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

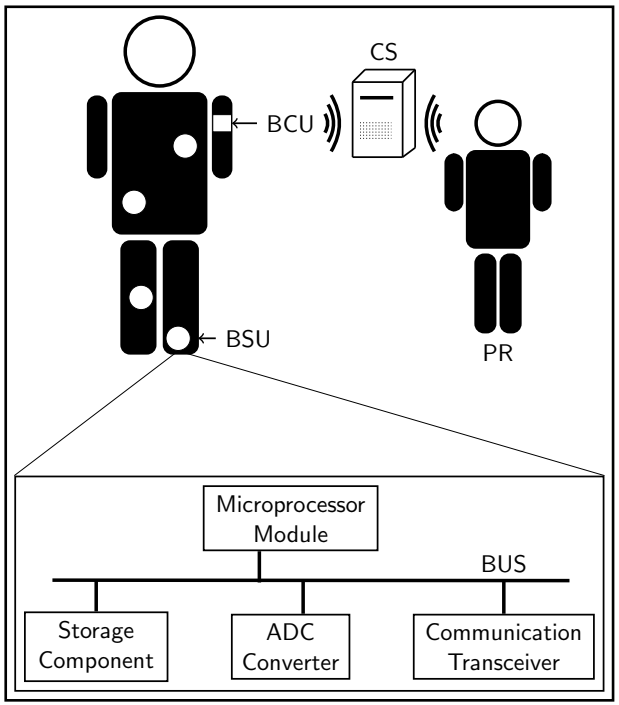
5 November 2020

Outline

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

- 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 reuse → 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 prone to 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 $\rightarrow$ 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 $\rightarrow$ 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

- 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

- 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

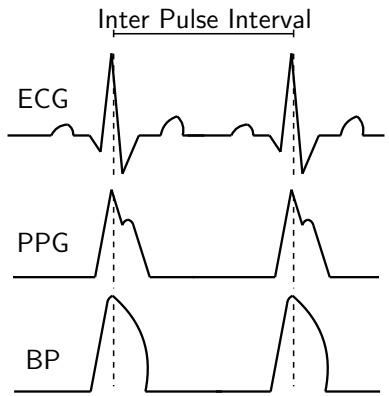
Deriving Cryptographic Keys from Physiological Signals

- 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, useeavaryng, random
- Appropriate physiological parameters
  - Inter-pulse interval (IPI)
  - Cross-power spectral density (CPSD)
  - Feature-level IPI-CPSD fused

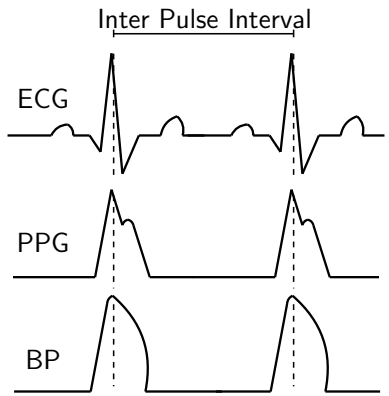
- Remote health monitoring systems
  - ECG, BP, oxygen saturation (via PPG) and BT
  - Different device specifically designed for recording
  - Specific place on the human body to be attached
- Choice considerations
  - Ability of biosensors on retrieving relevant data
  - Requirements of being used 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



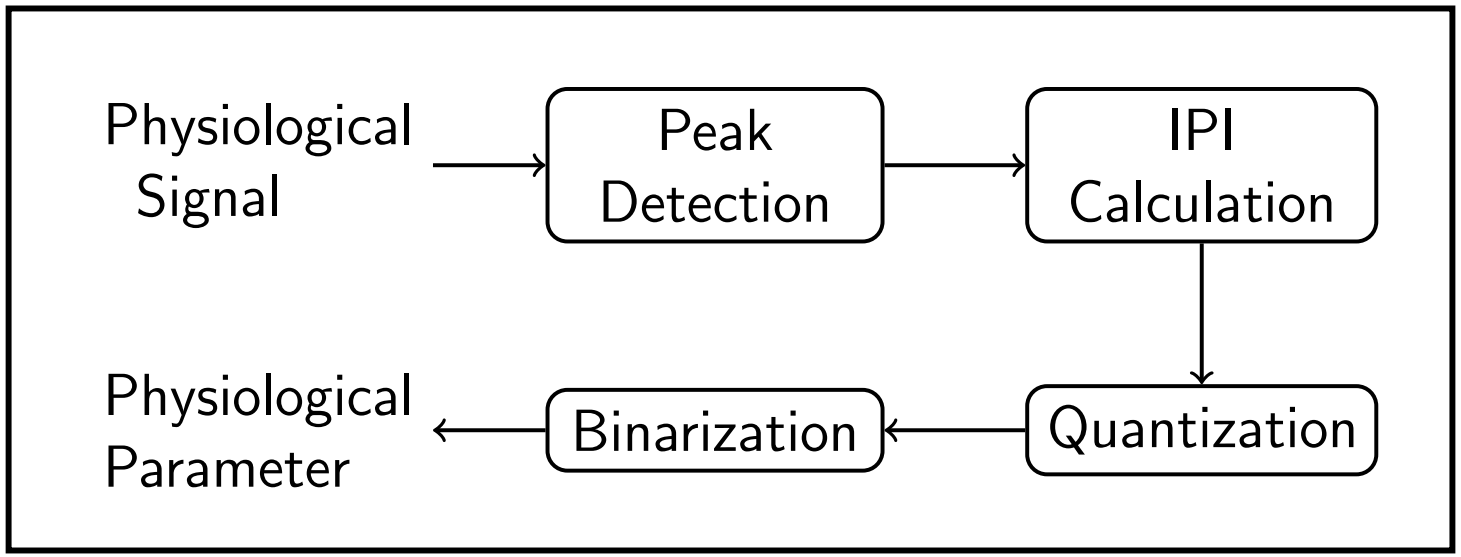
- Remote health monitoring systems
  - ECG, BP, oxygen saturation (via PPG) and BT
  - Different device specifically designed for recording
  - Specific place on the human body to be attached
- Choice considerations
  - Ability of biosensors on retrieving relevant data
  - Requirements of being used 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

– D. Karaolan Altop, A. Levi and V. Tuzcu, "Deriving Cryptographic Keys from Physiological Signals", *Pervasive and Mobile Computing*, vol. 39, pp. 65-79, Elsevier, DOI: 10.1016/j.pmcj.2016.08.004, August 2017.
– D. Karaolan Altop, A. Levi and V. Tuzcu, "Feature-level fusion of physiological parameters to be used as cryptographic keys", *IEEE International Conference on Communications (ICC 2017)*, pp. 1 - 6, Paris, France, May 2017.

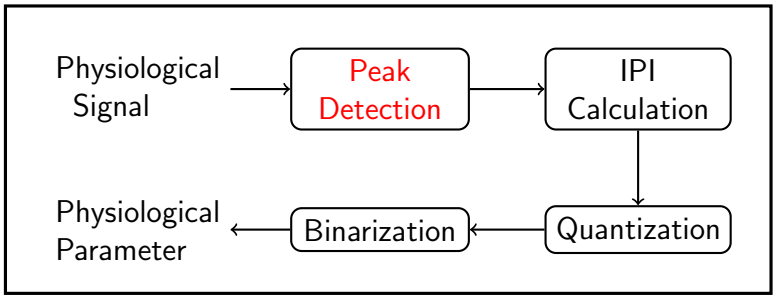
Time-Domain Physiological Parameter Generation

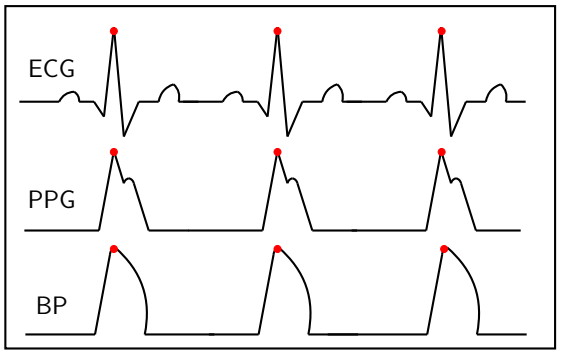


Time-Domain Physiological Parameter Generation

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

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





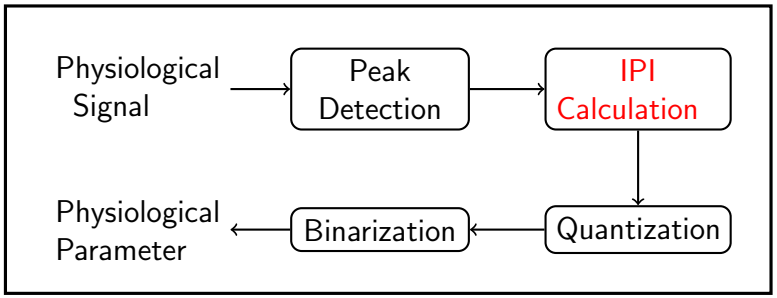
▸ Example

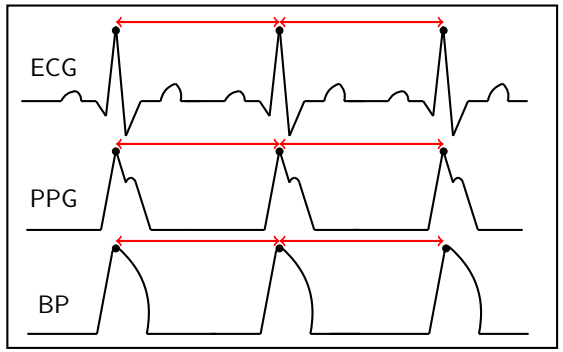
Time-Domain Physiological Parameter Generation

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

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

Example





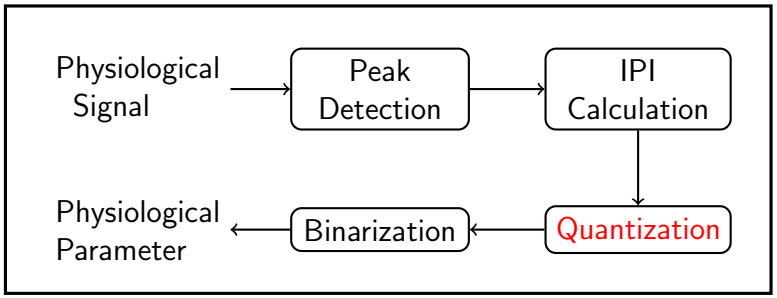
i.e.: $IPI^{init} = \{6, 8, 6, 3, 8, 9\}$ & $g = 2$

$IPI = \{14, 9, 17\}$

Time-Domain Physiological Parameter Generation

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

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



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

$min = 1$ & $max = 20$ & $s = 5$

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

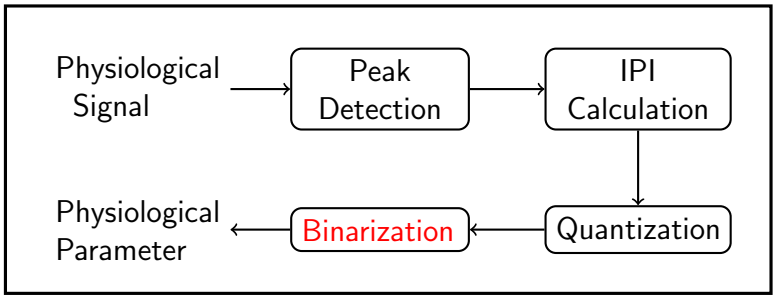
Codes: $\{0, 1, 2, 3\}$

Quantized IPI sequence: $\{2, 1, 3\}$

Time-Domain Physiological Parameter Generation

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

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

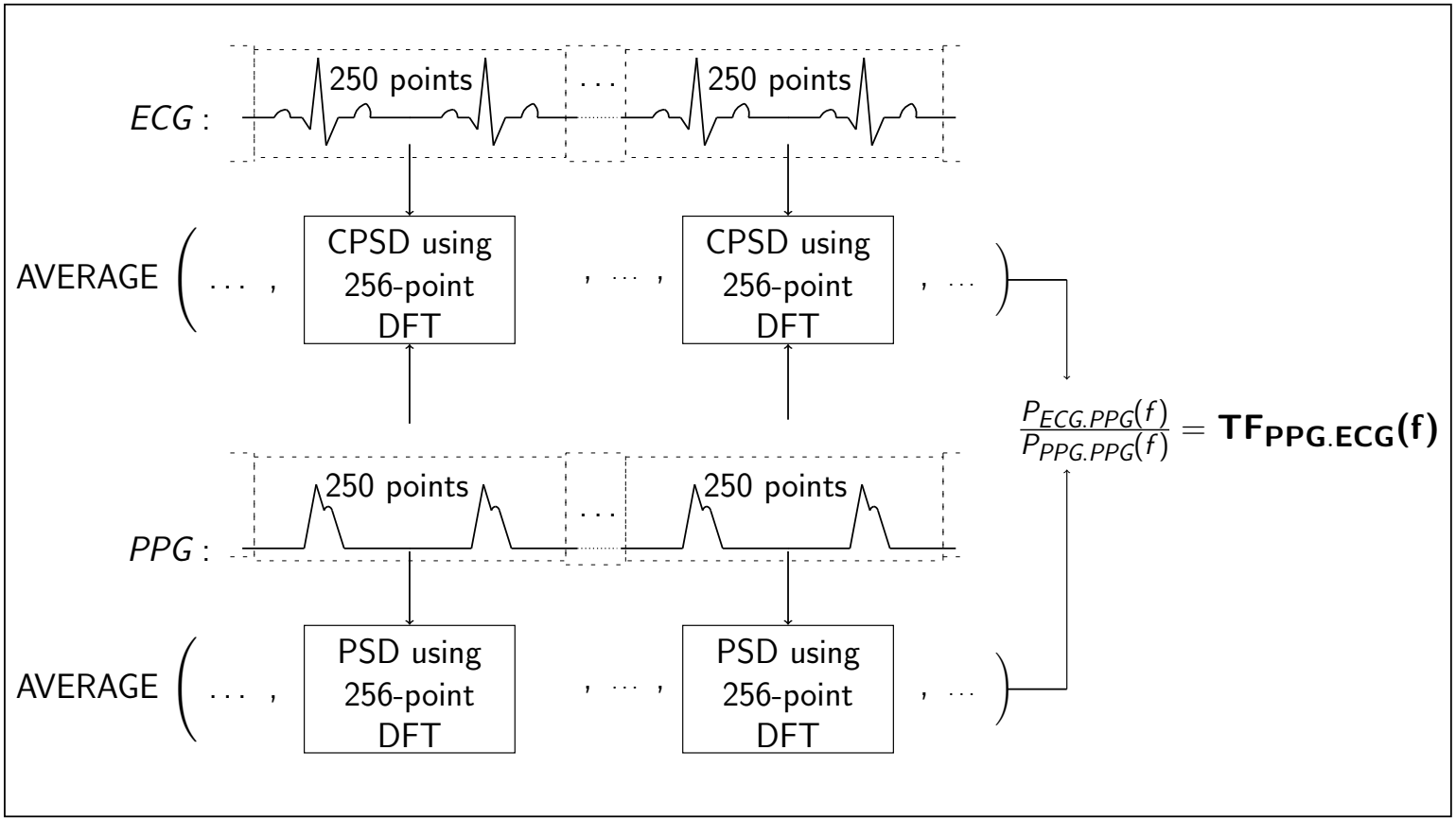


i.e.: Quantized IPI sequence: $\{2, 1, 3\}$

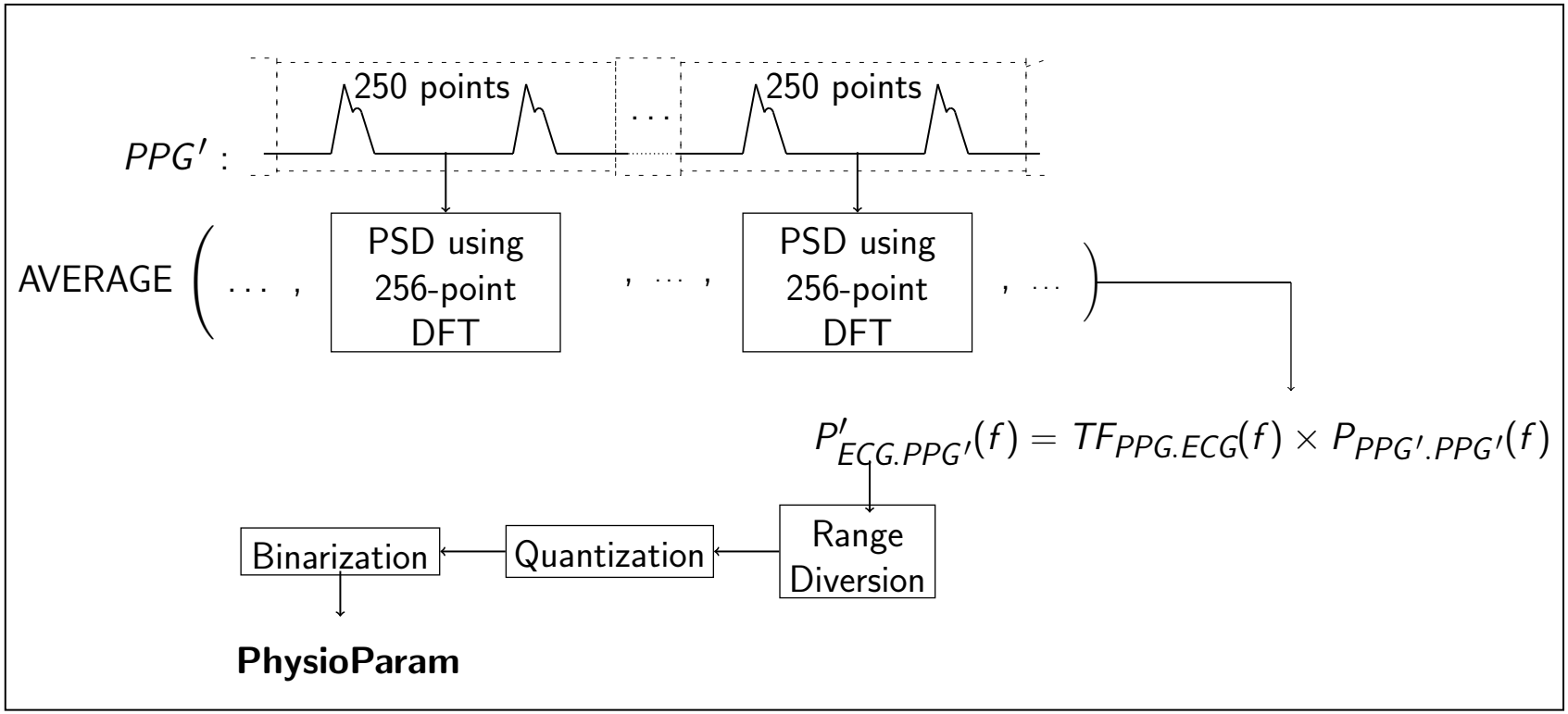
$$\{0, 1, 2, 3\} \mapsto \{00, 01, 11, 10\}$$

Encoded physiological parameter: $\{11, 01, 10\}$

Frequency-Domain Physiological Parameter Generation - Initialization Phase

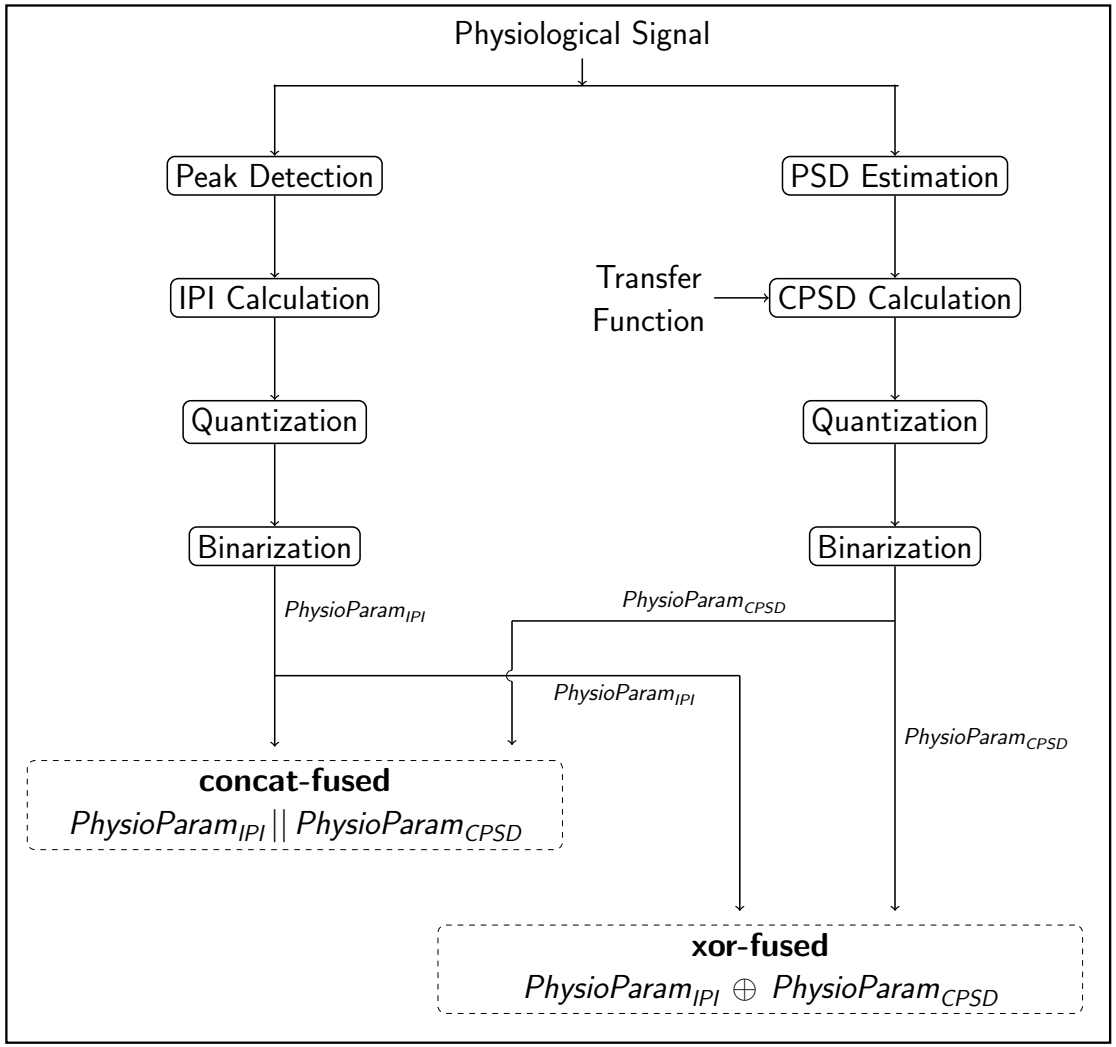


Frequency-Domain Physiological Parameter Generation - Operational Phase



▸ Example

Fused Physiological Parameter Generation



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
  - Now made public: `http://people.sabanciuniv.edu/levi/projects/114E557/`

▸ Details

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
  - Now made public: `http://people.sabanciuniv.edu/levi/projects/114E557/`

▸ Details

Performance Metrics

- Randomness
- Distinctiveness
- Error rates
- Temporal variance

Randomness - Shannon Entropy

Closer to 1 → Higher Entropy → Higher Randomness

l, g \ s	2	3	4	5	6	7	8	9	10	11	12	13
	PhysioBank-MIMIC-DB											
	IPI				**CPSD**							
32, 1	0.93	0.84	0.88	0.86								
64, 1	0.90	0.80	0.82	0.76								
128, 1	0.91	0.80	0.73	0.66	0.98	0.97	0.95	0.96				
64, 2	0.94	0.93	0.90	0.87								
128, 2	0.97	0.93	0.92	0.85	0.99	0.99	0.98	0.99				
128, 4	0.96	0.93	0.92	0.92	0.99	0.99	0.99	0.99				
	SU-PhysioDB											
	IPI						**CPSD**					
32, 1	0.97	0.98	0.97	0.94	0.93	0.90						
64, 1	0.96	0.92	0.87	0.83	0.83	0.84						
128, 1	0.98	0.95	0.91	0.87	0.79	0.75	0.99	0.99	0.99	0.99	0.98	0.97
64, 2	0.97	0.96	0.98	0.98	0.98	0.97						
128, 2	0.99	0.98	0.97	0.94	0.93	0.90	0.99	0.99	0.99	0.99	0.98	0.98
128, 4	0.99	0.98	0.96	0.96	0.97	0.98	0.99	0.99	0.99	0.98	0.98	0.99

	PhysioBank-MIMIC-DB			
	g_{CPSD}, s_{CPSD} \ s_{IPI}	**3**	**4**	**5**
concat-fused	**1, 9**	0.97	0.97	0.97
	4, 8	0.98	0.98	0.98
	4, 9	0.98	0.98	0.98
xor-fused	**1, 9**	0.99	0.99	0.99
	4, 8	0.99	0.99	0.99
	4, 9	0.99	0.99	0.99

	SU-PhysioDB			
	s_{CPSD} \ $l_{IPI}, g_{IPI}, s_{IPI}$	**64, 2, 3**	**128, 2, 5**	**128, 4, 4**
concat-fused	**9**	0.99	0.98	0.99
	11	0.99	0.98	0.99
	12	0.98	0.98	0.98
xor-fused	**9**	0.99	0.99	0.99
	11	0.99	0.99	0.99
	12	0.99	0.99	0.99

▸ Example

Randomness - Shannon Entropy

Closer to 1 → Higher Entropy → Higher Randomness

l, g \ s	2	3	4	5	6	7	8	9	10	11	12	13
	PhysioBank-MIMIC-DB											
	IPI				**CPSD**							
32, 1	0.93	0.84	0.88	0.86								
64, 1	0.90	0.80	0.82	0.76								
128, 1	0.91	0.80	0.73	0.66	0.98	0.97	0.95	0.96				
64, 2	0.94	0.93	0.90	0.87								
128, 2	0.97	0.93	0.92	0.85	0.99	0.99	0.98	0.99				
128, 4	0.96	0.93	0.92	0.92	0.99	0.99	0.99	0.99				
	SU-PhysioDB											
	IPI						**CPSD**					
32, 1	0.97	0.98	0.97	0.94	0.93	0.90						
64, 1	0.96	0.92	0.87	0.83	0.83	0.84						
128, 1	0.98	0.95	0.91	0.87	0.79	0.75	0.99	0.99	0.99	0.99	0.98	0.97
64, 2	0.97	0.96	0.98	0.98	0.98	0.97						
128, 2	0.99	0.98	0.97	0.94	0.93	0.90	0.99	0.99	0.99	0.99	0.98	0.98
128, 4	0.99	0.98	0.96	0.96	0.97	0.98	0.99	0.99	0.99	0.98	0.98	0.99

	PhysioBank-MIMIC-DB			
	g_{CPSD}, s_{CPSD} \ s_{IPI}	**3**	**4**	**5**
concat-fused	**1, 9**	0.97	0.97	0.97
	4, 8	0.98	0.98	0.98
	4, 9	0.98	0.98	0.98
xor-fused	**1, 9**	0.99	0.99	0.99
	4, 8	0.99	0.99	0.99
	4, 9	0.99	0.99	0.99

	SU-PhysioDB			
	s_{CPSD} \ $l_{IPI}, g_{IPI}, s_{IPI}$	**64, 2, 3**	**128, 2, 5**	**128, 4, 4**
concat-fused	**9**	0.99	0.98	0.99
	11	0.99	0.98	0.99
	12	0.98	0.98	0.98
xor-fused	**9**	0.99	0.99	0.99
	11	0.99	0.99	0.99
	12	0.99	0.99	0.99

▸ Example

Randomness - Shannon Entropy

Closer to 1 → Higher Entropy → Higher Randomness

l, g \ s	2	3	4	5	6	7	8	9	10	11	12	13
	PhysioBank-MIMIC-DB											
	IPI				**CPSD**							
32, 1	0.93	0.84	0.88	0.86								
64, 1	0.90	0.80	0.82	0.76								
128, 1	0.91	0.80	0.73	0.66	0.98	0.97	0.95	0.96				
64, 2	0.94	0.93	0.90	0.87								
128, 2	0.97	0.93	0.92	0.85	0.99	0.99	0.98	0.99				
128, 4	0.96	0.93	0.92	0.92	0.99	0.99	0.99	0.99				
	SU-PhysioDB											
	IPI						**CPSD**					
32, 1	0.97	0.98	0.97	0.94	0.93	0.90						
64, 1	0.96	0.92	0.87	0.83	0.83	0.84						
128, 1	0.98	0.95	0.91	0.87	0.79	0.75	0.99	0.99	0.99	0.99	0.98	0.97
64, 2	0.97	0.96	0.98	0.98	0.98	0.97						
128, 2	0.99	0.98	0.97	0.94	0.93	0.90	0.99	0.99	0.99	0.99	0.98	0.98
128, 4	0.99	0.98	0.96	0.96	0.97	0.98	0.99	0.99	0.99	0.98	0.98	0.99

	PhysioBank-MIMIC-DB			
	g_{CPSD}, s_{CPSD} \ s_{IPI}	**3**	**4**	**5**
concat-fused	**1, 9**	0.97	0.97	0.97
	4, 8	0.98	0.98	0.98
	4, 9	0.98	0.98	0.98
xor-fused	**1, 9**	0.99	0.99	0.99
	4, 8	0.99	0.99	0.99
	4, 9	0.99	0.99	0.99
	SU-PhysioDB			
	s_{CPSD} \ $l_{IPI}, g_{IPI}, s_{IPI}$	**64, 2, 3**	**128, 2, 5**	**128, 4, 4**
concat-fused	**9**	0.99	0.98	0.99
	11	0.99	0.98	0.99
	12	0.98	0.98	0.98
xor-fused	**9**	0.99	0.99	0.99
	11	0.99	0.99	0.99
	12	0.99	0.99	0.99

▸ Example

Randomness - Shannon Entropy

Closer to 1 → Higher Entropy → Higher Randomness

l, g \ s	2	3	4	5	6	7	8	9	10	11	12	13
	PhysioBank-MIMIC-DB											
	IPI				**CPSD**							
32, 1	0.93	0.84	0.88	0.86								
64, 1	0.90	0.80	0.82	0.76								
128, 1	0.91	0.80	0.73	0.66	0.98	0.97	0.95	0.96				
64, 2	0.94	0.93	0.90	0.87								
128, 2	0.97	0.93	0.92	0.85	0.99	0.99	0.98	0.99				
128, 4	0.96	0.93	0.92	0.92	0.99	0.99	0.99	0.99				
	SU-PhysioDB											
	IPI						**CPSD**					
32, 1	0.97	0.98	0.97	0.94	0.93	0.90						
64, 1	0.96	0.92	0.87	0.83	0.83	0.84						
128, 1	0.98	0.95	0.91	0.87	0.79	0.75	0.99	0.99	0.99	0.99	0.98	0.97
64, 2	0.97	0.96	0.98	0.98	0.98	0.97						
128, 2	0.99	0.98	0.97	0.94	0.93	0.90	0.99	0.99	0.99	0.99	0.98	0.98
128, 4	0.99	0.98	0.96	0.96	0.97	0.98	0.99	0.99	0.99	0.98	0.98	0.99

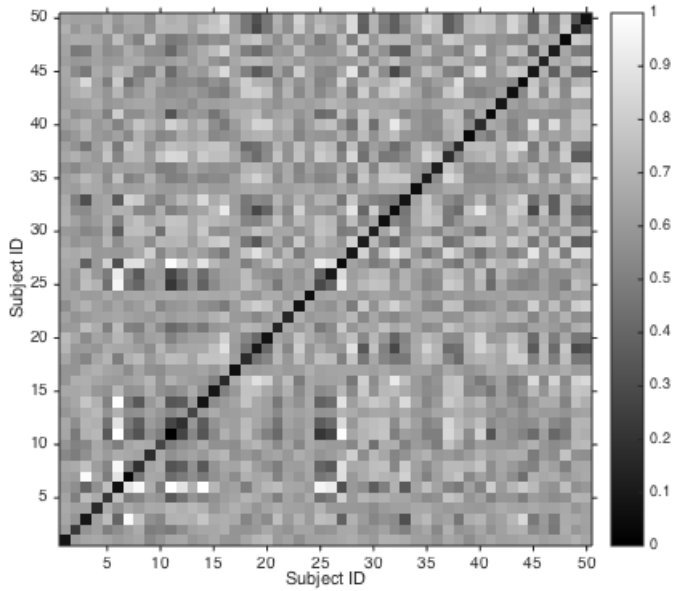
	PhysioBank-MIMIC-DB			
	g_{CPSD}, s_{CPSD} \ s_{IPI}	**3**	**4**	**5**
concat-fused	**1, 9**	0.97	0.97	0.97
	4, 8	0.98	0.98	0.98
	4, 9	0.98	0.98	0.98
xor-fused	**1, 9**	0.99	0.99	0.99
	4, 8	0.99	0.99	0.99
	4, 9	0.99	0.99	0.99
	SU-PhysioDB			
	s_{CPSD} \ $l_{IPI}, g_{IPI}, s_{IPI}$	**64, 2, 3**	**128, 2, 5**	**128, 4, 4**
concat-fused	**9**	0.99	0.98	0.99
	11	0.99	0.98	0.99
	12	0.98	0.98	0.98
xor-fused	**9**	0.99	0.99	0.99
	11	0.99	0.99	0.99
	12	0.99	0.99	0.99

▸ Example

Distinctiveness - Hamming Distance

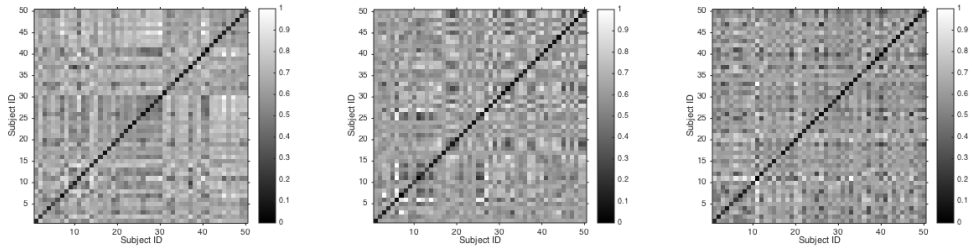
$D_s \Rightarrow$ average Hamming distance among the physiological parameters that are generated from the same host

$D_d \Rightarrow$ average Hamming distance among the physiological parameters that are generated from the different hosts



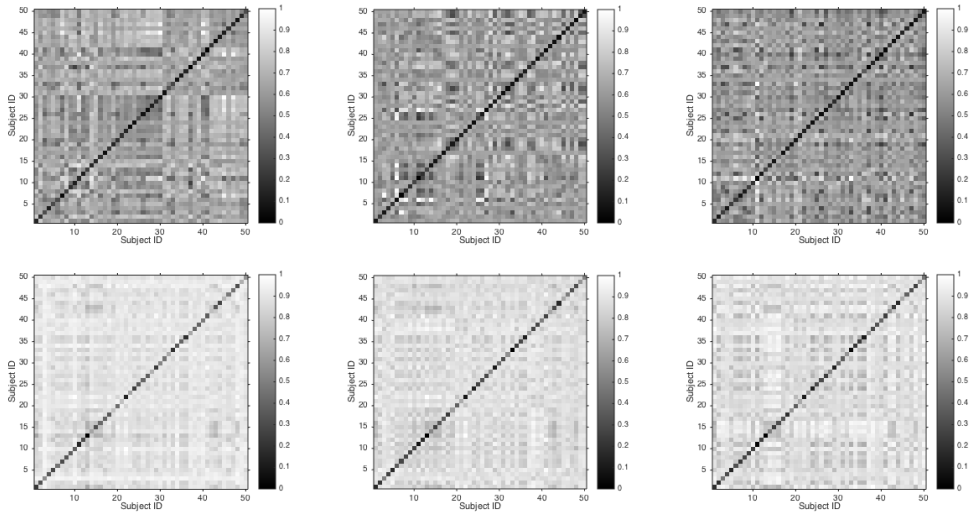
Distinctiveness - Hamming Distance

- IPI-based



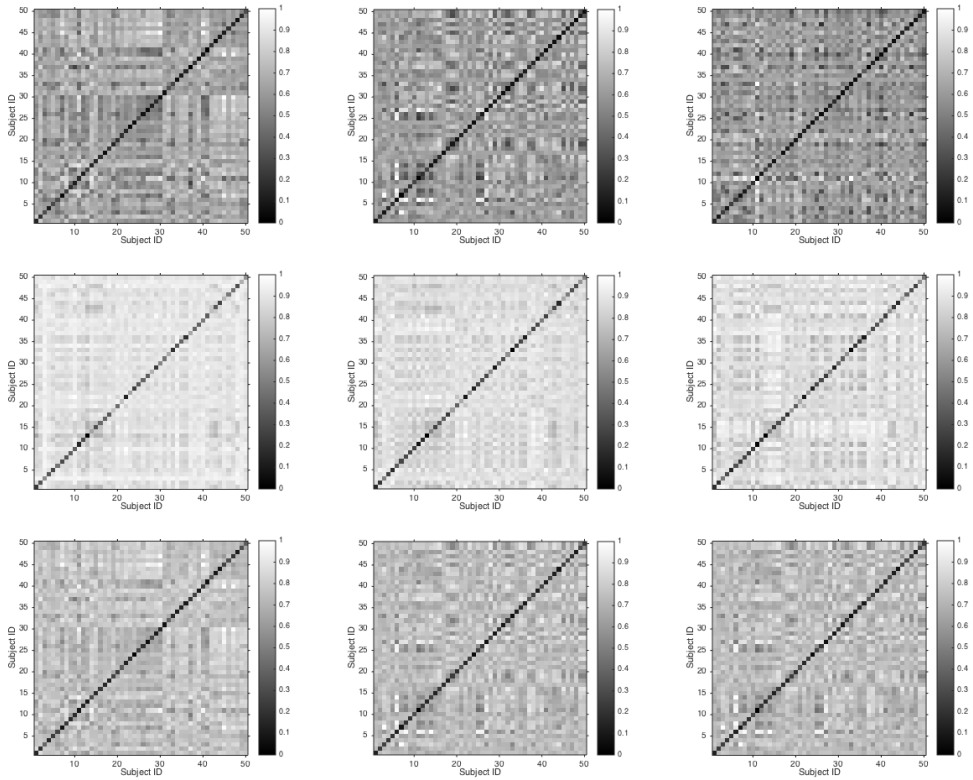
Distinctiveness - Hamming Distance

- IPI-based
- CPSD-based



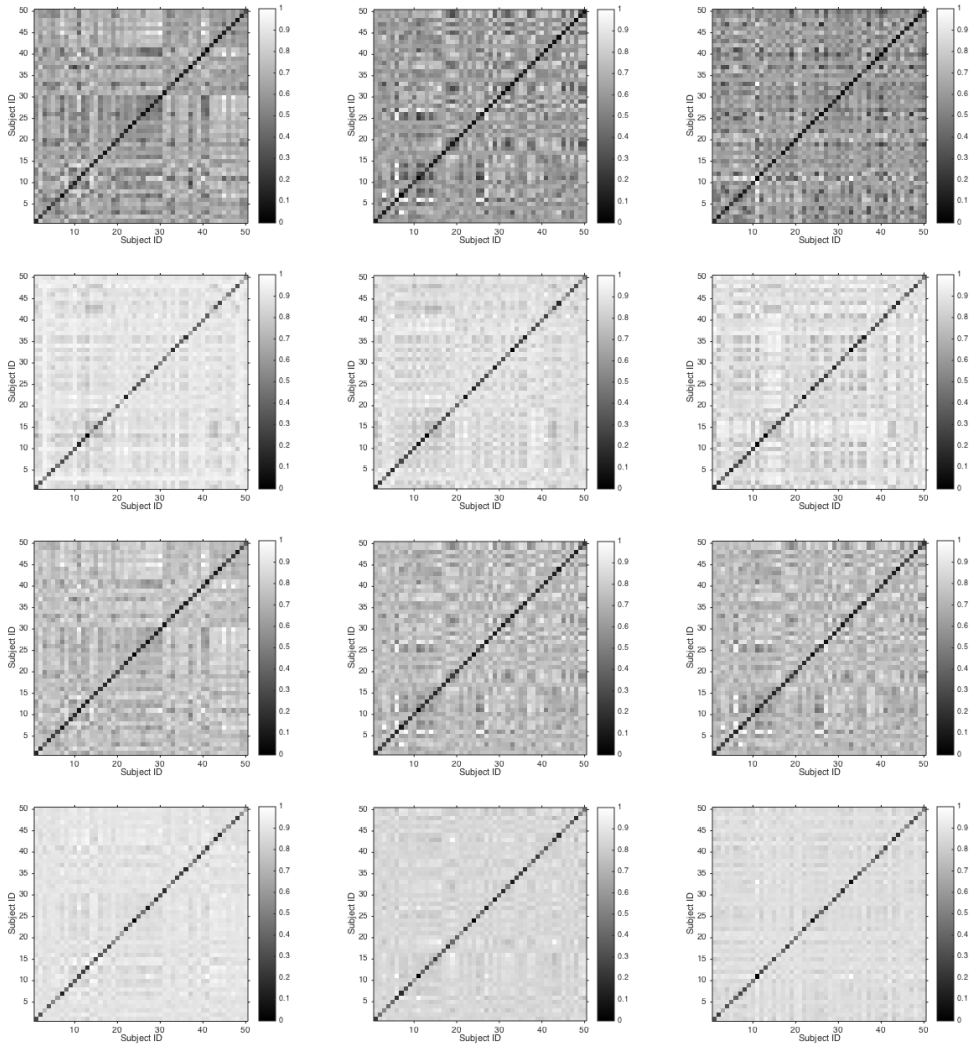
Distinctiveness - Hamming Distance

- IPI-based
- CPSD-based
- concat-fused



Distinctiveness - Hamming Distance

- IPI-based
- CPSD-based
- concat-fused
- xor-fused



Error Rates - EER (Equal Error Rate)

Dataset	Method	EER(%)
PhysioBank-MIMIC-DB	Time-domain	4.2
	Frequency-domain	15.3
	concat-fused	3.6
	xor-fused	12.0
SU-PhysioDB	Time-domain	4.1
	Frequency-domain	13.4
	concat-fused	2.0
	xor-fused	6.0

Temporal Variance - Temporal Ratio (R)

$R \geq 1$: Temporally Variant

$R < 1$: Temporally Invariant

l, g \ s	2	3	4	5	6	7	8	9	10	11	12	13
	PhysioBank-MIMIC-DB											
	IPI				CPSD							
32, 1	1.18	0.79	0.57	0.42								
64, 1	2.32	1.33	1.57	0.85								
128, 1	3.76	1.80	1.43	0.99	0.14	0.11	0.09	0.08				
64, 2	2.13	1.78	1.11	0.93								
128, 2	7.68	4.80	2.90	1.63	0.13	0.12	0.10	0.09				
128, 4	4.16	2.41	2.10	1.97	0.11	0.10	0.08	0.08				
	SU-PhysioDB											
	IPI						CPSD					
32, 1	2,07	1,69	1,61	1,73	1,39	1,18						
64, 1	3,22	2,46	1,94	1,35	1,24	1,35						
128, 1	3.14	3.11	2.68	2.40	1.67	1.36	0.24	0.21	0.21	0.18	0.18	0.19
64, 2	2,45	2,33	1,97	1,64	1,67	1,76						
128, 2	3,21	3,63	3,45	2,66	2,52	2,07	0.26	0.24	0.23	0.22	0.19	0.19
128, 4	3,16	2,70	2,31	2,32	2,08	1,91	0.24	0.24	0.23	0.23	0.22	0.23

	PhysioBank-MIMIC-DB			
	s_{IPI} / g_{CPSD}, s_{CPSD}	**3**	**4**	**5**
concat-fused	1, 9	0.58	0.59	0.54
	4, 8	0.69	0.69	0.64
	4, 9	0.64	0.64	0.59
xor-fused	1, 9	1.93	1.76	1.27
	4, 8	1.82	1.39	1.25
	4, 9	1.78	1.43	1.25
	SU-PhysioDB			
	$l_{IPI}, g_{IPI}, s_{IPI}$ / s_{CPSD}	**64, 2, 3**	**128, 2, 5**	**128, 4, 4**
concat-fused	**9**	0.69	0.75	0.69
	11	0.73	0.80	0.73
	12	0.73	0.80	0.74
xor-fused	**9**	1.05	1.37	1.24
	11	1.25	1.62	1.44
	12	1.38	1.72	1.53

Temporal Variance - Temporal Ratio (R)

$R \geq 1$: Temporally Variant

$R < 1$: Temporally Invariant

l, g \ s	2	3	4	5	6	7	8	9	10	11	12	13
	PhysioBank-MIMIC-DB											
	IPI				CPSD							
32, 1	1.18	0.79	0.57	0.42								
64, 1	2.32	1.33	1.57	0.85								
128, 1	3.76	1.80	1.43	0.99	0.14	0.11	0.09	0.08				
64, 2	2.13	1.78	1.11	0.93								
128, 2	7.68	4.80	2.90	1.63	0.13	0.12	0.10	0.09				
128, 4	4.16	2.41	2.10	1.97	0.11	0.10	0.08	0.08				
	SU-PhysioDB											
	IPI						CPSD					
32, 1	2,07	1,69	1,61	1,73	1,39	1,18						
64, 1	3,22	2,46	1,94	1,35	1,24	1,35						
128, 1	3.14	3.11	2.68	2.40	1.67	1.36	0.24	0.21	0.21	0.18	0.18	0.19
64, 2	2,45	2,33	1,97	1,64	1,67	1,76						
128, 2	3,21	3,63	3,45	2,66	2,52	2,07	0.26	0.24	0.23	0.22	0.19	0.19
128, 4	3,16	2,70	2,31	2,32	2,08	1,91	0.24	0.24	0.23	0.23	0.22	0.23

	PhysioBank-MIMIC-DB			
	s_{IPI} / g_{CPSD}, s_{CPSD}	**3**	**4**	**5**
concat-fused	1, 9	0.58	0.59	0.54
	4, 8	0.69	0.69	0.64
	4, 9	0.64	0.64	0.59
xor-fused	1, 9	1.93	1.76	1.27
	4, 8	1.82	1.39	1.25
	4, 9	1.78	1.43	1.25
	SU-PhysioDB			
	$l_{IPI}, g_{IPI}, s_{IPI}$ / s_{CPSD}	**64, 2, 3**	**128, 2, 5**	**128, 4, 4**
concat-fused	**9**	0.69	0.75	0.69
	11	0.73	0.80	0.73
	12	0.73	0.80	0.74
xor-fused	**9**	1.05	1.37	1.24
	11	1.25	1.62	1.44
	12	1.38	1.72	1.53

Temporal Variance - Temporal Ratio (R)

$R \geq 1$: Temporally Variant

$R < 1$: Temporally Invariant

l, g \ s	2	3	4	5	6	7	8	9	10	11	12	13
	PhysioBank-MIMIC-DB											
	IPI				CPSD							
32, 1	1.18	0.79	0.57	0.42								
64, 1	2.32	1.33	1.57	0.85								
128, 1	3.76	1.80	1.43	0.99	0.14	0.11	0.09	0.08				
64, 2	2.13	1.78	1.11	0.93								
128, 2	7.68	4.80	2.90	1.63	0.13	0.12	0.10	0.09				
128, 4	4.16	2.41	2.10	1.97	0.11	0.10	0.08	0.08				
	SU-PhysioDB											
	IPI						CPSD					
32, 1	2,07	1,69	1,61	1,73	1,39	1,18						
64, 1	3,22	2,46	1,94	1,35	1,24	1,35						
128, 1	3.14	3.11	2.68	2.40	1.67	1.36	0.24	0.21	0.21	0.18	0.18	0.19
64, 2	2,45	2,33	1,97	1,64	1,67	1,76						
128, 2	3,21	3,63	3,45	2,66	2,52	2,07	0.26	0.24	0.23	0.22	0.19	0.19
128, 4	3,16	2,70	2,31	2,32	2,08	1,91	0.24	0.24	0.23	0.23	0.22	0.23

	PhysioBank-MIMIC-DB			
	g_{CPSD}, s_{CPSD} \ s_{IPI}	**3**	**4**	**5**
concat-fused	1, 9	0.58	0.59	0.54
	4, 8	0.69	0.69	0.64
	4, 9	0.64	0.64	0.59
xor-fused	1, 9	1.93	1.76	1.27
	4, 8	1.82	1.39	1.25
	4, 9	1.78	1.43	1.25
	SU-PhysioDB			
	s_{CPSD} \ $l_{IPI}, g_{IPI}, s_{IPI}$	**64, 2, 3**	**128, 2, 5**	**128, 4, 4**
concat-fused	**9**	0.69	0.75	0.69
	11	0.73	0.80	0.73
	12	0.73	0.80	0.74
xor-fused	**9**	1.05	1.37	1.24
	11	1.25	1.62	1.44
	12	1.38	1.72	1.53

	Randomness	Distinctiveness	Temporal Variance	EER
singular IPI-based	✓	✓	✓	✓✓
singular CPSD-based	✓✓	✓✓✓	✗	✓
concat-fused	✓✓	✓✓	✗	✓✓
xor-fused	✓✓	✓✓✓	✓	✓

- 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 $\Rightarrow$ 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 $\Rightarrow$ 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

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 $\xrightarrow{reconcile}$ 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 $\xrightarrow{reconcile}$ 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 $\xrightarrow{reconcile}$ 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, 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

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

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

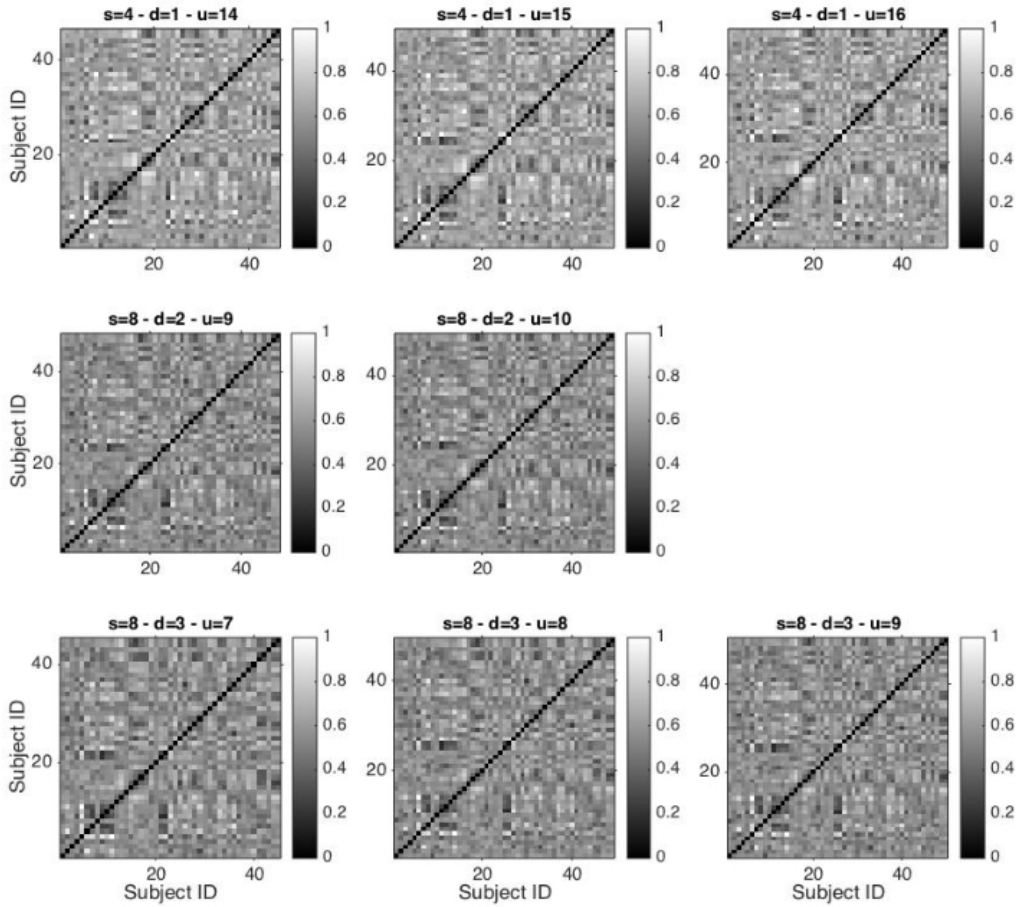
Parameters			True Match Rate (%)	False Match Rate (%)
s	d	n		
4	1	14	95	0
		15	99	0
		16	100	0.06
8	2	9	98	0.04
		10	99	0.04
	3	7	95	0.06
		8	99	0.22
		9	100	0.51

Randomness and Temporal Variance

Parameters			Randomness	Temporal Ratio
s	d	n		
4	1	14	0.9114	3.16
		15	0.9101	3.19
		16	0.9105	3.29
8	2	9	0.9092	2.48
		10	0.9099	2.50
	3	7	0.9091	2.37
		8	0.9100	2.64
		9	0.9109	2.69

▸ Example

Distinctiveness



Complexity: Average Number of Protocol Rounds

Parameters			Average Number of Protocol Rounds	
s	d	n	Source Biosensor	Conforming Biosensor
4	1	14	17.33	12.26
		15	71.78	50.13
		16	114.74	72.91
8	2	9	4.64	3.41
		10	5.81	4.09
	3	7	1	1
		8	1.28	1.14
		9	1.63	1.37

Complexity: Average Number of Protocol Rounds

Parameters			Average Number of Protocol Rounds	
s	d	n	Source Biosensor	Combining Biosensor
4	1	14	15.55	12.26
		15	71.78	50.13
		16	114.74	72.91
	2	9	4.64	3.41
		10	5.81	4.09
8	3	7	1	1
		8	1.28	1.14
		9	1.63	1.37

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

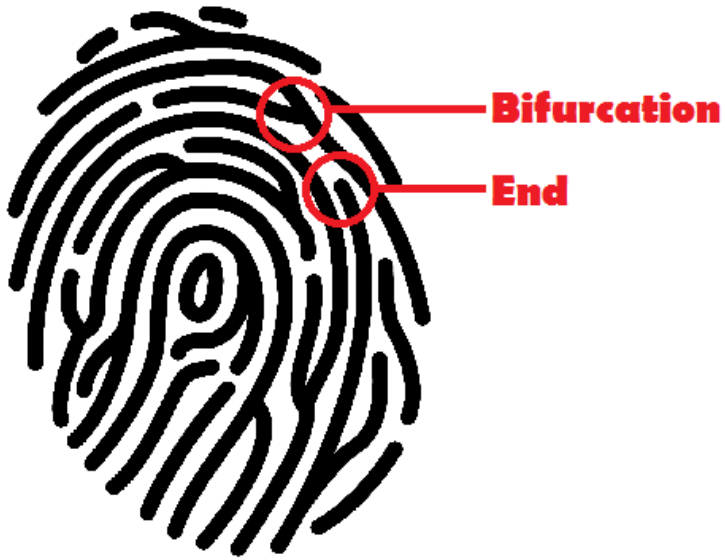
SKA-PB: Secure Key Agreement using Pure Biometrics

- 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: Users sharing 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

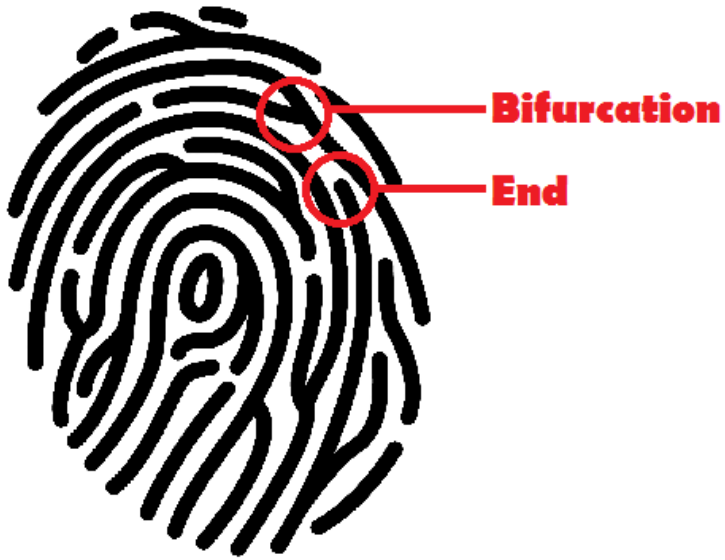
Enrollment Phase

- 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*



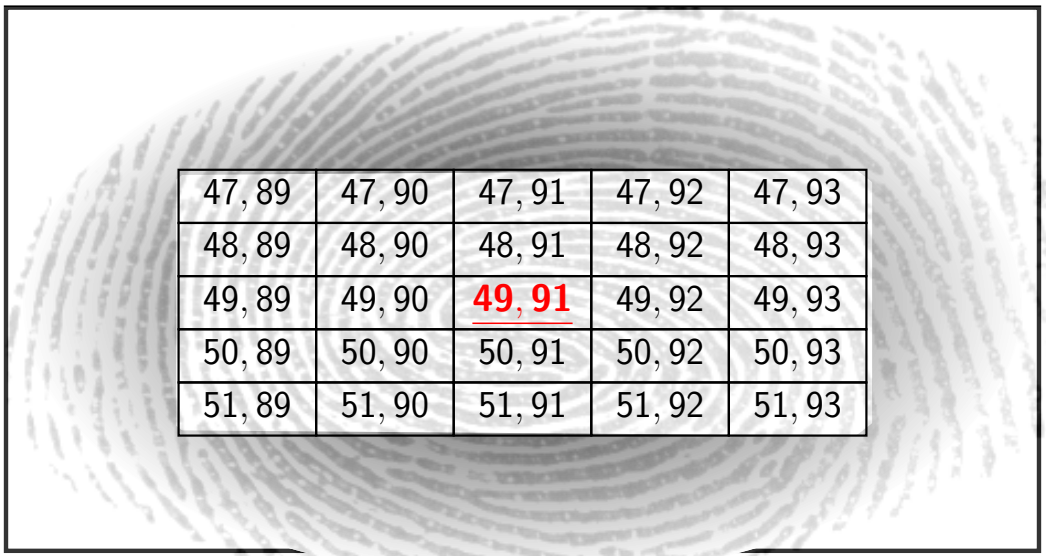
Enrollment Phase

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



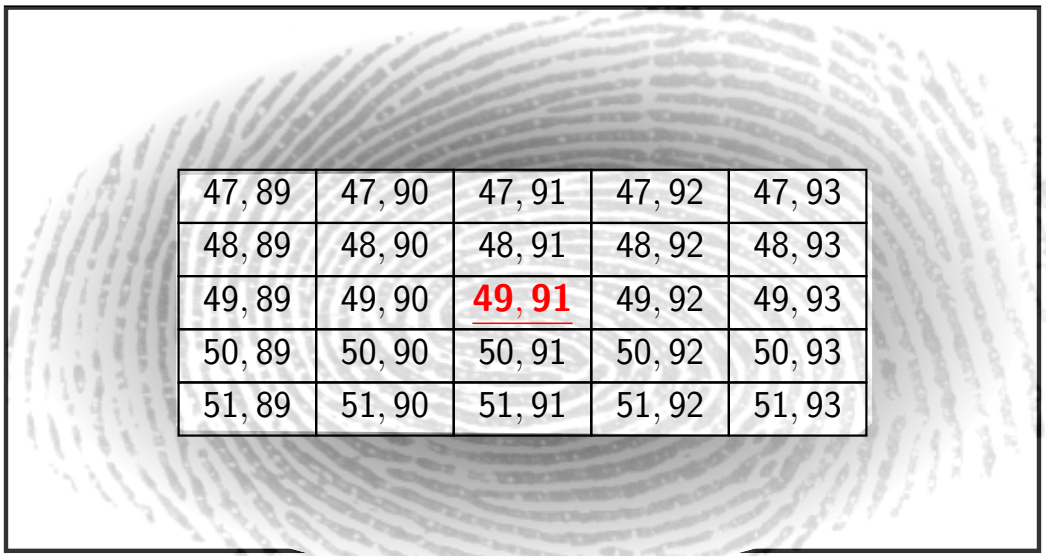
Enrollment Phase

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

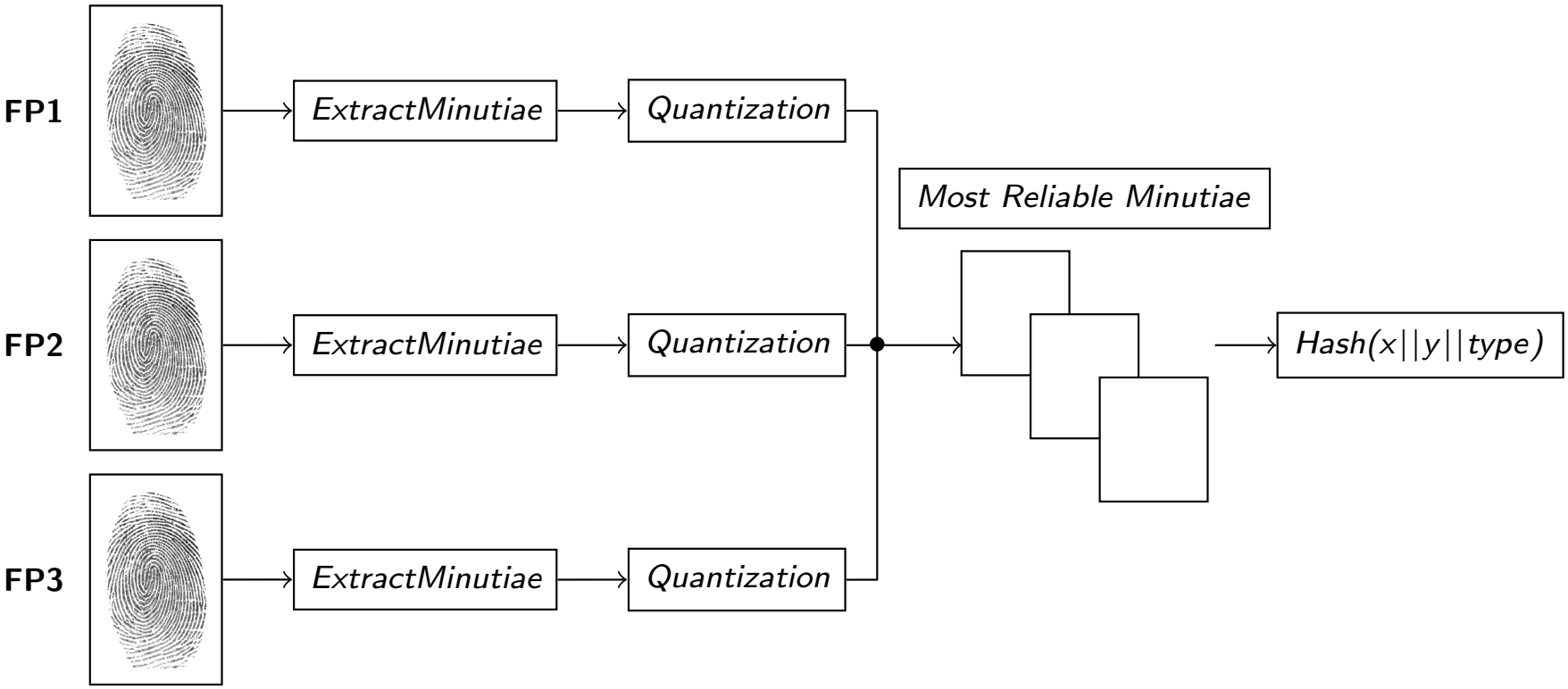


Enrollment Phase

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



Enrollment Phase



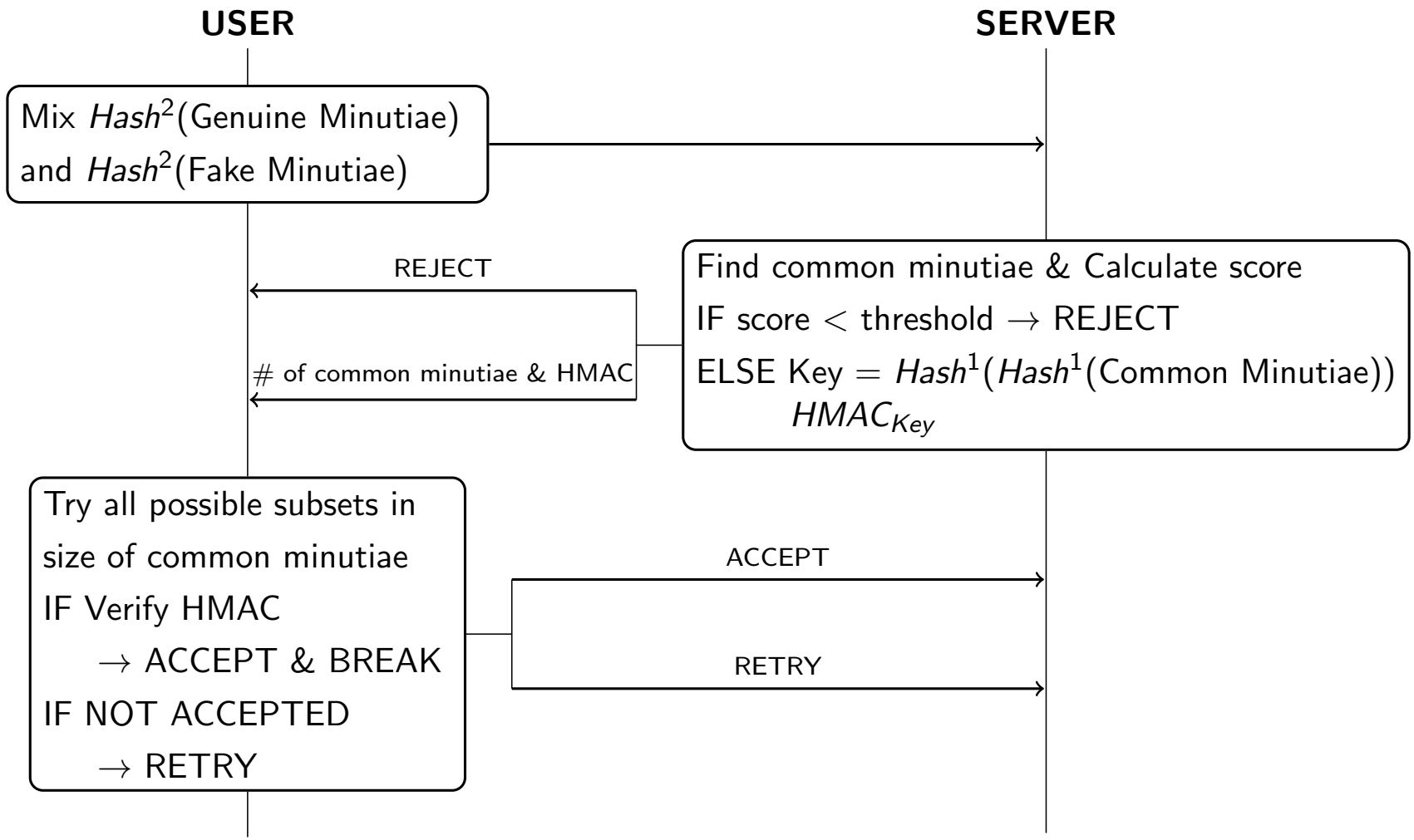
Verification Phase

- 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

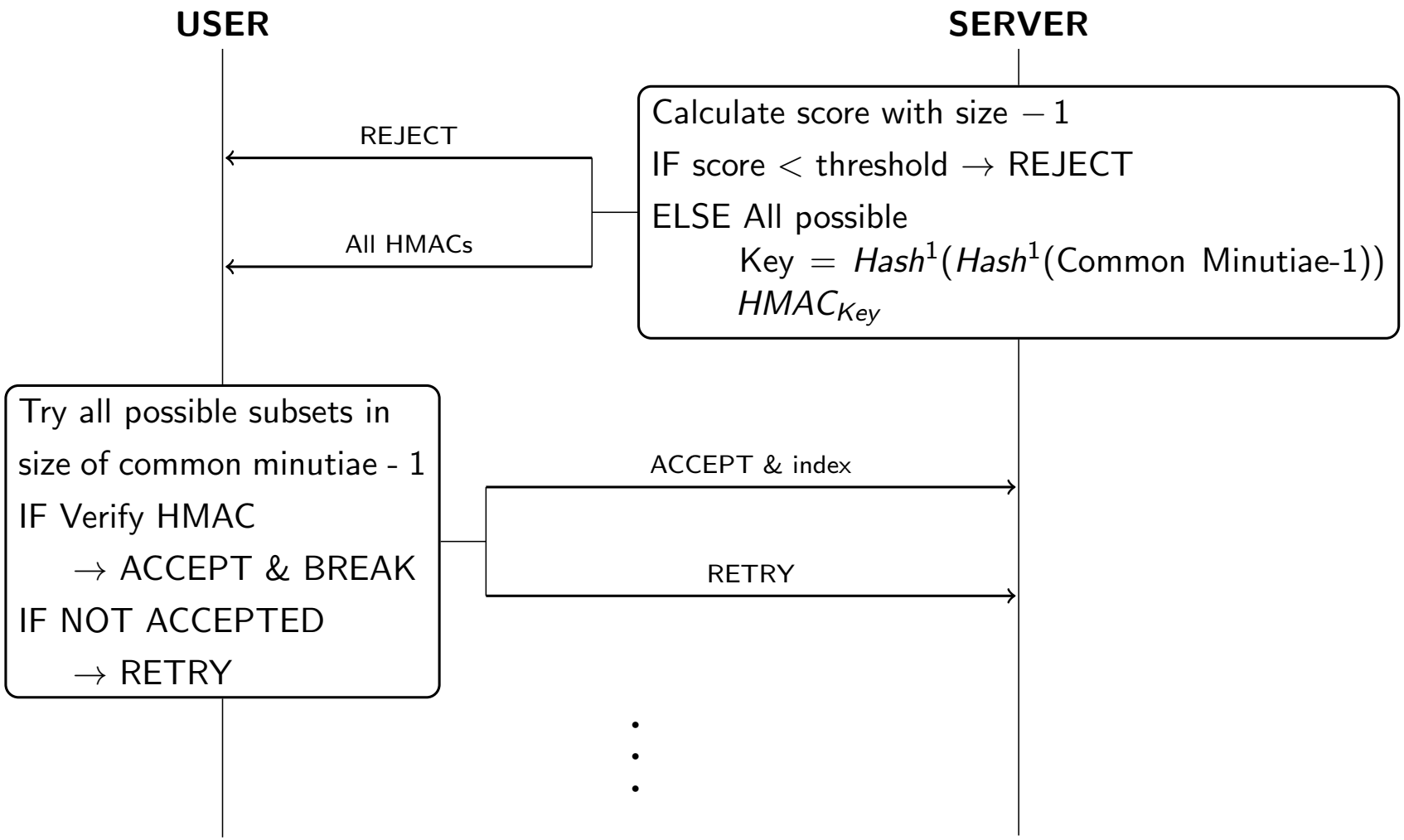
Verification Phase

- As in the enrollment phase, user side
  - Three fingerprint images of the same finger
  - Quantization according to the T_{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

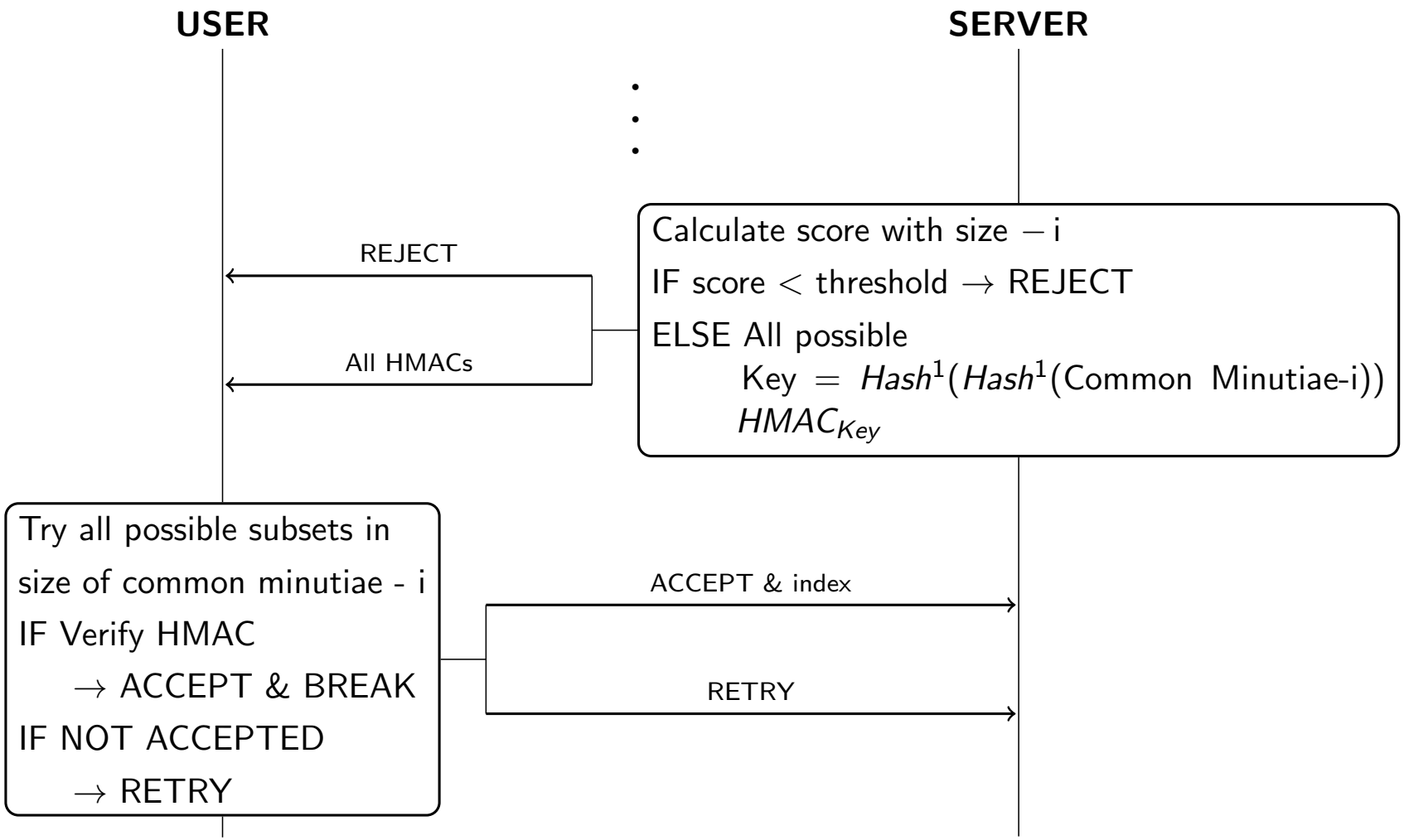
The Protocol



The Protocol



The Protocol

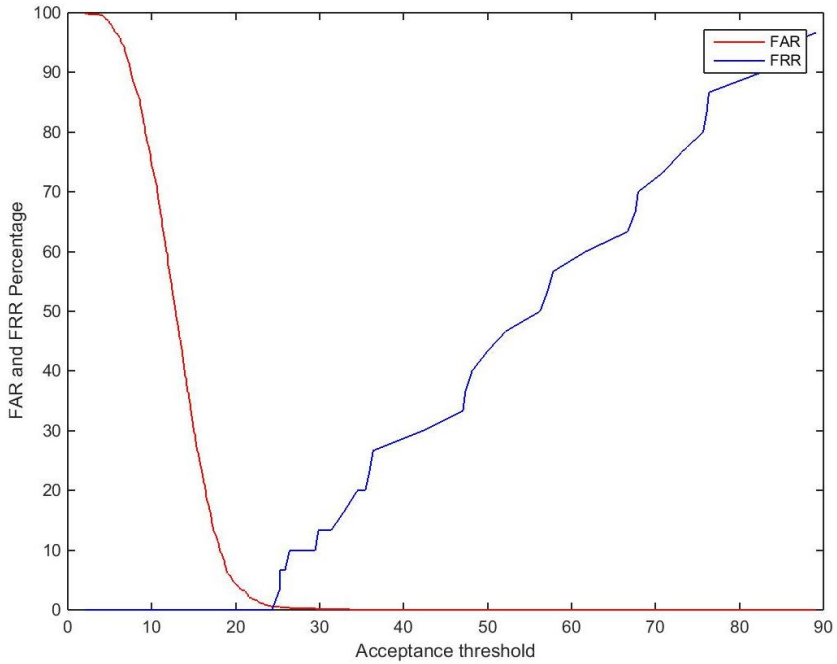


Settings

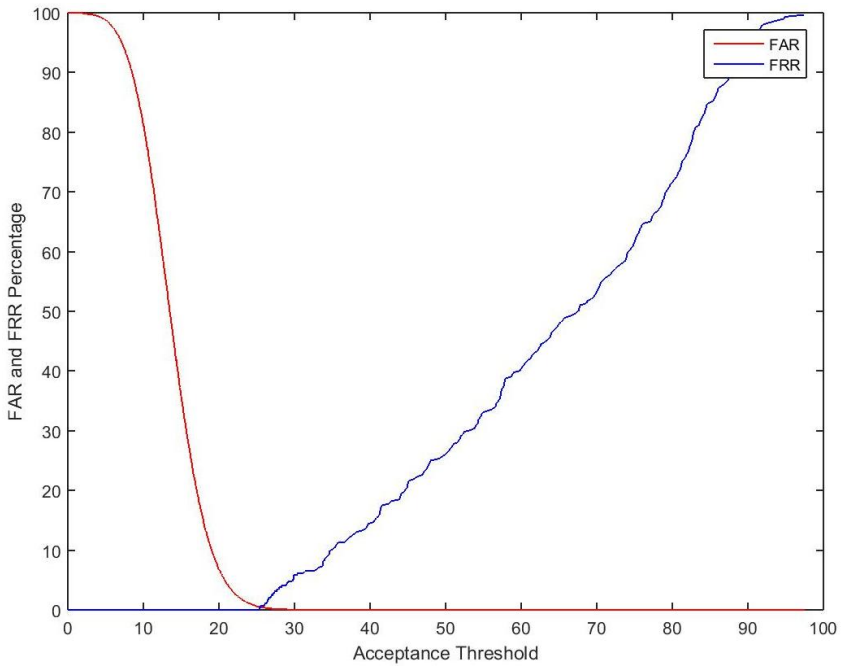
- 1^{st} Dataset: 30 fingerprints from Verifinger Sample Database*
  - 8 impressions: 3 for server, 5 for user
- 2^{nd} Dataset: 292 fingerprints from volunteers in Sabancı University
  - 10 impressions: 3 for server, 7 for user
- Alignment in MATLAB using intensity values
- Minutiae extraction using 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^{st} dataset



- 0.48 % EER with 2^{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^{st} dataset
      - $\approx 2^{98}$ hash and HMAC verifications
    - 2^{nd} dataset
      - $\approx 2^{110}$ 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

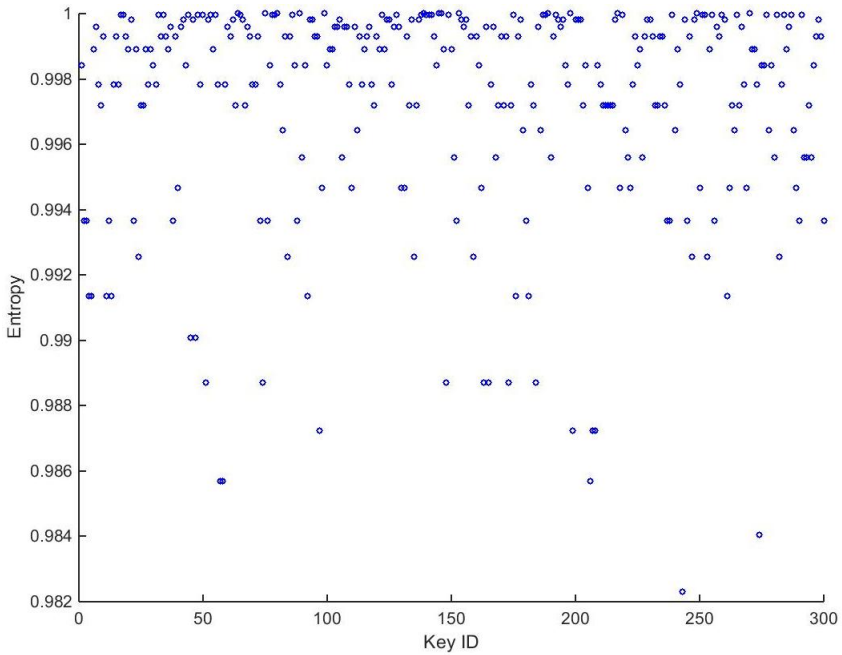
Brute-force Attack Analysis

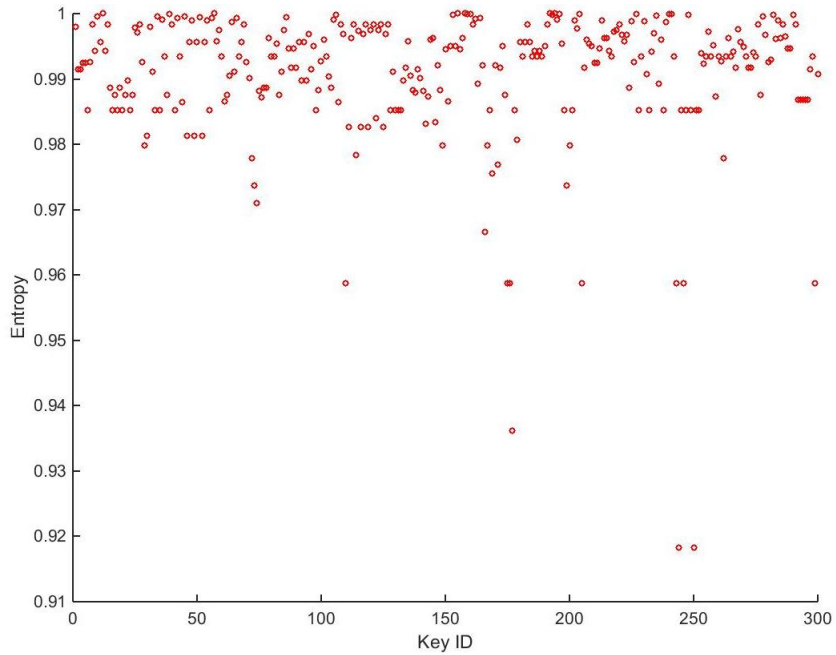
- Trying all possible keys $\Rightarrow 2^{256} \Rightarrow$ infeasible
- Intelligent brute-force attack
  - Generate all possible minutiae locations and types, and hashes
  - Does not search all possible minutiae combination $\Rightarrow$ Naive brute-force
  - Decrease search space to genuine and fake 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^{st} dataset

- All keys' entropy
  $Hash\,(x||y||type)$
- Minutiae' entropy
  $(x||y||type)$

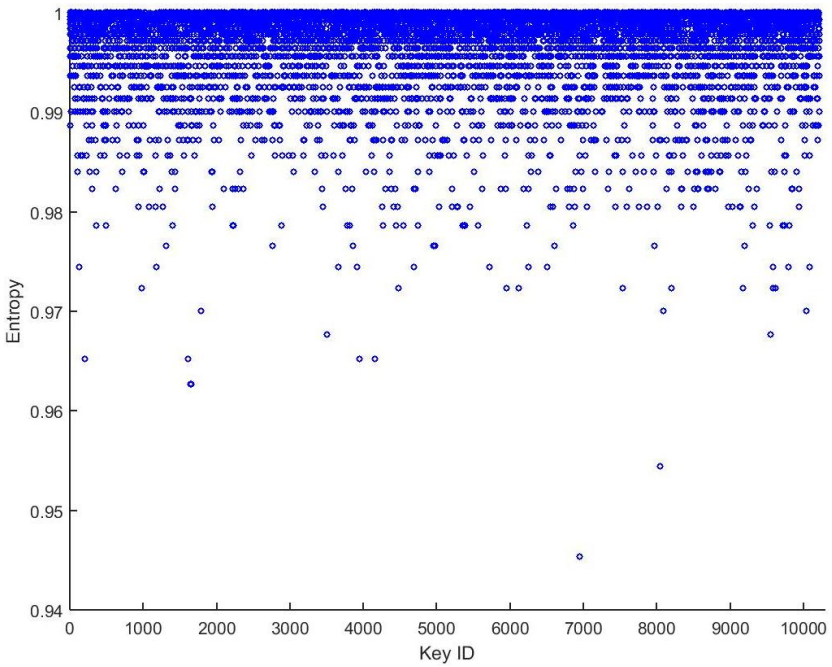


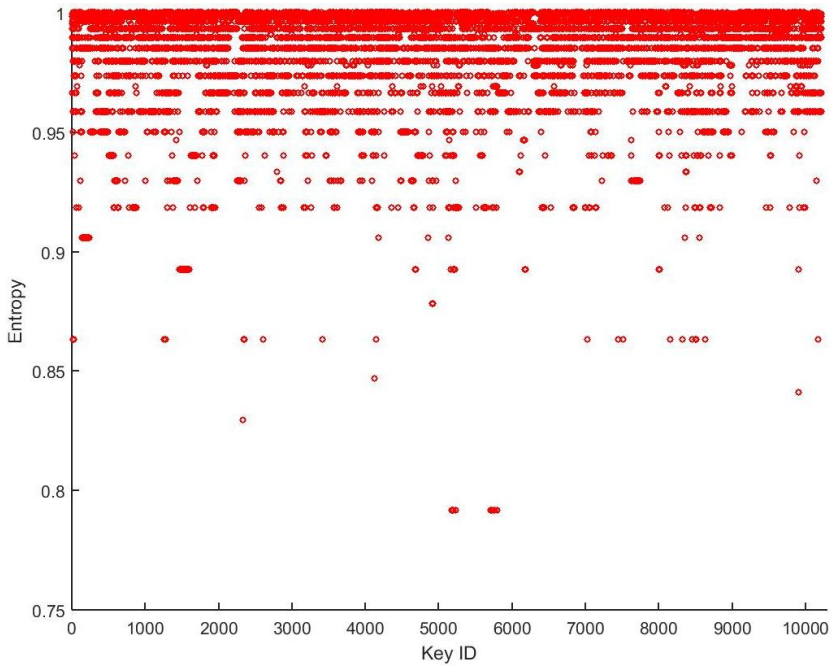


Randomness-Shannon's Entropy

2^{nd} dataset

- All keys' entropy
  $Hash(x||y||type)$
- Minutiae' entropy
  $(x||y||type)$





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) $\rightarrow$ the more different keys

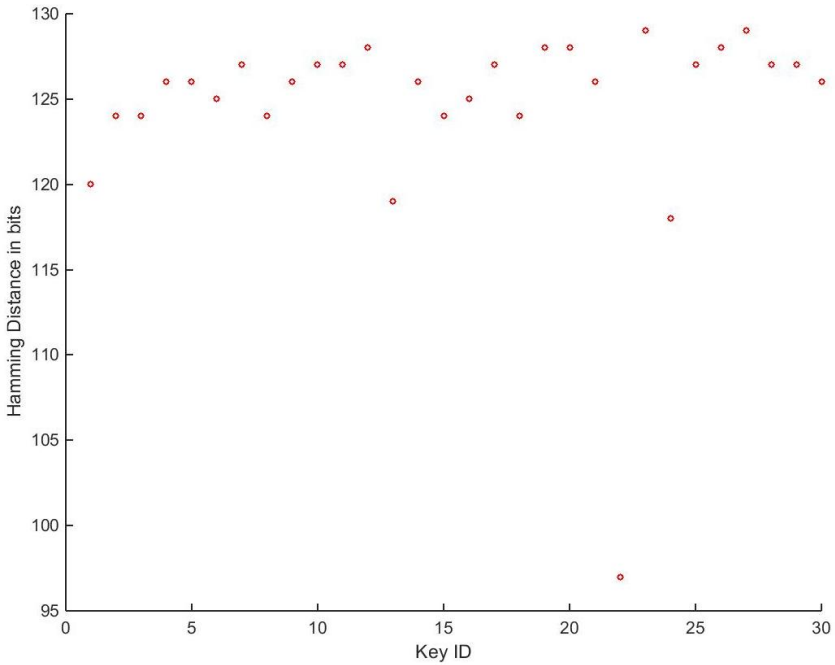
Distinctiveness-Hamming Distance

- 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) $\rightarrow$ the more different keys

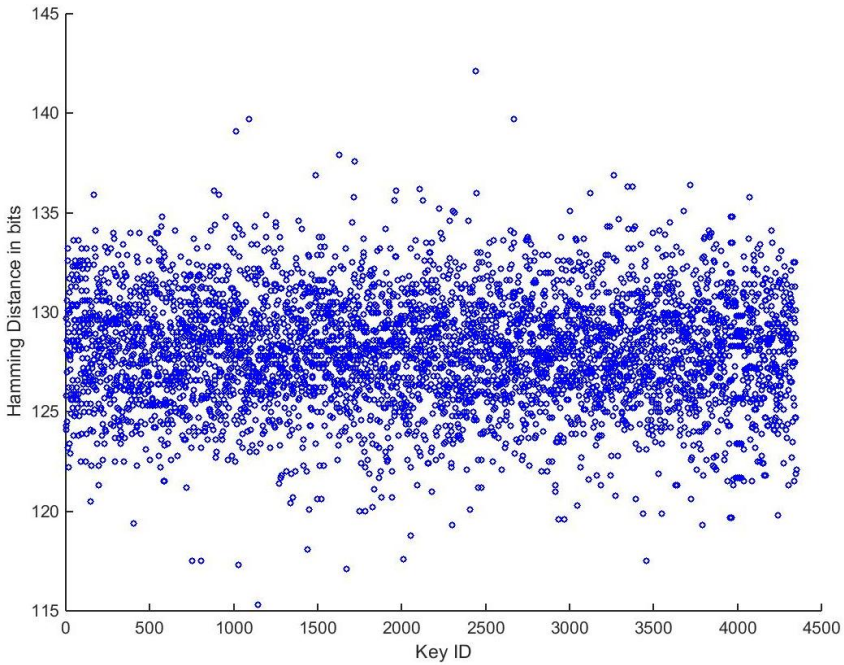
Distinctiveness-Hamming Distance

1^{st} dataset

- Same user's keys



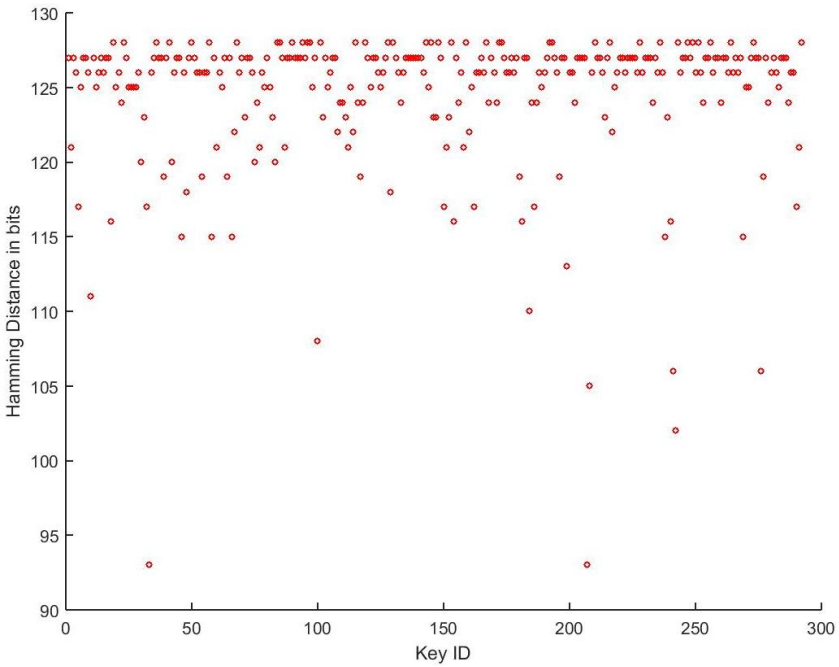
- Different users' keys



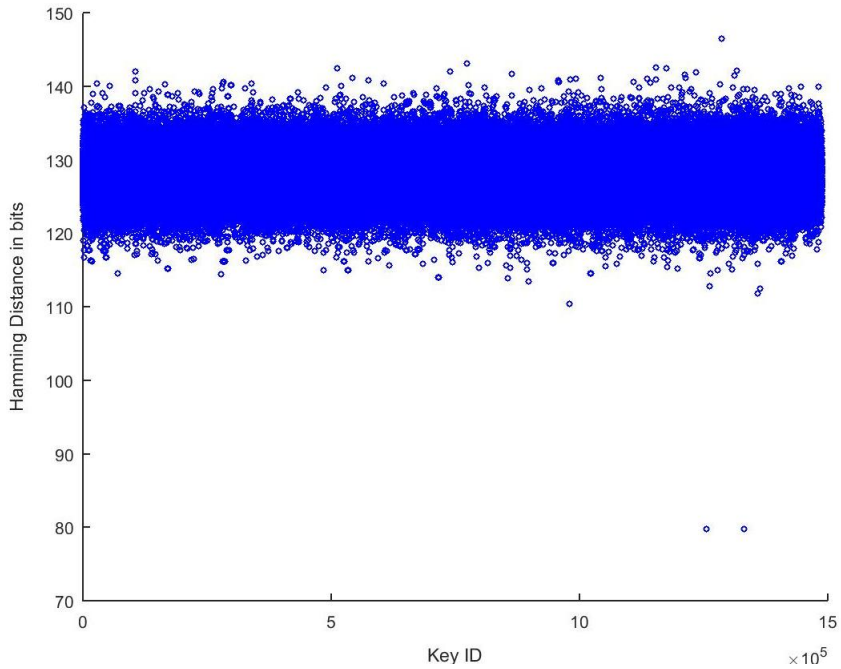
Distinctiveness-Hamming Distance

2^{nd} dataset

- Same user's keys



- Different users' keys



Computational Complexity

$$\sum_{i=n_{com}}^{n_{com}^{key}} \binom{n_{com}}{i}$$

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

n_{com}^{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

$$\sum_{i=n_{com}}^{n_{com}^{key}} \binom{n_{u}}{i}$$

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 $\tilde{=}$ 22.4 MB
  - 2^{nd} Dataset $\tilde{=}$ 332.8 KB
- Total size of the messages sent by the user
  - 1^{st} Dataset $\tilde{=}$ 13.75 KB
  - 2^{nd} Dataset $\tilde{=}$ 17.2 KB

Memory Requirements

1^{st} Dataset

- Server side
  - Average storage is 578.8 KB per subject
- User side
  - Average storage is 15 KB for each user

2^{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 $\Rightarrow$ 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

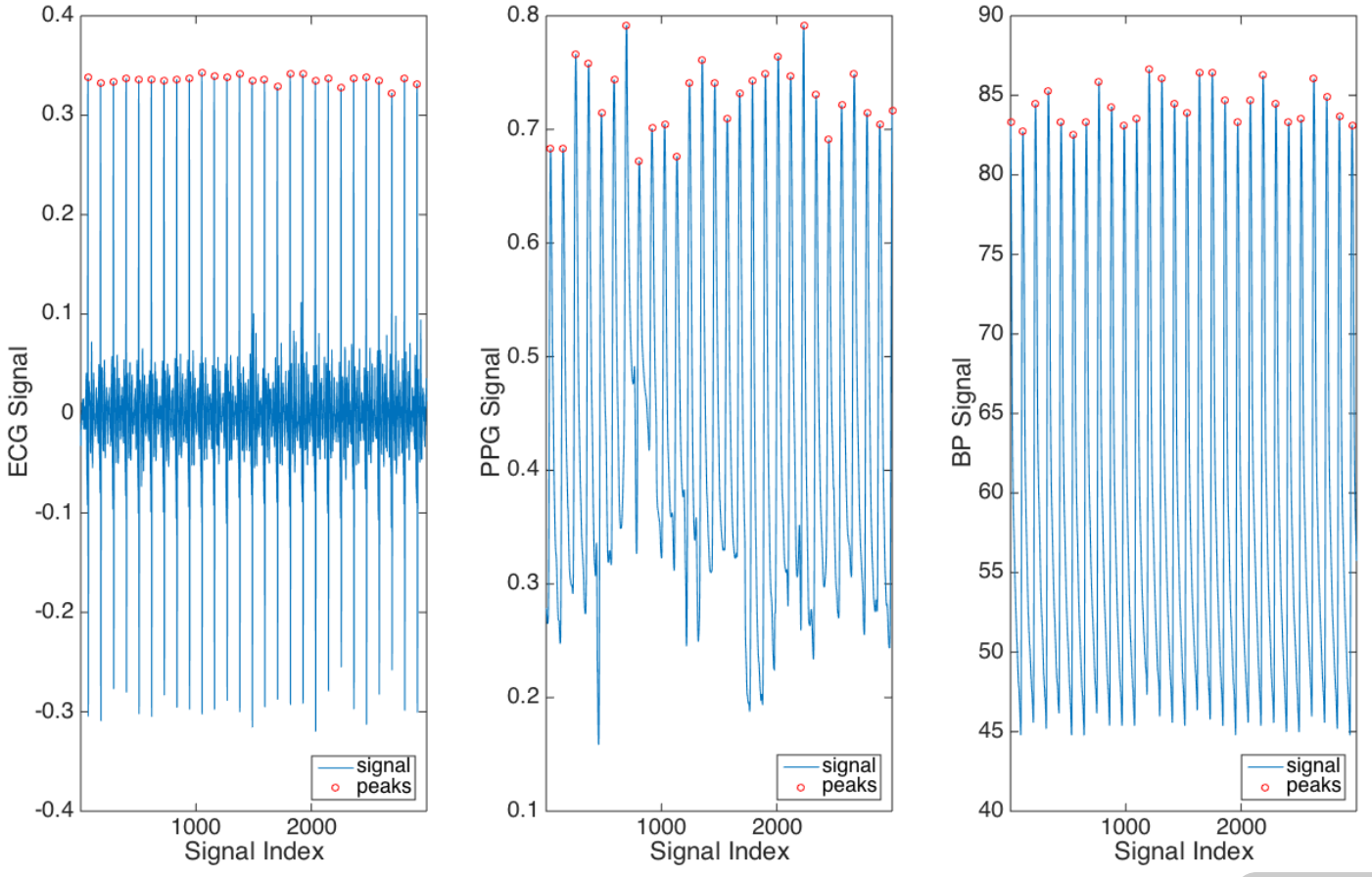
- Duygu Karaoğlan Altop was supported by TÜBİTAK BİDEB 2211-C and Turkcell Academy Technology Leaders Graduate Scholarship Program

- Dilara Akdoğan was supported by TÜBİTAK BİDEB 2228

THANK YOU!

Example: IPI Peak Points

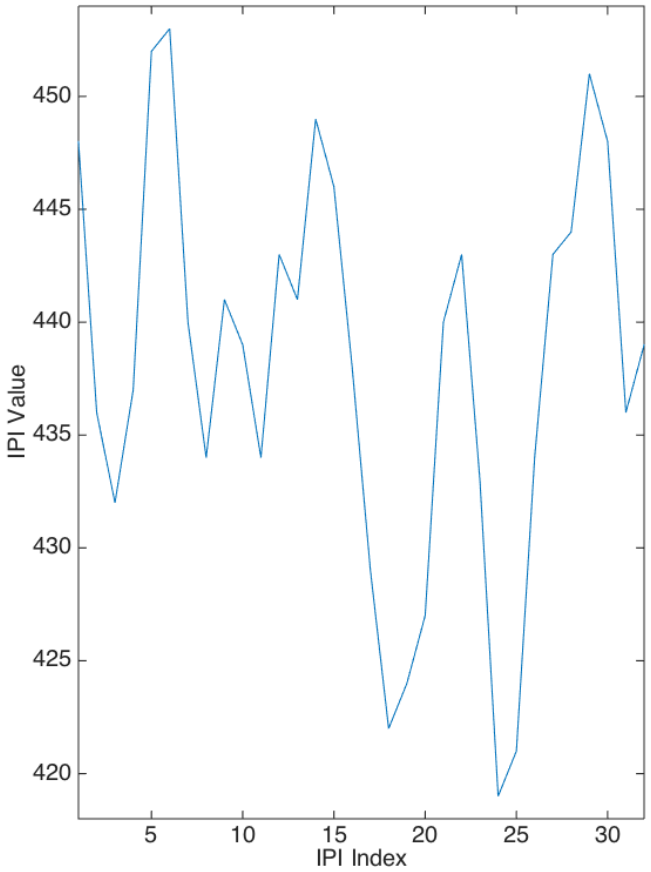
- FFT filtering and Matlab's *findpeaks* function
- Manual accuracy check $\rightarrow$ working correctly 100%

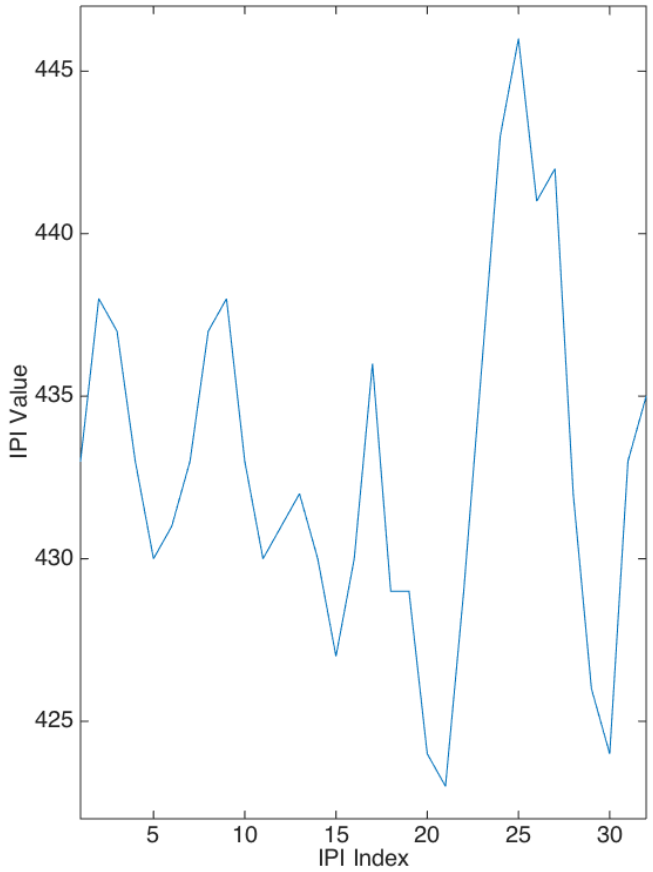


BACK

Example: IPI Sequence

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

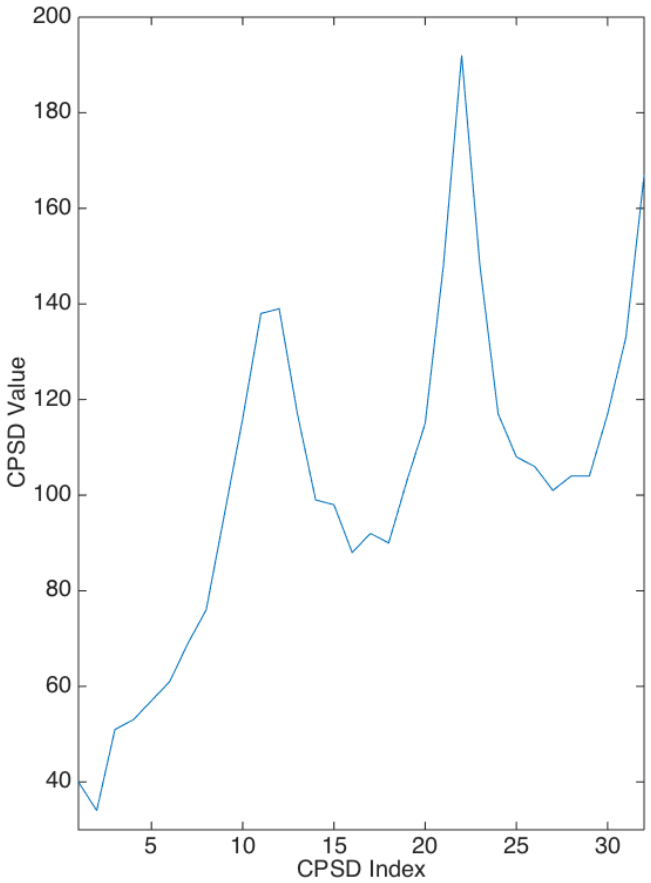


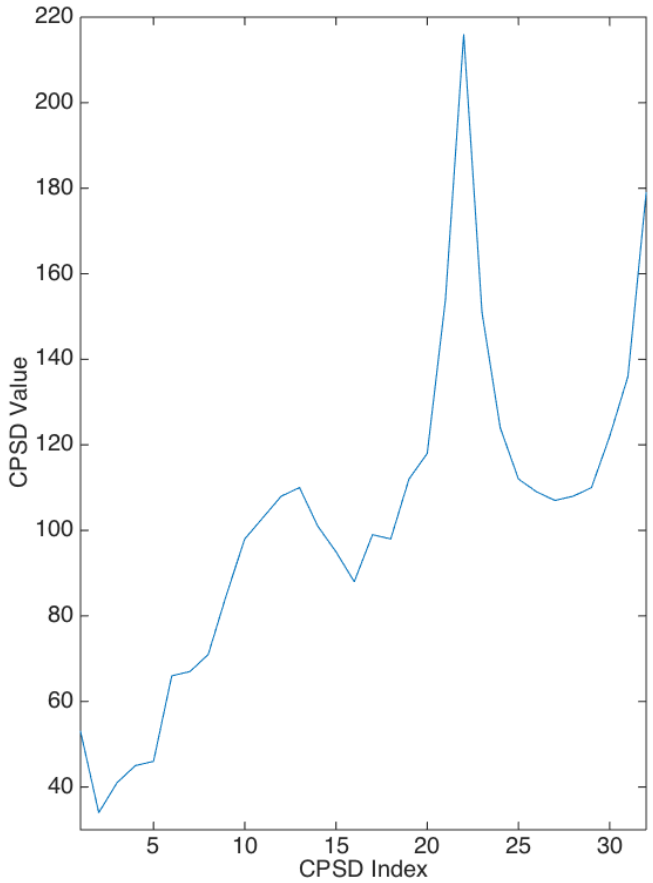


BACK

Example: CPSD Sequence

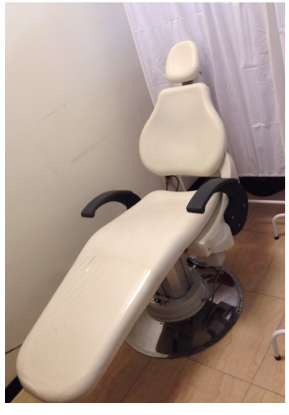
- Generated CPSD sequences - just before quantization
  - $l = 128,\ g = 4 \Rightarrow$ CPSD sequence length: 32
  - From 2 different users' BP signals

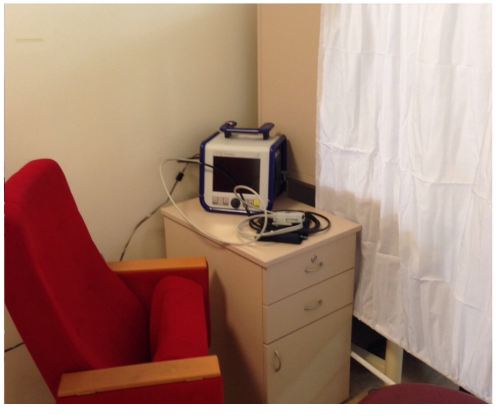




BACK

SU-PhysioDB Dataset Details





SU-PhysioDB Dataset Details





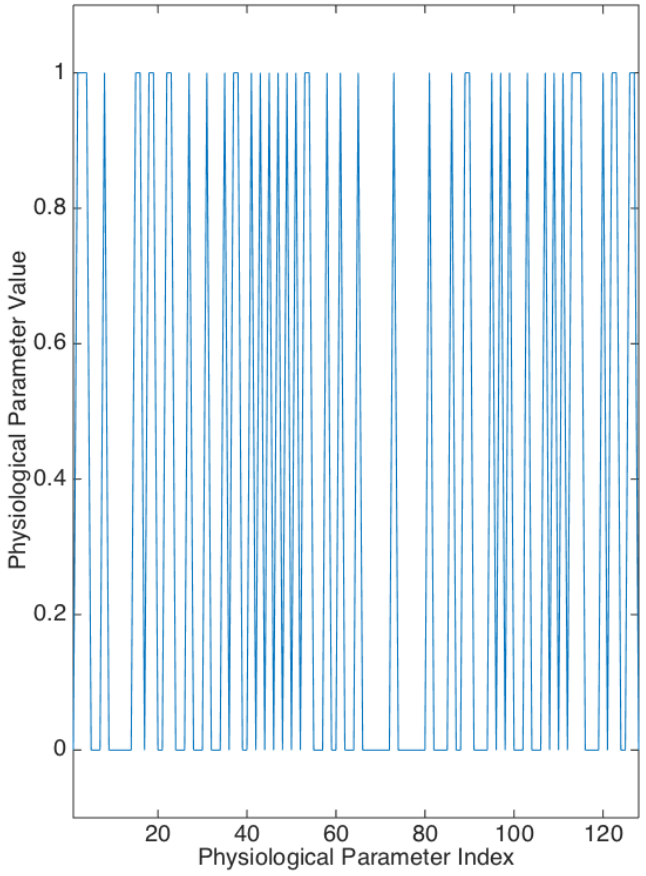


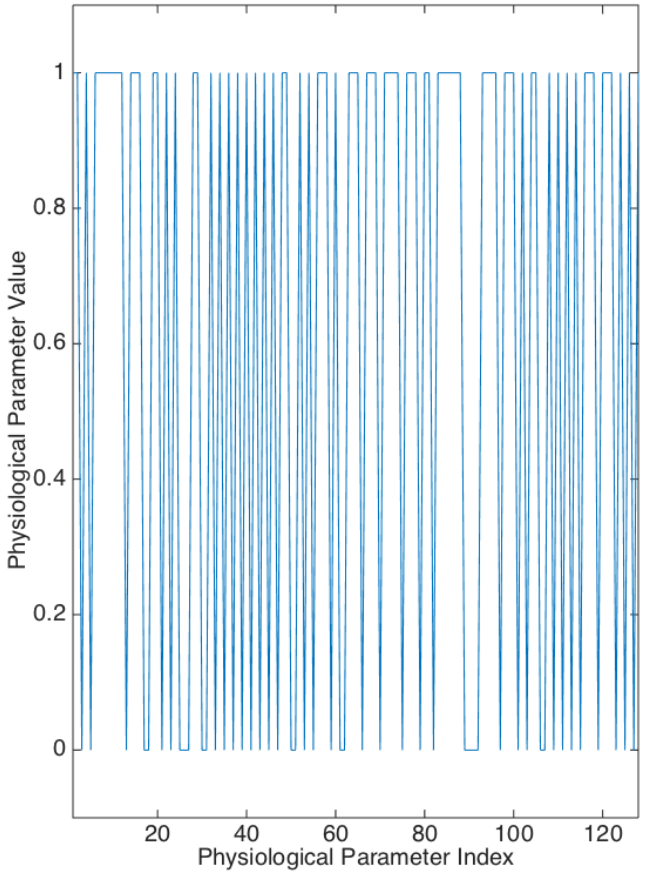

SU-PhysioDB Dataset Details

BACK

Example: IPI-based Physiological Parameter

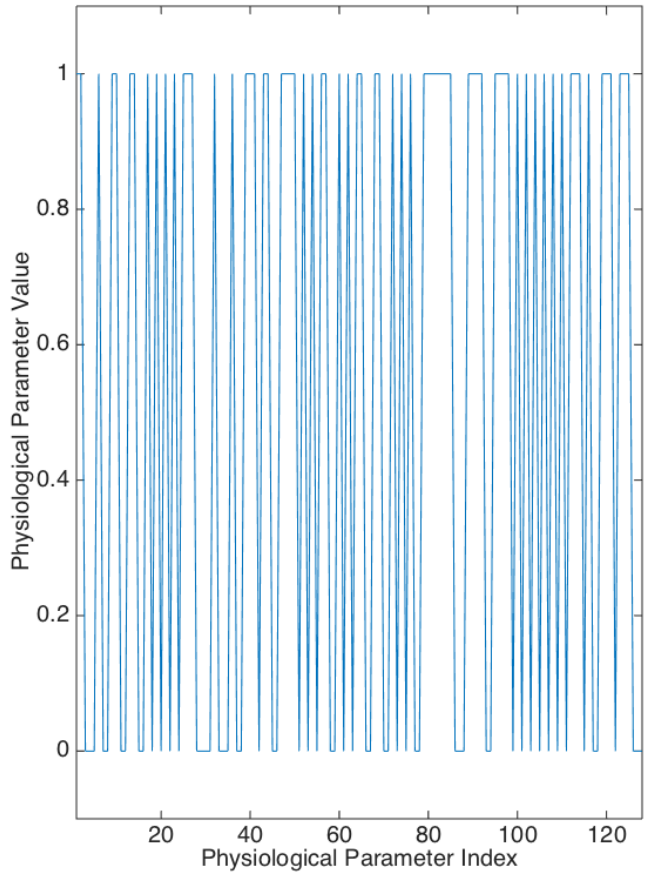
- Generated IPI-based physiological parameters
  - $l = 128,\ g = 4,\ s = 4$
  - From 2 different users' BP signals

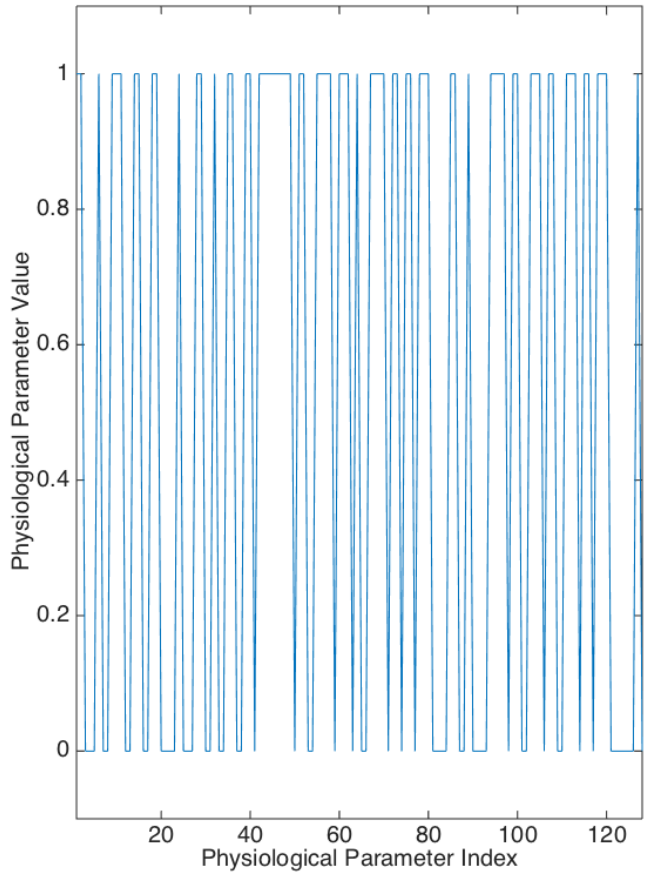




Example: CPSD-based Physiological Parameter

- Generated CPSD-based physiological parameters
  - $l = 128,\ g = 4,\ s = 9$
  - From 2 different users' BP signals

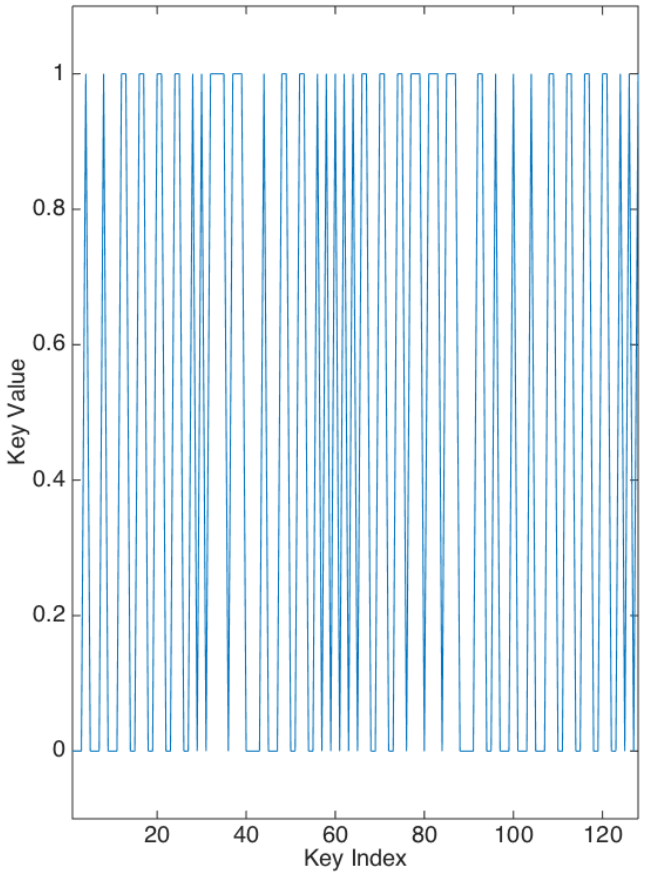


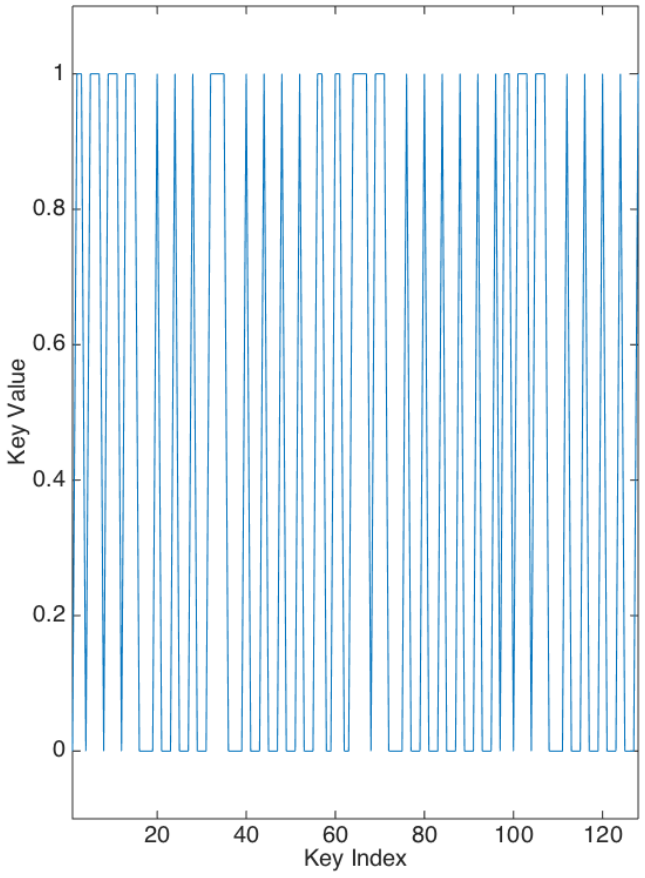


◂ BACK

Example: Agreed Symmetric Key

- Agreed symmetric cryptographic keys
  - From 2 different users' BP signals





BACK

Protocol Parameters

- s should not be too large
  - Output: $(4 * s * b)$-bit cryptographic keys
    - Key strength: 2^{4*s*b}
    - 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

r	s	d	**Effective Key Length (bits)**
11	4	1	≈ 131
7	8	2	≈ 132
		3	

Security Analysis - Threat Model

- Attacker's aim: learn the key or impersonate
- Secure channel is not assumed $\Rightarrow$ 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

Security Analysis - Resistance Against Attacks

- Brute-force attack
  - Classical brute-force
    - $(4 * s * b)$-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*r}

r	s	**Resistance Against Brute-Force**
11	4	2^{176}
7	8	2^{224}

- 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] $\Rightarrow$ IPI of PPG/ECG signals
  - Divide IPI into segments $\rightarrow$ map into binary words
- Bao et al.[2] $\Rightarrow$ IPI of PPG/ECG signals
  - Divide IPI into segments $\rightarrow$ accumulate $\rightarrow$ randomize $\rightarrow$ map into binary words

Method	Key Length (bit)	HTER
Poon et al.	128	4.26
Poon et al.	64	6.98
Bao et al.	64	2.83
Our Methods (max. CPSD-based)	128	0.135

[1] C. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health", *IEEE Communications Magazine*, 2006.

[2] S.-D. Bao, C. Poon, Y.-T. Zhang, and L.-F. Shen, "Using the timing information of heartbeats as an entity identifier to secure body sensor network", *IEEE Trans. on Information Technology in Biomedicine*, 2008.

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: $\binom{|S_C|}{v+1}$
  - Vault security: $\binom{|R|}{v+1}$
- 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: $\binom{m+s}{t+s}$

[3] K. K. Venkatasubramanian, A. Banerjee, and S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks", in *IEEE Trans. on Information Technology in Biomedicine*, 2010.

[4] K. K. Venkatasubramanian, A. Banerjee, and S. Gupta, "Plethysmogram-based secure inter-sensor communication in body area network", in *Proceedings of MILCOM*, 2008.

[5] F. Miao, L. Jiang, Y. Li, and Y.-T. Zhang, "Biometrics based novel key distribution solution for body sensor networks", in *Proceedings of IEEE EMBS*, 2009.

[6] J. Shi, K.-Y. Lam, M. Gu, M. Li, and S.-L. Chung, "Towards energy-efficient secure communications using biometric key distribution in wireless biomedical healthcare networks", in *Proceedings of BMEI*, 2009.

Related Work - Key Agreement Protocol

- Fuzzy Vault $\Rightarrow$ 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 $\Rightarrow$ IPI of ECG signals
  - $t \leq S_S \cap S_C \ \ \& \ \ 2(m-t) < m \Rightarrow 16 < t \leq 17$
  - Attack complexity: $\binom{m+s}{t+s}$

Method	Key Length (bit)	HTER (%)	Attack Complexity
Fuzzy Vault	124	9.65	2^{147}
Set Reconciliation	128	28.33	2^{47}
SKA-PS	131	2.53	2^{176}