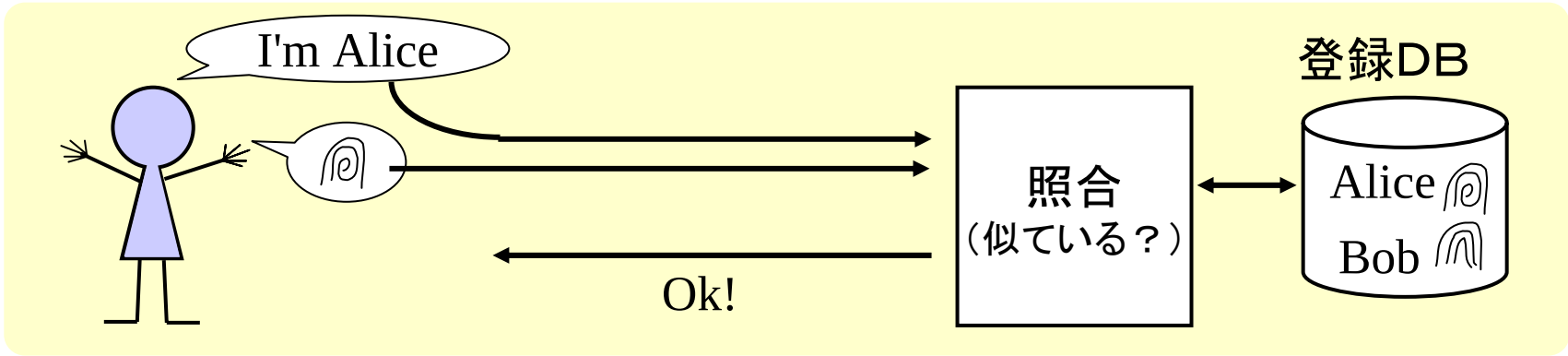
リモート生体認証の安全性

尾形わかは
東京工業大学

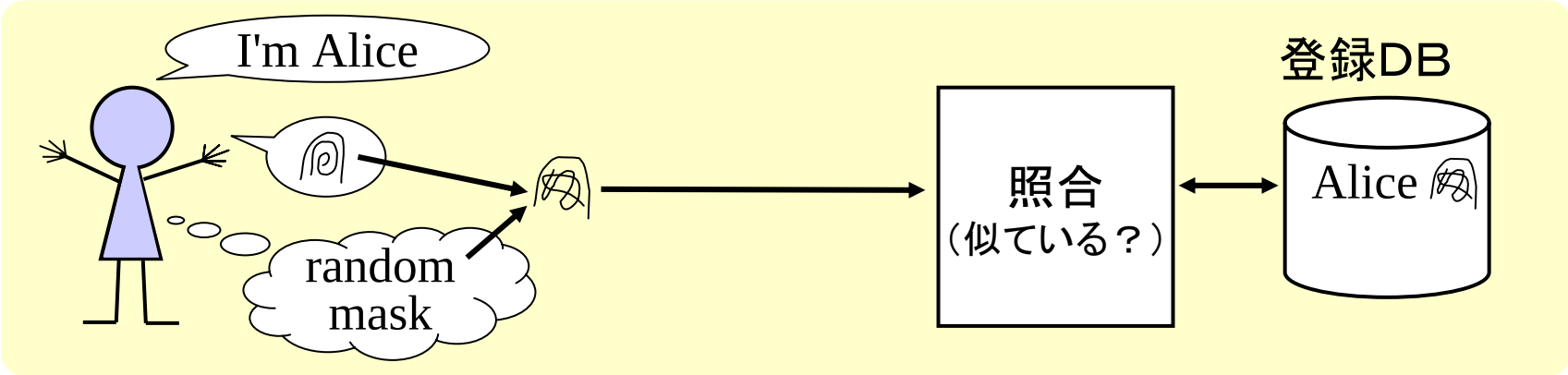
- 背景
- 攻撃モデルの考察
- 既存方式の評価
- まとめ

バイオメトリクス認証



- 問題点
  - 指紋などが他人に取られてしまったら，なりすましができてしまう．
  - その場合，登録取り消しをするが，指は10本しかない（眼なら2つしかない）
  - そもそも，生体情報はプライバシーなので，そのまま登録したくない．

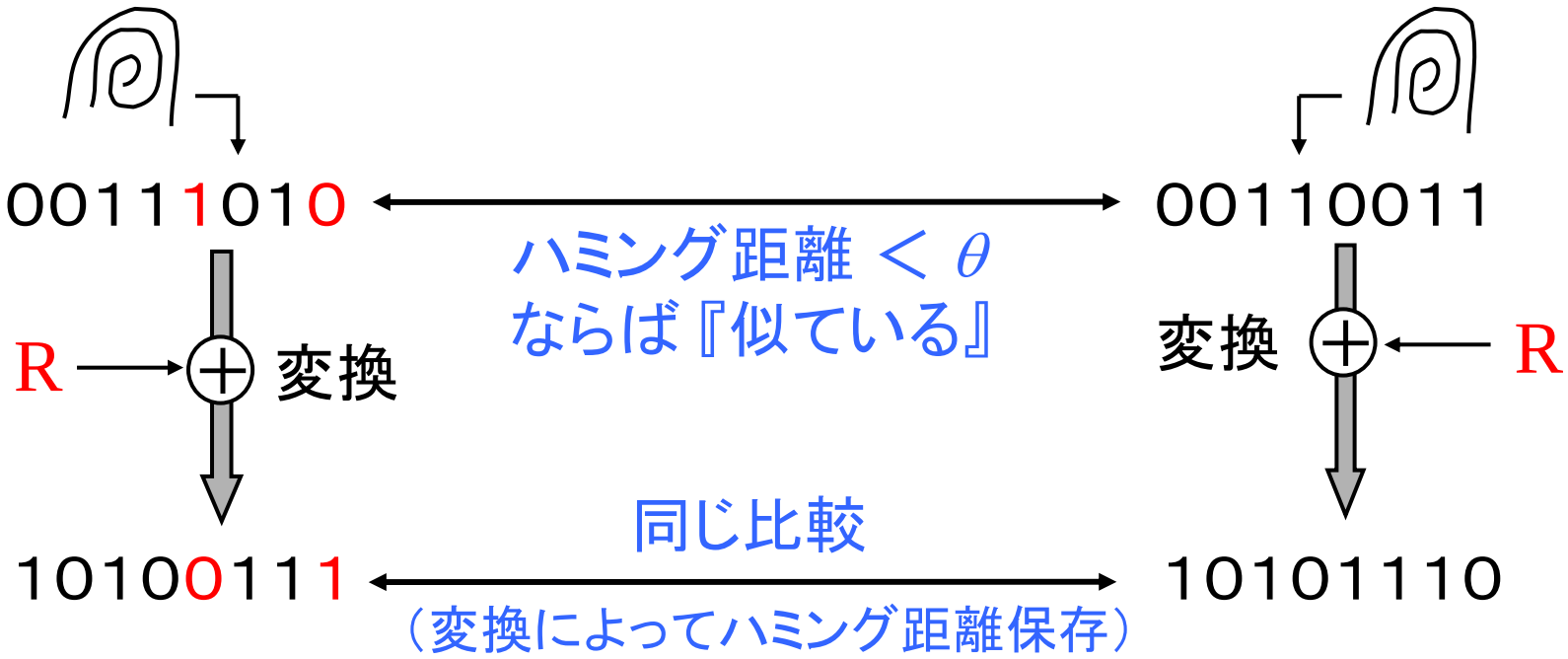
キャンセラブル方式



- 特長
  - Random maskにより変換した生体情報を登録
  - 認証時には，生体情報をrandom maskで変換してから，登録情報（テンプレート）と照合．
  - テンプレートがDBから漏洩した場合には，random maskを変えて登録し直せる．

キャンセラブル方式（例）

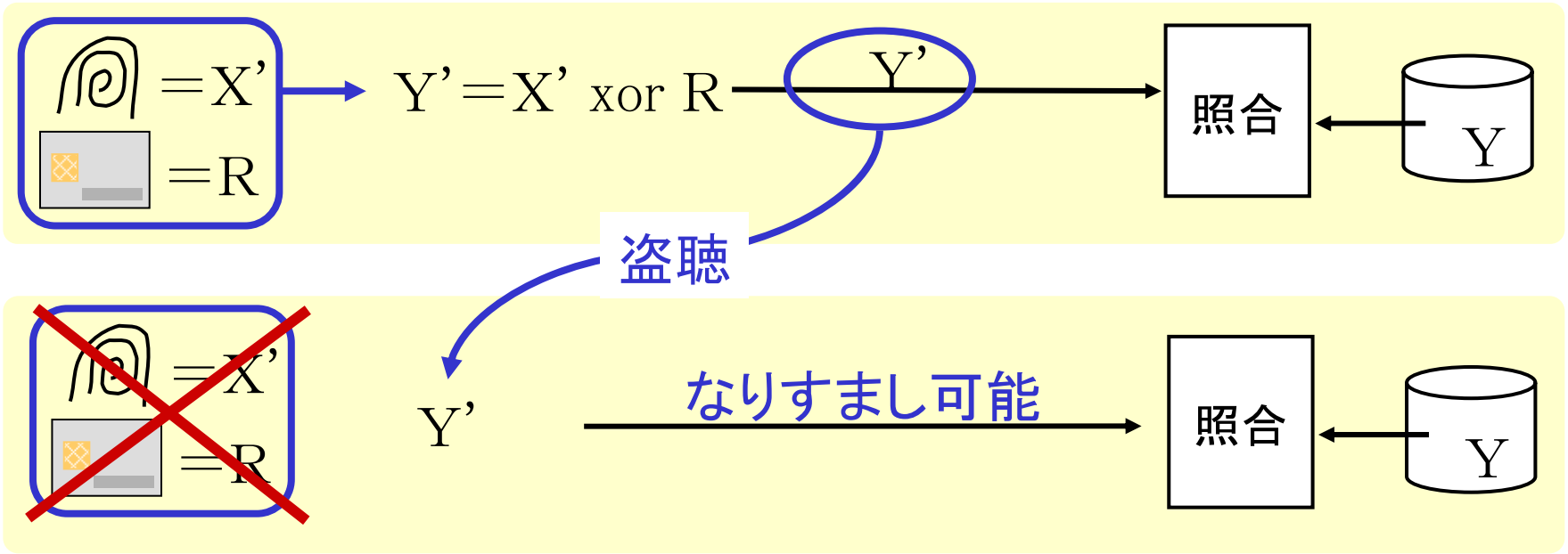
- Xorとハミング距離を用いた方式



ランダムビット列 R は，ICカードに保存してユーザが持ち歩く．

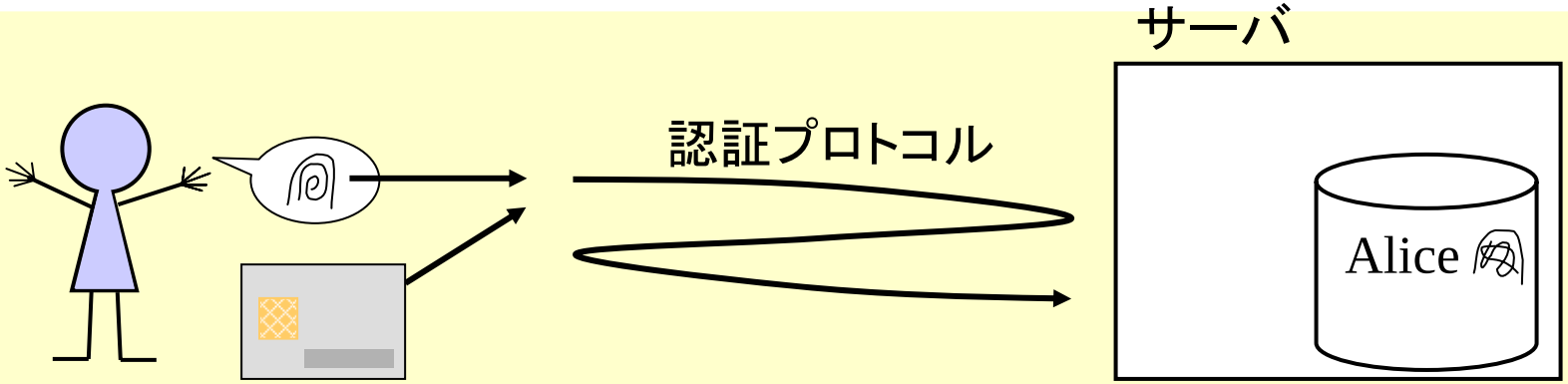
キャンセラブル方式の欠点

- 再送攻撃に弱い



- 比較はサーバが行う　→　何らかの情報が漏れるのではないか？

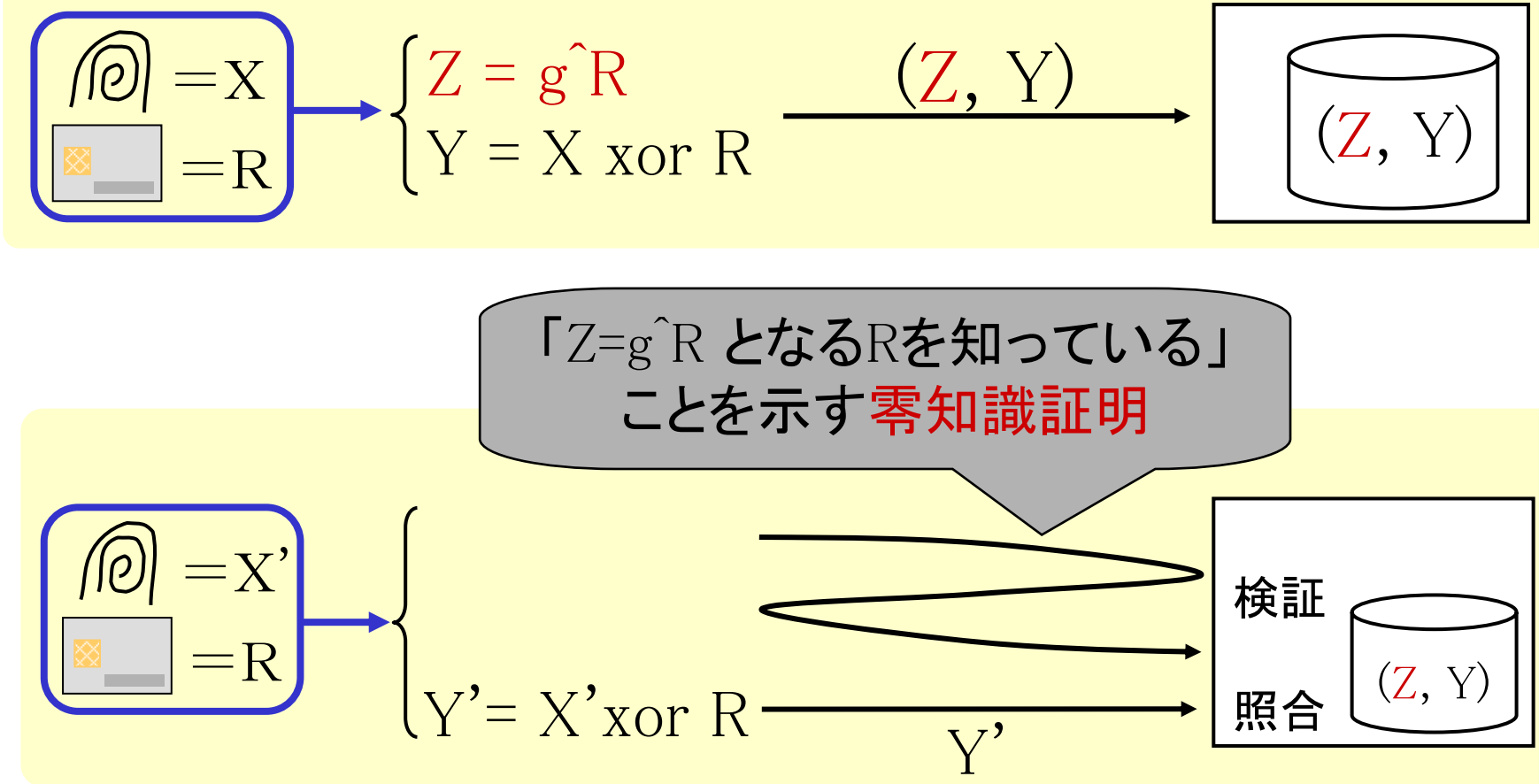
さらに安全な方式（例１）



- 特長
  - 再送攻撃を防ぐ
  - 零知識証明などの暗号技術を用いることにより，サーバへの情報漏洩をも防ぐ．

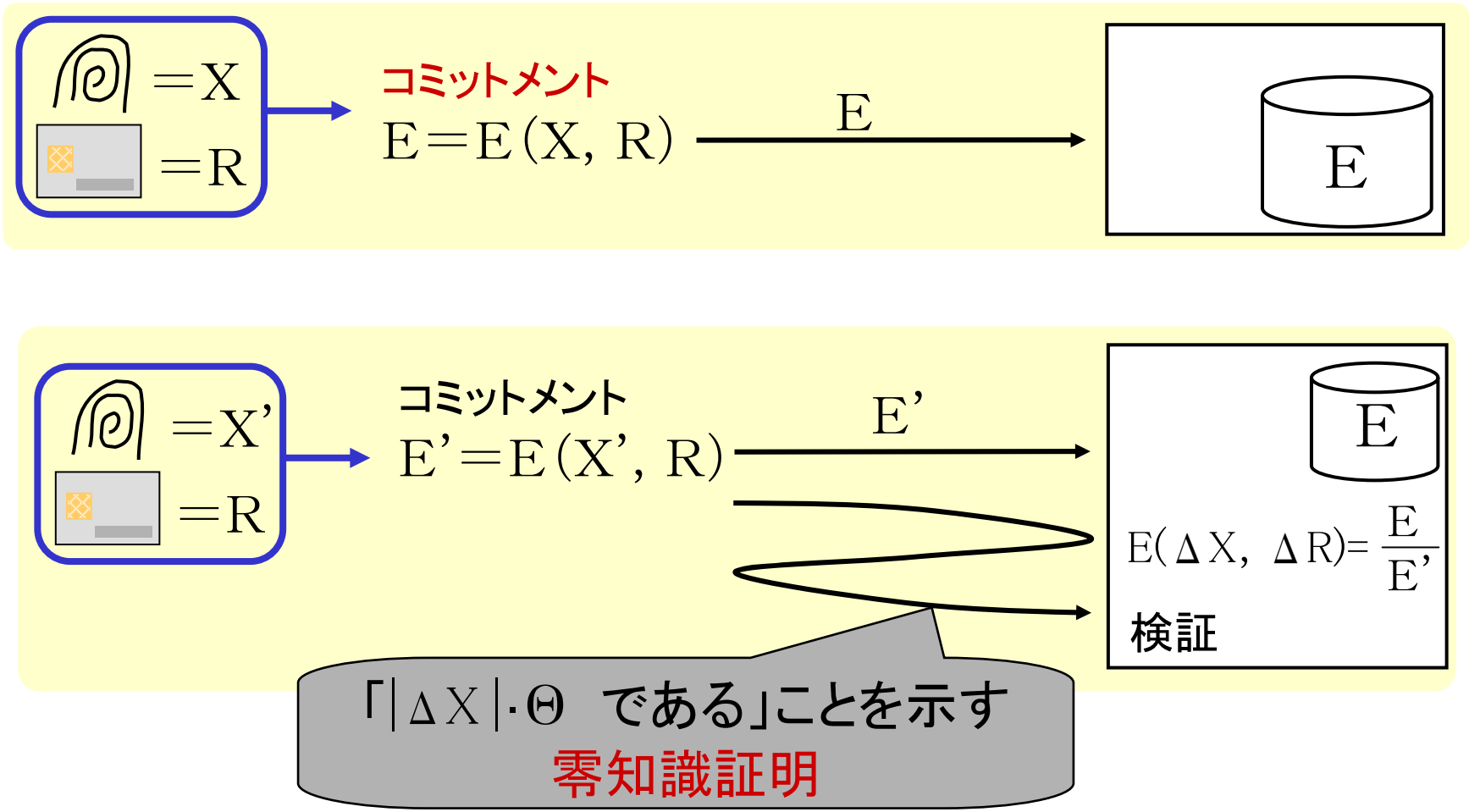
さらに安全な方式（例１）

- Xorとハミング距離　＋　ZKIP（零知識証明）



さらに安全な方式（例2）

- コミットメント　＋　距離のZKIP

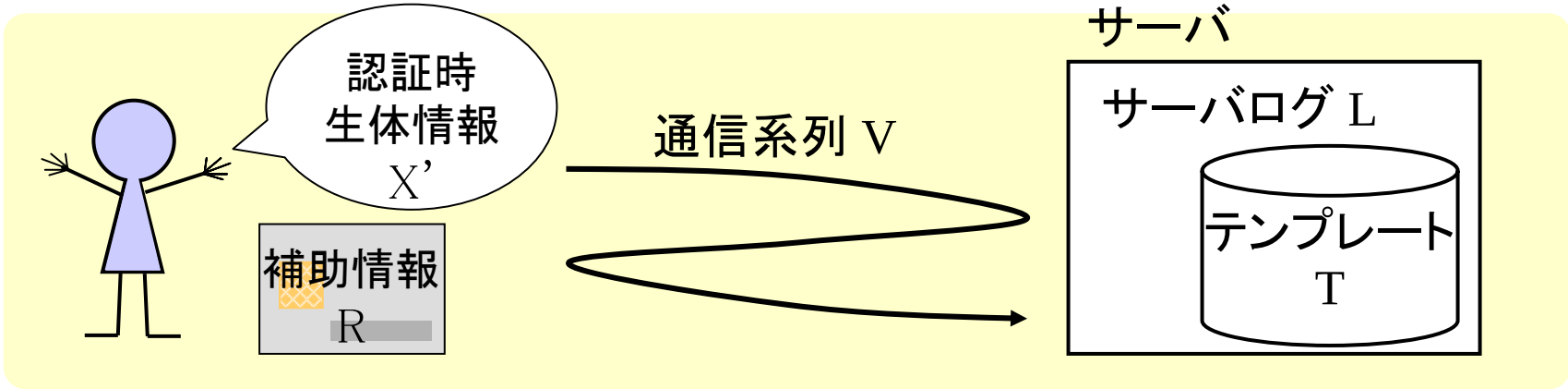


本研究

- リモート生体認証システムに対する攻撃モデルの考察

- 従来の安全性の定義
  - 尾形等のモデル[SITA2006]
    - （なりすまし，生体情報漏洩）×（アタックモデル）
  - 高橋等のモデル [SCIS2007]
    - 3つの安全性要件＋2つの追加要件

リモート生体認証のモデル



- 仮定
  - 補助情報 R とテンプレート T が同時に漏洩することはない.
  - サーバは常にプロトコルに従う.（passive）
  - （通信系列 V は暗号化されている.）

攻撃者の攻撃手段の分類

- 攻撃者が手に入れられる情報
  - 補助情報 R
  - テンプレート T
  - サーバ内ログ L（T を含む）
- サーバへのアクセスの有無
  - 受動的：アクセスしない
  - 能動的：アクセスする

攻撃者の目的の分類

- なりすまし
- 生体情報漏洩　（←システムから見た表現）
  - 生体情報を出力する
    - 登録時の生体情報 X，認証時の生体情報 X’
      ⇒　X に十分近い値を出力する
  - 生体情報を識別する
    - 攻撃者が予想したXに対して，実際に使用されている生体情報がXなのか，そうでないのかを識別

攻撃の分類（1）

- 考えうる全ての攻撃

攻撃手段		なりすまし	生体情報漏洩	
			生体情報を出力	生体情報を識別
受動的	R		T3-a	
	T			
	L		T1	
能動的	R	T3-b		
	T	T2		
	L			

T1～T3は，高橋らによる3つの分類

攻撃の分類（2）

- 考慮する必要のない攻撃の識別

攻撃手段		なりすまし	生体情報漏洩	
			生体情報を出力	生体情報を識別
受動的	R	（無意味）		
	T	（無意味）		
	L	（無意味）		
能動的	R			（不可避）
	T			
	L	（無意味）		

攻撃の分類（3）

- 等価な攻撃の特定

攻撃手段		なりすまし	生体情報漏洩	
			生体情報を出力	生体情報を識別
受動的	R		A1	B1
	T		A2	B2
	L		A3	B3
能動的	R	I1	A4	
	T	I2	=A2	=B2
	L		=A3	=B3

- テンプレートを知っていれば，能動的攻撃は内部でシミュレート可能

攻撃の分類（4）

- 攻撃の関係

攻撃手段		なりすまし	生体情報漏洩	
			生体情報を出力	生体情報を識別
受動的	R		A1→ I1	B1
	T		A2→I2	B2
	L		A3	B3
能動的	R	I1	A4 → I1	
	T	I2		
	L			

- 生体情報を出力できれば，なりすましも可能

攻撃の分類（5）

- 検討すべき攻撃

攻撃手段		なりすまし	生体情報漏洩	
			生体情報を出力	生体情報を識別
受動的	R			B1
	T			B2
	L		A3	B3
能動的	R	I1		
	T	I2		
	L			

攻撃の分類（まとめ）

- リモート生体認証システムに求める安全性

攻撃手段		なりすまし	生体情報漏洩	
			生体情報を出力	生体情報を識別
受動的	R		(T3-a)	B1
	T			B2
	L		A3 (T1)	B3
能動的	R	I1 (T3-b)		
	T	I2 (T2)		
	L			

これまでも議論されてきた

Rが乱数であれば問題なし

新たに考えなければならない攻撃

強い安全性の定義

- 満たすべき安全性
  - I1, I2 : R または T を得ても成りすまし不可.
  - A3 : 不正なサーバに対しても，生体情報が漏れない.
  - B1 : R は生体情報について何も漏らさない.
  - B3 : 不正なサーバが生体情報について何もわからない.（B2を含む）

新しい攻撃(B3)に関する考察

- B3:不正なサーバが生体情報について何もわからない

  ＝ 1ビットも漏れないことを要請？

- B3(B2)の具体的なシナリオ
  - テンプレートが漏洩(テンプレートは更新される)
  - 攻撃者は多くの生体情報を手に入れ，テンプレートがマッチするかどうかを確認し，生体情報を特定することが可能 (オフラインアタック)

既存のシステムの評価（１）

- SITAで発表した方式
  - I1，I2，A3：安全
  - B1：Rは乱数なので安全．
  - B3：安全
    - T は登録時の生体情報 X のコミットメント
      → Xに対して何の情報も漏らさない．
    - 認証プロトコルは，認証時の生体情報X'のコミットメント ＋ ZKIP
      → 何の情報も漏らさない

既存のシステムの評価(2)

- 高橋らがSCIS2007で発表した方式
  - I1, I2, A3:安全
  - B1:Rは乱数なので安全.
  - B3:
    - T = (g^R, Y=X+R mod M) の場合,
      Xを推測
      → Rを逆算
      → g^Rが正しいか検証可能
    - 方法によっては,不正なサーバが推測した生体情報が正しいかどうか確認可能.

まとめ

- 多数の攻撃について関連を考察し，検討に値する5つの攻撃を特定した.
  - 今までも考慮されてきた攻撃（3つ）
  - 既存方式が自明に満たす攻撃（1つ）
  - より強い安全性を求める攻撃（1つ）
    → テンプレート漏洩時のオフラインアタック
- 既存方式の安全性評価を行った.