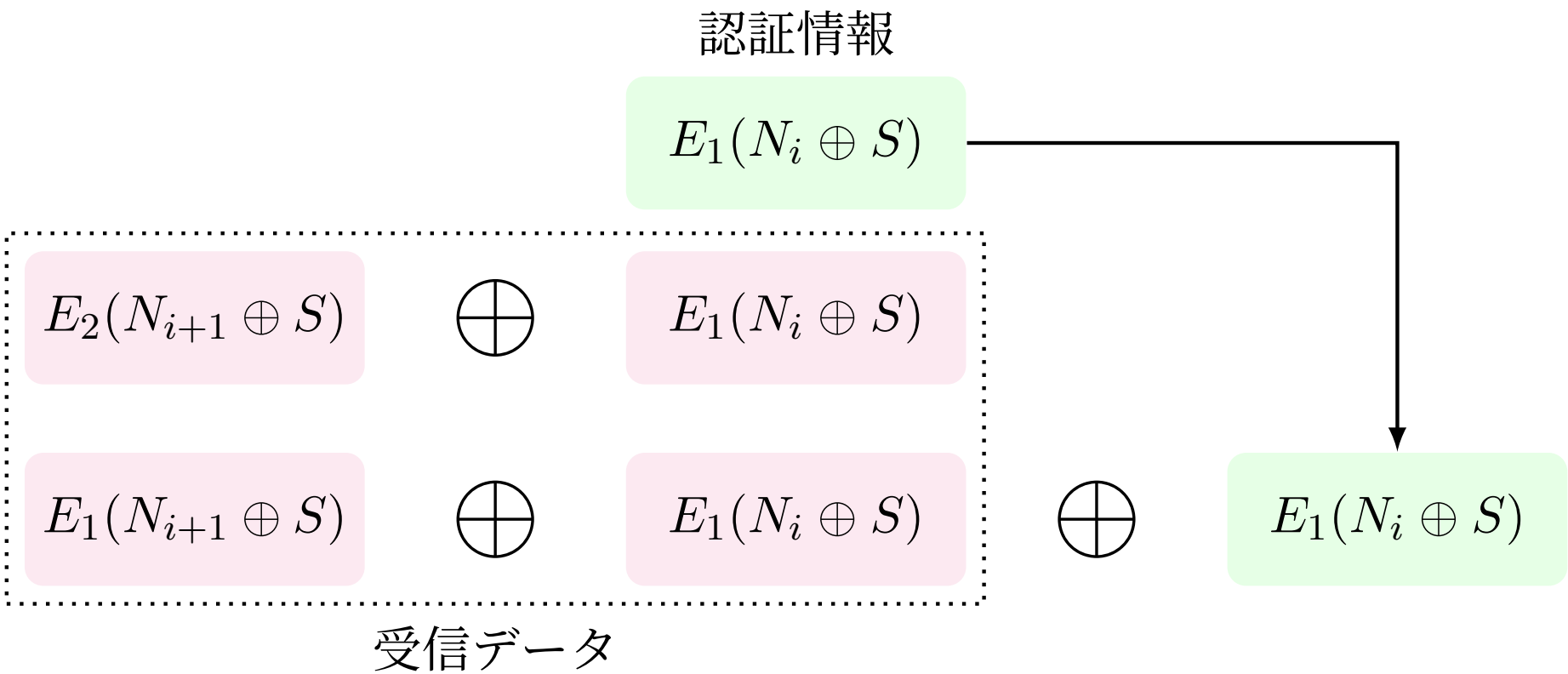
認証情報

$E_1(N_i \oplus S)$

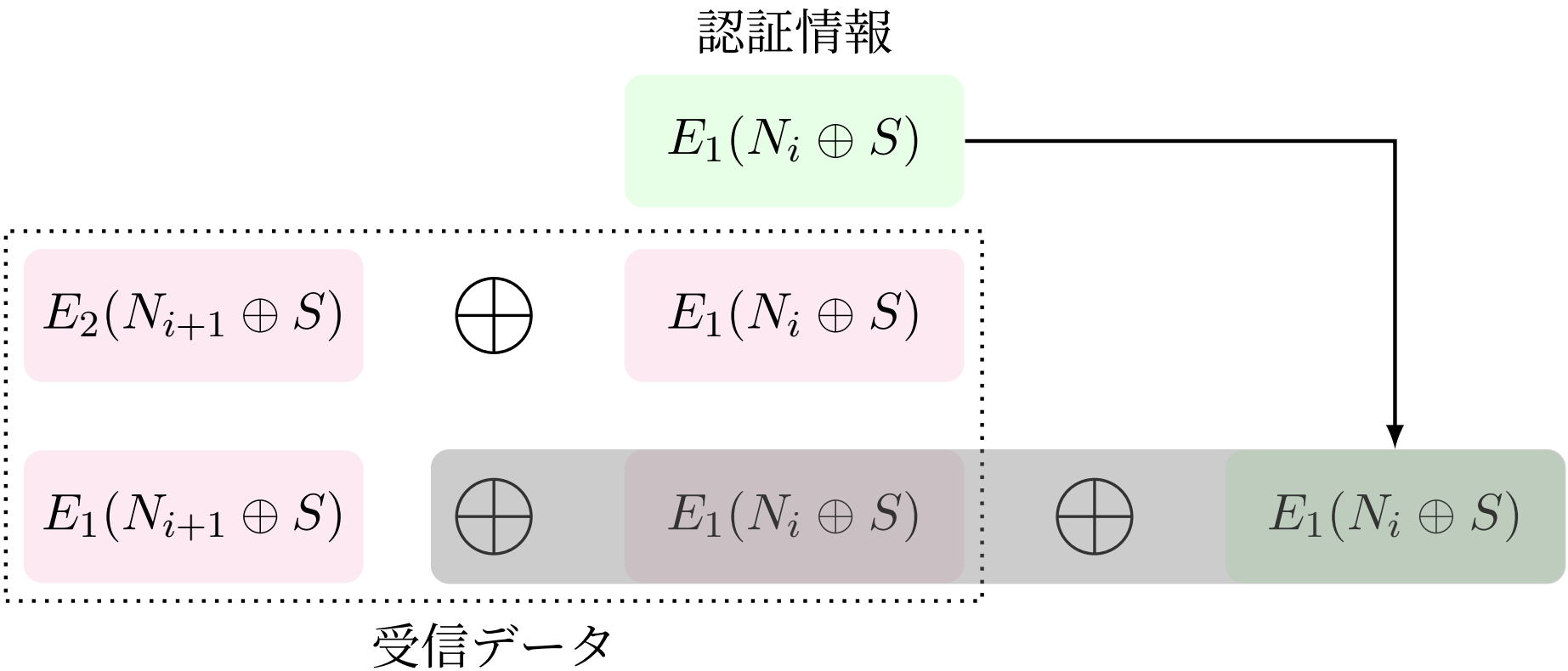


受信データ

Server 側の処理


認証情報
$E_1(N_i \oplus S)$
$E_2(N_{i+1} \oplus S)$
$E_1(N_i \oplus S)$
$E_1(N_{i+1} \oplus S)$
$E_1(N_i \oplus S)$
$E_1(N_i \oplus S)$
受信データ

Server 側の処理


認証情報
$E_1(N_i \oplus S)$
$E_2(N_{i+1} \oplus S)$
$E_1(N_i \oplus S)$
$E_1(N_{i+1} \oplus S)$
$E_1(N_i \oplus S)$
$E_1(N_i \oplus S)$
受信データ

Server 側の処理

認証情報

$E_1(N_i \oplus S)$

$E_2(N_{i+1} \oplus S)$ $\bigoplus$ $E_1(N_i \oplus S)$

$E_1(N_{i+1} \oplus S)$

保存

Server 側の処理

認証情報

$$E_1(N_i \oplus S)$$

$$E_2(N_{i+1} \oplus S) \quad \bigoplus \quad E_1(N_i \oplus S)$$

$$\underline{E_2(N_{i+1} \oplus S)}$$

Server 側の処理

認証情報

$$E_1(N_i \oplus S)$$

$$E_2(N_{i+1} \oplus S) \quad \oplus \quad E_1(N_i \oplus S)$$

$$\oplus$$

$$\underline{E_2(N_{i+1} \oplus S)}$$

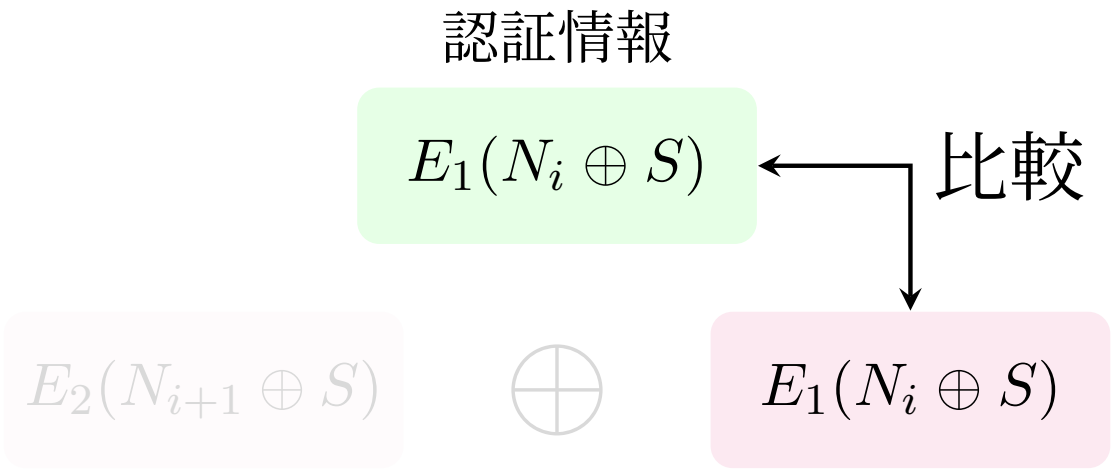
Server 側の処理

認証情報

$$E_1(N_i \oplus S)$$

$$E_2(N_{i+1} \oplus S) \oplus \underline{E_2(N_{i+1} \oplus S)} \quad \oplus \quad E_1(N_i \oplus S)$$

Server 側の処理



0 - 2. 危険性

サーバ情報漏洩の危険性

データセンターに格納してある情報が**悪意のある管理者**または，**不正侵入**によって盗まれた場合，認可されてしまう．その対策として，SAS-X がある．

リプレイアタック

複数回認証要求すると，認証情報 $E_1(N_i \oplus S)$ が得られる脆弱性．（排他的論理和でなく，和 $+$ の演算を加えることで，改善）

その脅威と SAS-X については，お預け（余力があれば次回）

0 - 2. 危険性

サーバ情報漏洩の危険性

データセンターに格納してある情報が**悪意のある管理者**または，**不正侵入**によって盗まれた場合，認可されてしまう．その対策として，SAS-Xがある．

リプレイアタック

複数回認証要求すると，認証情報 $E_1(N_i \oplus S)$ が得られる脆弱性．（排他的論理和でなく，和 $+$ の演算を加えることで，改善）

その脅威と SAS-X については，お預け（余力があれば次回）

0 - 2. 危険性

サーバ情報漏洩の危険性

データセンターに格納してある情報が**悪意のある管理者**または，**不正侵入**によって盗まれた場合，認可されてしまう．その対策として，SAS-Xがある．

リプレイアタック

複数回認証要求すると，認証情報 $E_1(N_i \oplus S)$ が得られる脆弱性．（排他的論理和でなく，和 $+$ の演算を加えることで，改善）

その脅威と SAS-X については，お預け（余力があれば次回）

0 - 2. 危険性

サーバ情報漏洩の危険性

データセンターに格納してある情報が**悪意のある管理者**または，**不正侵入**によって盗まれた場合，認可されてしまう．その対策として，SAS-Xがある．

リプレイアタック

複数回認証要求すると，認証情報 $E_1(N_i \oplus S)$ が得られる脆弱性．（排他的論理和でなく，和 $+$ の演算を加えることで，改善）

その脅威と SAS-X については，お預け（余力があれば次回）

1. 参考文献

- 情報セキュリティ講義資料（SAS 認証方式 2）[清水明宏教授]