Key Generation for Body Area Networks

SINCONF 2020

Albert Levi
joint work with Volkan Tuzcu (Medipol Uni.),
Duygu Karaoglan Altop and Dilara Akdogan

Sabancı University

5 November 2020
Outline

1. Introduction
2. Deriving Cryptographic Keys from Physiological Signals
3. SKA-PS: Secure Key Agreement using Physiological Signals
4. SKA-PB: Secure Key Agreement using Pure Biometrics
Introduction
Telemedicine: use of telecommunications technology to provide medical information and services

Rapid advances in wearable sensors: lightweight, small-sized, low power and intelligent monitoring

Body Area Networks: subset of Wireless Sensor Networks

- Self-organized, self-configured
- Biosensors: collect data & make decisions
- *Intra-BAN communication*

Communication through BCU and CS toward healthcare professional
- *Beyond-BAN communication*
Sensing, storage and communication security
- Monitoring mission critical processes → targeted attacks
  - Attacker → pacemaker: reveal ECG & electrical shock
- Sensitive personal medical information → privacy loss
  - HIV-positive care worker: suspended and dismissed from work & health status made public knowledge

Sensing and storage security depends on the device

Communication security should be strongly fulfilled
- Perform data fusion & data delivery
  - Communication channel radius → multihop
- Against eavesdropping and integrity attacks for beyond-BAN communication
- Need for encrypted and authenticated communication for different communication patterns → crypto keys

Node-to-host association via physiological signals and biometrics
Introduction

Deriving Cryptographic Keys from Physiological Signals
SKA-PS: Secure Key Agreement using Physiological Signals
SKA-PB: Secure Key Agreement using Pure Biometrics

Motivations

Contributions

- Sensing, storage and communication security
  - Monitoring mission critical processes $\rightarrow$ targeted attacks
    - Attacker $\rightarrow$ pacemaker: reveal ECG & electrical shock
  - Sensitive personal medical information $\rightarrow$ privacy loss
    - HIV-positive care worker: suspended and dismissed from work & health status made public knowledge

- Sensing and storage security depends on the device
- Communication security should be strongly fulfilled
  - Perform data fusion & data delivery
    - Communication channel radius $\rightarrow$ multihop
  - Against eavesdropping and integrity attacks for beyond-BAN communication
  - Need for encrypted and authenticated communication for different communication patterns $\rightarrow$ crypto keys

- Node-to-host association via physiological signals and biometrics
Sensing, storage and communication security

- Monitoring mission critical processes → targeted attacks
  - Attacker → pacemaker: reveal ECG & electrical shock
- Sensitive personal medical information → privacy loss
  - HIV-positive care worker: suspended and dismissed from work & health status made public knowledge

Sensing and storage security depends on the device

Communication security should be strongly fulfilled

- Perform data fusion & data delivery
  - Communication channel radius → multihop
- Against eavesdropping and integrity attacks for beyond-BAN communication
- Need for encrypted and authenticated communication for different communication patterns → crypto keys

Node-to-host association via physiological signals and biometrics
Sensing, storage and communication security
- Monitoring mission critical processes → targeted attacks
  - Attacker → pacemaker: reveal ECG & electrical shock
- Sensitive personal medical information → privacy loss
  - HIV-positive care worker: suspended and dismissed from work & health status made public knowledge

Sensing and storage security depends on the device

Communication security should be strongly fulfilled
- Perform data fusion & data delivery
  - Communication channel radius → multihop
- Against eavesdropping and integrity attacks for beyond-BAN communication
- Need for encrypted and authenticated communication for different communication patterns → crypto keys
- Node-to-host association via physiological signals and biometrics
Sensing, storage and communication security
- Monitoring mission critical processes → targeted attacks
  - Attacker → pacemaker: reveal ECG & electrical shock
- Sensitive personal medical information → privacy loss
  - HIV-positive care worker: suspended and dismissed from work & health status made public knowledge

Sensing and storage security depends on the device

Communication security should be strongly fulfilled
- Perform data fusion & data delivery
  - Communication channel radius → multihop
  - Against eavesdropping and integrity attacks for beyond-BAN communication
- Need for encrypted and authenticated communication for different communication patterns → crypto keys

Node-to-host association via physiological signals and biometrics
Introduction

Deriving Cryptographic Keys from Physiological Signals
SKA-PS: Secure Key Agreement using Physiological Signals
SKA-PB: Secure Key Agreement using Pure Biometrics

Motivations

Contributions

- Sensing, storage and communication security
  - Monitoring mission critical processes → targeted attacks
    - Attacker → pacemaker: reveal ECG & electrical shock
  - Sensitive personal medical information → privacy loss
    - HIV-positive care worker: suspended and dismissed from work & health status made public knowledge
- Sensing and storage security depends on the device
- Communication security should be strongly fulfilled
  - Perform data fusion & data delivery
    - Communication channel radius → multihop
  - Against eavesdropping and integrity attacks for beyond-BAN communication
    - Need for encrypted and authenticated communication for different communication patterns → crypto keys
- Node-to-host association via physiological signals and biometrics

Albert Levi
Key Generation for Body Area Networks
Sensing, storage and communication security
- Monitoring mission critical processes → targeted attacks
  - Attacker → pacemaker: reveal ECG & electrical shock
- Sensitive personal medical information → privacy loss
  - HIV-positive care worker: suspended and dismissed from work & health status made public knowledge

Sensing and storage security depends on the device

Communication security should be strongly fulfilled
- Perform data fusion & data delivery
  - Communication channel radius → multihop
- Against eavesdropping and integrity attacks for beyond-BAN communication
- Need for encrypted and authenticated communication for different communication patterns → crypto keys

Node-to-host association via physiological signals and biometrics
Propose 4 novel physiological parameter generation techniques and identify 4 appropriate parameters

- For the first time in literature, use BP with ECG & PPG
- Demonstrate suitability of generated physiological parameters on being used as cryptographic keys
- Generate temporally variant physiological parameters
- For the first time in literature, generate temporally invariant physiological parameters
- Propose a novel and efficient key agreement protocol, SKA-PS, providing secure node-to-host association
- Propose a novel and efficient biometric key agreement protocol using pure biometrics, SKA-PB.
  - Biometrics with unordered feature set, e.g. fingerprint
  - No helper component
  - Time variant key generation from time invariant biometrics
Propose 4 novel physiological parameter generation techniques and identify 4 appropriate parameters

For the first time in literature, use BP with ECG & PPG

Demonstrate suitability of generated physiological parameters on being used as cryptographic keys

Generate temporally variant physiological parameters

For the first time in literature, generate temporally invariant physiological parameters

Propose a novel and efficient key agreement protocol, SKA-PS, providing secure node-to-host association

Propose a novel and efficient biometric key agreement protocol using pure biometrics, SKA-PB.

- Biometrics with unordered feature set, e.g. fingerprint
- No helper component
- Time variant key generation from time invariant biometrics
Propose 4 *novel* physiological parameter generation techniques and identify 4 appropriate parameters

*For the first time in literature*, use BP with ECG & PPG

Demonstrate suitability of generated physiological parameters on being used as cryptographic keys

- Generate temporally variant physiological parameters
  - *For the first time in literature*, generate temporally invariant physiological parameters
- Propose a *novel and efficient* key agreement protocol, SKA-PS, providing secure node-to-host association
- Propose a *novel and efficient* biometric key agreement protocol using pure biometrics, SKA-PB.
  - Biometrics with unordered feature set, e.g. fingerprint
  - No helper component
  - Time variant key generation from time invariant biometrics
Propose 4 novel physiological parameter generation techniques and identify 4 appropriate parameters

*For the first time in literature*, use BP with ECG & PPG

Demonstrate suitability of generated physiological parameters on being used as cryptographic keys

Generate temporally variant physiological parameters

*For the first time in literature*, generate temporally invariant physiological parameters

Propose a novel and efficient key agreement protocol, SKA-PS, providing secure node-to-host association

Propose a novel and efficient biometric key agreement protocol using pure biometrics, SKA-PB.

- Biometrics with unordered feature set, e.g. fingerprint
- No helper component
- Time variant key generation from time invariant biometrics
Propose 4 novel physiological parameter generation techniques and identify 4 appropriate parameters

For the first time in literature, use BP with ECG & PPG

Demonstrate suitability of generated physiological parameters on being used as cryptographic keys

Generate temporally variant physiological parameters

For the first time in literature, generate temporally invariant physiological parameters

Propose a novel and efficient key agreement protocol, SKA-PS, providing secure node-to-host association

Propose a novel and efficient biometric key agreement protocol using pure biometrics, SKA-PB.

- Biometrics with unordered feature set, e.g. fingerprint
- No helper component
- Time variant key generation from time invariant biometrics
Introduction

Deriving Cryptographic Keys from Physiological Signals
SKA-PS: Secure Key Agreement using Physiological Signals
SKA-PB: Secure Key Agreement using Pure Biometrics

Motivations

Contributions

- Propose 4 novel physiological parameter generation techniques and identify 4 appropriate parameters
- For the first time in literature, use BP with ECG & PPG
- Demonstrate suitability of generated physiological parameters on being used as cryptographic keys
- Generate temporally variant physiological parameters
- For the first time in literature, generate temporally invariant physiological parameters
- Propose a novel and efficient key agreement protocol, SKA-PS, providing secure node-to-host association
- Propose a novel and efficient biometric key agreement protocol using pure biometrics, SKA-PB.
  - Biometrics with unordered feature set, e.g. fingerprint
  - No helper component
  - Time variant key generation from time invariant biometrics
Propose 4 novel physiological parameter generation techniques and identify 4 appropriate parameters

*For the first time in literature*, use BP with ECG & PPG

Demonstrate suitability of generated physiological parameters on being used as cryptographic keys

Generate temporally variant physiological parameters

*For the first time in literature*, generate temporally invariant physiological parameters

Propose a novel and efficient key agreement protocol, SKA-PS, providing secure node-to-host association

Propose a novel and efficient biometric key agreement protocol using pure biometrics, SKA-PB.

- Biometrics with unordered feature set, e.g. fingerprint
- No helper component
- Time variant key generation from time invariant biometrics
Deriving Cryptographic Keys from Physiological Signals
Remote health monitoring systems

- ECG, BP, oxygen saturation (via PPG) and BT
- Different device specifically designed for recording
- Specific place on the human body to be attached

Choice considerations

- Ability of biosensors on retrieving relevant data
- Requirements of being used as cryptographic keys
  - Universal, user-varying, random

Appropriate physiological parameters

- Inter-pulse interval (IPI)
- Cross-power spectral density (CPSD)
- Feature-level IPI-CPSD fused
Remote health monitoring systems
- ECG, BP, oxygen saturation (via PPG) and BT
- Different device specifically designed for recording
- Specific place on the human body to be attached

Choice considerations
- Ability of biosensors on retrieving relevant data
- Requirements of being used as cryptographic keys
  - Universal, user-varying, random

Appropriate physiological parameters
- Inter-pulse interval (IPI)
- Cross-power spectral density (CPSD)
- Feature-level IPI-CPSD fused
Remote health monitoring systems
- ECG, BP, oxygen saturation (via PPG) and BT
- Different device specifically designed for recording
- Specific place on the human body to be attached

Choice considerations
- Ability of biosensors on retrieving relevant data
- Requirements of being used as cryptographic keys
  - Universal, user-varying, random

Appropriate physiological parameters
- Inter-pulse interval (IPI)
- Cross-power spectral density (CPSD)
- Feature-level IPI-CPSD fused
Remote health monitoring systems
- ECG, BP, oxygen saturation (via PPG) and BT
- Different device specifically designed for recording
- Specific place on the human body to be attached

Choice considerations
- Ability of biosensors on retrieving relevant data
- Requirements of being used as cryptographic keys
  - Universal, user-varying, random

Appropriate physiological parameters
- Inter-pulse interval (IPI)
- Cross-power spectral density (CPSD)
  - Feature-level IPI-CPSD fused
Remote health monitoring systems
- ECG, BP, oxygen saturation (via PPG) and BT
- Different device specifically designed for recording
- Specific place on the human body to be attached

Choice considerations
- Ability of biosensors on retrieving relevant data
- Requirements of being used as cryptographic keys
  - Universal, user-varying, random

Appropriate physiological parameters
- Inter-pulse interval (IPI)
- Cross-power spectral density (CPSD)
- Feature-level IPI-CPSD fused
Propose 4 physiological parameter generation techniques
- Time-domain physiological parameter generation
- Frequency-domain physiological parameter generation
- Concat-fused physiological parameter generation
- XOR-fused physiological parameter generation

Identify 4 appropriate physiological parameters
- IPI-based physiological parameters
- CPSD-based physiological parameters
- IPI-CPSD concat-fused physiological parameters
- IPI-CPSD xor-fused physiological parameters


Time-Domain Physiological Parameter Generation

1. Physiological Signal
2. Peak Detection
3. IPI Calculation
4. Binarization
5. Quantization

Physiological Parameter
### Time-Domain Physiological Parameter Generation

**INPUT:** Signal, \( l, g, \text{ min}, \text{ max}, s, n \)

**OUTPUT:** PhysParam

1. \( P = \text{FindPeakLocations}(\text{Signal}) \)
2. for all \( i \in \{1, \ldots, l\} \) do
   3. \( IPI_{\text{init}}^{i} = P_{i+1} - P_{i} \)
   4. end for
5. \( IPI = \text{zeros}(l/g) \)
6. \( k = 1 \)
7. for \( i = 1 : g : l \) do
   8. for all \( j \in \{1, \ldots, g\} \) do
      9. \( IPI(k) = IPI(k) + IPI_{\text{init}}^{i+j-1} \)
   10. end for
   11. \( k = k + 1 \)
12. end for
13. \( \text{len}_{\text{part}} = \text{floor}(\text{max} - \text{min})/s \)
14. \( \text{part} = \text{zeros}(\text{len}_{\text{part}}) \)
15. \( \text{code} = \text{zeros}(\text{len}_{\text{part}} + 1) \)
16. for all \( i \in \{1, \ldots, \text{len}_{\text{part}}\} \) do
   17. \( \text{part}(i) = \text{min} + i \times s \)
   18. \( \text{code}(i) = i \mod 2^{n} \)
19. end for
20. \( IPI_{\text{quant}} = \text{Quantization}(IPI, \text{part}, \text{code}) \)
21. \( \text{PhysParam} = \text{GrayEncoding}(IPI_{\text{quant}}) \)
**Introduction**

**Deriving Cryptographic Keys from Physiological Signals**

SKA-PS: Secure Key Agreement using Physiological Signals

SKA-PB: Secure Key Agreement using Pure Biometrics

---

**Physiological Signals and Physiological Parameters**

**Physiological Parameter Generation Techniques**

**Performance Analysis**

**Summary**

---

**Time-Domain Physiological Parameter Generation**

**INPUT:** Signal, l, g, min, max, s, n  
**OUTPUT:** PhysParam

1. \( P = \text{FindPeakLocations}(\text{Signal}) \)
2. \( \text{for all } i \in \{1, \ldots, l\} \text{ do} \)
3. \( IPI_{\text{init}}^{i} = P_{i+1} - P_{i} \)
4. \( \text{end for} \)
5. \( IPI = \text{zeros}(l/g) \)
6. \( k = 1 \)
7. \( \text{for } i = 1 : g : l \text{ do} \)
8. \( \text{for all } j \in \{1, \ldots, g\} \text{ do} \)
9. \( IPI(k) = IPI(k) + IPI_{\text{init}}^{i}(i + j - 1) \)
10. \( \text{end for} \)
11. \( k = k + 1 \)
12. \( \text{end for} \)
13. \( \text{len}_{\text{part}} = \text{floor}((\text{max} - \text{min})/s) \)
14. \( \text{part} = \text{zeros}(\text{len}_{\text{part}}) \)
15. \( \text{code} = \text{zeros}(\text{len}_{\text{part}} + 1) \)
16. \( \text{for all } i \in \{1, \ldots, \text{len}_{\text{part}}\} \text{ do} \)
17. \( \text{part}(i) = \text{min} + i \ast s \)
18. \( \text{code}(i) = i \mod 2^n \)
19. \( \text{end for} \)
20. \( IPI_{\text{quant}} = \text{Quantization}(IPI, \text{part}, \text{code}) \)
21. \( \text{PhysParam} = \text{GrayEncoding}(IPI_{\text{quant}}) \)

---

**Example**

\[ i.e.: IPI_{\text{init}} = \{6, 8, 6, 3, 8, 9\} \ & \ g = 2 \]

\[ IPI = \{14, 9, 17\} \]
Introduction
Deriving Cryptographic Keys from Physiological Signals
SKA-PS: Secure Key Agreement using Physiological Signals
SKA-PB: Secure Key Agreement using Pure Biometrics

Physiological Signals and Physiological Parameters
Physiological Parameter Generation Techniques
Performance Analysis
Summary

Time-Domain Physiological Parameter Generation

**INPUT:** Signal, l, g, min, max, s, n

**OUTPUT:** PhysParam

1. $P = \text{FindPeakLocations}(\text{Signal})$
2. for all $i \in \{1, \ldots, l\}$ do
3.   $IPI_{i}^{\text{init}} = P_{i+1} - P_{i}$
4. end for
5. $IPI = \text{zeros}(l/g)$
6. $k = 1$
7. for $i = 1 : g : l$ do
8.   for all $j \in \{1, \ldots, g\}$ do
9.     $IPI(k) = IPI(k) + IPI_{i}^{\text{init}}(i + j - 1)$
10. end for
11. $k = k + 1$
12. end for
13. $\text{len}_{\text{part}} = \text{floor}(\text{max} - \text{min})/s$
14. $\text{part} = \text{zeros}(\text{len}_{\text{part}})$
15. $\text{code} = \text{zeros}(\text{len}_{\text{part}} + 1)$
16. for all $i \in \{1, \ldots, \text{len}_{\text{part}}\}$ do
17.   $\text{part}(i) = \text{min} + i \times s$
18.   $\text{code}(i) = i \mod 2^{n}$
19. end for
20. $IPI^{\text{quant}} = \text{Quantization}(IPI, \text{part}, \text{code})$
21. PhysParam = GrayEncoding($IPI^{\text{quant}}$)

i.e.: $IPI = \{14, 9, 17\}$

$\text{min} = 1 \& \ \text{max} = 20 \& \ s = 5$

Partitions: $\{1 – 5, 6 – 10, 11 – 15, 16 – 20\}$

Codes: $\{0, 1, 2, 3\}$

Quantized IPI sequence: $\{2, 1, 3\}$
Time-Domain Physiological Parameter Generation

**INPUT:** Signal, l, g, min, max, s, n

**OUTPUT:** PhysParam

1. \( P = \text{FindPeakLocations}(\text{Signal}) \)
2. \( \text{for all } i \in \{1, \ldots, l\} \text{ do} \)
3. \( IPI_{init}^i = P_{i+1} - P_i \)
4. \( \text{end for} \)
5. \( IPI = \text{zeros}(l/g) \)
6. \( k = 1 \)
7. \( \text{for } i = 1 : g : l \text{ do} \)
8. \( \text{for all } j \in \{1, \ldots, g\} \text{ do} \)
9. \( IPI(k) = IPI(k) + IPI_{init}(i + j - 1) \)
10. \( \text{end for} \)
11. \( k = k + 1 \)
12. \( \text{end for} \)
13. \( \text{len}_{part} = \text{floor}(\text{max} - \text{min})/s \)
14. \( \text{part} = \text{zeros}(\text{len}_{part}) \)
15. \( \text{code} = \text{zeros}(\text{len}_{part} + 1) \)
16. \( \text{for all } i \in \{1, \ldots, \text{len}_{part}\} \text{ do} \)
17. \( \text{part}(i) = \text{min} + i \times s \)
18. \( \text{code}(i) = i \mod 2^n \)
19. \( \text{end for} \)
20. \( IPI^{quant} = \text{Quantization}(IPI, \text{part}, \text{code}) \)
21. \( \text{PhysParam} = \text{GrayEncoding}(IPI^{quant}) \)

**i.e.:** Quantized IPI sequence: \{2, 1, 3\}

\{0, 1, 2, 3\} \mapsto \{00, 01, 11, 10\}

Encoded physiological parameter: \{11, 01, 10\}
Frequency-Domain Physiological Parameter Generation - Initialization Phase

$$P_{ECG,PPG}(f) = T_{PPG,ECG}(f)$$
Frequency-Domain Physiological Parameter Generation - Operational Phase

\[ P'_{ECG,PPG'}(f) = TF_{PPG,ECG}(f) \times P_{PPG',PPG'}(f) \]

---

Example
Fused Physiological Parameter Generation

Physiological Signal

- Peak Detection
- IPI Calculation
- Quantization
- Binarization

PSD Estimation

Transfer Function

CPSD Calculation

Quantization

Binarization

concat-fused

\( \text{PhysioParam}_{IPI} \parallel \text{PhysioParam}_{CPSD} \)

xor-fused

\( \text{PhysioParam}_{IPI} \oplus \text{PhysioParam}_{CPSD} \)
Experimental Datasets

- **PhysioBank-MIMIC-DB**
  - Simultaneous ECG, PPG and BP signals
  - PhysioBank MIMIC II Waveform database
  - 50 subjects, 125 Hz

- **SU-PhysioDB**
  - Simultaneous ECG and BP signals
  - Collected from volunteers in Sabanci University
  - 166 subjects, 4000 Hz
  - Now made public: http://people.sabanciuniv.edu/levi/projects/114E557/
Experimental Datasets

- **PhysioBank-MIMIC-DB**
  - Simultaneous ECG, PPG and BP signals
  - PhysioBank MIMIC II Waveform database
  - 50 subjects, 125 Hz

- **SU-PhysioDB**
  - Simultaneous ECG and BP signals
  - Collected from volunteers in Sabancı University
  - 166 subjects, 4000 Hz
Performance Metrics

- Randomness
- Distinctiveness
- Error rates
- Temporal variance
Randomness - Shannon Entropy

Closer to 1 → Higher Entropy → Higher Randomness

<table>
<thead>
<tr>
<th>l, g</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>32, 1</td>
<td>0.93</td>
<td>0.84</td>
<td>0.88</td>
<td>0.86</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64, 1</td>
<td>0.90</td>
<td>0.80</td>
<td>0.82</td>
<td>0.76</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128, 1</td>
<td>0.91</td>
<td>0.80</td>
<td>0.73</td>
<td>0.66</td>
<td>0.98</td>
<td>0.97</td>
<td>0.95</td>
<td>0.96</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64, 2</td>
<td>0.94</td>
<td>0.93</td>
<td>0.90</td>
<td>0.87</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128, 2</td>
<td>0.97</td>
<td>0.93</td>
<td>0.92</td>
<td>0.85</td>
<td>0.99</td>
<td>0.99</td>
<td>0.98</td>
<td>0.99</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128, 4</td>
<td>0.96</td>
<td>0.93</td>
<td>0.92</td>
<td>0.92</td>
<td>0.96</td>
<td>0.99</td>
<td>0.99</td>
<td>0.98</td>
<td>0.99</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example

Albert Levi

Key Generation for Body Area Networks
Randomness - Shannon Entropy

Closer to 1 → Higher Entropy → Higher Randomness

<table>
<thead>
<tr>
<th>l, g</th>
<th>PhysioBank-MIMIC-DB</th>
<th>PhysioBank-MIMIC-DB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IPI</td>
<td>CPSD</td>
</tr>
<tr>
<td>32, 1</td>
<td>0.93 0.84 0.88 0.86</td>
<td></td>
</tr>
<tr>
<td>64, 1</td>
<td>0.90 0.80 0.82 0.76</td>
<td></td>
</tr>
<tr>
<td>128, 1</td>
<td>0.91 0.80 0.73 0.66 0.98 0.97 0.95 0.96</td>
<td></td>
</tr>
<tr>
<td>64, 2</td>
<td>0.94 0.93 0.90 0.87</td>
<td></td>
</tr>
<tr>
<td>128, 2</td>
<td>0.97 0.93 0.92 0.85 0.99 0.99 0.98 0.99</td>
<td></td>
</tr>
<tr>
<td>128, 4</td>
<td>0.96 0.93 0.92 0.92 0.99 0.99 0.99 0.99</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>l, g</th>
<th>SU-PhysioDB</th>
<th>SU-PhysioDB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IPI</td>
<td>CPSD</td>
</tr>
<tr>
<td>32, 1</td>
<td>0.97 0.98 0.97 0.94 0.93 0.90</td>
<td></td>
</tr>
<tr>
<td>64, 1</td>
<td>0.96 0.92 0.87 0.83 0.83 0.84</td>
<td></td>
</tr>
<tr>
<td>128, 1</td>
<td>0.98 0.95 0.91 0.87 0.79 0.75 0.99 0.99 0.99 0.98 0.97</td>
<td></td>
</tr>
<tr>
<td>64, 2</td>
<td>0.97 0.96 0.98 0.98 0.98 0.97</td>
<td></td>
</tr>
<tr>
<td>128, 2</td>
<td>0.99 0.98 0.97 0.94 0.93 0.90 0.99 0.99 0.99 0.99 0.98 0.98</td>
<td></td>
</tr>
<tr>
<td>128, 4</td>
<td>0.99 0.98 0.96 0.96 0.97 0.98 0.99 0.99 0.99 0.99 0.99 0.99</td>
<td></td>
</tr>
</tbody>
</table>

Example

Albert Levi  Key Generation for Body Area Networks
Randomness - Shannon Entropy

Closer to 1 → Higher Entropy → Higher Randomness

<table>
<thead>
<tr>
<th>l, g</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IPI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32, 1</td>
<td>0.93</td>
<td>0.84</td>
<td>0.88</td>
<td>0.86</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64, 1</td>
<td>0.90</td>
<td>0.80</td>
<td>0.82</td>
<td>0.76</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128, 1</td>
<td>0.91</td>
<td>0.80</td>
<td>0.73</td>
<td>0.66</td>
<td>0.98</td>
<td>0.97</td>
<td>0.95</td>
<td>0.96</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64, 2</td>
<td>0.94</td>
<td>0.93</td>
<td>0.90</td>
<td>0.87</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128, 2</td>
<td>0.97</td>
<td>0.93</td>
<td>0.92</td>
<td>0.85</td>
<td>0.99</td>
<td>0.99</td>
<td>0.98</td>
<td>0.99</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128, 4</td>
<td>0.96</td>
<td>0.93</td>
<td>0.92</td>
<td>0.92</td>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>l, g</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IPI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32, 1</td>
<td>0.97</td>
<td>0.98</td>
<td>0.97</td>
<td>0.94</td>
<td>0.93</td>
<td>0.90</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64, 1</td>
<td>0.96</td>
<td>0.92</td>
<td>0.87</td>
<td>0.83</td>
<td>0.83</td>
<td>0.84</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128, 1</td>
<td>0.98</td>
<td>0.95</td>
<td>0.91</td>
<td>0.87</td>
<td>0.79</td>
<td>0.75</td>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
<td>0.98</td>
<td>0.97</td>
<td></td>
</tr>
<tr>
<td>64, 2</td>
<td>0.97</td>
<td>0.96</td>
<td>0.98</td>
<td>0.98</td>
<td>0.98</td>
<td>0.97</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128, 2</td>
<td>0.99</td>
<td>0.98</td>
<td>0.97</td>
<td>0.94</td>
<td>0.93</td>
<td>0.90</td>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
<td>0.98</td>
<td>0.98</td>
<td></td>
</tr>
<tr>
<td>128, 4</td>
<td>0.99</td>
<td>0.98</td>
<td>0.96</td>
<td>0.96</td>
<td>0.97</td>
<td>0.98</td>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
<td>0.98</td>
<td>0.98</td>
<td></td>
</tr>
</tbody>
</table>

Example
Randomness - Shannon Entropy

Closer to 1 → Higher Entropy → Higher Randomness

<table>
<thead>
<tr>
<th>l, g</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>IPI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32, 1</td>
<td>0.93</td>
<td>0.84</td>
<td>0.88</td>
<td>0.86</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64, 1</td>
<td>0.90</td>
<td>0.80</td>
<td>0.82</td>
<td>0.76</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128, 1</td>
<td>0.91</td>
<td>0.80</td>
<td>0.73</td>
<td>0.66</td>
<td>0.98</td>
<td>0.97</td>
<td>0.95</td>
<td>0.96</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64, 2</td>
<td>0.94</td>
<td>0.93</td>
<td>0.90</td>
<td>0.87</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128, 2</td>
<td>0.97</td>
<td>0.93</td>
<td>0.92</td>
<td>0.85</td>
<td>0.99</td>
<td>0.99</td>
<td>0.98</td>
<td>0.99</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128, 4</td>
<td>0.96</td>
<td>0.93</td>
<td>0.92</td>
<td>0.92</td>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>l, g</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>concat-fused</td>
<td>0.97</td>
<td>0.97</td>
<td>0.97</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xor-fused</td>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>l, g</th>
<th>64, 2</th>
<th>3</th>
<th>128, 2</th>
<th>5</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>concat-fused</td>
<td>0.99</td>
<td>0.98</td>
<td>0.98</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xor-fused</td>
<td>0.99</td>
<td>0.99</td>
<td>0.99</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example
Distinctiveness - Hamming Distance

\[ D_s \Rightarrow \text{average Hamming distance among the physiological parameters that are generated from the same host} \]

\[ D_d \Rightarrow \text{average Hamming distance among the physiological parameters that are generated from the different hosts} \]
Distinctiveness - Hamming Distance

- IPI-based
Distinctiveness - Hamming Distance

- IPI-based
- CPSD-based
Distinctiveness - Hamming Distance

- IPI-based
- CPSD-based
- concat-fused
Distinctiveness - Hamming Distance

- IPI-based
- CPSD-based
- concat-fused
- xor-fused
## Error Rates - EER (Equal Error Rate)

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Method</th>
<th>EER(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PhysioBank-MIMIC-DB</td>
<td>Time-domain</td>
<td>4.2</td>
</tr>
<tr>
<td></td>
<td>Frequency-domain</td>
<td>15.3</td>
</tr>
<tr>
<td></td>
<td>concat-fused</td>
<td>3.6</td>
</tr>
<tr>
<td></td>
<td>xor-fused</td>
<td>12.0</td>
</tr>
<tr>
<td>SU-PhysioDB</td>
<td>Time-domain</td>
<td>4.1</td>
</tr>
<tr>
<td></td>
<td>Frequency-domain</td>
<td>13.4</td>
</tr>
<tr>
<td></td>
<td>concat-fused</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>xor-fused</td>
<td>6.0</td>
</tr>
</tbody>
</table>
## Temporal Variance - Temporal Ratio ($R$)

- **$R \geq 1$: Temporally Variant**
- **$R < 1$: Temporally Invariant**

### Physiological Signals and Physiological Parameters

#### Performance Analysis

### Summary

### Key Generation for Body Area Networks
Temporal Variance - Temporal Ratio ($R$)

$R \geq 1$: Temporally Variant

$R < 1$: Temporally Invariant

<table>
<thead>
<tr>
<th>$l, g$</th>
<th>PhysioBank-MIMIC-DB</th>
<th>SU-PhysioDB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IPI</td>
<td>CRM</td>
</tr>
<tr>
<td>32, 1</td>
<td>$1.18 \ 0.79 \ 0.57 \ 0.42$</td>
<td>$2.07 \ 1.69 \ 1.61 \ 1.73 \ 1.39 \ 1.18$</td>
</tr>
<tr>
<td>64, 1</td>
<td>$2.32 \ 1.33 \ 1.57 \ 0.85$</td>
<td>$3.22 \ 2.46 \ 1.94 \ 1.35 \ 1.24 \ 1.35$</td>
</tr>
<tr>
<td>128, 1</td>
<td>$3.76 \ 1.80 \ 1.43 \ 0.99$</td>
<td>$3.14 \ 3.11 \ 2.68 \ 2.40 \ 1.67 \ 1.36$</td>
</tr>
<tr>
<td>64, 2</td>
<td>$2.13 \ 1.78 \ 1.11 \ 0.93$</td>
<td>$2.45 \ 2.33 \ 1.97 \ 1.64 \ 1.67 \ 1.76$</td>
</tr>
<tr>
<td>128, 2</td>
<td>$7.68 \ 4.80 \ 2.90 \ 1.63$</td>
<td>$3.21 \ 3.63 \ 3.45 \ 2.66 \ 2.52 \ 2.07$</td>
</tr>
<tr>
<td>128, 4</td>
<td>$4.16 \ 2.41 \ 2.10 \ 1.97$</td>
<td>$3.16 \ 2.70 \ 2.31 \ 2.32 \ 2.08 \ 1.91$</td>
</tr>
</tbody>
</table>
Temporal Variance - Temporal Ratio ($R$)

$R \geq 1$: Temporally Variant

$R < 1$: Temporally Invariant

<table>
<thead>
<tr>
<th>l.g</th>
<th>s</th>
<th>IPI</th>
<th>CPSD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1.18</td>
<td>0.79</td>
</tr>
<tr>
<td>32, 1</td>
<td>3</td>
<td>1.80</td>
<td>1.43</td>
</tr>
<tr>
<td>64, 1</td>
<td>4</td>
<td>1.78</td>
<td>1.11</td>
</tr>
<tr>
<td>128, 1</td>
<td>5</td>
<td>2.90</td>
<td>1.63</td>
</tr>
<tr>
<td>64, 2</td>
<td>6</td>
<td>2.10</td>
<td>1.97</td>
</tr>
<tr>
<td>128, 2</td>
<td>7</td>
<td>4.21</td>
<td>2.41</td>
</tr>
<tr>
<td>128, 4</td>
<td>8</td>
<td>4.16</td>
<td>2.10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>l.g</th>
<th>s</th>
<th>IPI</th>
<th>CPSD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>2.07</td>
<td>1.69</td>
</tr>
<tr>
<td>32, 1</td>
<td>4</td>
<td>3.22</td>
<td>2.46</td>
</tr>
<tr>
<td>64, 1</td>
<td>5</td>
<td>3.11</td>
<td>2.68</td>
</tr>
<tr>
<td>128, 1</td>
<td>6</td>
<td>3.14</td>
<td>3.11</td>
</tr>
<tr>
<td>64, 2</td>
<td>7</td>
<td>2.45</td>
<td>2.33</td>
</tr>
<tr>
<td>128, 2</td>
<td>8</td>
<td>3.21</td>
<td>3.63</td>
</tr>
<tr>
<td>128, 4</td>
<td>9</td>
<td>3.16</td>
<td>2.70</td>
</tr>
</tbody>
</table>
Each can be used in the key management protocols designed to secure the intra-BAN communications:

- Key binding (fuzzy commitment/vault)
- Key generation

Either directly or via some protocol regulations
SKA-PS: Secure Key Agreement using Physiological Signals
Secure Key Agreement using Physiological Signals

- Generates symmetric cryptographic keys from physiological parameters
- Secure key agreement $\Rightarrow$ application of set reconciliation technique
  - Set Reconciliation: finite field based protocol in which parties have two different sets and they learn the set differences without revealing the actual contents of the sets
  - Physiological parameter sequences $\Rightarrow$ appropriate sets

- Employ 2 different biosensors:
  - Source biosensor
  - Conforming biosensor

- Instantiate our protocol model using the IPI values derived from the ECG and BP signals
Secure Key Agreement using Physiological Signals

- Generates symmetric cryptographic keys from physiological parameters
- Secure key agreement ⇔ application of set reconciliation technique
  - Set Reconciliation: finite field based protocol in which parties have two different sets and they learn the set differences without revealing the actual contents of the sets
  - Physiological parameter sequences ⇔ appropriate sets

Employ 2 different biosensors:
  - Source biosensor
  - Conforming biosensor

Instantiate our protocol model using the IPI values derived from the ECG and BP signals
Secure Key Agreement using Physiological Signals

- Generates symmetric cryptographic keys from physiological parameters
- Secure key agreement ⇒ application of set reconciliation technique
  - Set Reconciliation: finite field based protocol in which parties have two different sets and they learn the set differences without revealing the actual contents of the sets
  - Physiological parameter sequences ⇒ appropriate sets

Employ 2 different biosensors:

- Source biosensor
- Conforming biosensor

Instantiate our protocol model using the IPI values derived from the ECG and BP signals
SKA-PS with Modifications on Set Reconciliation

- Input: Generated physiological parameters after quantization but before binarization, i.e. some integers
- Aim of biosensors: agree on a symmetric shared key
  - Conforming biosensor $\rightarrow$ source biosensor set
  - So what is going to be the set? All elements in a single set?
  - Conforming biosensor must understand where to remove and add difference elements
  - The way of doing this is to sort all elements in both sets; however, sorting reduces the randomness (not good)
  - Without sorting, the only option is brute-force search for the place of the elements $\rightarrow$ enormous computational cost
SKA-PS with Modifications on Set Reconciliation

- **Input:** Generated physiological parameters after quantization but before binarization, i.e. some integers
- **Aim of biosensors:** agree on a symmetric shared key
  - Conforming biosensor \( \xrightarrow{\text{reconcile}} \) source biosensor set
  - So what is going to be the set? All elements in a single set?
  - Conforming biosensor must understand where to remove and add difference elements
  - The way of doing this is to sort all elements in both sets; however, sorting reduces the randomness (not good)
  - Without sorting, the only option is brute-force search for the place of the elements \( \rightarrow \) enormous computational cost
SKA-PS with Modifications on Set Reconciliation

- Input: Generated physiological parameters after quantization but before binarization, i.e. some integers
- Aim of biosensors: agree on a symmetric shared key
  - Conforming biosensor $\xrightarrow{\text{reconcile}}$ source biosensor set
  - So what is going to be the set? All elements in a single set?
  - Conforming biosensor must understand where to remove and add difference elements
  - The way of doing this is to sort all elements in both sets; however, sorting reduces the randomness (not good)
  - Without sorting, the only option is brute-force search for the place of the elements $\rightarrow$ enormous computational cost
SKA-PS with Modifications on Set Reconciliation

**Our Solution:** Part by part processing
- Divide the input physiological parameters into sets with fixed number of *sorted* elements (in our tests 4 and 8)
- Protocol works in round-manner
  - Biosensors aim to find $r$ matching sets
  - Start with $r$ sets and try to reconcile them (only small amount of missing elements are allowed for each set)
  - If all successfully reconciled, Bingo!!! key is agreed
  - Otherwise add one more set and try all possible combinations with $r$ subsets to reconcile
  - Continue until:
    - They find $r$ successfully reconciled sets and key is agreed, or
    - All sets are tried and no success, protocol terminates without key agreement
SKA-PS with Modifications on Set Reconciliation

- **Our Solution**: Part by part processing
- Divide the input physiological parameters into sets with fixed number of *sorted* elements (in our tests 4 and 8)
- Protocol works in round-manner
  - Biosensors aim to find \( r \) matching sets
  - Start with \( r \) sets and try to reconcile them (only small amount of missing elements are allowed for each set)
  - If all successfully reconciled, Bingo!!! key is agreed
  - Otherwise add one more set and try all possible combinations with \( r \) subsets to reconcile
  - Continue until:
    - They find \( r \) successfully reconciled sets and key is agreed
    - All sets are tried and no success, protocol terminates without key agreement
SKA-PS with Modifications on Set Reconciliation

- **Our Solution:** Part by part processing
- Divide the input physiological parameters into sets with fixed number of *sorted* elements (in our tests 4 and 8)
- Protocol works in round-manner
  - Biosensors aim to find *r* matching sets
  - Start with *r* sets and try to reconcile them (only small amount of missing elements are allowed for each set)
  - If all successfully reconciled, Bingo!!! key is agreed
  - Otherwise add one more set and try all possible combinations with *r* subsets to reconcile
  - Continue until:
    - They find *r* successfully reconciled sets and key is agreed, or
    - All sets are tried and no success, protocol terminates without key agreement
SKA-PS with Modifications on Set Reconciliation

- **Our Solution**: Part by part processing
- Divide the input physiological parameters into sets with fixed number of *sorted* elements (in our tests 4 and 8)
- Protocol works in round-manner
  - Biosensors aim to find $r$ matching sets
  - Start with $r$ sets and try to reconcile them (only small amount of missing elements are allowed for each set)
  - If all successfully reconciled, Bingo!!! key is agreed
  - Otherwise add one more set and try all possible combinations with $r$ subsets to reconcile
  - Continue until:
    - They find $r$ successfully reconciled sets and key is agreed, or
    - All sets are tried and no success, protocol terminates without key agreement
SKA-PS with Modifications on Set Reconciliation

- **Our Solution**: Part by part processing
- Divide the input physiological parameters into sets with fixed number of *sorted* elements (in our tests 4 and 8)
- Protocol works in round-manner
  - Biosensors aim to find *r* matching sets
  - Start with *r* sets and try to reconcile them (only small amount of missing elements are allowed for each set)
  - If all successfully reconciled, Bingo!!! key is agreed
  - Otherwise add one more set and try all possible combinations with *r* subsets to reconcile
  - Continue until:
    - They find *r* successfully reconciled sets and key is agreed, or
    - All sets are tried and no success, protocol terminates without key agreement
SKA-PS with Modifications on Set Reconciliation

- **Our Solution**: Part by part processing
- Divide the input physiological parameters into sets with fixed number of *sorted* elements (in our tests 4 and 8)
- Protocol works in round-manner
  - Biosensors aim to find $r$ matching sets
  - Start with $r$ sets and try to reconcile them (only small amount of missing elements are allowed for each set)
  - If all successfully reconciled, Bingo!!! key is agreed
  - Otherwise add one more set and try all possible combinations with $r$ subsets to reconcile
- Continue until:
  - They find $r$ successfully reconciled sets and key is agreed, or
  - All sets are tried and no success, protocol terminates without key agreement
SKA-PS with Modifications on Set Reconciliation

- **Our Solution**: Part by part processing
- Divide the input physiological parameters into sets with fixed number of *sorted* elements (in our tests 4 and 8)
- Protocol works in round-manner
  - Biosensors aim to find $r$ matching sets
  - Start with $r$ sets and try to reconcile them (only small amount of missing elements are allowed for each set)
  - If all successfully reconciled, Bingo!!! key is agreed
  - Otherwise add one more set and try all possible combinations with $r$ subsets to reconcile
  - Continue until:
    - They find $r$ successfully reconciled sets and key is agreed, or
    - All sets are tried and no success, protocol terminates without key agreement
SKA-PS with Modifications on Set Reconciliation

- **Our Solution**: Part by part processing
- Divide the input physiological parameters into sets with fixed number of *sorted* elements (in our tests 4 and 8)
- Protocol works in round-manner
  - Biosensors aim to find \( r \) matching sets
  - Start with \( r \) sets and try to reconcile them (only small amount of missing elements are allowed for each set)
  - If all successfully reconciled, Bingo!!! key is agreed
  - Otherwise add one more set and try all possible combinations with \( r \) subsets to reconcile
  - Continue until:
    - They find \( r \) successfully reconciled sets and key is agreed, or
    - All sets are tried and no success, protocol terminates without key agreement

Albert Levi  
Key Generation for Body Area Networks
SKA-PS with Modifications on Set Reconciliation

- **Our Solution:** Part by part processing
- Divide the input physiological parameters into sets with fixed number of *sorted* elements (in our tests 4 and 8)
- Protocol works in round-manner
  - Biosensors aim to find $r$ matching sets
  - Start with $r$ sets and try to reconcile them (only small amount of missing elements are allowed for each set)
  - If all successfully reconciled, Bingo!!! key is agreed
  - Otherwise add one more set and try all possible combinations with $r$ subsets to reconcile
  - Continue until:
    - They find $r$ successfully reconciled sets and key is agreed, or
    - All sets are tried and no success, protocol terminates without key agreement
Inputs and Performance Metrics

- Input physiological parameter
  - IPI-based physiological parameter

- Performance metrics
  - True match and false match rates
  - Randomness, distinctiveness and temporal variance
  - Computational, communication and storage complexity
Inputs and Performance Metrics

- Input physiological parameter
  - IPI-based physiological parameter

- Performance metrics
  - True match and false match rates
  - Randomness, distinctiveness and temporal variance
  - Computational, communication and storage complexity
## True Match and False Match Rates

<table>
<thead>
<tr>
<th>Parameters</th>
<th>True Match Rate (%)</th>
<th>False Match Rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>s</td>
<td>d</td>
<td>n</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>16</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>95</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>100</td>
</tr>
</tbody>
</table>
Randomness and Temporal Variance

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Randomness</th>
<th>Temporal Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>s</td>
</tr>
<tr>
<td>Randomness</td>
<td></td>
<td>0.9114</td>
</tr>
<tr>
<td>Temporal Ratio</td>
<td></td>
<td>0.9101</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.9105</td>
</tr>
<tr>
<td>4</td>
<td>14</td>
<td>0.9114</td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td>0.9101</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>0.9105</td>
</tr>
<tr>
<td>2</td>
<td>9</td>
<td>0.9092</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>0.9099</td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>0.9091</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>0.9100</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>0.9109</td>
</tr>
</tbody>
</table>
Distinctiveness
### Complexity: Average Number of Protocol Rounds

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Average Number of Protocol Rounds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Source Biosensor</td>
</tr>
<tr>
<td>$s$</td>
<td>$d$</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
</tr>
</tbody>
</table>
## Complexity: Average Number of Protocol Rounds

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Average Number of Protocol Rounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>s d n</td>
<td>Source Biosensor</td>
</tr>
<tr>
<td>4 1 14</td>
<td>2.93</td>
</tr>
<tr>
<td>10</td>
<td>19</td>
</tr>
<tr>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>16</td>
<td>114.74</td>
</tr>
<tr>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>8 2 9</td>
<td>4.64</td>
</tr>
<tr>
<td>10</td>
<td>5.81</td>
</tr>
<tr>
<td>8 3 7</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>1.28</td>
</tr>
<tr>
<td>9</td>
<td>1.63</td>
</tr>
</tbody>
</table>

*ON THE AVERAGE*

Total key agreement latency: 6 sec
Communication complexity: 58 Byte
Storage complexity: 197 Byte
Conclusions for SKA-PS

- SKA-PS enables biosensors to agree on symmetric keys
  - Directly generated from the sensed data
  - Remarkably high true match rates
  - Exceedingly low false match rates
  - Low computational, communication and storage costs

- SKA-PS meets the requirements of BANs stemming from the limitations of the biosensors
  - Can fill the "lightweight security protocol"-gap in the literature
Conclusions for SKA-PS

SKA-PS enables biosensors to agree on symmetric keys
- Directly generated from the sensed data
- Remarkably high true match rates
- Exceedingly low false match rates
- Low computational, communication and storage costs

SKA-PS meets the requirements of BANs stemming from the limitations of the biosensors
- Can fill the "lightweight security protocol"-gap in the literature
Conclusions and Future Directions for Intra-BAN part

- Intra-BAN communication architecture
- Secure node-to-host association
- Use of physiological signals
- Highly random and distinctive physiological parameters
- Low error rate possessing physiological parameters
- Dynamic key agreement with low costs
Conclusions and Future Directions for Intra-BAN part

- Intra-BAN communication architecture
  - Secure node-to-host association
  - Use of physiological signals
  - Highly random and distinctive physiological parameters
  - Low error rate possessing physiological parameters
  - Dynamic key agreement with low costs

- Future work
  - Hardware implementation
  - Other physiological signals
SKA-PB: Secure Key Agreement using Pure Biometrics
Our key agreement protocol for beyond-BAN communication

Round-manner

- At each round, try to find a common set of minutiae

At the end

- Either, low similarity score so no key agreed
- Or, agreement on a secure symmetric key
  - Secure key: User-varying, time-varying, random
Our key agreement protocol for beyond-BAN communication

Round-manner
- At each round, try to find a common set of minutiae

At the end
- Either, low similarity score so no key agreed
- Or, agreement on a secure symmetric key
  - Secure key: User-varying, time-varying, random
Enrollment Phase

- Three fingerprint images of same finger; $FP_1$, $FP_2$, $FP_3$
- Minutiae extraction: $(x, y, type)$
  - $x$: x-coordinate of the minutia
  - $y$: y-coordinate of the minutia
  - type: type of the minutia, end or bifurcation
Enrollment Phase

- Three fingerprint images of same finger; $FP_1$, $FP_2$, $FP_3$
- Minutiae extraction: $(x, y, \text{type})$
  - $x$: x-coordinate of the minutia
  - $y$: y-coordinate of the minutia
  - type: type of the minutia, end or bifurcation
Enrollment Phase

*Neighborhood relation*

- \( T_{\text{dist}} \): Pre-defined distance threshold
- In the \( T_{\text{dist}} \)-neighborhood of \((x_j, y_j)\)
  - \( x \)-coordinate in \([x_j - T_{\text{dist}}, x_j + T_{\text{dist}}]\)
  - \( y \)-coordinate in \([y_j - T_{\text{dist}}, y_j + T_{\text{dist}}]\)

Quantize all minutiae at most \( T_{\text{dist}} \)-away to one representative minutia with smallest \( y \)-coordinate.
Enrollment Phase

- **Neighborhood relation**
  - \( T_{\text{dist}} \): Pre-defined distance threshold
  - In the \( T_{\text{dist}} \)-neighborhood of \((x_j, y_j)\)
    - \(x\)-coordinate in \([x_j - T_{\text{dist}}, x_j + T_{\text{dist}}]\)
    - \(y\)-coordinate in \([y_j - T_{\text{dist}}, y_j + T_{\text{dist}}]\)
  - Quantize all minutiae at most \( T_{\text{dist}} \)-away to one representative minutia with smallest \(y\)-coordinate
Enrollment Phase

FP1 \rightarrow \text{ExtractMinutiae} \rightarrow \text{Quantization} \rightarrow \text{Most Reliable Minutiae} \rightarrow \text{Hash}(x||y||\text{type})

FP2 \rightarrow \text{ExtractMinutiae} \rightarrow \text{Quantization} \rightarrow \text{Most Reliable Minutiae} \rightarrow \text{Hash}(x||y||\text{type})

FP3 \rightarrow \text{ExtractMinutiae} \rightarrow \text{Quantization} \rightarrow \text{Most Reliable Minutiae} \rightarrow \text{Hash}(x||y||\text{type})
Verification Phase

- As in the enrollment phase, user side
  - Three fingerprint images of the same finger
  - Quantization according to the $T_{dist}$-neighborhood
  - Most reliable minutiae
  - Hash

- Fake minutiae points generation
  - 10 times the number of genuine minutiae points
  - Indistinguishable from a genuine minutia point
  - We preserve $T_{dist}$-neighborhood relation
Verification Phase

- As in the enrollment phase, user side
  - Three fingerprint images of the same finger
  - Quantization according to the $T_{\text{dist}}$-neighborhood
  - Most reliable minutiae
  - Hash

- Fake minutiae points generation
  - 10 times the number of genuine minutiae points
  - Indistinguishable from a genuine minutia point
  - We preserve $T_{\text{dist}}$-neighborhood relation
The Protocol

**USER**

Mix $\text{Hash}^2$(Genuine Minutiae) and $\text{Hash}^2$(Fake Minutiae)

Try all possible subsets in size of common minutiae

IF Verify HMAC
   → ACCEPT & BREAK

IF NOT ACCEPTED
   → RETRY

**SERVER**

Find common minutiae & Calculate score

IF score < threshold → REJECT

ELSE Key = $\text{Hash}^1(\text{Hash}^1(\text{Common Minutiae}))$

$\text{HMAC}_{\text{Key}}$

ACCEPT

RETRY
The Protocol

**USER**

- Try all possible subsets in size of common minutiae - 1
  - IF Verify HMAC → ACCEPT & BREAK
  - IF NOT ACCEPTED → RETRY

**SERVER**

- Calculate score with size – 1
  - IF score < threshold → REJECT
  - ELSE All possible
    - Key = \(Hash^1(Hash^1(\text{Common Minutiae-1}))\)
    - \(\text{HMAC}_{\text{Key}}\)

- ACCEPT & index

- RETRY
The Protocol

USER

Try all possible subsets in size of common minutiae - i
IF Verify HMAC
    → ACCEPT & BREAK
IF NOT ACCEPTED
    → RETRY

SERVER

Calculate score with size - i
IF score < threshold → REJECT
ELSE All possible
    Key = Hash\(^1\)(Hash\(^1\)(Common Minutiae-i))
    HMAC\(_{Key}\)

All HMACs

ACCEPT & index

RETRY
Settings

1\textsuperscript{st} Dataset: 30 fingerprints from Verifinger Sample Database*
   - 8 impressions: 3 for server, 5 for user

2\textsuperscript{nd} Dataset: 292 fingerprints from volunteers in Sabancı University
   - 10 impressions: 3 for server, 7 for user

Alignment in MATLAB using intensity values

Minutiae extraction using Neurotechnology Biometric SDK 5.0 Verifinger, http://www.neurotechnology.com/

Both genuine and impostor tests

256-bit keys
Verification Performance

- 0.57% EER with 1\textsuperscript{st} dataset
- 0.48% EER with 2\textsuperscript{nd} dataset
Brute-force Attack Analysis

- Trying all possible keys $\Rightarrow 2^{256} \Rightarrow$ infeasible

- Intelligent brute-force attack
  - Generate all possible minutiae locations and types, and hashes
  - Does not search all possible minutiae combination $\Rightarrow$ Naive brute-force
  - Decrease search space to genuine and fake minutiae set of which hashes are transmitted during the protocol
    - Try all possible subsets and verify any HMAC

1\textsuperscript{st} dataset
- $\Rightarrow 2^{94}$ hash and HMAC verifications

2\textsuperscript{nd} dataset
- $\Rightarrow 2^{118}$ hash and HMAC verifications
Brute-force Attack Analysis

- Trying all possible keys $\Rightarrow 2^{256} \Rightarrow$ infeasible
- Intelligent brute-force attack
  - Generate all possible minutiae locations and types, and hashes
  - Does not search all possible minutiae combination $\Rightarrow$ Naive brute-force
  - Decrease search space to genuine and fake minutiae set of which hashes are transmitted during the protocol
    - Try all possible subsets and verify any HMAC

- 1\textsuperscript{st} dataset
  - $\Rightarrow 2^{94}$ hash and HMAC verifications
- 2\textsuperscript{nd} dataset
  - $\Rightarrow 2^{118}$ hash and HMAC verifications
Brute-force Attack Analysis

- Trying all possible keys $\Rightarrow 2^{256} \Rightarrow$ infeasible

- Intelligent brute-force attack
  - Generate all possible minutiae locations and types, and hashes
  - Does not search all possible minutiae combination $\Rightarrow$
  - Naive brute-force
  - Decrease search space to genuine and fake minutiae set of which hashes are transmitted during the protocol
    - Try all possible subsets and verify any HMAC

- $1^{st}$ dataset
  - $\Rightarrow 2^{94}$ hash and HMAC verifications

- $2^{nd}$ dataset
  - $\Rightarrow 2^{118}$ hash and HMAC verifications
Randomness-Shannon’s Entropy

1\textsuperscript{st} dataset

- All keys’ entropy
  \[\text{Hash}(x\mathbin{||}y\mathbin{||}\text{type})\]

- Minutiae’ entropy
  \[(x\mathbin{||}y\mathbin{||}\text{type})\]
Randomness-Shannon’s Entropy

2\textsuperscript{nd} dataset

- All keys’ entropy
  $\text{Hash}(x||y||\text{type})$
- Minutiae’ entropy
  $(x||y||\text{type})$

Albert Levi
Key Generation for Body Area Networks
Distinctiveness-Hamming Distance

- Same user must have different key after each protocol run
- Different users must have different keys

Hamming Distance

- Measuring the distinctiveness of the generated keys
- Number of bits which are different at the same positions of two equal length strings
- Closer to midpoint (128 for our case) → the more different keys
Distinctiveness-Hamming Distance

- Same user must have different key after each protocol run
- Different users must have different keys

Hamming Distance

- Measuring the distinctiveness of the generated keys
- Number of bits which are different at the same positions of two equal length strings
- Closer to midpoint (128 for our case) → the more different keys
Distinctiveness-Hamming Distance

1st dataset

- Same user’s keys
- Different users’ keys

---

Albert Levi

Key Generation for Body Area Networks
Distinctiveness-Hamming Distance

$2^{nd}$ dataset

- Same user’s keys
- Different users’ keys

Albert Levi  
Key Generation for Body Area Networks
Computational Complexity

\[ \sum_{i=n_{com}}^{n_{key}} \binom{n_{com}}{i} \]

\( n_{com} \): Number of common found minutiae by the server

\( n_{key} \): Number of minutiae with which the key is generated

- **Average server complexity**
  - \( 2^{17} \) with 1\(^{st} \) dataset
  - \( 2^9 \) with 2\(^{nd} \) dataset

\[ \sum_{i=n_{com}}^{n_{key}} \binom{n_{com}}{i} \]

\( n_u \): Number of genuine minutiae on the user side

- **Average user complexity**
  - \( 2^{39} \) with 1\(^{st} \) dataset
  - \( 2^{41} \) with 2\(^{nd} \) dataset
Communication Complexity

- Total size of the messages sent by the server
  - $1^{st}$ Dataset $\approx 22.4$ MB
  - $2^{nd}$ Dataset $\approx 332.8$ KB

- Total size of the messages sent by the user
  - $1^{st}$ Dataset $\approx 13.75$ KB
  - $2^{nd}$ Dataset $\approx 17.2$ KB
Memory Requirements

1\textsuperscript{st} Dataset
- Server side
  - Average storage is 578.8 KB per subject
- User side
  - Average storage is 15 KB for each user

2\textsuperscript{nd} Dataset
- Server side
  - Average storage is 702.8 KB per subject
- User side
  - Average storage is 18.75 KB for each user
Conclusions

- Design and analysis of a new bio-cryptographic key agreement protocol
- Secure key agreement without any helper or random data
- Resistance against known attacks
- Random and distinctive keys
- Computational complexity is relatively higher for user, but feasible for server
- Acceptable communication and memory overhead
Conclusions

- Design and analysis of a new bio-cryptographic key agreement protocol
- Secure key agreement without any helper or random data
  - Resistance against known attacks
  - Random and distinctive keys
  - Computational complexity is relatively higher for user, but feasible for server
  - Acceptable communication and memory overhead
Conclusions

- Design and analysis of a new bio-cryptographic key agreement protocol
- Secure key agreement without any helper or random data
- Resistance against known attacks
  - Random and distinctive keys
  - Computational complexity is relatively higher for user, but feasible for server
  - Acceptable communication and memory overhead
Conclusions

- Design and analysis of a new bio-cryptographic key agreement protocol
- Secure key agreement without any helper or random data
- Resistance against known attacks
- Random and distinctive keys
- Computational complexity is relatively higher for user, but feasible for server
- Acceptable communication and memory overhead
Conclusions

- Design and analysis of a new bio-cryptographic key agreement protocol
- Secure key agreement without any helper or random data
- Resistance against known attacks
- Random and distinctive keys
- Computational complexity is relatively higher for user, but feasible for server
- Acceptable communication and memory overhead
Conclusions

- Design and analysis of a new bio-cryptographic key agreement protocol
- Secure key agreement without any helper or random data
- Resistance against known attacks
- Random and distinctive keys
- Computational complexity is relatively higher for user, but feasible for server
- Acceptable communication and memory overhead
Future Work (Completed)

- Template renewal process ⇒ Non-invertible cancelable template
- Adaptation to ordered set of biometric features
Acknowledgments

This work was supported by TÜBİTAK (Scientific and Technological Research Council of Turkey) under grant 114E557

Duygu Karaoğlan Altop was supported by TÜBİTAK BİDEB 2211-C and Turkcell Academy Technology Leaders Graduate Scholarship Program

Dilara Akdoğan was supported by TÜBİTAK BİDEB 2228
THANK YOU!
Example: IPI Peak Points

- FFT filtering and Matlab’s `findpeaks` function
- Manual accuracy check → working correctly 100%
Example: IPI Sequence

- Generated IPI sequences - just before quantization
  - $l = 128$, $g = 4 \Rightarrow$ IPI sequence length: 32
  - From 2 different users’ BP signals
Example: CPSD Sequence

- Generated CPSD sequences - just before quantization
  - \( l = 128, \ g = 4 \Rightarrow \) CPSD sequence length: 32
  - From 2 different users’ BP signals
SU-PhysioDB Dataset Details
Generated IPI-based physiological parameters

- $l = 128$, $g = 4$, $s = 4$
- From 2 different users’ BP signals
Generated CPSD-based physiological parameters
- $l = 128$, $g = 4$, $s = 9$
- From 2 different users’ BP signals
Example: Agreed Symmetric Key

- Agreed symmetric cryptographic keys
- From 2 different users’ BP signals
Protocol Parameters

- $s$ should not be too large
  - Output: $(4 \times s \times b)$-bit cryptographic keys
    - Key strength: $2^{4s}$
    - Set strength: $2^{4s}$
  - Sorting decreases the number of possible combinations
    - Set: $\{0, 1\}$
    - Combinations: $\{\{0, 0\}, \{0, 1\}, \{1, 0\}, \{1, 1\}\}$
    - Sorted combinations: $\{\{0, 0\}, \{0, 1\}, \{1, 1\}\}$

- $d$ can be at most $(s/2 - 1)$
  - Characteristic polynomial of degree $s$ can be solved with $s + 1$ linear equations
  - $s$ also determines whether there is information leakage

- $r$ should be determined based on key strength

<table>
<thead>
<tr>
<th>$r$</th>
<th>$s$</th>
<th>$d$</th>
<th>Effective Key Length (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>4</td>
<td>1</td>
<td>$\approx 131$</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>$\frac{2}{3}$</td>
<td>$\approx 132$</td>
</tr>
</tbody>
</table>
Attacker’s aim: learn the key or impersonate

Secure channel is not assumed ⇒ attacker can
- Obtain protocol messages
- Attacker can learn the number of required sets
- Learn the combination index

Attacker can apply
- Brute-force attack
- Replay attack
- Classical impersonation attack
Brute-force attack

- Classical brute-force
  - $(4 \times s \times b)$-bit cryptographic keys with an effective strength of 131 bits $\rightarrow$ complexity is $2^{131}$

- Roots of the characteristic polynomial
  - Insufficient exchanged information $\rightarrow$ complexity is $2^{4s \times r}$

<table>
<thead>
<tr>
<th>$r$</th>
<th>$s$</th>
<th>Resistance Against Brute-Force</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>4</td>
<td>$2^{176}$</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>$2^{224}$</td>
</tr>
</tbody>
</table>

Replay attack

- Resists against proven by temporal variance evaluations

Classical impersonation attack

- Resists against proven by ultra low false match rates and distinctiveness evaluations
Related Work - Physiological Parameter Generation

- Poon et al.\(^1\) ⇒ IPI of PPG/ECG signals
  - Divide IPI into segments → map into binary words
- Bao et al.\(^2\) ⇒ IPI of PPG/ECG signals
  - Divide IPI into segments → accumulate → randomize → map into binary words

<table>
<thead>
<tr>
<th>Method</th>
<th>Key Length (bit)</th>
<th>HTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poon et al.</td>
<td>128</td>
<td>4.26</td>
</tr>
<tr>
<td>Poon et al.</td>
<td>64</td>
<td>6.98</td>
</tr>
<tr>
<td>Bao et al.</td>
<td>64</td>
<td>2.83</td>
</tr>
<tr>
<td>Our Methods (max. CPSD-based)</td>
<td>128</td>
<td>0.135</td>
</tr>
</tbody>
</table>

---


Related Work - Key Agreement Protocol

- **Fuzzy Vault**\(^3\),\(^4\),\(^5\) \(\Rightarrow\) Frequency feat. of PPG/ECG signals
  - \(S_S \cap S'_C < v < S_S \cap S_C\)
  - Computational complexity: \(\left(\binom{|S_C|}{v+1}\right)\)
  - Vault security: \(\left(\binom{|R|}{v+1}\right)\)

- **Set Reconciliation**\(^6\) \(\Rightarrow\) IPI of ECG signals
  - \(t \leq S_S \cap S_C \& 2(m - t) < m\)
  - Computational complexity: \(\binom{m}{t}\)
  - Attack complexity: \(\binom{m+s}{t+s}\)

---


Related Work - Key Agreement Protocol

- **Fuzzy Vault** ⇒ Frequency feat. of PPG/ECG signals
  - \( S_S \cap S'_C < v < S_S \cap S_C \Rightarrow 13 < v < 31 \)
  - Attack complexity: \( \binom{|R|}{v+1} \)
- **Set Reconciliation** ⇒ IPI of ECG signals
  - \( t \leq S_S \cap S_C \& 2(m - t) < m \Rightarrow 16 < t \leq 17 \)
  - Attack complexity: \( \binom{m+s}{t+s} \)

<table>
<thead>
<tr>
<th>Method</th>
<th>Key Length (bit)</th>
<th>HTER (%)</th>
<th>Attack Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuzzy Vault</td>
<td>124</td>
<td>9.65</td>
<td>( 2^{147} )</td>
</tr>
<tr>
<td>Set Reconciliation</td>
<td>128</td>
<td>28.33</td>
<td>( 2^{47} )</td>
</tr>
<tr>
<td>SKA-PS</td>
<td>131</td>
<td>2.53</td>
<td>( 2^{176} )</td>
</tr>
</tbody>
</table>